ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИЙ В ЭЛЕКТРОЭНЕРГЕТИКЕ (ПО ИТОГАМ 47-Й СЕССИИ СИГРЭ)

АВТОРЫ:

О.В. СИНЕНКО,
Д.Т.Н.,
АО «РТСофт»

А.Р. ВЕРИГО,
К.Т.Н.,
АО «РТСофт»

С.А. НЕСТЕРОВ,
АО «РТСофт»

С 26 по 31 августа 2018 г. в Парижском дворце конгрессов прошла 47-я Сессия СИГРЭ. 23 доклада, представленных по тематике Исследовательского комитета D2 «Информационные системы и телекоммуникации», позволяют достаточно полно проанализировать современное состояние данной области в электроэнергетике.

Ключевые слова: информационные системы и телекоммуникации; архитектура; дистанционный мониторинг; управление рисками; кибербезопасность; интернет вещей; большие данные; системы сбора и передачи данных; виртуализация; гибридные сети связи; MPLS-TP; TDM; SDH; интеграция технологий; управление жизненным циклом; автоматический анализ аварийных событий.

ВВЕДЕНИЕ

Деятельность Исследовательского комитета (ИК) D2 «Информационные системы и телекоммуникации» направлена на содействие прогрессу, инновационному развитию, а также международному обмену информацией и знаниями в области информационных систем и телекоммуникаций в энергетике.

В сферу интересов ИК входят следующие вопросы:

- Применение информационно-коммуникационных технологий в цифровых сетях, от сетей ультравысокого напряжения до распределительных сетей (электронные приборы учета, интернет вещей, большие данные, система энергетического менеджмента).
- Коммуникационные решения для обмена информацией при поставке электрической энергии.
- Эксплуатационная совместимость и обмен данными между сетевыми операторами, участниками рынка, внесетевыми объектами.
- Обеспечение кибербезопасности, от полевого оборудования до корпоративных информационных систем (ограничение систем управления, проектирование систем, внедрение, тестирование, эксплуатация и техническое обслуживание).
- Технологии и архитектурные решения, направленные на обеспечение непрерывности бизнес-процессов послеаварийного восстановления работоспособности.
- Информационные системы для поддержания процессов принятия решений при управлении основными активами.

Международный ИК D2 СИГРЭ в настоящее время представляют 240 экспертов из 41 страны, принимающих активное участие в работе основных структурных органов ИК — трех консультационных групп, пяти рабочих групп и четырех совместных рабочих групп с ИК B2, B5, C2, C6.

С 26 по 31 августа 2018 г. в Парижском дворце конгрессов прошла 47-я Сессия СИГРЭ — глобального сообщества экспертов по электроэнергетическим системам. В этом году мероприятие привлекло более 8500 специалистов-энергетиков из разных стран мира, включая 3800 делегатов из числа научных работников, ученых, инженеров, технических специалистов, генеральных директоров.

Представители Национального ИК D2 РНК СИГРЭ, созданного на базе АО «РТСофт», приняли активное участие в насыщенной программе 47-й Сессии CIGRE и внесли свой вклад в работу профильных мероприятий ИК D2.

Важным событием для Исследовательского комитета D2 стала официальная передача полномочий от прежнего председателя Международного ИК D2 Филиппа Куэнадона (Philippe Quenaudon) новому председателю, избранному 14 мая Административным советом СИГРЭ. Им стала руководитель Национального ИК D2 РНК СИГРЭ, генеральный директор АО «РТСофт» Ольга Викторовна Синенко.

28 августа на очередном заседании Международного ИК D2 регулярные и наблюдательные члены национальных комитетов, входящих в состав ИК D2, подвели итоги своей работы внутри каждой конкретной страны-участницы комитета. Руководителями и членами рабочих групп и совместных рабочих групп по направлениям деятельности ИК были предоставлены отчеты по состоянию работ в каждой из них. Важнейшим пунктом повестки дня заседания стал выбор предпочтительных тем для следующей, 48-й Сессии CIGRE, которая состоится в Париже в 2020 г. В ходе заседания в состав ИК D2 в качестве регулярного члена и представителя от Российской Федерации был включен технический директор по электроэнергетике АО «РТСофт» Алексей Анатольевич Небера.

По линии ИК D2 на Сессии было представлено 23 доклада по следующим предпочтительным темам:

1. ПТ1: Возможности и вызовы, связанные с использованием информационно-коммуникационных технологий применительно к микросетям и распределенным источникам энергии:
   - Коммуникационные решения, предназначенные для дистанционного мониторинга и эксплуатации оборудования автономных сетей.
   - Средства для осуществления контроля, мониторинга, обеспечения физической защиты и безопасности.
   - Вопросы стандартизации, обеспечения эксплуатационной совместимости и кибербезопасности.
2. ПТ2: Возможные варианты применения и внедрения виртуальной среды для сетей и инфраструктуры:
   - Возможности и преимущества, связанные с использованием программно-определяемых сетей и виртуализацией сетевых функций (SDN/NFV).
   - Проблемы, идентифицированные в ходе внедрения и использования структур виртуализации.
   - Стратегии, необходимые для безопасного развертывания SDN/NFV.
3. ПТ3: Обеспечение надежной и безопасной эксплуатации в условиях эволюционирующей среды:

ТОПОЛОГИЯ СЕТЕВОЙ АРХИТЕКТУРЫ LORA

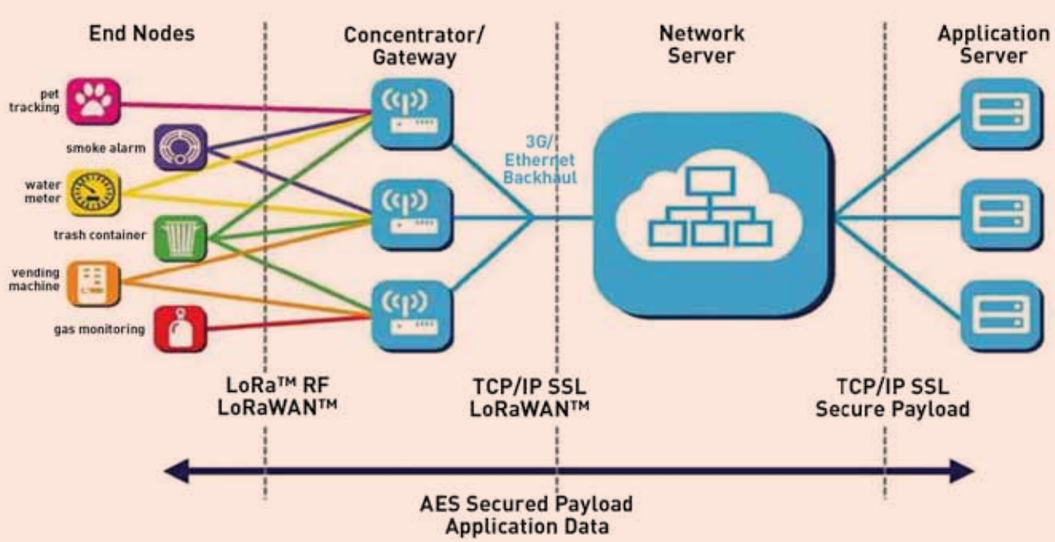

Рис. D2-101-1

– Применение информационно-коммуникационных технологий для поддержки управления и технического обслуживания основных активов.
– Управление жизненным циклом и интеграция традиционного и нового оборудования.
– Ситуационная осведомленность, управление рисками и реакция на инциденты в сфере кибербезопасности.

