МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ И ВЫСТАВКА

Организаторы

РОССЕТИ

РусГидро

АО «СО ЕЭС»
RUSSIAN POWER
SYSTEM OPERATOR

cigre
Россия

EXPO
Электрификация

При поддержке

МИНИСТЕРСТВО ЭНЕРГЕТИКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

cigre
SC B5

Научно-технический партнер

ВНИИР

РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ – 2021

29 сентября – 1 октября

г. Москва, ВДНХ, пав. № 55

СБОРНИК ДОКЛАДОВ

I ТОМ

Официальный партнер

30 ЭКРА

www.rza-expo.ru

ПРОГРАММНЫЙ КОМИТЕТ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ И ВЫСТАВКИ «РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ – 2021»

А.В. Жуков (АО «СО ЕЭС») – **председатель**

Г.С. Нудельман (ОАО «ВНИИР») – **зам. председателя**

J. Zakonjsek (CIGRE SC B5, Relarte Ltd., Slovenia) – **ученый секретарь**

A. Apostolov (PAC World, USA)

A. Bonetti (MEGGER Sweden AB, Sweden)

J. Cardenas (CIGRE SC B5, Spain)

P. Crossley (University of Manchester, UK)

D. Dolezilek (SEL, USA)

R. Loken (CIGRE SC B5, Norway)

I. Patriota de Siqueira (CIGRE SC B5, Brazil)

U. Rudež (University of Ljubljana, Slovenia)

V. Terzija (Center for Energy Science and Technology Skoltech, Russia)

А.А. Волошин (НИУ «МЭИ»)

В.С. Воробьёв (АО «СО ЕЭС»)

Н.А. Дони (ООО «НПП ЭКРА»)

Д.М. Дубинин (АО «СО ЕЭС»)

А.Л. Куликов (НГТУ им Р.Е. Алексеева)

А.А. Лисицын (АО «НТЦ ЕЭС»)

А.П. Морозов (ПАО «РусГидро»)

А.И Расщепляев (АО «СО ЕЭС»)

А.В. Саленов (ПАО «Россети»)

Е.И. Сацук (АО «СО ЕЭС»)

А.Г. Фишов (НГТУ)

В.С. Шевелев (ООО «Релематика»)

Том 1.

Содержание:

Секция 1: «Разработка, проектирование, наладка и эксплуатация РЗА ЦПС: опыт и практические результаты»

1.1. Опыт работы с технологической шиной в соответствии с МЭК 61850 в проекте НИОКР цифровой подстанции Statnett R. Loken (Statnett, Норвегия)
……..9 стр.

1.2. Применение оптических трансформаторов тока в проекте НИОКР цифровой подстанции Statnett R. Loken (Statnett, Норвегия)
……18 стр.

1.3. Оптические/Цифровые подстанции J. Cardenas (Adneli Consultant, Испания)
……23 стр.

1.4. Технические решения по применению оптических трансформаторов при построении цифровых подстанций. Опыт реализации. Преимущества и существующие проблемы М.А. Янин (АО «Профотек», Россия)
……40 стр.

1.5. Практика и перспективы применения цифровых измерительных трансформаторов тока и напряжения для релейной защиты и автоматики В.Д. Лебедев., А.А. Яблоков, Г.А. Филатова, Н.В. Кузьмина, А.В. Панащатенко, Е.С. Шагурина (ИГЭУ, Россия)
…… . ……..58 стр.

1.6. Опыт наладки и эксплуатации ЦПС 330 кВ «Металлургическая» Е.А. Войтенко (РУП «Гомельэнерго», Белоруссия)
……69 стр.

1.7. Оптимизированная архитектура ЦПС. Опыт внедрения цифровых систем защит и управления в распределительных сетях Н.Н. Дорофеев (ООО «ПиЭлСи Технолоджи», Россия)
……77 стр.

1.8. Разработка кластерной цифровой подстанции с функционально-динамической архитектурой Д.М. Фербиков, М.А. Хлыстов, Р.В. Неуступкин (АО «РАСУ», Россия)
……82 стр.

1.9. Опыт наладки и эксплуатации МП устройств РЗА на ЦПС Е.П. Егоров, И.А. Кошельков, М.А. Хе, Н.А. Тойдеряков (ООО НПП «ЭКРА», Россия)
……90 стр.

1.10. Особенности испытаний РЗА ЦПС на разных этапах «жизненного цикла» А.С. Шалимов (ООО НПП «Динамика», Россия)
……..101 стр.

1.11. Синхронизация времени интеллектуальных электронных устройств на подстанциях Р.С. Плакидин, П.В. Сеитов, В.Н. Бовыкин (ООО ИЦ «Энергосервис», Россия)
…….....108стр.
1.12. Метрологические характеристики и опыт внедрения преобразователей аналоговых сигналов Р.С. Плакидин, С.А. Пискунов, Д.Н. Попов, А.С. Соснин, А.В. Мокеев (ООО «Инженерный центр «Энергосервис», САФУ, Россия)
……..121 стр.

1.13. Способы передачи GOOSE сообщений между подстанциями для решения задач РЗ и ПА В.А. Харламов, С.Е. Романов, А.Х. Хасанов (ООО «Юнител Инжиниринг», Россия)
……..132 стр.

1.14. От проекта до объекта. Вызовы при реализации ЦПС и пути решения П.Г. Варганов, Н.В. Паршиков, Д.А. Удиков, А.Н. Донской (АО «ЧЭАЗ», Россия)
……..143 стр.

1.15. Автоматический синтез оптимальных проектных решений по построению РЗА ЦПС А.А. Волошин, Е.А. Волошин, Н.П. Грачева (Центр НТИ МЭИ, Россия)
……..149 стр.
1.16. Информационно-инструментальное средство сопровождения процесса проектирования ИТС (РЗА и АСУТП) С.П. Воробьев (АО «СиСофт Девелопмент», Россия)
……..158 стр.

1.17. Система удаленного мониторинга состояния и работы устройств РЗА Ю.В. Романов, О.А. Федоров, Д.С. Добрыдень, Д.В. Ясько (АО «РТСофт», ПАО «Россети», АО «СО ЕЭС», Россия)
……..166 стр.
1.18. Опыт внедрения цифровой релейной защиты различных производителей на полигонах ЦПС ПАО «Газпром Нефть» М.С. Завгородний (АО «Электронмаш», Россия)
…….176 стр.
1.19. Опыт разработки и применения файлов SCD в течение жизненного цикла ЦПС А. А. Клепиковский (КЭР Инжиринг), Н.В. Мараракина (ООО «ТЕКВЕЛ», Россия)
……..183 стр.
1.20. Практический опыт пусконаладки и ввода в эксплуатацию цифровых подстанций 3-й архитектуры В.В. Боровицкий (АО «ТЮМЕНЬЭНЕРГО», Россия), Д.О. Афанасьев Денис (ООО «ТЕКВЕЛ», Россия)
…….190 стр.
1.21. Кросс-платформенные решения для РЗА ЦПС А.А. Волошин, Е.А. Волошин, А.С. Холодов, Е.И. Рогозинников, А.К. Рыжков (Центр НТИ МЭИ, Россия)
…….206 стр.

1.22. Возможности применения облачных технологий для автоматизации функциональных испытаний систем РЗА ЦПС А.А. Лебедев, Д.О. Благоразумов (Центр НТИ МЭИ, Россия)
…….212 стр.

Секция 2: «Перспективы развития и применения стандарта МЭК 61850»

2.1. Проверка электронной проектной документации в формате файлов SCD для цифровых подстанций: требования и практический опыт Семеренко А.А., Третьяков Д.А. (ПАО «МРСК

Волги», Россия), Головин А.В., Аношин А.О. (ООО «ТЕКВЕЛ Разработка», Россия), Родни Хьюес (Rod Hughes Consulting Pty Ltd, Австралия
…….220 стр.

2.2. Повышение эффективности испытаний на цифровых подстанциях А. Апостолов (Omicron, США)
……..231 стр.

2.3. Опыт сертификации устройств соответствию требованиям стандарта МЭК 61850 М.Д.Ильин (АО «НИЦ ЕЭС», Россия)
……..248 стр.

2.4. Маршрутизируемые GOOSE-сообщения и их применения в системах противоаварийной автоматики А. Апостолов (Omicron, США)
……..254 стр.

2.5. Программный комплекс для оценки соответствия технических решений РЗА и АСУ ТП требованиям конкурсной документации М,И. Шведов (ОАО «МРСК Урала», Россия)
……..266 стр.

2.6. Особенности организации эксплуатации систем РЗА и АСУ ТП в условиях использования стандарта МЭК 61850 М.Н. Хабибуллин, А. Туитяров (ОАО «Сетевая компания», Россия)
……..274 стр.

2.7. Анализ и перспективы применения стандарта МЭК 61850 для ГЭС и ГАЭС Д.А.Жуков (ПАО «РусГидро», Россия), А.В. Головин (ООО «ТЕКВЕЛ», Россия)
……..278 стр.

2.8. Разработка формализованных функциональных требований к логическим узлам А.А. Волошин, А.А. Лебедев, Д.О. Благоразумов, В.А. Вальгер, Б.А. Сафронов, М.А. Хлыстов, А.С. Худяков, Р.В. Неуступкин, В.О. Болошин (ФГБОУ ВО «НИУ «МЭИ», АО «РАСУ», Россия)
……..291 стр.

2.9. Применение расширенного профиля передачи мгновенных значений аналоговых сигналов для дифференциальной защиты линии А.Н. Подшивалин, И.А. Капустина (ООО « Релематика» Россия)
……..302 стр.

Секция 3: Кибербезопасность – драйвер или тормоз развития?

3.1. Принципы реализации кибербезопасных решений для кроссплатформенной РЗА В.М. Зинин, Т.Р. Шарафеев, А.Л. Куликов (АО «НИПОМ», НГТУ им. Р.Е. Алексеева, Россия)
……..310 стр.

3.2. Технологии РЗА ЦПС, обеспечивающие повышенную устойчивость к кибератакам А.А. Волошин, Е.А. Волошин, С.М. Нухулов, В.И. Добринын, Д.О. Благоразумов (Центр НТИ МЭИ, Россия)
……..318 стр.

3.3. Практические аспекты внедрения требований безопасной разработки программного обеспечения для цифровой подстанции Е.А. Плетнева (АО «РАСУ», Россия)
……..329 стр.

3.4. Вопросы реализации доверенных Интеллектуальных Электронных Устройств В.Г. Карантаев (АО «Лаборатория Касперского», Россия)
……..336 стр.

3.5. Мониторинг цифровых энергообъектов А.А. Бондюгин (АО «Лаборатория Касперского», Россия)
……..343 стр.

3.6. Информационная безопасность РЗА и автоматизированных систем в электроэнергетике. Теория и практический подход Н.А.Дони, Р.В. Разумов, И.А. Кошельков, Д.В. Митрофанов (ООО НПП ЭКРА», Россия)
……..348 стр.

3.7. Особенности реализации устройств серии БЭМП в соответствии с требованиями к КИИ Н.В. Паршиков, И.А. Евграфов (ООО «НИЦ ЧЭАЗ», Россия)
……..356 стр.

3.8. Переход из системы координат «целостность, конфиденциальность, доступность» в систему координат «недоотпуск, время восстановления, ущерб» А.А. Волошин, Н.С. Лебедева (Центр НТИ МЭИ, Россия)
……..362 стр.

3.9. Должны ли мы применять методы информационной безопасности для распределительных сетей: вызовы и решения E. Weerathunga, A. Appukuttan, M. Kanabar, H. Bhatia, A. Chulkov (GE Renewable Energy, Великобритания, Россия)
……..374 стр.

3.10. Кибербезопасность, как необходимое условие цифровизации электроэнергетики Е.Л. Генгринович, (АО «ИнфоТеКС», Россия)
……..385 стр.

3.11. Актуальные направления развития нормативной базы в области обеспечения кибербезопасности систем промышленной автоматизациии Д.И. Правиков (РГУ нефти и газа (НИУ) имени И.М. Губкина, Россия)
……..389 стр.

3.12. Разработка микропроцессорных устройств РЗА. Требования информационной безопасности к процессу разработки А.А. Ларюхин (ООО «Интеллектуальные Сети», Россия)
…….393 стр.

3.13. «Мультишина 10G» цифровой подстанции - потенциальные проблемы, перспективы применения и возможности развития цифрового энергообъекта А.С. Шеметов, М.В. Никандров (ПАО «ФСК ЕЭС», ООО «Интеллектуальные Сети», Россия)
……..400 стр.

3.14. Вопросы и решения по информационной безопасности цифровых систем релейной защиты и автоматики электрических сетей А.В. Петухов (НТИ Энерджинет, Kaspersky, Россия)

……..408 стр.

3.15. Мониторинг защищенности и управление кибербезопасностью энергообъектов. Подходы и решения Д.А. Даренский, (Positive Technologies, Россия)
……...415стр.

3.16. Реализация требований к защите информации в энергосистемах с использованием встроенных решений .В. Крутских (ООО «ПиЭлСи Технолоджи», Россия)
……..422 стр.

СЕКЦИЯ 1.

«Разработка, проектирование, наладка и эксплуатация РЗА ЦПС: опыт и практические результаты»

1.1. CURRENT TRENDS AND CONCEPTUAL ISSUES OF PA SYSTEMS DEVELOPMENT: APPLICATION PRACTICE OF IEC 61850 STANDARD

Experience with IEC 61850 Process Bus in Statnett R&D project Digital Substation

R. LOKEN
Statnett
Norway

Contact person:
Rannveig Loken
rannveig.loken@statnett.no

Keywords: IEC 61850 - Digital Substation - Process bus –Topology – Network - Testing – IED –
Interoperability - Optical CT

Abstract:

A Digital Substation based on IEC 61850 9-2 [1] process bus is a complex system where Intelligent Electronic Devices (IEDs) interact with primary equipment and run both local and distributed software application functions. These functions are based on the exchange of information over the process bus and the station bus. The increasing levels of functional integration result in the development of many multifunctional IEDs that require interfaces with multiple primary devices.

The objective of the pilot project, Digital Substation [2], was to gain experience with Non-Conventional Instrument Transformers (NCIT) and process bus installations including interoperability issues. Further objective of the Digital Substation was to challenge some traditional Protection, Automation and Control System (PACS) design principles and investigate if such new ideas are feasible and also manageable from an operational point of view. Examples of investigated new principles:

- Use of one common Intelligent Electronic Device (IED) for protecting and controlling two transmission lines.
- Embedding protection and control functions to a Linux computer capable of protecting and controlling multiple transmission lines.

This paper will discuss aspects related to testing of the IED that includes protection and control for two transmission bays. The traditional hardwired test plug will not fulfil the requirements for the new design. Instead, the IEC 61850 offers a range of testing facilities that are investigated in this project. Ideally, it should be possible to test the protection functions for the different bays independently during all stages of testing.

1. Introduction

Statnett initiated a Digital Substation project based on IEC 61850 9-2 [1] aiming to gain experience and knowledge concerning concepts of a digital substation with Non-Conventional Instrument Transformers (NCIT) and a process bus, to become familiar with the technology and to additionally investigate the benefits this technique offers for future substation projects [2]. The Digital Substation, as shown in Fig. 1, is installed in a live 300kV line bay in parallel with an already existing PACS, unable to operate the live breakers of the overhead line. The conventional current and voltage measurements are connected to the Digital Substation from the existing PACS. The NCIT is connected in series with the existing conventional current transformer in the overhead line. It is possible to operate and monitor the Digital Substation through the dispatch centre.

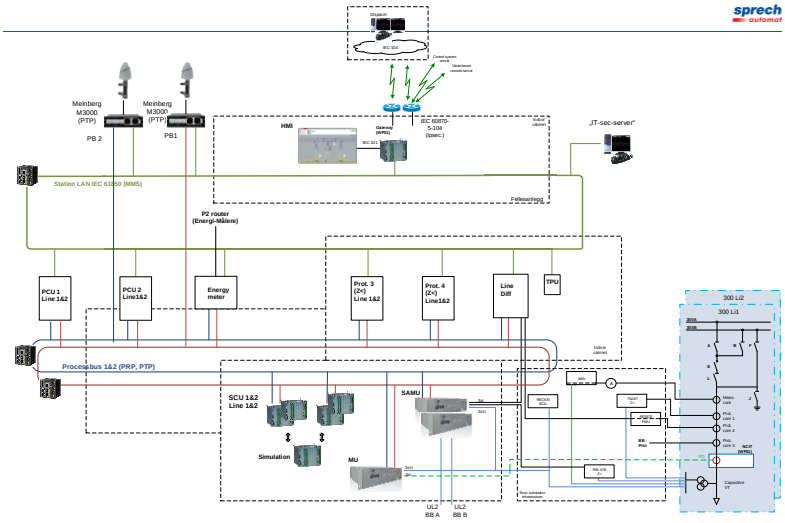


Fig. 1: Simplified Digital Substation topology and connection to existing PACS

The Digital Substation pilot includes protection and control functions for two 300 kV transmission lines in the same IED hardware (hereafter named Protection and Control Unit - PCU). This compact design challenges the traditional philosophy for Statnett transmission systems where protection and control functions are divided into separate hardware units.

The objective of this compact solution in the Digital Substation was to investigate if the PCU's are capable of processing two bays in parallel and if possible, to test protection for one line without affecting the operation of the other. Further, is controlling two line bays from one common PCU is manageable from an operational point of view. To achieve this, it was necessary to define the bay controller and protection functionalities of the PCU as independent and separate logical devices, each of which consists of a number of logical nodes.

This paper will discuss aspects related to topology and time synchronization in a Digital Substation. It will also include some experience from testing and operation of the Digital Substation.

2. Digital Substation Topology

A crucial characteristic of the Digital Substation is the level of interoperability between IEDs from different vendors [3]. Normally, Statnett uses two main protections for a 300kV bay, but in the Digital Substation this has been doubled to open up for investigations into the interoperability between equipment from even more vendors.

There are protection and control PCUs from three vendors in addition to an optical Current Transformer (CT) and Merging Units (MU), an energy meter (kWh), a Teleprotection Unit (TPU), and Global Positioning System (GPS) clocks, in addition to a Switchgear Control Units (SCU) and a Process Simulator. Fig. 2 below illustrates the topology of the Digital substation for practical purposes.

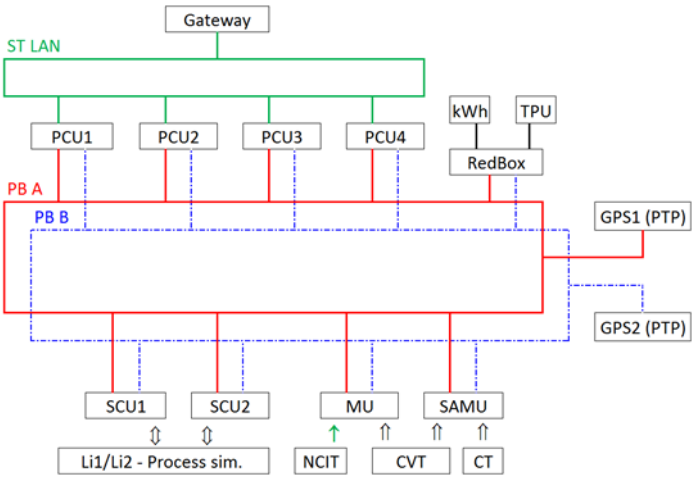


Fig. 2: Digital Substation Topology

The approach has been to combine many functions in a restricted number of PCUs. With reference to Fig. 2, the main Protection and Control Unit (PCU1) was configured with both the Bay Control Unit (BCU) and the protection functionality for two separate lines. Each of the bay control parts includes breaker closing functions such as synchro check, dead bus/dead line logic, and Automatic Reclosing (AR).

In this project, control of both lines was realised in the same display of the PCU, and there was no control from the Human-Machine Interface (HMI) panel. The HMI panel was used to get an overview of the full Digital Substation.

The back-up PCU2 was based on protection firmware implemented on a Linux based industry computer. PCU2 was similarly configured with control and protection for the same two bays, but was active as the bay controller only when the main PCU1 was in one of several failure modes. Although PCU2 is active as the bay controller only when PCU1 fails, protection functions from all the PCUs are of course active and operating in parallel at all times. PCU3 was configured with distance protection for lines 1 and 2, as well as Phasor Measurement Unit (PMU) functionality for line 1, and PCU4 contained distance protection for line 1.

One of the main challenges for the Digital Substation concept was to make the system fulfil the requirements on availability as we have today. In the Digital Substation, this was realised with process bus based on Parallel Redundancy Protocol (PRP) network redundancy technology, as shown in Fig. 2 above.

Redundancy for tripping and operation of the breaker was ensured by two SCUs. With the exception of the trip commands, which are always sent to both SCUs, PCU1 and PCU3 rely on SCU1 for operation and indications, whereas PCU2 and PCU4 rely on SCU2. PCU2 and PCU4 are fully independent from PCU1 and 3, and have auxiliary voltages from different circuits.

Time synchronization is an essential aspect of process bus applications and the system is synchronized from two time sources, GPS1 and GPS2, using the Precision Time Protocol (PTP) v2 to ensure 1µs accuracy.

The Sampled Values (SV) streams from the Merging Units (MU/ Stand-Alone Merging Unit (SAMU)) are currents and voltages measured on a real transmission line and bus bar, but the station

control units are operating only on a process simulator. SV streams, according to IEC61850-9-2LE with 80 samples per cycle (F4000S1I4U4), are used for metering, protection and control functions.

In this project, Line 1 and Line 2 are in reality the same line. With both an optical and a conventional current transformer measuring on one and the same, real transmission line, it is possible to see if there is a difference in protection response to the two measuring methods. Therefore, the different PCUs were configured to use SV streams from optical and conventional current transformers for the two lines in a PCU.

An additional benefit is that this distribution of SV streams also ensures redundancy in the measurement chain, and hence a single failure of an IED, an SCU or a merging unit does not lead to any restriction for the control (or protection) of the lines - control is available either via PCU1 or PCU2. In case of a double failure in both chains (MU/SAMUs/SCUs), the control and protection functionality is lost (as is the case in the current conventional solution with main 1 and main 2 protection system).

3. Time Synchronisation

The two grandmaster clocks were initially set up as one for each Process Bus. Additional cards were later installed in the grandmaster to establish the redundancy. Substation clocks (Meinberg M3000) were set up in a fully redundant configuration, please see Figure 3. At this stage, both Grand Masters are connected to both process buses. A multi-channel measurement system monitors the timing offset of available external references against the substation clock timescale. A reference selection algorithm chooses among external references based on availability and selected priority. The local rubidium oscillator is steered to follow the substation clock timescale and may be used for extended holdover if no other acceptable external references are available. At the time of commissioning, the two substation clocks were synchronised mainly by the GPS as the main source and the backup for each was the external rubidium oscillator.

The COSECTIME project also includes the first two Statnett's Cesium clocks, termed SNCs23 and SNCs24. Both clocks were calibrated for about half a year at JV (metrological department). One of the clocks, SNCs24, was tested for its sensitivity to ambient temperature and relative humidity, while the other clock operated continuously in clock laboratory with rather stationary temperature and relative humidity to characterize its long–term stability. One of the clocks was placed in Statnett office to establish a fibre link based on IEEE1588 PTP via Statnett Optical network to the Digital Substation. When this link was established, the Meinberg clocks were reconfigured to prioritise the PTP via fibre link as first priority, GPS as the second, and Oscillator as the third one. Later in the project a local atomic clock was placed in the same control room as the Digital Substation. It was PPS between the local Cesium and the Meinberg station clock. The station clock was also reconfigured to use cesium on the Digital Substation location as a time source. Cesium clock No. 1 located at remote clock site 1 failed after 482 days of continuous operation. While the clock controller reported fatal loss of lock on the cesium resonance, the clock continued operating on its internal crystal oscillator. In a normal operational mode, the crystal oscillator is continuously disciplined/calibrated to follow long-term accuracy and stability of the cesium resonance. No system for detection/logging of cesium clock alarms has currently been implemented.

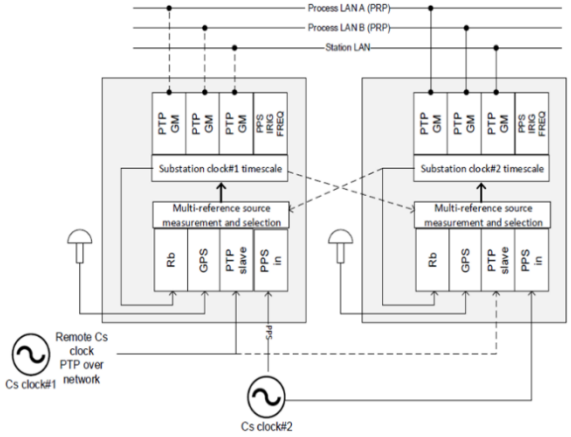


Fig. 3: Time Synchronisation and Distribution

4. Experience from testing

The tools and methods required for troubleshooting a Digital Substation are different from a PACS. At its most basic level, testing of a Digital Substation is the creation of simulated inputs to a function or device to verify the operation and performance expectations taking into account the type of test and the traffic in the communication network. When testing a Digital Substation, it is necessary to create simulated data as inputs to specific Logical Nodes or Logical Devices. In order to publish simulated data for testing, it is necessary to use a data message which the Digital Substation communication network can accept and transmit. This requires that the test system publishes messages based on the definitions of IEC 61850 and presented in the SCD file describing the Digital Substation.

In a Digital Substation, all signal voltages are replaced by GOOSE messages which are defined in the engineering phase, and if a signal is not planned or implemented, it will not be available. Special software tools are needed to listen to the process bus to see GOOSE signals and SV streams, and generally to check what happens in the system when it does not respond in the expected manner.

In a conventional station, the same test file can be used on several relays, all that is required is to reconnect the wires, but in the Digital Substation, the GOOSE configuration in the test files has to be changed as the IEDs have different names.

Another useful feature is the Sample Value Simulation Mode. If this was implemented in all PCUs, simulated SV streams could be sent to the process bus and only the PCU with Sim= TRUE would react to the simulated streams, whereas remaining PCUs would process the real SV streams. There would be no changes to the network required for testing, and in theory, testing could be conducted remotely. Unfortunately, the simulation mode is currently an optional feature in the standards and is not implemented by all vendors. This severely restricted the use of test and simulation mode during factory testing.

5. Operational Experience

During the operation phase, there have been a few experiences where the relays in the conventional station (PACS) have recorded a fault.

Start of distance protection

There was a record of a normal start in the distance protection in the PACS where both Protection 1 and 2 reacted to a fault. It was verified that all four protections PCUs in the pilot had also experienced a similar behavior with similar alarms with exactly similar time stamps.

Fault during transformer breakdown

In addition, there was an instance related to a breakdown of one of the transformers in the neighboring Frogner substation, where there was a trigger in the protections fault recorder from Furuset. The currents and voltages in fault-controlled phase L3 from PCU1 in the Digital Substation were compared with the error curves from the protection of the PACS.

All the values for current and voltages from SAMU, MU and conventional substation were superimposed with exactly the same response in that fault-control phase. This is shown in Figure 4 and Figure 5 below. Other observations were that the protection functions in the PCU1 protection have started 3 ms later than the normal protection, which may well be attributed to processing time in SAMU / MU and transmission time in the communication network.

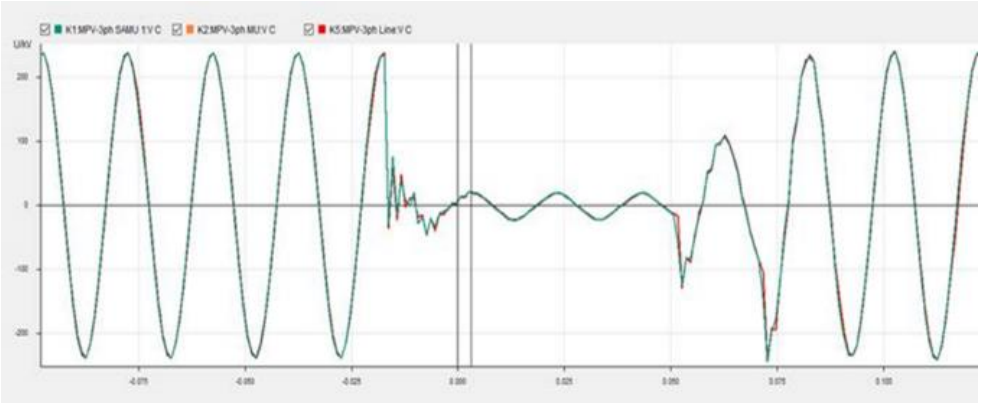


Fig. 4: Current measurements from SAMU, MU and analog

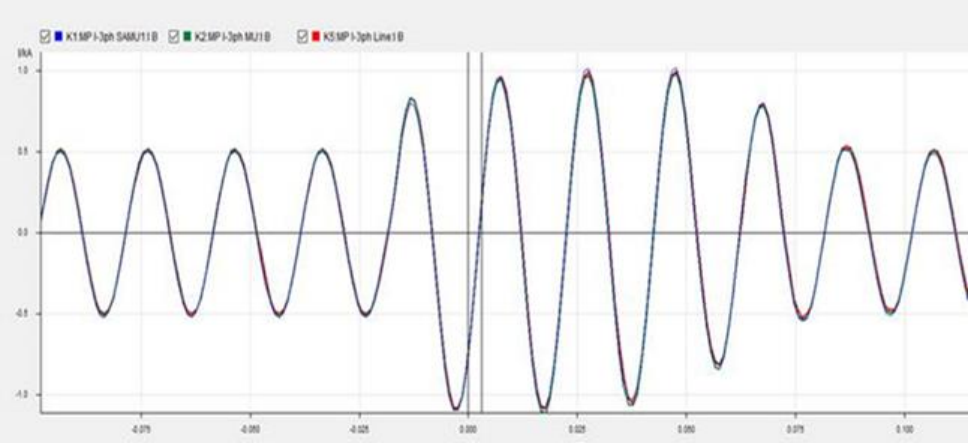


Fig. 5: Voltage measurements from SAMU, MU and analog

6. Conclusion

This paper reports practical experiences with the multivendor Digital Substation based on process bus technology. The different aspects related to topology, time synchronisation and interoperability are investigated. A different approach has been taken towards the implementation of a compact solution. Combining protection and control for two different lines, limitation and challenges, which emerge with this new technology, are also discussed.

From a communications point of view, bandwidth management control in some form is essential in order to prevent the Gigabit traffic in the trunk line from overloading the IEDs. The time synchronization is of great importance for correct operation of a process bus implementation to achieve a stable and functional system.

This paper also reports experiences from testing protection IEDs in a multivendor Digital Substation.

The IEC61850 standard has been around for a couple of decades and it is about time it is fully embraced by end-users and all vendors. The end-user should take great care in defining the IED functionality in order to ensure vendor interoperability. This would require the utilities and vendors to work closely together.

There is a need for all manufacturers to fully implement the features of the IEC 61850 standard that will improve the interoperability not only between the devices, but also between the engineering and testing tools.

BIBLIOGRAPHY

[1] IEC 61850 - including all parts and reports - Edition 2

[2] CIGRE B5-203_ Experience with process bus in Statnett R&D project Digital substation, R.S.J. Loken et al, CIGRE Paris session 2018

[3] 0286_Testing of IED in a digital substation Full paper DPSP 2018, L. Stensrud, B. Ohrn, R.S.J. Loken, N. Hurzuk, A. Apostolov (DPSP conference 13-15th of March 2018, Belfast, United Kingdom)

1.2. CURRENT TRENDS AND CONCEPTUAL ISSUES OF PA SYSTEMS DEVELOPMENT: APPLICATION PRACTICE OF IEC 61850 STANDARD

Application of optical current transformers in Statnett R&D project Digital Substation

R. LOKEN
Statnett
Norway

Contact person:
Rannveig Loken
rannveig.loken@statnett.no

Keywords: Optical CT - IEC 61850 - Digital Substation - Process bus –Topology

Abstract:

A Digital Substation based on IEC 61850 9-2 [1] process bus is a complex system where Intelligent Electronic Device (IED)s interact with primary equipment and run both local and distributed software application functions. These functions are based on the exchange of information over the process bus and the station bus. The increasing levels of functional integration result in the development of many multifunctional IEDs that require interfaces with multiple primary devices.

The objective of the pilot project, Digital Substation [2], was to gain experience with Optical Instrument Transformers (LPIT) and process bus installations including interoperability issues.

This paper will discuss aspects related to application of Optical Instrument Transformer (LPIT) in the pilot Digital substation.

1. Introduction

Statnett initiated a Digital Substation based on IEC 61850 9-2 [1] aiming to gain experience and knowledge concerning concepts of a digital substation with Optical Instrument Transformers (LPIT) and process bus, to become familiar with the technology and in addition investigate what benefits this technique offers for future substation projects [2]. A crucial characteristic of the Digital Substation is the level of interoperability between IEDs from different vendors [3].

2. Digital Substation with IEC 61850 Process Bus and Optical Current Transformer (LPIT)

The Digital Substation, as shown in Fig. 1, is installed in a live 300kV line bay in parallel with an already existing Protection Automation and Control System (PACS), not able to operate the live breakers of the overhead line. The conventional current and voltage measurements are connected to the Digital Substation from the existing Protection Automation and Control System. The Optical Instrument Transformers is connected in series with the existing conventional current transformer in the overhead line. It is possible to operate and monitor the Digital Substation through the dispatch centre.

The Digital Substation pilot includes protection and control functions for two 300 kV transmission lines in the same IED hardware (Hereafter named Protection and Control Unit - PCU). This compact design challenged the traditional philosophy for Statnett transmission systems where protection and control functions are divided in separate hardware units.

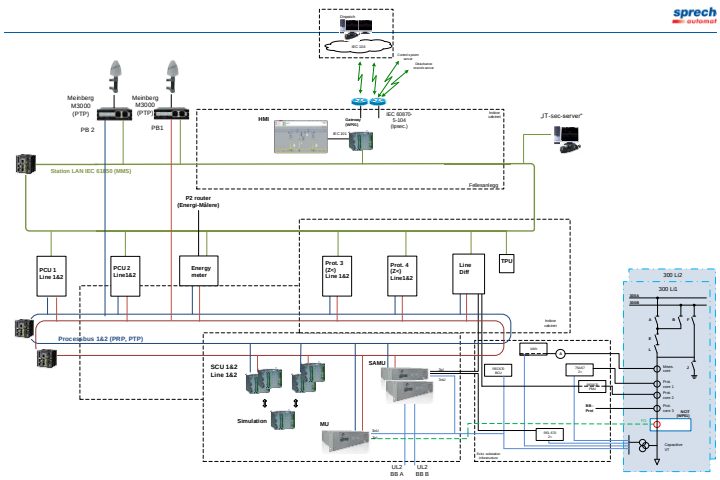


Fig. 1: Simplified Digital Substation topology and connection to existing PACS

3. Optical Current Transformer (LPIT)

The Sensor head of the Optical Current Transformer is connected to the High Voltage loop of the 300 kV transmission line in parallel with the existing conventional current transformer. The sensor head includes two fibers where the light from the Merging Unit is sent, and the angle of the light will be adjusted depending on the current in the 300 kV transmission line. The fiber from the sensor head is placed inside the insulator, down to the foundation and into the fiber merging cabinet in the outdoor cabinet. The safety of the system is better than a conventional Protection Automation and Control System with physical wires where arching could be a challenge. The pilot system have replaced the physical wires with optical sensor and fibers for the current measurement to the Protection Automation and Control System.

In addition there is no oil in the insulator, it is air cooled and the transport weight is lower than in a conventional current transformer.

4. Test of Optical Current Transformers

During the Factory Acceptance Test (FAT) all the components of the Optical Current transformer was tested according to normal procedures. The Optical Current Transformer including Merging Unit was calibrated for the actual measured values of the pilot project.

During the Site Acceptance Test the system was tested, including Optical Current Transformer, Merging Unit and Protection Control Unit. This verified the full protection and control chain for the system.

5. Application of Optical Current Transformer

The Optical Current Transformer was placed outdoor in the switchyeard in parallell with the conventional current transformers. The design was compact using the foundation for the conventional current transformers also for the Optical Current Transformer. The fiber from the Optical Current Transformer was merged in a outdoor cabinet in the switchyard and connected to the control room via a seperate fiber tube.

Climate conditions for the Optical Current Transformer have shifted between operation during warm summer months and cold winter months. During the pilot operation we have performed some upgrade and adjustments on the Merging Unit temperature settings.

The Sampled Values (SV) streams from the Merging Units (MU) and Stand Alone Merging Unit (SAMU)) are currents and voltages measured on a real transmission line and bus bar, but the station control units are operating only on a process simulator. SV streams according to IEC61850-9-2LE with 80 samples per cycle are used for metering, protection and control functions.

In this project the SV streams contain both current and voltage emerging from the same source (MU or SAMU). With both an optical and a conventional current transformer measuring on the same, real transmission line, it is possible to see if there is a difference in protection response to the two measuring methods. Therefore, the different PCU's were configured to use SV streams from optical and conventional current transformer for the two lines in a PCU, as shown in the table 1 below.

Table 1: Distribution of SV streams

Function		SV stream
PCU1	Line 1	SAMU
	Line 2	MU
PCU2	Line 1	MU
	Line 2	SAMU
PCU3	Line 1	MU
	Line 2	SAMU
PCU4	Line 1	SAMU

6. Conclusion

This paper has reported on a practical experience using Optical Current Transformer in a pilot project Digital Substation based on IEC 61850 process bus technology. The safety aspect related to use of optical fibers instead of the traditional hardwired current signal have been mentioned. The application of Optical Current Transformer in this pilot project is discussed. In addition, the climate condition for the outdoor installation have been included

BIBLIOGRAPHY

[1] IEC 61850 - including all parts and reports - Edition 2

[2] CIGRE B5-203_ Experience with process bus in Statnett R&D project Digital substation, R.S.J. Loken et al, CIGRE Paris session 2018

[3] 0286_Testing of IED in a digital substation Full paper DPSP 2018, L. Stensrud, B. Ohrn, R.S.J. Loken, N. Hurzuk, A. Apostolov (DPSP conference 13-15th of March 2018, Belfast, United Kingdom)

1.3. OPTICAL/DIGITAL SUBSTATION (ODS)

JORGE CARDENAS

Adneli Consultant (www.adneli.com)

Spain

Contact person:

Jorge Cardenas

jorge.cardenas@adneli.com

Keywords: CIT, NCIT, CT, CVT, Merging Unit, ODS, IED.

Abstract:

Primary equipment has traditionally been connected to protection & control (P&C) devices using copper wires. This traditional way of making the connections led to significant engineering effort, as thousands of different cables needed to be routed, installed, commissioned and maintained.

A full modern Substation is the one in which data related with primary processes is collected and digitized as much as possible, as close to the source as possible. From this point onwards, the data is exchanged with recipient devices via Ethernet instead of many kilometers of copper cabling. New Optical/Digital Substation (ODS) offer a solution and architecture in which the substation´s functionality is predominantly achieved in software, with less reliance on hardware and hardwiring implementations [1].

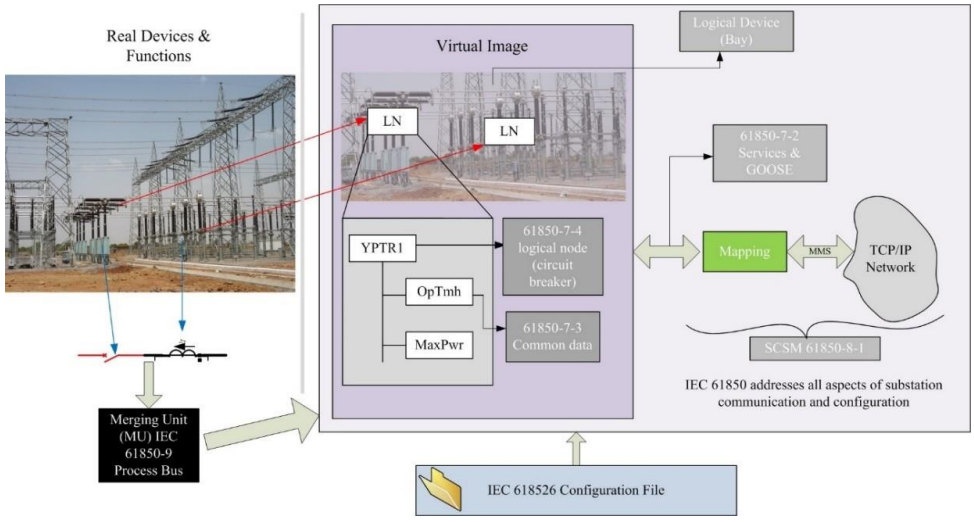


Figure 1. Optical/Digital Substation and its virtualization.

Functional integration of numerical devices helped reduce the number of boxes and connections and eventually led to compact panels. This technological evolution curtailed CAPEX for the materials for both new and expansion/replacement projects for P&C, as the material costs today are a small portion of the total installed cost of P&C systems. ODS by using Optical technology for sensing (CT´s and VT´s), combined with process bus standard, as described in IEC61869-9, helps reduce the complete chain costs: design, manufacturing, transportation, engineering, installation, maintenance, and time reduction in execution as well (up to 50%) [2], redundant in early installation availability; together with enhanced security and a footprint reduction (up to 73%) [1].

The present paper describes what an ODS is, together with the new technology associated with the Optical Sensors to measure voltage and current in HV Substations as sensing layer, integrated with Digital Technology [1, 2].

Special attention is also paid to new environment and concepts for Digital Substation testing, where in general, the use of protocol IEC 61850 is one of the key elements changing our vision for testing anelectrical substation [3].

1. SENSING TECHNOLOGIES IN USE

1.1. Conventional Instrument Transformers (CITs) and Handicaps

The purpose of Instrument transformers is to supply the protective relays with accurately scaled currentand voltages quantities for measurement, while at the same time insulating the relay from the high voltage and current of the power system. The proper selection of current and voltage transformers for protective relay applications is the responsibility of the system designer and takes into consideration requirements well beyond the scope of this paper.

1.1.1. Current Transformers

The most common current transformer construction is one in which the power system phase wire is passed through the hole in the center of an annular core or ring which is called "window" to form a primary winding. A second insulated wire is then wound around the core to form the secondary winding. This secondary wire is then brought to the relay for measurement. A CT with this type of construction is typically referred to as a toroidal or doughnut style of CT. The secondary continuous rating is typically 5 A in North America, and 1 A in many other parts of the world.

The operation of a CT is characterized by the equation of magnetizing forces according to which the primary current produces a magnetic flux that circulates through an iron core and induces a current in its secondary which is proportional to the current in its primary. When the primary current is so high that the core cannot handle any more flux, the CT is said to be in saturation. In saturation, there is no flux change when the primary current changes (as the core is already carrying maximum flux).

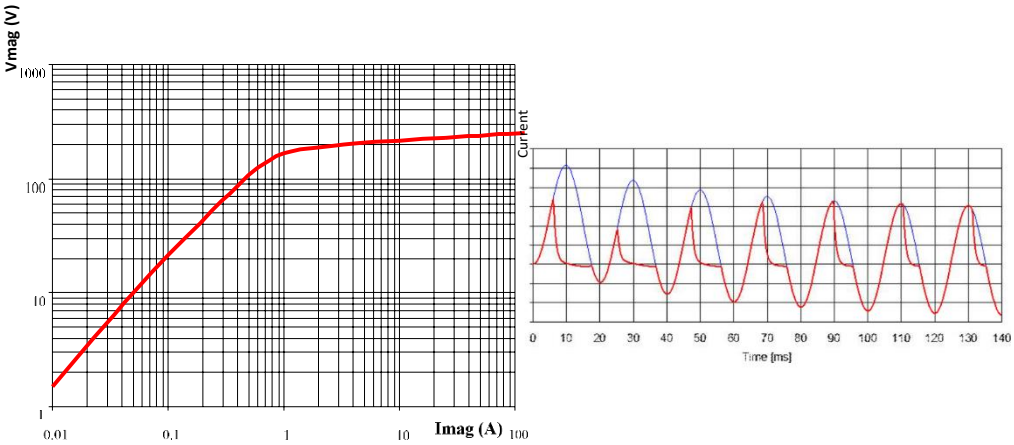


Figure 2. CT saturation curve relates magnetization current with voltage induced on CT secondary. The right-hand side picture shows the CT dynamic response on time with maximum DC offset.

1.1.2. Voltage Transformers

Voltage Transformers (VT) are used to isolate, step down and accurately reproduce the scaled voltage for the relay. The primary side of a VT needs to have the scaled System voltage, applied across the input terminals. The Secondary side of the VT will then accurately replicate a scaled-down version of the primary voltage over a defined voltage range.

There are two types of Voltage Transformers: the Electromagnetic Voltage Transformer and the Capacitive Voltage Transformer (CVT´s).

- Electromagnetic Voltage Transformers are usually used when accurate metering needs to be performed for lower voltage applications.
- Capacitive voltage transformers are commonly used in high voltage transmission line applications where the voltage is higher than 66 kV.

Electromagnetic Voltage Transformer works as a regular transformer and due to its physical characteristics, its cost tends to increase at a disproportionate rate to the primary voltage rating.

CVTs are normally used on higher voltage applications. CVTs consist of a number of series-connected capacitors placed between each phase and ground. The advantage of CVTs is that they cost relatively lower compared to the Voltage Transformers mainly for HV and EHV levels. Capacitive voltage devices have long been used in power systems as inputs to protective relays and protective relay systems. The CVT is basically a capacitance potential divider and consists of the following components:

- Coupling capacitors (typically ten).
- Compensating reactor.
- Step down transformer.
- And a Ferro resonance suppression circuit that is placed just before the output terminals for connecting to a relay.

Majority of CVT´s may exhibit a sub-harmonic transient when the system voltage is suddenly reduced so that the transient secondary voltage momentarily is not a replica of the primary. This transient is caused by the trapped energy ringing in the secondary compensating or tuning reactor and the associated circuit. This has not been a problem for electromechanical relays but may cause problems for solid state and numerical relays.

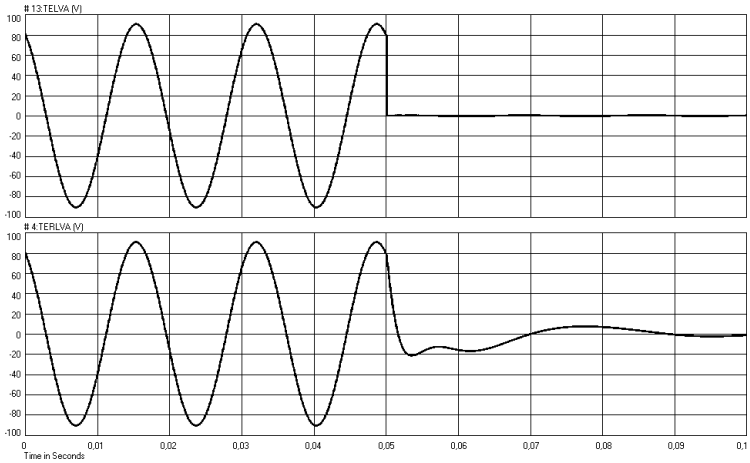


Figure 3. Transient response of a CVT: Secondary Voltage. In the upper signal we have the ideal expected voltage during a three-phase fault on the relay location. In the bottom signal we have the transient produced by the CVT on the secondary side.

Saturation in CTs and Sub-harmonic transients in CVTs limits their use particularly in relay applications, where it is necessary sometimes to incorporate complex algorithms to overcome both phenomena.

2. NEW TECHNOLOGIES IN SENSING BY USING NON-CONVENTIONAL INSTRUMENT TRANSFORMERS (NCIT)

2.1. Current Transformer Using Faraday Effect

The Faraday Effect is a magneto-optic effect (see Figure 4). The plane of polarization of input light beam is rotated in the transparent medium proportional to the intensity of the component of the appliedmagnetic field in the direction of the beam of light.

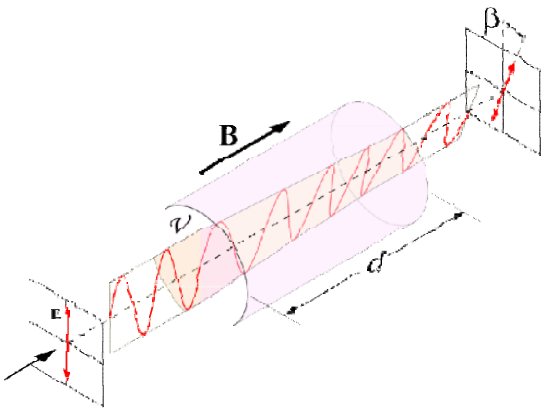


Figure 4. Basic Principle of Faraday's effect (source: Wikipedia)

The relation between the angle of rotation of the polarization $\beta[rad]$ and the magnetic flux densityin $B[T]$ the direction of light propagation in a diamagnetic medium with Verdet constant $v[rad/(T \cdot m)]$ and total length $d[m]$ is as follows:

$$\beta = vBd$$

2.1.1. Current Measurement

According to Ampere's theorem, equals the line integral of B along the closed loop C to current $I[A]$ inside the loop C $\mu_0[T \cdot m/A]$ hence, the relative magnetic permeability constant of the material.

$$\oint_C B \cdot dl = \mu_0 \cdot I \quad (2)$$

If light is propagated along loop C, the polarization rotation angle will be proportional to current I. There are two optical detection principles:

- ✓ Detecting the angle of rotation β directly at the change of strength of the light after passing thepolarizer
- ✓ Detecting the angle of rotation β using interference of two circular polarized light beams

The following is an example of Faraday Effect based current measurement system employing the interference measuring principle and optical fiber coil. Block diagram of the example current measurement system is shown in Figure 5.

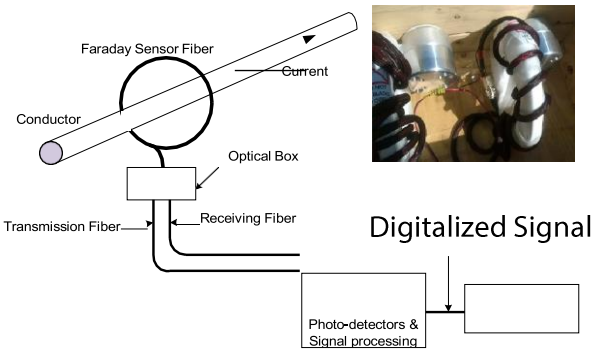


Figure 5. Schematic configuration of a Fiber optic current sensor based on Faraday Effect.

The system consists of a signal processing unit and a sensor head. Optical fiber for light guide is used to connect them.

The light source in the signal processing unit emits non-polarized and stabilized light beam. The light isconverted to linearly polarized light by the polarizer.

After passing the optical fiber for light guide, linearly polarized light is converted to circularly polarized light by quarter-wave plate (1/4 of λ) in the sensor head. Then the light is reflected by the mirror, input light and output light are interfered at the fiber coupler.

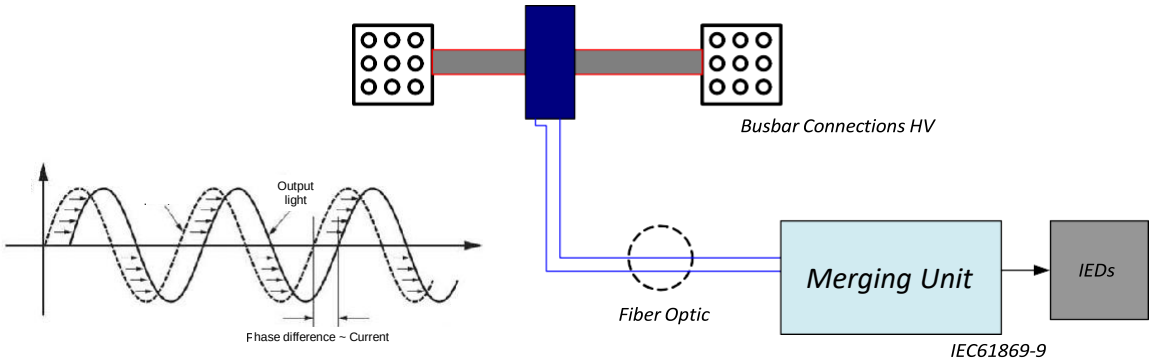


Figure 6. Phase difference between input and output optical current induced by Faraday Effect andapplication in an Optical CT.

2.1.2. Voltage Measurement – Change in the Refractive Index

Certain materials change their optical properties when subjected to an electric field. This is caused by the forces that distort the positions, orientations, or shapes of the molecules constituting the material. Theelectro-optic effect is the change in the refractive index resulting from the application of a DC or a low- frequency electric field (Figure 7).

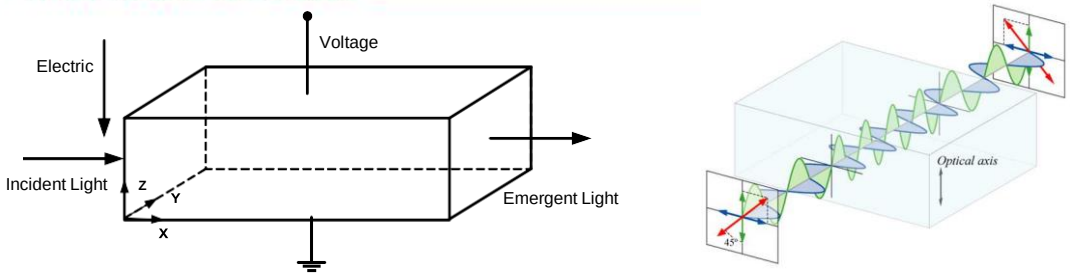


Figure 7. An electric field applied to an electro-optic material, changes its refractive index. This, in turn, changes the effect of the material on light traveling through it. The electric field therefore controls the light. The wave plate as a basis for voltage controlled Pockels effect (source: Wikipedia)

A field applied to an anisotropic electro-optic material, modifies its refractive indices and thereby its effect on polarized light. The dependence of the refractive index on the applied electric field takes oneof two forms:

- The refractive index changes in proportion to the applied electric field, in which case the effectis known as the linear electro-optic effect, or the Pockels effect.
- The refractive index changes in proportion to the square of the applied electric field, in whichcase the effect is known as the quadratic electro-optic effect of the Kerr effect.

The Pockels effect (after Friedrich Carl Alvin Pockels), occurs only in crystals that lack inversion symmetry, such as lithium niobate or gallium arsenide and in other non-centrosymmetric media suchas electric-field poled polymers or glasses.

Birefringence, or double refraction, is the decomposition of a light ray into two rays (the ordinary and the extraordinary ones) when it passes through certain types of material, depending on the light polarization, see Figure 7. This effect can only occur if the structure of the material is directionally dependent (anisotropic). If the material has a single axis of anisotropy (i.e., it is uniaxial) birefringence can be formalized by assigning two different refractive indices to the material for different polarizations.

The birefringence magnitude is then defined by equation (3) where n_e and n_o are the refractive indicesfor polarizations parallel (extraordinary) and perpendicular (ordinary) to the axis of anisotropy respectively:

$$\Delta n = n_e - n_o \tag{3}$$

The reason for birefringence is the fact that in anisotropic media the electric field vector $\vec{E}$ and the dielectric displacement $\vec{D}$ can be nonparallel (namely, for the extraordinary polarization), although being linearly related.

Practical implementations of Pockels cells for measurement of voltages between 115kV and 550kV have been reported **Error! Reference source not found.** The achieved accuracy corresponds to class 0.2 for metering as defined in IEC. They are used as an input to electronic metering and/or relaying systems. It should be noted that the application of this type of measuring systems lags in practice behind the resistive and capacitive voltage dividers.

Birefringence, or double refraction, is the decomposition of a light ray into two rays (the ordinary and the extraordinary ones) when it passes through certain types of material, depending on the light polarization, see Figure 7. This effect can only occur if the structure of the material is directionally dependent (anisotropic). If the material has a single axis of anisotropy (i.e., it is uniaxial) birefringence can be formalized by assigning two different refractive indices to the material for different polarizations.

The birefringence magnitude is then defined by equation (3) where n_e and n_o are the refractive indices for polarizations parallel (extraordinary) and perpendicular (ordinary) to the axis of anisotropy respectively:

$$\Delta n = n_e - n_o \tag{3}$$

The reason for birefringence is the fact that in anisotropic media the electric field vector $\vec{E}$ and the dielectric displacement $\vec{D}$ can be nonparallel (namely, for the extraordinary polarization), although being linearly related.

Practical implementations of Pockels cells for measurement of voltages between 115kV and 550kV have been reported **Error! Reference source not found.** The achieved accuracy corresponds to class 0.2 for metering as defined in IEC. They are used as an input to electronic metering and/or relaying systems. It should be noted that the application of this type of measuring systems lags in practice behind the resistive and capacitive voltage dividers.

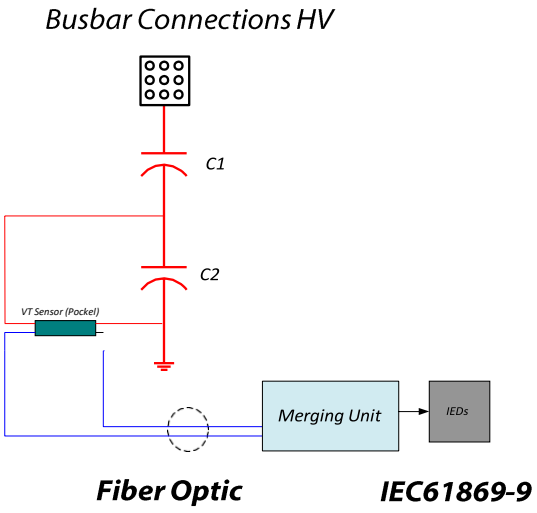


Figure 8. Optical Voltage Transformer [14]

Table I. Advantages of optical fiber current sensors. [4]

Compact and Light	They can be designed as compact because the sensing element is a long, thin, flexible optical fiber and is an insulating material.
Easiness of Installation	Installation on existing electric equipment is easy because the sensor can be installed without opening the high-power circuit.

Immunity from ElectromagneticNoise	They are immune to electromagnetic noise because all parts except for the electronic circuit consist of optical components.
Wide Measurement Range	Measurement of high frequency currents, or high currents can be possible because they are notprone to magnetic saturation, nor to sub-harmonic transients.
Long distance Signal Transmission	Long distance signal transmission is possible because waveform distortion and transmission losses are small.

1.1. Comparison on Current and Voltage Measuring Principles

Conventional instrument transformers (CITs) are well established in practice and are expected to remain in power systems for many more years. Their performance has been thoroughly studied and does not represent any secret for developers of complete secondary systems. Internal circuits as well as algorithms in modern IEDs are adjusted to different peculiarities like CT saturation, CVT transient response on big and fast voltage changes, etc.

Non-conventional instrument transformers (NCITs) have proved within last decade that they can be used in practice. In general, the results of test installations show better performances for CITs, especially when it comes to static amplitude and angular accuracy. Their basic operating principles secure in generally high accuracy within a wide frequency range. Some of them can measure even pure DC current and/or voltage, which is an advantage compared to the CITs. Their final accuracy and frequency response picture depends to a great extent on the quality and design of the electronic circuitry used to change the primary information (e.g., the rotation of a light beam) into equivalently low power DC current or voltage (generally analog) signal, which may later on be digitized within AD converters with different characteristics.

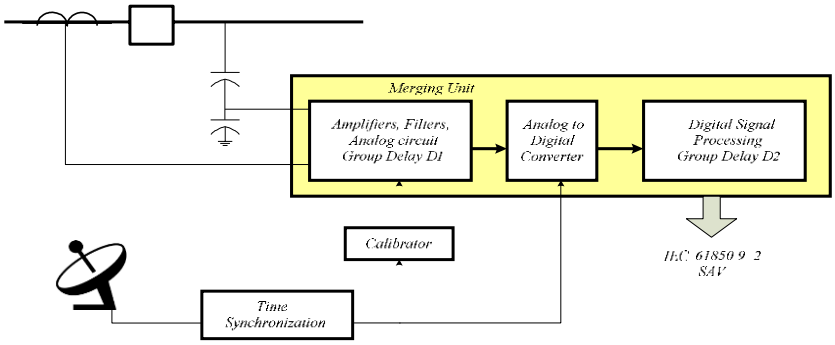
For many utilities, this change of philosophy in the design of substations is a challenge that must be overcome through the involvement of manufacturers, installers, and end-users in the transferring of knowledge with the aim of an economical, appropriate and suitable operation and maintenance (including Predictive Maintenance) of substation assets. Likewise, due to the continuous development of new products with increased capabilities of communication, safety, security and reliability, it is important to design substations in a way that equipment expansion (e.g., adding a new bay) and upgrade would be possible in a quick and cost-effective manner.

2.2. Merging Unit (MU)

Merging Units are needed for Optical Sensors, to convert analogue values into a message that the CPU in IEDs could understand. IEC 61850-9-1 defines Merging Unit as:

"Merging unit: interface unit that accepts multiple analogue CT/VT and binary inputs and produces multiple time synchronized serial unidirectional multi-drop digital point-to-point outputs to provide data communication via the logical interfaces."

The merging unit is an interface device which takes signals from the instrument transformer and sensors performing digital signal processing to generate and distribute output sampled value streams according to IEC 61850-9-2LE or IEC 61869-9 standardized definitions for communication with



substation IEDs and controllers.

*Figure 9. A Merging Unit block drawing***.**

Along with connecting with Non-Conventional Instrument Technology (NCIT) such as optical sensors and Rogowski coils, merging units (MU) can also work with conventional CTs and VTs to provide digital values of power system currents and voltages over communication buses. This analogue signal is then digitized with an Analogue to Digital Convertor (ADC) and sampled with a Digital Signal Processor (DSP) in synchronization with a standard clock signal. The DSP in a merging unit, also synchronized to the same clock source, makes the Sampled Values of the currents available on the IEC 61850 Process Bus, from where they can be collected by the IEDs. Additionally, with Analog Interface, MU must also provide a digital interface - IEC 60044-8 or IEC 61850-9-2.

2.3. Remote I/O and Process Interface Unit/Device

The remote I/O module (RIO) is intended to be the status and control interface for primary systems equipment such as circuit breakers, transformers, and isolator switches. RIOs under IEC 61850 may support only GOOSE publish-and-subscribe communications or may also support MMS client and server communications.

The process interface unit/device (PIU/PID), or simply PIU, combines a MU and a RIO into one device. It can publish analog values and equipment status and accept control commands for equipment operation as well.

3. HV and MV Optical-Digital Substation

Digitalization involves different disciplines and the one that in the recent years has experienced substantial changes is Protection, Control, Monitoring, and Information Management in HV and MV Substations. Main innovations are happening in these areas:

- Sensors: Optical sensors for primary equipment as Optical CTs and VTs.
- Protection and Control: IEC 61850 Process Bus, collecting current and voltage data andsending commands to Switchgear using fiber optic instead of copper wiring.
- Station Bus: Standardization of IEC 61850 as the communication protocol for all levels of the Substation. Possibility of using the same communication network for Process bus and Station Bus, simplifying the design.
- Introduction of Phasor Measuring Units (PMU) to provide synchronized analog data, also reducing the time for data collection, providing an effective real time.

- Extensive data management, converting it to information to optimize maintenance and operation.

The standards for communication in the new Optical/Digital Substation include:

- IEC 61850-1 Defines "Station Bus" for information exchange within the substation, as shownin the structure in Figure 10 and GOOSE for control values and trip commands.
- IEEE C37.118-2011 standard for synchrophasors.
- IEC 60870-5-104 or DNP 3.0 for SCADA data.
- Common Information Model (CIM) for consistency between referencing elements between substation and EMS/Wide Area Management System (WAMS).
- IEEE C37.111-2013 COMTRADE for transient data exchange.

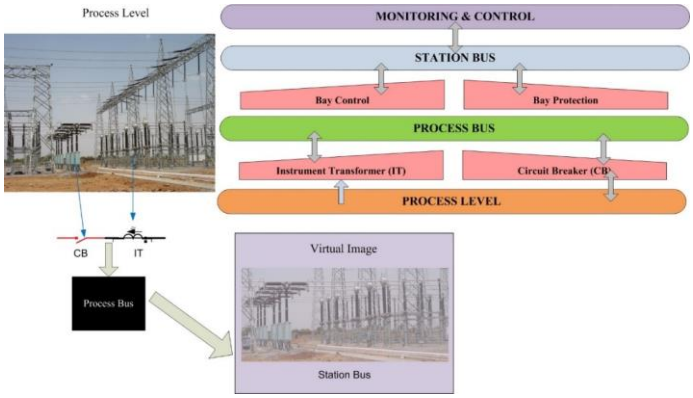


Figure 10. Architecture of a IEC61850 Substation

Goals and criteria for selecting primary and secondary equipment in Digital Substation can be summarized as follows [2, 6].

a. *Comprehensive and complete architecture*: After a complete architecture is created, design of Components, including optical VT/CTs, field (merging) units, Intelligent Electronic Devices (IEDs), communication infrastructure, signal datasets at protocol level, time synchronization method, etc. should demonstrate a complete interoperability as the primary goal is to deliver switchyard data to the PC&M devices.

b. *Reliability*: The overall system´s reliability decreases as the number of IEDs increase in the Installation because each additional element would directly impact the MTBF of the system; therefore, final architecture must consider a sufficient redundancy level. As a reference, in Tables 3, 4 and 5 we give a summary of some reliability calculations for individual components and for the complete system.

Table 3 Reliability of individual components [7, 9]

Element	MTBF (years)	Reliability
Protection relay	30 0	0.9967
Merging unit	30 0	0.9967
Switch	10	0.9900

	0	
Copper cables	10 0	0.9900
Fiber optic cables in the relay room	10 0	0.9900
Fiber optic cables in the substation switchyard	10 0	0.9900

Table 4 Reliability levels with conventional relays [10]

Architecture	Reliability
Non redundancy	0.9867
Primary and backup protection	0.9998

Table 5 Reliability of the Protection System in Process Bus [10]

Scenario	Network topology	Reliability
1	One merging unit, one relay and one switch	0.9639
2	Two merging units with redundant acquisition, one relay and one switch	0.9767
3	One merging unit and one relay with redundant Ethernet ports, and two switches	0.9925
4	Two merging units (redundant acquisition) and one relay with redundant Ethernet ports and twoswitches	0.9965
5	Two merging units (redundant acquisition) and two relays (redundant protection) with redundantEthernet ports and two switches	0.9999
6	Ring network topology with 6 IEDs	0.9911
	Ring network topology with 3 IEDs	0.9930

c. *Minimize co-dependencies*: Rules related to zones of protection must be considered when minimizing interactions with respect to other secondary elements from other protection zones. This criterion has proven to be one of the fundamentals of practical protection engineering, and it must be maintained irrespectively of the technology used.

d. *Scalability*: The system needs to facilitate future expansions with a minimum impact on performance and reliability. It must facilitate retrofits minimizing programmed outages. Safety: limitation of touch-and-step potential (voltage), risk of fire explosion, avoidance of unauthorized users or intrusion by continuous surveillance, and seismically qualified equipment are the main concerns for primary equipment. Personal safety is the main concern in secondary equipment. Fortunately, the use of fiber optic increases personal safety dramatically.

e. *Interoperability*: Primary equipment is more focused in “interchangeability”. IEDs should allow seamless communication within the secondary system, as well as interfacing to network management system, interoperability between different IEDs is of primary importance to the users.

f. *Environmental impact*: Site-adapt aesthetic, lowering above-ground level, limitation of electromagnetic and electric fields, low-level noise emission, and use of waste recycling, the carbon

footprint must be as small and as compact as possible.

g. *Controllability*: Improved local manual and automatic functions to achieve high response in real time.
h. *Economy*: Optical/Digital substation design should consider energy market participation, profit optimization and system operation risk reduction, with low-cost equipment, minimized life-cyclecost [1].
i. *Testability and maintainability*: The system needs to be provisioned to facilitate testing and maintenance. Testing is defined here as verification and re-verification of a complete PCM& Information Management after it has been deployed, as well as repairs, periodical or after a major work such as a Substation expansion, upgrades, or component replacement. In numerical relays, testing is based mainly in Software test methods as shown in Table 6. Maintainability is defined as the availability of simple, safe and trusted means of performing relay changes in parameters and functionality and replacing faulty elements of the system [11].

From the beginning, in Edition 1, the IEC 61850 standard included a test mode, through a test indicator in a way that a message published in the "test active" mode only would be treated by a subscriber with a "test active", too. In Edition 2 (E2), a new characteristic was added, the simulation. This indicator works in the same manner as a published message (only GOOSE or SV) with the characteristic that the "simulation active" condition only will be treated by a subscriber with "simulation active", too [12].

Table 6 Software test methods [13]

Black-Box Testing	Grey-Box Testing	White-Box Testing
The internal workings of an application need not to be known.	The tester has limited knowledge of theinternal workings of the application.	Tester has full knowledge of the internalworkings of the application.
Performed by end-users and alsoby testers and developers.	Performed by end-users and by testers anddevelopers.	Normally done by testers and developers.
Testing is based on external expectations - Internal behavior of the application is unknown.	Testing is done based on high-level databasediagrams and data flow diagrams.	Internal workings are fully known, and the testercan design test data accordingly.
*Not suited for algorithm testing.	*Not suited for algorithm testing.	*Suited for algorithm testing.
It is exhaustive and the least time-consuming.	Partly time-consuming and exhaustive.	The most exhaustive and time-consuming type oftesting.
This can only be done by trial and error method.	Data domains and internal boundaries can betested, if known.	Data domains and internal boundaries can bebetter tested.

(*) Non applicable to IEC 61850.

The IEC 61850 E2 standard also includes the possibility to block the physical actuation of the

process, by using the test/block feature. The device that is in test mode accepts the messages that come with this feature (test mode messages) reacting according to its defined settings, but it does not activate its physical outputs (as if wires were removed from the output contacts).

All these features give to IEC 61850 a very good environment for a safe and controlled testing.The knowledge of the internal behavior of the test object, or more specifically the logic or algorithms implemented, determine how the tests are being executed. Table 6 is applied for themost commonly used test methods for software testing.

3.1. Complementary Reduced Weight & Dimensions [1]

Different types of current and voltage NCITs have been developed so far. The practice has shown that NCCTs possess much smaller dimensions and are starting to be economic at voltage levels of 110kVand higher. NCVTs also show significant reduction in their dimensions (around 20% in height and 90% in mass).

In addition, there are considerable reduction in work and material in ODS compared with conventional installations [1, 2]:

- 90% reduction in the number of cables needed in a substation.
- A resulting 90% reduction in the amount of cable trench needed.
- An 80% to 90% reduction in the number of relay panels required.
- An 80% to 90% reduction in the size of control building.
- Up to 73% reduction in the footprint of the total switchyard.

REFERENCES

[1] Rich Hunt, Chirag Mistry: “Concrete & Steel: Where Process Bus Really Saves Money”, GE Grid Solutions,2017.
[2] Saeid Shoarinejad, Jorge Seco, Jorge Cardenas: “The Azerbaijani experiences in Digital Substation deployment. How Process Bus and IEC 61850 addresses Utility requirements.”.CIGRÉ Russia, 2015.
[3] Jorge Cardenas, Rannveig LØKEN, Joaquin Rodriguez, Diego Arribas, Daniel Ruiz Ayala: “HUMAN ASPECTS RELATED TO IEC 61850 TESTING: HOW TO BELIEVE OR DON´T BELIEVE IN TESTING.” DPSP 2020, Liverpool, UK.
[4] Kiyoshi KUROSAWA, Kazuomi SHIRAKAWA, Takehiko KIKUCHI: “Development of Optical Fiber Current Sensors and Their Applications.” 2005 IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific; Dalian, China.
[5] Javier Martín Herrera, Eduardo Villarreal, Javier Figuera, Joaquín Rodríguez, Pablo Jiménez, Jorge Cárdenas, Mohamed Boucherit, George Mikhael, Juan Manuel Parra, Javier Román, Andreas Jahr : “ OpticalCurrent measurement transmission over long distances and its application for fault discrimination in hybrid (overhead line + underground cable) transmission links.” CIGRÉ Russia, 2017.
[6] Ofgem: “Future Intelligent Transmission Network SubStation (FITNESS).” Scottish Power, 2015.
[7] U. B. Anombem, H. Li, P. Crossley, R. Zhang and C. McTaggart, “Process bus architectures for

substationautomation with life cycle cost consideration," 10th IET Int. Conf. on Developments in Power System Protection (DPSP), 2010.

[8] Bohnert K., Gabus P., Brändle H, Aftab K.: "Fiber-Optic Current and Voltage Sensors for High-Voltage Substations," Invited paper at 16th International Conference on Optical Fiber Sensors, October 13-17, 2003,Nara Japan, Technical Digest, pp 752-754.

[9] Mladen Kezunovic, Mohsen Ghavami, Chenyan Guo, Yufan Guan. George Karady: " The 21th CenturySubstation Design." PSERC Publication 10-15, September 2010.

[10] C.A. Dutra, S. L. Zimath, L.B. de Oliveira, "Framework for Process Bus Reliability Analysis," General Electric, CIGRÉ Sochi, Russia, 2015.

[11] D.McGINN, S.HODDER, B.KASZTENNY, D.MA. "CONSTRAINTS AND SOLUTIONS IN TESTINGIEC 61850 PROCESS BUS PROTECTION AND CONTROL SYSTEMS," B5-206, CIGRE Paris 2008.

[12] Alexander APOSTOLOV: "Protection Testing Considerations in Digital Substations," CIGRÉ 2018, Paris.

[13] Quick Guide. http://www.tutorialspoint.com. "Software Testing," 2018.

[14] GE Grid Solutions.

1.4. ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО ПРИМЕНЕНИЮ ОПТИЧЕСКИХ ТРАНСФОРМАТОРОВ ПРИ ПОСТРОЕНИИ ЦИФРОВЫХ ПОДСТАНЦИЙ. ОПЫТ РЕАЛИЗАЦИИ. ПРЕИМУЩЕСТВА И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

М.А. ЯНИН

АО «Профотек»

Российская Федерация

Контактное лицо:

Максим Янин

yanin@profotech.ru

Ключевые слова: IEC 61850-9-2, шина процесса, ТТЭО, оптический трансформатор тока, Smart Grid, РЗА, ток короткого замыкания, цифровая подстанция, ЦПС.

Современные изменения в сетевой инфраструктуре, вызванные переходом к технологии Smart Grid, требуют повышения наблюдаемости и управляемости сети. Контроль за параметрами сети становится более требователен к качеству измерения в широких диапазонах первичных токов и несинусоидальных режимах работы.

Измерения токов и напряжений, проводимые классическими измерительными трансформаторами, в таких условиях становятся недостаточно эффективными, и фокус внимания смещается на электронные измерительные трансформаторы.

Данный доклад подготовлен с целью трансляции опыта эволюции практики применения оптических трансформаторов тока на наиболее ярких пилотных проектах, выполненных компанией за последнее время.

Первый российский оптический трансформатор тока появился во Фрязинском институте радиотехники и электроники им. Котельникова в 2005–2006 годах. С 2010 года разработку начала финансировать компания «Роснано» на базе компании «Профотек», и сейчас ее продукции удалось встать в один ряд с продукцией таких известных производителей цифровых трансформаторов, как ABB, Alstom и Arteche.

Для превращения своей продукции в серийную компании «Профотек» пришлось реализовать ряд пилотных проектов, в рамках которых, кроме выявления и устранения недочетов в конструкции изделия, основной заказчик пытался получить ответ на более глобальные вопросы, связанные с концепцией реализации ЦПС. Ответы на эти вопросы получены при реализации пилотных проектов и тестов, проведенных в ведущих лабораториях мира. Краткое описание каждого из наиболее интересных пилотных проектов приведено ниже.

Основные вопросы, задаваемые по тематике ЦПС, на которые приходилось искать ответ, можно условно группировать следующим образом:

1. Насколько цифровые трансформаторы тока и напряжения при работе с защитами идентичны классическим в реальной ситуации КЗ или специфических переходных процессов?
2. Какие моменты эксплуатации являются критическими для функционирования ЦПС?
3. Каким образом достичь наиболее эффективного соотношения цена/качество при реализации ЦПС и как выбрать по максимуму преимущества ЦПС?
4. Как правильно проводить испытания цифровых трансформаторов и цифровых защит, чтобы убедиться в надежности проектируемого решения?

1. Натурные испытания аналоговых и цифровых защит, проведенные в независимой лаборатории CESI (Милан) по заказу сетевой компании TERNA.

В предварительном отборе поставщиков измерительных трансформаторов для ЦПС в качестве основного решения были отобраны ТТЭО и ДНЕЭ производства АО «Профотек», поставляемые в Европу под совместным брендом CONDIS/Profotech. Для тестов был изготовлен трехфазный ТТЭО с гибкими чувствительными элементами, позволяющими упрощенную установку на существующие выводы реакторов и трансформаторов, а также трёхфазный ДНЕЭ без емкостных делителей (для упрощения процедуры тестирования напряжение 57.7 В от источника подавалось на внешние измерительные модули, устанавливаемые в нижнем плече делителей). В качестве вторичных устройств тестировались наиболее распространенные модели защит, используемые на объектах компании TERNA: SEL 421, SIEMENS Siprotec 5 7SA87 и ABB REL 670. Причем в тесте использовались

одновременно по 2 терминала указанных моделей каждого из производителей: первый – классический с аналоговыми входами, второй – той же модели, но с цифровыми входами IEC61850-9-2LE.





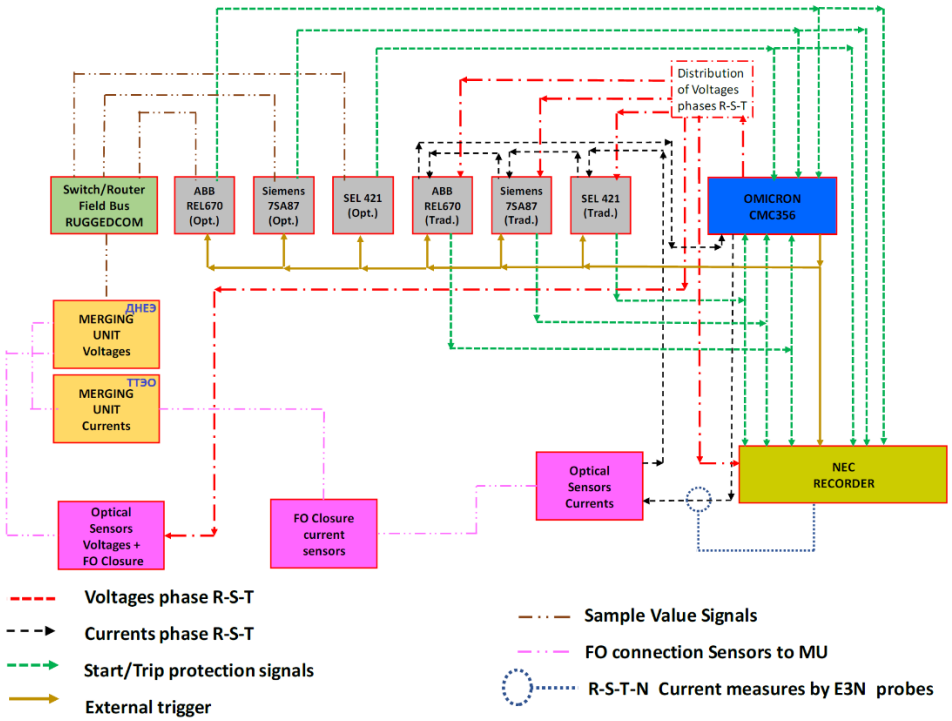


Участвовавшие в тестах защиты

Производитель	Модель	Тип	FW Version
SEL	SEL-421-5 Relay Protection Automation Control	Традиционная	V R324 V0-Z025013-D20180105
SEL	SEL-421-7 Relay Protection Automation Control	IEC-61850-9-2LE	V R324 V0-Z025013-D20180105
Siemens	Siprotec 7SA87 Line Protection	Традиционная	V.07.50
Siemens	Siprotec 7SA87 Line Protection	IEC-61850-9-2LE	V.07.50
ABB	REL670 Line distance protection	Традиционная	V 2.2
ABB	REL670 Line distance protection	IEC-61850-9-2LE	V 2.2

Синхронизация времени в устройствах происходила от единого источника точного времени MEINBERG LANTIME M300/GPS по протоколу 1PPS для ТТЭО и ДНЕЭ и протоколам IRIG-B + NTP для терминалов защит.

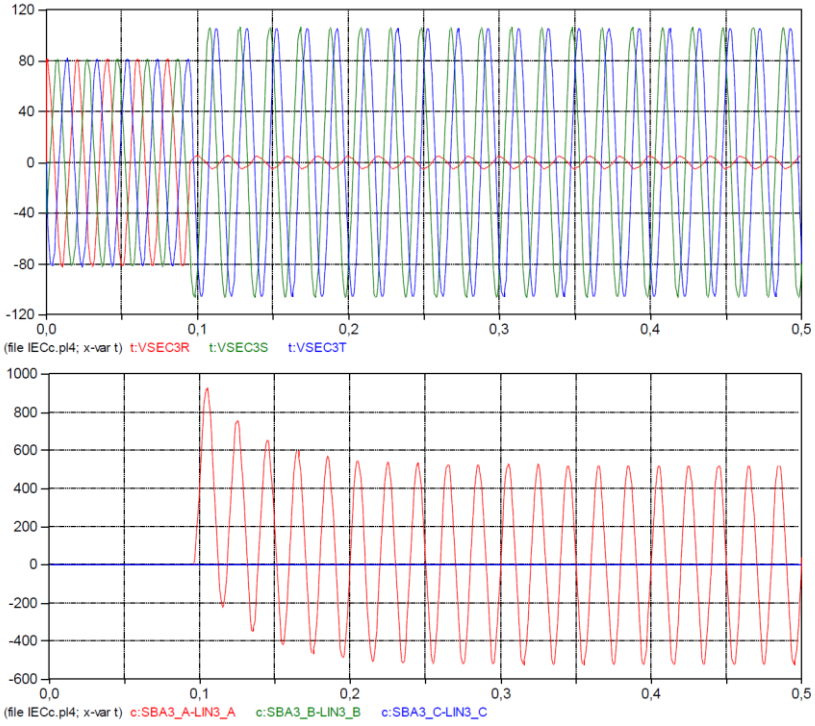
Схема включения обеспечивала одновременную подачу трехфазных токов и напряжений на аналоговые входы традиционных защит и на чувствительные элементы ТТЭО и ДНЕЭ. В качестве управляемого источника трехфазных токов и напряжений применялся Omicron CMC356. Для воспроизведения необходимого первичного тока на ТТЭО были применены вспомогательные электрические витки, обеспечивающие необходимое масштабирование первичного тока по условиям эксперимента. В процессе тестов происходила регистрация факта и времени срабатывания выходного реле терминалов РЗА, а также контроль записанных осциллограмм, функций ОМП и общих параметров функционирования терминалов.



В процессе исследования проводились следующие тесты, применяемые при сертификации терминалов РЗА:

Тест	ID test
Basic characteristic accuracy under steady state conditions	---
Basic directional accuracy under steady state conditions	---
Determination of accuracy related to time delay setting	IEC-a
Determination of the disenganging time	IEC-b
Dynamic Performance – SIR diagrams	IEC-c
Dynamic Performance – SIR/CVT diagrams	IEC-d
Dynamic Performance - Transient Overreach Tests	---
Steady State Harmonics Tests	---
Transient Oscillation Tests	IEC-e
Steady State Frequency Deviation Tests	---
Transient Frequency Deviation Tests	IEC-f
Double infeed tests for single line	IEC-g
Current reversal test	IEC-h
Evolving faults (only one line affected)	IEC-i
Evolving faults (both lines affected)	IEC-l

Пример осциллограммы одного из воспроизведенных тестов приведен ниже.



Основным результатом стало подтверждение идентичности срабатывания классических и цифровых защит при подаче тестовых сигналов на ТТЭО и ДНЕЭ во всех тестах. Основной выявленный недостаток – неточное присвоение меток времени цифровых потоков в терминалах при записи COMTRADE-файлов.

2. Подстанция ПС 500 кВ Тобол ПАО «ФСК ЕЭС» (Россия)

Подстанция 500 кВ Тобол — это узловая распределительная подстанция в Тюменской области, которая стала технологическим полигоном для тестирования новых устройств и измерительных систем в электроэнергетике. В рамках этого проекта в конце 2019 года на двух отходящих ВЛ 500 кВ (ЗапСиб-1 и ЗапСиб-2) была реализована информационная подсистема, функционирующая в соответствии с протоколом МЭК 61850-9-2. Главная особенность ВЛ 500 кВ ЗапСиб-1 и ЗапСиб-2 заключается в том, что для измерения электрического тока были установлены трансформаторы тока электронные оптические (ТТЭО) с классом точности 5TPE для нужд РЗА. Для измерения напряжения были установлены делители напряжения емкостные электронные (ДНЕЭ) с классом точности 0,2/3P и 0,2 соответственно.

ВЛ 500 кВ ЗапСиб-1 и ЗапСиб-2 связывают ПС 500 кВ Тобол с ПС 500 кВ ЗапСиб.

ПС 500 кВ ЗапСиб является центральной распределительной подстанцией (ПС глубокого ввода), которая питает «ЗапСибНефтехим» – самый масштабный в стране комбинат по глубокой переработке углеводородного сырья и выпуску полимерной продукции, входящий в состав крупнейшей нефтехимической компании в России ПАО «СИБУР Холдинг». ПС 500 кВ ЗапСиб оснащена четырьмя АТ 250 МВА, КРУЭ 110 кВ и ЗРУ-35 кВ.

Для оценки работоспособности информационной подсистемы в целом, а также для сравнения рабочих характеристик измерительных трансформаторов вовремя броска намагничивающего тока (БНТ) был проведен опыт постановки АТ-2 250 МВА под напряжение. На рис. 1 представлена упрощенная электрическая схема, которая отображает связь между ПС 500 кВ Тобол и ПС 500 кВ ЗапСиб по ВЛ 500 кВ ЗапСиб-2.

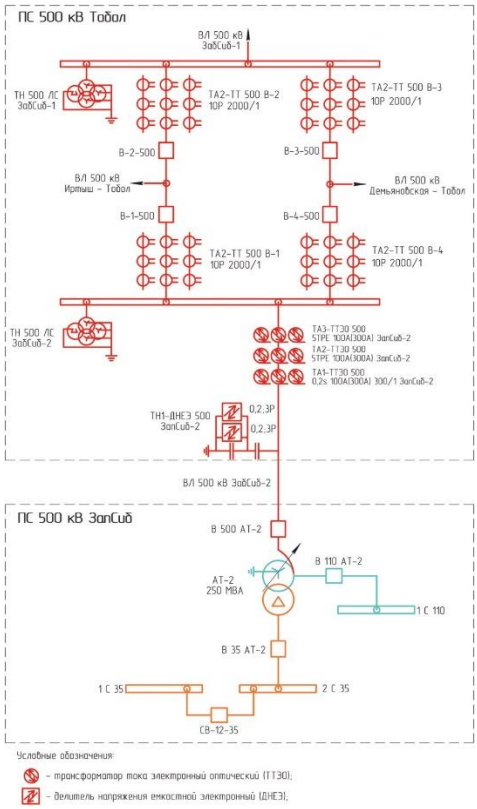


Рис. 1. Упрощенная электрическая схема связи ПС 500 кВ Тобол и ПС 500 кВ ЗапСиб.

Для оценки работоспособности информационной подсистемы в целом, а также для сравнения рабочих характеристик измерительных трансформаторов во время броска намагничивающего тока (БНТ) рабочей группой, созданной СО и ФСК для изучения поведения цифровых систем, был инициирован и проведен опыт постановки АТ-2 250 МВА под напряжение.

Осциллограммы для анализа были записаны регистратором аварийных событий (РАС), который позволяет регистрировать аналоговые и цифровые значения одновременно. При этом РАС подключен на сумму токов по двум плечам (В-1 и В-4) для получения значений аналогового тока на ВЛ 500 кВ ЗапСиб-2.

Основные выводы по результатам анализа осциллограмм:

1. Сравнительный анализ работы электромагнитных и оптических ТТ во время БНТ при постановке АТ-2 250 МВА под напряжение показал явные преимущества оптических ТТ. Это обусловлено отсутствием в оптическом ТТ явления намагничивания, что позволяет в свою очередь получать с них более достоверные данные о состоянии работы сети без искажений.

2. Гармонический анализ показал, что уровень передачи DC-составляющей для оптических ТТ выше по сравнению с электромагнитными ТТ.

При этом наблюдается снижение пикового значения, а также уменьшение действующего значения тока (RMS). DC-составляющая с электромагнитного ТТ со временем затухает, искажая тем самым представление терминалов РЗА о переходном процессе в системе. Таким образом, оптические ТТ потенциально позволяют выполнить защиту Т (АТ) с повышенной чувствительностью и быстродействием.

Рис.2. Насыщение электромагнитных ТТ (синий цвет) и оптических (желтый цвет) ТТ.

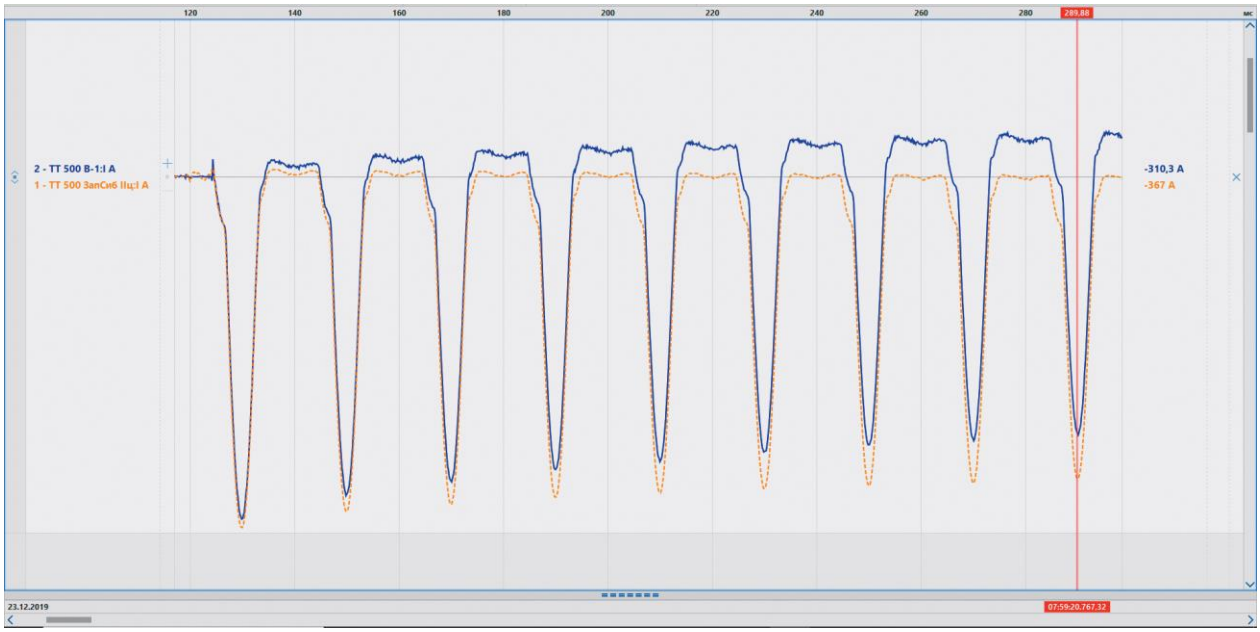


Рис.3. Разница действующего значения БНТ для с электромагнитных ТТ (синий цвет) и оптическихТТ (желтый цвет)

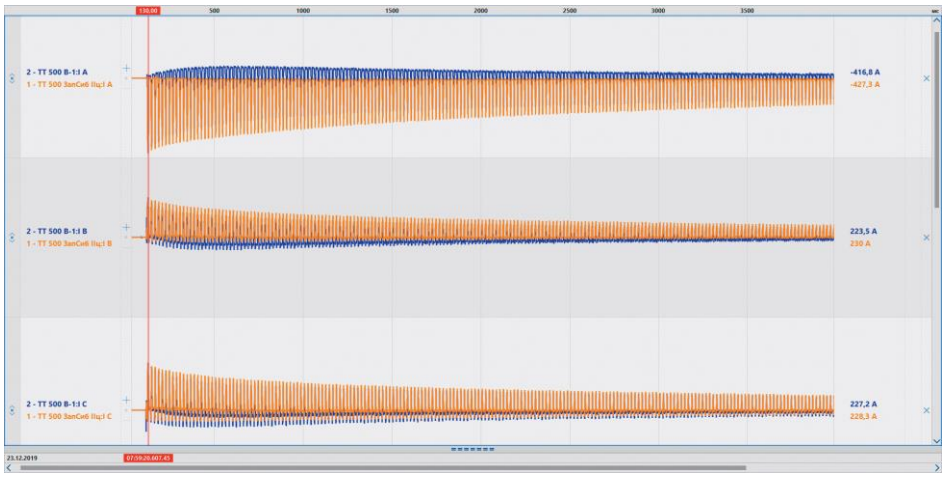


Рис. 4. Смещение кривой тока на электромагнитных ТТ (синий цвет) относительно кривой тока с оптических ТТ (желтый цвет)

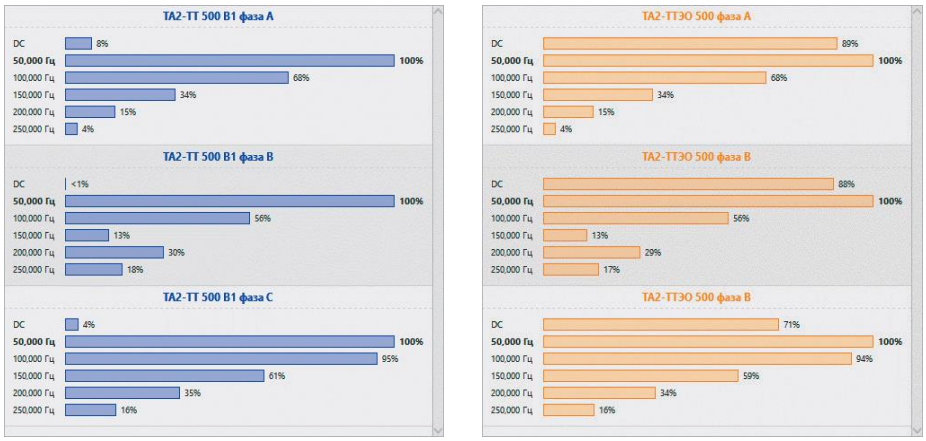
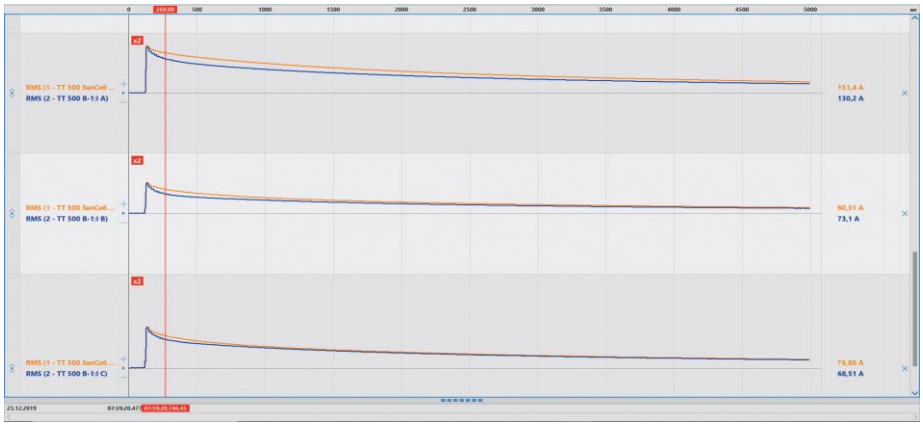


Рис. 5. Гармонический состав электромагнитных ТТ (синий цвет) и оптических ТТ (желтый цвет) в момент времени, равный 400 мс.

3. Испытательный центр лаборатории KEMA (г. Арнем, Нидерланды).

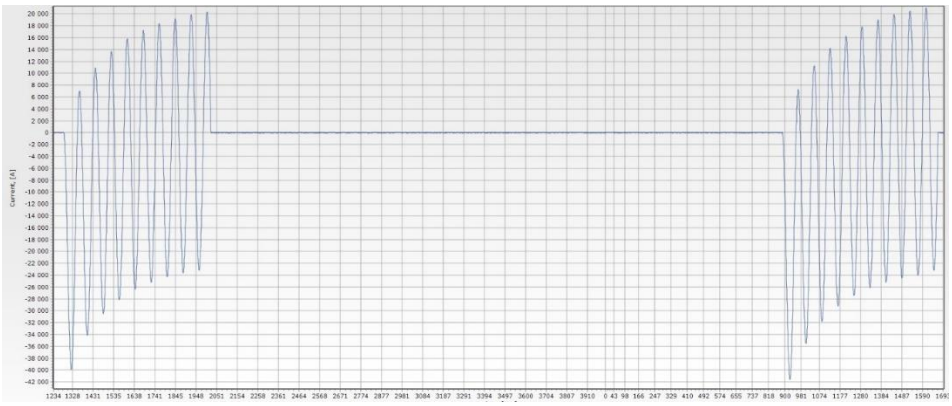


В 2018 году в испытательный центр лаборатории KEMA было поставлено 2 комплекта ТТЭО. В составе поставки были шинные трансформаторы тока 550 кВ с диапазоном измерений токов КЗ от 50 А до 180 кА (рис. 6а) и гибкие трансформаторы тока с диапазоном измерения токов КЗ от 500 А до 220 кА (рис. 6б). Цель поставки – использование ТТЭО в качестве эталонного средства измерения при коммутационных испытаниях для регистрации переходных процессов и на испытаниях токами короткого замыкания. В процессе эксплуатации ТТЭО постоянно использовался на тестах B-O-B-O (пример осциллограммы прилагается) и показал себя как надежный измеритель, не имеющий искажений формы кривой регистрируемых токов.



а) б)

Рис. 6. Оптические трансформаторы тока в лаборатории KEMA



В ноябре 2019 совместно с сетевой компанией TENNET проводилось тестирование реального однофазного КЗ в трехфазной сети с цифровыми защитами и трансформаторами ABB (рис. 7, 8), ТТЭО использовался как эталонный прибор, а также как альтернатива оптическим трансформаторам ABB в схемах дифзащиты линии.

На графике измерений (рис. 10) видно, что при КЗ традиционный трансформатор насыщается, а оптический позволяет без искажений измерить полный ток КЗ.

Основной вывод: натурным экспериментом подтверждена корректность работы дифзащиты линии при использовании вариантов: ТТЭО-АВВ; оптический ТТ АВВ-АВВ; MU (АВВ) – АВВ. При сравнении кривых КЗ, полученных от ТТЭО и от оптического ТТ АВВ выявлена их полная идентичность с мгновенной погрешностью не более 0,5%. В случае применения MU подтверждается большая зависимость от аналогового ТТ и большее время срабатывания защит.

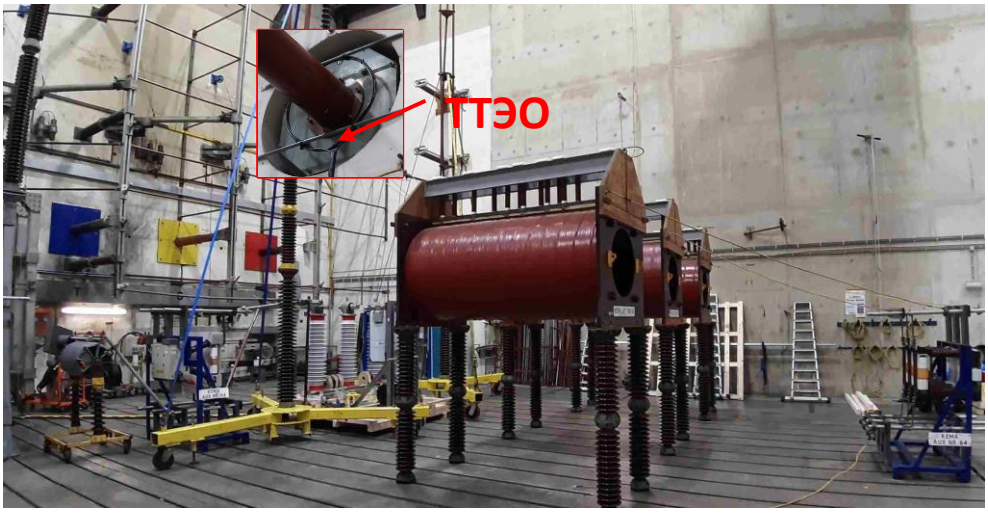


Рис.7. Проведение испытаний на однофазное КЗ (KEMA)

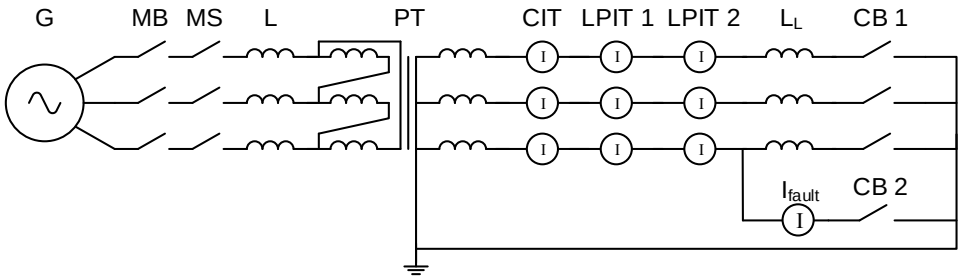


Рис. 8. Электрическая схема испытаний на однофазное КЗ (KEMA)

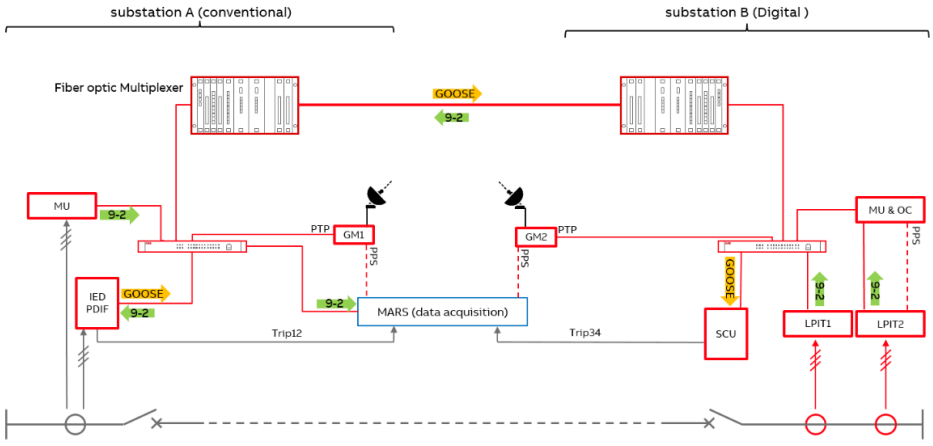


Рис. 9. Структурная схема испытаний на однофазное КЗ (KEMA)

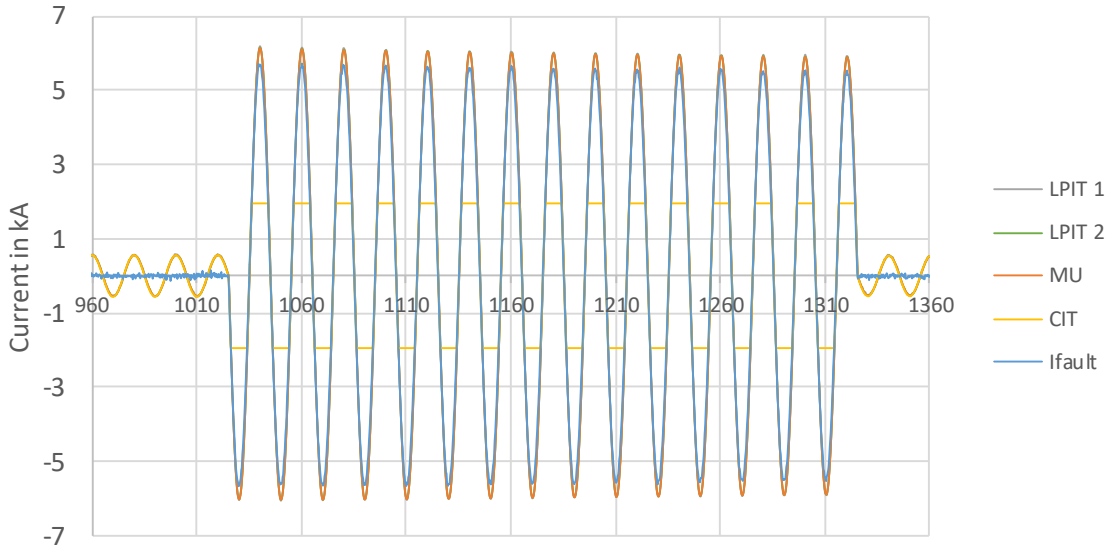


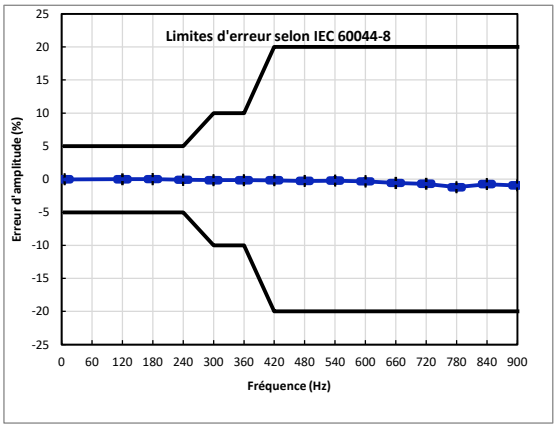
Рис. 10. Опыт проведения измерений при помощи различных ТТ (LPIT1 – ТТЭО «Профотек»)

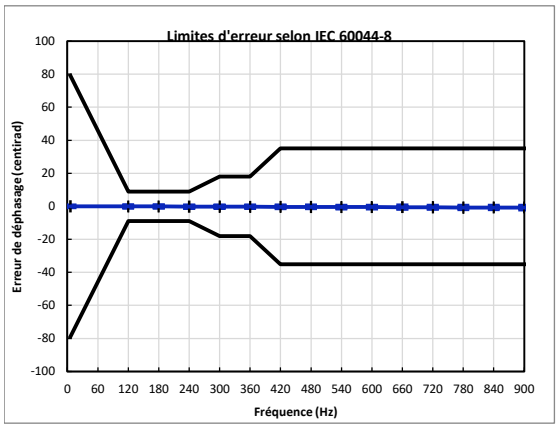
4. Квалификационные испытания оптических трансформаторов тока для поставки на пилотный проект 750 кВ Saguenay (Канада) компании Hydro Quebeck.

В 2018-2019 годах в исследовательском центре IREQ (Монреаль, Канада) проводились квалификационные испытания доступных на рынке оптических трансформаторов тока с целью определения поставщика решения для пилотного проекта 750кВ строящейся подстанции Saguenay. В качестве поставщика рассматривались трансформаторы Arteche, ABB, GE (USA), GE (бывш. Alstom/NXTphase), Trench (Siemens) и «Профотек» (под совместным брендом CONDIS/Profotech). Исследования включали в себя многостадийные отборочные испытания, включающие в себя: погрешности в рабочем и релейном диапазоне (включая исследование мгновенной погрешности по классу 5TPE), исследования частотных характеристик, исследование работы с системами синхронизации времени в различных режимах работы, температурные и вибрационные испытания и т. д. В ходе работ накоплен большой опыт проведения испытаний международного уровня и определены основные «болевые точки» оптических трансформаторов. В частности, обязательными квалификационными испытаниями признаны климатические, на мгновенную погрешность и на точность пропускания гармонических составляющих (графики погрешности приведены ниже).

Основной вывод: именно на этом пилоте полностью независимо протестирована корректная работа ТТЭО на частоте 60 Гц как базовой для расчета количества семплов в секунду и различных комбинаций выдаваемых потоков, т. е. фактически подтверждена работа по «Российскому» профилю МЭК 61850-9-2 за год до его утверждения. Подтверждено натурными испытаниями идеальное воспроизведение гармонического состава измеряемого сигнала вплоть до 1 000 Гц (что значительно превышает требования РЗА).







5. Гидроэлектростанция Nant de Drance (компания Swissgrid, Швейцария)

При реализации данного проекта решалась задача создания системы измерений AC и DC на высоковольтных кабелях трансформаторов гидрогенераторов 220 кВ и 330 кВ, обеспечивающей высокоточные измерения апериодического тока (рис. 12) в диапазоне от 5 А до 40 кА в условиях возможности работы без пересечения током нуля. Данная задача была решена при помощи ОТТ производства «Профотек» (рис. 13, 14). Успешно проведены квалификационные испытания.

Основной вывод: применение оптических ТТ является единственно возможным решением, гарантирующим динамический диапазон измерений токов в линиях генераторов от минимальных нагрузок до токов короткого замыкания независимо от переходного процесса.

Рис. 12. Пример асимметрии токов КЗ.

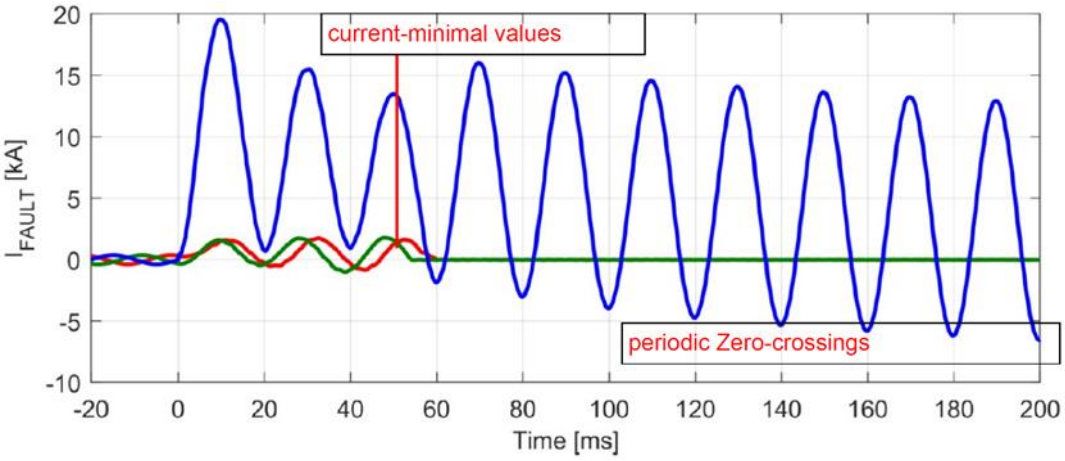


Рис.13 Точки установки ОТ

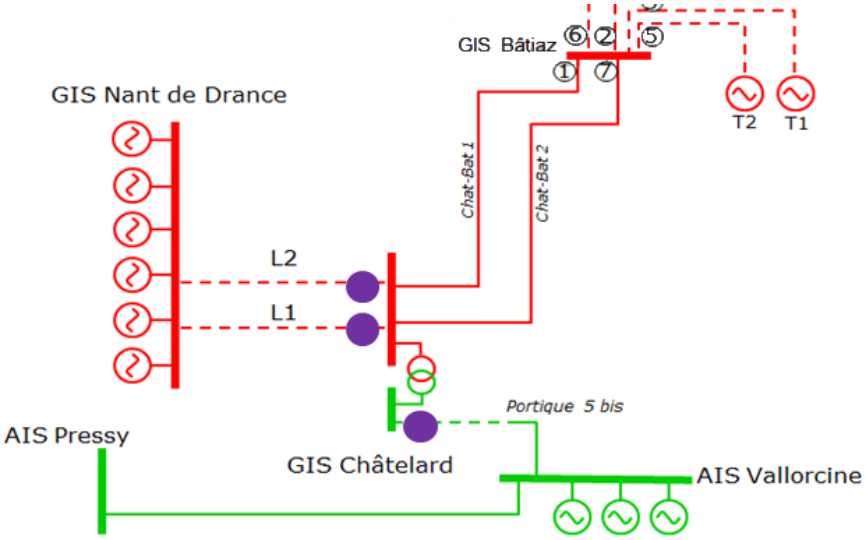




Рис. 14. ОТ «Профотек», установленные на высоковольтных кабелях.

6. Пилотный проект ЦПС с централизованными и децентрализованными защитами ПАО «Транснефть» на подстанциях 110 кВ Уват и 110 кВ Десна.

Пилотный проект интересен в первую очередь тем, что на данных подстанциях установлены оптические трансформаторы как на высокой (110 кВ), так и на низкой (6 кВ) сторонах, тем самым обеспечена возможность работы защит ЦПС в полном объеме. В качестве терминалов РЗА и серверов времени применена продукция компании ЭКРА, шины подстанции и процесса реализованы на коммутаторах Siemens RuggedCom.

В настоящее время проект находится в опытной эксплуатации, в период которой наработан значительный опыт эксплуатации, который уже был учтен в конструктиве и встроенном ПО как ТТЭО и ДНЕЭ, так и терминалов РЗА и серверов времени СВ-04. Обновленное с учетом полученных наработок оборудование находится в работе с постоянным контролем со стороны эксплуатации и производителей.

Основной вывод: для успешной работы ЦПС большого объема необходимо выполнение дополнительного контроля за серверами времени (реализованными в том числе в электронных трансформаторах и терминалах РЗА), коммутаторами, а также обеспечение требований ЭМС с нормами, превышающими указанные в ГОСТ Р МЭК 60044. Необходимо дополнительное исследование работы серверов времени в нагруженных сетях с PRP.

В результате накопленного опыта можно дать ответы на заданные вопросы:

Q.1. Насколько цифровые трансформаторы тока и напряжения при работе с защитами идентичны классическим в реальной ситуации КЗ или специфических переходных процессов?

A1.1. Полностью идентичны при работе в простых вариантах защит, используемых в стандартных применениях. Опыт сравнения показал 100%-ное совпадение результатов срабатывания традиционных и цифровых терминалов при условии качественной обработки первичного потока 61850-9-2 терминалом.

A1.2. При наличии значительных несинусоидальных переходных процессов альтернативы оптическим трансформаторам нет.

A.1.3. Выполненные по стандарту терминалы и оптические трансформаторы взаимозаменяемы в части информационных подсистем и позволяют эксплуатировать системы с разными производителями компонент, тем самым подтверждается основной принцип взаимозаменяемости.

A.1.4. Время срабатывания цифровых защит примерно на 2-5 мс дольше, чем у классических, т. к. 2 мс – это время, предусмотренное стандартом на измерение и выдачу пакетов измерений трансформаторами, от 0 до 3 мс добавляют производители РЗА для дополнительного контроля пришедших выборок. Данное время можно уменьшить путем оптимизации алгоритмов РЗА с учетом особенностей работы оптических трансформаторов. Пока можно констатировать факт того, что алгоритмы терминалов аналоговых и цифровых версий практически идентичны и в полной мере преимущества класса точности 5TPE не реализуют.

Q.2. Какие моменты эксплуатации являются критическими для функционирования ЦПС?

A.2.1. В первую очередь – система передачи данных. Неправильно настроенная или некорректно работающая шина процесса способна приводить к ложным выводам защит из работы и переполнению буферов событий. Необходимо на уровне SCADA подстанции или вспомогательных подсистем анализировать показатели сети передачи данных для выявления сбоев, а также контролировать топологию сети по таблицам разрешенной маршрутизации пакетов.

A.2.2. Во вторую очередь – работа системы синхронизации времени. Вторая по объему тестирования при ПНР и первая по количеству причин сбоев болевая точка. Необходимо намного больше внимания уделять тестированию серверов времени в различных режимах – работа по PRP, потеря и восстановление связи со спутниками, BMCA и т. д. По сравнению с объемом внимания, уделяемого работе электронных трансформаторов и терминалов РЗА, серверам времени выделено ничтожно малое количество. Опыт **всех** пилотных проектов реальных подстанций показал наличие огромного пласта неидентифицированных проблем по причине именно поведения серверов времени. Специально ради исключения таких сбоев во встроенное ПО трансформаторов добавлены функции контроля доверия серверам времени и отложенные реакции на внезапные изменения параметров, если «вдруг» источник времени через пару секунд передумает резко изменять шкалу времени. Количество «выбросов», регистрируемых из-за резкого изменения времени сервером после установки таких защит, снизилось практически до нуля, и специально введенные журналы событий контроля внешних подсистем регулярно фиксируют случаи неадекватного поведения системы времени.

A.2.3. Электромагнитная совместимость. Особо стоит отметить, что опыт эксплуатации в сложных условиях электромагнитной обстановки (ПС 500 кВ Тобол, ПС 110 кВ Десна и Уват, Испытательный центр ВЭИ, Испытательный центр KEMA) показали, что приведенные в стандартах

ГОСТ Р МЭК 60044 уровни ЭМС недостаточны и должны быть увеличены практически до максимальных.

А.2.4. Следует в обязательном порядке делать испытания терминалов на правильность присвоения меток времени в COMTRADE и алгоритмах по аналоговым, цифровым и бинарным входам. Практика показала, что терминалы правильно отрабатывают по алгоритмам, но далеко не все терминалы могут корректно записать все во встроенный РАС, ошибки присвоения времени бывают до нескольких десятков градусов как в одну, так и в другую сторону.

Q.3. Каким образом достичь наиболее эффективного соотношения цена/качество при реализации ЦПС и как выбрать по максимуму преимущества ЦПС?

А.3.1. Перейти от классических понятий кернов ТТ/ТН для комучета и РЗА к понятию унифицированного керна, когда один и тот же цифровой поток данных соответствует одновременно классу точности КУ и классу точности РЗА для переходных процессов. Данное обстоятельство позволяет снизить себестоимость электронных трансформаторов сразу на 20% по отношению к решениям, реализованным в прошлые годы (вместо 3 электронных блоков достаточно только двух – основного и резервного, как следствие – снижение стоимости, места в ячейках, потребления от СОПТ и т. д.). Как бонус в данном случае имеется возможность реализации бесшовного резервирования коммерческого учета при подписке счетчика одновременно на основной и резервный потоки.

А.3.2. Перейти к широкодиапазонным трансформаторам тока, когда один и тот же трансформатор может закрывать целый диапазон номинальных токов. Такой принцип заложен в унифицированных классах точности 1И, 2И, 1Р, 2Р СТО ПАО «Россети». Данный подход упрощает проектирование, снижает количество ЗиП в целом по сетям и приводит к снижению себестоимости за счет снижения номенклатуры выпускаемых изделий производителем.

А.3.3. Оптимизировать терминалы РЗА для снижения их номенклатуры, сделав более эффективные алгоритмы с учетом отсутствия намагничивания ТТ.

Q.4. Как правильно проводить испытания цифровых трансформаторов и цифровых защит, чтобы убедиться в надежности проектируемого решения?

А.4.1. Практически все испытания должны проводиться во включенном состоянии трансформаторов с контролем работы электроники. В первую очередь это касается высоковольтных испытаний, вибрации и испытаний ЭМС. Если для классических трансформаторов было достаточно критерия «сломался/нет», то для электронных важно поведение устройства во время испытаний.

А.4.2. Устройства, имеющие медные входные контакты (например, с разъемами RJ45), должны испытываться на ЭМС с подключенными кабелями стандартной длины, что существенно изменяет их устойчивость к помехам.

А.4.3. Климатические испытания должны проводиться в полном объеме, включая холодный старт, узлы отбора мощности от сети (если такие есть) должны подвергаться испытанию одновременно с основным изделием и находиться в тех же условиях.

А.4.4. Особое внимание следует обращать на работу устройств в условиях различного поведения серверов времени.

А.4.5. Терминалы РЗА должны в обязательном порядке иметь детальную диагностику в COMTRADE по статусу синхронизации потоков и битовым маскам качества получаемых замеров.

А.4.6. Крайне рекомендуется иметь предварительный протокол детальных испытаний на совместимость конкретного типа трансформаторов с конкретным типом терминала. На текущем этапе все производители активно дорабатывают технологию с учетом накапливаемого опыта, и в неоднозначно описанных случаях возможны несовпадения логики работы приборов.

Выводы

1. Технология ЦПС, построенная на применении оптических трансформаторов тока, является наиболее востребованной в мире, т. к. позволяет реализовать ранее недоступные возможности алгоритмов обеспечивая 100%-ное соответствие с теорией вне зависимости от исходного состояния трансформатора.

2. ЦПС является комплексным решением, каждый компонент которого должен всесторонне изучаться и детально тестироваться.

3. Должны быть разработаны адекватные требования к работе систем синхронизации времени и проведены испытания применяемых серверов времени на соответствие предъявляемым требованиям.

4. Учитывая существенный достигнутый прогресс в оптимизации программно-аппаратной базы электронных трансформаторов и терминалов РЗА, рекомендуется реализация ряда пилотных проектов на новейшей аппаратной базе. Опыт, накопленный на пилотных проектах, следует использовать при составлении программ квалификационных испытаний.

СПИСОК ЛИТЕРАТУРЫ

[1] CESI report prot. B6001763 – “Prove di interoperabilità su sensori ottici di Alta Tensione - Fase 1 - Definizione delle procedure di prova per la verifica dell’interoperabilità di TA Ottici e protezioni di differenti costruttori” – May 2019

[2] CESI report prot. B9009819 – “Prove di interoperabilità su sensori ottici di Alta Tensione - Fase 2 – Descrizione del circuito di prova per la verifica dell’interoperabilità di TA Ottici e protezioni di differenti costruttori” – September 2019

[3] CESI report prot. B9018829 – “Interoperability tests with HV Optical Sensors Part 3: First configuration test results (Condis-Profotech)” – December 2019

[4] IREQ. Rapport d’essais. Résultats de tests TCO MAXWELL/CONDIS EFOCT Novembre 2017

[5] IEC 60255-121 International Standard – “Measuring relays and protection equipment – Part 121: Functional requirements for distance protection” - Edition 1.0 2014-03

[6] T. Heid, T. Neumeier, F. Renaud, M.D. Vo, M. Yanin. "Monitoring of asymmetric short circuit currents at a hydro power plant using electronic fibre optical current transformers" CIGRE Session 2020, paper A3-223

[7] T. Heid, B. Paya, L. Basuyaux, M.D. Vo, M. Yanin. "Accuracy study of a combined low-power instrument transformer in different climatic and pollution conditions" CIGRE Session 2020, paper A3-224

[8] М. А. Янин, Р. И. Канафеев, Н. А. Иванов «Сравнительный анализ работы электромагнитных и оптических ТТ при броске тока намагничивания». ЭНЕРГОЭКСПЕРТ № 1 – 2020

1.5. ПРАКТИКА И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ИЗМЕРИТЕЛЬНЫХ ТРАНСФОРМАТОРОВ ТОКА И НАПРЯЖЕНИЯ ДЛЯ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИКИ

В. Д. ЛЕБЕДЕВ, А. А. ЯБЛОКОВ, Г. А. ФИЛАТОВА, Н. В. КУЗЬМИНА,
А. В. ПАНАЩАТЕНКО, Е. С. ШАГУРИНА

ФГБОУ ВО «Ивановский государственный энергетический университет имени В. И. Ленина» (ИГЭУ)
ООО НПО «Цифровые измерительные трансформаторы»

Российская Федерация

Контактное лицо:

В. Д. ЛЕБЕДЕВ

vd_lebedev@mail.ru

Ключевые слова: Цифровые трансформаторы тока и напряжения, пояс Роговского, цифровая обработка сигнала, релейная защита и автоматика.

Введение

В настоящее время активно разрабатываются и внедряются цифровые подстанции (ЦПС), основанные на совместной работе микропроцессорных устройств защиты и управления и электронных трансформаторов тока и напряжения (ТТ и ТН). Ведущие производители релейной защиты серийно выпускают микропроцессорные модули релейной защиты, адаптированные для работы с цифровыми потоками с использованием шины процесса по стандарту 61850-9-2LE. Несколько сложнее реализуются измерительные трансформаторы тока и напряжения. На основе накопленного опыта эксплуатации ЦПС появляются новые стандарты [1, 2], определяющие требования к аппаратно-программным средствам цифровой подстанции, в том числе и способы измерения электрических величин. Наиболее простой способ – дополнение стандартных трансформаторов тока и напряжения преобразователями аналоговых сигналов. Однако такой подход не полностью решает проблемы стандартных ТТ и ТН, такие, как насыщение магнитопровода, пожаро- и взрывобезопасность и др. Применение некоторых видов электронных трансформаторов, например, оптических, по причине высокой цены оправдано только на напряжениях выше 110-220 кВ. Характеристики цифровых трансформаторов, разработанных в ИГЭУ совместно с ООО НПО «Цифровые измерительные трансформаторы», позволяют использовать их в широком диапазоне напряжений от 6 до 220 кВ.

Целью работы является рассмотрение характеристик нетрадиционных первичных преобразователей тока и напряжения в составе цифровых измерительных трансформаторов, предназначенных для релейной защиты и автоматики, обобщение опыта и перспектив их применения.

Основная часть

Основные тенденции развития цифровых решений и результаты анализа первичных преобразователей тока и напряжения [3-5] свидетельствуют о необходимости анализа, разработки и внедрения цифровых трансформаторов тока и напряжения. Требования обеспечения качественной работы релейной защиты, а именно достижения ее основных показателей селективности, надежности, быстродействия и чувствительности, труднодостижимы на основе какого-то одного физического принципа. На основании выполненного анализа предложено использование в цифровых измерительных трансформаторах несколько первичных датчиков тока, выполненных на различных физических принципах: малогабаритный трансформатор тока ТТ, пояс Роговского ПР и магнитотранзистор МТ (гальваномагнитный преобразователь - магнитотранзисторное кольцо). Структура измерительного модуля цифрового трансформатора тока представлена на рис. 1. Такое сочетание дает не просто дублирование каналов измерения, но и более значимое с точки зрения надежности функциональное резервирование. Частотные характеристики первичных преобразователей неразрывно связаны как с обработкой сигналов в устройствах релейной защиты, автоматики и измерений, так, в конечном итоге, и с их алгоритмами работы. Таким образом, важной задачей является исследование частотных характеристик разработанных первичных преобразователей.

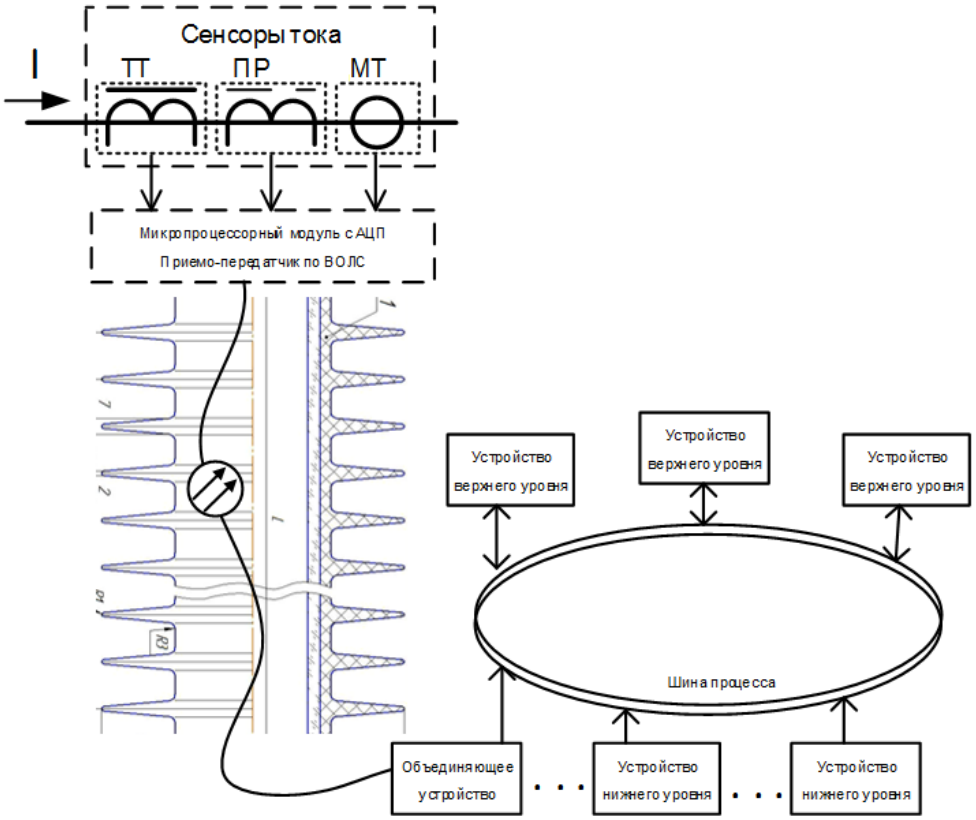


Рис. 1. Структурная схема измерительного трансформатора тока и шины процесса.

