ЦИФРОВАЯ ПОДСТАНЦИЯ

№12
2019

digitalsubstation.com

ЦИФРОВЫЕ ДВОЙНИКИ 20
Альтер эго новой энергетики

До того, как появились цифровые двойники, двойники были простыми или, если можно так выразиться, аналоговыми. Их можно было найти во многих культурах прошлого, они занимают видное место среди древних легенд, преданий, произведений искусства и в книгах разных, в основном мистических, авторов. Немцы, преуспевшие в жанре мифотворчества, дали им имя – доппельгангеры. Этим зловещим словом они окрестили привидение, которое не отбрасывает тени, и при этом кажется точной копией живого человека...

Как правило, появление доппельгангера не сулило ничего хорошего. Если его увидели родственники или друзья, это означало, что человеку грозила болезнь или другая напасть. Если же, не дай бог, человек сам увидел своего двойника, это и вовсе считалось предзнаменованием скорой смерти. Порой двойник пытался стать тому, чьей копией является, советчиком. Но советы эти, как правило, вели к чему-то нехорошему, злому. По этой причине люди любой ценой пытались избежать общения со своими доппельгангерами.

Так было раньше, в доцифровую, так сказать, эру. В наше время двойники оцифровались и присмирели. И это привело к тому, что они превратились в верных помощников людей, стали для нас отличным инструментом прогнозирования, ядром надежной предсказательной системы. Теперь человек сам формирует цифрового двойника моделируемого объекта еще на этапе проектирования, а затем последовательно совершенствует его за счет накопления данных о поведении реального прототипа. С помощью цифрового доппельгангера можно предугадать поведение объекта (системы) при любых изменяющихся условиях и требованиях. И это особенно важно для электроэнергетики, при решении задач интеллектуального управления ее высокотехнологичными структурами. В этом выпуске нашего журнала мы знакомим вас с концепцией цифровых двойников, подходами к их разработке и первыми шагами к их применению в энергетических системах.

— Виктор Посошков, главный редактор

Издатель
ООО «Цифровая подстанция»

Свидетельство о регистрации
СМИ № ФС77-61546

Адрес для корреспонденции
109004 Москва,
Шелапутинский пер., д. 1,
подвал №0, помещение I,
комната 1а, офис 2

Генеральный директор / Главный редактор
Виктор Посошков
pvi@digitalsubstation.com

Менеджер проекта
Елизавета Староверова
vem@digitalsubstation.com

Редактор
Роман Воронин
vrv@digitalsubstation.com

Иллюстратор
Виталий Тупицын

Дизайн и верстка
Андрей Тульнов-Соколов

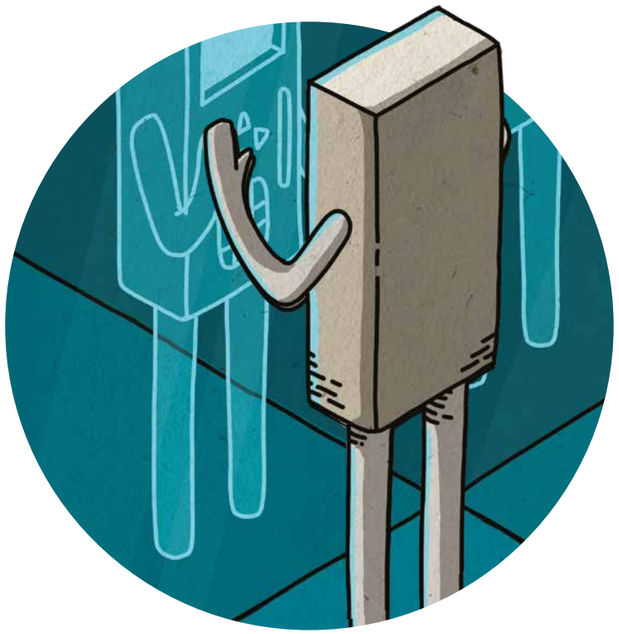
Если вы хотите оформить подписку или стать автором
editorial@digitalsubstation.com

Если вы хотите разместить у нас рекламу
sva@digitalsubstation.com

Отпечатано в типографии
ООО «РПК «Новые технологии»
www.adv-nt.ru
zakaz@adv-nt.ru

Тираж — 5 000 экз.

СОДЕРЖАНИЕ



В «СКОЛКОВО» БУДЕТ СОЗДАН ЦЕНТР ЦИФРОВЫХ РАЗРАБОТОК В ОБЛАСТИ ЭЛЕКТРОЭНЕРГЕТИКИ

21 октября на площадке Форума «Открытые инновации» «Россети» подписали с Фондом «Сколково» Соглашение о партнерстве и создании в «Сколково» партнерского Центра в области цифровых решений и технологий.

Соглашение направлено на развитие исследований и разработок для масштабной цифровой трансформации электроэнергетической отрасли с привлечением уникальных компетенций участников и партнеров «Сколково». На основании соглашения компании «Россети» присваивается статус Ключевого партнера Фонда «Сколково».

Подписи под документом поставили генеральный директор компании «Россети» Павел Ливинский и председатель Фонда «Сколково» Аркадий Дворкович в присутствии заместителя Председателя Правительства Российской Федерации Максима Акимова.

В рамках соглашения на территории Инновационного центра «Сколково» будут создаваться и отрабатываться цифровые и инновационные решения в области управления активами электросетевого комплекса, технологии современного учета энергопотребления и системы киберзащиты, а также интерактивные приложения и сервисы взаимодействия с потребителями услуг.

«На сегодня объем отраслевого заказа инновационных решений Сколково достиг 2 млрд. рублей. Консолидация усилий энергетиков и науки позволит отрабатывать крайне важные для функционирования и развития энергосистем передовые решения и принципиально новые подходы. В будущем технологические решения Центра цифровых разработок будут применяться на энергообъектах во всех регионах России», – отметил глава компании «Россети» Павел Ливинский.

«Сколково» входит в новую стадию партнерства с компанией «Россети». Оно предполагает, в том числе совместные исследования и разработки, проведение конкурсов на выявление лучших технологий, которые затем будут внедрены в российских магистральных и распределительных сетях.

«Россети» стали еще одной крупнейшей компанией, которая полномасштабно сотрудничает со «Сколково», активно заказывает продукты и услуги у сколковских разработчиков», – подчеркнул председатель Фонда «Сколково» Аркадий Дворкович ●

В ПРИАМУРЬЕ БУДУТ РЕАЛИЗОВАНЫ ТЕХНОЛОГИИ ЦИФРОВОЙ ПОДСТАНЦИИ

ПАО «ФСК ЕЭС» (Россети – ФСК ЕЭС) завершило первый этап проекта цифровизации подстанции 220 кВ «Благовещенская» в Амурской области. Впервые на объекте магистральных электросетей Дальнего Востока внедряется оборудование, позволяющее передавать в цифровом виде сигналы на всех уровнях управления системами релейной защиты и противоаварийной автоматики.

Специально для оборудования класса напряжения 35 кВ подстанции 220 кВ «Благовещенская» созданы инновационные микропроцессорные терминалы релейной защиты и автоматики (РЗА), работающие с цифровым форматом информации согласно международному стандарту МЭК 61850.

На первом этапе проекта на энергообъекте возведено новое комплектное распределительное устройство наружного применения (КРУН). Оборудование, предназначенное для приема, распределения и учета электроэнергии, а также для защиты электрических сетей переменного тока, произведено в России.

Ячейки КРУН имеют нетиповые решения. Для переформатирования аналоговых сигналов в цифровой вид в отсеках КРУН применены специальные преобразователи. Для удаленного осмотра состояния оборудования с автоматизированного рабочего места оперативного персонала в отсеках установлены видеокамеры.

На базе микропроцессорных терминалов реализуется принципиально новая система управления, контроля режимами и работы КРУН-35 кВ с применением волоконно-оптических линий связи. Они заменят контрольные кабели, которые использовались ранее, когда данные передавались в аналоговом формате. В результате будет повышена защита от помех и исключен риск некорректного срабатывания устройств РЗА. Одновременно будет обеспечена возможность обработки большого объема информации, повышена надежность всей системы релейной защиты и противоаварийной автоматики.

Следующим этапом проекта станут пуско-наладочные работы, постановка под напряжение оборудования и перевод питания потребителей на новое КРУН. Все мероприятия будут завершены к началу осенне-зимнего периода 2019/2020 гг. Мощность подстанции 220 кВ «Благовещенская» составляет 250 МВА. ●

НОВЫЙ ЦИФРОВОЙ КЛАСС ОТКРЫТ В УЧЕБНОМ КОМПЛЕКСЕ «РОССЕТИ ЛЕНЭНЕРГО»

18 октября 2019 года в Учебном комплексе «Россети Ленэнерго» (бренд ПАО «Ленэнерго») в поселке Терволово состоялась презентация нового учебного класса «Цифровой РЭС» при участии генерального директора компании «Россети» Павла Ливинского.

В учебном помещении на основе отечественного оборудования полностью воссоздана архитектура цифрового района электрических сетей – с индикаторами режимов работы сети, современными реклоузерами и возможностью дистанционного управления. В состав класса входят испытательный комплекс для релейной защиты и автоматики, оснащенный инновационной панелью управления и позволяющий осуществлять проверку и наладку сложных микропроцессорных терминалов, устройств синхронизации и счетчиков электроэнергии. Кроме того, в аудитории установлены шкафы низковольтных комплектных устройств для распределения электроэнергии, защиты и автоматизации процессов, шкафы защиты подстанционного оборудования для РЗА присоединений и др.

В ближайшее время ожидается установка АСУ ТП российского производства, которая также будет интегрирована в единую систему класса. Планируется, что в дальнейшем установленное оборудование будет привязано к оснащению полигона и будет регламентировать реальные рабочие процессы на территории комплекса. Кроме того, работа класса «Цифровой РЭС» будет происходить в непосредственной связке с оборудованием классов «Цифровая подстанция», в которых в настоящее время уже идет обучение специалистов.

«Компания «Россети» уверенно выступает в качестве драйвера цифровой трансформации электросетевой отрасли, который подразумевает не просто автоматизацию и модернизацию оборудования, но и повышение эффективности и производительности труда. Перед нами стоит более глобальная задача: добиться трансформации мышления – принципиального нового взгляда на процессы, которые происходят в электроэнергетике. В Учебном комплексе «Россети Ленэнерго» сегодня создаются уникальные возможности для получения необходимых компетенций и навыков. Развитие этого направления позволит создать на базе комплекса эталонный центр подготовки специалистов всех компаний группы «Россети» по программам дополнительного профессионального образования в области цифровой трансформации», – подчеркнул глава группы «Россети».

В настоящее время в Учебном комплексе «Россети Ленэнерго» началось обучение по пилотным программам для цифровых классов, которые включают автоматизированные рабочие места и оборудованы устройствами всех уровней, имеющихся на цифровой подстанции. С помощью цифровых классов преподаватели смогут объяснять инженерно-техническому персоналу философию цифровой трансформации и суть ее технологий, а также обучить его методам оперативно-технологического управления, обслуживания и эксплуатации оборудования, работы со специализированными программными модулями ●

В нашей стране одной из основных проблем развития цифровых технологий в энергетике остается нормативная база, не соответствующая современным потребностям, несмотря на множество обсуждений о потенциале и эффективности данного направления. Однако в России некоторые компании уже производят электронные трансформаторы тока и напряжения – например, ООО «АЙ-ТОР», ООО «Оптиметрик», АО «Профотек» и др., и устанавливают их на энергетических объектах, с организацией шины процесса в соответствии со стандартом IEC 61850. С 2015 года национальный технический комитет ТК 016 ПК-2 «Электрические сети (магистральные и распределительные)» ведет работу по созданию отечественных стандартов на измерительные трансформаторы, в том числе, применяемые на цифровых подстанциях.

РАЗВИТИЕ НАЦИОНАЛЬНЫХ СТАНДАРТОВ В ОБЛАСТИ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Григорий Ведерников
Станислав Осинцев
Ольга Петрова
ООО «Эльмаш (УЭТМ)»

Главный принцип в работе при разработке серии национальных стандартов – не банальный дословный перевод зарубежных стандартов и позиционирование их как ГОСТ Р, а лишь учет имеющегося зарубежного опыта для разработки отечественных стандартов, отвечающих современным требованиям, и их обобщение. В результате, любой пользователь получит полный объем актуальных данных для создания цифрового измерительного устройства и однозначное понимание терминологии путем исключения дублирования, что поможет внедрить общий базовый подход для работы с подобным оборудованием.

В качестве сравнения предлагаем рассмотреть, как развивается стандартизация в области измерительных трансформаторов на международном и национальном уровне на данный момент, а также возможные пути развития.

На международном уровне стандарты в области измерительных трансформаторов разрабатывает технический комитет МЭК ТК38 «Измерительные трансформаторы» (TC38 Instrument Transformers).

Работа в ТК38 ведется активно и направлена на то, чтобы своевременно и достаточно быстро реагировать на потребности рынка, отражать развитие технологий, устанавливать современные требования и повышать надежность работы оборудования.

Структура стандартов МЭК по измерительным трансформаторам (таблица 1) заключается в том, что общие требования ко всем трансформаторам объединены в первой части МЭК 61869-1, при этом все специфические требования к отдельным видам трансформатора представлены в соответствующих частях стандартов (МЭК 61869-2, МЭК 61869-3 и т.д.), что позволяет исключить дублирование в последующих частях.

Стоит обратить внимание, что наиболее активные работы ведутся по разработке следующих стандартов МЭК:

- МЭК 61869-1 «Общие требования к измерительным трансформаторам»;
- МЭК 61869-7 «Дополнительные требования к электронным трансформаторам напряжения»;
- МЭК 61869-8 «Дополнительные требования к электронным трансформаторам тока»;
- МЭК 61869-13 «Требования для отдельностоящих устройств сопряжения»;
- МЭК 61869-16 «Спецификация в электронном формате для измерительных трансформаторов»;
- МЭК 61869-99 «Словарь». Данный стандарт содержит все термины и определения в области измерительных трансформаторов;
- МЭК 63253-5713-8, совместно с IEEE «Трансформаторы напряжения большой мощности».

Более подробную информацию о техническом комитете ТК38, структуре руководящего аппарата, рабочих группах, разрабатываемых стандартах можно посмотреть на сайте МЭК https://www.iec.ch.

На национальном уровне в РФ в области измерительных трансформаторов действуют стандарты ГОСТ 7746-2015 «Трансформаторы тока. Общие технические условия» и ГОСТ 1983-2015 «Трансформаторы напряжения. Общие технические условия». Пересмотр данных стандартов был в 2015 г. и практически является клоном предыдущей версии стандарта 2001 г. Актуальные вопросы, касающиеся надежной работы сети, а именно по нормированию погрешности трансформаторов тока в переходных режимах и подтверждению антирезонансных свойств трансформаторов напряжения, в национальных стандартах не были отражены. Говорить о включении требований по электронным, емкостным, комбинированным трансформаторам и не приходится. Таким образом, очевидно, что за последние 10–14 лет никакого развития в области национальной стандартизации по измерительным трансформаторам в РФ не наблюдалось.

Наиболее логичным выходом в сложившейся ситуации кажется «внедрение переводов стандартов МЭК в качестве национальных и межгосударственных». Вошедшая уже в традицию данная стратегия и не обошла стороной стандарты на измерительные трансформаторы.

В таблице 2 представлены эквивалентные стандарты на основе стандартов МЭК.

Анализируя таблицу, можно сделать вывод, что к разработке эквивалентных стандартов приступают не ранее их официального выхода. В некоторых случаях срок между началом разработки и выходом эквивалентного стандарта составляет до 23 лет. За такой период произошел значительный скачок в развитии технологий, соответственно, и в развитии измерительных трансформаторов.

Считаем, что применение эквивалентных стандартов неприемлемо по отношению к РФ, так как в некоторых из них указано, что требования распространяются на оборудование только для экспортных поставок, а также не все указанные ссылочные документы приняты на территории РФ, и самое основное, что технические требования и методы испытаний не соответствуют национальным требованиям, например, в части климатических исполнений, уровней напряжений и др.

Ввиду того, что качество переводов страдает технической неграмотностью, применение и использование эквивалентных стандартов еще больше затрудняет их внедрение.

По нашему мнению, чтобы развиваться в области национальной стандартизации, российским специалистам и экспертам рабочих групп МЭК необходимо, начиная с момента начала разработки международного стандарта, вести параллельную работу по следующим направлениям:

- переводить международные стандарты на всех этапах их разработки, это возможно, так как русский язык, наряду с английским и французским, является одним из официальных языков МЭК;
- разрабатывать национальные стандарты по необходимым направлениям, с учетом требований, действующих и подходящих для РФ;
- формировать и высказывать позицию по проектам международных стандартов с учетом национальных интересов совместно с привлекаемыми ими специалистами на всех стадиях их разработки, и таким образом отражать национальные интересы в стандартах МЭК. От РФ, например, в международной рабочей группе РГ37 ТК38 по электронным трансформаторам тока и напряжения на сегодня 11 экспертов.

В результате такого подхода с выходом международного стандарта будут издаваться отечественные стандарты, соответствующие современным требованиям и качественные

Таблица 1.
Международные стандарты в области измерительных трансформаторов

Серия стандарта	Обозначение стандарта МЭК	Наименование стандарта
61869-1 Общие требования к измерительным трансформаторам	61869-2	Дополнительные требования к трансформаторам тока
	61869-3	Дополнительные требования к индуктивным трансформаторам напряжения
	61869-4	Дополнительные требования к комбинированным трансформаторам напряжения
	61869-5	Дополнительные требования к емкостным трансформаторам напряжения
	61869-7	Дополнительные требования к электронным трансформаторам напряжения
	61869-8	Дополнительные требования к электронным трансформаторам тока
	61869-9	Цифровой интерфейс для измерительных трансформаторов
	61869-10	Дополнительные требования к пассивным трансформаторам тока малой мощности
	61869-11	Дополнительные требования к пассивным трансформаторам напряжения малой мощности
	61869-12	Дополнительные требования к комбинированным электронным измерительным трансформаторам малой мощности
	61869-13	Отдельностоящие устройства сопряжения
	61869-14	Дополнительные требования для трансформаторов тока постоянного тока
	61869-15	Дополнительные требования для трансформаторов тока постоянного тока
	61869-16	Спецификация в электронном формате для измерительных трансформаторов
	61869-20	Требования безопасности к измерительным трансформаторам выше 1кВ
	61869-99	Словарь терминов по измерительным трансформаторам

Таблица 2.
Эквивалентные национальные стандарты на основе стандартов МЭК

Оригинальный стандарт МЭК			Эквивалентный стандарт	
Наименование	**Год начала разработки**	**Год выпуска**	**Наименование**	**Год выпуска**
IEC 61869-1	1994	2007	ГОСТ IEC 61869-1	2015
IEC 61869-2	2007	2012	ГОСТ Р МЭК 61869-2	2015
IEC 61869-3	2007	2011	ГОСТ IEC 61869-3-2012	2012
IEC 60044-7-1999	1987	1999	ГОСТ Р МЭК 60044-7	2010
IEC 60044-8-2002	1993	2002	ГОСТ Р МЭК 60044-8	2010

официальные переводы стандартов МЭК.

Учитывая отсутствие современной нормативной базы и руководствуясь вышесказанными подходами, Эльмаш УЭТМ в инициативном порядке разработал серию проектов национальных стандартов на классические измерительные трансформаторы, но работа в данном направление не закончилась. Сегодня в ПК-2 направлена серия проектов национальных стандартов по электронным измерительным трансформаторам на рассмотрение рабочей группы.

Для подготовки проектов стандартов на электронные измерительные трансформаторы были проанализированы и структурированы требования из всей серии МЭК 61869 (а также отдельных стандартов серии МЭК 60044). С целью исключения дублирования взаимосвязанные требования были объединены и логически распределены в соответствии с новой предложенной структурой. Весь массив полученной информации был наложен на ранее разработанную структуру национальных стандартов, где каждое из требований оценивалось на соответствие национальным принципам и подходам. Предпочтения отдавались отечественным подходам с учетом мирового опыта. Более того, часть методик отсутствовала как в российских, так и международных стандартах, а для некоторых методик испытаний не было однозначного понимания среди участников рабочих групп, например, в отношении испытаний на проверку точности измерения на цифровом выходе и точности измерения гармоник, проверка соответствия протокола передачи информации, проверка синхронизации и т.д. На основе собственного, а также общедоступного опыта российских производителей цифрового оборудования нами были предложены варианты методик по всем спорным вопросам и требованиям для исключения неоднозначности и двусмысленности. Параллельно с этим каждый пункт соответствующей части гармонизировался с уже имеющимися частями данной серии проектов стандартов и актуализировался с учетом современных реалий в нашей стране.

В результате мы получили три документа, охватывающих весь объем информации, необходимой для создания измерительных трансформаторов, пригодных для использования на цифровых подстанциях, при этом ссылаясь в них лишь на стандарты данной серии проектов стандартов, не требуя наличия доступа к дополнительным ресурсам:

ГОСТ Р (проект) – 6 «Общие технические условия на электронные трансформаторы»;

ГОСТ Р (проект) – 7 и ГОСТ Р (проект) - 8 дополнительные требования к трансформаторам напряжении и тока, соответственно.

В них представлены требования:

- к системе передачи цифрового сигнала;
- к цифровому интерфейсу обмена информацией;
- к протоколу передачи информации;
- к синхронизации сигнала;
- к интеграции трансформатора в АСУ ТП.

В течение следующего года мы планируем проработать все полученные замечания и утвердить проекты стандартов в качестве ГОСТ Р.

Ведутся работы над ГОСТ Р (проект) - 9 «Технические условия на автономные устройства сопряжения с шиной процесса». Параллельно готовится перевод IEC 61869-13 для официальной публикации на русском языке. Это поможет быстрее учесть зарубежный опыт в данном направлении, внести ясность в понимание базовых принципов работы подобного оборудования и использовать это при разработке национальных стандартов.

В завершение мы хотели бы призвать каждого к участию в разработке документов отечественной нормативной базы. Мы живем в одной стране и должны представлять наши общие интересы на международном уровне, а не ограничиваться лишь единичными представителями отдельных компаний, каждый из которых пытается лоббировать свои интересы или касаться лишь тех вопросов, с которыми он связан.

В РФ необходимо развитие национальных стандартов для всех видов измерительных трансформаторов, не ограничиваясь только индуктивными трансформаторами тока и напряжения, и к данной работе должны быть привлечены специалисты различных областей, проектирующих организаций, изготовителей, испытательных лабораторий, потребителей. Такой союз специалистов позволит создавать качественные и технически грамотные стандарты и, как следствие, надежное оборудование ●

ОПЫТ УЧАСТИЯ В НАЛАДКЕ ЦИФРОВОЙ ПОДСТАНЦИИ 330 кВ «МЕТАЛЛУРГИЧЕСКАЯ», БЕЛОРУССИЯ, РУП «ГОМЕЛЬЭНЕРГО»

Статья посвящена итогом сдачи в эксплуатацию цифровой подстанции 330/110/10 «Металлургическая» РУП «Гомельэнерго», поставку оборудования по которой осуществлялось компанией GE, а наладка – силами локальной наладочной организации.

Глеб Соколов
Руководитель отдела GE Grid Solutions

Компания GE реализовала новый проект по внедрению технологии цифровой подстанции. Внедрение новых технических решений – это всегда вызов как для производителя вторичного оборудования, так и для конечного заказчика (наладчика) – проектной организации.

Описание проекта

В августе 2019 года была сдана в эксплуатацию цифровая ПС 330/110/10 «Металлургическая» РУП «Гомельэнерго» филиале «Жлобинские электрические сети». Целью строительства подстанции было организовать надежное энергоснабжение расширения ОАО «БМЗ – управляющая компания холдинга «БМК». Первичное коммутационное оборудование располагается на ОРУ.

В начале проекта руководство РУП «Гомельэнерго» приняло смелое решение сделать подстанцию цифровой, с передачей измерений в цифровом виде (МЭК 61850-9.2LE) и работе с дискретными сигналами с помощью GOOSE-сигналов (включая отключение выключателей с применением GOOSE). Дублирование контуров управления аналоговый/цифровой не применялось. Так как выполнялась только реконструкция подстанции, были использованы традиционные измерительные трансформаторы, на керны которых были установлены соответствующие устройства оцифровки (merging units) – MU320.

Цифровые измерения выдаются в два сегмента шины процесса, к которым подключены два комплекта основных защит, что обеспечивает надежность работы системы релейной защиты. Оцифровка дискретной информации осуществляется устройствами сопряжения (merging unit) SCU с выдачей GOOSE сообщений в станционную шины. Архитектура станционной шины реализована с использованием протокола резервирования PRP с передачей по ней GOOSE и MMS сообщений. Синхронизация времени осуществляется по протоколу PTP с использованием серверов времени RT434. В качестве цифровых терминалов РЗА применены терминалы серии P40 Agile, производства GE. В качестве Ethernet коммутаторов применены промышленные коммутаторы серии S2024.

Наладка подстанции

Наладка объекта осуществлялась силами местных специалистов. В РУП «Гомельэнерго» уже с 2014 года эксплуатируется цифровая подстанция 110 кВ «Приречная», но для ее реализации была применена другая технология создания цифровой подстанции – HardFiber.

Рис. 1. Щит управления

Рис. 2. Шкаф наружной установки с устройствами УСШ и терминалами РЗА

Подстанция «Металлургическая» целиком базируется на стандарте МЭК 61850 и включает существенно больше оборудования по сравнению с ПС 110 «Приречная». В силу этого при наладке этой цифровой подстанции наладчикам пришлось учиться многому новому и столкнуться с новыми техническими вопросами. В целом, этап наладки успешно завершен, наладчиками получен бесценный опыт, а именно, на что стоит обращать внимание при наладке цифровых подстанции и какие применять техническое решения при проектировании/наладки цифровых подстанций класса напряжения 330 кВ. Помимо этого, сформирован ряд предложений и замечаний к оборудованию, которые обрабатываются производителем вторичного оборудования GE. Надо отметить, что в настоящий момент РУП «Гомельэнерго» имеет уникальный опыт наладки цифровых магистральных подстанций, которым не располагает ни одно другое предприятие в рамках Белоруссии и СНГ.

Практический опыт

Для компании GE этот проект был сложен тем, что мы выполняли роль только поставщика оборудования и оказывали штатную техническую поддержку. Обращение к производителю шло только при возникновении тех или иных технических вопросов (проблем). При этом сроки выполнения наладки были ограничены и, соответственно, требовалось осуществлять техническую поддержку в кратчайшие сроки. Со своей стороны мы, как производитель, попытались реализовать этот сервис с учетом пожелания заказчика по ускорению оперативности технической поддержки.

Дополнительно надо отметить высокий профессиональный уровень специалистов РУП «Гомельэнерго». Многие их пожелания и рекомендации по адаптации программного и аппаратного обеспечения будут учтены и реализованы в следующих программных прошивках оборудования.

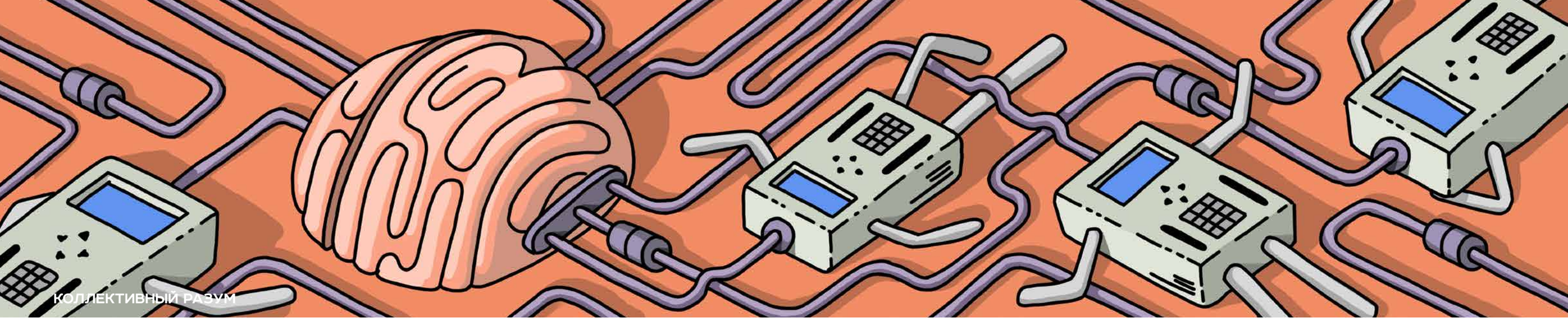
В качестве практического опыта стало понятно, что при реализации таких проектов крайне важную роль имеют типизированные технические решения, позволяющие избежать многих технических вопросов, и настройка сетевого оборудования в части фильтрации информации в коммуникационных шинах.

Заключение

В настоящий момент подстанция передается в работу, возникшие вопросы так или иначе будут сняты. В целом проект можно считать успешно завершенным. По его итогам компания GE планируем усилить команду технической поддержки, работающую по проектам в Белоруссии, и предложить заказчику рассмотреть варианты перехода к 100 % цифровой подстанции с использованием оптических трансформаторов тока и напряжения в качестве первичных источников измерений ●

Михаил Хайкин
Начальник службы релейной защиты и автоматики РУП «Гомельэнерго»

«Среди особенностей проектирования объектов с «шиной процесса» и «шиной станции» я бы выделил необходимость наличия в проекте архитектуры и топологии сетей передачи данных, таблицы GOOSE-коммуникаций, проработки вопросов необходимости и методов фильтрации трафика, таблицы параметризации всего сетевого оборудования, также расчетов загрузки сетей передачи данных, разработки «логической» схемы синхронизации устройств и анализа последствий выхода из строя отдельных устройств с разработкой алгоритма восстановления работоспособнос-ти, а также списка сигналов для SCADA систем» ●



«Коллективный разум» – уникальная рубрика на страницах журнала «Цифровая подстанция» и одноименного сайта! Ее цель – привлечь максимальное количество специалистов из России и мира для решения острых вопросов, с которыми не справиться в одиночку! Все тексты, приведенные в данной рубрике, – личные мнения специалистов и никак не отражают позиции компаний по рассматриваемым вопросам.

ФИЗИЧЕСКАЯ СЕГМЕНТАЦИЯ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ: ЗА И ПРОТИВ

В каждом СМИ найдется повод, чтобы заявить о своей непохожести на другие издания, предмет его гордости, его визитная карточка. В журнале «Цифровая подстанция» это можно сказать о рубрике Коллективный разум, в которой мы проводим опрос отечественных и зарубежных профессионалов по самым острым темам. Ответы могут быть спорными, даже в чем-то провокационными, но именно в этом, сборке разнообразных мнений, и состоит сила рубрики, ее привлекательность. На этот раз мы задавали вопросы, касающиеся физической сегментации локальных вычислительных сетей на цифровой подстанции.