Ниже приведен обзор наиболее интересных докладов.

Доклад D2-101 (Греция): Evaluation of a LoRaWAN Network for AMR (Анализ эффективности применения сети LoRaWAN для систем учета электроэнергии). N. HATZIARGYRIOU, I. VLACHOS, G. KIOKES, National Technical University of Athens, Hellenic Electricity Distribution Network Operator S.A., Hellenic Air-Force Academy

АРХИТЕКТУРА СЕРВЕРА LORAWAN

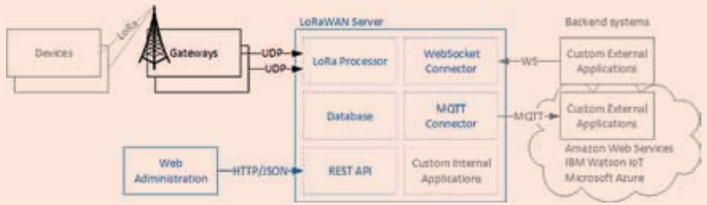

Рис. D2-101-2

В докладе D2-101 проведена оценка использования сети передачи данных LoRaWAN для внедрения системы AMR (Automatic meter reading — технология автоматического сбора и передачи данных о потреблении, диагностике и состоянии от приборов учета энергии). Оценка охватывает как аспекты радиопокрытия системы AMR, так и проблемы энергопотребления приемопередатчиков с батарейным питанием, подключаемых к счетчикам энергии.

В докладе приведено описание параметров частной сети LoRaWAN, расположенной в Мельтеми (Греция), которая использовалась для оценки этой беспроводной технологии большого радиуса действия малой мощности в составе усовершенствованной системы AMR.

СТРУКТУРА ГЛОБАЛЬНОЙ БАЗЫ ДАННЫХ ДЛЯ ОПЕРИРОВАНИЯ 4E

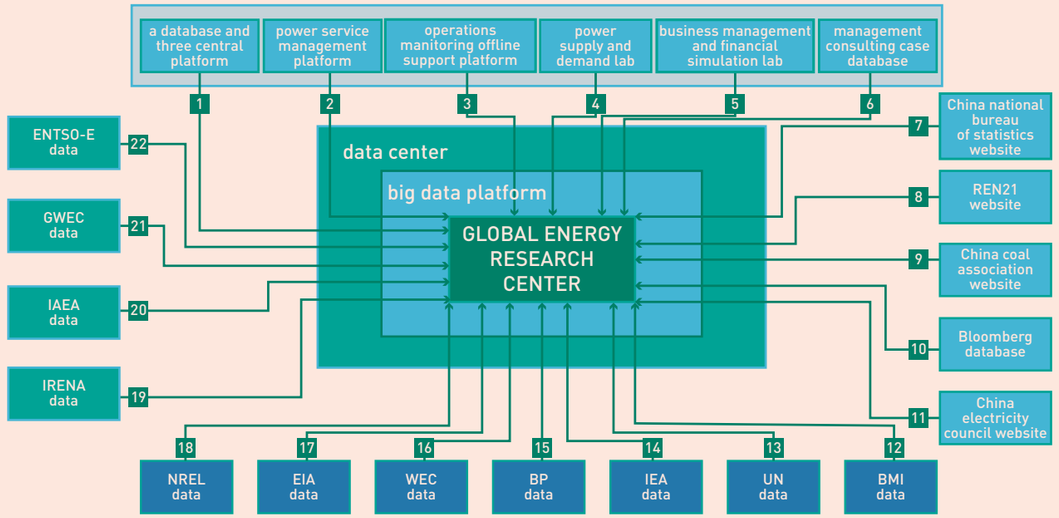

Рис. D2-102-1

Рассмотрены различные системы передачи данных, основанные на технологиях с низким потреблением: Bluetooth, ZigBee, Z-Wave, Sigfox, Neul, LoRa, 6LowPAN, Thread, NFC.

В ходе исследования было изучено покрытие радиосвязью и потребление энергии. Согласно результатам экспериментальных испытаний, было подтверждено, что первоначальный срок службы аккумуляторной батареи может составлять свыше 15 лет при передаче двух сообщений в день от прибора учета по сети LoRaWAN.

Доклад D2-102 (Китай): Study on the construction of global energy research system based on economic-energy-electricity-environment integration analysis (Изучение построения глобальной системы энергетических исследований на основе анализа интеграции экономики, энергетики, электричества и окружающей среды). W. KONG, G. LU, L. ZHAO, N. ZHANG, Y. ZHAO, X. CHEN State Grid Energy Research Institute

Работа D2-102 посвящена вопросам сбора разнородных данных и анализа большого количества данных. В докладе рекомендуется применение нового метода для создания глобальной исследовательской платформы в сфере электроэнергетики, в состав которой входит система сбора информационных данных 4E (economic, energy, electricity and environment — энергия, электроэнергия, экономика, окружающая среда), содержащая свыше 5000 индикаторов данных, способная проводить анализ интегрированных стратегий. В докладе описаны два конкретных случая использования предлагаемой платформы для анализа технологии электрохимического хранения энергии и отображения географической информации.

Для обеспечения сохранности, надежности, достоверности и целостности базы данных предложен метод очистки исходных данных для БД 4E.

Предлагаемая платформа позволяет удовлетворить потребности правительственных органов и глобальных организаций, направленные на своевременный и точный сбор данных касательно изменений объективных обстоятельств с целью анализа нормативных требований и разработки программ развития электроэнергетики. Платформа позволяет оценить потенциал использования источников разнородных данных при создании мощной системы выработки решений, которая может содействовать в разработке поэтапного плана выработки глобальных экономических стратегий для обеспечения рационального потребления энергоресурсов.