Для исследования характеристик первичных преобразователей тока был использован метрологический комплекс: аппаратно-программный комплекс OMICRON CMC 356 в качестве программируемого источника электрического сигнала в широком частотном диапазоне от 0 до 1 кГц; мультиметры Keysight 3458A для высокоточного измерения сигналов с эталонного и поверяемого трансформаторов тока; сертифицированный программный комплекс «EnergoEtalon» для управления мультиметрами при помощи персонального компьютера (ПК).

Выполненные исследования частотных характеристик датчиков тока демонстрируют высокую точность и линейность в исследуемом диапазоне частот и возможность использования их как для целей защиты, так и для целей учета электроэнергии. Эксперимент с подмагничиванием постоянным током, моделирующим апериодическую компоненту переходного тока короткого замыкания, показал существенные погрешности по амплитуде и фазе у электромагнитного трансформатора тока, в то время как пояс Роговского и магнитотранзистор сохранили метрологические показатели по переменной составляющей электрического тока без изменений, причем пояс Роговского осуществлял преобразование исключительно переменной составляющей, а МТ трансформировал весь спектр сигнала.

Физические характеристики первичных преобразователей, используемых в цифровом трансформаторе тока, позволяют распределить их по назначению: малогабаритный трансформатор тока – для целей учета электроэнергии, магнитотранзистор и пояс Роговского – для работы защиты и автоматики. Наличие нескольких датчиков тока, работающих на различных принципах, позволяет повысить точность измерения мгновенных значений в переходных режимах, осуществить резервирование устройств измерения токов короткого замыкания, снизить

погрешность расчета измеряемых величин, повысить быстродействие получения векторных величин тока.

Испытываемые образцы малогабаритного электромагнитного трансформатора тока продемонстрировали высокую точность в широком интервале частот и в диапазоне амплитуд токов от 1 до 120% $I_н$, что обеспечивает класс точности 0,2s с трехкратной перегрузочной способностью по току. Однако при наличии апериодических составляющих тока, насыщающих сердечник, у трансформатора возникают существенные погрешности. Кроме того, остается опасность сохранения остаточной намагниченности, которая, как показывает практика эксплуатации, может сохраняться длительное время.

Пояс Роговского и магнитотранзистор не насыщаются и наилучшим образом подходят для целей релейной защиты и автоматики. При этом наиболее информативным является именно МТ, охватывающий весь спектр сигнала, включая постоянный ток и медленно меняющиеся апериодические составляющие переходных токов. С появлением микропроцессорных устройств релейной защиты и автоматики неоднократно звучат слова о новых возможностях, предоставляемых этими устройствами за счет способностей обработки сигнала. Внедрение ЦПС также предполагает появление новых типов защит и использование кластерных защит. Однако построение принципиально новых типов защит зачастую ограничено возможностями традиционных электромагнитных трансформаторов тока в части скорости и точности передачи составляющих переходного процесса. Применение цифровых трансформаторов тока и напряжения снимает такие ограничения и позволяет разрабатывать новые алгоритмы работы защит. Также применение ЦТТН дает возможность модернизировать уже известные принципы выполнения защит и автоматики, в которых, например, сигнал апериодической составляющей за счет четкого ее выделения из тока переходного процесса может быть либо качественно подавлен, либо использован как информационный сигнал.

Работа основных защит характеризуется селективностью и быстродействием, для улучшения этих параметров важно точное преобразование мгновенных значений тока в первые моменты времени после возникновения замыкания. Для реализации этих потребностей наиболее подходит сигнал, поступающий с пояса Роговского, пропорциональный производной тока. Экспериментальные исследования, выполненные при реализации релейной защиты «мертвой зоны» [6-8], в которой было реализовано измерение с применением пояса Роговского, показали высокое быстродействие с временем подачи сигнала на отключение не более 4-5 мс.

Исследование различных методов расчета производной тока показало, что наибольшие погрешности расчета производной могут возникнуть при первом переходе (броске) тока [9, 10]. Рассматривались следующие способы расчета производной тока (рис. 2):

1. Применение «идеального» дифференциатора.

Использовался блок Derivative в Matlab, рассчитывающий приращение сигнала в двух последних точках:

$$y(t) = \frac{\Delta u}{\Delta t} = \frac{1}{\Delta t}(u_k - u_{k-1}), \qquad (1)$$

где Δt – интервал времени между текущей и предыдущей выборками (замерами), u_k и u_{k-1} – значения функции в текущей и предыдущей точках соответственно.

2. Применение реального дифференциатора.

Моделировались реальные дифференцирующие звенья с передаточной функцией вида

$$W(\mathrm{p}) = \frac{k(p)}{T_Д p + 1}, \qquad (2)$$

и различными значениями постоянными времени $T_Д$.

3. Аппроксимация кривой тока математической функцией *i(t)* и использование аналитически полученной функции *di(t)/dt*.

4. Использование для замера (расчета) производной пояса Роговского или его математической модели.

Показано, что применение ЦТТ и ТН за счет физического получения производной с датчика Роговского позволяет повысить точность замера производной тока, особенно точность при первых замерах (при наличии апериодической составляющей), что может существенно сказываться, например, на алгоритмах определения места повреждения по параметрам аварийного режима.

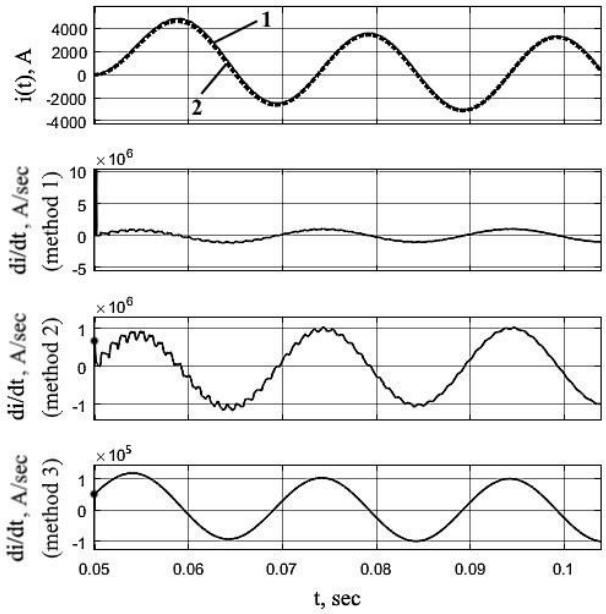


Рис. 2. Влияние метода расчета на определение значения производной тока в момент КЗ: 1 – кривая тока КЗ, 2 – аппроксимация тока КЗ функцией. Вторая осциллограмма (method 1) – вычисление «идеальным» дифференциатором; method 2 – вычисление реальным дифференциатором; method 3 – вычисление на математической модели пояса Роговского.

Аналоговый сигнал от первичных преобразователей в цифровом трансформаторе оцифровывается с помощью аналого-цифровых преобразователей. В настоящее время множество компаний выпускают аналого-цифровые преобразователи, обладающие высокой разрядностью (16, 18 и 24) и необходимой частотой дискретизации для выполнения задач защиты и учета электроэнергии.

Традиционно цепи учета электроэнергии и цепи релейной защиты были отделены друг от друга, что обусловлено следующими факторами:

1) способностью трансформатора тока насыщаться при больших токах;

2) ограниченная разрядность АЦП не позволяла с одинаковой точностью оцифровывать токи короткого замыкания и токи номинальных режимов;

3) учет электроэнергии и защиту энергообъектов осуществляли и осуществляют разные (раздельные) устройства.

Переход на цифровые технологии подразумевает физическое объединение канала учета электроэнергии с каналом релейной защиты в одной шине процесса, при этом сохраняются отдельные требования, такие, как 256 и 80 (96) отсчетов за период промышленной частоты для учета электроэнергии и защиты соответственно.

Анализируя результаты выполненных исследований, условия работы и назначение указанных преобразователей представляется возможным разработать алгоритм, позволяющий во всех режимах работы достигнуть максимально эффективного результата. Схема предварительной обработки сигналов, используемая для реализации указанного алгоритма, представлена на рис. 3.

Блок обработки сигнала сравнивает показания, полученные со всех трех датчиков, вносит корректирующие коэффициенты, обнаруживает наличие насыщения магнитопровода малогабаритного трансформатора тока и, если оно имеет место, передает результаты измерений от других первичных преобразователей, не подверженных насыщению. После размагничивания в процессе работы блок обработки сигналов автоматически возобновляет передачу данных от малогабаритного трансформатора тока как наиболее точного сенсора для учета электроэнергии. Результаты измерений с помощью малогабаритного трансформатора тока также могут быть востребованы релейной защитой, например, для целей дальнего резервирования, когда токи короткого замыкания незначительно отличаются от номинальных, а для принятия правильного решения нужна высокая точность.

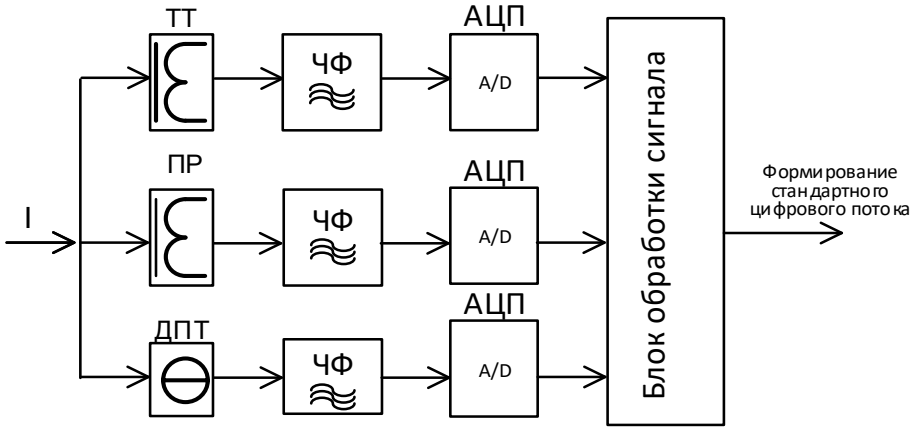


Рис. 3. Предварительная обработка сигналов цифрового трансформатора тока, полученная с первичных преобразователей, выполненных на различных физических принципах.

Для полноценной работы устройств релейной защиты и автоматики важно получать достоверную и своевременную информацию не только о мгновенных значениях тока, но и напряжения.

В настоящее время выполнен цикл научно-исследовательских работ, направленных на создание и исследование характеристик резистивных и резистивно-емкостных первичных преобразователей напряжения [11].

Результаты выполненных исследований при помощи метрологического комплекса показали, что разработанный первичный преобразователь напряжения имеет плавные амплитудно-частотную и фазочастотную характеристики без частотных всплесков, характерных для традиционных электромагнитных и емкостных трансформаторов напряжения.

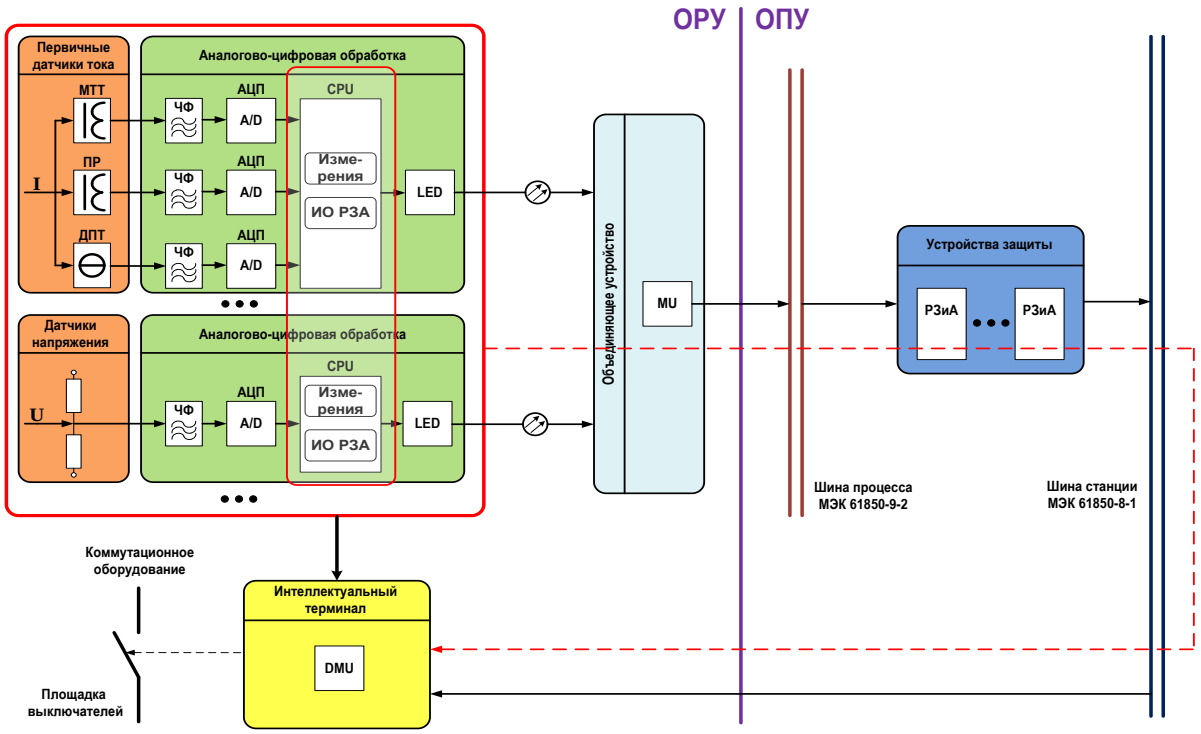
Явление остаточного заряда в емкостных трансформаторах напряжения может приводить к неправильным действиям релейной защиты и автоматики. Следует отметить, что данной проблемы не возникает у разработанного первичного преобразователя напряжения, и его работа также не приводит к возникновению феррорезоансных явлений.

Разработанные цифровые измерительные трансформаторы тока и напряжения успешно прошли совместные испытания с терминалами релейной защиты и автоматики производства АО “РАДИУС Автоматика”. В ходе испытаний была проверена совместимость оборудования при организации шины процесса, где источником информации выступал цифровой трансформатор тока и напряжения ЦТТН-6(10) кВ, а в качестве приемного устройства выступал терминал Сириус-2МЛ-02. Также оценены метрологические характеристики выстроенной измерительной системы, опробована работа терминала в режимах имитации протекания тока КЗ, проверена корректность механизма “подписки” терминала на SV-поток.

Комплекты цифровых комбинированных трансформаторов тока и напряжения 6 кВ установлены и успешно функционируют на открытом распределительном устройстве в цепи вводного присоединения КРУН 6 кВ в ЯНАО; на одной из подстанций ПАО “Газпром нефть”; в ячейке ЗРУ-6 кВ на ПС “Костромская-1” (ПАО “МРСК Центр”); на испытательном полигоне АО “НТЦ ФСК ЕЭС”. Также ООО НПО “ЦИТ” получило заключение об успешном завершении опытно-промышленной эксплуатации (ОПЭ) комплекта комбинированных цифровых трансформаторов тока и напряжения ЦТТН-6 кВ, установленных в ячейке ЗРУ 6 кВ на ПС “Ивановская-2”. Установленный комплект успешно отработал в течение всего срока ОПЭ, по завершению которой принято решение о продолжении ОПЭ с модернизацией установленного комплекта.

На основе использования цифровых трансформаторов тока и напряжения также была разработана многофункциональная система (рис. 4). Интеллектуальное устройство, обеспечивающее функции защиты автоматики и управления выключателем может быть установлено на открытом распределительном устройстве в непосредственной близи от коммутационных аппаратов. Преимуществом такого расположения является сокращение количества устройств, через которые передаётся и обрабатывается сигнал на пути преобразования от входных измеренных электрических величин до управляющего выходного сигнала. В текущей концепции построения цифровых подстанций данная многофункциональная система может быть внедрена в целях аппаратного и функционального резервирования относительно устройств шины процесса и шины станции, например, в условиях возможного информационного шторма.

Рис. 4. Многофункциональное устройство на базе ЦТТН



Помимо цифровых измерительных трансформаторов, новым направлением исследований является использование автоматизированных точек коммерческого учета электроэнергии (АТКУЭ) на линиях электропередачи 6–10 кВ. Для установки этих устройств не требуется рассекать провод воздушной линии и не требуется размещения дополнительных питающих элементов (рис. 5). Устройства в автоматическом режиме осуществляют расчет и передачу показаний потребленной электроэнергии. Измеренные устройством фазные токи и напряжения могут быть использованы для целей релейной защиты и автоматики.

В сетях среднего напряжения, в особенности на воздушных линиях, является актуальной разработка защит от однофазных замыканий на землю (ОЗЗ) и алгоритмов определения места ОЗЗ. Использование устройств АТКУЭ дает возможность реализации нескольких известных принципов выполнения таких защит:

– токовых защит нулевой последовательности, основанных на замере тока нулевой последовательности установившегося режима однофазного замыкания на землю;

– токовых направленных защит нулевой последовательности, основанных на замере тока и напряжения нулевой последовательности установившегося режима однофазного замыкания на землю;

– защит, использующих в качестве информационных параметров мгновенные значения электрических величин переходного процесса.

Все это позволяет использовать указанные устройства при построении систем для создания т. н. «цифровых РЭС».



Рис. 5: Процесс установки комплекта и 3D-модель АТКУЭ

Заключение

В работе представлены характеристики первичных преобразователей тока и напряжения, являющихся частью цифровых трансформаторов, применяемых для целей релейной защиты и автоматики. Использование специализированных преобразователей, основанных на разных физических принципах, позволяет обеспечить не только аппаратное, но и функциональное резервирование. Частотные характеристики первичных преобразователей напряжения демонстрируют плавные зависимости без выраженных частотных всплесков, характерных для традиционных электромагнитных и емкостных трансформаторов напряжения. Преобразователи тока продемонстрировали высокую точность высокую точность в широком интервале частот и в диапазоне амплитуд токов от 1 до 120% $I_н$, что обеспечивает класс точности 0,2s с трехкратной перегрузочной способностью по току.

Используемые первичные преобразователи не подвержены явлениям насыщения, остаточной намагниченности, феррорезонанса (что позволяет сократить количество и масштабы аварийных ситуаций), точно передают форму тока и напряжения во всех возможных режимах, в том числе при КЗ с апериодической составляющей. Созданные цифровые преобразователи тока и напряжения прошли успешные совместные испытания с микропроцессорными терминалами релейной защиты, отвечающими стандарту 61850-9-2LE, и установлены в опытную эксплуатацию на действующих открытых распределительных устройствах нескольких подстанций.

Разработанный алгоритм использования сигналов с нескольких первичных преобразователей для реализации функций релейной защиты и автоматики позволит повысить быстродействие и селективность защит, выполненных на известных принципах, а также разрабатывать новые алгоритмы работы защит, что является актуальным направлением исследований в связи с внедрением цифровых подстанций.

СПИСОК ЛИТЕРАТУРЫ

[1] СТО 56947007 - 29.240.10.256-2018. Стандарт организации ПАО «ФСК ЕЭС». Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС. – М., 2018.

[2] Корпоративный профиль МЭК 61850 ПАО «ФСК ЕЭС». Приложение 6 к Приказу от 17.05.2018 № 170 «О внесении изменений в приказ ОАО «ФСК ЕЭС» от 01.09.2014 № 373».

[3] Гречухин В. Н. Электронные трансформаторы тока и напряжения. Состояние, перспективы развития и внедрения на ОРУ 110-750 кВ станций и подстанций энергосистем, Вестник ИГЭУ, вып. 4, 2006, с. 35-42.

[4] Лебедев В. Д., Филатова Г. А., Нестерихин А. Е. Измерительные преобразователи тока для цифровых устройств релейной защиты и автоматики. Сб. докладов 4-ой Международной н.-т. конф. «Современные направления развития систем релейной защиты и автоматики энергосистем»: Екатеринбург: Изд-во РНК СИГРЭ, 2013.

[5] Отчет о НИР «Разработка теоретических основ создания высоковольтных (110-220 кВ) цифровых измерительных преобразователей тока с оптоэлектронным интерфейсом на базе фундаментальных физических законов с использованием современных материалов и микроэлектроники» выполненной в рамках приоритетного направления ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007 – 2013 годы» по заказу Минобрнауки, номер государственного контракта: 14.516.12.0005 - Иваново, ИГЭУ 2013 г.

[6] Жуков А. В., Воробьев В. С., Расщепляев А. И., Максимов Б. К., Арцишевский Я. Л., Борисов Р. К., Кузин А. С. Ликвидация коротких замыканий в «мертвой зоне» распределительных устройств энергообъектов. Энергия единой сети №6, 2014, с. 16-23.

[7] Патент на изобретение № 2508585 «Устройство для защиты от коротких замыканий в «мертвой» зоне открытых распределительных устройств объектов электроэнергетики высокого и сверхвысокого напряжения – на участках между трансформаторами тока и выключателями» // Шульгинов Н. Г., Жуков А. В., Воробьев В. С., Максимов Б. К., Арцишевский Я. Л., Расщепляев А. И., Кузин А. С., Борисов Р. К., Лебедев В. Д. Заявка № 2012147501 Приоритет изобретения 08 ноября 2012. Зарегистрировано в Государственном реестре изобретений Российской Федерации 27 февраля 2014 г.

[8] Жуков А. В., Воробьёв В. С., Расщепляев А. И., Арцишевский Я. Л., Кузин А. С., Борисов Р. К., Лебедев В. Д. Релейная защита «мертвой» зоны распределительных устройств объектов электроэнергетики. Сборник докладов XXII конференции «Релейная защита и автоматика энергосистем» Вопросы совершенствования и направления развития систем РЗА. – Москва, 2014 с. 14-20.

[9] Yablokov A., Filatova G., Timofeev A. Research of Methods for Fault Location Determination Using Signals from Digital Current and Voltage Transformers. – 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). Moscow, Russia. 2018. Pp. 1-5.

[10] Lebedev V., Shuin V., Yablokov A., Filatova G. Modeling of measuring current and voltage transformers in dynamic modes. Proceedings of 2014 International Conference on Mechanical Engineering, Automation and Control Systems, MEACS 2014. C. 6986890.

[11] Отчет о НИР «Разработка и исследование цифровых трансформаторов напряжения 110 кВ, основанных на фундаментальных физических законах с оптоэлектронным интерфейсом для

учета электроэнергии в интеллектуальной электроэнергетической системе с активно-адаптивной сетью» выполненной в рамках программы ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014 – 2020 годы» по заказу Минобрнауки, номер государственного контракта: 14.574.21.0072 - Иваново, ИГЭУ 2016 г.

[12] ГОСТ Р МЭК 60044-7-2010. Трансформаторы измерительные. Часть 7. Электронные трансформаторы напряжения. – М.: Стандартинформ, 2012. – 57 с.

1.6. ОПЫТ НАЛАДКИ И ЭКСПЛУАТАЦИИ ЦПС 330 КВ «МЕТАЛЛУРГИЧЕСКАЯ»

Е.А. ВОЙТЕНКО

РУП «Гомельэнерго»

Республика Беларусь

Контактное лицо:

Е.А. ВОЙТЕНКО
Voitenko_evgen@mail.ru

Ключевые слова: Шина процесса, goose-сообщения, МЭК 61850, синхронизация времени PTP, исполнительная документация, наладка ЦПС.

Введение

Летом 2019 года в Республике Беларусь введена в работу цифровая подстанция 330 кВ «Металлургическая».

Цель статьи: поделится опытом строительства первой цифровой подстанции в РБ.

Задача: обсудить с коллегами требования к цифровым ПС на разных этапах строительства.

Я не нашел в свободном доступе публикаций, содержащих описание технических проблем при реализации проектов строительства цифровых подстанций.

ОСНОВНАЯ ЧАСТЬ

Общая характеристика подстанции

Сторона 330 кВ подстанции выполнена по схеме «неполный четырехугольник», сторона 110 кВ - это две рабочие системы шин с обходной.

На ПС установлены классические трансформаторы тока и напряжения, которые подключены к устройствам сопряжения шины процесса. Прием и передача от/на первичное оборудование осуществляются через устройство сопряжения шины станции. По шине процесса осуществляется передача только SV-потоков и синхронизация времени. Таких шин на ПС две. К одной из них подключены устройства РЗА 1-го комплекса, ко второй – 2-го комплекса. Таким образом, на подстанции осуществляется дублирование шин данных.

Сеть шины станции используется для трафика GOOSE- и MMS-сообщений. Шина станции выполнена с использованием протокола резервирования PRP. На рисунке 1 представлена топология ЛВС подстанции.

Следует отметить, что на ПС не предусмотрено классических комплектов защит в качестве резервирования устройств РЗА, работающих по принципу «цифровая подстанция».

Оборудование РЗА установленное на ПС «Металлургическая»

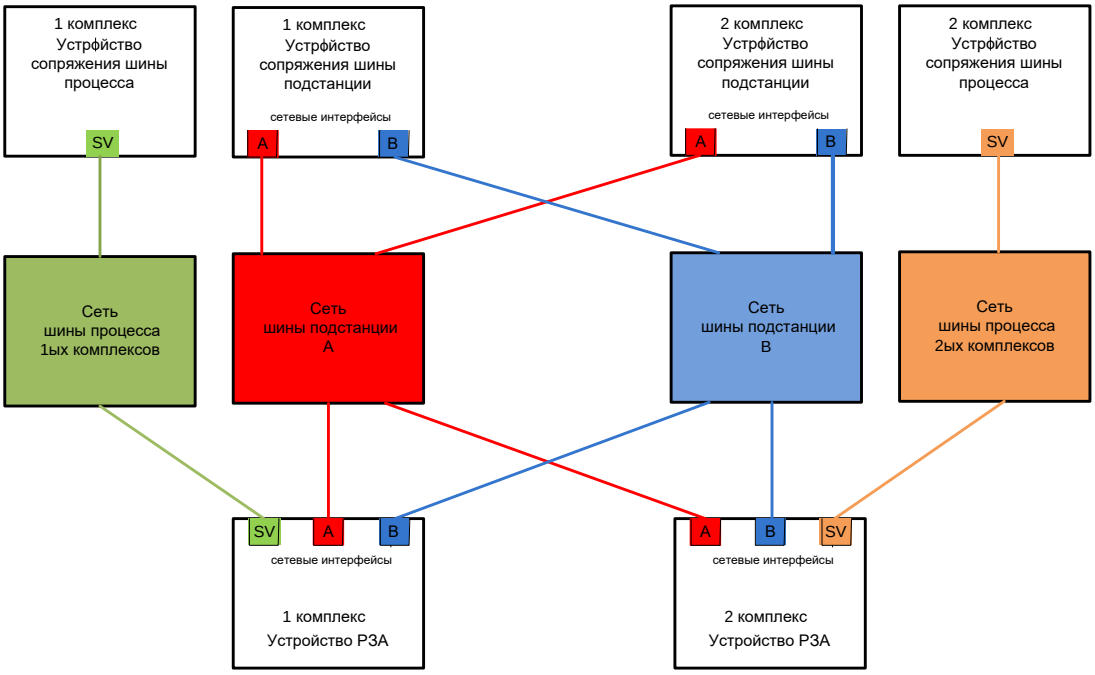
- Весь комплекс РЗА ПС выполнен на оборудовании фирмы ALSTOM (GE):
- Устройства защит и автоматики – Micom P446, P841, P743, P741;
- Автоматика выключателей 330 кВ и ПА – P841;
- В качестве защит ВЛ-110 кВ, 330 кВ – P446;
- ДЗШ-110 кВ – P741, P743. Полевые устройства P743 установлены на ОРУ-110кВ. Подключены непосредственно к цепям ТТ. Для резервирования защит линий 110 кВ в них выполнены токовые защиты.
- ДЗШ-330 кВ – P746.

Устройство сопряжения с шиной процесса – Reason MU320; устройство сопряжения с шиной станции – SCU; контроллеры ОБР и устройство сопряжения панели управления с шиной станции – Micom C264; серверы точного времени – RT 434; коммутаторы локальных сетей – Reason S2024;

На всех этапах строительства цифровой ПС персонал Гомельэнерго принимал непосредственное участие.

При этом возникали следующие трудности.

Рис. 1. Топология ЛВС



Недостатки проекта

На момент выпуска строительного проекта в Республике Беларусь не существовало нормативной базы, регламентирующей состав проектной документации цифровой подстанции. Основное отличие проекта ПС «Металлургическая» от классического проекта заключалось в наличии схем локальной сети. Файла полной конфигурации *.SCD у наладочной организации при строительстве не было. Что касается схем РЗА по присоединениям, то в проекте были лишь схемы электрических соединений. На рисунке 2 представлена схема терминала защит линии 330 кВ. Из схемы видно:

- перечень передаваемых сигналов в проекте отсутствует;

- логических блоков, описывающих коммуникацию между терминалами, нет;

- цепи тока и напряжения от устройств сопряжения никак не связаны с устройствами защит;

- нет специфических уставок для подписки SV-потоков и организации связи через шину станции.

Проект выполнен по правилам классических подстанций.

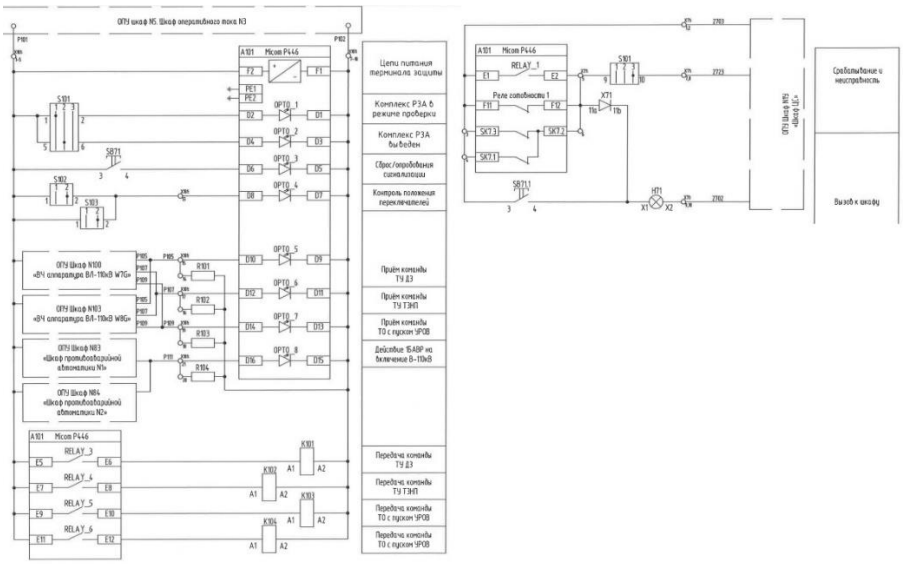


Рис. 2. Схема терминала РЗА ВЛ-330 кВ Micom P446

Главной проблемой проекта, на мой взгляд, стало полное отсутствие документации на «goose-коммуникацию» между устройствами РЗА. Составление списка всех необходимых сигналов (по сути, полноценный проект РЗА для классической подстанции) выполняла наладочная организация совместно с эксплуатацией. В итоге оптимальным вариантом визуализации виртуальных схем стала таблица Excel. Пример таблицы представлен на рисунке 3.Удобно если в таких таблицах есть следующая информация: сетевое название устройства РЗА; название dataset; назначение сигнала; широковещательный MAC-адрес goose-сообщения; метка VLAN; значение приоритетности сообщения; IP-адрес устройства; перечень устройств, подписанных на данное сообщение. Как мне кажется, вид и наполнение таких таблиц должны быть типизированы нормативными документами.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Источник						Назначение сигнала	примечание к сигналу	Получатель						Название dataset источника	Идентификатор принимаемого GOOSE сообщения	Название сигнала источника	Название входа у получателя
Монтажная единица	Место установки	Устройство						Монтажная единица	Место установки	Устройство							
		ID	IP адрес	Групповой MAC адрес	модель					ID	IP адрес	MAC адрес	модель				
A102	ОРУ УСШ АТ1 ОБР	SCU1T1D	172.16.21.2	:D0:32	Micom SCU(C066)	Неисправность MU1T1D	см.схему подкл SCU лист №77.3	A101	ОПУ шкаф защиты АТ №49	P1AT1	172.16.21.11		Micom P645	DatasetProcess	GoCB01	OptSpsGGIO1.ST.Ind1.stVal	System\GosGGIO1\Ind3
						Крышка БИ цепей ТТ MU1T1D вставлена										OptSpsGGIO1.ST.Ind2.stVal	System\GosGGIO1\Ind4
						Крышка БИ цепей ТТ общей обмотки АТ MU1T1D вставлена										OptSpsGGIO1.ST.Ind3.stVal	System\GosGGIO1\Ind5

Рис. 3. Таблица Goose-коммуникаций

Проектная организация не разрабатывала общий файл конфигурации подстанции *.SCD, о котором все техническое сообщество в русле цифровой подстанции говорит как об основном результате работы проектантов. Здесь, скорее, выскажу совсем непопулярное мнение. На мой

взгляд, в нынешних реалиях на этапе наладочных работ такой файл бесполезен. Первое и главное – в таком файле есть смысл, если его разрабатывали в том же программном обеспечении, которое будет использоваться наладчиками при выполнении работ. Вторая возможная проблема файла *.SCD - это сложность анализа проектных решений. Чем смотреть сигналы между терминалами, имея общий файл конфигурации, – непонятно. В данном случае на ум приходит лишь «колесо» компании «Тэквел», хотя в том или ином виде похожий функционал пробуют добавить в свой софт все производители терминалов защит. В нашем случае программа Micom S1 Agile смогла визуализировать *.cid файлы только терминалов защит, без устройств сопряжения.

На примере ПС «Металлургическая» стало ясно, что в проектной документации должны быть уставки (настройки) коммутаторов и серверов времени. Здесь важно понимать, что в зависимости от этих установок могут принципиально меняться логическая схема работы протокола синхронизации PTP и стабильность работы коммутаторов. Часть проектных работ, которая должна быть выполнена до этапа закупки оборудования:

- Обоснованная топология сети ЛВС с расчетами загрузки в различных режимах;

- Технология резервирования всех сетей;

- Определено количество переменных в dataset goose-сообщений каждого устройства РЗА;

- Определен способ вывода оборудования РЗА в ремонт;

- Рассмотрены ремонтные режимы ПС с рекомендациями по функционалу устройств РЗА;

- Определены места установки электронной части оптических ТТ и ТН;

- Определены места подключения испытательных установок.

Уже в процессе эксплуатации мы столкнулись с проблемой грызунов. Мышь, которая проникла в кросс-коробку в шкафу на ОРУ-330, повредила оптические пигтейлы одного из комплексов защит автотрансформатора. Срочный ремонт линий связи выполнял персонал службы РЗА. В проекте необходимо предлагать комплексную защиту от вредителей. Например, бронированные кабели и патчкорды, отпугиватели, применение специальных фитингов и монтажной пены.

Оборудование РЗА для цифровой ПС

В начале этого раздела хотел обозначить два момента. Первое: на объектах РУП «Гомельэнерго» установлено большое количество терминалов защит MICOM в классическом исполнении, и похожих проблем, как будет описано здесь, там не наблюдалось. Второе: обозначенные проблемы актуальны на начало ноября 2019 года.

В момент начала строительства ПС специалистами эксплуатации и наладочным персоналом обнаружилось, что одна часть поставленного оборудования работает с версией протокола edition 1, а другая – с версией edition 2. Это оказалось существенной проблемой, решение которой требовало много времени в процессе наладки. На сегодняшний момент мне известно только об одной программе, которая умеет корректно конвертировать файл *.cid(*.icd) из edition 2 в editon 1, это OMICRON IEDScout.

Основная проблема в поставленном оборудовании касалась устройства сопряжения с шиной станции SCU. Таких устройств на ПС установлено 24 шт., по два на каждый выключатель. Дело в том, что программа SCU Configurator, предназначенная для создания файла настроек *.cid, оказалась неработоспособной. Работоспособная программа у нас появилась через 2 месяца после включения ПС. Наладчикам приходилось файлы *.cid писать вручную в текстовом редакторе для каждого из 24 устройств. Такая работа заняла несколько рабочих недель. На мой взгляд, недопустимо со стороны завода-изготовителя реализовывать «готовый» продукт в виде устройства РЗА с такими проблемами.

Reason RT434 – это сервер времени PTP и SNTP, установленый на ПС 330 кВ «Металлургическая». Схема синхронизации выполнена так, что в шине процесса постоянно присутствуют два разных сервера времени. RT434 имеет 4 порта с различными MAC-адресами. Недостаток конкретно этой модели часов в том, что уставка приоритета пакетов PTP задаётся для всех портов одновременно. Это означает, что при идентичных топологиях двух сетей в обеих автоматически выбирается одно и то же устройство, как Grandmaster, а при его внезапной потере обе сети остаются без синхронизации на короткий промежуток времени.

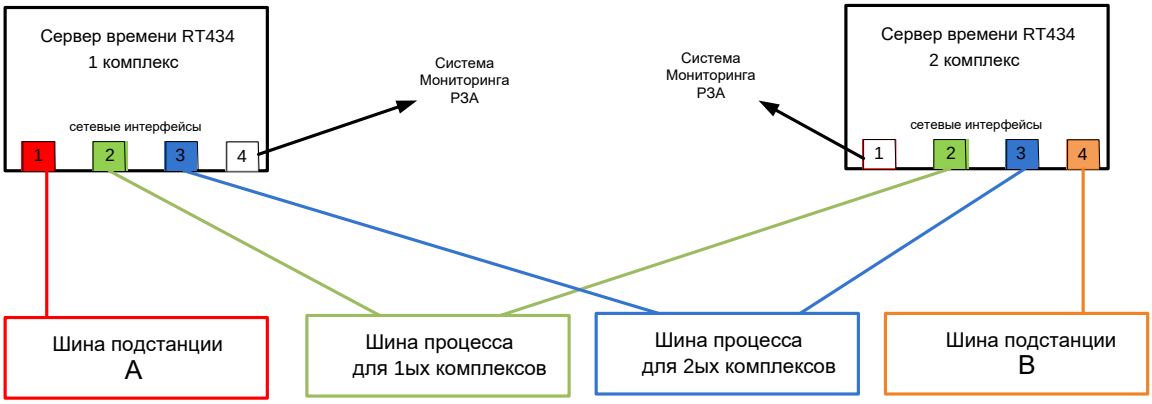


Рис. 4. Схема PTP синхронизации

Считаю нужным сказать, что в процессе наладки было выявлено еще много мелких проблем практически с каждым видом оборудования, входящего в полный комплекс РЗА цифровой ПС. Однако с выходом новых «прошивок» для устройств эти проблемы понемногу решаются уже в процессе эксплуатации. Например, для коммутаторов силами эксплуатационного персонала применена уже 4-я по счету версия внутреннего ПО, а терминал защиты регистрировал неисправность SV-потоков до 40 раз в сутки. Каждая такая работа требует вывода в ремонт большого количества устройств РЗА, что вызывает определенные трудности на ПС 330 кВ.

Программное обеспечение и испытательные установки

При производстве наладочных работ персонал пользовался ПО «Сетевой анализатор» от компании НПП «Динамика». В нашем распоряжении была ограниченная программная версия от полного программно-технического комплекса. Несомненное преимущество этого программного

продукта – это хорошая визуализация и простой понятный интерфейс. «Сетевой анализатор» использовался как экспресс-инструмент для того, чтобы:

- увидеть наличие goose-сообщений в сети;

- посмотреть значения переменной в dataset goose-сообщения;

-увидеть наличие SV-потока в сети;

-визуализировать данные SV-потока.

Если появляется необходимость более детального разбора поведения любого из устройств, применяется ПО WireShark. Функционал этого софта позволяет найти любой интересующий параметр передаваемого в сети пакета.

Испытательные установки, с которыми работал персонал, – это РЕТОМ 61850 и Omicron CMC 356 с пакетом ПО МЭК 61850. Использование этих устройств позволило выполнить весь необходимый объем проверок. К обязательным условиям проверок устройств РЗА на цифровой ПС стоит отнести и наличие минимум 2 ноутбуков и медиаконвертер у инженера СРЗА.

Также в состав оборудования эксплуатационного персонала необходимо добавлять весь спектр приборов для работы с ВОЛС (сварочный аппарат, измеритель мощности, рефлектометр, оптический тестер, микроскоп, источник видимого излучения).

Организация обслуживания устройств РЗА

Строительство подстанций, на которых используется стандарт МЭК 61850, требует новых знаний, которые необходимы специалистам служб РЗА. На сегодняшний момент мне не известны организации, проводящие на русском языке профильное обучение, способное полноценно подготовить инженера СРЗА к эксплуатации и наладке будущей ЦПС. Основные трудности, которые возникли у эксплуатационного персонала, связаны с настройкой сервиса синхронизации времени, коммутаторов ЛВС и проверкой оптических линий связи. Для понимания принципов работы этого оборудования необходимо знать основы протоколов RSTP, PTP, технологии VLAN. Хорошим началом введения в тему цифровых подстанций являются семинары компании «Теквел». Дополнительно инженеру РЗА необходимо получать углубленные знания по методам синхронизации времени и администрированию локальных сетей, понимать технологию передачи данных по оптико-волоконным линиям связи, способам контроля трафика в сети, иметь базовые навыки написания xml-кода. Считаю, что проблема обучения эксплуатирующего персонала – это в том числе и проблема производителей оборудования. Например, производитель не открывает полные алгоритмы работы узлов в логике устройства. У некоторых устройств недостаточно гибкая логика, например, мы не можем изменить условия пуска АПВ и т. д. Только предложив информацию в доступном виде, при проведении семинаров производитель может перебороть страх рядового релейщика перед оборудованием ЦПС. Дополнительно в службе РЗА должны присутствовать инженеры с профильным образованием по технологии компьютерных сетей и обслуживанию ВОЛС.

Уже в процессе наладочных работ стало ясно, что подходы к организации обслуживания устройств ЦПС сильно отличаются от привычных. Так, вывод устройств из работы не требует видимого обрыва, снятия опертока, вывода накладок.

Существенный минус устройств РЗА на ПС «Металлургическая» – это отсутствие специального сигнала в логике устройства, который мог бы выводить из работы тот или иной goose. Параметр, отвечающий за ввод тестовых меток в goose-сообщении, можно ввести только используя ИЧМ. При таком подходе оперативный персонал при необходимости вывода комплекса РЗА может только снять оперативное питание с устройства.

При обслуживании оборудования персоналом РЗА применяется два подхода:

1. Вывод в ремонт всех первых или вторых комплексов. Такой способ позволяет, используя существующую ЛВС, проверять терминалы защит и автоматики в комплексе и по отдельности. Первые и вторые комплексы работают независимо друг от друга и не имеют перекрестных связей. Благодаря этому ложные воздействия на работающее оборудование при проверках исключены.
2. Вывод в ремонт одного шкафа РЗА. В таком случае от терминала отсоединяются все оптические патчкорды. Для такой проверки необходимо строить ЛВС с терминалами защит, ноутбуками, испытательными установками. Это требует дополнительного оборудования: коммутатор, медиаконвертер, сервер времени.

Заключение

Несмотря на проблемы с подготовкой персонала и инертностью фирмы-изготовителя в решении вопросов при строительстве, у ЦПС есть ощутимые преимущества:

-возможность выполнять наладочные работы до реального строительства объекта;

-сокращение сроков монтажа вторичной коммутации;

-прозрачность всех процессов, происходящих на ПС. Постоянный мониторинг системой сбора информации, наличие goose-сообщений и данных SV-потоков;

-снижаются воздействия электромагнитного поля за счет применения оптических линий связи;

-отсутствуют проблемы с насыщением ТТ в случае применения оптических ТТ;

-уменьшается количество случаев замыканий на землю в оперативных цепях из-за небольшого количества медных кабелей;

-можно переходить на обслуживание комплекса РЗА «по фактическому состоянию».

Получив опыт строительства ЦПС РУП, «Гомельэнерго» планирует и дальше развивать это направление при новом строительстве или глубокой модернизации энергообъектов. Следующая на очереди – ПС 110 кВ с использованием КРУЭ и оптических ТТ и ТН. Руководство службы релейной защиты проводит политику непрерывного обучения персонала новым технологиям, делая акцент на теоретическую составляющую курса компьютерных сетей и методов тестирования оборудования ВОЛС. Одновременно пополняется состав программных и программно-технических средств, позволяющих полноценно обслуживать оборудование РЗА цифровой ПС.

1.7. ОПТИМИЗИРОВАННАЯ АРХИТЕКТУРА ЦПС. ОПЫТ ВНЕДРЕНИЯ ЦИФРОВЫХ СИСТЕМ ЗАЩИТ И УПРАВЛЕНИЯ В РАСПРЕДЕЛИТЕЛЬНЫХ СЕТЯХ

Н.Н. ДОРОФЕЕВ

ООО «ПиЭлСи Технолоджи»

Российская Федерация

Контактное лицо:

Н.Н. ДОРОФЕЕВ

dorofeev.n@tpz.ru

Ключевые слова: Оптимизированная архитектура ЦПС, цифровой распределительный пункт, цифровые системы защиты и управления, распределительные сети, опыт внедрения оптимизированной архитектуры ЦПС.

Введение

Развитие микропроцессорной техники является драйвером использования цифровых технологий в большинстве сфер современного общества. Энергетика – не исключение. Цифровизация функций защиты и управления ПС – неизбежный процесс эволюции.

Для работы функциональных алгоритмов устройств РЗА и АСУ ТП, работающих в структуре ЦПС II, III, IV архитектур, физическое устройство должно обладать лишь набором коммуникационных интерфейсов с соответствующими характеристиками, обеспечивающими интеграцию устройства в ЛВС шины подстанции и шины процесса. Это обстоятельство дает возможность раздельного рассмотрения аппаратной части устройства и его программного обеспечения.

Таким образом, любое устройство защиты и управления в аппаратной части и в части системного ПО превращается в некий промышленный компьютер, а функциональное наполнение обусловлено лишь набором инсталлированного ПО. Т. е. чтобы получить цифровой терминал, необходимо на специализированный промышленный компьютер под управлением ОС реального времени установить необходимый набор функциональных алгоритмов.

Специализированная аппаратная платформа должна соответствовать следующим требованиям:

- необходимая вычислительная мощность (в зависимости от набора прикладных функций),
- набор коммуникационных интерфейсов (не менее 4 портов Ethernet 100 или 1 000 Мбит/с),
- необходимый объем ОЗУ, ПЗУ (в зависимости от набора прикладных функций),
- наличие встроенного или подключаемого интерфейса «человек-машина»,
- охлаждение естественной конвекцией,
- соответствие требованиям по ЭМС для применения на ПС и станциях,
- соответствия требованиям по условиям применения на ПС и станциях,
- соответствие требованиям по электропитанию устройств РЗА и АСУ ТП.

Требования к программному обеспечению цифровых устройств РЗА и АСУ ТП:

- операционная система реального времени,
- скорость загрузки устройства, необходимая для устройств РЗА и ПА,
- встроенные средства обеспечения ИБ.

ООО «ПиЭлСи Технолоджи» пошло именно по этому пути при разработке устройств и комплексов РЗА и АСУ ТП цифровых подстанций.

Основная часть

Реализация прикладных функций защиты и управления выполняется набором логических узлов в соответствии с МЭК 61850 и корпоративным профилем данного стандарта. Таким образом, запустив на промышленном компьютере необходимый качественный и количественный состав логических узлов и коммуникаций между ними, мы получаем терминал с определенным набором функций, будь то защита, управление или любые другие. Ключевой момент тут состоит в том, что аппаратная часть устройства в данном случае не обладает определенной спецификой для выполнения того или иного набора функций, она универсальна и соответствует лишь, требованиям, предъявляемым выше. Таким образом, на идентичных компьютерах возможно реализовать терминал РЗА, контроллер присоединения, счетчик электроэнергии и т. д. Но также есть возможность запускать по несколько экземпляров «виртуальных» устройств или их комбинации на каждом компьютере в количестве, ограниченном лишь производительностью устройства.



Наша компания пошла по такому пути, в том числе при разработке комплекса автономного регистратора аварийных событий. Это лишь частный случай реализации концепции цифрового устройства РЗА. На аппаратную платформу из линейки TOPAZ производительностью, соответствующей объему обрабатываемых данных, инсталлированы экземпляры ПО регистратора по количеству сигналов контролируемых присоединений, состоящие из соответствующих логических узлов МЭК 61850.



Такой регистратор может принимать сигналы GOOSE и SV как из шины процесса и шины подстанции, так и иметь в составе шкафа ПАС и ПДС в качестве модулей ввода классических

дискретных и аналоговых сигналов. Во второй конфигурации устройство эксплуатируется на ряде подстанций 110-220 кВ в качестве автономного регистратора аварийных событий, а также аттестовано для применения в ПАО «Россети».

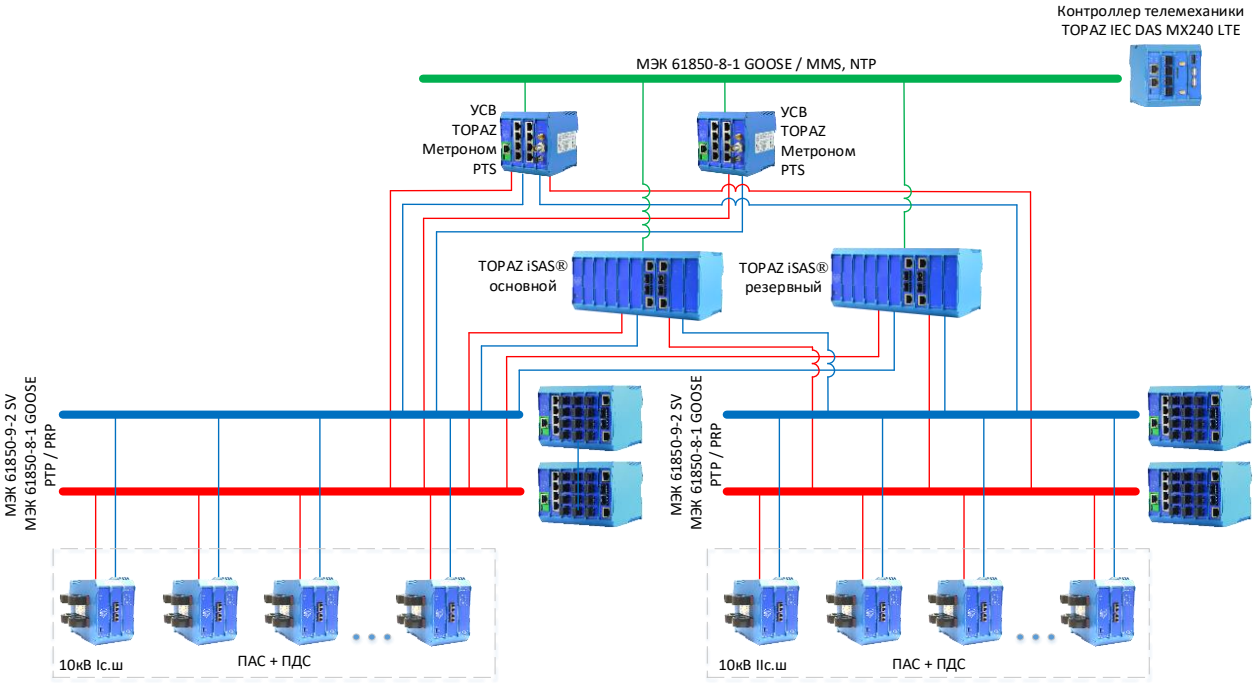
Рассмотрение функционального ПО отдельно от аппаратных платформ дает возможность построения системы защиты и управления цифровой подстанцией произвольной архитектуры. Т. е. при данном подходе возможно, как сохранение «классической» структуры распределения прикладных функций по физическим устройствам, так и централизация функций. Например, объединение различных защит одного объекта (КСЗ+ДЗЛ ВЛ), объединение однотипных защит нескольких объектов (защиты нескольких ВЛ) или объединение функций защиты и управления распределительным устройством как максимальная степень централизации. Безусловно, объединяя функции в одном физическом устройстве, мы повышаем уровень критической ответственности данного устройства, и, соответственно, во главу угла встает вопрос обеспечения надежности, который решается резервированием устройств (шкафов), несущих критические функции.

На наш взгляд, сама по себе технология ЦПС не несет фундаментально новых принципов защиты и автоматики. Технология позволяет лишь описать функции в виде логических узлов и стандартизирует коммуникационное взаимодействие между логическими и физическими устройствами, но она дает возможность применения новых архитектур, позволяющих оптимизировать подстанционные комплексы в части стоимости, выполняемых функций, надежности.

Централизация функций в данном случае есть метод снижения CAPEX и отчасти OPEX, это инструмент, который нам дает технология, а воспользоваться им или нет, необходимо решить на уровне нормативных актов, т. е. описать, где возможно применение централизации, а где нет.

Уже сегодня требования к АСУ ТП II и III архитектур описывают централизацию функций контроллера присоединения (1 контроллер на РУ), и это явный шаг в сторону оптимизации архитектуры ЦПС.

На наш взгляд, централизация уместна для реализации цифровых РЗА и телемеханики распределительных устройств 6-35 кВ. Наш опыт внедрения цифровых РП-10кВ позволяет сделать вывод, что стоимость централизованной цифровой системы защиты и управления соизмерима и конкурентна по стоимости с классическими системами аналогичного функционала.



Структурная схема цифрового РП-10 кВ.

Заключение

Применяя подход к раздельному рассмотрению аппаратной и логической частей устройств РЗА и АСУ ТП цифровых подстанций, мы получаем инструмент для создания любого устройства защиты и управления на универсальной программно-аппаратной платформе. Кроме этого, мы получаем возможность создания произвольных архитектур в части распределения функций по физическим устройствам как централизованных, так и децентрализованных. Решение о применении централизации функций должно лежать в области ответственности проектировщиков и регламентироваться нормативными актами, производитель должен дать лишь инструмент для построения той или иной концепции.

1.8. РАЗРАБОТКА КЛАСТЕРНОЙ ЦИФРОВОЙ ПОДСТАНЦИИ С ФУНКЦИОНАЛЬНО-ДИНАМИЧЕСКОЙ АРХИТЕКТУРОЙ

Д. М. ФЕРБИКОВ, М. А. ХЛЫСТОВ, Р. В. НЕУСТУПКИН

АО «РАСУ»

Российская Федерация

Контактное лицо:

Д. М. ФЕРБИКОВ

DMFerbikov@rasu.ru

Ключевые слова: Кластерная цифровая подстанция, функционально-динамическая архитектура.

Введение

В соответствии с программой инновационного развития и технологической модернизации Госкорпорации «Росатом» на период до 2030 года (в гражданской части), предполагающей развитие интеллектуальных электротехнических систем нового поколения, АО «РАСУ» ведутся разработки программно-технического комплекса (далее ПТК) «кластерная цифровая ПС» (далее КЦПС), основанного на применении стандарта IEC 61850 [1] и базирующегося на кластерном принципе с функционально-динамической архитектурой (далее ФДА). Данный ПТК предполагается внедрять на объектах энергетики в качестве продукта разработки ГК «Росатом».

В настоящее время не существует единого подхода к архитектуре цифровых подстанций, и на рынке представлены 4 варианта построения ПТК ЦПС [2], основанных на различной глубине применении в ПТК стандарта IEC 61850:

1. Архитектура построения ПС I типа, в которой обмен всей информацией между устройствами РЗА осуществляется дискретными и аналоговыми электрическими сигналами, передаваемыми по контрольному кабелю. Информационный обмен с верхним уровнем (SCADA) осуществляется по цифровому протоколу MMS;
2. Архитектура построения ПС II типа, в которой взаимодействие между устройствами РЗА выполняется при помощи объектно-ориентированных сообщений (протокол GOOSE), согласно стандарту МЭК 61850-8-1. Информационный обмен с верхним уровнем (SCADA) осуществляется по цифровому протоколу MMS. Измерения токов и напряжений передаются в виде электрических аналоговых сигналов с использованием контрольных кабелей;
3. Архитектура построения ПС III типа, в которой взаимодействие между устройствами РЗА выполняется при помощи объектно-ориентированных сообщений (протокол GOOSE), согласно стандарту МЭК 61850-8-1. Информация от измерительных устройств тока и напряжения передается в цифровом виде с использованием протокола передачи мгновенных значений (SV), согласно стандарту МЭК 61850-9-2. Информационный обмен с верхним уровнем (SCADA) осуществляется по цифровому протоколу MMS;
4. Архитектура построения ПС IV типа – централизованная ЦПС, в которой функции защиты и управления ПС реализованы в виде программных модулей, размещающихся на высокопроизводительной аппаратной платформе (сервере). Информационное взаимодействие компонентов выполняется аналогично архитектуре III.

Внедрение ПТК ЦПС направлено на достижение следующих базовых целей [3]:

– повышение качества и надежности функционирования;
– снижение затрат на создание и эксплуатацию.

Существующие в настоящий момент на рынке технические решения не в полной мере удовлетворяют описанным выше целям, т. к. основной массой производителей на данный момент времени построение цифровой подстанции осуществляется путем замены традиционных терминалов на терминалы с цифровыми интерфейсами с поддержкой МЭК 61850. При данном подходе к количеству терминалов, равному количеству терминалов в традиционной архитектуре подстанции, добавляется значительное количество дополнительного оборудования (коммутаторы, merging unit, устройства синхронизации времени и т. д.). Большее количество оборудования увеличивает стоимость создания и эксплуатации и без дополнительных проектных решений снижает надежность системы.

Для достижения требуемых целей создания ПТК ЦПС была разработана новая архитектура ПТК – кластерная ЦПС с функциональной динамической архитектурой. Данная архитектура может рассматриваться как гармоничный симбиоз архитектур № 3 и № 4, сочетающий лучшие характеристики данных архитектур.

Основная часть

КЦПС с функциональной динамической архитектурой построена на следующих основных понятиях.

1. **Кластер**. Кластером именуется совокупность устройств, включающих в себя источники первичной информации (устройства полевого уровня), коммутаторы и приемники первичной информации (устройства уровня присоединений – IED-устройства), объединенных по принципу концентрации наибольшего объема коммуникационного трафика внутри кластера. При формировании кластера дополнительно могут учитываться устоявшиеся регламенты эксплуатации, топологическое разделение по РУ и секциям. Первичной информацией считаются потоки данных в формате протокола МЭК 61850-9-2, данные в формате GOOSE-сообщений. Передача и прием первичных данных за пределы кластера не исключена, но должна иметь меньшую интенсивность и объем. Один и тот же источник первичных данных может являться источником данных для различных кластеров. Формирование кластеров выполняется на этапе проектирования.

2. **cIED**. Специализированные IED-устройства унифицированы и реализованы в промышленном исполнении для объектов энергетики в форм-факторе сменных аппаратных модулей (далее compact IED или cIED), устанавливаемых в шасси. Шасси обеспечивает коммуникационную функцию передачи и приема информации как между cIED внутри шасси, так и вне шасси. Шасси обеспечивает резервированное электропитание cIED, соблюдение теплового режима, защиту от внешних механических воздействий и электромагнитных помех, допускает «горячую» установку и извлечение модулей. Реализация модульной структуры с применением шасси снижает себестоимость изделий за счет меньшей механо- и материалоемкости в сравнении с традиционным решением, предусматривающим реализацию устройств в виде отдельных терминалов за счет применения общих конструктивных элементов, таких, как корпус, блок питания и коммуникационные модули.

3. **softIED**. Программное обеспечение IED-устройств (далее softIED) обеспечивает выполнение набора функций защиты и автоматизации подстанции и может быть запущено на любом из унифицированных аппаратных модулей (cIED). Первоначальное размещение softIED в пределах кластеров и шасси определяется на основании проектного решения, но в дальнейшем допускается, что под влиянием внешних и/или внутренних событий (например, отказ одного из модулей) определенный softIED будет запущен на свободном модуле (резервном) либо модуле, выполняющем менее приоритетную задачу, автоматически – без участия оператора. Реализация данного функционала позволяет значительно повысить надежность и отказоустойчивость системы, в результате использования функционально-динамической архитектуры превышающую надежность отдельно взятого элемента и не требующую дублирования всех устройств. Введение нового softIED либо замена любого из softIED не требует отключения и/или переконфигурирования остальных устройств (за исключением автоматических операций, выполняемых в рамках ФДА).

4. **Функционально-динамическая архитектура (ФДА).** В рамках cIED реализуется независимое от softIED программно-аппаратное решение, обеспечивающее реализацию

функционально-динамической архитектуры. В рамках ФДА предусматривается контроль работоспособности cIED и выполнения softIED, перераспределение функций при выявлении отказа или значительной неэффективности текущего распределения (при наличии более эффективного распределения), автоматическая блокировка отдельного softIED при выявлении программного сбоя, обеспечение работоспособности softIED в зависимости от приоритетности функций, им исполняемых. Указанный функционал выполняется без выделения центрального узла принятия решений – система гомогенна и выдерживает отказ любого из модулей.

5. **Либерализация рынка ПО.** Разделение аппаратного исполнения IED-устройства и программного обеспечения (softIED) позволяет расширить перечень возможных поставщиков решений, включив в него разработчиков ПО и алгоритмов, например, профильные институты и научные организации, небольшие коллективы разработчиков. Помимо аппаратного исполнения IED устройства, предусматривается разработка комплекса программных и отладочных средств (SDK), сервисов, обеспечивающих возможность для сторонних разработчиков выполнять разработку и продажу собственных программ (softIED). Данный подход позволит сформировать новый сегмент на рынке решений по автоматизации, изменить роли и место участников в уже существующих сегментах рынка.

6. **Интероперабельность.** Решение совместимо с IED-устройствами других производителей в части информационно-коммуникационного обмена, может резервировать или резервироваться IED-устройствами сторонних производителей, работать совместно с IED-устройствами других производителей за счет применения протоколов стандарта МЭК 61850.

Данные базовые принципы определяют архитектуру решения, нацеленного на снижение стоимости оборудования и ПО, снижение эксплуатационных затрат и повышение надежности.

Кластерная ЦПС интегрируется в шину станции и шину процесса, внедряемого ПТК, по аналогии с другими IED-устройствами (терминалами РЗА, КП, РАС) и не налагает специализированных требований в части организации полевого уровня. Источником аналоговых и дискретных сигналов для кластера являются преобразователи аналоговых и дискретных сигналов (ПАДС) шины процесса. Для передачи аналоговых величин используется протокол SV в соответствии со стандартом МЭК 61850-9.2. Для передачи дискретных сигналов от/к ПАДС и обмена сигналами между cIED используется протокол GOOSE в соответствии со стандартом МЭК 61850-8.1. Передача информации на верхний уровень ПТК выполняется по протоколу MMS в соответствии со стандартом МЭК 61850-8.1.

Средства контроля, защиты и управления (уровень IED-устройств)

IED-устройства реализуются как совокупность программно-аппаратного модуля (cIED) и функционального программного обеспечения (softIED). Архитектура решения предусматривает, что аппаратное и программное обеспечение могут быть разработаны и изготовлены разными компаниями независимо друг от друга. Функциональность программного обеспечения (softIED) определяется разработчиком программного обеспечения. В состав cIED, помимо непосредственно аппаратного обеспечения модулей, включается программно-аппаратный узел (далее FDA core), функционирующий независимо от вычислительного ядра, отвечающего за исполнение функционального программного обеспечения, и обеспечивающий функционирование механизмов ФДА и выполнение сервисных функций.

Шасси кластерной ЦПС обеспечивает выполнение коммуникационных функций для всех cIED, установленных в него. В связи с этим значительно сокращается потребность в коммутаторах и линиях связи, повышается надежность коммуникаций. Шасси поддерживают возможность подключения как к обычной Ethernet-сети, так и к сетям высокой доступности (PRP, HSR в соответствии с МЭК 62439-3). Использование шасси с интегрированными коммуникационными функциями позволяет сократить количество коммутаторов и линий связи в кластерной ЦПС более чем на 40% (в сравнении с традиционными архитектурами ЦПС №№ 1-4).

В рамках ПАК КЦПС в настоящее время реализуются следующие подсистемы:

– управления и телемеханики;
– релейной защиты и противоаварийной автоматики;
– регистрации аварийных событий (РАС);
– определения места повреждения (ОМП);
– учета электрической энергии;
– контроля качества электрической энергии (ККЭ).

Новые принципы резервирования кластерной ЦПС

Помимо традиционных средств обеспечения надежности работы кластерной ЦПС, включающей в себя в том числе резервирование оборудования и коммуникационной сети, предусматривается реализация следующих новых принципов резервирования, позволяющих качественно повысить надежность функционирования ПТК.

1. **Скользящий резерв**. В состав шасси вводится несколько резервных cIED. В случае отказа любого из основных cIED его функции (softIED) автоматически запускаются на одном из дополнительных cIED. В рамках данной схемы реализуется схема резервирования «N+m», где небольшое количество резервных модулей «m» резервирует целый пул из N устройств с различными функциями. В вырожденном случае реализуется схема «N+1». Количество резервных модулей определяется проектировщиком и может быть легко изменено в процессе эксплуатации.

2. **Вытесняющий резерв**. Всем функциям устройств (softIED) присвоен определенный приоритет. При отказе cIED средствами FDA производится поиск кандидата на вытеснение среди других cIED, выполняющих функции с меньшим приоритетом. При положительном исходе поиска запуск более приоритетной задачи вместо задачи, имеющей меньший приоритет, выполняется автоматически.

3. **Скамейка запасных**. Особый режим softIED («запасной»), дублирующий по набору реализованных функций действующий softIED, но реализованный другим разработчиком. «Запасной» softIED не выполнятся ни на одном из cIED. При выявлении режима циклических отказов действующего softIED в рамках ФДА принимается решение по замене данного softIED на «запасной» softIED. Использование данного режима предусматривается для особо ответственных задач и позволяет автоматически выявить и устранить ПО с проявившейся систематической ошибкой.

Реализация указанных алгоритмов предусматривает гибкие возможности для конфигурирования, в том числе отключающие или ограничивающие применение указанных методов. Способ применения тех или иных механизмов определяется пользователем системы либо в рамках проектирования.

Технико-экономическая эффективность кластерной ЦПС

Новая архитектура построения ПТК ЦПС в совокупности с новыми алгоритмами резервирования позволяет достичь базовых целей внедрения «цифровых» технологий. Внедрение КЦПС позволит получить:

Сокращение капитальных затрат (CAPEX)

1. Снижение стоимости оборудования и программного обеспечения, которое достигается за счет следующих факторов:

–унификация аппаратного исполнения модулей позволяет, снизив номенклатуру изготавливаемых модулей, повысить их серийность (количество одинаковых модулей), что значительно сокращает стоимость компонентов, накладные расходы, стоимость производства устройств;

–стоимость подсистемы электропитания переносится на группу устройств, т. е. на стоимость шасси;

–отсутствие индивидуальных корпусов устройств. Модули устанавливаются в единое шасси, при реализации которого достигается более высокое качество и меньшая стоимость, чем при индивидуальной реализации для каждого из устройств;

–интегрированное в шасси коммуникационное решение для взаимодействия cIED внутри шасси позволяет отказаться от дорогостоящих оптических интерфейсов для подключения каждого IED-устройства, сократить количество коммутаторов с оптическими интерфейсами в составе ЛВС ЦПС, снизить стоимость подключения IED-устройств за счет реализации интерфейса заводской готовности (установка модуля в шасси вместо использования внешнего патч-корда, прокладываемого вне защищенного корпуса шасси и включения в обычные незащищенные разъемные соединения);

–реализация программно-аппаратного cIED позволяет снизить затраты разработчиков на низкоуровневое программирование (поддержка аппаратуры, информационных протоколов, типовых процедур и т. д.);

–открытость архитектуры и средств разработки (SDK) приводит к повышению качества конкурентной борьбы между разработчиками, увеличению количества разработчиков и включению в их состав небольших научных коллективов, не обладающих на данный момент потенциалом к разработке изделия целиком, но имеющих собственные перспективные алгоритмические наработки.

2. Сокращение количества и номенклатуры оборудования.
3. Сокращение площади земельного участка, требуемого для строительства ПС.
4. Сокращение требуемой площади зданий и помещений ПС.
5. Сокращение и упрощение функциональных цепей вторичных соединений, клеммных рядов, кабельных связей.
6. Замена большого количества электрических кабелей малым количеством интерфейсного кабеля.
7. Сокращение времени на проектирование до 25% за счет типизации схемных и функциональных решений
8. Сокращение объема монтажных и наладочных работ до 50%.

Снижение операционных расходов (OPEX)

1. Снижение эксплуатационных затрат на техническое обслуживание, которое достигается за счет следующих факторов:

–унификация аппаратного исполнения IED-устройств позволяет сократить количество и номенклатуру ЗИП, упростить обучение персонала, сократить количество ошибок персонала, вызванное необходимостью обслуживания оборудования разных производителей;

–удешевление модернизации, достигаемое за счет возможности обновления ПО модулей, расширение функциональных возможностей установкой дополнительных модулей, возможность использования освободившихся модулей для решения новых задач для систем защиты и управления объекта;

–самовосстановление позволяет снизить требования к оперативности устранения отказов, обеспечив возможность перехода на обслуживание подстанции без постоянного присутствия персонала, сократить состав и количество выездных дежурных бригад и другого персонала;

–при реализации softIED разработчиками, имеющими реализацию устройств в традиционном виде, возможно сохранение средств конфигурирования и поддержки эксплуатации в виде, привычном для эксплуатирующего персонала. Данный подход позволяет сократить затраты на разработку ПО и не требует дополнительного обучения эксплуатирующего персонала.

2. Повышение надежности и отказоустойчивости ПТК ЦПС, которое достигается за счет следующих факторов:

–повышение качества аппаратного обеспечения, достигаемое на большей партии выпущенных устройств (на большей партии значительно быстрее выявляются недостатки аппаратуры, ее слабые места и более оперативно устраняются данные недостатки);

–простота и дешевизна аппаратных модулей позволяет внедрять резервирование для систем, не имеющих критически важного значения (например, АСУ ТП). В частности, резервирование модулей АСУ ТП может осуществляться в едином комплексе с резервированием РЗА. При этом стоимость резервирования по системе «N+1» (один модуль резервирует группу из N модулей) значительно меньше, чем стоимость дублирования (схема «2N»);

–система предусматривает эшелонированное резервирование критически важных систем (сначала резервные модули, потом модули с менее приоритетными задачами), что обеспечивает намного более высокий уровень отказоустойчивости, чем традиционное дублирование;

–восстановление работоспособности даже самой низкоприоритетной функции производится автоматически при наличии свободных модулей либо при появлении подобного модуля, что позволяет быстро и оперативно восстановить работоспособность системы путем механической замены, вышедших из строя модулей;

–свобода в выборе программного обеспечения позволяет в большем объеме выполнять резервирование функций алгоритмами и ПО от различных разработчиков;

–реализация ПО отдельно от аппаратного обеспечения и механизмы сертификации ПО обеспечивают большую прозрачность, независимость и качество тестирования ПО;

–доступность аппаратной части терминалов, реализация в них рутинных процедур взаимодействия с аппаратными узлами и коммуникационных протоколов ускоряют разработку и снижают трудоемкость реализации новых алгоритмов, открывают выход на рынок для инновационных решений, в том числе от небольших научных коллективов, молодых команд разработчиков;

–использование интегрированного в шасси коммуникационного решения повышает надежность коммуникаций, так как используются резервированные коммуникационные тракты высокой заводской готовности внутри защищенного шасси вместо внешних кабелей,

прокладываемых в том числе на значительные расстояния, имеющих высокую вероятность повреждения и не обеспечивающих гарантированное серийным производителем качество изготовления (например, обжимка на месте монтажа или сварка оптических волокон, осуществляемая непосредственно на объекте выездной бригадой).

3. Переход от планового технического обслуживания по времени к обслуживанию по состоянию за счет глубокой online-диагностики оборудования и реализации новых видов резервирования и самовосстановления системы.

4. Сокращение количества инцидентов информационной безопасности объекта [4] за счет повышения «киберзащищенности» ПТК, которое достигается за счет следующих факторов:

–сокращение количества доступных коммуникационных интерфейсов за счет интегрированного в шасси коммуникационного решения уменьшает количество потенциальных мест для проникновения в сеть ЦПС;

–независимость функционального ПО от системных функций и аппаратного обеспечения сокращает возможности для реализации вредоносных воздействий;

–повышение культуры и безопасности обслуживания объекта оперативным персоналом, уменьшение влияния «человеческого фактора», сокращение ущерба от неправильных действий персонала.

Заключение

Кластерная цифровая подстанция с функционально-динамической архитектурой является перспективным направлением в построении программно-технических комплексов защиты и управления энергообъектов, которое позволяет более эффективно по сравнению с представленными в настоящий момент техническими решениями достигать базисных целей внедрения цифровых технологий в электроэнергетике. Открытость архитектуры и независимость функционального (алгоритмического) программного обеспечения от аппаратной части позволяет реализовывать и другие алгоритмы промышленной автоматизации для применения новых цифровых технологий в других сферах промышленности.

СПИСОК ЛИТЕРАТУРЫ

[13]Туев Л. Е. Применение стандарта МЭК 61850 при проектировании цифровых подстанций // Энигма. 2020. №22-2. С. 184-191.

[14]Извеков Е. А., Грицинин Н. М. Конфигурации цифровых подстанций в современных электроэнергетических системах. // Энергоэффективность и энергосбережение в современном производстве и обществе. Материалы международной научно-практической конференции. 2020. С. 30-37

[15]Кириллов А. С., Кузьмина А. А. Кластерная цифровая подстанция в разрезе задач релейной защиты. // Релейщик. 2018. №1 (31). С. 18-23

[16]Латышов К. В., Волошин А. А. Проблемы обеспечения информационной безопасности цифровых подстанций. // Радиоэлектроника, электротехника и энергетика. 2021. Тезисы доклада на конференции. С.350.

1.9. ОПЫТ НАЛАДКИ И ЭКСПЛУАТАЦИИ МП УСТРОЙСТВ РЗА НА ЦПС

Е. П. ЕГОРОВ, И. А. КОШЕЛЬКОВ, М. А. ХЕ, Н. А. ТОЙДЕРЯКОВ

ООО НПП «ЭКРА»

Российская Федерация

Контактное лицо:

Е. П. ЕГОРОВ

ekra@ekra.ru

Ключевые слова: Цифровая подстанция, IEC 61850, ИЭУ (интеллектуальное электронное устройство).

Введение

В декабре 2018 года советом директоров ПАО «Россети» утверждена Концепция «Цифровая трансформация 2030». В качестве одной из приоритетных технологий выбрана «Цифровая подстанция» – различные архитектуры построения цепей защит и автоматики с применением стандарта IEC 61850. В конце первого квартала 2019 года введен СТО «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций (ЦПС) напряжением 110-220 кВ и узловых ЦПС напряжением 35 кВ», в котором описаны требования в том числе и к системам РЗА и АСУ ТП, работающим с применением стандарта IEC 61850. В 2020–2021 годах принят ряд СТО ФСК ЕЭС, регламентирующих применение типовых шкафов РЗА и АСУ ТП на ЦПС различных архитектур.

Первые опытные образцы интеллектуальных электронных устройств (ИЭУ – IED) с поддержкой стандарта IEC 61850 были созданы на ООО НПП «ЭКРА» более 10 лет назад, в 2008 году. В первую очередь была реализована поддержка MMS (Manufacturing Message Specification) сервисов и горизонтального обмена с помощью GOOSE (Generic Object-Oriented Substation Event) [1]. В 2012 году на предприятии были проведены лабораторные испытания прототипов устройств РЗА и ПА с поддержкой IEC 61850-9-2LE совместно с прототипами устройств merging unit (MU). Начиная с 2013 года реализован ряд пилотных проектов. Такой подход позволил предприятию в 2015 году получить сертификат соответствия требованиям IEC 61850 для ИЭУ в испытательной лаборатории KEMA и в 2018 году ввести в промышленную эксплуатацию ЦПС напряжением 110 кВ.

На сегодняшний день специалистами ООО НПП «ЭКРА» реализовано около 30 объектов ЦПС как в опытной, так и в промышленной эксплуатации по всей России. Получен опыт проектирования, проведения испытаний и наладки вторичного оборудования на объектах ЦПС. Были опробованы различные варианты организации шины процесса и шины станции на объектах и даже различные архитектуры построения самих защит (децентрализованные и централизованные защиты).

РЕАЛИЗАЦИЯ ЦПС

Резервирование и синхронизация оборудования для цпс

Традиционно устанавливаемое на подстанции сетевое оборудование относилось к компетенции специалистов автоматизированных систем управления (АСУ), и необходимость разбираться в его работе и настройках релейному персоналу отсутствовала. Сегодня становится актуальным вопрос: «На чьи плечи «падает» груз настройки и обслуживания сетевого оборудования, обеспечивающего работы шины процесса и шины станции?» В частности, для работы всего оборудования подстанции с цифровым управлением необходим правильно выбранный сетевой коммутатор, обеспечивающий поддержку всех требуемых протоколов (в том числе аппаратная поддержка PTP). Требуется обеспечить направление трафика между портами непосредственно в коммутаторе таким образом, чтобы обеспечивалась корректная работа всего объединённого сетью оборудования. Иногда, например, с целью снижения капитальных затрат, в проекте трафик-сервисов MMS и GOOSE обеспечивают одни и те же коммутаторы. Все вышесказанное формирует очевидный вывод: проектировщики МП РЗА и инженеры службы РЗА должны расширить свои компетенции в сфере сетевых коммуникаций.

Наличие дублирующего порта для каждого сетевого интерфейса позволяет обеспечить резервирование передачи информации, поддерживать протоколы «бесшовного резервирования

высокой доступности» (HSR – High Availability Seamless Redundancy) и «параллельного резервирования» (PRP – Parallel Redundancy Protocol) в случае возникновения отказов [6]. Это особо важно для автоматизации и управления технологическими процессами в приложениях, которые в своей работе полностью зависимы от скорости, точности времени и не могут допускать потери пакетов и задержки.

В качестве примера на рис. 6 представлена схема организации сетевого трафика для ПС 110/20 кВ «Медведевская». Проектом предусмотрено разделение всего трафика на три независимых кольца: сеть АСУ (шина станции), включая MMS-трафик, шина процесса GOOSE (обмен дискретными сигналами), шина процесса SV (выборочные значения аналоговых данных). Для реализации предложенного варианта с целью обеспечения резервирования шины процесса GOOSE в шкафах РЗА дополнительно устанавливались устройства резервирования RedBox (Redundancy Box) (рис. 7), что позволило организовать PRP-резервирование в соответствии с требованиями стандарта IEC 61850.

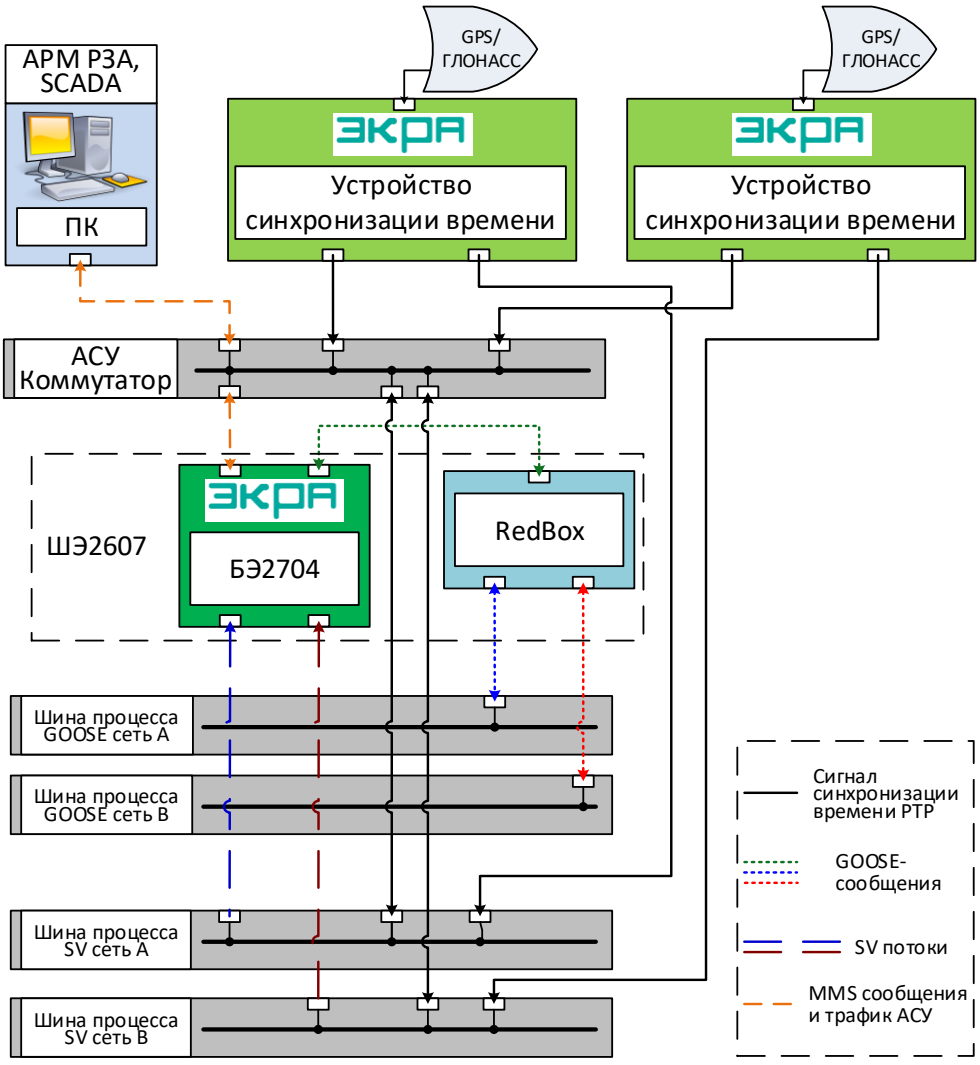


Рис. 6. Схема организации сетевого трафика для ПС Медведевская.

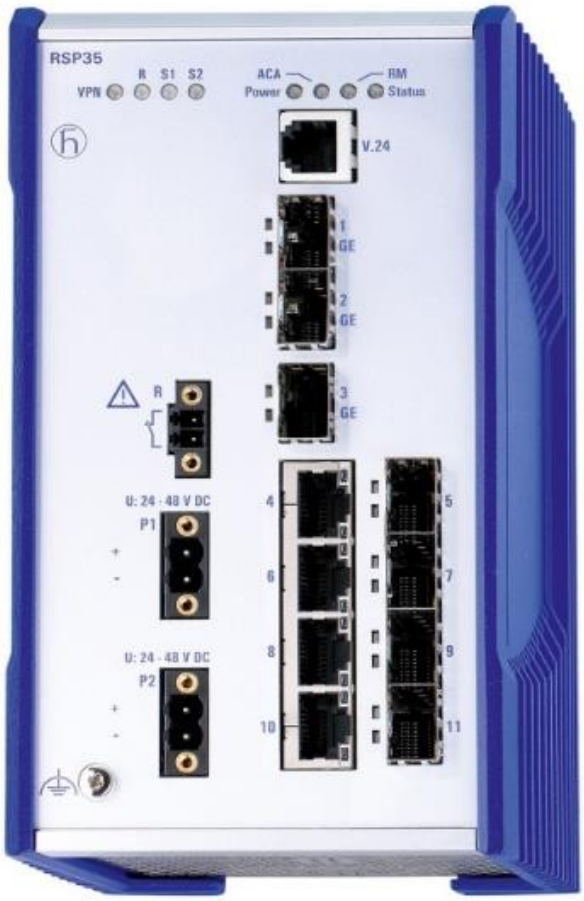


Рис. 7. Устройство RedBox

Аналоговые величины от измерительных трансформаторов тока и напряжения присоединений поступают на устройства для преобразования аналоговых сигналов ПАС, которые в широковещательном формате не только транслируют SV-потоки в шину процесса, но и получают через неё сигнал PTP от устройств синхронизации времени через коммутаторы (рис. 8).

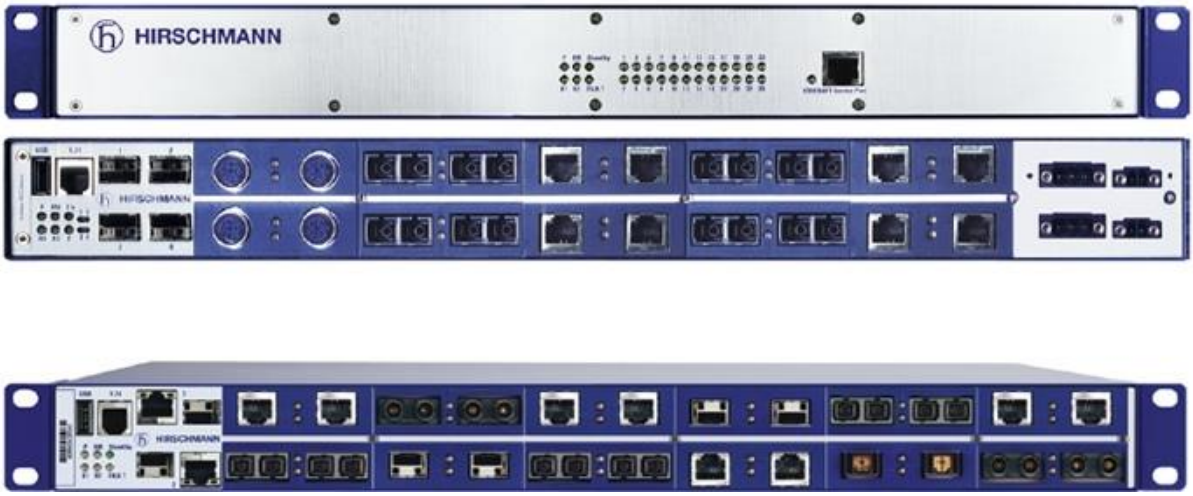


Рис. 8. Специализированные коммутаторы для электрических подстанций.

Перед поставкой всего комплекса оборудования устройства прошли заводские приёмо-сдаточные испытания в полном объёме, необходимом для МП РЗА, и, дополнительно, испытания на соответствие требованиям стандарта IEC 61850 всех поддерживаемых сетевых протоколов и коммуникационных сервисов. Завершающим этапом заводских испытаний являлась комплексная проверка оборудования, прошедшего соответствующее параметрирование для работ в сети. Дополнительно были проверены правильность измерения терминалами РЗА токов и напряжений, получаемых по коммуникационному сервису SV, взаимодействие (дискретные сигналы) с использованием GOOSE-сообщений, работа Supervisory Control and Data Acquisition (SCADA) системы с применением протокола MMS, в том числе управление коммутационными аппаратами и электронными оперативными переключателями.

Особенности конфигурирования GOOSE и SV

Для работы GOOSE-сообщений необходимо настроить несколько параметров: MAC-адрес широковещательной передачи данных, идентификатор приложения APPID и идентификатор Goose – GoID, которые должны быть уникальны для каждого устройства в сети (не должно быть два и более одинаковых APPID и GoID в одной подсети); приоритет и номер виртуальной подсети VLAN; параметр quality, который указывает состояние поля качества q при передаче сообщений; период отправки сообщений при отсутствии изменений. Когда заданы все необходимые параметры для устройства, может быть сформирован CID-файл (Configured IED Description), в котором описывается вся необходимая для дальнейшего взаимодействия информация об одном IED (Intellectual electronic device). Необходимость поддержки импорта файлов ICD указана в стандарте IEC 61850.

Для настройки подписки на GOOSE-сообщения широкое распространение получил метод Push-and-Drop, который должен упростить процесс наладки. Суть метода заключается в «перетаскивании» нужного сообщения на соответствующий вход IED-устройства из одной области экрана (в которой обычно располагается список доступных устройств с публикуемыми сообщениями) в другую. На рис. 9 показан пример окна настройки входящих сообщений фирменного программного обеспечения (ПО) австрийской компании Omicron. В левой верхней части экрана пользователю показаны доступные для конфигурирования двоичные входы, в нижней левой части – список доступных устройств с набором сообщений (на примере показано одно

устройство), в нижней правой части отображаются параметры выбранного IED-устройства. Для настройки входа выбирается необходимый сигнал, который «перетаскивается» на соответствующий вход.

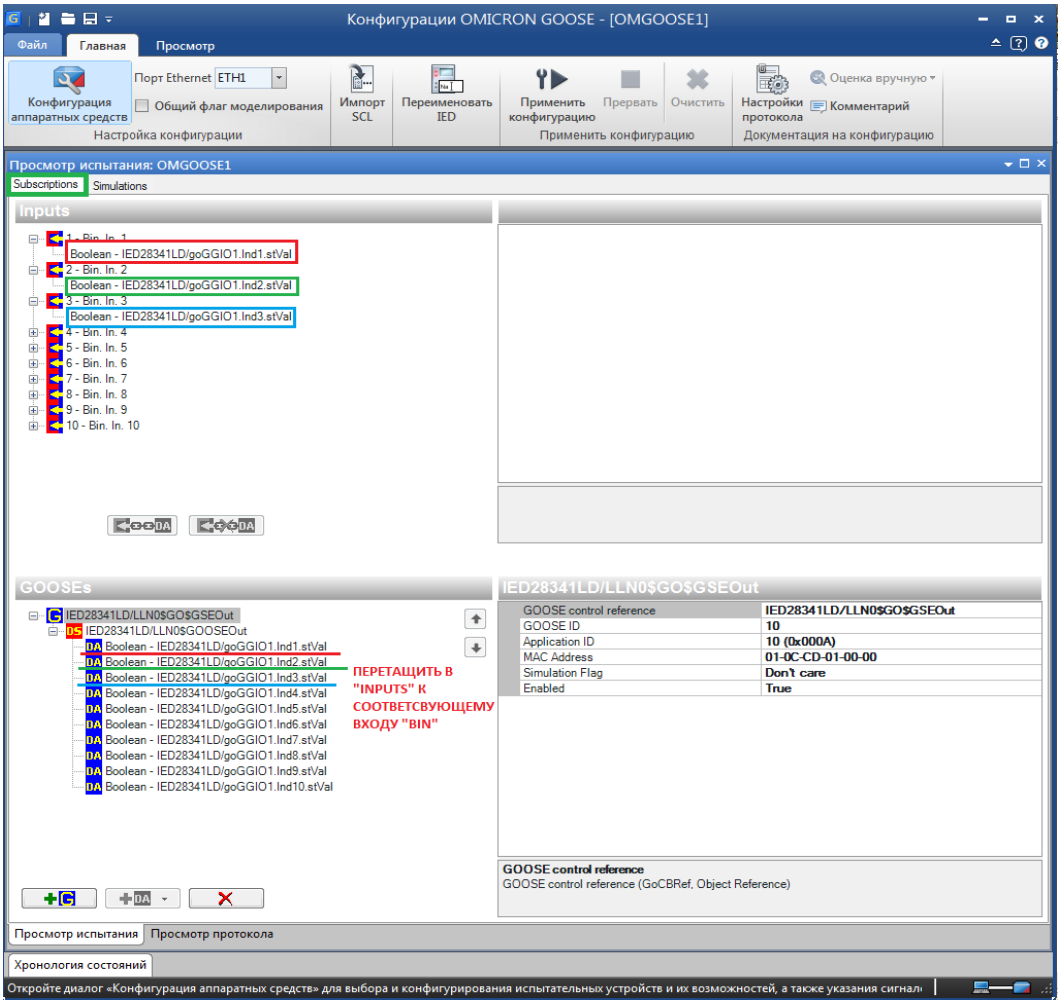


Рис. 9. Окно конфигурирования GOOSE-сообщения на вход устройства в ПО GOOSE Configuration для Omicron CMC

Как показала практика, этот метод (Push-and-Drop) удобен при настройке небольшого количества устройств. Когда возникает необходимость настройки четырех и более устройств, каждое из которых публикует в сеть по несколько десятков сигналов в GOOSE-сообщении, для того, чтобы найти нужное сообщение, уходит немало времени и сил, увеличивается вероятность ошибки, которую сложно обнаружить на этапе приемо-сдаточных испытаний.

Для реализованных ЦПС APPID, GoID и IP-адреса устройств задавались таким образом, что наладчик, зная только идентификатор GoID, уже имеет представление об остальных параметрах. Наиболее удобным способом настройки входящих GOOSE-сообщений в случае с ПС «Медведевская» признан табличный вариант, пример приведён на рис. 10. Очевидно, что при настройке сообщений от одного источника отличается только номер элемента данных, входящих сообщений. Ошибки при таком представлении параметров заметны сразу, а вероятность механической опечатки стремится к нулю, т. к. используется метод «копировать – вставить».

Наименование	Разрешение в...	Значение вхо...	Групповой MAC адрес ...	Числовой иде...	Строковый идентификато...	Ожидаемое з...	Номер элемен...	Тип элемента д...
Вход GOOSE 31	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	5	boolean
Вход GOOSE 32	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	8	boolean
Вход GOOSE 33	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	7	boolean
Вход GOOSE 34	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	10	boolean
Вход GOOSE 35	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	9	boolean
Вход GOOSE 36	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	14	boolean
Вход GOOSE 37	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	13	boolean
Вход GOOSE 38	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	12	boolean
Вход GOOSE 39	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	11	boolean
Вход GOOSE 40	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	16	boolean
Вход GOOSE 41	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	15	boolean
Вход GOOSE 42	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	18	boolean
Вход GOOSE 43	есть	выкл	010CCD010107	107	W4G_DMU13_107	1	17	boolean
Вход GOOSE 44	есть	выкл	010CCD010062	62	QCG_P18_062	1	36	boolean
Вход GOOSE 45	есть	выкл	010CCD010062	62	QCG_P18_062	1	37	boolean
Вход GOOSE 46	есть	выкл	010CCD010062	62	QCG_P18_062	1	38	boolean
Вход GOOSE 47	есть	выкл	010CCD010067	67	W4G_P22_067	1	1	boolean
Вход GOOSE 48	есть	выкл	010CCD010068	68	W4G_P23_068	1	1	boolean
Вход GOOSE 49	есть	выкл	010CCD010083	83	KG_P33_083	1	18	boolean
Вход GOOSE 50	есть	выкл	010CCD010083	83	KG_P33_083	1	31	boolean
Вход GOOSE 51	есть	выкл	010CCD010084	84	KG_P34_084	1	18	boolean
Вход GOOSE 52	есть	выкл	010CCD010084	84	KG_P34_084	1	31	boolean
Вход GOOSE 53	есть	выкл	010CCD010070	70	W4G_P24_070	1	1	boolean
Вход GOOSE 54	есть	выкл	010CCD010108	108	W4G_DMU14_108	1	8	boolean

Рис. 10. Окно конфигурирования входящих GOOSE-сообщений в ПО Atlas для терминала БЭ2704.

Настройка устройства МП РЗА для работы с коммуникационным сервисом SV незначительно отличается от настроек для GOOSE-сообщений. Аналоговые величины в формате SV-потоков, так же, как и GOOSE-сообщения, передаются в широковещательном формате (multicast) от источника и обрабатываются только устройствами-подписчиками. На один поток может быть подписано теоретически неограниченное число устройств МП РЗА, при этом нагрузка на измерительные трансформаторы тока не увеличивается. Идентификация потоков устройствами-подписчиками, в соответствии с требованиями стандарта, осуществляется по MAC-адресу широковещательной передачи данных, идентификатору потока (svID) и идентификатору приложения (APPID). К идентификатору потока (svID) предъявляется строгое требование уникальности в рамках одного объекта (сети), идентификатор приложения (APPID) настоятельно рекомендуется задавать также уникальным в сети. Дополнительно при работе с SV может быть определён номер виртуальной сети (VLAN ID), что позволяет при соответствующей настройке коммутатора снизить нагрузку на коммуникационный процессор устройства МП РЗА, обрабатывающий SV-потоки, и порт коммутатора. Учитывая небольшое количество установок потоков SV, для настройки не требуется новых программных решений, на рис. 11 показано окно программы EKRASMS с параметрами потока.

Защита трансформаторов. Поток 1-1

Параметр	Текущее значение
MAC-адрес	010CCD040001
AppID	16385
svID	OMICRON_CMC_SV1
VLAN ID	0

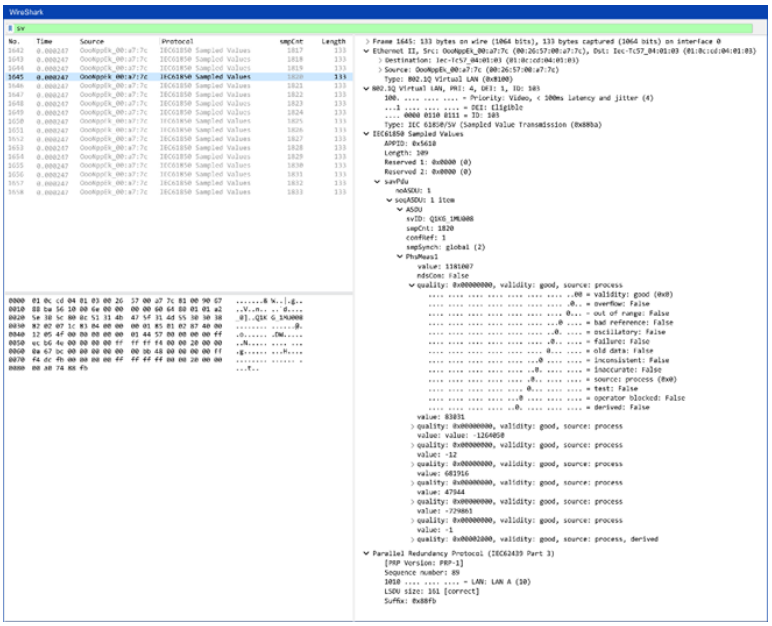
Рис. 11. Окно конфигурирования SV-потоков в терминале БЭ2704 в ПО EKRASMS.

Настройка испытательного оборудования тоже несколько отличается от привычных для наладчика действий. Особое внимание нужно уделить вопросу синхронизации времени. Испытательные установки РЕТОМ и Omicron поддерживают различные варианты синхронизации времени: с применением протокола точного времени PTP, от сигнала 1PPS, протокол IRIG-B и т. д. Допустимым при проведении приемо-сдаточных испытаний и одновременно наиболее простым вариантом является имитация флага синхронизации от внутренних часов испытательной установки.

Поиск неисправностей

При проведении испытаний устройств, взаимодействующих согласно стандарту IEC 61850, возникают ошибки, обусловленные некорректной настройкой оборудования связи, устройств синхронизации времени и самих устройств МП РЗА в части описываемых протоколов и коммуникационных сервисов. Для выявления причин возникновения таких ошибок используется различное ПО, анализирующее сетевой трафик. Широкое распространение получила бесплатная программа – анализатор сетевого трафика (сетевой сниффер) Wireshark. Программа отслеживает и записывает весь сетевой трафик, имеет большое количество настроек, в значительной степени упрощающих процесс анализа и поиска ошибок. На рис.12 показан пример окна программы, в верхней части содержится список пакетов данных (в примере показаны GOOSE-сообщения), в средней части детали анализируемого пакета (адрес назначения, источника, идентификаторы и даже значения непосредственно GOOSE-сообщений), а в нижней части приведена шестнадцатеричная форма пакета данных.

Рис. 12. Окно анализатора трафика в ПО Wireshark.



Существует и более узкоспециализированное профильное ПО, например, IEDScout и SVScout. Программа IEDScout получила широкое признание и часто выступает в роли «арбитра» при возникновении спорных ситуаций при взаимодействии, например, устройства МП РЗА и SCADA-системы. Отличительной особенностью IEDScout является возможность создания имитации устройства с применением CID-файла, отправки MMS и GOOSE-сообщений.

Программа SVScout позволяет визуализировать потоки аналоговых величин в виде осциллограмм и векторных диаграмм, анализировать состояние всех параметров потока, таких, как поля качества, флаг синхронизации и т. д. Отсутствие необходимости подключения дополнительного оборудования для использования программы делает её незаменимым инструментом при работе с SV-потоками.

После предварительной настройки GOOSE-сообщений и SV-потоков приёмо-сдаточные испытания шкафов МП РЗА не отличаются от аналогичных испытаний для устройств, реализованных без поддержки стандарта IEC 61850. Управление дискретными сигналами и аналоговыми величинами осуществляется с помощью стандартного ПО как для испытательных установок РЕТОМ производства ООО НПП «Динамика», так и для устройств фирмы Omicron.

Язык SCL

Проектная документация на ЦПС включает в себя разработку единого электронного проекта, состоящего из файлов, содержащих полное описание объекта проектирования, с применением языка SCL (System Configuration description Language), согласно стандартам IEC 61850-4 и IEC 61850-6. SCL – это язык описания параметров конфигурации ИЭУ на ЦПС, созданный на основе расширенного языка разметки XML (eXtensible Markup Language).

В рамках проектирования ЦПС и входящих в ее состав интеллектуальных электронных устройств (ИЭУ – IED) используются, например, файлы с расширением:

• SSD – описание спецификации ПС;

• ICD – описание возможностей ИЭУ;

• SCD – описание конфигурации ПС;

• CID - описание сконфигурированного ИЭУ.

На стадии разработки проекта ЦПС, согласно требованиям стандарта организации ОАО «ФСК ЕЭС» «Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ», создается файл описания спецификации подстанции в формате SSD (System Specification Description). В данном файле содержится описание первичной схемы подстанции и распределения логических узлов, необходимых для реализации функций РЗА, мониторинга и т. д.

Проектная организация после выбора поставщиков оборудования РЗА запрашивает и получает от них файлы описания возможностей устройств в формате ICD (IED Capability Description), в которых описываются все логические устройства, логические узлы, элементы данных и атрибуты данных, а также предварительно сконфигурированные наборы данных (Dataset) для блоков управления отправкой SV-потоков (SV267 Control Block), GOOSE-сообщений (GOOSE Control Block) и MMS-отчетов (Report Control Block).

Полученные ICD-файлы импортируют в SSD-файл с помощью конфигуратора подстанции, в котором разработчик распределяет ранее выбранные логические узлы по соответствующим ИЭУ с получением на выходе первой версии SCD-файла (Substation Configuration Description), описывающего конфигурацию данной подстанции. В частности, в SCD-файле содержится информация о спецификации ИЭУ и информационном обмене между ними.

После внесения всей необходимой информации проводится проверка SCD-файла на наличие ошибок в программах-валидаторах SCL, после чего он в составе рабочей документации может быть направлен изготовителю терминалов РЗА для анализа и выдачи замечаний, на основе которых будет получена вторая версия SCD-файла.

Получив скорректированный SCD-файл, изготовители РЗА на этапе проведения приемо-сдаточных испытаний посредством конфигуратора ИЭУ загружают информацию из SCD-файла в устройства, получая продукт, готовый к отправке на объект.

На объекте проводятся пуско-наладочные работы (ПНР), во время которых уточняется фактическая конфигурация устройств и при необходимости вносятся финальные корректировки в SCD-файл. Готовый SCD-файл третьей версии может быть загружен в сетевые анализаторы для мониторинга процессов информационного обмена в сетях ЦПС.

Заключение

Использование новых протоколов передачи данных и коммуникационных сервисов при реализации устройств релейной защиты диктует новые требования к компетенциям, которыми должен обладать инженер РЗА. При кажущейся простоте эксплуатации новых устройств РЗА возникают более жесткие требования по подготовке квалифицированного персонала, особенно в переходный период.

Использование конфигураторов SCL позволяет на всех этапах проектирования находить и оперативно устранять ошибки в настройках информационного обмена между ИЭУ, обусловленные человеческим фактором. Использование всех возможностей SCL-файлов – наиболее правильный и перспективный путь развития технологии ЦПС.

Внедрение новых подходов и технологий должно осуществляться по эволюционному пути. Релейная защита всегда была и остается положительно-консервативной, именно это позволяет обеспечивать бесперебойное электроснабжение потребителей.

СПИСОК ЛИТЕРАТУРЫ

[1] IEC 61850-8-1: Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) –Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3 - Ed.2.
[2] Руководство по эксплуатации. Устройство преобразования аналоговых сигналов для сопряжения с шиной процесса БЭ2704V750. ЭКРА.650321.062/
[3] Руководство по эксплуатации. Терминал дискретного ввода-вывода БЭ2704V752. ЭКРА.650321.063РЭ.
[4] Терминалы серии БЭ2704. Руководство по эксплуатации. ЭКРА.656132.265-01.РЭ.
[5] IEC/IEEE 61850-9-3: Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation.
[6] IEC 62439-3: Industrial communication networks – High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).
[7] Руководство оператора. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ SCL EXPRESS КОНФИГУРАТОР ЦИФРОВОЙ ПОДСТАНЦИИ. ЭКРА.00054-01 34 01.

1.10. ОСОБЕННОСТИ ИСПЫТАНИЙ РЗА ЦПС НА РАЗНЫХ ЭТАПАХ «ЖИЗНЕННОГО ЦИКЛА»

А. С. ШАЛИМОВ

ООО «НПП «Динамика»

Российская Федерация

Контактное лицо:

А. С. ШАЛИМОВ

shalimov-as@retom.ru

Ключевые слова: Релейная защита и автоматика, имитационное тестирование, цифровая испытательная система, IEC 61850

Введение

Интеллектуальные электронные устройства (ИЭУ) релейной защиты и автоматики (РЗА) цифровых подстанций (ЦПС) с шиной процесса (протоколы IEC 61850-9-2 и IEC 61850-8-1 GOOSE) требуют соответствующего подхода к тестированию с учётом их программно-аппаратных особенностей и цифровой среды передачи информации в шине процесса и шине станции энергообъекта.

В настоящее время нормативно-техническая документация в области тестирования и решения для автоматизации испытаний устройств РЗА, как правило, повторяют традиционные методы проверки микропроцессорных терминалов, требующих оценки параметров срабатывания функций РЗА и правильности функционирования логической части устройств.

При этом объём испытаний системы РЗА ЦПС должен определяться соответствующими нормативными документами для каждого из этапов «жизненного цикла» энергообъекта (наладка, эксплуатация, послеаварийная проверка, профконтроль и т. д.), включающими перечень дополнительных проверок, обусловленных требованиями технологии ЦПС, которые следует применять в ходе приёмки и эксплуатации ИЭУ РЗА.

Далее рассматриваются специфические особенности испытаний ИЭУ на разных этапах «жизненного цикла», сочетающие традиционные и цифровые методы тестирования алгоритмов функций РЗА.

Испытания ИЭУ РЗА с поддержкой IEC 61850-9-2LE и IEC 61869-9

Перечень испытаний элементов системы РЗА ЦПС должен формироваться исходя из архитектуры РЗА и локально-вычислительной сети (ЛВС) ЦПС и соответствующего этапа «жизненного цикла».

При наладке и приёмке ИЭУ перечень испытаний должен быть дополнен:

– тестированием ИЭУ в схеме с первичными преобразователями (в том числе с учётом особенностей электронно-оптических измерительных трансформаторов и электромагнитных (ЭМ) измерительных трансформаторов с преобразователями аналоговых сигналов);

– тестированием встроенных в преобразователи аналоговых сигналов (ПАС) функций РЗА;

– тестированием ИЭУ с учётом среды передачи информации, а именно искажений сетевых данных в ЛВС ЦПС;

– комплексным испытанием ИЭУ с повышенной информационной нагрузкой.

Указанные испытания актуальны также при обновлении версий внутреннего программного обеспечения ИЭУ и изменении конфигурации элементов сетевого оборудования ЛВС ЦПС.

Тестирование ИЭУ в схеме «трансформатор тока – релейная защита» (ТТ – РЗ), когда проверяются алгоритмы блокирования функций РЗА при насыщении ЭМ измерительного трансформатора тока (ТТ) [1], становится недостаточным, поскольку для ЦПС дополнительно к искажению формы аналогового сигнала на входе ПАС добавляются искажения сетевых данных в шине процесса. Комплексное искажение аналоговых данных SV-потока при насыщении измерительных ЭМ ТТ и сетевых искажений (например, пропуски сетевых пакетов) в ЛВС (шине процесса) объективно затрудняет анализ алгоритмов восстановления ИЭУ формы аварийного сигнала. Соответственно, следует рассматривать схемы тестирования «электромагнитный преобразователь – преобразователь аналоговых сигналов – локально-вычислительная сеть – интеллектуальное электронное устройство» (ЭМП – ПАС – ЛВС – ИЭУ). На рис. 1, 2 приведены соответственно схемы тестирования для испытательных систем с аналоговыми каналами и цифровыми интерфейсами. Для ЦПС с электронно-оптическими первичными преобразователями (ЭОТ) актуальна схема тестирования ЭОТ – ЛВС – ИЭУ, учитывающая «выбросы» мгновенных значений в передаваемых данных SV-потоков (IEC61850-9-2 Sampled Values).

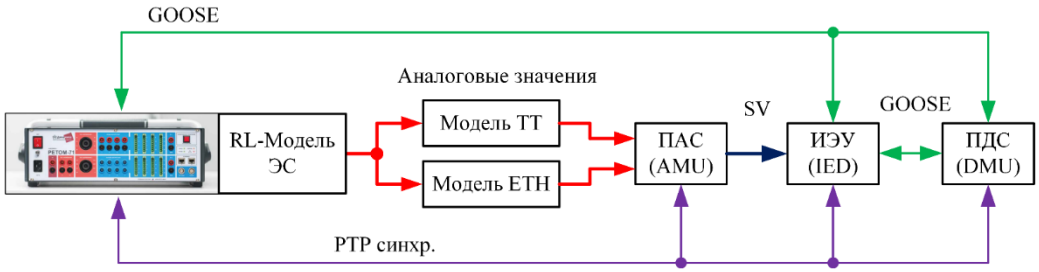


Рис. 1. Схема тестирования «ЭМП – ПАС – ЛВС – ИЭУ» для испытательной системы с аналоговыми каналами.

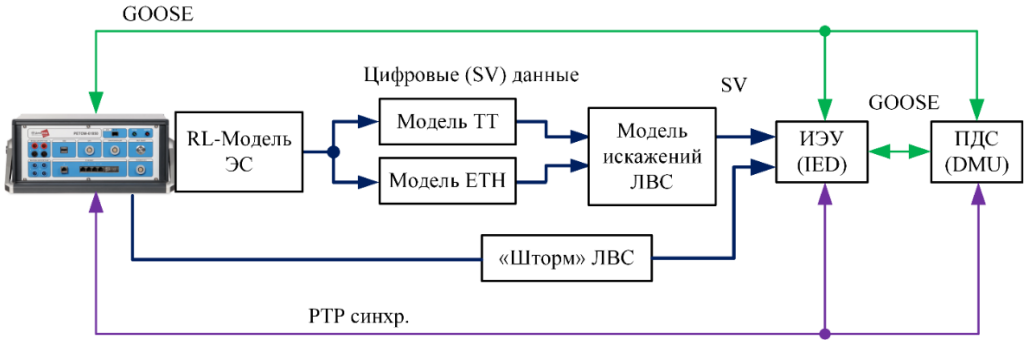


Рис. 2. Схема тестирования «ЭМП – ПАС – ЛВС – ИЭУ» для цифровой испытательной системы.

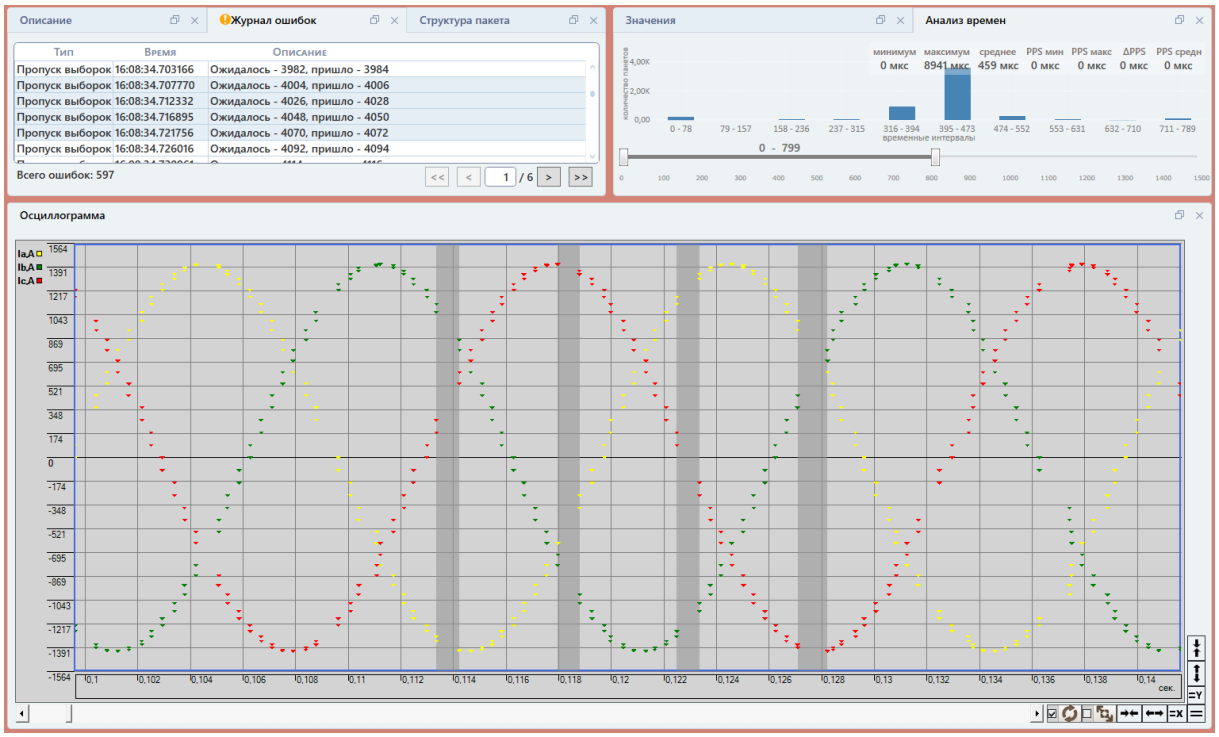
Алгоритмы функций ИЭУ РЗА, таких, как дифференциальные защиты трансформаторов, генераторов, шин, использующих измерения от разных оптических ТТ или ПАС, а также при разделении аналоговых данных тока и напряжения по разным SV-потокам (для измерительных органов с двумя подведёнными величинами – дистанционные защиты, органы направления мощности) могут неправильно функционировать из-за неидеальной синхронизации (или её нарушении) SV-потоков от разных издателей, а также из-за задержек промежуточных сетевых элементов. Компенсация несинхронно принимаемых данных осуществляется специальным буфером ИЭУ, проверка функционирования которого (правильность работы, а также время буферизации цифровых отсчётов) может осуществляться с применением соответствующего функционала цифровых испытательных комплексов [2].

При выполнении аттестационных, пуско-наладочных и эксплуатационных испытаний также может быть востребована проверка алгоритмов аппроксимации цифровых отсчётов принимаемых потоков и блокирования измерительных органов ИЭУ РЗА при моделировании пропадания и перемешивания выборок в SV-потоках. Указанные процессы могут возникать в ЛВС шины процесса при эксплуатации ЦПС в неопределённое время, соответственно, ИЭУ должны проверяться на отстройку (компенсацию потери информации) от данных процессов.

Испытания ИЭУ с поддержкой спецификации IEC 61850-9-2LE [3] применяются при заводских и наладочных испытаниях с использованием режима генерации искажений данных в SV-потоках [4, 5] с учётом параметров буфера компенсации ИЭУ: пропуск сетевых пакетов с цифровыми отсчётами, их перемешивание и смещение относительно начала секунды (smpCnt = 0). С учётом стандарта IEC 61869-9 «Требования к цифровым интерфейсам измерительных трансформаторов» [6] и его применения в рамках «Корпоративного профиля МЭК 61850 ПАО «ФСК ЕЭС» сетевые искажения в SV-потоках, а именно пропуски, становятся более критичными для алгоритмов РЗА, поскольку в отличие от IEC 61850-9-2LE, где в одном сетевом пакете передавалось значение одной выборки токов и напряжений (noASDU = 1), в IEC 61869-9 для целей РЗА предусмотрена передача двух выборок (noASDU = 2) в одном пакете. Таким образом, возможность испытаний ИЭУ с имитацией искажений SV (рис. 3) при проверке параметров срабатывания ИЭУ или послеаварийной проверке с использованием COMTRADE-файлов аварийных осциллограмм является ещё более востребованным инструментом испытательных систем при приёмке из наладки и послеаварийных проверках РЗА ЦПС.

Рис. 3. Пример процесса искажения данных SV-потока IEC61869-9.

Актуальной темой эффективного функционирования ИЭУ РЗА являются также медленно изменяющиеся задержки распространения сетевых пакетов SV в шине процесса, при которых постепенно возникает фазовый сдвиг между SV-потоками двух издателей, который может привести к неправильной работе функций ИЭУ РЗА. При этом тестирование алгоритмов РЗА имитацией смещения SV-потока с шагом в один цифровой отсчёт (250 мкс для IEC61850-9-2LE) в ряде случаев не позволит провести полноценную проверку при автоматическом регулировании глубины буфера компенсации задержек цифровых отсчётов, поскольку рассинхронизация издателей SV-потоков на реальных объектах, как правило, является медленным процессом. Таким образом, необходим



соответствующий механизм тестирования при смещении (задержке) SV-потока с заданным значением в диапазоне от 1 до 100 мкс/с, например, реализованный в [2]. Цифровая испытательная система моделирует и воспроизводит процесс смещения по времени одного SV-потока относительно другого с возможностью проверки реакции ИЭУ РЗА – алгоритма блокирования действия и сигнализации и недостоверности принимаемых данных. На рис. 4 приведён пример имитации медленного смещения (100 мкс/с) одного SV-потока, содержащего данные фазных токов, относительно SV-потока, содержащего напряжения и реакции на данный процесс ИЭУ по протоколу GOOSE (логические сигналы блокировки сигнала пуска дистанционной защиты и

срабатывания логического сигнала недостоверности данных в шине процесса IEC61850-9-2 в исходящем сообщении).

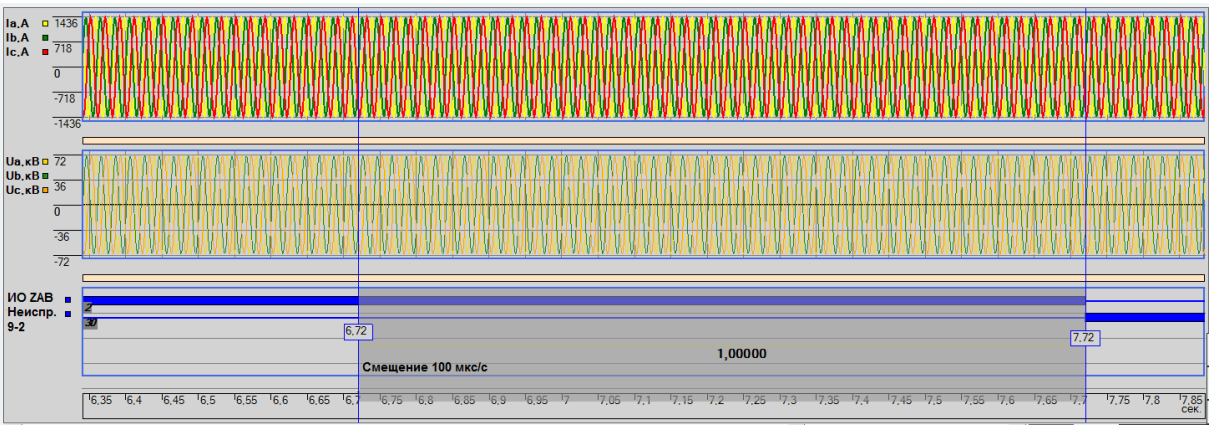


Рис. 4. Пример моделирования смещения SV-потока с заданной скоростью.

Заключение

Тестирование системы релейной защиты и автоматики (РЗА) объектов с шиной процесса (протокол IEC 61850-9-2) предполагает дополнительный объём и методологию соответствующих испытаний, связанных с отличием интеллектуальных электронных устройств от МП терминалов РЗА.

Необходима разработка нормативно-технической базы по дополнительным методам тестирования устройств РЗА с поддержкой протоколов IEC61850 для повышения надёжности и эксплуатационной эффективности комплексов РЗА ЦПС.

Рассмотренные методы испытаний применялись при пусконаладочных испытаниях и профконтроле отдельных ИЭУ и комплексов ИЭУ РЗА присоединений на реальных энергообъектах – «цифровых подстанциях» с применением протоколов MMS, GOOSE и SV (IEC 61850-9-2LE).

СПИСОК ЛИТЕРАТУРЫ

[1] Шалимов А. С. Динамическое тестирование релейной защиты с учётом переходных процессов в трансформаторах тока // Релейная защита и автоматизация, 2017. № 2 (27). С. 16-19.

[2] Комплекс программно-технический измерительный цифровой РЕТОМ-61850. Руководство по эксплуатации БРГА.441461.014 РЭ. Редакция 130617.

[3] IEC 61850-9-2 LE (Lite Edition). Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2.

[4] Шалимов А. С. Тестирование специальных алгоритмов устройств релейной защиты с использованием шины процесса IEC 61850-9-2LE // Релейная защита и автоматизация, №3 (28), 2017. С. 39-42.

[5] Безденежных М. Н., Дони Н. А., Егоров Е. П., Кошельков И. А., Петров А. А., Шалимов А. С. Особенности тестирования цифровой дифференциальной защиты шин 110-750 кВ на основе протокола IEC61850-9-2LE // Релейная защита и автоматизация. 2018. № 2(31). С. 41-47.

[6] IEC 61869-9 Instrument Transformers – Part 9: Digital Interface for Instrumental Transformers, 2016.

1.11. СИНХРОНИЗАЦИЯ ВРЕМЕНИ ИНТЕЛЛЕКТУАЛЬНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ НА ПОДСТАНЦИЯХ

Р. С. ПЛАКИДИН, П. В. СЕИТОВ, В. Н. БОВЫКИН

ООО «Инженерный центр «Энергосервис»

Российская Федерация

Контактное лицо:

П. В. СЕИТОВ

p.seitov@ens.ru

Ключевые слова: Время, синхронизация, точность,

шкала, частота, эталон, метка времени.

Введение

Внедрение современных информационно-коммуникационных технологий позволяет повысить эффективность управления и мониторинга состояния первичного оборудования электрических станций и подстанций. Однако с развитием технологий появляется необходимость в совершенствовании методов диагностики и проверки корректности работы нового оборудования, используемого для создания следующего поколения автоматизированных систем на базе стека стандартов МЭК 61850.

Обеспечение отсчетов единого времени во всех элементах автоматизированной системы – на сегодня одна из важнейших задач. Примером может служить передача мгновенных значений токов и напряжений от измерительных трансформаторов тока и напряжения в цифровом виде. Это позволяет добиться значительных преимуществ, связанных с использованием как новых типов измерителей, основанных на отличных от традиционного подхода принципов, так и с использованием стандартной сетевой инфраструктуры взамен многочисленных кабельных связей для передачи текущих значений с помощью аналоговых сигналов на значительных уровнях тока и напряжения.

С другой стороны, технология SV-потоков (стандарт IEC 61850-9-2) предъявляет серьезные требования к используемому для её реализации оборудованию, в том числе и с точки зрения синхронизации времени устройств. Так как теперь важно не только измерить величину, но и указать с высокой точностью, в какой момент времени были проведены данные измерения. Благодаря метке времени, присвоенной с требуемой точностью, мы имеем возможность сравнивать и использовать для расчета вторичных величин (частота, мощность, показатели качества и другие) оцифрованные выборки мгновенных значений токов и напряжений, полученные через локальную вычислительную сеть (сети) от разных первичных устройств. Соответственно, мы получим возможности для текущего мониторинга и последующего анализа на основе качественно новых данных по сравнению с традиционными «аналоговыми» автоматизированными системами.

Синхронизация времени встроенных часов интеллектуальных электронных устройств зависит от многих аспектов, в том числе явно неотносящихся к оборудованию автоматизированной системы управления подстанцией. Развитие техники на сегодняшний день позволяет с помощью глобальных спутниковых систем навигации ГЛОНАСС и GPS получить доступ к атомному эталону частоты в любой точке планеты. При том, что данный источник первичных сигналов в состав автоматизированной системы подстанции не входит, и контролировать процесс его работы можно только по косвенным признакам. Здесь может просматриваться общая тенденция на взаимопроникновение как отдельных функций в оборудовании для различных систем, так и (на примере систем мониторинга переходных режимов) широкое использование для своих задач

данных, полученных от прочих автоматизированных систем. Само семейство стандартов МЭК 61850 является ярким примером того, что не стоит пытаться каждый раз на своих страницах, в своей системе описать, реализовать все протоколы и функции, которые могут понадобиться для полноценного функционирования автоматизированной системы. Достаточно сослаться на уже готовые стандарты, технологии, импортировать данные, полученные на уже имеющемся оборудовании с тем, чтобы оптимизировать затраты на реализацию новых систем и подсистем.

В докладе рассматриваются методы диагностики и проверки точности синхронизации устройств автоматизированных систем по основным протоколам синхронизации времени, предусматриваемым в соответствии со стандартами МЭК 61850. Проверка точности синхронизации осуществляется как с помощью типового оборудования, так и с помощью специальных функций, реализованных в типовом оборудовании для автоматизированных систем подстанций. Приводятся обоснования требований к точности синхронизации встроенных часов интеллектуальных электронных устройств, таких, как устройства сопряжения с шиной процесса, электронные датчики тока и напряжения с возможностью выдачи результатов измерений в виде потоков оцифрованных выборок мгновенных значений (Sampled Values, IEC 61850-9-2, далее SV), многофункциональные измерительные преобразователи, счетчики электроэнергии, терминалы релейной защиты. Объясняется влияние установленных требований на точность результатов измерений первичных и расчетных величин параметров трехфазной электрической сети. Указывается на потенциальную возможность повышения точности результатов измерений измерительных устройств путем повышения точности синхронизации встроенных в интеллектуальные электронные устройства часов.

Основная часть

Синхронизации времени встроенных часов интеллектуальных электронных устройств зависит от многих аспектов, в том числе явно неотносящихся к оборудованию автоматизированной системы управления подстанцией. Развитие техники на сегодняшний день позволяет с помощью глобальных спутниковых систем навигации ГЛОНАСС и GPS получить доступ к атомному эталону частоты в любой точке планеты. При том, что данный источник первичных сигналов в состав автоматизированной системы подстанции не входит, и контролировать процесс его работы можно только по косвенным признакам. Здесь может просматриваться общая тенденция на взаимопроникновение как отдельных функций в оборудовании для различных систем, так и (на примере систем мониторинга переходных режимов) широкое использование для своих задач данных, полученных от прочих автоматизированных систем. Само семейство стандартов МЭК 61850 является ярким примером того, что не стоит пытаться каждый раз на своих страницах, в своей системе описать, реализовать все протоколы и функции, которые могут понадобиться для

полноценного функционирования автоматизированной системы. Достаточно сослаться на уже готовые стандарты, технологии, импортировать данные, полученные на уже имеющемся оборудовании с тем, чтобы оптимизировать затраты на реализацию новых систем и подсистем.

Государственные первичные атомные эталоны времени, которые являются хранителями самого понятия «секунда» и вокруг которых возведены целые институты, обеспечивают отклонение частоты не более 10^{-14}—10^{-15}, то есть ошибка в 1 секунду будет накапливаться на протяжении 30 миллионов лет. Разумеется, столь высокая точность не нужна в большинстве приложений, в том числе в системах автоматизации подстанций (ПС). Но какая же точность требуется от систем времени, контролирующих работу ПС? Что стоит за сухими цифрами технических требований и насколько они оправданны? А самое главное, соответствуют ли им внутренние часы интеллектуальных электронных устройств (ИЭУ) и позволяют ли они соотносить значения и события во времени настолько точно, насколько это необходимо для ведения режимов в реальном времени, анализа текущих процессов, регистрации аварий и учета электроэнергии?

Согласно современным требованиям, предъявляемым к синхронизации времени в автоматизированных системах учета электроэнергии (АИИС КУЭ), синхронизация времени в приборах учета должна выполняться с точностью не хуже ±5 секунд в сутки [1]. Такая точность вполне достаточна, так как не вызовет существенного искажения объема учтенной электроэнергии за расчетный период.

К автоматизированным системам управления подстанций (АСУ ТП) требования существенно строже: точность синхронизации устройств должна быть не хуже 1 мс [2], 100 мс [13], 1 сек [14] — это необходимо для фиксации меток времени событий (изменение состояния коммутационных аппаратов, сигналов срабатывания защит и автоматики и пр.).

В сетях передачи данных АСУ ТП для синхронизации времени, как правило, используют протокол NTP (SNTP) или синхронизацию по выделенным линиям (PPS, IRIG).

Протокол сетевого времени NTP и его вариант SNTPv4 (Simple Network Time Protocol, RFC 5905) обеспечивает точность порядка 1–50 мс [3]. Для большей части электронного оборудования этого достаточно, но гарантировать более высокую точность по протоколу NTP невозможно из-за непредсказуемых сетевых задержек.