1. Как вы считаете, целесообразна ли физическая сегментация локальных вычислительных сетей на цифровой подстанции?
2. Какие факторы в пользу / против этого решения вы можете назвать?
3. Если да, то по какому принципу, на ваш взгляд, должна быть выполнена такая сегментация (например, по видам трафика, по географическому расположению, по типам подключаемого оборудования)?
4. Если сегментация сетей выполняется, то следует ли делать связь между сегментами с помощью межсетевых экранов для обеспечения доступа к каждому из сегментов из одной точки?
5. Должны ли подходы к сегментации отличаться в зависимости от класса напряжения присоединений, устройства которых включены в локальную сеть, и какие различия вы бы предложили?
6. Какую роль при выборе принципов сегментации сетей должен играть вопрос информационной безопасности?

Николай Дони

Директор по науке – заведующий отделом систем РЗА ООО НПП «ЭКРА», к.т.н.

1. Да, физическое разделение ЛВС целесообразно.

2. В настоящее время ЦПС не привносит ничего нового с точки зрения РЗА, меняется только среда передачи данных. С целью, как минимум, не ухудшить время локализации и устранения аварии, основной задачей для ЦПС является бесперебойная работы «шины процесса». Работа «шины процесса» непосредственно связана с тем, какие еще функции и задачи выполняет ЛВС, в которой и реализован «процесс». Например, некорректная настройка оборудования с целью обеспечения максимально возможного, на применяемой аппаратно-программной базе, уровня информационной безопасности, может привести к невозможности передачи данных с необходимым временем. Обратная ситуация – недостаточно хорошо настроенная система ИБ может стать причиной, по которой ЦПС будет подвержена дистанционному взлому. Избежать подобного можно, например, изолировав «шину процесса» от «шины станции» на физическом уровне.

3. Исходя из вопроса разделения зон ответственности, на наш взгляд, имеет смысл разделение ЛВС по функциональному признаку. Так, для обеспечения надежности и исключения вероятности влияния, например, работ по АСУ ТП на устройства РЗА, целесообразно отделить «шину процесса» (GOOSE-сообщения и SV-потоки) от «шины станции» (MMS-отчеты и команды), ЛВС для АИСКУЭ также следует выполнять изолировано от остальных сетей.

Кроме того, для организации «шины процесса» требуется более дорогое сетевое оборудование, аппаратно поддерживающее прецизионную синхронизацию времени (IEEE 1588) и требуются «бесшовные» методы резервирования (PRP, HSR). К сетевому оборудованию «шины станции» таких требований нет, поэтому для этого сегмента можно использовать более дешевое сетевое оборудование.

4. При проведении наладки системы РЗА наличие единой точки доступа будет большим плюсом. Но не стоит забывать, что наличие единой точки доступа также делает систему в целом более уязвимой. Один из возможных вариантов – ограничить использование портов, или совсем отключить их на межсетевых экранах, после проведения наладочных работ.

5. В настоящее время мы не прорабатывали вопросы сегментирования сетей в зависимости от класса напряжения. На практике, для объектов, на которых мы реализовали системы РЗА с применением технологии ЦПС, не применялась сегментация в зависимости от класса напряжения.

6. Вопрос информационной безопасности давно перешел из теоретической плоскости в практическую. Кибератаки – это уже не что-то неосязаемое, а вполне реальная угроза. При выборе принципов сегментации сетей целесообразно руководствоваться соображениями максимальной безопасности объектов энергетики, но не забывать, что ЛВС на ЦПС является средой передачи релейной информации, транспортировка которой критична ко времени. Оптимальным, с точки зрения информационной безопасности и быстродействия, на наш взгляд, будет полная физическая изоляция «шины процесса» ●

ЦПС не привносит ничего нового с точки зрения РЗА, меняется только среда передачи данных. С целью, как минимум, не ухудшить время локализации и устранения аварии, основной задачей для ЦПС является бесперебойная работы «шины процесса».

Михаил Селезнев

Начальник отдела АСУ ТП и метрологии департамента релейной защиты, метрологии и автоматизированных систем управления технологическими процессами ПАО «ФСК ЕЭС»

ции во всех точках, процессах и системах, поэтому я считаю, что физическая сегментация должна применяться только в случаях, когда этого невозможно избежать. Кроме того, на сегодняшний день достаточно технологий, чтобы безопасно и эффективно разделить трафик внутри одной физической сети.

2. Ранее считалось, что физическая сегментация – основной метод выполнения требований по информационной безопасности, однако сейчас этот подход является устаревшим. Это был главный фактор в пользу физической сегментации. В настоящее время стало очевидно, что данные техпроцесса необходимы в корпоративных системах.

Физически разделить сети очень часто стараются, чтобы разграничить зоны ответственности, например, между релейщиками и асушниками по видам трафика GOOSE, MMS и SV. На мой взгляд, это неэффективно, необходимо менять организационную структуру в соответствии с возможностями, которые предоставляет современная техника и технологии. В противном случае это может привести к увеличению количества оборудования и снижению надежности.

3. Если без сегментации все же не обойтись, например, при достижении максимума пропускной способности сети, ее целесообразно провести по типам подключаемых систем, а также по классам напряжения на подстанции.

4. Да, безусловно, не уверен, что при этом сегментация может считаться физической.

5. Чем выше класс напряжения, тем больше устройств и систем начинает применяться на одном присоединении, к тому же, предъявляются повышенные требования по быстродействию, поэтому на высоких классах напряжения физическая сегментация наиболее актуальна для выполнения требований по быстродействию.

6. На сегодняшний день наиболее эффективным методом выполнения требований по информационной безопасности считается Secure by design. Т.е. когда вопросы информационной безопасности решаются на этапе разработки и построения системы, а не потом, когда применяются на готовых системах средства наложенной безопасности. Исходя из этого, выбор принципов сегментации должен быть одним из способов выполнения требований по информационной безопасности ●

Физически разделить сети часто стараются, чтобы разграничить зоны ответственности, например, между релейщиками и асушниками. На мой взгляд, это неэффективно, необходимо менять организационную структуру в соответствии с возможностями, которые предоставляет современная техника и технологии.

Алексей Аношин

Исполнительный директор ООО «Теквел»

1. Если под физической сегментацией понимать полное отделение каких-либо сегментов сети без возможности доступа к ним на сетевом уровне, то такая сегментация не целесообразна, более того, скорее вредна. Если же понимать под этим выделение физических сегментов (например, «шины процесса») с возможностью доступа туда на сетевом уровне (например, через межсетевые экраны), то такая сегментация может быть целесообразной. Например, выделение в отдельный сегмент сети, к которой подключаются устройства полевого уровня (ПАС / ПДС) и устройства защиты соответствующих присоединений – это распространенная и логичная практика. Стоит, правда, сказать, что физическое выделение какого-либо сегмента сети вовсе не избавляет от необходимости логической сегментации (то есть обеспечения фильтрации трафика на коммутаторах).

2. В пользу физической сегментации сети можно выделить следующие факторы: сокращение объемов трафика, передаваемых по сети (актуально, в первую очередь, для объектов с обширным применением протокола SV), упрощение процесса проектирования и наладки оборудования (физическая сегментация проще и нагляднее логической), разделение зон ответственности служб (например, «шина процесса» для релейщиков, «шина станции» для АСУшников).

Те же факторы, если посмотреть на них под другим углом, говорят и против этого решения. Во-первых, все современные управляемые сетевые коммутаторы позволяют управлять распространением данных по сети, так что сегментировать сеть для того, чтобы разделить данные в этой сети, вовсе не требуется. Во-вторых, зачастую вопросы физической сегментации неминуемо упираются в необходимость передачи, пускай и малого количества, сигналов между сегментами, и в таком случае решение этой задачи оказывается уже весьма нетривиальным. В-третьих, сегментация на самом деле не решает задачи разделения доступа к сети специалистов разных служб, поскольку в таком случае, например, может потребовать создания 3 отдельных сетей SV: для РЗА, АСУ ТП и учета, что видится совершенно безрассудным. Против полного выделения каких-либо сегментов (то есть без возможности доступа на сетевом уровне к указанным сегментам) говорит лишение возможности мониторинга этих сегментов без прямого доступа к этому сегменту (физически) либо без посредников (устройств, подключенных в этот сегмент). Если обратиться к практике обслуживания современных IT-систем, то в них инженер со своего рабочего места сегодня может легко проконтролировать состояние любого сетевого узла, вплоть до каждого порта коммутатора, что, очевидно, ведет к существенной оптимизации затрат на обслуживание. Физическое отделение, каких-либо сегментов, очевидно, приведет к невозможности такого.

3. С моей точки зрения, единственный целесообразный вариант физической сегментации сетей – их разделение по физическому местоположению. То есть сегмент сети, объединяющий устройства полевого уровня (ПАС / ПДС), расположенные на ОРУ, и устройства уровня присоединения (РЗА, КП, счетчики), расположенные в ОПУ, может быть целесообразно выделить (при условии, что устройства РЗА, КП имеют выделенный интерфейс).

4. Да, как уже отмечалось выше, даже в случае сегментации по местоположению отдельных сегментов сетей между ними все равно должны быть обеспечены соединения. Например, доступ к устройствам полевого уровня должен быть обеспечен с устройств верхнего уровня, чтобы получать без посредников диагностическую информацию.

5. Да, но это как правило обусловлено не столько самим классом напряжения, сколько физическим расположением вторичного оборудования для разных классов напряжения. Например, очевидно, что для оборудования в КРУ не требуется никакая сегментация сетей, поскольку без видимых эффектов она будет только приводить к удорожанию. На высоких же классах напряжения с большим количеством устройств из расчета на присоединение может быть целесообразно даже выделение сегментов на отдельное присоединение или пару присоединений (например, в случае схемы 3/2).

6. Вопрос информационной безопасности, безусловно, должен рассматриваться в числе остальных влияющих факторов. Однако, правильнее, на мой взгляд, будет говорить о том, что решения по информационной безопасности должны учитывать наличие тех или иных выделенных сегментов сети, а не наоборот ●

Все современные управляемые сетевые коммутаторы позволяют управлять распространением данных по сети, так что сегментировать сеть для того, чтобы разделить данные в этой сети, вовсе не требуется. Сегментация на самом деле не решает задачи разделения доступа к сети специалистов разных служб.

Максим Грибков

Директор департамента РЗА ПАО «МОЭСК»

1. Физическая сегментация локальных вычислительных сетей на цифровой подстанции необходима.

2. Основной фактор в пользу физического разделения локальных вычислительных сетей – снижение загрузки по трафику коммутаторов и отсутствие необходимости настройки фильтрации SV-потоков и Goose-сообщений. Также немаловажным фактором является повышение уровня информационной безопасности и разделение уровня эксплуатационной ответственности между эксплуатационными подразделениями.

3. Сегментация должна быть выполнена с учетом выделения трех отдельных подсетей:

- SV -потоки;
- Goose-сообщения;
- mms.

При этом для каждой подсети должен быть свой сервер единого времени.

4. Нет, не следует, в целях повышения уровня информационной безопасности .

5. Подходы к сегментации отличаться не должны, типизация решений снижает возможное количество ошибок.

6. Одну из основных ●

Артем Перепелицын

Директор по управлению проектами АО «НИЦ ЕЭС»

1. С точки зрения реализации основных функций ЦПС, сегментирование нецелесообразно. Более рациональным представляется логическое разделение. Возможно, есть целесообразность физического сегментирования ЛВС по требованиям информационной безопасности для объектов с высокой категорией КИИ.

2. Доводы «за» физическое сегментирование:

- некоторое упрощение параметрирования оборудования ЛВС в отличие от логического разделения;

• улучшение информационной безопасности.

Доводы «против»:

• увеличение количества коммутаторов, что равно увеличению как капитальных затрат на сооружение объекта, так и затрат на эксплуатацию. Стоимость - это один из ключевых факторов сдерживающих внедрение технологии ЦПС;

• на практике возникает техническая необходимость связи со всеми сегментами ЛВС. При физическом сегментировании, задачи тоже решаются, но технические решения получаются не вполне рациональными.

4. Не рационально. Это еще большее увеличение стоимости объекта.

5. Класс напряжения, на мой взгляд, не принципиален. Ключевую роль в решении о физическом сегментировании играют решения о необходимой надежности системы с точки зрения информационной безопасности, которая хоть и связана с классом напряжения, но не напрямую.

6. На мой взгляд, информационная безопасность – единственный обоснованный аргумент в пользу физической сегментации ●

Иван Скрыпник

Руководитель отдела телекоммуникаций компании «ЛАНИТ-Интеграция»

1. Однозначного ответа на этот вопрос не существует. Сегментацию локальных вычислительных сетей вполне можно выполнить как физически, так и логически без какого-либо ущерба для функционала.

Существуют и давно используются техники сегментации ЛВС, основанные на виртуализации, которые позволяют это сделать и на канальном уровне модели OSI – VLAN, и на сетевом уровне – VRF.

2. «За» физическую сегментацию локальных вычислительных сетей есть следующие факторы:

• высокая отказоустойчивость. Если вдруг начинаются аппаратные проблемы на активном сетевом оборудовании или канале связи, то, конечно, они способны повлиять на все логические сегменты. Физическое разделение оборудования и каналов связи снимает эту проблему;

Межсетевые экраны последнего поколения, системы предотвращения вторжений, глубокое инспектирование пакетов и другие инструменты позволяют обнаруживать и блокировать даже самые сложные сетевые угрозы. Но окончательное решение всегда остается за архитектором.

• упрощается внедрение, поддержка и модернизация. На этапе пуско-наладки требуемая настройка сетевого оборудования проще, чем в случае, когда требуется планирование виртуальных сущностей. Персоналу в целом проще поддерживать такие системы, ниже требуемый экспертный уровень специалистов сопровождения. То же самое применимо и в случае модернизации ЛВС;

• ниже цена ошибок. Человеческий фактор часто является причиной сбоев работы систем. Это могут быть ошибки дизайна сети, конфигурации сетевого оборудования или обнаруженные уязвимости в коде устройств. В случае логического сегментирования возрастают риски.

Но есть факторы, которые указывают на то, что более предпочтительна логическая сегментация:

• ниже стоимость. Конечно, в случае логической сегментации, совместно используется общее сетевое оборудование, не требуется прокладка дополнительных, иногда очень дорогостоящих, линий связи, что очень снижает стоимость, поддержку и эксплуатацию ЛВС. Меньше оборудования – меньше обслуживающего персонала, ниже затраты на оплату труда, электроэнергии, ниже стоимость модернизации;

• ниже нагрузка на обслуживающий персонал. Из-за меньшего количества оборудования и «окон» управления;

• гибкие возможности адаптации. Проще реализуются возможности внесения изменений. Например, изменение существующих сегментов: расширение, объединение, дробление, добавления новых сегментов. Задача касается только изменения конфигурации устройств, не требуя долгих и дорогостоящих действий вроде закупки нового оборудования, прокладки новых кабелей и т.д.

3. Обычно сегментация делается по функционалу, то есть по назначению подсистемы. Но это не аксиома. В каждом индивидуальном случае могут быть факторы, влияющие на выбор архитектора.

4. Безусловно, с точки зрения удобства эксплуатации и администрирования удобнее, чтобы связь между сегментами была, хотя бы для целей администрирования и мониторинга состояния ЛВС «из одного окна». Индустрия сейчас предлагает богатый выбор межсетевых экранов, способных обеспечить очень тонкую настройку правил взаимодействия между сегментами. Но опять-таки в каждом индивидуальном случае архитектура решения может быть продиктована наличием дополнительных факторов, которые требуется учитывать.

5. Логическая и физическая сегментации эквивалентны, если используется качественное оборудования зарекомендовавших себя вендоров, резервирование оборудования и каналов связи, а также при отсутствии руководящих требований.

6. С точки зрения информационной безопасности физическая сегментация иногда бывает необходима. Если такого требования нет, то современные инструменты обеспечения ИБ на сети позволяют обеспечить очень высокие показатели защиты. Межсетевые экраны последнего поколения, системы предотвращения вторжений, DPI (глубокое инспектирование пакетов), профилирование подключенных устройств, системы поведенческого анализа и другие инструменты позволяют обнаруживать и блокировать даже самые сложные сетевые угрозы. Окончательное решение всегда остается за архитектором, который, как правило, учитывает весь спектр доступной информации и способен оценить риски ●

Игорь Метс

Elering AS, Эстония

1. Суть вопроса может сводиться скорее к экономической и эксплуатационной эффективности технического решения, чем к обеспечению санкционированного доступа ко всем элементам логических узлов и наделению широкими возможностями мониторинга информационного потока на подстанции.

В зависимости от приоритета поставленной задачи в исходном техническом задании или его технических требованиях назначаются ключевые критерии в отношении величин доступности, надежности, степени резервирования, среднего времени до отказа и других неотъемлемых параметров системы, в данном случае касаемо ЛВС МЭК 61850. Если определяющим фактором является цена, то остальные вышеназванные критерии могут сильно повлиять на выбор одного или другого предложения по техническим решениям. Зачастую, увеличение величины надежности одного компонента системы на 1 % может вызвать увеличение стоимости целого проекта в 1,5 раза.

Исходя из вышесказанного, можно сформулировать целесообразность физической сегментации ЛВС на подстанции, предварительно ответив на следующие вопросы:

• какая цель физической сегментации ЛВС (передача критических по времени событий при недоступности узла напр., при условии «n-1»; повышение пропускной способности информационного потока; разделение ЛВС по принадлежности собственнику; и др.):

• где «работает» физическая сегментация ЛВС;

• какие услуги/функции предоставляют ЛВС (здесь, стоит упомянуть анализ рисков, что должен быть составлен на момент рассматривания разных предложений);

• как будет осуществляться наладка, тестирование, обновление и мониторинг системы ЛВС при дальнейшей эксплуатации;

• какие будущие планы по расширению ЛВС планируются, как это осуществить в случае необходимости и как при этом обеспечить взаимозаменяемость или совместимость линеек, версий продукта как внутри семейства, так и между разными производителями (закрытая проприетарная система; открытая система на базе МЭК, IEC, EN; открытая система на базе МЭК, IEC, EN с некоторыми проприетарными решениями, неподдерживаемые другими аппаратными и/или программными производителями).

2. Общие факторы, влияющие на принятие решения об использовании физической сегментации ЛВС на подстанции, приведен ниже.

За:

• контрактное разграничение зон ответственности;

• распределение нагрузки информационного потока по форме и типам пользователей;

• распределение нагрузки по шинам процесса и станции.

Против:

• стоимость оборудования;

• выход их строя оборудования ведет за собой сбой выполнения услуги / функции.

3. В этом вопросе нет единого подхода – это определяет энергетическое предприятие. Поэтому, используются различные варианты принципов сегментации ЛВС.

Например,

• по типу физической топологии ЛВС подстанции:

— локальная (круговая, звезда, цепи, смешанная);

— наружная (собственные расширенные подсоединения, подсоединения Третьей Стороны);

— распределенная (локальная + наружная);

• по типу информационных потоков:

— дигитальные измерения МЭК 61850-9-2;

— MMS, GOOSE, временная синхронизация, удаленный доступ;

• по видам оборудования релейной защиты и других средств автоматики на подстанции:

— основная релейная защита №1;

— основная релейная защита №1+x;

— резервная релейная защита №1;

— резервная релейная защита №1+x:

— различные системы автоматики;

— вспомогательные системы автоматики;

• по классам напряжения;

• по степени важности (устройства, обслуживающие транзитные высоковольтные линии электропередачи; все релейное оборудование узловой подстанции; все релейное оборудование, обслуживающее резервное кольцо электропередач и др.);

• по видам производителей обо-

рудования релейной защиты других средств автоматики.

4. Когда реализуется сегментация ЛВС, то прежде следует определить степени риска и ущерба, связанные с проникновением в какой-либо или в несколькие сегменты ЛВС. Далее, как уже было упомянуто в предыдущих пунктах, необходимо определить четкие границы ответственности за оборудование, т.к. все «чужие» устройства должны, как правило, оставаться за межсетевым экраном.

Однако, при соответствующей договоренности, в т.н. отдельной специфической «демилитаризированной зоне» DMZ должны быть все те сегменты ЛВС, которые не относятся к одному предприятию, но также являются важными звеньями для организации системной автоматики (напр., между Сетевым оператором и оператором распределительных сетей).

Будучи в структуре одного предприятия, сегменты ЛВС могут находиться за межсетевым экраном и не иметь централизованного доступа, в целях энергетической безопасности и обеспечения непрерывной подачи электроэнергии.

Отдельного внимания необходимо удостоить и устройства поставщика / оператора Телекома, если таковой используется и не является частью Сетевого оператора / энергетической компании. В этой части, нужно четко понимать и прослеживать маршрутизацию информационных потоков подстанции, осуществляемую Телеком оператором. Это, прежде всего, касается тех подстанций, которые связанны технологически (МЭК 61850-9-2 измерения по шине процесса, передача GOOSE и т.п.).

5. Ответ на этот вопрос можно найти в ответе на вопрос 3.

6. В наши дни, кибербезопасность популярная тема не только в СМИ, но и во всех сферах, которые подверглись дигитализации и дискретизации, попутно получив основанный на TCP/IP пользовательский интерфейс. Эту тему невозможно описать несколькими предложениями, поэтому стоит ограничиться основными характеристиками, которые необходимо помнить:

- кибербезопасность нуждается в постоянном мониторинге и анализе событий;
- со временем без обновлений оставшаяся киберзащита всегда ухудшается;
- за кибератаками могут стоять как люди извне, так и люди изнутри;
- всегда стоит обучать свой персонал ●

Евгений Войтенко
Инженер СРЗА РУП «Гомельэнерго»,
Республика Беларусь

1. Считаю, что физическая сегментация ЛВС на цифровой подстанции обязательна.

2. Аргументы «против» физической сегментации:

- физическое разделение сети всегда сопровождается большим количеством коммутаторов, а это дорого;
- разделение сети требует большего количества серверов времени;
- отсутствие полной картины по процессом происходящем на подстанции с одного переносного АРМ. При наладки и эксплуатации появляется необходимость (для разных целей) сниффером отследить пакеты в сети.

Аргументы «за» физическую сегментацию:

- удобство в обслуживании. При проверке устройства РЗА, подключенного к одной физической сети, нет излишнего воздействия сигналами на устройства, находящиеся в другой сети;
- повышается надежность. При выходе из строя одного из элементов сети коммутатор локализует проблему только на одном сегменте комплекса РЗА;
- снижение нагрузки на сетевое оборудование во время нормальной работы и во время аварийных процессов в первичной сети.

3. Считаю рациональным разделять сети сразу по двум критериям. Первое: сети SV потоков должны быть отделены от сети GOOSE + MMS. Второе: при наличии на ПС двух независимых комплексов РЗА сети, которые их обслуживают, тоже должны быть физически разделены. Третье: при строительстве ПС с большим количеством присоединений сети можно разделять по классам первичного напряжения или по присоединениям.

4. Необходимость такой связи определяет архитектура построения верхнего уровня. Если SCADA состоит из нескольких контроллеров, то приоритетно на каждую физическую сеть устанавливать отдельный контроллер. И именно такая архитектура верхнего уровня, на мой взгляд, верная. Другой задачи, для которой необходимо каким-то образом объединить физически разделенные сети, я не вижу.

5. Считаю, что такое разделение искусственное и его не нужно делать. Принципы работы сети, в общем, не отличаются от того, какой класс напряжения обслуживает устройство РЗА, подключенное в ЛВС. Единственный видимый аргумент такого разделения – это повышение надежности для сети, обслуживающей сверхвысокий класс напряжения. Однако определяющими все-таки должны быть критерии, изложенные в п.3

6. На этот вопрос сложно отвечать специалисту РЗА. Для компетентного ответа необходимо знать факторы, влияющие на кибербезопасность. Безусловно, если проектом рекомендовано разделять по этому критерию сети, то это необходимо учитывать. Но это не должно быть определяющим при разработке архитектуры сети ●

Разработка изделий и продукции на основе технологии цифровых двойников позволяет в кратчайшие сроки создавать глобально конкурентоспособную и востребованную высокотехнологичную продукцию, значительно снижать объемы физических и натурных испытаний, которые в традиционном подходе необходимы для «доводки изделия до требуемых характеристик путем большого числа испытаний опытных образцов», что, в целом, в сравнении с традиционными подходами позволяет обеспечивать снижение временных, финансовых и иных ресурсных затрат в разы, в некоторых случаях – в 10 раз и более.

ОПРЕДЕЛЕНИЕ, РАЗРАБОТКА И ПРИМЕНЕНИЕ ЦИФРОВЫХ ДВОЙНИКОВ

ПОДХОД ЦЕНТРА КОМПЕТЕНЦИЙ НТИ СПБПУ «НОВЫЕ ПРОИЗВОДСТВЕННЫЕ ТЕХНОЛОГИИ»[1]

Алексей Боровков

Проректор по перспективным проектам СПбПУ, руководитель Центра компетенций НТИ СПбПУ «Новые производственные технологии», руководитель Инжинирингового центра (CompMechLab®) СПбПУ

Юрий Рябов

Начальник отдела технологического и промышленного форсайта Инжинирингового центра (CompMechLab®) СПбПУ

Развитие цифровой экономики (Digital Economy) в современном мире во многом обусловлено эффективной работой со стремительно увеличивающимися большими объемами данных (Big Data), а точнее, с содержательными («умными») данными (Smart Big Data), включая снижение объемов «мусорных» данных и трансакционных издержек, а также повышение прозрачности и наглядности процессов генерации и обработки данных.

Центральное место в экономике по праву занимает материальное производство – высокотехнологичная промышленность, отвечающая, в первую очередь, требованиям высокой производительности труда, экономической эффективности и глобальной конкурентоспособности.

Для удовлетворения этим требованиям необходимым и актуальным этапом развития высокотехнологичной промышленности является цифровая трансформация бизнес-процессов и бизнес-моделей, то есть фактически трансформация высокотехнологичной промышленности в цифровую промышленность ***путем разработки и применения цифровых двойников (Digital Twin, DT; учитывая опыт Центра компетенций НТИ СПбПУ «Новые производственные технологии»):***

- поведения в различных условиях эксплуатации реальных материалов, объектов / продуктов / изделий / систем / машин / конструкций / оборудования / … / киберфизических систем на основе семейства взаимоувязанных математических моделей высокого уровня адекватности реальным материалам, объектам и физико-механическим процессам, которые можно описать лишь нестационарными нелинейными дифференциальными уравнениями в частных производных (цифровой двойник 1-го типа – ***DT-1***);
- разнообразных технологических процессов, с помощью которых создаются реальные материалы и реальные объекты / изделия / продукты / … (например, литейные процессы для металлических изделий, процессы вакуумной инфузии для композитных конструкций, процессы штамповки, металлообработки, сварки, сборки и т. д.), которые представляют собой нестационарные нелинейные процессы, описываемые как и в случае ***DT-1*** нелинейными нестационарными уравнениями в частных производных (цифровой двойник 2-го типа – ***DT-2***).

[1] Статья подготовлена на основе краткого доклада «Цифровые двойники в высокотехнологичной промышленности», представленного в рамках Первого Всероссийского форума «Новые производственные технологии», состоявшегося 3–4 октября 2019 года в СПбПУ [1]

Важно отметить, что эти глобальные изменения сопровождаются развитием принципиально новых бизнес-процессов и бизнес-моделей на всех уровнях и, конечно же, изменением корпоративной культуры в компаниях.

Цифровой двойник: ключевые компоненты

Согласно определению Центра компетенций НТИ СПбПУ «Новые производственные технологии», ***цифровой двойник – это, прежде всего, технология, процесс проектирования***, в основе которого лежит разработка и применение семейства сложных мультидисциплинарных математических моделей, описываемых 3D нестационарными нелинейными дифференциальными уравнениями в частных производных [2], с высоким уровнем адекватности:

- поведению в различных условиях эксплуатации реальных материалов, объектов / систем / машин / конструкций / …
- разнообразным технологическим процессам, с помощью которых создаются реальные материалы и реальные объекты / изделия / продукты / …,

– и, конечно, ***цифровой двойник – это технология (процесс) создания глобально конкурентоспособной продукции***, интегрирующая следующие необходимые ключевые компоненты [1]:

0. ***Best-in-class («лучшие в классе») технологии мирового уровня***, из которых путем комплексирования формируется цепочка создания глобально конкурентоспособной продукции, которую представим формулой, используя (для простоты) для операции комплексирования знак операции суммирования:

$$\boldsymbol{P}^{WL}_{best-in-class} = \sum_{i=1}^{n} \alpha_i \boldsymbol{T}_i^{WL} \quad (1)$$

$$\sum_{i=1}^{n} \alpha_i = 1 \quad (2)$$

где

$\boldsymbol{P}^{WL}_{best-in-class}$ *– best-in-class глобально конкурентоспособная продукция (Product) мирового уровня (WL – World Level),*

$\boldsymbol{T}_i^{WL}$ *– i-ая best-in-class технология мирового уровня,*

α_i *– весовой коэффициент, определяющий вклад i-ой best-in-class технологии мирового уровня* $\boldsymbol{T}_i^{WL}$ *в разработку глобально конкурентоспособной продукции, причём выполняется равенство (2).*

Подчеркнем, что как только в сумме появится (будет применена) технология, не отвечающая мировому уровню, которая не является лучшей для решения рассматриваемого класса задач, то, понятно, общий уровень продукции, измеряемый по тем или иным характеристикам, снижается – достаточно вспомнить общие концепции о «слабых звеньях в цепи» и «узких местах».

1. ***Системный инжиниринг***, «отвечая за всю картину в целом», позволяет обеспечивать и контролировать выполнение требований к продукции на протяжении всего жизненного цикла изделия / системы /…

Следовательно, необходимы подходы и методы, которые позволят в каждый момент времени в процессе разработки «держать в поле зрения» всю систему и все ее взаимодействующие между собой (или – «друг с другом») подсистемы / компоненты / узлы / …

Это особенно важно, поскольку известно, что в конечном итоге уровень конкурентоспособности изделия / системы / … определяется его наиболее «слабыми» компонентами (опять-таки, вспомним концепцию «слабого звена» – «общая сила цепи определяется ее слабейшим звеном», а не компонентами, которые спроектированы и / или произведены на мировом уровне).

2. ***Многоуровневая матрица*** $\boldsymbol{M}_{\text{DT}}$ ***требований / целевых показателей и ресурсных*** (временных, финансовых, технологических, производственных, экологических и т. д.) ***ограничений*** – ключевой элемент технологии разработки цифрового двойника.