БЛОК-СХЕМА СОРТИРОВКИ, ВЫБОРА, СОПОСТАВЛЕНИЯ И ВОССТАНОВЛЕНИЯ ДАННЫХ ИЗ НЕСКОЛЬКИХ ИСТОЧНИКОВ

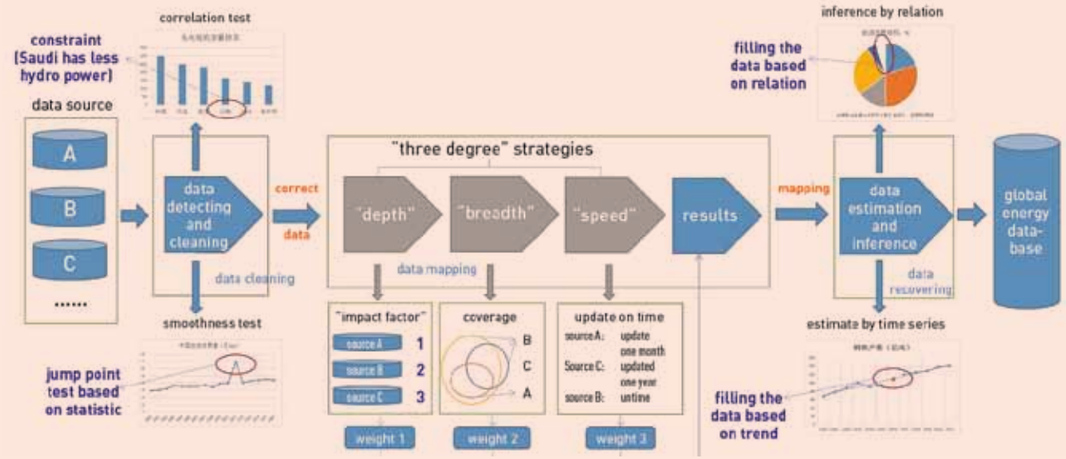

Рис. D2-102-2

Доклад D2-201 (Австралия) Substation Virtualisation: An Architecture for Information Technology and Operational Technology Convergence for Resilience, Security and Efficiency (Подстанционная виртуализация: архитектура информационных технологий и оперативных технологий для обеспечения устойчивости, безопасности и эффективности). V. TAN, PSC Consulting

В докладе D2-201 приведено описание преимуществ имплементации технологии виртуализации на подстанциях. В настоящее время для множества информационных (IT) и операционных технологий (OT) требуется обработка в граничной области вследствие таких причин, как задержка в сети, большой объем собранных данных (большие данные) и географическое разнообразие мест сбора данных (интернет вещей). В этой работе представлена архитектура подстанции, в которой

АРХИТЕКТУРА ИНФРАСТРУКТУРЫ ПОДСТАНЦИИ С ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ COTS, КОТОРОЕ СОЗДАЕТ ВИРТУАЛЬНУЮ СЕТЬ И ПРИЛОЖЕНИЯ

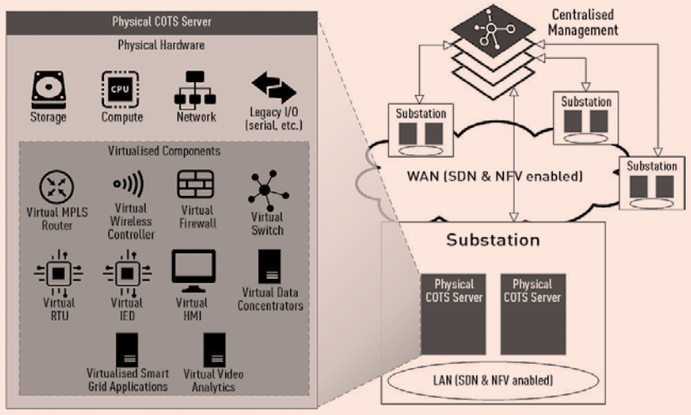

Рис. D2-201-1

все приложения и сети виртуализированы с использованием общего набора оборудования и систем управления. Это позволяет упростить имплементацию и управление приложениями, которые расположены в географически разнесенных местах в составе электроэнергетической системы.

Виртуализация дает возможность для конвергенции сервисов IT и OT на подстанциях в сети Smart Grid. Виртуализация серверов и сетей обеспечивается виртуальной машиной по технологии программно-определяемой сети (SDN) и позволяет использовать несколько аппаратных компонентов, консолидируемых в более эффективную платформу. Преимущества этой консолидации включают повышение операционной эффективности в управлении сервисами, снижение затрат на развертывание меньшего количества оборудования и повышение безопасности благодаря специализированному набору инструментов, а также снижение затрат в течение жизненного цикла при замене оборудования и платформы.

Интеллектуальная подстанция представляется как распределенная станция обработки данных. Ценность Smart Grid в значительной степени зависит от способности энергокомпаний эффективно обрабатывать распределенные источники данных. Из-за большого объема и распределенного характера данных, генерируемых в Smart Grid, они должны быть организованы и обработаны иерархическим и распределенным образом.

ВНЕДРЕНИЕ ВИРТУАЛИЗАЦИИ В СУЩЕСТВУЮЩУЮ ТЕЛЕКОММУНИКАЦИОННУЮ СРЕДУ НА ПОДСТАНЦИИ БЕЗ ИСПОЛЬЗОВАНИЯ ETHERNET

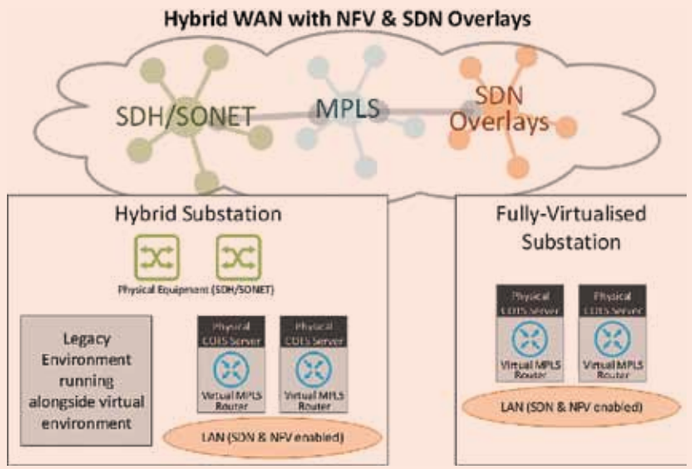

Рис. D2-201-2

Такой подход снижает нагрузку на обработку и обмен данными в центрах обработки данных энергокомпаний и хорошо согласовывает алгоритмы распределенной обработки больших данных с применением искусственного интеллекта (AI). В предлагаемом подходе распределенной обработки данных они организованы в соответствии со следующими иерархиями:

- Данные из распределительной сети (интеллектуальный учет, EV, датчики распределительной сети) агрегируются на распределительных ПС.
- Данные из передающей сети (датчики контроля состояния, PMU, эксплуатационная диагностика) объединяются на передающих ПС.