На примере многофункционального измерительного преобразователя ЭНИП-2 [4] проверим, насколько точно синхронизируются устройства по SNTP. Для этого соберем схему, представленную на рис. 1.

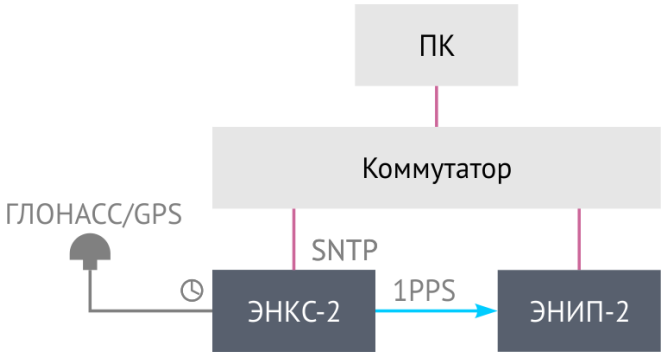
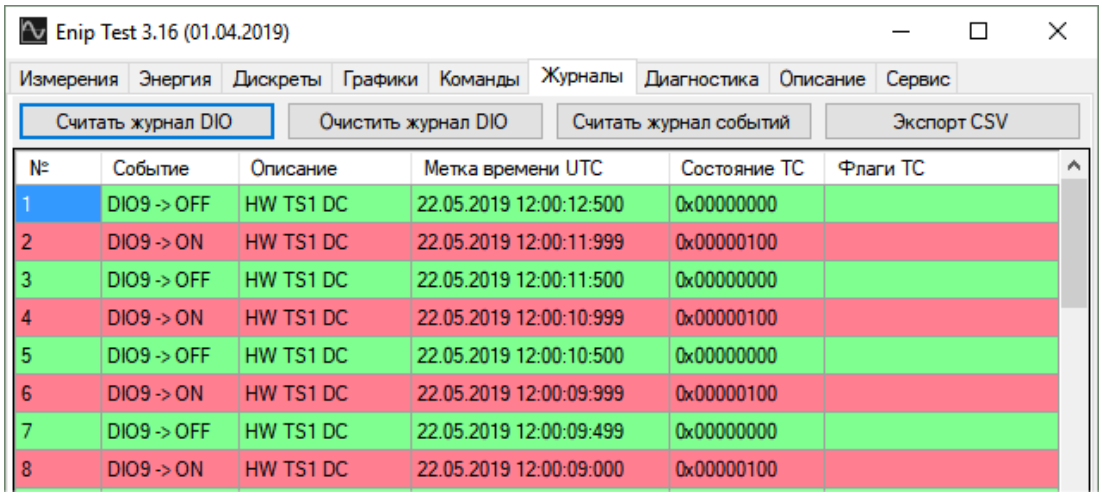


Рис. 1. Схема измерения точности синхронизации времени измерительного преобразователя ЭНИП-2 с помощью блока коррекции времени ЭНКС-2.

ЭНИП-2 синхронизируется по сети от блока коррекции времени ЭНКС-2 [5]. Одновременно выход PPS блока коррекции времени ЭНКС-2 через транзисторный ключ подключается к дискретному входу синхронизируемого ЭНИП-2.

Оценка точности синхронизации ЭНИП-2 определяется по присвоенной метке времени срабатывания дискретного входа от PPS. Фронт сигнала PPS составляет 500 мс. Результат опыта фиксируется по данным в журнале событий дискретных сигналов ЭНИП-2 (рис. 2), который показывает, что незагруженная локальная сеть и протокол SNTP вполне уверенно обеспечивают точность не хуже 1 мс.



№	Событие	Описание	Метка времени UTC	Состояние ТС	Флаги ТС
1	DIO9 -> OFF	HW TS1 DC	22.05.2019 12:00:12:500	0x00000000	
2	DIO9 -> ON	HW TS1 DC	22.05.2019 12:00:11:999	0x00000100	
3	DIO9 -> OFF	HW TS1 DC	22.05.2019 12:00:11:500	0x00000000	
4	DIO9 -> ON	HW TS1 DC	22.05.2019 12:00:10:999	0x00000100	
5	DIO9 -> OFF	HW TS1 DC	22.05.2019 12:00:10:500	0x00000000	
6	DIO9 -> ON	HW TS1 DC	22.05.2019 12:00:09:999	0x00000100	
7	DIO9 -> OFF	HW TS1 DC	22.05.2019 12:00:09:499	0x00000000	
8	DIO9 -> ON	HW TS1 DC	22.05.2019 12:00:09:000	0x00000100	

Рис. 2. Оценка точности синхронизации ЭНИП-2 по меткам времени в журнале событий [6].

Более высокие требования к синхронизации времени предъявляются на цифровых подстанциях (ЦПС) и в системах мониторинга переходных режимов (СМПР).

Устройства ЦПС, являющиеся публикаторами SV и образующие шину процесса, должны быть синхронизированы с точностью в 1 мкс [7, 8].

Устройства синхронизированных векторных измерений, входящие в состав СМПР, также должны быть синхронизированы с точностью 1 мкс [9].

Для достижения точности синхронизации с точностью в 1 мкс можно использовать выделенные каналы по протоколам IRIG и сигналам PPS [10]. Однако стандарт IEC/IEEE 61850-9-3 предлагает более эффективный и удобный способ синхронизации вышеуказанных систем — синхронизацию времени по сети Ethernet с применением протокола PTP (IEC 61588:2009 / IEEE Std 1588-2008) [11].

В сети с поддержкой PTP принята топология ведущего и ведомых устройств, где подчиненные часы синхронизируются с главными «гроссмейстерскими» часами (рис. 3). Гроссмейстерские часы, как правило, синхронизируются от приемников GPS/ГЛОНАСС. Протокол PTP дает возможность точно учитывать задержку распространения пакетов в сети Ethernet. Для этого при построении сети применяются Ethernet-коммутаторы с поддержкой PTP, так называемые прозрачные часы, которые учитывают задержку времени на передачу PTP-пакета далее по маршруту, изменяя при этом содержимое пакета.

Для PTP разработаны различные профили. Профиль для электроэнергетики (Power Profile) первоначально был описан в документе IEEE C37.238-2011. Впоследствии профиль Power Profile Utility был представлен в IEC/IEEE 61850-9-3:2016. Текущая редакция профиля Power Profile для электроэнергетики описана в стандарте IEEE C37.238-2017, который решает проблемы совместимости первой редакции Power Profile с Power Profile Utility.

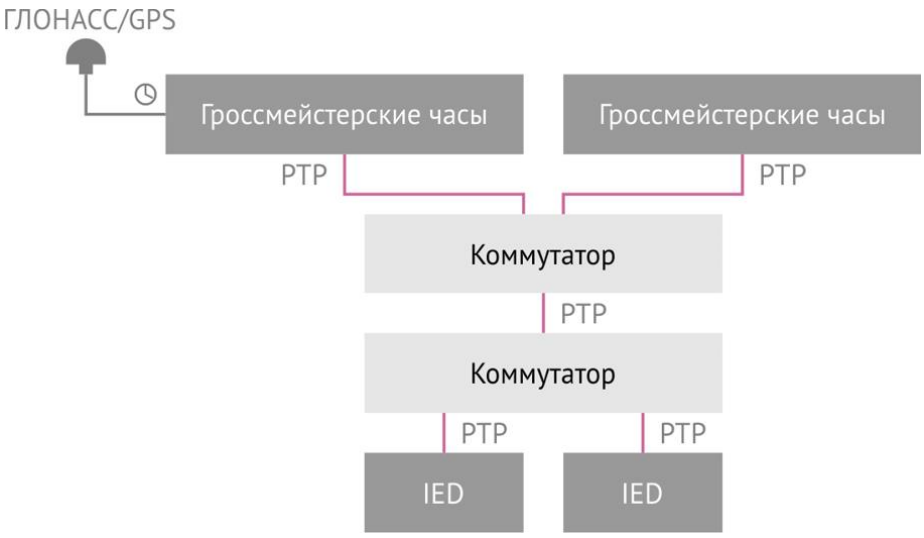


Рис. 3. Пример локальной сети с синхронизацией часов устройств (IED) по PTPv2.

Таким образом, применение PTP для синхронизации устройств в сети связано и с правильным проектированием (количество коммутаторов, топология, количество гроссмейстерских часов и т. д.), и с корректностью настроек устройств (выбор профиля или настройка конкретных параметров). Только в этом случае гарантирована точность не хуже ±1 мкс [11].

Теперь попробуем разобраться, отчего на цифровой подстанции так важна точность не хуже 1 мкс и как можно проверить такую точность синхронизации времени в оконечном устройстве?

Предварительно выскажем мнение: в случае с преобразователями аналоговых сигналов возможна только косвенная оценка — по погрешности измерения абсолютного угла.

Обычно представление о том, что система синхронизации работает в соответствии с нормативными требованиями, основано на параметрах применяемого источника синхронизации. То есть пользователь имеет сертифицированный источник времени (средство измерения), но фактически оценить точность синхронизации времени в устройствах способен лишь косвенно и часто без возможности получить конкретные цифры.

В свою очередь PTP позволяет проверить работу системы синхронизации и связанной с ней сетевой инфраструктуры, для чего применяются эталонные приемники протокола PTP с выходами PPS. Но об этом чуть позже.

Для начала определим, какие погрешности могут возникнуть при проблемах с определением времени выборки SV. Например, для потока SV с частотой выборок 12 800 Гц (256 выборок на период для частоты 50 Гц) замена значения выборки на соседнюю в случайном порядке дает погрешность по RMS до 0,25%. Это равнозначно отклонению времени измерений на величину от -78,125 до +78,125 мкс.

Такое поведение средства измерения оказало бы заметное влияние на амплитуду гармоник высокого порядка. Однако здесь мы описали чисто теоретическую ситуацию, а фактически если измерения начнут отставать из-за точности синхронизации, то выборки будут сдвигаться все вместе (то есть измеренные значения будут сдвинуты относительно реальной кривой оцифрованного сигнала на одинаковое время).

Традиционные электромагнитные трансформаторы тока и напряжения подключены непосредственно к измерительным приборам (терминалам РЗиА и другим IED), измерительная информация от ТТ и ТН поступает в реальном времени процесса. На цифровой подстанции

измерительная информация передается только в цифровом виде, а значит, чтобы сопоставить полученные SV от разных преобразователей аналоговых сигналов (устройство сопряжения с шиной процесса, Merging Unit далее ПАС), необходимо как минимум синхронизировать их внутренние часы, то есть привязать к одной системе отсчета, например, к всемирному координированному времени UTC. В ПАС необходимо запускать АЦП в моменты времени, строго соответствующие выбранному значению SV, а затем маркировать измерения (SmpCnt [12]). В таком случае ПАС будут делать выборки в условно одинаковые моменты времени (с погрешностью синхронизации). Однако передаваемые выборки доставляются до подписчиков SV с задержками, определяемыми быстродействием ПАС, характеристиками и режимом работы локальной сети. Устройства, подписанные на SV, упорядочивают полученные значения по значению SmpCnt, тем самым «восстанавливают» во времени кривые сигналов друг относительно друга. Ошибка синхронизации времени ПАС в 1 мкс соответствует абсолютной погрешности, равной 1,08 угловых минут.

Таким образом, точность синхронизации времени в устройствах ПАС напрямую влияет на их угловую погрешность, от которой в свою очередь зависят измерение мощности, учет электроэнергии, точность векторных измерений в устройствах – подписчиках SV.

Стандарт IEC 61869-9 требует, чтобы при потере синхронизации времени поток SV выдавался с точностью 1 мкс в течение 5 секунд. Переход с одних гроссмейстерских часов на другие, как правило, занимает не более 3 секунд (3 интервала announce frame), а значит, во время смены источника синхронизации качество потока SV не должно изменяться.

Заметим, что точность в 1 мкс исключительно важна именно для публикаторов SV, а для приемников SV (счетчики, устройства контроля параметров качества, РЗА, РАС) допустима синхронизации с точностью 1 мс (например, NTP), поскольку сам поток SV уже несет информацию о времени в пределах одного периода промышленной частоты (SmpCnt).

Исходя из сказанного выше, логично утверждать, что в процессе наладки и сдачи в эксплуатацию цифровой подстанции следует уделять особое внимание проверке системы синхронизации времени. Для этого на исследуемом участке сети (например, на самом удаленном, который находится за максимальным количеством коммутаторов от гроссмейстерских часов) необходимо принять сигнал PTP и сравнить с эталонным значением всемирного координированного времени:

- используя эталонное устройство с приемником GPS/ГЛОНАСС, которое также может принять PTP-сигнал и определить погрешность синхронизации;

- используя эталонное устройство с приемником GPS\ГЛОНАСС и импульсным выходом (PPS), преобразователь сигналов PTP в PPS и осциллограф для сравнения двух сигналов PPS (рис. 4).

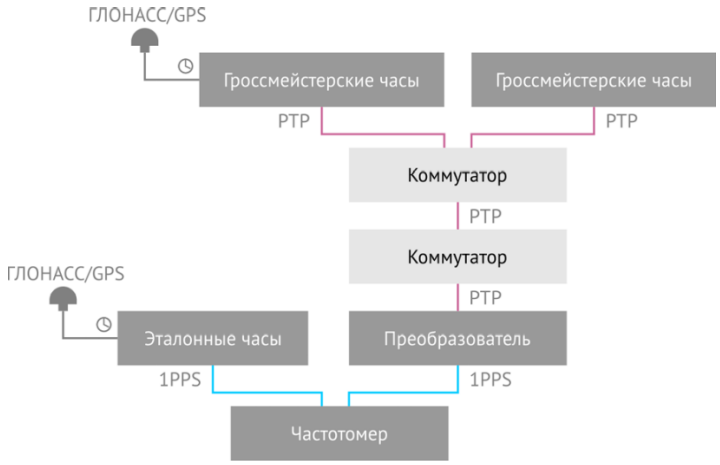


Рис. 4. Тестирование сети сравнением сигналов PPS.

Если точность синхронизации в результате проверки окажется не хуже 1 мкс, значит, можно сделать вывод, что сеть организована и настроена правильно. Если в дальнейшем сеть не будет перестроена, то можно допустить, что со временем точность синхронизации не изменится.

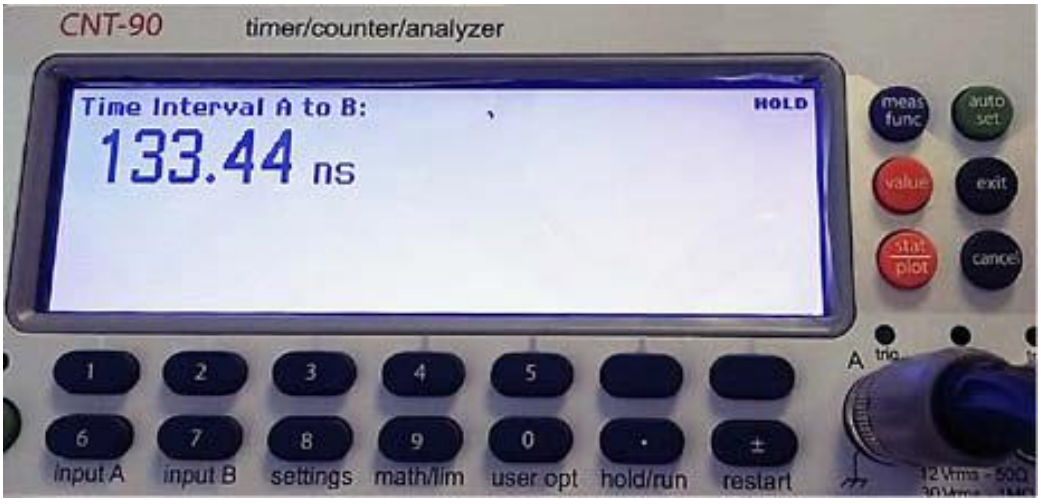
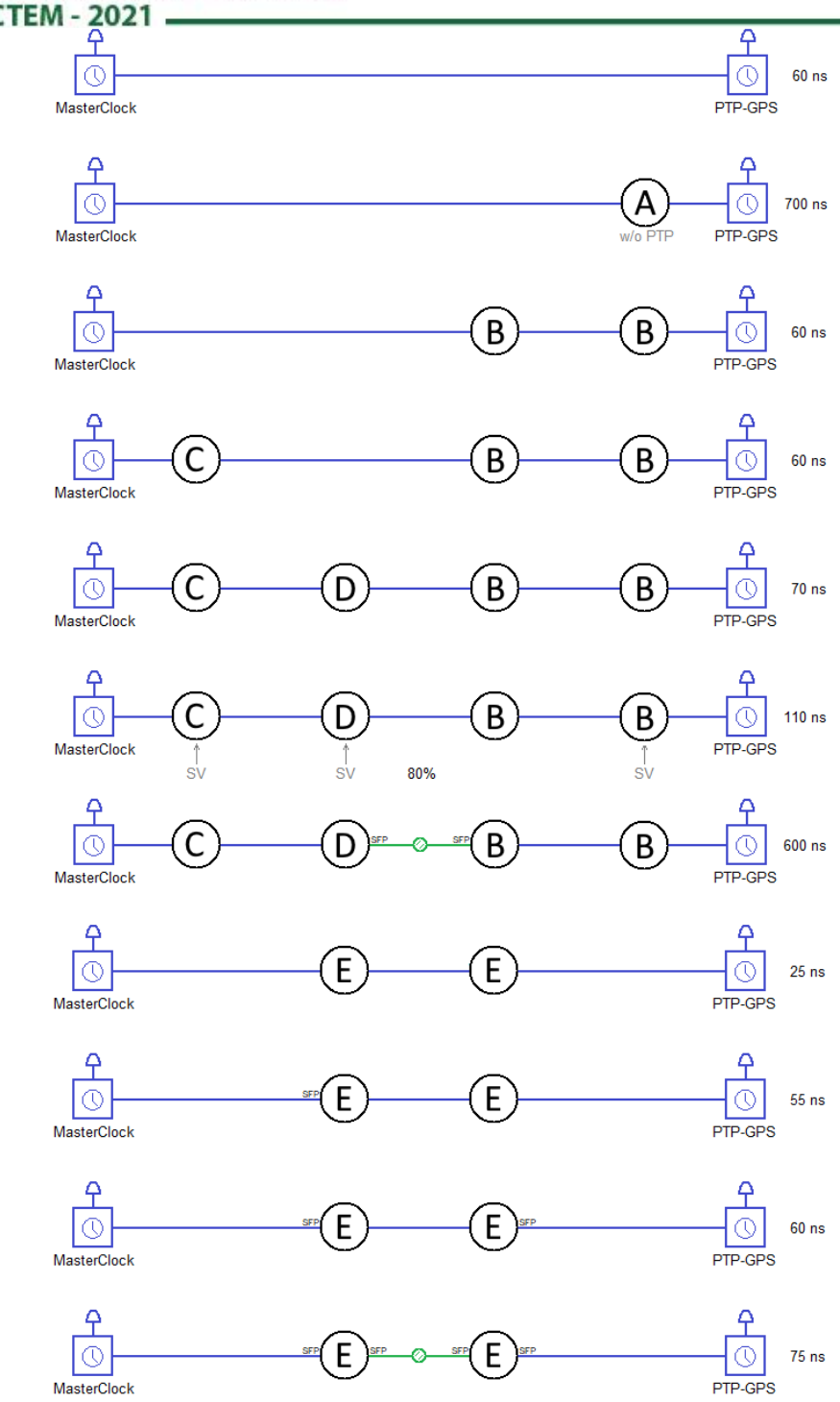


Рис. 5. Результат сравнения разницы эталона с фактическим значением метки времени.

На рис. 6 приведены результаты измерений расхождений метки времени, передаваемой по PTP на различных участках локальной сети, с метками, получаемыми от ГЛОНАСС/GPS эталонными часами – блоком коррекции времени ЭНКС-2. В качестве преобразователя синхронизирующих сигналов из меток времени, транслируемых по PTP, в импульсы 1PPS также использовался ЭНКС-2.

Приведенные результаты показывают, как в разных условиях с использованием оборудования нескольких производителей ошибка метки времени в локальной сети может отличаться от нескольких нс до сотен нс и больше. Понимание подобных особенностей работы протокола PTP необходимо при создании локальной сети для ЦПС и организации синхронизации времени по [11].



B, C, D, E - коммутаторы с поддержкой PTP
A - коммутатор без поддержки PTP
SV - несколько публикаторов SV потоков 256 и 80
MasterClock - Ведущие часы PTP
PTP-GPS - ЭНКС-2 - устройство определяющее отклонение меток времени PTP от шкалы времени ГЛОНАСС/GPS

Рис. 6. Разница меток времени, передаваемых по протоколу PTP, со временем эталона.

Заметим, что источники SV – ПАС, как правило, не имеют выхода PPS, поэтому определить погрешность синхронизации в этих устройствах напрямую невозможно. Обратимся к стандарту на устройства сопряжения IEC 61869-13, который в п. 5.6 поясняет:

«Требования к точности SAMU (ПАС) напрямую включают все погрешности, связанные с синхронизацией времени». То есть угловая погрешность напрямую зависит от погрешности синхронизации времени и, следовательно, судить о точности синхронизации устройства можно только косвенно – по угловой погрешности.

Стандарт IEC 61869-13 устанавливает различные классы точности для измерительных каналов тока и напряжения. Например, для такого распространенного класса точности, как 0,2, по угловой погрешности напряжения требуется уложиться в 10 угловых минут. Это значение включает и возможную погрешность синхронизации, которая при требовании к точности синхронизации 1 мкс (1,08 угловых минуты) составляет 1,08% от общей погрешности.

Для класса 0,05, которому в настоящее время могут соответствовать только лабораторные установки, это уже 2,5 угловых минуты. Доля погрешности синхронизации для класса 0,05 составит уже 43,2% от общей погрешности. Учитывая, что серийное измерительное устройство необходимо поверять, то есть должен существовать эталонный генератор аналогового сигнала с точностью выше в несколько раз, чем поверяемое устройство, то выпуск измерительных устройств с классом точности 0,05 представляет собой экономически неоправданную задачу. Перейти на класс 0,05 может помочь в том числе и повышение точности синхронизации, что в свою очередь может дать больший запас по погрешности на измерения.

Заключение

В заключение сделаем следующие выводы:

- синхронизация времени чрезвычайно важна для обеспечения точности измерения на цифровых подстанциях;

- оценка точности системы синхронизации времени может быть осуществлена с помощью эталонных приемников сигналов синхронизации с импульсными выходами и должна проводиться в рамках приемо-сдаточных испытаний системы.

СПИСОК ЛИТЕРАТУРЫ

[1] п. 2.3, Приложение № 11.1. к Положению о порядке получения статуса субъекта оптового рынка и ведения реестра субъектов оптового рынка, «Автоматизированные информационно-

измерительные системы коммерческого учета электрической энергии (мощности). Технические требования», ред. от 21.08.2020 г.

[2] п. 14.1.12, СТО 56947007-25.040.80.266-2019, Типовые технические требования к ССПИ ПС с функцией удаленного управления ПС из ЦУС», ПАО «ФСК ЕЭС», 2019 г.

[3] RFC 4330, Simple Network Time Protocol (SNTP) Version IPv4, IPv6 and OSI, D. Mills, University of Delaware, January 2006.

[4] ЭНИП.411187.002 РЭ, Преобразователь измерительный многофункциональный ЭНИП-2, Руководство по эксплуатации, Ред 05.2021.

[5] ЭНКС.681730.001 РЭ, Блок коррекции времени ЭНКС-2, Руководство по эксплуатации, Ред. 04.2021.

[6] ЭНИП.411187.003 ПО, ENIP Test Программное обеспечение, Руководство пользователя, 2018 г.

[7] п. 4.2.1, СТО 56947007-29.240.10.265-2019 «Общие требования к метрологическому контролю измерительных каналов ЦПС», ПАО «ФСК ЕЭС», 2019 г.

[8] п.11.1.3.3, IEC 61850-5:2013, International Standard, Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models, 2013.

[9] п. 5.6, СТО 59012820.29.020.011-2016 «Релейная защита и автоматика. Нормы и требования», АО «СО ЕЭС», 2016.

[10] п.6.904.1, IEC 61869-9:2016, International Standard, Instrument transformers – Part 9: Digital interface for instrument transformers, 2016.

[11] п.7.2, IEC 61850-9-3:2016, International Standard, Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation, 2016.

[12] Таблица 14, IEC 61850-9-2:2011, International standart, Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3, 2011.

[13] СТО 34.01-6.1-002-2016, Программно-технические комплексы подстанций 35-110 (150) кВ. Общие технические требования, ПАО «Россети», 2017 г.

[14] СТО 34.01-6.1-001-2016, Программно-технические комплексы подстанций 6-10 (20) кВ. Общие технические требования, ПАО «Россети», 2017 г.

1.12. МЕТРОЛОГИЧЕСКИЕ ХАРАКТЕРИСТИКИ И ОПЫТ ВНЕДРЕНИЯ ПРЕОБРАЗОВАТЕЛЕЙ АНАЛОГОВЫХ СИГНАЛОВ

Р. С. ПЛАКИДИН [1], С. А. ПИСКУНОВ [1], Д. Н. ПОПОВ [1], А. С. СОСНИН [1], А. В. МОКЕЕВ [2]

[1] ООО «Инженерный центр «Энергосервис»,

[2] Северный (Арктический) федеральный университет

Российская Федерация

Контактное лицо:

Р. С. ПЛАКИДИН

rplakidin@ens.ru

Ключевые слова: Цифровая подстанция, измерительные трансформаторы, преобразователи аналоговых сигналов (ПАС), интеллектуальные электронные устройства, переходный режим, частота среза, постоянная времени, С-О-С-О, В-О-В-О.

Введение

При разработке и внедрении в составе цифровых подстанций преобразователей аналоговых сигналов (SAMU, ПАС), подключаемых к традиционным электромагнитным трансформаторам тока (ТТ) и напряжения (ТН), необходимо уделять особое внимание их работе в условиях переходных процессов [1]. Метрологические характеристики преобразователей аналоговых сигналов (ПАС) определяются преимущественно характеристиками промежуточных измерительных преобразователей сигналов, в качестве которых чаще всего используются промежуточные электромагнитные трансформаторы тока (ПТТ) и напряжения [2]. В меньшей степени оказывают влияние на указанные характеристики оставшаяся аналоговая часть ПАС, АЦП и особенности микроконтроллера (поддержка целочисленных операций или операций над числами с плавающей запятой). Таким образом, необходимо учитывать совокупность метрологических характеристик измерительных трансформаторов и ПАС. В связи с этим в докладе рассмотрены требования современных стандартов к точности измерений в установившемся и в переходных режимах как для первичных измерительных преобразователей, так и ПАС. При этом основное внимание в докладе уделено требованиям к измерительным трансформаторам тока (ТТ) и токовым измерительным каналам ПАС, содержащим в своем составе ПТТ.

В докладе рассмотрен практический опыт реализации данных требований на примере преобразователей аналоговых сигналов ENMU, подключаемых к традиционным электромагнитным трансформаторам тока и напряжения. Рассмотрены способы определения динамических характеристик ПАС. Приведены сравнительные характеристики исследованных отдельных измерительных компонентов. Рассмотрены результаты исследования совместного влияния насыщения трансформатора тока (первичного измерительного преобразователя тока) и промежуточного трансформатора тока (вторичного преобразователя) на форму сигнала. Приведен анализ негативного влияния искаженного сигнала на различные виды защит.

Требования к метрологическим характеристикам ТТ и ПАС

Международный стандарт [3] и идентичный ему ГОСТ [4] содержат описание дополнительных требований к работе ТТ в различных переходных режимах, в том числе связанных с наличием в первичном токе апериодической составляющей при возникновении электромагнитного переходного процесса. В этом случае традиционные ТТ насыщаются, что приводит к большой погрешности измерений [5]. Для корректной работы устройств защиты ТТ должны иметь иммунитет к апериодической составляющей и не насыщаться как можно дольше: время противодействия насыщению ТТ в переходном режиме должно быть достаточным для работы защит.

Соблюдение данных требований необходимо как для ТТ [6, 7], так и для ПАС [8]. Необходимо учитывать два взаимосвязанных требования к ПАС: требование к точности измерения в динамическом нормированном рабочем цикле B-O-B-O (C-O-C-O duty cycle) и к заявленной нижней частоте среза частотной характеристики ПТТ.

Описание испытательного сигнала и расчетные формулы приведены в указанных стандартах. Для работы в переходных режимах для ТТ стандартом [3] определены классы точности TPX, TPY, TPZ. Аналогичным образом и для защитных токовых каналов ПАС стандартом [7] предусмотрены классы точности: 2TPM, 6TPM, 10TPM.

Программно-технический комплекс

Для проведения исследования метрологических характеристик ПАС применяется программно-технический комплекс (ПТК), в состав которого входит специализированное ПО «SVTest2» и испытательное оборудование российских и зарубежных производителей [14].

На рисунке 1 приведена структурная схема ПТК, используемая при статических и динамических испытаниях ПАС (SAMU) соответственно.

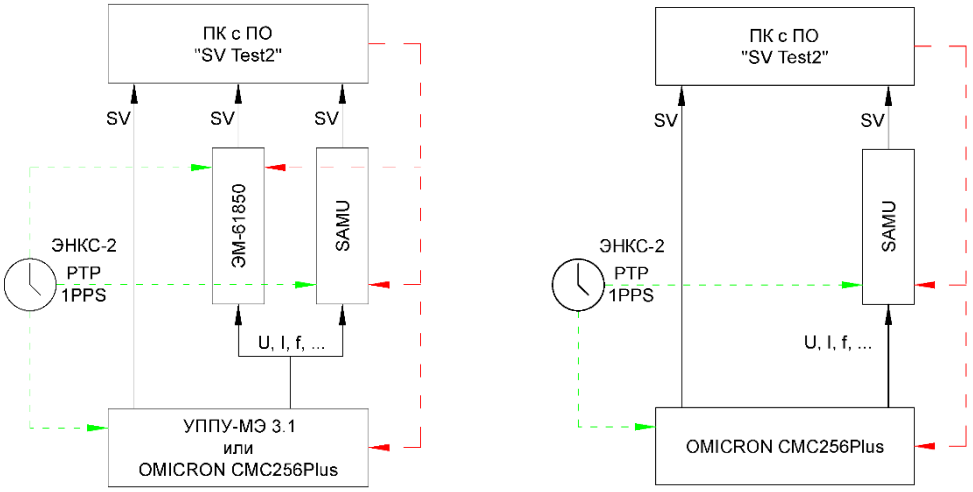


Рис. 1. Структурные схемы ПТК при проведении испытаний ПАС: обобщенная (слева), для испытаний динамических характеристик (справа).

Важнейшим компонентом ПТК, объединяющим функциональные возможности всех аппаратных составляющих, является ПО «SVTest2», разработанное специалистами ООО «Инженерный центр «Энергосервис». ПО «SVTest2» позволяет воспроизводить на генераторе сигналы произвольной формы. Для исследования точности в динамическом нормированном рабочем режиме (C-O-C-O duty cycle) в ПО «SVTest2» предусмотрен упрощенный способ описания сигнала путем ввода основных параметров режима (t', t'', t_{fr}, T_p, I). Режим сравнения потоков SV в ПО «SVTest2» позволяет наблюдать в реальном времени и производить запись потоков SV, принимаемых от эталона и исследуемого ПАС (SAMU).

Исследование характеристик ПАС согласно IEC 61869-13

Ниже рассматривается исследование выполнения ПАС требований стандарта IEC 61869-13 по работе в переходных процессах, а именно требования к точности измерения в динамическом нормированном рабочем режиме (C-O-C-O duty cycle).

Выполнение указанных требований в основном определяется характеристиками промежуточных трансформаторов тока (ПТТ), чаще всего устанавливаемых во внешних ПАС (SAMU) для обеспечения масштабирования сигнала и гальванической развязки. Подобные трансформаторы устанавливаются в устройствах РЗА и других ИЭУ, но их исследование является сугубо внутренним делом производителей таких устройств. Следует отметить, что существуют и принципиально иные способы указанного преобразования сигнала, но именно промежуточные

трансформаторы тока наиболее массово применяются как в ПАС, так и в ИЭУ с аналоговыми входами.

Необходимость проведения исследований обусловлена тем, что большинство производителей ПТТ не приводят необходимые для ПАС характеристики, в том числе амплитудно-частотные и фазово-частотные характеристики в различных условиях эксплуатации, а также влияние на процесс преобразования тока апериодической составляющей.

В качестве объекта исследований используется многофункциональный измерительный преобразователь аналоговых сигналов ENMU, подключаемый к традиционным электромагнитным ТТ и ТН. При этом ENMU подключается как к релейным, так и к измерительным обмоткам ТТ и обеспечивает формирование SV-потоков как для устройств РЗА, так и для измерительных интеллектуальных устройств.

Для исследований соответствия точности измерения в динамическом нормированном рабочем режиме (C-O-C-O duty cycle) в ENMU были установлены пять ПТТ российских и зарубежных производителей, обозначим их под номерами 1, 2, 3, 4, 5. Номинальные токи всех исследуемых образцов не менее 100 А. При этом первые три ПТТ обладают иммунитетом к апериодической составляющей, т. е. обеспечивают минимальные искажения составляющей промышленной частоты и высших гармоник при наличии во входном токе апериодической составляющей.

С помощью ПО «SVTest2» производилось исследование ENMU с указанными ПТТ. Так как программа позволяет сохранять результаты исследований, то дальнейшие исследования производились при использовании математического пакета Mathcad.

На рис. 2 представлены результаты исследований 3 и 4 ПТТ. Эталонный сигнал показан на кривой 0 (действующее значение синусоидальной составляющей 50 Гц 25 А, начальное значение апериодической составляющей $25\sqrt{2}$, постоянная времени 120 мс).

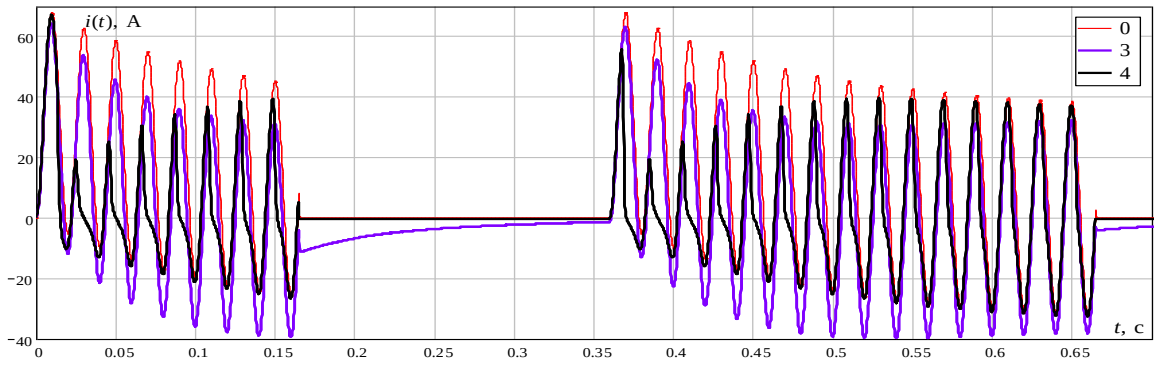


Рис. 2. Исследование ПАС при использовании 3 и 4 ПТТ.

На рис. 3 представлены начальные области двух переходных участков (первая и вторая подача сигнала) для всех исследуемых ПТТ. Из представленных графиков следует, что быстродействующие защиты в первом цикле сработают правильно при использовании всех исследуемых ПТТ, тогда как во втором цикле при использовании ПТТ без иммунитета к апериодическим составляющим

значительно искажают форму кривой тока, что приведет к существенной задержке срабатывания защиты.

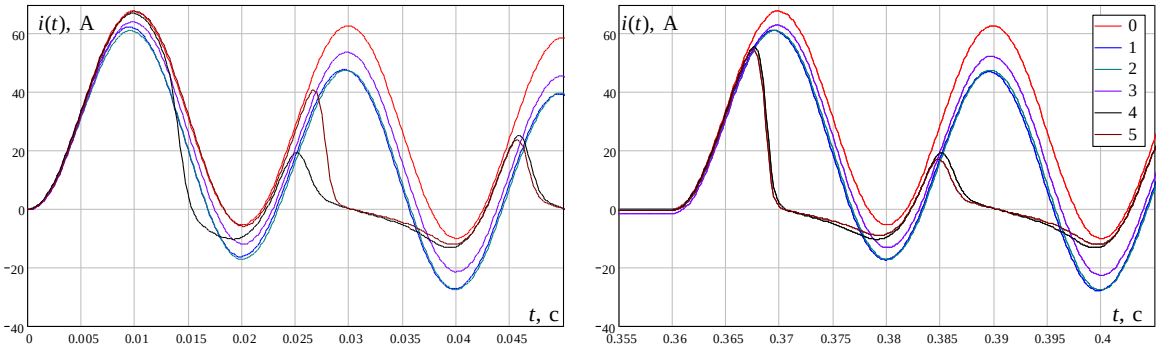


Рис. 3. Исследование ПАС при использовании пяти ПТТ:
0 – исходный сигнал; 1, 2, 3, 4, 5 – после ПТТ.

Последнее наглядно продемонстрировано на рис. 4, где приведена оценка амплитуды основной гармоники при использовании алгоритма Фурье, широко применяемого во многих устройствах РЗА зарубежных и российских производителей [9].

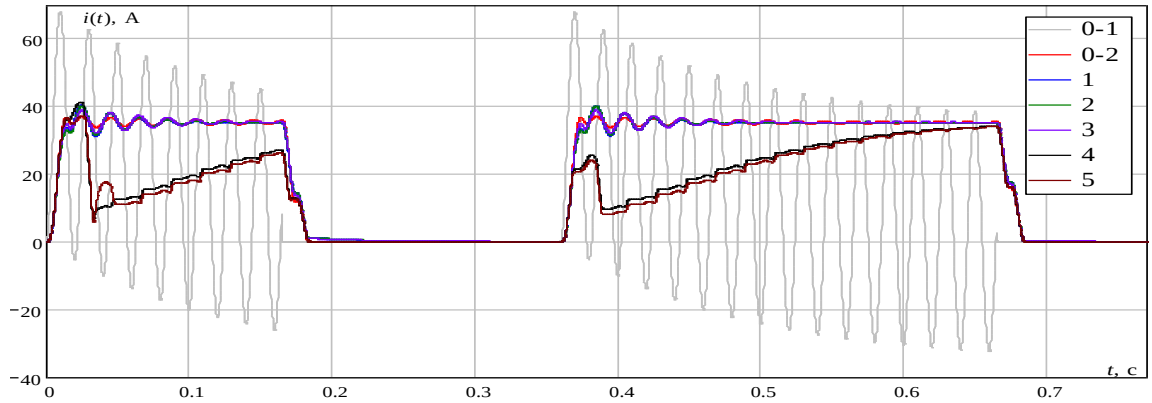


Рис. 4. Исследование ПАС при использовании пяти ПТТ.

0-1– исходный сигнал,

0-2 – исходный сигнал после обработки алгоритмом Фурье,

1, 2, 3, 4, 5 – сигналы после обработки выходных сигналов ПТТ алгоритмом Фурье.

Корректное восстановление синусоидальной и апериодической составляющей возможно лишь в случае использования 1-3 ПТТ.

Рассмотрим восстановление синусоидальной составляющей для 3 ПТТ (рис. 5) на основании оценки комплексной амплитуды первой гармоники при использовании алгоритма Фурье. Красным цветом показан исходный синусоидальный сигнал, фиолетовым – восстановленный сигнал.

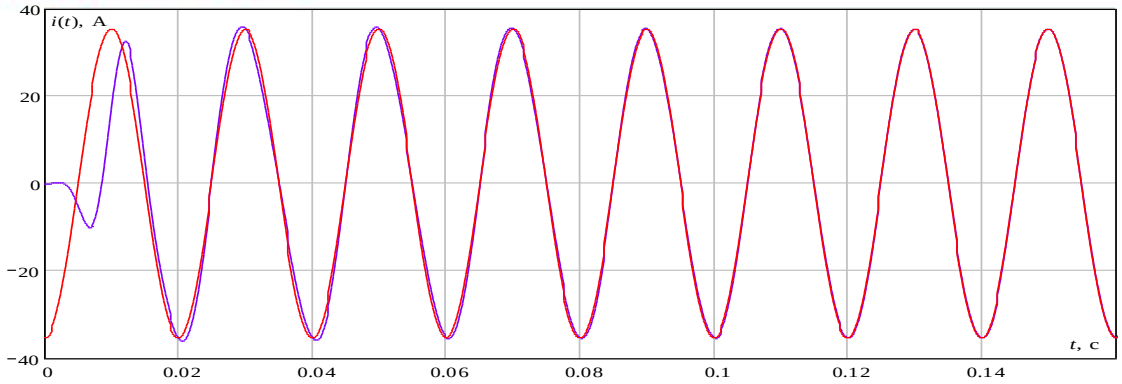


Рис. 5. Восстановление синусоидальной составляющей 3-го образца.

Восстановление апериодической составляющей возможно на основе оценки нулевой гармоники (рис. 6). Погрешность восстановления апериодической составляющей зависит от соотношения постоянной времени входного сигнала (T_l) и постоянной времени фильтра самого ПАС (T_{sec}). Как следует из приведенных графиков, для восстановления апериодической составляющей требуется применение более сложных алгоритмов. Это особенно важно для защит, которые используют полную информацию о токах и напряжениях [10]. Наилучшим решением для указанных защит будет применение современных первичных измерительных преобразователей тока и напряжения и применение в составе ПАС промежуточных измерительных преобразователей тока, которые не вносят нелинейных искажений в случае наличия апериодической составляющей.

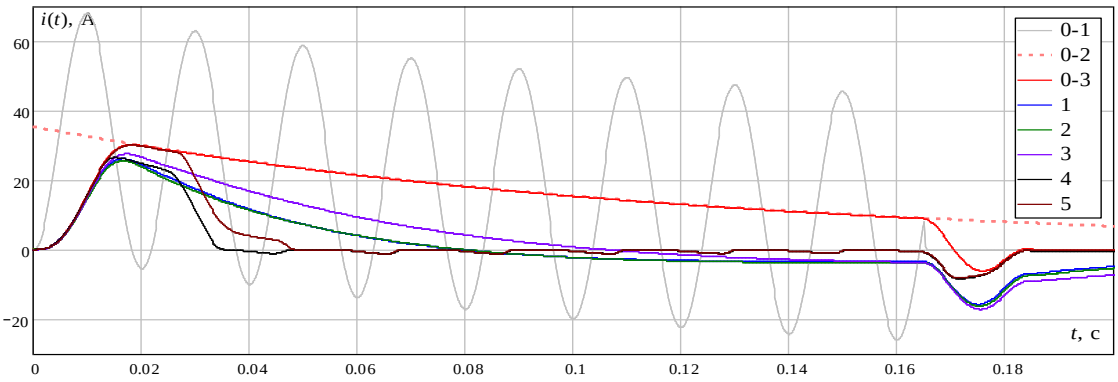


Рис. 6. Восстановление апериодической составляющей.

0-1 – исходный сигнал,

0-2 – исходная апериодическая составляющая,

0-3 – оценка апериодической составляющей по исходному сигналу,

1, 2, 3, 4, 5 – оценка апериодической составляющей по выходным сигналам ПТТ.

Но в измерительном канале тока влияние на качество измерений (сохранение информации содержащейся в исходном сигнале) оказывает не только ПТТ, но и измерительный ТТ. Рассмотрим моделирование совместного влияния ТТ и ПТТ на исходный сигнал.

В ходе исследований проведено математическое моделирование совместной работы первичных измерительных трансформаторов тока и промежуточных трансформаторов тока нескольких типов.

В качестве промежуточных трансформаторов тока были использованы модели ПТТ под номерами 3 и 4. Математические модели ПТТ были разработаны в программной среде MATLAB/Simulink. Кроме того, было разработано две модели первичного измерительного трансформатора тока (ТТ). Технические параметры первой модели: коэффициент трансформации 1000/5 А, класс точности релейной обмотки 10Р, номинальная вторичная нагрузка 15 ВА и номинальная предельная кратность 10. Вторая модель – с аналогичными техническими параметрами, но соответствующая классам точности для работы в переходных режимах [3].

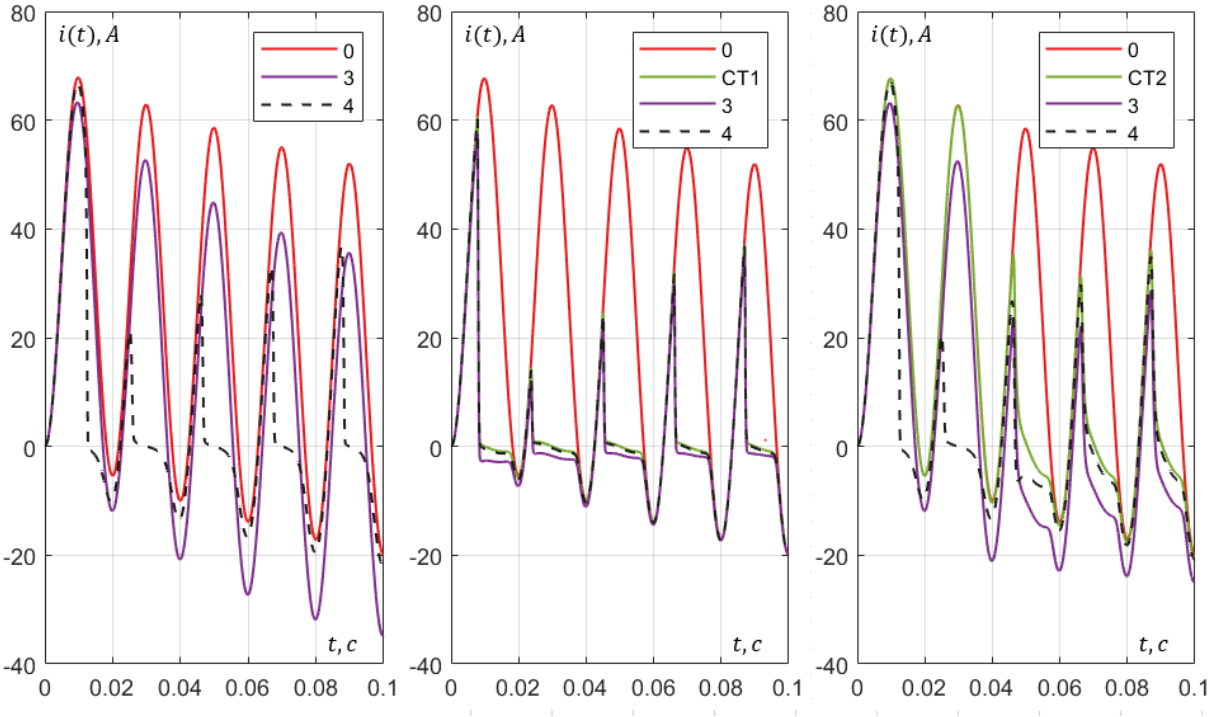
На рис. 7 показаны результаты моделирования совместной работы ТТ и ПТТ. В первом случае (рис. 7, левый график) исходный сигнал подается на первичную обмотку ПТТ (номер 3 и 4), во втором и третьем – на первичную обмотку ТТ (СТ1 и СТ2 соответственно), а со вторичной обмотки ТТ – на первичную обмотку ПТТ. Значения исходного сигнала на центральном и правом графике (рис. 7), а также все значения сигнала после ПТТ приведены ко вторичной обмотке первичного ТТ.

Эталонный сигнал показан кривой 0 (действующее приведенное значение синусоидальной составляющей 50 Гц 25 А, начальное значение апериодической составляющей $25\sqrt{2}$, постоянная времени 120 мс).

Когда эталонный сигнал 0 подается непосредственно на первичную обмотку ПТТ (рис. 7, левый график), форма сигнала после ПТТ соответствует ранее полученным данным об исследовании работы реальных ПТТ под номером 3 и 4 (рис. 2).

При подаче исходного сигнала на первичную обмотку СТ1 (первая модель) происходит искажение формы сигнала в результате насыщения сердечника данного ТТ (рис. 7, центральный график), при этом его номинальная предельная кратность не превышена. Таким образом, модель СТ1 при наличии значительной апериодической составляющей в исходном сигнале не обеспечивает его передачу в переходном режиме. Сигнал после ПТТ имеет схожую форму, но для модели ПТТ под номером 3 смещен вниз относительно вертикально оси, что можно объяснить различной частотой среза данных моделей ТТ и ПТТ.

В случае, когда ТТ обеспечивает передачу исходного сигнала в переходном режиме в течение некоторого времени (рис. 7, правый график, вторая модель ТТ обозначена СТ2), искажение сигнала может внести промежуточный трансформатор тока (на рис. 7 модель ПТТ под номером 4), который насыщается раньше СТ2.



0 – исходный сигнал,

CT1, CT2 – сигнал после трансформатора тока,

3, 4 – сигнал после ПТТ.

Рис. 7. Моделирование работы трансформаторов тока.

Таким образом, для корректной передачи исходного сигнала в измерительном канале необходимо правильно подходить к выбору не только измерительных трансформаторов тока, но и промежуточных. Классы точности ТТ и ПТТ должны быть скоординированы для работы в переходном режиме. В противном случае даже применение ПТТ с классами точности ТРМ без соответствующего класса ТТ не гарантирует правильной трансформации первичного тока.

Исследование частоты среза (cutoff frequency) ПТТ проводилось двумя способами (рис. 11).

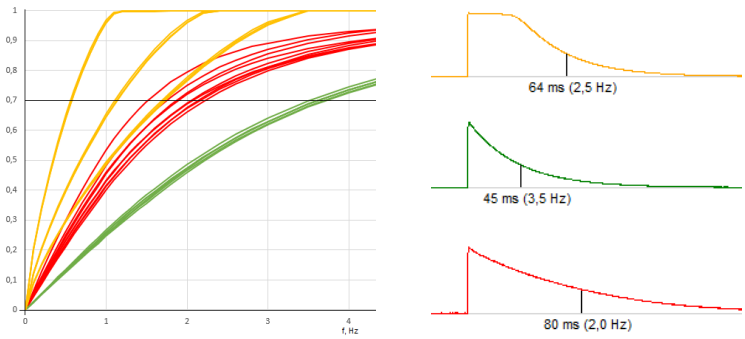


Рис. 11. Определение частоты среза: путем снятия АЧХ (слева) и анализом отклика на ступенчатый сигнал (справа).

Для снятия АЧХ с помощью ПТК подавался сигнал необходимой амплитуды и частотой от 0,1 до 10 Гц с шагом 0,1 Гц, записывалась осциллограмма с последующим расчетом среднеквадратического значения (RMS). Для определения частоты среза анализом отклика на ступенчатый сигнал с помощью ПТК подавался ступенчатый сигнал необходимой амплитуды и записывалась осциллограмма. Результаты определения частоты среда обеими методами сходятся между собой. Чем меньше частота среза, тем лучше устройство пропускает апериодическую составляющую. Частота среза измерительного канала определяется по наихудшей частоте среза компонентов канала (ТТ, ПАС, устройство РЗА).

Опыт внедрения пас

Преобразователь аналоговых сигналов ENMU внесен в реестр средств измерений в январе 2019 года (73811-19). С января 2018 ENMU проходит опытно-промышленную эксплуатацию в качестве источника данных для устройства РЗА и системы учета на ПС «Магистральная». В сентябре 2019 года успешно прошел испытания на совместимость с терминалами защит «ЭКРА» и «Прософт» на базе испытательного комплекса ОАО «Сетевая компания».

ПО «SVTest2» и преобразователь ENMU в августе 2019 года были использованы при исследованиях характеристик высоковольтных трансформатора напряжения на эффекте Поккельса с цифровым выходом. ENMU был откалиброван с высокой точностью и использован в составе эталонной установки для преобразования эталонного аналогового сигнала в SV-поток, а ПО «SVTest2» использовалось как удобный инструмент для сравнения значений и записи результатов.

Поскольку ПАС может быть использован в различных автоматизированных системах, то он должен соответствовать требованиям, предъявляемым к устройствам этих систем, в том числе требованиям, предъявляемым к РЗА, системам телемеханики, системам мониторинга переходных режимов, системам коммерческого учета электроэнергии и измерения показателей качества. В конце 2019 года ENMU в составе АИИС КУЭ цифровой подстанции внесен в реестр средств измерений (76297-19, 76298-19).

Кроме того, ENMU является также многофункциональным интеллектуальным устройством [[11]]. В качестве примера многофункционального преобразователя аналоговых сигналов можно привести устройство ENMU, которое обеспечивает формирование и передачу не только «сырых» оцифрованных мгновенных значений токов и напряжений, но и измерение и передачу синхровекторов токов и напряжений.

Преобразователи аналоговых сигналов ENMU внедрены в составе цифровых подстанций ПС 500 кВ «Тобол», ЦПС 110/6 кВ «Уват» и ЦПС 110/6/6 кВ «Десна». В процессе пусконаладочных работ на указанных подстанциях использовался ПТК и ПО «SVTest2». При этом использовались два режима функционирования: управление Omicron CMC 256 plus для проверки правильности настройки оборудования и просмотр и сравнение потоков в реальном времени. При испытаниях был организован доступ (настроены права доступа) к коммутатору в шине процесса. К коммутатору был подключен ноутбук с ПО «SVTest2», что позволило увидеть в реальном времени все потоки SV, сравнивать их между собой или с эталонным потоком, просматривать значения амплитуд, фаз, мощностей, проводить анализ спектрального состава сигнала.

Всего поставлено заказчикам более 300 преобразователей сигналов ENMU. В настоящее время ведется подготовка к серийному производству нового поколения ENMU с поддержкой совмещенной шины процесса и шины подстанции (мультишина). В преобразователях сигналов нового поколения заложена возможность применения в токовых измерительных каналах ПАС различных промежуточных измерительных преобразователей, соответствующих требуемым характеристиками.

Заключение

При разработке устройств РЗА, а также при проектировании измерительных каналов релейной защиты необходимо учитывать требования современных международных стандартов к работе в переходном режиме.

Полученный опыт разработки и применения ПАС показывает, что требования стандартов являются не только достижимыми на практике, но и необходимыми в применении.

Производители ТТ, ПАС, РЗА должны указывать не только погрешность в статическом режиме, но и погрешность в динамическом режиме совместно с максимальной постоянной времени, при которой рассчитана указанная погрешность, а также АЧХ устройства, постоянную времени входного фильтра.

Кроме того, соблюдение требований стандартов и декларирование указанных характеристик позволит разрабатывать и применять новые алгоритмы релейной защиты.

СПИСОК ЛИТЕРАТУРЫ

[1] Холст С., Законьшек Я. Поведение традиционных трансформаторов тока в переходных режимах и его влияние на характеристики традиционных систем релейной защиты на базе шины процесса // Релейщик. – 2020. – №3. – С.20-25

[2] Булычев А. В., Ванин В. К. Исследование частотных характеристик трансформаторов тока // Энергетика (Изв. высш. учеб. заведений). – 1987. – №8. – С.16–21

[3] IEC 61869-2:2012. Instrument transformers - Part 2: Additional requirements for current transformers, 2012

[4] ГОСТ Р МЭК 61869-2-2015 Трансформаторы измерительные - Часть 2: Дополнительные требования к трансформаторам тока, 2015

[5] С. Л. Кужеков, А. А. Дегтярев, Б. Б. Сербиновский. О требованиях к трансформаторам тока и устройствам релейной защиты в переходных режимах при наличии апериодической составляющей в первичном токе // Сб. трудов междун. IV научно.-техн. конф. "Современные направления развития систем релейной защиты и автоматики энергосистем". – Ек, 2013

[6] IEC 61869-1 ED2 Draft. Instrument transformers - Part 1: General requirements, 2020

[7] IEC 61869-9:2016. Instrument transformers - Part 9: Digital interface for instrument transformers, 2016

[8] IEC 61869-13 ED1 Draft. Instrument Transformers - Part 13: Stand-alone Merging Unit, 2020

[9] Understanding microprocessor-based technology applied to relaying // Report of Working Group I16 of the Relaying Practices Subcommittee IEEE, 2004

[10] Антонов В. И. Адаптивный структурный анализ электрических сигналов: теория и ее приложения в интеллектуальной электроэнергетике. – Чебоксары: Изд-во Чувашского ун-та, 2018. – С.333

[11] Мокеев А. В. и др. Многофункциональные устройства для цифровых подстанций // Энергия Единой сети. – 2019. – № 6. – С. 8-16

[12] V. Skendzic, D. Dolezilek. New and emerging solutions for sampled value process bus IEC 61850-9-2 standard – an editor's perspective // Relay Protection and Automation for Electric Power Systems, 2017

[13] Рожкова Л. Д., Козулин В. С. Электрооборудование станций и подстанций. М.: Энергоатомиздат, 2007. С. 150

[14] Плакидин Р. С., Ульянов Д. Н., Попов Д. Н., Соснин А. С., Мокеев А. В. Требования к метрологическим характеристикам преобразователей аналоговых сигналов // «Релейная защита и автоматизация» №1 (42) 2021, С. 38-45.

1.13. СПОСОБЫ ПЕРЕДАЧИ GOOSE-СООБЩЕНИЙ МЕЖДУ ПОДСТАНЦИЯМИ ДЛЯ СИСТЕМ РЗА

В. А. ХАРЛАМОВ, С. Е. РОМАНОВ, А. Х. ХАСАНОВ

ООО «Юнител Инжиниринг»

Российская Федерация

Контактное лицо:

В. А. ХАРЛАМОВ

V.Harlamov@uni-eng.ru

Ключевые слова: Цифровая подстанция, МЭК 61850, GOOSE, устройство передачи аварийных сигналов и команд, каналы связи.

Введение

В настоящее время в российской электроэнергетике команды релейной защиты (РЗ) и противоаварийной автоматики (ПА) передаются по высокочастотным (ВЧ) каналам, цифровым сетям связи (ЦСС) и выделенным оптическим волокнам (ОВ) с помощью устройств передачи аварийных сигналов и команд (УПАСК). Для передачи дискретных сигналов, в том числе команд РЗ и ПА, на цифровых подстанциях (ЦПС) на базе МЭК 61850 используются GOOSE-сообщения согласно МЭК 61850-8-1, передаваемые между устройствами РЗА по внутриобъектовой локальной вычислительной сети (ЛВС) Ethernet. Определены три типа архитектур построения подстанций (ПС):

- архитектура I типа (традиционная ПС), в которой обмен информацией между устройствами РЗА осуществляется дискретными и аналоговыми электрическими сигналами, передаваемыми по контрольным кабелям, а обмен информацией с автоматизированными системами управления технологическими процессами (АСУ ТП) осуществляется по MMS согласно МЭК 61850-8-1;
- архитектура II типа (ЦПС), в которой измерения тока и напряжения передаются в виде электрических аналоговых сигналов по контрольным кабелям, взаимодействие между устройствами РЗА выполняется при помощи GOOSE-сообщений, а обмен информацией с АСУ ТП осуществляется по MMS;
- архитектура III типа (ЦПС), в которой измерения токов и напряжений передаются с использованием мгновенных значений SV согласно IEC 61850-9-2, взаимодействие между устройствами РЗА выполняется при помощи GOOSE-сообщений, а обмен информацией с АСУ ТП осуществляется по MMS.

Для упрощения проектирования, эксплуатации и технического обслуживания систем РЗА необходима типизация обмена GOOSE-сообщениями как внутри объектов, так и между объектами. Совершенно очевидно, что ЦПС не будут внедрены в энергопредприятиях сразу и повсеместно, и поэтому типовые решения должны обеспечивать передачу команд РЗ и ПА между ПС с архитектурой I типа и ЦПС с архитектурами II и III типов. При этом типизация обмена GOOSE-сообщениями между ПС должна использовать наилучшие доступные технологии и не должна являться препятствием для развития систем РЗА.

Варианты передачи goose-сообщений между пс

Согласно МЭК 61850 [1], для обмена GOOSE-сообщениями между объектами электроэнергетики можно использовать два варианта.

Первый вариант, показанный на рис. 1, – туннелирование, где между объектами организуется широкополосный Ethernet-канал, по которому с помощью оборудования сетей связи передаются GOOSE-сообщения.



Рис. 1. Туннелирование для передачи GOOSE-сообщений между ЦПС.

Второй вариант, показанный на рис. 2, – шлюз, который предполагает использование УПАСК для обмена GOOSE-сообщениями между объектами. В данном варианте УПАСК на передающей стороне преобразует дискретные сигналы из GOOSE-сообщений в кодированные аналоговые или цифровые сигналы, которые предназначены для надежной и безопасной передачи и приема команд РЗ и ПА по каналу. На приемной стороне УПАСК из принятых по каналу кодированных сигналов формирует GOOSE-сообщения.



Рис. 2. Использование УПАСК для передачи GOOSE сообщений между ЦПС.

Среды распространения сигналов для передачи goose-сообщений между пс

Как уже отмечалось выше, в настоящее время в российских энергопредприятиях команды РЗ и ПА передаются по ВЧ-каналам, ЦСС и выделенным ОВ.

При туннелировании для передачи GOOSE-сообщений необходимы цифровые каналы между ПС. По ЦСС и выделенным ОВ такие каналы могут быть организованы. В то же время, учитывая необходимость передачи команд РЗ и ПА при наличии короткого замыкания на ЛЭП, организовать высоконадежные цифровые ВЧ-каналы для GOOSE-сообщений невозможно [2]. Таким образом, при использовании туннелирования в качестве типового решения для передачи GOOSE-сообщений необходим полный отказ от использования ВЧ-каналов.

При использовании шлюза в передатчике УПАСК GOOSE-сообщения преобразуются в ВЧ-сигналы, которые передаются по ВЧ-тракту, а на другой стороне канала УПАСК из принятых ВЧ-сигналов формирует GOOSE-сообщения. Таким образом, при использовании шлюза в виде УПАСК возможно организовывать передачу GOOSE-сообщений не только по ЦСС и выделенным ОВ, но и по ВЧ-каналам.

Требования к скорости передачи данных в канале по цсс

Существует мнение, что современные телекоммуникационные технологии могут обеспечить практически неограниченную пропускную способность ЦСС между ПС. Однако это не так. Увеличение скорости передачи данных в ЦСС накладывает физические ограничения на протяженность оптических волокон (рис. 3) [3]. Уменьшение мощности передатчиков и ухудшение чувствительности приемников делают невозможным достижение высокой пропускной способности ЦСС при больших расстояниях между ПС (за разумные капитальные затраты и затраты на эксплуатацию и обслуживание). Поэтому важными являются предъявляемые туннелированием и шлюзом требования к пропускной способности каналов.

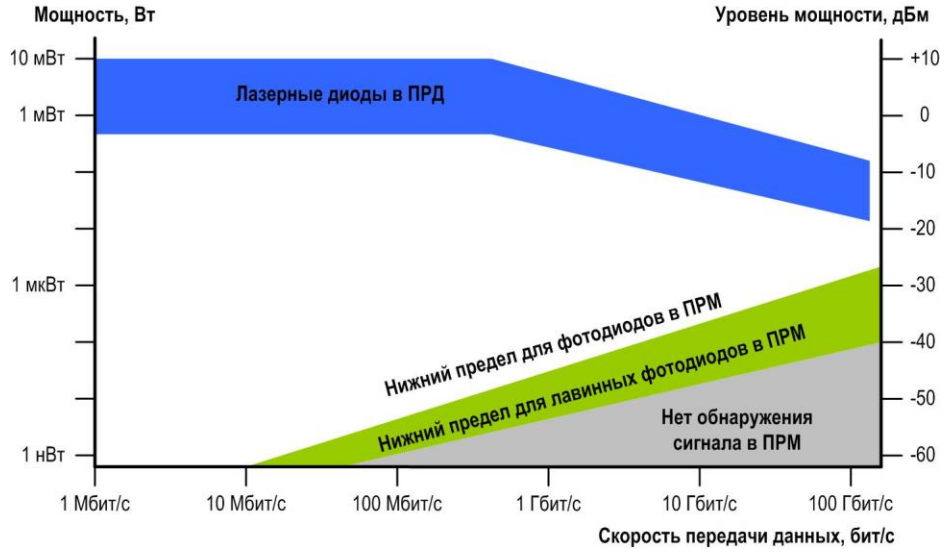


Рис. 3. Зависимости мощности оптических передатчиков и чувствительности оптических приемников от скорости передачи данных.

Для УПАСК большинства производителей, которые обеспечивают функциональность шлюза, для передачи от 1 до 8 команд (GOOSE-сообщений с 1-8 командами) требуются каналы со скоростью 64 кбит/с. Для передачи 8 команд с требуемыми надежностью и безопасностью может быть использована посылка длиной 16 байт (128 бит). Если предположить, что канал обладает нулевой задержкой, то время прохождения ее по каналу составит 2 мс (без учета обработки в УПАСК).

Требования к пропускной способности канала Ethernet для прохождения GOOSE-сообщения с 8 командами за 2 мс при туннелировании приведены в таблице 1.

Формат передачи данных GOOSE сообщения	**Размер GOOSE сообщения, байт**	**Требуемая скорость передачи данных, кбит/с**
BOOLEAN	168	672
BOOLEAN + Quality	205	820

SPS	301	1204

Табл. 1. Требуемая пропускная способность канала для прохождения GOOSE-сообщения с 8 командами за время 2 мс.

Таким образом, туннелирование требует существенно большей пропускной способности каналов по ЦСС, чем шлюз в виде УПАСК.

Надежность передачи GOOSE-сообщений

Параметры передачи GOOSE-сообщений, принятые в ПАО «ФСК ЕЭС», приведены на рис. 4. При отсутствии изменений в состоянии передаваемых сигналов GOOSE-сообщения передаются с интервалами в 1 секунду, а при наступлении изменений производится повторение передачи с меньшими интервалами. Таким же образом GOOSE-сообщения будут передаваться по каналу между ПС в случае туннелирования.



Рис. 4. Параметры передачи GOOSE-сообщений.

При использовании шлюза в виде УПАСК GOOSE-сообщения преобразуются в сигнал, который передается по каналу между ПС практически непрерывно.

Предположим, что время прохождения по каналу одного GOOSE-сообщения как при использовании туннелирования, так и при использовании шлюза составляет 2 мс. На рис. 5 показан прием GOOSE-сообщений при наличии ошибки в канале. Ошибки в канале приводят к потере передаваемых данных.

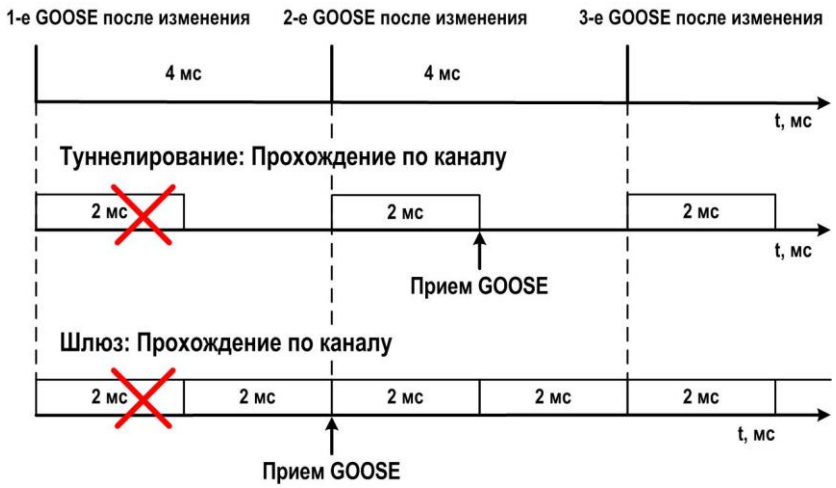


Рис. 5. Прием GOOSE-сообщений при наличии ошибок в канале.

При наличии ошибки в канале GOOSE-сообщение будет принято только при повторной его передаче по каналу. Так как передатчик в шлюзе в виде УПАСК непрерывно передает по каналу сигналы о состоянии GOOSE-сообщений на его коммуникационном Ethernet-интерфейсе, то прием GOOSE-сообщения произойдет ранее, чем в случае туннелирования. При увеличении вероятности ошибок в канале между ПС возрастет вероятность возникновения ошибок при прохождении второго GOOSE-сообщения при туннелировании, что еще больше увеличит время его передачи по сравнению со шлюзом в виде УПАСК.

Таким образом, при наличии ошибок в канале время передачи GOOSE-сообщений при туннелировании будет больше, чем при использовании шлюза в виде УПАСК, и, следовательно, надежность передачи команд РЗ и ПА при туннелировании будет меньше.

Следует отметить, что увеличение скорости передачи данных в туннеле между ПС не приведет к увеличению надежности передачи GOOSE-сообщений, т. к. параметры их передачи (интервалы между GOOSE-сообщениями) останутся теми же.

Мониторинг состояния и пропускной способности канала по цсс между пс

Без контроля состояния и пропускной способности каналов по ЦСС между ПС невозможно обеспечить требуемое время передачи команд РЗ и ПА и надежность их передачи. В настоящее время УПАСК, выполняющие передачу команд РЗ и ПА между ПС с архитектурой I типа, обеспечивают данный контроль.

То же можно сказать и про УПАСК, которые выполняют функцию шлюза при передаче GOOSE-сообщений между объектами. Они преобразуют GOOSE-сообщения в сигнал, который практически постоянно передается по каналу между ПС, и способны обеспечить непрерывный мониторинг состояния и пропускной способности каналов по ЦСС.

Передаваемые по туннелям GOOSE-сообщения не могут обеспечить непрерывный мониторинг состояния и пропускной способности каналов по ЦСС в принципе. Причина состоит в том, что GOOSE-сообщения передаются по каналу не постоянно, а с некоторой периодичностью (рис. 4). Если по какой-либо причине, например, из-за ошибки персонала, обслуживающего ЦСС, пропускная способность Ethernet-туннеля между ПС будет снижена, то при передаче GOOSE-сообщения с интервалами в одну секунду это не будет обнаружено. Также будет недоступен контроль ошибок в канале и прерываний канала, которые произошли между передачей GOOSE-сообщений (такой контроль важен, т. к. может свидетельствовать о деградации или неисправности канала). Отсутствие при туннелировании достоверного мониторинга состояния и пропускной способности каналов по ЦСС для передачи команд РЗ и ПА уменьшит надежность функционирования систем РЗА на ПС с архитектурами II и III типов по сравнению с существующими ПС с архитектурой I типа.

Оперативное управление приемом команд

При использовании туннелирования в оборудовании ЦСС невозможно организовать визуальную сигнализацию прохождения отдельных команд РЗ и ПА по каналу и обеспечить

управление вводом и выводом приема отдельных команд ключами. Согласно концепции развития РЗА [4], оперативный персонал ПС или оперативно-выездной бригады должен иметь возможность изменить режим работы устройства с применением местного управления, т. е. вводить и выводить команды РЗ и ПА ключами, что особенно важно для команд ПА, которые реализуются на ПС и могут далее проходить через нее транзитом.

В шлюзе в виде УПАСК возможно реализовать индикацию передачи и приема команд РЗ и ПА и функцию ввода/вывода приема команд программными логическими ключами как всех вместе, так и по отдельности.

Наладка и эксплуатация

В отличие от команд РЗ, которые передаются между двумя или небольшим числом ПС в случае наличия у ЛЭП ответвлений, команды ПА передаются в пределах всей энергосистемы. При туннелировании этим и обусловлена большая сложность наладки и эксплуатации систем с передачей команд ПА. В частности, при туннелировании большой проблемой является отсутствие визуальной сигнализации передачи и приема команд, которые реализуются на ПС и могут далее проходить через нее транзитом, а также отсутствие возможности ввода и вывода приема отдельных команд программными логическими ключами.

В случае туннелирования при наладке возможны конфликты, связанные с одинаковыми ID приложений, разными VLAN и разными MAC-адресами многоадресной рассылки GOOSE-сообщений на разных ЦПС (рис. 6).

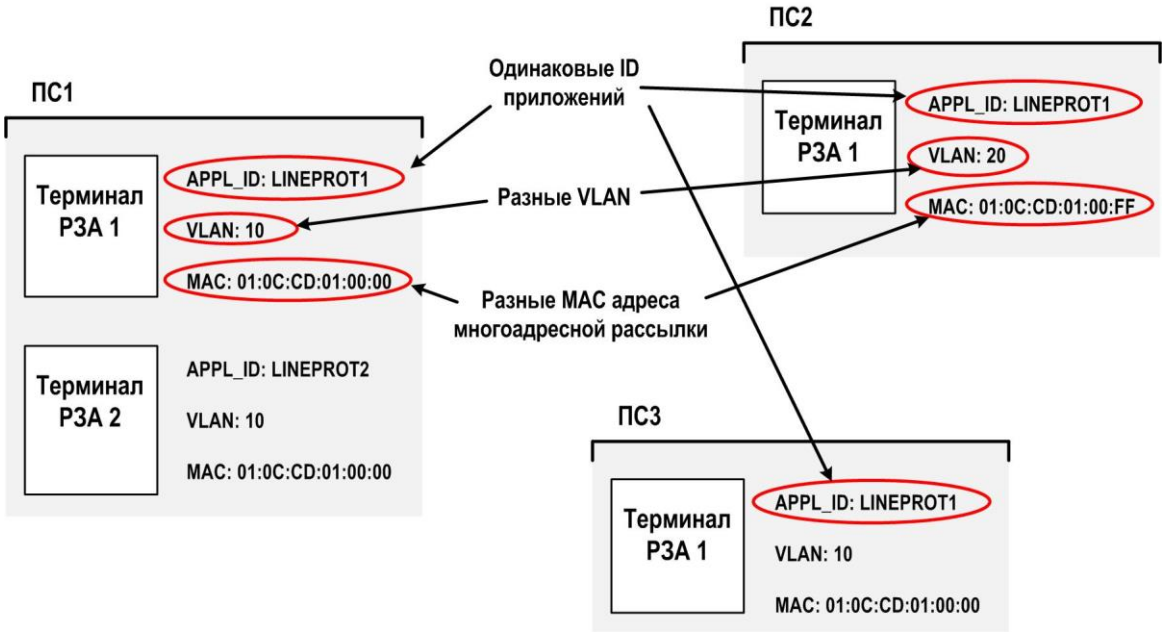


Рис. 6. *Возможные конфликты при передаче GOOSE-сообщений между ЦПС без использования УПАСК.*

При туннелировании эксплуатацию существенно усложняет отсутствие постоянного контроля состояния и пропускной способности каналов по ЦСС между ПС. В принципе невозможно ответить

на вопрос: «А сейчас система способна передать команды РЗ и ПА за требуемое время и с требуемой надежностью?»

Обеспечение информационной безопасности

При туннелировании физическая изоляция между собой ЛВС на разных объектах отсутствует, что приводит к большим проблемам обеспечения информационной безопасности системы РЗА в целом, особенно когда объекты принадлежат разным собственникам. Стандартное использование межсетевых экранов для изоляции ЛВС здесь проблематично.

При использовании УПАСК обеспечивается полная физическая изоляция ЛВС на разных объектах, что упрощает обеспечение информационной безопасности системы РЗА в целом. По сути дела, УПАСК являются идеальными межсетевыми экранами между ЛВС на разных объектах.

Кроме того, как отмечалось выше, при туннелировании невозможно обеспечить постоянный контроль состояния и пропускной способности каналов по ЦСС. Таким образом, преднамеренное или непреднамеренное поражение Ethernet-канала РЗА, например, снижение его пропускной способности или снижение его приоритета, не будет обнаружено. Поэтому при туннелировании более остро стоит вопрос обеспечения информационной безопасности не только ЛВС разных объектов, но и самих каналов по ЦСС между объектами.

Передача команд рз и па между пс i архитектуры и цпс ii и iii архитектур

Туннелирование не позволяет обеспечить передачу команд РЗ и ПА между традиционными ПС и ЦПС.

Передача команд РЗ и ПА между ЦПС и традиционными ПС обеспечивается установкой УПАСК с портами Ethernet для приема и публикации GOOSE-сообщений, выполняющего функцию шлюза, и УПАСК с дискретными входами и выходами, что показано на рис. 7. Очевидно, что данные УПАСК должны быть совместимы на канальном уровне, т. е. использовать в ВЧ-каналах одни и те же кодированные ВЧ-сигналы, а при работе по ЦСС или выделенным ОВ – одни и те же кодированные цифровые сигналы и протоколы взаимодействия.

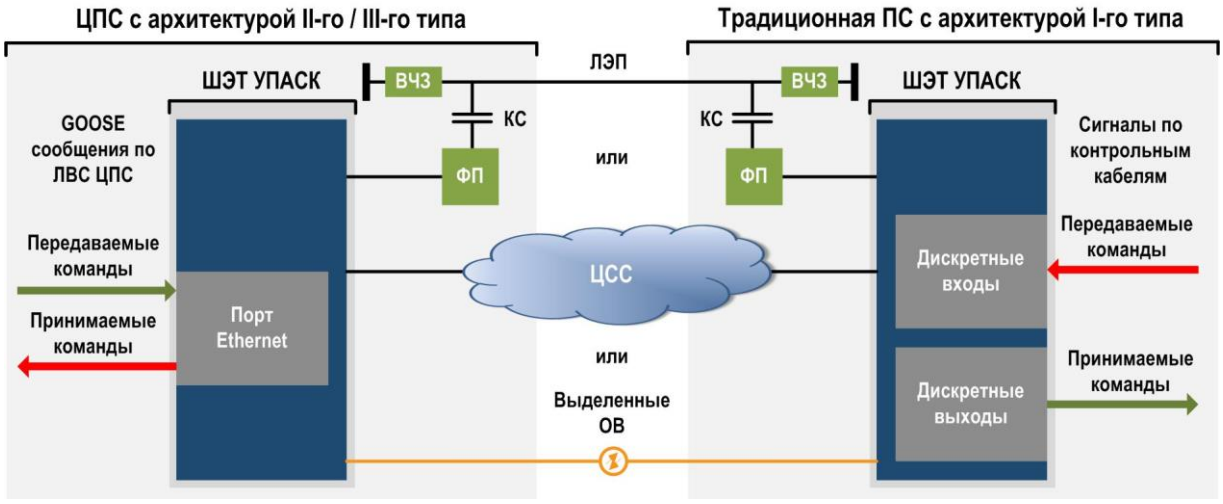


Рис. 7. Передача команд РЗ и ПА между ЦПС и ПС с традиционной архитектурой.

Выбор варианта передачи goose-сообщений между объектами в типовых решениях

Сравнение вариантов передачи команд РЗ и ПА между ПС с помощью GOOSE-сообщений приведены в таблице 2.

Табл. 2. Сравнительные характеристики использования туннелирования и шлюза/УПАСК.

Характеристика	Туннелирование	Шлюз в виде УПАСК
Совместимость устройств на канальном уровне	Обеспечивается	В настоящее время не обеспечивается
Возможность широковещательной передачи команд по ЦСС без переприема их устройствами РЗА на промежуточных ПС	Обеспечивается	Обеспечивается
Использование ВЧ-каналов	Невозможно	Возможно
Требования к пропускной способности каналов по ЦСС	Требуются широкополосные каналы	Могут быть использованы узкополосные каналы
Надежность передачи GOOSE-сообщений по ЦСС	Более низкая	Более высокая
Мониторинг состояния и пропускной способности канала по ЦСС	Невозможен	Возможен
Визуальное отображение передачи и приема команд	Не обеспечивается	Обеспечивается
Оперативный ввод и вывод команд РЗ и ПА программными логическими ключами	Невозможен	Возможен
Наладка и эксплуатация	Крайне сложная	Более простая
Конфликты из-за одинаковых ID приложений, разных VLAN и разных адресов многоадресной рассылки GOOSE-сообщений на разных ЦПС	Возможны	Невозможны
Обеспечение информационной безопасности	Сложное	Более простое
Передача команд РЗ и ПА между ЦПС и ПС с традиционной архитектурой	Невозможна	Возможна

В последние время для передачи команд РЗ и ПА предлагается использование маршрутизируемых GOOSE-сообщений (R-GOOSE) [5]. GOOSE могут передаваться между ПС по Ethernet-каналам (уровень L2). По IP каналам (уровень) L3 GOOSE-сообщения передаваться не могут. Для передачи GOOSE-сообщений на уровне L3 к ним добавляется заголовок UDP/IP

(формируется R-GOOSE), который позволяет широковещательно передавать их по IP-сетям. Очевидно, что R-GOOSE присуще большинство из указанных выше недостатков «обыкновенных» GOOSE-сообщений. При этом возрастают требования к пропускной способности каналов, и еще более усложняется обеспечение информационной безопасности.

В силу указанных выше причин в типовых решениях ПАО «ФСК ЕЭС» принят вариант передачи GOOSE-сообщений между ПС, использующий принцип шлюза. Использование туннелирования для обмена GOOSE-сообщениями между ПС не предусматривается. Рассматриваются только типовые решения с использованием УПАСК, работающих по ВЧ-трактам (УПАСК ВЧ), ЦСС (УПАСК ЦС) и выделенным ОВ (УПАСК ОВ).

Данные типовые решения не ограничивают развитие систем РЗА. Для повышения качества функционирования систем РЗА производители УПАСК могут развивать методы передачи сигналов по ВЧ-трактам, ЦСС и выделенным ОВ.

Кроме того, для передачи команд РЗ и ПА между объектами с использованием GOOSE-сообщений [6]:

- описан типизированный обмен GOOSE-сообщениями (сформирован перечень сигналов и логических узлов с обозначениями по МЭК 61850 взамен обезличенных GGIO как для систем РЗ, так и систем ПА),
- сформирован перечень типовых информационных сигналов УПАСК с обозначениями согласно МЭК 61850, выдаваемый в АСУ ТП и в формате COMTRADE,
- сформирован типовой перечень управляющих сигналов УПАСК от АСУ ТП с обозначениями согласно МЭК 61850.

При развитии систем РЗА в случае необходимости данный перечень команд РЗ и ПА, информационных сигналов, передаваемых в АСУ ТП, и управляющих сигналов от АСУ ТП может быть расширен.

Заключение

Принятая в ПАО «ФСК ЕЭС» типизация передачи GOOSE-сообщений между объектами с использованием УПАСК, выполняющих функцию шлюза, не является тормозом развития систем РЗА. Наоборот, она позволяет упростить внедрение новых технологий, исключая многие потенциальные риски. Кроме того, упрощаются проектирование, эксплуатация и техническое обслуживание систем РЗА, использующих передачу GOOSE-сообщений между объектами электроэнергетики.

СПИСОК ЛИТЕРАТУРЫ

[1] IEC/TR 61850-90-1: 2010. Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations.

[2] Харламов В. А., Романов С. Е. Перспективы использования ВЧ каналов в системах РЗА // Релейщик. 2015. №2. С. 32-36.

[3] Scalable Communication Transport Solutions Over Optical Networks, CIGRE Working Group D2.35, Technical Brochure, May 2015.

[4] Приложение №1 к протоколу Правления ОАО «Россети» от 22.06.2015 № 356пр. Концепция развития релейной защиты и автоматики электросетевого комплекса // Релейщик. 2015. №3. С. 28-43.

[5] A.Apostolov Wide Area GOOSE Applications for Inter-Substation Communications // CIGRE. Study Committee B5. 2019 Colloquium. June 24-28, 2019. Tromso, Norway

[6] Харламов В. А., Хасанов А. Х. Передача команд РЗ и ПА в рамках корпоративного профиля МЭК 61850 // Релейная защита и автоматизация. 2019. №2. С. 36-40.

1.14. ОТ ПРОЕКТА ДО ОБЪЕКТА.

ВЫЗОВЫ ПРИ РЕАЛИЗАЦИИ ЦПС И ПУТИ РЕШЕНИЯ

П.Г. ВАРГАНОВ, Н.В. ПАРШИКОВ, А.Н. ДОНСКОЙ, Д.А.УДИКОВ

АО «ЧЭАЗ»

Российская Федерация

Контактное лицо:

Д.А.УДИКОВ

d.udikov@cheaz.ru

Ключевые слова: БЭМП, Digital Substation, ЦПС, IEC 61850, SCL, SSD, SCD, ICD, CID, валидация, система сквозного проектирования, CHEAZ Substation Configuration Tool, CHEAZ IED Configuration Tool.

Введение

Продолжается активное внедрение цифровых подстанций в отечественной энергетике. В последнее время можно заметить тенденцию перехода на более продвинутые архитектуры. В новых проектах уверенно используются цифровые защиты, работающие на отключение, при этом резервирование классическими устройствами не предусматривается. Специалистам приходится решать проблемы и задачи, с которыми ранее сталкиваться не приходилось. Становится актуальным обмен опытом и выработка общих подходов к решению проблем.

В докладе на РЕЛАВЭКСПО-2021 мы рассказывали об опыте АО «ЧЭАЗ» по реализации проектов цифровых подстанций. Поэтапно рассматривали процесс проектирования с возникающими «подводными камнями».

В данном докладе мы расскажем о разрабатываемой АО «ЧЭАЗ» системе сквозного проектирования, которая должна решить большинство проблем, существующих на разных этапах реализации ЦПС, представим наше видение идеального процесса проектирования и его соответствие международным и корпоративным стандартам, профилям и техническим отчетам.

О разработке

Переход от классических схем РЗА на цифровые модели стандарта IEC 61850 существенно изменяет и саму логику РЗА. Кроме того, информационное представление устройств МПРЗА во внешнем мире (АСУ ТП) изменяется от плоского адресного пространства простых протоколов связи (Modbus, семейство МЭК 60870-5) до иерархической объектной модели данных и сложных механизмов информационных потоков и подписок согласно множеству документов стандарта:

- описание модели данных (IEC 61850-6, IEC 61850-7-3, IEC 61850-7-4);
- описание протоколов обмена (IEC 61850-8-1, IEC 61850-9-2);
- описание процесса системного проектирования (IEC 61850-4);
- описание методики моделирования программируемой логики применительно к ЦПС (IEC TR 61850-90-11).

Из-за избыточной гибкости и недостаточной конкретности стандарта ведущие энергетические и промышленные компании в настоящее время разрабатывают корпоративные профили, собственные стандарты, методические указания и нормы проектирования. Также крупные заказчики МПРЗА вполне логично выставляют определённые требования к представлению и функционированию внутренней логики устройств, чтобы процесс проектирования не зависел от конкретного производителя.

В результате производителям МПРЗА приходится разрабатывать всевозможные программные переходники и адаптеры, которые отрицательно сказываются не только на производительности, но и на гибкости расширения функционала, и на стабильности работы устройств.

В данной ситуации оптимальным для нас решением представляется полная переработка существующих технических решений с учетом новых стандартов и требований. В ходе открытого НИОКР на АО «ЧЭАЗ» проводится реорганизация схем внутренней логики в соответствии с требованиями корпоративного профиля и объединение инструментов в одну инфраструктуру под рабочим названием «Система сквозного проектирования».

Основные функции разрабатываемой системы:

– создание функциональных схем внутренней логики МПРЗА в соответствии с корпоративными типовыми техническими решениями по ПА, РЗ, АСУ ТП и СОПТ ПАО «ФСК ЕЭС» с возможностью проверки функционирования в режиме симулятора;

– создание СПЛ для МПРЗА с привязкой к SCL-файлу в соответствии с техническим отчетом IEC TR 61850-90-11 и корпоративными типовыми техническими решениями по ПА, РЗ, АСУ ТП и СОПТ ПАО «ФСК ЕЭС»;

– создание описания возможностей интеллектуального электронного устройства (IED Configuration Tool);

– создание системной спецификации (System Specification tool);

– создание системной конфигурации (System Configuration tool);

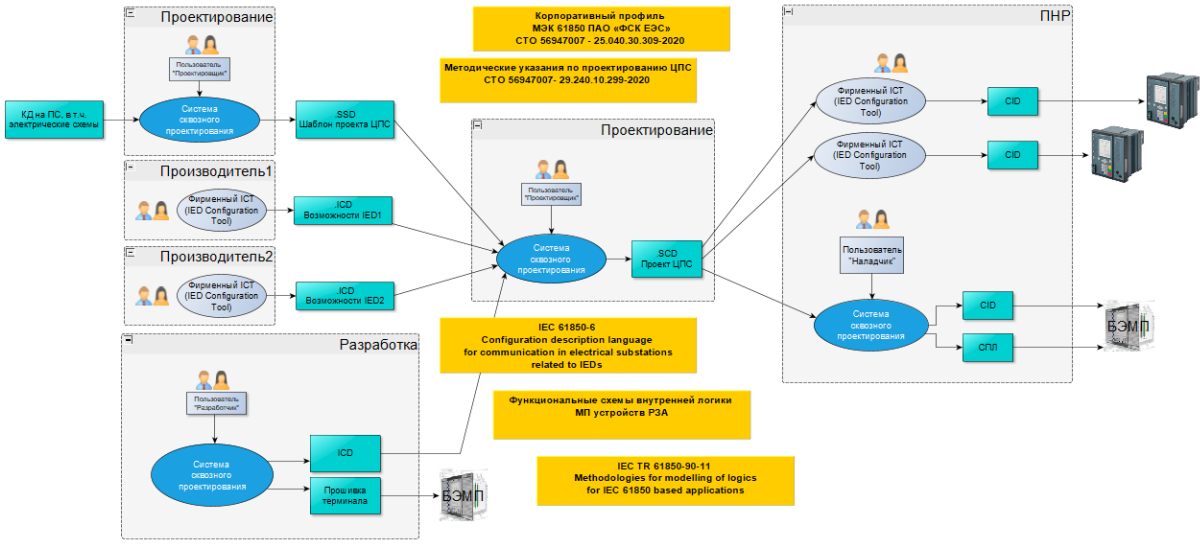
– создание документации (Documentation tool);

– валидация выходных и входных данных;

– создание, редактирование и хранение повторно используемых компонент и схем;

– доступ к функциональным возможностям системы в зависимости от роли пользователя на каждом этапе реализации ЦПС за счет применения иерархического ролевого управления доступом.

В результате данной разработки мы как производители МПРЗА планируем получить лёгкость разработки линейки современных расширяемых надежных устройств с минимальной зависимостью от аппаратной платформы, проектировщики — систему проектирования, которая не зависит от конкретного производителя, а наладчики — инструмент, который позволит сконфигурировать интеллектуальное электронное устройство параметрами из проектного решения – SCD-файла.



Система сквозного проектирования.

Функциональные схемы

Алгоритмы релейной защиты в разрабатываемой системе будут представлены в виде функциональных блоков, которые в проекции на модель стандарта IEC 61850 представляют собой логические устройства (LDevice). Каждый функциональный блок состоит из логических блоков (логических функций – LogicalNode) и связей между ними (ExtRef, InRef). Таким образом, создавая функциональную схему, мы одновременно создаем полноценную модель устройства в

соответствии с IEC 61850. Подобный подход формализован, например, в работе под названием «Разработка функциональных схем внутренней логики МП устройств РЗА и МП» в рамках работ, проводимых ПАО «Россети».

При этом доступ к алгоритмам РЗА, существенно связанным с аппаратной частью устройств МПРЗА, система сквозного проектирования открывает только пользователям с ролью «Разработчик».

Свободно программируемая логика (спл)

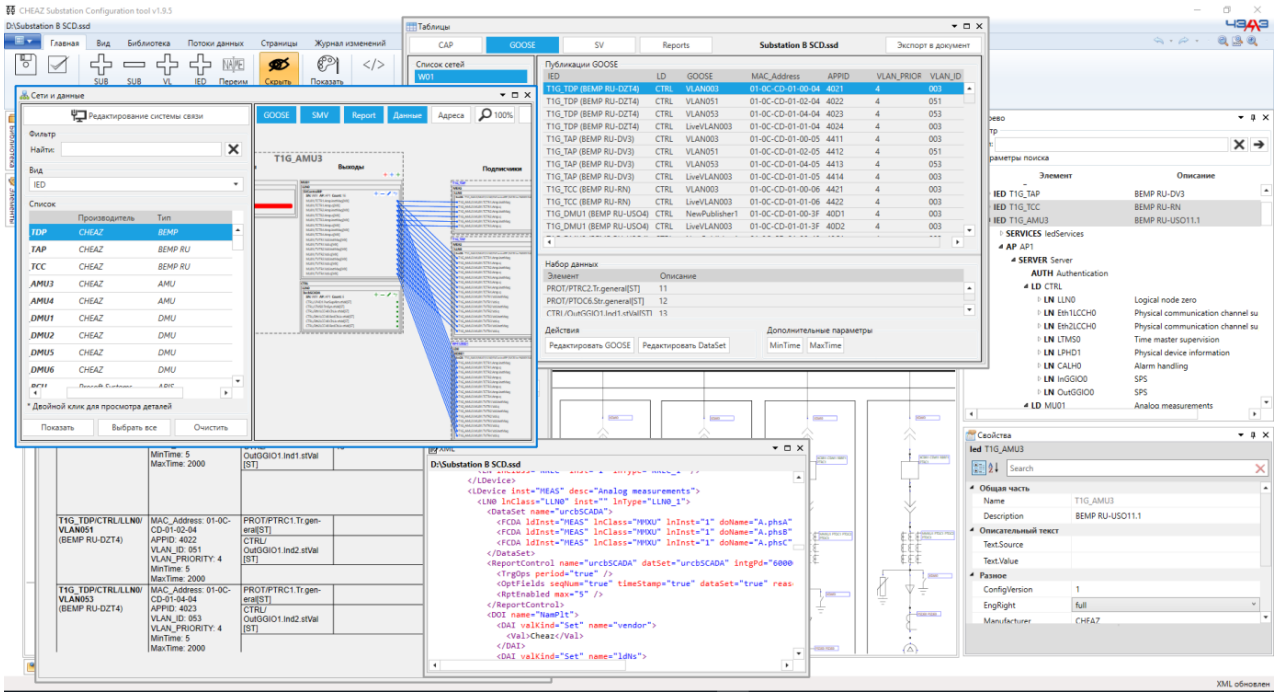
Так как изменение алгоритмов базового функционала сторонними пользователями не допускается, а на практике возникают случаи, когда необходимо реализовать различные комбинации входных/выходных данных, не предусмотренные производителем, используется инструмент создания СПЛ. Данной теме посвящён технический отчет IEC TR 61850-90-11, а дополняет его работа под названием «Разработка описания схем свободно программируемой логики внутри SCL-файла» в рамках работ, проводимых ПАО «Россети».

Данный функционал будет включен в состав модулей SCT и ICT и доступен пользователям с ролями «Проектировщик» и «Наладчик».

Проектирование

За этапы создания системной спецификации (SSD), системной конфигурации (SCD) и документации отвечает модуль под рабочим названием SCT. Он будет создан на основе существующего программного обеспечения «CHEAZ Substation Configuration Tool», а результат его работы будет максимально полно отвечать документам:

– СТО 56947007-25.040.30.309-2020 «Корпоративный профиль МЭК 61850 ПАО «ФСК ЕЭС»;
– СТО 56947007-29.240.10.299-2020 «Методические указания по проектированию ЦПС».



Модуль SCT.

Работа с модулем SCT будет доступна пользователям с ролью «Проектировщик».

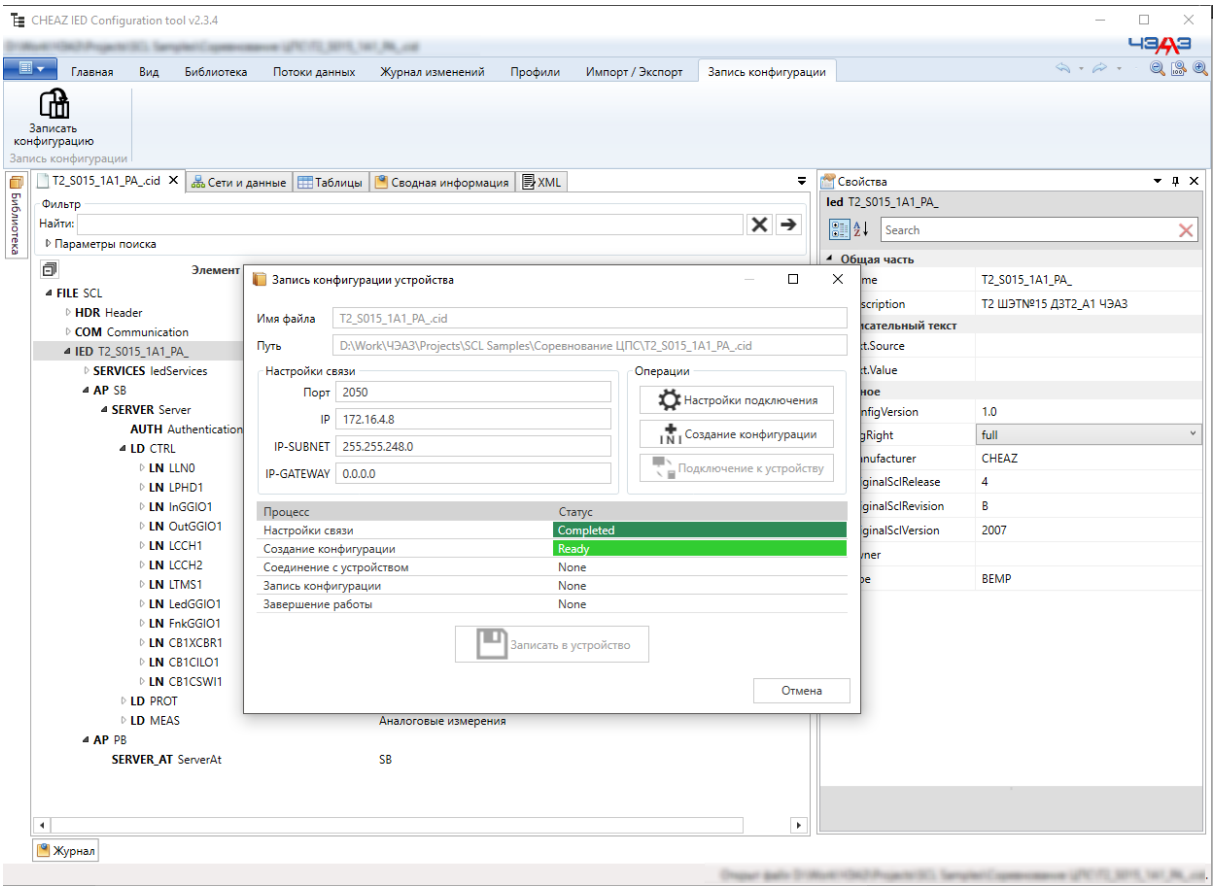
Пусконаладочные работы

Одним из самых сложных и запутанным на данный момент является процесс конфигурирования устройств на этапе пусконаладочных работ (ПНР). Каждый производитель МПРЗА предоставляет свой инструмент для конфигурирования, как того требует стандарт. Однако до сих пор бытуют «экономные» решения, которые вынуждают пусконаладочные бригады повторять часть процесса проектирования информационного обмена для отдельных устройств.

Чтобы минимизировать трудозатраты и исключить ошибки, связанные с человеческим фактором на этапе ПНР, необходимо по возможности все необходимые параметры устройств (информационные потоки данных, уставки, параметры служб, СПЛ и т. п.) задать на этапе проектирования.

Ключевым моментом нашей разработки, о котором мы еще не упоминали, является задание уставок посредством CID-файла в соответствии с разрабатываемым АО «НТЦ ФСК ЕЭС» документом под названием «Правила записи уставок функций РЗА Типовых шкафов ПАО «ФСК ЕЭС».

Перед нами стоит задача максимально упростить процесс конфигурирования на этапе ПНР, а для этого все изменения отдельных параметров устройств необходимо проводить через систему проектирования системной конфигурации с обязательным ведением журнала регистрации изменений.



Модуль ICT.

Работа с модулем ICT будет доступна пользователям с ролью «Наладчик».

Заключение

Модульность построения системы сквозного проектирования позволит запускать отдельные инструменты в зависимости от этапа реализации ЦПС и уровня доступа пользователя.

По мере развития данного проекта будут добавляться модули для настройки функций информационной безопасности, модули для диагностики и управления терминалов серии БЭМП для эксплуатирующих организаций и т. п.

По возможности инструменты будут использовать общие программные решения, что избавит от необходимости контролировать версии отдельных инструментов и обеспечит совместимость входных и выходных данных отдельных модулей.

ЛИТЕРАТУРА

[1] СТО 56947007-25.040.30.309-2020 «Корпоративный профиль МЭК 61850 ПАО «ФСК ЕЭС».
[2] СТО 56947007-29.240.10.299-2020 «Методические указания по проектированию ЦПС».

1.15. АВТОМАТИЧЕСКИЙ СИНТЕЗ ОПТИМАЛЬНЫХ ПРОЕКТНЫХ РЕШЕНИЙ ПО ПОСТРОЕНИЮ РЗА ЦПС

А.А. ВОЛОШИН, Е.А. ВОЛОШИН, Н.П. ГРАЧЕВА

Центр НТИ МЭИ

Российская Федерация

Контактное лицо:

Н.П. ГРАЧЕВА

grach.np@gmail.com

Ключевые слова: Релейная защита, цифровая подстанция, МЭК 61850, онтология, база знаний, методы искусственного интеллекта.

Введение

В настоящее время разработка проекта цифровой подстанции является достаточно сложным и трудоемким процессом: необходимо не только осуществить все классические шаги, включающие определение состава функций и терминалов РЗА, состава сигналов для каждой функции и т. д., но также выбрать архитектуру цифровой подстанции, разработать локальную вычислительную сеть, определить состав устройств сопряжения с объектом и создать перечень файлов, описанных в стандарте МЭК 61850.

Существующие сегодня информационные технологии позволяют автоматизировать многие процессы, уменьшив количество ручного труда, а, следовательно, время выполнения задач, а также вероятность ошибок, вызванных человеческим фактором. Применение методов искусственного интеллекта для автоматизации процесса проектирования дает возможность автоматического синтеза проектной документации комплекса РЗА ЦПС с учетом различных архитектур и типов оборудования.

Однако труд проектанта является достаточно творческим и аналитическим процессом, следовательно, необходимо использование методов, реализующих данные процессы. Разработка и реализация данной методики и являются целью данного доклада.

Основная часть

Проектирование комплекса РЗА энергообъекта производится на основании нормативной документации и собственных знаний и опыта проектанта, что зачастую является достаточно сложным и трудоемким процессом. Процесс проектирования комплекса РЗА ЦПС можно условно разделить на несколько этапов, в которые входят:

- выбор функций релейной защиты в соответствии с действующей нормативно-технической документацией (НТД);
- определение ТТ, ТН и выключателей, сигналы которых необходимы для работы функции;
- выбор терминалов РЗА;
- определение состава устройств сопряжения с объектом и подключенного к ним оборудования;
- создание ЛВС.

Конечно, перечисленные выше шаги – не полный перечень этапов, выполняемых в процессе проектирования, однако целью данного исследования была автоматизация этих шагов.

Для создания проекта комплекса РЗА ЦПС прежде всего необходимо задать информацию об энергообъекте. Данная информация включает в себя схему первичного оборудования, а также информацию, необходимую для определения состава комплекса РЗА: мощность оборудования, наличие питания с другого конца линии, уровень ТКЗ и т. д. Ввод информации предполагается либо с помощью сбора схемы в разработанном интерфейсе, либо импорта файла *.ssd (при наличии) и ввода дополнительной информации, которая не содержится в файле в соответствии со стандартом МЭК 61850. В первом случае на основании собранной схемы файл ssd будет сгенерирован автоматически.

Итак, после ввода исходных данных можно переходить непосредственно к процессу определения состава функций комплекса РЗА, который, как было сказано выше, производится на

основании нормативной документации и собственных знаний, и опыта проектанта. Современные программные средства позволяют описать эти знания в формальном виде и применить их при разработке программ для достижения желаемого результата. Для создания инструмента, способного одновременно содержать требования, предъявляемые НТД, и отражать творческий процесс анализа схемы, была выбрана технология баз знаний, которая позволяет формализовать существующую нормативно-техническую базу проектной документации и накопленный опыт для автоматизации процесса проектирования комплекса РЗА цифровой подстанции.

База знаний (англ. knowledge base) – формализация предметной области и ее представление в форме семантической сети, допускающая осуществление логических выводов и осмысленную обработку информации. В соответствии с [1], она является информационной моделью области знаний, имеющей вид ориентированного графа, вершины которого соответствуют объектам предметной области, а дуги (рёбра) задают отношения между ними. Структура такого графа соответствует триплету, который является формой представления данных в онтологиях. Онтологии являются каркасом базы знаний (БЗ) и создают базис для описания основных понятий предметной области, необходимых для полноценного функционирования системы [2]. Согласно [3], онтологии в области информационных технологий представляют собой формализацию некоторой области знаний с помощью концептуальной схемы.

Таким образом, база знаний позволяет не только хранить и систематизировать накопленный опыт и знания, но и применять его в автоматизированном виде. Однако для создания БЗ необходимо не только понимать синтаксические особенности её структуры, но и понимать применимость хранимой в ней информации.

Прежде всего была разработана онтологическая модель подстанции, содержащая информацию о типах оборудования, их взаимосвязях, а также перечень правил, содержащихся в НТД. Стоит отметить, что онтология позволяет описывать требования НТД для разных производителей/структур, что позволяет обеспечить применение данной технологии в различных областях энергетики.

После чего разработанную модель необходимо заполнить информацией, полученной на этапе ввода данных. Информация о схеме записывается в базу знаний из SSD-файла (сгенерированного или импортированного) и дополнительных данных, введенных пользователем. После записи данных мы получаем базу знаний конкретного энергообъекта. Однако этих данных недостаточно для обработки схемы подстанции и синтеза перечня функций РЗА. Данную схему необходимо обработать и достроить недостающие связи, определить недостающие элементы оборудования, защиту которого необходимо обеспечить, например, такие, как ошиновка трансформатора, для этого применяется механизм логического вывода (МЛВ, ризонер). Первичная обработка базы знаний энергообъекта позволяет достроить такие связи, как, например, наличие электрической связи между индивидами оборудования на схеме подстанции (рис. 1).

$$\forall x, y \in E(x\ hasElectricalConnection\ y \leftrightarrow x\ hacCN\ c \in C\ \wedge\ y\ hasCN\ c \ni C\ \wedge\ x \neq y) \quad (1)$$

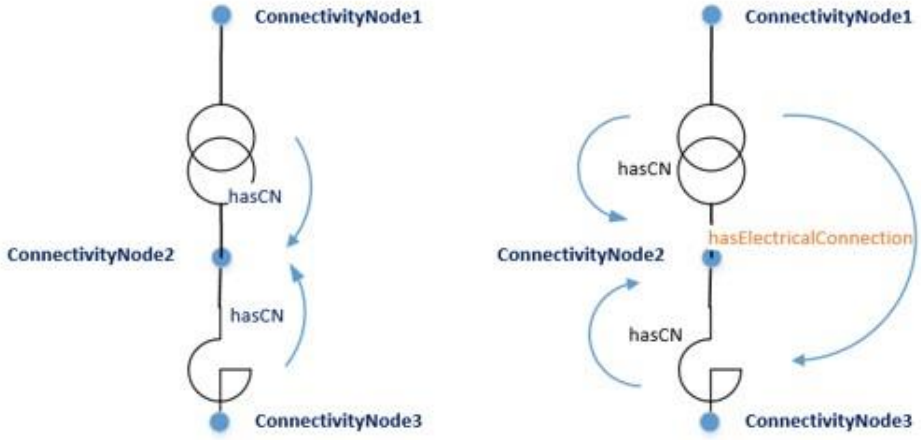


Рис. 1. Пример работы МЛВ для достраивания неявных свойств.

После того как недостающие связи достроены, при помощи ризонера происходит анализ схемы, на основании чего делается вывод о том, какие функции РЗА необходимо установить на подстанцию. Синтез функций релейной защиты осуществляется на основании НТД, описанной в терминах БЗ. Так как определение состава функций РЗА является задачей комплексного анализа схемы, а не отдельных её элементов (например, необходимо учитывать уровни напряжения или количество выключателей, которыми элемент подключается к остальной части схемы), то для распределения функций защит по оборудованию требуется составление более сложных условий в совокупности с глубокими запросами к онтологии. Для решения этой проблемы был выбран итерационный подход к построению правил, с поочередным запуском их в онтологии, что позволяет учесть и проверить все возможные варианты. Условия, необходимые для распределения комплектов защит по оборудованию, формировались на основе нормативной документации [4, 5] путем структурирования и классификации заложенных в ней знаний.

На основе составленной классификации был сформирован список рекомендаций по установке защит для каждого типа оборудования ЦПС с учетом его особенностей. Проведенный анализ позволил определить так называемые опорные точки выбора функций защит в соответствии с нормативно-технической документацией и описать этот процесс в базе знаний с использованием МЛВ.

Таким образом, процесс формирования базы знаний требований по защите первичного оборудования ЦПС был разбит на подэтапы, в ходе которых были определены оптимальные инструменты и решения для работы с онтологиями.

Разработанная база знаний требований по релейной защите позволяет в автоматизированном режиме определить первичную схему подстанции и синтезировать перечень функций релейной защиты для рассматриваемого энергообъекта.

Для осуществления привязки функций релейной защиты и автоматики к конкретным измерительным трансформаторам тока и напряжения необходимо произвести большее количество итераций. Это обусловлено тем, что данная задача требует охвата опыта проектантов,

информации о связях на подстанции и творческого подхода человека. Таким образом был разработан алгоритм, позволяющий реализовать это в следующих ступенях:

1. Поиск и привязка для каждого объекта оборудования соответствующих ему измерительных трансформаторов и выключателей.

2. Оценка состава защит объектов оборудования и «перекрещивание» защищаемых зон с помощью защит с абсолютной селективностью.

3. Расстановка основных защит индивидов оборудования по ТТ с учетом зон, определенных в пункте 3.

4. Расстановка резервных защит в соответствии со схемой подстанции и информацией о связи объектов ТТ и оборудования.

5. Поиск ближайших ТН для индивидов оборудования без собственных ТН с последующей привязкой к ним соответствующих защит, контролирующих значение напряжения.

6. Поиск ТН для индивидов оборудования с собственными ТН с целью обеспечения резервирования сигналов.

Вышеупомянутый алгоритм имеет в своей основе следующие методики работы с базой знаний:

• формирование необходимых связей путем рекурсивных запросов к онтологии;

• получение новых знаний посредством логических выводов, построенных на совокупности правил.

После выполнения данных шагов на основе анализа задействованных в работе комплекса РЗА ТТ, ТН и выключателей формируется перечень MU на основе требований к устройству сопряжения с объектом, формируемых пользователем или определенных по умолчанию.

Данный подход предусматривает использование механизмов баз знаний и логического вывода для определения требуемого набора функций РЗА для обеспечения надежной и полноценной защиты первичного оборудования подстанций в соответствии с нормами технологического проектирования. Для задачи распределения определенного набора функций по микропроцессорным устройствам данный стек технологий также подходит ввиду следующих факторов:

• отсутствие необходимости перерабатывать данные, полученные на предыдущем этапе работы программного комплекса – функции сразу готовы к распределению по терминалам;

• высокая наглядность распределения, обусловленная семантической моделью построения баз знаний;

• наглядная и легко изменяемая форма введения начальных условий распределения в алгоритм.

По совокупности факторов применение механизмов баз знаний и логического вывода является наиболее перспективным путем решения задачи распределения функций релейной защиты и автоматики по микропроцессорным устройствам.

Для решения данного вопроса была разработана отдельная база знаний – база знаний комплекса РЗА подстанции. Под входными данными задачи в данном случае подразумевается предопределенный набор функций РЗА, реализуемых на подстанции в соответствии с нормами технологического проектирования и руководящими указаниями отраслевых предприятий, с привязкой к первичному оборудованию подстанции, к вторичным измерительным трансформаторам, которые данная защита использует, а также к силовым выключателям, на которые действует данная защита.

Ввиду наличия ситуаций, когда одна и та же защита одновременно является основной для одной единицы оборудования подстанции и резервной – для другой единицы, введена дифференциация типов защит:

- основная;
- резервная;
- технологическая.

Ядром данного программного модуля является построенная базовая модель онтологии базы знаний, включающая в себя классы и свойства, которые содержат данные об элементах подстанции, функциях РЗА и терминалах, и обеспечивающие взаимосвязь между ними, а также базовый набор правил распределения функций по терминалам в соответствии с требованиями НТД. Данная модель является унифицированной и содержит основную логику работы алгоритма; на ее основе в дальнейшем формируется уникальная модель для каждого проекта подстанции.

Далее в соответствии с внесенными пользователем данными об универсальном терминале (в случае их отсутствия данные формируются по умолчанию) происходит автоматическое распределение функций РЗА по терминалам в соответствии с требованиями, определяемыми НТД.

Цифровая подстанция подразумевает использование локальной вычислительной сети (ЛВС) для передачи данных внутри подстанции. При этом разработанная ЛВС должна соответствовать требованиям, предъявляемым к экономичности и надежности, то есть гарантировать своевременную доставку пакетов и необходимый уровень резервирования.

Поэтому следующим этапом разработки ПТК стало определение её структуры, что в свою очередь подразумевает:

– выбор коммутаторов ЛВС;

– определение схемы подключения оборудования (то есть терминалов РЗА и MU) к коммутаторам;

– определение виртуальных связей (прокладка VLAN) внутри сети.

При анализе алгоритмов оптимизации было принято решение об использовании генетического алгоритма (ГА), применение которого для оптимизации топологии сети было рассмотрено в [6]. Генетический алгоритм – эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе [7]. В данной работе применение ГА обуславливается гибкостью задания условий и

требований, предъявляемых к сети, которую данный алгоритм реализует с помощью использования штрафных функций.

Для решения второй подзадачи было принято использовать алгоритм A* (A-стар, A-star etc.). Данный алгоритм относится к классу алгоритмов поиска пути ГА графе и будет подробнее рассмотрен ниже. В ходе работы было выявлено, что оценка данного этапа требует наибольшего количества времени и мощности вычислительных ресурсов, в связи с этим было принято решение о необходимости оценки загрузки каналов и трассировки информационных потоков только в случае, если сеть валидна к оценке с точки зрения аппаратных показателей. Ниже приведен перечень целевых функций, разработанных для оценки качества локальной вычислительной сети.

$$Cst2 = \sum_{I=1}^{NI} ChOC_I + \sum_{S=1}^{NS}(ChNC_S + ChNGC_S + ChSC_S) + \sum_{PL=1}^{NPL} M_{PL} + c \cdot FRr + Astar \quad (2)$$

– $ChOC_I$ – функция проверки наличия как минимум одной связи у каждого IED-устройства. Данная функция проверяет включение цифрового устройства в ЛВС;

– $ChNC_S$ – функция проверки количества подключений IED-устройств к каждому из коммутаторов, в которой проверяется, чтобы количество занятых портов коммутаторов не превышало количество портов имеющихся;

– $ChNGC_S$ – функция проверки количества занятых портов коммутаторов, используемых для соединения коммутаторов друг с другом, которая осуществляет как проверку на превышение по аналогии с предыдущей функцией, так и проверку на отсутствие, что означает исключение коммутатора из сети;

– $ChSC_S$ – функция проверки на наличие хотя бы одного подключения к IED- (MU)-устройству у каждого из коммутаторов. Данная функция необходима для равномерного распределения устройств по коммутаторам и исключения использования лишних коммутаторов в схеме локальной вычислительной сети, что связано как с экономическими показателями, так и с оценкой коэффициента надежности схемы.

– M_{PL} – поиск колец среди коммутаторов в топологии, отсутствие которых необходимо для корректной работы протокола RSTP в режиме до отключения. Данная функция необходима для учета колец на этапе трассировки потоков в силу того, что потоки не должны быть проложены по разным ветвям кольца, чтобы исключить перегрузку каналов связи на этапе проектирования;

– FRr – подсчет количества физических связей, которое нужно для минимизации связей в том числе в экономических целях;

– Astar является результатом работы модуля трассировки SV-потоков.

Для того чтобы оценить работоспособность синтезированного комплекса РЗА, необходимо провести оценку его показателей надежности (ПН).

В настоящее время методические указания по расчету ПН РЗА цифровой подстанции отсутствуют.

Однако традиционно существуют два метода для расчета показателей надежности РЗА:

– цепи (матрицы) Маркова;

– блок-схемы надежности.

Однако данные методы имеют следующие недостатки, затрудняющие выполнение расчетов с использованием существующих методик:

1) Высокая трудоемкость аналитического расчета показателей надежности и, как следствие, высокая вероятность ошибки в силу проявления «человеческого фактора».

2) Применение различных архитектур для реализации РЗА цифровых подстанций требует разработки новых диаграмм надежности для каждой архитектуры.

3) Изменение ДН в ходе эксплуатации ПС в связи с изменением активной топологии локальной вычислительной сети (ЛВС) для «шины процесса». Подобное изменение может быть вызвано, например, работой протокола RSTP (Rapid Spanning Tree Protocol), когда вследствие отказа какого-либо элемента сети происходит перестроение существующей активной топологии ЛВС. Данная технология при построении ДН требует предусматривать все возможные варианты изменения структуры, что усложняет проведение расчета.

4) Недостаточность методики диаграмм надежности для расчета показателей надежности комплексов РЗА с гибкой функциональной архитектурой.

Кроме того, перечень традиционно используемых показателей надежности не отражает надежность комплекса РЗА в целом, т. к. они предназначены для оценки показателей надежности отдельных функций. Для функционально интегрированных систем РЗА необходимы дополнительные критерии.

Для решения указанных проблем была разработана новая методика для автоматизированного расчета показателей надежности РЗА на основе применения мультиагентной системы для моделирования функционального состояния комплекса РЗА ЦПС.

Программная реализация данной методики выполнена на языке программирования Java с применением мультиагентной системы (МАС) на основе программных библиотек JADEX с применением интеллектуальных агентов по модели belief-desire-intension software model (BDI). Выбор МАС для расчета был обусловлен тем, что данная методология позволяет моделировать поведение каждого объекта-агента оборудования в соответствии с его типом.

В соответствии с [8], мультиагентная система – это система, состоящая из двух и более агентов или интеллектуальных агентов. Важно отметить, что такая система не имеет общей цели (целевой функции), а агенты имеют только свои локальные цели (целевые функции). Реализация общей требуемой функциональности МАС выполняется путём включения в неё интеллектуальных агентов с целями, соответствующими отдельным составляющим общей функциональности.

Мультиагентная система состоит из агентов-оборудования и агентов-функций. Каждый агент использует сервисы для взаимодействия с другими агентами. Взаимосвязь агентов определяется в соответствии с проектной документацией и структурой комплекса РЗА. Так, например, при моделировании сценария отказа УСО, агент функции РЗА получает информацию о недоступности необходимых измерений от агентов оборудования, связывающих его с агентом УСО. Таким образом формируется перечень отказавших функций при отказе отдельных устройств комплекса РЗА ЦПС для различных сценариев. Под сценарием в данной методике понимается независимый отказ одной или нескольких (k) единиц оборудования в зависимости от типа сценария.

После того как все сценарии смоделированы, производится оценка интегральных критериев, разработанных для оценки показателей надежности цифровых подстанций, на основе которых можно сделать вывод о надежности комплекса РЗА цифровой подстанции и произвести изменения комплекса при необходимости, повысив его надежность.

Заключение

Таким образом, была разработана методика автоматического синтеза проектных решений комплекса РЗА с применением методов искусственного интеллекта на основании импортированных данных о схеме РЗА.

Применение онтологического моделирования позволяет реализовать творческую и аналитическую часть процесса проектирования, что в свою очередь дает возможность автоматизировать процесс проектирования таким образом, что изменение НТД не требует переписывания большей части кода программы, достаточно изменить только правила, описывающие НТД.

СПИСОК ЛИТЕРАТУРЫ

[1] N. D. Roussopoulos, A semantic network model of data bases, 1977.
[2] Ю. А. Загорулько и Г. Б. Загорулько, Онтологии и их практическое применение в системах, основанных на знаниях., Новосибирск: Институт математики им. С. Л. Соболева СО РАН, 2011.
[3] В. А. Лапшин, Онтологии в компьютерных системах., Москва: "Научный мир", 2010.
[4] СТО 56947007-29.240.10.248-2017 Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ.
[5] ГОСТ Р МЭК 61850, 2009.
[6] И. Б. Плесовских, «Оптимизация одноранговой вычислительной сети при помощи генетического алгоритма.,» Вестник Омского университета, № 2, pp. 185-188, 2012.
[7] M. E. Bratman, «Intentions, Plans and Technical Reason» Philosopical Review, т. 100, № 2, 1987.
[8] S. D. McArhur, V. M. Catterson, N. D. Hatziargyriou и T. Funabashi, «Multi-Agent Systems for Power Engeneering Applications - Part 1: Concepts, Approaches and Technical Challenges» IEEE Transactions On Power Systems, т. 22, № 4, 2007.

1.16. ИНФОРМАЦИОННО-ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО СОПРОВОЖДЕНИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ ИТС (РЗА И АСУТП)

С. П. ВОРОБЬЕВ

АО «СиСофт Девелопмент»

Российская Федерация

Контактное лицо:

С. П. ВОРОБЬЕВ

vorobev@csoft.ru

Ключевые слова: Цифровая подстанция, электронный каталог, корпоративные технические решения, САПР.

Введение

Предметом исследования является процесс оптимизации и автоматизации производственных процессов проектирования, наладки и эксплуатации устройств ИТС объектов электросетевого хозяйства ПАО «ФСК ЕЭС» с использованием технологии «Цифровая подстанция».

Обзор текущего уровня исследования

С учётом разнообразия вариантов технических решений, принимаемых при проектировании ИТС ПС, включая архитектуру построения сети, используемое оборудование и пр., была проведена работа по составлению каталога типовых технических решений и перенесению его в электронный вид, пригодный для автоматизированной обработки машинным кодом. В рамках научно-исследовательской и опытно-конструкторской работы по теме «Разработка корпоративных типовых технических решений по РЗА и АСУ ТП для ПАО «ФСК ЕЭС» было выпущено и внедрено программное средство, предназначенное к применению при разработке:

– однолинейной схемы ПС в соответствии с СТО ПАО «ФСК ЕЭС» (СТО 56947007-29.240.021-2009);
– схемы ИТС;
– отображения и экспорта проектной информации;
– ведения баз данных проектов.

Применение программного средства преследует следующие цели:

– повышение надёжности работы ИТС (ПА, РЗиСА, АСУ ТП) за счет применения типовых решений и автоматизации процесса проектирования;
– снижение затрат на проектирование, строительство и эксплуатацию ПС;
– уменьшение времени проектирования, в том числе стадии разработки основных технических решений, стадии разработки проектной документации.

Цель и новизна доклада (исследования).

В рамках выполнения научно-исследовательской и опытно-конструкторской работы «Разработка электронного каталога типовых проектных решений для проектирования и конфигурирования оборудования системы защиты, управления ПС, включая решения по Цифровым ПС с применением наилучших доступных технологий» были определены требования и порядок расширения функционала программно-технического комплекса «Электронный каталог типовой проектной документации на РЗА и АСУТП (ЭК РЗА и АСУ ТП)».

Модернизированная система ПТК «ЭК РЗА и АСУ ТП» предназначена для комплексного информационно-инструментального сопровождения процессов разработки проектной документации в части ПА, СОПТ, РЗиСА и АСУ ТП.

Основная часть

При создании системы руководствовались в первую очередь целями снижения затрат на всём жизненном цикле систем РЗА и АСУ ТП средствами повышения уровня типизации технических решений и создания доступного электронного каталога профильной типовой документации ПАО «ФСК ЕЭС».

Также одной из целей было повышение эффективности исполнения процессов проектирования и сопровождения объектов электросетевого хозяйства ПАО «ФСК ЕЭС» путем сокращения непроизводительных и дублирующих операций, операций, выполняемых «вручную», оптимизации информационного взаимодействия участников процессов. Повышение качества проектных решений достигается в том числе и за счет оперативности представления, полноты, достоверности и удобства форматов отображения информации.

В процессе модернизации существующей системы учитывались требования к обязательному соблюдению этапности и объёму выполнения перечня работ, включающих в себя:

— актуализацию и дополнение электронной базы корпоративных решений 6-35 кВ, 110-220 кВ, 330-750 кВ;

— разработку программного модуля для проектирования СОПТ в составе программно-технического комплекса «ЭК РЗА и АСУ ТП»;

— разработку программного модуля для проектирования ПА в составе программно-технического комплекса «ЭК РЗА и АСУ ТП»;

— разработку программного модуля для проектирования АСУ ТП в составе программно-технического комплекса «ЭК РЗА и АСУ ТП».

С целью проверки работоспособности системы, определения соответствия системы требованиям ТЗ, а также решения вопроса о возможности перевода системы в опытную эксплуатацию (далее – ОЭ) обязательно проведение предварительных (перед началом ОЭ) приемочных испытаний подсистем программного комплекса.

На первом, уже реализованном этапе (НИОКР-1), областью применения системы являются процессы проектирования, наладки и эксплуатации комплексов РЗиСА и АСУ ТП в части создания ПД, выгрузки отчетов (работа с базой сигналов, с объёмами шкафов, ТТ к шкафам и пр.), ведение базы данных типовых решений. Реализована возможность формирования однолинейной схемы ПС (SLD) в соответствии с СТО 56947007-29.240.10.249-2017 ПАО «ФСК ЕЭС и схемы ИТС в соответствии с СТО 56947007-29.240.021-2009 ПАО «ФСК ЕЭС» с использованием типовых технических решений, хранящихся в базах данных ПТК «ЭК РЗА и АСУ ТП», посредством графического редактора для создания схемы ИТС, файла SSD. Также реализована возможность экспорта файла SSD в номенклатуре МЭК 61850.

В настоящий момент ведётся работа по актуализации и дополнению электронной базы корпоративных решений 6-35 кВ, 110-220 кВ, 330-750 кВ.

Важно отметить принцип реализации в части графического представления. Чтобы исключить разрастание базы данных условно графических обозначений, было принято решение использовать «атомарные» условно-графические обозначения (далее – УГО).

«Атомарное» УГО – УГО минимальной схемы. Из «атомарных» УГО создаются УГО сложного оборудования.

УГО оборудования соответствуют первичному оборудованию, а «атомарные» УГО являются минимальным логическим представлением схемы (например, разъединитель с заземляющим ножом представляется атомарным УГО разъединителя и атомарным УГО заземляющего ножа). Каждое УГО имеет точки присоединения (узлы) и набор параметров. Для удобства навигации по схеме и последующего анализа оборудование разделяется на присоединения [2]. «Атомарные» УГО хранятся в базе данных типовых технических решений.

ПТК «ЭК РЗА и АСУ ТП» функционирует в комплексе с *базой данных типовых технических решений*. Проект разрабатываемого объекта находится в *базе данных проектов*.

База данных типовых технических решений содержит перечень структурно-функциональных схем, характеристик, типового оборудования РЗиСА, АСУ ТП, СОПТ, ПА. Стоит отметить, что в *базе данных типовых технических решений* содержатся принципиальные схемы, списки функций, выполняемых типовым оборудованием РЗиСА, АСУ ТП, СОПТ, ПА, и списки сигналов, характерных для функций перечисленных групп оборудования.

База данных проектов включает в себя полный перечень информации относительно текущих и завершенных проектов в части исходных данных, технических зданий, проектной документации, технических решений и пр.

За счет реализации системы обмена данными со смежными ПТК (ПТК «Приёмка» и ПТК «Эксплуатация») ПТК «ЭК РЗА и АСУ ТП» служит базовым элементом в формируемой системе информационного сопровождения оборудования, систем РЗиСА, АСУ ТП, ПА и СОПТ на всех стадиях жизненного цикла.



Рис. 1. Взаимодействие ПТК.

Давайте рассмотрим порядок работы ПТК «ЭК РЗА и АСУ ТП» на примере проекта новой ПС. В первую очередь создаётся титул проекта. Следующим шагом осуществляется информационное моделирование объекта проектирования. Дальше по результатам информационного моделирования и проектирования формируется проектная документация по форме шаблонов вывода данных с последующим сохранением в базе данных проектов.