Эта матрица целевых показателей $\boldsymbol{M}_{\text{DT}}$ предназначена для обеспечения рациональной «балансировки» большого количества (несколько тысяч или десятков тысяч) целевых характеристик как объекта в целом, так и его компонентов в отдельности, которые, как правило, «конфликтуют» между собой:

- как на одном уровне, так и на разных уровнях описания системы,
- как на одном этапе, так и на разных этапах жизненного цикла,

более того, нужно не только достичь целевых характеристик, но и удовлетворить множеству ресурсных ограничений.

Матрица целевых показателей $\boldsymbol{M}_{\text{DT}}$ должна обеспечивать возможность не только отслеживать взаимное влияние компонентов или нарушение тех или иных ограничений, но и позволять в кратчайшие сроки вносить необходимые изменения и уточнения – осуществлять оперативное «управление требованиями и изменениями» в процессе реализации проекта.

По мере каскадирования и декомпозиции целевых показателей и ограничений, происходит наполнение и последовательное формирование матрицы целевых показателей – как правило, «сверху-вниз», в соответствии с концепцией «нисходящего проектирования» (см. рис. 1).

Последующая итерационная рациональная «балансировка» основана на повышении адекватности описания объекта / системы / машины / конструкции / … на разных этапах жизненного цикла семейством взаимоувязанных мультидисциплинарных математических моделей.

В результате, после проведения физических / натурных / … испытаний и достижения высокого уровня соответствия данным испытаний мы получаем матрицу $\boldsymbol{M}_{\text{DT}}^{(*)}$, которая соответствует цифровому двойнику объекта / системы / машины / кон-

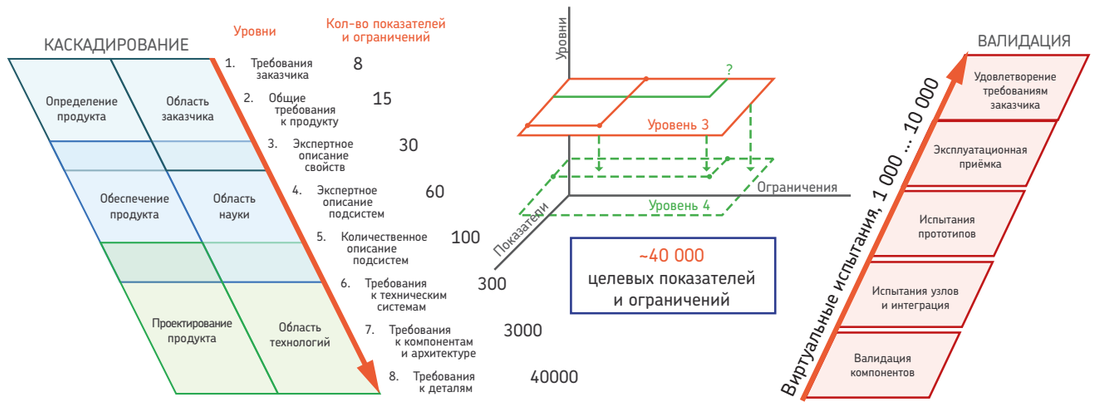


Рис. 1. К формированию матрицы целевых показателей и ресурсных ограничений [1]

струкции / … и для которой характерны рациональная «балансировка» конфликтующих целевых показателей и удовлетворение ресурсным ограничениям.

Для разработки полноценного цифрового двойника на основе семейства мультидисциплинарных математических моделей высокого уровня адекватности принципиально важным и обязательным является этап ***валидации (Validation)*** – процесс определения степени соответствия (уровня адекватности) математических / численных / компьютерных / … моделей реальным объектам / системам / машинам / конструкциям / … и реальным физико-механическим / технологическим / … процессам на основе достоверных данных физических / натурных испытаний.

3. ***«Виртуальные испытания» & «Виртуальные стенды» & «Виртуальные полигоны».***

В процессе разработки полномасштабного цифрового двойника сложных объектов / систем / машин / конструкций / …, необходимо выполнить, как правило, десятки тысяч виртуальных испытаний материалов, узлов, компонентов, подсистем и систем, причём, как показывает опыт, количество виртуальных испытаний примерно соответствует количеству целевых показателей и ограничений, представленных в матрице $\boldsymbol{M}_{\text{DT}}^{(\text{Nм})}$.

Для проведения виртуальных испытаний и получения достоверных результатов необходимы разработка и применение высокоадекватных виртуальных аналогов всего применяемого испытательного оборудования, испытательных стендов и полигонов, которые применяются при проведении физических и натурных испытаний – семейства виртуальных испытательных стендов и виртуальных испытательных полигонов.

Полученное в результате применения всех вышеперечисленных подходов, методов и технологий семейство высокоадекватных мультидисциплинарных математических моделей позволяет обеспечить отличие между результатами виртуальных испытаний и физических / натурных испытаний в пределах ± 5% или меньше.

Цифровой двойник – основа цифровой трансформации бизнес-процессов и бизнес-моделей

В соответствии с определением Центра компетенций НТИ СПбПУ «Новые производственные технологии», цифровой двойник объекта / продукта / изделия / системы / машины / конструкции / … (Digital Twin, DT-1) содержит следующие компоненты:

- DT-1.0. Семейство best-in-class технологий мирового уровня $\boldsymbol{T}_i^{WL}\, i = 1, n$;
- DT-1.1. Семейство матриц целевых показателей / требований и ресурсных ограничений

$$\{\, \boldsymbol{M}_{\text{DT}} : \boldsymbol{M}_{\text{DT}}^{(0)}, \boldsymbol{M}_{\text{DT}}^{(1)}, \dots, \boldsymbol{M}_{\text{DT}}^{(\text{Nм})} \};$$

- DT-1.2. Семейство взаимоувязанных высокоадекватных валидированных мультидисциплинарных математических моделей

$$\{\, \boldsymbol{ММ} : \boldsymbol{ММ}^{(1)}, \boldsymbol{ММ}^{(2)}, \dots, \boldsymbol{ММ}^{(\text{Nмм})} \};$$

- DT-1.3. Множество виртуальных испытаний

$$\{\, \boldsymbol{ВИ} : \boldsymbol{ВИ}^{(1)}, \boldsymbol{ВИ}^{(2)}, \dots, \boldsymbol{ВИ}^{(\text{Nви})} \};$$

- DT-1.4. Множество виртуальных стендов

$$\{\, \boldsymbol{ВИС} : \boldsymbol{ВИС}^{(1)}, \boldsymbol{ВИС}^{(2)}, \dots, \boldsymbol{ВИС}^{(\text{Nвис})} \};$$

- DT-1.5. Множество виртуальных полигонов

$$\{\, \boldsymbol{ВИП} : \boldsymbol{ВИП}^{(1)}, \boldsymbol{ВИП}^{(2)}, \dots, \boldsymbol{ВИП}^{(\text{Nвип})} \}.$$

Все эти компоненты участвуют в процессе разработки цифрового двойника и ***необходимы для обеспечения***:

- ***рационального выбора весовых коэффициентов*** α_i (2), определяющих вклад i-ой best-in-class технологии мирового уровня $\boldsymbol{T}_i^{WL}$ в разработку цифрового двойника объекта / продукта / изделия / системы / машины / конструкции / … ;
- ***глобальной*** (для всей системы) и ***локальной*** (для подсистем, компонентов, деталей, …) рациональной ***«балансировки»*** конфликтующих между собой целевых показателей и ресурсных ограничений,

то есть для получения ***сбалансированной матрицы целевых показателей и ресурсных ограничений*** $\boldsymbol{M}_{\text{DT}}^{(*)}$.

Именно такое комплексное определение позволяет говорить о ***новой парадигме проектирования***, которая делает ***процесс проектирования полностью прозрачным, принятие решений – обоснованным*** (например, на основе сотен / тысяч / десятков тысяч виртуальных испытаний) и ***полностью задокументированным***, при этом значительно снижая многочисленные и разнообразные коммуникационные и трансакционные издержки.

Кроме того, за счет новой парадигмы проектирования становится возможным уйти от традиционной ситуации, когда число изменений изделия (в силу допущенных ошибок или полученных новых, ранее не учтенных сведений, в первую очередь – сведений о поведении опытного образца, полученных по итогам многочисленных и дорогостоящих натурных испытаний) и, соответственно, возрастающие затраты на их внесение распределяются на протяжении всего жизненного цикла разработки – от стадии проектирования до начала серийного производства (известно, что чем позже вносятся изменения, тем большие издержки несет компания). В итоге становится принципиально возможным сосредоточить основную долю изменений и затрат на стадии проектирования, тем самым значительно минимизировать общий объем затрат, сократить издержки и обеспечить создание наукоемких высокотехнологичных изделий нового поколения в кратчайшие сроки (см. рис. 2) [2].

Наконец, новый процесс проектирования, как правило, одновременно происходит ***по нескольким,***

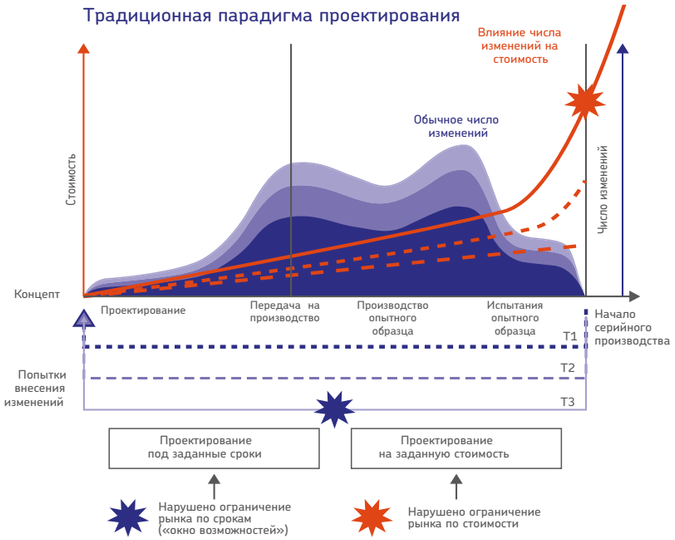


Рис. 2. Сравнение традиционного и передового подхода к проектированию [2]

в некоторых случаях – по десяткам траекторий проектирования, причем, и это принципиально важно, во-первых, чтобы процесс проектирования по нескольким траекториям происходил бы ***без увеличения длительности*** и ***стоимости выполнения проекта***, обеспечивая его эволюцию как ***непрерывного процесса прохождения множества «ворот качества» (Quality Gates) для каждой из траекторий проектирования***; а во-вторых, из всего множества траекторий в результате проектирования несколько траекторий, приводят к результатам, которые все удовлетворяют требованиям технического задания, а потому возникает важный вопрос – ***«какое же из решений, принадлежащих подмножеству траекторий следует «материализовать», то есть взять за основу для реализации / изготовления?»***, что позволяет в дальнейшем серьёзно задуматься об изменении / усовершенствовании бизнес-модели, выводя на рынок, в зависимости от конъюнктуры рынка, необходимое решение, оставляя другие решения, другие цифровые двойники, «в засаде» / «на будущее».

Во многих случаях большой вклад в повышение уровня адекватности математических моделей вносит учёт данных о технологических процессах изготовления деталей / узлов / компонентов / … – например, литьё метал-

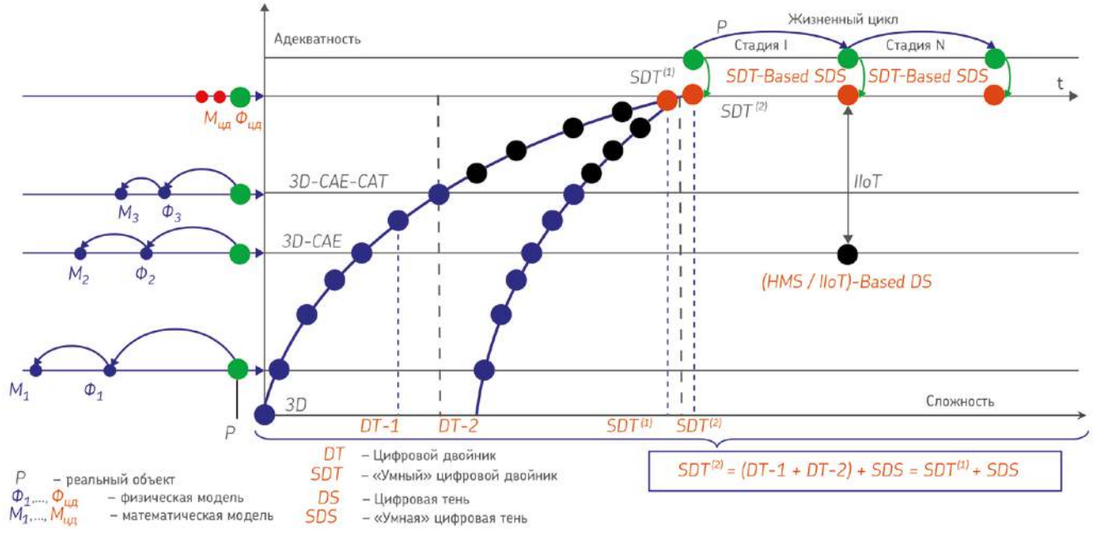


Рис. 3. Семейство физических и математических моделей. Цифровой двойник, «умный» цифровой двойник, цифровая тень [1]

лических изделий, штамповка, сварка, сборка, …, фактически важен учёт «предварительного» напряжённо-деформированного состояния, утонения, коробления и т. д. деталей после технологических процессов, наконец, изготовление композиционных материалов и формирование композитных структур, например, методом вакуумной инфузии [2].

Соответственно, ***семейство высокоадекватных мультидисциплинарных математических моделей технологических процессов***, применяемых для изготовления продукции, а также сопутствующих виртуальных испытаний, виртуальных стендов, виртуальных полигонов Центр компетенций НТИ СПбПУ «Новые производственные технологии» называет ***цифровым двойником технологических процессов (Digital Twin, DT-2)***.

Комплексирование цифрового двойника объекта / системы / машины / конструкции / … ***(DT-1)*** и цифрового двойника технологических процессов ***(DT-2)*** в рамках единой полномасштабной цифровой модели позволяет сформировать ***«умный» цифровой двойник 1-го уровня (Smart Digital Twin, SDT(1))***, который обладает «генетической памятью», то есть «знает» и «помнит» как его «изготавливали» и в какой последовательности его «собирали».

Применение ***SDT(1)*** позволяет организовать ***процесс «цифровой сертификации»*** – специализированный бизнес-процесс, основанный на тысячах / десятках тысяч виртуальных испытаний как отдельных компонентов, так и всей системы в целом, ***целью которого является прохождение с первого раза всего комплекса натурных, сертификационных, рейтинговых и прочих испытаний [3].***

Подчеркнем, что ***DT-1*** и еще в большей степени ***SDT***, дают четкое представление о расположении критических зон в конструкции, в которых имеет смысл размещать те или иные датчики (акселерометры, тензометры, датчики температуры, давления и т. д.), то есть отвечает на важные вопросы: ***«Где измерять?»*** и ***«Что измерять?»*** [4] и позволяет сформировать «умные» большие данные (Smart Big Data) и «умную» цифровую тень (Smart Digital Shadow, ***SDS***) в отличие от Big Data и цифровой тени (Digital Shadow, ***DS***), которая, как правило, формируется по цепочке: датчики → промышленный интернет (IIoT) →Big Data.

Понятно, что объем Big Data значительно больше объема Smart Big Data, содержит, как правило, очень много «мусорных» данных и, что самое интересное, вообще может не содержать Smart Big Data, то есть содержательных данных, обладающих высоком уровнем информационной насыщенности.

Это принципиально важные достоинства полномасштабных умных цифровых двойников и умных цифровых теней, которые позволяют:

- радикально сократить число требуемых датчиков и получаемый объем больших данных (как правило, потоковых данных),
- значительно сократить или полностью исключить «мусорные данные», формируя «содержательные данные» – полные и достоверные данные, отличающиеся информационной насыщенностью (***«Вы сразу же добываете обогащённую руду»*** – по меткому выражению профессора А.А. Аузана, декана экономического факультета МГУ им. М.В. Ломоносова), что является характерным признаком внутреннего обогащения данных,
- увеличить скорость обработки данных и внесения необходимых изменений в ***SDT(1)*** для его трансформации в «умный» цифровой двойник второго уровня ***SDT(2)***.

В дальнейшем, по мере эксплуатации объекта / системы / машины / конструкции … происходит постоянное «обучение» цифрового двойника:

- как в соответствии с изменениями, происходящими на протяжении жизненного цикла реального объекта (например, «умный» цифровой двойник объекта / конструкции / … / сооружения … ***SDT(1)*** – цифровой двойник «становится в процессе эксплуатации ещё умнее» – ***SDT(2)***, если он учитывает особенности произведённых ремонтов, которые, безусловно, изменяют остаточный ресурс объекта / конструкции / … / сооружения …),
- так и по результатам математического моделирования (виртуальных испытаний) ситуаций, в которых реальный объект не эксплуатировался или испытания провести невозможно, в первую очередь, в соответствии с соображениями безопасности или чрезмерной дороговизны (см. рис. 3).

В итоге формируется ***семейство цифровых двойников***:

{ DT-1, DT-2, SDT(1), SDT(2), … , SDT(Nsdt) }.

Дополнительная информация, полученная на этапе эксплуатации, а затем учтеная в цифровом двойнике, естественно, повышает уровень адекватности цифрового двойника – «обучает» ***SDT***: ***SDT(1), SDT(2), … , SDT(Nsdt)***, и позволяет в дальнейшем моделировать с его помощью различные возможные и «непредвиденные» ситуации и эксплуатационные режимы. Например, позволяет оценивать уровень возможных повреждений, накопление и развитие повреждений, оценивать фактически выработанный ресурс и оценивать остаточный ресурс, осуществлять планирование и управление обслуживанием и ремонтами высокотехнологичного оборудования.

Заключение

С помощью разработанных «цифровых двойников, сидящих в засаде» (А.И. Боровков), компании-лидеры мировых высокотехнологичных рынков обеспечивают, в трактовке декана экономического факультета МГУ им. М.В. Ломоносова профессора А.А. Аузана, «гарантированное зарезервированное развитие», выводя на рынок последовательно, по мере необходимости, в зависимости от складывающейся конъюнктуры рынка, решения из подмножества траекторий, каждому из которых соответствует свой цифровой двойник из семейства ***DT-1*** или «умный» цифровой двойник из семейства ***SDT***.

Производство («материализация цифрового двойника») и поставка продукции с конкурентными характеристиками реализуется в кратчайшие сроки – вспомним, что на этапе проектирования уже учтены все особенности и ограничения технологических и производственных процессов конкретного предприятия.

Принципиально важно понимать, что в данном случае физический объект (изделие, продукт, машина, конструкция, …) является репликой (полномасштабной копией) цифрового объекта (цифрового двойника ***DT-1*** или ***SDT(1)***), а не наоборот, как это принято считать, значительно упрощая ситуацию и сокращая возможности для высокотехнологичного бизнеса, «подстраивая технологию-драйвер под свое понимание».

Понятно, что когда физический объект «вышел» на этап эксплуатации, то на этап эксплуатации «вышел» и цифровой двойник ***DT-1*** или ***SDT(1)***), а к процессу эксплуатации подключаются цифровые тени (***DS*** или ***SDS***), формируя множественные обратные связи (см. рис. 3):

- на этап эксплуатации – для оптимизации процесса с учетом различных режимов эксплуатации,
- на этап производства – для оптимизации производства, в первую очередь, критических компонентов, подсистем, агрегатов…,

наконец, самая важная обратная связь –

- в начало процесса перепроектирования критических узлов или проектирования высокотехнологичной продукции нового поколения с учетом опыта эксплуатации, технического обслуживания и ремонтов.

Итак, в зависимости от возникающей конъюнктуры на высокотехнологичных рынках (в первую очередь, автомобилестроения, авиастроения и космической отрасли, судостроения, двигателестроения, нефтегазового машиностроения и других отраслей машиностроения), поставка продукции высокотехнологичными компаниями – мировыми лидерами осуществляется в рамках реализации современной триады:

Технологический прорыв → → Технологический отрыв → → Технологическое лидерство / превосходство,

для реализации которой ***играют ключевую и определяющую роль семейства цифровых двойников, «умных» цифровых двойников и «умных» цифровых теней***

{ DT-1, DT-2, SDT(1), SDS(1), SDT(2), SDS(2), SDT(3), … }

●

ЛИТЕРАТУРА ►**1.** Цифровые двойники в высокотехнологичной промышленности. Краткий доклад (сентябрь 2019 года) / А.И. Боровков, А.А. Гамзикова, К.В. Кукушкин, Ю.А. Рябов. СПб.: ПОЛИТЕХ-ПРЕСС, 2019. 62 с. ►**2.** Боровков А.И., Рябов Ю.А., Марусева В.М. Новая парадигма цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения // Цифровое производство: методы, экосистемы, технологии / МШУ СКОЛКОВО. 2018. С. 24–44. http://assets.fea.ru/uploads/fea/news/2018/04_april/12/cifrovoe-proizvodstvo-032018.pdf. ►**3.** Цифровые двойники и цифровая трансформация предприятий ОПК / А.И. Боровков, Ю.А. Рябов, К.В. Кукушкин, В.М. Марусева, В.Ю. Кулемин // Оборонная техника. 2018. № 1. С. 6–33. http://assets.fea.ru/uploads/fea/news/2018/05_may/17/oboronnaya-technika.pdf. ►**4.** Боровков А.И., Рябов Ю.А. Цифровые двойники: определение, подходы и методы разработки // Цифровая трансформация экономики и промышленности: сборник трудов научно-практической конференции, 20–22 июня 2019 г. / под ред. А.В. Бабкина. СПб.: ПОЛИТЕХ-ПРЕСС, 2019. С. 234–245. http://assets.fea.ru/uploads/fea/news/2019/06_june/24/INPROM_Cifrovye_dvoyniki.pdf.

Под цифровым двойником обычно подразумевается виртуальная модель реального физического объекта или процесса, которая, по сути, представляет собой сложную математическую модель, позволяющую с высокой точностью описывать поведение реального физического объекта или системы, а также технологического/производственного процесса или сервисов. За счет применения цифрового двойника становится возможным сосредоточить основную долю изменений и затрат на стадии проектирования. Это позволяет сократить издержки, возникающие на остальных этапах жизненного цикла.

«ЦИФРОВЫЕ ДВОЙНИКИ» И «ЦИФРОВЫЕ ТЕНИ» В ЭЛЕКТРОЭНЕРГЕТИКЕ

Евгений Грабчак
Заместитель министра энергетики РФ

Елена Медведева
Заместитель директора Департамента оперативного контроля и управления в электроэнергетике Минэнерго России

Не секрет, что в настоящее время в электроэнергетике высокий уровень износа основных производственных фондов, а темпы их обновления недостаточны. Продление ресурса основного технологического оборудования осуществляется преимущественно за счет продления срока службы и использования систем прогнозирования. Поставщики таких систем – производители оборудования либо сторонние компании. В первом случае система, прежде всего, используется для подтверждения корректной эксплуатации оборудования в рамках гарантийного срока и для осуществления своевременного сервиса. Таким образом, с оборудования действительно снимается большой объем технологической информации (цифровая тень или цифровой след). С учетом такого подхода собственник оборудования хочет понимать, насколько предлагаемый производителем сервис оптимален и не избыточен – какова его технико-экономическая эффективность. Подобный запрос порождает предложение от альтернативных поставщиков таких систем. И ядром этих систем являются экспертные модели, основанные на опыте специалистов, участвующих в эксплуатации оборудования.

Сегодня предпринимаются попытки заместить экспертные модели технологиями больших данных, искусственного интеллекта, машинного обучения и другими. Важно понимать, что они смогут служить только для быстрого выявления аномального тренда («что-то происходит не так»), но не для прогноза, когда и что случится, чтобы принять превентивные меры. Но даже для этого применения требуются формализованные экспертные модели и достаточный объем соответствующих моделям унифицированных данных, чтобы «обучить» эти технологии.

Таким образом, указанные системы не обладают прогнозным потенциалом и позволяют собственнику оборудования (объекта) принять краткосрочные ситуативные решения – невозможно понять, как и почему улучшить ту или иную конструкцию оборудования (цепочки оборудования), а также управлять жизненным циклом оборудования/объекта (собственник получает определенный уровень (не)эффективности постфактум от поставщика оборудования).

Учитывая имеющиеся ограничения по стоимости электроэнергии, вполне обоснованно уже сейчас переходить на модель управления жизненным циклом как отдельного оборудования, так и энергосистемы в целом. Имеющийся опыт эксплуатации производственного оборудования необходимо учитывать в новых требованиях к продукции при обновлении, производить не разовую модернизацию, а постоянное улучшение энергосистемы за счет вывода устаревших технологий и их замены на более современные – обеспечить постепенное обновление как возраста оборудования, так и используемых технологий.

В этих условиях компания заинтересована покупать не «железо», а полезный эффект, соответствующий набору функциональных требований: себестоимость производимого продукта/услуги и гибкую совместимость с элементами технологической цепочки (как внутри компании, так и в отраслевой цепочке создания ценности).

В сквозной модели жизненного цикла функциональные требования потребителя к энергокомпании транслируются энергокомпанией к производителю оборудования (рис. 1).

И от оборудования, и от электроснабжения как от продукта требуется быстро менять свои свойства в зависимости от предпочтений потребителя. Возникает необходимость использования инструментов, позволяющих ускорить процессы разработки, производства и внедрения новых продуктов и сервисов. Это становится возможным при условии использования цифровых двойников – совместимых между собой и с разными уровнями детализации.

Переход на идеологию управления жизненным циклом ставит задачу формирования цифрового двойника еще на этапе проектирования, а затем его последовательного совершенствования за счет накопленных данных о поведении реального объекта моделирования.

На этапе эксплуатации он дает возможность прогнозировать поведение объекта/системы/процесса в условиях изменяющихся условий и требований. Возможно моделирование любых условий воздействия, поэтому цифровой двойник – это отличный инструмент прогнозирования, ядро любой предсказательной системы. Прогнозный потенциал цифрового двойника принципиально отличает его от «цифровой тени», которая представляет собой набор данных о поведении объекта в прошлом, являясь, по сути, памятью об опыте объекта [1].

При этом важны следующие моменты. Во-первых, процесс создания адекватного цифрового двойника зачастую лежит на стыке различных дисциплин и требует участия специалистов соответствующих областей знания. Становится необходимым формирование экосистемы цифрового моделирования, удобным инструментом взаимодействия для которых являются цифровые платформы.

В феврале 2019 года в Научно-исследовательском корпусе Санкт-Петербургского политехнического университета Петра Великого (СПбПУ) состоялось рабочее совещание руководства Центра компетенций НТИ СПбПУ «Новые производственные технологии» с представителями Министерства энергетики Российской Федерации и энергетических компаний Российской Федерации по вопросам технологии цифровых двойников

Рис. 1.

Во-вторых, доверие к цифровым моделям должно подтверждаться либо экспериментальным путем, что иногда довольно затруднительно, либо определяться открытостью и многократным использованием библиотек моделей отдельных узлов, расчетных алгоритмов, предварительно настроенных моделей для конкретных типов оборудования конкретного производителя. Иностранные компании не спешат делиться своими наработками в области создания цифровых двойников.

В-третьих, в настоящее время в электроэнергетике еще слаба нормативная база, стимулирующая переход к сквозному использованию цифровых двойников на всех этапах жизненного цикла.

Минэнерго России видит свою задачу, прежде всего, в формировании условий и стимулов в виде нормативной базы, направленной на широкое внедрение в отрасль новых подходов к выстраиванию взаимоотношений между всеми участниками электроэнергетического рынка, базирующихся на широкомасштабном применении цифровых двойников и информационных моделей. Для этого будет целенаправленно формироваться единая информационная среда на основе платформенных решений, а также экосистема, которая включает в себя научные институты, производителей оборудования и энергокомпании, и базируется на принципах выстраивания взаимовыгодных отношений и использовании единых подходов, стандартов и платформенных решений ●

ЛИТЕРАТУРА ►1. Боровков А.И., Марусева В.М., Рябов Ю.А. «Умные» цифровые двойники – основа новой парадигмы цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения // Трамплин к успеху. – 2018. – № 13. – С. 12–16. URL: http://assets.fea.ru/uploads/fea/news/2018/04_april/12/tramplin-uspeha_13-16.pdf

Цифровой двойник энергетической системы рассматривается в качестве основного инструмента интеллектуального управления высокотехнологичной инфраструктурой распределенной энергетики. Предложена архитектура цифрового двойника. В качестве примера применения цифрового двойника приведен расчет оптимальной конфигурации гибридной системы энергоснабжения. Выполнена макетная программная реализация цифрового двойника энергосистемы активного потребителя низкого напряжения на базе продуктов Nrjpack, Matlab Simulink и Homer PRO.

ПОДХОДЫ К РАЗРАБОТКЕ И ПРИМЕНЕНИЮ ЦИФРОВЫХ ДВОЙНИКОВ ЭНЕРГЕТИЧЕСКИХ СИСТЕМ

Сергей Андрюшкевич
ООО «ИТСГ Регион»

Сергей Ковалев
Институт проблем управления
им. В.А. Трапезникова РАН

Евгений Нефедов
Институт арктических технологий
Московского Физико-Технического Института

Концепция цифрового двойника относится к числу основополагающих в контексте четвертой промышленной революции (Industrie 4.0). Цифровой двойник (Digital Twin, DT) – это виртуальная копия технического объекта, достоверно воспроизводящая и задающая структуру, состояние и поведение оригинала в реальном времени [1]. Будучи интеллектуальной надстройкой над средой Интернета вещей (Internet of Things, IoT), Цифровой двойник является ключевым базовым элементом высокотехнологичной системы управления. По данным Gartner, к 2021 году почти половина крупных промышленных компаний будут использовать технологию цифровых двойников, чтобы повысить точность оценивания производительности изделий и технических рисков, достигнув при этом повышения операционной эффективности изделий примерно на 10 % [2].