На рис. D2-201-1 показана архитектура инфраструктуры интеллектуальной подстанции для виртуализации сети и приложений при использовании имеющегося оборудования (COTS).

На рис. D2-201-2 представлен подход к интеграции существующей телекоммуникационной среды на подстанции, где применены устаревшие компоненты без использования Ethernet. На такой ПС существующие функции и технологии остаются неизменными, а виртуализация внедряется наряду с существующей инфраструктурой: сеть синхронной связи (SDH/SONET/PDH) остается неизменной — это позволяет энергокомпании использовать преимущества интеллектуальной виртуальной подстанции без ущерба для существующих операционных функций.

Доклад D2-202 (Япония): Benefit and Resolution of operational issues for information and communication systems using virtualization techniques in the electric power industry (Преимущество и ре-

КОНЦЕПЦИЯ SDN'S VTN

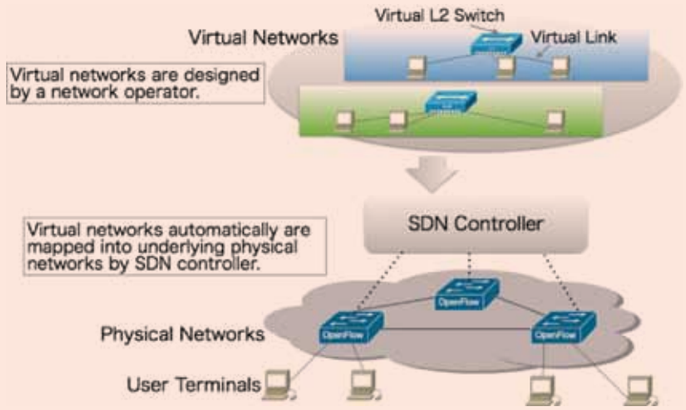

Рис. D2-202-1

ОБРАБОТКА ДОСТУПА В PVLD

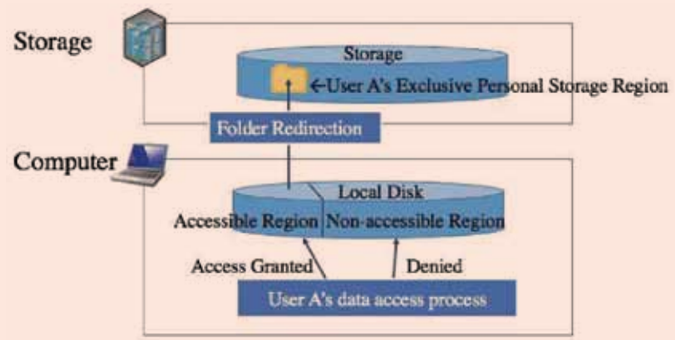

Рис. D2-202-2

шение проблем эксплуатации информационных и коммуникационных систем в электроэнергетике с использованием методов виртуализации). H. DOI, D. KARIU, K. SAKAMOTO, M. SUSUKITA, T. SHIMA, H. NAGASAKI, Central Research Institute of Electric Power Industry, Kyushu Electric Power Co., Inc., Electric Power Development Co., Inc., Kansai Electric Power Co., Inc., Humming Heads. Inc., JP Business Service Corporation

В докладе D2-202 описывается опыт электроэнергетической системы в использовании программно-определяемых сетей (SDN) и развертывании новой инфраструктуры виртуальных рабочих мест (VDI), а также улучшении систем дискового хранения с использованием метода частичной виртуализации локального диска (PVLD), разработанных на основе концепции виртуализации (рис. D2-202-1). Что касается применения SDN, то существующие процессы развертывания сети могут быть усложнены и включать необходимость координации множества задач. Электроэнергетические компании используют SDN для уменьшения времени имплементации изменений или развертывания новых сетей посредством внесения автоматических изменений в сеть. Эти компании оптимизировали методы для повышения управляемости, безопасности и снижения расходов при эксплуатации настольных систем, основанных на тонком клиенте.

На примере компаний Kyushu Electric и J-Power продемонстрирована подготовка к внедрению виртуализации тонких клиентов с использованием технологии Virtual Desktop Infrastructure VDI для повышения эффективности работы приложений и безопасности устройств, причем на первом шаге использована только виртуализация локальных дисков корпоративных рабочих станций и виртуализация систем просмотра интернета.

Механизмы частично виртуализированного локального диска (Partially virtualized local disk, PVLD), доступ к компьютеру и эксклюзивный регион личного хранилища проиллюстрированы на рис. D2-202-2.

Доклад D2-301 (Бразилия): Building a Secure Network Policies, Architecture and Incident Responses. CASE CHESF (Разработка стратегий обеспечения безопасности сетей, архитектура и реагирование на инциденты: CHESF). Rodrigo Leal, Pablo Mascarenhas, CHESF

ЛОКАЛЬНАЯ СЕТЬ ПОДСТАНЦИИ

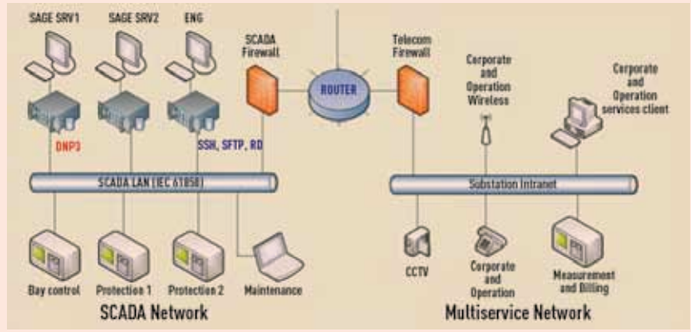

Рис. D2-301

В докладе рассматривается задача построения комплексной системы защиты информации IT- и OT-активов компании Chesf.

Chesf — дочерняя компания бразильской электроэнергетической компании Eletrobras, крупнейший производитель электроэнергии в Бразилии, владелец более 130 энергообъектов, включая 12 гидроэлектростанций и одну биогазовую теплоэлектростанцию, занимающаяся производством, распределением и продажей электроэнергии на северо-востоке страны. В связи с обширной географической и информационной распределенностью, внедрением беспроводных технологий, большими объемами передаваемой информации, в т. ч. выходящей за рамки технологических данных, перед компанией во весь рост встали проблемы обеспечения информационной безопасности (включая физические и поведенческие аспекты) в оперативной и корпоративной среде.