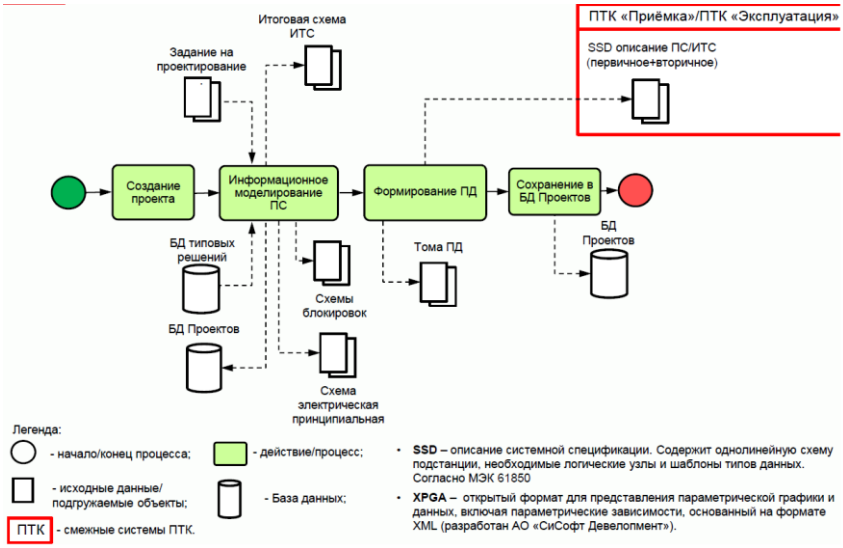


Рис. 2. Бизнес-процесс, описывающий структуру ПТК «ЭК РЗА и АСУ ТП» при работе с проектом новой ПС.

Процесс проектирования на основе информационного моделирования в ПТК «ЭК РЗА и АСУТП», аналогично процессу «классического» проектирования, включает три этапа.

На первом этапе выполняется формирование однолинейной схемы ПС (SLD). При создании схемы используются атомарные УГО электротехнического оборудования из БД САПР.

На втором этапе выполняется автоматизированное распределение шкафов и функций ИТС по элементам однолинейной схемы (SLD) ПС и формируется схема ИТС ПС. Также на данном этапе формируется SSD файл описания ИТС ПС в формате SCL МЭК 61850 с последующим сохранением в БД проекта. С этой целью в ПТК «ЭК РЗА и АСУТП» предусмотрены соответствующие инструменты: Мастер ПА, Мастер РЗиСА, Мастер АСУТП, SCL-навигатор и команда генерации SSD-файла. [1, 2].

На третьем этапе выполняется автоматизированная разработка технических решений для отдельных ИТС (ПА, РЗиСА, АСУТП), а также СОПТ посредством специализированных программных модулей в составе ПТК «ЭК РЗА и АСУТП»:

модуль автоматизированного проектирования ПА;

модуль автоматизированного проектирования СОПТ;

модуль автоматизированного проектирования АСУТП;

модуль автоматизированных расчетов цепей ТТ/ТН.

Автоматизация процесса проектирования отдельных ИТС достигается, прежде всего, за счет экспорта данных из информационной модели схемы ИТС ПС.

В случае работ над проектом существующего объекта электросетевого хозяйства (модернизации или реконструкции) процесс моделирования аналогичен. Предусматривается импорт ИД из БД проектов, разработка ПД и экспорт в БД проектов.

Работа модуля автоматизированного проектирования ПА предусматривает создание структурной схемы ПА. В основе работы модуля лежит импорт информации о существующем оборудовании объектов района противоаварийного управления из ПТК «Эксплуатация», а также из информационной модели схемы ИТС проектируемой ПС. Для преобразования информации, импортированной из ПТК «Эксплуатация», в УГО структурной схемы ПА в составе ПТК «ЭК РЗА и АСУ ТП» предусматривается модуль конвертации.

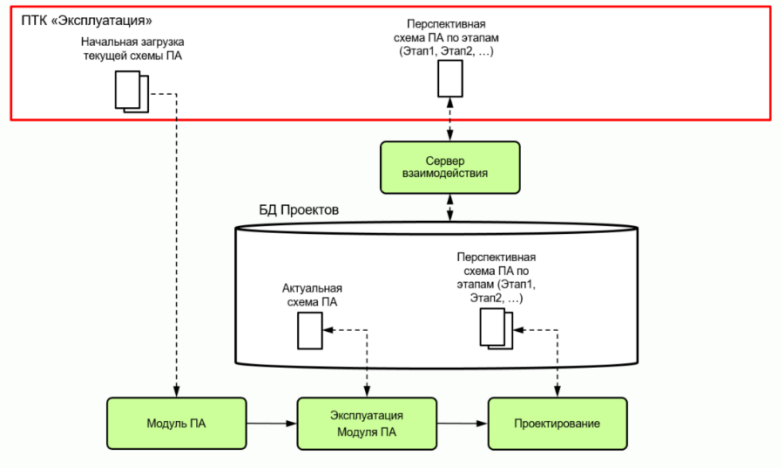


Рис. 3. Схема работы ПТК «ЭК РЗА и АСУТП» в части эксплуатации и проектирования ПА.

На основании данных, содержащих информацию о состоянии сети, строится «Текущая схема ПА». Построение «Перспективной схемы ПА» осуществляется посредством добавления решений на основных этапах проектирования с перспективой развития. Данная структура претерпевает перманентную актуализацию на основании данных из ПТК «Эксплуатация» по мере реализации проектов (данных о введении оборудования в эксплуатацию) до тех пор, пока не достигнет состояния «Актуальной схемы ПА».

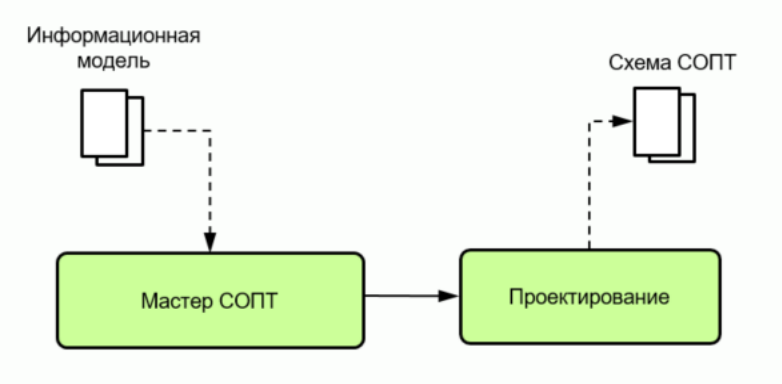


Рис.4. Схема работы ПТК «ЭК РЗА и АСУТП» в части проектирования СОПТ.

Автоматизированное проектирование СОПТ осуществляется на основе информации об архитектуре построения ИТС ПС, данных об электропотреблении шкафов ИТС, проведенных расчетов, введенных ограничивающих условий и пр.

Информация об архитектуре построения ИТС ПС вводится пользователем вручную при заполнении «Анкеты ПС». Информация об электропотреблении шкафов ИТС импортируется из информационной модели схемы ИТС ПС, содержащей предварительно заполненные карточки электропотребления типовых шкафов и нетиповых (заполняются пользователем вручную при разработке схемы ИТС ПС).

Согласно данным, содержащимся в карточках электропотребления шкафов ИТС, программный модуль автоматизированного проектирования СОПТ выполняет распределение потребителей по типовым шкафам ШРОТ с возможностью ручной корректировки.

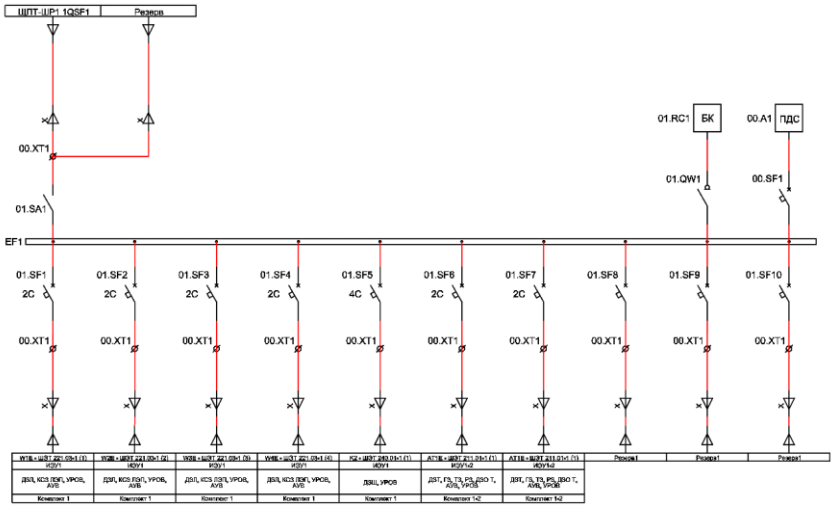


Рис. 5. Образец схемы однолинейной.

В рамках ПТК «ЭК РЗА и АСУТП» реализованы расчеты металлических и дуговых токов короткого замыкания при питании от батареи, а также расчеты металлических и дуговых токов короткого замыкания при питании от зарядных устройств. Результаты расчетов записываются в атрибутивную информацию элементов модели для последующего анализа пользователем и сохранения в отчетной документации.

Работа модуля автоматизированного проектирования АСУТП предусматривает создание структурной схемы АСУТП. В основе работы модуля лежит импорт информации об устройствах полевого уровня и уровня присоединения АСУТП из информационной модели схемы ИТС ПС, а также данные об архитектуре построения ИТС ПС, введенные пользователем при заполнении «Анкеты ПС».

Импорт информации из информационной модели схемы ИТС подстанции обеспечивается за счет передачи атрибутов шкафов ИТС, необходимых для построения структурной схемы АСУТП (интерфейсы, протоколы информационного обмена и т. д.).

Результатами работы модулей автоматизированного проектирования являются тома ПД (текстовая, графическая части), а также файл SSD в формате SCL согласно МЭК 61850. Текстовая часть томов ПД формируется посредством заполнения текстовых шаблонов, оформленных в соответствии с ГОСТ 21.1101. О формировании графической части говорилось ранее.

Заключение

В заключение можем резюмировать, что модернизация и расширение функционала в части ПА, АСУТП, СОПТ, расчёта и проверки ТТ/ТН дает новый уровень повышения автоматизации проектной деятельности с применением программно-технического комплекса «Электронный каталог типовой проектной документации на РЗА и АСУТП». Применение стандарта МЭК 61850 с использованием файлов, описанных на языке SCL, обеспечивает возможность автоматизированного проектирования подстанций с применением устройств ИТС различных поставщиков и производителей, что в свою очередь позволяет осуществлять интеграцию с системами со множеством реализаций этого стандарта без потери данных или сложных перекодировок [3].

Разрабатываемое программное средство учитывает требования актуальной нормативно-технической документации ПАО «ФСК ЕЭС», а также опыт эксплуатации объектов ЕНЭС.

ЛИТЕРАТУРА

[17] Жуков А. В., Хасанов А. Х., Воробьев С. П., Вяткин Р. В., Алексеев И. А. Отчёт о научно-исследовательской работе «Разработка корпоративных типовых технических решений по ПА, РЗ, АСУ ТП и СОПТ ПАО «ФСК ЕЭС» в рамках расширения информационного и инструментального обеспечения электронного каталога РЗА и АСУ ТП». Этап № 1. «Организационные работы. Общие требования. Разработка корпоративных технических решений по составу и реализации функций РЗА и локальной противоаварийной автоматики для элементов сети 6 – 35 кВ, 110 – 220 кВ, 330 – 750 кВ». Раздел № 1.1 «Организационные работы. Общие требования. Том № 4. Редакция №2. Техническое задание на модернизацию и расширение программно-технического комплекса «ЭК РЗА и АСУ ТП», 2019.

[18] Жуков А. В., Хасанов А. Х., Воробьев С. П., Вяткин Р. В. Отчёт о научно-исследовательской работе «Разработка корпоративных типовых технических решений по ПА, РЗ, АСУ ТП и СОПТ ПАО «ФСК ЕЭС» в рамках расширения информационного и инструментального обеспечения электронного каталога РЗА и АСУ ТП». Этап № 1. «Разработка корпоративных технических решений по составу и реализации функций РЗА и локальной противоаварийной автоматики для элементов сети 6 – 35 кВ, 110 – 220 кВ, 330 – 750 кВ». Раздел № 1.15. «Разработка программного адаптера, преобразующего нативный открытый электронный формат используемой САПР в SCL файлы всех типов в соответствии с МЭК 61850», 2019.

[19] Жуков А. В., Хасанов А. Х., Ковыршина Т. В., Бурмейстер М. В., Булатов Р. В. Отчет о научно-исследовательской и опытно-конструкторской работе «Разработка корпоративных типовых технических решений по ПА, РЗ, АСУ ТП и СОПТ ПАО «ФСК ЕЭС» в рамках расширения информационного и инструментального обеспечения электронного каталога РЗА и АСУ ТП». Этап № 1. «Организационные работы. Общие требования. Разработка корпоративных технических решений по составу и реализации функций РЗА и локальной противоаварийной автоматики для элементов сети 6 – 35 кВ, 110 – 220 кВ, 330 – 750 кВ». Раздел № 1.1. Организационные работы. Общие требования. Том № 3. Редакция № 1. «Подтверждение конкурентоспособности продукции, планируемой к производству на основе результатов Работ», 2020.

1.17. СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА СОСТОЯНИЯ И РАБОТЫ УСТРОЙСТВ РЗА

Ю. В. РОМАНОВ, О. А. ФЕДОРОВ, Д. С. ДОБРЫДЕНЬ, Д. В. ЯСЬКО

АО «РТСофт», ПАО «Россети», АО «СО ЕЭС»

Российская Федерация

Контактное лицо:

О. А. ФЕДОРОВ

fedorov_oa@rtsoft.ru

Ключевые слова: АСМ РЗА, мониторинг РЗА, оценка правильности работы РЗА, анализ аварий, обслуживание по состоянию.

Введение

Начиная с 90-х годов в России при реконструкциях и новом строительстве объектов электроэнергетики активно начинают устанавливаться микропроцессорные устройства релейной защиты и автоматики (МП РЗА). Они стали компактнее в размерах, более функциональными, но одновременно и более сложными по техническому исполнению, чем традиционные электромеханические панели защит. С развитием микропроцессорной базы устройств РЗА повышается и их сложность. Каждый производитель с каждым годом совершенствует и усложняет как аппаратное, так и внутреннее программное обеспечение устройств. При этом условия эксплуатации и правила технического обслуживания для микропроцессорных устройств РЗА по сравнению с электромеханическими защитами не поменялись – персонал служб РЗА и дежурный персонал по месту осуществляют периодическую визуальную оценку состояния: по сигналам светодиодной индикации или по информации на ИЧМ устройства РЗА, при возникновении общего сигнала неисправности в АСУТП или загорании общей лампы «Неисправность» на панели. Не исключаются случаи, когда внутренняя неисправность устройства носит спонтанный и временный характер – возникает и пропадает. Это может нигде не фиксироваться и не выявляться при плановых работах по техническому обслуживанию или в процессе эксплуатации, не привлекая внимания персонала. Но это является явным признаком нарушения нормальной работы устройства МП РЗА и причиной дальнейшего выхода из строя из-за внутренних дефектов, повреждений или критических ошибок.

Также сложным и мало автоматизированным остается процесс анализа и оценки правильности работы защит при разборе аварийных событий, связанных с повреждениями первичного оборудования, аварийными отключениями выключателей или некорректной работой самих защит. От момента фиксации аварии до сбора полной аварийной информации и от момента получения и ручного разбора аварийной информации до установления причин неправильной работы РЗА и определения возможных ошибок может пройти от нескольких часов до нескольких дней.

Результаты проведенного анализа показали востребованность автоматизации процессов мониторинга и анализа работы РЗА. Большинство мировых производителей устройств РЗА уже сейчас или занимаются разработкой, или предлагают инженерное программное обеспечение с функциями мониторинга РЗА своего производства. Лидирующие позиции в данном сегменте рынка занимают крупные компании/холдинги из Китая и США, являющиеся мировыми лидерами производства МП РЗА и обеспечивающие охрану своих разработок на различных территориях для дальнейшей коммерциализации. Отечественные производители устройств РЗА в рамках развития собственного оборудования и расширения списка предоставляемых услуг также реализуют функционал мониторинга РЗА в своем ПО. Поэтому каждый производитель РЗА в части мониторинга привязан к своему инженерному ПО, а задача автоматизации анализа аварийных событий и оценки функционирования РЗА в большинстве случаев никак не решается.

Все эти сложности привели к тому, что в 2018 г. ПАО «Россети» провело методическую работу и выпустило стандарт организации СТО 34.01-4.1-007-2018, предъявляющий требования к автоматизированному мониторингу устройств РЗА, в котором описаны требования к автоматизации процесса дистанционного контроля за состоянием современных микропроцессорных устройств РЗА на объектах электроэнергетики и анализу аварийной информации.

Одновременно с этим группа компаний АО «РТСофт» начала вести собственную разработку системы мониторинга РЗА для решения задач по удаленному непрерывному контролю исправного состояния микропроцессорных устройств РЗА и оценки правильности их работы.

В 2019 г. группа компаний АО «РТСофт» по заказу ПАО «Россети ФСК ЕЭС» при участии АО «СО ЕЭС» в рамках НИОКР реализовала проект по созданию автоматизированной системы мониторинга и анализа функционирования МП устройств РЗА для задач диагностики и обеспечения в дальнейшем надежного телеуправления на объектах ЕНЭС в соответствии с требованиями СТО. Проект выполнялся с установкой и опытно-промышленной эксплуатацией системы на подстанциях 220 кВ «Псоу», «Черноморская», «Поселковая» пилотной зоны внедрения филиала ПАО «ФСК ЕЭС» – «Кубанское предприятие магистральных электрических сетей», в самом предприятии и в филиале АО «СО ЕЭС» «Региональное диспетчерское управление энергосистемы Краснодарского края и Республики Адыгея (Адыгея)» (Кубанское РДУ).

Основная часть

Основной целью создания системы мониторинга РЗА стало установление регулярного контроля возникающих явных неисправностей внешних и внутренних компонентов устройства МП РЗА, автоматизация процессов расследования аварийный событий и своевременное выявления ошибок в настройках устройств РЗА для повышения надежности функционирования системы релейной защиты и автоматики в целом на объектах электроэнергетики.

Общим назначением системы является автоматизация задач персонала служб релейной защиты ПАО «Россети ФСК ЕЭС» и АО «СО ЕЭС» по контролю и поддержанию правильности работы устройств РЗА, сбору информации об аварийных событиях и процессах, функциональной систематизации полученных данных, а также автоматизация разбора аварийных ситуаций и формирование комплекса послеаварийных мероприятий и рекомендаций.

Также внедрение систем удаленного мониторинга РЗА в ПАО «Россети ФСК ЕЭС» позволяет получить многофункциональный информационно-аналитический инструмент, который должен стать информационной основой для осуществления перехода на техническое обслуживание устройств РЗА по их фактическому состоянию.

Реализация проекта выполнялась в несколько этапов.

1. Сбор и анализ информации о типах и видах внутренних неисправностей устройств РЗА основных отечественных и зарубежных производителей. Получение и подтверждение информации от производителей РЗА. Систематизация данных. Определение типовых внешних и внутренних неисправностей микропроцессорного устройства РЗА.
2. Проектирование системы, выбор технических решений, разработка архитектуры, определение функциональной и структурной схемы, определение основных функциональных компонентов мониторинга и анализа функционирования РЗА.
3. Разработка алгоритмов обработки данных, мониторинга РЗА, анализа аварийных событий и оценки функционирования устройств РЗА и реализуемых функций защит.
4. Описание и формирование структуры базы данных, классов и атрибутов информационной модели устройств РЗА. Структура модели выполняется на основе использования общей информационной модели (МЭК 61970/61968), которая расширена дополнительной семантикой для описания устройств РЗА.

5. Проектирование интерфейсов и программного обеспечения системы. Объединение программной реализации алгоритмов с пользовательскими интерфейсами.

6. Разработка полигона для испытаний в соответствии с техническими требованиями, программой и методикой проведения испытаний. Проведение заводских испытаний работы программного комплекса.

7. Разработка моделей «цифровых двойников» устройств РЗА. Создание математической модели энергосистемы в области пилотной зоны.

8. Установка и настройка программно-технического комплекса АСМ РЗА на объектах внедрения. Интеграция со смежными системами АСУ ТП и АРМ РЗА на подстанции.

9. Настройка информационного взаимодействия между компонентами системы на подстанциях, в предприятии и диспетчерском центре.

10.Проведение комплексных испытаний работы программного комплекса с выводом оборудования на подстанциях.

11.Проведение опытно-промышленной эксплуатации.

В результате изучения материалов по микропроцессорным устройствам РЗА основных отечественных и зарубежных производителей было выявлено, что разные устройства РЗА, в зависимости от производителя, модели и года выпуска обладают разным ресурсом по мониторингу исправности внутренних компонентов. Это определяется не только техническим развитием программной и аппаратной платформы, но и целями самих производителей повысить надежность своих устройств РЗА за счёт самодиагностики программного и аппаратного обеспечения. Поэтому объем самодиагностики может достигать порядка 200-250 сигналов с одного устройства и будет постоянно увеличиваться. По итогу в системе выделены следующие компоненты контроля технического состояния МП РЗА:

- самодиагностика программного обеспечения,
- самодиагностика аппаратного обеспечения,
- контроль перезагрузок устройства и их частоты,
- контроль исправности цепей измерения тока,
- контроль исправности цепей измерения напряжения,
- контроль состояния питания оперативных цепей,
- контроль исправности коммуникации со SCADA энергообъекта,
- контроль состояния каналов и каналообразующей аппаратуры связи для РЗА (основные защиты линии, обмен сигналами телезащиты),
- контроль изменения конфигурации устройства,
- контроль изменения положений переключающих устройств РЗА.

Табл. 1. Компоненты мониторинга в системе

Компонент мониторинга	**Регистрируемые неисправности МП РЗА**
Самодиагностика программного обеспечения	Сбой внутреннего программного обеспечения платформы устройства. Сбой внутренней операционной системы реального времени устройства.

Компонент мониторинга	**Регистрируемые неисправности МП РЗА**
Самодиагностика аппаратного обеспечения	Неисправность электронных модулей микропроцессорного устройства.
Контроль перезагрузок	Перезагрузка устройства. Частая перезагрузка устройства.
Контроль состояния цепей измерения тока	Неисправность выявляется по факту срабатывания функции блокировки при неисправности цепей тока (КЦТ). Неисправность выявляется при пофазном сравнении значений аналоговых сигналов измерений переменного тока между разными обмотками одного ТТ или разными ТТ одного присоединения.
Контроль состояния цепей измерения напряжения	Неисправность выявляется по факту срабатывания функции блокировки при неисправности цепей напряжения (БНН, КЦН). Неисправность выявляется при пофазном сравнении значений аналоговых сигналов измерений переменного напряжения между разными обмотками одного ТН или смежными ТН одного уровня напряжения.
Контроль состояния питания оперативных цепей	Неисправность питания микропроцессорного устройства. Неисправность питания входных оперативных цепей. Неисправность питания выходных оперативных цепей. Неисправность питания оперативных цепей выявляется при ухудшении параметров сети оперативного постоянного тока.
Контроль состояния коммуникации со SCADA	Ошибки или сбой передачи цифровых данных и сообщений в АСУ ТП. Ошибки или сбой обмена GOOSE сообщениями. Неисправность цифровых каналов связи с АСУ ТП.
Контроль состояния каналов и каналообразующей аппаратуры связи для РЗА	Неисправность каналов связи для РЗА (ДЗЛ, ДФЗ, защиты с телеускорением, защиты с телеблокировкой, телеотключение). Неисправность каналообразующей аппаратуры для РЗА (ДЗЛ, ДФЗ, защиты с телеускорением, защиты с телеблокировкой, телеотключение).

Компонент мониторинга	**Регистрируемые неисправности МП РЗА**
Контроль изменения конфигурации устройства	Недопустимые значения заданных параметров конфигурации микропроцессорного устройства. Изменение группы или параметров конфигурации микропроцессорного устройства. Изменение версии (прошивки) внутреннего ПО микропроцессорного устройства. Дефект конфигурации микропроцессорного устройства выявляется при сравнении с эталонной утвержденной конфигурацией.
Контроль изменения положений переключающих устройств РЗА	Изменение положений переключающих устройств РЗА. Отклонение от нормального положений переключающих устройств РЗА выявляется при сравнении с эталонными положениями для схемно-режимной ситуации.

В ходе разработки системы была реализована двухуровневая архитектура для оптимизации работы аналитических функций системы и нагрузки на каналы передачи данных. На нижнем уровне – подстанциях 220 кВ «Псоу», «Черноморская», «Поселковая» ПАО «Россети ФСК ЕЭС» – установлены отдельные сервера ПТК АСМ РЗА для сбора файлов и данных измерений из АСУ ТП и АРМ РЗА по протоколу МЭК 60870-5-104 и SMB от объектов мониторинга на подстанциях:

- МП РЗА, включая внутренние программно-аппаратные компоненты устройства и внешние цепи, реализующие заданные функции РЗА и обслуживаемые (оперативно и технически) как единое целое;
- переключающие устройства РЗА (переключатели, испытательные блоки, функциональные клавиши, относящиеся к устройству РЗА);
- первичные коммутационные аппараты – силовые выключатели, на которые воздействуют устройства РЗА при срабатывании;
- элементы смежных систем и оборудование энергообъекта, которые влияют на работу и функционирование устройств РЗА: автоматические выключатели ЩПТ и ШРОТ, каналообразующая аппаратура и оборудование связи для РЗА.

При организации сбора данных предпринимаются меры по обеспечению информационной безопасности устройств РЗА путем помещения серверов системы в отдельный демилитаризованный сегмент локальной сети, организованной с использованием межсетевых экранов. В ПТК АСМ РЗА на подстанциях осуществляется локальная обработка файлов и данных измерений, выполняется мониторинг состояния исправности РЗА, фиксация и анализ аварийных событий в пределах подстанции и на отходящих ЛЭП.

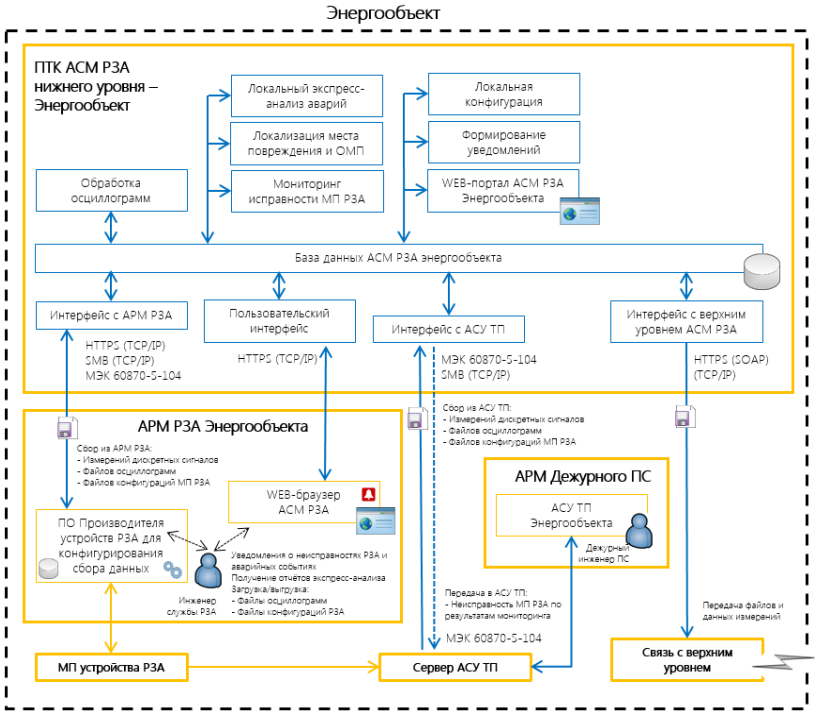


Рис. 1. Функциональная схема ПТК АСМ РЗА подстанции.

Результаты мониторинга и анализа по существующим цифровым каналам связи передаются на верхний уровень системы. Сервер ПТК АСМ РЗА верхнего уровня установлен в Кубанском ПМЭС, где происходят системный анализ результатов с нижнего уровня, долговременное хранение файлов и данных и визуализация результатов мониторинга и анализа аварий. Также программные компоненты верхнего уровня установлены на сервер в ЦОД Исполнительного аппарата АО «СО ЕЭС» с доступом посредством web-сервисов пользователей Кубанского РДУ. Туда передаются результаты анализа аварийных событий на объектах ПАО «Россети ФСК ЕЭС» и файлы данных с сервера ПТК АСМ РЗА Кубанского ПМЭС. Взаимодействие между компонентами АСМ РЗА между уровнями обеспечивается средствами межпрограммного обмена внутри системы по стеку TCP/IP на основе протокола прикладного уровня HTTPS, поверх которого используется протокол SOAP.

Интерфейс пользователя на каждом уровне построен на основе WEB-портала, доступ к которому обеспечивается на рабочих местах пользователей через интернет-браузер.

В рамках проекта был разработан следующий функционал:

1) непрерывный мониторинг и контроль исправности внутренних компонентов МП РЗА, исправности внешних оперативных и измерительных цепей и смежного оборудования, влияющего на работу РЗА, во всех электрических режимах;

2) периодический мониторинг и контроль соответствия фактических параметров настройки устройств РЗА и заданий по их настройке (эталонов);

3) непрерывный мониторинг и контроль соответствия фактических положений оперативных переключающих устройств РЗА в шкафах с заданными оперативными положениями;

4) фиксация аварий и локализация места и вида повреждения (включая программное определение места повреждения на ВЛ) в энергосистеме пилотной зоны;

5) оперативное оповещение персонала о зафиксированных неисправностях РЗА и аварийных событиях;

6) автоматический анализ развития аварийных событий по фактическим дискретным сигналам и файлам осциллограмм от МП РЗА;

7) формирование отчетов по результатам мониторинга РЗА и анализу аварийных событий;

8) оценка правильности пусков и срабатываний ступеней функций РЗА;

9) двусторонний автоматический обмен информацией по расследованию аварийного события между компонентами верхнего уровня: Предприятием ПАО «Россети ФСК ЕЭС» и ДЦ АО «СО ЕЭС»:

a) передача на уровень АО «СО ЕЭС» уведомлений об аварийном событии и данных с результатами анализа аварии (дата и время, место и фаза повреждения, ОМП на ЛЭП) на основе обработки информации, собранной на подстанциях ПАО «Россети ФСК ЕЭС»;

b) передача на уровень АО «СО ЕЭС» файлов записи осциллограмм от МП РЗА по аварийному событию;

c) передача на уровень АО «СО ЕЭС» файлов конфигураций МП РЗА, собранных с подстанций ПАО «Россети ФСК ЕЭС»;

d) передача на уровень ПАО «Россети ФСК ЕЭС» файлов результатов моделирования аварии, сформированных в программном комплексе PF.Protection Анализ РЗА и содержащих требования на пуски и срабатывания устройств РЗА ЛЭП и оборудования 110 кВ и выше на основании актуальной расчетной модели энергосистемы и моделей устройств релейной защиты («цифровой двойник»).

В ходе проведения наладочных работ была выполнена конфигурация функций осциллографирования МП РЗА на подстанциях с добавлением всех каналов пуска, срабатывания, ускорения и блокировок для каждой ступени функции РЗА для полноценного анализа и оценки правильности работы. Также была выполнена синхронизация на подстанции всех МП РЗА от одного источника точного времени.

Комплексные испытания системы проводились в два этапа. 1-й этап был проведен на полигонах АО «РТСофт» и НТЦ ФСК ЕЭС. Для испытаний с помощью испытательных установок воспроизводились различные аварийные режимы (25 опытов с различными условиями, видами и местами повреждения на модели сети) с использованием МП РЗА разных производителей (ЭКРА, Релематика, ABB, Siemens, Радиус-Автоматика). Полученные файлы записи осциллограмм загружались в АСМ РЗА для проверки корректности работы реализованных алгоритмов анализа и оценки правильности срабатываний и пусков РЗА. Итогом первого этапа испытаний АСМ РЗА стало подтверждение корректной работы реализованных алгоритмов обработки и анализа данных.

Второй этап проведен на объектах внедрения. Испытания проводились с выводом из работы КВЛ 220 кВ Черноморская – Поселковая и ВЛ 220 кВ Псоу – Поселковая. Тестовые данные для имитации аварийных режимов подготовлены на основе реальных данных аварии, а также с использованием моделирования повреждения на модели сети Кубанского РДУ с использованием ПК PF.Protection. В ходе испытаний была проверена успешная фиксация и обработка аварии на уровне подстанций. Передача результатов анализа и аварийной информации на уровень Кубанского ПМЭС. Объединение информации с двух подстанций в одну аварию и системный

анализ. Передача результатов системного анализа аварии и файлов осциллограмм с уровня ПАО «Россети ФСК ЕЭС» на уровень АО «СО ЕЭС». Проведение моделирования в ПК PF.Protection на уровне АО «СО ЕЭС» для оценки правильности работы РЗА с учётом моделирования работы «цифровых двойников».

ФСК ЕЭС

Экспресс-отчёт по аварии (технологическому нарушению) от 2019-12-19

1. Общие сведения

Время формирования отчёта	2020-02-26 14:00:10 +0300
Статус	Расследование

2. Энергообъекты

№	Энергообъект	Собственник	Диспетчер
1	ПС 220 кВ Поселковая	Кубанское ПМЭС	Кубанское РДУ
2	РП 220 кВ Черноморская	Кубанское ПМЭС	Кубанское РДУ

3. Информация о повреждении

Место повреждения	КВЛ 220 кВ Черноморская - Поселковая
Время возникновения	2019-12-19 08:26:11.503 +0000
Время окончания	2019-12-19 08:26:12.349 +0000
Время ликвидации первоначального повреждения	2019-12-19 08:26:11.611 +0000
Поврежденные фазы	AB0
Расстояние до места повреждения на линии, км	ПС 220 кВ Поселковая: 2,000 РП 220 кВ Черноморская: 49,000
Переходные сопротивления в месте повреждения на линии, ом	RfAB = 0,418533075645611 RfAB = 0,595130464497386
Общая длительность аварийного режима, мс	847
Общее время ликвидации первоначального повреждения, мс	108.3

Рис. 2. Отчёт, формируемый системой, по результатам анализа аварии.

В настоящее время автоматизированная система мониторинга и анализа функционирования устройств РЗА завершила этап опытно-промышленной эксплуатации и переведена в промышленную эксплуатацию. За это время система фиксировала и анализировала возникающие случаи аварийных событий в сетях 110 и 220 кВ, а также случаи неисправностей РЗА, в том числе частый перезапуск и неправильные настройки. Успешный опыт внедрения позволяет говорить о целесообразности использования таких систем.

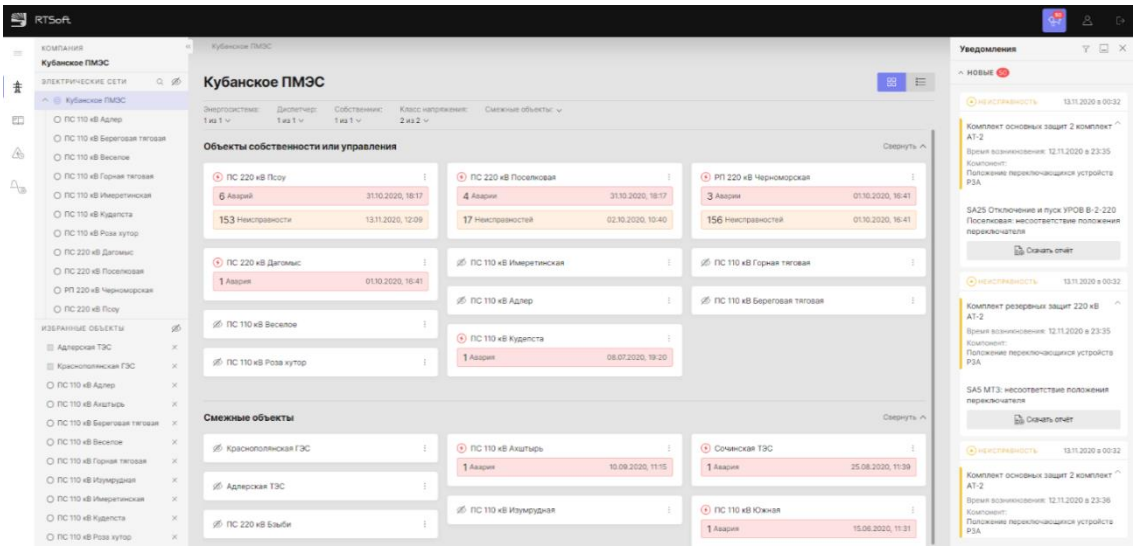


Рис. 3. Интерфейс действующей системы АСМ РЗА.

Заключение

Успешная реализация проекта в целом, дальнейшее развитие и масштабирование системы мониторинга и анализа функционирования устройств РЗА на объектах ЕНЭС позволит снизить число аварий из-за неисправностей и неправильной работы устройств РЗА, что повысит бесперебойность штатного функционирования критических процессов передачи и распределения электрической энергии. Использование системы обеспечит активный информационный обмен между субъектами электроэнергетики для предупреждения аварий, связанных с работой РЗА.

Дальнейшее внедрение и использование систем удаленного мониторинга состояния и работы устройств РЗА на объектах электроэнергетики позволит осуществить переход на техническое обслуживание устройств РЗА по их фактическому состоянию, отказаться от ряда плановых работ, что в итоге приведет к сокращению постоянных эксплуатационных затрат на излишние работы, выполняемые при ТО в планово-предупредительном режиме, и позволит снизить нагрузку на персонал.

СПИСОК ЛИТЕРАТУРЫ

[1] ПАО «Россети». СТО 34.01-4.1-007-2018. Технические требования к автоматизированному мониторингу устройств РЗА, в том числе работающих по стандарту МЭК 61850. 2018.

[2] Dr. Vladimir Gurevich. Reliability of microprocessor-based relay protection devices - myths and reality. EngineerIT - May 2008.

[3] X. Luo, Student Member, IEEE, and M. Kezunovic, Fellow, IEEE. Automated Analysis of Digital Relay Data Based on Expert System.

[4] N. Zhang, Student Member, IEEE, and M. Kezunovic, Fellow, IEEE. Verifying the Protection System Operation Using an Advanced Fault Analysis Tool Combined with the Event Tree Analysis.

1.18. ОПЫТ ВНЕДРЕНИЯ ЦИФРОВОЙ РЕЛЕЙНОЙ ЗАЩИТЫ РАЗЛИЧНЫХ ПРОИЗВОДИТЕЛЕЙ НА ПОЛИГОНАХ ЦПС ПАО «ГАЗПРОМ НЕФТЬ»

М. С. ЗАВГОРОДНИЙ

АО «Электронмаш»

Российская Федерация

Контактное лицо:

М. С. ЗАВГОРОДНИЙ

m.zavgorodnii@electronmash.ru

Ключевые слова: РЗА, Цифровая подстанция, МЭК 61850-9-2LE.

Введение

Предметом исследования являются особенности оборудования РЗА различных производителей для цифровых подстанций в разрезе проектирования системы, пусконаладочных работ и эксплуатации.

В данный момент большинство существующих цифровых подстанций выполнены на оборудовании одного поставщика, как правило, в виде комплексного проекта, когда все работы по внедрению выполняет собственно производитель РЗА.

Целью доклада является освещение ряда проблем, возникающих на разных стадиях реализации в связи с отличиями обработки цифровых данных в устройствах РЗА и сопряжения с шиной процесса, а также описание способов их решения.

Основная часть

Отличием цифровой защиты в контексте данного доклада примем замену сухих контактов и реле на события (GOOSE), а цепей измерения на выборочные значения (SV).

Внедрение GOOSE не встречает сегодня каких-либо серьезных затруднений, больше вопросов возникает в части передачи выборочных значений.

Передача измерений выборочными значениями актуальна также для задач регистрации аварийных событий и учета электроэнергии на ЦПС, но в рамках доклада рассмотрены только выводы относительно устройств релейной защиты и сопряжения с шиной процесса.

График работы по созданию цифровых объектов энергетики компании «Газпром нефть» предусматривает опытную эксплуатацию Полигона ЦПС защит вводных ячеек 35 кВ (2019 год), опытную эксплуатацию цифровой ДЗТ (2020 год), а также реконструкцию двух РУ 6 кВ с использованием шины процесса и централизованной цифровой защиты в ближайшие годы.

При создании Полигонов ЦПС в компании «Газпром нефть» были поставлены следующие цели:

- определение практической сферы применения положений стандарта МЭК 61850-9-2LE;

- выделение существенных требований к вторичному оборудованию для ЦПС;

- испытания информационной совместимости оборудования различных производителей;

- обучение персонала особенностям работы с новыми типами оборудования;

- создание базы документации по наладке и эксплуатации оборудования ЦПС.

На полигоне Омского НПЗ (далее ЦПС ОНПЗ) установлены два комплекта цифровых защит для вводных ячеек РУ 35 кВ ГПП-6Н. Так как подстанция действующая, установить цифровые датчики тока и напряжения не представилось возможности, а действие защиты организовано на сигнал.

Для анализа работы полигона в реальном времени, фиксации результатов опытной эксплуатации установлена система мониторинга с возможностью удаленного доступа.

Структурная схема Полигона ЦПС ОНПЗ представлена на рисунке 1.

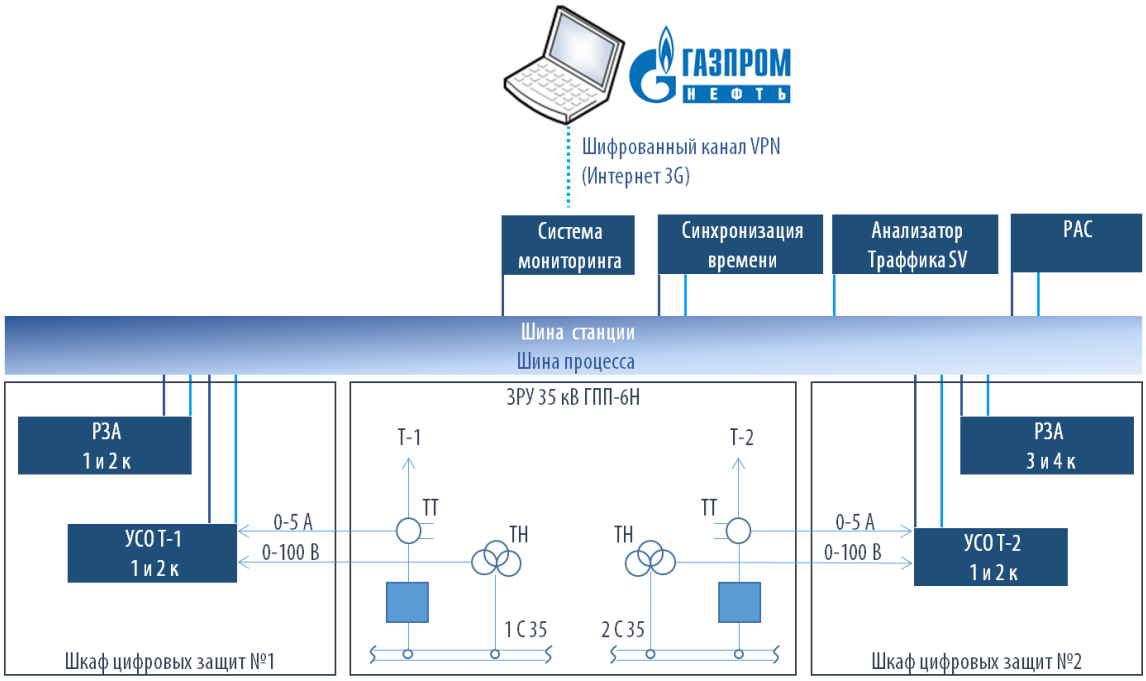


Рис. 1. Структурная схема Полигона ЦПС ОНПЗ.

На полигоне Московского НПЗ (далее ЦПС МНПЗ) установлены три терминала ДЗТ с подключением через устройства сопряжения по трем сторонам трансформатора. Помимо сравнения терминалов РЗА, были установлены счетчики и регистраторы различных типов. Структурная схема Полигона ЦПС МНПЗ представлена на рисунке 2.

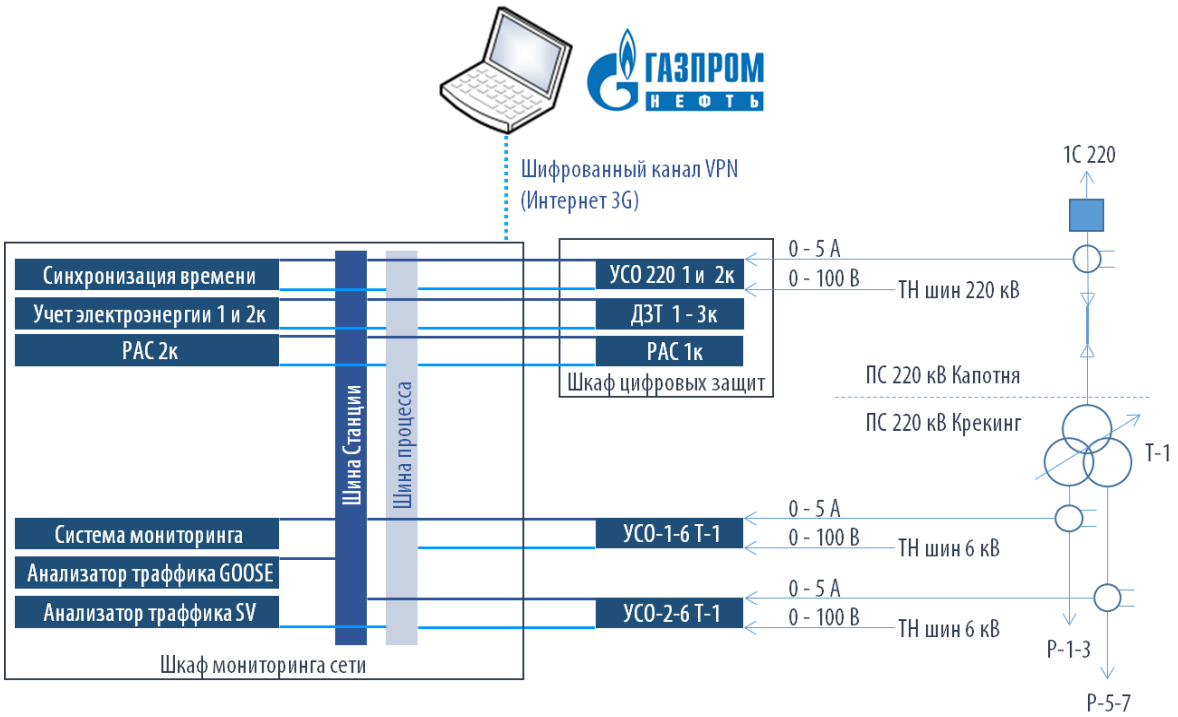
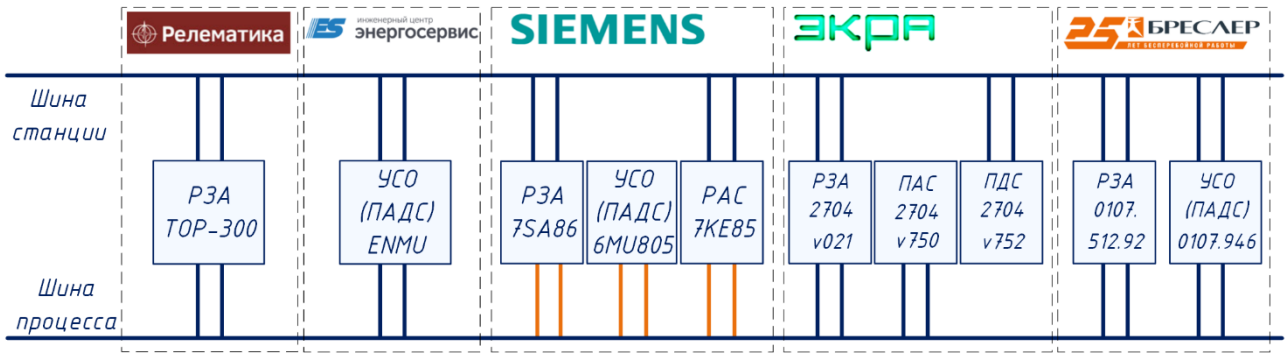


Рис. 2. Структурная схема Полигона ЦПС МНПЗ.

Для ЦПС ОНПЗ комплекты из терминалов цифровых защит и устройств сопряжения предоставили НПП «Бреслер», ЭКРА, Сименс, а также ООО «Релематика» совместно с ИЦ «Энергосервис», так как на момент запуска полигона у них не было соответствующих комплектов. При выборе оборудования для ЦПС МНПЗ мы сконцентрировали наши усилия на сравнении реализации цифровыми устройствами различных производителей (АББ, Сименс, ЧЭАЗ) традиционных функций: РЗА, РАС, учета, в то же время устройства, формирующие цифровую инфраструктуру, не сравнивали, установили одного типа (ИЦ «Энергосервис»).

В ходе разработки основных технических решений была спроектирована эталонная схема с разделением шины процесса и шины станции, к оборудованию защит и устройствам сопряжения сформированы единые технические требования, направленные производителям оборудования. В процессе привязки решения к устройствам выявлены коммуникационные отличия. Среди них наиболее существенные для устройств сопряжения – это подход к синхронизации единого точного времени и выбор сети для публикации GOOSE. Различия в организации коммуникаций устройств ЦПС ОНПЗ представлены на рисунке 3.



Названия рисунков должны быть размещены под рисунками и набраны 10 шрифтом. Рисунки и таблицы нумеруются последовательно арабскими цифрами.

	Физический интерфейс	Синхронизация	Публикация GOOSE	Диагностика по MMS
ENMU (ПАДС)	Ethernet 100 BASE TX	PTP (L2)	Шина станции	Есть
6MU805 (ПАДС)	Ethernet 100 BASE FX	NTP + PPS	Шина процесса	Нет
2704v750 (ПАС)	Ethernet 100 BASE TX	PTP (L2)	(не применимо)	Нет
2704v752 (ПДС)	Ethernet 100 BASE TX	NTP	Шина станции	Есть
0107.946 (ПАДС)	Ethernet 100 BASE TX	PTP / L3	Шина станции	Есть

Рис. 3. Различия в организации коммуникаций устройств ЦПС ОНПЗ.

Так как стандартом не регламентируется разделение сетей [1], пришлось гибко подойти к разделению шины станции и шины процесса. По шине процесса предполагались передача выборочных значений и синхронизация точного времени по PTP, по шине станции MMS и GOOSE. В связи с публикацией одним из устройств сопряжения событий GOOSE на шине процесса решено было организовать для этого трафика туннель по VLAN между шиной процесса и шиной станции.

Из-за отсутствия поддержки частью оборудования синхронизации точного времени по PTP, запущен NTP-сервер, доступ к которому понадобился как по шине процесса, так и по шине станции, здесь также применили VLAN. Этих сложностей удалось избежать при проектировании ЦПС МНПЗ за счет применения устройств сопряжения одного типа.

Для оценки результатов при проведении опытов применены два различных способа – система мониторинга на базе ПЛК собственной разработки «Электронмаш» и серийный цифровой регистратор аварийных событий (Сименс). Программа опытной эксплуатации включает следующие опыты:

1. Сравнение работы защит различных производителей при использовании их собственных устройств сопряжения;

2. Сравнение работы защит при использовании МП РЗА и устройств сопряжения различных производителей совместно;

3. Сравнение работы различных терминалов МП РЗА при получении измерений от одного устройства сопряжения;

4. Проверка резервирования устройств сопряжения;

5. Проверка резервирования сетевого подключения;

6. Проверка достаточности пропускной способности сети;

7. Проверка системы единого точного времени;

8. Проверка реакции системы на сетевой шторм, поданный с Ретом 61850.

По результатам проведенных опытов практически проверена совместимость устройств различных производителей. Расхождений ни в GOOSE, ни в SV не выявлено. На работу цифровых защит не влияет тип выбранного устройства сопряжения. При едином источнике цифровых измерений работа цифровых защит также выполняется одинаково.

Выявлено влияние синхронизации времени. Некоторыми производителями наличие синхронизированного потока выборочных значений заявлено как необходимое требование для работы цифровой защиты. Это требование обосновано для дифференциальных защит, но работа дистанционной защиты, ТЗНП и МТЗ возможна без синхронизации. Некоторые терминалы действительно не поддерживают работу с несинхронизированными выборочными значениями. Получается, что потеря синхронизации времени означает для цифровой подстанции с таким оборудованием потерю защит. Как заявлено производителем, блокировка защит при потере синхронизированных выборок выполняется для исключения ложного срабатывания.

Практически проверена работа защит с получением резервированных измерений от двух устройств сопряжения. У одного из производителей эта функция не реализована, а для одного из терминалов существенным условием для реализации резервирования измерений является

синхронизация выборочных значений. Таким образом, доступна только одна из возможностей – либо резервирование измерений, либо устойчивость защиты к сбою синхронизации времени.

Выяснена реакция цифровых защит на «Информационный шторм», имитированный устройством «Ретом-61850», подключенным к одному из коммутаторов шины процесса в режиме генерации 60 потоков SV по 80 выборок. Половина из устройств релейной защиты в этом режиме показала стабильное отображение измерений, отсутствие ошибок, и обеспечила срабатывание при имитации повреждения. Другие заблокировали действие защит, их производители дали такое пояснение: подается информационная нагрузка в одной из двух резервированных по PRP сетей в размере более 100 Мбит/с, что превышает максимально допустимое для порта терминала по заявленным техническим характеристикам. Действительно, 60 потоков SV80, если каждый считать за 5 мбит [2], составляют 300 мбит/с. Особенность проведенного опыта состоит в том, что на шине процесса формируются пакеты выборочных измерений, не маркируемые тэгом PRP в одной из независимых сетей, и решением может быть игнорирование таких сетевых пакетов. В настоящий момент такая доработка производителями не выполнена. Чтобы эту особенность исключить, требуется резервированное подключение «Ретом-61850» в обе сети PRP. Результаты опытов обобщены в таблице 1.

	Реакция на SV без	Возможность	Реакция на
Устройс	Защита в работе	ДА	Защита в работе
Устройс	Защита в работе	Только	Блокировка
Устройс	Блокировка защит	НЕТ	Защита в работе
Устройс	Защита в работе	ДА	Блокировка

Табл. 1. Результаты опытов.

Одним из результатов, выявленных вне запланированных опытов, были зафиксированные отличия в значениях тока на шине процесса при отсутствии нагрузки, обусловленные различным подходом производителей к аналого-цифровому преобразованию. Так, половина устройств передавали нулевые значения, а половина – 19 А в первичных величинах при коэффициенте трансформации 1000/5. Традиционно применяемые терминалы МП РЗА содержат АЦП и блок обработки в одном корпусе, при использовании цифровых защит с применением устройств сопряжения АЦП оказывается вынесенным, а его связь с блоком обработки выполняется по шине процесса и таким образом становится контролируемой, именно поэтому эти отличия удалось зафиксировать.

По результатам пуско-наладочных работ для каждого из полигонов сформирована исполнительная документация, включающая как традиционный комплект РД в виде схем и чертежей, так и scd-файл станции. Комплект РД для ЦПС отражает все связи по SV, GOOSE, MMS, при этом он разработан без привязки к scd-файлу и без использования специальных программных средств. Конфигурации устройств (.cid-файлы) созданы на основе РД каждым производителем в собственном пакете программного обеспечения. Из отдельных .cid-файлов собран единый файл станции, однако в силу такого метода его формирования он унаследовал все недостатки исходных файлов. Причиной отсутствия разработанного на этапе рабочего проектирования файла

конфигурации станции является отсутствие доступного программного обеспечения для его разработки, визуализации и загрузки на устройства различных производителей.

ЗАКЛЮЧЕНИЕ

Выявленные различия оборудования РЗА различных производителей затрудняют процесс проектирования. При наладке и в эксплуатации совместимость и корректная работа обеспечиваются соблюдением со стороны производителей требований разделов стандарта МЭК 61850 по передаче данных.

На этапе проектирования при применении оборудования различных производителей затрудняющим фактором является отсутствие доступных инструментов автоматизированного проектирования с возможностью создания и дальнейшего использования файла конфигурации станции в соответствии с МЭК 61850.

Вывод по совместимости оборудования по шине процесса и шине станции практически доказывает возможность применения на ЦПС оборудования различных производителей.

Ряд ограничений, накладываемых условиями синхронизации единого точного времени на систему РЗА, должен учитываться при проектировании и эксплуатации ЦПС как один из ключевых факторов надежности.

ЛИТЕРАТУРА

[1] Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations / IEC/TR 61850-90-1 Edition 1.0 2010-03 / IEC, Geneva, Switzerland

[2] Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3 / IEC 61850-9-2 / IEC, Geneva, Switzerland

1.19. ПЕРСПЕКТИВЫ РАЗВИТИЯ И ПРИМЕНЕНИЯ СТАНДАРТА МЭК 61850. ОПЫТ РАЗРАБОТКИ И ПРИМЕНЕНИЯ ФАЙЛОВ SCD В ТЕЧЕНИЕ ЖИЗНЕННОГО ЦИКЛА ЦПС

Н. В. МАРАРАКИНА, А.А. КЛЕПИКОВСКИЙ

Н. В. МАРАРАКИНА

ООО «ТЕКВЕЛ»

Российская Федерация

Контактное лицо:

Н. В. МАРАРАКИНА

mnv@tekvel.com

Ключевые слова: ЦПС, SCD, ICT, SST, SDT, ИЭУ, IEC61850.

Аннотация

Грамотное поэтапное проектирование и последующее управление проектной информацией является основой для реализации подстанции. Требование к проектированию цифровых подстанций внесло изменение в привычный цикл разработки документации энергообъекта. Принципиальным отличием между процессами проектирования стала подготовка электронного проекта на языке описания конфигурации SCL.

Под электронным проектом ЦПС подразумевается файл SCD, который представляет собой виртуальную модель подстанции. Файл содержит конфигурации всех интеллектуальных электронных устройств (ИЭУ) и способен поддерживаться конфигураторами ИЭУ (ICT) независимо от производителя. SCD способен объединить между собой этапы жизненного цикла подстанции, собирая по ходу реализации информацию, которая значительно ускорит наладку ЦПС. Так же SCD дает гибкость в изменении проектных данных и обеспечивает хранение большого объема актуальной информации по объекту в одном файле.

Как показывает практика, в настоящий момент ситуация с SCD-файлом далека от эталонной и требование о наличии этого файла в составе документации воспринимается больше как добавочный элемент усложнения традиционной системы. Происходит это из-за того, что возникает большое количество трудностей при работе с SCD. Однако чтобы получить выгоду новой концепции, предложенной IEC61850, необходимо ее корректно интерпретировать и правильно применять.

На основании опыта разработки и применения файла SCD в докладе выделяется ряд наиболее важных вопросов.

Вопросы выбраны следующие:

- как довериться САПР и забыть о блокноте при разработке SCD?

- как сделать SCD за три недели, если ICD дадут через 3 месяца?

- кто в силах загрузить и применить данные из SCD/CID в конфигураторы IED?

- кто обновит SCD?

В докладе приведены реальные примеры возникающих проблем, с которыми приходится сталкиваться всем, кто имеет дело с разработкой и применением SCD-файла. Отсутствие конкретных решений приводит не только к потере преимуществ разработки SCD-файла, но и применения ЦПС в целом. На основании приведенной информации и проделанного анализа в докладе будут предложены возможные пути решения изложенных проблем.

Введение

В последние годы в связи с прогрессом в разработке оборудования связи для более скоростной передачи данных во всем мире началось бурное развитие цифровизации в электроэнергетическом секторе. Для унификации передачи и использования информации между устройствами различных производителей на подстанции был введен стандарт МЭК 61850. Стандарт разрабатывался как универсальный инструмент, который поможет упорядочить решения

различных производителей оборудования для обмена данными, и стал использоваться в том числе отечественными производителями оборудования релейной защиты и автоматизированных систем управления.

В целом стандарт помогает упростить наладку и обслуживание энергообъекта за счет глубокой проработки решений на этапе проектирования и выдачи файла электронной модели конфигурации подстанции SCD в формате языка SCL, но на практике при его разработке и применении возникает ряд вопросов.

Как довериться САПР и забыть о блокноте при разработке SCD?

Как уже известно, цифровая подстанция и SCD-файл – понятия, неразрывно связанные друг с другом. Должное применение SCD в жизненном цикле ЦПС не представляется возможным без описания в файле правильно составленной конфигурации в соответствии со стандартом МЭК 61850.

Разработка качественного SCD-файла должна начинаться с наличия инструмента конфигурации системы (SCT), который способен выдавать такие SCD-файлы. Не будем принимать во внимание многофункциональность, автоматизацию и удобство пользователя, которые в данном случае являются второстепенной задачей. Обозначим главное требование – возможность работы и выдачи файлов конфигурации в соответствии со стандартом МЭК 61850. В настоящий момент на российском рынке не представлено САПРа, который мог бы с уверенностью заявить о такой работе.

Распространённым явлением является избыточная и некорректная функциональность SCT. САПР способен менять фиксированные параметры, указанные в ICD файлах, прописывать значения за ICT, а также создавать «невалидную» конфигурацию. В целом, ошибки при работе возникают как синтаксические, так и смысловые.

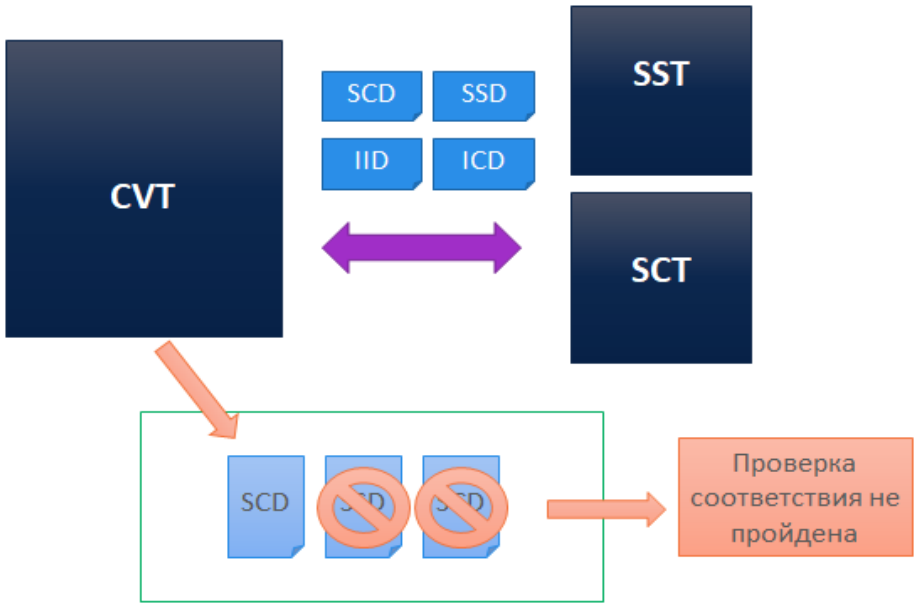
Синтаксические ошибки еще можно обнаружить с помощью валидатора, который сравнивает XML-схему с файлом. Исправить их можно либо через блокнот, либо ждать, когда программисты устранят некорректную работу САПР. Используется в 99% случаев первый вариант. Чем такой способ плох? Как минимум тем, что правка SCD вручную в блокноте опасна. Без должных знаний стандарта или по невнимательности можно исправить файл так, что конфигурация не загрузится ни в один ICT, и понять, почему, будет достаточно проблематично. К сожалению, в настоящий момент без ручной правки в блокноте не обходится ни один разработчик SCD-файла. Так как сделать корректный SCD в некорректно работающем ПО по-другому невозможно.

Если говорить о смысловых ошибках, валидатор синтаксиса тут уже вряд ли сможет помочь. Приведу пример: в предоставленном ICD-файле определен фиксированный набор данных, то есть его состав нельзя изменять. Также в ICD указано максимально возможное количество выдаваемых GOOSE-сообщений, равное одному. САПР позволяет изменить фиксированный набор данных и задать отправку двух GOOSE-сообщений. Ошибочное конфигурирование будет обнаружено только тогда, когда конфигурацию устройства из SCD будут пытаться записать на устройства. Ошибка, допущенная проектировщиком SCD из-за САПРа, не ограничивающего возможности своей работы, приведет либо к неиспользуемости SCD, либо к его масштабному переконфигурированию.

Из описанного примера вытекает вопрос: как же можно быть уверенным проектировщику SCD в работе своего САПРа? Ответ один – прохождение испытаний систем автоматизированного проектирования на соответствие требованиям стандарта МЭК 61850. Методики испытаний изложены в 10-й главе МЭК 61850. Что касается реализации таких испытаний, начать можно с того, что сейчас в нормативно-правовых документах не регламентируется прохождение испытаний для систем автоматизированного проектирования с поддержкой языка конфигурирования SCL на соответствие требованиям стандарта МЭК. Также отсутствует автоматизированный инструмент для проверки, с помощью которого будут проводиться испытания.

В настоящий момент ведется НИОКР ПАО «Россети Кубань» по разработке CVT-инструмента для проверки SST и SCT.

CVT – Conformance Verification Tool – инструмент для проверки соответствия требованиям стандарта МЭК 61850 и профилей.



Испытания для САПР предполагается проводить следующим образом: CVT будет предоставлять SCL-файлы для SCT/SST и воспроизводить действия согласно методикам испытаний, изложенным в 10-й главе МЭК 61850. Выдаваемый после испытаний SCL-файл будет проверяться CVT на момент соответствия ожидаемому результату работы SCT/SST.

При введении документов для систем автоматизированного проектирования с поддержкой языка конфигурирования SCL и введение CVT в использование не может накладывать обязательную проверку всех SCT/SST как допуск к их использованию. Скорее наличие пройденной / не пройдённой проверки на соответствие будут являться одним из основных пунктов заказчика при выборе проектной организации для разработки SCD-файла.

Тем не менее, регламентация соответствия и разработка инструмента значительно ускорят усовершенствование САПРов.

Как сделать SCD за три недели, если ICD дадут через 3 месяца?

Второй вопрос, возникающий при разработке SCD-файла, – где взять актуальный ICD-файл или когда будет предоставлен ICD- (IID-) файл. Зачастую на это не обращается должного внимания. Ставятся только требования и сроки к предоставлению готового SCD, не обращая внимания, что ICD могут быть предоставлены к концу назначенного срока.

Предлагается прописать требования о наличии на официальном сайте производителя ICT, из которого можно выгрузить актуальный ICD-файл. Либо хранение актуальных ICD в каталоге на сайте. Эти решения будут оптимальными и решат вопрос с поиском ICD. Также имеет место хранить на сайте и в ICT каталог с предыдущими версиями ICD-файлов, в случае если проект разрабатывался по более поздней версии прошивки устройства.

Кто в силах загрузить файл и применить данные из SCD/CID в конфигураторы IED?

Использование электронного файла модели подстанции должно быть под силу квалифицированному персоналу, прошедшему любое базовое обучение основам МЭК 61850. На сегодняшний день на эту роль больше всего подходят сотрудники наладочных организаций с опытом внедрения систем АСУ или микропроцессорных РЗА.

Но как показывает практика, какой бы квалификации ни был персонал и какой опыт бы он ни имел, если работа с оборудованием конкретного производителя идет впервые, то, скорее всего, он столкнётся с большим количеством тонкостей реализации. Практически у каждого производителя есть свои особенности при работе как с конфигураторами, так и с терминалами, о которых не написано в мануалах и которые можно узнать только опытным путем.

Конфигураторы отечественных производителей далеко не всегда способны загрузить информацию из SCD, наверное, в этом и заключается основная проблема. По идее, работа наладчика с применением SCD должна упроститься и включать в себя следующий объем работ:

1. Назначать входящие сигналы на внутренние входы в устройстве с помощью ICT.
2. Обновлять прошивку устройства и высылать актуальные IID проектировщику для актуализации SCD.
3. Связывать сигналы, которые содержатся в наборах данных, с сигналами, сконфигурированными в самом устройстве, если не предусмотрена автоматическая подвязка через ICT.
4. Сообщать проектировщику SCD о проблемах с импортом файла в ICT.

Но в действительности, кроме умений работы с конфигураторами IED и работой с терминалом, от наладчика требуется умение понимать язык конфигурации системы (SCL). Ведь для наладки нужно использовать SCD, где есть практически полная конфигурацией на все устройства. А что делать, если информация не подгружается? Открывать SCD-файл в блокноте и на основании его конфигурировать вручную через ICT, что фактически равняется переписать SCD.

Для выявления всех особенностей работы с оборудованием правильным решением будет пройти обучение у производителя цифрового оборудования, которое планируется применять на объекте. А для того чтобы упростить требования к персоналу, который мог бы использовать электронный файл проектной документации, необходимо предусмотреть следующие решения:

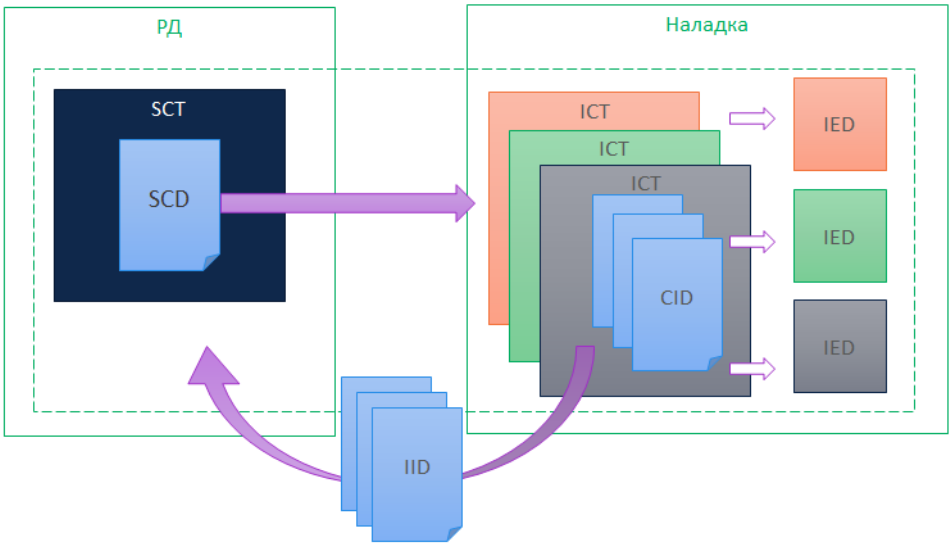
1. Разработать регламенты пути разработки и применения файла электронной рабочей документации от передачи исходных ICD-файлов производителей IED до внедрения готового SCD на объекте.
2. Разработать понятные руководства на конфигураторы IED.
3. Производителю предусмотреть возможность конфигураторов автоматически заполнять нужные поля в CID, которые необходимы для корректной работы только их IED-устройств.
4. Регламентировать передачу файла, созданного в САПР, для настройки IED производителем до отгрузки.

Данная тема подводит к последнему вопросу в рамках данной публикации.

Кто обновит SCD?

Последний экспортируемый файл SCD из SCT на этапе разработки рабочей документации – это еще не законченный SCD. Ему предстоит пройти несколько итераций, чтобы действительно соответствовать конфигурации введенной в работу подстанции. Как уже ранее упоминалось, SCD-файл должен проходить через конфигураторы всех IED, которые используются на объекте. Жизненный цикл SCD-файла на этом не заканчивается.

Конфигуратор IED извлекает из SCD информацию на свое устройство. Конфигурация проходит дополнительную настройку и пополняется информацией из других файлов с уставками, логикой и прочими необходимыми данными для терминала. После завершения настройки полная конфигурация в виде CID-файла загружается в терминал. Так же вместе с CID должен выгружаться IID-файл, который на данном этапе будет соответствовать конфигурации из CID-файла. IID-файл должен отдаваться проектировщикам SCD-файла для его актуализации.



По времени между составлением рабочей документации и пусконаладочными работами может пройти от 6 до 12 месяцев. Как показывает практика, за это время актуализация SCD может поменяться. Сейчас у многих отечественных производителей идет доработка в части соответствия их оборудования корпоративному профилю, СТО и стандарту МЭК61850, соответственно, ICD меняются. Если модель возможностей IED в SCD и CID не изменяется, обновить конфигурацию такого IED с помощью определенного инструмента не должно вызывать проблем. Но как обновить файл, если новый ICD имеет отличное описание модели возможностей от изначально предоставленного ICD? Меняются реализация функций, описание функционала, из-за чего меняются наборы данных и, соответственно, описания входящих подписок.

Если актуализацией файла после конфигураторов IED занимается проектировщик, то кто будет заниматься актуализацией файла, после смены прошивки? Ведь изменение SCD в таком случае может сводиться к разработке нового SCD-файла. Принято считать, что за ведение SCD отвечает проектировщик, но он не может каждый раз нести ответственность за разработчика оборудования, который совершенствует и обновляет возможности своих устройств.

Производителю стоит обеспечить обратную совместимость ICD и конфигураторов IED после обновления прошивки IED-устройства.

Вывод

По итогам разработки и опытной эксплуатации SCD-файла можно сделать вывод, что есть ряд проблем, которые требуют внимания и быстрого решения в первую очередь от производителей оборудования и разработчиков программного обеспечения САПР.

Решение проблем, описанных в статье, значительно бы упростило проектирование и введение цифровой подстанции в эксплуатацию. Достичь этого возможно путем регламентирования действий, который выполняет каждая из сторон – участников создания ЦПС, а также постоянного диалога и обмена информацией между проектировщиком, производителем оборудования и специалистом, который проводит пусконаладочные работы на объекте.

1.20. ПРАКТИЧЕСКИЙ ОПЫТ ПУСКОНАЛАДКИ И ВВОДА В ЭКСПЛУАТАЦИЮ ЦИФРОВЫХ ПОДСТАНЦИЙ 3-Й АРХИТЕКТУРЫ

В.В. БОРОВИЦКИЙ, Д.О. АФАНАСЬЕВ

АО «ТЮМЕНЬЭНЕРГО», ООО «ТЕКВЕЛ»

Российская Федерация

Контактное лицо:

В.В. БОРОВИЦКИЙ

Ключевые слова: ЦПС, SCD, ICT, SST, SDT, ИЭУ, IEC61850.

Введение

Наладка ПС никогда не была легкой задачей, ЦПС с применением МЭК 61850 не исключение. Опыт наладчиков говорит об одном и том же. Даже имея большой опыт и работая на множестве объектов, каждый раз встречаются новые проблемы. Вы можете быть мастером наладки устройств одного производителя или работать с разными, но вывод всегда один – проблем не избежать. На самом деле не все так печально, как может показаться. Для того чтобы разобраться в проблемах наладки, сделаем несложное дело – выделим особые темы.

Проанализировав десятки нестандартных ситуаций, мы обратили внимание, что все они имеют общий корень, прослеживается определенная закономерность. Это говорит о том, что для решения нестандартных проблем наладки достаточно выработать единое правило, соблюдение которого обеспечит не просто решение, а позволит не встречаться с ними вовсе. На практике это правило должно применяться именно перед началом работ, но не в процессе. Решать их на ходу не лучший вариант, так как это говорит о том, что вы уже встретились с нестандартной проблемой и теперь ищете решения, тратя на это драгоценное время. Таким образом, для того чтобы избежать подобных ситуаций, выделим первую область обсуждения – **начало наладочных работ**.

Безусловно, из общего количества проблем есть как нестандартные случаи, так и часто встречающиеся. Такие проблемы перетекают из одного проекта в другой. И для их решения недостаточно соблюдать определенное правило, нужно иметь конкретные знания в части МЭК 61850. Необходимо понимать назначение каждого коммуникационного параметра MMS, GOOSE и Sampled Value, а также разбираться в механизмах работы сетевого оборудования. Но бывает, что знание не всегда ограничивает от возникающих проблем, порой это может быть следствием особенностей реализации оборудования в части МЭК 61850. Для того чтобы обратить внимание на такие сложности, выделим еще несколько тем – **наладка MMS**, **наладка GOOSE и Sampled Value**.

Начало наладочных работ

Стандартное начало работ можно описать как подготовку наладчика в части сбора исходных данных и ПО. В объем исходных данных для конфигурирования части МЭК 61850 входит SCD-файл, а в объем исходного ПО – IED Configuration Tool (ICT). Само использование SCD-файла в качестве исходных данных вопросов не вызывает, достаточно использовать нужный функционал конфигуратора ИЭУ. Но часто бывает так, что, имея исходный SCD и ПО, наладчику приходится дорабатывать конфигурацию устройства: прописывать подписчиков на Report, GOOSE или Sampled Value; описывать сетевые и коммуникационные параметры; описывать входные сигналы. В половине случаев это не связано с недостатком SCD, насколько полно будет использоваться конфигурация устройства из SCD-файла, определяется лишь реализацией ICT. Таким образом, на этом этапе выделяем две проблемы:

- недостаток или недоработка SCD-файла;
- недостаток ICT.

Если известно, что ICT не вел себя таким образом ранее или не должен так реагировать на входные данные, то первая идея – обратиться к разработчикам SCD. Если для наладки выделено достаточно времени, то такой подход будет верным. Но с практической точки зрения все не так,

наладка не терпит промедления. Как поступать в этой ситуации, определено стандартом МЭК 61850-6 ed 2.1, глава 5.3.

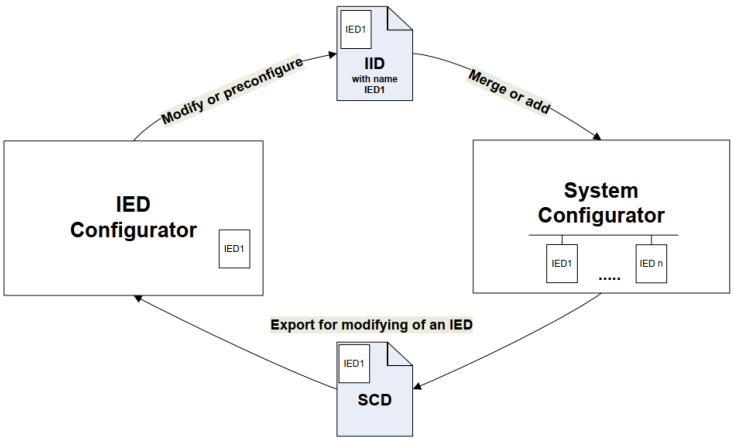


Рис. 1. Применение IID-файла.

Как видно из схематичного описания применения IID файла, стандарт предусматривает обновление SCD-файла при помощи доработки проекта в ICT. Такое взаимодействие между наладчиком и проектировщиком будет продуктивным и потребует минимального вложения времени. На практике такой подход игнорируется и ведет к затягиванию процесса наладки. Ожидание обновленного SCD-файла может затянуться на неопределенный промежуток времени. Во избежание такой ситуации инициатором обновления проекта должен быть наладчик.

Не всегда проблема с импортом проекта может быть выражена в некорректном SCD-файле, тогда стоит обратить внимание на ICT. Частой ошибкой наладчиков является использование опыта применения ПО предыдущих проектов. Ошибка заключается в отсутствии контроля актуальных версий применяемого ПО. Стоит обратить на это особое внимание. Работая по одному из проектов, пришлось столкнуться с тем, что ICT не распознавал конфигурацию устройства из SCD-файла в полной мере. Для решения вопроса были предприняты меры – официальное письмо к разработчику ПО. Ответ был ожидаемым: «На данный момент конфигуратор не поддерживает импорт информации из SCD-файла в следующем объеме…» На тот момент не оставалось ничего, кроме как продублировать информацию из SCD-файла в ICT. Был получен опыт, опыт негативный. Далее последовал следующий объект, где потребовалось налаживать устройства от того же производителя. Во избежание затягивания наладочных работ, еще до выезда на объект конфигурации устройств дорабатывались в ICT. В ходе последующих работ на объекте приступили к импорту конфигураций в устройства и столкнулись с тем, что импорт проходил с ошибкой. Как оказалось позже, ошибка заключалась в использовании ICT старой версии. Далее по большой случайности было выяснено, что обновленный конфигуратор ИЭУ начал распознавать конфигурацию устройств из SCD-файла в полной мере. Вывод – перед началом работ необходимо удостоверится в актуальности применимого ПО.

Рецепт кажется полным, но есть еще один нюанс. Для этого рассмотрим наш следующий опыт наладки. Для наладки был подготовлен SCD-файл в конфигураторе производителя. Это исключало какие-либо проблемы стыковки SCD-файла и ICT. При этом ПО было скачано с официального сайта, что гарантировало исключение проблем с использованием неактуальной

версии. После выезда на объект конфигурации устройств были импортированы в сами устройства, и ошибок при импорте не наблюдалось. Приемка работ была выполнена успешно, но через некоторое время эксплуатация обратила внимание на то, что в SCADA отображалась неактуальная информация. Состояние сигналов не соответствовало действительности, а качество сигналов было нормальным. При диагностировании было выяснено, что у некоторых устройств зависла модель данных. Она просто не обновлялась. Коммуникационные сервисы Report и GOOSE продолжали работу, но толку от этого не было из-за отсутствия обновления данных. Было определено, что помогает лишь перезагрузка устройства, но проблема повторялась через несколько часов или дней. Исходя из этого была выяснена причина, по которой это не диагностировалось ранее. В процессе наладки устройства перезагружались, порой несколько раз за день. Дальнейший анализ занял не один день, но устранить проблему не удавалось. Для разрешения сложившейся ситуации была подключена техподдержка производителя устройств, и она сообщила о том, что версия прошивки очень старая и необходимо выполнить обновление. Обновление действительно помогло. Надо учесть, что это лишь один из примеров проблем из-за неактуальной прошивки устройства в части МЭК 61850. Будет правильным сделать вывод о том, что для успешного начала наладочных работ необходимо озадачиться обновлением прошивок устройств до последних версий.

Подводя итог по подготовке к наладочным работам на ЦПС, мы имеем три правила:

- Обновление ICT до последней версии;
- Обновление неполного SCD-файла при помощи IID-файла;
- Обновление прошивки устройства до последней версии.

Казалось бы, три небольших правила, но добыты они при помощи горького опыта. Соблюдение этих правил обеспечивает:

- уменьшение срока наладки от 1 до 2 недель;
- уменьшение шанса встречи с проблемами наладки ЦПС;
- уменьшение шанса выезда на объект по гарантийным случаям;
- улучшение качества наладочных работ.

Наладка MMS

Вопросы наладки MMS являются одними из самых сложных. Это связано с гибкостью настроек, которые предоставляет этот протокол передачи данных. А это, в свою очередь, требует действительно глубоких познаний в принципе работы протокола. Часто вопросы настройки MMS оставляют на самый последний момент, так как наладка систем верхнего уровня является крайним этапом наладки в целом. Только после готовности вторичного оборудования и настройки ЛВС предоставляется возможность выполнить проверку прохождения данных. Часто бывает так, что настройки отчетов на устройствах оставляют по умолчанию. Это касается не только процесса наладки, но и разработки SCD-файла. В иных ситуациях отчеты настроены идеально, но возникает другая проблема, проявляется она в гибкости протокола. Устройства верхнего уровня, подключившись к вторичному оборудованию, могут задавать параметры отчетов. Что приводит к рассинхронизации проектного решения из SCD-файла и фактической реализации. Контролировать это сложно, так как в настройке информационного взаимодействия учувствуют инженеры, ответственные за наладку разных вторичных систем. В итоге возникающие проблемы часто

вызваны именно этим. Протокол MMS предназначен для стыковки разных систем, а на стыках всегда заметны шероховатости. Из общего количества проблем MMS часто возникают следующие:

- учащенная передача отчетов;
- некорректная работа буферизируемых отчетов;
- проблемы выполнения команд.

Учащенная передача отчетов

Проблема отчетов зачастую проявляется в учащенной передаче отчетов. Возникает она по причине пренебрежения настройками отчетов или установке значений по умолчанию. Часто такая проблема возникает с не буферизируемыми отчетами. В чистых цифрах количество формируемых отчетов может достигать 1 000 в минуту, а усугубляется все количеством устройств на объекте. Как правило, это приводит к повышению нагрузки на вычислительные мощности принимающей стороны и переполнению очереди обрабатываемых данных. На практике мы имели опыт наблюдать за работой SCADA-системы в таком режиме. Проблема проявлялась в зависании системы и, как следствие, пропуске регистрации данных. Выяснить причину не удалось сразу, так как анализ CID-файлов передающей стороны привел к выводу, что проблем быть не должно. Как оказалось, принимающая сторона при подписке на отчеты задавала совершено иные параметры, что и вызвало такую проблему. Чтобы разобраться в этом, стоит понять, как это работает. Стандарт МЭК61850-8-1 Ed2.1 описывает сервисы SetBRCBValues\SetURCBValues, которые позволяют принимающей стороне редактировать параметры отчетов перед их активацией (рис. 2 и 3).

ACSI component name	MMS named component name	ACSI Basic Type	Comment
RptID	RptID	VisString129	See 8.1.2.5 May not be written when RptEna=TRUE
RptEna	RptEna	BOOLEAN	
DatSet	DatSet	ObjectReference	See 8.1.3.2.2 May not be written when RptEna=TRUE
ConfRev	ConfRev	INT32U	May not be written
OptFlds	OptFlds	RCBReportOptions	See 8.1.3.13 May not be written when RptEna=TRUE
BufTm	BufTm	INT32U	May not be written when RptEna=TRUE
SqNum	SqNum	INT16U	May not be written
TrgOps	TrgOps	TriggerConditions	See 8.1.3.9 May not be written when RptEna=TRUE
IntgPd	IntgPd	INT32U	May not be written when RptEna=TRUE
GI	GI	BOOLEAN	
PurgeBuf	PurgeBuf	BOOLEAN	May not be written when RptEna=TRUE
EntryID	EntryID	EntryID	See 8.1.3.5 May not be written when RptEna=TRUE
TimeOfEntry	TimeofEntry	EntryTime	May not be written
ResvTms	ResvTms	INT16	May not be written when RptEna=TRUE
Owner	Owner	Octet64	See 8.1.2.4 and 17.1.2 May not be written

Рис. 2. Параметры буферизируемого отчета.

ACSI component name	MMS named component name	ACSI Basic Type	Comment
RptID	RptID	VisString129	See 8.1.2.5 May not be written when RptEna=TRUE
RptEna	RptEna	BOOLEAN	
Resv	Resv	BOOLEAN	May not be written when RptEna=TRUE
DatSet	DatSet	ObjectReference	See 8.1.3.2.2 May not be written when RptEna=TRUE
ConfRev	ConfRev	INT32U	May not be written
OptFlds	OptFlds	RCBReportOptions	See 8.1.3.13 May not be written when RptEna=TRUE The values of buffer-overflow and entryID shall be ignored
BufTm	BufTm	INT32U	May not be written when RptEna=TRUE
SqNum	SqNum	INT8U	May not be written
TrgOps	TrgOps	TriggerConditions	See 8.1.3.9 May not be written when RptEna=TRUE
IntgPd	IntgPd	INT32U	May not be written when RptEna=TRUE
GI	GI	BOOLEAN	
Owner	Owner	Octet64	See 8.1.2.4 and 17.1.2

Рис. 3. Параметры не буферизируемого отчета.

Из общего перечня параметров обратим внимание на TrgOps, IntgPd и GI. Часто системы верхнего уровня работают с этими параметрами на свое усмотрение или на усмотрение инженера. TrgOps определяет причины формирования отчетов. Всего существует 5 триггеров:

- data change. Формирование отчета по изменению значения сигнала;
- quality change. Формирование отчета по изменению качества сигнала;
- data update. Формирование отчета по обновлению данных;
- integrity. Периодическое формирование отчета;
- general interrogation. Формирование отчета по запросу клиента.

Рассмотрим, как триггеры передачи данных могут повлиять на частоту формирования отчетов. Ошибка в применении триггера data change проявляется в комбинации с неверно заданными порогами нечувствительности. Эта проблема свойственна не буферизируемым отчетам, которые применяются для передачи аналоговых значений, а им присуще частое изменение значения. Теперь представим, что отчет связан с набором данных, где перечислены 10 измерений и порог нечувствительности задан как 0,001. И после такой фатальной ошибки умножим количество устройств на 100. Частое изменение аналоговых значений приводит к тому, что устройство формирует до 100 отчетов в минуту. Теперь перемножим и получим цифру в **10 000** отчетов.

Триггер integrity – еще одна причина частого формирования отчетов. В комбинации с параметром IntgPd он определяет период формирования отчетов вне зависимости от того, изменили сигналы свое состояние или нет. Более того, при отправке отчета по данному триггеру отправляется весь набор данных. Рассмотрим пример. Набор данных устройства содержит 50 сигналов. Включен триггер integrity, и параметр IntgPd имеет значение 100. Значение IntgPd указывается в миллисекундах. Такой отчет будет формироваться 600 раз в минуту. Теперь вспомним о 100 устройствах и получаем цифру в **60 000** отчетов в минуту.

Следующий триггер заслуживает отдельного рассмотрения – это GI. Системы верхнего уровня, как правило, предоставляют возможность определить период запросов отчетов от передающего устройства вне зависимости от изменения сигналов. В этом случае передается весь набор данных. И тут представим ситуацию, что система верхнего уровня запрашивает отчет раз в секунду. Путем несложных расчетов получаем цифру в **6 000** отчетов в минуту от 100 устройств. А теперь представим, что в настройке отчетов были допущены все три ошибки, и получаем цифру в **76 000** отчетов в минуту. Действительно внушительные цифры, особенно если сравнить с нормальной настройкой отчетов, где можно уменьшить цифру до **200** отчетов в минуту. Именно с такой проблемой пришлось столкнуться нам. Как избежать этого? Достаточно придерживаться следующих правил:

- не оставлять настройки отчетов по умолчанию;
- не использовать сервисы SetBRCBValues\SetURCBValues на стороне клиента.

Некорректная работа буферизируемых отчетов

Буферизируемый отчет предназначен для сохранения отчетов в энергонезависимом буфере устройства. Это говорит о том, что даже после разрыва связи клиент может переподключиться к серверу и получить пропущенные данные. Работа этих отчетов кажется понятной, но есть тонкости настройки, о которых часто забывают. В нашей практике эта проблема встречалась часто и решалась изменением лишь одного параметра. Но чтобы разобраться в этом, разберем один случай. На энергообъекте была установлена SCADA, которая опрашивала сотню устройств при помощи буферизируемого отчета. В ходе перезапуска системы в листе событий регистрировалось множество событий со старой меткой времени. История повторялась после каждой перезагрузки, лист событий заполнялся большим количеством ненужной информации. На первый взгляд все казалось понятным. Устройства передавали в SCADA всю информацию из буфера данных. Эксплуатирующая организация попросила разобраться с этим и поменять отчеты на не буферизируемые. По их мнению, проблема скрывалась только в этом, так как на остальных объектах проблема решалась таким образом. Да, это можно назвать решением, но оно было неверным. Чтобы разобраться с этим, был проведен анализ CID-файлов устройств, и проблема не была выявлена. Как позже оказалось, как и в случае с частыми отчетами, ошибка скрывалась в настройках SCADA. Был отключен параметр EntryID, и после его активации все благополучно забыли о проблеме. Теперь стоит сделать уточнение. В составе параметров настраиваемых в отчетах есть поля OptFlds. Данные поля предназначены для добавления в отчеты дополнительной информации, которая может быть необходима клиенту. Стандарт МЭК 61850-8-1 Ed.2 описывает 9 опциональных полей.

ACSI value of BRCState	MMS bit position
Reserved	0
sequence-number	1
report-time-stamp	2
reason-for-inclusion	3
data-set-name	4
data-reference	5
buffer-overflow	6
entryID	7
conf-revision	8
segmentation	9

Рис. 4. Опциональные поля буферизированного отчета.

Расшифровка назначения полей:

- sequence-number. Счетчик отчета в последовательности переданных отчетов;
- report-time-stamp. Метка времени отчета;
- reason-for-inclusion. Причина передачи данных по триггерам;
- data-set-name. Ссылка на набор данных отчета;
- data-reference. Ссылка на элементы данных, включенных в отчет;
- buffer-overflow. Переполнение буфера;
- entryID. Уникальный идентификатор отчета;
- conf-revision. Ревизия набора данных отчета;
- segmentation. Признак разбиения отчета на несколько посылок.

Таким образом становится понятным, что каждому новому отчету в буфере устройства присваивается уникальный идентификатор EntryID. Если устройство верхнего уровня получило отчет с информацией о его уникальном идентификаторе, оно понимает, какой отчет из буфера был получен последним. Теперь представим, что произошел разрыв связи, и во время её отсутствия устройство записало новые отчеты в буфер. Связь восстановилась, клиент перед активацией связи отправляет информацию с идентификатором последнего принятого отчета. Таким образом, передающая сторона понимает, что отдать нужно только те отчеты, которые были записаны после него. Если же во время разрыва связи новых отчетов не было, то в момент восстановления не будет передан ни один отчет. Такой режим до ввода отчета в работу называется ресинхронизацией.



Рис. 5. Ресинхронизация буферизированного отчета.

Чтобы избегать таких проблем стоит делать следующее:

- для буферизированных отчетов всегда добавлять опциональное поле EntryID;
- не оставлять настройки отчетов по умолчанию;
- не использовать сервисы SetBRCBValues\SetURCBValues на стороне клиента.

Проблемы выполнения команд

Стандарт МЭК 61850-7-2 предусматривает сервис Control, который реализуется при помощи протокола MMS. Часто при выполнении наладочных работ нужно проверить выполнение команд. Сложности вызывает проблема диагностирования причины невыполнения. В нашей практике мы столкнулись с интересной задачей. Как бы мы ни прикладывали свои знания, не удавалось понять, почему не получается выполнить оперирование коммутационным аппаратом. Применение специализированного ПО не давало свои плоды. После долгих изысканий все же удалось выяснить причину. Скрывалась она в ошибке, которая была допущена в матрице назначений устройства. Сигнал о включенном положении выключателя блокировал возможность оперирования им. Обнаружить эту проблему помог не анализ матрицы назначений, а изменение режима управления. Стандарт МЭК 61850-7-2 Ed 2.1 описывает четыре режима управления объектом:

- Direct Control with Normal Security. Прямая команда без обратной связи;
- SBO Control with Normal Security. Команда с выбором объекта управления без обратной связи;
- Direct Control with Enhanced Security. Прямая команда с обратной связью;
- SBO Control with Enhanced Security. Команда с выбором объекта управления и обратной связью.

Под выбором объекта управления подразумевается резервирование права управления во избежание одновременной подачи команды от разных источников. Под обратной связью подразумевается возврат информации о причине невыполнения команды. Поле, которое отвечает

за информацию о причине невыполнения команды, называется AddCause. Именно использование этого поля помогло направить наши взгляды в нужном направлении. Причиной, почему не удалось сразу разобраться в проблеме, оказалось неверное использование режимов управления. Изначально использовался режим SBO Control with Normal Security, но после изменения режима на SBO Control with Enhanced Security добавилась возможность диагностировать выполнение команды. Для диагностирования неисправности поле AddCause может возвратить 28 различных ответов:

- Unknown. Команда не выполнена по неизвестной причине;
- Not-supported. Объект не поддерживает функцию управления;
- Blocked-by-switching-hierarchy. Команда управления не выполнена из-за местного режима управления;
- Select-failed. Операция управления не удалась из-за неудачного выбора;
- Invalid position. Заданное положение не было достигнуто;
- Position reached. Объект уже находится в нужном положении;
- Parameter-change-in-execution. Параметры управления были изменены в последовательности управления, которая еще не завершена;
- Step-limit. Достигнут предел положения (например РПН);
- Blocked-by-mode. Логический узел, содержащий объект управления находится в режиме blocked;
- Blocked-by-process. Логика или алгоритмы устройства блокируют управление;
- Blocked-by-interlocking. Условия проверки блокировки не дают управлять (например ОБР);
- Blocked-by-synchrocheck. Условия проверки синхронизма не дают управления;
- Command-already-in-execution. Команда подавалась ранее, операция выполняется;
- Blocked-by-health. Управление блокировано из-за внутренней ошибки ИЭУ;
- 1-of-n-control. Управляющее воздействие было заблокировано, поскольку другое управляющее воздействие в домене (например, подстанции) уже запущено;
- Abortion-by-cancel. Оперирование было отменено пользователем;
- Time-limit-over. Завершение команды превышает ожидаемое время;
- Abortion-by-trip. Команда отменена из-за срабатывания РЗА;
- Object-not-selected. Команда не выполнена, так как объект не выбран;
- Object-already-selected. Выбор не выполнен, так как объект уже выбран;
- No-access-authority. Клиент не имеет прав для выполнения команды;
- Ended-with-overshoot. Управляющее воздействие выполнено, но объект принял не ожидаемое положение;
- Abortion-due-deviation. Действие управления было прервано из-за отклонения между значением команды и ожидаемым значением;
- Abortion-by-communication-loss. Действие управления было прервано из-за потери связи с клиентом, выдавшим управление;
- Blocked-by-command. Действие управления заблокировано из-за того, что атрибут данных CmdBlk.stVal установлен в TRUE;
- None. Команда выполнена успешно;
- Inconsistent-parameters. Параметры между последовательными службами управления не совпадают, например, ctlNum службы Select и Operate отличаются;
- Locked-by-other-client. Другой клиент уже зарезервировал объект управления.

В нашем примере возвращался ответ Blocked-by-interlocking, что позволило довольно точно определить причину отклонения команды. Чтобы упростить диагностику проблемы, советуем использовать режимы управления Direct Control with Enhanced Security или SBO Control with Enhanced Security.

Наладка GOOSE и Sampled Value

В отличие от MMS, сервисы GOOSE и SV выглядят довольно простыми. Если отчеты поддерживают множество различных механизмов формирования данных, то GOOSE и SV значительно проще. Простота обусловлена тем, что это трафик особой важности, где необходима скорость формирования, передачи и обработки данных. Без этой информации устройства, выполняющие вторичные функции, теряют исходные данные, а это приравнивается к выводу устройств из работы. Коммуникационные сервисы GOOSE и SV инкапсулируют информацию прямиком на канальный уровень, где используется протокол Ethernet. При этом минуются все вышестоящие уровни модели OSI, а возможность вещания трафика без установки связи обеспечивается при помощи Multicast MAC-адреса назначения. Получатели данных сами определяют, какой трафик им нужен, подписываясь на него. Распаковка таких данных проста – достаточно поймать нужный Ethernet-кадр из сети и приступить к считыванию полезной информации. Но несмотря на этот простой механизм, проблемы все равно возникают. В большинстве случаев это связано с особенностями реализации коммуникационных сервисов GOOSE и SV разных производителей. Эта тема объединена под одним флагом, так как большинство проблем общие для обоих коммуникационных сервисов. Далее разберем часто возникающие проблемы:

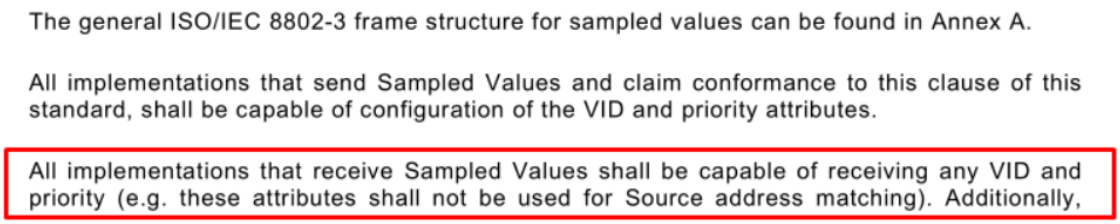
- применение параметра VLAN ID на стороне подписчика;
- присвоение multicast MAC адресов;
- синхронизация времени и работа защит.

Применение параметра VLAN ID на стороне подписчика

В части настройки исходящих GOOSE/SV имеется интересный параметр VLAN ID, он требует особого внимания. Указывается данный параметр наряду с параметрами MAC address и APPID и по ошибке интерпретируется как некий дополнительный параметр для фильтрации входящей информации на стороне приемника. Для того чтобы разобрать это, рассмотрим пример.

На одном из налаживаемых объектов была настроена система, где в сети передавался трафик GOOSE/SV. При этом для передачи и приема информации использовались устройства одного производителя. На первый взгляд казалось, что проблем быть не должно, ведь в такой ситуации гарантируется полная стыковка. Но в действительности устройства – приемники сообщали о том, что не видят нужных данных в сети. После этого последовало несколько дней для выяснения причины. На стороне отправителя все параметры соответствовали ожидаемым, а ЛВС имела корректные настройки. Для определения проблемы было использовано ПО WireShark. При помощи ноутбука подключились к каналу связи вместо устройства приемника и наблюдали, что весь трафик доходит. На стороне приемников была корректно описана подписка. Диагностировать проблему не удавалось довольно долго, но помог эксперимент. Отправитель и приемник данных были подключены напрямую, минуя сетевое оборудование. После этого приемник начал индицировать о наличии ожидаемых данных. Таким образом было установлено, что проблема в сетевом оборудовании. В действительности это оказалось не так, проблема скрывалась на стороне

подписчика. Согласно стандарту МЭК 61850-8-1 и 61850-9-2, тег VLAN должен обязательно присутствовать во всех публикуемых кадрах SV/GOOSE. Предназначен он для приоритизации и разделения трафика в пределах сетевого оборудования. То есть эта информация нужна исключительно сетевому оборудованию для ограничения приемника от ненужных данных. Если тег VLAN ID задан при конфигурировании SV/GOOSE, то это значение должно присутствовать в Ethernet-кадре, если он не задан, тогда значение должно быть равно 0. Также, согласно стандарту МЭК 61850, подписчик не должен осуществлять идентификацию входных данных при помощи VLAN ID.


The general ISO/IEC 8802-3 frame structure for sampled values can be found in Annex A.

All implementations that send Sampled Values and claim conformance to this clause of this standard, shall be capable of configuration of the VID and priority attributes.

All implementations that receive Sampled Values shall be capable of receiving any VID and priority (e.g. these attributes shall not be used for Source address matching). Additionally,

Рис. 6. Требование стандарта в части VLAN ID на стороне приемника.

Теперь разберем, что же произошло. Ethernet-кадр с тегом VLAN ID, проходящий по сети, может терять тег, кадру может присваиваться другое значение тега VLAN ID, или же публикуемая издателем информация может иметь дефолтное значение VLAN ID, равное 0, и тег, согласно уставке Native VLAN порта коммутатора, может изменять свое значение. Проанализировав это, становится понятно, что если на стороне подписчика параметр VLAN ID отвечает за идентификацию входных данных, то может случиться так, что итоговый VLAN ID может поменять свое значение и подписчик не увидит нужного GOOSE/SV. Именно с такой проблемой пришлось столкнуться нам. На выходе из коммутатора со всех Ethernet-кадров, перенаправляемых коммутатором, снимался тег VLANID. Исправив эти настройки, взаимодействие между устройствами стало работать в нормальном режиме. Для того чтобы избежать таких ситуаций, рекомендуем:

- внимательно анализировать, по каким признакам подписчик идентифицирует входящий трафик;
- на стороне подписчика не использовать излишние параметры фильтрации трафика;
- давать обратную связь производителю оборудования.

Присвоение multicast MAC-адресов

Параметр MAC-адрес является еще одним параметром, при помощи которого можно выполнить фильтрацию трафика в сети. Для этого сетевое оборудование имеет функцию MAC Filtering. Также MAC-адрес может применяться для фильтрации входящего трафика на стороне приемника. Стандарт МЭК 61850 описывает рекомендуемые значения для коммуникационных сервисов GOOSE и SV. Но даже с этим параметром бывают проблемы. На своей практике мы столкнулись с интересной ситуацией. В этом примере использовалось оборудование одного производителя. Получив SCD-файл, была начата процедура импорта конфигураций в устройства. ICT производителя успешно выполнил валидацию файла и принял конфигурации своих устройств. Далее был выполнен импорт конфигураций в сами устройства. На этом этапе никаких сообщений об ошибке не выдавалось. Но в ходе проверки прохождения GOOSE-сообщений обнаружилось, что подписчик не видит входных данных. И в этой ситуации потребовалось немало времени, чтобы обнаружить проблему. Проблема заключалась в том, что все GOOSE-сообщения в SCD файле имели

MAC address, значение которого не соответствовало рекомендуемому стандартом МЭК 61850. Рекомендуется для GOOSE-сообщений в качестве 4 октета MAC-адреса указывать значение 01, а было задано 11. Подписчик обращал на это внимание и отбрасывал кадр как не соответствующий разрешённому пулу. После корректировки MAC-адресов система начала функционировать исправно. Возникает вопрос: почему об этом стало известно на таком позднем этапе? Факторов было несколько:

- устройства одного производителя по-разному реагировали на MAC-адрес вне рекомендуемого пула. Публикатор допускал формирование такого GOOSE, но подписчик реагировал на это негативно;
- ICT производителя не сообщал об этом и допускал задавать такие MAC-адреса как со стороны отправителя, так и со стороны приемника;
- отбрасывать такие MAC-адреса является некорректной реакцией приемника, так как допустимый пул MAC-адресов является **рекомендуемым**.

Если с первыми двумя пунктами все ясно (проблема кроется в реализации ПО производителей), то третий пункт вызывает особый интерес.

Annex B
(informative)

Multicast address selection

In order to increase the overall performance of multicast message reception (e.g. GOOSE, and sampled values), it is preferable to have the Media Access Control (MAC) hardware perform the filtering. The hash algorithms in the various integrated circuits do vary. It is recommended, as a system integrator, to evaluate the impact of these algorithms when assigning destination multicast addresses.

Vendors of IEC 61850-8-1 implementations that send these types of messages should provide recommendations of addressing based upon the MAC IC's hash algorithms. One such recommendation might appear as follows:

The multicast addresses (octet string of size 6) used within this standard shall have the following structure:

- The IEEE standardized MAC address format for multicast assigns the two bits in the first octet to represent multicast, broadcast or unicast. The first bit transmitted shall be set to a value of 1 indicating multicast. The second bit transmitted shall be set to a value of zero (0) indicating not broadcast.
- It is recommended that the second and third octets have a value of 0C-CD.
- The fourth octet should be 01 for GOOSE, 02 for GSSE, and 04 for multicast sampled values.
- The value of 00-00-00-00-00-00 shall be used to indicate that the multicast address has not been configured.
- The last two octets should be used as individual addresses assigned by the range defined in Table B.1.

Table B.1 – Recommended multicast addressing example

Service	Recommended address range assignments	
	Starting address (hexadecimal)	Ending address (hexadecimal)
GOOSE	01-0C-CD-01-00-00	01-0C-CD-01-01-FF
GSSE (deprecated)	01-0C-CD-02-00-00	01-0C-CD-02-01-FF
Multicast sampled values	01-0C-CD-04-00-00	01-0C-CD-04-01-FF

Рис. 7. Рекомендуемый пул MAC-адресов.

В соответствии со стандартом МЭК 61850-8-1 первый октет multicast GOOSE/SV обязательно должен иметь значение 01. Обязательность этого совершенно оправдана, значение 1 говорит сетевому оборудованию что данный Ethernet-кадр multicast. Второй и третий октет рекомендуется указывать как 0C-CD. Тут стоит обратить внимание на **рекомендацию**. Это значит, что GOOSE/SV могут иметь MAC-адрес вне определенного пула. Четвертый октет **рекомендуется** указывать как 01 для GOOSE и 04 SV. И тут обращаем внимание, что это **рекомендация.** С последними двумя октетами история аналогична. Стоит обратить внимание что таблица B.1 имеет имя столбца «**Recommended** address range assignments». Избежать это можно, только получив опыт конфигурирования устройств, поэтому перед началом работ стоит проверить устройства в части обмена GOOSE/SV.

Синхронизация времени и работа защит

Последней темой, рассматриваемой в данном докладе, является вопрос синхронизации SV и реакция устройств РЗА на тип синхронизации SV. Эта проблема выделена в отдельную тему, так как с этим приходится сталкиваться часто. В соответствии со стандартом МЭК 61850-9-2, устройства, осуществляющие формирование данных при помощи коммуникационного сервиса SV, должны быть синхронизированы по времени. Индикацией того, что устройство синхронизировано, является флаг SmpSynch. Флаг SmpSynch может принимать три значения.

SmpSynch	INT8U	Indicates how the sampled values sent by the **SVCB** are synchronized by clock signals: 0 = **SV** not synchronized by an external clock signal; 1 = **SV** synchronized by a local area clock signal; 2 = **SV** synchronized by a global area clock signal; 3 to 255 = Reserved values – Do not use. Note: SampledValue publisher compliant with previsous versions of this standard may have used the value 5 to 254. Please refer to the backward compatibility annex of IEC 61850-9-2.	M

Рис. 8. Состояния флага SmpSynch.

Для уточнения дадим расшифровку каждого значения:

- SmpSynch = 2: устройство получает синхронизацию с хорошим сигналом от спутников GPS/Глонасс;
- SmpSynch = 1: устройство получает синхронизацию от внутренних часов сервера времени. Данный режим активируется, если сервер времени имеет плохой сигнал от спутников GPS/Глонасс;
- SmpSynch = 0: сервер времени отсутствует в сети, или синхронизация не доходит до устройства.

В связи с тем, что режимы синхронизации в составе SV-потока могут быть разными, каждый производитель РЗА строит свой алгоритм работы в каждом режиме. Порой алгоритмы работают слишком грубо. В чем это проявляется? Рассмотрим пример из нашего опыта. В ходе наладки на объекте имелось устройство РЗА, которое получало измерения от ПАС при помощи SV-потока. На тот момент не были сконфигурированы серверы времени из-за чего все SV-потоки имели SmpSynch = 0. Когда пришло время проверять вторичные функции РЗА, обратили внимание, что устройство не реагирует на превышение токовых значений КЗ. Для того чтобы разобраться, в чем дело, было

принято решение о симуляции SV-потоков от испытательной установки. Симулированные SV-потоки подавались с SmpSynch = 2, на тот момент мы не обратили на это внимания. Устройство начало корректно работать, воздействуя на выключатель. После долгих изысканий флаг SmpSynch симулируемого SV-потока был переведен в значение 1 – защита работала. После перевели флаг SmpSynch в значение 0 и обнаружили, что ни одна вторичная функция защиты не работала. Терминал РЗА вывел абсолютно все защиты из работы из-за флага SmpSynch = 0. На первый взгляд такая реакция кажется корректной, но это не так. Такая реакция устройства актуальна только в том случае, если выводится дифференциальная защита, дистанционная защита или направленная защита. Это связано с тем, что для подобных защит в качестве исходной информации могут использоваться SV-потоки от разных ПАС, а это может привести к ложному срабатыванию защит. Простые защиты, которым достаточно иметь SV-поток от одного источника, выводиться не должны. К этим защитам можно отнести ТО, МТЗ, ТЗНП, ЗМН и т. д.

На вопрос, как решить проблему подобного рода, ответ дан в самом описании. Для того чтобы избегать таких ситуаций, советуем на ранних этапах наладки озаботиться вопросом настройки серверов времени или использованием испытательных установок. Стоит учесть, что подобные проблемы могут быть устранены самим производителем, достаточно дать обратную связь.

Итог

Из нашего опыта можно сделать вывод, что можно потратить много времени на выяснение причин, получить хороший опыт и глубоко разобраться в проблеме, но так и не найти ответа. В особо сложных случаях единственно правильным вариантом будет обращение к производителю. Порой ответственность за качество и скорость выполнения работ должен брать на себя наладчик. О какой ответственности идет речь? В первую очередь это подготовка к наладке, которая проявляется в следующем:

- анализ проекта SCD;
- сбор и обновление нужных программных инструментов;
- приобретение опыта в работе с ICT;
- анализ возможностей используемых устройств в проекте;
- тестирование устройств с моделированием рабочих режимов;
- анализ положений стандарта МЭК 61850 в спорных и сложных ситуациях.

Данный список хоть и содержит краткую информацию, но содержит важные основы успешного выполнения наладки – вся основная работа может быть выполнена заранее. Мы уверены, что этот доклад принесет что-то новое в существующий багаж знаний или поможет решить существующую проблему.

1.21. КРОСС-ПЛАТФОРМЕННЫЕ РЕШЕНИЯ ДЛЯ РЗА ЦПС

А.А. ВОЛОШИН, Е.А. ВОЛОШИН, А.С. ХОЛОДОВ, Е.И. РОГОЗИННИКОВ, А.К. РЫЖКОВ

Центр НТИ МЭИ

Российская Федерация

Контактное лицо:

А.А. ВОЛОШИН

voloshinaa@mpei.ru

Ключевые слова: Архитектура устройств РЗА, виртуализация, виртуальная РЗА.

Введение

В настоящее время в мировой энергетике идет тренд по внедрению цифровых подстанций, которые главным образом основываются на стандарте МЭК 61850. Возможны несколько архитектур построения комплекса РЗА (децентрализованная, централизованная и гибридная), которые отличаются от традиционных, обладают различными показателями стоимости, надежности и живучести. Существующий функционал, заложенный в современные устройства РЗА, может быть недостаточен для построения подобных архитектур. В данном докладе пойдет речь о внутренней структуре устройств РЗА, о том, как её необходимо изменить для обеспечения совместимости с данными архитектурами.

Основная часть

При классическом построении комплекса РЗА на подстанции функции релейной защиты разделяются на основные и резервные. Их, как правило, помещают в одно устройство (пример – уРЗА защиты линии), а для обеспечения надежности данные устройства дублируют.

Практически во всех современных устройствах РЗА имеется операционная система (UNIX-подобная), и их можно представить как специализированный промышленный компьютер с набором приложений (функций РЗА). С современным уровнем развития вычислительной техники у подобных устройств достаточно мощности для того, чтобы разместить в них сразу несколько приложений-функций (централизованная архитектура). В таком подходе существует единая платформа для запуска и обработки приложений, что является уязвимым местом в системе. Необходимо обеспечить изоляцию работы приложения для того, чтобы выход из строя одного не приводил к выходу из строя остальных.

Выделены три основных подхода для построения внутренней архитектуры устройства.

В первом подходе часть приложений (основные и резервные защиты присоединения) помещаются в вычислительный контейнер, в котором обеспечивается ограничение в используемых ресурсах (ОЗУ, ЦПУ, LAN). Для построения необходимы платформа РЗА, которая будет управлять данными контейнерами и следить за их состоянием, а также средний уровень ОС (middleware), который будет обеспечивать связь между контейнерами. Контейнеризация существенно увеличивает надежность, но в такой структуре уязвимым местом является средний уровень.

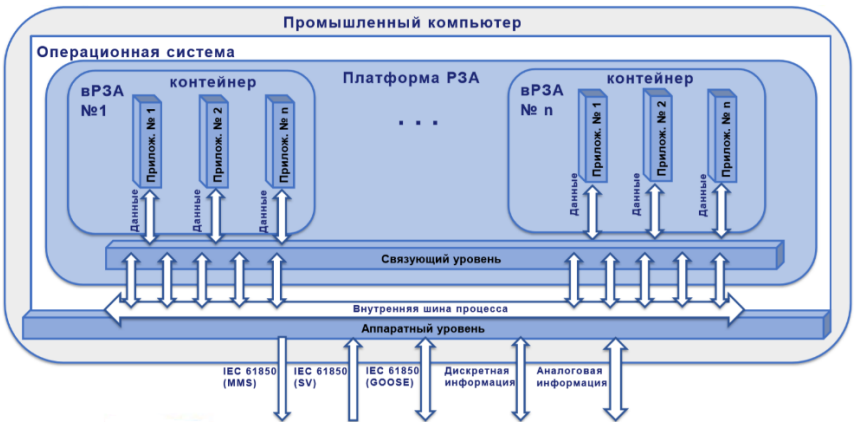


Рис. 1. Архитектура РЗА с применением технологий контейнеризации.

Во втором подходе предлагается использовать виртуализацию – внутри основной операционной системы создаются виртуальные машины, в которых эмулируется поведение дополнительных операционных систем. Данный подход позволяет реализовать «виртуальный терминал РЗА» любого производителя РЗА, причем внутри одного устройства могут быть терминалы разных производителей одновременно. Данный подход обеспечивает более высокую степень изолированности, поскольку производит полную эмуляцию ОС. Минусом является высокое потребление вычислительных ресурсов устройства из-за больших накладных расходов на виртуализацию. В ходе исследований выявлено, что существует предельное число виртуальных машин, при котором обеспечивается устойчивость работы системы в целом. Превышение данного числа может привести к отказу функционирования всех виртуальных устройств.

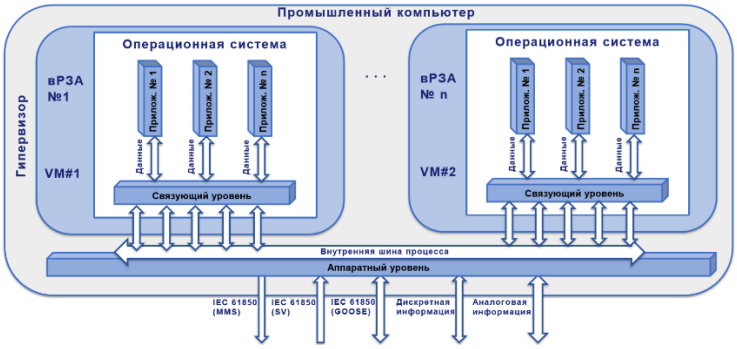


Рис. 2. Архитектура РЗА с применением технологий виртуализации.

В третьем (гибридном) подходе предлагается обеспечить физическую изоляцию функций РЗА путем построения модульной архитектуры устройства. Каждый модуль является аналогом отдельного устройства РЗА. Рассмотрев все сервисы внутри одного устройства, можно заметить, что лишь часть из них требует обеспечения режима жесткого реального времени. Одним из главных преимуществ данной архитектуры является оптимальное использование вычислительных ресурсов путем физической группировки сервисов, требующих обработки данных в режиме реального времени и без него. Единственным минусом является повышение стоимости устройства РЗА, имеющего такую архитектуру.

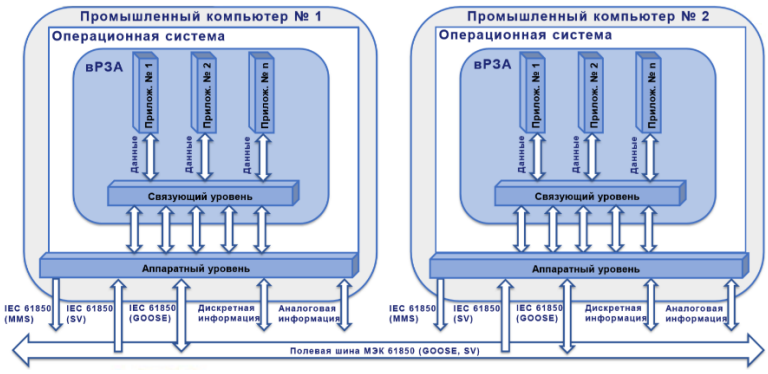


Рис. 3. Архитектура РЗА с модульным построением.

С появлением дополнительной абстракции в виде виртуального устройства РЗА (контейнеризация, виртуализация, физической разделение) возникает несоответствие с текущей структурой устройств РЗА, описанной стандартом МЭК 61850. Программное либо аппаратное выделение устройства РЗА в дополнительный уровень по своему функционалу является физическим уровнем (Physical Device – Named IED). Таким образом, можно сказать, что переход на новую архитектуру в настоящее время невозможен, поскольку в текущей реализации стандарта нет термина для описания дополнительной (виртуальной, физической) прослойки.

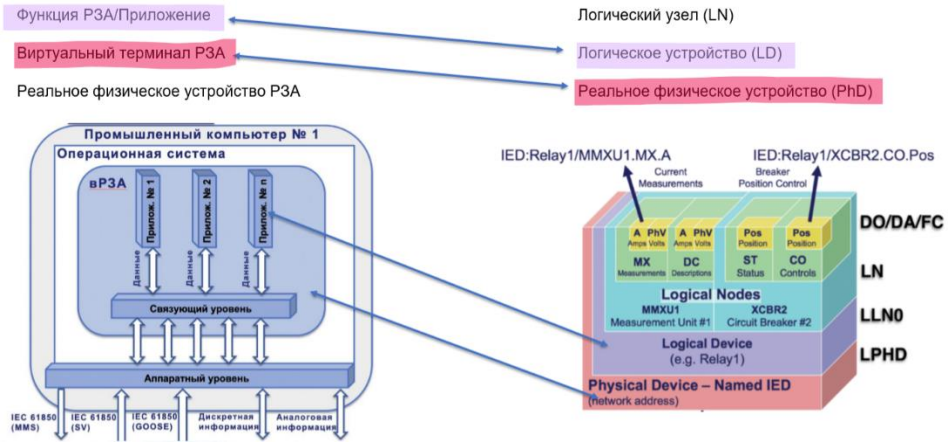


Рис. 4. Связь новой архитектуры с текущей версией стандарта МЭК 61850.

При использовании дополнительных уровней абстракции в построении новой архитектуры РЗА возникает закономерный вопрос: допустимо ли использовать технологии контейнеризации и виртуализации с точки зрения выполнения вычислений в режиме Real-Time? Для исследования этого вопроса были произведены опыты с применением отечественных и иностранных устройств РЗА. Была собрана модель реального времени в ПАК RTDS, и для данных устройств производились опыты коротких замыканий при различных углах токовых сигналов. В сумме для каждого устройства было произведено около 64 000 коротких замыканий, статистика по результатам представлена на рисунке 5.

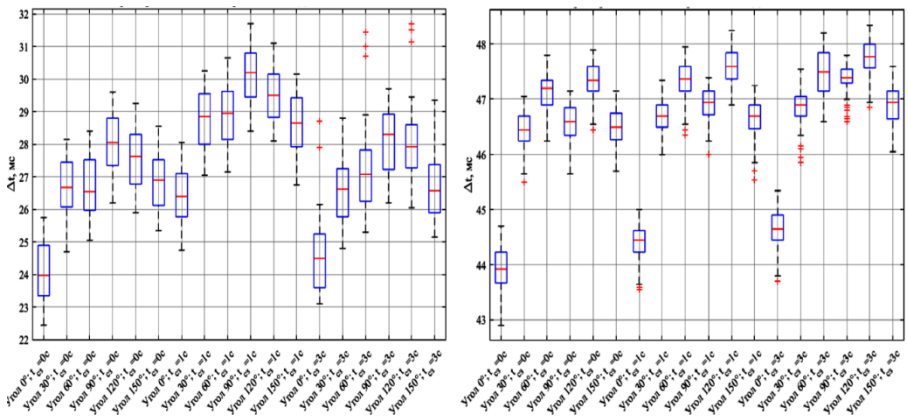


Рис. 5. Статистика по времени срабатывания устройств РЗА (слева – отечественный терминал, справа - иностранный).

По статистике разброса времени срабатывания, для каждого опыта мы видим разброс во времени ±10 мс, что по факту для процессоров, производящих вычисления в режиме Real-Time, является «Вечностью». Также на диаграмме видны аномальные выбросы по времени срабатывания (красные крестики).

Производились опыты по исследованию влияния частоты дискретизации на работу фильтра Фурье, который применяется во всех современных терминалах РЗА. Здесь дополнительно стоит сказать об избыточности передаваемых данных по стандарту МЭК 61850 Sampled Values, поскольку уменьшение частоты расчета фильтров практически не влияет на изменение времени срабатывания устройств. У большинства производителей вычисления производятся с частотой 1 кГц, что в 4 раза реже данных, которые передаются по стандарту.

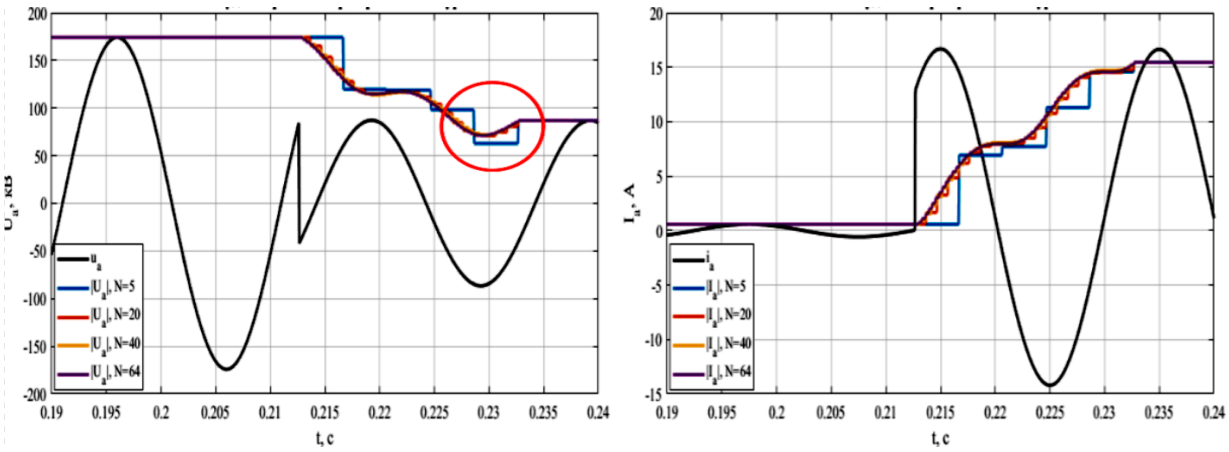


Рис. 6. Амплитуды преобразования Фурье напряжения и тока при количестве выборок N = 5, 20, 40, 64.

Исходя из рассмотренных выше результатов, можно сделать вывод, что при реализации архитектур с применением технологий контейнеризации и виртуализации допустимо в вычислениях использование режима «мягкого реального времени». В наших исследованиях это не приводит к увеличению времени срабатывания РЗА. Применение «жесткого реального времени» должно приводить к гарантированному и быстрому срабатыванию с минимальным разбросом, что не наблюдается в существующих терминалах. Следует отметить, что применение «жесткого реального времени» в вычислениях ведет к небольшому увеличению нагрузки на CPU вследствие увеличения количества контекстных переключений. Усложнение аппаратной и программной архитектуры только для обеспечения «жесткого реального времени» бессмысленно.

Для исследования внутренних архитектур были проведены опыты для второй и третьей архитектуры. Использовался промышленный компьютер с процессором Intel core I7, 16 гб ОЗУ. По второй архитектуре выявлено предельное количество виртуальных машин, при котором обеспечивается устойчивость всей системы, – 16 шт. Добавление новых виртуальных машин ведет к нелинейному увеличению нагрузки. В ходе опыта загрузка ЦПУ превысила 80%. Дальнейшее увеличение числа виртуальных машин приводит к непредсказуемому поведению функций РЗА. В

ходе опыта выявлена необходимость проработки возможностей «мягкого» пуска виртуальных машин, поскольку во время старта наблюдается значительное увеличение нагрузки на CPU.

При испытании гибридной архитектуры было запущено 64 функции РЗА в рамках одного устройства. Нагрузка на ЦПУ при этом составила всего 30 %. Увеличение числа функций РЗА в данной архитектуре ведет к линейному увеличению нагрузки на ЦПУ, что свидетельствует об оптимальном распределении сервисов по отдельным модулям.

В обеих архитектурах время срабатывания функций релейной защиты варьировало в пределах 5–20 мс.

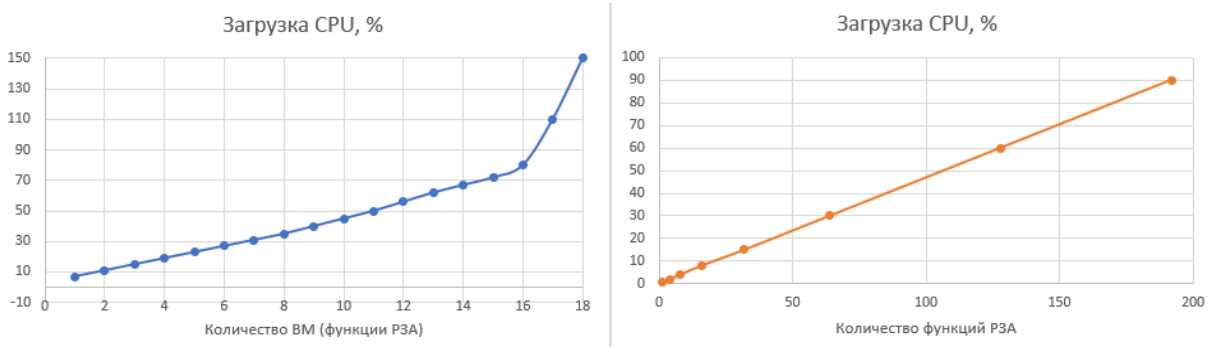


Рис. 7. Нагрузка на CPU в зависимости от количества запущенных функций РЗА при различных архитектурах (применение виртуализации – слева, гибридная архитектура – справа).

Заключение

Все три архитектуры могут быть использованы в современных терминалах РЗА, так как обеспечивают необходимые требования к самим функциям РЗА, включая время срабатывания.

При разработке новых устройств РЗА рекомендуется использовать гибридную архитектуру, поскольку она обеспечивает оптимальное распределение нагрузки по отдельным сервисам и высокий уровень надежности.

Текущая версия стандарта не позволяет описать все аспекты новой архитектуры.