К числу высокотехнологичных объектов, управление которыми целесообразно организовывать на базе цифровых двойников, относятся современные системы распределенной энергетики, включающие разнообразные энергоприемники, локальное генерирующее оборудование на возобновляемых источниках и накопители электроэнергии. Однако, закономерно, что технологиям построения цифровых двойников, заимствуемым из машиностроительных отраслей, присущи характерные недостатки, такие как потребность в громоздких дорогостоящих программных инструментах и высококвалифицированном персонале, хорошо заметная в немногочисленных примерах цифровых двойников энергосистем [3]. Не хватает однозначно интерпретируемых достоверных данных в стандартных машино-читаемых форматах, адекватных математических моделей, приборного оснащения. Не ясно, как автоматически собрать целостный цифровой двойник большой энергосистемы из двойников составляющих, с учетом правил их соединения. Очень медленно развиваются технологии типа порождающего проектирования (Generative Design), позволяющие автоматически находить оптимальные проектные решения по энергоснабжению [4]. Эти недостатки особенно остро ощущаются в жизненном цикле энергосистем массовых небольших потребителей низкого уровня напряжения (0,4 кВ).

В статье предложены подходы к преодолению этих недостатков при проектировании и эксплуатации систем управления объектами распределенной энергетики. Развитие этих подходов позволит эффективно организовать на базе цифровых двойников оценку и прогнозирование генерации, потребления, хранения, передачи энергоресурсов во всех аспектах, а также управление режимами, предсказательный мониторинг состояния оборудования, верификацию моделей и алгоритмов, виртуальную апробацию и оптимизацию проектных решений, обучение персонала объектов.

Архитектура цифрового двойника энергетической системы

По структуре цифровой двойник представляет собой комплекс взаимосвязанных компьютерных моделей, способных достоверно отобразить объект-оригинал, его состояние и поведение при различных условиях окружающей среды и управляющих воздействиях. Модели образуют представление полного жизненного цикла объекта, позволяющее обнаруживать, анализировать, прогнозировать и предотвращать нежелательные ситуации в ходе эксплуатации объекта. В частности, модели используются для решения следующих задач:

- сверка компьютерного представления оригинала с данными из реального мира;
- оповещение персонала и поддержка принятия решений;
- прогнозирование изменений оригинала с течением времени;
- выявление новых возможностей применения оригинала и экономических эффектов.

Эти задачи обладают высокой актуальностью и для энергосистем. Сверка моделей с данными из реального мира подразумевает автоматическое снабжение математических и имитационных моделей цифрового двойника структурированными актуальными исходными данными из базовых информационных компонентов, которые описывают энергосистему в различных аспектах и наполняются из смежных программных систем в реальном времени по мере возникновения. Чтобы исключить разночтения в именовании и интерпретации понятий, с которыми оперирует цифровой двойник, в основу его информационного обеспечения помещается онтологическая модель энергетической инфраструктуры, для формирования которой накоплен значительный задел [5 и др.]. Над ней надстраиваются следующие информационные компоненты цифрового двойника энергосистемы, как показано на рисунке 1:

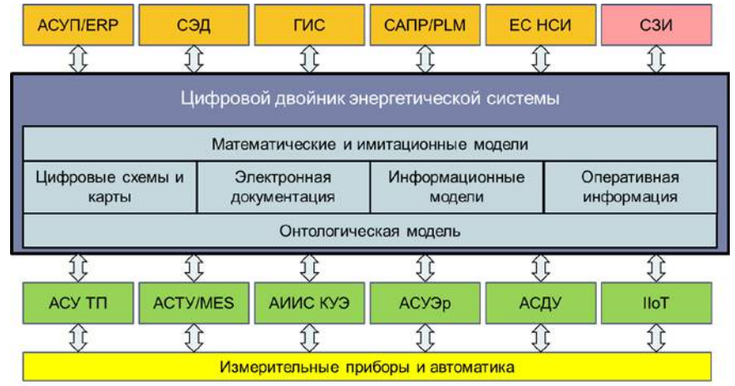


Рис. 1. Архитектура цифрового двойника энергетической системы

- цифровые схемы и карты (в первую очередь однолинейная схема электроснабжения);
- электронная документация (проектно-сметная, эксплуатационная и др.);
- информационные модели (мастер-данные – сведения о субъектах, об объектах, о составе и характеристиках оборудования, сопутствующие справочники и т.д.);
- оперативная информация (результаты приборных измерений потребления и первичных характеристик технического состояния оборудования).

Для цифровых двойников больших многокомпонентных объектов, таких как энергосистемы, характерна проблема, состоящая в сложности соединения рабочих моделей (двойников) составляющих компонентов в единое слаженное целое. Фактически соединение требует виртуально воспроизвести процесс строительства энергосистемы на информационных и математических моделях, с проставлением корректных взаимосвязей между ними. Перспективный подход к решению этой проблемы предложен на базе математического аппарата теории категорий [6].

Информационное моделирование инфраструктуры активного потребителя

Процесс формирования цифрового двойника крупноблочно показан на рисунке 2. Видно, что онтологическое моделирование составляет в нем фундамент стадии проектирования и служит основой для формирования информационного обеспечения.

Для энергетической инфраструктуры потребителей онтологическое моделирование затруднено тем обстоятельством, что широко распространенные обобщенные информационные модели (common information models – CIM), служащие источником терминов и отношений, в основном ориентированы на крупные энергетические объекты: электростанции, линии электропередачи, подстанции. Информационное моделирование активных энергетических объектов потребления низкого напряжения представляет сложную задачу, в том числе ввиду высокой вариативности имеющегося у них генерирующего и потребляющего энергетического оборудования. Недостающие термины и отношения заимствуются из стандартов ISO 17800 (модели микрогрида), IEC 61850 (модели интеллектуальных электрических устройств), OASIS EMIX (модели

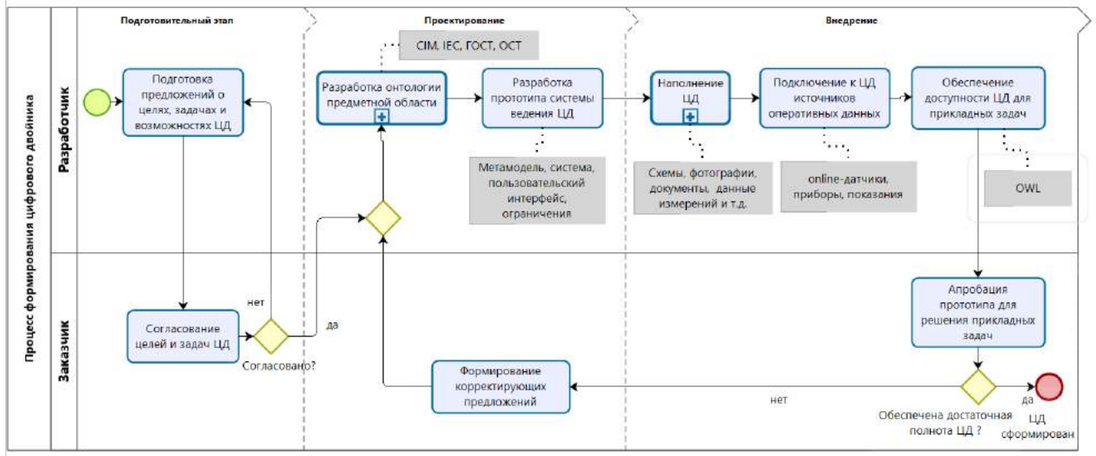


Рис. 2. Процесс формирования цифрового двойника (ЦД)

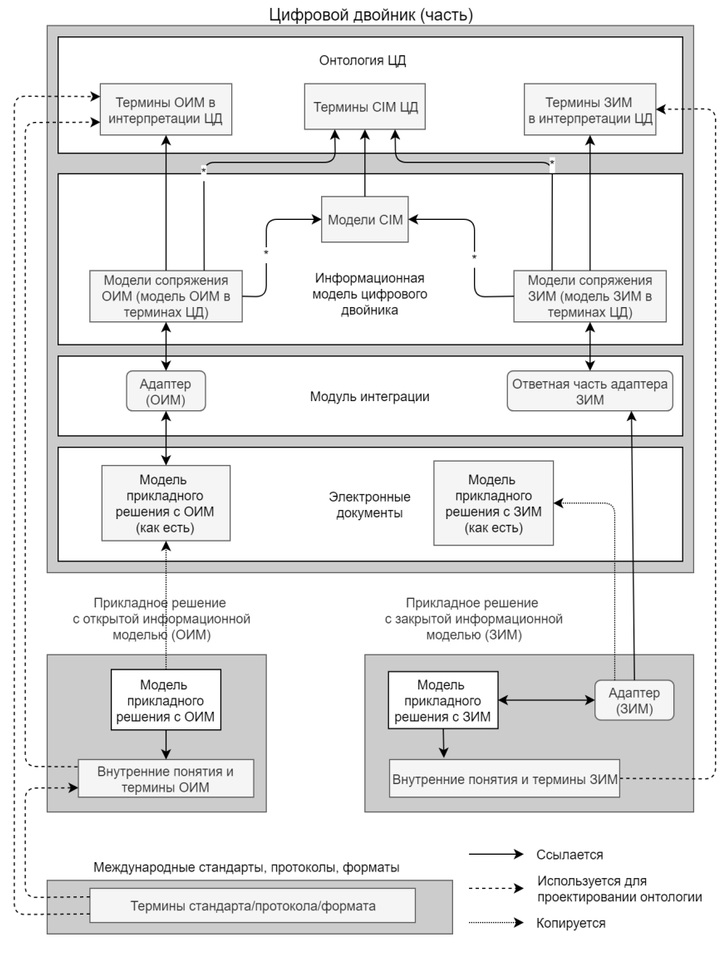


Рис. 3. Интеграция цифрового двойника с приложениями

обмена информацией рыночного характера), а также моделей описания наблюдений и прогнозов погоды и т.д.

Информационные модели, структура которых сформирована на основе открытых онтологий и стандартов, называются открытыми (ОИМ) и естественным образом являются предпочтительной основой для интеграции информационно-управляющих и рыночных приложений с цифровым двойником. Однако, как показано выше на схеме архитектуры, цифровой двойник должен быть интегрирован с широким спектром специализированных инструментов, которые используются при проектировании и эксплуатации энергетических объектов, в том числе САПР, АСУ ТП и т.д. Информационные модели, реализованные в таких инструментах, часто имеют характер закрытых (ЗИМ), и для интеграции на их базе требуется ввести связующие элементы – модели сопряжения, как показано на рисунке 3. Например, такой подход целесообразен для подключения к цифровому двойнику системы поддержки проектирования небольших энергосистем на базе САПР AutoCAD, в качестве интерактивного «редактора» ряда фрагментов информационной модели. Еще одним примером служит интеграция со шлюзами сбора оперативных данных с сенсоров и выдачи команд исполнительным ме-

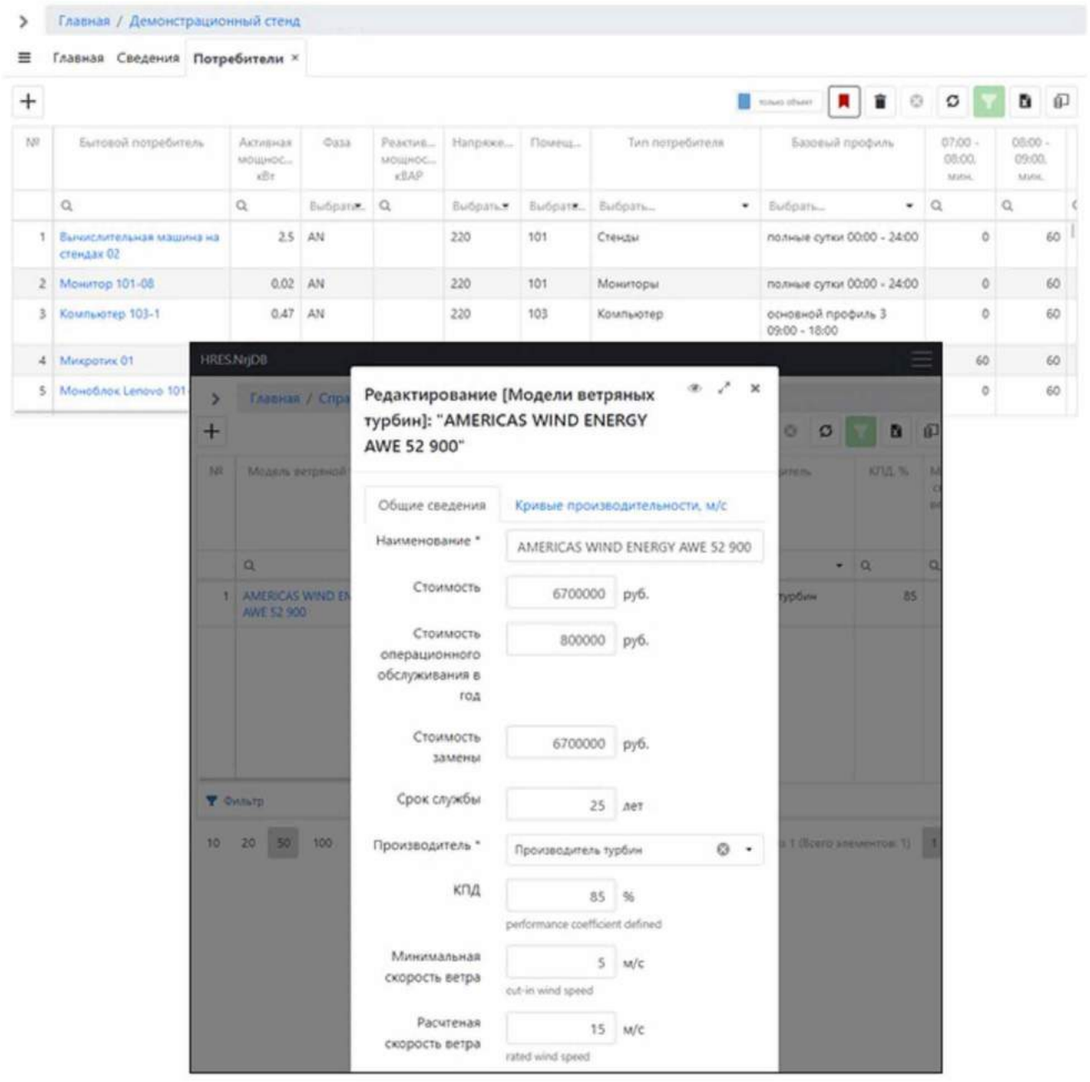


Рис. 4. Пример экранов отображения и ввода элементов информационной модели

ханизмам, разработанными на базе платформы IoT Eclipse Kura.

Для ведения информационных моделей и других базовых компонентов цифрового двойника энергетической системы пилотного объекта можно использовать отечественный программный комплекс Nrjpack. Примеры экранов комплекса, предназначенных для отображения и ввода элементов информационной модели, показаны на рисунке 4.

Архитектурную основу комплекса составляет метамодель – описание информационных сущностей, характеристик, связей между ними, получаемое из онтологии. Такое проектное решение позволяет автоматизировать выполнение рутинных программистских задач:

- компоновка форм пользовательского интерфейса для выполнения операций создания, просмотра, обновления и удаления данных (CRUD-операции);
- формирование структуры и наполнения базы данных;
- выгрузка информационной модели для передачи на вход математическим и имитационным моделям.

Тем самым существенно сокращаются затраты времени и труда на итеративное заполнение и актуализацию двойника, по сравнению с традиционным подходом (domain driven design, DDD [7]). Дело в том, что традиционно элементы онтологии представляются в виде классов и объектов, описанных непосредственно в исходном тексте программ. В такой ситуации при изменении онтологии недостаточно перенастроить метамодель через пользовательский интерфейс:

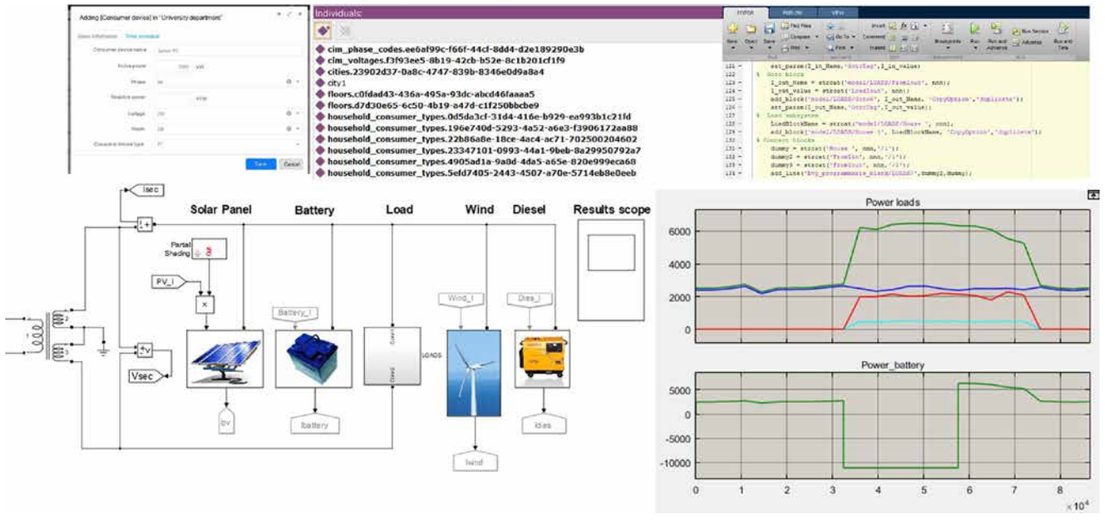


Рис. 5. Пример имитационной модели функционирования энергосистемы

нужно изменить исходный текст, перекомпилировать, протестировать и установить новую версию программного обеспечения.

Программный комплекс Nrjpack построен по архитектуре CQRS (command query request segregation), которая предполагает разделение набора обращений пользователя к системе на два независимых потока: запросы и команды. При внесении изменений в информационную модель или метамодель пользователь фактически формирует запрос на изменение, на который система реагирует изменением структуры данных или их наполнения посредством формирования соответствующих событий.

Следует подчеркнуть, что архитектура CQRS реализована не только для сущностей информационной модели (данных), но и для сущностей метамодели (типов), что позволило выделить в отдельный поток события, направленные на изменение структуры информационной модели, а не только наполнения. Одним из способов обработки событий является представление информационной модели в реляционной базе данных. Такой подход, традиционный для высоконагруженных систем, представляет особый интерес в задачах создания и ведения цифрового двойника, поскольку позволяет формировать разные реляционные проекции, оптимизированные под разные варианты использования двойника.

На базе метамодели в программном комплексе реализована автоматическая выгрузка полного набора сведений об объекте в файл на стандартном языке онтологического моделирования OWL (Ontology Web Language). Инструменты выгрузки основываются на метамодели и поэтому автоматически адаптируются под изменения онтологии.

Поиск оптимальной конфигурации гибридной системы энергоснабжения

В качестве прикладной задачи для практического применения цифрового двойника рассмотрим автоматический поиск оптимальной конфигурации гибридной системы энергоснабжения (Hybrid Renewable Energy System, HRES) для заданного объекта, у которого известны профиль потребления и погодные условия. Такая система содержит локальное генерирующее оборудование (в том числе на ВИЭ) и накопители электроэнергии, которые, вместо или в дополнение к централизованной энергосети, снабжают объект электроэнергией. Оптимальная конфигурация предполагает такое сочетание компонентов генерации и накопителей, которое дает наибольший эффект в части эксплуатации по сравнению с пассивным питанием от внешней сети. Оптимизация выполняется для трех целевых функций: годовая стоимость системы, вероятность потери электроснабжения и количество вредных выбросов в атмосферу. Проектными переменными задаются количество устройств каждого вида и установочные параметры; с ограничениями в виде диапазонов значений переменных. В качестве примера можно привести решение этой задачи при помощи эволюционного алгоритма [8]. Однако большинство подобных алгоритмов требуют значительных вычислительных ресурсов, поэтому на практике можно применять более «легковесные» оптимизаторы HRES. Примером служит пакет HOMER Pro, разработанный специально для быстрого нахождения экономически субоптимальных конфигураций систем распределенной энергетики. Модель в HOMER Pro для поиска оптимальной конфигурации включается в число составляющих математической модели цифрового двойника энергосистемы.

К важнейшим функциям цифрового двойника относится проверка работы найденной конфигурации в имитационном режиме (симуляция). Эту функцию можно реализовать посредством адаптации известной типовой электротехнической модели энергосистемы в программном пакете Matlab Simulink [9]. В модели содержатся элементы распределенных энергетических ресурсов – электрическая сеть, элементы ВИЭ, дизель-генератор, накопитель, и программно реализованы средства для их соединения в заданную конфигурацию. Конфигурация, определяемая в результате работы модели HOMER Pro, автоматически воссоздается в динамической модели Matlab Simulink. Таким путем на практике достигается автоматическое соединение моделей компонентов в единый комплекс. Далее пользователь цифрового двойника получает возможность исполнять полученную имитационную модель при различных интересующих его параметрах и условиях, например, оценивать реакцию энергосистемы на то или иное управляющее воздействие, как показано на рисунке 5.

В свою очередь, на вход пакету HOMER Pro передается описание объекта потребления (информационная модель), сформированное в программном комплексе Nrjpack. Передача происходит автоматически, путем преобразования и загрузки в HOMER Pro представления информационной модели файлом в формате OWL, сгенерированным в NrjPack. При этом, для каждого энергоприемника по указанным в информационной модели параметрам, таким как номинальная мощность и режим функционирования, формируется оценочный почасовой профиль потребления. При наличии данных фактического потребления с приборов учета, доступных через шлюзы IoT, производится калибровка оценочного профиля. В ситуации, когда один прибор учета охватывает несколько энергоприемников, измеренный им суммарный профиль программно «раскладывается» по их профилям, посредством алгоритмов так называемой дезагрегации [10]. Сформированные и откалиброванные профили энергоприемников передаются на вход модели Matlab Simulink для проведения симуляции, а сложенный из них общий профиль нагрузки поступает на вход модели HOMER Pro для подбора субоптимальной для данного профиля потребления конфигурации HRES.

В качестве альтернативы электротехническим моделям, записанным на Matlab Simulink, рассматриваются модели, построенные путем машинного обучения глубоких нейронных сетей. Предлагаются архитектуры и примеры нейронных сетей, в том числе рекуррентных и сверточных, для решения ряда ключевых задач интеллектуального управления в энергетике, таких как прогнозирование нагрузки, прогнозирование цены электроэнергии, оптимизация распределения нагрузки между доступным генерирующим оборудованием, оценка и прогнозирование технического состояния энергетического оборудования, диагностика отказов и катастроф. Можно ожидать, что в перспективе нейросетевые модели, подкрепленные другими средствами компьютерной математической статистики, смогут занять лидирующее положение в составе цифрового двойника энергосистемы.

Заключение

Подходы к построению цифрового двойника, предложенные в настоящей работе, позволяют без излишних затрат труда и времени сформировать удобную в использовании виртуальную копию энергосистемы, способную воспроизводить структуру, состояние и поведение оригинала с достаточной для ряда практических целей степенью полноты, достоверности и оперативности. Это было подтверждено в цикле разработки макета цифрового двойника для энергосистем пилотных активных потребителей низкого напряжения [11]. Макет позволяет рассчитывать субоптимальные конфигурации энергосистемы и выполнять реалистичную имитацию ее поведения, в том числе в переходных режимах (переключение между источниками). Тем самым, был реализован классический цифровой двойник базового типа (Baseline Twin) [12]. Полученные результаты являются основополагающими для проектирования систем интеллектуального управления энергетической инфраструктурой будущего ●

ЛИТЕРАТУРА ►**1.** Madni A.M., Madni C.C., Lucero S.D. Leveraging digital twin technology in model-based systems engineering // Systems. 2019. Vol. 7(1). P. 7. https://www.mdpi.com/2079-8954/7/1/7. ►**2.** Pettey C. Prepare for the impact of digital twins. Stamford, CT, USA: Gartner, 2017. ►**3.** Brosinsky C., Westermann D., Krebs R. Recent and prospective developments in power system control centers: Adapting the digital twin technology for application in power system control centers // Proc. 2018 IEEE International Energy Conference ENERGYCON. IEEE, 2018. P. 1–6. ►**4.** Kovalyov S.P. An approach to develop a generative design technology for power systems // Proc. VI International Workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security" (IWCI 2019). Advances in Intelligent Systems Research. 2019. Vol. 169. P. 79–82. https://www.atlantis-press.com/proceedings/iwci-19/125917306. ►**5.** Ковалев С.П. Применение онтологий при разработке распределенных автоматизированных информационно-измерительных систем // Автометрия. 2008. Т. 44, № 2. С. 41–49. ►**6.** Nolan J.S., Pollard B.S., Breiner S., Anand D., Subrahmanian E. Compositional models for power systems // Proc. Applied Category Theory Conf. ACT 2019. NIST, 2019. https://www.nist.gov/publications/compositional-models-power-systems. ►**7.** Evans E. Domain-Driven Design – Tackling Complexity in the Heart of Software. Addison-Wesley, 2004. 529 p. ►**8.** Ming M., Wang R., Zha Y., Zhang T. Multi-objective optimization of hybrid renewable energy system using an enhanced multi-objective evolutionary algorithm // Energies. 2017. Vol. 10. P. 674. https://www.mdpi.com/1996-1073/10/5/674. **9.** Hiroumi M. Simplified model of a small scale micro-grid. https://se.mathworks.com/help/physmod/sps/examples/simplified-model-of-a-small-scale-micro-grid.html. ►**10.** Faustine A., Mvungi N.H., Kaijage S., Michael K. A survey on non-intrusive load monitoring methodies and techniques for energy disaggregation problem // arXiv, 2017. https://arxiv.org/abs/1703.00785. ►**11.** Andryushkevich S.K., Kovalyov S.P., Nefedov E. Composition and application of power system digital twins based on ontological modeling // Proc. 17th IEEE Intl. Conf. Industrial Informatics INDIN'19. Helsinki-Espoo, Finland: IEEE, 2019. P. 1536–1542. ►**12.** Erikstad S. Design patterns for digital twin solutions in marine systems design and operations // Proc. 17th Intl. Conf. Computer and IT Applications in the Maritime Industries COMPIT'18. Hamburg, Technische Universität Hamburg, 2018. P. 354–363.

Системы автоматизации, защиты и управления цифровыми подстанциями на базе шины процесса МЭК 61850 все чаще становятся частью проектов нового строительства и реконструкции. Эти современные системы используют технологии GOOSE и выборок мгновенных значений (SV) для передачи важных данных реального времени внутри подстанции; как правило, это связи между устройствами преобразования дискретных и аналоговых сигналов (ПДС/ПАС) на уровне технологического процесса и ИЭУ защиты и управления на уровне присоединения. Но даже на цифровых подстанциях передача сигналов релейной защиты на другую подстанцию выполняется проводами через традиционные интерфейсы TDM (временное мультиплексирование, англ. TDM) или напрямую через оптоволокно. Это не только противоречит концепции цифровой подстанции, но и создает проблемы для глобальных сетей связи (WAN), которые в долгосрочной перспективе превратятся в операционные технологические сети на базе коммутации пакетов. Использование надежной связи в реальном времени на базе технологий GOOSE и SV вне пределов подстанции не только подчеркивает концепцию цифровой подстанции и поддерживает общие тенденции в сфере технологий связи, но и открывает невиданные возможности внедрения новых функций, выходящих за рамки подстанций, а также новых подходов к текущим решениям с улучшенным быстродействием.

ОБМЕН ДАННЫМИ МЭК 61850 В РЕАЛЬНОМ ВРЕМЕНИ МЕЖДУ ЦИФРОВЫМИ ПОДСТАНЦИЯМИ ДЛЯ РЕАЛИЗАЦИИ НОВЫХ ПРИНЦИПОВ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИЗАЦИИ

Рамон Бейкли
ABB Switzerland Ltd.
Швейцария

Адольф Фрей
ABB Switzerland Ltd.
Швейцария

Стефан Мейер
ABB Switzerland Ltd.
Швейцария

При выводе технологий МЭК 61850 за границы подстанций возникает множество вопросов касательно быстродействия, а также проектирования, пуско-наладки, испытаний и техобслуживания. В некоторой степени это связано с принадлежностью сервисов GOOSE и SV ко 2 уровню сетевой модели и с изначальной ориентацией на внутриподстанционные ЛВС. Необходимо уделять внимание таким аспектам, как доступность сервисов, гарантированное быстродействие, корректная работа приложения, конфликты конфигурации, разделение сетей в пределах подстанции и информационная безопасность. Важное значение имеют новые возможности с точки зрения повышения быстродействия, доступности, интеграции, а также сокращения затрат. Например, было продемонстрировано [1], что при переходе с традиционной дистанционной защиты, использующей проводные подключения, на сообщения GOOSE и волоконно-оптические кабели быстродействие улучшается на 5 мс.

Требования к функциям релейной защиты

В данном разделе приведен обзор требований к критически важным функциям РЗА, а также перечислены обязательные условия для использования GOOSE и SV в схемах защиты. Аналогичная информация принимается за основу при оценке подходящих технологий для защиты линии с использованием GOOSE и SV.

Требуемое быстродействие для устранения короткого замыкания

Рис. 1. Стандартное время срабатывания РЗА с передачей телесигналов согласно МЭК 60834-1

в схемах защит линии определено в МЭК 608341. Как правило, время устранения КЗ (Tc) для ЛЭП высокого напряжения составляет 3-6 периодов промышленной частоты [2]. В системах защиты с передачей телесигналов критическим параметром быстродействия является максимальное время передачи (Tac). Для цифровых систем связи значение Tac должно быть менее 10 мс (в некоторых рекомендациях речь идет даже о 5 мс [4]). Эта величина рекомендована для любых схем защит высоковольтных линий, независимо от типа интерфейса связи.

Указанное время передачи должно гарантироваться также для функций РЗА на базе GOOSE или SV. Помимо минимального времени передачи, для дифференциальной защиты важна точная синхронизация измерений, поскольку в ином случае может произойти ошибочное или неселективное срабатывание. Использование SV для дифференциальной защиты создает новые проблемы в этой области, поскольку теперь обе подстанции должны иметь один источник времени, и должна быть обеспечена синхронизация двух временных зон (т.е. двух подстанций). Расхождение в синхронизации по времени будет иметь те же последствия, что и асимметрия каналов связи в традиционном режиме работы с «эхо»-сигналом, при котором максимальная разница задержек в разных направлениях не должна превышать 200–400 мкс. Это означает, что удаленные концы линии электропередачи должны быть синхронизированы с минимальным временным отклонением в одной и той же области. Это достигается путем синхронизации со спутником (например, спутники GPS) или концепцией синхронизации по сети. В любом случае информация о времени имеет критически важное значение, и требует диагностики и проверки.

Кроме того, если для функций релейной защиты используются пакетные технологии, такие как GOOSE или SV, необходимо принять особые меры по защите критически важных данных от несанкционированного изменения и доступа к шинам станции и процесса МЭК 61850 со стороны глобальной вычислительной сети.