На уровне доступа располагаются генерирующие компании, подстанции, сооружения и телекоммуникационное оборудование. На этом уровне для построения сети применяется Gigabit/Fast Ethernet, топология сети — «кольцо». На подстанциях (рис. D2-301) для коммуникации между IED используется IEC 61850 (GOOSE), между IED и HMI — MMS. В перспективе для защиты IEC 61850 будет применяться IEC 62351. В качестве SCADA используется SAGE — собственная разработка исследовательского центра Eletrobras на базе Linux CentOS. Удаленное управление реализуется только по протоколу DNP3 over IP, удаленное сервисное обслуживание — только внутри корпоративной сети с определенных инженерных станций с предустановленным набором сервисного ПО по SSH/RDP. Все сети горизонтально и вертикально сегментированы и защищены с помощью сетевых экранов. Для каждой группы устройств создается свой VLAN, все неиспользуемые порты на коммутаторах отключаются. Также на всех устройствах все неиспользуемые сетевые порты и небезопасные сервисы (ftp, telnet и т. п.) закрыты и отключены. Планируется модернизация системы идентификации и аутентификации для объединения функций контроля доступа к IP-сети со стороны IT-команды как для IT-, так и для OT-оборудования.

На уровне распределения располагаются 6 региональных офисов, в каждом из которых установлены 2 коммутатора для организации сети с топологией двойного кольца с нижним уровнем доступа и балансировкой нагрузки. На этом уровне применяется технология MPLS.

На уровне агрегации — распределенные сервисы управления и администрирования. Для каждого сервиса используется выделенная географически распределенная виртуальная сеть, применяется технология Carrier Ethernet.

Для защиты корпоративной сети Chesf в настоящее время используются сетевые экраны, аутентифи-

РАБОЧИЕ ГРУППЫ ИССЛЕДОВАТЕЛЬСКОГО КОМИТЕТА (ИК) D2

РГ1 «Информационно-управляющие системы в электроэнергетике»

РГ2 «Совершенствование сетей связи и телекоммуникации для приложений в электроэнергетике»

РГ3 «Развитие сетей Smart Grid и Microgrids, технологии Smart Meters & Meter Data Management»

РГ4 «Обеспечение информационной безопасности (ИБ) для систем и управления в электроэнергетике»

РГ5 «Эксплуатация информационных телекоммуникационных систем и сервисов»

РГ-6 «Информационно-аналитические системы в задачах управления жизненным циклом электросетевого оборудования»

РЕАЛИЗОВАННАЯ ЧАСТНАЯ СЕТЬ VERIZON PIP

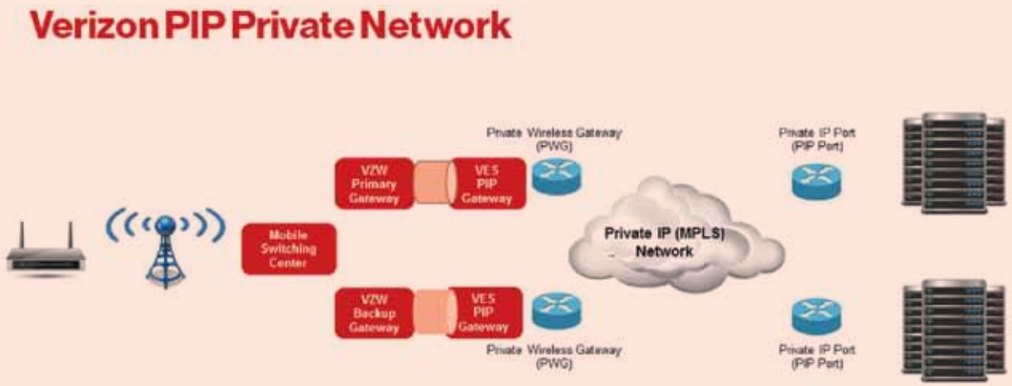

Рис. D2-302

кация пользователей с помощью AD и протоколов Kerberos, RADIUS для проводных/беспроводных устройств.

Планируется введение дополнительной защиты на всех устройствах в сети, что позволит решить следующие задачи:

- полная защита локальных сетей региональных офисов и сервисов;
- построение DMZ;
- контроль доступа всех подключающихся к сети устройств;
- предотвращение атак на IP-сеть в реальном времени с выявлением подозрительного трафика;
- централизованное управление политиками безопасности для распределенных ресурсов сети;
- создание отчетов и представлений для событий безопасности со встроенными возможностями выявления корреляций между событиями и проведение аудитов.

Также планируется создать группу реагирования на инциденты компьютерной безопасности (CSIRT) из специалистов компании по автоматизации, телекоммуникациям, эксплуатации и ИТ. Эта группа будет отвечать за весь необходимый спектр работ по защите.

Доклад D2-302 (США): A Hybrid Communications Network Approach for Advanced Applications on the Modern Grid (Подход к созданию гибридной сети связи для прогрессивных приложений в современной сети). J. P. KNAUSS, National Grid

В докладе описываются способы модернизации электрической инфраструктуры Северной Америки, использование надежных и гибких способов обмена данными и обеспечения безопасного взаимодействия сетей, что является фундаментальным требованием эффективной эксплуатации и управления основными активами сети с целью удовлетворения растущих требований потребителей. Внедряемые современные инновационные решения помогают обеспечить операционную гибкость, устойчивость и масштабируемость. Новый подход к созданию сети с низким временем ожидания, высокой пропускной способностью и готовностью позволил достичь требуемого уровня функциональности, обеспечивающего значительные функциональные усовершенствования для поддержки существующих и перспективных прикладных потребностей современной сети.

Описаны связанные с прогрессом проблемы перехода от устаревающих технологий к новым решениям (аналоговые модемы 2G — 3G) и связанные с этим риски. Как одно из решений применены технологии Private IP (PIP), которые использовались для создания новой сети с безопасным подключением и сквозной интеграцией с бэк-офисными системами. Это решение виртуальной частной сети MPLS уровня 3 обеспечивает безопасное подключение к нескольким концентраторам в разных расположениях, выполняя требования по избыточности системы и возможности переключения при отказе (см. рис. D2-302).

Благодаря тщательному планированию и проектированию была разработана сетевая архитектура, которая позволяла интегрировать данные с полевых устройств в первичные бэк-офисные системы (например, концентраторы данных, SCADA, портал управления и т. п.). Решения виртуальной маршрутизации и пересылки (VRF) были определены для установления желаемого подключения ко всем необходимым средствам, включая как первичные, так и резервные центры управления системой, а также центры обработки данных.