Литература

[1] IEC 61850 Standard

1.22. ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ АВТОМАТИЗАЦИИ ФУНКЦИОНАЛЬНЫХ ИСПЫТАНИЙ СИСТЕМ РЗА ЦПС

А. А. ЛЕБЕДЕВ, Д. О. БЛАГОРАЗУМОВ

Федеральное государственное бюджетное образовательное учреждение «Национальный исследовательский университет «МЭИ»

Российская Федерация

Контактное лицо:

А. А. ЛЕБЕДЕВ

LebedevAndA@mpei.ru

Ключевые слова: Релейная защита и автоматика, цифровая подстанция, интеллектуальное электронное устройство, МЭК 61850, испытания, виртуализация, облачные технологии, виртуальная лаборатория.

Введение

Нарастающее применение цифровых технологий в системах релейной защиты и автоматики (РЗА) цифровых подстанций (ЦПС), несомненно, позволяет реализовывать все более сложные и нестандартные технические решения по защите и управлению энергообъектами. Благодаря цифровым способам преобразования сигналов и передачи информации, многие функции, выполняемые микропроцессорными устройствами РЗА, преобразуются в достаточно комплексные и сложные наборы алгоритмов. Наряду с этим существенно расширяются и усложняются требования нормативных технических документов, возрастает степень их детализации и контроля исполнения. Все это приводит к необходимости включения производителями цифровых устройств РЗА дополнительных условий, ограничений и проверок в базовые, уже устоявшиеся алгоритмы релейной защиты, автоматики и управления для их соответствия требованиям не только общих нормативно-технических документов, но и корпоративных стандартов.

Очевидно, что представленные в совокупности факторы требуют контроля и подтверждения разрабатываемых проектных технических решений, а также мониторинга и проверки работоспособности комплекса устройств релейной защиты и управления на этапе пусконаладочных работ (ПНР) и в процессе эксплуатации. В настоящее время традиционный подход к проведению подобных комплексных испытаний является достаточно трудоемким и технически сложным процессом, включающим в себя целый ряд мероприятий: создание модели объекта защиты и управления и окружающего его фрагмента энергосистемы, подключение к модели и испытательному оборудованию реальных устройств релейной защиты и управления, формирование набора соответствующих тестовых сценариев, проведение самих испытаний с моделированием подготовленных сценариев и режимов, обработку результатов испытаний, выполнение корректирующих мероприятий (при необходимости), формирование отчетных документов.

Эффекты и возможности цифровых технологий при их комплексном и разумном применении, как правило, носят всесторонний характер, что подтверждается реализацией цифровых виртуальных устройств, адекватных цифровых моделей реального времени и даже цифровых двойников, имитирующих поведение сложных технологических процессов. Благодаря высокому современному уровню развития цифровых технологий, возможно создание многофункциональных виртуальных лабораторий, обладающих всем необходимым инструментарием для тестирования и отладки различного программного обеспечения. Такие решения, построенные на облачных сервисах, используются в ИТ-индустрии уже достаточно давно и зарекомендовали свою значимость в задачах автоматизации проверок и выявления каких-либо ошибок и негативных закономерностей в работе тестируемых программных продуктов. Аналогичным образом, используя инструменты специализированной виртуальной лаборатории, могут быть выполнены и испытания функционального программного обеспечения устройств РЗА, если последние будут представлены в виде комплекса виртуальных интеллектуальных электронных устройств. Такой подход обеспечит снижение затрат на создание сложного испытательного комплекса и вспомогательной периферии и сокращение времени на проведения самих испытаний благодаря возможности их полной автоматизации.

Основная часть

Отмеченные выше тенденции применения и развития цифровых технологий по своему определению призваны обеспечить упрощение задач проектирования, а также типизацию

технических решений по защите и управлению для энергетических объектов. Между тем, накопленный на сегодня опыт фактически свидетельствует о постепенном снижении степени детализации разрабатываемых проектных решений и усложнению таким образом самой формы их представления, что в конечном счете значительно затрудняет их восприятие, анализ и контроль на предмет соответствия действующим нормам и правилам. Затруднительным становится также контроль функционального взаимодействия различных устройств РЗА не только на уровне межобъектных связей, но даже на уровне единого энергообъекта. Очевидно, что внедрение проектных решений без их предварительного апробирования и проведения комплексных испытаний сопряжено с определенными рисками, связанными не только с увеличением сроков ввода объекта в эксплуатацию, но и с возникновением нештатных и аварийных ситуаций из-за неправильной работы систем РЗА уже в процессе самой эксплуатации энергообъекта.

Важно отметить, что проведение стандартных и типовых заводских испытаний отдельных функций и компонентов систем релейной защиты, автоматики и управления, проводимых посредством индивидуальных испытательных комплексов и фрагментарных ограниченных моделей энергообъекта, является недостаточным. Подход по подтверждению и верификации правильности и функциональной целостности проектных технических решений должен быть комплексным и учитывать требования не только технического задания, но и действующих нормативно-технических документов.

С ростом количества оборудования РЗА, применяемого на цифровой подстанции, и повышением степени его «цифровизации» возрастает число и самих испытаний, которые необходимо выполнять для анализа правильности работы тестируемого оборудования и системы в целом, усложняются и методики проведения испытаний, повышаются требования к функциональным возможностям испытательных комплексов. В современных условиях испытания цифровых комплексов РЗА следует обеспечивать не только проведением комплексных испытаний с использованием полного состава испытываемого оборудования, но и применением цифровой модели реального времени объекта защиты и управления. При этом внесение изменений в параметры работы модели электроэнергетического объекта, регулярная необходимость корректировки настроечных параметров оборудования РЗА, а также появление новых сценариев тестирования и режимов работы энергообъекта приводят к многократному повторению испытаний.

Вместе с тем, текущий уровень развития программно-аппаратных средств РЗА и наметившиеся мировые тенденции к универсальности их исполнения наравне с расширением применения цифровых технологий открывают новые возможности для автоматизации процессов проведения их испытаний и комплексной диагностики в процессе эксплуатации. Применение универсальных программно-аппаратных платформ приводит к исключению или частичному ослаблению зависимости в реализации определенного набора функций РЗА от типа и производительности выбранной платформы интеллектуальных электронных устройств (ИЭУ). Преимущества такого исполнения несомненны и позволяют выполнить необходимые функции систем РЗА без каких-либо существенных ограничений технической реализации самой программно-аппаратной платформы. Наиболее существенным требованием при этом, кроме производительности самого микропроцессора чувствительной к степени сложности алгоритмического обеспечения РЗА, является развитость периферии и цифровых коммуникационных интерфейсов. Независимость исполнения функционального (алгоритмического) обеспечения релейной защиты, автоматики и управления от аппаратной части и базового программного обеспечения делает возможным его

отделение от реальных физических устройств. Это означает, что разработанное в соответствии с проектными решениями функциональное программное обеспечение может быть инкапсулировано в виде отдельной самостоятельной сущности, в том числе виртуальной, для его проверки и проведения испытаний с использованием инструментов виртуализации и облачных сервисов. Безусловно, подобные решения должны обеспечивать сохранение уникальной информационной модели каждого ИЭУ, соответствующей стандарту МЭК 61850. При этом само аппаратное обеспечение также может быть подвержено соответствующим испытаниям, гарантирующим его исправность и надежность.

Приведенные в совокупности факторы позволяют пересмотреть и в некоторой степени обновить применяемые методы к проведению функциональных испытаний комплексов релейной защиты, автоматики и управления цифровых подстанций. Представление функций РЗА ЦПС в виде отдельных и независимых, но в то же время самодостаточных цифровых сущностей, а также широко применяемые в сфере ИТ инструменты виртуализации и облачных сервисов могут обеспечить проведение комплексных испытаний функционального обеспечения РЗА не только для отдельных устройств, но для системы в целом, учитывая при этом все необходимые взаимодействия и влияния. При самом первом приближении предлагаемый подход можно рассматривать аналогично реальным физическим испытательным полигонам. Для проведения испытаний в виртуальной лаборатории имитируется вся необходимая цифровая инфраструктура: виртуальные сетевые коммутаторы, виртуальные устройства синхронизации времени, виртуальные серверы и АРМ и т. д.

В общем виде виртуальная испытательная лаборатория для тестирования функционального (алгоритмического) обеспечения устройств релейной защиты, автоматики и управления цифровых подстанций может быть представлена модульной структурой на рис. 1.

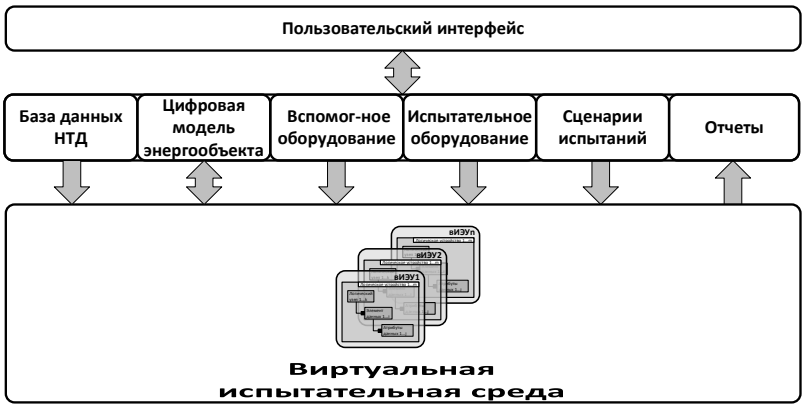


Рис. 1. Упрощенная модульная структура виртуальной лаборатории.

Основное назначение модулей виртуальной испытательной лаборатории следующее:

- виртуальная испытательная среда – модуль виртуальной среды, обеспечивающий запуск и выполнение виртуальных экземпляров вспомогательных и тестируемых устройств и проведение самих испытаний;

- база данных НТД – база знаний, предназначенная для хранения и поддержания в актуальном состоянии технической информации, требований и ограничений в форме онтологий;
- цифровая модель энергообъекта – модуль, симулирующий режимы основного технологического оборудования;
- вспомогательное оборудование – модуль виртуализации оборудования вспомогательной инфраструктуры;
- испытательное оборудование – наборы программных инструментов для настройки методов и режимов испытаний;
- сценарии испытаний – модуль, содержащий наборы тестовых сценариев и хранящий правильную последовательность их запуска и проведения, а также информацию о режимах работы основного технологического оборудования;
- отчеты – модуль, обеспечивающий формирование отчетных результатов выполнения испытаний;
- пользовательский интерфейс – модуль, обеспечивающий взаимодействие с пользователем, настройку и управление процессом испытаний.

Если рассматривать структуру виртуальной испытательной лаборатории как законченный облачный сервис с подготовленной разработчиком и настроенной пользователем испытательной инфраструктурой, то наибольшее значение имеет вопрос интеграции самого «предмета» испытаний. В зависимости от назначения и степени сложности выполняемых виртуальной лабораторией функций тестирования, может быть осуществлено два механизма интеграции тестируемого функционального (алгоритмического) обеспечения систем РЗА: в виде полностью сконфигурированных исполняемых файлов аналогично исполняемым в реальных физических ИЭУ, а также в виде конфигурационных тестовых файлов, например, в формате XML.

Выбор способа интеграции определяется также требованиями к объему проводимых испытаний. Так, например, для типовой проверки структуры и синтаксиса конфигурационных файлов устройств РЗА, также являющихся частью их функционального (алгоритмического) обеспечения, на соответствие стандарту МЭК 61850 в виртуальную лабораторию достаточно загрузить только электронные файлы в формате SCL – файлы с расширением *.iid, *.icd и *.cid. На основании информации, содержащейся в данных файлах, а также используя требования НТД, могут быть сделаны выводы о функциональной достаточности тестируемого алгоритмического обеспечения устройств РЗА защиты и управления определенным энергообъектом. Для тестирования взаимодействия устройств РЗА по стандарту МЭК 61850 дополнительно могут быть загружены конфигурационные файлы с расширением *.scd и *.sed. Между тем, известно, что стандарт МЭК 61850 не регламентирует требования к реализации свободно программируемой логики цифровых устройств релейной защиты, автоматики и управления, с использованием которой может быть реализована существенная часть их функционального (алгоритмического) обеспечения. В таком случае для проведения комплексных автоматизированных функциональных испытаний систем РЗА на базе виртуальной лаборатории требуется полноценная интеграция программного образа функционального (алгоритмического) обеспечения устройств РЗА в виде их исполняемых файлов.

По своему назначению виртуальная испытательная лаборатория может быть использована на всех основных этапах жизненного цикла систем РЗА ЦПС. В случае применения инструментов виртуальной лаборатории для комплексного анализа и тестирования проектных решений,

безусловно, должна осуществляться не только формальная проверка соответствия синтаксиса информационной модели устройств РЗА стандарту МЭК 61850, но и подтверждение разработанных технических решений действующим нормам и правилам. Наличие в виртуальной лаборатории цифровой модели электроэнергетического объекта или возможность интеграции с таковой делает доступным проведение автоматических проверок систем РЗА при различных режимах работы и самого энергообъекта. По набору предварительно заданных сценариев могут быть проверены рассчитанные уставки устройств РЗА, отработаны проектные алгоритмы сетевой и противоаварийной автоматики. Выводы о корректности или некорректности результатов проверок могут выполняться на основе состава сигналов, полученных от виртуальных сущностей устройств РЗА, интегрированных в виртуальную испытательную среду, с фиксацией времени их возникновения и последовательности и последующего сравнения с предварительно сформированными эталонными перечнями сигналов. Данные перечни сигналов должны соответствовать правильному поведению цифровой модели энергообъекта в различных режимах и быть получены на основе результатов работы алгоритмов логического вывода из базы знаний и анализа электрической схемы энергообъекта. При необходимости эталонные перечни сигналов могут быть верифицированы пользователем вручную. Кроме того, в качестве дополнительного инструмента анализа правильности проектных технических решений могут использоваться осциллограммы аварийных и нештатных режимов работы.

Для возможности внесения изменений в проектные решения систем РЗА при проведении проверок их работоспособности и соответствия требованиям нормативно-технической документации виртуальная испытательная лаборатория может обладать дополнительными инструментами системы автоматического проектирования (САПР). Такие функции должны обеспечивать синтаксическую корректировку SCL-файлов по стандарту МЭК 61850, правильный подбор значений уставок срабатывания и исправление алгоритмов взаимодействия комплекса устройств РЗА по цифровым коммуникационным интерфейсам, в том числе и межобъектного взаимодействия. Протестированное и при необходимости скорректированное посредством инструментов САПР функциональное (алгоритмическое) обеспечение РЗА, разработанное на стадии проектирования, таким образом может быть полностью подготовлено для реализации в реальных физических устройствах.

Применение инструментов виртуальной испытательной лаборатории может быть распространено и на последующие стадии жизненного цикла цифровых комплексов РЗА для осуществления непрерывного мониторинга их работоспособности и выявления и анализа отклонений в работе или проверки правильности функционирования в нештатных режимах. При переходе к этапу ПНР функции виртуальной лаборатории могут быть применены для выверки и сравнения функционирования уже установленного и налаженного реального комплекса устройств РЗА с его цифровой моделью (цифровой «двойник»), запущенной посредством инструментов виртуальной лаборатории. Подход к осуществлению вывода о корректности или ошибках функционирования цифровых устройств РЗА должен быть аналогичен применению виртуальной испытательной лаборатории на стадии проектирования. Многократные испытаний также могут быть автоматизированы посредством сравнения с эталонными перечнями сигналов и осциллограмм, соответствующих цифровой модели системы РЗА, верифицированной, например, при проверках на стадии проектирования.

В процессе эксплуатации систем РЗА ЦПС инструменты виртуальной испытательной лаборатории могут быть также использованы для анализа и проверки правильности работы

системы при срабатывании устройств защиты, автоматики и управления, изменении режимов работы энергообъекта или возникновении нештатных и аварийных ситуаций. Сформированные реальными физическими устройствами РЗА перечни сигналов и файлы осциллограмм могут быть интегрированы в виртуальную среду для воспроизведения исследуемого режима работы и диагностики функционирования системы РЗА в каждом анализируемом случае. Существенной особенностью данной стадии является возможность использования виртуальной лаборатории в режиме реального времени для мониторинга функционирования физического комплекса цифровых устройств РЗА. Кроме того, дополнительным преимуществом стадии эксплуатации может являться возможность использования результатов анализа накопленных данных о функционировании работы комплекса РЗА и возможностей предиктивной аналитики для выявления каких-либо закономерностей и оценки работы функций защиты, автоматики и управления при их анализе. Отмеченное в целом может способствовать исключению повторяющихся ошибок в работе комплекса устройств РЗА или сокращению аварийных ситуаций энергообъекта, благодаря своевременным корректировкам функционального (алгоритмического) обеспечения цифровых устройств РЗА, которые также предварительно могут быть апробированы в виртуальной испытательной среде.

Для применения всех представленных возможностей инструментов виртуальной испытательной лаборатории на стадиях пусконаладочных работ и эксплуатации комплекса цифровых устройств РЗА требуется промежуточный модуль интеграции с облачными сервисами, который может представлять собой специализированное устройство, обеспечивающее данное сопряжение или реализующее облачные сервисы локально.

Немаловажным является также отметить обязательную автоматизацию процесса формирования отчетной документации по результатам проведенных тестов функционального (алгоритмического) обеспечения устройств релейной защиты, автоматики и управления в виртуальной испытательной лаборатории.

Заключение

Таким образом, применение виртуальных инструментов, построенных на механизмах облачных сервисов, для автоматизации испытаний, дистанционной проверки правильности работы и диагностики систем защиты, автоматики и управления цифровых подстанций позволит осуществлять комплексную проверку и контроль работоспособности систем РЗА на всех стадиях жизненного цикла при существенной минимизации затрат, благодаря исключению необходимости организации реальных испытательных полигонов.

СЕКЦИЯ 2.

«Перспективы развития и применения стандарта МЭК 61850»

2.1. ПРОВЕРКА ЭЛЕКТРОННОЙ ПРОЕКТНОЙ ДОКУМЕНТАЦИИ В ФОРМАТЕ ФАЙЛОВ SCD ДЛЯ ЦИФРОВЫХ ПОДСТАНЦИЙ: ТРЕБОВАНИЯ И ПРАКТИЧЕСКИЙ ОПЫТ

А.А. СЕМЕРЕНКО, Д.А.ТРЕТЬЯКОВ, А.В. ГОЛОВИН, А.О. АНОШИН, РОДНИ ХЬЮЕС

ПАО «МРСК Волги», ООО «ТЕКВЕЛ Разработка», Rod Hughes Consulting Pty Ltd

Россия, Австралия

Контактное лицо:

А.В. ГОЛОВИН

gav@tekvel.com

Keywords: МЭК 61850, цифровая подстанция, SCL, SCD.

Аннотация:

Стандарт МЭК 61850 определяет модели данных, коммуникационные сервисы, а также язык и процесс конфигурирования интеллектуальных электронных устройств (ИЭУ). Он определяет три вида программных инструментов для инжиниринга и шесть типов конфигурационных файлов на языке SCL (System Configuration Language), создание которых производится на этапе проектирования. Люди могут читать файлы SCL, но простое чтение не даёт полного и точного понимания работы комплексов РЗА и АСУ ТП.

Существующее инструментальное программное обеспечение для конфигурирования ИЭУ может в определенной степени обеспечивать визуализацию содержимого файлов SCL. Однако большинство таких программ разработано и предназначено для конфигурирования ИЭУ отдельно взятого производителя. Это делает невозможным или существенно осложняет задачу визуализации и проверки файлов SCL для проектов с участием нескольких фирм-производителей. Помимо этого, основные принципы контроля качества призывают к использованию при проверке технических решений инструментов, отличных от тех, которые использовались для разработки технических решений, поскольку последние, как показывает практика, могут создавать и скрывать допускаемые ошибки.

В реализуемых проектах обмен сигналами согласно коммуникационным сервисам GOOSE, Sampled Values и Reports обычно описывается с помощью таблиц Microsoft Word/Excel и структурно-функциональных схем, вручную формируемых специалистами проектных организаций. Данные таблицы чаще всего не соответствуют информационному обмену, описанному в файле SCD (System Configuration Description), также являющимся результатом рабочего проектирования и передаваемом далее на этап выполнения пуско-наладочных работ. Таким образом, работа по выявлению ошибок и их устранению мигрирует на этап выполнения пуско-наладочных работ на объекте и приводит к увеличению сроков ввода объектов в эксплуатацию, что противоречит основным принципам стандарта МЭК 61850 и цифровизации в целом. Складывающаяся ситуация прямо противоречит устоявшейся практике, когда все принципиальные технические решения в части РЗА и АСУ ТП, как результат проектирования, проходят экспертизу у конечного заказчика и системного оператора.

Настоящая публикация описывает основные принципы и практический опыт выполнения проверки файлов электронной проектной документации в виде файлов SCL. Представлены основные требования к визуализации, проверке и детальному анализу обмена данными согласно коммуникационным сервисам стандарта МЭК 61850 на основании файлов SCD. В результате проверок становится возможным валидировать файл SCD на соответствие стандарту МЭК 61850; верифицировать информационный обмен между ИЭУ ЦПС: идентифицировать отсутствующие и избыточные сигналы для передачи; ограничить использование логических узлов общего назначения и убедиться в использовании логических узлов и объектов данных согласно профилю стандарта МЭК 61850; проконтролировать правильность задания коммуникационных и прикладных параметров сообщений и др. Указанное позволяет достичь более высокого технического совершенства комплексов РЗА и АСУ ТП, простоты и удобства их эксплуатации.

Использование языка SCL при проектировании цифровых энергообъектов

Известно, что в отличие от других коммуникационных стандартов для электроэнергетики, стандарт МЭК 61850 определяет язык конфигурирования системы SCL (System Configuration Language), который может быть использован для описания первичной схемы энергообъекта, реализуемых на нем функций, конфигураций ИЭУ и информационного обмена между ИЭУ.

Сегодня язык SCL используется для решения следующих задач:

- описание первичной схемы энергообъекта, состава реализуемых функций на элементах энергообъекта;
- описание моделей данных и функциональных возможностей ИЭУ, привязки функций к ИЭУ;
- описание коммуникационных параметров ИЭУ и информационного обмена между ИЭУ.

Есть еще две возможности, которые дает SCL, широко не используемые в проектах сегодня:

- описание уставок (по сути, является частью описания модели данных ИЭУ, но, являясь опциональным, широко не используется);
- описание программируемой логики, что не определено в [1], но описано в одном из технических отчетов стандарта МЭК 61850.

Упомянутые сценарии использования языка SCL закрывают все аспекты конфигурации ИЭУ. То есть через некоторое время файл SCL может стать единственным файлом конфигурации ИЭУ, что может быть чрезвычайно удобно для использования и версионирования.

Язык SCL и его восприятие человеком

Язык SCL основан на языке разметки Extensible Markup Language (XML). Язык XML может быть использован для описания практически любой структурированной информации. Он определяет набор правил для создания текстовых документов в машиночитаемом формате для того, чтобы исключить человеческий фактор при передаче информации от одного программного обеспечения другому. В то же время XML как текст в некоторой степени остается воспринимаемым человеком, что дает ему возможность проанализировать отдельные разделы файла SCL.

SCL является частным случаем XML, который определяет семантику и синтаксис, применимые для систем автоматизации энергообъектов. Ограничения по структуре и содержанию документа определены схемой языка SCL, которая фиксирует требования к структуре файлов SCL.

На практике файлы SCL, описывающие реальные объекты, могут содержать более миллиона строк кода. Несмотря на то, что файлы могут быть прочитаны человеком, их размер и кодировка делает практически невозможным их интерпретацию, понимание и анализ человеком. К примеру, становится чрезвычайно сложно отследить то, что тот или иной сигнал передается от одного ИЭУ другому, по сравнению с чтением принципиальных электрических схем.



Рис. 1. Фрагмент файла SCL.

Проверка информационного обмена между ИЭУ по МЭК 61850

GOOSE и Sampled Values являются одними из самых значимых коммуникационных моделей стандарта МЭК 61850, которые дают возможность применять цифровые коммуникации в комплексах релейной защиты и автоматики. Передача GOOSE и Sampled Values сообщений производится на канальном уровне в многоадресном режиме с использованием модели «издатель-подписчик», когда на одно публикуемое сообщение может подписаться любое количество ИЭУ [2, 3].

Стандарт МЭК 61850 определяет правила описания публикации GOOSE/Sampled Values сообщений, а также подписки на них. Однако найти соответствующие поля в файле SCL и составить полноценную картину о предусмотренном информационном обмене оказывается чрезвычайно сложно по уже обозначенным причинам. Для того, чтобы решить эту проблему многие инженеры вручную создают таблицы, где отражаются публикации сообщений и подписки на них.

Создание таких таблиц имеет ряд существенных недостатков:

- при создании вручную таблицы могут содержать ошибки;
- отсутствие возможности быстрого обзора параметров сообщений и состава наборов данных;
- сложность анализа и поддержки при большом количестве ИЭУ в проекте;
- отсутствие возможности для автоматизации проверок.

При наличии около ста ИЭУ в проекте оказывается крайне непросто верифицировать конфигурацию, используя табличную форму.

Даже в том случае, если подобные таблицы или иная сопроводительная документация формируется системами автоматизированного проектирования по условиям стандарта МЭК 61850, разумным является использование сторонних инструментов для верификации файлов SCL, в которых не производилось их создание, поскольку сами САПР могут также вносить ошибки. Проверка результатов выполненных работ с использованием независимых инструментов является одним из основных принципов контроля качества.

Все указанное применительно к GOOSE и Sampled Values коммуникациям также относится и к отчётам (Reporting) – коммуникационной модели, обеспечивающей передачи телеинформации в АСУ ТП энергообъекта.

Отсутствие возможности выполнить полноценную проверку файла SCD на этапе проектирования влечет за собой серьёзные проблемы на этапах пуско-наладочных работ и эксплуатации энергообъекта. Эти проблемы приводят к увеличению сроков ввода объектов в эксплуатацию и неправильной работе РЗА в эксплуатации, в том числе при выполнении операций технического обслуживания.

Валидация файлов SCL

Валидация является базовым и обязательным этапом проверки электронной проектной документации на языке SCL. Как уже упоминалось, синтаксис и структура файлов SCL определяются схемой SCL, приведенной в [1]. Схема SCL является неотъемлемой частью стандарта МЭК 61850 и распространяется Международной Электротехнической Комиссией (МЭК) вместе со стандартом в виде набора файлов XSD, которые и используются для валидации. При этом стоит сделать несколько замечаний.

- На сегодняшний день существует три версии схемы SCL, которые могут использоваться для валидации: схемы редакций 1, 2 и 2.1 стандарта МЭК 61850.
- Для редакции 2 стандарта МЭК 61850 существует 2 схемы – ревизии А и Б. При этом действующей является только одна – ревизии Б, однако некоторые версии конфигураторов могут использовать ревизию А из-за того, что не были обновлены производителями своевременно.
- В некоторых случаях производители могут незначительным образом модифицировать файлы XSD для того, чтобы согласовать их со своими внутренними конфигурационными файлами. Это, в свою очередь, может приводить к проблемам функциональной совместимости.

С учётом изложенного можно сделать вывод о том, что наилучшим вариантом, в особенности, в проектах с использованием ИЭУ различных фирм-производителей, является использование независимого программного инструмента для валидации, что позволит фиксировать все возможные несоответствия стандарту МЭК 61850, которые могут вызвать проблему функциональной совместимости.

Визуальный анализ информационного обмена

Как уже было указано ранее, файлы SCL, в частности, файлы SCD содержат в себе информацию об обмене данными между ИЭУ согласно коммуникационным сервисам Sampled Values и GOOSE, вплоть до отдельных элементов данных (объектов или атрибутов данных). Это даёт возможность визуализировать коммуникации между ИЭУ проекта и фиксировать ошибки и несоответствия. Наличие различных видов отображения коммуникаций (отображение коммуникаций между всеми ИЭУ проекта, коммуникаций только для выбранного ИЭУ, подписчиков на элементы данных выбранных сообщений, назначений элементов данных сообщений на внутренние сигналы ИЭУ и др.) позволяет поэтапно анализировать правильность организации связей, фиксировать как отличия в паттерне (то есть в повторяющемся образце) коммуникаций, так и смысловые ошибки (передачу и использование не тех сигналов, что требуются; неиспользование требуемых сигналов и др.). Такие решения, как цветовая кодировка линий связи в зависимости от типа коммуникаций (GOOSE/Sampled Values), направление прорисовки линий связи в интерактивном режиме при визуализации, возможность отображения текстовых описаний для ИЭУ и передаваемых данных на языке пользователя (при их наличии в файле SCD) упрощает анализ информационного обмена. Пример визуализации согласно описанному формату представлен на рисунках 2-4.

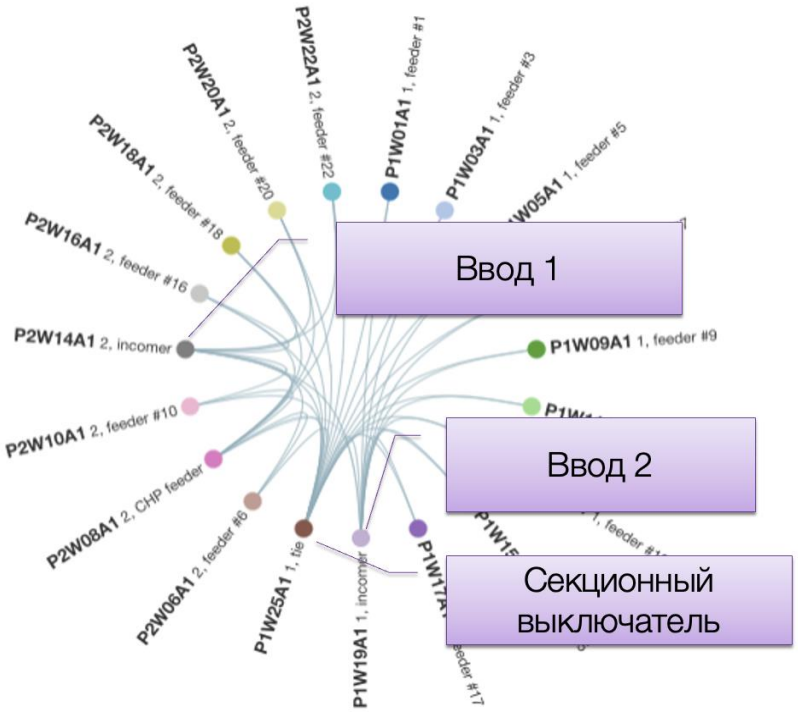


Рис. 2. Визуализация файла SCD в целом.

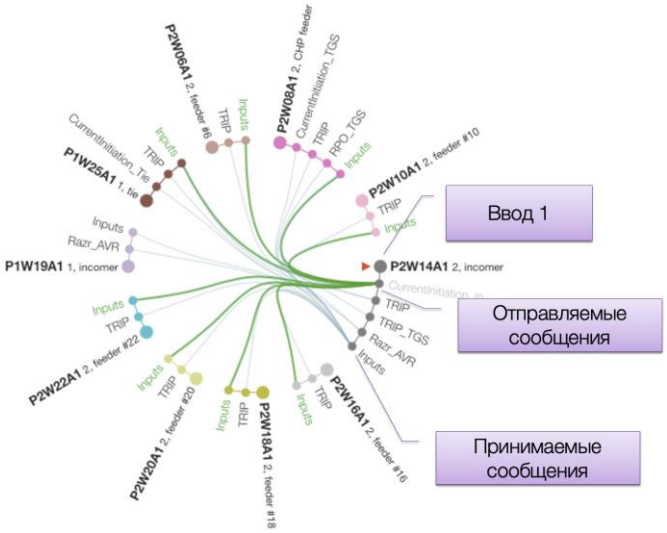


Рисунок 3. Визуализация информационного обмена для одного из ИЭУ проекта.



Рис. 4. Анализ состава сигнала в сообщениях и их назначений на виртуальные входы в ИЭУ-подписчиках.

Автоматический анализ файлов SCL

Несмотря на то, что визуализация предоставляет возможность идентифицировать ошибки, допущенные при разработке файла SCD, человеческий фактор при проведении такого анализа остается весомым, а значит, сохраняется вероятность пропуска ошибок, в частности при рассмотрении больших проектов. По этой причине чрезвычайно важно иметь функциональность автоматического анализа файлов SCD согласно предопределённым алгоритмам.

Перечень проверок, которые могут производиться в автоматическом режиме:

- GOOSE/SV-сообщение не имеет подписок;
- наборы данных содержат элементы, на которые отсутствует подписка;
- наличие подписок на несуществующие элементы данных;

- атрибуты качества либо не передаются, либо на них отсутствует подписка;
- GOOSE/SV-сообщения имеют идентичные MAC-адреса назначения и др.

Последующие подразделы подробно рассматривают каждую из перечисленных проверок, а также их влияние ошибок на функционирование системы.

GOOSE/SV-сообщение не имеет подписчиков

Существуют две наиболее вероятные причины наличия в проекте GOOSE/SV-сообщений, не имеющих подписчиков.

- Заводская конфигурация ИЭУ включала в себя предварительно сконфигурированные блоки управления передачей сообщений, которые либо не были удалены, либо не были переконфигурированы под проектные.
- В проекте либо отсутствует ИЭУ-подписчик, либо отсутствует подписка у существующего в проекте ИЭУ (которая в действительности требуется).

В первом случае при наличии большого количества таких сообщений сеть может перегружаться, и это может приводить либо к увеличению задержек информационного обмена, либо к сбоям информационного обмена (потере сообщений). Во втором случае, когда либо отсутствует ИЭУ-подписчик, либо отсутствует подписка у существующего ИЭУ, это является ошибкой конфигурирования. Данная ошибка может приводить к неправильной работе функций РЗА и АСУ ТП.

Наборы данных сообщений содержат элементы, на которые отсутствует подписка

Наличие в проекте наборов данных, включающих в себя элементы, на которые отсутствует подписка, очень похоже на ту ситуацию, когда сообщения не имеют подписчиков. Причины возникновения данной ситуации следующие:

- наборы данных были предварительно сконфигурированы производителем ИЭУ и не изменялись при конфигурировании системы;
- требуемая подписка отсутствует.

Первая ситуация может не оказывать негативного влияния на функционирование системы, однако сообщения будут иметь больший размер и могут увеличиться времена их передачи по сети и обработки ИЭУ. На практике авторы встречали проекты с наборами данных, включающими в себя 90 элементов, из которых только на 3 элемента была организована подписка. Вторая ситуация является ошибкой, которая может приводить к неправильному функционированию РЗА и АСУ ТП, и требует обязательной корректировки.

Задана ссылка на несуществующий элемент

Наличие в проекте подписок (ссылок) на несуществующие элементы является ошибкой и означает то, что были внесены изменения в конфигурацию издателя. Например, какой-либо элемент набора данных публикуемого сообщения был удалён и/или заменён на новый или был удален или изменён блок управления передачей сообщения. Указанное может происходить после изменения файла конфигурации ИЭУ-издателя в проекте. Часто возникновение этой ошибки приводит и к появлению ранее описанных ошибок (GOOSE/SV-сообщение не имеет подписчиков и/или набор данных содержит элементы, на которые

отсутствует подписок). Указанная ошибка может приводить к неправильному функционированию комплексов РЗА и АСУ ТП и требует корректировки.

Атрибуты качества либо не передаются, либо на них отсутствует подписка

Атрибуты качества являются важным элементом данных для систем, функционирующих на основе стандарта МЭК 61850. Атрибут Validity в составе атрибута качества может использоваться в алгоритмах РЗА для предотвращения неправильного функционирования в условиях плохого качества сигналов (q.validity=invalid/questionable) и при нарушении исправности коммуникаций. Помимо этого, атрибут качества играет важную роль в эксплуатации комплексов РЗА и АСУ ТП - при отсутствии атрибута качества в публикуемых сообщениях невозможно выполнять техническое обслуживание устройства РЗА и АСУ ТП в эксплуатации.

Практический опыт выполнения проверки файлов SCL

Выступая в роли заказчика в зоне эксплуатационной ответственности сетевой компании, были запроектированы пять цифровых подстанций с различными схемами распределительных устройств. Три из них запроектированы по III архитектуре (с применением протокола MMS для интеграции устройства РЗА и КП в единую систему АСУ ТП, применением протокола GOOSE для быстрой передачи информации между устройствами уровня присоединения (РЗА и КП) и передачи информации между устройствами защиты и автоматики и ПДС, а также применением протокола Sampled Values для передачи данных измерений токов и напряжений от устройств ПАС), и 2 запроектированы по II архитектуре (с применением протокола MMS для интеграции устройства РЗА и КП в единую систему АСУ ТП, применение протокола GOOSE для быстрой передачи информации между устройствами уровня присоединения (РЗА и КП) и передачи информации между устройствами защиты и автоматики и ПДС).

В ходе рассмотрения 5 проектов цифровых подстанций был выявлен ряд типовых ошибок файлов SCL (SSD, SCD), несущих как общие требования к оформлению файлов, для дальнейшего упрощения работы с ним в том числе и эксплуатирующим персоналом, так и ряд серьезных недочетов в части логики работы устройств РЗА, не устранение которых на этапе рассмотрения проектной документации привело бы к необходимости изменению файла SCD файла на этапе выполнения пуско-наладочных работ и к их затягиванию.

Перечень ошибок, выявленных в ходе рассмотрения визуализированных файлов SSD специалистами РЗА и АСУ ТП

- У присоединений (уровнень Bay) диспетчерские наименования первичного оборудования некорректны или отсутствуют.
- Используются не корректные классы логических узлов.
- Состав логических узлов не соответствует заявленным требованиям.
- Присоединения имеют идентичное обозначение.

Перечень ошибок, выявленных в ходе рассмотрения визуализированных файлов SCD специалистами РЗА и АСУ ТП:

- SV-потоки не прописаны или прописаны не в полном объеме.

- Настройка SV-произведена неверно (smvID одинаковый для всех устройств);
- В файле отсутствуют GOOSE-сообщения устройств РЗА, включающие в себя сигналы УРОВ, ЛЗШ, АВР.
- Идентичные IP-адреса устройств.

К наиболее значимым выявленным ошибкам можно отнести:

- ввод 10 кВ системы шин Т-1 ошибочно действует на отключение Т-2;
- отсутствуют GOOSE сообщения ввода 10 кВ с СВ-10 кВ и ОЛ-10 кВ;
- ПДС Т-1 подписан на действие основных защит Т-2;
- регистратор аварийных событий, контролирующий сигналы положения выключателя, берет сигналы с устройств РЗА, а не с ПДС;
- при проектировании ЦПС разных производителей выявлено несоответствие APPID некоторых устройств завяленным в руководстве по эксплуатации диапазонам;
- присутствие в файле SCD устройств РЗА, отсутствующих в проекте подстанции;
- при поэтапном вводе ПС 110 кВ формирование SV-потоков с измерениями от ТН 110 кВ 1, 2 с.ш. на первых этапах предусматривалось выполнять в ПАС линий до момента установки ТН 110 кВ 1,2 с.ш. При рассмотрении SCD-файлов поэтапной реконструкции ПС SV-поток для ТН 110 кВ 1,2 с.ш. не был переподписан в момент установки ПАС ТН 110 кВ 1,2 с.ш.;
- при рассмотрении файлов SCL также неоднократно выявлялось несоответствие сигналов АСУ ТП завяленным перечням в проектной и рабочей документации.

Выявление ошибок в файлах SCL, связанных с особенностями взаимосвязи ИЭУ разных производителей, позволяет разработчику файлов при необходимости обратиться на заводы изготовители, для получения разъяснений. Ошибки, связанные с неправильной логикой работы РЗА, могут быть выявлены только на последних этапах ПНР при опробовании действия РЗА на коммутационные аппараты.

Все ошибки, выявленные на этапе ПНР, ложатся на плечи наладчиков, что влечет за собой задержку ввода оборудования в работу.

Выводы

Проверка электронной проектной документации в формате файлов SCD с использованием специализированных инструментов позволяет обнаружить ошибки в коммуникационных параметрах ИЭУ, а также ошибки информационного обмена согласно коммуникационным моделям GOOSE, Sampled Values и Report на стадиях проектирования и, как следствие, обеспечить наиболее эффективное и своевременное выполнение пусконаладочных работ. Помимо этого, наличие корректного файла SCD позволит полноценно решать следующие задачи:

- использовать SCD-файл при последующей реконструкции и модернизации объекта проектирования;
- использовать SCD-файл при процедурах технического обслуживания и проверках ИЭУ с использованием испытательных установок и программного-обеспечения сторонних фирм-производителей;

- применять системы мониторинга и диагностики вторичных коммуникаций согласно коммуникационным сервисам стандарта МЭК 61850;
- применять системы мониторинга информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

[1] IEC 61850-6, Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs.
[2] IEC 61850-8-1, Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
[3] IEC 61850-7-2, Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)

2.2. ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИСПЫТАНИЙ НА ЦИФРОВЫХ ПОДСТАНЦИЯХ

А. АПОСТОЛОВ

Omicron

США

Контактное лицо:

А. АПОСТОЛОВ

alex.apostolov@omicronenergy.com

Введение

Переход электроэнергетической отрасли в сторону более умной сети характеризуется существенными усилиями, направленными на повышение эффективности выполнения всех задач и сокращение времени перебоев электроснабжения в случае инцидентов, связанных с работой многофункциональных устройств РЗА. Широкомасштабное внедрение защит на подстанциях с поддержкой МЭК 61850 и повышенный интерес во внедрении цифровых подстанций с передачей сигналов тока и напряжения в цифровой форме (Sampled Values) обеспечивает возможность разрабатывать и внедрять системы защиты, автоматики и управления, который могут быть испытаны у дистанционном режиме.

Испытания систем релейной защиты и автоматики с применением проводных связей между устройствами в большинстве случаев требуют бригады на удаленный объект. Замена проводных интерфейсов на коммуникации по стандарту МЭК 61850 позволит обеспечить удаленный доступ к подстанции для организации дистанционных испытаний.

Замена части или всех проводных интерфейсов на цифровые коммуникации требует разработки и внедрения методов и инструментов, которые обеспечат сохранение того же уровня безопасности во время процедур испытаний, в то же время позволяя воспользоваться всеми преимуществами, которые предоставляет МЭК 61850.

В настоящей публикации в первую очередь даётся определение дистанционных испытаний и даётся ответ, почему нам необходимы дистанционные испытания». Далее рассмотрены принципы изоляции ИЭУ с точки зрения испытаний на подстанции под напряжением, связанные с проверкой определенного функционального элемента, рассматриваются как локальные, так и распределенное защиты. Специалисты, участвующие в испытаних схем релейной защиты и систем АСУ ТП, обычно используются физическую изоляцию испытуемых устройств с использованием испытательных блоков, которые с одной стороны позволяют разорвать цепь управления выключателем, одновременно с этим позволяя заменить аналоговые сигналы от измерительных трансформаторов тока и напряжения, сигналами от испытательной установки.

Во второй части доклада рассмотрены нововведения второй редакции стандарта МЭК 61850, которые могут использоваться для виртуальной изоляции компонентов схемы защиты.

В заключительной части доклада рассмотрены методы и инструменты, которые могут быть использованы для выполнения испытаний на базе требований, определенных в МЭК 61850 ред. 2, и как они отвечают требованиям по виртуальной изоляции с практической точки зрения. В качестве выводов рассмотрены преимущества и трудности, связанные с дистанционными испытаниями систем релейной защиты и автоматики на базе коммуникаций по МЭК 61850.

Определения

Одна из главных проблем в обсуждении любого предмета – это неправильное понимание. Его можно существенно уменьшить, или даже вовсе исключить благодаря ясному описанию предмета посредством хорошего определения.

Когда мы думаем о действенности и эффективности, существует множество вещей, которые можно перепутать, поскольку люди считают, что эти два понятия примерно одинаковы по смыслу.

Все последующие выкладки в настоящем докладе будут базироваться на следующих определениях, которые даны после анализа множества различных определений, доступных в интернете.

Действенность — это мера, в которой цели достигаются без учёта затрачиваемых ресурсов.

Эффективность — это степень, в которой ресурс используется для эффективного достижения цели.

В последующих разделах доклада мы проанализируем, во-первых, инструменты и способы, которые могут быть использованы для эффективных испытаний различных типов устройств защиты и управления, основываясь на некоторых конкретных примерах.

После разъяснения того, как мы можем убедиться в успешных испытаниях объекта, мы сконцентрируемся на том, как сделать это наиболее эффективным способом.

Испытания в эксплуатации

Одним из ключевых требований для правильного проведения испытаний в эксплуатации является определение необходимости таких испытаний. Испытания в эксплуатации — это вид испытаний, который проводится для обнаружения и идентификации проблем с оборудованием или подтверждения, что различные действия по изменению уставок, обновлению или ремонту устройств защиты или другого оборудования были выполнены корректно. Объем испытаний зависит от того какие из перечисленных операций выполнялись.

Испытания в случае корректного срабатывания релейной защиты

Последствия неисправностей различных элементов системы, обеспечивающей отключение коротких замыканий можно разделить на два вида: защита не срабатывает в случаях, когда это требуется и защита срабатывает в случаях, когда это не требуется. Эти два типа отказов обычно обнаруживаются, когда система находится в работе и происходит КЗ. Работу защиты необходимо проанализоровать с тем, чтобы определить причину некорректной работы и принять корректирующие мероприятия для предотвращения некорректной работы системы в будущем.

Отказ срабатывания

Основная функция релейной защиты – это детектировать повреждения в энергосистеме и предпринимать необходимые действия, направленные на отключение поврежденного оборудования от остальной части системы. В некоторых случаях, если повреждение на

магистральной или распределительной линии носит временный характер, защита может также предпринять попытку восстановления режима, предшествующего повреждению, с использованием функций автоматического повторного включения.

Отказ срабатывания в случае короткого замыкания может привести к нарушению устойчивости энергосистемы из-за возрастающего времени воздействия повреждения при срабатывании резервных защит и отключения неповрежденных элементов системы.

Ложное и излишнее срабатывание

Как показали расследования многих системых аварий, основной причиной их становилось срабатывание системы защиты в режиме без повреждений. Такие отказы также должны быть исключены, поскольку они также могут вести к негативным последствиям для устойчивости энергосистемы и приводить к ухудшению условий и широкомасштабному развитию аварии.

Требования к испытаниям в случае некорректной работы

Испытания в эксплуатации в случае некорректной работы могут быть двух типов:

- испытания для определения причины срабатывания;
- испытания для подтверждения, что корректирующие мероприятия были проведены успешно.

Определение причины некорректной работы обычно в первую очередь выполняется путем подачи осциллограмм токов в момент повреждения, снятых самими устройствами защиты или регистраторами аварийных событий на подстанции. Второй способ является более предпочтительным по ряду причин:

- на запись в некорректно сработавшем устройстве может оказать влияние отказ самого устройства или других компонентов системы, например, измерительных трансформаторов или токовых цепей;
- частота дискретизации в устройстве защиты может быть слишком маленькой для корректного воспроизведения нештатной ситуации в системе.

В некоторых случаях сравнение записей, сделанных корректно работающими устройствами защиты, с записями с других устройств может указать на причину некорректной работы и помогает определить отказавший элемент.

После установления причин некорректной работы, требуется предпринять корректирующие мероприятия, после которых должны быть выполнены испытания, подтверждающие успешность корректирующих мероприятий. Испытания в этом случае могут базироваться на воспроизведении тех же самых файлов, чтобы были использованы для определения причин некорректной работы, а также иных тестах, направленных на проверку изменений в уставках и программируемой логике.

Требования по функциональной изоляции в ходе испытаний

Требования по функциональной изоляции в основном зависят от того какой элемент испытывается и какова цель этих испытаний. В последующих разделах мы выделим те случаи, в которых испытания должны производиться в нормальном режиме функционирования, а когда мы должны использовать другие режимы, обеспечивающие виртуальную изоляцию.

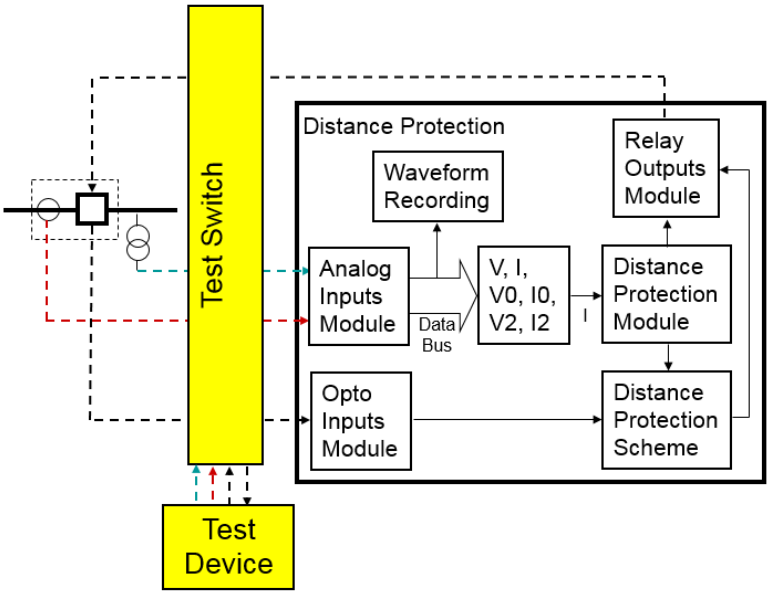


Рис. 1. Физическая изоляция при испытаниях.

Требования по функциональным испытаниям устройств и распределенных функций также определяют методы испытаний для обоих типов систем, основанные на следующем порядке испытаний компонентов системы:

- функциональные испытания отдельных ИЭУ, используемых в схеме;
- функциональные испытания распределенных функций в рамках подстанции.

В традиционных устройствах защиты с проводными связями изоляций осуществлялся физически (рис. 1), используя испытательные блоки, которые полностью отключают устройство от оборудования подстанции.

На цифровых подстанциях с МЭК 61850 физическая изоляция невозможна, поэтому необходимо применять функции, заложенные в стандарт в целях проведения испытаний.

Возможности стандарта МЭК 61850 редакции 2, предназначенные для испытаний

Для проведения испытаний компонентов системы на базе стандарта МЭК 61850 на включенном оборудовании в редакции 1 стандарта уже было предложено множество возможностей, которые могли использоваться при испытаниях. Эти возможности включают:

- возможность переводить функцию или функциональный элемент (логические узлы и логические устройства) в режим тестирования;
- возможность снабжения GOOSE-сообщения меткой, сообщающей о том, что оно отправлено в целях испытаний;

- возможность снабжения команд управления метками, указывающими на то, что они используются в целях испытаний;
- возможность добавления к любым данным, отправляемым с сервера, метки флага качества, указывающей на то, что значение используется для целей тестирования.

Однако в редакции 1 не давалось четкого определения, как эти возможности должны быть использованы. Как следствие, они не поддерживались многими производителями, в связи с чем совместимость не могла быть гарантирована.

В редакции 2 стандарта были сделаны неободимые улучшения. Помимо более детализированного определения требований по отношению к существующим возможностям, также были добавлены дополнительные возможности.

Режим тестирования функции

Логические узел или логическое устройство может быть переведено в режим тестирования с использованием объекта даных **Mod** соответствующего логического узла или логического узла LLN0. Пояснения по поведению функций в этом режиме даны на рис. 2 и 3. Команда управления может быть подана либо посредством сервиса управления, либо с помощью GOOSE-сообщения, которое подписчик интерпретирует как команду. Если команда подаётся с флагом TEST установленным в значение ложь (FALSE), она будет исполнена в том случае, если функция (логический узел или устройство) находится в режиме ON. Если устройство находится в режиме тестирования (Mod = Test), оно не будет выполнять команд (рис. 2).

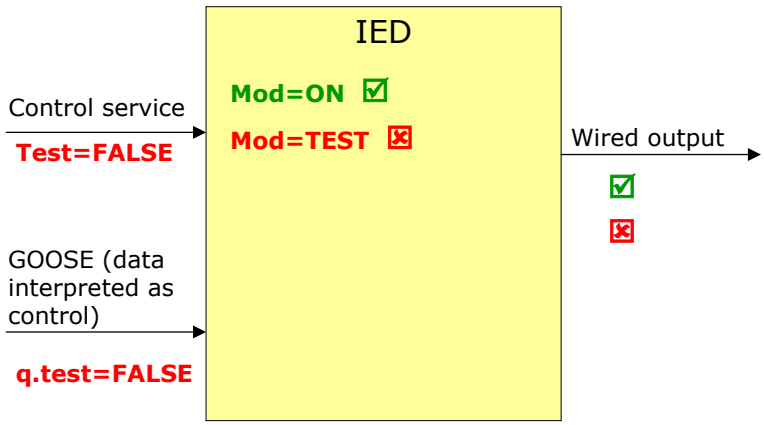


Рис. 2. Команда с Test=FALSE.

Если команда передаётся с флагом Test = TRUE, то она не будет исполнена в том случае, если функция, на которую она подаётся, будет иметь режим "ON". Если функция находится в режиме тестирования (Beh = Test) команда будет выполнена и проводной выход функции (например, релейный выход отключения выключателя) будет активирован. Если функция

переведена в режиме "TEST-BLOCKED", команда будет обработана, все реакции на команду (например, отправка подтверждения приёма команды) будут выполнены, но физический контакт не будет активирован (рис. 3). Режим "TEST-BLOCKED" особенно полезен при выполнении испытаний на устройствах, включенных в работу.

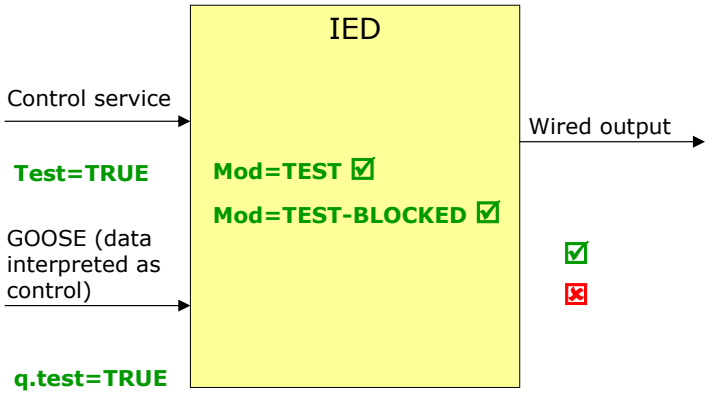


Рис. 3. Команда с Test = TRUE.

Симуляция сообщений

Ещё одно новшество второй редакции – это возможность приёма GOOSE-сообщений или SV-потоков от симулятора или испытательной установки. Этот подход объясняется на рис. 4. Сообщения GOOSE или Sampled Values имеют флаг, указывающий на источник сообщения: было ли оно отправлено реальным устройством или симулятором (испытательной установкой). С другой стороны, устройство имеет в логическом узле LPHD (логический узел физического устройства ИЭУ) объект данных, определяющий, какие сообщения должно принимать устройство: рабочие или симулированные. Если объект данных Sim установлен в значение TRUE, то ИЭУ на всех GOOSE-сообщений, на которые оно подписано, будет принимать те, для которых флаг Simulation имеет значение TRUE. Если для какого-то GOOSE-сообщения отсутствует его симулированный дубликат, то устройство продолжит принимать рабочее GOOSE-сообщение. Возможность может быть активирована только для ИЭУ целиком, так как ИЭУ должно принимать либо симулированные сообщения, либо рабочие. Приём двух сообщений одновременно может создать ситуацию разности нагрузки и, следовательно, привести к некорректным результатам испытаний.

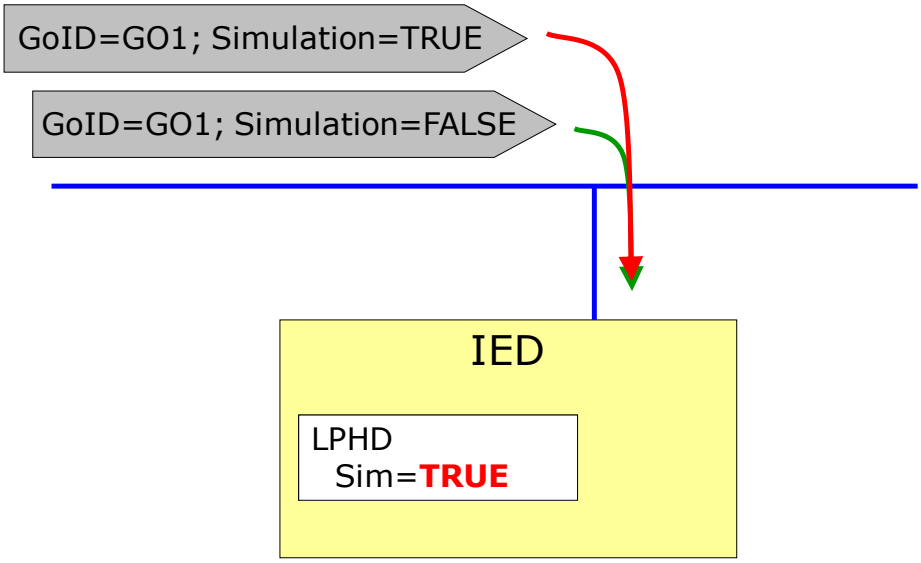


Рис. 4. Симуляция GOOSE-сообщения.

Зеркалирование команд управления

Третья возможность, добавленная в стандарт — это зеркалирование команд управления. Благодаря этому появляется возможность испытывать и контролировать работу команд управления, в то время как испытуемое устройство подключено к оборудованию.

Команда управления подаётся на управляемый объект. Как только команда была получена, устройство должно активировать атрибут данных opRcvd. Затем устройство должно обработать команду. Если команда принята, атрибут данных opOk будет активирован с теми же временными характеристикиами (например, длительность импульса), что и физический выходной контакт. Атрибут данных tOpOk — это метка времени для атрибута opOk и физического выхода.

Эти атрибуты данных принимают свои значения независимо от выходного реле: выходное реле не должно срабатывать, если функция находится в режиме TEST-BLOCKED. Таким образом, указанные атрибуты позволяют проконтролировать работу функции, включая временные характеристики, без реального физического воздействия на выходное реле.

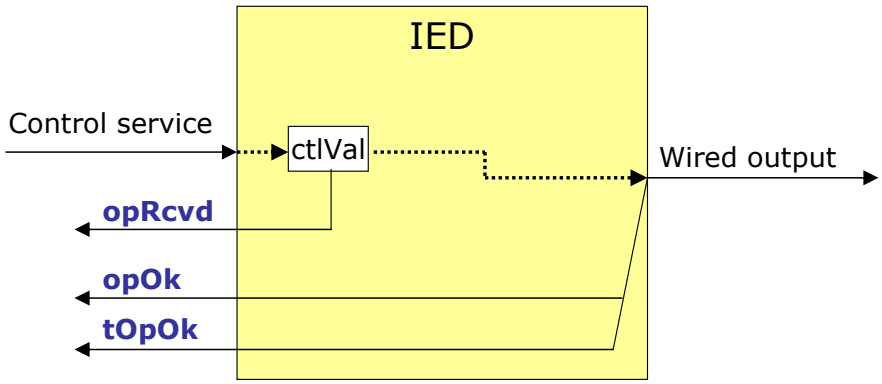


Рис. 5. Зеркалирование информации управления.

Изоляция и испытания устройства в системе

Комбинируя механизмы, описанные в предыдущих секциях, становится возможным испытывать устройство, подключенное к системе. Рассмотрим это на коротком примере.

Предположим, что мы хотим проверить работу основной защиты, которая получает поток Sampled Values от преобразователя аналоговых сигналов. В логическом узле LPHD основной защиты объект данных Sim должен быть установлен в значение TRUE, логическое устройство защиты должно быть переведено в режим TEST и логический узел XCBR, как интерфейс для силового выключателя, должен быть переведн в режиме TEST-BLOCKED. Испытательная установка должна отправлять потоки Sampled Values с теми же идентификационными параметрами, что и обычный рабочий поток, но с установленным флагом симуляции в значение Истина (TRUE).

После этого устройство защиты будет принимать мгновенные значения от испытательной установки и инициирует срабатывание. Логический узел XCBR (выключатель) примет и обработает этот сигнал отключения, однако, срабатывание выходных реле не произойдёт. Срабатывание функции можно проверить благодаря атрибутам XCBR.Pos.opOk, характеристики по времени можно проверить с помощью атрибута данных XCBR.Pos.tOpOk.

Продвинутые функции симуляции

Наконец, в стандарт были добавлены улучшенные возможности по симуляции, которые могут быть использованы при функциональных испытаниях. Концептуально это описано на рис. 6. Как уже было отмечено ранее, в редакции 2, была добавлена возможность описать ссылки на входы логических узлов. Это делается с помощью нескольких экземпляров объектов данных **InRef** общего класса данных ORG. Объект данных содержит два атрибута со ссылками на объекты: одна как ссылка на объект используемый в качестве рабочего входа, а другая — ссылка на объект, используемый при проведении испытаний. Путём активации атрибута данных **tstEna**, функция, реализуемая логическим узлом, должна использовать в качестве входного сигнала объект данных, на который указывает тестовая ссылка, вместо объекта данных рабочего входа.

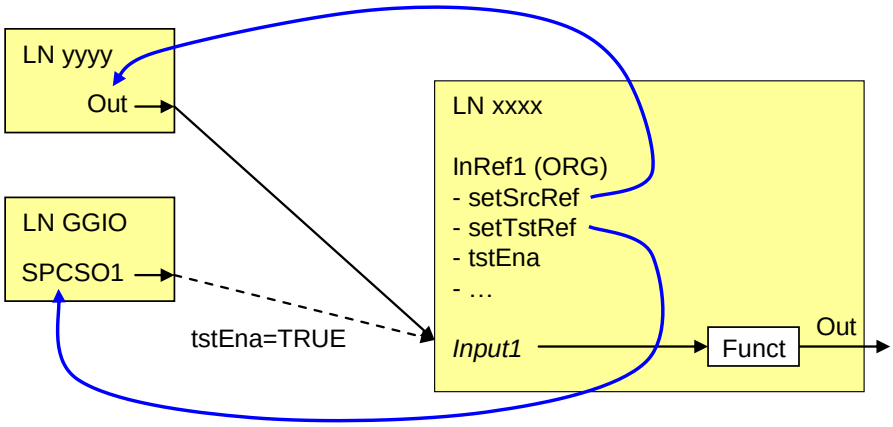


Рис. 6. Симулированные входы.

С помощью этой функции, как показано в рассматриваемом примере, можно тестировать логические функции, например, оперативной блокировки. Вместо того, чтобы брать реальные положения различных коммутационных аппаратов в качестве входной информации, логический узел (в данном случае CILO) может использовать в качестве входных данные с логического узла GGIO. Благодаря этому испытательная система может легко изменять значения различных объектов данных логического узла GGIO для симуляции тестовых состояний, которые необходимо испытать. Рассматриваемый логический узел может быть как внешним (объекты данных принимаются GOOSE-сообщением) или может быть реализован в самом устройстве для обеспечения возможности испытаний.

Обратите внимание, что хотя такой способ позволяет выполнить детальное тестирование с индивидуальными данными на каждом входе, его не всегда можно использовать для оценки работоспособности системы. Поскольку индивидуальные входы переключаются, что может изменить ситуацию относительно приёма и обработки GOOSE-сообщений, то поведение функции в динамике может измениться.

Мониторинг сервисов

В то время как мониторинг событий, формируемых прикладными функциями, был возможен ещё в первой редакции стандарта путём передачи отчетов или сохранения событий в журнал, это было невозможно для событий, связанных с коммуникациями.

С этой целью во второй редакции была представлена концепция мониторинга коммуникационных сервисов. Были определены экземпляры объектов данных для каждого вида сервиса, которые отражают значения параметров соответствующего сервиса. Такой объект данных может быть включен в набор данных для передачи в отчете или записи в журнал.

Методы испытаний

Для того, чтобы обеспечить эффективность испытаний, в первую очередь нам необходимо определить критерии эффективности, то есть ресурсы, которые требуется минимизировать. Мы можем использовать время, уходящее на подготовку, выполнение и оформление результатов испытаний в качестве ключевого параметра.

Методики функциональных испытаний можно разделить на следующие категории. Они относятся к различным уровням сложности и функциональности отдельных устройств, которые используются на разных уровнях иерархии системы, а также типам распределенных функций, реализованных в них. В этом случае требуется выбор правильных методик испытаний для определенного вида испытаний, а также использование корректных инструментов, которые могут автоматизировать процесс испытаний.

С этой точки зрения наиболее широко применяются следующие методики испытаний:

- функциональные испытания элементов;
- интеграционные испытания;
- функциональные испытания;
- испытания системы.

Функция в этом случае может рассматриваться как подсистема с другим уровнем сложности, например, если функцией считаь полную резервированную функцию защиты, то функция мониторинга системы может рассматриваться как подфункция.

Вне зависимости от того для каких элементов проводятся испытания, тестируемый объект должен отвечать критериям пригодности к испытаниям. Указанные критерии — это технические решения, заложенные на этапе разработки, которые позволяют однозначно определить статус системы (работоспособна, неработоспособна, ухудшена работоспособность) или подсистемы во времени. Пригодность к испытаниям пытается квалифицировать те атрибуты проектирования системы, которые улучшают характеристики в части обнаружения и отключения повреждений. С точки зрения пригодность к испытаниям, функциональный элемент системы защиты — это единица, которую можно испытывать, посколько он является наименьшим элементом, который может существовать сам по себе и обмениваться информацией с другими элементами в системе защиты.

Ещё один пункт, который надо принимать во внимание — это цель испытаний: проводятся ли они как приёмосдаточные для нового устройства или функции, либо выполняются при пусконаладочных работах для защищаемого элемента, либо выполяются в эксплуатации для всей системы защиты. С этой точки зрения различные методики могут применяться даже если испытания проводятся для одного и того же функционального элемента или функции.

For example the testing of a system monitoring function during the user acceptance phase may focus on the testing of the measuring element characteristic using search test methods, while during the commissioning the operating times for different system conditions be the important ones achieved through transient simulation methods.

Знания о внутреннем поведении испытуемого объекта или, точнее говоря, его логике или реализуемых алгоритмах, определяют как именно выполняются испытания. С этой точки зрения методики испытаний можно разделить на следующие группы:

- испытания «черного ящика»;
- испытания «белого ящика».

Важным аспектом, который необходимо учитывать в ходе испытаний, является доступность резервирующих устройств, выполняющих различные функции защиты.

В последующих разделах различные методики испытаний, указанные выше, рассматриваются более подробно.

Испытания «черного ящика»

Испытания «черного ящика» — это очень часто используемая методика испытаний, где испытатель рассматривает испытуемый объект как «черный ящик». Это означает, что нас не интересует внутренне поведение и структура испытуемой функции. Информация для испытаний полностью черпается из технических характеристик без преимуществ, которые может дать знание внутренней структуры функции.

Испытания по методике «черного ящика» обычно используются для:

- функциональных испытаний элементов ;
- заводских испытаний систем РЗА;
- приёмосдаточных испытаний системы РЗА на объекте.

Поскольку функциональные элементы определяются как наименьшие единицы, которые могут существовать и быть испытаны самостоятельно, ясно, что испытания методом «черного ящика» — это единственный способ, который может применяться для их испытаний.

Реакцию испытуемого объекта на тестовые воздействия можно контролировать с помощью испытательной установки посредством срабатывания физических выходных реле, коммуникационных сообщений или отчетов.

Испытания «белого ящика»

Испытания по принципу «белого ящика» — это методика, когда испытуемая система рассматривается не только с точки зрения реакции на тестовые воздействия, но также рассматривается её внутренняя структура и поведение. В случае системы защиты это означает, что рассматривается не только срабатывание системы по её функциональной границе, но также рассматривается обмен сигналами между различными компонентами системы.

Такая стратегия испытаний позволяет нам исследовать внутренню структуру испытуемого объекта, что полезно в случае анализа поведения, в особенности, если испытание не пройдено.

В такой стратегии, испытательная система формирует тестовые данные, исследуя логику испытуемого объекта, не игнорируя при этом и требования технических характеристик. Целью таких испытаний является достижение высокого покрытия испытаниями через анализ работы различных компонентов комплексной функции и обмена сигналами или сообщениями между ними в условиях испытаний.

Этот метод особенно полезен, когда испытываются распределенные функции, основанные на различных логических интерфейсах. Анализ поведения компонентов функций или функциональных элементов достигается посредством мониторинга обмена сообщениями между компонентами испытуемого объекта.

Сценарии испытаний, тем не менее, не должны отличаться от тех, что используются при испытаниях по принципу «черного ящика».

В системах на базе МЭК 61850 испытания по принципу «белого ящика» проводить сравнительно просто, достаточно подписаться на GOOSE-сообщения, наборы данных которых содержат атрибуты, отражающие статусы всех функциональных элементов, которые используются для реализации испытуемой функции (например, SF_M на рис. 7).

Испытания по принципу «сверху вниз»

Испытания по принципу «сверху вниз» — это методика, которая может широко применяться для систем релейной защиты, особенно в ходе приёмосдаточных испытаний на объекте, когда мы можем исходить из того, что все компоненты системы уже были налажены и испытаны.

Испытания «сверху-вниз» могут проводиться обоими методами: как по принципу «черного ящика», так и по принципу «белого ящика».

Испытания начинаются с целой системы, с последующими тестированием отдельных функций и под-функций и, если это требуется, испытаниями функциональных элементов.

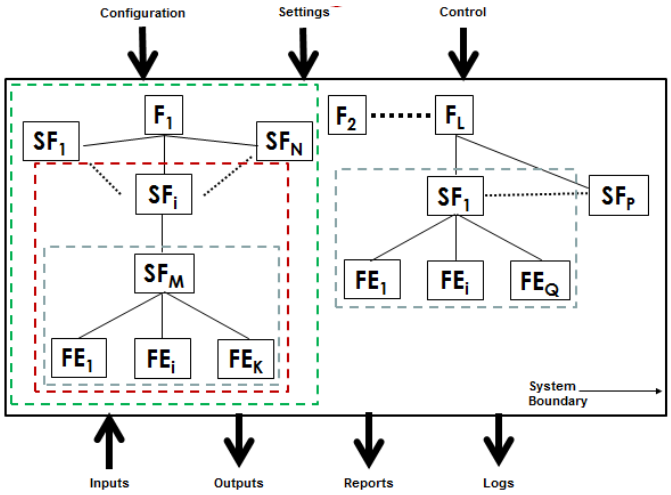


Рис. 7. Испытания «сверху вниз» для функций мониторинга системы.

В случае заводских ПСИ, когда не все компоненты системы или подсистемы доступны, испытательная система должна быть в состоянии симулировать их работу, ожидаемую в сценария теста. В этом случае испытательная система создает так называемые «заглушки» функций или функциональных элементов, которые сейчас недоступны.

Каждый функциональный элемент испытывается в соответствии с программой испытаний по стратегии «сверху вниз».

Если мы рассматриваем систему защиты, реализованную в соответствии с МЭК 61850, то для испытаний в соответствии с принципом «сверху вниз» в первую очередь нам необходимо будет найти функциональную границу.

Испытания отдельных компонентов системы могут потребоваться в том случае, если какой-либо из тестов верхнего уровня не будет пройден. Функциональная граница для всех этих видов испытаний будет различной и будет требовать различного набора испытательных воздействий от испытательной установки, а также мониторинга поведения функциональных элементов с использованием различных сигналов или коммуникационных сообщений.

Испытания по принципу «снизу вверх»

Испытания «снизу вверх» — это методика, которая предполагает начало испытаний с самого низа: обычно с функциональных элементов, используемых в системе, например, РТОС.

Этот метод лучше подходит для испытаний на соответствие типу производителем или приёмочной комиссией заказчика.

При испытаниях комплексных многоуровневых функций или систем, для отсутствующих функциональных элементов должны быть созданы их виртуальные модели. Испытательная система должна быть в состоянии симулировать отсутствующие компоненты системы при выполнении, например, заводских ПСИ.

Между методами «сверху вниз» и «снизу вверх» есть много схожих аспектов. Основным же отличием этих методов является порядок, в котором выполняются испытания и количество требуемых опытов.

Требования к инструментальному обеспечению испытаний

Из предыдущих разделов этой статьи становится понятно, что инструменты, используемые при испытаниях, должны удовлетворять требованиям всех перечисленных различных видов испытаний, рассмотренных выше.

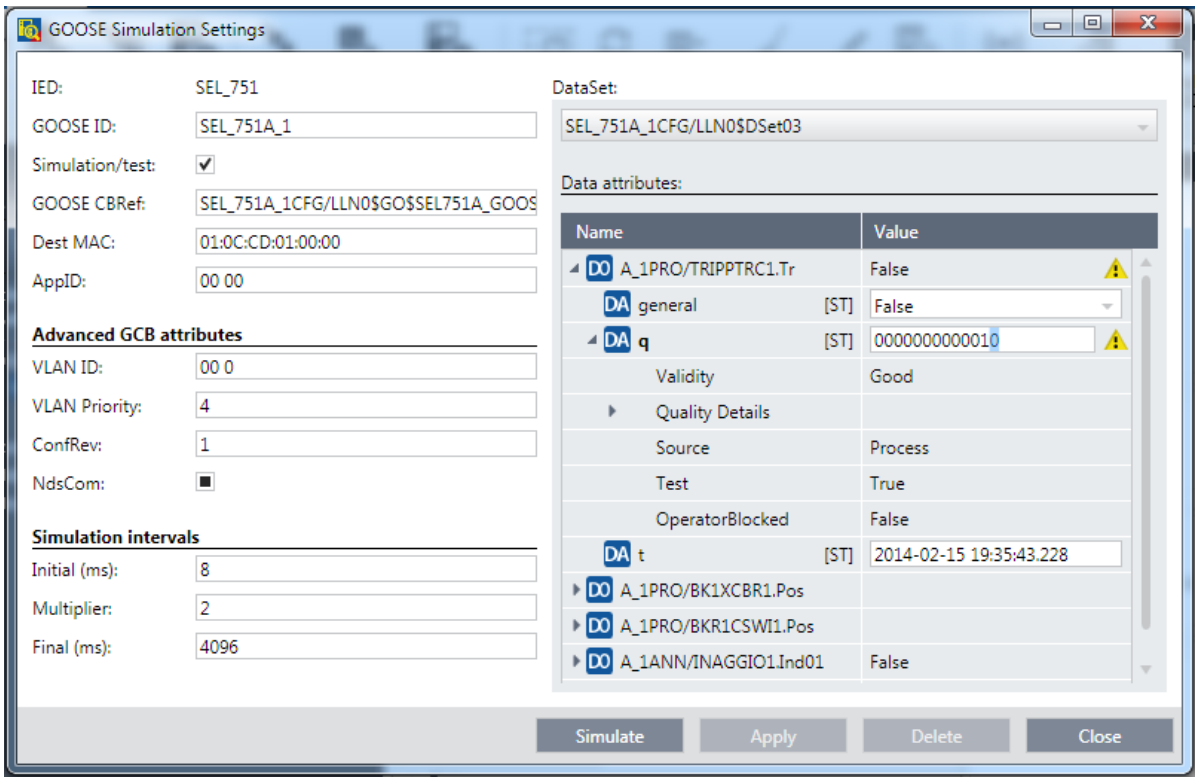


Рис. 8. Обеспечение виртуальной изоляции при испытаниях.

Существует две разновидности инструментов для испытаний:

- аппаратные — это различные испытательные устройства, которые формируют аналоговые сигналы или коммуникационные сообщения, как это требуется для испытаний функции;

- программные — различные программные инструменты, которые используются для определенных видов испытаний, создания тестовой конфигурации, симуляции режимных условий, а также оценки результатов испытаний и формирования отчётной документации.

Для обеспечения виртуальной изоляции испытательные устройства должны обеспечивать возможность управления в нормальном режиме, то есть отправлять сообщения с объектами данных, атрибуты Test в которых имеют значение «Ложь» (False). Как показано выше, всё это требуется, когда в виртуальной изоляции нет необходимости.

В таких случаях как испытания в эксплуатации или при наладке нового комплекта защиты присоединения или схемы управления на объекте под напряжением, испытательное оборудование должно отправлять сообщения с флагом симуляции или тестирования установленным в значение "Истина" (True), с тем, чтобы исключить нежелательное отключение выключателей.

Требования и преимущества дистанционных испытаний

Цифровые подстанции на базе стандарта МЭК 61850 позволяют существенно повысить эффективность испытаний в эксплуатации. Это становится возможным благодаря доступности в стандарте возможностей, позволяющих изолировать испытуемый объект и

испытательную системы от остального оборудования, находящегося в работе, без необходимости физических переключений соединений или оборудования на подстанции.

Одним из преимуществ цифровых подстанций является то, что все устройства (ИЭУ РЗА, АРМы и испытательные устройства) подключены к коммуникационной сети подстанции. Если инструменты, используемые для испытаний, подключены к сети подстанции на постоянной основе, становится возможным проводить испытания в дистанционном режиме. Это может быть полезно во многих случаях:

- большое расстояние между подстанцией и базой, на которой располагается обслуживающий персонал;
- плохая транспортная доступность;
- плохие метеорологические условия;
- требования по снижению длительности отключений, требуемых для операций обслуживания.

Дистанционные испытания повышают эффективность испытаний путём исключения необходимости выезда на подстанцию для проведения испытаний. Это ведёт к значительному снижению времени, необходимого бригаде обслуживающего персонала для выполнения соответствующих испытаний.

Дополнительная возможность экономии времени вытекает из отсутствия необходимости физических коммутаций испытательного оборудования на объекте.

Возможность изолировать только функциональные элемент, который должен быть испытан, повышает эффективность функционирования энергетической системы, так как позволяет не отключать нагрузку, защищаемую испытуемым элементом.

Для обеспечения возможности дистанционных испытаний система должна отвечать следующим требованиям:

- аналоговые и дискретные интерфейсы между оборудованием уровня процесса и устройствами защиты, автоматики и управления должны быть цифровыми (SV и GOOSE в соответствии с МЭК 61850);
- поддержка виртуальной изоляции испытуемых объектов;
- защищенный дистанционный доступ к испытательной системе подстанции.

Концепция дистанционного тестирования может быть реализована с использованием различных способов. Один из таких способов показан на рис. 9.

Испытательная система на удаленной подстанции включает следующие компоненты:

- АРМ для испытаний, на котором развернуто испытательное программное обеспечение, поддерживающие возможности редакции 2 стандарта МЭК 61850 и требуемые инструменты функциональных испытаний;
- испытательные устройства, обеспечивающие формирование тестовых воздействий и оценку результатов для каждого опыта.

Доступ к АРМу, используемому при испытаниях, организован через частную облачную сеть и требует использования технологий защиты информации, доступных для организации удаленного доступа с АРМ инженерного персонала с ограничением доступа только для авторизованных пользователей.

Инженерный и технический персонал осуществляют доступ к удаленному рабочему месту на подстанции с использованием функций удаленного доступа с применением совершенных средств защиты.

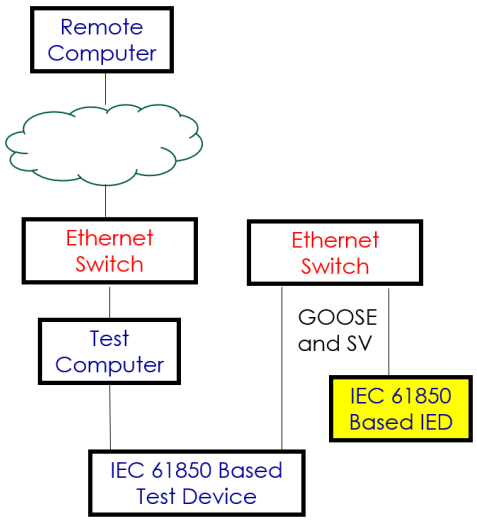


Рис. 9. Удаленная система для проведения испытаний.

В зависимости от требований по конкретным испытаниям и типу проводимых испытаний, логические узлы, устройства или целые ИЭУ переводятся в требуемые режимы, обеспечивающие их виртуальные изоляцию.

Выводы

Редакция 2 стандарта МЭК 61850 представила множество новых функций, которые в значительной степени усилили стандарт.

Среди нововведений есть несколько, которые должны в существенной степени облегчить жизнь конечным пользователям, при условии, что эти нововведения будут поддерживаться в устройствах. Эти нововведения разработаны не только для обеспечения возможности автоматизации испытаний, но для проведения испытаний в дистанционном режиме.

Проведения испытаний в дистанционном режиме из удаленного инженерного центра привносит значительные преимущества в части эффективности, безопасности и сокращения времени технологических перерывов.

2.3. ОПЫТ ПРОВЕРКИ УСТРОЙСТВ НА СООТВЕТСТВИЕ МЭК 61850. НАИБОЛЕЕ ВОСТРЕБОВАННЫЕ И САМЫЕ РЕДКО ВСТРЕЧАЮЩИЕСЯ СЕРВИСЫ

М. Д. ИЛЬИН

АО «НИЦ ЕЭС»

Российская Федерация

Контактное лицо:

М. Д. ИЛЬИН

ilin@nicees.ru

Keywords: МЭК 61850, сертификация, сертификационные испытания.

Введение

В докладе приводится анализ выданных UCA International Users Group (UCAIug) сертификатов на соответствие требованиям стандарта МЭК 61850, выданных отечественным производителям. Проводится оценка влияния нормативной базы на реализацию сервисов МЭК 61850 и тенденцию реализации сервисов МЭК 61850 у производителей.

Целью доклада является ознакомление аудитории с текущим состоянием и тенденцией использования сервисов МЭК 61850 в устройствах РЗА и других устройств вторичной коммутации.

Основная часть

Начиная с 2005 года, компания UCAiug начала выдавать сертификаты соответствия МЭК 61850. С тех пор изменилось многое: менялись процедуры испытаний, появилась новая редакция стандарта, в данный момент идет разработка следующей редакции МЭК 61850. Стандарт развивается благодаря внедрению идей стандарта в устройства, которые впоследствии устанавливаются на подстанциях. А после опытной эксплуатации замечания могут быть переданы разработчикам стандарта МЭК 61850. Для этого действует специальный сайт https://iec61850.tissue-db.com/ где собирается информация по несоответствиям и спорным моментам в стандарте. В дальнейшем эта информация просматривается разработчиками стандарта и даются рекомендации по устранению несоответствий. Вместе со стандартом развивается и сопутствующие продукты: Системы автоматизированного проектирования (САПР), в котором учтены особенности МЭК 61850; анализаторы трафика; программное обеспечение для проверки соответствия МЭК 61850.

Первые отечественные продукты были сертифицированы в конце 2014 года. На момент подготовки доклада было выдано 24 сертификата отечественным производителям (данные получены с сайта UCAIug).

http://www.ucaiug.org/org/TechnicalO/Testing/Lists/IEC61850Ed1ClientCertificates/AllItems.aspx).

Реализация функций устройств в МЭК 61850 формируется на основе сервисов. Статистика реализованных сервисов по сертифицированным российским устройствам приведена в табл. 1.

Табл. 1. Распределение блоков сервисов МЭК 61850 по сертифицированным российским устройствам.

	ed.	1	2	2+	3	4	4+	5	6	7	9a	9b	9c	12a	12b	12c	12d	13	14	15	Total
EKRA BE2704	1	+	+	-	-	+	-	+	+	-	+	+	-	+	-	-	-	+	+	-	10
Energoservice-ENIP2	1	+	+	+	-	-	-	+	+	-	+	+	-	+	-	-	+	+	-	-	10
OOO-MP3 MP3-1	1	+	+	-	-	+	-	+	+	-	+	+	-	+	-	-	+	+	+	-	11
NPP-Bresler 0107.511	1	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	+	+	+	-	14
IC-Bresler TOR200 L	1	+	+	-	-	-	-	+	+	-	+	+	-	+	-	-	+	+	+	-	10
IC-Bresler TOR30C AUV KSZ	1	+	+	-	-	-	-	+	+	-	+	+	-	+	-	-	+	+	+	-	10
RadiusAvtomatika Sirius-3-LV-03	2	+	+	+	-	-	-	+	+	-	+	+	-	+	-	-	-	+	+	-	10
NIPOM P0301	1	+	+	+	-	+	-	+	+	-	+	+	-	+	-	-	-	+	+	-	11
ElectroPribor_PQI96_PQI120M_PQI120MP	1	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	2
CHEAZ BEMP DZT	2	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	+	+	+	-	14
TECON 311FS	2	+	+	-	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	12
EKRA 217 0603	2	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	+	+	+	-	14
PLC-Technology TOPAZ IEC DAS	2	+	+	-	-	-	-	+	+	-	+	+	-	+	-	-	+	+	+	-	10
CHEAZ BEMP RU-02.5.220.ET	2	+	+	+	-	+	+	+	+	-	+	+	-	+	+	+	+	+	+	-	15
SVEY_AURA-07-R	2	+	+	-	-	-	-	+		-		+	-	+	-	-	-	+	+	-	7
EKRA BE2704V019	2	+	+	-	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	12
EKRA BE2502A0103	2	+	+	-	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	12
JSCVNIIR RITM	1	+	+	+	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	13
Prosoft-systems RES-3-6185C	2	+	+	-	-	-	-	+	+	-	+	+	-	-	-	-	-	+	+	-	8
URALENERGOSERVICE LLC KEDR-2.0	2	+	+	-	-	-	-	+	+	-	+	+	-	+	-	-	-	+	+	-	9
Prosoft systems MKPA	2	+	+	-	-	-	-	+	+	-	+	+	-	-	-	-	-	+	+	-	8
DEP depRTU	2	+	+	+	-	-	-	+	+	-	+	+	-	+	-	-	+	+	+	-	11
BMRZ-152-KSZ	2	+	+	+	-	-	-	-		-	+	+	-	-	-	-	-	+	-	-	6
BMRZ-LT	2	+	+	+	-	+	-	+	+	-	+	+	-	+	+	-	-	+	+	-	12
BMRZ-TD	2	+	+	-	-	-	-	-		-	+	+	-	-	-	-	-	+	-	-	5
Total		25	24	11	0	12	5	22	21	0	23	24	0	20	5	4	14	25	21	0	

Согласно статистике прошедших сертификационные испытания устройств, чаще всего реализуют следующие блоки соответствия сервисов: 1 Basic exchange, 13 Time sync, 2 Data Set, 9b GOOSE Subscribe, 9a GOOSE Publish, 5 Unbuffered Reporting, 6 Buffered Reporting, 14 File transfer 12a Direct Control. В устройствах вообще не реализованы: 3 Substitution, 7 Logging, 9c GOOSE management, 15 Tracking. Все эти сервисы не получили распространения и в мире: лишь несколько производителей реализовали данные сервисы в своих устройствах.

Сервис Substitution (подстановка) реализуют в своих устройствах такие известные компании, как Siemens, ABB, NARI, Beijing Sifang Automation. Logging (журналирование) сертифицировано всего на 1 устройстве Schneider Electric. GOOSE management вообще не сертифицирована ни на одном из устройств. Tracking (отслеживание) – ABB, Siemens, Sprecher, Toshiba, Beijing Sifang Automation.

Ниже приведен анализ, почему данные сервисы не востребованы производителями.

- Substitution – переводом устройства в режим тестирования и подачей сигналов в флагом качества Test для проверки функций устройства, а для проверки выходных реле возможно ручное управление состояние входов и выходов.
- Logging – данный сервис представляет интерес для производителя устройства, но для эксплуатирующей организации данная информация излишняя. Практически все

производители собирают данную информацию с помощью их собственного конфигурационного ПО.

- Tracking – используется для отслеживания изменений в устройствах как простых атрибутов, так отчетов и других блоков управления. В перспективе представляет интерес для эксплуатирующих организаций, т.к. имеет описанную в стандарте структуру данных, в отличие от Logging.

В целом, перечисленные сервисы являются вспомогательными для устройств вторичной коммутации и SCADA систем и информация, передаваемая через эти сервисы, и может быть представлена через другие сервисы, как указано выше.

В 2017 году ПАО «ФСК ЕЭС» ввело в действие СТО 56947007-29.120.70.241-2017, в котором были определены требования к наличию определенных сервисов МЭК 61850 (всего их 12) в устройствах релейной защиты и автоматики (РЗА). И, как видно из табл. 2, количество реализованных сервисов в устройствах РЗА после принятия упомянутого СТО увеличилось. До 2017 года в отечественном устройстве РЗА было в среднем реализовано 10,4 сервиса, а после уже 13,2.

Табл. 2. Распределение блоков сервисов МЭК 61850 по сертифицированным устройствам РЗА.

	ed.	1	2	2+	3	4	4+	5	6	7	9a	9b	9c	12a	12b	12c	12d	13	14	15	Итого	Год
BMRZ-152-KSZ	2	+	+	+	-	-	-	-		-	+	+	-	-	-	-	-	+	-	-	6	2014
BMRZ-LT	2	+	+	+	-	+	-	+	+	-	+	+	-	+	+	-	-	+	+	-	12	2016
BMRZ-TD	2	+	+	-	-	-	-	-		-	+	+	-	-	-	-	-	+	-	-	5	2014
EKRA BE2704	1	+	+	-	-	+	-	+	+	-	+	+	-	+	-	-	-	+	+	-	10	2015
OOO-MP3 MP3-1	1	+	+	-	-	+	-	+	+	-	+	+	-	+	-	-	+	+	+	-	11	2015
NPP-Bresler 0107.511	1	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	+	+	+	-	14	2015
IC-Bresler TOR200 L	1	+	+	-	-	-	-	+	+	-	+	+	-	+	-	-	+	+	+	-	10	2015
IC-Bresler TOR30C AUV KSZ	1	+	+	-	-	-	-	+	+	-	+	+	-	+	-	-	+	+	+	-	10	2015
RadiusAvtomatika Sirius-3-LV-03	2	+	+	+	-	-	-	+	+	-	+	+	-	+	-	-	-	+	+	-	10	2015
NIPOM P0301	1	+	+	+	-	+	-	+	+	-	+	+	-	+	-	-	-	+	+	-	11	2016
CHEAZ BEMP DZT	2	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	+	+	+	-	14	2016
TECON 311FS	2	+	+	-	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	12	2016
EKRA 217 0603	2	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	+	+	+	-	14	2017
CHEAZ BEMP RU-02.5.220.ET	2	+	+	+	-	+	+	+	+	-	+	+	-	+	+	+	+	+	+	-	15	2017
EKRA BE2704V019	2	+	+	-	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	12	2018
EKRA BE2502A0103	2	+	+	-	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	12	2018
JSCVNIIR RITM	1	+	+	+	-	+	+	+	+	-	+	+	-	+	-	-	+	+	+	-	13	2018

Ниже приведена статистика по сервисам всех сертифицированных устройств на соответствие серверу МЭК 61850 в UCAIug (табл. 3).

Табл. 3. Распределение блоков сервисов МЭК 61850 по сертифицированным устройствам на соответствие серверу МЭК 61850.

№	Сервис	Кол-во	% от общего числа
13	Time Synchronization	892	96,7%
1	Basic Exchange	886	96,1%

№	Сервис	Кол-во	% от общего числа
5	Unbuffered Reporting	852	92,4%
2	Data Sets	833	90,3%
6	Buffered Reporting	803	87,1%
12a	Direct Control	754	81,8%
9a	GOOSE Publish	750	81,3%
9b	GOOSE Subscribe	724	78,5%
14	File Transfer	674	73,1%
12d	Enhanced SBO Control	638	69,2%
4	Setting Group Selection	450	48,8%
12c	Enhanced Direct Control	434	47,1%
2+	Data Set Definition	312	33,8%
12b	SBO Control	291	31,6%
4+	Setting Group Definition	188	20,4%
3	Substitution	165	17,9%
15	Tracking	46	5,0%
7	Logging	1	0,1%
9c	GOOSE Management	0	0,0%
	Итого	922	

Как видно, в мире похожее с Россией распределение по использованию сервисов МЭК 61850. Это Time Synchronization, Basic Exchange, Unbuffered Reporting, Data Sets, Buffered Reporting, Direct Control, GOOSE Publish, GOOSE Subscribe, File Transfer, Enhanced SBO Control. Перечисленные сервисы были реализованы в более чем половине сертифицированных устройств.

Заключение

МЭК 61850 стал основным стандартом на «Цифровых подстанциях». И чтобы иметь возможность поставлять оборудование цифровые объекты, производителям необходимо иметь устройства, работающие согласно этому стандарту, соответственно реализовывать сервисы. В ближайшем будущем тенденция реализации сервисов сохранится прежней: отчеты, GOOSE, управление, передача файлов будут реализовываться практически во всех устройствах.

В свою очередь, эксплуатирующие организации заинтересованы в надежной работе своих объектов. Для этого они разрабатывают нормативную документацию, в частности, регламентирующую наличие тех или иных сервисов в устройствах вторичной коммутации, тем самым стимулируя производителей на реализацию требуемых сервисов. Именно эксплуатирующие организации будут определять востребованность тех или иных сервисов.

ЛИТЕРАТУРА

[1] Kasztenny B., Whatley J., Urden E.,Burger J., Finney D., Adamiak M. / Unanswered Questions about IEC 61850. What needs to happen to realize the vision? // 32nd Annual Western Protective Relay Conference, October 25-27, 2005

2.4. МАРШРУТИЗИРУЕМЫЕ GOOSE-СООБЩЕНИЯ И ИХ ПРИМЕНЕНИЯ В СИСТЕМАХ ПРОТИВОАВАРИЙНОЙ АВТОМАТИКИ

А. АПОСТОЛОВ

«ОМИКРОН электроникс»

США

Контактное лицо:

А. АПОСТОЛОВ

E-mail: alex.apostolov@omicronenergy.com

ВВЕДЕНИЕ

IEC 61850 has been identified for more than ten years as a cornerstone technology for the Smart Grid. Одним из ключевых компонентов, которые наделяют его такой ролью, являются общие объектно-ориентированные события на подстанции (GOOSE), которые обеспечивают одноранговую коммуникацию между многофункциональными интеллектуальными электронными устройствами (ИЭУ) и отвечают требованиям к высокоскоростной передаче данных между системами и устройствами защиты и автоматики. Изначально они были разработаны как немаршрутизируемые сообщения, используемые в пределах подстанции и передаваемые по локальной сети. Успех использования GOOSE-сообщений в системах релейной защиты подстанций делает его привлекательным для использования между ИЭУ в системах противоаварийной автоматики. Эти приложения накладывают ряд новых требований, связанных с одноранговыми коммуникациями. В настоящей публикации, во-первых, представляется концепция маршрутизируемых GOOSE-сообщений (R-GOOSE), а также обсуждаются вопросы их применения в системах передачи аварийных сигналов и команд.

Несмотря на то, что GOOSE-сообщения уже использовались в системах защиты и автоматики за пределами подстанций, тот факт, что они передаются по глобальным сетям, делает их уязвимыми для кибератак.

Для решения этой проблемы в рабочей группе 10 технического комитета 57 МЭК был разработан технический отчёт МЭК 61850-90-5 [2], который определил передачу синхронизированных векторных измерений и GOOSE-сообщений по глобальным сетям. Коммуникационный протокол базируется на полном 7-уровневом стеке OSI и использует групповую рассылку TCP/UDP. Документ также описывает использование сквозного шифрования на базе стандарта МЭК 62351.

Доступность безопасных одноранговых коммуникаций позволяет применять маршрутизируемые GOOSE-сообщения в системах противоаварийной автоматики. Двунаправленные коммуникации между устройствами РЗА и ПА, обеспечивающие мониторинг состояния энергосистемы, а также выполнение необходимых воздействий, необходимых для отключения поврежденных участков и поддержания устойчивости энергосистемы.

Преимущества применения R-GOOSE для систем противоаварийной автоматики представлены в заключении.

Схемы противоаварийной автоматики

Схемы противоаварийной автоматики (ПА) — это распределенные функции, базирующиеся на обмене информацией и сигналами управления между ИЭУ, расположенными на различных подстанциях и присоединениях по всей энергосистеме.

Они играют очень важную роль в поддержании надежного функционирования энергосистемы за счёт применения следующих функций:

- изменение конфигурации системы;
- адаптация уставок защит;
- управление распределенными источниками электроэнергии;
- управление нагрузкой;

- ограничение нагрузки.

Поэтому крайне важно убедиться, что они полностью испытаны перед вводом в работу.

ПА можно рассматривать как систему, состоящую из трех главных функциональных элементов:

- элементы мониторинга системы;
- элементы защиты;
- исполнительные элементы.

Элементы мониторинга системы выполняют следующие функции:

- обнаруживают изменения в электрической схеме;
- обнаруживают изменение нагрузки;
- обнаруживают изменения генерации.

Задачей противоаварийной автоматики является определение того, что какое-то из вышеперечисленных изменений или их комбинации представляют угрозу устойчивости энергосистемы. Если существует вероятность локального или широкомасштабного нарушения, необходимо принять решение и направить сигнал для выполнений действий, предотвращающих нарушение или, по крайней мере, снижающих негативные последствия от него.

Функция исполнительных органов заключается в том, чтобы получить сигнал от ПА и выполнить локально требуемые действия.

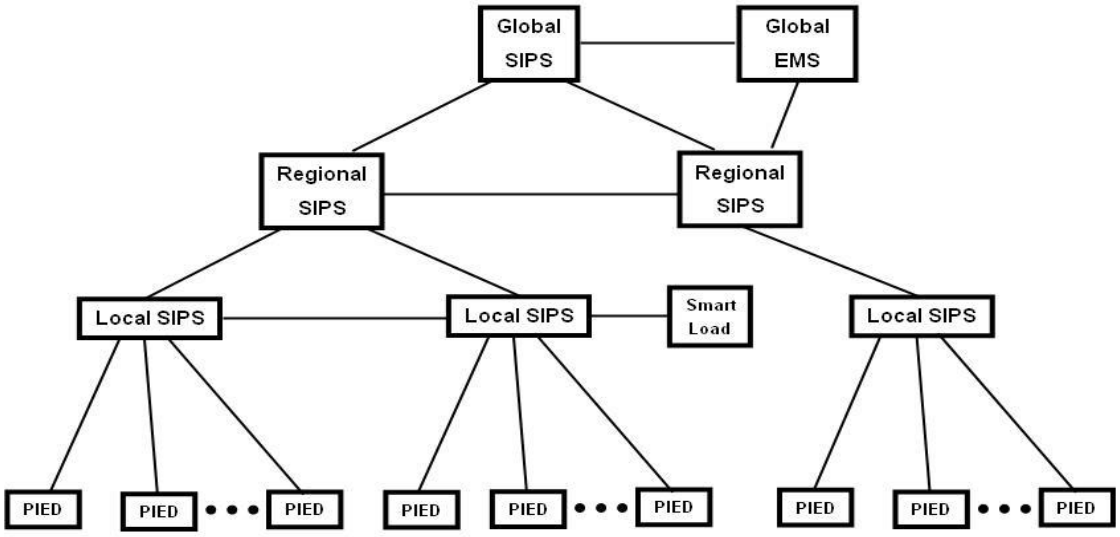


Рис. 1. Упрощенная структурная схема иерархической схемы противоаварийной автоматики.

ПА может быть простой или комплексной с различным количеством уровней иерархии в зависимости от сложности системы. На рис. 1 показана многоуровневая ПА, которая использует многофункциональные ИЭУ в качестве устройств, осуществляющие функции мониторинга и исполнительных органов на различных уровнях системы.

Как можно видеть на рис. 1, противоаварийная автоматика на системном уровне требует применения различных типов коммуникаций:

- между многофункциональными интеллектуальными электронными устройствами (ИЭУ) внизу иерархии и на уровне станции (локальная ПА);

- между устройствами ПА на одном уровне;
- между различными уровнями ПА;
- между системой ПА и интеллектуальной нагрузкой.

Все обозначенные выше коммуникационные интерфейсы могут базироваться на различных протоколах и использовать различные типы коммуникационных связей. МЭК 61850 играет возрастающую роль благодаря значительным преимуществам, которыми обладают высокоскоростные одноранговые сообщения при реализации различных функциональных элементов схемы.

Функции мониторинга обычно основываются на следующем:

- измерения тока, напряжения, активной и реактивной мощности;
- синхронизированные векторные измерения;
- мониторинг состояния коммутационных аппаратов, связанных с магистральными линиями, трансформаторами и генераторами.

Исполнительные элементы обычно воздействуют на выключатель или другие коммутационные устройства для выполнения определенных действий, таких как реконфигурация сети или сброс нагрузки. Они могут также снижать выработку распределенной генерации или полностью останавливать её.

GOOSE и R-GOOSE

GOOSE-сообщения были разработаны для обеспечения одноранговых коммуникаций на подстанциях и поэтому имеют трехуровневых коммуникационный стек и мультикаст MAC-адресацию.

Одноранговые коммуникации — это особый вид коммуникаций в системах на базе МЭК 61850. Это одна из отличительных особенностей стандарта, которая делает его привлекательным для специалистов в области РЗА. Одноранговые коммуникации дают возможность любой паре ИЭУ, подключенных к сети подстанции, обеспечивать информационный обмен с одинаковыми правами, в отличие от коммуникаций типа «ведущий — ведомый». Высокоскоростные одноранговые коммуникации в системах РЗА на базе МЭК 61850 используют специальные методы для достижения различных требований. Очень важно, что концепция модели Общего События на Подстанции (Generic Substation Event - GSE) основана на передаче функцией информации о возникшем событии на подстанции, а не передаче команды. Этот способ разработан для обеспечения надежной высокоскоростной коммуникации между различными устройствами или функциями и позволяет заменить проводные соединения между устройствами при помощи обмена сообщений, одновременно с этим увеличивая функциональность систем защиты, автоматики и управления. В рассматриваемом механизме используется модель «Издатель – Подписчик» без установления соединения между сторонами (рис. 2).

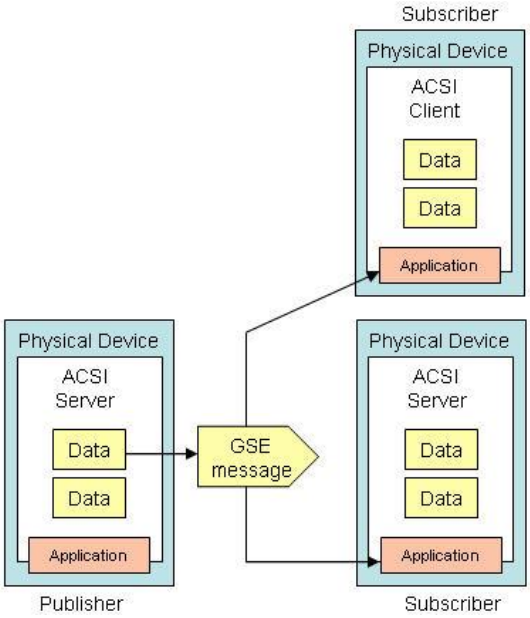


Рис. 2. Механизм «издатель — подписчик».

Модель включает несколько особенностей, которые могут быть использованы для повышения надежности и готовности системы. В то же время корректное использование этих возможностей в реализованных устройствах позволит сократить необходимый объем технического обслуживания и повысить гибкость системы. Изначально GOOSE-сообщения были разработаны для коммуникаций на подстанции, но благодаря тем преимуществам, которые они приносят, появилась необходимость определить способ их применения для коммуникаций между подстанциями.

Для понимания различий между подстанционными GOOSE и GOOSE, предназначенными для передачи по глобальной сети, необходимо рассмотреть некоторые детали модели Общего События на Подстанции.

Модель GSE можно рассматривать как механизм для оповещения информации о событии логическими устройствами. Достигаемая производительность в части задержек передачи данных, готовности и надежности зависит от реализации в конкретном устройстве.

Модель общего события на подстанции используется для обмена значениями из набора атрибутов данных, которые определяется как Набор Данных (Data Set). GOOSE поддерживает передачу широкого спектра типов данных, организованных в наборы данных.

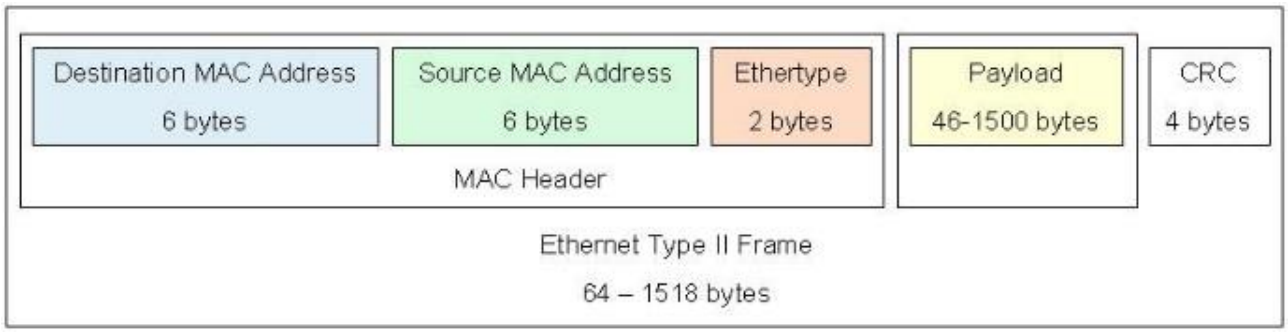
Издатель записывает значения в буфер передачи на передающем конце и распространяет их в широковещательном режиме по локальной сети подстанции различным подписчикам — клиентам или серверам.

Данные, передаваемые в GOOSE-сообщениях — это коллекция значений атрибутов данных, являющихся членами набора данных. Приёмник читает значения из локального буфера на приёмном конце. Управлением процесса передачи занимается блок управления GSE. Если значение хотя бы одного атрибута данных изменилось, буфер передачи

отправителя обновляется при помощи локальной службы публикации и значения передаются мгновенно с помощью GOOSE-сообщения.

Механизм издатель-подписчик позволяет ИЭУ-источнику доставить данные до нескольких приёмных ИЭУ, таким образом значительно повышая эффективность использования коммуникационного интерфейса. В коммуникационных сетях подстанций для этого применяется групповой (мультикаст) MAC-адрес в кадре Ethernet, как показано в табл. 1.

Табл. 1. Кадр Ethernet типа II.



Где:

адрес назначения (6 байт) идентифицирует станцию (-и), которой адресован кадр,

адрес источника (6 байт) определяет адрес источника сообщения.

Длина составляет 6 октетов и содержит значение адреса управления доступом к среде (MAC-адреса), по которому будет направляться GOOSE-сообщение. Адреса должны быть Ethernet-адресами, для которых бит групповой (multicast) рассылки установлен в значение TRUE.

Если порт подключен к 802.1Q-совместимому устройству (например, такому, как сетевой коммутатор), эти тегированные фреймы могут включать информацию по членству в виртуальных локальных сетях (VLAN), позволяя тем самым VLAN распространяться на множество коммутаторов.

Определенные коммуникационные сервисы у приёмника обновляют содержимое своих приёмных буферов, а полученные новы значения сразу передаются к соответствующим функциям.

Поскольку GOOSE-сообщения предназначены в качестве замены проводных связей, используемых для защиты и управления, в МЭК 61850 предусмотрены механизмы, позволяющие обеспечить надёжную доставку требуемой информации.

Когда новое значение атрибута привело к широковещательному распространению нового GOOSE-сообщения, механизм повторной отправки обеспечивает передачу того же значения с интервалом времени, увеличивающимся от минимального до максимального, и позднее передаётся с этим интервалом до очередного изменения.

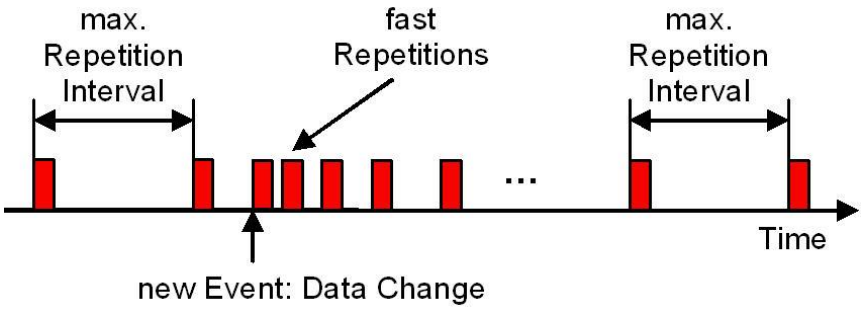


Рис. 3. Механизм повторной отправки GOOSE.

Как показано на рис. 3, сразу после изменения интервал очень короткий — всего несколько миллисекунд, а затем увеличивается, пока не достигнет значения в несколько секунд. Благодаря такому методу решаются две важные задачи:

- однократная потеря сообщения не приведет к отказу функционирования системы;
- любое новое устройство может информировать всех подписчиков о своём состоянии;
- позволяет любому новому устройству узнать состояние всех устройств-отправителей, на сообщения которых оно подписано.

GOOSE-сообщения содержат информацию, которая позволяет устройствам-подписчикам не только узнавать об изменении состояния, но также знать о том, когда последнее изменение состояния произошло. Это позволяет приёмникам устанавливать метку времени для любого события.

В то же время механизм повторной передачи может быть использован как способ непрерывной диагностики коммуникационного интерфейса — то, что было невозможным в традиционных системах с проводными соединениями.

GoCB class			
Attribute name	**Attribute type**	**r/w**	**Value/value range/explanation**
GoCBName	ObjectName		Instance name of an instance of GoCB
GoCBRef	ObjectReference		Path-name of an instance of GoCB
GoEna	BOOLEAN	r/w	Enabled (TRUE) | disabled (FALSE)
GoID	VISIBLE STRING129	r/w	Attribute that allows a user to assign an identification for the GOOSE message
DatSet	ObjectReference	r/w	
ConfRev	INT32U	r	
NdsCom	BOOLEAN	r	
DstAddress	PHYCOMADDR	r	
Services SendGOOSEMessage GetGoReference GetGOOSEElementNumber GetGoCBValues SetGoCBValues			

Рис. 4. Блок управления передачей GOOSE-сообщений.

Счетчик состояния и счетчик последовательности могут быть использованы для обнаружения сбоев и вторжений, существенно повышая, таким образом, информационную безопасность без необходимости применения шифрования или других методов ИБ.

Блок управления передачей GOOSE, определенный в редакции 2 [1] стандарта МЭК 61850 (см. рис. 4) включает атрибуты, которые определяют поведение одноранговых коммуникаций в отношении к режиму работы логического устройства, а точнее его логического узла LLN0.

Атрибут GoCBName (имя блока управления GOOSE) идентифицирует GoCB в пределах логического устройства, а GoCBRef (ссылка на блок управления GOOSE) — это уникальный путь к блоку управления:

LDName/LLN0.GoCBName

GoEna (включить GOOSE) указывает, что блок управления GOOSE (если установлен в значение TRUE) введет в работу для отправки GOOSE-сообщений. В значении FALSE он перестаёт передавать GOOSE-сообщения.

Идентификатор GoID — это задаваемая пользователем идентификация GOOSE-сообщения.

Атрибут DatSet — это ссылка на набор данных, атрибуты которого будут передаваться.

ConfRev — это атрибут, определяющий количество раз изменения конфигурации ссылок в наборе данных. Счётчик увеличивается каждый раз, когда конфигурация изменяется.

NdsCom (требуется наладка) устанавливается в значение ИСТИНА, если атрибут DatSet имеет пустое значение, чтобы указать на необходимость донастройки блока управления GoCB.

Адрес DstAddress — это специфический адрес конкретного комуникационного протокола, например, MAC-адрес, указатель приоритета и другая информация

Table 9-3 – R-GOCB Definition

Attribute name	Attribute type	r/w	m	Value/value range/explanation
GoEna	Boolean	rw	m	
GoID	Visible-string	r	m	
DatSet	Visible-string	r	m	
ConfRev	Unsigned	r	m	
NdsCom	Boolean	r	m	
DstAddress	UDPCOMADDR*	r	m	
MinTime	Unsigned	r	o	
MaxTime	Unsigned	r	o	
FixedOffs	Boolean	r	o	
SecurityEnable**	ENUMERATED	r	o	None, Signature, SignatureAndEncryption
* The definition of UDPCOMADDR can be found in Table 9-5. **Additional attribute to be added to the control block.				

Рис. 5. Блок управления R-GOOSE.

Для блока управления R-GOOSE, определенного в МЭК 61850-90-5, атрибут DstAddress имеет формат UDPCOMMADR. Его структура включает атрибуты, которые поддерживают применение как IPv4, так и IPv6 адресов.

Как уже отмечалось, содержание GOOSE-сообщения позволяет принимающим устройствам выполнять обработку данных для исполнения необходимых действий. Ниже представлены некоторые атрибуты GOOSE-сообщения, которые помогают выполнять ранее описанные функции.

T — метка времени, указывающая на момент времени последнего изменения значения счётчика StNum.

Значение StNum указывает на номер состояния — счётчик, который увеличивается всякий раз, когда изменяются значения атрибутов данных, передаваемых в GOOSE-сообщении. Начальное значение — 1.

SqNum — это последовательный счетчик, значение которого увеличивается каждый раз при повторной отправке GOOSE-сообщения без изменений данных. Начальное значение — 1.

Simulation – это параметр, указывающий, что GOOSE-сообщение используется для целей тестирования (если флаг Simulation имеет значение TRUE), а сообщение было передано

испытательной установкой и не должно использоваться для нормального функционирования.

Подписчик GOOSE-сообщения будет обрабатывать симулированное сообщение вместо реального рабочего в том случае, если соответствующий режим введён в ИЭУ.

Это неприменимо к сообщениям, которые передаются по глобальной сети. По этим причинам в техническом отчёте МЭК 61850-90-5 в качестве протокола передачи данных на неограниченно большие расстояния был выбран протокол UDP/IP.

Протокол Интернет (IP) — это протокол 3-го уровня. Сетевой уровень добавляет возможность маршрутизации сообщений поверх канального уровня. При приёме данных на сетевом уровне, данные об адресе источника и назначения, содержащиеся в каждом пакете, проверяются, чтобы определить достигли ли данные финального адреса назначения. Если да, то данные третьего уровня форматируются в пакеты, передаваемые на транспортном уровне. Протокол IP позволяет маршрутизировать пакеты данных (IP-пакеты) между различными сетями на любые расстояния.

Протокол Пользовательских Датаграмм (UDP) — это транспортный протокол 4-го уровня. Тогда как TCP (Протокол Управления Передачей) — это протокол, предполагающий установку соединения между клиентом и сервером перед началом передачи, UDP — не требуется предварительной установки соединения, что делает его более подходящим для GOOSE-коммуникаций.

Сетевой трафик UDP организуется в форме датаграмм. Датаграмма состоит из одного блока сообщения. Первые 8 (восемь) байт датаграммы содержат заголовочную информацию, а остальные — данные сообщения.

Датаграмма UDP состоит из 4 полей по 2 байта каждое:

- номер порта источника;
- номер порта назначения;
- размер датаграммы;
- контрольная сумма.

Контрольная сумма UDP защищает сообщение от изменения при передаче. Значение контрольной суммы представляет собой закодированное значение датаграммы, вначале рассчитанное отправителем, а потом рассчитываемое приёмником в целях проверки. Если контрольная сумма не совпадает, что указывает на искажение или повреждение информации при передаче, протокол UDP обнаружит это. Контрольная сумма в UPD является необязательной в отличие от TCP, где она является обязательной.

Множество применений протокола IEEE C37.118 с использованием UDP для поточной передачи данных синхронизированных векторных измерений свидетельствуют о возможности применения этого протокола и для маршрутизируемых GOOSE-сообщений.

В таблице ниже показаны требования по применению UDP.

Табл. 2. Требования по реализации UDP.

UDP	Mandatory/Optional/ eXcluded
Source Port	M
Destination Port	M
Length	M
Checksum	M

Применение R-GOOSE в противоаварийной автоматике (ПА)

The R-GOOSE described above has multiple applications in SIPS. Применение R-GOOSE приносит ряд существенных преимуществ для глобальных распределенных приложений, в особенности когда они основаны на беспроводных коммуникационных технологиях. Требования по защите информации, определенные в МЭК 61850-90-5 и МЭК 62351 обеспечивают высокий уровень защищенности, являющийся одним из ключевых аспектов для ПА.

R-GOOSE могут применяться как для вертикальных, так и для горизонтальных коммуникаций в иерархических ПА.

Ниже приведены некоторые возможные применения R-GOOSE коммуникаций в ПА.

- Передача R-GOOSE с аналоговыми значениями нагрузки и выработки между локальными элементами мониторинга системы ПА и верхними уровнями иерархии ПА.
- Передача R-GOOSE с дискретными сигналами положений коммутационных аппаратов между локальными элементами ПА и верхними уровнями ПА.
- Передача R-GOOSE с аналоговыми значениями агрегированной нагрузки и мощности между верхними уровнями ПА.
- Передача сигналов отключения и управления между верхними уровнями ПА и локальными исполнительными элементами с помощью R-GOOSE.

ВЫВОДЫ

R-GOOSE является важным дополнением в арсенале инструментов инженеров РЗА, занимающихся разработкой схем ПА.

Протокол позволяет разрабатывать и реализовывать высокоскоростные одноранговые коммуникации в схемах противоаварийной автоматики, что позволяет повысить надежность энергосистемы.

ССЫЛКИ

[1] IEC TR 61850 7-2:2010 Communication networks and systems in substations –Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)

[2] IEC TR 61850 90-5:2012 Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

[3] IEC TS 62351-6:2007 Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850

2.5. ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ОЦЕНКИ СООТВЕТСТВИЯ ТЕХНИЧЕСКИХ РЕШЕНИЙ РЗА И АСУ ТП ТРЕБОВАНИЯМ КОНКУРСНОЙ ДОКУМЕНТАЦИИ

М.И. ШВЕДОВ

ОАО «МРСК Урала»

РОССИЯ

Контактное лицо:

М.И. ШВЕДОВ

shvedov@ rosseti-ural.ru

ВВЕДЕНИЕ

Бизнес-процесс создания цифровых подстанций предполагает создание файлов электронной документации на языке SCL согласно стандарту IEC 61850. На стадии разработки проектной документации формируется файл электронного описания спецификации SSD (System Specification Description). SSD-файл описывает однолинейную схему подстанции, определяет состав оборудования, реализуемые функции и требования ко всем системам цифровой подстанции, вне зависимости от производителя (рис. 1).

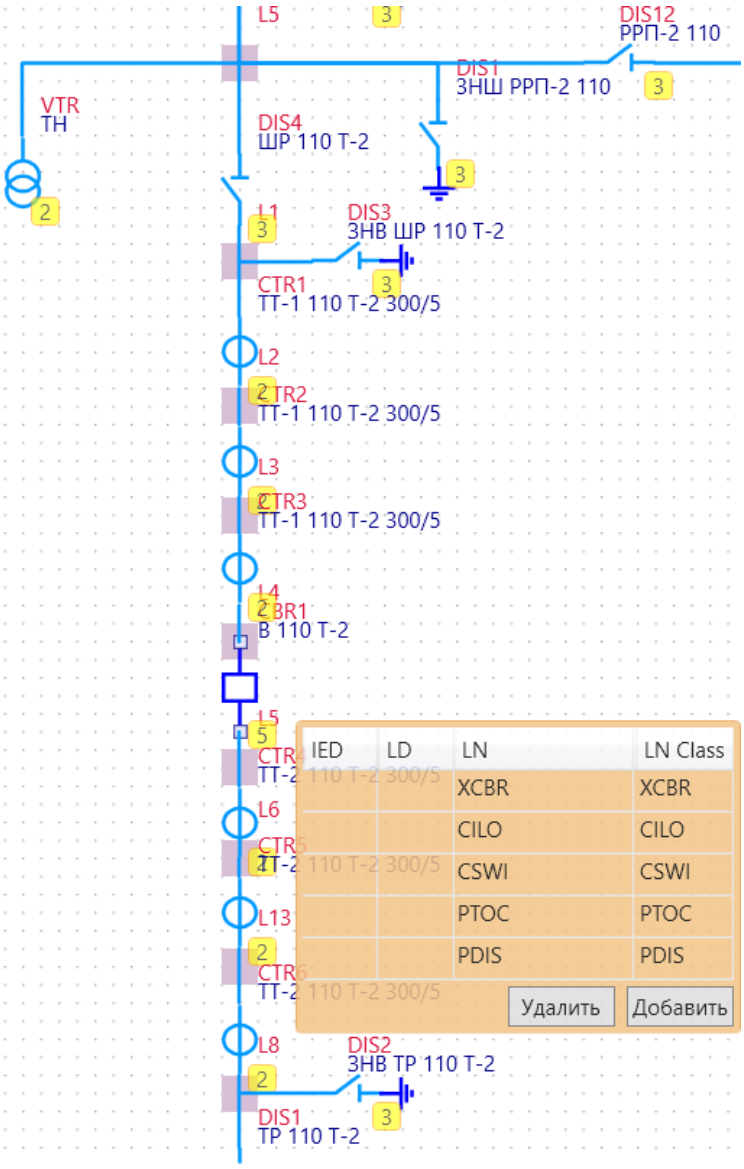


Рис.1. Создание SSD-файла в САПР.

Формирование SSD-файла на этапе разработки проектной документации позволяет:

1. Получить типизированное электронное описание первичного оборудования подстанции согласно IEC 61850-6 для упрощения оценки результатов проектирования и интеграции электронной схемы в SCADA.

2. Получить перечень функций вторичных систем подстанции с привязкой к первичному оборудованию.

3. Типизировать проектные решения, описанные в едином формате, что позволяет упростить их анализ и редактирование.

Файл SSD является основной частью конкурсной документации, на его основе происходит выбор подходящего оборудования. Особое внимание требуется уделять распределению функций защит и автоматики на все присоединения.

Следующим этапом при выборе оборудования является проверка соответствия предлагаемого состава функций в файлах конфигурации терминалов производителей ICD с требуемым набором функций в файле SSD. Для корректного сравнения оба файла должны быть описаны в стандартизированной семантике и синтаксисе IEC 61850. Этот процесс крайне важен, ведь таким образом заказчик выбирает наиболее подходящие терминалы под необходимые функции цифровой подстанции. Зачастую в терминалы закладывают намного больше функций, чем необходимо реализовать на объекте впоследствии. За счёт оптимизации функционала происходит коррекция стоимости оборудования, что является важным фактором для электросетевой компании при выборе оборудования разных производителей. При проведении конкурсных процедур сравнение файла SSD и файлов ICD заводов-изготовителей будет иметь главное значение для определения победителя на поставку оборудования для цифровых подстанций. Вручную выполнять сравнение SSD-файла и нескольких десятков ICD-файлов достаточно сложно и трудозатратно, данный процесс требует автоматизации.

Автоматизация процесса предполагает создание методики и алгоритмов для оценки соответствия предлагаемых технических решений в части РЗА и АСУ ТП требованиям технической части конкурсной документации. Важным требованием к процессу сравнения SSD и ICD-файлов является предварительная валидация относительно схемы SCL стандарта МЭК 61850 в соответствующей редакции для исключения получения некорректных отчётов и проведения некачественного отбора производителей оборудования. Данный процесс возможен только при качественно спроектированном SSD-файле с полным распределением всех требуемых узлов к присоединениям и одновременно корректными ICD-файлами для каждого присоединения.

В России на данный момент имеется пока единственное решение для данной процедуры. По заказу ОАО «МРСК Урала» была выполнена научно-исследовательская работа по разработке методики алгоритмов для оценки соответствия предлагаемых технических решений в части РЗА и АСУ ТП требованиям технической части конкурсной документации, сформированной в виде SSD-файла. Итогом работы стал программный комплекс, отвечающий всем требованиям для проведения конкурсных процедур.

Функционал программного комплекса

	Действия пользователя	**Функционал ПК**	**Ожидаемый результат**
	Загрузка SSD-файла	Обработка SSD-файла и его валидация	Успешная загрузка при прохождении

		относительно схемы SCL стандарта МЭК 61850 (1, 2 редакция)	валидации (корректный синтаксис файла SSD)
			Неуспешная загрузка (файл имеет ошибки и требуется его доработка/корректировка в САПР проектной организацией)
	Загрузка файлов ICD (файлы конфигурации терминалов заводов-изготовителей)	Обработка ICD файлов и их валидация относительно схемы SCL стандарта МЭК 61850 (1, 2 редакция)	Успешная загрузка при прохождении валидации (корректный синтаксис файла ICD)
			Неуспешная загрузка (файл имеет ошибки и требуется его доработка / корректировка заводом-изготовителем)
	Запуск проверки соответствия	Проверка соответствия требований обрабатываемого SSD-файла доступной функциональности МП устройств согласно их файлам ICD	Формирование отчётов о соответствии требованиям файла SSD по отдельной заявке или сравнительном анализе предложений разных поставщиков (рис. 2)
	Анализ отчётов специалистами заказчика		
	Выбор наиболее подходящего оборудования для реализации проекта		

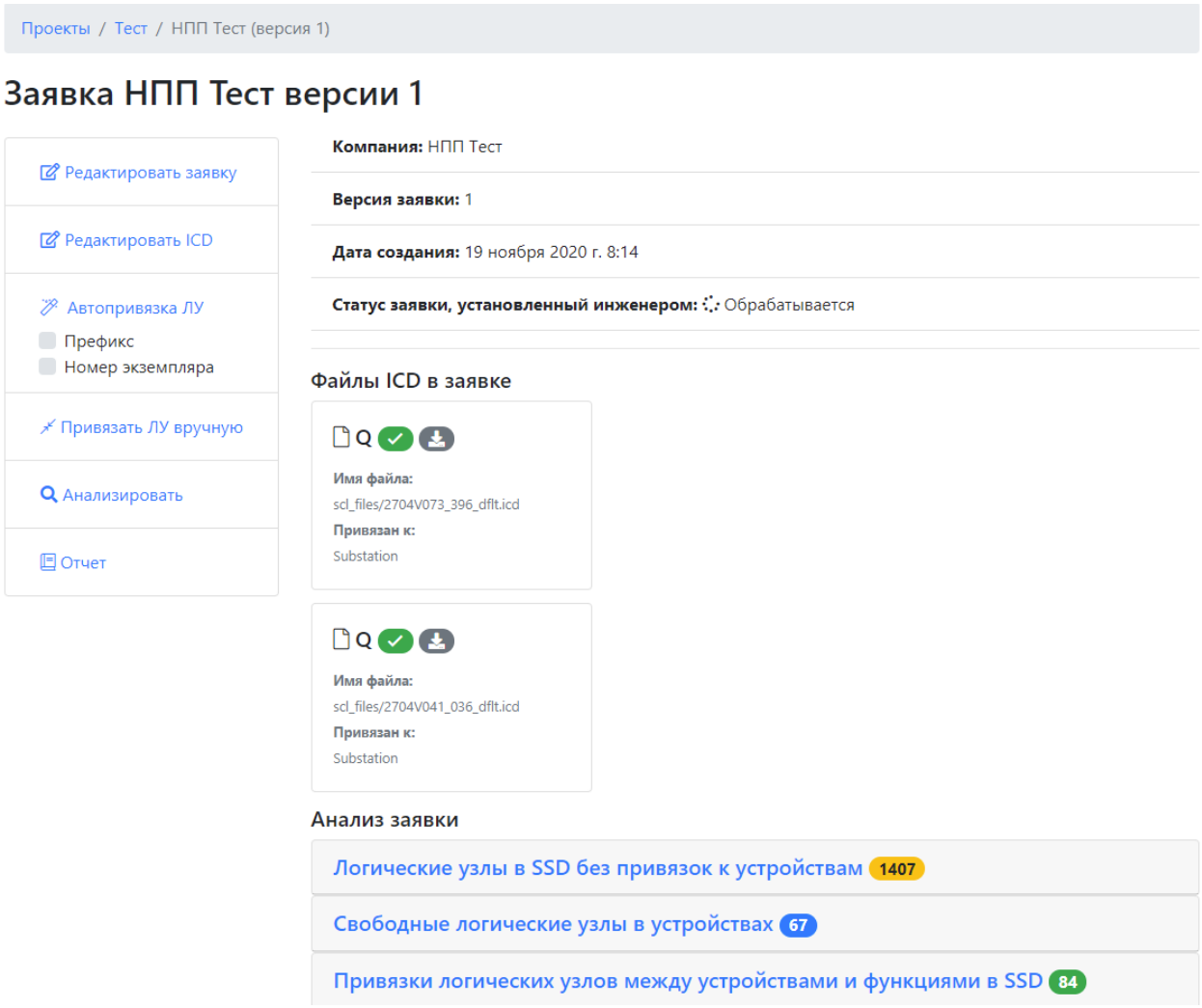


Рис. 2. Функционал комплекса после запуска процесса анализа.