Влияние на проектные решения

На современных традиционных или цифровых подстанциях структура внутренних сетей связи подразумевает наличие шины станции и шины процесса МЭК 61850, которые полностью изолированы от сети связи между подстанциями, используются отдельные порты ИЭУ (как правило, несовместимые с МЭК 61850) и передаются только обработанные данные из терминала, а не исходные

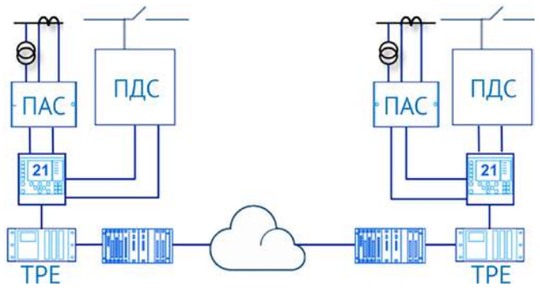


Рис. 2. Функциональные модули традиционной дистанционной защиты линии

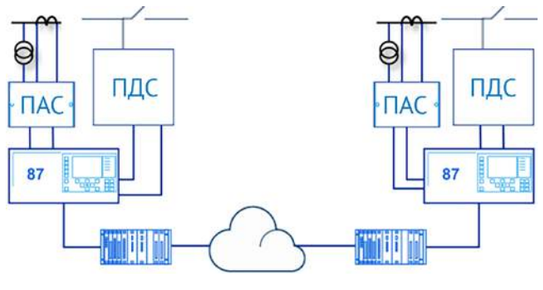


Рис. 3. Функциональные модули традиционной дифференциальной защиты линии

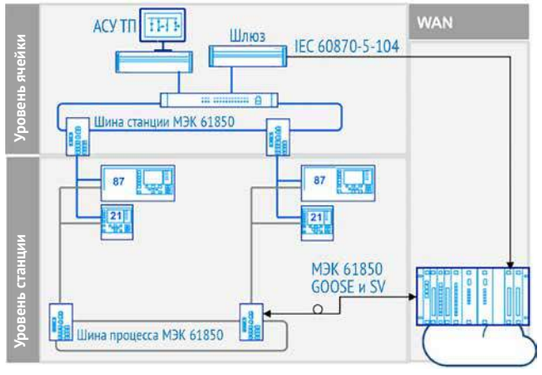


Рис. 4. Схема подстанции, использующей технологии GOOSE и SV для защиты линии

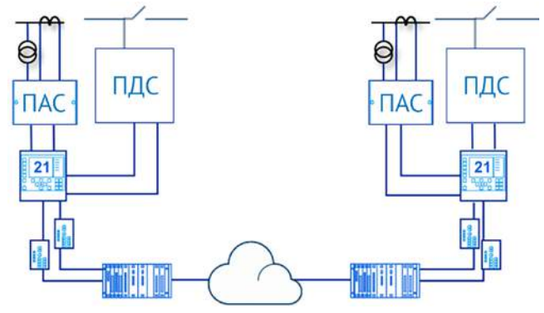


Рис. 5. Функциональные модули дистанционной защиты линии на базе GOOSE.

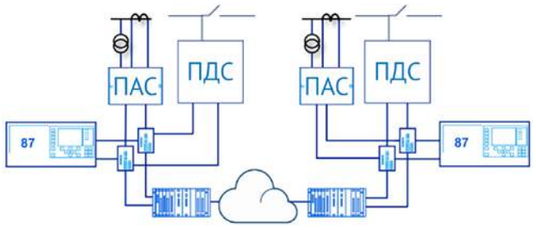


Рис. 7. Функциональные модули дистанционной защиты линии на базе технологии SV в соответствии с МЭК 61850

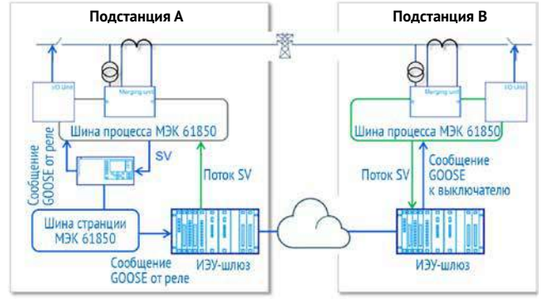


Рис. 8. Концепция обмена сообщениями SV и GOOSE между подстанциями

данные с полевого уровня. Рис. 3 демонстрирует подобную схему, в которой обработанные в терминале данные передаются между двумя концами линии электропередачи для реализации функции защиты линии. В представленной схеме сигналы дистанционной защиты обрабатываются дополнительно с помощью внешнего устройства передачи сигналов и передаются по каналу E1 (2 Мбит/с) в сети WAN. Данные для дифференциальной защиты линии передаются посредством протокола IEEE C37.94. В любом случае традиционная технология TDM, применяемая для передачи сигналов от защит, устанавливает лишние требования к преобразованию при использовании глобальной сети с коммутацией пакетов. Доступность и быстродействие схемы ограничены сложностью решения, которое подразумевает наличие множества устройств и подключений при ограниченных возможностях диагностики или резервирования.

На рис. 2 представлены функциональные модули традиционной дистанционной защиты линии.

Как правило, устройства передачи телесигналов (УПАСК, англ. TPE), а также соединения между терминалами, УПАСК и оборудованием связи являются нерезервированными и, значит, ограничивают доступность всего решения. Кроме того, многие подсистемы в рамках такого решения не диагностируются, и обработка сигналов в них ограничивает быстродействие всей схемы защиты. На рис. 3 проиллюстрировано то же самое, но для традиционной дифференциальной защиты линии. Очевидно, что любые исходные данные, необходимые для текущего сравнения на дальнем конце линии, сначала должны быть обработаны в локальном терминале, прежде чем будут переданы на другой конец. Применение концепции МЭК 61850 позволяет существенно уменьшить сложность всей схемы защиты.

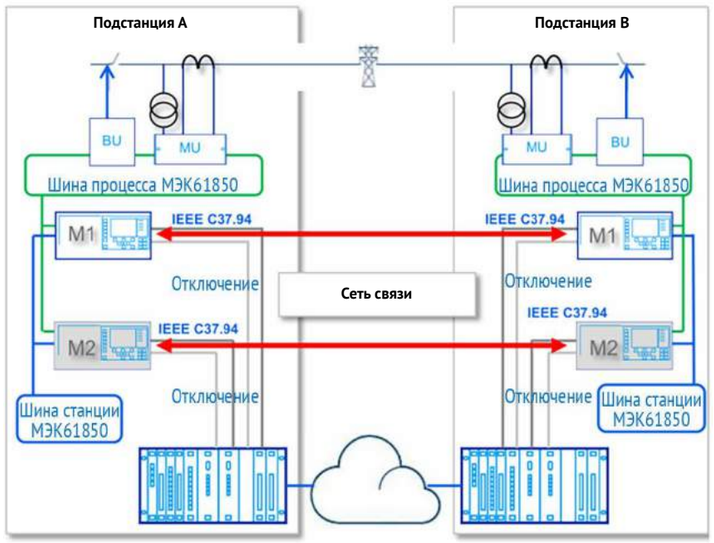


Рис. 6. Связь между терминалами в традиционной дифференциальной защите

На рис. 4 показано, как выглядит подстанция, использующая сообщения GOOSE и SV для защиты линии. Несущие опасный для персонала потенциал и недиагностируемые медные кабели заменяются на оптоволокно, подключения к ИЭУ – на доступ к шинам станции и процесса. Такое решение имеет множество преимуществ, таких как:

- существенное снижение затрат на монтаж кабелей
- невосприимчивость к электромагнитным помехам
- существенное уменьшение используемых устройств или повышение надежности за счет резервирования при том же количестве оборудования
- снижение требований к пространству на подстанциях
- расширение функций диагностики
- повышение доступности за счет применения схем резервирования на базе стандарта МЭК 61850 и устранения единичной точки отказа
- взаимозаменяемость/интеграция устройств от разных производителей благодаря использованию только стандартных сервисов связи МЭК 61850
- связь только на основе коммутации пакетов без необходимости преобразования в TDM

На рис. 5 представлены функциональные модули, обеспечивающие работу дистанционной защиты линии на базе технологии GOOSE. Наиболее очевидные изменения по сравнению с традиционным методом (рис. 2) – это упрощение схемы за счет отказа от функционального модуля УПАСК, а также возможность резервирования соединений между ИЭУ и оборудованием связи на основе протокола PRP.

Применение новых принципов для дифференциальной защиты линии, аналогично дистанционной защите, в корне меняет суть дифференциальной защиты. В настоящее время дифференциальная защита линии основана на двух (или более – в случае разветвленных линий) терминалах РЗА, установленных по концам линии электропередачи, которые обмениваются результатами измерения тока и позволяют устройствам-приемникам вычислять дифференциальный ток. Даже несмотря на то, что интерфейсы для связи стандартизованы (например, соответствуют IEEE C37.94), само решение является полностью проприетарным. Это означает, что для выполнения функций дифференциальной защиты линии необходимо наличие двух терминалов от одного производителя на каждом конце линии. Для конфигураций с резервированием требуется наличие на каждом конце линии двух терминалов от разных производителей. На рис. 6 представлена типичная конфигурация с терминалами защиты M1 и M2 на каждом конце линии.

Как только появляется возможность передать данные «полевого» уровня между противоположными концами линии электропередачи, в концепцию дифференциальной защиты линии можно внести фундаментальное изменение. Реле больше не зависит от обработанных и, соответственно, проприетарных данных, поступающих с другой стороны. Наличие доступа к технологии SV не только обеспечивает реальную возможность взаимодействия устройств разных производителей, но и позволяет строить совершенно новые оптимизированные схемы дифференциальной защиты линии. Терминал дифференциальной защиты с одной стороны линии электропередачи получает локальную и удаленную информацию о токе и напряжениях посредством стандартизованных потоков SV. С помощью этой информации терминал может выполнять функцию защиты и определять, есть ли замыкание в линии. В случае обнаружения КЗ терминал отправляет сигналы аварийного отключения в виде сообщений GOOSE как в направлении локального ПДС выключателя, так и в направлении удаленного ПДС. На рис. 8 изображена новая концепция.

Если взглянуть на все решение для дифференциальной защиты линии целиком, то новая концепция обеспечивает существенное сокращение количества задействованных функциональных модулей, что приводит к упрощению схемы при одновременном увеличении доступности. Терминалы дифференциальной защиты линии имеют прямой доступ к полевым данным, поступающим от ПАС или электронных датчиков на своей подстанции, а также с удаленной подстанции через оборудование связи WAN. Использование протоколов PRP или HSR обеспечивает резервирование, обычно недоступное в традиционных схемах, а применение технологии GOOSE гарантирует полноценную диагностику для всей схемы. Кроме того, два терминала резервируют друг друга, поскольку имеют доступ к полевым данным с обоих концов линии и могут посылать ко-

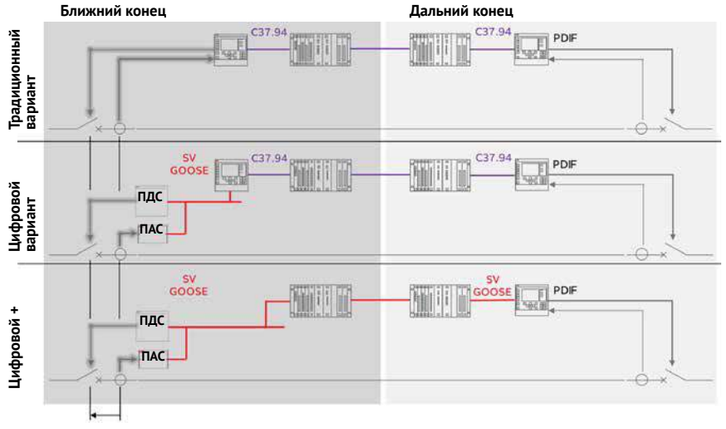


Рис. 9. Обзор различных вариантов дифференциальной защиты линии

манды на оба конца. Это означает, что схема с резервированием, требующая в настоящее время наличия четырех ИЭУ, может в дальнейшем быть обеспечена посредством двух ИЭУ и устройств уровня процесса. На рис. 7 представлена подобная схема. Сравнивая с рис. 3, можно заметить, что улучшены функции резервирования, а также снижена сложность, так как используется на два терминала меньше.

Техническое решение

Решение включает несколько функций, обеспечивающих надежный, высокодоступный и безопасный обмен данными между подстанциями по сети WAN на базе технологий GOOSE и SV в соответствии с МЭК 61850.

Интеграция по МЭК 61850

Решение для передачи сообщений GOOSE и SV по сети WAN построено на базе ИЭУ, выступающего в роли шлюза в соответствии с МЭК 61850. Это подразумевает полноценную поддержку MMS для диагностики и контроля всех сопутствующих параметров, обеспечивающих интеграцию в систему автоматизации подстанции.

Преобразование «на ходу»

Как правило, каждая подстанция во многом является копией другой – для устройств в рамках подстанции используются одинаковые правила присвоения имен и сетевые адреса, которые уже задействованы на удаленной подстанции. Из-за этого практически невозможно соединить две подстанции без внесения существенных изменений в конфигурации или без наличия специальных функций для решения указанной проблемы в составе шлюзового ИЭУ. Шлюзовое ИЭУ может решить проблему с помощью механизма преобразования, способного переводить специальные поля данных на скорости физического соединения без внесения дополнительных задержек. Механизм преобразования исправляет возможные конфликты данных путем замены предварительно определенных полей в сообщениях GOOSE или SV.

Фильтр «белого списка» и туннелирование

Из соображений кибербезопасности, масштабируемости и нагрузки на канал связи данные GOOSE и SV не следует передавать на все остальные подстанции. В данном случае должен применяться принцип «нужной информации», т.е. только необходимые данные GOOSE и SV должны передаваться на удаленные подстанции. Это обеспечивается с помощью фильтрующего блока, который гарантирует, что локальная и удаленная подстанции (и шины процесса) могут обмениваться только необходимой информацией. Для этого организуется фильтрация на передающей стороне и формируется «белый список» на принимающей стороне. Кадр GOOSE или SV может проходить в систему и туннелироваться в направлении принимающей стороны, только если совпадут критерии фильтрации для GOOSE/SV. Весь остальной трафик остается в сети локальной подстанции и не обрабатывается системой. Аналогичный процесс выполняется в отношении соединения между глобальной вычислительной сетью WAN и шиной станции/процесса. Только соответствующие заданным критериям сообщения могут попасть на подстанцию, в то время как все остальные сообщения/пакеты отбрасываются. Дополнительным расширением этого функционала является аутентификация. Все это вместе формирует надежную функцию брандмауэра на уровне L2, которая разграничивает зоны безопасности, но при этом позволяет обмениваться данными в реальном времени между концами линии.

Диагностика, аутентификация и резервирование

Соединение подстанций друг с другом подразумевает передачу данных за пределы подстанций по глобальной сети WAN. Это устанавливает дополнительные требования к информационной безопасности, а также контролю потоков данных в целях обеспечения надежности и защиты. Проблема кибербезопасности решается с помощью аутентификации пакетов данных AES-256 на уровне приложения во избежание повторения, трансформации или манипулирования данными в сети WAN. Чтобы гарантировать максимальную доступность, все каналы передачи данных постоянно диагностируются, и в случае отказа канала выдается сигнал тревоги. При обрыве сетевого соединения функция резервирования обеспечивает мгновенное переключение на второй тракт данных в сети WAN.

Для задач наладки и обслуживания решение предоставляет функции диагностики данных GOOSE и потоков SV в устройствах связи, позволяющие контролировать туннелирование каждого отдельного GOOSE и SV.

Поддержка HSR/PRP

ИЭУ, выполняющее функции шлюза, является частью подстанции, соответствующей МЭК 61850, поэтому поддерживает уже ставшие стандартными протоколы резервирования HSR и PRP и гарантирует благодаря этому максимальные надежность и быстродействие.

Применение, потенциал новой системной архитектуры

В отличие от традиционных подстанций, где ИЭУ защиты и управления индивидуально и независимо друг от друга собирают и используют данные процесса в реальном времени, на цифровых подстанциях данные процесса собираются полевыми устройствами и передаются в ИЭУ защиты и управления по сети связи. При передаче данных по сетям Ethernet их доступность для широкого спектра функций внутри и вне подстанции ограничивается лишь архитектурой сетей связи и управлением потоками передаваемых данных. По сравнению с сегодняшней ситуацией, когда обмен аналоговыми данными в реальном времени ограничен дифференциальной защитой линии между терминалами одного и того же производителя, а также функциями передачи векторных измерений для глобальной централизованной системы мониторинга и управления переходными режимами, потенциал передачи выборок аналоговых значений

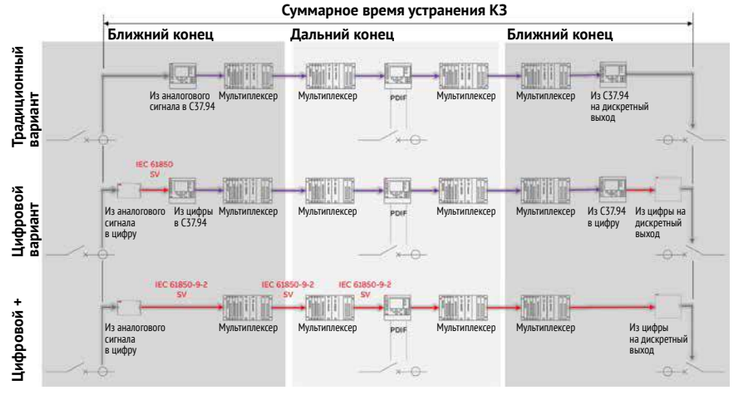


Рис. 10. Обзор различных вариантов дифференциальной защиты линии

и данных GOOSE между несколькими подстанциями открывает новые возможности для решения задач релейной защиты, управления и автоматизации во всей энергосистеме. Приведенные ниже примеры дают идеи выхода за границы традиционных решений и призывают обратить внимание на новые решения, которые становятся возможными благодаря доступности дискретных и аналоговых данных в реальном времени.

В тех случаях, когда есть каналы связи между подстанциями, а сами подстанции цифровые, подобные решения легко внедрить – необходимо лишь дополнить оборудование связи устройствами для обмена данными GOOSE и SV.

Автоматическое регулирование напряжения

Как правило, функции АРН работают на основе напряжения, измеренного непосредственно на низкой стороне силового трансформатора. Передача измерений напряжения с дальних концов линии в функцию АРН на понижающей подстанции может помочь оптимизировать регулирование напряжения и минимизировать число операций устройства регулирования под нагрузкой (РПН). Это не только продлевает срок службы устройства РПН, но и повышает стабильность сети.

Интеграция возобновляемых источников энергии

Для регулирования генерации распределенных ветряных или солнечных электростанций обычно требуется измерять ток и напряжение в точках подключения к сети. Возможность передачи аналоговых результатов измерений, полученных в точке подключения к сети, диспетчеру электростанции без необходимости протягивания цепей от трансформаторов тока за пределы подстанции позволяет использовать оборудование совместно, избежать дополнительных зависимостей и ограничений во время эксплуатации и обслуживания.

По мере распространения возобновляемых источников энергии необходимо решать новые задачи в области релейной защиты. Более слабые токи короткого замыкания могут создать трудности для традиционных схем защиты и требуют разработки новых подходов, например, к защите линии. В то время как дистанционная защита линий широко используется для ЛЭП, сети со сложной конфигурацией и слабыми токами короткого замыкания нуждаются в дифференциальной токовой защите. Дальнейшая цифровизация подстанций, заключающая в передаче выборок аналоговых значений по технологической сети, дает возможность внедрения экономически эффективных функций дифференциальной защиты, при которых устройство, уста-

Рис. 11. Разница времени устранения КЗ [мс] в сравнении с традиционной схемой C37.94 64 кбит.

новленное на одной подстанции, способно обрабатывать потоки SV как со своей, так и с удаленных подстанций.

Схемы противоаварийной автоматики (ПА)

Схемы противоаварийной автоматики традиционно основываются на дискретных данных и, иногда, на аналоговых значениях, передаваемых, к примеру, по протоколу C37.94 между ИЭУ в составе подстанций. Изредка используются данные векторных измерений, которые обрабатываются в центральной точке. Возможность обмена данными процесса между подстанциями в реальном времени позволяет внедрить новые решения по противоаварийной автоматике с использованием дискретных и аналоговых данных, поступающих с нескольких подстанций в сети.

Быстродействие

После обсуждения новых подходов к дифференциальной защите линий в главе 3 особый интерес вызывает быстродействие, обеспечиваемое различными подходами. На рис. 9 представлен обзор описанных ранее схем. Традиционный подход с проводными соединениями между ИЭУ дифференциальной защиты линий и трансформатором тока и выключателем, а также со связью между ИЭУ и подстанциями с использованием C37.94 сравнивается с двумя цифровыми вариантами. В одном варианте – «цифровом» – ИЭУ дифференциальной защиты линий преобразуют выборки мгновенных значений и данные GOOSE в формат C37.94 и обратно; в другом – «цифровом+» – между подстанциями передаются выборки SV и сообщения GOOSE. Во втором случае присутствует только одно ИЭУ дифференциальной защиты линии, обрабатывающее SV и GOOSE, которые поступили с обоих концов линии.

Ключевым показателем при анализе быстродействия является суммарное время устранения КЗ. Как правило, этот интервал включает также значения времена срабатывания и горения дуги для выключателя, которые не учитываются в тестовых испытаниях. Поскольку основное внимание уделено передаче сигнала, только ИЭУ РЗА на «дальнем» конце линии выполняет функцию дифференциальной защиты (PDIF), а ИЭУ на «ближнем» конце используется только для получения и передачи сигнала в рамках этой упрощенной схемы.

Суммарное время устранения КЗ

В описанном контексте суммарное время устранения КЗ – это промежуток времени между изменением силы подаваемого тока до значения, соответствующего КЗ, на одном из концов линии (ближний конец) и моментом получения сигнала аварийного отключения выключателем на ближнем конце линии, сформированного ИЭУ дифференциальной защиты на другом конце линии. На рис. 10 показаны те же варианты дифференциальной защиты, но с точки зрения передаваемых потоков данных. Устройство на ближнем конце линии отображено дважды: как источник аналоговых измерений и как приемник дискретных сигналов аварийного отключения. ИЭУ РЗА на «дальнем» конце линии (отмеченное как «PDIF») получает данные слева (ближний конец), выполняет функцию дифференциальной защиты PDIF с учетом локальных данных и посылает сигнал аварийного отключения направо (к устройствам, которые физически являются снова теми же, что установлены на ближнем конце линии).

В целях более точной оценки влияния связи между подстанциями на время устранения КЗ тестовая схема отличается от реальной системы тем, что функция PDIF выполняется только на одном конце линии (утверждение верно и для традиционного варианта). Это означает, что данные должны быть переданы дважды через канал связи – сначала аналоговые значения от локальной подстанции без функции PDIF на удаленную подстанцию с PDIF. Затем информация об аварийном отключении должна вернуться с дальнего конца на выключатель ближнего конца, где измеряется промежуток времени с момента изменения силы тока на величину, соответствующую КЗ, до момента поступления сигнала аварийного отключения с дальнего конца.

Тестовая схема и измерительное оборудование

Используемая тестовая схема состоит из двух комплектов оборудования для современной подстанции со следующими компонентами:

- Телекоммуникационное оборудование, использующее технологию передачи MPLS-TP для данных GOOSE, SV и C37.94
- Коммутатор L2-уровня, на котором построена шина станции и шина процесса
- Преобразователь аналоговых сигналов, подключенный к трансформатору тока и выполняющий измерения аналоговых сигналов и их преобразование в потоки данных SV согласно МЭК 6180-9-2
- Терминал дифференциальной защиты линии, одновременно выступающий в роли преобразователя дискретных сигналов с релейными выходами, срабатывающими при получении сигнала аварийного отключения от подстанции на дальнем конце
- Гроссмейстерские часы PTP для синхронизации

Для подачи токов и измерения времени устранения КЗ использовалось устройство Omicron CMC356.

В трех разных тестовых схемах, изображенных на рис. 9, использованы одинаковые аппаратные компоненты, описанные выше; устройство Omicron подключалось к различным платам аналоговых входов, а также использовались различные конфигурации устройства дифференциальной защиты.

Условия измерений

Поток данных C37.94 для традиционного и цифрового вариантов передается с помощью телекоммуникационного оборудования. Этот канал связи между подстанциями добавляет задержку времени устранения КЗ, равную 1 мс. Эта постоянная задержка времени в обоих направлениях передачи данных необходима для выполнения функций дифференциальной защиты независимо от часов GPS.

Используемый терминал РЗА оснащен двумя различными интерфейсными модулями C37.94. Один из них поддерживает канал передачи данных между двумя подстанциями с пропускной способностью 64 кбит, второй – 2 Мбит. Для получения полного представления о суммарном времени устранения КЗ для различных модулей и, следовательно, для разной пропускной способности канала связи измерения всегда выполняются для обоих модулей.

Результаты измерений

На диаграмме ниже приведено относительное время устранения КЗ по сравнению с традиционным решением для канала 64 кбит, которое является наиболее распространенным на текущий момент.

В силу особенностей тестовой схемы, в которой канал связи между подстанциями учитывается дважды (аналоговый сигнал в одну сторону и дискретный сигнал в обратную сторону), зарегистрированные значения необходимо поделить на два, чтобы оценить разницу задержки времени передачи в одном направлении.

По сравнению с традиционной схемой с пропускной способностью канала 64 кбит/с можно заметить, что увеличение скорости связи для интерфейса C37.94 до 2 Мбит/с существенно уменьшает время устранения КЗ в рамках проанализированной схемы. В цифровом варианте с шиной процесса для GOOSE и SV требуется немного больше времени из-за дополнительной задержки, обусловленной добавлением устройства ПДС, которое получает сигнал аварийного отключения по протоколу GOOSE и перенаправляет его на свои дискретные выходы. Дополнительное время можно полностью компенсировать за счет применения ПДС с быстродействующими выходами – исключая промежуточные реле и используя твердотельные выходы, срабатывающие быстрее традиционных релейных выходов.

В варианте «Цифровой+», где отсутствует преобразование аналоговых значений или цифровых выборок МЭК 61850 в формат C37.94, а также по протоколу C37.94 не передаются дискретные данные, достигается существенное сокращение времени передачи, влияющее на время устранения КЗ. В основном это обусловлено тем фактом, что в данном варианте используются только технологии с коммутацией пакетов, и в нем отсутствует необходимость преобразования кадров Ethernet в технологию с коммутацией каналов C37.94. Использование Ethernet для связи как внутри подстанции, так и между подстанциями, упрощает структуру системы и не требует изменения технологий передачи данных.

Выводы

Как продемонстрировано в настоящей статье, на базе современных технологий и стандартов возможно внедрение новых «продвинутых» концепций цифровой подстанции. Подобные схемы обладают существенными преимуществами: расширенные возможности обмена данными с ускорением времени срабатывания защиты, увеличение наглядности решений, повышение доступности и, наконец, наличие потенциала для экономии средств за счет упрощения проектных решений, монтажа и технического обслуживания. Тем не менее, существует потребность в существенных изменениях подходов к проектированию подстанций, синхронизации с точным временем в масштабе всей сети и внутреннему взаимодействия служб эксплуатации, а также в принятии новых решений, не применявшихся ранее. Цифровизация энергетических систем, увеличение сложности сетей из-за интеграции все большего количества возобновляемых источников приводит к усложнению схем защиты. Усиливающееся стремление создать высокоэффективную сеть при минимизации затрат дает толчок к поиску новых решений. Реализация описанного решения – это один из возможных ответов на множество вызовов в электроэнергетике ●

ЛИТЕРАТУРА ►**1.** R. Baechli, M. Kranich, R. Chowdhury, M. Haeusler и Y. A. Jassassi, «Релейная защита на базе обмена МЭК 61850 GOOSE между подстанциями», CIGRE-GCC, Маскат, 2017 г. ►**2.** «Техническая брошюра CIGRE 192. Релейная защита с использованием каналов связи», август 2001 г. ►**3.** «МЭК 60834-1. Аппаратура РЗА с передачей телесигналов для энергетических систем. Эксплуатационные характеристики и испытания», МЭК, Женева, Швейцария, октябрь 1999 г. ►**4.** «Техническая брошюра CIGRE 521. Релейная защита линий и систем на базе цифровых каналов и коммутации пакетов», декабрь, 2012 г.

В промышленности требования к ЛВС становятся все более серьезными, т.к. АСУ ТП берут на себя все больший функционал, и потери данных могут повлечь серьезные издержки. Например, в энергетике, если на терминал РЗА не попадут вовремя данные от измерительных преобразователей, то это может быть чревато распространением короткого замыкания на смежные участки электросети, что скажется убытками гораздо более серьезными, нежели в случае своевременного отключения участка с КЗ. Поэтому часто в проектах энергетики можно встретить требование «Время восстановления менее 1 мс».

ПРОТОКОЛЫ «БЕСШОВНОГО» РЕЗЕРВИРОВАНИЯ PRP И HSR

Илья Смирнов
Менеджер по продукции «Сетевые технологии»
ООО «Феникс Контакт РУС»

Резервирование сети на основе таких распространенных в промышленности протоколов, как RSTP, MRP, DLR и прочих подобных, основано на изменении топологии в случае возникновения какой-либо неисправности при передаче данных. Изменение топологии занимает определенное время (от миллисекунд до секунд в зависимости от протокола), которое и называется «временем восстановления». В течение этого времени связи с частью сети нет и, соответственно, данные теряются. Т.е. привычные технологии кольцевого резервирования не позволяют обеспечить время восстановления меньше 1 мс. Ввиду этого набирают популярность технологии так называемого «бесшовного» резервирования — PRP и HSR. Резервирование на основании PRP и HSR осуществляется, в отличие от вышеобозначенных протоколов, не за счет перестроения топологии, а за счет дублирования фреймов. Каждый фрейм дублируется отправителем, и оба фрейма передаются разными путями, а принимающий узел обрабатывает фрейм, пришедший первым, и отбрасывает второй. Данный принцип работы не требует выполнения перестроения топологии и, соответственно, данный протокол действует практически «бесшовно».

Структура сети

«Бесшовное» резервирование реализуется на конечных узлах, а не на сетевых компонентах. Это одно из самых главных отличий PRP и HSR от других протоколов резервирования, таких как RSTP или MRP. Рассмотрим особенности структуры сети для PRP и HSR.