Доклад D2-307 (Тайланд): Challenges in EGAT telecommunication system integration (Проблемы в интеграции телекоммуникационной системы EGAT). P. CHIEWCHARAT, C. PONGMALA, W. YUTTACHAI, Electricity Generating Authority of Thailand (EGAT)

В докладе описан опыт компании EGAT, внедрившей технологию многопротокольной коммутации по меткам — профиль передачи (MPLS-TP), которая может работать с применением технологии TDM и пакетной технологии в существующей сети компании, в целом базирующейся на технологии синхронной цифровой иерархии (SDH). Технология SDH не способна эффективно работать с приложениями, которые разработаны на базе пакетной технологии, что обуславливает необходимость увеличения пропускной способности при передаче данных, как, например, от камер наблюдения или при оказании мультисервисных услуг. К тому же SDH, которая считается одной из самых надежных технологий для энергетических компаний, может скоро исчезнуть из-за прекращения производства соответствующих электронных компонентов. Некоторые службы электроэнергетической компании, осуществляющие управление и защиту, все еще передают свои данные по существующей сети, так как это может гарантировать время передачи и задержки. Кроме того, компанией EGAT была предложена концепция управления в течение всего срока службы для коммуникационного оборудования, а также программа TeleHealth, которая позволяет выполнить оценку индекса технического состояния для информирования о состоянии каждого узла в сети и предоставления рекомендаций касательно плана закупок.

Интеграция в устаревшую систему телекоммуникации технологии MPLS-TP предлагается по двум стратегиям, показанным на рисунке D2-307. Первая — замена существующего SDH оборудованием с расширенной пропускной способностью для поддержки. Для EGAT предполагаемая скорость передачи данных для каждого канала передачи IP-пакетов составляет приблизительно 1 Гбит/с.

По второй стратегии 52 узла оборудования MPLS-TP будут приобретены, установлены и начнут эксплуатироваться отдельно от существующей системы SDH.

Приводится оценка затрат на внедрение сети MPLS-TP, которая примерно на 30 процентов больше затрат на развертывание SDH повышенной емкости. Также интересными являются выводы авторов об энергопотреблении и операционных расходах на эксплуатацию одного телекоммуникационного узла в технологии SDH и MPLS-TP, которые отличаются почти в 2,8 раза.

ДВЕ СТРАТЕГИИ ДЛЯ ТЕЛЕКОММУНИКАЦИОННОГО ПРОЕКТА В СЕВЕРО-ВОСТОЧНОЙ ЧАСТИ ТАИЛАНДА

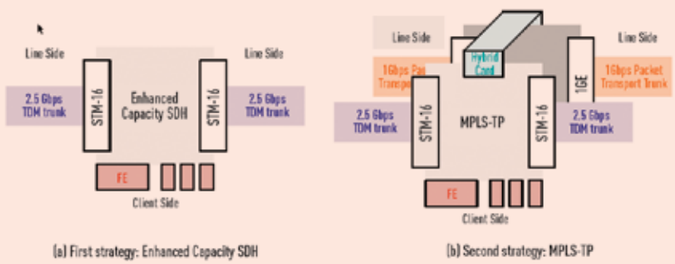

Рис. D2-307

Доклад D2-309 (Южная Африка): Network and Data Cybersecurity Strategy of the Electrical Power System (Стратегия обеспечения кибербезопасности сети и данных в электроэнергетической системе). Matthew Taljaard, Eskom Holdings SOC Ltd.

В докладе из Южной Африки обсуждается стратегия взаимодействия оборудования операционных технологий (OT, Operational Technology) и информационных технологий (IT, Information Technology) с фокусом на обеспечение кибербезопасности для электроэнергетических компаний, так как в Южной Африке в настоящее время осуществляется переход от изолированных сетей к объединенным энергосистемам. Применение средств обеспечения взаимодействия сетей сторонних производителей предоставляет широкие возможности, однако в значительной степени повышает риски в сфере кибербезопасности для существующих систем, использующих операционные технологии.

Обсуждается концепция безопасной зоны, которая фокусируется на за-

щите данных, от источника передачи до адресата, защита от угроз в области кибербезопасности и обеспечение взаимодействия с другими сетями. Также рассматривается концепция создания всеобъемлющего интегрированного центра обеспечения безопасности и возможности коммерческого использования излишней пропускной способности без возникновения угроз в сфере кибербезопасности при ведении бизнеса в электроэнергетической системе.

Отмечается различный подход к приоритизации задач для OT и IT. Для OT это «доступность — целостность — конфиденциальность», для IT — наоборот: «конфиденциальность — целостность — доступность». Вследствие этой инверсии приоритетов соединение технологий несет риски для обеих сторон.

Есть три варианта решения проблемы безопасного соединения:

- физическая изоляция систем, что остается единственным приемлемым решением на самом критическом уровне;
- изоляция на уровне протоколов (конвертация данных);
- использование сетевых экранов с контролем потоков данных между защищенными областями.

На рис. D2-309 приведен пример схемы организации сети согласно последнему варианту.

Сеть имеет несколько защищенных областей — безопасных зон, которые разделяют данные в сети на основе их атрибутов для бизнеса.

ISOC (Integrated Security Operations Centre) — Центр управления интегрированной безопасностью.

EPU OTN (Electrical Power Utility Optical Transport Network) — Оптическая транспортная сеть энергопредприятия.

КОНЦЕПЦИЯ ПОСТРОЕНИЯ ЗАЩИТЫ ДАННЫХ

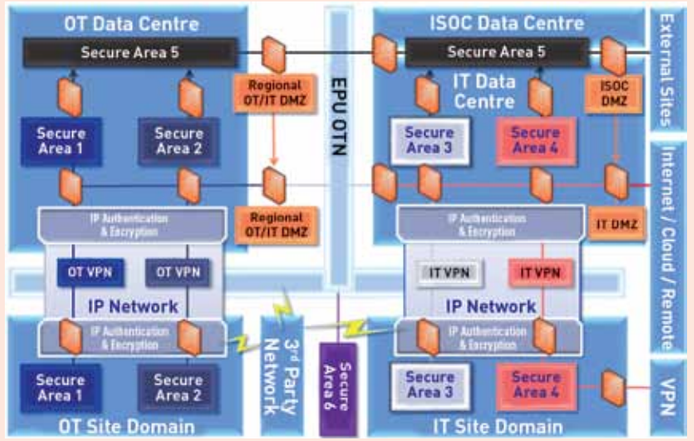

Рис. D2-309

Область OT рекомендуется разделить на две безопасные зоны:

Secure Area 1 — Безопасная зона 1. Критические OT-сервисы. Непосредственно обеспечивают управление, контроль и мониторинг энергосистемы в реальном времени.