Согласно разработанной методике в программный комплекс загружается SSD-файл подстанции и создаётся необходимое количество заявок для каждого производителя. В заявку загружаются ICD-файлы (для примера на рис. 2 указаны только два файла, на самом деле их должно быть намного больше), и проводится анализ индивидуально по каждой заявке. Результатом анализа служат три набора узлов:

1. **Узлы в SSD без привязки к устройствам.** Все узлы в SSD должны быть привязаны, иначе последующее проектирование SCD будет невозможным без корректировки. На данный список требуется обратить особое внимание, т.к. предлагаемое оборудование не соответствует требованиям технической части заказчика.
2. **Свободные узлы в устройствах.** Данный список является возможностью для оптимизации набора функций в устройствах, что, возможно, приведет к снижению стоимости оборудования. Также на список следует обратить внимание, т.к. следует рассмотреть возможность расширения подстанции и, соответственно, заложить заранее необходимые узлы в проект. В этом случае наличие узлов в списке не будет являться недостатком.

3. **Привязки узлов между функциями SSD и ICD.** В данном списке отображаются все связанные узлы, что является формой для подведения итогов экспертизы проекта (рис. 3).

Привязки логических узлов между устройствами и функциями в SSD 84

#	ЛУ в SSD	ЛУ в ICD	Имя файла ICD	Анал
1	Substation# PowerTransformer#T1, LNode#GASTSIML1	IED#Q, AccessPoint#S1, Server#None, LDevice#LD, LNode#SIML1	scl_files/2704V073_396_dflt.icd(11)	
2	Substation# PowerTransformer#T1, LNode#GASTSIML2	IED#Q, AccessPoint#S1, Server#None, LDevice#LD, LNode#SIML2	scl_files/2704V073_396_dflt.icd(11)	
3	Substation# PowerTransformer#T2, LNode#GASTSIML1	IED#Q, AccessPoint#S1, Server#None, LDevice#LD, LNode#SIML3	scl_files/2704V073_396_dflt.icd(11)	
4	Substation# PowerTransformer#T2, LNode#GASTSIML2	IED#Q, AccessPoint#S1, Server#None, LDevice#LD, LNode#SIML4	scl_files/2704V073_396_dflt.icd(11)	
5	Substation# VoltageLevel#G1, Bay#W1G, ConductingEquipment#QSG11_W1G, LNode#W1G_QSG11CSWI1	IED#Q, AccessPoint#S1, Server#None, LDevice#LD, LNode#QCSWI1	scl_files/2704V073_396_dflt.icd(11)	
6	Substation# VoltageLevel#G1, Bay#T1G, LNode#INSTPDIF1	IED#Q, AccessPoint#S1, Server#None,	scl_files/2704V041_036_dflt.icd(10)	

Рис.3. Список связанных логических узлов.

Грамотно спроектированный SSD-файл позволяет сократить время на проектирование SCD. Сейчас мало времени уделяют SSD-файлу в связи с отсутствием каталога типов узлов. В созданных проектах подстанций в основном сигналы передаются в узлах общего назначения GGIO, каждый сигнал должен иметь описание, иначе это будут обезличенные сигналы, которые сложно будет идентифицировать при экспертизе и, соответственно, увеличится время экспертизы и создаст дополнительные проблемы наладчикам.

Опытная эксплуатация программного комплекса демонстрирует множество проблем в процессе создания цифровой подстанции. Главной проблемой является некачественный SSD-файл, для решения которой требуется активное и осознанное участие заказчика в процессе проектирования и грамотное проектирование подрядной организацией. В дальнейшем возникает вопрос о том, кто должен создавать SSD-файл, т. к. специалисты эксплуатирующей организации лучше знают детали, например, реконструируемой подстанции и на определение состава функций в устройства займёт гораздо меньше времени.

Необходимо отметить, что данный программный комплекс является частью бизнес-процесса и использовать только его недостаточно для качественной работы. SSD-файл перед загрузкой в программный комплекс требуется предварительно проверить в независимом программном комплексе для экспертизы, приёмки и дальнейшей корректной работы файла. Как должен выглядеть бизнес-процесс?

1. Формирование проектной организацией SSD-файла с учётом требований электросетевой компании по описанию однолинейной схемы первичного оборудования, составу реализуемых функций и их распределению оборудованию без привязки к производителям устройств РЗА и АСУ ТП.
2. Проверка SSD-файла в независимом от производителей ПТК (валидация относительно схемы SCL).
3. Загрузка файлов SSD подстанции и ICD одного производителя или нескольких в ПК. У каждого производителя должен быть ICD файл на каждое уникальное устройство с определенным набором заложенных функций (защиты отходящей линии 6-35 кВ, защиты трансформатора, защиты ЛЭП 110 кВ и т. д.). Таким образом, ПК проводит анализ и сравнение SSD-файла с несколькими файлами ICD каждого производителя. ПК сравнивает требуемые функции в SSD и имеющиеся функции в ICD.
4. По результатам анализа проводится конкурс и определяется завод-изготовитель для сборки оборудования с необходимым функционалом.
5. SSD-файл подстанции и ICD-файлы терминалов направляются проектной организации.
6. Проектная организация формирует SCD-файл (файл конфигурации подстанции) из SSD и ICD файлов.
7. Проверка SCD-файла в независимом от производителей ПТК.
8. Формирование рабочей документации.
9. Стадия ПНР – наладчики загружают проверенный SCD-файл в терминалы и проводят необходимые испытания и проверки.
10. Эксплуатация.

По итогам внедрения и опытной эксплуатации были сделаны следующие выводы.

1. Описанный выше комплексный подход, а именно проектирование SSD-файла на начальном этапе, при создании цифровой подстанции имеет наибольший экономический эффект, т. к. задействует разные автоматизированные программные комплексы и практически исключает ошибки до стадии ПНР, что позволяет существенно сократить время на всех стадиях процесса.
2. Для более эффективного распределения трудозатрат и качественного отбора поставщиков оборудования требуется внедрение нескольких программных комплексов для экспертизы файлов и их сравнения.

3. Применение ПК в ОАО «МРСК Урала» на данный момент недостаточно широко в связи с некачественно выполненными работами до конкурсных процедур. В перспективе ПК должен стать одним из основных инструментов в процессе проектирования ЦПС, которым должны пользоваться все электросетевые компании.

2.6. ОСОБЕННОСТИ ТЕСТИРОВАНИЯ ВЗАИМОДЕЙСТВИЯ СЛОЖНЫХ УСТРОЙСТВ РЗА НА ЦИФРОВОЙ ПОДСТАНЦИИ

М.Н. ХАБИБУЛЛИН, А.М. ТУИТЯРОВ, И.Г. НУРТДИНОВ

АО «Сетевая компания»

г. Казань

Ключевые слова:

МЭК 61850, цифровая подстанция, эксплуатация.

На сегодняшний день на объектах АО «Сетевая компания» эксплуатация устройств релейной защиты и автоматики, автоматизированной системы управления технологическими процессами производится согласно действующей нормативно-технической документации [1-2].

Ввиду активного освоения и внедрения технологии цифровых подстанции в АО «Сетевая компания» вопросы эксплуатации РЗА и АСУТП стоят особенно остро.

При этом в процессе эксплуатации возникают следующие вопросы:

• какую методику применять при проведении проверки взаимодействия устройств с фиксацией прохождения GOOSE – сообщений и SV потоков без воздействия на смежное оборудование;

• какую версию стандарта МЭК 61850 применять при проектировании цифровых подстанций;

• как разделять зоны ответственности персонала, отвечающего за работоспособность и техническое обслуживание различных элементов цифровой подстанций.

С этими и многими другими вопросами уже сталкиваются электросетевые компании.

Принципиальный порядок и последовательность выполнения испытаний и измерений устройств релейной защиты, автоматики и телемеханики, такие как проверка алгоритмов срабатывания устройств РЗА, проверки аналоговых входов, дискретных входов и выходов, электрической прочности изоляции при переходе с традиционной на цифровую подстанцию не меняются. Основные изменения касаются принципов проверки взаимодействия устройств релейной защиты, АСУТП и учета электрической энергии.

В АО «Сетевая компания» принят 8-летний цикл технического обслуживания устройств РЗА. Согласно нормативно-техническим документам техническое обслуживание УРЗА подразделяется на наладку, первый профилактический контроль, профилактический контроль, профилактическое восстановление.

Техническое обслуживание устройств РЗА и АСУТП можно разделить на обслуживание с выводом первичного оборудования и без вывода первичного оборудования.

Техническое обслуживание без вывода первичного оборудования обусловлено наличием общеподстанционных устройств релейной защиты и противоаварийной автоматики, таких как дифференциальная защита шин, автоматическая частотная разгрузка. Зачастую сжатые сроки вывода первичного оборудования не позволяют проверить все устройства РЗА в полном объеме. В связи с этим, возникает необходимость в выводе устройств РЗА без вывода первичного оборудования.

Независимо от того, как производится техническое обслуживание – с выводом первичного оборудования или без, вопрос проверки взаимодействия устройств в действующей локально-вычислительной сети без реального воздействия на смежные системы остается актуальным для персонала, обслуживающего подстанции, в которых связи между смежными системами можно разорвать физически.

Следует выделить основные требования к обслуживанию цифровых подстанций:

• проверки взаимодействия необходимо проводить в рабочей схеме без исключения проверяемых устройств из локально-вычислительной сети;

• проверка GOOSE-сообщений и SV-потоков, отправленных с помощью испытательной установки и принимаемых устройствами, должна производиться с использованием специального флага, который присваивается всему сообщению для исключения воздействий на смежное оборудование;

• в децентрализованной архитектуре релейной защиты, устройства при проверке должны быть полностью переведены в режим тестирования со всеми стандартными функциями и пользовательскими алгоритмами. Смежное устройство, находящееся в рабочем состоянии, например, ДЗШ, принимающее GOOSE-сообщения, должно зафиксировать это сообщение, но со специальной меткой качества без воздействия на отключение.

Дифференциальная защита шин (ДЗШ) является сложной защитой, работа которой зависит сразу от нескольких устройств – измерительных преобразователей и устройств РЗА. При отказе выключателя присоединения посредством соответствующего сигнала (УРОВ), отправленного на терминал ДЗШ, должна быть погашена вся секция шин, закрепленная за этим присоединением (рис. 1.).

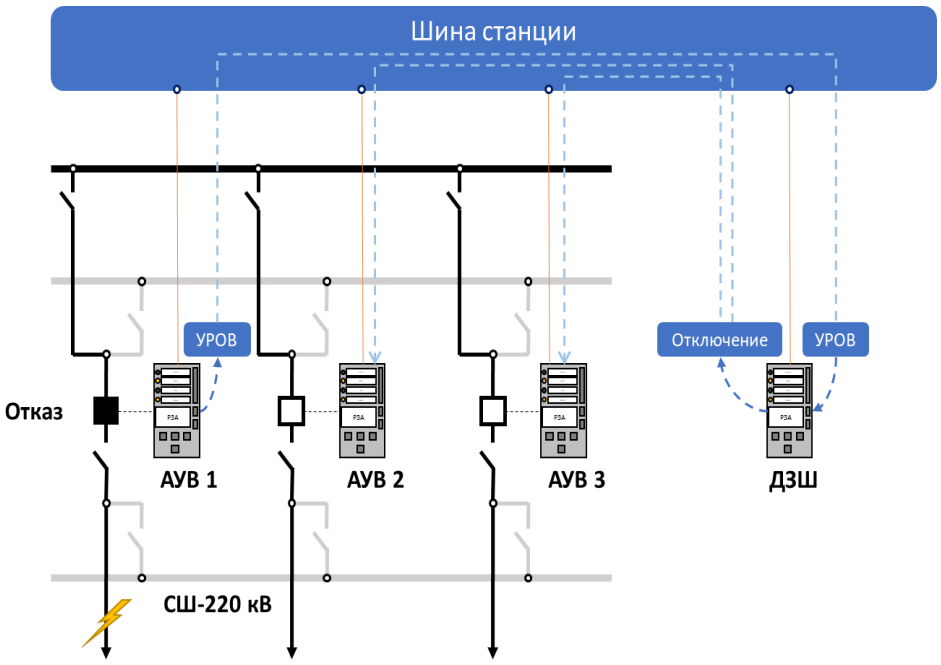


Рис. 1. Работа УРОВ на ПС 220 кВ.

На действующей цифровой подстанции данный сигнал отправляется по шине станции или шине процесса по протоколу МЭК 61850-8-1 посредством GOOSE-сообщения.

В условиях эксплуатационных испытаний (например, во время первого профилактического контроля) терминал обычно переводится в режим «TEST ON», а присоединение полностью выводится из работы. При этом терминал реагирует на подписанный SV-поток и принимает GOOSE сообщения с соответствующих преобразователей

аналоговых сигналов (ПАС) и преобразователей дискретных сигналов (ПДС), которые находятся в режиме «TEST ON». Интеллектуальные электронные устройства (IED), находящиеся в рабочем режиме «TEST OFF», сообщения с меткой «TEST» не принимают.

Для проверки взаимодействия нескольких терминалов, необходимо все терминалы перевести в один режим работы. Например, при проверке прохождения сигнала УРОВ от терминала АУВ 1 до терминала ДЗШ необходимо полностью вывести терминал ДЗШ из работы, что нежелательно. При выводе ДЗШ из работы резервирует его функции, как правило, суммарная резервная защита шин (СРЗШ), которая выполняет также функцию УРОВ, но с большей выдержкой времени, в отличие от быстродействующей ДЗШ.

На сегодняшний день данная проверка может производиться двумя способами: анализом сетевого трафика с помощью сниффера или полным выводом всех IED из работы для их тестирования.

Первый способ подразумевает высокую степень сложности операций и влияние человеческого фактора на результат. Во втором случае в процедуру тестирования включаются долгосрочные работы по выводу IED из работы. Кроме того, на подстанциях, где проводится реконструкция, нет возможности вывести все присоединения из работы.

Для упрощения проведения данной проверки и отказа от вывода терминала ДЗШ из работы предлагается следующее решение. Реализовать на IED, который находится в режиме «TEST OFF», возможность фиксации сообщений с меткой «TEST» без воздействия на конечные элементы управления.

СПИСОК ЛИТЕРАТУРЫ

[1] СТО 56947007-33.040.20.141-2012. Правила технического обслуживания устройств релейной защиты, автоматики, дистанционного управления и сигнализации подстанций 110-750 кВ. Стандарт организации ОАО «ФСК ЕЭС». Дата введения 2012-12-28

[2] СТО 56947007-25.040.40.236-2016. Правила технической эксплуатации АСУ ТП ПС ЕНЭС. Общие технические требования. Стандарт организации ПАО «ФСК ЕЭС». Дата введения: 15.12.2016.

2.7. АНАЛИЗ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СТАНДАРТА МЭК 61850 ДЛЯ ГЭС И ГАЭС

Д.А. ЖУКОВ, А.В. ГОЛОВИН,

ПАО «РусГидро», ООО «ТЕКВЕЛ»

Российская Федерация

Контактное лицо:

Жуков Дмитрий Андреевич

ZhukovDA@rushydro.ru

Ключевые слова:

МЭК 61850, ГЭС, ГАЭС.

ВВЕДЕНИЕ

Стандарт МЭК 61850 широко применяется на электрических станциях и подстанциях как в Российской Федерации, так и за рубежом. Преимущества стандарта МЭК 61850 над другими существующими стандартами на коммуникационные протоколы в электроэнергетике заключаются в наличии следующих аспектов:

- единая система наименования данных: стандарт определяет классы логических узлов и общие классы данных. Логические узлы представляют собой модель той или иной функции и включают в себя описание её входных и выходных данных – объектов данных, принадлежащих определённому общему классу данных. Общие классы данных, в свою очередь, определяют атрибуты данных. Классы логических узлов, объекты и атрибуты данных имеют определённое наименование. При организации передачи данных производится передача не индексированных точек данных, как в других существующих коммуникационных протоколах, а вышеупомянутых объектов и атрибутов данных, что значительно упрощает процедуры инжиниринга и эксплуатации систем автоматизации энергообъектов;
- коммуникационные сервисы для решения различных задач в рамках информационно-технологических систем энергообъектов: стандарт не ограничивается набором коммуникационных сервисов, предназначенных для интеграции устройств в АСУ ТП, включая в себя сервисы для передачи мгновенных значений (Sampled Values) и быстрой передачи дискретных и аналоговых событий (GOOSE), что не предполагают другие коммуникационные стандарты;
- язык конфигурирования системы: стандарт определяет язык конфигурирования системы System Configuration Language (SCL) для описания моделей данных устройств и информационного обмена между ними. С использованием данного языка и файлов на его основе возникает возможность автоматизировать выполнение пуско-наладочных работ, загружая файлы SCL, разработанные на этапе проектирования, в интеллектуальные электронные устройства (ИЭУ) на этапе пусконаладки.

Основные главы первой редакции стандарта МЭК 61850 были изданы в период с 2002 по 2005 гг. Первоначальной задачей, которая решалась при разработке стандарта, - стандартизация информационного обмена в пределах систем автоматизации подстанций. Первая редакция фокусировалась, прежде всего, на комплексах релейной защиты, автоматики и АСУ ТП подстанций. Начиная с 2009 года, уже изданные главы были обновлены и также были разработаны новые документы, которые также затронули вопросы организации измерений, контроля качества электроэнергии, мониторинга и диагностики электрооборудования и др. Расширилась и область применения стандарта: она вышла за пределы подстанции, сегодня стандартом рассматриваются следующие аспекты:

- моделирование функций и данных гидроэлектростанций и малой генерации ([1] и [2] соответственно);
- моделирование функций и данных ветроэлектростанций (документы серии МЭК 61400);
- описание коммуникаций между подстанциями, а также между подстанциями и центрами управления ([3] и [4], соответственно);
- моделирование функций и данных автоматики распределительной сети и др.

Учитывая это, стандарт получил наименование стандарта для коммуникационных сетей и систем для объектов электроэнергетики – Communication networks and systems for power utility automation.

В настоящей публикации особое внимание уделено применению стандарта МЭК 61850 в рамках систем автоматизации гидроэлектростанций (ГЭС) и гидроаккумулирующих электростанций (ГАЭС), в частности, в контексте использования стандарта МЭК 61850 для реализации специфичных программно-технических комплексов (ПТК) ГЭС/ГАЭС, а также представлен анализ стандарта [1] - МЭК 61850-7-410 «Гидроэлектростанции – Системы связи для мониторинга и управления» и технического отчёта [5] - МЭК 61850-7-510 «Руководящие указания по моделированию данных на гидроэлектростанциях», анализ достаточности положений указанных документов и примеры моделирования ПТК, специфичных для ГЭС/ГАЭС.

ДОКУМЕНТЫ СЕРИИ МЭК 61850, ПРИМЕНИМЫЕ ДЛЯ ГЭС/ГАЭС

Существует два документа из серии МЭК 61850, относящиеся к ГЭС/ГАЭС:

- Международный стандарт МЭК 61850-7-410, редакция 2.1. Данный стандарт определяет дополнительные общие классы данных и классы логических узлов, необходимые для применения стандарта МЭК 61850 на ГЭС/ГАЭС. Основные отличия редакции 2.1 данного стандарта по отношению к предыдущим редакциям заключаются в следующем:
  - классы логических узлов, присутствовавшие в первой редакции МЭК 61850-7-410:2007, которые не были специфичны для гидроэлектростанций, перемещены в МЭК 61850-7-4 [6];
  - добавлены классы логических узлов общего назначения, отсутствующие в [6], необходимые для моделирования систем управления и мониторинга гидроэлектростанциями;
  - обновлены определения классов логических узлов;
  - примеры моделирования функций и сопроводительная информация перемещены в технический отчет МЭК 61850-7-510.
- Технический отчет МЭК 61850-7-510. Данный отчет описывает то, как использовать классы логических узлов, представленные в МЭК 61850-7-410, а также в других документах серии МЭК 61850 для моделирования функций автоматики, управления и мониторинга на ГЭС/ГАЭС. К примеру, отчёт рассматривает примеры моделирования следующих систем:
  - групповое регулирование активной мощности;
  - групповое регулирование напряжения и реактивной мощности;
  - системы возбуждения;
  - управление гидроагрегатом и др.

Логические узлы, специфичные для гэс/гаэс

Среди специфичных для гидроэлектростанций классов логических узлов стандарт [1] определяет классы узлов согласно табл. 1. Данные классы логических узлов моделируют оборудование ГЭС/ГАЭС и функции, применяемые на данных объектах.

Табл. 1. Классы логических узлов, специфичных для ГЭС/ГАЭС.

	Класс логического узла	**Описание**
	HBRG	Подшипник вала генератора. Предназначен для моделирования параметров подшипника.
	HCOM	Комбинатор. Применяется для регулирования угла положения лопастей для повышения эффективности турбины.
	HDAM	Плотина. Применяется для описания плотины.
	HDFL	Управление дефлектором
	HDLS	Контроль утечки в плотине. Применяется для контроля утечки в плотине.
	HEBR	Электрический тормоз
	HGPI	Индикатор положения затвора
	HGOV	Контроль режима управления генератора
	HGTE	Затвор водосбросных сооружений
0	HITG	Затвор водоприемника
1	HJCL	Групповое управление
2	HLKG	Контроль утечки
3	HLVL	Указатель уровня воды
4	HMBR	Механический тормоз
5	HNDL	Игольчатый затвор
6	HNHD	Водоприемник
	HOTP	Защита от перелива плотины

7		
8	HRES	Водохранилище
9	HSEQ	Контроллер последовательности гидроагрегата
0	HSPD	Мониторинг скорости
1	HSST	Уравнительный резервуар
2	HTGV	Направляющий аппарат (поворотный затвор)
3	HTRB	Лопасти ротора
4	HTRK	Сороудерживающая решетка
5	HTUR	Турбина
6	HVLV	Запорная арматура
7	HWCL	Управление водой
8	ACTM	Выбор режима управления
9	AJCL	Групповое управление генерацией

Для примера рассмотрим класс логического узла HTGV, предназначенный для моделирования направляющих аппаратов гидротурбины согласно табл. 2. Класс описывает данные, которые могут потребоваться для организации взаимодействия с другими устройствами или оператором.

Например, если рассмотреть измеряемые параметры, объект PosPct позволяет фиксировать и передавать другим устройствам позицию направляющего аппарата в процентах от полного открытия или же можно передавать угол открытия, используя объект PosDeg.

Аналогично объекты, соответствующие уставкам, позволяют, обращаясь к устройству по одному из коммуникационных протоколов, считывать текущие данные об уставках и изменять их.

Каждый объект задан определённым общим классом данных, который в свою очередь, предполагает описание структуры данных объекта. Большая часть общих классов данных описывается в [5], другая — в [1].

Табл. 2. Структура логического узла HTGV.

HTGV				
Имя объекта данных	**Общий класс данных**	**Описание**	**T**	**M/O/C**
LNName		Сочетание prefix, LN class и LN instance		
Объекты данных				
NamPlt	LPL	Паспортные данные		M
Информация о состоянии				
Beh	ENS	Индикация поведения		M
Health	ENS	Индикация исправности		M
PosCls	SPS	Затвор закрыт		O
PosOpn	SPS	Затвор полностью открыт		O
PosSNL	SPS	Скорость затвора без нагрузки		O
SMLkdCls	SPS	Серводвигатель зафиксирован в закрытом положении.		Omulti
SMLkdMnt	SPS	Серводвигатель зафиксирован в положении технического обслуживания.		Omulti
PinAlm	SPS	Тревога при потере контакта		Omulti
RodAlm	SPS	Тревога при изгибе стержня		Omulti
DvWrn	SPS	Предупреждение об отклонении затвора		Omulti
DvAlm	SPS	Сигнал тревоги об отклонении затвора		Omulti

HTGV				
Имя объекта данных	**Общий класс данных**	**Описание**	**T**	**M/O/C**
Измеряемые параметры				
PosPct	MV	Позиция в процентах от полного открытия.		Cmulti
PosDeg	MV	Угол открытия		Cmulti
SMPres	MV	Давление серводвигателя для перемещения		Omulti
Управляемые объекты				
Mod	ENC	Режим работы		M
OpCntRs	INC	Сброс счетчика операций		O
PosSpt	APC	Уставка положения		O
DithAct	SPC	Активировать колебания		O
Параметры				
PosSNLSet	ASG	Скорость вращения без нагрузки		O
DvWrnSpt	ASG	Уставка предупреждения об отклонении затвора		Omulti
DvAlmSpt	ASG	Тревога отклонения затвора		Omulti
CbrRng	ASG	Диапазон калибровки		O
ClsLim	RST	Предел закрытия		O
ClsLimHys	ASG	Гистерезис предела закрытия		O
ClsTmsSet	ING	Время закрытия		O
OpnTmsSet	ING	Время открытия		O
DithOfs	ASG	Смещение		O

МОДЕЛИРОВАНИЕ ФУНКЦИЙ

С использованием классов логических узлов, приведенных в [1] и [6], становится возможным моделирование функций управления, автоматики и мониторинга на ГЭС/ГАЭС. В качестве примера рассмотрим функцию группового регулирования активной мощности (рис. 1) согласно [1] и [8] на примере ГРАМ для 4 ГА.

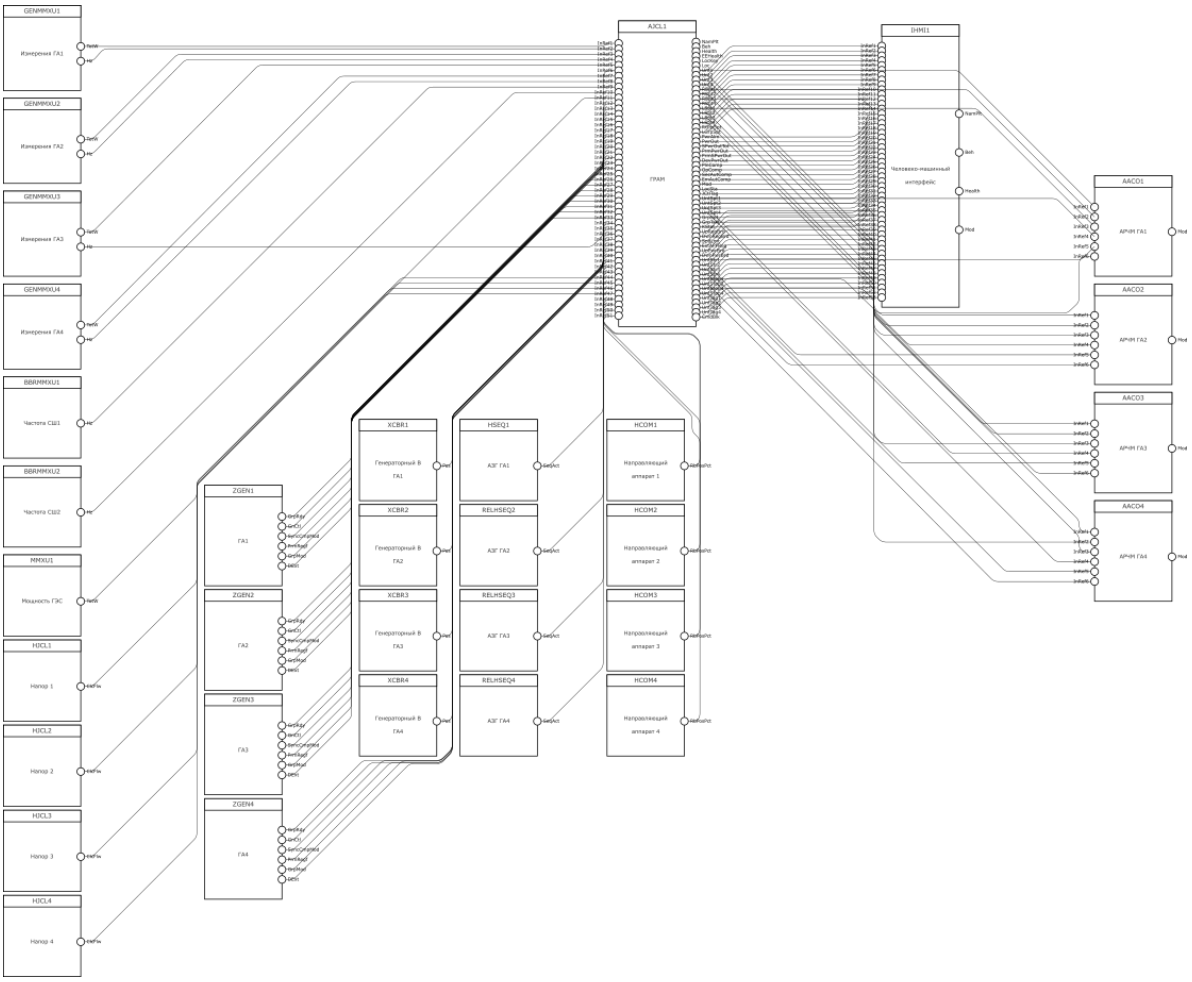


Рис. 5. Пример моделирования группового регулирования активной мощности.

Логический узел IHMI представляет собой человеко-машинный интерфейс (ЧМИ). Через ЧМИ оператор получает доступ к установке параметров и режима ГРАМ логического узла AJCL (табл. 3) – данный узел обеспечивает координацию работы гидроагрегатов на станции и позволяет описывать команды для трех и более гидроагрегатов. Какие агрегаты участвуют в групповом регулировании определяется объектом данных с порядковым номером ГА Unt логического узла AJCL. Оператор может установить режим работы ГРАМ по активной мощности или частоте, уставки режимов, границы регулирования и прочие параметры. В приведенном на рис. 1 примере также используется информация о параметрах работы ГА от САУ ГА для каждого ГА, сигналы АЗГ для каждого ГА, частоты СШ1 и СШ, положения генераторных выключателей, данные о напоре, данные с направляющих аппаратов. Выдача команд ГРАМ осуществляется на АРЧМ в составе САУ ГА. Присутствует ключ работы от УВК ЦС АРЧМ, задача параметров от которой может осуществляться аналогично ЧМИ с использованием протокола MMS при соответствующем положении ключа ExtAPFReg. Возможно заведение сигналов ПА (индивидуально для проекта), поведение которых определяется внутренними алгоритмами, выведены различные составляющие задания (от плановой мощности, от исполняющейся диспетчерской команды, от АВРЧМ, от ПА).

Табл. 3. Структура логического узла AJCL.

AJCL				
Имя объекта данных	**Общий класс данных**	**Описание**	**T**	**M/O/C**
LNName		Сочетание prefix, LN class и LN instance		
Объекты данных				
Описание				
NamPlt	LPL	Паспортные данные		M
Информация о состоянии				
Beh	ENS	Индикация поведения		M
Health	ENS	Индикация исправности		M
EEHealth	ENS	Индикация исправности внешнего оборудования		M
LocKey	SPS	Положение ключа режима управления (ИСТИНА - местное, ЛОЖЬ - дистанционное)		M
Loc	SPS	Поведение местного управления		M
Unt	SPS	Генератор {номер экземпляра} вносит мощность		Omulti
RSpt	SPS	Увеличить уставку в ИЭУ для генерирующей установки {номер экземпляра}	T	Omulti
LSpt	SPS	Уменьшить уставку в ИЭУ для генерирующей установки {номер экземпляра}	T	Omulti
RGrpSpt	SPS	Увеличить уставку в ГРАМ		E

AJCL				
Имя объекта данных	**Общий класс данных**	**Описание**	**T**	**M/O/C**
LGrpSpt	SPS	Уменьшить уставку в ГРАМ		E
PwrAlm	SPS	Предупредительная сигнализация отклонения фактической мощности		E
Измеряемые параметры				
PwrOut	MV	Мощность, вносимая от находящихся под групповым управлением установок		O
SPwrOut	MV	Суммарная генерируемая электростанцией мощность		O
PrmPwrOut	MV	Первичная мощность, вносимая от находящихся под групповым управлением установок		E
PrmSPwrOut	MV	Суммарная генерируемая электростанцией первичная мощность		E
DevPwrOut	MV	Величина отклонения фактической мощности от первичной		E
PlnComp	MV	составляющая задания от плановой мощности		E
OpComp	MV	составляющая задания от исполняющейся диспетчерской команды		E
SecAutComp	MV	составляющая задания от устройств АВРЧМ		E
EmAutComp	MV	составляющая задания от ПА		E

AJCL				
Имя объекта данных	**Общий класс данных**	**Описание**	**T**	**M/O/C**
Элементы управления				
Mod	ENC	Режим работы		M
RegMod	SPC	Режим регулирования (0 – мощности; 1 – частоты)		E
LocSta	SPC	Блокировка дистанционного управления		M
JCtlTag	TAG	Сервисная метка для группового управления, закрепленная на оборудованием		O
UntSpt	APC	Уставка по активной мощности для генератора {номер экземпляра}		Omulti
GrpSpt	APC	Групповое задание мощности ГЭС		E
GrpTskf	APC	Уставка частоты ГЭС		E
KStat	APC	Статизм по частоте		E
UpRegBrd	APC	Верхняя граница регулирования		E
DwnRegBrd	APC	Нижняя граница регулирования		E
SpdLmt	APC	Максимальная скорость изменения задания мощности		E
ExtAPFReg	SPC	Автоматическое регулирование от УВК ЦС АРЧМ		E
UpPwrBrd	APC	Верхняя граница мощности ГЭС		E
DwnPwrBrd	APC	Нижняя граница мощности ГЭС		E

AJCL				
Имя объекта данных	**Общий класс данных**	**Описание**	**T**	**M/O/C**
UntStr	SPC	Пуск генератора {номер экземпляра}		Omulti
UntStop	SPC	Остановка генерации установки {номер экземпляра}		Omulti
UntTag	TAG	Сервисная метка, закрепленная за генерирующей установкой {номер экземпляра}		Omulti
CmdBlk	SPC	Блокировка управления		O

Алгоритм работы вычисляет распределение заданной оператором активной мощности по каждому агрегату группы с учетом получения сигнала от ГА о достижении предела регулирования, режима СК и прочих параметров на основе индивидуальных условий и характеристик работы каждого агрегата: активной мощности ГА и ГЭС (MMXUx.TotW), частоты сети (MMXUx.Hz) и др.

Стандартизация описания типовых функций ГЭС/ГАЭС согласно МЭК 61850 в ПАО «РУСГИДРО»

В ПАО «РусГидро» ведется работа по стандартизации описания типовых функций технологической автоматики и ПТК ГЭС/ГАЭС с использованием стандарта МЭК 61850 в следующем объеме:

- ПТК САУ гидроагрегата;
- ПТК системы возбуждения (контроллер регулятора возбуждения);
- ПТК АРЧМ (контроллер регулятора частоты вращения и активной мощности);
- ПТК виброконтроля (возможна реализация в составе ПТК САУ ГА);
- АУВ генератора (в составе РЗ генератора);
- ПТК ГРАМ;
- ПТК ГРНРМ;
- ПТК РУСА (рационального управления составом агрегатов);
- ПТК АБП (дизель генератора);
- ПТК Мониторинга ГТС;
- ПТК АРЗ (аварийно-ремонтных затворов);
- ПТК Затворов водосливной плотины;
- ПТК ЭТО (электротехнического оборудования – управление РПН, коммутационными аппаратами, распределительными устройствами);
- ПТК ЩПТ (щит постоянного тока);

- ПТК Системы пожарной сигнализации.

Результаты данной работы обеспечат возможность типизации технических решений с использованием стандарта IEC 61850, а, в совокупности с другими инструментами стандарта МЭК 61850, достичь сокращения сроков проектирования и пусконаладочных работ ГЭС/ГАЭС, повысить эффективность их эксплуатации, что подтверждается опытом электросетевых компаний.

Выводы

Стандарт МЭК 61850 предоставляет все необходимые инструменты и базу для стандартизации описания функций технологической автоматики ГЭС/ГАЭС. Успех применения стандарта для систем управления ГЭС/ГАЭС будет зависеть от настойчивости и последовательности эксплуатирующих организаций и разработчиков решений в вопросах типизации функций управления и их представления в информационной модели МЭК 61850.

СПИСОК ЛИТЕРАТУРЫ

[1] IEC 61850-7-410:2012+AMD1:2015 CSV. Communication networks and systems for power utility automation - Part 7-410: Basic communication structure - Hydroelectric power plants - Communication for monitoring and control, Edition 2.1.
[2] IEC 61850-7-420:2009. Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes, Edition 1.0.
[3] IEC TR 61850-90-1:2010. Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations, Edition 1.0.
[4] IEC TR 61850-90-2:2016. Communication networks and systems for power utility automation - Part 90-2: Using IEC 61850 for communication between substations and control centres, Edition 1.0.
[5] IEC TR 61850-7-510:2012. Communication networks and systems for power utility automation - Part 7-510: Basic communication structure - Hydroelectric power plants - Modelling concepts and guidelines, Edition 1.0.
[6] IEC 61850-7-4:2010+AMD1:2020 CSV. Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes, Edition 2.1.
[7] СТО 70238424.27.140.033-2010. Гидроэлектростанции. Технические и автоматизированные системы. Условия поставки. Нормы и требования.
[8] СТО 59012820.27.140.001-2014. Нормы участия гидроагрегатов гидравлических и гидроаккумулирующих электростанций в нормированном первичном регулировании частоты.

2.8. РАЗРАБОТКА ФОРМАЛИЗОВАННЫХ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К ЛОГИЧЕСКИМ УЗЛАМ

А. А. ВОЛОШИН, А. А. ЛЕБЕДЕВ, Д. О. БЛАГОРАЗУМОВ,

В. А. ВАЛЬГЕР, Б. А. САФРОНОВ, М. А. ХЛЫСТОВ, А. С. ХУДЯКОВ, Р. В. НЕУСТУПКИН, В. О. БОЛОШИН

ФГБОУ ВО «НИУ «МЭИ», АО «РАСУ»

Российская Федерация

Контактное лицо:

А. А. ВОЛОШИН

voloshin.aa@yandex.ru

Ключевые слова:

РЗА ЦПС, функциональные требования, информационная модель, типизация логических узлов, корпоративный профиль, МЭК 61850.

ВВЕДЕНИЕ

Для исследования проблемы определения функциональных требований к логическим узлам в рамках комитета B5 CIGRE была создана рабочая группа B5.64 «Методы определения функциональных требований к релейной защите и автоматике энергосистем». В соответствии с отчетом рабочей группы [1], опубликованным в 2018 году, МЭК 61850 является наиболее популярным языком описания оборудования и процессов на подстанции. Отчет преимущественно рассматривает распространенность применяемых методов и форматов (языков) описания конфигурации среди участников рынка, но не затрагивает детального описания процесса и рабочего порядка формирования функциональных требований.

Целью данного исследования является анализ проблем разработки функциональных требований на основе практического примера разработки функций РЗА подстанции, соответствующих требованиям серии стандартов МЭК 61850. Отличительной чертой исследования является учет перспективного развития систем централизованной РЗА, РЗА с миграцией функций, а также автоматизированных систем тестирования ЦПС при разработке функциональных требований к логическим узлам.

ОСНОВНАЯ ЧАСТЬ

Особенности МЭК 61850, затрудняющие разработку функциональных требований

Определение функциональных требований к логическим узлам невозможно без понимания структуры логического устройства, содержащего данные ЛУ. Однако, какой-либо нормативной базы, содержащей стандартизированные описания логических устройств согласно информационной модели МЭК 61850, на текущий момент не существует. В связи с чем для разработчика или исследователя проблематика разработки функциональных требований к логическим узлам неизбежно включает в себя проблему разработки функциональных требований и к логическому устройству.

Поскольку состав логических устройств нормативно не определяется, возможны различные подходы к компоновке логических узлов в логические устройства. В рамках данного исследования использовался принцип соответствия функции РЗА определенному обособленному логическому устройству. При попытке подбора состава логических узлов для логического устройства определенной функции РЗА возник ряд проблем, среди которые можно выделить 3 основные категории, описанные далее.

1. МЭК 61850 не определяет источники сигналов, на основе которых происходит формирование значений объектов данных логического узла. Указанный факт приводит к неоднозначности подходов реализации функции РЗА на основе логических узлов, а следовательно и неоднозначности состава логических узлов в логическом устройстве. Таким образом, невозможно однозначно сформулировать функциональные требования к логическому узлу, не определяя строгим образом набор входных сигналов, необходимых для работы узла.

На примере свободно конфигурируемой логики терминалов РЗА фирмы ABB, можно наблюдать, что производители, стремящиеся использовать МЭК 61850 для полного описания структурно-функциональных схем алгоритма вынуждены аналогичным образом определять входные сигналы функциональных блоков, соотносящихся с логическими узлами информационной модели. Проблема данной практики заключается в том, что входные

сигналы логических узлов и связи между ними определяются лишь в проприетарном ПО производителя и не находят отражения в составе SCL файлов.

2. МЭК 61850 не рассматривает функционал обработки и формирования измерений в составе информационной модели, а также не определяет логические узлы обработки и преобразования измерений для нужд релейной защиты. Данный подход обеспечивает полную свободу производителям в вопросе обработки и преобразования измерений, что позволяет продолжить применение разработанного ранее алгоритмического обеспечения. Недостатком данной практики является отсутствие понимания порядка распределения измерений по логическим узлам – каждый логический узел с точки зрения информационной модели уже содержит необходимый набор измерений, что приводит к неоднозначности структуры реализации функций защит, а, следовательно, и функциональных требований. Таким образом, можно сделать вывод, что однозначное понимание алгоритмического источника преобразованных измерений в рамках информационной модели МЭК 61850 отсутствует.

3. МЭК 61850 преимущественно описывает логические узлы, выполняющие базовые функции к которым можно отнести, например, различного рода реле. В то же время, значительное количество отечественных подходов к построению РЗА не предусмотрено: блокировка качаний по разрешающему принципу работы, блокировка неисправности цепей напряжения, АВР и ВНР, логическая защита шин, ДФЗ и прочие высокочастотные защиты, функции противоаварийной автоматики, а также многие другие. Существующий корпоративный профиль ФСК ЕЭС [2] стремится обеспечить адаптацию МЭК 61850 к отечественным реалиям, однако ограничивается лишь внедрением новых классов логических узлов и объектов данных, в связи с чем проблемы отсутствия указанных источников входных данных и неопределенной структуры логических устройств остаются актуальными и для корпоративного профиля [2].

Изменение подхода к применению логических узлов

На текущий момент МЭК 61850 подразумевает, что информационная модель – это лишь семантически определенный интерфейс для вывода данных наружу, в то время как фактическими источниками данных является алгоритмическое обеспечение за рамками информационной модели. Данная практика представляет интерес как для производителей, поскольку не требует существенного изменения разработанного ранее алгоритмического обеспечения функций РЗА, так и обеспечения наладки АСУ ТП, поскольку значимость имеет лишь набор данных и их формат. Указанный факт приводит к проблеме, что информационные модели, а, следовательно, и принципы функционирования логических узлов одного и того же класса могут значительно отличаться у различных производителей. Постановка вопроса определения функциональных требований к логическим узлам несколько абсурдна, поскольку функциональные требования необходимо в первую очередь определять для алгоритмического обеспечения, а не для интерфейса, извлекающего из него данные. Сложившаяся практика применения стандарта характеризуется отличием структуры информационной модели от структуры алгоритмического обеспечения, отсутствием однозначно определяемых источников данных для ЛУ, отсутствием стандартизированной структуры информационной модели функций РЗА, что в совокупности существенно

препятствует развитию технологий централизованной РЗА, РЗА с мигрирующими функциями, а также автоматизированных комплексов проектирования и наладки РЗА ЦПС.

В связи с перспективами развития вышеперечисленных технологий, было принято решение изменить подход применения логических узлов таким образом, чтобы логический узел подразумевал обособленное и независимое алгоритмическое обеспечение функции. При данном подходе определение функциональных требований к логическим узлам идентично определению функциональных требований к обособленному алгоритмическому обеспечению логического узла, в связи с чем возникает необходимость определения необходимого набора входных сигналов и данных.

В ходе исследования были составлены логические устройства, отражающие функции РЗА объектов среднего и высокого класса напряжений, для входящих в их состав логических узлов произведено расширение информационной модели: объекты данных были категоризированы на группы входных сигналов, выходных сигналов и параметров настройки; в случае необходимости добавлены новые объекты данных (преимущественно входных сигналов); разработано алгоритмическое обеспечение логических узлов в соответствии с установленными категориями. В результате проведения работ обнаружилась необходимость расширения информационной модели МЭК 61850 новыми классами логических узлов, преимущественно в случаях реализации отечественных подходов к построению РЗА, не предусмотренных в рамках МЭК 61850, а также описания логических узлов обработки измерений. Результаты разработки алгоритмического обеспечения приведены далее.

Унификация функций различных защит в составе логических узлов

В рамках проектирования логических устройств было обнаружено, что некоторые логические узлы, например ЛУ реле, применяются в большом количестве логических устройств защит различного типа, при этом в процессе проектирования часто встречается необходимость обеспечить в рамках логического узла специфический для данной защиты функционал. В качестве примера подобного случая можно привести узлы PDIS, для которых в зависимости от защищаемого объекта необходимо устанавливать характеристику срабатывания определенного типа (полигональную, эллиптическую и т.п.). Применение МЭК 61850 и корпоративного профиля ФСК ЕЭС [2] предполагает, что описанные в рамках стандартов логические узлы представляют собой базовый класс данных, в то время как какое-либо специфическое применение логического узла должно быть выполнено отдельным классом, наследующим данные из общего класса и содержащим требуемые нововведения. Указанный подход выгоден с точки зрения разработки информационной модели в соответствии с принципами ООП, но для внешнего наблюдателя в лице наладчика или автоматической системы контроля указанный подход оборачивается огромным количеством схожих по типу, но уникальных относительно друг друга логических узлов, особенности работы которых необходимо обрабатывать и учитывать в каждом случае отдельно.

В связи с перечисленными выше особенностями, было принято решение о реализации общего исполнения ряда логических узлов, специфическое применение которых требуется в различных защитах. Реализация общего функционала в рамках объединенного логического узла подразумевает возможность варьирования функциональности логического узла за счет варьирования параметров настройки узла и использования лишь необходимых объектов данных из обобщенного перечня. Например, для экземпляров узлов PTOC, отражающих

токовые пусковые органы ВЧ-защит, можно ввести контроль направленности, в то время как для узлов РТОС, отражающих МТЗ присоединений среднего уровня напряжения, направленность контролироваться не будет. Примерами подобных унифицированных узлов являются следующие логические узлы: PTRC, RDIR, PTUV, PTOV, PTOC, OPAP и AUAP (новые классы ЛУ, отражающие универсальные ступени оперативного и автоматического ускорения любых ступенчатых защит), PDIS, PDIF, PSCH (узел ВЧ ПП, предусматривающий работу как с ДФЗ, так и с ВЧБ/НВЧЗ). В то же время, для некоторых ЛУ функциональное обеспечение оказалось настолько различным, что возникла необходимость формирования производных новых классов ЛУ, а при отсутствии близкого к узлам МЭК 61850-7-4 [3] функционала – необходимость определения совершенно новых классов логических узлов. Новые классы логических узлов были определены для функций АВР, ВНР, БК, ЗДЗ, ЗНФ, ЗНР, ЗОФ, ЛЗШ, ГЗ, ВЧ защит и др.

Общая структура логических узлов

В процессе разработки алгоритмического обеспечения логических узлов для каждого узла был составлен список объектов данных входных сигналов, объектов данных выходных сигналов, параметров настройки.

В ходе разработки алгоритмического обеспечения была обнаружена структурная схожесть узлов одинакового назначения. Данные закономерности систематизированы посредством описания повторяющихся структур в составе алгоритмического обеспечения логических узлов определенного типа назначения.

Логические узлы в зависимости от своего назначения (измерительные, пуско-функциональные и функциональные) имеют единую, типизированную структуру реализации. Логические узлы любого назначения в обязательном порядке должны содержать блоки задания/редактирования уставок, валидации типа данных подключенного сигнала, присвоения меток времени выходным сигналам.

Измерительные логические узлы в зависимости от назначения могут содержать блоки предварительной обработки входных сигналов, фильтрации входных сигналов, обеспечения дополнительных расчетов параметров на основе отфильтрованных сигналов.

Пуско-функциональные логические узлы в зависимости от назначения могут содержать блоки подготовки данных для пусковых органов, непосредственно пусковых органов, блоки логической части, обеспечивающие учет прочих факторов для формирования результирующего сигнала срабатывания пускового органа.

Функциональные логические узлы содержат исключительно блоки логической части, обеспечивающие работу селекторов и логических операций с входными сигналами.

Разработка логических устройств (функций) РЗА на основе логических узлов нового типа

В результате изменения подхода каждый логический узел становится носителем цельного алгоритма, выполняющего определенную функцию, а также обладает однозначно определяемыми входными и выходными сигналами. Таким образом, на основе логических узлов нового типа существует возможность формирования цельного алгоритма релейной защиты. Структура алгоритмического обеспечения полученной защиты будет идентична информационной модели МЭК 61850, что имеет ряд преимуществ:

- модульная структура схемы защиты – структурно-функциональная схема защиты состоит из независимых друг от друга модулей, что обеспечивает широкий выбор требуемой

функциональности на этапе проектирования – например выбора количества и типа ступеней в используемой защите, выбора используемых функций (ускорение, контроль направленности, и т.п.);

- строгое определение взаимосвязей и информационного обмена между логическими узлами как в составе одного логического устройства, так и в составе различных логических устройств, что упрощает понимание и восприятие принципов функционирования защиты, а также позволяет предсказуемо оценивать влияние изменения режимов работы логического узла на работу функции релейной защиты и определять источники сигналов измерений для узлов, что является критически важным для функционирования централизованной РЗА, РЗА с миграцией функций, а также автоматизированных систем проектирования и наладки подстанции;
- модульная структура схемы защиты с полностью предсказуемым поведением логических узлов позволяет не только автоматическим образом контролировать исправную работу защиты, но и автоматически проектировать необходимую конфигурацию защит.

Недостатком подхода определения логического узла как обособленной части алгоритмического обеспечения является необходимость для производителей изменять разработанное ранее алгоритмическое обеспечение терминалов, не имеющего общих черт со структурой информационной модели МЭК 61850. Также следует отметить, что разработка алгоритмов, соответствующих структуре информационной модели МЭК 61850, образует проблему реализации в рамках алгоритма обработки меток качества сигналов, в то же время принципы присвоения меток качества выходных сигналов на основании меток качества входных сигналов не регламентированы и реализуются на усмотрение производителя. Таким образом, существует необходимость использования единообразных принципов при формировании меток качества выходных сигналов для исключения необходимости обособленного учета поведения различных логических узлов.

Рассмотреть структурную схему разрабатываемых логических устройств можно на примере разработки логического устройства МТЗ, предназначенного для воздушных линий среднего уровня напряжения. Функция МТЗ состоит из двух логических устройств – непосредственно логического устройства МТЗ и устройства измерений, содержащего ЛУ, осуществляющие обработку и преобразование измерений для нужд релейной защиты. Выделение логического устройства измерений необходимо, поскольку сформированные измерения могут быть использованы другими функциями РЗА, кроме МТЗ, что позволяет избежать потерь вычислительной мощности и дублирования вычислений. Схема логических устройств функции МТЗ приведена на рис. 1, назначение логических узлов на схеме описано в табл. 1.

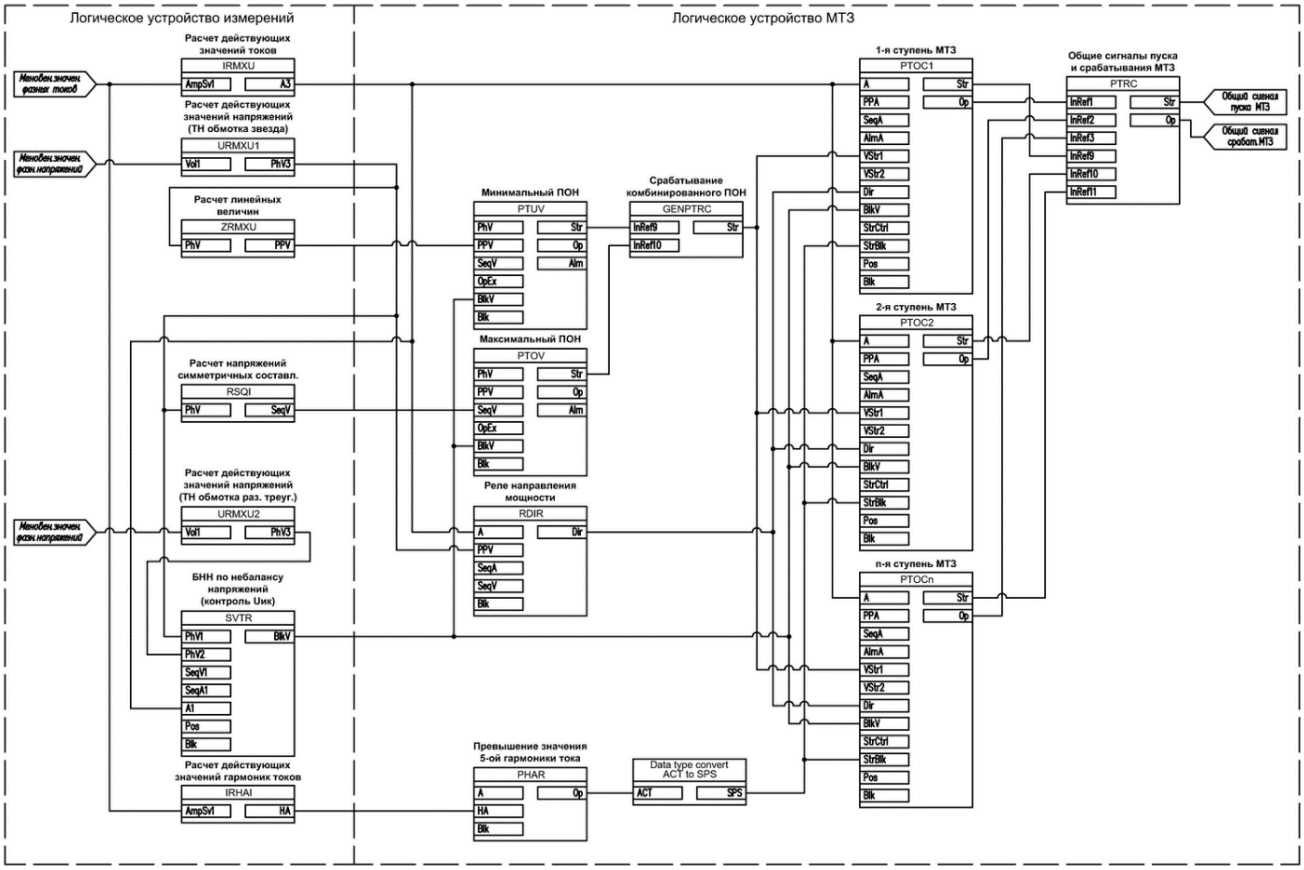


Рис. 1. Структурно-функциональная схема логических устройств МТЗ.

Табл. 1. Описание назначения ЛУ.

Наименование ЛУ	Назначение ЛУ	Тип узла	В наличии в МЭК 61850/ КП ФСК ЕЭС
IRMXU	Формирование действующих значений токов на основе мгновенных значений	измерительный	-/-
URMXU	Формирование действующих значений напряжений на основе мгновенных значений	измерительный	-/-
ZRMXU	Формирование линейных токов, напряжений на основе действующих фазных значений	измерительный	-/-
RSQI	Вычисление векторов токов и напряжений симметричных составляющих	измерительный	-/-
IRHAI	Расчет действующих значений гармоник токов	измерительный	-/-
SVTR	Блокировка неисправности цепей	пуско-	-/+

	напряжения	функциональный	
PTOV	Максимальное реле напряжения, контролирует напряжение обратной последовательности	пуско-функциональный	+/+
PTUV	Минимальное реле напряжения, контролирует линейные напряжения	пуско-функциональный	+/+
RDIR	Реле направления мощности	пуско-функциональный	+/+
PHAR	Реле превышения определенной гармоники тока, контролирует 2-ю гармонику тока	пуско-функциональный	+/+
PTOC	Ступень максимальной токовой защиты, контролирует фазные токи	пуско-функциональный	+/+
GENPTRC	Объединение сигналов пуска и срабатывания ступеней защит по схеме И/ИЛИ	функциональный	-/-
PTRC	Объединение сигналов пуска и срабатывания ступеней защит	функциональный	+/+

Представленные логические узлы обладают универсальной функциональностью для любых их применений в составе функций РЗА, которая ограничивается для применения МТЗ посредством корректной конфигурации входов ЛУ и параметров настройки. Так, для узла ступени МТЗ PTOC в качестве контролируемого тока возможен выбор фазных (*A*) или линейных (*PPA*) токов, токов симметричных составляющих (*SeqA*) или аварийных токов (приращений) (*AlmA*). В рамках данного логического устройства контролируются лишь фазные токи. В составе узла предусмотрен контроль ПОН различных СШ, контроль требуемой направленности, информацию о которой формирует узел РНМ RDIR, контроль БНН с возможностью вывода контроля ПОН или направленности при срабатывании БНН, контроль сигнала ступени автоматического ускорения, контроль положения разъединителя (применятся для аварийной МТЗ). В рамках применения МТЗ для узла введен лишь контроль единичного комбинированного ПОН и требуемой направленности («вперед»), а также контроль БНН.

В рамках исследования было разработано ПО конфигуратора, который позволяет формировать логические устройства посредством добавления в проект и определения соединений различных разработанных логических узлов (представленных в рамках ПО как библиотеки функциональных элементов), конфигурировать добавленные узлы для обеспечения требуемых режимов работы, выгружать бинарные файлы полученных функций, адаптированные под требуемую целевую платформу. Следует отметить, что в рамках стандартного синтаксиса SCL файлов не предусмотрены элементы, отражающие входные сигналы логических узлов или связи между логическими узлами в рамках одного физического устройства. Механизм применения объектов данных ссылок вида *InRef* и *BlkRef* неприменим, поскольку последние лишены семантического смысла. В связи с данной проблемой для отражения и сохранения связей логических узлов в проекте был разработан формат файлов CLD, содержащий строгое описание информационного обмена между логическими узлами.

Подготовка функций РЗА к аттестации

Структура работ по тестированию разработанных функций РЗА представлена на рис. 2.

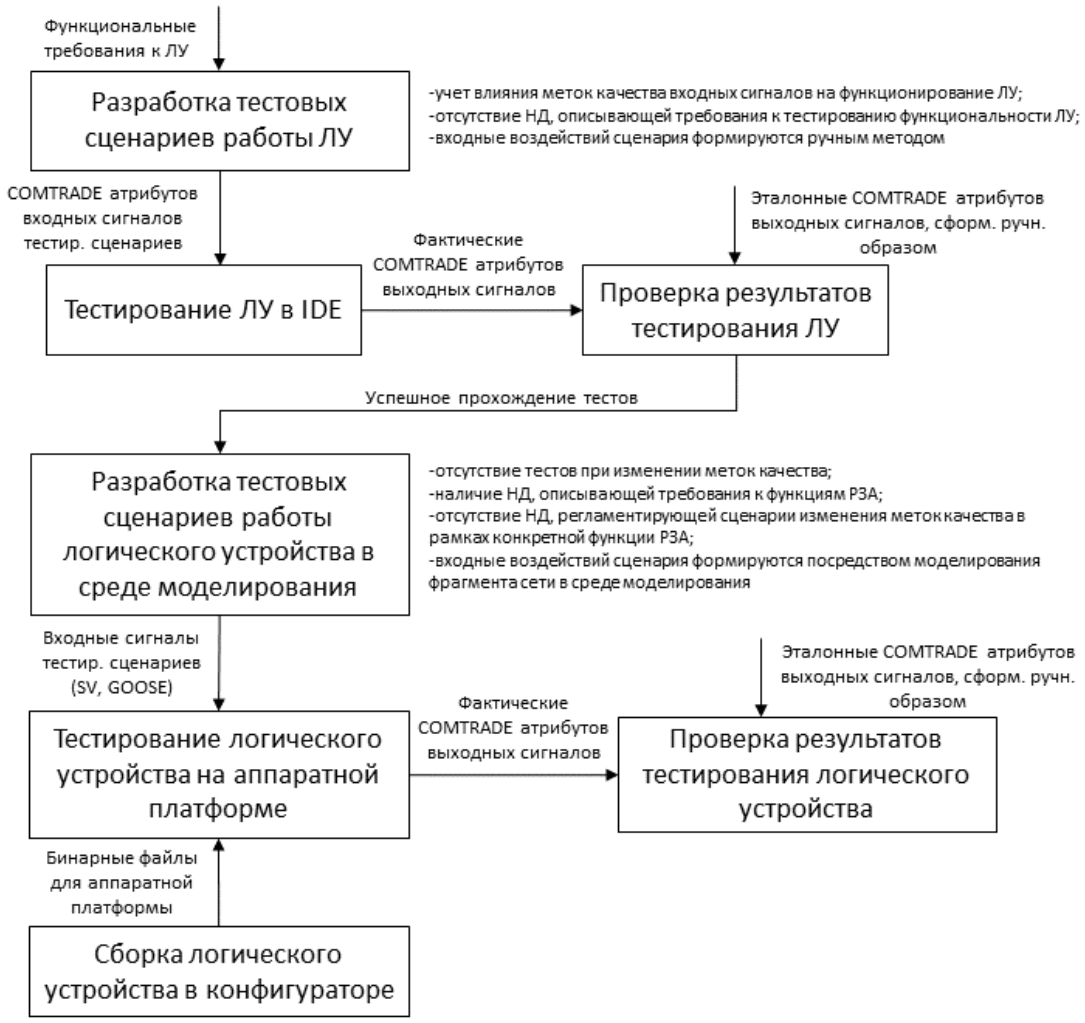


Рис. 2. Структура работ по тестированию разработанных функций.

Следует отметить отсутствие какой-либо тематической документации, которая могла бы быть опорой при подборе необходимых опытов для тестирования ЛУ, поскольку отраслевые СТО в области ПМИ описывают лишь тестирование функции РЗ в целом, а не ее функциональных частей, в то время как МЭК 61850-10 [4] не предусматривает раскрытия функциональных особенностей устройства, а определяет лишь тестирование наличия внешних интерфейсов в виде тех или иных объектов данных. Более того, отсутствуют какие-либо методики разработки тестов, учитывающих корректность присвоения меток качества выходным сигналам.

Ручное формирование графиков входных воздействий ЛУ исключило необходимость моделирования схем энергосистемы на данном этапе, что позволило разрабатывать ЛУ независимо друг от друга.

Отсутствие необходимости учета опытов при неисправных метках качества входных сигналов для логических устройств обусловлено тем фактом, что данные опыты были рассмотрены на этапе тестирования ЛУ, тем самым поведение ЛУ предсказуемо определяет функционирование логического устройства.

В качестве среды моделирования применялся комплекс RTDS, в рамках которого была спроектирована модель электрической сети, содержащей защищаемый объект и воссоздавались тестируемые режимы работы сети. Полученные в ходе моделирования режимов измерения и дискретные сигналы (напр. положения выключателя) были опубликованы в виде SV-потоков и GOOSE сообщений и переданы на аппаратную платформу по ЛВС. В рамках аппаратной платформы производилась запись COMTRADE-файлов выходных сигналов.

Заключение

Результаты исследования позволяют утвердить следующие тезисы.

- Распространенность применения серии стандартов МЭК 61850 и их преимущественное применение для описания оборудования подстанции подразумевают необходимость применения стандартов для новых систем РЗА и новых задач, однако требования стандарта не адаптированы к реализации инновационных систем и решений в области РЗА.
- Функциональные требования к логическим узлам невозможно определить без определения архитектуры логических устройств. Отсутствием нормирования структуры логических устройств приводит как к проблемам с взаимосовместимостью решений, так и различной практике применения логических узлов. Корпоративные профили также не решают данной проблемы, поскольку не содержат нормированной структуры логического устройства защиты.
- Реализация централизованной РЗА, РЗА с миграцией функций и систем автоматизированного проектирования и наладки терминалов РЗА ЦПС существенно затруднены рамками стандарта МЭК 61850 отделяющего информационную модель и алгоритмическое обеспечение. Для решения данной проблемы необходимо установить соответствие логического узла определенному изолированному независимому алгоритмическому обеспечению.
- Описание взаимодействия ЛУ (для определения структуры логического устройства), а также определение функциональных требований ЛУ и его алгоритмического обеспечения требует однозначного указания входных и выходных данных ЛУ/алгоритма. МЭК 61850 на данный момент не удовлетворяет данному требованию, поскольку применение объектов данных ссылок *lnRef* и *BlkRef* предоставляет возможность определения связи, однако последняя не обладает семантическим смыслом, что существенно усложняет процесс проектирования/наладки. Необходимо ввести расширение стандарта как в части описания объектов данных логических узлов, так и в части SCL синтаксиса для обеспечения возможности указания однозначных семантически понятных связей между логическими узлами в составе одного физического устройства.
- Определение логического узла как структуры, содержащей специализированное алгоритмическое обеспечение, требует создания набора логических узлов, обеспечивающих преобразование и формирование измерений для нужд релейной защиты.

- Необходима стандартизация ПМИ логических узлов, а также принципов формирования меток качества объектов данных в рамках функционального обеспечения РЗА, отсутствующая на данный момент.
- В рамках исследования была проведена работа, наглядно иллюстрирующая возможность полного цикла реализации функций РЗА, структура алгоритмического обеспечения которых соответствует структуре информационной модели МЭК 61850.

ЛИТЕРАТУРА

[1] Siqueira, I.P., Faarooqui, N.U., Nair, N.-K.C.: A Review of International Industry Practices for Specification of Functional Requirements of Protection, Automation and Control. CIGRE Science & Engineering, N. 11, Paris, France, June 2018.

[2] СТО 56947007 -25.040.30.309-2020». Корпоративный профиль МЭК 61850 ПАО «ФСК ЕЭС».

[3] IEC 61850-7-4:2010, Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes.

[4] IEC 61850-10:2012, Communication networks and systems for power utility automation - Part 10: Conformance testing.

2.9. ПРИМЕНЕНИЕ РАСШИРЕННОГО ПРОФИЛЯ ПЕРЕДАЧИ МГНОВЕННЫХ ЗНАЧЕНИЙ АНАЛОГОВЫХ СИГНАЛОВ ДЛЯ ДИФФЕРЕНЦИАЛЬНОЙ ЗАЩИТЫ ЛИНИИ

А. Н. ПОДШИВАЛИН, И. А. КАПУСТИНА

ООО «Релематика»

Российская Федерация

Контактное лицо:

А. Н. ПОДШИВАЛИН

podshivalin_an@relematika.ru

Ключевые слова:

Продольная дифференциальная защита линий, протокол передачи данных, вычислительные сети.

ВВЕДЕНИЕ

Электрические сети развиваются по пути оптимизации и унификации технических решений. Совершенствуется информационная и телекоммуникационная инфраструктура, развивается автоматизация процессов передачи и распределения электрической энергии [1]. Вводятся и уточняются отраслевые стандарты в области цифровых подстанций. Продольная дифференциальная защита линии (ДЗЛ), применяемая в сетях всех классов напряжения, долгое время остается в стороне от этой трансформации. С одной стороны, терминалы с функцией ДЗЛ уже реализуют обмен цифровой информацией по цифровым каналам связи. С другой стороны, принцип ДЗЛ выставляет к каналам связи намного более высокие требования, чем обмен устройств релейной защиты и автоматики на подстанции между собой (горизонтальные связи) и с автоматизированными системами управления и сбора информации.

Для ДЗЛ требуется долговременная стабильная связь между подстанциями с заранее определенными характеристиками. Канал связи играет важную роль при синхронизации времени полукомплектов ДЗЛ, а потому каждый производитель использует проприетарный протокол передачи данных. На практике каналы организуют по выделенным оптическим волокнам или с использованием синхронной сети мультиплексоров. Обмен между полукомплектами ДЗЛ и оборудованием связи выполняют в соответствии с международным стандартом IEEE C37.94 [2].

Стандарт IEEE C37.94 описывает протокол передачи и физический уровень интерфейса связи. Преобразователь IEEE C37.94 в протоколы для оборудования связи представляет собой либо составной модуль мультиплексора, либо отдельное устройство, которое фактически обеспечивает совместимость технологий РЗА и систем связи (рис. 1). Существующие преобразователи вносят приемлемую задержку в канал связи между полукомплектами, не искажая их синхронизацию времени. Принято дублировать каналы связи и обеспечивать бесшовное переключение ДЗЛ на резервные маршруты передачи информации. Все эти меры гарантируют малую вариацию задержки в канале связи во время работы защиты и позволяют реализовать дифференциальный принцип.



Рис. 1. Архитектура связи с использованием интерфейса IEEE C37.94.

В настоящее время в системах связи наблюдается тенденция замены синхронных интерфейсов на протоколы пакетной передачи данных, в том числе в промышленных вычислительных сетях электроэнергетики. Однако такие принципы связи повышают неопределенность величины задержки в канале, а потому появились гибридные решения.

Синхронные каналы могут успешно имитироваться такими технологиями, как MPLS (multi-protocol label switching, многопротокольная коммутация по меткам). Однако их применение накладывает ограничения на общую пропускную способность сети связи [3]. В то же время существуют другие технологии, позволяющие передавать информацию, необходимую для ДЗЛ, в сетях Ethernet. Например, в стандарте МЭК 61850 предусмотрена передача пакетов Sampled Values (SV, МЭК 61850-9-2), содержащих данные о мгновенных значениях аналоговых сигналов, дискретизация которых синхронизирована с астрономическим временем [4]. Принцип использования SV в локальных сетях был продемонстрирован во многих пилотных и коммерческих проектах цифровых подстанций [5]. Теоретически этих входных данных достаточно для дифференциального алгоритма в составе защиты, однако на практике надежность меток времени, установленных серверами времени на разных подстанциях, вызывает вопросы [6]. Необходимо техническое решение, которое будет обеспечивать автономность системы защиты. Одновременно желательно предоставить возможность совместного использования устройств различных производителей на разных сторонах линии электропередачи. Для удовлетворения этим требованиям в докладе предложен общий открытый формат передачи критичных по времени данных для устройств защиты по сети Ethernet, обеспечивающий независимую синхронизацию времени полукомплектов ДЗЛ.

ПЕРЕДАЧА ДАННЫХ ДЗЛ В СЕТИ ETHERNET

Современные устройства ДЗЛ обмениваются следующими видами информации:

- величины токов и напряжений,
- пользовательские дискретные сигналы,
- проприетарные сигналы состояния,
- информация для синхронизации времени.

Величины токов и напряжений должны быть предпочтительно представлены в виде выборок токов и напряжений с частотой дискретизации 1000 Гц и более [7]. Каждая выборка должна быть точно соотнесена с абсолютным (астрономическим) или относительным (для терминала) временем. Информация о синхронизации должна быть достаточной для соотнесения текущего времени терминала и времени выборки. Пользовательские сигналы – дополнительный сервис, предоставляемый устройствами ДЗЛ, дублирующий и расширяющий функционал систем сбора и передачи информации.

Рассмотрим протоколы и схемы передачи данных, обеспечивающие необходимые виды и качество информации в полукомплектах ДЗЛ. Предполагается, что пользовательские дискретные сигналы в сетях пакетной передачи данных могут передаваться по известным протоколам GOOSE (МЭК 61850-8-1) или R-GOOSE (МЭК 61850-90-5). Для этих данных важна надежность, тогда как допустимая задержка в передаче информации может достигать 10-20 мс [7]. Для передачи аналоговых сигналов предусматривается модифицированный, расширенный по функциональности механизм SV, названный E-SV. Используются следующие свойства механизмов SV:

- измерение, синхронизированное с тактами локального сервера точного времени;
- способ кодирования аналоговой информации в пакете.

Синхронизацию времени для E-SV нужно выполнять по особому алгоритму. E-SV – механизм двунаправленной связи типа «точка – точка» двух абонентов в сети Ethernet. Для работы с локальной синхронизацией времени на подстанциях пакеты E-SV дополнительно содержат информацию об относительном времени, которая позволяет определять смещение моментов замера отсчетов аналоговых сигналов относительно времени второго абонента, а также сигналы диагностики информационного обмена. Абоненты используют элементы механизма и допущения «эхо»-метода для определения меток времени: маршрут и время доставки пакетов в обоих направлениях одинаковые. Коммутаторы должны использовать технологии автоматического построения симметричных двунаправленных маршрутов для сетей Ethernet. Известны решения и с параллельным резервированием маршрутов [8]. Результирующая задержка в канале рассчитывается каждым полукомплектом независимо с применением статистических методов, например, аналогично протоколу сетевого времени NTP [9]. При изменении задержки процесс синхронизации полукомплектов начинается заново.

Видятся два применения E-SV в зависимости от качества системы синхронизации времени на подстанциях: с относительным и абсолютным временем. Информация для синхронизации времени в составе пакета представлена в табл. 1.

Табл. 1. Информация для синхронизации времени в составе пакета данных E-SV.

Номер поля	Назначение поля
1	Номер пакета
2	Номер последнего полученного пакета
3	Метка времени замера отсчетов
4	Метка времени отправки пакета
5	Метка времени последнего приема пакета от удаленного устройства

Возможные схемы с различным распределением функций между устройствами показаны на рис. 2 и 3. В схеме «2-2» по рис. 2 устройство защиты опрашивает оба устройства измерения и, тем самым, получает возможность синхронизировать между собой аналоговые сигналы обоих концов линии. Предполагается, что для связи E-SV используются выделенные порты устройств. Такое разделение сетей SV (не используются для алгоритма ДЗЛ) и E-SV необходимо для разделения требований к сетевому оборудованию внутри и между подстанциями и обеспечения естественного приоритета трафика. В этой схеме устройства ДЗЛ находятся в одной информационной сети, но обмен данными между собой не производят. Это дает дополнительное преимущество схеме в части резервирования действия защиты. Возможно и упрощение схемы до одного полукомплекта ДЗЛ с реализацией команд отключения удаленного конца.

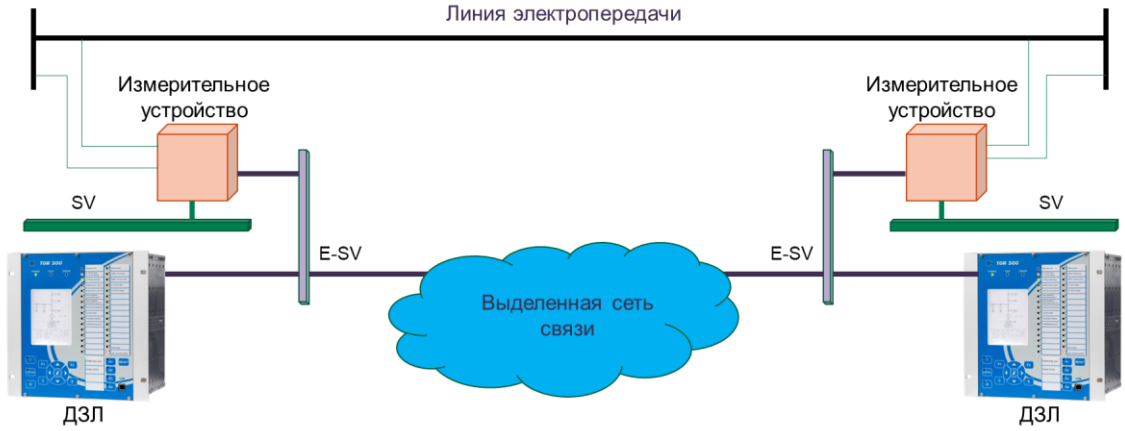


Рис. 2: Архитектура связи «2-2» с использованием E-SV.

В схеме «1-1» по рис. 3 устройства измерения и устройства защиты синхронизированы от локальных серверов времени на подстанции. Устройства защиты получают локальные аналоговые измерения по технологии SV, а удаленные – по технологии E-SV. Синхронизация данных разных подстанций производится внутри устройства ДЗЛ. Преимуществом схемы является замыкание требований E-SV в рамках устройств защиты.

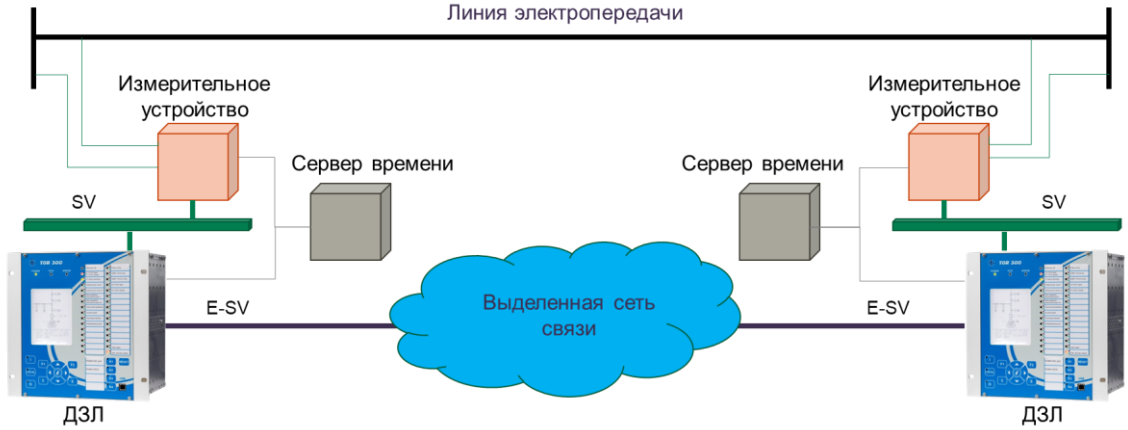


Рис. 3. Архитектура связи «1-1» с использованием E-SV.

Предложенные схемы обладают высокой степенью автономности, поскольку потеря сигналов синхронизации серверами точного времени и устройствами измерения с глобальным временем не приводит к мгновенному отказу или излишнему действию ДЗЛ. Система продолжает функционировать на основе стабильного относительного времени каждого ее элемента. Система оказывается также нечувствительной к малым отклонениям и к скольжениям в службах времени отдельных компонентов, так как протокол E-SV позволяет рассчитывать на краткосрочную (на каждом интервале в пределах нескольких секунд) стабильность их внутренних таймеров.

В одном пакете E-SV могут передаваться одна или несколько выборок, содержащих отсчеты (срез) токов и напряжений в момент дискретизации. Выбор оптимального числа является предметом будущего исследования. Проведем оценку требований к пропускной способности каналов связи при передаче пяти выборок в одном пакете. Для выполнения ДЗЛ измерение на каждой подстанции должно производиться с частотой дискретизации от 1 до 4 кГц (здесь и далее рассматривается сеть с промышленной частотой 50 Гц). Обмен информацией между подстанциями достаточно производить с частотой дискретизации данных не более 1 кГц, что означает не более 0,5 Мбит/с на один комплект токов или напряжений. Включенный объем дополнительной информации для синхронизации не превышает 50% от объема аналоговых данных.

Предложенная система синхронизации данных двух подстанций представляется работоспособной, если загрузка сети невысока, пропускная способность канала связи составляет не менее 10 Гбит/с, а также возможно настроить приоритеты обработки различных видов трафика [8]. Один и тот же сегмент связи может использоваться как часть маршрута связи десяти комплектов ДЗЛ. Это свойство технологии E-SV окажется полезным в регионах с высокой концентрацией электрических сетей, например, в мегаполисах.

Полукомплекты ДЗЛ должны выполнять постоянную автоматическую диагностику качества каналов связи, наблюдая стабильность периода пакетов E-SV. Если отклонение значительное, полукомплекты могут блокировать расчет и ожидать восстановления характеристик связи.

Технология E-SV может быть оформлена в виде открытого стандарта и реализована в измерительных устройствах и в терминалах защиты различных производителей. Это повысит гибкость в развитии и цифровизации электрической и информационной сетей. Однако эксплуатация «смешанных» ДЗЛ от разных производителей может столкнуться со следующими эффектами, ранее не характерными для традиционных ДЗЛ:

1. Различные чувствительность и быстродействие полукомплектов ДЗЛ, установленных на разных концах линии электропередачи.
2. Необходимость согласования работы полукомплектов защиты на этапе проектирования за счет перекрестного отключения (отключения удаленного конца линии).
3. Усложнение процесса испытаний полной схемы ДЗЛ.

Тем не менее, переход на пакетную передачу данных будет означать применение наиболее современных технических решений в области коммуникаций, увеличенный срок службы систем защиты.

Заключение

Таким образом, в докладе предложена и описана технология E-SV, развивающая идеи МЭК 61850-9-2 (SV). Такое техническое решение обладает высокой степенью автономности и не зависит от систем глобального времени. Протокол может быть оформлен в виде открытого стандарта и реализован в измерительных устройствах и в терминалах защиты различных производителей. Это значительно упростит применение ДЗЛ как основной защиты сетей, соединяющих объекты разных собственников.

ЛИТЕРАТУРА

[1] Положение ПАО «Россети» «О единой технической политике в электросетевом комплексе», 08.11.2019, https://www.rosseti.ru/investment/science/tech/doc/tehpolitika.pdf

[2] C37.94-2002 – IEEE Standard for N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment.

[3] Харламов В. А., Хасанов А. Х. Высоконадежные каналы по цифровым сетям связи для существующих и перспективных систем РЗА // Релейщик. 2015. №2. С.18-22.

[4] Standard IEC 61850. Сети и системы связи на подстанциях. Часть 9-2 – «Описание специфического сервиса связи (SCSM) — Выборочные значения по ИСО/МЭК 8802-3».

[5] Astic J-Y., Leitloff V. et al "Postes Intelligents" Design, Test and Commissioning of Rte's first completely Digital Substation // PAC World. 2018. September. P. 46-51.

[6] Time in Protection Applications – Time sources and distribution Methods: Special Report // CIGRE SC B5 Colloquium. 2019. P.1-6.

[7] Терминал продольной дифференциальной защиты линий 110-220 кв типа «ТОР 300 ДЗЛ 52Х». Руководство по эксплуатации. Описание функций защит. АИПБ.656122.011-014 РЭ2. 2019.

[8] Stefanka M. The Parallel Redundancy Protocol over Wide Area Networks. Smart Grid and Renewable Energy. 07. 147-153. 10.4236/sgre.2016.74011.

[9] RFC 5905. Network Time Protocol Version 4: Protocol and Algorithms Specification.

СЕКЦИЯ 3.

«Кибербезопасность – драйвер или тормоз развития?»

3.1. ПРИНЦИПЫ РЕАЛИЗАЦИИ КИБЕРБЕЗОПАСНЫХ РЕШЕНИЙ ДЛЯ КРОСС-ПЛАТФОРМЕННОЙ РЗА

В.М. ЗИНИН, Т.Р. ШАРАФЕЕВ, А.Л. КУЛИКОВ

АО «НИПОМ», НГТУ им. Р. Е. Алексеева

Россия

Контактное лицо:

В.М. ЗИНИН

v.zinin@nipom.ru

Ключевые слова

РЗА, МЭК 61850, информационная безопасность АСТУ, кибербезопасность, МЭК 62351-6, КИИ, ФСТЭК, ЦПС, ИЭУ.

ВВЕДЕНИЕ

Указом Президента РФ № 216 от 13 мая 2019 года утверждена обновлённая «Доктрина энергетической безопасности Российской Федерации» [1], закрепляющая на законодательном уровне следующие основные угрозы и риски:

- одной из основных трансграничных угроз обозначено «противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов топливно-энергетического комплекса»;
- одним из основных рисков названо «несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков».

Таким образом «Доктрина энергетической безопасности Российской Федерации» задает направление на дальнейшее развитие импортозамещения в системах технологического управления электроэнергетическим комплексом, объекты которого относятся к критической информационной инфраструктуре (КИИ) [2].

С введением в действие 29 марта 2019 года СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ» [3] ПАО «Россети» сформировало нормативную базу для создания интеллектуальных электронных устройств (ИЭУ) и проектирования объектов электрических сетей на новых (цифровых) принципах.

Предметом исследования авторов доклада является изучение возможности использования серийно выпускаемых вычислительных средств промышленной автоматизации и операционных систем для разработки кибербезопасных решений для кросс-платформенной РЗА в составе цифровых подстанций (ЦПС) с последующей типизацией.

В докладе представлен обзор новой технологии разработки кибербезопасных решений для кросс-платформенной РЗА, результатом которой являются серийно выпускаемые изделия – ИЭУ РЗА, удовлетворяющие современным и перспективным требованиям развития автоматизированных систем технологического управления в электрических сетях.

Цель доклада – познакомить с особенностями применения ИЭУ РЗА, созданными по данной технологии в составе ЦПС, и показать перспективы её дальнейшего развития с учетом обновленной «Доктрины энергетической безопасности Российской Федерации» и обновления отраслевой нормативной базы в ходе цифровой трансформации отрасли.

РАЗВИТИЕ МЭК 61850 В ЧАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с СТО 34.01-21-004-2019 ПАО «Россети» единичным объектом АСТУ (согласно СТО 56947007-29.240.10.248-2017) является центр питания (ЦПС) напряжением 6-220 кВ с использованием МЭК 61850 в качестве стандарта передачи данных.

На рис. 1 показаны изменения, которые обсуждаются в настоящее время международной группой разработки IEC 61850-8-1/AMD1 ED2 для внесения в обновлённую редакцию стандарта. Как можно увидеть (выделено красным пунктиром), в профиле IEC 61850 появился IEC 62351-6 «Управление энергетическими системами и связанным с этим обменом информацией. Безопасность данных и коммуникаций. Часть 6. Безопасность для IEC 61850». Для потоков данных, выходящих за пределы ПС, применение IEC 62351-6 будет обязательным, внутри технологической вычислительной сети ПС рекомендуемым.

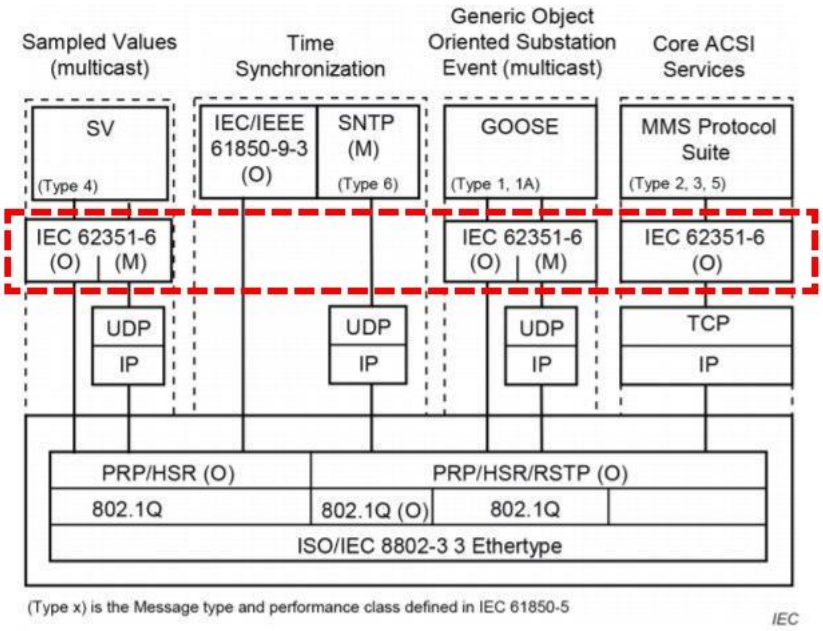


Figure 1 – Overview of functionality and profiles

Рис. 1. Развитие стандарта МЭК 61850 в части информационной безопасности.

Дальнейшее развитие МЭК 61850 подразумевает встраивание функций ИБ в ИЭУ. Большинство выпускаемых сегодня интеллектуальных электронных устройств для ЦПС, поддерживающих МЭК 61850, не удовлетворяют в полном объеме IEC 62351-6 и СТО 34.01-21-004-2019 (в части ИБ). Исторически при формировании технических требований к разработке ИЭУ наличие функций информационной безопасности не учитывалось. Встраивание функций ИБ снижает быстродействие ИЭУ, что недопустимо для РЗА.

Цифровая трансформация электроэнергетики заставляет искать пути создания новой технологии разработки интеллектуальных электронных устройств для ЦПС, и ИЭУ РЗА в частности, лишенной этих технологических ограничений.

Важно также отметить, что IEC 62351 до сих пор не принят в РФ в качестве национального стандарта, хотя фактически применяется в системах технологического управления различного назначения, в том числе и объектов критической информационной инфраструктуры (КИИ).

ТЕХНОЛОГИЯ РАЗРАБОТКИ КИБЕРБЕЗОПАСНЫХ РЕШЕНИЙ ДЛЯ КРОСС-ПЛАТФОРМЕННОЙ РЗА

Современное развитие вычислительной техники характеризуется тенденцией удешевления компонентной базы (микропроцессоров, оперативной памяти, систем хранения, интерфейсных микросхем и т. д.) при росте её надёжности и производительности. В результате этого получили широкое распространение вычислительные средства промышленной автоматизации, выпускаемые серийно и имеющие высокую степень стандартизации. Также сегодня имеется возможность выбора серийно выпускаемых операционных систем для промышленных (космических, военных) условий применения, имеющих развитую систему информационной безопасности, в том числе и сертифицированных ФСТЭК.

При разработке кибербезопасных решений для кросс-платформенной РЗА выделяется несколько уровней абстракции, часть из которых представляет собой доверенную аппаратно-программную платформу, не зависящую от конкретного производителя.



Рис. 2. 5 уровней абстракции при создании кроссплатформенного ИЭУ.

Использование доверенной аппаратно-программной платформы обеспечивает информационную безопасность разрабатываемого ИЭУ РЗА в соответствии с требованиями ФСТЭК [4] и одновременно освобождает производителя ИЭУ от трудоемких процессов технического сопровождения (аттестации) аппаратного исполнения. Основные усилия производителя ИЭУ направлены на разработку, совершенствование алгоритмической базы и поддержание прикладного функционального программного обеспечения устройств, устойчивого к угрозам информационной безопасности.

При реализации кибербезопасных решений (рис. 2) для кросс-платформенной РЗА в качестве аппаратной составляющей применяются серийно выпускаемые промышленные вычислители, в основе которых лежат распространённые микропроцессоры как импортного (Intel, AMD, ARM), так и отечественного (Эльбрус, Байкал) производства, что формирует первый уровень абстракции. На втором и третьем уровне абстракции используются серийные операционные системы, имеющие соответствующую сертификацию ФСТЭК (Astra Linux, Alt Linux, Elbrusd, «Нейтрино», QNX). Первые три уровня не зависят от конкретного производителя ИЭУ. Четвертый и пятый уровни абстракции модели кросс-платформенного ИЭУ собственно и представляют собой кросс-платформенное функциональное программное обеспечение ИЭУ и коммуникации МЭК 61850. Требования по информационной безопасности (ИБ) изначально закладываются в информационную модель МЭК 61850 ИЭУ при его создании. ИЭУ, созданные с использованием данной технологии, поддерживают [5]:

- SSL/TLS-шифрование для МЭК 61850-8-1 (MMS) между ИЭУ и другими технологическими подсистемами ЦПС, а также между ЦУС;
- двухфакторную аутентификацию на ИЭУ РЗА и АРМ эксплуатационного и оперативного персонала технологической вычислительной сети (шине станции) ЦПС при удаленном доступе к ИЭУ;
- ролевой доступ к элементам интерфейса ИЭУ в зависимости от функциональных обязанностей персонала;
- протоколирование событий безопасности на уровне отдельного ИЭУ, ЦПС и ЦУС.

В настоящее время мы продолжаем работы по реализации (встраиванию) имитовставки в GOOSE-сообщения. Эта функциональность также станет частью информационной модели МЭК 61850 кросс-платформенных ИЭУ.

Реализация 5-уровневой модели кроссплатформенного ИЭУ осуществляется с помощью специализированного «Кодогенератора управляющего ПО», который представляет собой инновационный инструмент создания кроссплатформенных решений для «киберзащищенной ЦПС с динамичной архитектурой», где ИЭУ РЗА – один из функциональных элементов (рис. 3).



Рис. 3. Процесс создания кросс-платформенного ИЭУ с использованием «Кодогенератора управляющего ПО»

«Кодогенератор управляющего ПО» включает в себя библиотеку компонентов, с помощью которой специалисты предметной области без программирования в визуальном режиме создают логические схемы ИЭУ, проверяют их корректность, определяют состав групп локального периметра безопасности с правами доступа к элементам интерфейса и функциям ИЭУ. При создании логической схемы ИЭУ «Кодогенератор…» автоматически формирует информационную модель МЭК 61850 ИЭУ, включая атрибуты информационной безопасности, что существенно упрощает создание и конфигурирование файлов стандарта МЭК 61850. После создания логической схемы ИЭУ можно подать на её вход заранее подготовленный Comtrade-файл и проверить корректность работы ИЭУ в различных режимах. После этого «Кодогенератор…» генерирует программный код на языке «Си», который компилируется для выполнения на перечисленных выше аппаратно-программных платформах. Важно отметить независимость генерируемого программного кода от операционной системы и микропроцессора и его идентичность, а также, типизацию и стандартизацию модели ИБ ИЭУ.

С помощью «Кодогенератора…» создаются ИЭУ различного функционального назначения:

- ✓ ИЭУ РЗА для 6-220 кВ;
- ✓ ИЭУ АСУ ТП, оперативной блокировки, автоматики управления нормальными и аварийными режимами;
- ✓ ИЭУ контроллеры присоединений;

✓ ИЭУ технического учета ЭЭ и контроля качества ЭЭ.

Использование «Кодогенератора…» минимизирует количество ошибок при создании ИЭУ, а время его создания, в зависимости от сложности и наличия соответствующего математического аппарата (алгоритмической базы) в «Кодогенераторе...», составляет 2-3 недели.

В таблице 1 приводятся требования по информационной безопасности, реализованные в ИЭУ РЗА, созданном с использованием «Кодогенератора…», соответствующие Распоряжению ПАО «Россети» № 282р от 30.05.2017 г. «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети» [6].

№ п/п	Идентификатор	Наименование требования
1	FAU_GEN.1	Генерация данных аудита
2	FAU_GEN.2	Ассоциация идентификатора пользователя
3	FAU_SAR.1	Просмотр журналов аудита
4	FAU_STG.1	Защищенное хранение журнала аудита
5	FAU_STG.3	Действия в случае возможной потери данных аудита
6	FAU_STG.4	Предотвращение потери данных аудита
7	FDP_ACC.1	Ограниченное управление доступом
8	FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
9	FIA_AFL.1	Обработка отказов аутентификации
10	FIA_ATD.1	Определение атрибутов пользователя
11	FIA_UAU.2	Аутентификация до любых действий пользователя
12	FIA_UAU.7	Аутентификация с защищенной обратной связью
13	FIA_UID.2	Идентификация до любых действий пользователя
14	FMT_MSA.1	Управление атрибутами безопасности
15	FMT_MSA.3	Инициализация статических атрибутов
16	FMT_MTD.1	Управление данными ФБО
17	FMT_SMF.1	Спецификация функций управления
18	FMT_SMR.1	Роли безопасности
19	FTA_SSL.1	Блокирование сеанса, инициированное функциями безопасности

Табл. 1. Требования по информационной безопасности, реализованные в ИЭУ РЗА

Табл. 2 показывает детализацию требования FMT_SMR.1 (Роли безопасности) в этом же ИЭУ РЗА.

Название группы	Функциональные обязанности, роли	Права доступа к элементам интерфейса и функциям ИЭУ РЗА
Администратор(ы)	Представители компании-производителя и/или компании, выполняющей ПНР	Полный доступ к элементам интерфейса и параметрированию
Специалист(ы) по ИБ	Специалист по ИБ	Управление пользователями
Эксплуатационный персонал	Специалисты, отвечающие за эксплуатацию ИЭУ (для ИЭУ РЗА – инженеры РЗА)	Параметрирование с некоторыми ограничениями (калибровка, настройка параметров ЛВС)
Оперативный персонал	Специалисты ОВБ, диспетчерский персонал ПС	Ввод/вывод функций РЗА и автоматики, чтение осциллограмм, журнала событий
Читатель	Руководящий персонал ПС	Чтение осциллограмм, журнала событий

Специалист(ы) по АСУ ТП	Инженер по связи, инженер по ИТ	Настройка параметров ЛВС

Табл. 2. Детализация функционального требования FMT_SMR.1 (Роли безопасности) в ИЭУ РЗА.

ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИИ

ИЭУ РЗА для электрических сетей 6-220 кВ, созданные по описанной технологии, неоднократно представлялись на отраслевых научно-технических советах, признаны отраслевым профессиональным сообществом и аттестованы в ПАО «Россети».

Технология позволяет расширить область её применения для типизации и стандартизации ИЭУ различного функционального назначения АСТУ цифровых подстанций (рис. 3), т. е. для проектирования ЦПС с заданной степенью централизации/децентрализации и сценариями резервирования в реальном времени - «киберзащищённых ЦПС с динамичной архитектурой». Основными критериями при выборе варианта являются: надежность, стоимость и соответствие отраслевым требованиям и стандартам.

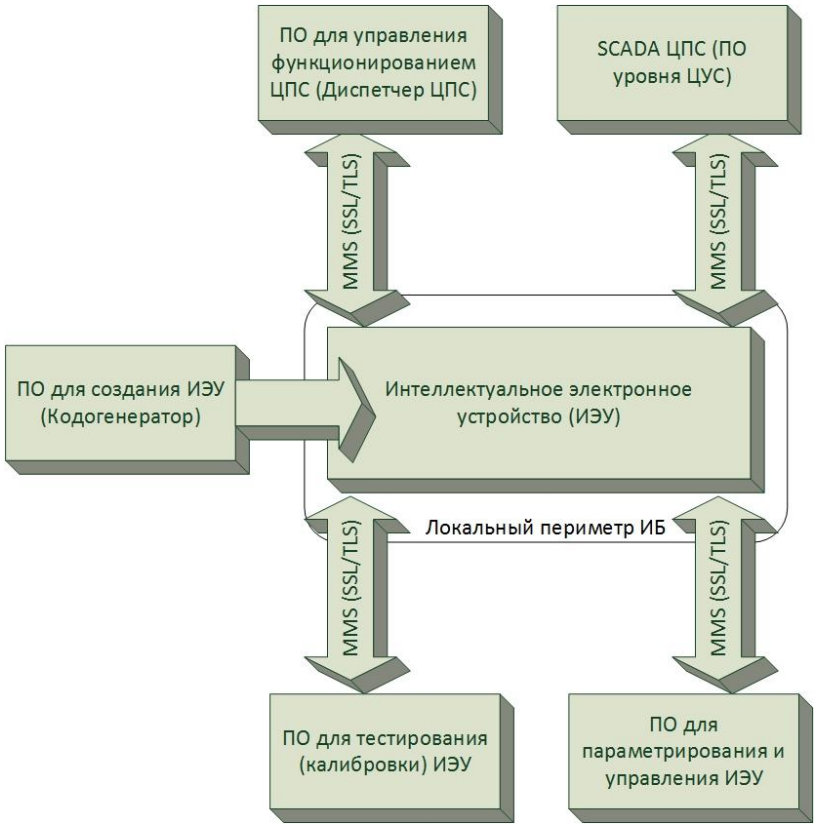


Рис. 4. ИЭУ в составе «Киберзащищенной ЦПС с динамичной архитектурой»

На «киберзащищённых ЦПС с динамичной архитектурой» подсистема информационной безопасности становится полноценной технологической подсистемой объекта критической информационной инфраструктуры (КИИ) наряду с РЗА, АСУ ТП, АИИСКУЭ и т. д. Для каждого ИЭУ АСТУ ЦПС типизируется «локальный периметр безопасности», обеспечивающий индивидуальную устойчивость к киберугрозам и возможным несанкционированным или ошибочным действиям.

ВЫВОДЫ

1. Подсистемы РЗА и АСУ ТП ЦПС являются наиболее критичными компонентами с точек зрения угроз несанкционированного вмешательства. Одна из точек зрения, основанная на абсолютной изоляции указанных подсистем ЦПС, не соответствует перспективам интеллектуализации современной электроэнергетики. Такой подход фактически препятствует дальнейшей оптимизации электроэнергетических систем и формированию технологического управления передачей и распределением электроэнергии, которое должно учитывать растущую долю распределенной мини- и микрогенерации. Предпочтительным является подход к созданию комплексной системы кибербезопасности, структурные компоненты которой учитывают индивидуальные для ЦПС функциональные особенности и правила противодействия киберугрозам.
2. Технология разработки кибербезопасных решений для кросс-платформенной РЗА с последующим расширением области её применения на типизацию и стандартизацию ИЭУ различного функционального назначения АСТУ ЦПС позволяет создавать «киберзащищённые ЦПС с динамичной архитектурой».
3. Использование доверенной аппаратно-программной платформы, базирующейся на отечественных микропроцессорах и сертифицированных ФСТЭК операционных системах для создания кроссплатформенных ИЭУ различного функционального назначения АСТУ ЦПС, предпочтительно для снижения технологической зависимости электроэнергетической отрасли РФ и минимизации угроз и рисков, изложенных в обновлённой «Доктрине энергетической безопасности Российской Федерации».

ЛИТЕРАТУРА

[1] Указ Президента РФ № 216 от 13 мая 2019 года «Об утверждении Доктрины энергетической безопасности Российской Федерации» (http://www.consultant.ru/document/cons_doc_LAW_324378/)
[2] Федеральный закон № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации» (http://www.consultant.ru/document/cons_doc_LAW_220885/)
[3] СТО 34.01-21-004-2019 ПАО «Россети» «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ»
[4] Приказ ФСТЭК России №76 от 2 июня 2020 года «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/2126-vypiska-iz-trebovanij-po-bezopasnosti-informatsii-utverzhdennykh-prikazom-fstek-rossii-ot-2-iyunya-2020-g-n-76)
[5] Карантаев В. Г. Вопросы кибербезопасности в меняющейся электроэнергетической отрасли. «Релейщик» № 1(33) 2019 г., с. 48-51
[6] Распоряжение ПАО «Россети» № 282р от 30 мая 2017 года «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети»

3.2.ТЕХНОЛОГИИ РЗА ЦПС, ОБЕСПЕЧИВАЮЩИЕ ПОВЫШЕННУЮ УСТОЙЧИВОСТЬ К КИБЕРАТАКАМ

А.А. ВОЛОШИН, Е.А. ВОЛОШИН, С.М. НУХУЛОВ, В.И. ДОБРЫНИН, Д.О. БЛАГОРАЗУМОВ
Центр НТИ МЭИ
Россия

Контактное лицо:

voloshin.aa@yandex.ru

Ключевые Слова

Кибербезопасность, вейвлет-анализ, цифровая обработка.

ВВЕДЕНИЕ

Актуальность вопросов кибербезопасности автоматизированных систем критически важных объектов вообще и объектов электроэнергетики, в частности, с каждым годом растет. По данным ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team) за 2016 год было зарегистрировано 290 инцидентов кибербезопасности на объектах критической инфраструктуры США. Причем на третьем месте по количеству кибератак располагается сектор энергетики – 59 случаев кибератак [1]. По данным российской компании Positive Technologies, за 2020 г. было произведено 47 уникальных атак на промышленный сектор (атаки, использующие одинаковое ПО или методы вторжения, считались за один инцидент), большинство из них (89%) было направлено на инфраструктуру предприятия (компьютеры, серверы и сетевое оборудование) [2].

В индустрии электроэнергетики цифровые технологии стали внедряться на нижнем (полевом) уровне для решения задач повышения эффективности управления производственными процессами. Драйвером развития такого подхода служат стандарт МЭК 61850 и программа цифровизации экономики России. Цифровая трансформация в энергетике происходит за счет создания Smart Grid (интеллектуальных сетей), составляющими частями которых являются цифровые питающие и распределительные центры (ЦПС – цифровая подстанция).

Архитектура энергетических объектов нового поколения может быть подвержена кибератакам: атакам доступа, атакам модификации, DoS- и DDoS-атакам, комбинированным атакам. Поэтому есть необходимость в обеспечении защиты информации и сохранении функциональной безопасности цифровых подстанций.

Широко распространены технические решения по защите цифровых технологий от кибератак, предусмотренные архитектурой устройств и систем, используемых на энергообъектах, и заключающиеся в использовании наложенных средств защиты (межсетевых экранов /Firewall/, систем обнаружения вторжений /IDS/, Endpoint-антивирусов, систем контроля и управления доступом /СКУД/, SIEM /Security Information and Event Management/ и SOC /Security Operation Center/), а также внутренних средств защиты (сертификатов доверия при обращении и загрузке ПО /Trusting Self-Signed Certificates/, систем идентификации и аутентификации пользователей на инженерном ПО /RBAC – Role based access control/, криптографических защит информации).

Разрабатываются в мире и средства и системы защиты информации, в частности операционные системы со встроенными механизмами защиты, которые позволяют освободить прикладное ПО от необходимости предусматривать защитные функции и, как следствие, избавиться от ошибок (Kaspersky OS).

Наложенные средства защиты необходимы в использовании при недостаточности функций, встроенных в используемое ПО и устройства, однако есть проблемы установки в уже действующие сети, а также проблемы совместимости оборудования различных поставщиков.

Известны технические решения по обеспечению бесперебойного электропитания потребителей электроэнергетической системы, в том числе и путем исключения ложных срабатываний логических органов релейной защиты (РЗ), базирующиеся на введении для последних соответствующей выдержки времени на срабатывание и блокировании на это время исполнительных органов РЗ [3], [4], [5]. Однако использование выдержки времени отрицательно сказывается на быстродействии РЗ.

Известен также способ бесперебойного электропитания потребителей электроэнергетической системы, предусматривающий, помимо измерения абсолютных значений напряжения и тока, их динамический анализ и сравнение измеренных значений, т. е. более полный контроль энергорежима на защищаемом потребителе, позволяющий с помощью передаваемых по каналу связи результатов анализа к логическому органу уменьшить количество ложных срабатываний РЗ [6]. Недостаток такого способа связан с

несовершенством используемого динамического анализа переходных процессов и, как следствие, с возможными ошибками в работе логического органа.

Следует заметить, что в последнее время находят применение технические решения по реализации динамического анализа электрических параметров с помощью вейвлет-преобразований [7], 8].

Целью доклада является обеспечение бесперебойного электроснабжения потребителей с повышением защиты потребителей от кибератак и сохранением высокого качества их защиты от повреждений в сети электроснабжения.

Для достижения цели предлагается способ бесперебойного электропитания потребителей с использованием интеллектуальной сети электроснабжения, согласно которому у потребителей устанавливают устройства РЗ, реагирующие на недопустимое отклонение от нормальных электрических рабочих параметров, в сети электроснабжения непрерывно измеряют рабочие электрические параметры и анализируют переходные процессы по их вейвлет-преобразованию, а в случае возникновения повреждений в сети пуск устройств РЗ и аварийное отключение соответствующих потребителей осуществляют при выходе значений вейвлет-функции за заданные пределы.

ОСНОВНАЯ ЧАСТЬ

Сравнение преобразования Фурье с вейвлет-преобразованием

Комплексное непрерывное вейвлет-преобразование в настоящее время является одним из наиболее активно развивающихся методов гармонического анализа нестационарных сигналов [9][10]. Приведем сравнение с преобразованием Фурье.

Интегральное преобразование Фурье и ряды Фурье являются основой гармонического анализа. Получаемые в результате преобразования коэффициенты Фурье поддаются достаточно простой физической интерпретации, причем простота ни в коем случае не умаляет важности последующих выводов о характере исследуемого сигнала. Применение интегрального преобразования и рядов Фурье (в вычислениях, аналитических преобразованиях) очень наглядно, все необходимые свойства и формулы выписываются с помощью всего двух действительных функций $\sin t, \cos t$ (или одной комплексной — синусоидальной волны $e^{it} = \cos t + i \sin t,\ i = \sqrt{-1}$) и достаточно легко доказываются [11].

Преобразование Фурье и ряды Фурье являются прекрасным математическим аппаратом для физической интерпретации процессов при анализе характеризующих их сигналов. Однако иногда они оказываются недостаточно эффективными.

Реальный сигнал всегда (или, как правило) принадлежит пространству функций $f(t)$, определенных на всей действительной оси $R(-\infty, \infty)$ и обладающих конечной энергией (нормой):

$$\|f\| = \left(\int_{-\infty}^{\infty} |f(t)|^2 dt \right)^{1/2} < \infty.$$

. Преобразование Фурье сигнала $f(t)$ с конечной энергией, определенной нормой $\|f\|$, представляет собой спектр этого сигнала:

$$\hat{f}(\omega) = \int_{-\infty}^{\infty} f(t)\, e^{-i\omega t} dt.$$

В некоторых случаях физическая интерпретация с помощью формулы бывает затруднительна. Так, чтобы получить спектральную информацию на выбранной частоте, необходимо иметь и прошлую и будущую временную информацию; к тому же формула не учитывает, что частота может эволюционировать со временем. Преобразование Фурье, например, не отличает сигнал, представляющий собой сумму двух синусоид с разными частотами, от сигнала, состоящего из тех же синусоид, включающихся последовательно одна за другой.

Кроме того, известно, что частота сигнала обратно пропорциональна его продолжительности. Поэтому для получения высокочастотной информации с хорошей

точностью важно извлекать ее из относительно малых временных интервалов, а не из всего сигнала; и наоборот – низкочастотную спектральную информацию извлекать из относительно широких временных интервалов сигнала.

Часть описанных трудностей снимается при использовании оконного преобразования Фурье. Однако бесконечно осциллирующая базисная функция (синусоидальная волна) не позволяет получать по-настоящему локализованную информацию. Элементом базиса вейвлет-преобразования является хорошо локализованная функция, быстро стремящаяся к нулю вне небольшого интервала, что позволяет провести «локализованный спектральный анализ». Иными словами, вейвлет-преобразование автоматически обладает подвижным частотно-временным окном, узким на малых масштабах и широким на больших масштабах.

Поскольку вейвлет-преобразование есть скалярное произведение анализирующего вейвлета на заданном масштабе и анализируемого сигнала, коэффициенты интегрального вейвлет-преобразования содержат комбинированную информацию об анализирующем вейвлете и анализируемом сигнале (как и коэффициенты преобразования Фурье, которые содержат информацию о сигнале и о синусоидальной волне).

Выбор анализирующего вейвлета, как правило, определяется тем, какую информацию необходимо извлечь из сигнала. Каждый вейвлет имеет характерные особенности во временном и в частотном пространстве, поэтому иногда с помощью разных вейвлетов можно полнее выявить и подчеркнуть те или иные свойства анализируемого сигнала.

Наиболее часто используемый комплексный базис строится на основе хорошо локализованного в частотном и временном пространстве вейвлета Морле (Morlet) [12]:

$$\psi(r) = e^{ik_0 r} e^{\left(-\frac{r^2}{2}\right)},$$
$$\hat{\psi}(k) = \theta(k) e^{\left(-\frac{(k-k_0)^2}{2}\right)}$$

плоская волна, модулированная гауссианом единичной ширины. На рисунке 1 вейвлет Морле показан с центральной частотой $k_0 = 6$ Гц. С увеличением k_0 возрастает угловая избирательность базиса, но ухудшается пространственная.

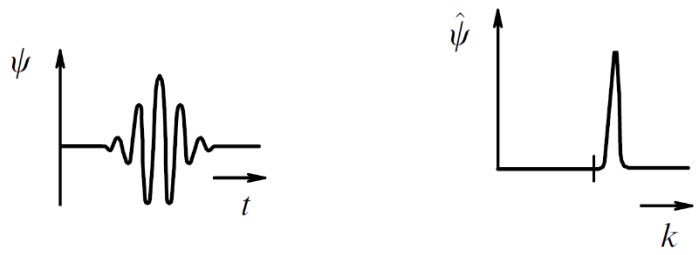


Рис. 1: Вейвлет Морле.

Объект исследования

Объектом исследования является ПС 500/110/10 кВ (см. рис. 2), смоделированная в ПК RTDS (RSCAD).

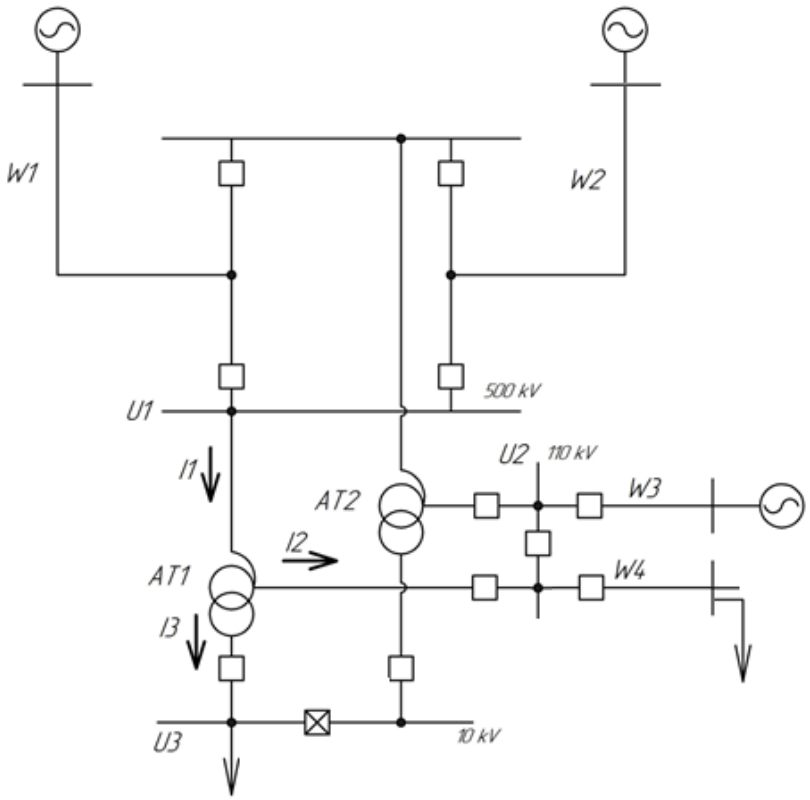


Рис. 2: Схема моделируемой сети

Параметры элементов исследуемой сети представлены в табл. 1 – 4.

Табл. 1. Параметры автотрансформатора АТДЦТН 250000/500/110-У1.

Трансформатор	Номинальное напряжение, кВ			Напряжение КЗ, %			Потери, кВт	
	ВН	СН	НН	ВН-СН	ВН-НН	СН-НН	ХХ	КЗ
АТДЦТН 250000/500/110-У1	500	121	10,5	10,5	38,0	27,0	180	625

Табл. 2. Параметры линий W1-W4.

Линии	$U_{ном}$, кВ	L, км	S, мм^2	R_1, Ом/км	R_0, Ом/км	X_1, Ом/км	X_0, Ом/км	B, см/км
W1	500	300	3x300	0,029	0,087	0,308	0,924	$3,6*10^4$
W2	500	500	3x300	0,029	0,087	0,308	0,924	$3,6*10^4$
W3	121	50	1x300	0,118	0,332	0,405	1,215	$2,8*10^4$
W4	121	50	1x300	0,118	0,332	0,405	1,215	$2,8*10^4$

Табл. 3. Параметры эквивалентных энергосистем.

Линии	$U_{ном}$, кВ	Угол, градусы	R_1, Ом	R_0, Ом	X_1, Ом	X_0, Ом
S1	500	0	0,5	0,67	0,7	0,93
S2	500	15	0,4	0,54	0,62	0,84
S3	121	7	1,2	1,56	1,43	1,93

Табл. 4. Параметры нагрузок.

Нагрузка	P, МВт	Q, МВар
СН	50	5
НН	2x15	2x1,5

Описание способа

Для реализации пускового органа (ПО) используется вейвлет-преобразование, так как оно позволяет проводить анализ переходного процесса и определять с заданной точностью момент возникновения аварийной ситуации.

Непрерывное вейвлет-преобразование определяется выражением:

$$CWT^{\psi}(\tau, s) = \frac{1}{\sqrt{|s|}} \int f(t) \cdot \psi_{jk}^{*}\left(\frac{t-\tau}{s}\right) dt,$$

где ψ_{jk}^{*} – комплексно сопряженная функция материнского вейвлета;

τ – параметр сдвига;

s – параметр масштаба.

В качестве базиса был выбран вейвлет Морле:

$$\psi_{jk}(t) = \frac{1}{\sqrt{\pi f_{\text{п}}}} e^{-\frac{t}{f_{\text{п}}}} e^{j2\pi f_{\text{ц}} t},$$

где $f_{\text{ц}}$– центральная частота вейвлета;

$f_{\text{п}}$– ширина полосы пропускания.

В качестве анализируемой функции пусковым органом используется функция модуля коэффициентов комплексного вейвлет-преобразования:

$$|c| = \left|\langle f_{A,B,C}, \psi_{jk} \rangle\right|.$$

Схема предлагаемого способа защиты от кибератак представлена на рисунке 3.

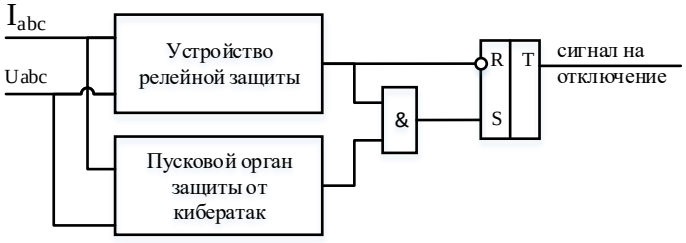


Рис. 3. Схема предлагаемого способа защиты от кибератак.

При возникновении аварийной ситуации, когда требуется срабатывание устройства защиты, пусковой сигнал от устройства релейной защиты будет разрешен пусковым органом защиты от кибератак, работа которого основана на вейвлет-преобразовании и фиксации момента аварийной возмущения.

При возникновении в сети несинусоидальных режимов и искажений формы синусоиды тока вследствие действия систем управления напряжения, а также при появлении сигналов от устройств РЗ, сформированных злоумышленником, пусковой орган защиты от кибеатак фиксирует значение вейвлет-функции ниже заданного порогового и предотвращают формирование сигналов на отключение от устройств РЗ.

Для расчета модуля коэффициентов вейвлет-преобразования Морле формируют буфер мгновенных значений тока и напряжения во временном окне от 1 до 3 мс.

Проведение опытов

Проведем опыт однофазного короткого замыкания на шинах СН (см. рисунок 2). Примем параметры вейвлета Морле $f_{ц} = 31250$ Гц, $f_{п} = = 31250$ Гц для частоты дискретизации 1 МГц. Параметр масштаба выбран $s = 32$. В результате работы алгоритма времена достижения максимумов модулей коэффициентов вейвлет преобразования равны соответственно U_A: $t_{|c.max|} = 201{,}350$ мс; U_B: $t_{|c.max|} = 203{,}350$ мс; U_C: $t_{|c.max|} = =203{,}150$ мс; I_A: $t_{|c.max|} = 200{,}350$ мс; I_B: $t_{|c.max|} = 199{,}850$ мс; I_C: $t_{|c.max|} = 199{,}850$ мс.

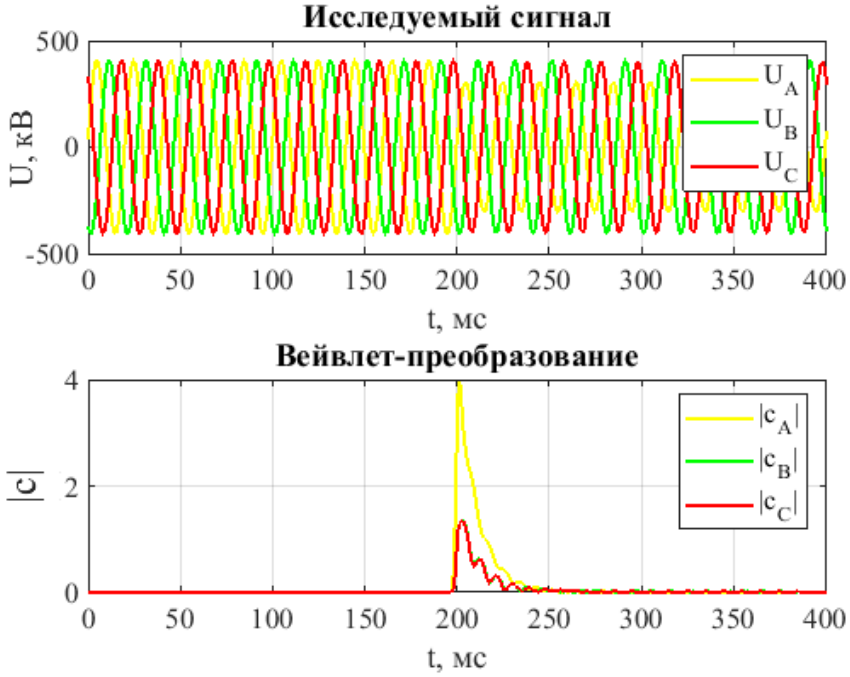


Рис. 4. Определение максимума модуля коэффициентов вейвлет-преобразования напряжений на шинах ВН при однофазном КЗ на шинах СН.

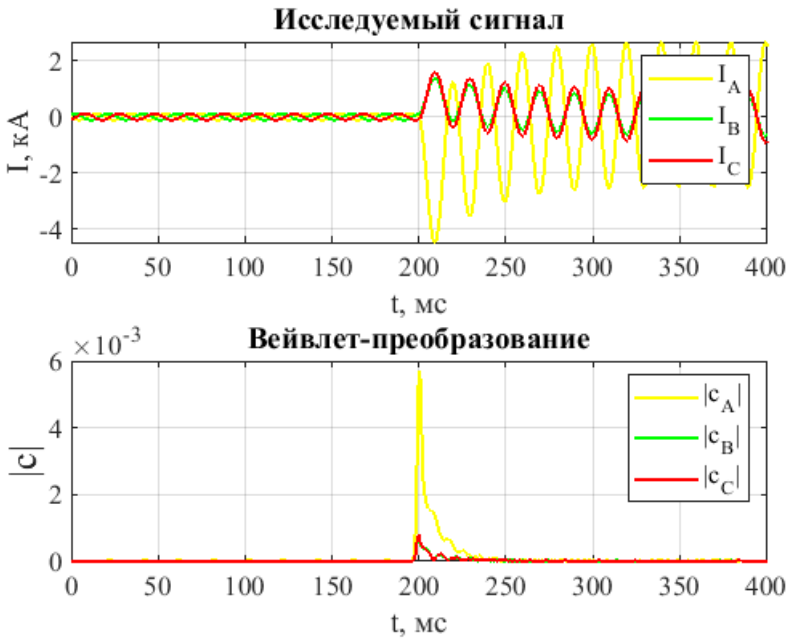


Рис. 5. Определение максимума модуля коэффициентов вейвлет-преобразования токов через линию W1 при однофазном КЗ на шинах СН.

Из осциллограмм (рис. 4, 5) видно, что скачок модуля коэффициентов вейвлет-преобразования происходит одновременно в трех фазах напряжения и тока.

Проведем опыт однофазного КЗ в фазе В за автотрансформатором АТ2 на стороне СН в момент 20 мс от начала моделирования . Результаты опыта сведены в табл. 5.

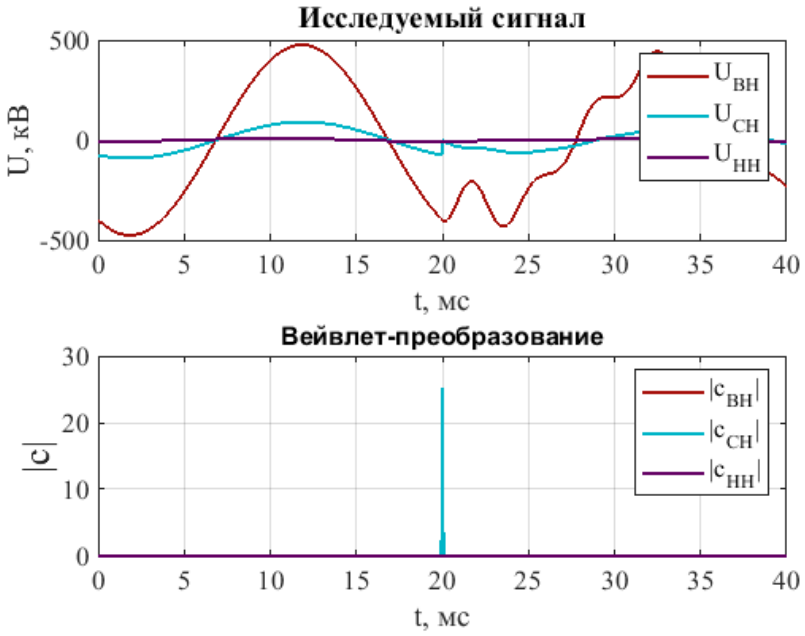


Рис. 6. Определение максимума модуля коэффициентов вейвлет-преобразования напряжений с трех сторон АТ при однофазном КЗ на шинах СН.

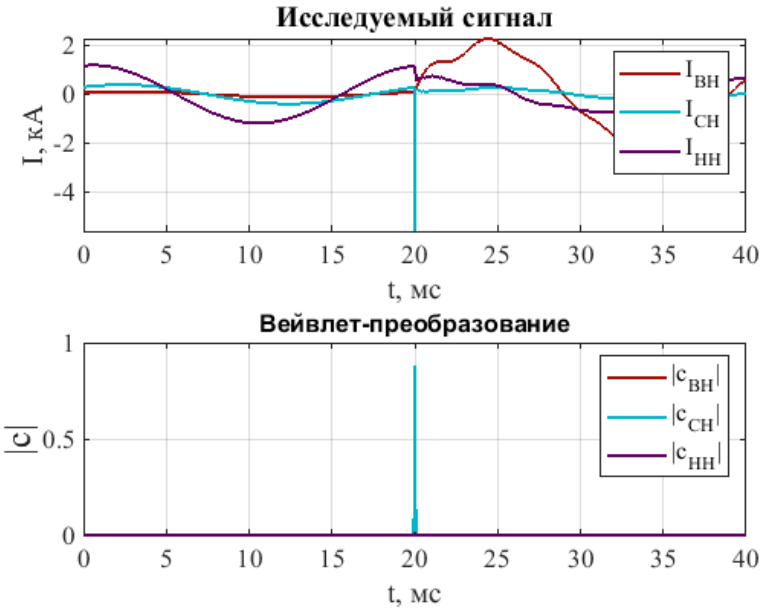


Рис. 7. Определение максимума модуля коэффициентов вейвлет-преобразования токов с трех сторон АТ при однофазном КЗ на шинах СН.

Табл. 5. Результаты опыта однофазного КЗ на шинах СН.

		U_A	U_B	U_C	I_A	I_B	I_C
ВН	$\|c_{max}\|$	0,4335	0,1546	0,1597	0,0307	0,0307	0,1662
	$t_{\|c.max\|}$, мс	20,003	20,003	20,003	20,003	20,003	20,003
СН	$\|c_{max}\|$	2220,6	406,843	406,842	222,583	0,1955	0,1955
	$t_{\|c.max\|}$, мс	20,003	20,003	20,003	20,003	20,002	20,002
НН	$\|c_{max}\|$	9,6763	0,000077	9,6763	1,3165	0,00001	1,3165
	$t_{\|c.max\|}$, мс	20,003	20,001	20,003	20,003	20,001	20,003

По результатам опыта можно судить о том, что погрешность определения момента КЗ относительно устройств с трех сторон АТ не превышает 1 мс.

При возникновении несинусоидальных режимов вследствие действия систем управления напряжения может происходить искажение функции синусоиды тока. Проведем опыт с наличием гармоник на шинах ВН с величинами 150 А, 75 А, 30 А для 2-й, 4-й и 6-й гармоники соответственно и однофазным КЗ в конце линии W4. Периодический характер изменения и малая величина модуля коэффициента (см. рис. 8-9) свидетельствует об отсутствии требований для срабатывания ПО, вследствие чего алгоритм синхронизации времени не запускается.

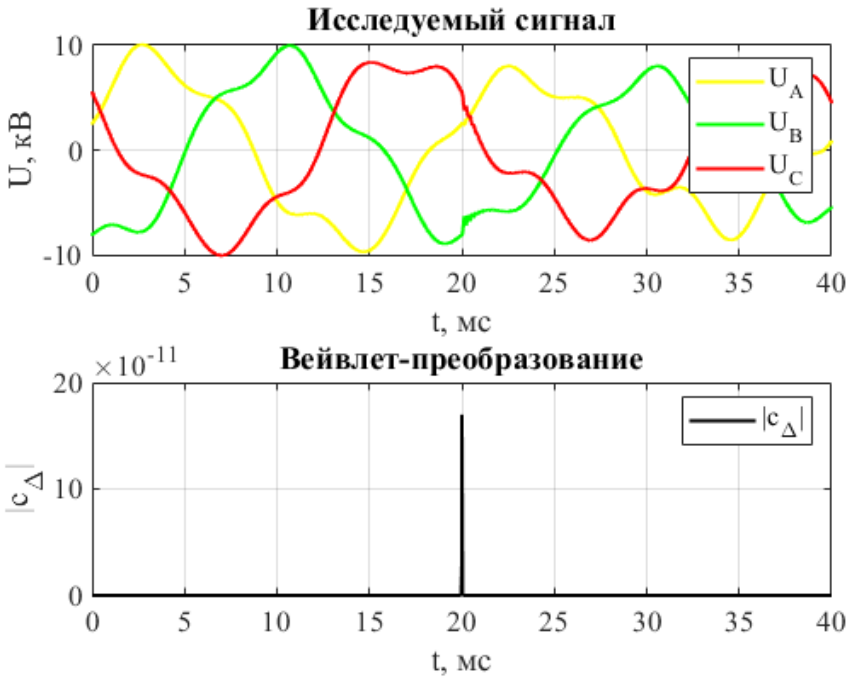


Рис. 8. Осциллограммы напряжения на шинах НН при несинусоидальном режиме.