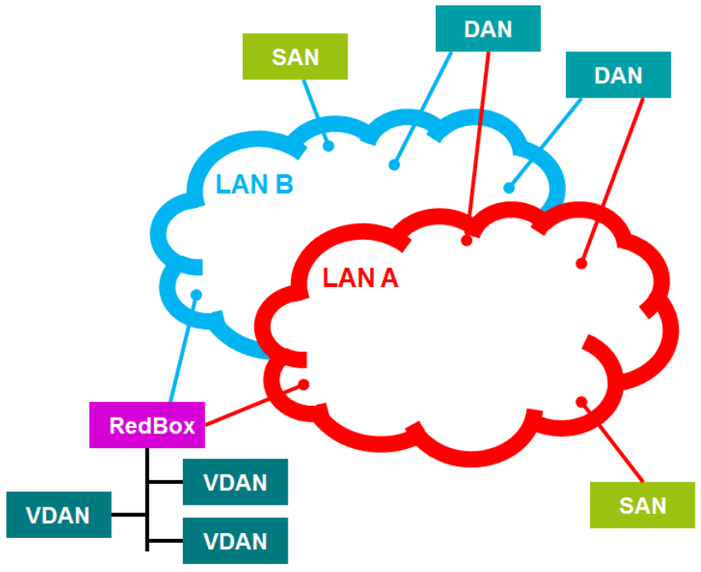


Рис. 1. Структура сети PRP

PRP – структура сети

Конечный узел имеет два Ethernet-интерфейса, которые подключаются к двум изолированным друг от друга сетям, действующим параллельно и имеющим независимую топологию (т.е. топологии этих двух сетей могут быть как одинаковыми, так и различаться). Сети должны быть изолированными для того, чтобы любая неисправность и остановка передачи данных в одной сети не влияли на вторую, т.е. даже питание сетей осуществляется от разных источников. Никаких прямых соединений между этими сетями быть не должно. Эти две сети обычно называются LAN A и LAN B. Как уже обозначалось ранее, они могут иметь различные топологии, а также различную производительность. Задержки в передачи данных также могут различаться. В сети могут присутствовать следующие элементы:

- DAN (Dual Attached Node) — узел, который подключается к обеим сетям и посылает/принимает дублированные фреймы;
- SAN (Single Attached Node) — узел, который подключается только к одной сети (LAN A или LAN B) и посылает/принимает обычные фреймы;
- В случае, когда к PRP-сети необходимо резервировано подключить устройство, имеющее один Ethernet-интерфейс, и без поддержки протокола PRP, используется так называемый Redundancy Box (чаще RedBox). На RedBox'е пакет от устройства дублируется и передается в сеть PRP, так словно данные передаются от DAN. Более того, устройство, которое находится за RedBox'ом, видится для остальных устройств как DAN. Такой узел называется виртуальный DAN или VDAN (Virtual DAN).

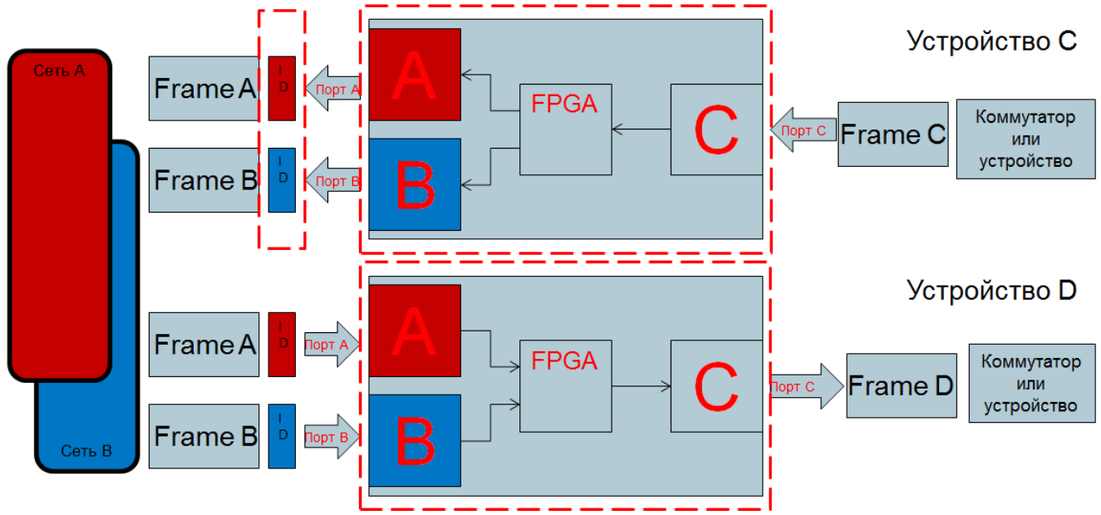


Рис. 2. Принцип работы RedBox'а

HSR – структура сети

Принцип действия HSR заключается в том, что все устройства объединяются в кольцо и все сообщения, также как и в PRP, дублируются. Устройство отправляет оба фрейма через кольцо: одну копию по часовой стрелке, другую — против. Приемник получает обе копии, но обрабатывает только первую, а вторую удаляет. Если с каким-то из линков что-то случается, и один из дублированных фреймов не приходит, то про-

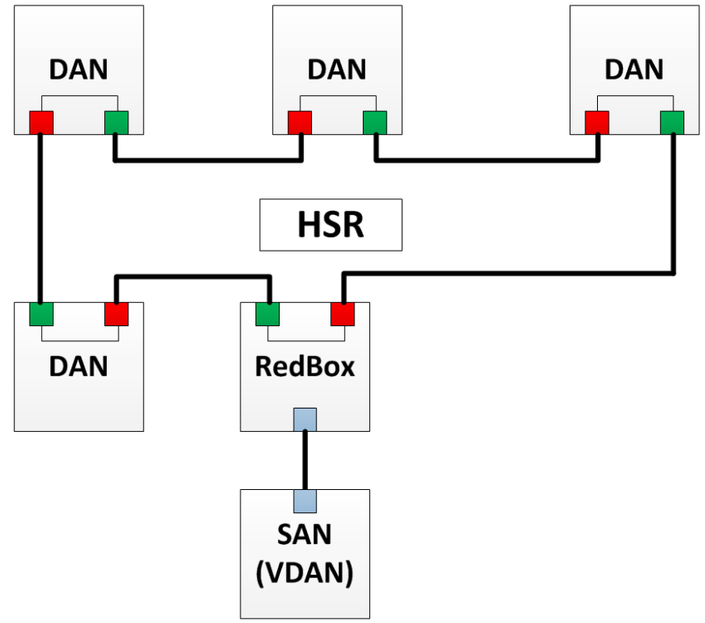


Рис. 3. Структура сети HSR

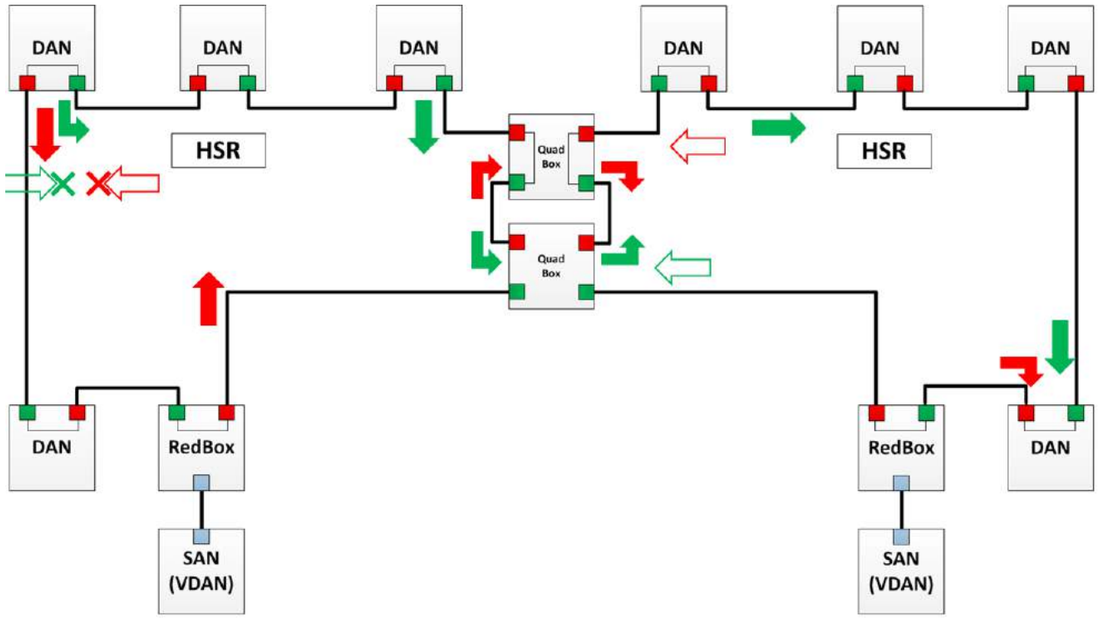


Рис. 4. Пример использования QuadBox

сто принимается другой. Все HSR-устройства имеют два Ethernet-интерфейса — порт A и порт B. В соответствии с протоколом HSR в сети могут существовать следующие элементы:

- SAN — узел, имеющий только один Ethernet-интерфейс. Такой узел может быть подключен к HSR-сети исключительно через RedBox;
- DAN — узел, который может обмениваться данными внутри HSR-кольца (может посылать/принимать дублированные фреймы);
- RedBox — также как и в PRP, RedBox позволяет подключить устройство, имеющее один Ethernet-интерфейс, к HSR-сети. Устройство, которое находится за RedBox'ом, видится для остальных устройств как DAN. Такой узел называется виртуальный DAN или VDAN (Virtual DAN);
- QuadBox - это новый элемент, который вводит HSR. Это устройство, имеющее четыре HSR-порта. Оно позволяет объединять два HSR-кольца. В каждом кольце QuadBox выполняет роль DAN и может пересылать данные из одного кольца в другое.

Структура DAN

Для PRP и для HSR структура DAN похожа. Каждый DAN имеет два интерфейса, действующих параллельно и подключенных к верхнему уровню одного коммуникационного стека через так называемый уровень LRE — link redundancy entity. На данном уровне выполняются все функции резервирования.

Оба интерфейса DAN имеют одинаковые MAC-адреса и один IP-адрес. Это позволяет сделать резервирование прозрачным для верхнего уровня. Особенно важен тот факт, что это позволяет использовать протокол ARP для DAN также, как и для любого нерезервированного узла. Однако, конечно, в структуре DAN для PRP и для HSR имеются и нюансы.

PRP – структура DAN

Когда с верхнего уровня посылается фрейм, LRE дублирует его и посылает оба пакета через порты практически одновременно. Оба фрейма передаются параллельно через две сети с разными задержками. В идеальной ситуации они доставляются на узел назначения с минимальной разницей во времени. При получении LRE приемника передает на верхний уровень первый принятый фрейм, а второй отбрасывает. LRE создает дублированные фреймы при отправке и обрабатывает их при получении. Данный уровень, по отношению к верхнему уровню, представляет собой обычный интерфейс нерезервированного сетевого адаптера. LRE выполняет две задачи: обработка дублированных фреймов и управление резервированием. Для реализации управления LRE добавляет к каждому фрейму 32-битный трейлер контроля резервирования (redundancy control trailer — RCT) и удаляет его при получении фрейма.

HSR – структура DAN

Фрейм, присланный с верхнего уровня, дублируется уровнем LRE, и пакеты посылаются через порт A и порт B практически одновременно (1 и 2 на рис. 6). Приемник при получении фрейма передает его на уровень LRE, а также перенаправляет на другой порт и передает дальше в кольце (3, 4). Если фрейм приходит на отправитель, то дальше этот фрейм не передается, а уничтожается (5, 6).

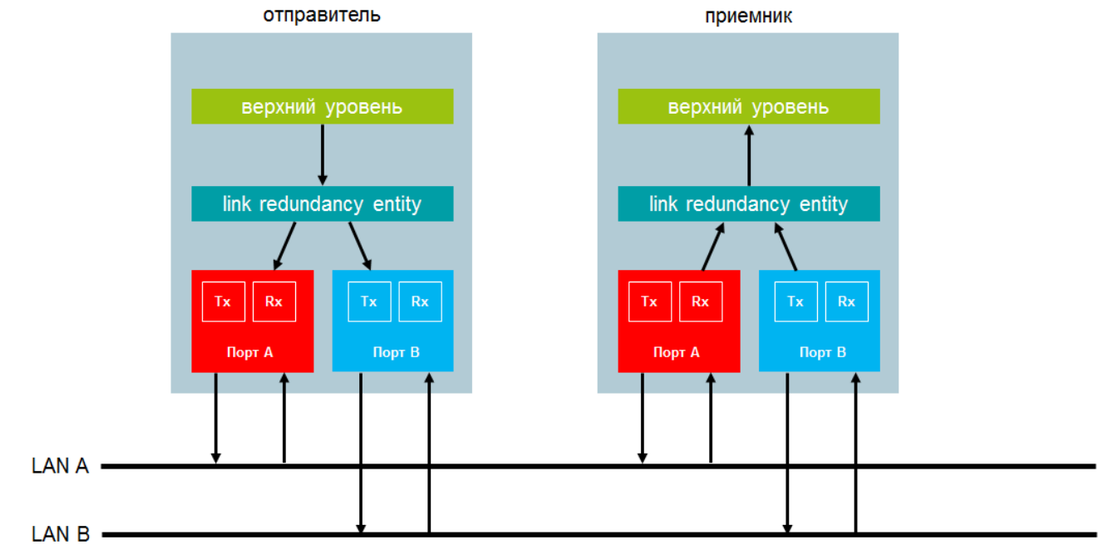


Рис. 5. Передача данных между двумя DAN в PRP

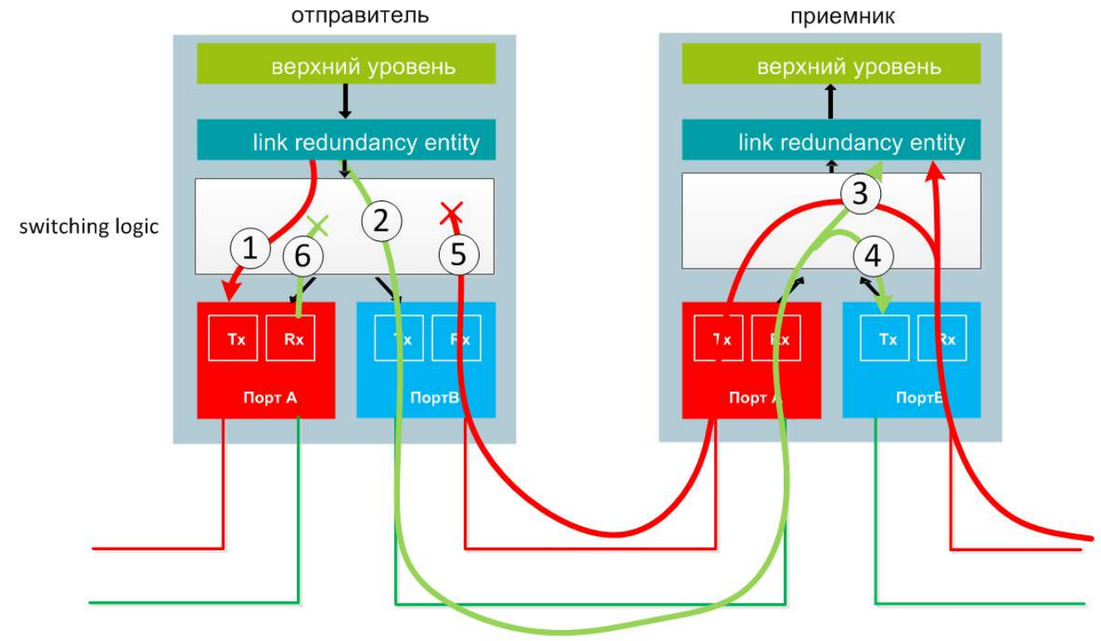


Рис. 6. Передача данных между двумя DAN в HSR

На уровень LRE приходят оба фрейма, но на верхний уровень передается тот, который был прислан быстрее, а дублированный фрейм отбрасывается. LRE добавляет к каждому фрейму 48-битный HSR-тег (сродни добавлению VLAN-тега) и удаляет этот тег при получении.

Взаимодействие между SAN и DAN

В PRP SAN может быть подключен к любой сети – LAN A или LAN B, но такой узел не поддерживает функций резервирования. Поэтому SAN, подключенный к одной сети, не сможет обмениваться данными с другим подобным узлом, подключенным ко второй сети. Для взаимодействия с SAN DAN генерирует специальные фреймы. Эта необходимость вызвана тем, что SAN в обычном фрейме от резервированного устройства должен игнорировать RCT, что сделать не пред-

Рис. 7. Фрейм с добавленным RCT

ставляется возможным, так как SAN не может отличить RCT от обычного блока данных IEEE 802.3. В свою очередь, DAN понимает, что отправляет фрейм на SAN и не добавляет RCT в фрейм. Он просто пересылает один фрейм с верхнего уровня на тот интерфейс, к которому подключен SAN. Другими словами, если DAN не может определить, что обменивается данными с другим DAN, то он не добавляет RCT в фрейм. В HSR SAN не может быть подключен напрямую к сети. Его можно подключать исключительно через RedBox

Режимы работы DAN

При работе с дублированными фреймами, принимаемыми на обоих интерфейсах (в случае их исправности), DAN необходимо принять один из фреймов, а второй отбросить. В PRP есть два метода обработки:

Duplicate accept — метод, при котором оба пришедших фрейма принимаются и перенаправляются на верхний уровень;

Duplicate discard — метод, при котором узел-приемник считывает информацию из RCT пришедшего фрейма для того чтобы определить, какой фрейм отбрасывать.

Для HSR рассмотрим наиболее популярные режимы U и X.

Duplicate accept

DAN, работающий в данном режиме не отбрасывает ни один из фреймов при обработке на канальном уровне. Фреймы отправляются в LAN A и LAN B без RCT. LRE приемника просто перенаправляет оба фрейма на верхний уровень, предполагая, что при дальнейшей передаче дубликаты будут уничтожены (в IEEE 802.1D четко прописано, что протоколы верхнего уровня должны уметь обрабатывать дублированные фреймы). Например, протоколы TCP и UDP имеют высокий уровень устойчивости к дублированным фреймам. Данный метод очень прост в реализации, но имеет серьезный недостаток — он не предоставляет никаких возможностей контроля сети, т.к. никаким образом не отслеживается корректность приема обоих фреймов.

Duplicate discard на канальном уровне

При использовании второго метода в фрейм добавляется поле, состоящее из четырех октет — RCT (redundancy control trailer). Трейлер добавляется на уровне LRE, когда фрейм принимается от верхнего уровня. RCT состоит из следующих параметров:

- 16-битный номер последовательности;
- 4-битный идентификатор сети, 1010 (0xA) для LAN A и 1011 (0xB) для LAN B;
- 12-битный размер фрейма.

Из-за добавления к фрейму RCT-трейлера его размер получается больше максимального размера фрейма, определенного в стандарте IEEE 802.3-2005. Для передачи данных внутри сети с PRP оборудование должно быть сконфигурировано для передачи данных размером 1496 октет. Из-за этого не каждый коммутатор подходит для использования в LAN A или LAN B.

Каждый раз, когда канальный уровень посылает фрейм на какой-то определенный адрес, отправитель увеличивает номер последовательности для соответствующего узла и отправляет идентичные фреймы через оба интерфейса. Узел-приемника должен определить дубликаты, основываясь на информации из RCT.

Алгоритм метода Duplicate discard

Приемник предполагает, что фреймы, присылаемые от любого источника, работающего по протоколу PRP, посылаются последовательно с постоянно возрастающим номером. Номер последовательности, который ожидается у следующего фрейма хранится в переменных ExpectedSeqA и соответственно ExpectedSeqB.

При приеме, корректность последовательности может быть проверена при помощи сравнения значения ExpectedSeqA (ExpectedSeqB) с номером последовательности полученного фрейма, хранящемся в переменной currentSeq в RCT. При положительном результате, переменная ExpectedSeq устанавливается на один больше, чем currentSeq для того, чтобы далее можно бы было выполнять корректную проверку на данной линии.

Для обоих интерфейсов существует динамический интервал отбрасывания фрейма (sliding drop window) для парных номеров последовательности. Верхней границей данного интервала является ExpectedSeq (следующий ожидаемый номер последовательности на данном интерфейсе), исключая само данное значение, а нижней границей данного интервала является startSeq (наименьший номер последовательности, при котором происходит отбрасывание дублированного фрейма с таким номером последовательности). После проверки правильности номера последовательности, приемник решает отбрасывать данный фрейм или нет. Предположим, что LAN A имеет ненулевой размер интервала отбрасывания фрейма (рис. 8). Фрейм из LAN B, чей номер лежит в данном интервале, будет отброшен. Все остальные фреймы из LAN B будут приняты и отправлены на верхний уровень.

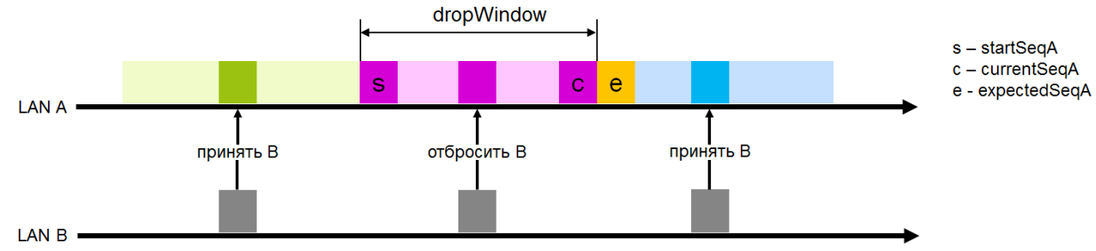


Рис. 8. Интервал отбрасывания фрейма (drop window)

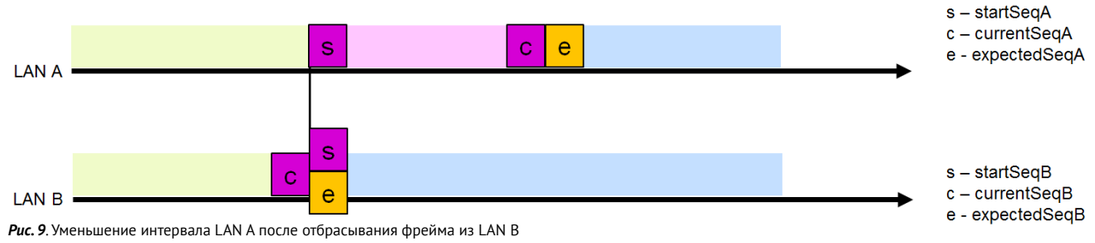


Рис. 9. Уменьшение интервала LAN A после отбрасывания фрейма из LAN B

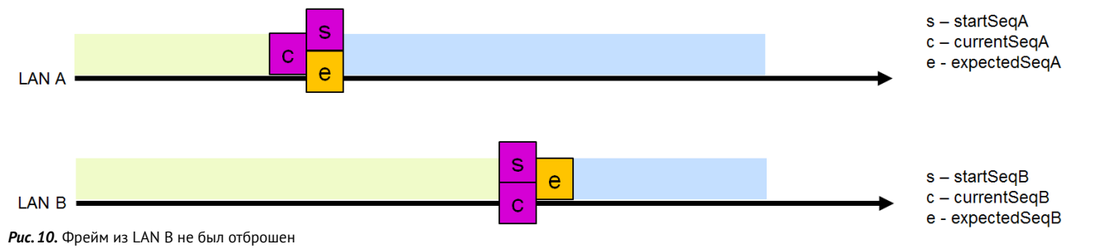


Рис. 10. Фрейм из LAN B не был отброшен

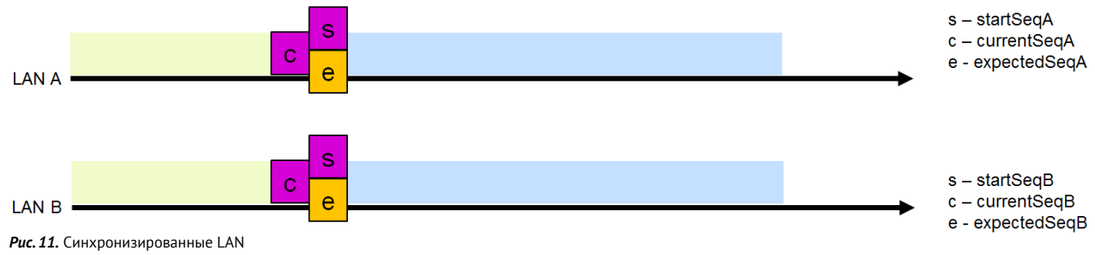


Рис. 11. Синхронизированные LAN

Отбрасывая фрейм из LAN B, уменьшается размер интервала LAN A, т.к. после получения данного фрейма не ожидается никаких фреймов с меньшим номером на данном интерфейсе. Соответственно, startSeqA устанавливается на один больше, чем currentSeqB. При этом размер интервала отбрасывания фрейма LAN B сбрасывается до 0 (startSeqB = = expectedSeqB), т.к. очевидно, что фреймы LAN B «отстают» от LAN A и никакие фреймы из LAN A не должны быть отброшены.

В ситуации на рис. 9, когда несколько фреймов из LAN A приходят подряд, но из LAN B не приходит ничего, то они принимаются, т.к. их currentSeq находится вне интервала отбрасывания фрейма LAN B и интервал LAN A увеличивается на одну позицию. Если фреймы из LAN A продолжают приходить, а из LAN B по-прежнему ничего не приходит, при достижении максимального размера интервала startSeqA начинает также увеличиваться на единицу. Когда принимаемый фрейм находится вне интервала отбрасывания фрейма другого LAN, то этот фрейм сохраняется, а размер интервала данного интерфейса устанавливается равным 1, что означает, что только фрейм из другого

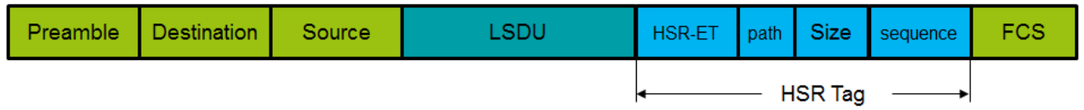


Рис. 12. Фрейм с добавленным HSR-тегом

LAN с таким же номером последовательности будет отброшен, в то время как drop window другого интерфейса устанавливается равным 0, что означает, что ни одного фрейма не будет отброшено (рис. 10).

Наиболее общая ситуация – когда оба интерфейса синхронизированы и размер обоих интервалов равен 0 (рис. 11), что означает, что будет принят фрейм того интерфейса, который придет первым, и интервал данного интерфейса будет увеличен до 1, что позволит отбросить фрейм от другого интерфейса с таким же номером последовательности.

Из-за наличия идентификатора LAN в RCT, дублированные фреймы различаются на один бит (и имеют разные контрольные суммы). Приемник проверяет принадлежность фрейма к интерфейсу (т.е. проверяет, что фрейм с идентификатором LAN A пришел на интерфейс A). Приемник не отбросит данный фрейм, т.к. он может содержать полезную информацию в блоке данных, но в этом случае будет увеличен на единицу счетчик cntWrongLanA или cntWrongLanB. Так как подобные ошибки не разовые (перепутаны местами LAN A и LAN B), то счетчик будет возрастать постоянно.

Передача HSR-трафика на канальном уровне

При передаче данных внутри HSR-сети к каждому фрейму добавляется HSR-тег. HSR-тег состоит из следующих параметров:

- 16-битного HSR Ethertype
- 4-битного индикатора направления (path indicator)
- 12-битного размера фрейма
- 16-битного номера последовательности

Отправитель вставляет одинаковые номера последовательности отправляемым дублированным фреймам и затем инкрементирует номер последовательности для каждой посылки, отправленной с данного узла.

Приемник отслеживает номера последовательности всех фреймов от каждого источника, от которого он принимает данные (источники он различает по MAC-адресу). Если фреймы приходят с разных линий и имеют одинаковый источник и номер последовательности, то один из них принимается, а второй отбрасывается.

Для контроля сети, на каждом устройстве ведется таблица всех узлов в сети, от которых он принимает данные. Это позволяет обнаружить исчезновение узлов и ошибки на шине.

Узел определяет фрейм, который он отправил по источнику и по номеру последовательности.

Узел HSR никогда не отбрасывает фрейм, который он ранее не получал. Узел определяет практически все дублированные фреймы, но в случае, если их немного, он их не удаляет, т.е. фрейм просто проходит все кольцо и уничтожается на отправителе.

В стандарте алгоритм определения дублированных фреймов не определен. В качестве возможных методов могут быть использованы хэш-таблицы, очереди и отслеживание номеров последовательности.

Режим U

В данном режиме узел, который принимает фрейм, уничтожает дубликат и не позволяет ему распространяться дальше. В случае, если фрейм все-таки были передан далее, то он уничтожается на следующих узлах. Данный режим позволяет разгрузить кольцо от Unicast-трафика. На схеме красными стрелками обозначены пакеты с HSR-тегом, отправленные с порта «A» (в дальнейшем — фрейм «A»). Зелеными стрелками обозначены пакеты с HSR-тегом, отправленные с порта «B» (в дальнейшем — фрейм «B»). Пустыми стрелками обозначен отброшенный трафик, т.е. фреймы, которые бы передавались при обычной работе, но в данном режиме были отброшены. Крестом обозначается удаление трафика из кольца (в любом случае).

Режим X

В данном режиме узел не передает фрейм дальше и отбрасывает его, если такой фрейм был получен с другого направления. Например, DAN 1 на изображении не передаст дальше фрейм «B», т.к. он уже получил фрейм «A», а DAN 2 не будет передавать далее фрейм «A», т.к. уже получил фрейм «B». В случае, если в алгоритме произошла где-то ошибка и фреймы были переданы далее, то они будут отброшены на следующих узлах или на узле, на котором они были созданы. Режим X не применим для сообщений PTP и для передачи supervision frame.

Контроль сети

PRP

Приемник проверяет, что все фреймы приходят последовательно и корректно принимаются на обоих каналах. Он поддерживает счетчики ошибок, которые можно прочитать, например, через SNMP. Все устройства поддерживают таблицы узлов, с которыми они обмениваются данными. В этих таблицах содержится информация о времени, когда последний фрейм был отправлен или получен от конкретного узла и другую информацию, касающуюся протокола PRP. В то же время, данные таблицы позволяют обнаружить соединения, в которых необходимо синхронизировать номера последовательности, а также обнаружить нарушенные последовательности и пропавшие узлы. Диагностика основана на том, что каждый DAN периодически посылает диагностический фрейм (supervision frame), который позволяет проверить целостность сети и наличие узлов. В то же время данные фреймы позволяют проверить какие устройства выступают в качестве DAN, определить их MAC-адреса и в каком режиме они работают — duplicate accept или duplicate discard.