Secure Area 2 — Безопасная зона 2. Некритические OT-сервисы. Сервисы поддержки — нарушение их работы не ведет к нарушению работы энергосистемы.

Все данные, входящие или выходящие из среды OT, проходят только через DMZ. Любые данные, поступающие в Безопасную зону 1, не проходят через Безопасную зону 2 и наоборот. Т. е. все безопасные зоны отделены друг от друга.

Область IT делится также на две безопасные зоны:

Secure Area 3 — Безопасная зона 3. Оперативные корпоративные сервисы. Предназначены для OT-сервисов, размещенных в инфраструктуре ИТ. Отделены от остальной части ИТ-сети предприятия. Для них требуется согласованное управление со стороны IT/OT.

Secure Area 4 — Безопасная зона 4. Корпоративные сервисы IT, которые не влияют на работу OT. Корпоративные услуги находятся в ведении ИТ-служб.

Любое внешнее соединение должно сначала пройти через IT DMZ, прежде чем попасть в нужную безопасную зону, аналогично безопасным зонам OT. И здесь так же, как и для OT, данные, предназначенные для одной из зон, не проходят через соседнюю.

Выход во внешнюю сеть должен быть сделан в одной логической точке. Интернет, облако, удаленный доступ и другие подобные внешние соединения должны проходить через системы безопасности ИТ, прежде чем перейти в нужную безопасную зону.

Доклад D2-312 (Россия): Development of information-analytical system for automatic fault analysis and relay protection performance evaluation (Разработка информационно-аналитической системы для автоматического анализа аварийных событий и оценки правильности работы устройств РЗА). D. A. ZHUKOV, RusHydro, PJSC

В докладе представлены результаты проектирования и имплементации информационно-аналитической системы, предназначенной для автоматического анализа отказов и оценки функциональных показателей системы защиты. Информационная модель и алгоритмические службы системы были разработаны в соответствии с техническими условиями и рекомендациями, приведенными в стандартах МЭК 61850, МЭК 61970/61968, однако информационная метамодель была расширена с использованием новой семантики. Оценка функциональных характеристик обнаружения возможных отказов релейной защиты основывается на автоматическом сравнении информации, полученной от полевых устройств DPR, DFR, RTU, с данными о расчетных эталонных операциях систем релейной защиты, полученных посредством цифрового моделирования. Этот процесс требует проведения детального моделирования идентифицированных событий отказа и работы реле. Результаты такого моделирования используются в качестве исходных данных при сравнении фактической информации от релейных устройств для обнаружения несоответствий и подачи аварийных сигналов при возникновении возможных скрытых отказов в настройках или работе реле.

Доклад D2-313 (Япония): Approach to Maintaining Secure Operation of Various Systems in Japanese Electric Companies (Методы обеспечения безопасной работы различных систем в электрических компаниях Японии). T. Hikino (Tohoku Electric Power Co., Inc.), T. Okabe (TEPCO Power Grid, Inc.), T. Kan, T. Tashiro (Kyushu Electric Power Co., Inc.), Y. Okunishi (Kyuden Business Solutions Co., Inc.), T. Seki (Nishimu Electronics Industries Co., Ltd.)

В докладе приведено общее описание «Рекомендаций по обеспечению безопасности систем управления», изданных в Японии, и рассматриваются несколько примеров реализации этих рекомендаций разными энергетическими компаниями.

ПРИМЕР МОДЕЛИ РЕЛЕЙНОЙ ЗАЩИТЫ ДЛЯ ГЕНЕРАТОРА

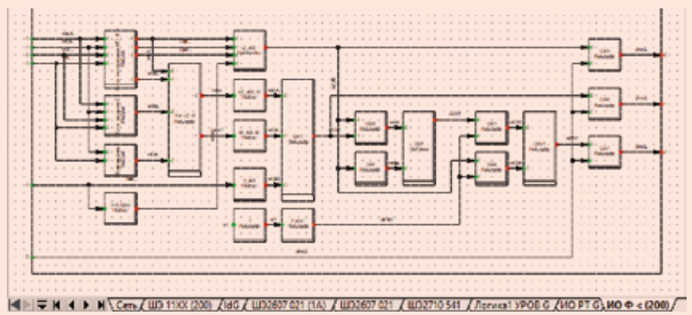

Рис. D2-312

Компания Kyushu Electric Power Company (KYUSHU EPCO) параллельно с постепенным переводом устаревшего оборудования циклической передачи данных (CDT, Cuclic Data Transfer) на современные IP-протоколы реализовала механизм разделения IP-сетей различного назначения. Это было сделано разложением IP-протокола на исходные данные и восстановлением этих данных в другой IP-протокол с помощью специальных устройств ретрансляции, установленных на границе между сетями, что позволило логически разделить различные сети и предотвратить распространение инцидентов безопасности между ними. На рис. D2-313 на с. 20 показан способ реализации с использованием эталонной модели OSI.

Компания Tohoku Electric Power Company описала опыт построения системы защиты инфраструктуры для своих 20 000 клиентских терминалов, серверного сегмента из нескольких тысяч серверов и сотен бизнес-систем, построенных в разное время по разным правилам.

Для упорядочивания коммуникаций между серверным и клиентским сегментами был проведен анализ журналов межсетевых экранов, осложненный тем, что некоторые журналы были очень большими (более 1 млрд записей в месяц). Более того, некоторые коммуникации происходили только в определенные интервалы времени, например начало или конец года либо конец финансового года. Вся эта работа заняла 3 года.

Компания Kyushu Electric Power Company реализовала свой пилотный проект по мониторингу информационных систем с помощью технологий машинного обучения и больших данных.

Система мониторинга этой компании собирает информацию о производительности всех серверов и устройств связи с определенными интервалами. Для особо важной информации устанавливаются пороговые значения, и любые собранные данные, превышающие пороги, обнаруживаются как аномалии. Но этот механизм подходит не всегда и иногда может давать очень большое количество предупреждений в зависимости от настройки порога, что дает риск пропуска критических предупреждений. Поэтому для определения возможности раннего выявления и предотвращения сбоев были использованы возможности машинного обучения:

1. Мониторинг отказов путем анализа данных, полученных в нормальном состоянии — за счет создания модели обнаружения отклонений и отказов, которые не могут быть зафиксированы по порогу мониторинга.
2. Обнаружение аномалий путем настройки процесса ввода данных, анализа, построения модели и настройки ее параметров.
3. Верификация оценки правильности срабатывания алгоритмов машинного обучения по раннему обнаружению сбоев.