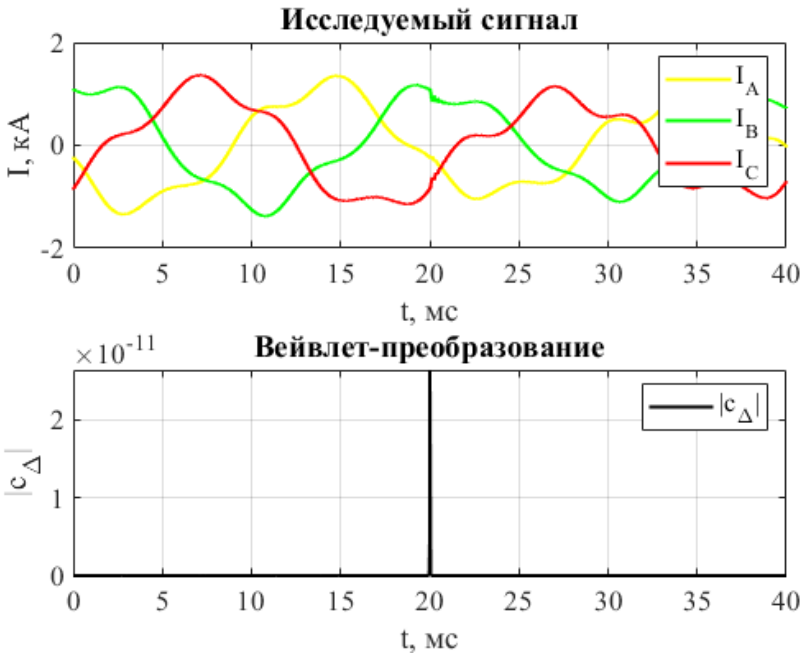


Рис. 9. Осциллограммы тока через АТ1 НН при несуидальном режиме.

ЗАКЛЮЧЕНИЕ

Был предложен способ обеспечения бесперебойного электроснабжения потребителей с повышением защиты потребителей от кибератак и сохранением высокого качества их защиты от повреждений в сети электроснабжения. В основе способа лежит алгоритм фиксации аварийных возмущений в синусоидах тока и напряжения. Работа алгоритма заключается в вейвлет-преобразовании синусоид тока и напряжения, результатом такого преобразования являются модули комплексных коэффициентов базисного вейвлета. Величина модулей комплексных коэффициентов отражает наличие возмущений в сигналах напряжения и тока.

Продемонстрированные опыты показывают, что в момент появления аварийных ситуаций, коротких замыканий, на временной диаграмме модулей комплексных коэффициентов появляется всплеск. В отсутствии коротких замыканий, модули комплексных коэффициентов сохраняют маленькие величины.

В соответствии с этим, если в цифровых сетях злоумышленниками будет сгенерирован сигнал на отключение от релейной защиты, он будет заблокирован пусковым органом защиты от кибератак.

ЛИТЕРАТУРА

[1] The 2016 ICS-CERT Year in Review is a compilation of ICS-CERT programmatic activities for the past year. URL: https://www.us-cert.gov/sites/default/files/Annual_Reports/ Year_in_Review_FY2016_Final_S508C.pdf (дата обращения 05.07.20)

[2] Актуальные киберугрозы: I квартал 2020 года. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/#id10 (дата обращения 05.07.20)

[3] Заявка на патент РФ № 2011154185. 2011.12.29. Устройство контроля и управления сингалами релейной защиты и противоаварийной автоматики.// Романов С. Е., Борисов А. М.

[4] Заявка на патент РФ № 4135497. 1986.10.21. Устройство для проверки аппаратуры релейной защиты и автоматики // Жуков С. Ф., Дьяченко М. Д.

[5] Заявка на патент РФ № 2016113201, 2016.04.06. Централизованное устройство релейной защиты и управления подстанции с распределительным устройством высшего напряжения, выполенным по схеме мостик с выключателями в цепях линий и ремонтной перемычкой со стороны линий.// Иванов С. В., Широкин М. Ю., Гайдаш А. А.

[6] Заявка на патент РФ № 2015146341/07, 2015.10.27. Система терминалов релейной защиты. // Тихомиров А. А.

[7] Заявка на патент США № US2005146224A1. Method and system for detecting stand-alone operation of a distributed generating system // Huang S. J., Lin J. M. и др.

[8] Заявка на патент Германия № DE 102011079652 A1. Verfahren zum Sperren eines Schalters.// Goetz J., Kiendl T., Nerl C.

[9] Малла С. Вэйвлеты в обработке сигналов. М.: Мир, 2005.

[10] Е. Б. Постников. Вейвлет-преобразование с вейвлетом Морле: методы расчета, основанные на решении диффузных дифференциальных уравнений.// Компьютерные исследования и моделирование. 2009 Т.1 №1 С.5-12

[11] Н. М. Астафьева, Вейвлет-преобразование: основы теории и примеры применения. // Успехи физических наук. Ноябрь 1996 г. Том 166, №11.

[12] Grossmann A, Morlet J SIAM J. Math. Anal. 15 723 (1984)

3.3. ПРАКТИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЦИФРОВОЙ ПОДСТАНЦИИ

Е. А. ПЛЕТНЕВА
АО «РАСУ»
Российская Федерация

Контактное лицо:

Е. А. ПЛЕТНЕВА

EAPletneva@rasu.ru

Ключевые слова:

АСУ ТП, цифровая подстанция, безопасная разработка, информационная безопасность, средства разработки, статический анализ, динамический анализ, тестирование на проникновение, функциональное тестирование ФБО, защищенная инфраструктура разработки, РБПО.

ВЕДЕНИЕ

Значительные изменения в сфере обеспечения безопасности информации в законодательстве РФ, произошедшие в последнее время, затронули как предприятия, эксплуатирующие объекты КИИ, так и предприятия-изготовители средств автоматизации и информатизации для таких объектов. Изменения в законодательстве привели к тому, что под понятие «субъектов КИИ» (субъектов критической информационной инфраструктуры) попало намного больше (чем представлялось изначально) предприятий и организаций, относящихся к совершенно разным отраслям, от медицины и науки до оборонно-промышленного комплекса и энергетики. Согласно внесенным в соответствии с приказом ФСТЭК России №35 от 20 февраля 2020 года [1] в требования изменениям, начиная с 2023 года, всё прикладное программное обеспечение, реализующее выполнение функций объектов КИИ, должно быть разработано в соответствии с требованиями к разработке безопасного ПО. А поскольку для АО «РАСУ» конечными потребителями всегда являлись критически важные объекты, и в организации ведется работа по созданию новых продуктов компании, в том числе для цифровой подстанции, руководством организации было принято однозначное решение двигаться в сторону повышения уровня защищенности не только вновь разрабатываемых, но и уже успешно выпускаемых продуктов ИТ в части встраивания в них средств защиты информации и обеспечения процесса разработки безопасного ПО.

ОСНОВНАЯ ЧАСТЬ

На текущий момент в АО «РАСУ» определен следующий подход к разработке защищенных программных и программно-аппаратных средств с встроенными средствами защиты информации: в первую очередь разрабатывается план работ, исходя из поставленной задачи и текущего состояния продукта, это может быть, как разработка с «нуля», так и модернизация и/или развитие текущих продуктов ИТ в организации. В случае модернизации ранее разработанных продуктов ИТ добавляется ряд мероприятий, связанных с предпроектным обследованием:

– проведение анализа текущей проектной, программной и эксплуатационной документации на продукт;

–проведение анализа текущей архитектуры программного продукта и определение схем критических информационных потоков;

–проведение идентификации и инвентаризации информационных и защищаемых активов ПО, субъектов и объектов доступа, допустимых типов операций над объектами доступа;

–определение предварительных границ объекта оценки для проведения оценки соответствия в системе сертификации ФСТЭК России;

–проведение предварительного функционального тестирования базовых функций ПО.

Следующий этап - это проведение анализа требований БИ. Проводится анализ действующих НПА ФСТЭК России, НМД, а также отраслевых локальных нормативных актов Заказчиков (Госкорпорация «Росатом», ПАО «Россети», Минэнерго, ПАО «ФСК ЕЭС» и др.) для определения требований БИ к продукту. После проведения анализа разрабатывается проект задания по безопасности.

Далее необходимо уточнить в случае модернизации продукта ИТ или спроектировать в случае разработки нового продукта ИТ его архитектуру с учетом требований БИ. Можно выделить следующие основные мероприятия:

–разработку модели угроз применительно к продукту с учетом сред его функционирования и условий эксплуатации на объектах информатизации;

–доработку/разработку и документальное оформление проекта верхнего уровня;

–детальное проектирование архитектуры с учетом требований БИ;

– доработку проекта задания по безопасности;
– формирование ТЗ на разработку (модернизация/ развитие) продукта ИТ.

Далее осуществляется переход на этап разработки/доработки продукта ИТ. Этот этап подробно не рассматривается в рамках настоящего доклада в связи с тем, что в зависимости от принятых в команде разработки процессов, перечень мероприятий по разработке и их цикличность будут меняться. Для каждого продукта разрабатывается свой детальный план-график, в котором уже прорабатывается и приоритизируется перечень функций для реализации. Команда ИБ в данном случае формирует план своей работы, исходя из исходных условий, представленных командой разработки.

Особое внимание хотелось бы уделить квалификационному тестированию, ввиду того, что именно данные процессы оказывают максимальное влияние на уровень защищенности конечного продукта.

Статический анализ. С начала 2020 года в организации выстраивается процесс статического анализа: запущен регулярный статический анализ одного из разрабатываемых продуктов. Изначально был выбран подход по максимально раннему включению статического анализа в процесс разработки. Однако, с учетом необходимости проведения требующих определенного времени конкурсных закупочных процедур, было принято решение начать работы, используя OpenSource продукты и «пробные» версии коммерческих средств. Данный подход вывел нас на реализацию внутреннего подпроекта по выбору инструментальных средств анализа, причем касающихся не только статического, но и динамического тестирования, а также тестирования на проникновение. На данный момент в статическом анализе реализуется переход от внешнего контроля к двойному циклу проверки. Первый цикл – встраивание в CI/CD анализаторов кода и блокирование «заливки» изменений в общий репозиторий до устранения срабатываний анализатора. Второй цикл – работа экспертов на стендах с копией репозитория. Сам процесс статического анализа начинается с разработки плана анализа и подготовки инфраструктуры для проведения работ. Следующим шагом является выбор, установка и настройка инструментальных средств анализа; реконфигурация настроек инструментальных средств и/или разработка собственных утилит при необходимости. Затем отбирается образец исходных текстов для анализа и проводится анализ с помощью инструментальных средств (статических анализаторов). Отбор образцов в настоящий момент осуществляется автоматическим образом, используя подготовленные экспертами скрипты, но процесс анализа пока осуществляется на исследовательском стенде экспертов ИБ. Со временем, когда статический анализ будет встроен в CI/CD и IDE, дублирования репозиториев, их синхронизации и отслеживания в ручном режиме идентичности текущей ревизии исходных текстов с анализируемой, не потребуется. После завершения инструментального анализа экспертом по статическому анализу проводится экспертиза результатов работы инструментальных средств, определяются фрагменты/участки кода, не покрываемые статическими анализаторами, и проводится ручной анализ таких фрагментов/участков кода. При выявлении недостатков, обнаруженных в результате проведения статического анализа, формируются сообщения об ошибке и реестр недостатков (включаются в отчет о статическом анализе исследуемых продуктов), разрабатываются рекомендации по их устранению.

Динамический анализ. Для того, чтобы выстроить процесс динамического анализа с нашей точки зрения требуется разделить его на базовые составляющие и постепенно внедрять отдельные компоненты. За базис было выбрано фаззинг-тестирование, поскольку данный вид тестирования входит в обязательный минимум по всем действующим методикам выявления уязвимостей. При выборе инструментальных средств анализа мы столкнулись с тем, что готовых решений для организации фаззинг-тестирования разрабатываемых нашей организацией программных продуктов нет – все доступные OpenSource-средства решают отдельные частные задачи, а, например, для качественного фаззинг-тестирования промышленных протоколов или, тем более, протоколов собственной разработки имеющиеся средства не подходят. Нами были рассмотрены: AFL, libFuzzer, KLIO и ряд других. Мы

понимаем, что само фаззинг-тестирование не подразумевает наличие «коробочных решений». К фаззинг-тестированию предъявляются требования по генерации входных последовательностей и их дальнейшей интеллектуальной мутации. То есть, для начала мы должны описать структуру данных, которые обрабатывает тот или иной входной интерфейс, задать логику для генерации входных данных, определить принципы мутации и в целом алгоритм работы с каждым интерфейсом программы, в том числе и с внутренними. Очень важно провести фаззинг-тестирование всех компонентов разрабатываемого продукта, а не только входных интерфейсов ФБО. Конечно, приоритет и первоочередность должна отдаваться именно интерфейсам ФБО, но ограничиваться только этим нельзя. Самые опасные уязвимости выявляются при фаззинг-тестировании не только ФБО. Например, утечки памяти, состояние «гонки и паники» выявляются вне зависимости от качества реализации ВСЗИ в продукте, если смотреть на это в отдельности от всего функционала системы. После проведения первичных исследований нами был выбран подход по разработке «собственного» фаззера, базирующегося на OpenSource решении. Основная причина этого – отсутствие альтернативных вариантов, хотя мы продолжаем проведение изыскательных работ и, в случае выявления подходящего инструментального средства, автоматизирующего процесс фаззинг-тестирования, обязательно будем его апробировать и, по возможности, включать его в процесс квалификационного тестирования. Для фаззинг-тестирования нами также, как и для статического анализа выбран подход по его внедрению на самых ранних этапах разработки продукта. Начиная с 16 недели 2020 года запущен процесс еженедельного фаззинг-тестирования с постоянным видоизменением/развитием процесса (разрабатывается/развивается фаззер, увеличивается покрытие фаззинг-тестирования, добавляются методы тестирования). Помимо этого, для динамического анализа мы используем методы инструментации исходного текста, применяются разные типы санитайзеров, что позволяет выявлять достаточное количество специфических дефектов, которые невозможно выявить, используя только принципы фаззинг-тестирования. Инструментация позволяет выявить:

– выход за пределы массива;
– утечки памяти;
– гонки по данным;
– чтение неинициализированной памяти;
– использование нулевого указателя;
– переполнения;
– использование указателя после освобождения;
– попытки использовать переменную вне scope;
– попытки дважды освободить память;
– попытки прочитать структуры, не учитывая выравнивания полей в памяти;
– переполнение знаковых, конвертация, которая может привести к переполнению значений.

Под санитайзером понимается инструментирующий алгоритм для детектирования ситуаций некорректного поведения ПО. Наиболее наглядными примерами используемых в организации санитайзеров являются Valgrind (применяется принцип инструментации во время выполнения), Clang Sanitizers (применяется принцип инструментации во время компиляции).

На данный момент процесс динамического анализа и фаззинг-тестирования выглядит следующим образом: на первом этапе разрабатывается план анализа и тестирования, далее проводятся работы по подготовке исследовательского стенда. В данный вид работ входят: подготовка инфраструктуры анализа и тестирования; выбор, установка и настройка инструментальных средств анализа и тестирования; реконфигурация настроек инструментальных средств и/или разработка собственных утилит. После завершения подготовительных процедур осуществляется отбор образца для анализа и тестирования. Методы отбора отличаются для стадии первичных или приемочных испытаний и стадии

регулярного цикла анализа. После отбора образца проводится инструментация исходного кода с помощью инструментального ПО и/или санитайзеров, а также осуществляется разработка тестовых кейсов. Далее производится анализ и фаззинг-тестирование, после завершения которых экспертом по динамическому и фаззинг-тестированию осуществляется экспертиза полученных результатов. При выявлении недостатков, обнаруженных в результате проведения динамического анализа и фаззинг-тестирования, формируются сообщения об ошибке и реестр недостатков (включаются в отчет о фаззинг-тестировании исследуемых продуктов), разрабатываются рекомендации по их устранению.

Функциональное тестирование ФБО. По мере разработки ФБО проводится в штатном режиме QA-тестирование, на всех этапах выпуска релиза разрабатывается ПМИ и проводится контрольное тестирование. Базируется ПМИ на функциональных требованиях безопасности, описанных в задании по безопасности, которое, в свою очередь, базируется на нормативных правовых актах ФСТЭК России и национальных стандартах по защите информации. На данный момент используется преимущественно ручное тестирование, поскольку исследуемые продукты находятся в стадии разработки, и нет нужной степени документирования, а автоматизация в части проверки функций ФБО не всегда возможна. Задача экспертов ИБ проводить тестирование «от обратного». Специалисты должны выявить не только соответствие заявленному сценарию работы функционала ИБ, но и пути обхода реализованных функциональных возможностей безопасности, чтобы до выхода продуктивного релиза устранить возможные скрытые каналы.

Тестирование на проникновение. Данный вид квалификационного тестирования в нашей организации находится на начальной стадии проработки, в настоящее время апробируются различные инструментальные средства тестирования, осуществляется поиск новых. К тому же, на данный момент окончательно не завершена разработка исследуемых продуктов, чтобы провести тестирование в полной мере в среде, максимально соответствующей их предполагаемым условиям эксплуатации. Разрабатывается концептуальное описание процесса тестирования на проникновение и апробируются подходы и методы, используя опыт мирового сообщества (международные базы знаний, шаблоны атак CAPEC и т.д.).

По итогам работы по подбору инструментальных средств статического и динамического анализов хотелось бы также поделиться проблематикой, с которой пришлось столкнуться:

–ограничения на возможность использования анализаторов зарубежных изготовителей (ограничения госдепа США);

–ограниченный список поддерживаемых анализаторами языков программирования (если C/C++ максимально распространены с точки зрения анализаторов, что не является однозначно позитивным фактором, то языки типа Golang представлены исключительно в OpenSource решениях, а попытки апробации коммерческих решений для указанного языка привели к негативному впечатлению);

–высокий объем ручного анализа и результатов отработки анализаторов, а также исходных текстов в целом.

В части динамического анализа:

–отсутствие «готовых решений» для разрабатываемых продуктов в сфере промышленной автоматизации (специфические протоколы, протоколы собственной разработки и т. д.) и, как следствие, необходимость разрабатывать/развивать собственный инструментарий анализа;

–необходимость организации непрерывно функционирующих «фаззинг-ферм» (доп. финансовые затраты с высоким уровнем первоначальных вложений).

Вышеуказанная проблематика оказывает свое влияние на становление процессов разработки безопасного программного обеспечения (далее – РБПО), но уже в настоящий момент компании удалось организовать регулярный цикл проведения статического и динамического анализов, а также функционального тестирования. Функциональное

тестирование и тестирование на проникновение носят менее регулярный характер. Это связано с тем, что проведение функционального тестирования зависит от объема реализации функций безопасности, а тестирование на проникновение – от готовности релиза. Тестирование на проникновение на текущий момент скорее развивается параллельно с разработкой продуктов ИТ, что свойственно при начальных циклах разработки продуктов. По итогам проведения регулярного статического и динамического анализа в организации выпускаются сводные еженедельные отчеты, в которых представлены подробные сведения о процессе проведения анализа и тестирования, приведены данные об используемых инструментальных средствах, в том числе собственной разработки, о выявляемых дефектах и взаимодействии с разработчиками (все подтвержденные несоответствия фиксируются в системе управления проектами), дается статистика выявления и устранения дефектов, мест их возникновения. Изложенные в отчетах материалы полностью позволяют воспроизвести процесс и могут быть предъявлены аудиторам, включая испытательные лаборатории, для подтверждения внедрения процессов РБПО в части статики и динамики, могут быть полезны другим разработчикам ПО в компании, которые ведут разработку используя языки C/C++/Go. Разрабатываемые отчеты не статичны, поскольку процессы в стадии становления и до конца проекта по внедрению РБПО будут развиваться до требуемого показателя.

ЗАКЛЮЧЕНИЕ

В целом, если говорить о трудностях, с которыми столкнулись эксперты ИБ в ходе реализации работ по внедрению РБПО на текущий момент, необходимо отметить сложность в донесении до команд разработчиков важности и нужности перехода на новый для них процесс, который, к сожалению, требует от них гораздо большего погружения в сферу обеспечения безопасности информации и более критического взгляда на их работу. Это не всегда проходит гладко. Команда ИБ каждый раз должна подбирать сильную аргументацию и со своей стороны максимально погружаться и в продукт, и в специфику используемых языков программирования. Таким образом, эксперты ИБ не могут стоять в стороне и быть исключительно надзирающим органом, а должны становиться частью команды разработки. И это является основой для реализации процессов: разработка и безопасность не противопоставляются друг другу, а дополняют и взаимоусиливаются. Основной акцент – повышение качества разрабатываемых продуктов.

Промежуточным итогом реализации проекта по внедрению методологии РБПО может служить ряд констатаций фактов:

–РБПО – это дорого (финансовые затраты на инструментарий, оборудование, трудовые ресурсы). Оптимизировать затраты возможно, но в этом случае нужно особое внимание уделить выстраиваю процессов;

–РБПО – это эффективно. Уже на начальном этапе внедрения можно сделать вывод не просто об увеличении уровня защищенности продукта, но и в целом о повышении качества изделий (все это видно по итогу проведения тестирования и фиксации в аналитических отчетах, особенно применительно к «готовым» продуктам);

–РБПО – работа на перспективу. Полноценно внедряя процессы и процедуры РБПО, мы снижаем риск возникновения критичных уязвимостей в уже готовом, прошедшем сертификацию СЗИ ФСТЭК России изделии, а тем самым снижаем финансовую нагрузку от возможных рекламаций.

АО «РАСУ», выбрав путь полного внедрения процессов и процедур РБПО, сможет оценить эффективность данного выбора по итогам оценки соответствия разрабатываемых (частично развиваемых) в настоящий момент продуктов ИТ. Сейчас можно констатировать, что это сложная, но решаемая задача. В настоящий момент компания решает возникающие проблемы и вопросы самостоятельно. Но существует понимание, что серьезные дополнительные эффекты возможны и при объединении усилий с другими организациями, занимающимися разработкой безопасного ПО, для совместного решения проблемных вопросов, а также передачи опыта.

Также следует отметить, что для проведения квалификационного тестирования ИБ требуется высокий уровень компетенций персонала. Да, мы имеем жесткий дефицит «готовых» специалистов на рынке труда и их высокую стоимость. В том числе поэтому АО «РАСУ» взят курс на формирование целевой команды РБПО и «взращивание» квалифицированных кадров в рамках организации, используя в том числе ресурс молодых специалистов. Комплексный подход, а также вектор развития, направленный на собственную компетентную команду, поможет в достижении конечной цели, которой является соответствие всех продуктов ИТ, разрабатываемых АО «РАСУ», требуемому уровню доверия и защищенности согласно действующему российскому и международному законодательству.

ЛИТЕРАТУРА

[13] Приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

3.4. ВОПРОСЫ РЕАЛИЗАЦИИ ДОВЕРЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ

В. Г. КАРАНТАЕВ
АО «Лаборатория Касперского»
Россия

Контактное лицо:

В. Г. КАРАНТАЕВ

vladimir.karantaev@gmail.com

Ключевые слова:

Интеллектуальные электронные устройства, релейная защита и автоматика, безопасная разработка программного обеспечения, встроенные операционные системы реального времени, механизмы защиты, средства защиты информации.

ВВЕДЕНИЕ

Доклад посвящен рассмотрению практических вопросов создания защищенных интеллектуальных электронных устройств. В силу сформированных требований по импортозамещению и требований по защите критической информационной инфраструктуры РФ актуальной задачей является подготовка обзора, посвященного вопросам создания защищенных ИЭУ. В докладе рассмотрены актуальные возможности для построения взаимовыгодных кооперационных цепочек: вендор SOC, разработчик ИЭУ, вендор средств защиты информации.

ОСНОВНАЯ ЧАСТЬ

С определенной долей уверенности можно утверждать после первых экспертных заявлений о необходимости придерживаться подхода «security by design» при создании автоматизированных и автоматических систем управления технологическими процессами накоплен серьезный теоретический и практический опыт.

Регуляторы поддержали экспертов и закрепили в отечественных нормативно-правовых актах порядок, согласно которому приоритетному применению подлежат средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов Критической Информационной Инфраструктуры РФ. Анализ практики применения ФЗ № 187 «О безопасности критической информационной инфраструктуры РФ» показывает, что в подавляющем количестве случаев комплексы релейной защиты и автоматики (РЗА) относятся к значимым объектам критической информационной инфраструктуры.

Содержание приказа ФСТЭК России от 25.12.2017 N 239 (ред. от 20.02.2020) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (Зарегистрировано в Минюсте России 26.03.2018 N 50524) в редакции Приказа ФСТЭК России от 20.02.2020 N 35 было дополнено требованиями п. 29.2-29.4, вступающими в силу 01.01.2023.

Как следует из пункта 29.3, требования по внедрению безопасной разработки программного обеспечения (БРПО) будут распространяться на процессы разработки любого прикладного программного обеспечения, используемого на значимых объектах КИИ, а не только ПО, реализующего функции безопасности.

Внедрение процессов БРПО является практическим отражением принципа Security-by-design (безопасности на архитектурном уровне) при разработке программного обеспечения и программно-аппаратных комплексов, в том числе интеллектуальных электронных устройств релейной защиты и автоматики (ИЭУ РЗА).

Таким образом, требования будут распространяться в том числе на разработку ПО, реализующего алгоритмы релейной защиты, сетевые протоколы МЭК 61850, в случае, если (ИЭУ комплексов РЗА войдут в состав значимых объектов КИИ в чем нет сомнений, а также на ПО, используемое для конфигурирования ИЭУ.

Анализ новой отраслевой методики, выпущенной ПАО «Россети» в августе 2020 года показал, что один из основных заказчиков ИЭУ ожидает увидеть в продуктах, претендующих на выход в рынок должны содержать развитый функционал встроенных средств защиты информации [1].

Автор ранее в своих докладах и статьях обращался к концепции создания цифровых подстанций в киберзащищенном виде, которую невозможно реализовать без ключевых элементов – защищенных ИЭУ [2,3].

В своих выступлениях автор не раз доносил свою точку зрения о том, что реализация концепции Secure by design (встроенных средств защиты информации в промышленных системах автоматизации) и требований безопасной разработки выглядит наиболее перспективно с учетом необходимости удовлетворять требования по функциональной

надежности и безопасности, наличия требований по быстродействию телекоммуникационных протоколов и оптимальности затрат.

При этом реализация указанных положений возможно на основе экосистемных партнерств: разработчиков микропроцессоров и модулей на их основе, разработчиков операционных систем, вендоров средств защиты информации и вендоров ИЭУ.

Многие вендоры придерживаются схожих позиций:

Лаборатория Касперского предложила концепция «иммунных» продуктов, разрабатываемых на базе операционной системы собственной разработки [5].

Несколько отечественных вендоров средств криптографической защиты информации (СКЗИ) (АО «ИнфоТеКС», ООО «ТСС», АО «Актив-софт») успели разработать и предложить рынку встраиваемые средства криптографической защиты, разработаны и доведены до уровня национальных стандартов требования к специализированным протоколам криптографической защиты информации.

Обзор источников [7, 8] показывает, что практические исследования в области реализации криптографически защищенных протоколов MMS, GOOSE, SV и R-GOOSE, R-SV (IEC 61850-90-50) подходят к логическому завершению с положительным результатом. Практическое внедрение этих наработок является вопросом ближайших нескольких лет.

Интересным является то, какое влияние указанные выше изменения оказали на планы разработки отечественных ИЭУ и представить мнение автора о том, с какими трудностями могли столкнуться разработчики при проектировании ИЭУ устройств в защищенном исполнении. Попытаться дать ответ, какие действия могут быть предприняты.

С методологической точки зрения при создании защищенного ИЭУ необходимо начинать с разработки модели угроз и нарушителя, после чего планомерно подбирать механизмы безопасности, которые могут помочь в противодействии выявленным угрозам и сценариям реализации атак.

С большим сожалением необходимо констатировать, что на отраслевом уровне до сих пор не разработана базовая модель угроз для комплексов РЗА и ИЭУ, в частности.

Базовая модель угроз для комплекса РЗА и типа устройств ИЭУ позволит вендорам СЗИ предложить производителям ИЭУ набор готовых архитектурных шаблонов проектирования и законченных механизмов безопасности, использование которых многократно упростит создание защищенных ИЭУ, оптимизирует затраты вендора ИЭУ на создание и время вывода продукта на рынок.

В качестве примера использования вышеописанного методического подхода можно назвать: фреймфорк PSA certified, предложенный ассоциацией, которая была организована компанией ARM, концепцию создания иммунных продуктов Лаборатории Касперского [5, 6].

При этом возможности реализации каждой из концепций опираются на особенности аппаратной (Центрального процессора, СнК) и программной платформы (операционной системы), используемой в конечном изделии, в контексте данного доклада под конечным изделием понимается ИЭУ.

Первая в списке актуальных решаемых задач – выбор аппаратной платформы для ИЭУ.

В РФ в условиях сформированных требований к применению отечественных электронных компонент в изделиях, применение которых планируется в Критической Информационной Инфраструктуре (КИИ), выбор невелик, но он есть.

В горизонте 2021–2023 выбор производителей ИЭУ будет лежать между центральными процессорами (ЦП) архитектуры ARMv8-A и ЦП с VLIW архитектурой.

Важно отметить, что отечественные разработчики ЦП пока не предложили специализированного ЦП для встраиваемых индустриальных систем. В число наиболее часто упоминаемых проблем применения существующих отечественных ЦП называются: уровень энергопотребления и стоимость SOC.

Анализ доступных на рынке РФ отечественных ЦП и СнК, а также доступной информации о практическом опыте применения и докладов научно-технических советов позволяет сделать вывод, что отдельные отечественные производители ИЭУ успешно решают

задачи теплоотведения не только в 20-25 Вт, но и больше, оптимизации используемого программного обеспечения, что позволяет конечному изделию ИЭУ удовлетворять всем отраслевым требованиям, необходимые периферийные устройства могут быть реализованы при разработке референс дизайна SoM.

К 2023–2026 г.г. вероятно появление специализированных российских ЦП, использующих RISC V архитектуру, разработанных специально для встраиваемых индустриальных систем.

Архитектурные решения, принятые при проектировании ИЭУ, выполняемые функции формируют требования к количеству вычислителей, а значит, к количеству центральных процессоров (ЦП), выбору архитектуры ЦП.

У российских производителей ИЭУ и электроэнергетической отрасли в целом есть уникальный шанс повлиять на развитие ЦП в РФ, сформировав платежеспособный спрос и требования к будущему ЦП и системе на кристалле (СнК), одновременно решая задачу формирования требований к планируемым к выпуску SoM (система на модуле) на базе новых ЦП. На данный момент не хватает разработанных референс-дизайнов SoM (систем на модуле) требуемых форм факторов, которые могли бы быть использованы производителями ИЭУ.

Необходимо констатировать, что речь об отечественных фаблес компаниях, но этот факт не должен вводить в заблуждение, так как компаний, обладающих собственным производством ЦП особенно, основанном на выпуске ЦП на основе «тонких технических процессов» в мире насчитываются единицы.

Специалисты в области информационной безопасности также предъявляют дополнительные требования к разработчикам СнК, которые могут прямо влиять на создание защищенных ИЭУ РЗА. Некоторым из требований посвящен доклад [4]. Например, с целью обеспечения целостности и аутентичности ПО, используемого в ИЭУ, в СнК должна быть реализована «chain of trust», то есть совокупность программно-аппаратных компонент, обеспечивающая доверенную загрузку встроенной операционной системы и контроль целостности в процессе эксплуатации. Также реализация «chain of trust» позволяет предотвратить атаки «на цепочку» поставки, ставшие столь популярными в последние годы.

Доверенная загрузка СнК, использующая ЦП ARM архитектуры, может использовать режим «Trust Zone» для предоставления механизмов безопасности с повышенными гарантиями надежности, например, доверенное хранилище, возможность выполнения криптографических операций, контроль целостности исполняемых компонент встроенной операционной системы реального времени (ядра) и наиболее критичных модулей – алгоритмов РЗА, хранимых осциллограмм, РАС и т. д.

Реализация «цепочки доверия» начиная с самых ранних этапов загрузки СнК и предоставление дополнительных механизмов защиты, на основе доверенной среды исполнения обладает преимуществами по сравнению с существующими средствами доверенной загрузки, которые «начинают свою работу» на этапе загрузки UEFI, то практически на финальном этапе запуска СнК.

Разработка «доверенного хранилища» может потребовать от разработчиков СнК, а точнее SoM: защиту от НСД, физический датчик случайных чисел (ФДСЧ), доверенные периферийные устройства.

Для производителей ИЭУ для формирования столь специфичных полноценных требований к аппаратной платформе необходимо обладать разработанной моделью угроз, пониманием перечня требуемых для реализации механизмов безопасности и зависимости реализуемых механизмов от возможностей аппаратной платформы. Оптимальным выглядит партнерство между вендорами: ИЭУ, СЗИ и аппаратной платформы.

Вторая составляющая ИЭУ, роль которой многократно возросла за последний годы и определяет тренд в развитии ИЭУ – это программная составляющая.

В РФ специфика разработки ИЭУ состоит в том, что у различных вендоров ИЭУ сложились соответствующие инженерные подходы, которые достаточно сильно отличаются друг от друга. Встречаются реализации программного обеспечения с использованием

ассемблера, операционных систем реального времени, которые могут поставляться зарубежными производителями СнК или заимствоваться в Open Source, стоит отметить, что применение коммерческих операционных систем также находит применение.

При этом анализ деятельности рабочих групп СИГРЭ и иных международных инициатив показывает, что существует устойчивый тренд к реализации и переходу на «программные платформы», что существенным образом будет влиять на устоявшиеся бизнес модели вендоров ИЭУ и, конечно, соответствующим образом повлияют на стратегию технологического развития.

«Программная платформа» для ИЭУ устройств может базироваться на использовании коммерческой операционной системы реального времени. Важным фактом являются критерии, по которым выбираются подобные ОС производителями встраиваемых систем.

Обратимся к двум источникам [7, 8].

На рис. 1 и рис. 2 приведены критерии выбора ОС, которые предъявляются производителями встраиваемых систем.

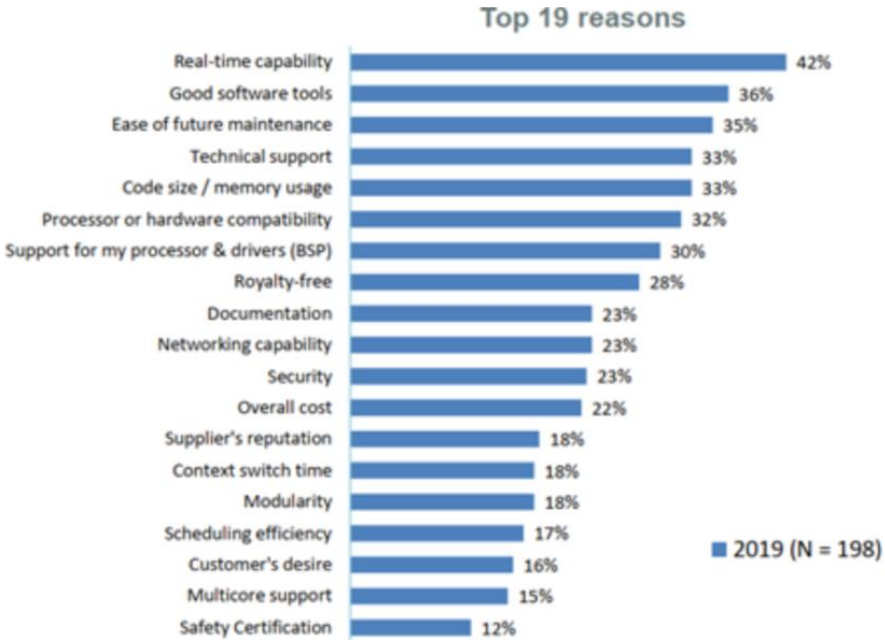


Рис. 1. Причины выбора коммерческих операционных систем согласно Embedded Markets Study 2019 года.

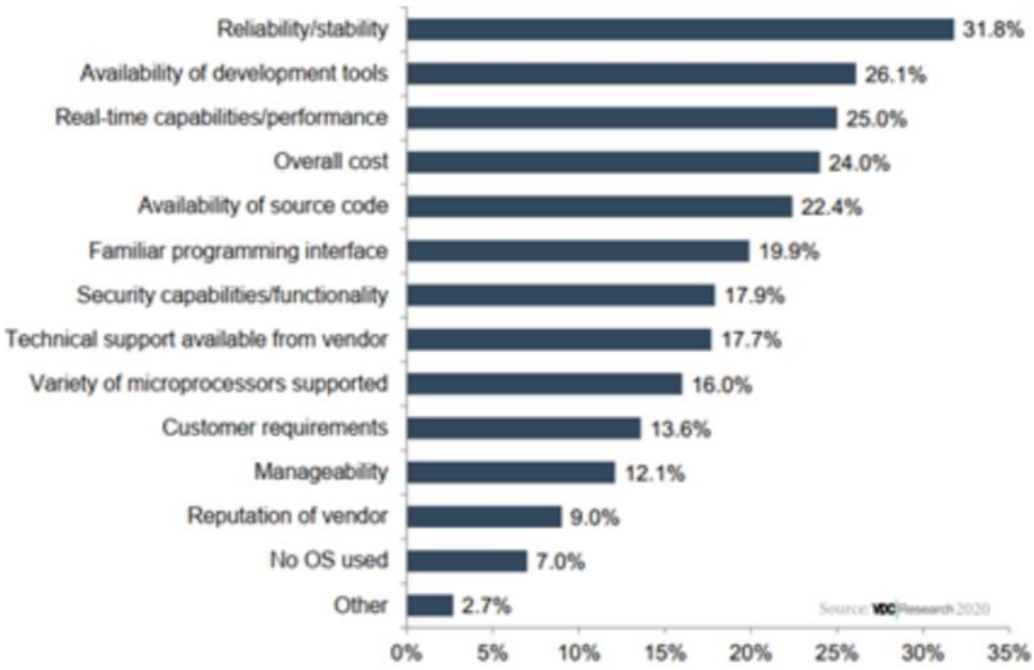


Рис. 2. Причины выбора коммерческих операционных систем согласно исследованию VDC 2020 года.

Согласно проведенным исследованиям, разработчики встраиваемых систем ожидают от поставщиков коммерческих операционных систем качественную с высоким уровнем SLA техническую поддержку с расширенным сроком поддержки от 10 лет.

К ожидаемым требованиям по обеспечению надежности и детерминированному поведению ядра ОС, сетевой подсистемы добавляются требования по наличию и предоставлению качественных средств разработки.

Далеко не все поставщики встраиваемых операционных систем реального времени готовы к таким требованиям, стоит отметить, что на российском рынке отсутствуют отечественные ОС, специально разработанные для встраиваемых систем.

На рис. 3 приведены результаты исследования, посвященного приоритетам механизмов безопасности, реализация и использование которых востребована во встраиваемых системах.

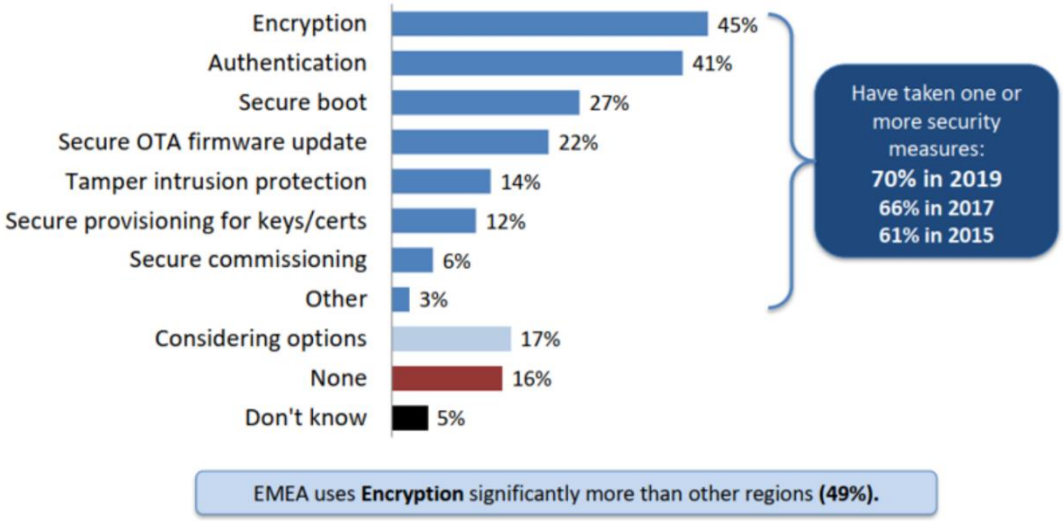


Рис. 3. Механизмы безопасности, реализация которых ожидается во встраиваемых системах согласно Embedded Markets Study 2019 года.

Реализация части из указанных механизмов может зависеть от особенностей используемой СнК. Перспективным представляется сотрудничество производителей СнК и

вендоров СЗИ, которые могут предложить рынку SDK с готовым набором необходимых законченных механизмов безопасности, используя которые вендор ИЭУ может быстро разработать защищенное ИЭУ с митигацией актуальных и будущих угроз безопасности.

ЗАКЛЮЧЕНИЕ

По результатам приведенного обзора можно утверждать, что есть все предпосылки к реализации на практике концепции «secure by design» при разработке ИЭУ.

:

- Сформированы нормативно-правовые акты, создающие основу требований для использования концепции «secure by design».
- Активно развиваются международные стандарты и сформирован план разработки отечественных нормативно-технических документов, которые являются методической базой для реализации концепции «secure by design».
- Формирование кооперационных цепочек вендоров ИЭУ, СнК и СЗИ взаимовыгодно и позволит разработать защищенные ИЭУ, сократить затраты на их разработку, а также время вывода на рынок. Создаст хороший потенциал экспортопригодных технологий.

ЛИТЕРАТУРА

[14] Методика проверки (аттестации) цифрового оборудования и систем на соответствие требованиям по безопасности информации (приказ ПАО «Россети» от 28.08.2020 №391). [Электронный ресурс]. URL: https://www.rosseti.ru/investment/science/attestation/ (дата обращения: 08.08.2021)

[15] Карантаев В. Г. Частные вопросы реализации киберзащищенной цифровой подстанции / В. Г. Карантаев, В. И. Карпенко // Релейщик. – 2019. – № 2(34). – С. 48-52.

[16] Vladimir Karantaev, Vladislav Karpenko Aspects of the concept of cyber-protected objects of a digital electrical network with elements of Zero Trust Architecture in Russia / E3S Web Conf.Volume 288, 2021 International Symposium “Sustainable Energy and Power Engineering 2021” (SUSE-2021), https://doi.org/10.1051/e3sconf/202128801032 Published online: 14 July 2021.

[17] А. Самоделов, Повышение защищенности доверенного хранилища GPD Trusted Storage на основе технологии ARM TrustZone и особенностей архитектуры СнК с ядрами ARM v.8 Андрей Самоделов, материалы конференции «РусКрипто 2021». [Электронный ресурс]. URL: https://www.ruscrypto.ru/resource/archive/rc2021/files/12_samodelov.pdf (дата обращения: 08.08.2021)

[18] M. Udin Cyber Immunity — a new era in cybersecurity. [Электронный ресурс]. URL: https://youtu.be/UOFb8tXzX4U (дата обращения: 08.08.2021)

[19] What Is the PSA Certified IoT Security Framework? [Электронный ресурс]. https://www.psacertified.org/what-is-psa-certified/ (дата обращения: 08.08.2021)

[20] Implementing Secure Routable GOOSE and SV Messages Based on IEC 61850-90-5 [Электронный ресурс] https://ieeexplore.ieee.org/document/8979307 (дата обращения: 08.08.2021)

[21] Hussain, S. M. S. A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges / S. M. S. Hussain, T. S. Ustun, A. Kalam // IEEE Transactions on Industrial Informatics. – 2020. – Vol. 16. – No 9. – P. 5643-5654. – DOI 10.1109/TII.2019.2956734.

3.5. МОНИТОРИНГ ЦИФРОВЫХ ЭНЕРГООБЪЕКТОВ

А.А. БОНДЮГИН
АО «Лаборатория Касперского»
Россия

Контактное лицо:

А.А. БОНДЮГИН

Andrey.Bondyugin@kaspersky.com

Ключевые слова: SV/Goose, PAC, IED

ВВЕДЕНИЕ

Реализация ведомственных проектов по цифровизации электроэнергетического комплекса и применение современных технологий при строительстве и эксплуатации подстанций и иных типов энергообъектов повышает актуальность задач всестороннего мониторинга правильности работы первичного и вторичного оборудования энергообъекта. На сегодняшний день не существует решений, которые бы в полной мере закрывали все потребности владельцев и эксплуатирующих организаций в части решения данных задач.

Доклад посвящен подходам Лаборатории Касперского к реализации универсального мониторинга цифровых энергообъектов, включая мониторинг технологических параметров работы электротехнического оборудования (электрический режим), мониторинг корректности функционирования сетевой инфраструктуры (сетевой режим) и мониторинг состояния киберзащищенности.

ОСНОВНАЯ ЧАСТЬ

Проблема контроля правильности работы оборудования энергообъектов (подстанций) существовала и до появления стратегии цифровизации электроэнергетики и стандартов серии МЭК-61850. За решение этих задач отвечала система регистрации аварийных ситуаций (РАС), которая осуществляла расчет электрических параметров работы электроустановок и оценку правильности работы устройств релейной защиты и противоаварийной автоматики (РЗА и ПА) на основании данных, получаемых через собственные каналы аналогового и дискретного ввода.

В рамках эксплуатации цифровых подстанций необходимость осуществления контроля электрического режима работы энергообъекта сохранилась, но теперь работа регистратора аварийных ситуаций основывается на данных, передаваемых в цифровом виде с использованием протокола Ethernet. В состав функций мониторинга электрического режима входят:

- прием пакетов по протоколам SV/Goose;
- расчет параметров работы электротехнического оборудования;
- выявление аварийных ситуаций и запуск регистратора по заданным уставкам;
- осциллографирование и запись осциллограмм;
- ведение журнала событий;
- уведомление пользователя/оператора о выявленных аномалиях.

Применение цифровых технологий и стандартов серии МЭК-61850 при проектировании и эксплуатации энергообъектов привело к необходимости, помимо контроля электрического режима, осуществлять контроль правильности параметров работы сетевой инфраструктуры, так как она является важнейшим элементом вторичных систем цифровых подстанций (или иных объектов) и обеспечивает непрерывное и стабильное компонентов данных систем. В рамках мониторинга сетевого режима может осуществляться:

- контроль параметров сетевого трафика (скорость, загрузка канала);
- регистрация ошибок и искажений в пакетах SV/GOOSE;
- изменение режима работы IED;
- запись трафика в формате .pcap;
- мониторинг временных меток в пакетах Ethernet;
- визуализация коммуникаций;
- ведение журнала событий;

- расчет статистики по каждому компоненту АСУ ТП и по сети в целом (трафик, интервалы отправки сообщений, количество TCP-retransmits).

Цифровизация неизбежно несет за собой новые киберриски, и в проблему обеспечения информационной безопасности АСУ ТП цифровых энергообъектов сейчас вовлечены все участники рынка систем автоматизации и средств защиты информации. Многие вендоры АСУ ТП в настоящее время реализуют встроенные средства защиты информации в составе своих программно-технических комплексов и готовят комплексные предложения по автоматизации, учитывая требования по информационной безопасности на этапе проектирования систем. При этом вендоры средств информационной безопасности со своей стороны предлагают специализированные решения, позволяющие обеспечить защиту объектов электроэнергетики от современных киберугроз.

В контексте темы доклада особый интерес представляют средства мониторинга промышленных сетей, которые позволяют обеспечить наблюдаемость и контроль состояния защищенности инфраструктуры энергообъектов в режиме реального времени. Необходимость их применения обусловлена как соображениями обеспечения практической защищенности объектов электроэнергетики, так и реализацией отдельных требований законодательства РФ по защите значимых объектов критической информационной инфраструктуры.

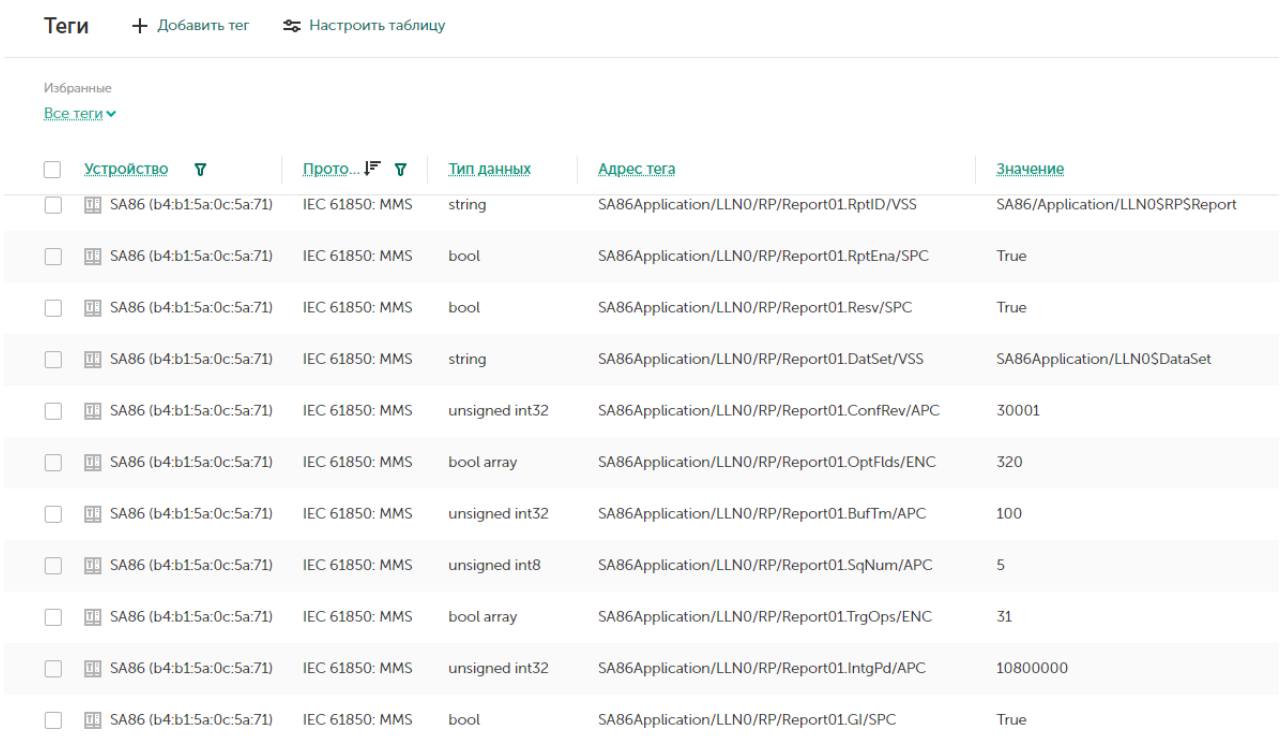
К числу необходимых функций системы мониторинга состояния защищенности относятся:

- инвентаризация активов и обнаружение уязвимостей промышленного оборудования;
- контроль целостности сети;
- обнаружение вторжений;
- контроль параметров технологического процесса в реальном времени;
- управление инцидентами.

Таким образом, при проектировании цифровых подстанций (или иных типов объектов) необходимо предусматривать решения, осуществляющие «технологический» мониторинг (электрический и сетевой режимы), а также программно-аппаратные комплексы, обеспечивающие мониторинг информационной безопасности, что создает дополнительную финансовую и кадровую нагрузку на владельца объекта.

Но при тщательном рассмотрении характеристик данных решений можно заметить, что функционал средств мониторинга информационной безопасности, в дополнение к различным технологиям обнаружения компьютерных атак, реализует сценарии мониторинга «технологического», в силу того, что в данных продуктах обеспечиваются поддержка промышленных протоколов, визуализация сетевых взаимодействий, контроль правильности коммуникаций и другие функции, интересные специалистам по автоматизации и технологическим процессам в энергетике. Таким образом, обеспечивается возможность реализации универсального мониторинга.

Детальное рассмотрение возможностей реализации универсального мониторинга предлагается рассмотреть на примере протоколов семейства МЭК-61850 и решения Kaspersky Industrial Cybersecurity (KICS) for Networks, являющегося средством анализа и мониторинга состояния защищенности промышленных сетей. В части функционала инспекции промышленных протоколов данное решение имеет возможность отслеживания системных команд для всех протоколов, описанных в стандартах серии МЭК-61850 (MMS, GOOSE, SV), а также позволяет отслеживать параметры технологического процесса (теги), содержащие данные телесигнализации и телеизмерений, в режиме реального времени в соответствии с моделью данных МЭК-61850 для протоколов MMS и GOOSE (пример интерфейса KICS for Networks с отображением действительных значений тегов протокола MMS приведен на рис. 1).



Теги + Добавить тег Настроить таблицу

Избранные
Все теги

Устройство	Прото...	Тип данных	Адрес тега	Значение
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	string	SA86Application/LLN0/RP/Report01.RptID/VSS	SA86/Application/LLN0RPReport
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	bool	SA86Application/LLN0/RP/Report01.RptEna/SPC	True
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	bool	SA86Application/LLN0/RP/Report01.Resv/SPC	True
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	string	SA86Application/LLN0/RP/Report01.DatSet/VSS	SA86Application/LLN0$DataSet
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	unsigned int32	SA86Application/LLN0/RP/Report01.ConfRev/APC	30001
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	bool array	SA86Application/LLN0/RP/Report01.OptFlds/ENC	320
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	unsigned int32	SA86Application/LLN0/RP/Report01.BufTm/APC	100
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	unsigned int8	SA86Application/LLN0/RP/Report01.SqNum/APC	5
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	bool array	SA86Application/LLN0/RP/Report01.TrgOps/ENC	31
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	unsigned int32	SA86Application/LLN0/RP/Report01.IntgPd/APC	10800000
SA86 (b4:b1:5a:0c:5a:71)	IEC 61850: MMS	bool	SA86Application/LLN0/RP/Report01.GI/SPC	True

Рис. 10. Пример отображения значений тегов MMS в режиме реального времени.

Для протокола MMS вышеописанные механизмы позволяют, во-первых, отслеживать неразрешенные команды (в общем списке поддерживаемых команд – более 100 наименований), а также ошибки и аномалии формирования пакетов (например, buffer not valid, exception caught, wrong packet format). Во-вторых, появляется возможность отслеживания параметров электрического режима за счет наличия правил контроля тегов, позволяющих задать произвольные уставки и условия формирования события о нештатной (аварийной ситуации), в том числе с использованием скриптов на языке Lua. Для всех регистрируемых событий обеспечивается сохранение «сырого» трафика в формате *.pcap*, что с одной стороны обеспечивает необходимой информацией специалистов по расследованию компьютерных инцидентов, а с другой формирует необходимую базу для анализа возникшей аварийной ситуации.

Похожий функционал доступен и для протокола GOOSE. Здесь, по аналогии с MMS, имеется возможность отслеживания системных команд (например, изменение состояния выключателя, изменение статуса защиты) и контроля правильности коммуникаций, включая сбои счетчиков stNum/sqNum, сбои синхронизации, несоответствие ConfRev, изменение значений сигналов и флагов качества. Также актуальна возможность контроля тегов с использованием правил с произвольными условиями, позволяющая выявлять аномалии и аварийные ситуации. Мониторинг GOOSE коммуникаций может быть усилен интеграцией с сетевым оборудованием. Специализированные коммутаторы имеют функцию GOOSE Check, которая позволяет коммутатору определять проходящие через него GOOSE сообщения, а затем отслеживать их передачу и статус (например, выявлять задержки или поддельные сообщения, а также определять смену маршрута существующих пакетов или появление новых). Данный функционал позволяет осуществить точечное распределенное обнаружение аномалий в коммуникациях по МЭК-61850 и обогатить данные, которые пользователь получает через интерфейс системы мониторинга.

Для протокола SV возможности мониторинга включают механизмы контроля правильности коммуникаций, в том числе обнаружение пакетов неправильного формата/размера, нарушение последовательности SV-пакетов, изменение конфигурации SV-потоков.

Важно отметить, что конфигурирование модулей анализа промышленных протоколов не требует ручной настройки, достаточно лишь импортировать конфигурацию IED в формате *.cid*, *.scl*, *.icd*, после чего разбор протоколов будет осуществляться в автоматическом режиме. Более того, будут предложены шаблоны правил контроля параметров технологического процесса (тегов) на основании статистических данных об изменении значений тега за определенный промежуток времени, что отчасти упрощает работу по созданию конфигурации системы мониторинга.

Помимо функций глубокого анализа промышленного трафика, система мониторинга защищенности имеет дополнительный функционал, который будет полезен специалистам по автоматизации и обеспечению непрерывности технологических процессов. К данным функциям относятся инвентаризация сетевой инфраструктуры и контроль целостности сети, а также построение карты сетевых взаимодействий.

Немаловажным фактором является то, что по своей архитектуре средство мониторинга защищенности промышленной сети является полностью пассивным решением, которое работает с копией сетевого трафика, получаемого со всех коммутаторов сети цифрового энергообъекта. Это позволяет достичь полной наблюдаемости как с точки зрения информационной безопасности, так и с точки зрения правильности работы технологического оборудования. При этом обеспечивается безопасность и непрерывность технологического процесса за счёт исключения некорректного влияния на него со стороны системы мониторинга.

ЗАКЛЮЧЕНИЕ

Использование средств мониторинга состояния защищенности сети ЦПС позволяет не только решить задачи, связанные с обнаружением признаков кибератак, но и решить задачи контроля правильности коммуникаций, выявления и регистрации отклонений, аномалий, аварийных ситуаций в работе электротехнического оборудования.

Безусловно, для решений, которые были специально разработаны для обеспечения защищенности от кибератак, еще есть большое количество потенциальных точек роста в части обеспечения наблюдаемости цифрового энергообъекта с технологической стороны. Но применение единого универсального решения для мониторинга позволит владельцу объекта достичь экономии бюджета, обеспечить простоту и удобство внедрения и эксплуатации (все задачи решаются через единую консоль), а также упростит решение возникающих проблем, так как в силу моновендорности решения точка обращения в техническую поддержку будет единой.

3.6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЗА И АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЭЛЕКТРОЭНЕРГЕТИКЕ. ТЕОРИЯ И ПРАКТИЧЕСКИЙ ПОДХОД

Н. А. ДОНИ, В. А. НАУМОВ, Р. В. РАЗУМОВ, И. А. КОШЕЛЬКОВ, Д. В. МИТРОФАНОВ
ООО НПП «ЭКРА»
Россия

Контактное лицо:

И. А. КОШЕЛЬКОВ

ekra@ekra.ru

Ключевые слова:

Релейная защита и автоматика, информационная безопасность, кибербезопасность, автоматизированные системы управления.

ВВЕДЕНИЕ

В электроэнергетике наступил период повсеместного внедрения передачи информации по цифровым каналам связи. Вопрос строительства цифровых подстанций (ЦПС) плавно, но быстро переходит из теоретической в практическую плоскость. Сформировалось понимание, что внедрение новых подходов влечет за собой ряд проблем, с которыми ранее электроэнергетики не сталкивались, или сталкивались в минимальном объеме. Две ключевые из них – потребность в изучении инженерами-энергетиками, в частности инженерами РЗА, сетевых технологий и вопросы информационной безопасности (ИБ) [1, 6, 7].

Нередко всерьез обсуждается востребованность универсального специалиста, обладающего навыками инженера РЗА, инженера АСУ, инженера систем связи и т. д. Потребность в таких специалистах продиктована зачастую невозможностью определения четких границ зон ответственности специалистов смежных служб при повсеместном внедрении цифровых каналов передачи данных на различных уровнях. Например, при использовании одной локально-вычислительной сети (ЛВС) для передачи трафика сервисов MMS и GOOSE, практически невозможно определить, в чью зону ответственности попадает эта ЛВС – сотрудников службы РЗА, или сотрудников службы АСУ.

Аналогичная ситуация наблюдается в сфере ИБ. Информационная безопасность (кибербезопасность) объектов электроэнергетики обеспечивается, прежде всего, применением аппаратных и программных технических средств, ограничивающих несанкционированный доступ к системе, приводящий к нарушению технологического процесса производства, распределения и потребления электроэнергии.

Часто вопрос ИБ рассматривается в отрыве от технологических процессов энергообъектов. По нашему мнению, правильным является подход, при котором любое техническое решение, связанное с повышением уровня ИБ, должно рассматриваться в разрезе его влияния на надежность функционирования всех защищаемых процессов, а значит и на надежность функционирования энергообъектов в целом.

Немаловажным требованием при построении систем ИБ является учет человеческого фактора (действия наладочного и эксплуатационного персонала, подрядчиков, сотрудников диспетчерского центра, имеющих доступ к удаленному управлению энергообъектами и т. д.), который часто становится источником реализации киберугроз [8, 9].

ОСНОВНАЯ ЧАСТЬ

Автоматизированные системы управления для электроэнергетики являются объектами критической информационной инфраструктуры (далее – КИИ) согласно федеральному закону от №187-ФЗ «О безопасности КИИ РФ» вступившего в силу 01.01.2018. К таким объектам предъявляются требования по обеспечению ИБ, которые зависят от категории значимости объекта и условий его эксплуатации. В зависимости от категории значимости, требуемого уровня защищенности и актуальных угроз безопасности информации в подсистеме ИБ объектов критической информационной инфраструктуры (далее – ОКИИ) должны быть реализованы следующие организационные и технические меры:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;

- защита информационной (автоматизированной) системы и ее компонентов;
- планирование мероприятий по обеспечению безопасности;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- реагирование на инциденты ИБ;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Техническое решение по ИБ ОКИИ должно соответствовать набору мер защиты информации в соответствии с приказом ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». В состав проектируемых подсистем информационной безопасности могут входить:

- подсистема защиты от несанкционированного доступа;
- подсистема безопасного межсетевого взаимодействия;
- подсистема анализа защищенности;
- подсистема антивирусной защиты;
- подсистема обнаружения вторжений;
- подсистема резервного копирования;
- подсистема мониторинга событий ИБ.

Входящие в состав подсистем средства ИБ проходят оценку соответствия в форме сертификации, испытаний или приемки в соответствии с Федеральным законом от 27.12.2002 г. № 184-ФЗ «О техническом регулировании».

В качестве организационных мер по обеспечению безопасности ОКИИ применяется:

- организация контроля физического доступа к программно-аппаратным средствам компонента ОКИИ и его линиям связи;
- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств;
- описание в организационно-распорядительных документах действий пользователей и администраторов компонента ОКИИ по реализации организационных мер;
- определение администратора безопасности ОКИИ;
- информирование и обучение персонала;
- отработка действий пользователей и администраторов ОКИИ по реализации мер по обеспечению безопасности ОКИИ и восстановлению информационной инфраструктуры и обрабатываемой информации.

При традиционном подходе к защите информации с использованием только наложенных средств защиты информации, независимо от степени защиты системы, человеческий фактор (ошибки персонала) может являться причиной реализации угроз ИБ. Такие вопросы должны решаться на этапе проектирования автоматизированных систем технологического управления со встроенными средствами защиты информации с учетом требований ИБ и функциональной надежности.

На человеческий фактор стоит смотреть достаточно широко, ведь он проявляется не только на этапе эксплуатации системы РЗА: он заложен и в аппаратной части, и в программном обеспечении, которое используется в системе РЗА, и даже в самих системах защиты информации. Всё это придумано и изготовлено человеком, а значит, фактор ошибки там уже присутствует. Однозначно надо учитывать возможные ошибки и халатность сотрудников организации, непосредственно задействованных в технологическом процессе. Многие ошибки весьма предсказуемы и ожидаемы, поэтому своевременный анализ и корректировка действий работников позволяет избежать больших проблем. Для повышения уровня осведомлённости работников необходимо выстраивать систему постоянной погружённости персонала в вопросы обеспечения безопасности как с помощью

целенаправленного обучения и информирования, так и с применением плановых и внеплановых контрольных мероприятий.

С чем столкнулись мы при проработках систем ИБ в продукции компании ЭКРА и реализации систем ИБ на объектах ключевых заказчиков [2, 3, 5]?

1. Нелогичные требования к оборудованию РЗА и автоматизированным системам управления и учета:

- требования, основанные на предположении, что к устройствам РЗА и автоматизированным системам из сети Internet (подключение по Ethernet) есть прямой доступ;
- требования, основанные на предположении, что есть прямой доступ к устройствам РЗиА и автоматизированным системам людей извне (с улицы);
- проекция всех требований по ИБ только к устройствам РЗА без формирования требований к остальным устройствам и системам энергообъекта;
- переделка требований по ИБ к системам РЗА из готовых требований к устройствам корпоративного сегмента и т. д.

2. Логичные требования к оборудованию РЗА и автоматизированным системам управления и учета [2, 3, 6, 7]:

- идентификация и аутентификация пользователей не только по группам доступа, но и по персоналиям;
- регистрация событий безопасности – ведение полной хронологии изменений, вносимым каждым пользователем, а также просматриваемой информации;
- блокировка учетных записей при переборе паролей доступа;
- разделение полномочий (ролей) по группам пользователей (инженер РЗА, инженер АСУ ТП, оперативный персонал), в соответствии с должностными обязанностями;
- ограничение параллельных сеансов доступа пользователей;
- контроль целостности компонентов программного обеспечения (во время запуска и работы устройств);
- резервное копирование и восстановление программного обеспечения и конфигурации устройств и т. д.

К настоящему времени проделана большая работа по созданию информационной волны и актуальности проблематики вокруг систем ИБ и киберугроз в электроэнергетике. Адаптация требований ИБ к оборудованию РЗА, а не слепое копирование требований из других отраслей – важнейшая задача текущего дня.

Обеспечение защиты на технологических участках генерации энергии и доставки конечным пользователям нуждается в повышенном контроле. Главным объектом защиты в энергетической сфере является не информация, а технологический процесс. Система безопасности в таком случае должна обеспечить целостность технологического процесса и автоматизированных систем управления.

Проектирование системы ИБ в сфере энергетики начинается с прогнозирования и оценки рисков безопасности. Основной метод оценки – моделирование возможных угроз, которое помогает рационально распределять ресурсы при организации системы безопасности и предотвратить реализации киберугроз.

Значимость ИБ в энергетической сфере определяется последствиями реализации информационных киберугроз. Киберугрозы – это не только материальный ущерб или удар по репутации, но, прежде всего, – вред здоровью граждан, подрыв экологии, нарушение инфраструктуры города или региона.

Подходы к построению ЦПС, а также их оборудованию и коммуникационных сетей универсальны. И это, с точки зрения ИБ, при отсутствии должного внимания к ней, ведет к упрощению кибератак и стандартизации взломов (чего нельзя, например, сделать на ПС, построенной на электромеханической базе, или сложно сделать на ПС с традиционными микропроцессорными терминалами, использующими всё многообразие протоколов связи и подходов к индивидуальному проектированию).

Фильтрация на прикладном уровне промышленных протоколов, ограничение запускаемого программного обеспечения и подключаемых съемных носителей, позволяют создать замкнутую среду функционирования АСУ и реализовать несколько эшелонов защиты информации. Это снижает вероятность атак на промышленные системы, обеспечивая оперативное обнаружение инцидентов.

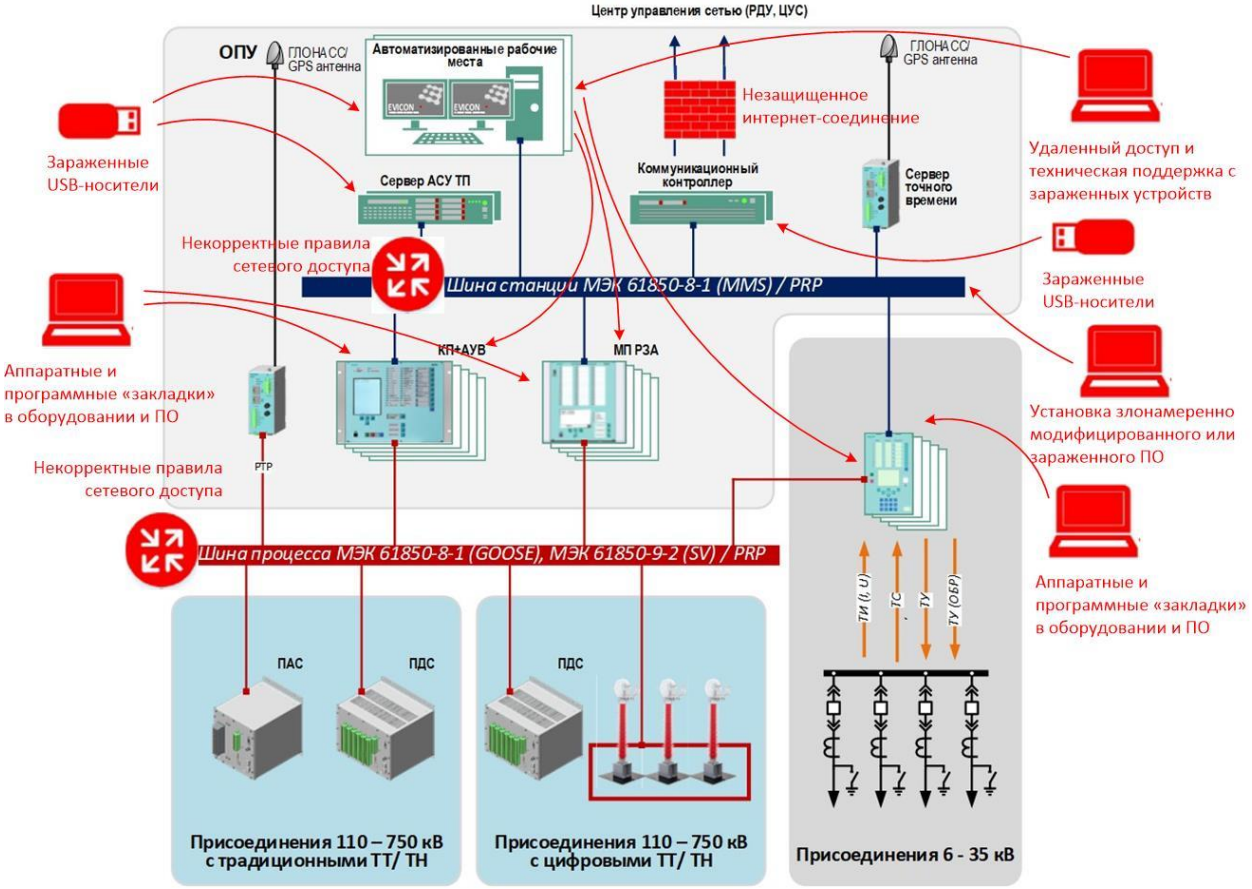


Рис. 1. Основные векторы атак на ЦПС.

На ЦПС можно стандартизировать группы оборудования, которые могут быть подвергнуты кибератакам с последующим нарушением режимов нормального функционирования:

- коммуникационное оборудование (в т. ч. коммутаторы и маршрутизаторы) и цифровые сети энергообъекта;
- микропроцессорные устройства РЗА (РЗ, ПА, сетевая автоматика и т. д.);
- внешние цифровые каналы обмена технологической и оперативной информации (по отношению к нашей ЦПС объектами и диспетчерскими центрами).

При таком многообразии оборудования стоит изначально разделить все возможные кибеугрозы по типам и группам, а также распределить противодействие по ним по типам оборудования и вторичным системам на объекте. Тем самым не перегружать ключевой технологический элемент ЦПС – микропроцессорные устройства РЗА, а лишь использовать его для уменьшения поверхности атаки. Основной объем задач ИБ и ее первых эшелонов должен возлагаться на указанное выше вторичное оборудование ПС.

Одним из способов повышения качества защищенности объектов энергетики (и, прежде всего, ЦПС) является сегментация цифровых сетей, заключающаяся в разбиении сети на логические сектора, разделенные между собой средствами защиты, препятствующими распространению угрозы на несколько сегментов. Такой подход, дополнительно, существенно повышает надежность функционирования системы, в т. ч. при кибератаках.

Преимущества сегментации технологической сети:

- максимально возможная изоляция самого важного сегмента сети – РЗА. В идеале – физическая изоляция шины процесса, в ряде случаев – логическая;
- организация эшелонированной обороны – злоумышленнику придется вскрывать сеть слоями, направляя трафик через межсетевой экран с системой обнаружения вторжений на каждом этапе;
- коммуникации между сегментами РЗА и АСУ жестко ограничиваются.

Многие этим решением пренебрегают уже на этапе проектирования по различным причинам, например, снижение капитальных затрат [8, 10, 12].

В интернете и СМИ часто мелькают новости и международная статистика, где главными странами-источниками кибератак на все окружающее вокруг являются Северная Корея, Иран, Россия, Китай… Это говорит (на наш взгляд) лишь о том, что, помимо реальных технических проблем и вполне понятных методов решений, тематика ИБ сильно политизируется. Как следствие, возникают коммерческие структуры вокруг тематики ИБ, которые заняты более решением политико-коммерческих задач, а не реальной ИБ объектов электроэнергетики и промышленности. Как следствие, учитывая все приведенные факторы, мы должны подходить к вопросам ИБ лишь технически и статистически, руководствуясь заповедью “не навреди”. На практике мы:

- не строили системы ИБ по ценам, превышающим или сопоставимым со стоимостью вторичных систем РЗиА на объекте;
- прагматично не перегружали оборудование вторичных систем защиты, автоматики и управления объемом требований по ИБ, превышающим или сопоставимым порой с их основным функционалом;
- не заставляли функционировать систему ИБ во вред основному технологическому процессу на объектах энергетики – распределению электроэнергии, а также управлению этим процессом и защите от повреждений.

Наличие жизненного цикла безопасной разработки программного обеспечения по ГОСТ-Р 56939-2016 позволяет внедрять в программное обеспечение эффективные встроенные средства защиты информации и минимизирует количество ошибок и уязвимостей программного обеспечения. Встроенные средства защиты информации — это средства защиты, являющиеся неотъемлемой частью компонентов системы, обеспечение ИБ в которых не является основным функционалом, например, разграничение прав доступа в автоматизированной системе, парольная защита пользователей, разграничение прав доступа пользователей контроль целостности программного обеспечения и конфигурации, журнал событий безопасности.

Для повышения уровня безопасности в микропроцессорных устройствах РЗА нами реализованы следующие встроенные средства защиты информации.

- Самодиагностика:
• при включении терминала;
• во время работы терминала;
• контроль целостности прошивки терминала путем подсчета контрольных сумм.
- Восстановление программного обеспечения и конфигурации:
• возврат на предыдущие конфигурации;
• возврат к заводской конфигурации.
- Защита от несанкционированного доступа:
• доступ к системе с использованием пароля;
• разграничение доступа с использованием ролевой модели;
• ограничение параллельных сеансов доступа пользователей.
- Регистрация событий и действий пользователей:
• все попытки авторизации пользователя (успешная/неуспешная);

• блокировка ИЧМ при достижении установленного количества неверного ввода пароля;
• попытки разблокирования интерактивного сеанса;
• изменение прав доступа группы пользователей.
- Порты связи:
• большинство по умолчанию отключено;
• рекомендуется отключить все неиспользуемые порты.

В крупных сетевых и генерирующих компаниях РФ отсутствует открыто публикуемая статистика по вторжению и попыткам кибератак на их объекты. Как следствие, процесс формирования подходов и предлагаемых решений большей частью строится на гипотетических измышлениях, и порой чрезмерно завышенных относительно уровня реальной проблемы.

Однако согласно проведенному Научно-техническим центром ФГУП «ГРЧЦ» исследованию кибератак на критическую инфраструктуру в мире и в России на основе открытых новостных и статистических источников, а также исследованиям Group-IB, Positive Technologies, Kaspersky и других крупных компаний, специализирующихся на кибербезопасности, прогнозируется, что в 2021 году волна кибератак шифровальщиков затронет российский бизнес и достигнет СНГ [13].

При подходах к построению систем ИБ иногда забывают об основных свойствах РЗА, описанных на первых страницах любой книги по релейной защите и автоматике – это селективность, быстродействие, чувствительность и надежность. Зачастую избыточные требования к ИБ, и в особенности к встроенным средствам ИБ устройств, могут существенным образом снижать один из самых важных параметров РЗА – надежность, как аппаратную, так и функциональную. Понижение аппаратной надежности терминалов РЗА происходит из-за значительного увеличения вычислительных ресурсов при обязательном требовании отсутствия принудительного охлаждения устройств. Пример – необходимость использования криптографии в темпе процесса обмена информацией. Реальное понижение надежности основной функции РЗА – отказ в действии при необходимости действия или излишние отключения могут приводить к экономическим потерям в энергетике, соизмеримым или большим, чем от предполагаемых кибератак.

Поиск здравого компромисса – одна из ключевых задач при составлении технических требований к системам ИБ и реализации технических решений не только для специалистов АСУ по безопасности, но и важная задача для специалистов в области РЗА [10, 11, 12].

Среди технических мер по ИБ наиболее эффективным является размещение оборудования и ПО в зонах с различным уровнем ИБ, среди которых наивысший уровень имеет зона, включающая устройства РЗА. Еще одной эффективной технической мерой может быть использование специализированного (проприетарного) ПО в первую очередь операционных систем (или их отсутствие) и сетевых протоколов.

ЗАКЛЮЧЕНИЕ

1. В настоящий момент важнейшей задачей является определение разумно обоснованных требований по ИБ к вторичным системам энергообъектов, в том числе и к устройствам РЗА, не ухудшающих их основные свойства [2, 3].

2. Проведение работ по ИБ (аттестация оборудования РЗА, согласование технических требований на устройства РЗА) не может проходить в отрыве от специалистов по РЗА [5].

3. При формировании требований по ИБ не стоит полагаться на РЗА как на единственный элемент в системе ПС, к которому предъявляются сколь-либо значимые требования ИБ, хотя возможно это наиболее удобно т. к. данный сегмент вторичного оборудования ПС максимально локализован в РФ и имеется возможность активно влиять на производителей [4].

4. Создание эшелонированной системы ИБ, состоящей из нескольких логических рубежей, за счет сегментирования сети и выделения демилитаризованной зоны существенно повышает надежность функционирования системы, в т. ч. при кибератаках. [2, 3, 10].

5. Важнейшим аспектом при разработке безопасного программного обеспечения является наличие защищенной инфраструктуры среды разработки с применением мер защиты достаточных не только для нивелирования угроз безопасности информации, но и сохраняющие эффективный процесс изготовления программного продукта [4, 8, 9].

ЛИТЕРАТУРА

[22] Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».

[23] Распоряжение ПАО «ФСК ЕЭС» от 30.08.2016 г. № 367р «Об утверждении минимально необходимых организационных и технических требований к обеспечению информационной безопасности автоматизированных систем технологического управления, используемых для функционирования электросетевого комплекса ПАО «ФСК ЕЭС».

[24] Распоряжение ПАО «Россети» от 01.04.2016 г. № 140 «Об утверждении минимальных требований к информационной безопасности АСТУ».

[25] Распоряжение ПАО «Россети» от 30.05.2017 № 282р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети».

[26] Приложение № 1 к приказу ПАО «Россети» от 28.08.2020 № 391 «Методика проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе».

[27] Приказ ФСТЭК № 31 от 14.03.2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

[28] Приказ ФСТЭК от 25 декабря 2017 года № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации».

[29] ГОСТ Р 56939 - 2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

[30] ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения».

[31] ГОСТ Р МЭК 62443-2-1-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики».

[32] ГОСТ Р ИСО МЭК 15408-1-2012 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель"».

[33] ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

[34] Материалы сайта: https://rdc.grfc.ru/2021/07/kiberataki_na_kii/#post-1443-_Toc74839594

3.7. ОСОБЕННОСТИ РЕАЛИЗАЦИИ УСТРОЙСТВ СЕРИИ БЭМП В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ К КИИ

Н.В. ПАРШИКОВ, И.А. ЕВГРАФОВ
АО «ЧЭАЗ»
Россия

Контактное лицо:

И.А. ЕВГРАФОВ

i.evgrafov@cheaz.ru

Ключевые слова:

Информационная безопасность, устройства серии БЭМП, критическая информационная инфраструктура, релейная защита и автоматика, РЗА.

ВВЕДЕНИЕ

На сегодняшний день происходит повсеместное внедрение цифровых технологий. Данная тенденция наблюдается и в энергетической отрасли. Кроме неоспоримых плюсов, цифровизация несет и ряд новых проблем. Одной из них является проблема реализации мер информационной безопасности, которые предназначены для защиты данных и поддерживающей инфраструктуры от случайного или преднамеренного вмешательства. Для обеспечения данной защиты в РФ приняты следующие нормативные документы:

– № 256-ФЗ от 21 июля 2011 года «О безопасности объектов топливно-энергетического комплекса» (далее ФЗ № 256);

– № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации» (далее ФЗ № 187);

– Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (далее 31 приказ ФСТЭК);

– Приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– Распоряжение ПАО «Россети» от 30.05.2017 № 282р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети» (далее 282 распоряжение Россетей).

Вышеперечисленные нормативные акты накладывают дополнительные требования на устройства серии БЭМП, выполняющие функции релейной и автоматики.

ОСНОВНАЯ ЧАСТЬ

По ФЗ № 187 информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, используемые на объектах энергетики попадают под категорию критической информационной инфраструктуры.

По 31 приказу ФСТЭК и 282 распоряжению Россетей устройства РЗА серии БЭМП относятся к автоматизированным системам управления. Поэтому, для выполнения требований нормативных документов, в устройствах БЭМП были реализованы функций информационной безопасности.

Просто внедрение функций безопасности не является достаточным: по 282 распоряжению Россетей требует сертификации во ФСТЭК программного обеспечения устройств серии БЭМП. Тут возникает некоторое затруднение, так как уже разработано более 20 типоисполнений устройств серии БЭМП. Сертифицировать программное обеспечение каждого типоисполнения было бы затратно и трудоемко. Для решения данной проблемы программное обеспечение устройств серии БЭМП было разделено на две части как показано на рисунке 1. В первой реализованы функции безопасности и в ней производится контроль информационного обмена с сервером телемеханики, сервером системы сбора и передачи информации и прочими системами. Эта часть называется программное обеспечение устройств серии БЭМП (далее ПОУБ). ПОУБ будет сертифицировано во ФСТЭК. Вторая часть будет выполнять функции релейной защиты и автоматики. Она называется технологическое программное обеспечение (далее ТПО). ТПО получает данные от внешней среды только через ПОУБ.

Такое модульное построение системы позволит, единожды пройдя сертификацию, реализовать все необходимые типоисполнения устройств серии БЭМП. При этом требования нормативной документации будут выполнены.

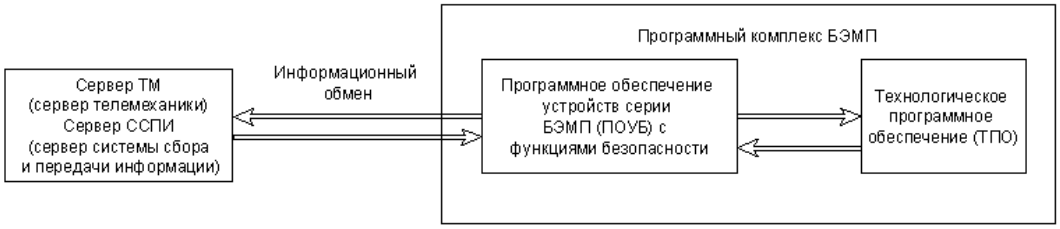


Рис. 1.Программный комплекс БЭМП.

Разработка функций информационной безопасности производилась в следующей очередности.

1. Выбор профиля защиты. **Профиль защи**ты (protection profile) – независимое от реализации изложение потребностей в безопасности для некоторого типа объекта оценки (по ГОСТ 15408-1). В нашем случае объектом оценки является ПО устройств серии БЭМП.

2. Разработка задания по безопасности на основе профиля защиты. **Задание по безопасности** (security target) – зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного объекта оценки (по ГОСТ 15408-1).

3. Разработка технического задания на основе задания по безопасности с учетом технических особенностей платформы БЭМП.

4. Реализация функций информационной безопасности в устройствах БЭМП.

Блок-схема разработки функций информационной безопасности изображена на рис. 2.

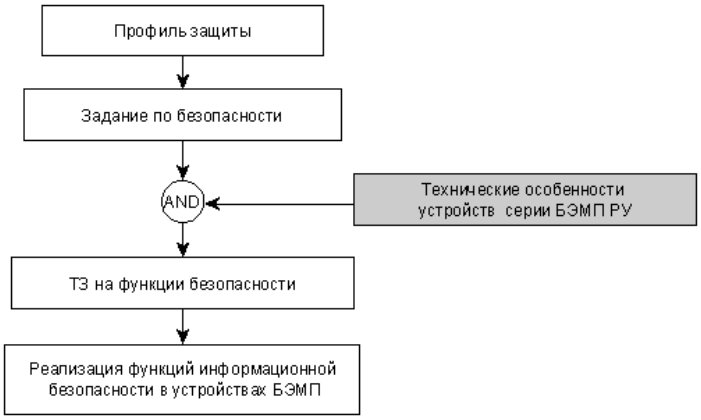


Рис. 2. Этапы реализации функций безопасности
в устройствах серии БЭМП.

Основные затруднения, возникшие при реализации функций информационной безопасности, проистекали из профиля защиты. Для прохождения сертификации во ФСТЭК, необходимо использовать профиль защиты, утвержденный ФСТЭК. Поэтому за основу был взят профиль защиты операционной системы как наиболее подходящий. Но он не учитывает особенности устройств релейной защиты и среды их эксплуатации, некоторые требования трудно выполнить на встраиваемых системах, к которым относится наше устройство, так как они существенно отличаются от персонального компьютера, на котором функционирует операционная система.

Реализованные в устройствах серии БЭМП функции безопасности можно разделить на три типа: превентивные, детективные, корректирующие.

Превентивные предназначены предотвращать реализацию угроз. К этому типу функций безопасности относятся идентификация, идентификация с использованием физических идентификаторов; аутентификация и авторизация; возможность добавления и удаления

пользователей; ролевая система доступа к устройству; доступ по разрешенным IP и MAC адресам.

Фундаментом функций безопасности устройств серии БЭМП является система управления доступом. На данный момент основными типами систем управления доступом являются мандатная, дискреционное, ролевая. Решено было применять изображенную на рисунке 3 ролевую систему доступа, так как она является наиболее подходящей для применения в устройствах РЗА. Она не требует настройки прав каждого пользователя в отдельности и не позволяет передавать свои права другим пользователям. Для присвоения прав пользователю достаточно присвоить ему определенную роль, за которой закреплены данные права. Присвоение роли пользователя тоже является правом, поэтому им обладает ограниченное количество ролей.

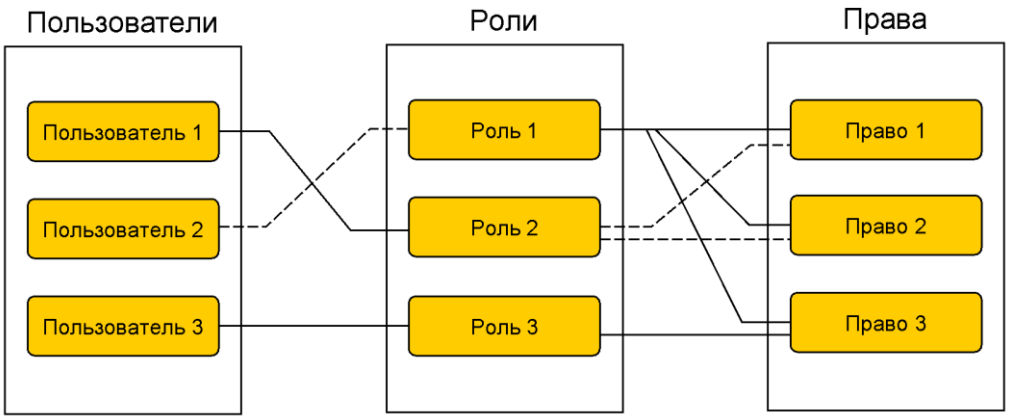


Рис. 3. Ролевая система доступа.

Были выделены объекты доступа в устройствах серии БЭМП: уставки и прочие настройки РЗА, время в устройстве (изменение и синхронизация) и прочие. Права на доступ к данным объектам были разбиты на группы. Эти группы прав были присвоены ролям, реализованным в устройствах серии БЭМП.

Для работы с устройством пользователю необходимо пройти процедуру идентификации и аутентификации: предъявить свой логин, пароль и физический идентификатор, которые являются его атрибутами безопасности. Если все предъявленные пользователем атрибуты верны, происходит авторизация и на устройстве открывается сеанс пользователя.

Для SCADA-систем производится только идентификация. Идентификаторами являются IP- и MAC-адреса. Чтобы SCADA-система получила на устройстве соответствующие права, она должна подключаться с устройства, имеющего IP- и MAC-адреса, занесенные в список разрешенных на устройстве БЭМП.

Детективные предназначены для обнаружения воздействия угроз. К ним относится журнал аудита безопасности. В нем фиксируются все действия субъектов с терминалом, касающиеся информационной безопасности: подключение к USB-порту, отключение от USB-порта, добавление удаление пользователей, настройка параметров безопасности и других событий безопасности. Данный журнал позволяет определить кто, когда, по какому порту выполнял действия над объектами в устройствах БЭМП. Для сохранения журнала аудита реализовано его скачивание с устройства, а также сигнализация эксплуатирующему персоналу о его заполнении на объем более чем на 75%.

Коррективные предназначены для восстановления терминала к состоянию, до реализации угрозы. К ним относятся функции сохранения и загрузки настроек

технологических, релейной защиты терминала, кроме настроек функций информационной безопасности, обновление программного обеспечения.

Для взаимодействия с функциями безопасности устройств серии БЭМП было доработано программное обеспечение «Проводник БЭМП» и разработано программное обеспечение «Администратор безопасности БЭМП».

В «Проводник БЭМП» добавлена возможность аутентификации пользователя. Без прохождения процедур аутентификации и авторизации у пользователя не будет доступа к настройкам функций РЗА, портов связи и параметров устройства, не связанных с безопасностью. После аутентификации пользователь сможет работать только с теми объектам доступа в устройстве, которые разрешены его роли.

Программное обеспечение «Администратор безопасности БЭМП» предназначено для настройки функций безопасности: добавления, удаления, редактирования пользователя; считывания журнала аудита; настройка времени прекращения сеанса пользователя, при его бездействии и прочих функций. Для получения доступа к вышеперечисленному функционалу пользователю необходимо пройти процедуры аутентификации и авторизации.

Ни «Проводник БЭМП» ни «Администратор безопасности БЭМП» не выполняют функции безопасности. Все функции безопасности реализованы внутри устройств серии БЭМП.

Для работы с устройством через его интерфейс человек-машина, пользователю необходимо выбрать свой логин, ввести пароль, предъявить аппаратный идентификатор, как показано на рис. 3. После успешного прохождения этих процедур, пользователь получит доступ к функционалу в соответствии с присвоенной ему ролью.



Рис. 3. Предъявление пользователем атрибутов безопасности: логина, пароля, физического идентификатора.

ЗАКЛЮЧЕНИЕ

Использование на энергообъектах устройств серии БЭМП с функциями безопасности позволит значительно повысить их защищенность от киберугроз, обеспечит отчетность действий персонала с устройствами серии БЭМП.

ЛИТЕРАТУРА

[1] Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности: Учеб для вузов. - М.: Горячая линия-Телеком, 2006.- 544 с.: ил.

[2] Бондарев В. В. - Введение в информационную безопасность автоматизированных систем: Учеб. пособие. - М.: Издательство МГТУ им. Н. Э. Баумана, 2016. - 250с.

3.8. ПЕРЕХОД ИЗ СИСТЕМЫ КООРДИНАТ «ЦЕЛОСТНОСТЬ, КОНФИДЕНЦИАЛЬНОСТЬ, ДОСТУПНОСТЬ» В СИСТЕМУ КООРДИНАТ «НЕДООТПУСК, ВРЕМЯ ВОССТАНОВЛЕНИЯ, УЩЕРБ»

А. А. ВОЛОШИН, Н. С. ЛЕБЕДЕВА, А. В. КУРГАНОВ

Федеральное государственное бюджетное образовательное учреждение
«Национальный исследовательский университет «МЭИ»

Россия

Контактное лицо:

А. А. ВОЛОШИН

VoloshinAA@mpei.ru

Ключевые слова:

Релейная защита и автоматика, цифровая подстанция, информационная безопасность, оценка экономического ущерба.

ВВЕДЕНИЕ

Современные объекты электроэнергетической системы состоят из двух тесно связанных между собой систем: физической, реализующей технологический процесс, и информационно-коммуникационной, выполняющей управление технологическим процессом. Обе эти системы вместе образуют единую киберфизическую систему. По мере повышения степени использования современных информационных технологий и средств вычислительной техники как на уровне первичного оборудования, так и на уровне вторичных систем подстанции, таких как система релейной защиты и противоаварийной автоматики, система автоматизированного управления технологическим процессом, система мониторинга переходных процессов и др., происходит общее усложнение киберфизической системы, повышается ее уязвимость с точки зрения информационной безопасности, а значит, становится необходимой разработка специальных мер защиты от кибератак.

В качестве возможных технологических последствий инцидентов информационной безопасности можно привести следующие технологические нарушения:

- подмена информации об измерениях параметров режима энергосистемы;
- подача ложных сигналов на вход микропроцессорных терминалов РЗА и АСУ ТП;
- формирование ложных сигналов управления коммутационными аппаратами;
- искажение меток единого времени.

Перечисленные выше технологические нарушения в свою очередь могут привести к:

- ложным отключениям межсистемных связей и потребителей;
- несрабатываниям в аварийных режимах или излишнем срабатывания в нормальных режимах устройств релейной защиты и автоматики в аварийных режимах;
- передаче ложной информации в системы диспетчерского управления.

Таким образом, кибератаки могут стать причиной значительного экономического ущерба как для электросетевых компаний, так и для потребителей электроэнергии, не говоря уже о том, что последствия кибератак могут представлять опасность для жизни и здоровья людей.

В настоящем докладе рассматриваются возможные методы оценки технологических последствий инцидентов информационной безопасности, в соответствии с которыми возможно определение стоимостных показателей ущерба, возникающего в результате проведения кибератак на объекты электроэнергетической инфраструктуры.

Оценка экономического ущерба от кибератак на цифровые подстанции МЭС и РЭС, приводящих к нарушению электроснабжения потребителей, недоотпуску электрической энергии электросетевыми компаниями, аварийным отключениям элементов электрической сети и повышенным потерям электрической энергии в послеаварийных режимах, может быть выполнена по результатам расчета режимов. Для полной оценки стоимостных показателей ущерба должны быть также вычислены затраты на аварийно-восстановительные (внеплановые) ремонты оборудования.

Другим важным пунктом при проведении оценки стоимостных показателей экономического ущерба для электрических подстанций является оценка стоимости системы обеспечения информационной безопасности в соотношении с возможным ущербом от потенциальных кибератак, необходимая для выработки подходов к выбору оптимальной архитектуры построения систем информационной безопасности.

Для наглядной оценки влияния стоимости решений по ИБ на снижение технологических ущербов при реализации компьютерных атак предложен способ отражения системы координат, применяемой в ИБ «целостность, доступность, конфиденциальность» в систему координат «недоотпуск, время восстановления, ущерб». Для осуществления указанного перехода разработан способ моделирования технологических нарушений возникающих при реализации компьютерных атак. При этом используется как информация о структуре информационно-коммуникационной системы, так и модель подстанции и

прилегающих электрических сетей. Для каждого элемента информационно-коммуникационной инфраструктуры разрабатывается модель влияния киберинцидентов на их технологическое функционирование. При реализации киберинцидента моделируется то или иное технологическое (функциональное) поведение устройства (например, формирование команды управления КА). Это поведение на следующем шаге передается в модель, отражающую технологические процессы. В модели технологических процессов при этом соответствующее управляемое оборудование меняет свое состояние в соответствии с поступившей командой, затем рассчитываются новые значения технологических параметров. На основе рассчитанных значений технологических параметров определяется, на каких элементах физической системы значения технологических параметров входят в диапазон аварийных значений. Таким образом определяются поврежденные элементы. Для каждого типа поврежденного элемента на основе справочных данных определяется стоимость ремонта/замены оборудования и времени, которое для этого необходимо. На третьем шаге информация о поврежденном оборудовании передается в модель прилегающих сетей, по результатам расчетов в которой определяется, какие потребители будут отключены при рассматриваемом инциденте. На основе информации об объеме отключенной нагрузки и времени восстановления рассчитываются ущербы потребителей от недоотпуска электроэнергии.

ОСНОВНАЯ ЧАСТЬ

Как уже отмечалось ранее, цифровые подстанции состоят из большого числа взаимосвязанных компонентов: первичного высоковольтного оборудования и оборудования вторичных систем, таких, как РЗА, АСУТП, АИИСКУЭ, СМПР и др. Для оценки потенциальных последствий кибератак на указанные устройства была проведена их классификация по степени вовлеченности в процесс управления технологическим процессом с целью выявления тех из них, которые имеют наиболее высокое влияние на технологический процесс, а значит, могут представлять наибольший интерес для нарушителей информационной безопасности. Для каждого типа оборудования была проанализированы:

- потенциальная возможность кибератаки;
- возможные технологические нарушения, вызванные кибератаками;
- срок наступления последствий кибератаки.

Результаты проведенного анализа представлены в табл.

Тип оборудования	**Потенциальная возможность кибератаки**	**Возможные технологические нарушения**	**Сроки наступления последствия кибератаки**
Высоковольтное первичное оборудование коммутационное оборудование без микропроцессорных блоков управления	отсутствует	отсутствуют	-
Высоковольтное первичное оборудование коммутационное оборудование с микропроцессорными блоками управления без подключения к информационно-телекоммуникационной инфраструктуре подстанции	отсутствует	отсутствуют	-
Высоковольтное первичное коммутационное оборудование с микропроцессорными блоками управления с подключением к информационно-телекоммуникационной инфраструктуре подстанции	присутствует	– нарушение работоспособности сетевых портов микропроцессорных блоков; – блокировка приема управляющих воздействий; – проведение несанкционированных операций управления коммутационным оборудованием.	незамедлительные
Высоковольтное первичное измерительное оборудование с микропроцессорными блоками – цифровые ТТ и ТН	присутствует	– нарушение работоспособности сетевых портов микропроцессорных блоков; – подмена цифровых потоков информации об аналоговых параметрах режима работы силового оборудования. –	незамедлительное, среднесрочное
Преобразователи	присутствует	– нарушение	незамедлительное,

Тип оборудования	**Потенциальная возможность кибератаки**	**Возможные технологические нарушения**	**Сроки наступления последствия кибератаки**
аналоговых сигналов		работоспособности сетевых портов ПАС; – подмена цифровых потоков информации об аналоговых параметрах режима работы силового оборудования.	среднесрочное
Преобразователи дискретных сигналов	присутствует	– нарушение работоспособности сетевых портов ПДС; – блокировка приема управляющих воздействий; – проведение несанкционированных операций управления коммутационным оборудованием.	незамедлительное
Терминалы РЗА	присутствует	– нарушение работоспособности сетевых портов микропроцессорных терминалов; – ложное срабатывание устройств РЗА; – несанкционированное изменение уставок срабатывания устройств РЗА; – передача на вход терминалов ложных цифровых потоков информации об аналоговых параметрах режима работы силового оборудования.	незамедлительное, среднесрочное
Контроллеры присоединений	присутствует	– нарушение работоспособности сетевых портов контроллеров присоединений; – проведение несанкционированных	незамедлительное, среднесрочное

Тип оборудования	**Потенциальная возможность кибератаки**	**Возможные технологические нарушения**	**Сроки наступления последствия кибератаки**
		операций управления коммутационным оборудованием; неправильная работа ОБР	

Табл. 1. Анализ возможных технологических последствий инцидентов информационной безопасности для различных видов оборудования.

Табл. 1. Продолжение.

Коммутаторы и маршрутизаторы	присутствует	– нарушение работоспособности сетевых портов коммутаторов и маршрутизаторов; – переполнение буфера коммутатора или маршрутизатора; – уменьшение скорости передачи данных; – полная загрузка локальной вычислительной сети (ЛВС). –	незамедлительное, среднесрочное.
Многофункциональные измерительные устройства, УСВИ, терминалы РАС	присутствует	– нарушение работоспособности сетевых портов устройств; – подмена цифровых данных о значениях параметров режима электрической сети	среднесрочное, долгосрочное
Контроллер СКУД	присутствует	– проникновение сотрудника в любое время и в любое охраняемое СКУД помещение для шпионажа, кражи или других злонамеренных действий; – проникновение на охраняемую территорию злоумышленника под	незамедлительное, среднесрочное

		видом легального сотрудника компании; – блокировка всех дверей на подконтрольной территории; – полное отключение СКУД; – правка сотрудниками логов своего рабочего времени. –	
Серверы точного времени	присутствует	– нарушение работоспособности сетевых портов серверов точного времени; – подмена информации о времени фиксации измерений параметров режима, времени фиксации событий на подстанции. –	незамедлительное, среднесрочное
АРМ РЗА, АРМ оперативного персонала	присутствует	– потеря удаленного управления интеллектуальными устройствами и коммутационными аппаратами; – несанкционированное удаленное управление интеллектуальными устройствами и коммутационными аппаратами	незамедлительное
Шлюз телемеханики АСУ ТП	присутствует	– несанкционированное удаленное управление интеллектуальными устройствами и коммутационными аппаратами	незамедлительное

Кроме того, были рассмотрены возможные типы киберугроз для оборудования цифровых подстанций.

На цифровых подстанциях киберугрозы могут быть внутренними и внешними. Внешние киберугрозы могут быть реализованы посредством несанкционированного подключения к оборудованию систем передачи телемеханической информации.

Внешние киберугрозы подразделяются на две категории: блокирующие, а также имитирующие и модифицирующие.

Блокирующие кибератаки могут приводить к отказу в работе, созданию затора при передаче данных, засылке вируса, физзификации данных.

Имитирующие и модифицирующие атаки включают в себя блокирование персонализации доступа для пользователей, реупорядочение и смешение данных, клонирование данных, организацию сбоев в работе системы единого времени, подмену данных, приводящую в том числе к сбою в работе вторичных систем.

Очевидно, что с точки зрения стоимостной оценки ущерба, как для электросетевых компаний, так и для потребителей электроэнергии, наиболее опасными являются кибератаки, потенциально приводящие к несанкционированным отключениям первичного оборудования, и, соответственно, к значительному недоотпуску электроэнергии и проведению ремонтно-восстановительных работ.

Оценку технологических последствий инцидентов информационной безопасности для электросетевых компаний предлагается выполнять на основе расчета следующих компонентов:

- затрат на аварийно-восстановительные (внеплановые) работы по ремонту отказавшего оборудования;
- недополучение величины стоимости компенсации потерь электроэнергии, которую бы выплатил потребитель в случае отсутствия нарушения электроснабжения;
- дополнительных расходов на выработку и передачу электроэнергии в периоды аварийных, послеаварийных и ремонтных режимов работы электроснабжающей системы (до восстановления оптимального режима), связанных с включением менее экономичного оборудования и повышением потерь электроэнергии в сетях.

Затраты на аварийно-восстановительные (внеплановые) работы по ремонту отказавшего оборудования определяются по формуле:

$$З_{\text{рем}}^{\text{ав}} = \sum_{i=1}^{n} з_{\text{рем}i}^{\text{ав}} m_i,$$

где $з_{\text{рем}i}^{\text{ав}}$ – средняя стоимость восстановления поврежденного оборудования i-го типа; m_i – число единиц однотипного оборудования; n – число типов оборудования.

Стоимость компенсации потерь электроэнергии, которую бы выплатил потребитель в случае отсутствия нарушения электроснабжения определяется по следующей формуле:

$$\Delta З_{\text{сист}} = \sum_{i} \frac{\beta}{100} \Delta P_{ni} \Delta t_i C_{0\Delta Э},$$

где:

β – норматив технологических потерь электроэнергии при ее передаче по ЕНЭС, %

ΔP_{ni} – снижение мощности в i-м узле нагрузки при k-м технологическом нарушении, кВт;

Δt_i – длительность k-го технологического нарушения, ч;

$C_{0\Delta Э}$ – средняя ставка тарифа на оплату потребителями услуг по передаче

электроэнергии по ЕНЭС нормативных технологических потерь электрической энергии (мощности) в ЕНЭС, руб./кВт·ч.

Дополнительные расходы на выработку и передачу электроэнергии в периоды аварийных, послеаварийных и ремонтных режимов работы электроснабжающей системы можно определить по следующей формуле:

$$\Delta З_{\text{сист}}^{\text{ав}} = \beta(P_{max}^{\text{ав}} - P_{max}^{\text{н}})\tau_{max}C_{0\Delta Э},$$

где $\Delta P_{max}^{\text{ав}}, \Delta P_{max}^{\text{н}}$ – передаваемые мощности в сети при аварийных и нормальных режимах их работы; τ_{max} – число часов максимальных потерь мощности в электрических сетях; $C_{0\Delta Э}$ – ставка тарифа на компенсацию потерь электроэнергии в сети.

Оценка технологических последствий инцидентов информационной безопасности для потребителей зависит от времени возникшего перерыва в электроснабжении и от типа потребителей и может быть вычислена по формуле:

$$C_0 = \sum_j Y_j(\Delta t_j) \cdot \Delta P_{nj} \cdot \tau_j,$$

где

Y_j – экономический ущерб потребителей для j-го узла нагрузки (определяется по табл. 2), руб./кВт·ч;

ΔP_{nj} – снижение мощности в j-м узле нагрузки при k-м технологическом нарушении (определяется по результатам расчета электрического режима),кВт;

Δt_j – длительность нарушения электроснабжения в j-м узле нагрузки при k-м технологическом нарушении;

j – порядковый номер узла нагрузки, от 1 до Nn (где Nn – суммарное количество узлов нагрузки).

Для наглядного представления результатов расчетов технологических последствий инцидентов информационной безопасности возможно построение диаграммы, приведенной на рис. 7.1.

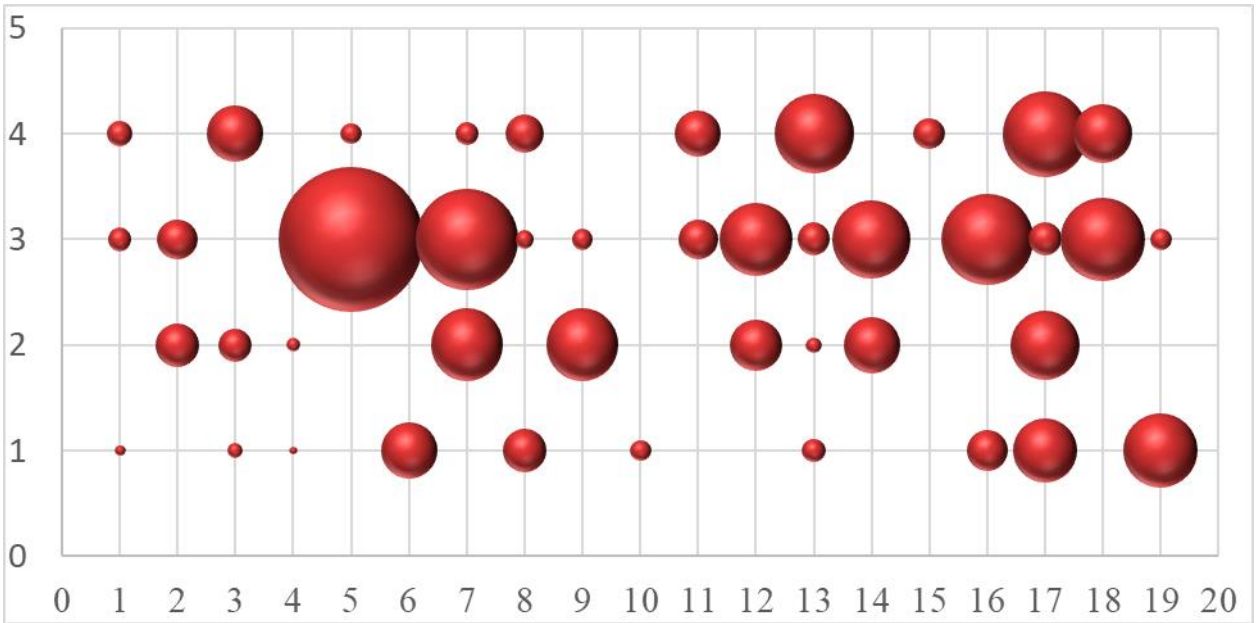


Рис. 1. Оценка технологических последствий кибератак.

На данной диаграмме по горизонтальной оси обозначены узлы цифровой подстанции, которые потенциально могут быть подвергнуты кибератакам. На вертикальной оси обозначены все возможные виды кибератак для рассматриваемого электроэнергетического объекта. В точках пересечений абсцисс и ординат обозначен потенциальный ущерб от проведения кибератаки, обозначенной на вертикальный оси, на узел ЦПС, обозначенный на горизонтальной оси. Объем сферы прямо пропорционален ущербу от рассматриваемой кибератаки на указанный узел.

Алгоритм построения графика сводится к следующему.

Выполняется анализ всех узлов, входящих в первичную схему рассматриваемого объекта, а также во вторичные системы ЦПС с целью выделения из них тех, на которые могут быть организованы кибератаки.

Выполняется анализ всех видов кибератак, которые могут быть организованы для данного электроэнергического объекта, в соответствии с моделью киберугроз.

Для каждого узла и для каждого вида киберугроз выполняется расчет стоимостных показателей последствий кибератаки на данный узел, в соответствии с вышеприведенными формулами расчета ущербов.

По результатам расчетов по п. 3 выполняется построение диаграммы оценки технологических последствий инцидентов информационной безопасности, приведенной на рис.1.

Построенная диаграмма наглядно отражает результаты проведенных расчетов стоимостных показателей технологических последствий инцидентов информационной безопасности, а также позволяет определить типы кибератак и узлы ЦПС, с наиболее тяжелыми экономическими последствиями.

На основе данных, рассчитанных для построения диаграммы оценки технологических последствий кибератак, а также данных о возможностях различных систем информационной защиты по противодействию тем или иным кибератакам, возможно построение гистограммы вероятного эффекта от применения различных систем информационной безопасности. Примерный вид диаграммы приведен на рис. 2, где для различных вариантов исполнения систем информационной безопасности представлена оценка вероятного эффекта от применения рассматриваемой системы.

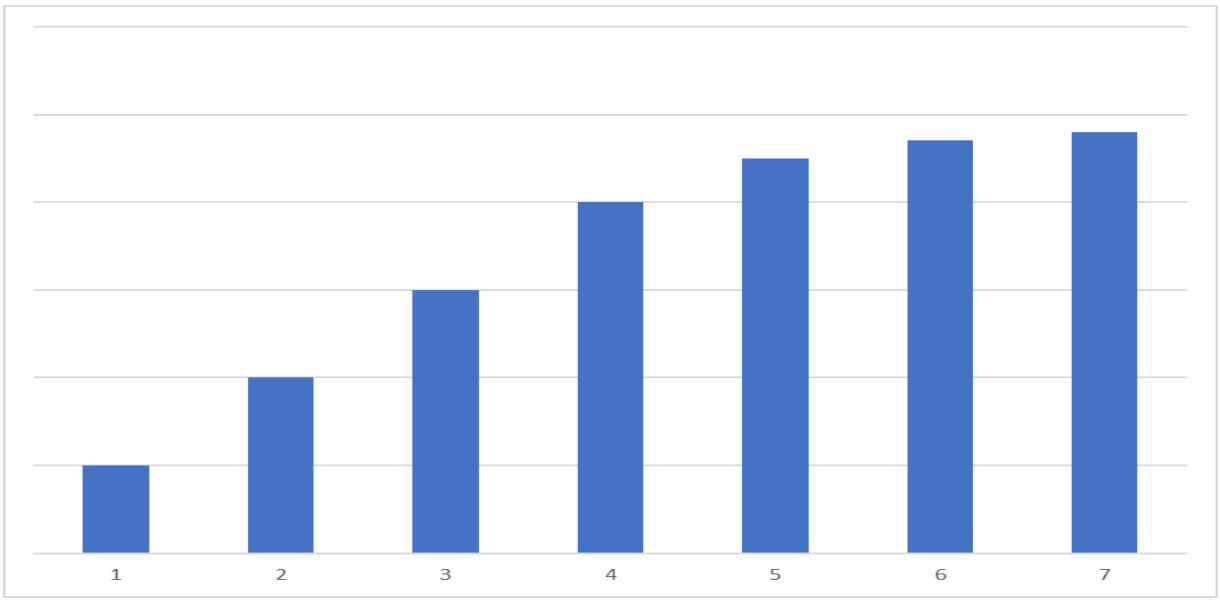


Рис. 2. Вероятный эффект от применения различных систем информационной безопасности.

Дополнительно при учете информации о стоимости реализации той или иной системы информационной безопасности возможно построение графика, позволяющего оценить эффективность вложений при реализации систем информационной безопасности. Для построения графика предлагается разделить стоимостное выражение вероятного эффекта от внедрения конкретной системы информационной безопасности на стоимость рассматриваемой системы. На рис. 3 приведен возможный вид такого графика, из которого можно сделать вывод о том, реализация какой из систем будет наиболее рациональна с точки зрения эффективности вложений.

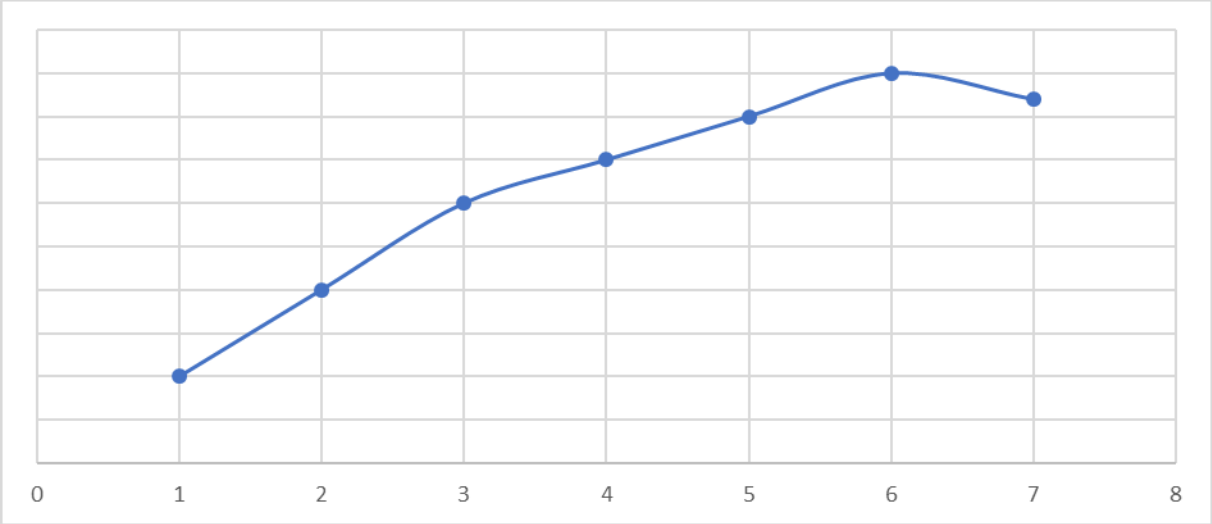


Рис.3. Оценка эффективности вложений при реализации систем информационной безопасности.

ЗАКЛЮЧЕНИЕ

Наметившийся несколько лет назад тренд на применение специализированных систем информационной безопасности на объектах электроэнергетической инфраструктуры приводит к тому, что системы защиты становятся все более сложными и дорогостоящими, а оценка эффективности вложений в указанные системы не всегда представляется возможной. В связи с этим в настоящем докладе предложена методика оценки стоимостных показателей технологических последствий инцидентов информационной безопасности на объекты как магистральных, так и распределительных электрических сетей, а также оценки эффективности вложений при реализации систем информационной безопасности на основе данных о стоимости внедрения системы ИБ и вероятного эффекта от ее применения.

3.9. ДОЛЖНЫ ЛИ МЫ ПРИМЕНЯТЬ МЕТОДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ РАСПРЕДЕЛИТЕЛЬНЫХ СЕТЕЙ: ВЫЗОВЫ И РЕШЕНИЯ

EROSHAN WEERATHUNGA , MITAL KANABAR , ABHILASH APPUKUTTAN , HIMANSHU BHATIA

GE Grid Solutions,
Grid Solutions
Маркем, Канада
Стаффорд, Великобритания

Контактное лицо:

EROSHAN WEERATHUNGA

Eroshan.Weerathunga@ge.com

Ключевые слова: информационная безопасность, распределительные сети, стратегия информационной безопасности, архитектура информационной безопасности.

АННОТАЦИЯ

Киберугрозы для электросети усиливаются, а атаки становятся все более изощренными и более целенаправленными. Ситуация на Украине в 2015 году продемонстрировала, что атака на распределительную сеть может привести к массовому отключению электроэнергии. Большая часть критически важной инфраструктуры – от транспорта до здравоохранения – питается от распределительных сетей. Кроме того, распределительные системы имеют большую поверхность для атаки ввиду географически рассредоточенных устройств. В дополнение к этому, интеграция возобновляемых источников энергии и микросети добавляет уязвимостей системы безопасности для удаленного управления распределительной сетью.

В настоящей статье исследуются киберугрозы и проблемы, характерные для Распределительных систем управления. Также обсуждаются архитектура информационной безопасности и стратегии глубокоэшелонированной защиты для Распределенной системы управления. Далее в настоящем документе описывается важность функций информационной безопасности интеллектуальных электронных устройств (IED), таких как Ролевая Модель Управления Доступом (RBAC), журналы событий центральной аутентификации и безопасности, а также способы интеграции IED-устройств со сторонними системами безопасности для обеспечения сквозной информационной безопасности, например, Сервер Управления Сведениями и Событиями, важными для безопасности (SIEM), системы управления паролями, межсетевые экраны и системы обнаружения вторжений (IDS) Если интеллектуальные устройства IED поддерживают встроенные функции информационной безопасности, нет необходимости использовать любых внешних шлюзов безопасности с использованием географически распределенные контроллеры в распределительных сетях. Наконец, в настоящей статье обсуждается, как объединить технологии, процессы и людей со службами безопасности, такими как оценка рисков безопасности, обучение и управление исправлениями.

ВВЕДЕНИЕ

Распределение электроэнергии обеспечивает питанием важнейшие секторы инфраструктуры, включая секторы водоснабжения, транспорта, телекоммуникаций, здравоохранения и финансов. С развитием интеллектуальных городов, интеллектуальных автомобилей и интеллектуальных домов наша зависимость от распределения электроэнергии продолжает расти бурными темпами. Чтобы удовлетворить растущий спрос на электроэнергию, энергораспределительные станции применяют цифровые технологии и средства связи для повышения своей эффективности и конкурентоспособности на рынке. Но многочисленные преимущества современных все более цифровых и взаимосвязанных инфраструктур сопровождаются серьезными проблемами в области информационной безопасности.

На уровне электрической сети атака в контексте информационной безопасности означает сбой или отказ оборудования, перебои или длительные перерывы энергоснабжения. Из-за географической разрозненности активов распределительная сеть имеет большую площадь для атаки. Большое расстояние между распределительными контроллерами/IED, масштабирование и разделение в управлении стали самыми большими проблемами для безопасности распределительных станций. Некоторые подстанции находятся в сельской местности, на открытых полях, без обеспечения какой-либо информационной или физической безопасности. Огромное количество географически разрозненных элементов сети означает, что требования к информационной безопасности между системами и во всем их объеме очень сложны в плане управления и реализации.

Угрозы для критической инфраструктуры варьируются от стихийных бедствий, экстремальных погодных условий до физических атак и атак на информационную безопасность. Учитывая все угрозы и места, в которых могут произойти данные атаки, последствия могут сильно различаться. Не все компоненты электросети считаются одинаково важными. Инфраструктура передачи и генерации считается более критичной, чем локальная распределительная инфраструктура, учитывая последствия ее отказа. Повреждение оборудования генерации и передачи, как правило, может привести к самым серьезным и пагубным последствиям. Это не означает, что распределительная сеть защищена от кибер-атаки. В атаке на информационную безопасность в Украине в декабре 2015 года точкой атаки была распределительная система, что привело к отключению 225 000 клиентов [1].

В большинстве случаев взломщики нацеливаются на легкие мишени, нежели жестко защищенные системы. Взломщик с большей вероятностью подключиться к распределительным подстанциям с недостаточной базовой информационной безопасностью и физической защитой. Кибератака на распределительную подстанцию может включать: управление выключателями для отключения подачи энергии или сбой в работе SCADA, чтобы сделать нагрузку неустойчивой. Иногда утверждают, что атака на распределительную сеть будет иметь влияние только на региональном уровне, но не для общей энергосистемы. Однако хорошо организованная атака на информационную безопасность в нескольких распределительных станциях (атака на Украину в 2015 году) может привести к отключению электроэнергии во многих регионах, оставив большое количество клиентов без света. Если взломщик получит доступ к управляющему центру (Master) распределительной SCADA-системы (физически или удаленно), риск значительно выше, поскольку управляющий центр SCADA разрешает доступ к другим элементам распределительной сети и, возможно, линиям передачи в пределах системы.

КИБЕРАТАКА НА УКРАИНУ

23 декабря 2015 года в Украине произошла первая известная успешная атака на информационную безопасность, нацеленная на энергосистему. Атака была направлена на региональный уровень распределения (110 кВ и ниже); хакерам удалось временно прервать подачу электроэнергии в различные регионы Украины [1]. Были атакованы три распределительные подстанции, что привело к нескольким сбоям, в результате которых

примерно 225 000 клиентов в разных областях Украины были лишены электроэнергии. Вскоре после атаки украинские чиновники заявили, что перебои были вызваны кибератакой. Обслуживание удалось восстановить через несколько часов отключения, но сообщается, что затронутые подстанции продолжают работу в режиме эксплуатационных ограничений [1].
Взломщики использовали различные возможности, включая адресный фишинг, варианты вредоносного ПО BlackEnergy 3, внедрение, сбор учетных данных и доступ к сети ICS. Отдельным лицам в электроэнергетических компаниях по электронной почте в виде вложений были направлены вредоносные документы Office. Когда пользователь включает макросы в документах, взломщики используют функциональные возможности макросов Office для установки вредоносного ПО BlackEnergy 3 на компьютеры. Похоже, что взломщики получили доступ более чем за шесть месяцев до фактической атаки. На протяжении шести месяцев взломщики находились в сети, собирая учетные данные, повышая права доступа и перемещаясь по всей системе, используя её уязвимости. Используя украденные учетные данные и подключения виртуальной частной сети (VPN) подстанций, взломщики смогли перенести атаку на сегменты коммуникационной сети, в которых функционировали диспетчерские рабочие станции и серверы SCADA. Злоумышленники захватили контроль над рабочими станциями оператора, тем самым блокируя доступ в системы для операторов. Взломщики использовали ЧМИ удаленной системы SCADA для размыкания выключателей и отключили как минимум 27 подстанций (общее число, вероятно, выше) в автономном режиме в трех энергетических компаниях [1]. Злоумышленники загрузили вредоносную прошивку на устройства последовательного шлюза в Ethernet, чтобы нельзя было отправлять удаленные команды для возврата подстанций в рабочее состояние. Затронутые клиенты даже не могли сообщить об отключении электроэнергии в колл-центр компании, так как злоумышленники совершили атаки типа «отказ в обслуживании» на колл-центр с тысячами звонков.
Атака на Украину была стратегически выполнена, но основа для атаки базировалась на недостатках кибер-гигиены. Это свидетельствует о том, что человеческий фактор является элементом, часто пользующимся для осуществления кибератак, который может серьезно повлиять на подачу энергии.

ДИРЕКТИВЫ NIS

Директива о сетевой и информационной безопасности (NISD) – акт Европейского Союза (ЕС) об информационной безопасности, нацеленный на улучшение информационной безопасности операторов основных услуг (OES) и поставщиков цифровых услуг (DSP) [2]. NISD применяется к организациям во всех государствах – членах ЕС, которые предоставляют «основные услуги», т. е. энергетическая, транспортная инфраструктура, банковские и финансовые услуги, водоснабжение, здравоохранение и цифровая инфраструктура (интернет-провайдеры, DNS-провайдеры и т. д.).

Директива NIS состоит из трех частей.

1. Национальные возможности: Каждое государство должно иметь национальную стратегию для достижения и поддержания более безопасной сети и систем информационной безопасности.
2. Межгосударственное сотрудничество: Сотрудничество и доверие между членами ЕС, например, оперативная группа реагирования на инциденты, связанные с компьютерной безопасностью ЕС (CSIRT), стратегическая группа сотрудничества NIS
3. Национальный надзор за критической инфраструктурой: Государствам-членам следует изложить требования безопасности и процедуры сообщения о конкретных инцидентах для операторов основных услуг и поставщиков цифровых услуг.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В РАСПРЕДЕЛИТЕЛЬНЫХ СЕТЯХ

Многочисленные преимущества современных все более цифровых и взаимосвязанных инфраструктур приводят к проблемам в области информационной безопасности на распределительных станциях.

Сети и коммуникация

Распределительные станции полагаются на коммуникационные сети для передачи данных о рабочем состоянии оборудования, мониторинга рабочих условий и передачи текущих изменений. Функции Распределительной автоматики (DA) и усовершенствованная распределительная сеть позволяют подстанциям быстро обнаруживать, изолировать и устранять неисправности. Уязвимости сети из-за неправильной конфигурации, плохого управления и недостаточной осведомленности о безопасности делают коммуникационные сети одними из самых широко используемых точек входа среди злоумышленников. Службы Эксплуатации все больше полагаются на удаленный доступ, чтобы управлять географически распространенными подстанциями, повышать удобство и снижать затраты. Незащищенный доступ или подключение к критически важным системам с помощью удаленных инструментов и устройств часто называют наиболее часто используемой точкой входа для кибер-инцидентов.

Ближе к клиенту также развернуты интеллектуальные счетчики и инфраструктура автоматического учета (AMI), домашние сети (HAN), устройства накопления энергии, зарядные станции для транспортных средств, а также бытовые средства контроля солнечной и ветровой энергии. Большинство из этих устройств используют беспроводную связь. Вместе они составляют большую, сложную, неоднородную сеть под названием Полевая Сеть (FAN). Одна из основных проблем в современной распределительной сети заключается в том, как контролировать и защищать такие FAN. FAN сталкиваются с различными угрозами. Злоумышленник может попытаться отключить питание в определенной локальной области. Измерения могут быть подделаны, изменены или перехвачены, что может привести к неправильному выставлению счетов клиентам и потере конфиденциальности их данных.

Протоколы связи, используемые в сетях ICS, такие как IEC 101, IEC 103, IEC 104 и Modbus, не имеют практически никаких средств безопасности: из-за отсутствия возможностей аутентификации сообщения могут быть перехвачены, подделаны или изменены.

Устройства

Энергетическая инфраструктура превратилась в цифровую инфраструктуру, которая все больше опирается на интеллектуальные электронные устройства (IED), использующие методы цифровой связи для мониторинга и управления операциями. На некоторых распределительных подстанциях работает устаревшее оборудование, а на других – тесно связанное цифровое оборудование. При этом распределительную сеть сложно защитить из-за географической распределенности и тысяч удаленных подстанций с дистанционным управлением. Это дает злоумышленникам возможность выбирать целью уязвимости устаревшие технологии или инструменты эксплуатации для доступа к новым IED-устройствам. Устройства, взаимодействующие с системой Распределительной Автоматики или функционирующие как ее часть (DA), также создают новые угрозы для предприятий и энергосети. Многие компоненты распределительной автоматики (DA), такие как IED, содержат встроенное программное обеспечение и имеют удаленные функции обслуживания, мониторинга и управления. Современные IED-устройства должны быть спроектированы с функциями информационной безопасности, которые, с одной стороны, сделают их надежными и устойчивыми к кибератакам, а с другой стороны, позволят им интегрироваться с системой безопасности, такой как центральный сервер аутентификации, сервер управления сведениями и событиями, важными для безопасности (SIEM) и система управления паролями.