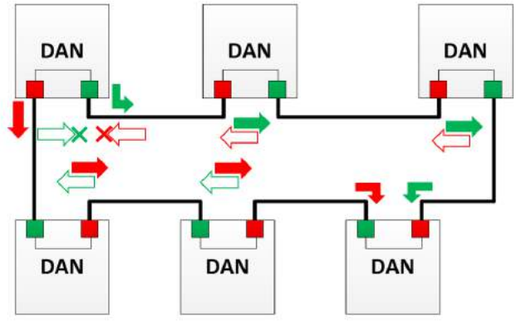


Рис. 13. Режим U

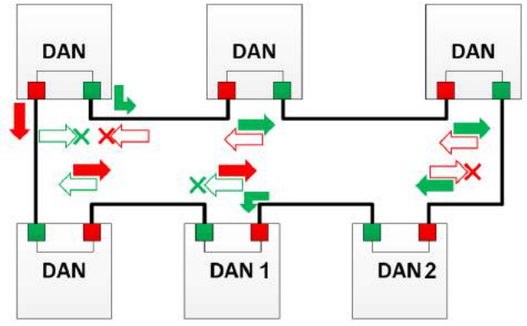


Рис. 14. Режим X

HSR

Каждый узел постоянно проверяет все линки.

Каждый узел периодически посылает диагностический фрейм (на оба порта), содержащий информацию о состоянии узла. Этот фрейм принимается всеми узлами, включая отправителя. Когда отправитель принимает собственное диагностическое сообщение, то выполняется проверка целостности физического канала. Интервал посылки диагностического фрейма сравнительно большой (несколько секунд), т.к. он не требуется для обеспечения резервирования, а нужен только для диагностических целей. Все узлы заносят в таблицу всех партнеров, которых удалось обнаружить, и регистрируют время, когда узел последний раз был активен, а также все пропущенные фреймы и фреймы, присланные не последовательно.

Таблица 1.
Плюсы и минусы HSR и PRP

	PRP	HSR
Бесшовное резервирование	Да	Да
Необходимость дополнительного оборудования для организации сети	Да	Нет
Экономичность	+ (требуется дублированная сеть)	+++ (не требуется дублированная сеть, не требуется дополнительное сетевое оборудование)
Гибкость	+++ (можно использовать в паре с другими протоколами, например, RSTP, HSR и т.д. Топологию сетей можно продумать абсолютно разную и любых масштабов)	+ (сложно сделать большую сеть, плохая совместимость с другими протоколами резервирования, топология может быть только кольцо, а также возможны различные варианты сопряжения этих колец)
Диагностика	Есть	Есть

Все произошедшие изменения топологии также регистрируются и вся информация может быть получена по SNMP.

Заключение

Нельзя сказать, что один протокол лучше другого — они созданы немного для разных применений (Таблица 1). И HSR, и PRP позволяют организовать бесшовное резервирование сети, но HSR позволяет создавать более бюджетные решения. Тем не менее подобная экономичность влечет за собой сложности, т.к. сеть на основе HSR достаточно сложно масштабировать, и применения не очень гибкие. Низкая гибкость обуславливается ограниченной топологией (кольцо, сопряжение колец), а также плохой совместимостью протокола с другими технологиями. Поэтому HSR лучше подходит для резервирования небольших систем и интеграции в большую сеть. Организовать резервирование всей сети на основе HSR достаточно проблематично. PRP же, в свою очередь, является решением более дорогим, но позволяющим организовать достаточно масштабную сеть, которую в дальнейшем можно будет расширять без проблем, т.к. данный протокол дает возможность удобно интегрировать практически любые технологии и реализовывать совершенно разные топологии ●

Ознакомиться с оборудованием Phoenix Contact вы можете на стр 3.
www.phoenixcontact.ru

В статье описывается проблема выхода из строя СОЕВ на подстанциях, и пути возможного решения проблемы. Представлено легко тиражируемое решение производства ООО «ПиЭлСи Технолоджи»: сервер времени TOPAZ МЕТРОНОМ PTS. Изделие подходит для замены выходящих из строя СОЕВ на различных АСУ ТП, а устойчивое функционирование гарантированно производителем. TOPAZ МЕТРОНОМ PTS полностью подходит под все требования программы импортозамещения и внесен в Государственный Реестр Средств Измерений Российской Федерации. Опытная эксплуатация подтвердила все заявленные производителем характеристики.

ОПЫТ ИСПОЛЬЗОВАНИЯ УСТРОЙСТВА СИНХРОНИЗАЦИИ ВРЕМЕНИ TOPAZ МЕТРОНОМ PTS (СЕРВЕРА ВРЕМЕНИ) В АСУ ТП ЭЛЕКТРИЧЕСКИХ ПОДСТАНЦИЙ 220 кВ

Игорь Сапожников
Московские высоковольтные сети

Рис. 1. Устройство синхронизации времени TOPAZ Метроном PTS

Более трети электрических подстанций Московских высоковольтных сетей – филиала ПАО «МОЭСК» оснащено автоматизированными системами управления технологическими процессами (АСУ ТП ПС). Одно из существенных условий их правильного функционирования – синхронизация времени всех устройств, интегрированных в АСУ ТП. Эту задачу выполняет система обеспечения единого времени (СОЕВ).

Схемы организации СОЕВ определялись архитектурными решениями АСУ ТП. В первых проектах (конец 90-х – начало 2000 гг.) интеграция осуществлялась, в основном, по последовательным интерфейсам RS485/RS232 на скорости 9600 бод. Точное время синхронизировалось в серверах АСУ ТП со спутников через GPS163/164 MEINBERG, подключенный через COMпорт. Затем серверы раздавали время терминалам РЗА с использованием возможностей протокола SPABUS (позднее МЭК 60870-5-103). Сохраняя архитектуру СОЕВ, позднее приемник точного времени к серверам АСУТП стали подключать через Ethernet.

Значительное изменение в архитектуре СОЕВ произошло с появлением протокола МЭК 61850 для подключения терминалов РЗА к серверам АСУ ТП. Это позволило производить синхронизацию времени не последовательно, через серверы АСУ ТП, а непосредственно с сервера точного времени по протоколу NTP. В проекты АСУ ТП стали закладывать NTP-сервера точного времени типа LANTIME M300 GPS, а для АСУ ТП на базе решений SIEMENS-SICLOCKGPS1000 и SICLOCKTM 400. Однако, со временем, эксплуатация АСУ ТП столкнулась с интенсивным выходом из строя СОЕВ на подстанциях различных производителей. Перед эксплуатирующими организациями встал вопрос, каким образом производить восстановление СОЕВ? Сам факт перехода на синхронизацию по NTP позволил, в качестве временного решения, обеспечить синхронизацию времени от сервера АСУТП, настроив у него NTP-сервер (и NTP-клиента для синхронизации его собственного времени по каналам с верхнего уровня управления). Однако решение, при котором работоспособность СОЕВ зависит от работоспособности канала связи, выходящего за пределы подстанции, можно рассматривать только как временное.

Рис. 2. Сервер точного времени SIEMENS - SICLOCK GPS1000

Рис. 3. Сервер точного времени SIEMENS – SICLOCK TM 400

Объемы ЗИП не позволяли произвести замену на всех объектах.

Политика импортозамещения вызвала затруднения с обоснованием необходимости приобретения импортного оборудования. На эти обстоятельства наложилась проблема 2099, вызывающая необходимость перепрошивки серверов времени SICLOCK. В качестве решения описанных проблем возникла идея заменить вышедшие из строя серверы времени (LANTIME M300 GPS, SICLOCK) на сервер времени отечественного производителя TOPAZ Метроном PTS. Опыт применения TOPAZ Метроном PTS показал возможность полноценной замены оборудования иностранных производителей, при этом полностью сохраняется весь функционал. С экономической точки зрения затраты и сроки на интеграцию оборудования сравнимы или значительно ниже.

Производитель успешно прошел отраслевые аттестации, получил сертификаты и лицензии Таможенного союза, ПАО «Газпром», ПАО «Россети», ФСТЭК, ФСБ. Компания является российским предприятием без иностранного капитала, производственная деятельность осуществляется только на территории РФ. К уникальным особенностям всей продукции компании можно отнести: информационная безопасность – ПО разработано в России и не используются исходные коды зарубежного происхождения, оригинальная операционная система, основанная на ОС Linux и независимость критически важных процессов от иностранных компонентов.

Синхронизация времени	
Пределы допускаемого абсолютного смещения собственной шкалы времени (ШВ) относительно ШВ Российской Федерации UTC(SU) в режиме синхронизации по сигналам ГЛОНАСС/GPS, нс	±200
Пределы допускаемого абсолютного смещения собственной ШВ относительно ШВ Российской Федерации UTC(SU) в режиме синхронизации по протоколу NTP, SNTP, мкс	±100
Пределы допускаемого абсолютного смещения собственной шкалы времени (ШВ) относительно ШВ Российской Федерации UTC(SU) на выходе Ethernet по протоколу PTP, нс	±250
Пределы допускаемой абсолютной погрешности хранения формируемой ШВ в автономном режиме за сутки, мс	±20
Передача данных	
Интерфейс Ethernet	до 16 портов
Тип разъема Ethernet	RJ-45 (опционально – LC оптический MM/SM, SFP)
Скорость обмена данными, Мб/сек	10/100/1000
Протоколы передачи данных Ethernet	NTP, SNTP, Modbus TCP, ГОСТ Р МЭК 60870-5-104
Протоколы резервирования	RSTP, PRP, HSR
Поддержка SNMP	есть
Интерфейс RS-485	до 8 портов
Протоколы передачи данных RS-485	МЭК 60870-5-101 (master/slave); Modbus RTU/ASCII (slave)

Функционал TOPAZ Метроном PTS

Устройство работает под управлением операционной системы Linux. Настройка, управление и контроль работы осуществляется посредством WEB- интерфейса, либо через консоль. Устройство поддерживает функции самодиагностики и передачу диагностической информации посредством SNMP.

Синхронизация собственных часов осуществляется с помощью сигналов спутниковых навигационных систем ГЛОНАСС/ GPS.

TOPAZ Метроном PTS обладает довольно гибкой архитектурой, и в зависимости от карты заказа может содержать практически неограниченное количество интерфейсов связи.

Уже базовая комплектация включает 2 порта Ethernet 1000BASE, 4 порта RS 485, выход 1PPS (электрический и оптический). Стоит отметить, что во всех комплектациях устройство поддерживает синхронизацию по протоколу PTPv2 (IEEE1588) в соответствии с энергетическим профилем IEC 61850-9-3, что является необходимым условием для сервера точного времени, применяемого в Цифровых подстанциях. Опытная эксплуатация производится для двух АСУ ТП с зимы 2019 г. Оборудование ООО «ПиЭлСи Технолоджи» показало удобство при монтаже, наладке и устойчивое функционирование. Представляется целесообразным, в целях унификации, производить замену выходящих из строя серверов и приемников времени всех АСУ ТП на данное изделие.

Устройство прекрасно вписалось в концепцию импортозамещения, а технические возможности TOPAZ Метроном PTS позволяют организовывать совместную работу с устройствами АСУ ТП и интегрируемыми в АСУ ТП терминалами (более подробно было описано выше).

ООО «ПиЭлСи Технолоджи» смогла не только разработать качественный продукт в нужное время с необходимым функционалом, но и сделать решение, которое беспроблемно интегрируются в существующие системы заказчика. Дополнительный существенный плюс – внесение сервера времени производства ООО «ПиЭлСи Технолоджи» в Государственный Реестр Средств Измерений Российской Федерации ●

Селективное выявление однофазных замыканий на землю (ОЗЗ) в воздушных сетях напряжением 6-35 кВ с изолированной нейтралью — чрезвычайно сложная задача. Напряжения и токи нулевой последовательности зависят от характеристик сети и переходного сопротивления в месте ОЗЗ. Например, при обрыве провода ВЛ переходные сопротивления иногда составляют несколько кОм, а токи нулевой последовательности, как правило, менее 1 А. Для обеспечения селективности в таких случаях необходимо, чтобы направленные токовые защиты от ОЗЗ были чувствительны к первичным токам порядка 0,1-0,3 А. При такой чувствительности защиты от ОЗЗ могут срабатывать от разного рода небалансов в сети, которые воспринимаются как признак возникновения ОЗЗ. Значения небалансов ограничивают минимальные уставки защиты, и становится сложно осуществить направленную токовую защиту от ОЗЗ, которая всегда бы работала правильно.

ЦЕНТРАЛИЗОВАННАЯ ЗАЩИТА ОТ ОЗЗ НА БАЗЕ УСТРОЙСТВ ПРОИЗВОДСТВА НТЦ «МЕХАНОТРОНИКА»

Проблема

Одна из главных проблем в реализации селективной защиты от ОЗЗ в сетях 6(10) кВ ПАО «Татнефть» – погрешности трансформаторов тока нулевой последовательности (ТТНП) при контроле малых емкостных токов. При этом погрешности ТТНП определяются не только конструкцией и качеством изготовления трансформаторов, но и условиями их применения. В области малых токов из-за погрешности ТТНП направленная защита может воспринимать емкостной ток собственного присоединения как активно-емкостной и срабатывать неселективно.

Решение

Возможности интеллектуальных устройств БМРЗ производства НТЦ «Механотроника» позволили построить централизованную защиту и решить задачу селективности ОЗЗ путем организации совместного анализа данных в локальной сети терминалов ПС и шкафа функционального контроллера ШФК-МТ с программным комплексом WebScadaMT. В используемом принципе выполняется как сопоставление токов нулевой последовательности, так и анализ динамики их изменения на всех присоединениях.

При разработке селективного устройства защиты от ОЗЗ в сетях 6 (10) кВ ПС-36 НГДУ «Альметьевнефть» ПАО «Татнефть» были поставлены следующие задачи:

1. Повысить достоверность и автоматизировать процесс определения поврежденного присоединения с использованием тока $3I_0$.

2. Уменьшить вероятность излишнего действия направленной защиты.

3. Обеспечить непрерывность действия устройства при устойчивых ОЗЗ.

4. Обеспечить регистрацию одиночных и повторно-кратковременных ОЗЗ.

Решение данной задачи было реализовано следующим образом:

- с помощью БМРЗ, установленных на ПС 110/35/6 (10) кВ, обеспечивается регистрация процессов и предварительная обработка данных, характеризующих ОЗЗ;
- результаты предварительной обработки с устройств БМРЗ передаются в ШФК-МТ;
- функциональный контроллер на основе анализа данных определяет аварийную отходящую линию и передает результаты анализа в АСУ верхнего уровня и в локальную сигнализацию на ПС.

В качестве направленной защиты в серийных интеллектуальных устройствах серии БМРЗ применена высокочувствительная защита от ОЗЗ (СНОЗЗ). В ее алгоритме предусмотрено использование следующих величин:

- действующего значения основной гармоники тока нулевой последовательности $3I_0$, используемого для отстройки от небаланса и наводок во вторичной цепи ТТНП;
- действующего значения основной гармоники напряжения нулевой последовательности $3U_0$. Уставка по напряжению $3U_0$ используется для отстройки от небаланса в цепях обмоток ТН;
- угла между векторами основных гармоник $3I_0$ и $3U_0$.

Защита СНОЗЗ является автономной. Для организации централизованной защиты от ОЗЗ были внесены дополнения в существующие алгоритмы устройств БМРЗ: анализируются ток и мощность нулевой последовательности при переходном процессе в начальный момент ОЗЗ и в стационарном режиме, контролируется производная мощности при переходном процессе.

В устройствах были БМРЗ реализованы следующие алгоритмы цифровой обработки сигналов и защиты от ОЗЗ:

- фильтрация высокочастотных составляющих для обеспечения их полного подавления, что позволяет не учитывать броски высокочастотных составляющих;
- вычисление ортогональных составляющих и действующего значения основной гармоники сигналов для подавления высокочастотных составляющих при переходных процессах;
- вычисление действующего среднеквадратического значения сигнала для получения информации о полной мощности сигнала, включая высокочастотные составляющие.

Рис. 1. Функциональная схема алгоритма защиты от ОЗЗ

Элементы защиты

В созданной централизованной защите (рис. 1) выполнен совместный анализ токов $3I_0$ по фидерам и их фаз, а также действия имеющихся в устройствах направленных защит. БМРЗ, установленные на отходящих фидерах подстанции, осуществляют контроль напряжения и токов нулевой последовательности. При возникновении ОЗЗ устройства осуществляют усреднение и накопление величин токов нулевой последовательности с последующей передачей накопленных значений в шкаф функционального контроллера.

Защита от ОЗЗ выполнена с контролем напряжения $3U_0$ и тока $3I_0$. При превышении значений напряжения $3U_0$ заданной уставки $3U_{0нб}$ в программный комплекс WebScadaMT передается дискретный сигнал и начинается обработка и усреднение значений тока $3I_0$. Результаты расчетов, коэффициент трансформации ТТНП k3I0 и дискретные сигналы, формируемые в блоке «Функции обработки и усреднения значений», передаются для дальнейшей обработки функциональным контроллером.

В качестве АРМ могут использоваться компьютеры, находящиеся в одной сети со шкафом ШФК-МТ.

Источниками информации и приемниками команд управления ШФК-МТ являются терминальные узлы:

- интеллектуальные устройства РЗА БМРЗ-150;
- счетчики электроэнергии;
- внешний АРМ при его поставке;
- система диспетчерского управления (АСДУ), при ее подключении к каналу обмена информацией (Ethernet);
- другое оборудование, предоставляющее и принимающее информацию по цифровым, дискретным и аналоговым каналам связи.

В программном комплексе WebScadaMT осуществляется групповой анализ однофазных замыканий на землю. Для выполнения анализа функциональный контроллер получает от устройств БМРЗ многофакторную информацию о процессах, происходивших на контролируемом блоком фидере (усредненные и пиковые значения токов нулевой последовательности, направление мощности нулевой последовательности и ее изменение при переходном процессе, положение коммутационных аппаратов). Анализ данной информации осуществляется специализированным алгоритмом с применением настраиваемых весовых функций и алгоритмов нечеткой логики.

Выводы

Результаты исследований показывают, что возможности комплекса в составе микропроцессорных интеллектуальных устройств БМРЗ и ШФК-МТ с программным комплексом WebScadaMT позволяют обеспечить селективную централизованную защиту от ОЗЗ. Важным преимуществом данного решения является отсутствие необходимости в оснащении дополнительным оборудованием существующих ПС или РУ.

Пуск централизованной защиты от ОЗЗ осуществляется в соответствии с заданными уставками. Централизованная защита от однофазных замыканий на землю при ОЗЗ через переходное сопротивление (дерево) работает правильно и обеспечивает селективное определение фидера с ОЗЗ.

Результаты исследований по экспериментальной оценке возможности селективного определения поврежденного присоединения при ОЗЗ на воздушных линиях сетей 6 (10) кВ ПАО «Татнефть» оцениваются как положительные. Разработка и внедрение централизованной защиты от однофазных замыканий позволила достичь поставленных целей ●

МЕХАНОТРОНИКА
Интеллектуальные устройства релейной защиты

ООО «НТЦ «Механотроника»
г. Санкт-Петербург
тел. 8 800 250-63-60
WWW.MTRELE.RU

Сегодня один из самых актуальных вопросов в энергетики России – внедрение и тестирование «цифровых подстанций», реализованных с применением стандарта МЭК 61850 [1]. Заказчиками рассматриваются различные варианты технических решений, которые, впрочем, сводятся к двум основным вариантам: организации релейной защиты с распределением функций по отдельным терминалам и выполнение комплекса РЗА всего объекта в одном или нескольких централизованных устройствах. В статье рассматривается опыт испытаний комплекса цифровой централизованной защиты (далее – ЦЦЗ) подстанции 110/35/6 кВ [2].

КОМПЛЕКСНОЕ ТЕСТИРОВАНИЕ ЦИФРОВОЙ ПОДСТАНЦИИ С ИСПОЛЬЗОВАНИЕМ СИМУЛЯТОРА RTDS

Техническое решение предусматривает интеграцию в одном устройстве функций релейной защиты и автоматики, измерения, сигнализации и управления коммутационной аппаратурой всей подстанции. Сбор информации о состоянии объекта по стандарту МЭК 61850 позволяет минимизировать количество точек подключения к первичному оборудованию и обеспечивает доступность измерений для всех функций РЗА. Применение централизованного подхода обеспечивает минимизацию горизонтальных связей между устройствами и сокращение коммуникационного оборудования на подстанции по сравнению с децентрализованными решениями. Также необходимо отметить значительный экономический эффект от реализации такого решения: уменьшение количества устройств защиты и медных кабелей, времени на монтаж и ввод в эксплуатацию.

В процессе разработки и внедрения централизованной защиты, возникает необходимость тестирования не только отдельных его компонентов, но и проведения комплексных испытаний в условиях, максимально приближенных к условиям работы защищаемого объекта. Комплексное тестирование позволяет не только проверить правильность работы отдельных функций и измерительных органов устройства, но и убедиться в корректности алгоритмов взаимодействия всей системы защиты и автоматики объекта с использованием GOOSE-сообщений, а также проверить корректность задания уставок и настроек защиты для различных режимов защищаемого объекта.

Основная особенность тестирования ЦЦЗ – моделирование работы большого количества аналоговых и дискретных сигналов, поступающих со всего защищаемого объекта. Применение портативного программно-аппаратного симулятора RTDS позволяет не только имитировать работу энергосистемы, но и выдавать необходимое количество SV-потоков и GOOSE-сообщений с получением полноценной обратной связи от тестируемого устройства. Удобный графический редактор RSCAD позволяет создавать и корректировать модель объекта энергосистемы, ускоряя процесс выявления наиболее сложных режимов для работы устройства.

Испытания цифровой централизованной защиты

Испытания ЦЦЗ с помощью программно-аппаратного комплекса RTDS проводятся на схеме «Цифрового двойника» – ПС 110/35/6 кВ «Пойковская» Тюменской энергосистемы, представленной на рис. 1.

Испытаниям подвергается шкаф ЦЦЗ (рис. 2) производства ООО «Релематика», включающий в себя:

- два терминала ЦЦЗ типа «ТОР 300 ПС 701» (исполнение 3/4) с функциональными кнопками (36шт.) и цветным TFT экраном (800x480);
- два управляемых коммутатора третьего уровня типа MOXA PT-G7828 для приема и передачи цифровых сигналов МЭК 61850;
- сервер точного времени типа Метроном-600.

Программно-аппаратный комплекс RTDS был предоставлен фирмой ЗАО «ЭнЛАБ», являющейся эксклюзивным представителем в России компании RTDS Technologies, Канада. В его состав вошли:

- портативный шкаф симулятора RTDS с установленными в нем двумя процессорными модулями PB5, модулем приема-передачи интерфейса рабочей станции GTWIF, двумя модулями сетевых интерфейсов GTNET и модулем интерфейса панелей ввода-вывода GTFPI;
- модуль универсальный программируемый GTFGA с 16 медными портами Ethernet, обеспечивающий передачу девяти SV-потоков, необходимых для работы двух комплектов централизованной защиты;
- ноутбук с установленным программным обеспечением RSCAD.

Комплексные испытания централизованной защиты предусматривают проведение ряда опытов коротких замыканий (далее – КЗ) в прилегающей сети и в пределах защищаемого объекта (на рис. 1 отмечены точки КЗ, рассматриваемые в рамках данного тестирования):

- металлические КЗ в различных точках;
- трехфазные, междуфазные, однофазные и двухфазные КЗ на землю с различными переходными сопротивлениями;
- одновременные КЗ в двух точках энергосистемы;
- КЗ, переходящие из одного вида в другой в одной точке с любыми моментами и временами перехода;
- КЗ, переходящие из одной точки в другую, в том числе с изменением вида КЗ в любой момент и с любым временем перехода;
- повреждения, моделируемые на фоне отклонений частоты сети, а также на фоне качаний.

В дополнение к различным условиям КЗ проверяются определенные рабочие команды, вызывающие различные переходные процессы, например, пусковые токи намагничивания силовых трансформаторов и т.д.

Во время испытаний учитывается угол включения на КЗ, варьируются значения параметров системы (напряжение и сопротивление) для обеспечения полноценного тестирования комплекса защит в минимальных и максимальных режимах работы сети.

В качестве нагрузки в различных режимах подключается динамическая нагрузка, эквивалентный асинхронный двигатель, синхронный компенсатор, батарея статических конденсаторов. Проводятся испытания работы защиты при различных переключениях в энергосистеме и скачкообразном изменении нагрузки.

Корректность работы отдельных функциональных блоков защиты контролируется с помощью светодиодной индикации и осциллограмм, записанных терминалом РЗА, а также дискретных сигналов, получаемых от устройства РЗА программой RSCAD по протоколу МЭК 61850.

Информация о текущем состоянии подстанции (положение КА, электрические величины) и работоспособности защит дублируется в АСУ ПТК «UniSCADA» (далее – ПТК) производства ООО «Релематика» по стандарту МЭК 61850 (MMS), выполняющая функцию АРМ оперативного персонала. ПТК на основе полученных с устройств РЗА осциллограмм, уставок и конфигурации автоматически формирует протокол анализа действия защит, что позволяет перейти с периодического технического обслуживания на обслуживание по состоянию.

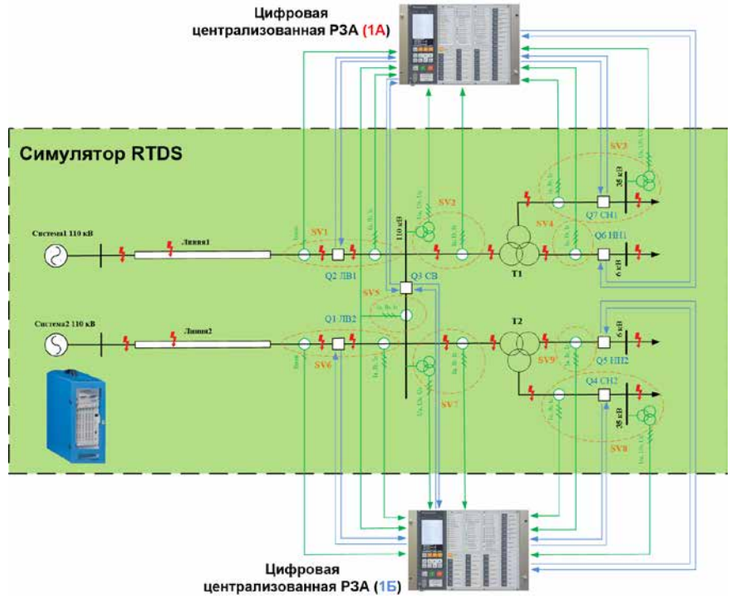


Рис. 1. Схема подключения ЦЦЗ, управление КА, разделение аналоговых сигналов на SV-потоки и основные точки моделируемых коротких замыканий (КЗ)

Процедура испытаний выглядит следующим образом (рис. 3):

1. Создается модель сети в программе RSCAD. Данные по параметрам энергосистемы, линий, трансформаторов и прочее предоставляются заказчиком.
2. Выбирается режим работы сети, место и вид КЗ.
3. RSCAD проводит расчёт режима, в результате чего выдаются значения токов и напряжений в реальном времени.
4. Симулятор RTDS подаёт расчётные величины токов и напряжений в наблюдаемых узлах (в формате SV выборок) на терминалы ЦЦЗ.
5. RSCAD фиксирует реакцию терминалов и встроенных функций защит на данный вид повреждения и корректирует их значения в режиме реального времени для новой конфигурации системы.
6. АСУ ПТК «UniSCADA» собирает и отображает в реальном времени положение КА, электрические величины на однолинейной мнемосхеме под-

Рис. 2. Шкаф цифровой централизованной защиты с подключением симулятора RTDS

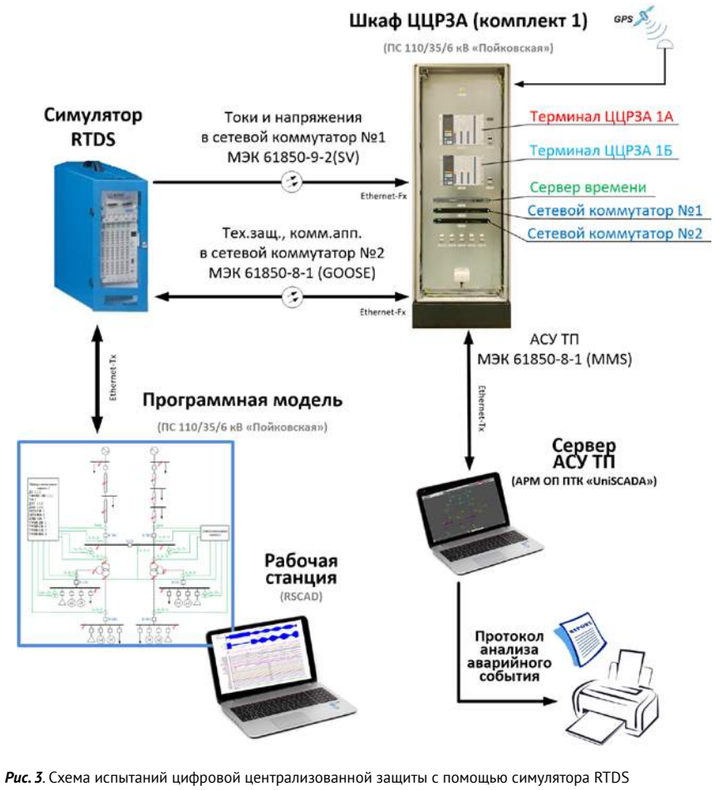


Рис. 3. Схема испытаний цифровой централизованной защиты с помощью симулятора RTDS

станции, а также работоспособность устройств ЦЦЗ. По мимо этого, ПТК удаленно осуществляет управление КА и защитами.

7. На основе полученных осциллограмм, уставок и конфигурации с устройств РЗА в сервере АСУ ПТК «UniSCADA» автоматически формирует протокол анализа аварийного события.

8. Выбирается иной режим работы и вид КЗ, и далее повторяется п.3 и следующие.

Несомненным преимуществом такого вида испытаний является высокая достоверность моделирования режимов работы сети, значительное количество расчетных видов и мест КЗ для оценки работоспособности комплекса защит и получение величин токов и напряжений в наблюдаемых узлах при КЗ в разных точках сети защищаемого объекта.

Разумеется, подобный объем работ затруднительно проводить для каждого энергообъекта во время приемо-сдаточных испытаний (далее - ПСИ) оборудования. При этом на стадии реализации пилотных проектов внедрения цифровых ПС текущий подход оправдан. С другой стороны, имея на руках готовые значения уставок и конфигураций оборудования, подготовленных для реального энергообъекта, возможно значительно сократить пуско-наладочные работы на подстанции при проведении ряд таких испытаний на стадии заводских ПСИ.