Доклад D2-315 (Россия) Data Analytics Platform for Power Equipment Intelligent Lifecycle Management (Модель системы интеллектуального управления жизненным циклом электросетевого оборудования). A. I. KHALYASMAA, S. A. EROSHENKO, Ural Federal University named after the first President of Russia B. N. Yeltsin

В докладе представлена модель платформы для анализа данных с целью получения достоверных оценочных результатов касательно функционального состояния оборудования электроэнергетической сети, что необходимо для развертывания эффективных программ технического обслуживания и ремонта на базе методов обнаружения информации в базах данных. В предложенной системе извлечение информации из данных осуществляется посредством повышения градиента на деревьях принятия решений. В рамках представленных исследований были разработаны методологические, математические и алгоритмические основы интеллектуальной платформы анализа данных. Подтверждение предложенной модели основывалось на данных технической диагностики за период с 2005 г. по 2017 г. и представляет собой оценку функционального состояния оборудования реальной сети передачи электроэнергии в составе региональной электроэнергетической системы. В этой системе результаты оценки технического состояния были получены с использованием вероятностного подхода для проведения дальнейшего анализа технических и технологических рисков и, в завершение, для разработки сетевыми компаниями стратегий планового технического обслуживания и ремонта на основе эффективности.

Разработанная модель была использована в качестве независимого инструмента — модели автоматизированной системы, предназначенной для интегрированной оценки состояния оборудования электроэнергетической сети. В противоположность этому система может быть имплементирована в виде дополнительного модуля (подсистемы) для создания современной системы управления производственными активами (ERP — планирование ресурсов предприятия) в интересах заинтересованных групп электроэнергетической сети. Это предоставляет возможность не только улучшить технологическое управление высоковольтным энергетическим оборудованием, но и разработать эффективные инвестиционные программы для электроэнергетических компаний, оптимизировать стратегии экономии энергии и ресурсов, усовершенствовать тарифную политику в электроэнергетической индустрии на основе использования надежных источников энергии с учетом действия различных внешних факторов, что тем самым позволит гарантировать явные экономические эффекты.

ПРИМЕР КОНВЕРТАЦИИ IP-ПРОТОКОЛА

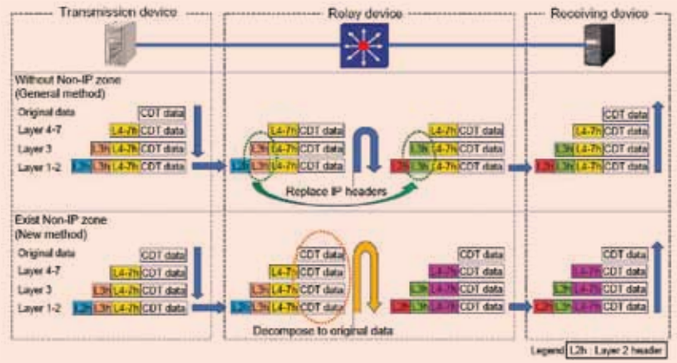

Рис. D2-313

ЗАКЛЮЧЕНИЕ

По итогам участия Исследовательского комитета D2 СИГРЭ в 47-й Сессии можно выделить основные особенности развития информационных систем и телекоммуникаций (ИСиТ) для электроэнергетики нового поколения, отличающейся массовым внедрением распределенной генерации ЭЭ, технологиями накопления электрической энергии, активными распределительными сетями и новыми концепциями эксплуатации и управления оборудованием энергосистем.

К таким особенностям развития ИСиТ следует отнести внедрение технологий больших данных, машинного обучения, искусственного интеллекта, появление новых надежных и эффективных средств телекоммуникаций, что подтверждают предоставленные для Сессии доклады. Так, совершенно очевиден рост IP-трафика между электросетевыми объектами и центрами управления, что значительно обостряет необходимость решения вопросов о миграции к сетям с пакетной коммутацией. Эти вопросы остаются актуальными и сейчас, подтверждением чему являются тематики очередных коллоквиумов СИГРЭ в 2019 г. не только по ИК D2, но и по ИК B5. Также проблемы миграции к сетям с пакетной коммутацией включены в тематику грядущей Сессии СИГРЭ 2020 г.

Несомненный интерес вызывает создание и внедрение автоматизированных систем анализа состояния первичного и вторичного оборудования, в чем заметно участие российских разработчиков.

Пристальное внимание международных исследовательских групп уделяется вопросам сбора и анализа большого количества разнородных данных. Применяемые при этом методики и алгоритмы нацелены на оперативное получение новых типов данных, требующихся для управления современными энергосистемами с распределенными источниками энергии стохастического типа.

Необычайно широкие возможности предоставляют технологии виртуализации систем и сервисов, разворачиваемые в ИТ-инфраструктуре энергокомпаний. Это направление также подтверждает свою актуальность и находит отражение в опыте реализации пилотных проектов в разных странах.

Общей основой для решения многих прикладных задач следует признать технологии беспроводной передачи информации, в том числе маломощные, использующие батарейное питание и представляющие компоненты технологий интернета вещей (IoT). Эти технологии также находят свое применение в электроэнергетике, что подтверждается авторами докладов.

И, наконец, следует сказать о направлениях исследований, посвященных информационной безопасности. Актуальность этой темы в последнее время постоянно растет, что и нашло отражение в нескольких докладах.

Состоявшаяся в августе 47-я Сессия, центральное событие в деятельности крупнейшей международной организации, еще раз доказала, что СИГРЭ — это уникальная площадка для международного сотрудничества и обмена опытом в сфере электроэнергетики с представителями ведущих организаций отрасли, изучения инновационных технологий и влияния на их создание и внедрение.

СТРУКТУРА РАЗРАБОТАННОЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ

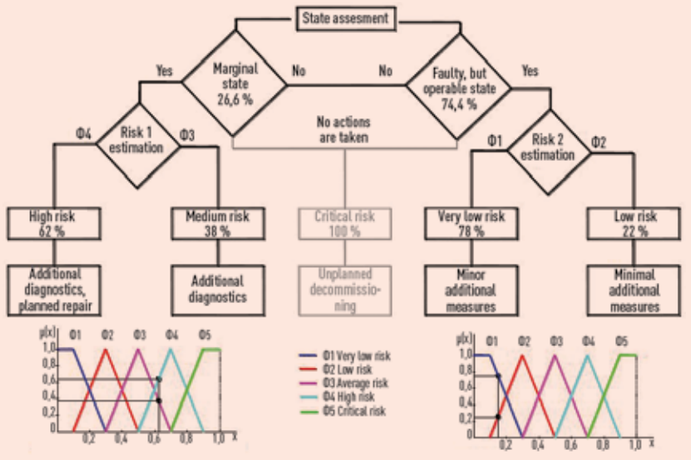

Рис. D2-315