Уязвимость в устройстве IED может стать проблемой, если она будет обнаружена и использована злоумышленниками. В зависимости от характера уязвимости злоумышленник может использовать различные схемы проникновения. Примерами уязвимостей устройства могут быть: обход системы защиты прошивки, пароли по умолчанию, производственные

дефекты, ошибки программирования и конструктивные упущения. Производители IED должны следовать процессу обеспечения безопасного жизненного цикла разработки (SDLC), чтобы создать надежную прошивку и найти ее уязвимости в цикле разработки.

Незащищенные IED, требующие дополнительный шлюз безопасности

Поставщики незащищенных IED должны предоставлять дополнительное устройство, функционирующее как шлюз безопасности. Это требует установки и обслуживания дополнительного шлюза. Следовательно, увеличиваются требуемые капитальные и операционные расходы для создания Системы автоматизации. В целом общая стоимость владения (TCO) распределительной сетью возрастает. Следовательно, интеллектуальные устройства IED следующего поколения должны обеспечивать встроенную информационную безопасность для систем безопасного распределения.

Недостаточная кибергигиена

Взломщик с большей вероятностью получит доступ к распределительным подстанциям с недостаточной базовой информационной безопасностью. Часто организационная информационная безопасность ухудшается из-за плохой кибер-гигиены, например, использование слабого пароля или его отсутствие, отсутствие смены пароля, сегрегация сети, неисправленное программное обеспечение и даже недостаток физической безопасности. Злоумышленники используют плохую осведомленность персонала об информационной безопасности чаще, чем атакуют активы напрямую.

Фишинг и заражение вредоносными программами являются наиболее распространенной точкой входа, используемой злоумышленниками. Настраиваемые атаки «адресный фишинг» могут быть очень эффективными для убеждения получателей в подлинности, чтобы те выдавали свои учетные данные. Как и на примере атаки на информационную безопасность в Украине в 2015 году, успешный адресный фишинг или внедрение вредоносных программ могут обеспечить злоумышленникам пути к корпоративным сетям и системам управления.

Отсутствие персонала, обеспечивающего информационной безопасности

Распределительные сети охватывают большую географическую область, и требуется несколько сотрудников, которые будут безопасно и эффективно управлять энергосистемой. Коммунальные службы продолжают сталкиваться с проблемами при приеме на работу достаточного количеств персонала для обеспечения безопасности системы управления. Это может быть отчасти связано с тем, что безопасность ICS является специализированной областью и мало практикующих специалистов имеют опыт в области информационной безопасности.

АРХИТЕКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Распределительная автоматика (DA) и усовершенствованная распределительная сеть позволяют подстанциям быстро обнаруживать, изолировать и устранять неисправности. На рисунке 1 показан вид инфраструктуры связи в распределительной сети, такой как глобальная сеть (WAN) и полевая сеть (FAN). FAN соединяет интеллектуальные счетчики, реклозеры, зарядные станции для электромобилей общего пользования, солнечные и ветряные электростанции с распределительными подстанциями и/или центром управления. Распределенные полевые устройства обычно оснащены радиосвязью, беспроводной или сотовой связью для передачи данных в точки сбора и, в конечном итоге, обратно в центры управления подстанциями с использованием транзитных коммуникационных сетей. На уровне центра управления может быть реализовано много решений, включая: системы управления распределением (DMS), систему управления данными измерений (MDMS), систему усовершенствованной распределительной автоматики (ADA) и начальный узел инфраструктуры интеллектуальных счетчиков (AMI). Службы безопасности, показанные на рисунке 1, обеспечивают управление доступом, службы каталогов, обнаружение вторжений и управление сведениями и событиями, важными для безопасности, для всей системы распределения.

Для выполнения директив NIS требуется многоуровневая активная стратегия информационной защиты, включающая глубокоэшелонированный подход. Подход «глубокоэшелонированная защита» – это наслоение элементов защиты, позволяющее успешно защитить инфраструктуру несколькими уровнями защиты, которые распределены по всей сети управления. Некоторыми из этих средств контроля защиты являются управление уязвимостями, управление активами, управление пользователями, контроль доступа, защита границ, обнаружение вторжений, эффективное управление инцидентами, планы резервного копирования и планы восстановления.

Антивирусные решения и вайтлистинг помогают сдерживать, обнаруживать или предотвращать распространение вредоносного кода в Центре управления и локальных сетях подстанций. Управление учетными записями пользователей осуществляется в Microsoft Active Directory (AD), а центральная аутентификация, авторизация и учет (AAA) обеспечиваются через сервер службы идентификации удаленных пользователей (RADIUS). Все счетчики и устройства, которые присоединяются к FAN, должны пройти аутентификацию, прежде чем им будет разрешен доступ к системе распределенной автоматики (DAS). Сеть FAN передает учетные данные нового устройства на централизованный сервер службы идентификации удаленных пользователей (RADIUS). Как только устройство аутентифицируется, ему разрешается присоединяться к сети и устанавливать связь с другими узлами.

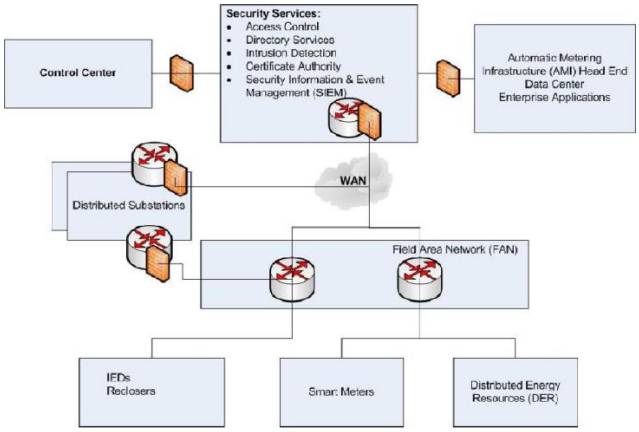


Рис. 1. Схема системы распределенной автоматики.

Весь трафик, исходящий из FAN, должен проходить через высокопроизводительный брандмауэр. Между зонами используется межсетевой экран для фильтрации входящего и исходящего сетевого трафика на основе правил и политик безопасности. Важным аспектом обнаружения угроз является управление сведениями и событиями, важными для безопасности (SIEM). SIEM собирает данные из различных журналов и коррелирует события, происходящие в разных частях сети, чтобы идентифицировать критические инциденты в системе безопасности, обеспечивая более быстрый согласованный ответ. Система обнаружения проникновений в сеть (NIDS) используется в инженерных сетях для анализа сетевого трафика с целью обнаружения и сообщения о вредоносных действиях или нарушениях политики. NIDS использует технику для обнаружения вредоносных действий, основанную на сигнатурах или аномалиях, либо гибридную.

Данные от интеллектуальных счетчиков и устройств автоматизации распределения проходят через общедоступную или частную сеть WAN до того, как попадают в центр управления. Чтобы обеспечить целостность и конфиденциальность данных для интеллектуальных счетчиков и устройств автоматизации распределения, настоятельно рекомендуется зашифровать данные с помощью IPSec или другого метода защищенного туннелирования, если данные проходят через общедоступное или частное транзитное соединение WAN.

ИНТЕГРАЦИЯ IED С СИСТЕМАМИ БЕЗОПАСНОСТИ

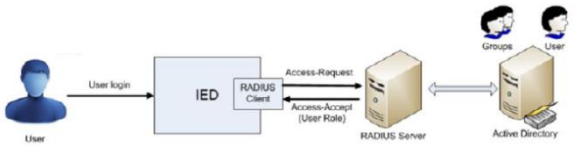
Подстанции тщательно выбирают функции безопасности IED для интеграции с существующими системами безопасности. Подстанции могут использовать различные

инструменты безопасности с функциями безопасности IED для обеспечения глубокоэшелонированной защиты. Если интеллектуальные устройства IED поддерживают встроенные функции информационной безопасности, это устранит необходимость использования любых внешних шлюзов безопасности через географически распределенные контроллеры в распределительных сетях.

Аутентификация и авторизация пользователей

Спецификация IEC 62351-8 определяет управление доступом с использованием ролей (RBAC) для использования в масштабах всей энергосистемы [3]. Настоящий стандарт описывает критерии для определения ролей, назначения ролей и сопоставления ролей и прав в отношении энергосистем. Он также предоставляет обязательный список сопоставлений ролей и прав, которые подстанции могут использовать в своих конфигурациях IED. Управление отдельными пользователями и группами пользователей происходит в Microsoft Active Directory (AD). Благодаря централизованному управлению пользователями, в случае переназначения или передачи, авторизованный электронный доступ отдельного лица может быть легко отменен в AD. Каждому пользователю назначается пароль и роль. Следует использовать надежные пароли в соответствии с правилами сложности паролей.

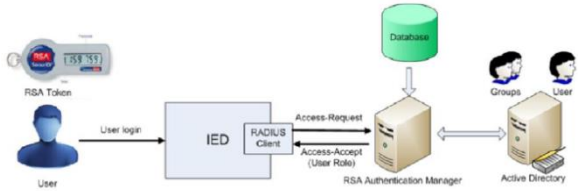
Служба идентификации удаленных пользователей (RADIUS) – это протокол клиент-сервер, который позволяет IED-устройствам безопасно взаимодействовать с центральным сервером для аутентификации пользователей и авторизации их доступа к запрошенным IED-устройствам. RADIUS позволяет предприятиям поддерживать учетные записи пользователей в центральной базе данных, которую могут использовать все IED-устройства, и обеспечивает централизованную аутентификацию, авторизацию и учет для пользователей. Следовательно,



это создает одну точку отказа. Таким образом, для повышения надежности системы рекомендуется использовать основной и дополнительный серверы RADIUS.

Рис. 2: Вход в систему пользователя RADIUS.

На рисунке 2 показано, как пользователь получает доступ к IED-устройству и проходит проверку подлинности и авторизацию на сервере RADIUS. Пользователь просто входит в IED, затем клиент IED RADIUS отправляет запрос доступа серверу RAIDUS. Если имя пользователя установлено и введен правильный пароль, сервер RADIUS возвращает ответ с разрешением доступа обратно в устройство IED. Это сообщение информирует клиента RADIUS в IED о том, что попытка подключения аутентифицирована и авторизована. Основными протоколами



RADIUS являются протокол аутентификации по квитированию вызова (CHAP) и протокол аутентификации по паролю (PAP).

Рис. 3. Двухфакторная аутентификация.

Защищенные протоколы RADIUS представляют собой методы расширяемого протокола аутентификации (EAP), такие как безопасность на транспортном уровне EAP (EAP-TLS), туннельная безопасность на транспортном уровне EAP (EAP-TTLS) и защищенный расширяемый протокол аутентификации EAP (EAP-PEAP).

Двухфакторная аутентификация рекомендуется к использованию ввиду того, что она обеспечивает дополнительный уровень безопасности, а не только пароли. Двухфакторная аутентификация (также известная как 2FA) является подмножеством многофакторной аутентификации. Двухфакторная аутентификация – это метод подтверждения идентификатора пользователя с использованием комбинации двух разных факторов: знание (что-то, что он знает), владение (что-то, что у него есть) и присущность (то, чем он является). На рисунке 4 показан пример системы двухфакторной аутентификации, в которой используется пароль (что-то, что он знает) и аппаратный ключ безопасности (что-то, что он имеет).

Регистрация событий системы защиты

Операторам распределительных сетей требуется повышенная видимость сетевой инфраструктуры для выявления потенциальных вторжений и сбоев в критически важных устройствах и приложениях до их возникновения. Устройства управления сведениями и событиями, важными для безопасности (SIEM) собирают данные из различных журналов и обеспечивают анализ предупреждений безопасности в режиме реального времени. События безопасности, такие как входы и выходы из системы, блокировки пользователей из-за многочисленных сбоев при входе в систему, изменения конфигурации/настроек, обновления прошивки, сбои доступа к серверу, являются примерами действий, которые необходимо отслеживать и предоставлять SIEM для анализа. Если обнаружена аномалия, SIEM можно настроить на оповещение операторов о серьезности вторжения.

IED-устройства могут поддерживать функции как локальной, так и удаленной регистрации. IED-устройства используют протокол системного журнала для отправки событий безопасности в SIEM. Клиент системного журнала будет находиться в каждом устройстве IED, а сервер системного журнала будет встроен в SIEM. Устройства IED могут быть настроены на отправку сообщений системного журнала, чтобы сообщать обо всех событиях и ошибках. Сообщение системного журнала, предоставляемое IED, включает в себя приоритет, уровень серьезности, дату, время и информацию сообщения. Затем SIEM генерирует предупреждения, уведомления и аварийные сигналы в ответ на аномалию, выявленную анализом системного журнала.

Управление привилегиями

Владельцам учетных записей с привилегиями, таким как администраторы, инженеры и операторы, назначаются критически важные привилегии, такие как изменение настроек, обновление прошивки и изменение учетных записей пользователей в распределительных сетях. Учетные записи с привилегиями часто становятся мишенью для взломщиков и внутренних злоумышленников из-за их прав и привилегий. Следовательно, пароли учетных записей с привилегиями необходимо регулярно менять и хранить в надежных хранилищах. Управление привилегированными пользователями (PIM) – это область управления идентичностью, ориентированная исключительно на привилегированные учетные записи. Пароль по умолчанию в IED должен быть изменен, а пароли локальных пользователей должны регулярно меняться с использованием решения PIM.

СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В постоянно меняющейся среде киберугроз организациям необходимо иметь гибкие и динамичные стратегии информационной безопасности для защиты от развивающихся угроз. С целью предотвращения рисков для информационной безопасности требуются специальные решения по безопасности, надежные IED-устройства, четко определенные процессы безопасности и ориентированный на безопасность образ мышления во всей организации.

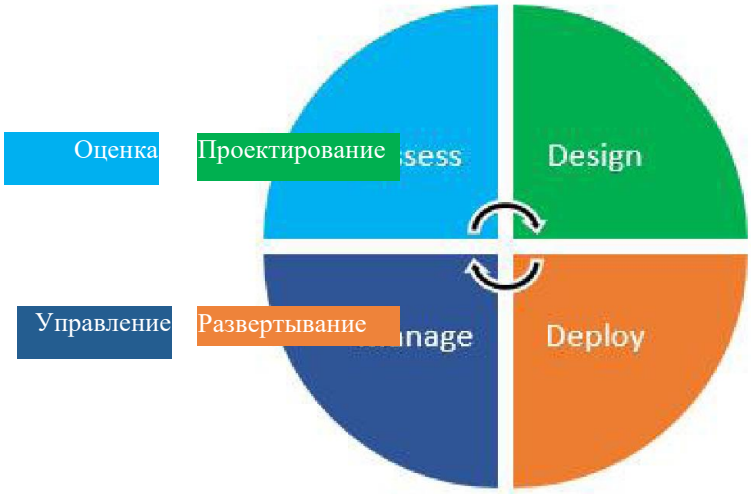


Рис. 4. Четырехэтапный процесс для улучшения состояния системы информационной безопасности.

Успешная стратегия информационной безопасности должна учитывать всех три основополагающих элемента: Люди, процессы и технологии. Сотрудники могут создавать один из самых серьезных рисков для информационной безопасности. Кибератаки будут специально нацелены на сотрудников как фокус атаки, основанный на недостатке знаний о передовых методах обеспечения безопасности и базовых правилах кибер-гигиены. Тем не менее, при условии хорошей подготовки в области информационной безопасности, они также могут стать «социальным межсетевым экраном» и первой линией обороны. Процессы обеспечивают наличие в организации политик и руководств по информационной безопасности для упреждающего предотвращения и быстрого и эффективного реагирования в случае инцидента в системе информационной безопасности. Должны быть предусмотрены соответствующие политики и процессы безопасности для управления подходом организации к обеспечению безопасности сетевых и информационных систем, а также для обеспечения применения надлежащих мер при использовании сторонних услуг и привлечении внешних поставщиков. Существует множество технологий безопасности, которые организация может внедрить для наслаивания защиты. Но крайне важно сначала выявить существующие бреши в безопасности, а затем выбрать средства обеспечения безопасности на основе их способности интегрироваться в существующую систему.

Как показано на рис. 3, организации могут использовать четырехэтапный процесс, чтобы улучшить состояние информационной безопасности. Первым шагом является понимание текущего состояния безопасности системы, выявление существующих мер по смягчению последствий, слабых мест и рисков в системе безопасности. Следующим шагом является определение мер по снижению риска и разработка архитектуры безопасности для предотвращения рисков для информационной безопасности. Третий шаг заключается в развертывании утвержденных и проверенных решений по обеспечению безопасности для улучшения состояния безопасности системы. В качестве последнего шага система должна управляться в течение срока службы системы с необходимыми исправлениями и обновлениями.

Стратегия информационной безопасности состоит из технических и организационных требований. Некоторые из организационных элементов – это управление, процесс управления рисками, цепочка поставок и обучение персонала. В качестве технических средств контроля предприятия должны развертывать решения по обеспечению безопасности для управления уязвимостями, активами, пользователями, контроля доступа, обнаружения угроз, защиты границ, обнаружения вторжений и резервного копирования системы. Эти системы обеспечения безопасности, сетевые устройства, инженерные рабочие

станции и устройства IED должны постоянно обновляться с необходимыми исправлениями и обновлениями, чтобы поддерживать уровень безопасности.

ЗАКЛЮЧЕНИЕ

Распределительные сети превратились в цифровую инфраструктуру, которая все больше опирается на интеллектуальные электронные устройства (IED), использующие методы цифровой связи для мониторинга и управления операциями. Но преимущества современных все более цифровых и взаимосвязанных инфраструктур дорого обходятся. Информационная безопасность стала основной проблемой, а кибератаки стали серьезным риском. В результате развития среды киберугроз потребуется критически важная инфраструктура для подготовки многоуровневой стратегии активной защиты киберпространства, включающей современные средства контроля защиты и четко определенные политики в области безопасности в соответствии с директивой NIS. Подстанции могут использовать средства защиты IED с различными защитными системами для достижения необходимой глубокоэшелонированной защиты.

ССЫЛОЧНЫЕ ДОКУМЕНТЫ

[1] Р. М. Ли, М. Дж. Ассанте, Т. Конвей, «Анализ кибератаки на энергосистему Украины», 2019 г. [онлайн]. Доступ:
https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[2] Агентство по обеспечению сетевой и информационной безопасности ЕС, 2019 г. [онлайн]. Доступ: https://www.enisa.europa.eu/topics/nis-directive
[3] IEC 62351-8, Управление энергетическими системами и связанный с ним информационный обмен. Безопасность данных и коммуникаций. Часть 8. Управление доступом с использованием ролей

3.10. КИБЕРБЕЗОПАСНОСТЬ – НЕОБХОДИМОЕ УСЛОВИЕ ЦИФРОВИЗАЦИИ ЭЛЕКТРОЭНЕРГЕТИКИ

Е. Л. ГЕНГРИНОВИЧ
ОАО «Инфотекс»
Российская Федерация

Контактное лицо:

Е. Л. ГЕНГРИНОВИЧ

Evgeny.Gengrinovic@infotecs.ru

Ключевые слова:

Цифровизация, надежность, SCADA, ICS, АСУТП, критическая инфраструктура, киберугрозы, информационная безопасность, системная надежность, технолог, технологический процесс.

ВВЕДЕНИЕ

Цифровизация в электроэнергетике становится необратимым процессом. И функционал релейной защиты и автоматики так же стал частью этого тренда.

Изменения в электроэнергетике, идут такими быстрыми темпами, что времени на подготовку и анализ всех изменений и потенциальных угроз и переподготовку кадров, просто не остается.

Новые технологии и сервисы (возобновляемая энергетика, электромобили, мощные накопители и т. д.) требуют от энергетиков нового качества услуг. Обеспечить их, используя старые технологии управления, невозможно, так же, как и остановить прогресс. В этих условиях необходимо тщательно прорабатывать концепцию обеспечения технического процесса, строить новое дерево отказов, учитывающее особенности работы программного обеспечения, закладывать элементы информационной безопасности уже на стадии проектирования. Вносить изменения в требования по эксплуатации, в том числе к уровню квалификации и количеству персонала, менять процедуры метрологического контроля. То есть в ближайшем будущем изменения должны коснуться всех процессов, связанных с эксплуатацией, контролем и управлением технологическими процессами в энергетике.

Целью данного доклада является формирование понимания важности вопросов информационной безопасности в процессах цифровизации электроэнергетики, степени их влияния на надежность модернизируемых систем, а также адекватности создаваемых новых бизнес-процессов.

ОСНОВНАЯ ЧАСТЬ

Новые технологии и идеи требуют новых бизнес-процессов и стандартов. Одновременно должны меняться методологии тестирования и проверок внедряемых решений, требования к квалификации персонала, меняться алгоритмы управления активами, учитываться новые аспекты, такие, как «ограничение аппетита к риску» – сбалансированность выгод, затрат, надежности и безопасности.

Сложность задачи увеличивается на порядок, если сразу не решить вопросы стандартизации. Прежде всего, это:

- унифицированные протоколы;
- единая модель данных;
- совместимость оборудования разных производителей;
- унификация инженерных инструментов, используемых в процессе эксплуатации;
- рассмотрение ИБ как части модели;
- управление системой;
- управление активами.

Отдельная тема анализа – как информационная безопасность может влиять на надежность технологических процессов. Необходимо прояснить ряд аспектов, например:

- доступность: можно ли получить данные?
- целостность: корректны ли представленные данные?
- конфиденциальность: данные доступны только для уполномоченных лиц/систем?

При этом не все компоненты интеллектуальной сети имеют объективно одинаковый уровень требований к ИБ. Так как ключевой фактор – это общая надежность энергосистемы, то решения не всегда лежат в области ИТ, например, изменение конфигурации интеллектуальной сети может привести к снижению требований к ИБ отдельных компонент.

Если рассматривать вопросы ИБ, с точки зрения сохранения функциональной надежности, то существенную роль начинает играть корректно подготовленная «Промышленная модель угроз и нарушителя», направленная, в первую очередь на сохранение работоспособности техпроцесса, а не сетей передачи данных и вычислительных средств, как в классическом ИТ.

Политика ИБ формируется на основе решаемых бизнес-задач и соответствующего им госрегулирования, важную роль играет моделирование и симуляция (цифровые двойники), анализ больших данных, в том числе по сетевым аномалиям, уровня квалификации персонала ИБ. Технологии, сами по себе, могут обеспечить только 50% ИБ, вторая часть – это наличие квалифицированного персонала. На этом фоне существенную роль начинают играть правильно выстроенные процессы подготовки персонала, дефицит которого, на сегодняшний день, по международным оценкам, составляет до 70% в области ИБ в целом, не говоря уже о специалистах, сфокусированных на электроэнергетике.

Очень важная тема – периодические независимые аудиты КИИ, позволяющие выявить «слабые» места. Перенос на российскую регуляторную почву, наиболее распространенных западных технологий защиты данных, таких, как TLS и VPN.

Понимая данные тенденции, компания «Инфотекс», помимо того, что предлагает конкретные продукты и сервисы для повышения информационной безопасности критической инфраструктуры, активно работает в направлении обогащения Заказчиков знаниями и компетенциями, в части повышения уровня квалификации персонала ИБ Заказчика. Работа ведется одновременно по нескольким направлениям. В учебном центре «Инфотекс» разработаны и согласованы ФСТЭК курсы по переподготовки персонала по информационной безопасности. Обучение организовано, в том числе с отработкой практических навыков на киберполигоне Ampire. Киберполигон Ampire, также предлагается как отдельный продукт. Он был разработан с использованием навыков и опыта дочерней компании ОАО «Инфотекс» – «Перспективный мониторинг». Первый релиз продукта состоялся в сентябре 2019 года. В ноябре запущен в промышленную эксплуатацию в одном из московских университетов. Сейчас ведутся переговоры с рядом российских и зарубежных заказчиков.

Киберполигон обеспечивает построение «цифровых двойников» корпоративной сети и центра мониторинга информационной безопасности заказчика, включая специфические компоненты, например, сегменты СКАДА/АСУТП. Также базовыми компонентами продукта являются автоматический генератор компьютерных атак и набор шаблонов обучающих сценариев. Таким образом, специалисты заказчика получают уникальную возможность безопасной отработки практических навыков обеспечения информационной безопасности, на инфраструктуре практически полностью идентичной той, за эксплуатацию которой они отвечают. Киберполигон позволяет значительно упростить процедуру организации и проведения киберучений, теперь уже нет необходимости останавливать технологические процессы или ограничивать себя жесткими временными рамками ремонтной заявки. Отрабатывая до автоматизма навыки, специалисты также получают возможность выстраивать командную работу, осуществлять делегирование, испытывать новые технологии и бизнес-процессы. В тесном взаимодействии с Центром НТИ МЭИ идет подготовка интеграции в цифровую модель корпоративной сети, как ЦПС в целом, так и цифровых терминалов РЗА различных производителей. Интеграция обеспечивается путем эмуляции работы устройств, либо включением в модель киберфизических элементов, в зависимости от решаемой задачи. Пока основной интерес проявляют высшие учебные заведения, подготовка молодых кадров с практическими навыками работы на тренажере, существенно повышает ценность выпускников профильных специальностей на рынке труда. Будущее за корпоративными заказчиками. «Цифровые двойники» и так уже являются трендом в развитии технологий, поэтому их применение в развитии защищенной информационной инфраструктуры будет вполне естественным и позволит оптимизировать многие эксплуатационные бизнес-процессы.

Другое важное направление создание корпоративных центров ГОССОПКА. «Перспективный Мониторинг» уже в течение ряда лет предлагает заказчикам создание подобных центров «под ключ» или как услугу от сервис-провайдера в своем лице. В зависимости от уровня зрелости собственных служб ИБ, заказчик принимает решение об

использовании первого или второго варианта. В обоих случаях свою задачу «Перспективный Мониторинг» видит в защите интересов клиента и развития у него собственных компетенций.

Если, вкратце, остановиться на предлагаемых компанией «Инфотекс» инструментах, то здесь в первую очередь стоит упомянуть реализацию TLS на российских алгоритмах и ViPNet платформу, позволяющую построить симметричную VPN сеть с конфигурацией практически любой сложности.

TLS позволяет обеспечить:

- защищенный удаленный HTTPS-доступ к ресурсам (обратный прокси-сервер);
- аутентификацию по сертификатам ключей проверки электронной подписи;
- работы с пользователями, обладающими сертификатами ключей проверки электронной подписи, изданными различными удостоверяющими центрами;
- режимы односторонней и двусторонней аутентификации;
- поддержку политик разграничения доступа;
- автоматическое поддержание актуальности списков аннулированных сертификатов (CRL);
- поддержку кластера с балансировкой нагрузки за счет внешнего балансировщика.

ViPNet-платформа за счет симметричного шифрования со специальной схемой управления ключами обеспечивает конфиденциальность потоков данных, высокую производительность и низкое энергопотребление, а также высокую пропускную способность. Гибкое подключение в доверенную инфраструктуру территориально распределенных объектов производственной инфраструктуры, внутреннее решение проблем конфликтов локальных IP адресов обеспечивает переносимость инфраструктуры как между локальными дата центрами, так и в облачную инфраструктуру.

Уникальным на российском рынке, является серия продуктов SIES, представляющая собой криптографический SDK, который производители функционального оборудования могут использовать в своих продуктах, не погружаясь глубоко в вопросы криптографии. ПАК SIES, в том числе, в ряде случаев, снимет вопросы необходимости взаимодействия с Регуляторами для конечного производителя функционального оборудования.

ЗАКЛЮЧЕНИЕ

Вопросы ИБ должны стать неотъемлемой частью процесса цифровизации в электроэнергетике от стадии формирования требований к архитектуре до вывода решений из эксплуатации. Грамотное формирование и совершенствование ИБ-политик позволит гарантировать не только сохранение уровня надежности технологических процессов, но и в ряде случаев его значительно повысить.

3.11. АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ НОРМАТИВНОЙ БАЗЫ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

Д. И. ПРАВИКОВ
РГУ нефти и газа (НИУ) им. И. М. Губкина
Российская Федерация

Контактное лицо:

Д. И. ПРАВИКОВ

dip@gubkin.pro

Ключевые слова: киберзащита систем промышленной автоматизации, кибератаки на электросети, требования к системам киберзащиты**.**

ВВЕДЕНИЕ

В последнее время в среде экспертов все более активно обсуждается вопрос о кибербезопасности систем электроснабжения различного уровня. Увеличение степени автоматизации и информатизации систем управления энергообеспечением с одной стороны, и, с другой стороны, практически полная зависимость всей остальной критической инфраструктуры от стабильности и качества электропитания, приводят к необходимости формирования повышенных требований по обеспечению кибербезопасности в указанной сфере.

Вместе с тем, в работах отечественных исследователей отмечается, что в системах киберзащиты критическим параметром является время от момента начала атаки до момента ее парирования и восстановления работоспособности управляемой системы.

Если исходить из существующих нормативных документов и экспертных отчетов, то можно отметить следующие разнонаправленные подходы к требованиям времени выявления компьютерного инцидента в автоматизированных системах управления (включая время на его реагирование) между требованиями по категории электроснабжения, временем на восстановление после кибератаки и требованиями по защите значимых объектов критической информационной инфраструктуры.

Так, в соответствии с требованиями для объектов электроснабжения первой категории перерыв может быть не более времени переключения автомата (0,4с - для напряжения 380В по ПУЭ).

Вместе с тем, в соответствии с Постановлением Правительства Российской Федерации от 28 октября 2009 г. № 846 «Об утверждении Правил расследования причин аварий в электроэнергетике», решение о проведении расследования принимается не позднее 24 часов с момента получения органом федерального государственного энергетического надзора информации об аварии, а само расследование проводится в течение 20 дней с момента принятия решения о расследовании.

В соответствии с экспертными оценками, изложенными, в частности, в докладе Global Threat Report 2019[1], выделяется параметр «время прорыва», который в целях обеспечения безопасности преобразовывается в правило 1–10–60 (1 минута на обнаружение вторжения, 10 минут на расследование и 1 час на отражение и исправление ситуации).

В соответствие с приказом ФСТЭК России от 25 декабря 2017 г. № 239 требования к времени реагирования на внештатные ситуации не предъявляется.

Таким образом, проблема заключается в фактическом отсутствии согласованных требований по времени реагирования на компьютерный инцидент в нормативной базе российских регуляторов с учетом существующего российского и международного опыта.

Исходя из изложенного, представляется целесообразным обеспечить согласование требований по реагированию на инциденты информационной безопасности, учитывающее фактор времени в системах непрерывного функционирования, примером которых могут служить системы электроснабжения объектов особой группы первой категории.

ОСНОВНАЯ ЧАСТЬ

Для определения степени актуальности решаемой задачи обратимся к мнению экспертов. По данным, приведенным в докладе Hybrid Conflict Neither war, nor peace, подготовленном Bianca Torossian, Lucas Fagliano и Tara Görder, число кибератак на критическую инфраструктуру государств резко возросло за последнее десятилетие. «Кибератака на критическую инфраструктуру – это раскрытие или уничтожение или получение несанкционированного доступа к системам, которые обеспечивают продовольствие, воду, энергию, транспорт, связь или здравоохранение. Примеры таких атак включают кибератаку 2012 года на Саудовскую национальную нефтяную компанию Saudi Aramco и две атаки, совершенные в 2015 году: атаку вымогателей WannaCry на Национальную

[1] https://www.africacybersecurityconference.com/document/CrowdStrike_GTR_2019.pdf

службу здравоохранения Соединенного Королевства и атаку на украинскую энергетическую распределительную компанию».

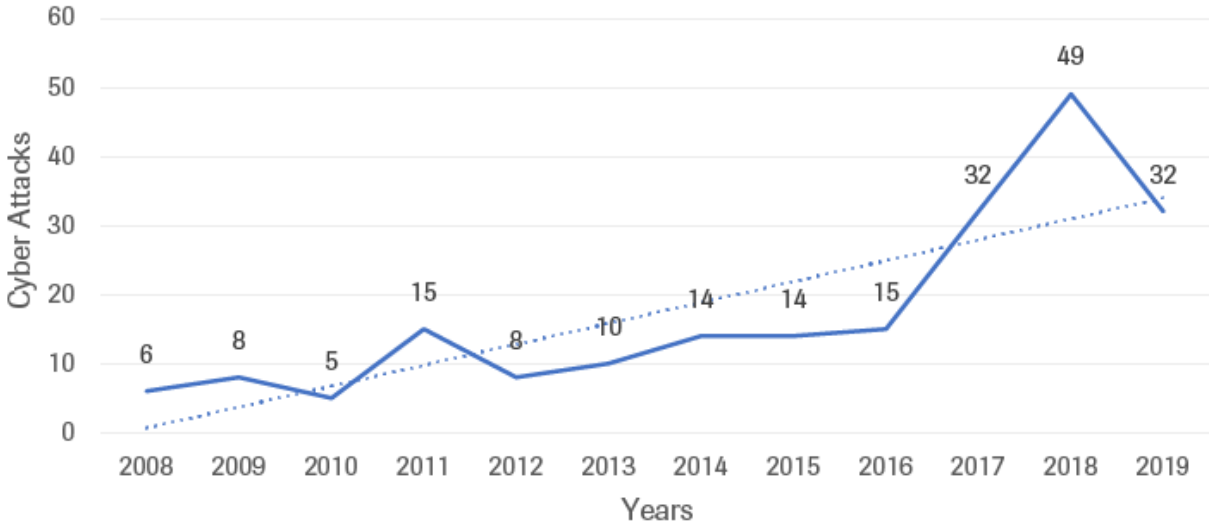


Рис. 11. Количество кибератак на критическую инфраструктуру.

Исходя из представленных данных, объекты электроэнергетики могут являться целью проведения в отношении них кибератак.

В соответствии с существующими правилами для особой группы первой категории объектов электроснабжения предусматривается две независимых линии электропитания (для удобства дальнейшего изложения первой и второй), дополненных третьим взаимно независимым источником, реализованным, как правило, в виде дизель-генератора или другого генерирующего устройства. Исходя из общих соображений, можно предположить следующий обобщенный алгоритм срабатывания систем резервирования.

В штатном режиме функционирует первая линия электропитания.

В случае потери питания по первой линии срабатывает автоматика переключения, и снабжение потребителя переводится на вторую линию. На первой линии ведутся восстановительные работы.

В случае восстановления нормальной работоспособности первой линии она становится резервной, а штатное снабжение ведется по второй линии.

Если до момента восстановления первой линии на второй происходит сбой, то подключается третий источник электроэнергии, имеющий ограниченный ресурс. В зависимости от ситуации системы, которые запитываются по данной схеме, могут переводиться в режим планового останова.

Для моделирования ситуации возможной кибератаки сделаем следующие допущения. Независимые линии электропитания имеют автоматизированную систему управления технологическим процессом (АСУ ТП), доступную для внешнего нарушителя. Атака считается протяженной по времени, начиная от внедрения в систему и заканчивая выдачей команд по прекращению электроснабжения. Считается, что программное средство скрытого информационного воздействия остается в системе управления и блокирует попытки восстановить электроснабжение как по первой, так и по второй линии. Считается, что кибератака приводит только к отключению электропитания, физические повреждения систем электроснабжения невозможны. Третий независимый источник (дизель-генератор) с точки зрения кибератак неуязвим.

Основным предположением для описываемой модели является допущение, что в случае целевой кибератаки воздействию будут подвергнуты первая и вторая линии электропитания. В результате, при существующем алгоритме функционирования, система практически сразу переключится на третий источник.

Исходя из предложенной модели, алгоритм срабатывания систем резервирования должен быть изменен следующим образом.

В штатном режиме функционирует первая линия электропитания.

В случае потери питания по первой линии, срабатывает автоматика переключения, и снабжение потребителя переводится на третий источник электроэнергии, ресурс которого должен быть рассчитан по схеме, изложенной ниже.

Инициируется выявление возможного факта кибератаки. Если в ходе расследования, время которого ограничивается принудительно, данный факт не подтверждается, считается, что сбой был вызван причинами, не связанными с кибератакой. Осуществляется переход на вторую линию электропитания. На первой линии ведутся восстановительные работы, восстанавливается ресурс третьего источника электроэнергии.

Дальнейшее функционирование ведется по схеме, описанной выше.

Если в ходе расследования выявляется факт кибератаки, то:

а) на первой линии фиксируются цифровые следы, связанные с функционированием программного средства скрытого информационного воздействия;

б) проводится анализ уязвимостей системы управления первой линии;

в) программно-аппаратная среда восстанавливается с эталонной копии;

г) системы управления второй линией анализируются на предмет наличия следов возможного вторжения;

д) выявляются и нейтрализуются уязвимости системы защиты для обеих линий.

Если все пять шагов реализованы за время, меньшее, чем время работы третьего источника, то происходит переключение электроснабжения на первую линию.

Если для указанных шагов требуется время, большее, чем время работы третьего источника, то в случае отсутствия следов вторжения в системах управления второй линии происходит переключение на нее. Восстанавливается ресурс третьего источника, продолжается расследование компьютерного инцидента.

Вернемся к вопросу обсуждения времени реагирования на инцидент. В своем докладе на «SOC форуме 2019» представители СО ЕЭС привели следующие цифры: «на головном SOC компании осуществляется обработка порядка 1 000 000 000 событий за сутки, по результату которой создается до 30 кейсов в сутки. Среднее время обработки кейса (фактически инцидента) за 2018 год составило 7,5 часов».

Таким образом, имеющаяся практика расследования инцидента не может считаться удовлетворительной по времени, особенно, если речь идет о прекращении электроснабжения населения и объектов критической инфраструктуры.

ЗАКЛЮЧЕНИЕ

Учитывая изложенное, представляется целесообразным разработать проект требований к системам киберзащиты критической информационной инфраструктуры, обеспечивающей защиту от кибератак в условиях крупномасштабного конфликта, их парирование и восстановление. С учетом того, что построение таких систем возможно только с применением искусственного интеллекта, рассмотреть возможность внесения дополнений в Национальную стратегию развития искусственного интеллекта на период до 2030 года, утвержденную Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

3.12. РАЗРАБОТКА МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ РЗА. ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ К ПРОЦЕССУ РАЗРАБОТКИ

А.А. ЛАРЮХИН
ООО «Интеллектуальные Сети»
Российская Федерация

Ключевые слова:

А.А. ЛАРЮХИН

laruhin@igrids.ru

Ключевые слова:

РЗА, безопасная разработка, информационная безопасность, средства разработки.

ВВЕДЕНИЕ

Одним из ключевых трендов 2019 года стал процесс цифровизации энергетики и промышленности. Для отрасли релейной защиты и автоматики это выразилось, прежде всего, в драматическом усложнении программной части микропроцессорных устройств РЗА. Современные отраслевые требования уже давно вышли за рамки только защиты от аварийных либо аномальных режимов работы электрооборудования. Обыденностью стало рассмотрение устройств РЗА как полноценных участников обмена потоками данных в рамках интегральных автоматизированных информационных систем, выполняющих функции АСУ ТП.

Современное развитие устройств РЗА и в целом промышленных интеллектуальных устройств привело к появлению неизбежной проблемы обеспечения информационной безопасности. У данной проблемы существуют два пути решения, которые не являются взаимоисключающими: создание безопасных систем и создание безопасных компонентов.

В данной работе не будет рассматриваться создание безопасных систем, а всё внимание будет уделено созданию безопасных компонентов в аспекте обеспечения безопасности интеллектуальных устройств РЗА.

На сегодняшний день государственное регулирование в Российской Федерации в части создания «безопасных компонентов» представлено только для средств защиты информации через процедуры сертификации ФСТЭК России. По всей видимости, для стимуляции разработчиков ПАО «РОССЕТИ» апеллирует именно к этим процедурам в своём распоряжении [1]. Таким образом, интеллектуальные устройства РЗА выступают в роли средств защиты информации.

Процесс сертификации задаёт ряд требований к сертифицируемому продукту: требования к функциям безопасности, требования к качеству кода и требования к производству и поддержке. Темой данной статьи является рассмотрение аспектов требований к производству и поддержке программного продукта, которые в значительной мере пересекаются с понятием безопасной разработки, ранее обозначавшимся термином «безопасного жизненного цикла» (SDL).

Аспекты безопасной разработки стали объектом внимание исследователей ещё с начала XXI века в связи с интенсивным развитием сферы информационных технологий, но сконцентрированы были по большей части на обеспечении качества исходного кода и покрытия тестированием.

На момент выпуска распоряжения 282р ПАО «РОССЕТИ» требования к производству и поддержке задавались ГОСТ Р ИСО/МЭК 15408-3-2013 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ». Данный стандарт содержит перечень требований доверия – обобщённого описания наборов конкретных требований к документации, процедурам и мерам, необходимым для поддержания безопасного жизненного цикла программного продукта.

По логике применения стандарта необходимо выбрать набор требований доверия для программного продукта на этапе создания задания по безопасности и в дальнейшем его придерживаться. Тем не менее, требования доверия были сформулированы таким образом, чтобы не поставить разработчика в жёсткие рамки, что приводило к затруднениям в их применении: необходимо было переформулировать требования для конкретного продукта.

В 2018 году ФСТЭК России выпустил в замену данного стандарта «Требования по безопасности информации», утвержденные приказом ФСТЭК России от 30 июля 2018 г. № 131 [2]. В данном документе использован опыт разработки профилей защиты и внедрения требований доверия, что позволило провести более строгую группировку отдельных требований, а также изложить их более понятным языком.

Вторым важным стандартом в вопросе безопасной разработки является ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». Это обобщенное изложение требований разработки, основанное на понятии жизненного цикла программного обеспечения.

Применение как общих требований безопасной разработки, так и требований доверия в том или ином виде выявило целый ряд проблем в процессе внедрения:

- разработчик на своём уровне не мыслит категориями жизненного цикла, концентрируясь на процессах;
- внедрение безопасной разработки происходит уже на этапе существования готового продукта, а не при проектировании продукта с ноля, как предполагают требования;
- требования безопасной разработки, по сути, приходят на замену неписанных процессов существования продукта, таких как тестирование и поддержка.

Задачей данной статьи является рассмотрение проблемных аспектов внедрения безопасной разработки при создании безопасных интеллектуальных устройств РЗА.

ОСНОВНАЯ ЧАСТЬ

При рассмотрении проблем безопасной разработки и создаваемых в связи с этой задачи документов важно отметить, что оценкой документации и реализованных процессов занимается аккредитованная лаборатория, участвующая в процессе сертификации. Тем не менее, разработка необходимой документации остаётся задачей разработчика микропроцессорного устройства РЗА.

В соответствии со сложившейся практикой категорирования объектов электроэнергетической инфраструктуры для всех интеллектуальных устройств будут предъявляться требования 4 уровня доверия. Последовательно рассмотрим эти требования, в чём нам поможет открытая публикация фрагмента «Требований по безопасности информации», опубликованного на сайте ФСТЭК России.

При изучении требований доверия, разработчик вначале сталкивается с требованием создания модели безопасности средства защиты информации. Под моделью безопасности понимается формальное описание потоков информации и правил управления доступом [3]. Данное простое описание скрывает за собой необходимость разработки абстрактного математического описания системы, выполненного на основе задания по безопасности и проектной документации.

При этом, как правило, разработчик не обладает ни опытом, ни компетенцией в разработке моделей безопасности, часто даже не вполне представляя правильного названия политики управления доступом реализована в его изделии. Это влечёт за собой необходимость найма стороннего исполнителя и трансляции замечаний и уточнений между тремя частниками процесса: исполнителем, разработчиком и лабораторией.

Далее перед разработчиками встают требования к архитектуре, функциональной спецификации и проектированию средства. Их разумно объединить, так как требования покрываются разработкой описания архитектуры и функциональной спецификацией средства.

Эти требования порождают две крупные проблемы перед разработчиком сразу две значительные проблемы.

Первой проблемой является понимание структуры и содержания ожидаемых документов. Сфера информационной безопасности обладает удивительной способностью создавать терминологическую путаницу для программистов, например, под функциональной спецификацией в данном случае понимается перечень функций безопасности, изложенный изначально в задании по безопасности – на этапе разработки функциональной спецификации разработчик в ходе консультаций с лабораторией получает правильное понимание задачи.

Второй проблемой проектирования средства является тот факт, что разработчик вынужден работать с уже готовым исходным кодом, по сути, документируя его. В этой ситуации разработчик вынужден кропотливо изучать и описывать имеющийся у него код, как правило, имеющий значительную историю разработки.

Обе эти проблемы приводят к значительным трудозатратам и необходимости долгосрочного планирования в разрезе работы инженеров-программистов. Безусловно, требования к проектированию в свою очередь способны значительно повысить качество исходного кода и выявить возможные проблемные и потенциально уязвимые конструкции исходного кода, но дело затрудняется ограниченными сроками работ и необходимостью менять подход к управлению разработки.

Дальнейшие требования к среде разработки и управлению конфигурации во многом пересекаются с требованиями системы менеджмента качества: необходимость детального описания среды разработки (от персональных компьютеров и периферийного оборудования до программных сред разработки и хранения) и необходимость детального описания методов управления не только исходным кодом, но и всей проектной документацией по умолчанию, являются актуальными задачами для любой современной компании. Проблемой является то, что, помимо непосредственно разработки и документирования кода изделия, разработчик, в частности инженеры-программисты, должен уделить внимание совместной работы с отделом управления качества для актуализации, а иногда и разработки таковой документации. Это тем более усложняется тем, что для разработки микропроцессорных устройств РЗА фокус внимания разработчика, как правило, смещён в сторону аспектов физического существования устройства РЗА – большая часть документации СМК предприятия касается именно готового изделия, его физических компонентов и сопутствующей технической документации.

Требования к разработке документации по безопасности разработки средства в свою очередь касаются мер безопасности, внедренных на самом предприятии. По большей части современные предприятия уже реализуют значительные меры по защите конфиденциальности и целостности исходного кода и документации изделий, но будет справедливым отметить, что такие меры не всегда подвергаются строгому документированию. В данном случае разработчик сталкивается с необходимостью уточнения принятых мер, создания строго их описания и проверки их исполнения. В ряде случаев это требование приводит к необходимости изменения подхода к мерам безопасности: изменение конфигурации корпоративной ЛВС, закупка дополнительного ПО и оборудования, изменения регламентов.

Раздел требований к тестированию становится очередным источником ряда проблем для разработчика. Если необходимость полного документирования процесса тестирования уже выглядит привычно на фоне вышеизложенного, то конкретные требования по тестированию, ссылающиеся на конфиденциальную методику тестирования вносят дополнительные сложности.

Под испытаниями по выявлению уязвимостей и недекларированных возможностей средства понимаются три вида испытаний:

- статический анализ исходного кода;
- фаззинг-тестирование;
- тестирование на проникновение.

Статический анализ исходного кода на сегодняшний день является хорошо изученным и описанным методом испытаний программных продуктов. В данном случае для разработчика проблемой становится только выбор подходящего инструмента и его приобретение.

Фаззинг-тестирование, в свою очередь, на сегодняшний день относительно неплохо проработано для веб-приложений и ряда приложений, работающих в распространённых средах, таких, как операционные системы Windows. В случае микропроцессорных устройств РЗА основную сложность вызывает проведение автоматизированных тестов и анализ покрытия исходного кода тестами. Перед разработчиком стоит нетривиальная задача – инструментирование исходного кода микропроцессорного устройства РЗА и создание на основе устройства РЗА стенда таким образом, чтобы это позволило проводить более 1 000 тестов, анализируя прирост покрытия кода и результаты исполнения кода в каждом тесте.

Тестирование на проникновение значительно усложняется для разработчика необходимостью специальных компетенций в сфере информационной безопасности – знания методов эксплуатации уязвимостей программного обеспечения, что создаёт кадровую проблему. Одним из решений такой кадровой проблемы является привлечение сторонних специалистов к проведению тестирования, что также создаёт ряд документальных сложностей.

Отдельной значительный пласт задач встаёт перед разработчиком в связи с требованиями к поддержке безопасности средства. Нетрудно заметить, что требования пересекаются с концепцией СМК. В данном случае требования к поддержке безопасности средства объединяют под собой также ранее упомянутые требования к тестированию и разработке. Сложностью является необходимость проработки всех сценариев, связанных с выявлением уязвимости в программном коде микропроцессорного устройства РЗА. Для примера на рис. 1 приведена EPC-диаграмма процесса сбора сведений об ошибках и уязвимостях, разработанного в ООО «Интеллектуальные Сети».

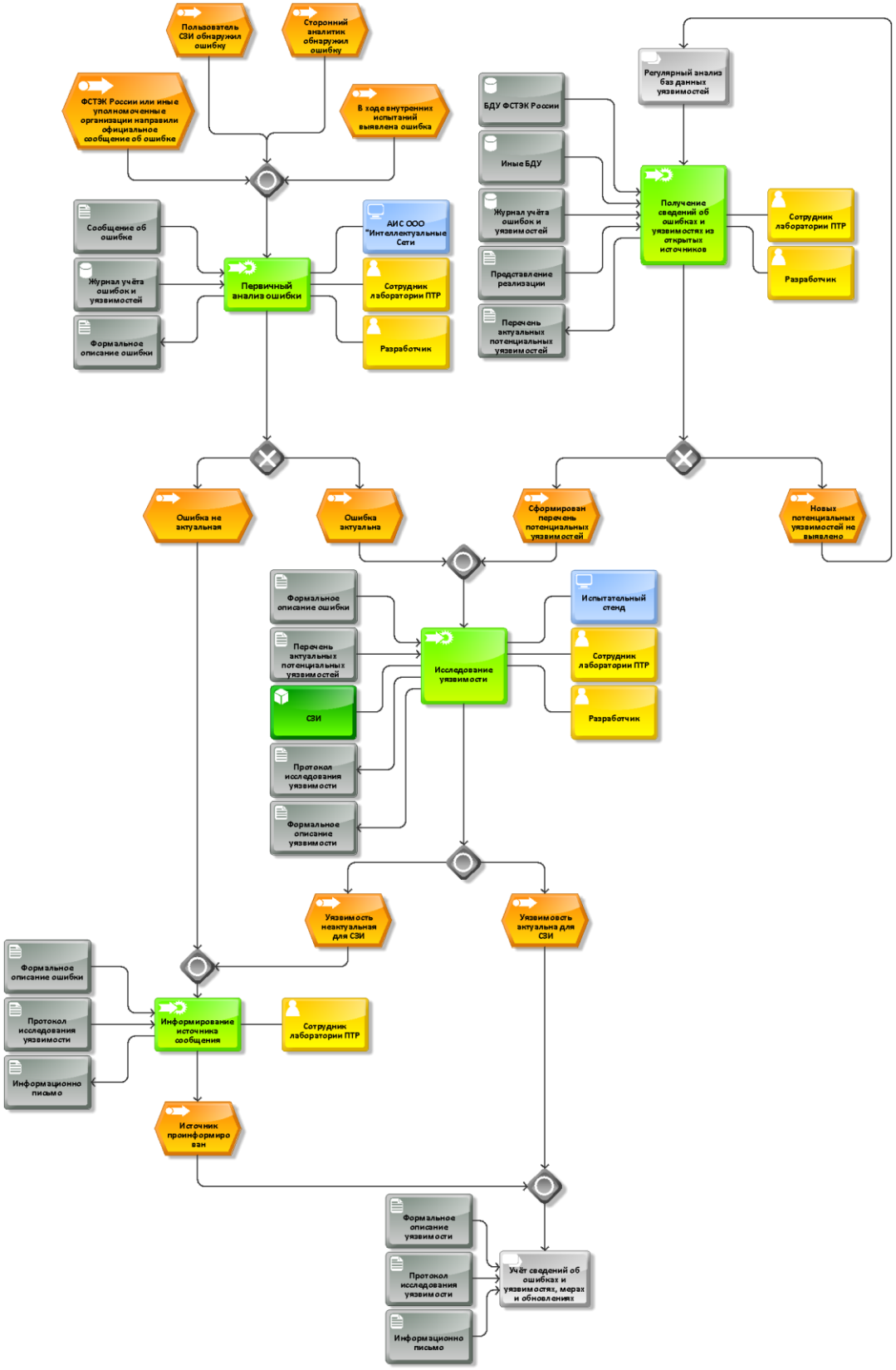


Рис. 1. EPC-диаграмма процесса сбора сведений об ошибках и уязвимостях, разработанного в ООО «Интеллектуальные Сети».

Таким образом, перед разработчиком стоит задача разработки детальной инструкции действий персонала по поддержке безопасности средства, в которой необходимо учесть все возможные события и предусмотреть все результаты проводимых работ.

При этом требования устанавливают жесткие временные рамки на разработку и доведение до пользователей компенсирующих мер – 48 часов с момента обнаружения недостатка, и разработку и поставку обновлений – 60 дней с момента обнаружения недостатка.

Это ставит перед разработчиком необходимость постоянного поддержания готовности отделов разработки и тестирования и непрерывного контроля за разработанным программным кодам микропроцессорного устройства РЗА. При этом необходимость регулярного тестирования микропроцессорного устройства РЗА как в хоте регулярного поиска уязвимостей, так и в случае обнаружения недостатка возвращает нас к проблеме специальных компетенций в вопросах фаззинг-тестирования и тестирования на проникновения, что в свою очередь означает либо необходимость регулярного привлечения сторонних специалистов, либо расширения штата.

ЗАКЛЮЧЕНИЕ

Рассмотренные в статье проблемы внедрения безопасной разработки показывают, что на сегодняшний день перед разработчиком встаёт целый ряд отдельных затратных по ресурсам и времени задач. Все эти задачи выражаются в необходимости изменения процесса разработки на более строгий и документированный, с детальным описанием каждого шага деятельности. При этом перед разработчиком стоит задача получения целого ряда специфических компетенций, связанных с информационной безопасностью. Таким образом, означенные проблемы в значительной степени заставляют разработчика рассматривать своё изделие как IT-продукт.

Безусловно, рассмотренные требования представляются разумным способом повышения качества программного кода микропроцессорных устройств РЗА, но насколько оправдана строгость данных требований остаётся открытым вопросом.

ЛИТЕРАТУРА

[35] Распоряжение ПАО «Россети» от 15.11.2018 № 512р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети»

[36] Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 30 июля 2018 г. N 131 https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/2050-vypiska-iz-trebovanij-po-bezopasnosti-informatsii-utverzhdennykh-prikazom-fstek-rossii-ot-30-iyulya-2018-g-n-131

[37] Ерохин, Погонышева, Степченко «Безопасность информационных систем. Учебное пособие» Издательство: Флинта, 2016 г. ISBN: 978-5-9765-1904-6

3.13. «МУЛЬТИШИНА 10G» ЦИФРОВОЙ ПОДСТАНЦИИ – ПОТЕНЦИАЛЬНЫЕ ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ И ВОЗМОЖНОСТИ РАЗВИТИЯ ЦИФРОВОГО ЭНЕРГООБЪЕКТА

М. В. НИКАНДРОВ, А. С. ШЕМЕТОВ

ООО «Интеллектуальные Сети», ПАО «ФСК ЕЭС»
Россия

Контактное лицо:

М. В. НИКАНДРОВ

nikandrov@igrids.ru

Ключевые слова:
Цифровая подстанция, мультишина, информационная безопасность.

ВВЕДЕНИЕ

Ускоренное развитие информационно-коммуникационных технологий, внедрение технологий цифровых энергообъектов предъявляет новые требования к скорости и надежности передачи информации в локальной информационной сети объекта (далее ЛВС). Один из вариантов повышения пропускной способности и оптимизации стоимости локальной сети является применение высокоскоростной «мультишины» на скорости 10 Гбит/с и выше.

Такое решение на 30-50% дешевле применяемых сегодня решений, но потенциально несет в себе риски снижения уровня киберзащищённости.

На практике «мультишины» пока не применяются, в статье описаны результаты расчетов и стендовых испытаний.

ОПИСАНИЕ ПРОБЛЕМАТИКИ

Цифровизация энергетики помимо безусловных преимуществ неизбежно ставит перед нами целый ряд проблем, одной из которых становятся последствия увеличения объёма передаваемой по локальной вычислительной сети информации, и неизбежное усложнение топологии локальных вычислительных сетей.

Переход от классических схем вторичного оборудования электростанций и электроподстанций, в которых информация передавалась посредством дискретных и аналоговых сигналов (что обозначается профессиональным жаргонизмом «по меди»), к чисто цифровой передаче и обработке сигналов посредством современных протоколов, таких как МЭК 61850-9-2, прежде всего, создаёт необходимость создания высокоскоростных, высоконадежных локальных вычислительных сетей. Проблема усугубляется возникновением дополнительных требований, предъявляемых к современным объектам энергетики — это появления и интеграция системы технологического и охранного видеонаблюдения, системы мониторинга оборудования, усложнение систем учета и контроля качества энергии.

На сегодняшний день это приводит к созданию на современных объектах энергетики каскадов косвенно связанных локальных вычислительных сетей, которые выполняют широкий спектр задач обеспечения автоматизации энергоснабжения.

При этом с дальнейшим развитием «цифровой энергетики», а особенно с переходом на технологии Sample Value растут требования к детерминированности времени доставки и объёмам передаваемой информации в локальных сетях объектов энергетики, для выполнения которых требуется наращивать пропускную способность сетевого оборудования и усложнять топологию локальных вычислительных сетей.

Выделение шин для различных данных таких как MMS, GOOSE, SV не приводит к увеличению надёжности так как отказ шины с SV или отказ шины с GOOSE приводит к потере функций РЗА, потеря шины с MMS приводит к потере наблюдаемости и управляемости объекта. Выход любой шины — это недопустимый режим с точки зрения современной ПС. По теории вероятности, чем больше элементов, тем больше вероятность их отказа. Поэтому решения, при которых разделяются данные по разным шинам, – тупиковые и вызваны неготовностью устройств РЗА к работе с сетевыми картами 1 Гбит/с.

Накопленный опыт и исследования позволяют относительно строго ранжировать данные ЛВС в соответствии их критичности для обеспечения функционирования объекта, что наиболее заметно выразилось в рамках обеспечения информационной безопасности объектов критической информационной инфраструктуры, что подводит нас к необходимости уделять внимание информационной безопасности локальных вычислительных сетей объектов энергетики. Если в «классических» схемах вторичного оборудования потенциальный нарушитель должен был получить физический доступ к вторичному оборудованию для нарушения его работы, то на сегодняшний день накоплен достаточно данных, заставляющий рассматривать удалённый доступ к сетям передачи данных

информационной инфраструктуры энергетики как фактическую угрозу стабильности технологического процесса.

Сложившийся на сегодня подход к организации сетей передачи данных объектов информационной инфраструктуры энергетики ставит следующие проблемы:

- критическое значение локальных вычислительных сетей в процессах генерации, передачи и распределения электроэнергии;
- увеличение количества, повышение сложности и стоимости локальных вычислительных сетей;
- затруднение контроля и обеспечения информационной безопасности локальных вычислительных сетей.

Перечисленные проблемы имеют тенденции к дальнейшему нарастанию в связи с дальнейшим усложнением цифровых систем автоматизации энергетики, а значит, их актуальность будет только увеличиваться в дальнейшем.

Как одно из перспективных решений, способных в значительной мере остановить рост стоимости ЛВС, удовлетворяющую возрастающим требованиям, выступает применение высокоскоростной «мультишины» на скорости 10 Гбит/с и выше.

В отличие от уже применяемого подхода, в котором различные процессы автоматизации обеспечиваются физически разделёнными локальными вычислительными сетями, применение высокоскоростной «мультишины» подразумевает создание единой физической локальной сети, в которой для различных процессов автоматизации поддерживаются отдельные виртуальные локальные вычислительные сети (VLAN). Высокая пропускная способность сетевого оборудования позволяет безболезненно поддерживать все необходимые процессы автоматизации, таким образом, данное решение, наоборот, позволит удовлетворять потребности в пропускной способности сетей энергообъекта при ощутимом увеличении количества сетевого оборудования.

ПОЧЕМУ «ГИГАБИТА» УЖЕ НЕ ХВАТАЕТ?

Расчет нагрузки сети для шины процесса может быть оценён по следующей формуле:

$$V = \sum_1^N V_{GOOSE\,i} + \sum_1^N V_{SV\,i}, \qquad (1)$$

где V – нагрузка сети, более, $V_{GOOSE\,i}$ – нагрузка сети единичного устройства, генерируемая GOOSE-сообщениями, $V_{SV\,i}$ – нагрузка сети единичного устройства, генерируемая SV-сообщениями, N – общее количество устройств.

Согласно стандарту СТО 56947007-29.240.10.302-2020 «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС», эмпирические значения нагрузки от потоков SV для типовых шкафов РЗА для 195 потоков РЗА (типовой пример подстанции) составляют 998,4 Мб/с для МЭК 61850-9-2LE либо 670,8 Мб/с для профиля ПАО «ФСК ЕЭС» на базе МЭК 61869-9.

Для аналогичной схемы нагрузка сети, генерируемая GOOSE-сообщениями, составит 128,8 Мб/с.

Таким образом, формула 2 примет значения:

- $V = 1127{,}2$ Мб/с, для МЭК 61850-9-2LE;
- $V = 799{,}6$ Мб/с, для профиля ПАО «ФСК ЕЭС» на базе МЭК 61869-9.

Для оценки стабильности и производительности сети используется коэффициент использования сети, рассчитываемый по формуле:

$$\eta = \frac{V}{V_{max}}, \qquad (3)$$

где η – коэффициент использования сети, V – нагрузка сети, V_{max} – максимально возможная нагрузка сети (для классической сети $V_{max} = 1$ Гб/с).

Подставляя полученные значения в формулу 3 нетрудно убедиться, что для МЭК 61850-9-2LE нагрузка превышает технически возможную, а для профиля ПАО «ФСК ЕЭС» на базе МЭК 61869-9 $\eta = 0{,}781$.

При этом, согласно СТО 56947007-29.240.10.302-2020 «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС» с учетом современного развития промышленных коммутаторов для ПС ЕНЭС максимально допустимый коэффициент использования сети определен в размере 0,75.

Таким образом, в классической схеме цифровой подстанции возникает необходимость искусственного деления шины процесса для обеспечения приемлемой нагрузки на сеть. Использование высокоскоростной «мультишины» на скорости 10 Гбит/с и выше позволит в свою очередь полноценно выстроить процессы автоматизации электроснабжения без поиска компромиссных решений.

ПРОБЛЕМЫ ПРИМЕНЕНИЯ И ПРЕИМУЩЕСТВА «МУЛЬТИШИНЫ»

Усложнение ЛВС и неготовность персонала

Тем не менее, применение высокоскоростной «мультишины» на скорости 10 гигабит/с и выше неизбежно создаёт определённые сложности. Прежде всего, это рост требований к компетенции персонала, как обслуживающего объект энергетики, так и проектирующего сети передачи данных и осуществляющего его пуско-наладочные работы.

Стоит отметить, что уже сегодня оперативный персонал не понимает, как работает ЛВС, для него это «волшебная сеть», соединяющее устройство, поэтому дальнейшее усложнение конфигурации не ухудшает ситуацию, наоборот, понимание единой физической сети с разделением на виртуальные позволит организовать процесс обслуживания шины данных с требуемым качеством и надёжностью.

Вопросы информационной безопасности

Очевидным вопросом к использованию «мультишины» становится обеспечение информационной безопасности. При поверхностном взгляде на ситуацию неизбежным недостатком видится объединение различных объектов информационной инфраструктуры (РЗА, АСУ ТП, АИИСКУЭ, диспетчерское управление, видеонаблюдение) в одну физическую сеть.

При анализе классической схемы цифровой подстанции, построенной согласно СТО 56947007-29.240.10.302-2020 «Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС» [1] очевидно, что наиболее критичными для обеспечения безопасности электроснабжения являются сети, в которые включены устройства РЗА: шина процесса и шина станции. Это значит, что при обеспечении информационной безопасности необходимо наибольшее внимание уделить защите именно этих сегментов.

Опыт проектирование систем обеспечения информационной безопасности указывает, что требования безопасности, предъявляемые различным системам, не имеют принципиальных различий, отличаясь лишь строгостью требований. Подход по ограничению доступа пользователей в сегменты технологической сети передачи данных цифровой подстанции одинаков для всех сегментов, а это, в свою очередь, означает, что их безболезненно можно заменить на виртуальные локальные сети (VLAN) в рамках «мультишины».

Для купирования рисков информационной безопасности предлагается использовать расширенные возможности по управлению информационными потоками и контролю информационного обмена, которые появляются при использовании высокоскоростного интерфейса. В первую очередь это применение технологии RSPAN (Remote Switch Port Analyzer) для увеличения контролирующей возможности объектовых систем обнаружения вторжения. Используя расширенные возможности инжиниринга трафика и RSPAN, мы можем

направлять весь трафик L3 между интеллектуальными устройствами на систему обнаружения вторжения, не используя дорогостоящие брокеры сетевых пакетов, тем самым повышая уровень киберзащищенности на сетевом уровне.

Таким образом мы получаем более эффективную систему безопасности без дополнительного оборудования, что означает за снижение затрат на обязательные сегодня комплексы информационной безопасности.

Вопросы надежности

Надёжность функционирования цифровой подстанции строится на тех же принципах, что и надёжность функционирования классической «доцифровой» подстанции: наиболее критичной системой является РЗА, менее критичной является система АСУ ТП, такие же системы как АИИСКУЭ, видеонаблюдение и подобные рассматриваются как важные, но некритичные для процесса электроснабжения.

Таким образом, вопрос надёжности электроснабжения должен рассматриваться на основании систем РЗА – отказ сетевого оборудование приведёт к нарушению сетевой передачи SV-потоков и GOOSE-сообщений, что потенциально ведёт к отказу РЗА. Из этого следует, что надёжность «мультишины» должна сравниваться с надёжностью шины процесса, как самого критичного компонента.

Для оценки надёжности используется величина: вероятность безотказной работы R(t)– вероятность того, что в пределах заданной наработки отказ объекта не возникнет.

Для шины вероятность безотказной работы может быть грубо рассчитана следующим образом:

$$\tilde{R}_{\text{ш}}(t) = \prod_1^n \tilde{R}_i(t), \qquad (2)$$

где $\tilde{R}_i(t)$ – вероятность безотказной работы одного коммутатора, n – общее количество коммутаторов.

В данном расчёте не учитывается надёжность проводных соединений.

Из формулы 2 видно, что на различие вероятность безотказной работы шины будет влиять количество коммутаторов n и вероятность безотказной работы одного коммутатора $\tilde{R}_i(t)$.

Результаты экспертизы существующих проектов показывают, что общее количество сетевых устройств 10 гигабит/с будет идентично или незначительно превышать количество сетевых устройств шины процесса в классических цифровых подстанциях, а значит, для обеспечения приемлемого уровня надёжности требуются устройства «мультишины», имеющие не меньшую вероятность безотказной работы, что на данном этапе вполне достижимо. Безусловно, более точная оценка надёжности потребует серьёзного исследования как классических схем цифровых подстанций с выполнением детальных расчётов надёжности, так и предлагаемого решения с применением высокоскоростной «мультишины».

Стоимость решения и предложения рынка

На сегодняшний день с развитием цифровых технологий вопрос стоимости оборудования и решений является ключевым. Цифровая подстанция должна в перспективе стать дешевле классической на всем жизненном цикле.

Наименование	**Цена**	**Количество**	**Стоимость, Евро**
Промышленный коммутатор 24*100 мб	4 866,04	4	19 464,16
Промышленный коммутатор 26*1 Гб	6 672,15	2	13 344,29
Промышленный коммутатор 24*1 Гб + 2*10 Гб	6 942,99	2	13 885,99

Табл. 1. Сравнение стоимости «мультишины» и «классических» решений.

Хотя оборудование с поддержкой скоростей 10 Гбит/с дороже, но его требуется практически в два раза меньше. Уже сегодня только экономия на промышленных коммутаторах составляет более 40%, к этому можно добавить экономию на аппаратных частях интеллектуальных устройств, для которых будет достаточно два сетевых интерфейса на 1 Гбит/с, терминалы РЗА, ПАС, ЭОБ оптических ТТ и ТН будут иметь один интерфейса для работы с «мультишиной», а не два и более, что снизит количество портов в ЛВС.

Отдельно стоит обратить внимание на гораздо меньший выбор сетевого оборудования: если для классических технологических сетей передачи данных представлен довольно широкий выбор сетевого оборудования, то использование «мультишины» пока приводит к сужению номенклатуры сетевого оборудования. На сегодня только крупные компании, такие как Siemens, Phoenix Contact и Huawei предлагают промышленные решения на таких скоростях, тем не менее, потенциальная польза решения гарантирует в дальнейшем вовлечение крупных компаний в разработку и производства пригодных к использованию коммутаторов.

ДЕТЕРМИНИРОВАННОСТЬ ДОСТАВКИ

Применение высокоскоростных интерфейсов позволит в ближайшее время перейти к применению Time Sensitive Networking (TSN).

Time Sensitive Networking – стандарт передачи данных в реальном масштабе времени в детерминированных сетях Ethernet. TSN представляет собой набор стандартов, которые обеспечивают обмен стандартизированными сообщениями в обычных сетях Ethernet. По определению Института инженеров по электротехнике и радиоэлектронике (IEEE), TSN представляет собой форму управления сетевым трафиком, которая обеспечивает строго определенное время задержек при передаче. Все устройства в сети TSN должны быть синхронизированы друг с другом от единого эталона времени для поддержания связи в реальном времени. Сети TSN обеспечивают фиксированную гарантированную и своевременную доставку чувствительного к задержкам.

Применение TSN должно позволить гарантировать время доставки критически важных данных для устройств РЗА.

РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

На базе испытательной лаборатории ООО «Интеллектуальные Сети» проведены натурные испытания «мультишины» 10G.

Структурная схема тестового стенда представлена на рис. 1.

ЛВС построена промышленных коммутаторах Phoenix Contact FL EP7428R.

Устройство Siemens SIPROTEC 5 6MU85 представляет собой конвертор аналогового сигнала в SV-поток. К нему подключено устройство PETOM-61 (на схеме не показано) аналоговыми проводами. Устройство генерирует один SV-поток с 80 выборками, VLAN 500 и приоритетом 4. Устройство Siemens SIPROTEC 5 7UT87 подписано на этот SV-поток.

Устройства 6MU85 и 7UT87 синхронизированы по протоколу PTP, источником которого являются часы точного времени ЭКРА СВ-02А.

Устройство PETOM 61850 выдает в сеть потоки с метками VLAN на максимальной возможной скорости интерфейса 1 Гбит/с.

Источник (являющийся одновременно и SCADA-сервером) и приёмник данных подключены к коммутаторам по 10-гигабитному оптическому линку. Соединение между коммутаторами имеет скорость 10 Гбит/с.

Устройство 7UT87 так же передаёт в SCADA систему по протоколу MMS-измерения. Метки VLAN не используются.

После успешной синхронизации по PTP и установления корректного соединения между 6MU85 и 7UT87 (на 7UT87 не должен иметь статус «failure»), на источнике данных запускается передача данных на скорости 10 Гбит/с.

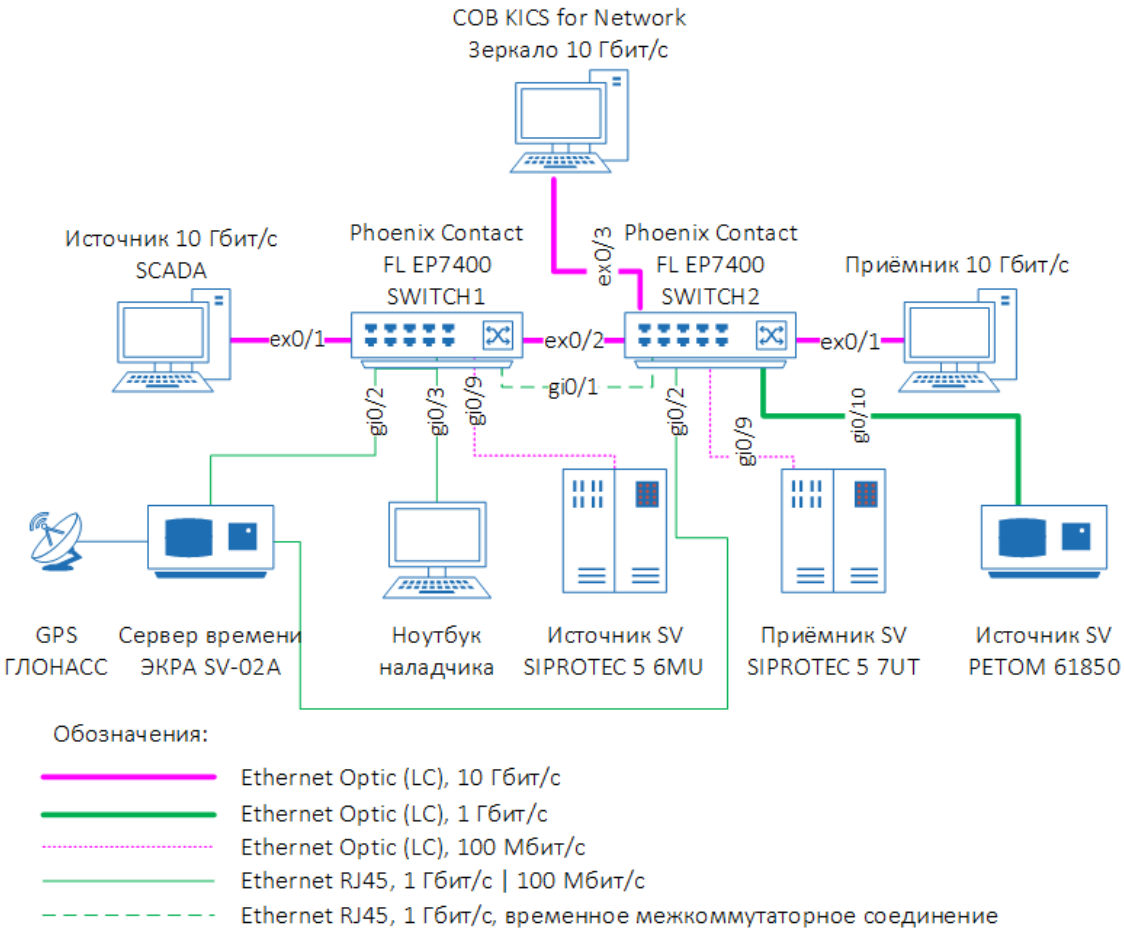


Рис. 1. Структурная схема испытательного стенда.

Загрузка канала на скорости 10 Гбит/с организовывается следующими способами (не одновременно):

- устройство PETOM 61850 выдает в сеть потоки SV (128 и 80 точек на период) с метками VLAN отличными от тестируемой пары терминалов на максимальной возможной скорости интерфейса 1 Гбит/с;
- утилитой iperf3 (на приёмнике iperf3 запускаемой как сервер, а на источнике – как клиент) создавался информационный поток, близкий к максимальному.

В результате тестирования как с обычным приоритетом портов ex0/1, так и с повышенным, скорость передачи составила ~9,35 Гбит/с, и передача между устройствами 6MU85 и 7UT87 не нарушалась, система обнаружения вторжения KICS for Network работала в штатном режиме (использовался RAID 0 на SSD).

ВЫВОДЫ

Таким образом, применение высокоскоростной «мультишины» на скорости 10 гигабит/с и выше позволяет обеспечить следующие преимущества:

- обеспечение высокой надёжности и отказоустойчивости локальных вычислительных сетей энергообъектов, а значит, и обеспечить высокую стабильность автоматизации цифровой энергетики;
- значительно снизить стоимость сетевого оборудования и значительно упростить физическую топологию локальной вычислительной сети энергообъекта;

- повысить наблюдаемость процессов передачи и обработки информации в локальной вычислительной сети энергообъекта, что облегчает и удешевляет создание систем обеспечения информационной безопасности при повышении их эффективности.

3.14. ВОПРОСЫ И РЕШЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ СИСТЕМ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИКИ ЭЛЕКТРИЧЕСКИХ СЕТЕЙ

А.В. ПЕТУХОВ
НТИ Энерджинет, Kaspersky
Россия

Ключевые слова: Kaspersky ICS-CERT, ЦУС

ВВЕДЕНИЕ

Тема информационной безопасности цифровых, автоматизированных и информационных систем электроэнергетики находится в фокусе внимания не только среди специалистов по информационной безопасности, но и правительства, органов исполнительной власти Российской Федерации, а также высшего руководства других государств.

В конце января 2021 года эксперты ВЭФ опубликовали 16-й доклад о наиболее значимых глобальных рисках [2]. Как и последние 5 лет, в числе основных рисков специалисты выделили нарушение киберзащиты.

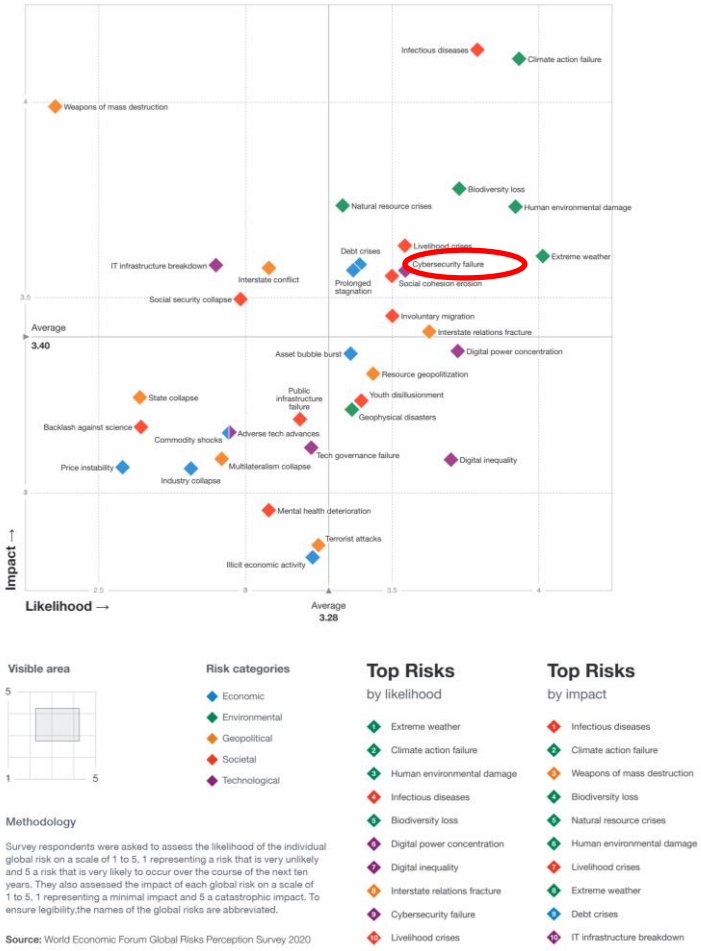


Рис. 12. *Глобальные риски.*

Вместе с тем, согласно аналитическому отчёту «Ландшафт угроз для систем промышленной автоматизации. Статистика за второе полугодие 2020» Kaspersky ICS-CERT [3], на 38,55% анализируемых компьютеров, работающих в промышленной сети, по всему миру хотя бы 1 раз за 2020 год была заблокирована угроза информационной безопасности. То есть

[2] https://www.weforum.org/reports/the-global-risks-report-2021

[3] https://ics-cert.kaspersky.ru/reports/2021/03/25/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/#_Toc66286063

каждый третий компьютер был подвержен воздействию вредоносной программы и кибератаке.

В России этот показатель составляет 39,5%. Стоит отметить, что процент компьютеров в промышленных системах энергетической сферы (по всему миру), на которых были заблокированы вредоносные объекты – 36,9% (рис. 2).

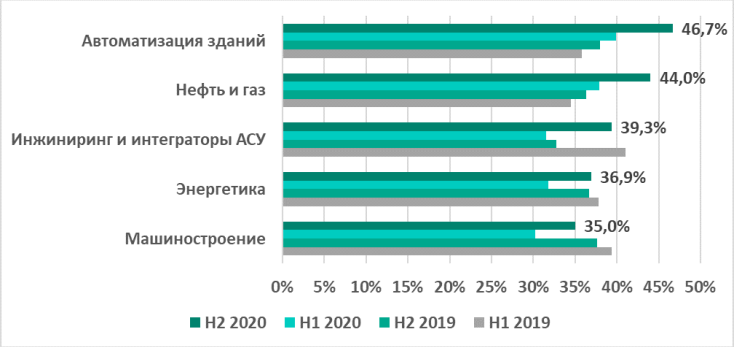


Рис. 2. Процент компьютеров в промышленных системах, на которых была заблокирована угроза информационной безопасности по отраслям.

Рассмотрим современные вопросы обеспечения информационной безопасности цифровых систем релейной защиты и автоматики электрических сетей на обезличенном примере существующей цифровой подстанции (далее ЦПС) 110 кВ.

В состав ЦПС входят следующие устройства.

- Сервер автоматизированной системы управления технологическим процессом (далее – АСУ ТП), предназначенный для:
  - выполнения функций сбора и визуализации информации о работе комплекса интеллектуальных систем релейной защиты и автоматики (далее – ИС РЗА);
  - автоматического сбора и хранения файлов записи осциллограмм аварийных событий, формируемых ИС РЗА.
- Устройство конфигурирования и настройки РЗА, представляющее собой ноутбук с предустановленным прикладным ПО, используемый исключительно в целях выполнения ремонтно-эксплуатационных работ по настройке и обновлению программного обеспечения (далее – ПО) ИС РЗА и устройств измерений (далее УИ).
- Серверы точного времени и коммутационное оборудование локальной вычислительной сети (далее – ЛВС).
- Шкафы РЗА № 1 и № 2 с терминалами ИС РЗА.
- Шкафы с устройствами измерений.

При этом:

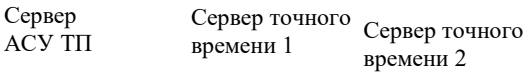
1. Сервер АСУ ТП в автоматическом режиме собирает в архив осциллограммы аварийных событий.
2. Сервер сбора осциллограмм по линии связи между ЦПС 110кВ и Центром управления сетями филиала МРСК (далее – ЦУС), проходящей по сетям связи общего пользования, забирает сформированные осциллограммы из архива АСУ ТП по протоколу FTP.

3. Специалистам РЗА в ЦУС обеспечивается возможность получения осциллограмм с сервера сбора осциллограмм.
4. Локальный доступ к серверу АСУ ТП имеют:
   - оперативный и оперативно-ремонтный персонал подстанции, который выполняет эксплуатацию и ремонт АСУ ТП и ИС РЗА;
   - персонал сервисных организаций, который может выполнять работы по ремонту АСУ ТП и ИС РЗА.
5. Работы по настройке и обновлению ПО ИС РЗА и устройств измерений СИ выполняет оперативно-ремонтный персонал подстанции и/или персонал сервисных организаций, которые с помощью УКН ИС РЗА локально подключаются к соответствующему оборудованию.

Рассматривая данный пример, с точки зрения информационной безопасности сразу выделяются следующие узкие места.

- Канал с удалённым объектом, ЦУС в частности.
- Рабочие станции и сервера, а особенно ноутбук (ИС РЗА), к которым есть доступ внешнего персонала (например, оперативно-ремонтный и персонал сервисных организаций).
- Единая резервированная сеть (PRP), построенная на физически единых коммутаторах.

В случае с цифровой подстанцией, возникает увеличенный риск того, что, используя единую шину данных и единое коммутационное оборудование, ущерб может быть и физическим. Детальнее об угрозах, возможностях реализации угроз и их последствиях можно прочитать в отчёте рабочей группы «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики» [4], сформированной на базе исследовательских комитетов B5 и D2 РНК СИГРЭ. Это значит, что злоумышленник с высоким потенциалом (компетенциями), явно может попасть в периметр объекта и воздействовать на него. Более того, для всего МРСК это значит, что потенциально злоумышленник с высоким потенциалом может попасть в ЦУС, а далее на все остальные ПС и отключить их одновременно, как это было, например, на Украине в 2015 и 2016 годах, когда регионы зимой оставались по 8 часов без электричества.



[4] http://energyexpert.ru/content/view/1569

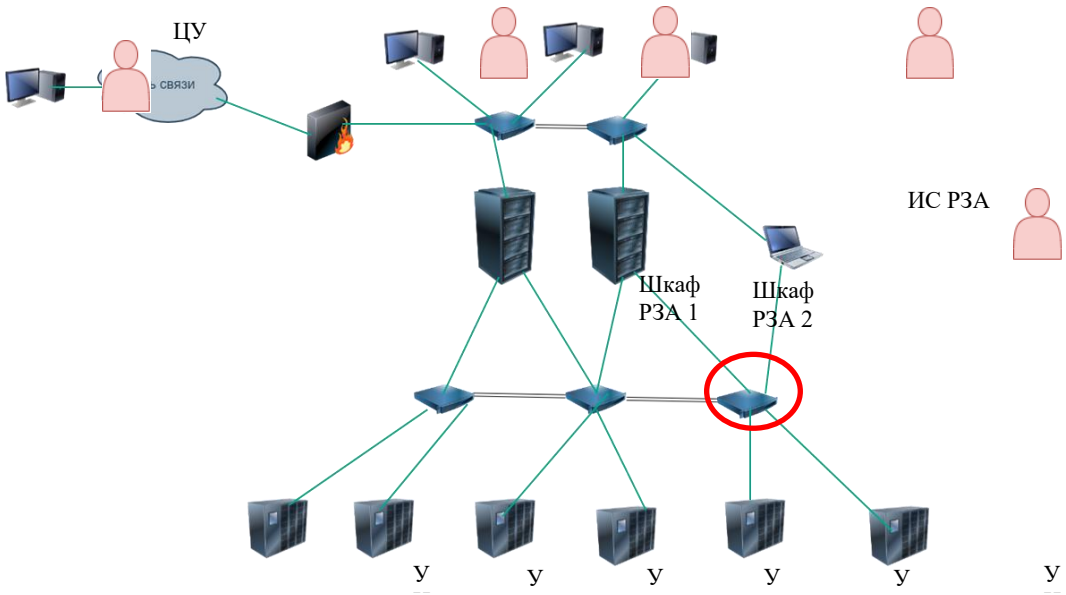


Рис. 3. Обобщённая схема ЦПС.

Согласно законодательной базе, основными документами, для разработки мер защиты информации предприятий и объектов ТЭК являются:

- Приказ ФСТЭК России № 235 от 21.12.2017 (ред. 27.03.2019) «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;
- Приказ ФСТЭК России № 239 от 25.12.2017 (ред. 26.03.2019) «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»;
- Приказ ФСБ России № 367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»;
- Приказ ФСБ России № 196 от 06.05.2019 «Об утверждении требований к средствам ГосСОПКА»;
- Приказ Министерства энергетики РФ от 6 ноября 2018 г. № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования» (СУМиД).

Вместе с тем, например, для дочерних компаний ПАО «Россети» (таких как предприятий МРСК) также действует ряд их внутренних требований, включая:

- Распоряжение ПАО «Россети» от 30.05.2017 № 282р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем. технологического управления электросетевого комплекса Группы компаний «Россети»;
- Распоряжение ПАО «Россети» от 01.04.2016 № 140р «Об утверждении минимальных требований к информационной безопасности АСТУ».

Из данных документов следует постулат о том, что приоритетными являются базовые (штатные) меры защиты, разработанные или согласованные разработчиком систем

автоматизации, а внедрение мер, не согласованных с разработчиком, не рекомендуется. НО для ПАО «Россети», разработчики должны проработать вопросы ИБ.

Это требует глубокой проработки мер ИБ разработчиком ЦПС на самом раннем этапе, так как для обеспечения информационной безопасности потребуется разработать модель угроз на стадии проектирования и предусмотреть:

- вычислительные ресурсы как на АРМах и серверах, так и у сетевого оборудования для средств защиты информации;
- каналы связи, для передачи информации ИБ вне производственного процесса;
- соответствующие интерфейсы у устройств, место в шкафах и обеспечение их электропитанием;
- разработанные правила и рекомендации по настройке базового ПО, средств защиты информации и процессов эксплуатации объекта, включая процессы реагирования на события ИБ в рамках логики работы автоматизированной системы.

Поставщик рассматриваемой подстанции прорабатывает вопросы ИБ в соответствие с лучшими практиками и требованиями по информационной безопасности. Стратегическая работа ведётся в части разработки безопасной и надёжной системы, позволяющей быть устойчивой ко всем видам воздействий путём распределения системы управления и релейной защиты между вычислительным оборудованием таким образом, что выход всех вычислительных модулей до последнего в любом порядке и формате не повлияет на работу автоматики и РЗА. При этом вопросы информационной безопасности также анализируются на данной стадии и учитываются при выборе аппаратных платформ, операционной системы и формирующейся сети с её особенностями.

Так как стратегическая работа не закончена, то в текущем релизе для предоставления Заказчикам безопасных и надёжных решений, был сформирован стенд, на котором проведены испытания средств защиты информации (далее СрЗИ). Целью данных испытаний было обеспечить максимальную защиту, используя максимально необходимый функционал СрЗИ, не нарушая логику работы комплекса и не влияя на его производительность. По итогам тестирования с рядом производителей сформированы долгосрочные отношения в части взаимодействия, обмена экспертизой, и взаимной поддержки в вопросах исследования угроз информационной безопасности. Как итог, в части технических мер защиты информации применены: Kaspersky KICS for Nodes, Kaspersky KICS for Networks и ИнфоТеКС IG на уровне подстанции. Также проработаны все вопросы по мониторингу и управлению ИБ, требуемые Заказчиком и регулятором.

Узкие места, обозначенные вначале, соответственно защищаются следующим подходом.

Для защищённого соединения с ЦУС используется криптографическая защита каналов связи, межсетевое экранирование и фильтрация трафика.

Для защиты серверов точного времени, АСУ ТП, ноутбука ИС РЗА применяются: контроль подключаемых устройств, контроль запускаемых приложений, анализ целостности файлов, защита от шифрования, антивирусная защита, передача событий со средств защиты информации в централизованную систему информационной безопасности.

Для защиты от сложных атак, воздействующих на оборудование или сеть, применяется комплекс мер, в основе которых – выявления атак на ранних стадиях с помощью технологии

пассивного анализа трафика внутри сети ЦПС, позволяющей определять новые устройства в сети, имеющиеся уязвимости для них и выявлять вредоносное ПО в трафике.

От того, насколько производитель систем автоматизации проработал требования регуляторов, например, идентификацию и авторизацию пользователей, ролевую модель, контроль запускаемых приложений и целостности файлов приложения, сбор и передачу отчётов работе ПО и системы, а также процессы резервирования и восстановления, зависит то, насколько объект будет надёжен и отвечать требованиям информационной безопасности. Причём это характерно для всех поставщиков систем релейной защиты и автоматики электрических сетей, как аналоговых подстанций, так и цифровых, и объектов «Интернета энергии» [5], развиваемых в рамках НТИ «Энерджинет».

[5] https://idea-go.tech/

3.15. МОНИТОРИНГ ЗАЩИЩЕННОСТИ И УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ ЭНЕРГООБЪЕКТОВ. ПОДХОДЫ И РЕШЕНИЯ

Д.А. ДАРЕНСКИЙ
Positive Technologies
Россия

АННОТАЦИЯ

Управление кибербезопасностью энергообъектов должно реализовываться посредством базовых процессов: мониторинга защищенности, управления конфигурациями, обновлениями, правами пользователей, инцидентами, средствами защиты, а также реагированием и расследованием инцидентов. При этом важно учитывать архитектуру и прикладную логику функционирования самих систем управления и защиты, особенности их эксплуатации. Управление кибербезопасностью энергообъектов должно быть в первую очередь направлено на контроль производственных рисков. При реализации функций комплексных систем управления кибербезопасностью нельзя ограничиваться только областью информационной безопасности — такие системы должны уметь анализировать события ИБ с учетом логики и режимов технологических процессов, а также особенностей отдельных платформ промышленной автоматизации различных производителей.

Специалисты Positive Technologies разработали ряд подходов и решений для централизованного мониторинга и управления кибербезопасностью энергообъектов с использованием как стандартных, так и уникальных технологий.

Цифровизация энергетики не оставляет сомнений в необходимости обеспечивать и управлять кибербезопасностью всей информационно-технологической инфраструктуры электросетевых предприятий. Вопросы кибербезопасности корпоративных сегментов инфраструктуры давно и успешно решаются, а вот к задачам безопасности технологических сегментов и систем промышленной автоматизации энергокомпании только приступают.

Крупнейшие энергокомпании России активно строят или уже построили центры оперативного реагирования на угрозы ИБ (security operations center, SOC) или аналогичные центры управления кибербезопасностью. Безусловно, во многом их к этому подтолкнули законодательные инициативы и требования регулирующих органов. Изначально компании ставили своей целью обеспечение формального соответствия требованиям законодательства в части защиты критической информационной инфраструктуры (КИИ), но сейчас помимо формального комплаенса хотят получить практический результат и пользу. Крайне важный вопрос — влияние создаваемых систем и процессов управления ИБ на основные производственные процессы. Компании хотят видеть прямые и косвенные положительные экономические, производственные, инвестиционные, технологические эффекты и понимать, насколько положительно такие решения влияют на надежность и наблюдаемость систем, их доступность и устойчивость к негативным воздействиям.

ВЫЗОВЫ

Построение систем централизованного мониторинга и управления кибербезопасностью таких сложных и критически важных инфраструктурных объектов, как электрические сети среднего и высокого класса напряжения, имеет множество технологических, инфраструктурных, организационных и методологических ограничений и вызовов. Инфраструктура таких сетей в России — одна из крупнейших в мире. В мире нет опыта реализации систем централизованного мониторинга и управления кибербезопасностью инфраструктур такого масштаба — отсутствуют как методология, так и практический опыт. Нет четкого понимания, каким образом выстраивать процессы и организационную структуру компании, как обеспечить качественное реагирование на инцидент кибербезопасности на подстанции, если она находится на удалении в несколько часовых поясов. Пока нет и ясного понимания, какие события или их последовательность являются инцидентами кибербезопасности в АСУ ТП подстанции или системе релейной защиты (РЗ) и противоаварийной автоматики (ПА), а какие события инцидентами не являются.

Еще один вызов — соотнесение между собой всех событий, регистрируемых системами технологического мониторинга, управления и защиты, их анализ и понимание текущего состояния защищенности объекта в целом с учетом всех технологических и технических изменений, которые происходят в процессе эксплуатации объекта. Сегодня подстанции среднего и высокого классов напряжения оснащены системами, которые так или иначе

обеспечивают контроль за состоянием оборудования и процессов переключений, защиты оборудования и линий электропередач, линий связи, технологической сети объекта, вычислительных ресурсов и их безопасностью. Несмотря на то, что развитие систем технологического управления медленно, но верно движется в сторону предиктивной аналитики и управления объектами с учетом прогнозирования состояний и режимов функционирования оборудования, данные из существующих систем на сегодняшний день обрабатываются и анализируются специалистами с различной квалификацией и являются разрозненными, на их основе невозможно получить полную и достоверную картину о состоянии объекта в режиме реального времени.

Вместе с тем обеспечить корректную работу систем кибербезопасности в части выявления аномалий, инцидентов или кибератак без привязки к режиму функционирования объекта, специфике и логике процесса практически невозможно, равно как и организовать в таких случаях своевременное и эффективное реагирование на такие инциденты.

ЧТО ЖЕ ДЕЛАТЬ?

В целом, задачи обеспечения защиты и управления кибербезопасностью на энергообъектах могут решаться двумя путями. Первый ориентирован на защиту от киберугроз без учета прикладной и функциональной специфики энергообъектов, второй — на снижение прежде всего производственных рисков. Каждый из указанных подходов имеет свои преимущества и ограничения.

Подход, ориентированный на защиту от киберугроз, является классическим. Все этапы построения типичных систем защиты и управления кибербезопасностью имеют обширную методологическую основу и технологический базис. Данный подход позволяет решить все типовые задачи безопасности и реализовать необходимый набор мер защиты энергообъектов даже в условиях серьезных финансовых и иных ресурсных ограничений. Однако отсутствует возможность оценить, насколько эффективна такая система. Как правило, службам эксплуатации при таком подходе системы кибербезопасности никакой пользы не приносят — а иногда даже наоборот, создают дополнительные проблемы и ограничения при эксплуатации и обслуживании основных систем автоматизации в их зоне ответственности. При этом часто возникает ситуация, когда с точки зрения служб ИБ системы кибербезопасности вроде бы должны повышать в целом устойчивость и надежность основных систем, а с точки зрения служб эксплуатации оперативно-диспетчерских служб позитивные эффекты не заметны. О каком-либо положительном влиянии на эффективность управления технологическими процессами говорить не приходится. Иными словами, службы ИБ решают сугубо свои задачи, польза от которых для других служб не видна или не понятна. При таком подходе ничтожно мало или отсутствует влияние степени защищенности от киберугроз на общие показатели функциональной надежности, на скорость принятия решений, эффективность реагирования на инциденты, а также на ощутимое снижение вероятности критически значимых производственных рисков. В итоге целесообразность реализации таких систем для энергокомпаний может оказаться под вопросом.

Создание комплексных систем кибербезопасности, ориентированных на снижение производственных рисков, только начинает рассматриваться службами ИБ российских промышленных предприятий. На многих предприятиях не энергетической отрасли ИБ-службы активно взаимодействуют как с производственными подразделениями, так и со специалистами подразделений по управлению рисками в целях определения конкретных прикладных задач. Такой подход имеет ряд сложностей. Во-первых, область кибербезопасности на промышленных предприятиях традиционно существует в стороне от риск-менеджмента. На многих предприятиях реестры производственных или операционных рисков существуют параллельно с моделями угроз и моделями нарушителей, которыми руководствуются специалисты подразделений информационной безопасности. Специалисты по управлению рисками на предприятиях не учитывают киберугрозы при оценке вероятности и значимости рисков. В то же время специалисты по информационной безопасности того же предприятия при оценке киберугроз не имеют возможности адекватно

и реалистично оценить степень их влияния на производство и специфичные для него риски. Во-вторых, даже если специалисты производственных подразделений, служб ИБ, ИТ и управления рисками выработают единые правила взаимодействия, то техническая реализация комплексной системы, которая бы контролировала все аспекты безопасности производственных активов, потребует серьезных изменений на технологическом, процессном и организационном уровнях компании.

Тем не менее подход, ориентированный на снижение производственных рисков, имеет ряд неоспоримых преимуществ. Во-первых, он позволяет определить оптимальный перечень мер, технологий и ресурсов, необходимых для снижения действительно серьезных производственных рисков, что безусловно положительно скажется на соотношении стоимости реализации решений и их эффективности. Во-вторых, это позволит сфокусировать деятельность на решении в первую очередь прикладных задач, направленных на обеспечение реальной безопасности и защиту основных активов от действительно актуальных угроз.

ПОДХОДЫ POSITIVE TECHNOLOGIES

Компания Positive Technologies имеет многолетний опыт и глубокую экспертизу в области промышленной кибербезопасности. Специалисты компании провели десятки исследований систем промышленной автоматизации и защищенности энергообъектов, выявили сотни уязвимостей, сотни промышленных объектов используют решения Positive Technologies. Сегодня компания реализует ряд инициатив, цель которых объединить технологии безопасности, методологии управления производственными рисками и операционные технологии индустриальных систем. В рамках данных инициатив Positive Technologies ведет работу по направлениям разработки методологии риск-ориентированного подхода при создании систем управления промышленной кибербезопасностью и развития комплексных систем централизованного мониторинга и управления промышленной кибербезопасностью.

Если говорить в общем о методологии реализации риск-ориентированного подхода, то эксперты Positive Technologies считают ключевыми следующие этапы работ:

1. Верифицировать ключевые производственные риски, имеющие высокую значимость и наибольшую стоимость ущерба.
2. Выявить угрозы кибербезопасности, способные негативно повлиять на основное оборудование и технологически процессы и тем самым вызвать возникновение верифицированных производственных рисков.
3. Определить и доказать вероятность реализации векторов атак и киберугроз, определить техники и тактики, смоделировать профиль нарушителя или атакующего.
4. Разработать оптимальный перечень мер защиты, качественно влияющих на снижение вероятности реализации киберугроз и уровень достижимости векторов атак. Состав мер необходимо направить в первую очередь на максимально возможное снижение вероятности возникновения производственного риска вследствие реализации киберугроз.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ПОДХОДА

Одним из наиболее значимых производственных рисков при эксплуатации электроподстанций является авария с частичным или полным разрушением или нарушением геометрии конструктива трансформатора. Причины возникновения такого риска, стоимость ущерба и восстановления, а также вероятность его возникновения технологам хорошо известны. Одной из таких причин являются некорректная работа систем управления и защиты. К нарушению режимов работы систем автоматизации могут приводить сбои в работе систем, которые могут быть вызваны случайными или намеренными действиями персонала или сторонних лиц. Систематизация причин сбоев, возможных ошибок конфигурации, имеющихся уязвимостей и доступных способов (техник и тактик) воздействия на компоненты систем автоматизации позволяют определить состав актуальных киберугроз, достижимость

векторов атак и вероятность возникновения инцидентов, способных привести к реализации конкретного риска — аварии трансформатора.

Безусловно, такой подход более трудоемкий: универсального ПО, облегчающего разработку, и готовых решений по данному направлению нет. Для реализации отдельных этапов (без учета их связанности между собой, например верификации рисков, моделирования киберугроз или выявления тактик кибератак) есть методологическая и нормативно-техническая база, и она более чем внушительна. По отдельности для этих задач разработано и применяется большое количество стандартов, инструментов и технологий, но в единый комплексный подход это пока не объединено. С точки зрения решения прикладных задач практической кибербезопасности энергообъектов такой комплексный подход дает максимально полезный результат, позволяет сфокусироваться на действительно важных задачах обеспечения защиты и управления безопасностью, имеющих критически важное значение не только для служб ИБ, но и других смежных подразделений компаний.

Еще одно направление инициатив Positive Technologies — создание решений, позволяющих строить централизованные масштабируемые системы мониторинга и управления промышленной кибербезопасностью с учетом отраслевой и прикладной специфики конкретного предприятия или компании. Данное направление является логическим продолжением разработки методологий реализации риск-ориентированного подхода, о котором говорилось выше.

Это достаточно серьезный вызов, с которым уже столкнулись многие промышленные компании, и на который рынки кибербезопасности и промышленной автоматизации, по сути, пока не могут ответить. Например, энергокомпаниям важно оценивать надежность производственных активов в целом и управлять ею. Необходимо видеть всю картину целиком: техническое состояние основного оборудования, статистику по сбоям и режимам систем управления, состояние инженерной и IT-инфраструктуры, события ИБ и состояние систем антитеррористической защиты. Желательно, чтобы совокупность этих показателей отражалась в единой среде с универсальным представлением данных. От «зоопарка» различных систем и разрозненных данных, которые не дают полной картины, все уже устали. Количество «брошенных» систем, которые оказались бесполезными или неэксплуатируемыми порой исчисляется десятками. Данные в этих системах могут быть полезными, но их интерпретация, анализ и использование требуют такого количества ресурсов, что каждая отдельная система сама по себе становится экономически неэффективной.

Более того, владеть необходимым уровнем прозрачности инфраструктуры и понимания текущей ситуации на объектах недостаточно — важно иметь средства поддержки принятия решений при оперативно-технологическом управлении. Такие возможности должны базироваться на результатах прогнозного моделирования вариантов управляющих воздействий или событий в системах. Недостаточно просто видеть то, что происходит, или сам факт критически важных изменений. Необходимо иметь возможность превентивного воздействия — на основе прогноза развития ситуации, вероятных событий или изменения режимов функционирования систем.

Специалисты Positive Technologies тестируют ряд технологических решений, которые в совокупности нацелены выполнять подобные задачи в области промышленной кибербезопасности, а в перспективе и безопасности промышленных объектов в целом. Разработку Positive Technologies ведет в тесном сотрудничестве как с отечественными, так и зарубежными производителями средств промышленной автоматизации. Опытные образцы сейчас уже проходят тестирование на нескольких действующих промышленных объектах. Кроме того, тестирование таких комплексных решений ведется параллельно с апробацией методологии реализации риск-ориентированного подхода. Причем их тестирование выполняется путем проведения полноценных киберучений с фиксацией реальных результатов и выводами об их эффективности. Специалисты Positive Technologies уверены: такой подход к построению комплексных систем безопасности, ориентированных в первую

очередь на решение прикладных задач, обеспечит максимально контролируемую и безопасную среду на промышленных предприятиях.

Positive Technologies предлагает не просто комплекс продуктов и технологий, но и необходимый объем экспертизы, который поможет в решении специфичных для индустриальных систем задач безопасности. Пакеты экспертизы будут включать наборы правил (настроек) для компонентов комплексного решения, таких как MaxPatrol SIEM, PT ISIM, MaxPatrol 8. Кроме того, такой подход подразумевает наличие достаточного объема документированных рекомендаций и практические кейсы реализации конкретных прикладных задач безопасности с помощью продуктов Positive Technologies.

Ниже приведен ряд кейсов, которые можно будет решать с помощью разработки компании.

1. Комплексный мониторинг безопасности индустриальных систем. Данное решение включает возможность сбора, обработки и анализа событий узлов промышленной инфраструктуры системного и прикладного характера. Такие события могут быть обогащены данными, получаемыми при анализе трафика технологических сетей. При этом полученные события могут быть скоррелированы как с данными технологических процессов, так и с событиями из внешних вспомогательных систем, не имеющих прямого отношения к технологическим или производственным процессам. Это дает возможность контролировать аномальное поведение компонентов систем, действия пользователей, неавторизованные подключения, нелегитимный трафик, влияние событий и действий пользователей на критически значимые параметры технологических процессов, рассчитывать достижимость потенциально опасных векторов атак и вероятность развития наиболее серьезных инцидентов безопасности. Данное решение позволяет использовать штатные средства логирования и экспорта системных и прикладных событий контроллеров, терминалов релейной защиты, сетевого и вычислительного оборудования, СКУД, систем технологического видеонаблюдения, систем видеоконтроля соблюдения правил техники безопасности, СПО. При этом отсутствует прямое взаимодействие средств мониторинга с целевыми системами и влияние на технологические и производственные процессы.
2. Выявление технологического фрода. Решение позволяет выявлять воздействия и отклонения в информационно-измерительных системах. Простой пример: энергокомпании могут иметь на балансе десятки тысяч приборов коммерческого учета. Выявлять факты неправомерного вмешательства, переконфигурирования или просто «угона» приборов учета в такой обширной инфраструктуре без соответствующих средств автоматизации невозможно. Кроме того, мало просто иметь средства мониторинга и обнаружения, необходимо чтобы средства уже имели базовый объем экспертизы для реализаций необходимых функций.
3. Мониторинг защищенности и расчет достижимости векторов атак. Объекты цифровизации строятся с использованием компонентов, имеющих уязвимости. Сети и архитектура систем проектируются и внедряются с ошибками безопасности. Доступ к инфраструктуре систем управления и технологических защит часто не регламентирован и не контролируется. Совокупность подобных факторов приводит к наличию потенциальных векторов кибератак или деструктивного воздействия на системы и технологические процессы. Понимание наличия таких векторов, возможность определения их критичности и достижимости позволяет оптимизировать затраты на обеспечение необходимых и достаточных мер защиты.
4. Проверка соответствия уровня защищенности. Регулирование вопросов безопасности энергообъектов с каждым годом ведется все активнее. Поэтому необходимо обеспечивать проверку соответствия требованиям политик

безопасности и текущего законодательства на постоянной основе. Более того, помимо соответствия обязательным требованиям регулирующих органов и законодательства появляется практика проверки соответствия требованиям производителей средств промышленной автоматизации. Такая практика базируется на том, что производители несут гарантийные обязательства по поставляемым системам. Гарантийные обязательства производители вполне резонно могут не исполнять, если в процессе эксплуатации возникновение гарантийного случая вызвано нарушениями требований по обеспечению кибербезопасности.

По данным исследований и прогнозов Positive Technologies, внимание к теме кибератак, в особенности целевых атак (APT, advanced persistent threat), существенно повысилось: руководство промышленных и энергетических компаний осознает необходимость внедрения эффективных систем, которые способны не только противодействовать отдельным угрозам, но и выявлять действия высококвалифицированных хакеров. Это возможно при реализации риск-ориентированного подхода и использовании комплексных технологических решений.

3.16. РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ В ЭНЕРГОСИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ ВСТРОЕННЫХ РЕШЕНИЙ

И.В. КРУТСКИХ
ООО «ПиЭлСи Технолоджи»
Россия

Контактное лицо:

И.В. КРУТСКИХ

ikrutskih@tpz.ru

Ключевые слова:
Информационная безопасность систем, защита информации, антивирусная защита.

ВВЕДЕНИЕ

Информационная безопасность критически важной инфраструктуры – вопрос, имеющий огромное значение не только для отдельных предприятий, но и для государства в целом, поэтому российское правительство уделяет этой теме большое внимание. В 2018 году был принят закон 187-ФЗ «О безопасности критической информационной инфраструктуры». Он расшил перечень информационных систем, к безопасности которых выдвигается ряд обязательных требований со стороны государства. Теперь их владельцы несут ответственность за их безопасность, в том числе уголовную. Для таких систем вводится понятие «критическая информационная инфраструктура» (КИИ). К данной категории относятся информационные системы и сети, нанесение ущерба которым может привести к возникновению угрозы для здоровья и жизни людей, негативно повлиять на экономическую, политическую, экологическую и социальную устойчивость региона и государства в целом.

ОСНОВНАЯ ЧАСТЬ

Требования к встроенным СЗИ АСТУ электросетевого комплекса ПАО «Россети»

Одной из систем, безопасность которых должна быть обеспечена в соответствии с Федеральным законом, являются электрические сети страны. Оператор электрических сетей в России, ПАО «Россети», сформулировало требования к встроенным средствам защиты информации (СЗИ) автоматизированных систем технологического управления (АСТУ) электросетевого комплекса. Эти требования, которые были утверждены распоряжением ПАО «Россети» от 30.05.2017 № 282Р, распространяются на аппаратно-программное обеспечение, применяемое в составе АСТУ, в том числе предназначенное для управления и встроенное в оборудование соответствующих подсистем. Применяются при выполнении работ по защите, созданию, модернизации и эксплуатации, приемке (включая процесс аттестации оборудования, материалов и систем в электросетевом комплексе ПАО «Россети») и испытаний систем, входящих в состав АСТУ ПАО «Россети» и его дочерних предприятий (ДЗО).

Компоненты АСТУ, поставляемые и эксплуатируемые на объектах электросетевого комплекса группы компаний «Россети», должны обладать встроенными СЗИ. Производитель АСТУ и/или электрооборудования обязан подтвердить соответствие встроенных СЗИ указанным требования форме сертификации указанного оборудования и/или программного обеспечения в системе сертификации ФСТЭК.

ПАО «Россети» выделило следующие угрозы информационной безопасности систем:

- внедрение вредоносного ПО и программных закладок;
- несанкционированное уничтожение, модификация, копирование и блокирование информации, изменение конфигурации и настроек;
- анализ и перехват потоков информации между удалёнными процессами;
- нарушение целостности данных в рамках протокола обмена;
- модификация информации;
- несанкционированная конфигурация, настройка и нарушение штатного режима работы;

- хищение оборудования.

Определен ряд мер по защите информации в АСТУ:

- идентификация и аутентификация удаленных контроллеров ТМ;
- аутентификация внешних пользователей и процессов;
- контроль целостности программной среды;
- защита информации, передаваемой по каналам связи;
- применение межсетевых экранов на периметрах объектов;
- управление доступом пользователей, регистрация событий доступа;
- обнаружение и предотвращение сетевых вторжений;
- антивирусная защита.

Защита каналов передачи данных в АСТУ должна быть обеспечена с помощью следующих мер.

- Идентификация и аутентификация удалённых контроллеров ТМ («ГОСТ Р 28147-89. Криптоалгоритмы для данных, передаваемых по внешним каналам связи»).
- Аутентификация внешних пользователей и процессов (ГОСТ 34.11. На базе однонаправленных ключевых хэш-функций реализуется двусторонняя аутентификация).
- Контроль целостности программной среды («ГОСТ 34.11. Расчёт и хранение контрольной суммы с помощью ключевой криптографической хеш-функции»).
- Защита информации, передаваемой по каналам связи («ГОСТ 34.11. Генерация имитовставки для передаваемой информации»).
- Применение межсетевых экранов на периметрах объектов.
- Управление доступом пользователей, регистрация событий доступа.
- Обнаружение и предотвращение сетевых вторжений.
- Антивирусная защита.

РАЗРАБОТКИ КОМПАНИИ «ПИЭЛСИ ТЕХНОЛОДЖИ»

ООО «ПиЭлСи Технолоджи» – российская компания, которая занимается разработкой и внедрением инновационных решений, направленных на автоматизацию всех процессов в энергетике. Эта отрасль в любом государстве является стратегической, а следовательно, нуждается в особой защите. Наряду с защитой аппаратного обеспечения на первый план выходит кибербезопасность.

Информационная безопасность – ключевой аспект разработок компании «ПиЭлСи Технолоджи». Создавая специализированное программное обеспечение и программно-технические комплексы с использованием встроенных решений на базе ПТК TOPAZ, специалисты «ПиЭлСи Технолоджи» сумели реализовать все перечисленные выше требования к защите информации в энергосистемах. В частности, исключительной особенностью этих программных продуктов является отечественная разработка, благодаря чему удалось отказаться от использования исходных кодов аналогичных систем зарубежного производства.

Комплексные системы обеспечения информационной безопасности, которые ООО «ПиЭлСи Технолоджи» проектирует, разрабатывает и внедряет, имеют все необходимые свидетельства на используемые товарные знаки и регистрационные свидетельства на программное обеспечение. Данные системы совместимы с системами других производителей («Шнейдер Электрик», «Сименс», АББ и др.), при этом обеспечивают независимость критически важных процессов от оборудования и программного обеспечения зарубежного производства.

В контроллерах и серверах используется операционная система на базе LINUX. Разрешение № РРС 00-044430 свидетельствует о допустимости применения данных решений на опасных производственных объектах. Кроме того, компания «Пи Эл Си Технолоджи» имеет лицензию ФСТЭК России № 1329 от 23.10.2014 г. на осуществление деятельности по разработке и производству средств защиты конфиденциальной информации.

Рассмотрим ключевые особенности упомянутой выше системы TOPAZ, которая является одной из центральных разработок «ПиЭлСи Технолоджи» и к настоящему времени успешно внедрена на многих предприятиях стратегически важных отраслей.

Комплекс решений TOPAZ

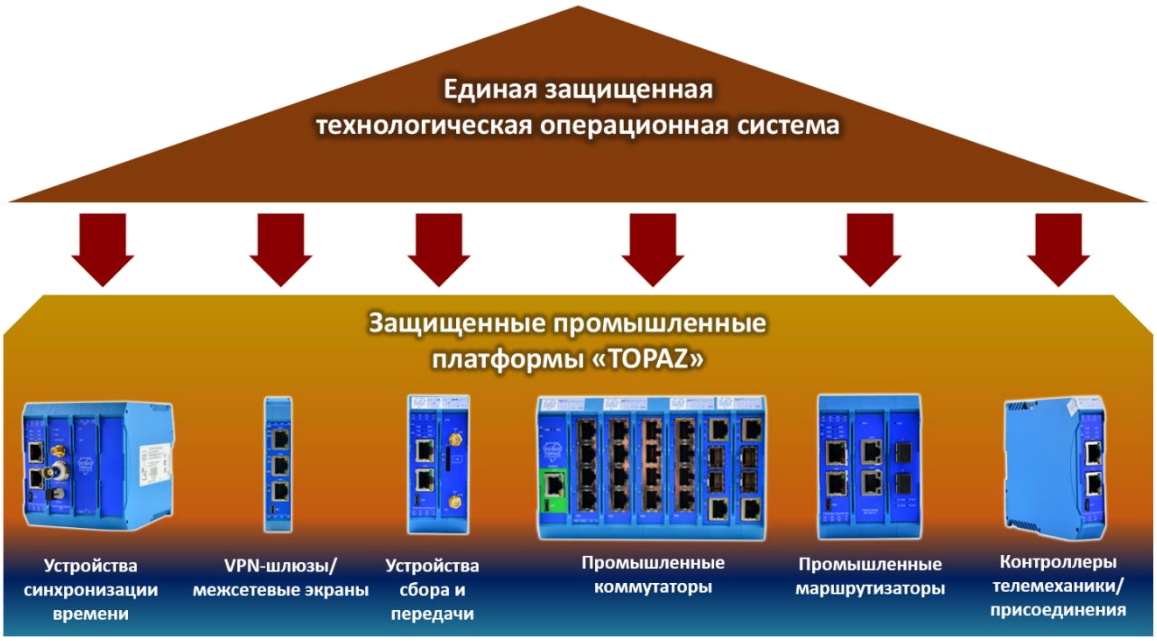


Рис. 1. Экосистема защищенных решений TOPAZ.

TOPAZ – это обширный комплекс программных и аппаратных решений (ПТК), создающих целую «экосистему» (рис. 1), в которой поддерживается высочайший уровень защищенности. Достаточно сказать, что в настоящее время программно-технический комплекс TOPAZ с успехом используется при построении:

- систем безопасности объектов критической информационной инфраструктуры 1, 2 и 3 категорий значимости (Приказ ФСТЭК России от 29 декабря 2017 г. № 239);

- систем 1, 2 и 3 классов защищенности АСУ ТП (Приказ ФСТЭК России от 14 марта 2014 г. № 31);

- государственных информационных систем 1, 2 и 3 классов защищенности (Приказ ФСТЭК России от 11 февраля 2013 г. № 17).

В этих и других системах ПТК TOPAZ обеспечивает информационную безопасность самых разных подсистем. Входящие в его состав решения используются для идентификации и аутентификации, управления доступом, для ограничения программной среды, в подсистемах сбора, регистрации и аудита событий информационной безопасности, для обеспечения целостности и доступности, для управления конфигурацией, межсетевого экранирования и сегментирования промышленной сети и т. д.

Основное достоинство представленной линейки решений – единая аппаратная платформа, гарантирующая информационную защиту системы. Необходимо отметить и программное обеспечение, полностью разработанное отечественными специалистами и не содержащее исходных кодов аналогичных систем зарубежного производства (о чем уже говорилось выше). Это ПО успешно прошло сертификацию в ФСТЭК России и может применяться в ключевых системах, к которым предъявляются особые требования, такие, как:

- АСУ энергоснабжением;

- АСУ наземным и воздушным транспортом;

- АСУ добычей и транспортировкой нефти и газа;

- АСУ экологически опасными производствами;

- автоматизированные системы предупреждения и ликвидации чрезвычайных ситуаций.

На заводе ООО «ПиЭлСи Технолоджи» обеспечен полный цикл собственного производства микропроцессорных систем, управляемых специализированным ПО. В контроллерах и серверах применяется единая операционная система на базе ядра Linux – ОС TOPAZ LINUX.

Эта защищенная ОС с прикладным технологическим программным обеспечением используется в устройствах синхронизации времени и VPN-шлюзах (межсетевых экранах), устройствах сбора и передачи данных и промышленных коммутаторах, промышленных маршрутизаторах и многих других устройствах. Механизмы безопасности, которые применяются ОС TOPAZ LINUX, реализуются на самых разных уровнях: от ядра ОС до промышленных протоколов. Например, обязательно выполняется идентификация и аутентификация на уровне ОС, СУБД, SCADA и т.п. Имеется разграничение доступа по ролевой и дискреционной моделям. Ведется аудит событий безопасности, причем обеспечена возможность передачи результатов аудита на верхний уровень системы. Поддерживаются

криптографические функции для шифрования данных при необходимости. Выполняется фильтрация промышленных протоколов и сегментирование промышленных сетей. Осуществляется контроль целостности программной среды. Наряду с этими функциями ОС TOPAZ LINUX обеспечивает возможность подключения дополнительных модулей безопасности для аутентификации и контроля действий наладчиков.

Оборудование TOPAZ

Кратко охарактеризовав программную часть ПТК, перейдем к его аппаратному обеспечению и расскажем о некоторых ключевых решениях.

Промышленный контроллер TOPAZ

Центральным звеном любой автоматизированной системы, в том числе системы построенной в экосистеме TOPAZ, является контроллер. Промышленный контроллер TOPAZ оборудован множеством защитных функций. Он может выполнять идентификацию/аутентификацию пользователей, как локальную, так и удаленную по протоколу RADIUS. Обеспечивает гибридную настройку правил доступа к защищенной информации в зависимости от заданной роли пользователя (администратор, оператор и т. п.). Также промышленный контроллер TOPAZ защищает память от снятия остаточной информации (так называемое гарантированное затирание). Он контролирует целостность программной среды и фиксирует несанкционированное изменение конфигурации/настроек/установок, выполняет аудит событий безопасности с возможностью отправки информации на верхний уровень по протоколам SYSLOG, SNMP и др. Причем информация может быть зашифрована: промышленный контроллер TOPAZ поддерживает криптографические алгоритмы (в том числе ГОСТ).

Сетевые устройства связи

Важную роль в обеспечении информационной безопасности системы играет сетевое оборудование связи: маршрутизаторы, коммутаторы и пр. В рамках ПТК TOPAZ разработаны как маршрутизаторы с функцией VPN, так и различное оборудование с функцией межсетевого экрана.

VPN (от Virtual Private Network – «виртуальная частная сеть») – это технология, позволяющая реализовать в сети отдельное, дополнительное, соединение (или несколько соединений) поверх основного для передачи особо секретных данных. Маршрутизатор TOPAZ с функцией VPN поддерживает протоколы IPSec и Open VPN для выполнения данной задачи. Также он способен:

- шифровать трафик по алгоритмам ГОСТ;
- создавать статистическую и динамическую маршрутизацию (RIP v1/v2, OSPF v2, BGP v4);
- обеспечивать маршрутизацию на основе правил для интерфейсов;

- отслеживать TCP сессий, контролировать корректность установления соединений.

Еще одно устройство связи ПТК TOPAZ – это маршрутизатор с функцией межсетевого экрана. Он служит для межсетевого экранирования, способен обеспечивать защищенный удаленный доступ и блокировать недоверенные маршруты.

Коммутатор с функцией межсетевого экрана имеет гораздо большие «полномочия». Он может осуществлять фильтрацию по MAC и IP-адресам (в том числе промышленным протоколам) с использованием адресных листов. Поддерживает технологии локальной сети VLAN, способен отслеживать TCP-сессии, контролируя корректность установки соединения. Данный коммутатор контролирует доступ разных пользователей к настройкам в соответствии с их полномочиями и соответственно поддерживает механизмы идентификации/аутентификации. В нем реализованы механизмы фильтрации трафика, которые позволяют коммутатору отсеивать запросы на получение данных по протоколу SNMP от неавторизованных клиентов и защитить устройства от иных несанкционированных запросов.

Преимущество встроенных механизмов для защиты информации

Таким образом, мы видим, что в целях защиты информации ООО «ПиЭлСи Технолоджи» применяет технологию встраивания защитных средств и механизмов непосредственно в оборудование программно-технического комплекса. Такой подход дает целый ряд преимуществ. Во-первых, функции информационной безопасности изначально реализованы в контроллерах АСТУ и ВСУ ТП, что позволяет выполнить все требования регулятора и повышает надежность системы. Во-вторых, так проще заказчику, ведь он в лице одной компании получает как исполнителя, так и поставщика, отвечающего за всю защищенную систему. В-третьих, в такой системе контроль целостности передаваемой информации по каналам связи реализован периодической проверкой состава ПО путем формирования и сверки с эталонной контрольной суммой файлов системы. Также в такой системе организованы доверенные каналы передачи данных и доверенная загрузка обновлений, реализован принцип разграничения прав доступа на основе дискреционной модели и в соответствии с матрицей доступа, настраиваемой на этапе проведения пусконаладочных работ. Для снижения вероятности НСД предусмотрено использование ВОЛС, подключаемых прямо к каналам верхнего и среднего уровней АСУ.

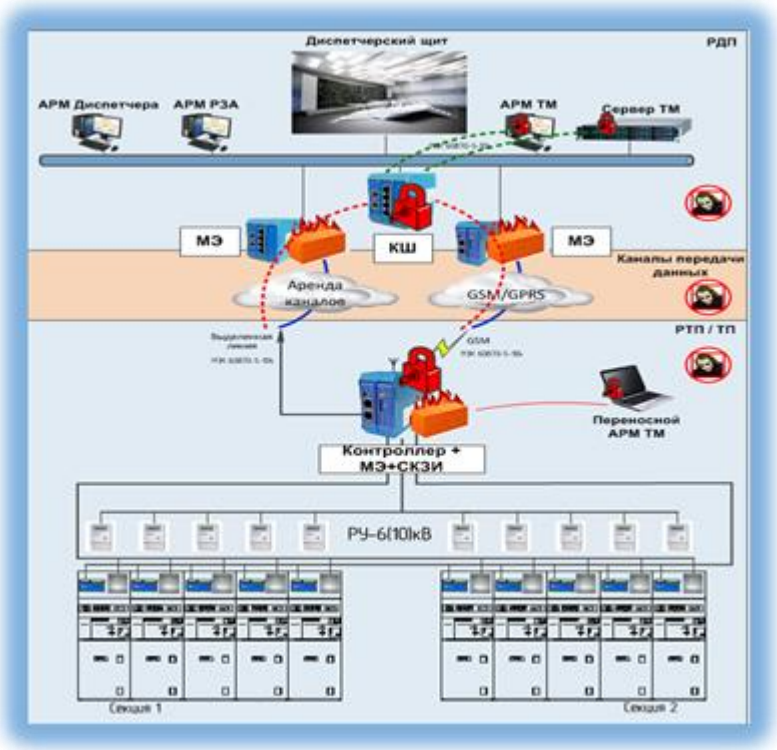


Рис. 2 Примеры реализации.

Защита от НСД к шкафам управления реклоузерами, защита SIM-карт и серверов ССПИ

- Система СКУД и СБ может быть развернута на существующем оборудовании TOPAZ в ДП. Требуется организация ведения реестра SIM-карт на сервере СКУД и СБ в ДП.

- Шкаф дооснащается модулем контроля доступа, который позволит контролировать доступ к шкафу при открытии двери и выявлять попытки НСД третьих лиц.

- При НСД, срабатывают механизмы гарантированного уничтожения ключевой информации (ключей и сертификатов VPN) на сервере ССПИ и/или конфигурации и файловой системы сервера ССПИ, чтобы контроллер перестал выполнять коммуникационные функции.

- Компактная IP-видеокамера в шкафу. Видеопоток направляется на сервер ССПИ, который осуществлять выборку фотографий и передает на сервер фиксации доступа в ДП.

- Организованы доверенные каналы передачи данных и доверенная загрузка обновлений, позволяющие обеспечить защиту от перехвата и подмены информации и предотвратить доступ к внутренней сети компании.

Преимущества решения TOPAZ в области информационной безопасности масштабны:

1. Реализация функций защиты информации, встроенных непосредственно в устройства TOPAZ, на базе которого строится АСТУ, АСУ ТП, ССПИ, АСКУЭ и т. п. – экономически и функционально выгодное решение.

2. Наличие встроенных средств защиты информации, соответствующих требованиям российского законодательства для обеспечения безопасности АСУ ТП и КИИ.

3. Поддержка расширенного репозитория прикладного ПО для устройств TOPAZ (SCADA, телемеханика, промышленные протоколы, встроенная криптография и т. п.).

4. 100 %-ная российская разработка и сертифицированное производство с учетом требований заказчиков и регуляторов.

5. Отсутствие недекларированных возможностей в ОС и прикладном ПО.

6. Совместимость с решениями отечественных вендоров в области информационной безопасности.

Соответствия требованиям регуляторов и заказчиков

Система информационной безопасности, разработанной на базе ПТК TOPAZ, в полной мере соответствует:

- требованиям ПАО «Россети» к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети» (Распоряжение № 282Р);

- требованиям ФСТЭК РД НДВ по 4-му уровню контроля отсутствия недекларированных возможностей;

- требованиям ФСТЭК – профиль защиты ОС;

- требованиям приказов ФСТЭК № 31 и № 239 в части реализации технических мер защиты на объектах КИИ и в АСУТП/ССПИ;

- требованиям ФСБ России к шифровальным (криптографическим) средствам в части реализации криптографических алгоритмов ГОСТ;

- ГОСТу 15408-2012 (часть 2, 3) в части реализации функциональных требований безопасности и требований доверия безопасности;

- стандартам IEC 62351 (часть 3, 5, 7-10) в части реализации механизмов безопасности.