По результатам испытаний были скорректированы некоторые уставки и параметры защиты. Во время испытаний зафиксировано, что тестируемая ЦЦЗ подстанции 110/35/6 кВ «Пойковская» обеспечивает чувствительность и селективность работы при всех видах повреждений.

Выводы

1. В ходе испытаний с применением стандарта МЭК 61850-9-2 (SV-потоки) ЦЦЗ показала работоспособность во всех режимах испытаний.

2. Времена действия защит во всех режимах не превысили заданные параметры.

3. Применение для испытаний программно-аппаратного комплекса RTDS значительно улучшило качество проведения испытаний, повысило надежность срабатывания комплекса защит и значительно снизило связанные с испытаниями расходы.

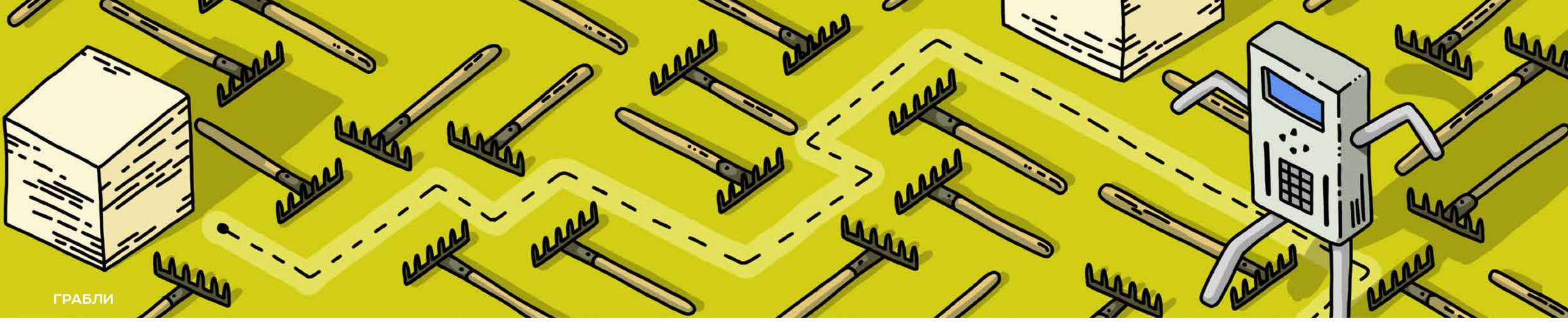
4. Функция автоматического формирования протокола анализа действия защит позволила оперативно решать вопросы в части правильности работы устройств ЦЦЗ.

5. Управление и мониторинг «цифровой подстанции» с помощью АСУ ПТК «UniSCADA» позволило дистанционно собирать всю необходимую информацию с ЦЦЗ, производить их конфигурацию, а также диагностику, в том числе вспомогательного оборудования, в реальном времени.

6. Рекомендуется проведение такого рода испытаний для пилотных проектов внедрения «цифровых ПС» ●

ОБ АВТОРАХ:
Михаил Шамис // К.т.н., генеральный директор ЗАО «EnLAB», г.Чебоксары, Россия.
Янез Законьшек // Технический директор ЗАО «EnLAB», г.Чебоксары, Россия.
Ирина Подшивалина // К.т.н., заведующий сектором моделирования, ООО «Релематика», г.Чебоксары, Россия.
Дмитрий Кержаев // К.т.н., заведующий отделом разработки цифровых подстанций, ООО «Релематика», г.Чебоксары, Россия.
Александр Алексеев // Заместитель директора Департамента стратегического развития, ООО «Релематика», г.Чебоксары, Россия.

ЛИТЕРАТУРА ►**1.** IEC 61850-2. Communication networks and systems in substations – Parts 2: Glossary, technical specification. Edition 1 (Термины и определения) ►**2.** Иванов С.В., Буров А.В. Централизованная релейная защита подстанции 110/35/6 кВ на принципах системной интеграции алгоритмов защит в едином устройстве. «Электроэнергия. Передача и распределение» №5 (44) Сентябрь-Октябрь 2017. ►**3.** Мочалов Д.О., Законьшек Я.В., Шамис М.А. Комплексы моделирования в реальном времени современных энергосистем. «Релейная защита и автоматизация», № 1, 2013.



Исторически сложилось, что системе оперативного тока (СОПТ) уделяется недостаточно внимания. Однако, зачастую аварии на энергообъектах (отключение линии в результате ложной работы РЗА или аварийного снижения сопротивления изоляции) связаны с вопросами, относящимися к СОПТ. Требования к СОПТ, основанные на обеспечение надежности питания, чувствительности и быстродействии, ремонтопригодности, были сформулированы лишь в 2010 году в виде отдельного стандарта организации [1], когда микропроцессорные устройства РЗА уже повсеместно применялась на энергообъектах. В настоящее время мы являемся участниками нового витка развития, именуемого «цифровой трансформацией энергообъктов». Ключевое звено в переходе к «цифровизации» – создание цифровых подстанций (ЦПС). ЦПС в первую очередь воспринимается как объект, в котором все процессы информационного обмена между элементами подстанции и внешними системами, управление работой подстанции осуществляется в цифровом виде на базе стандарта МЭК 61850. Сегодня «цифровизация» затронула, в основном, системы релейной защиты, управления и автоматики, а СОПТ вновь «обошла стороной». Несмотря на введение в 2018 году нового стандарта по проектированию [2], который закрепляет требования СТО от 2010 г. и дополняет его требованиями по структуре питания потребителей, системе контроля изоляции и мониторинга, в нем все равно не в полной мере раскрываются требования к реализации СОПТ для ЦПС.

НОВЫЕ ТРЕБОВАНИЯ К СОПТ ПРИ «ЦИФРОВИЗАЦИИ» ПОДСТАНЦИИ

Аксар Виноградов
ООО НПП «ЭКРА», Чебоксары

Игорь Волков
ООО НПП «ЭКРА», Чебоксары

Константин Быков
ООО НПП «ЭКРА», Чебоксары

В реализуемых ЦПС классическая структура СОПТ не претерпевает значительных изменений, за исключением организации питания новых ответственных потребителей «полевого уровня», таких как преобразователи аналоговых сигналов (ПАС) и дискретных сигналов (ПДС). Питание блоков ПАС и ПДС должны иметь такую же категорию надежности, что и МП РЗА. Появление новых ответственных потребителей возлагает все больше ответственности на контроль целостности этих цепей и предъявляет все более жтсткие требования к оборудованию контроля изоляции [8]. Что касается системы мониторинга, то ее структура остается неизменной: обмен данными выполняется по радиальной схеме от измерительных приборов к системе мониторинга СОПТ. Далее информация передается в АСУ ТП подстанции в виде отчетов по технологии «клиент-сервер» (MMS-отчеты) (рис. 1).

Однако, существует проблема содержания MMS-отчетов.

Цель стандарта МЭК 61850 заключается в обеспечении взаимодействия между «интеллектуальными электронными устройствами» (ИЭУ). Обмен информацией между ИЭУ достигается механизмами, основанными на четко определенных информационных моделях логических устройств и узлов. Отечественная редакция стандарта МЭК 61850 [5] среди типовых логических узлов для СОПТ содержит только один формат логического узла ZBAT, описывающего передачу сигналов от аккумуляторной батареи.

В иностранной редакции стандарта IEC 61850[6] в списке типовых логических узлов для сети постоянного тока имеет еще 2 логических узла: зарядно-выпрямительное устройство – ZSCR, измерительные приборы постоянного тока – MMDC. Если посмотреть на список объектов данных в этих логических узлах, то мы увидим, что обе версии стандарта в настоящее время не содержат полный перечень сигналов, указанный в таблице 4 п.8.6.5 СТО [2]. В результате отечественные производители оборудования СОПТ вынуждены прибегать к использованию общих логических узлов GGIO. Описание функций устройства с помощью общего логического узла стандартом МЭК 61850 не запрещается. Но при этом теряются логические взаимосвязи, приводящие к тому, что, во-первых, проектировщик или наладчик не может идентифицировать назначение сигналов в логическом устройстве, а во-вторых, в будущем невозможно будет заменить СОПТ без полного переконфигурирования системы ПС.

Поэтому целесообразно применять общие логические узлы только для описания функции свободно-программируемой логики, не описываемые стандартными логическими узлами. Необходимо как можно скорее создать национальный профиль стандарта МЭК 61850, содержащий полный перечень логических устройств и узлов, описывающий функции элементов СОПТ в полном объеме.

Реализация описания объектов данных логических узлов – задача сложная, решив которую, откроется новая возможность технологии МЭК 61850 – цифровое взаимодействие между компонентами СОПТ с целью построения адаптивной СОПТ. Например, к простейшим функциям адаптивности, которыми можно наделить систему мониторинга СОПТ – возможность динамического изменения уставок контроля напряжения АБ в различных режимах работы: подзаряд, уравнительный заряд, тест АБ. Логический узел ZBAT уже имеет атрибуты данных уставок повышенного HiBatVal и пониженного уровня LowBatVal. Если бы зарядно-выпрямительные устройства уже имели возможность динамически передавать информацию о своем режиме заряда, то система мониторинга принимала бы данный сигнал, выполняла его логическую обработку в сочетании с сигналами состояния коммутационных аппаратов, идентифицировала текущий режим работы АБ и корректировала бы уставки порогов. В результате отсутствует ложная сигнализация в АСУ ТП о неисправности в ЩПТ.

И это лишь малая часть функциональных возможностей, которые можно реализовать в СОПТ для увеличения удобства эксплуатации и надежности функционирования!

Из всего вышесказанного следует, что при предъявлении требований к СОПТ и ее элементам необходимо исходить не только из требований по выдачи информации в АСУ ТП по протоколу МЭК 61850, но и возможности цифрового взаимодействия компонентов СОПТ между собой с целью управления и построения адаптивной системы с функциями диагностики и прогнозирования состояния оборудования без участия человека.

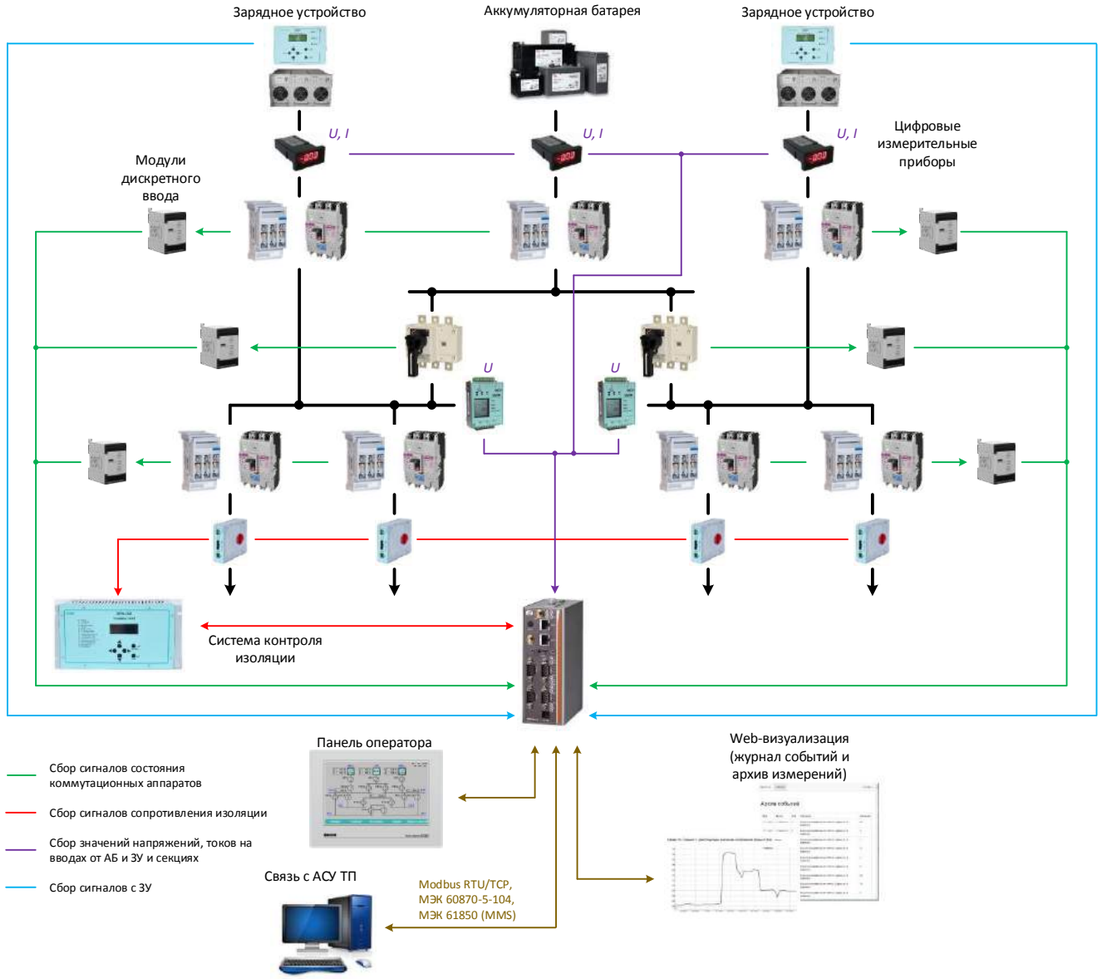


Рис. 1. Структура традиционной системы мониторинга СОПТ

Для полноценной реализации ЦПС необходимо предъявлять к СОПТ следующие дополнительные критерии:

1. Автоматическое изменение конфигурации силовой цепи с возможностью дистанционного переключения, которая предполагает изменение структурной схемы от состояния элементов и режимов работы СОПТ. Например, автоматическое переключение секции ЩПТ, ввода питания ШРОТ или потребителей ШРОТ на «чистый источник» при угрозе потери питания потребителей в результате ухудшения изоляции, ослабления контактного соединения или иных неисправностей.

2. Автоматическое изменение настроек параметров элементов с возможностью дистанционного переключения уставок. В зависимости от режима работы СОПТ должны изменяться уставки технологических параметров (повышенного или пониженного напряжения, тока подзаряда АБ и т.д.) и карты селективности.

3. Прогнозирование состояния компонентов. Наличие расчетно-аналитических методов обработки данных для комплексной оценки состояния оборудования с целью прогнозирования выхода из строя оборудования.

4. Дистанционная диагностика элементов. Возможность удаленного тестирования оборудования и режимов работы системы с помощью испытательного комплекса, стационарно расположенного на ПС, для комплексной оценки состояния с целью планирования обслуживания и ремонта оборудования.

5. Элементы должны иметь взаимозаменяемую модульную структуру с автоматической идентификацией при вводе в эксплуатацию. Вышедшие из строя элементы должны выводиться автоматически из работы с максимальным сохране-

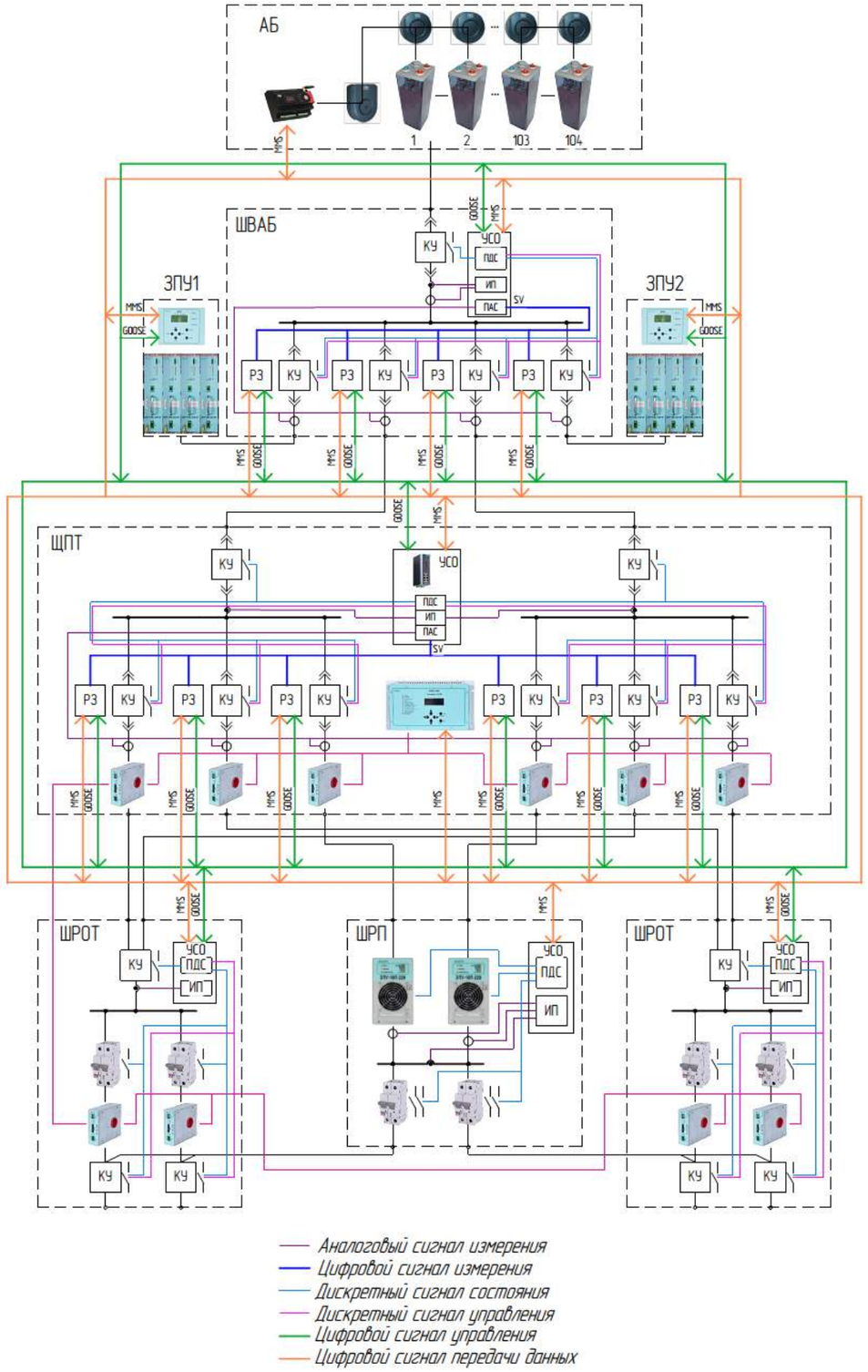


Рис. 2. Структурная схема СОПТ

нием функций системы за счет других элементов (аппаратное резервирование), безопасно демонтироваться. Вновь подключаемые к сети элементы должны беспрепятственно устанавливаться и после прохождения идентификации должны автоматически конфигурироваться системой.

Принимая во внимание вышеуказанные критерия, структурная схема СОПТ может быть представлена следующим образом (рис. 2), где
АБ – аккумуляторная батарея с системой поэлементного контроля;
ЗПУ – зарядно-питающие устройства;
КУ – управляемое коммутационное устройство;
ПАС – преобразователь аналоговых сигналов;
ПДС – преобразователь дискретных сигналов;
РЗ – микропроцессорное реле защиты постоянного тока;
ШРОТ – шкаф распределения оперативного тока;
ШРП – шкаф резервного питания;
ЩПТ – щит постоянного тока;
УСО – устройство сопряжения с объектом.

Для реализации ЦПС существующие стандарты [3, 4] необходимо дополнить следующими техническими требованиями:

1. Аккумуляторная батарея (АБ).

1.1. Должны применяться необслуживаемые, стационарные свинцово-кислотные, герметичные АБ или литий-ионный АБ с проектным сроком службы не менее 20 лет. Допускается использовать стационарные свинцово-кислотные, герметичные АБ в виде моноблоков со сроком эксплуатации не менее 12 лет.

1.2. АБ должна иметь стационарную системой контроля параметров отдельных элементов.

1.3. Система контроля параметров отдельных элементов АБ должна контролировать напряжение, температуру и сопротивления каждого элемента (моноблока), отслеживать режим работы АБ в целом, собирать, хранить и анализировать данные, обеспечивать передачу данным по протоколу МЭК 61850-8-1 MMS.

1.4. Система контроля параметров отдельных элементов АБ обязательно должна поддерживать сервис календарной синхронизации по протоколу SNTP в соответствии с требованиями стандарта МЭК 61850-8-1.

2. Зарядно-подзарядное устройства (ЗПУ).

2.1. Должны применяться ЗПУ модульной конструкции;

2.2. Выходная мощность зарядного устройства должна обеспечивается набором отдельных модулей питания (МП), количество которых определятся максимальным выходным током МП;

2.3. ЗПУ и МП должны иметь естественное охлаждение;

2.4. Должна обеспечиваться параллельная работа двух ЗПУ на стороне выпрямленного напряжения с симметричным делением тока нагрузки;

2.5. При перегреве ЗПУ должны снижать свою выходную мощность без полного останова;

2.6. В ЗПУ должен обеспечивать режим равномерного распределения тока нагрузки между МП;

2.7. Конструкция ЗПУ должна обеспечивать замену МП под нагрузкой;

2.8. ЗПУ должен иметь встроенную интеллектуальную систему управления и мониторинга;

2.9. Система управления и мониторинга должна обеспечивать управление режимами работы ЗПУ в реальном масштабе времени и контролировать внутренние параметры ЗПУ и исправность блоков МП;

2.10. При подключении МП должны автоматически идентифицироваться и конфигурироваться системой управления;

2.11. ЗПУ обязательно должно поддерживать сервис календарной синхронизации по протоколу SNTP в соответствии с требованиями стандарта МЭК 61850-8-1;

2.12. ЗПУ должен передавать данные с использованием протокола МЭК 61850-8-1 GOOSE, MMS.

3. Распределительные устройства постоянного тока (РУПТ) (ЩПТ, ШРОТ).

3.1. В составе первого и второго уровня защиты должны применяться предохранители, устанавливаемые в предохранитель-выключатель-разъединитель (ПВР) или коммутационные устройства (КУ) с дистанционным управлением.

Применение типа коммутационного аппарата определяется от степени автоматизации объекта и наличия постоянного дежурного и обслуживающего персонала: при наличии персонала достаточно применить ПВР, при отсутствии – управляемые КУ.

Совместно с КУ должны применяться интеллектуальные электронные устройства релейной защиты постоянного тока (ИЭУ РЗПТ), позволяющие селективно и с необходимым быстродействием локализовать повреждение.

ИЭУ РЗПТ должны иметь функцию логической селективной защиты.

Совместно с ИЭУ РЗПТ в коммутационных узлах должны быть применены оптические или аналоговые датчика тока совместно с ПАС из состава УСО РУПТ.

ИЭУ РЗПТ должен передавать данные с использованием протокола МЭК 61850-8-1 GOOSE, MMS.

На третьем уровне защиты в цепях питания непосредственных потребителей должны применяться автоматический выключатель постоянного тока и устройство коммутации с возможностью дистанционного управления.

Устройство коммутации предназначено для перевода цепей индивидуальных потребителей на резервную шину питания для поиска фидера с замыканием на землю и изоляции от цепей АБ.

Возможность дистанционного управления устройства коммутации в цепях индивидуальных потребителей определяется от степени автоматизации объекта.

3.2. В состав РУПТ должно входить устройство сопряжения с объектом (УСО).

УСО должна обеспечивать функции мониторинга и прогнозирования состояния оборудования.

УСО должен иметь функции:

- контроль состояния разборных контактных соединений;
- учет механического и электрического ресурса коммутационных аппаратов;
- контроль времени наработки на отказ внутренних элементов электронных устройств;
- контроль деградации плавкой вставки предохранителей при применении в качестве защитных устройств на первом и втором уровне защиты;

В составе УСО могут входить преобразователи дискретных сигналов и аналоговых сигналов – ПАС и ПДС, измерительные преобразователи – ИП.

ПАС формирует SV-потоки для целей РЗПТ (защитные).

ПДС обеспечивает ввод дискретных сигналов от коммутационных аппаратов, формировать GOOSE-сообщения по изменению дискретных сигналов.

ИП обеспечивает измерение параметров текущего режима и передает данные по протоколу МЭК 61850-8-1 MMS.

УСО обязательно должна поддерживать сервис календарной синхронизации по протоколу SNTP в соответствии с требованиями стандарта МЭК 61850-8-1.

УСО должно иметь функцию самодиагностики функционирования.

УСО должна поддерживать тестовый режим функционирования.

Самодиагностика узлов УСО должна обеспечивать обнаружение отказа с точностью до отдельного модуля (блока), входящего в состав УСО. Обнаруженные сбои и отказы функционирования узлов устройства должны фиксироваться в журнале событий устройства, а также отражаться в виде визуально-доступной сигнализации.

УСО должно передавать данные с использованием протокола МЭК 61850-8-1 GOOSE, MMS.

3.3. В состав РУПТ должна входить система контроля изоляции (СКИ)

Для исключения ложной работы ДВ при существующей уставке снижения сопротивления изоляции равной 20 кОм «Авария», необходимо применять выравнивающие резисторы не более 10 кОм.

Должна быть обеспечена возможность настройки датчиков на режим включения и отключения с уставкой аварийного снижения изоляции каждого фидера.

Датчик контроля сопротивления изоляции должен обеспечивать самовосстановление из режима перенасыщения магнитопровода датчика и сохранять работоспособность в случае кратковременных бросковых токов в одном из проводов присоединения или наведении импульсных помех.

На корпусе датчиков контроля сопротивления изоляции должны быть светодиоды, сигнализирующие о снижении сопротивления изоляции присоединения ниже уставки или о неисправности датчика.

Система контроля изоляции должна иметь функцию непрерывного измерения сопротивления полюсов сети полюсов относительно «земли».

СКИ должна поддерживать тестовый режим функционирования.

Обнаруженные сбои и отказы функционирования узлов устройства должны фиксироваться в журнале событий устройства с архивированием, а также отражаться в виде визуально-доступной сигнализации с возможностью квитирования неисправности.

СКИ обязательно должна поддерживать сервис календарной синхронизации по протоколу SNTP в соответствии с требованиями стандарта МЭК 61850-8-1.

СКИ должна иметь функцию самодиагностики функционирования.

СКИ должно передавать данные с использованием протокола МЭК 61850-8-1 MMS.

3.4. Конструкция РУПТ должна иметь модульную структуру, обеспечивающая безопасное и быстрое обслуживание ●

ОБ АВТОРАХ:

Аксар Виноградов // Руководитель направления систем оперативного постоянного тока департамента НКУ и КРУ НПП «ЭКРА». ► Окончил в 2006 г. электротехнический факультет ЧГУ им И.Н. Ульянова.

Игорь Волков // Руководитель группы автоматизации и мониторинга департамента НКУ и КРУ НПП «ЭКРА». ► Окончил в 2007 г. электротехнический факультет ЧГУ им И.Н. Ульянова.

Константин Быков // Заместитель директора департамента НКУ и КРУ НПП «ЭКРА». ► Окончил в 1999 г. электротехнический факультет ЧГУ им И.Н. Ульянова.

ЛИТЕРАТУРА ►**1.** Стандарт организации ПАО «ФСК ЕЭС» СТО 56947007-29.120.40.041-2010 «Системы оперативного постоянного тока подстанций. Технические требования». ►**2.** Стандарт организации ПАО «ФСК ЕЭС» СТО 56947007-29.120.40.262-2018 Руководство по проектированию систем оперативного постоянного тока (СОПТ) ПС ЕНЭС. Стандарт организации, 2018. ►**3.** Стандарт организации ПАО «ФСК ЕЭС» СТО 56947007-29.240.10.256-2018 Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС. ►**4.** Стандарт организации ПАО «РОССЕТИ» СТО 34.01-21-004-2019 Цифровой питающий цент. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35кВ. ►**5.** ГОСТ Р МЭК 61850-7-4-2011 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 4. Совместимые классы логических узлов и классы данных. ►**6.** 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. ►**7.** Возможна ли цифровая подстанция? – стандарт МЭК 61850 вселяет надежду [Электронный ресурс] – Режим доступа: https://www.compel.ru/lib/96422 – дата обращения: 9.10.19. ►**8.** 8. Галкин И.А, Лопатин А.А., Виноградов А.Ю. «К вопросу о требованиях к оборудованию контроля сопротивления изоляции СОПТ, снижающие ложную работу устройства релейной защиты и автоматики». Журнал «Релейная защита и автоматизация», № 1, 2019.

Организаторы

АО «СО ЕЭС»

РусГидро

cigre Россия

РОССЕТИ ФСК ЕЭС

Электрификация

При поддержке

МИНИСТЕРСТВО ЭНЕРГЕТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

cigré B5

Научно-технический партнер

ВНИИР

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

Релейная защита и автоматика энергосистем-2020

26 - 28 мая 2020
Москва
Центр Международной Торговли (ЦМТ)

www.rza-expo.ru

Программно-технический комплекс «АСУ-МТ»

Комплекс предназначен для построения систем контроля и управления объектами электроэнергетики, систем сбора и передачи оперативной информации подстанций, автоматизированных систем управления технологическими процессами подстанций с высшим уровнем напряжения 6-220 кВ, автоматизированных систем диспетчерского управления. Комплекс «АСУ-МТ» включает:

ШФК-МТ - шкаф функционального контроллера

Назначение: сбор, управление, обработка и передача данных на верхний уровень. Принимает до 288 ТС и выдает до 160 ТУ.

ШАСУ-МТ - шкаф автоматизированной системы управления

Назначение: сбор, управление, обработка и передача данных на верхний уровень. Без приема и передачи ТС и ТУ.

ШКП-МТ- шкаф контролируемого пункта

Назначение: расширение возможностей системы по сбору дискретной и цифровой информации.

Программный комплекс WebScadaMT

- Встроенный конвертер протоколов
- Формирование отчетов
- Прикладные алгоритмы АСУЭ

К шкафу ШФК-МТ можно подключить несколько ШКП-МТ

Возможность импорта SCL-файлов (SSD, BCC и/или CID)

Сопряжение с системами автоматизированного контроля и учета электроэнергии (АИИС КУЭ)

ООО «НТЦ «Механотроника» более 29 лет разрабатывает и производит интеллектуальные устройства релейной защиты и автоматики. Развиваясь и совершенствуясь, предприятие наращивает выпуск существующих устройств и решений и создает новые, превосходящие по своим параметрам продукцию мирового уровня.

МЕХАНОТРОНИКА®
Интеллектуальные устройства релейной защиты

198206, Санкт-Петербург, ул. Пионерстроя, д. 23, лит. А
Единый телефон тех. поддержки: **8 (800) 250-63-60**
www.mtrele.ru