Обновлённым сетям электроснабжения требуется виртуализация подстанций

Коул Вебер, Шринивас Кумар

Операторы сетей электроснабжения обновляют распределительные системы с учётом происходящих в отрасли изменений, и информационные технологии играют в этом процессе всё более важную роль. Специальное оборудование подстанций позволяет воспользоваться преимуществами технологии виртуализации, благодаря которой коммунальные предприятия могут виртуализировать свои подстанции в любой точке мира.

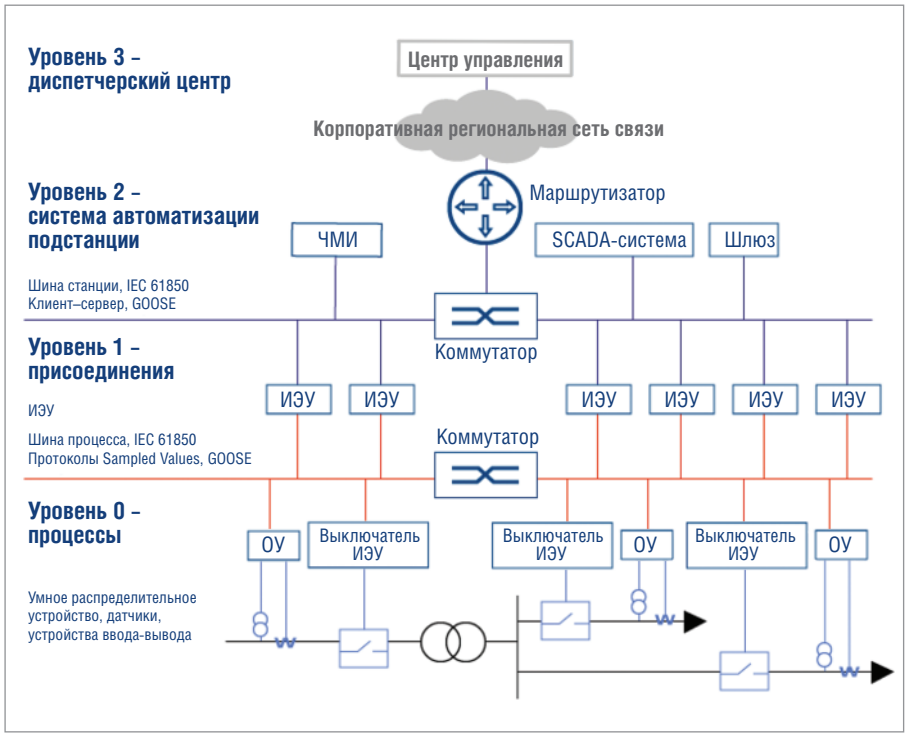
Распространённые в развитых странах системы передачи и распределения электроэнергии, или просто сети (англ., grid), отличаются поразительно высокими показателями надёжности и времени безотказной работы, особенно с учётом значительной доли фондов, находящихся в эксплуатации уже несколько десятков лет. Современные сети должны решать задачи, которые не были предусмотрены при их проектировании, например, осуществлять передачу двунаправленных потоков мощности при электроснабжении от распределённых источников энергии (РИЭ), многие из которых представляют собой небольшие электростанции, вырабатывающие энергию из возобновляемых источников и работающие только периодически. Устаревшие системы требуют обновления, при этом любые работы по их устройству или переустройству должны выполняться с учётом новейших требований к обслуживанию и потребностей в электроснабжении. Несоблюдение этих требований приводит к катастрофам, аналогичным той, которая недавно произошла в штате Техас.

Старые фонды уже почти отслужили свой срок и требуют замены, а поскольку расширяются сети для подключения новых строительных объектов и электростанций, разработчики ищут такие решения, которые не уступали бы в надёжности современным технологиям или даже превосходили бы их. В будущем потребуется применение современных вычислительных средств, таких как серверы-гипервизоры и дублирующие сетевые архитектуры, основанные на протоколах бесшовного резервирования HSR/PRP (протокол параллельного резервирования соединений / протокол параллельного резервирования), для обеспечения необходимых функций автоматического управления и передачи данных при внедрении, эксплуатации, техническом обслуживании и обеспечении надёжности сетей на уровне выше текущего.

Рис. 1. Распределительные подстанции понижают напряжение в распределительных сетях до уровня местных распределительных сетей, а также выполняют ряд других функций автоматического управления, защиты и контроля

Подстанции являются важнейшими элементами эксплуатации сетей, обеспечивающими повышение напряжения для передачи в сеть или его понижение до уровня систем распределения электроэнергии. В статье подробно описаны распределительные подстанции, применяемые для понижения напряжения в распределительных сетях до уровней, соответствующих требованиям на входе в распределительные трансформаторы, монтируемые на столбах и на бетонных подушках (рис. 1), которые, в свою очередь, понижают напряжение до уровней местных распределительных сетей в 120/240/480 В переменного тока в целях электроснабжения промышленных, торговых и жилых объектов.

Помимо традиционных функций, связанных с выходящими потоками мощности, распределительные подстанции в настоящее время могут принимать вхо-



Условные обозначения:

ЧМИ – человеко-машинный интерфейс; ИЭУ – интеллектуальные электронные устройства; GOOSE – протокол передачи данных о событиях на подстанции; Sampled Values – протокол передачи оцифрованных мгновенных значений от измерительных трансформаторов тока и напряжения; ОУ – объединительное устройство.

Рис. 2. Устройства уровня 0 распределительной подстанции связаны с центром управления при помощи шины процессов и шины станции

дящие потоки мощности от РИЭ, что значительно усложняет их работу. Для решения этой и других проблем необходима виртуализация.

Эта технология позволяет нескольким операционным системам и связанным с ними приложениям работать одновременно на единой аппаратной платформе. Недавние и ожидаемые в будущем технические разработки позволят таким виртуальным машинам (ВМ) реагировать в течение долей миллисекунды в самых критических ситуациях, например, при срабатывании релейной защиты.

Свыше 90% потребностей касаются обновления и восстановления существующих фондов с устройством новых подстанций, спроектированных и построенных на основе современных технологий.

Оборудование распределительных подстанций

На современных распределительных подстанциях используются различные устройства для выполнения всех необходимых рабочих функций (рис. 2). Помимо традиционных функций, связанных с выходящими потоками мощности, распределительные подстанции способны в настоящее время принимать входящие потоки мощности от РИЭ, что значительно усложняет их работу. На рис. 2 представлены некоторые из этих устройств в составе стандартной системы автоматизации подстанции (САП), а также некоторые другие устройства, каждое из которых выполняет одну или несколько основных функций.

- *Защита и контроль:* полностью независимые элементы, работающие в режиме реального времени.
- *Автоматизация:* управление и контроль, отдельные элементы, работающие в режиме реального времени.

Устройства *защиты и контроля* включают интеллектуальные электронные устройства (ИЭУ), оснащённые защитными предохранителями для отслеживания их работы. Объединительное устройство (ОУ) занимается сбором выходных цифровых многоканальных сигналов синхронно от трансформаторов тока и напряжения, а затем передаёт эти данные по протоколу IEC 61850-9 защитным, измерительным и контрольным устройствам.

ИЭУ выполняют важные функции, такие как релейная защита, удалённое обнаружение неисправностей, мониторинг и регулировка уровней мощности и напряжения, автоматическое переключение между источниками питания для передачи данных по шине и повторное подключение питающих линий после временных сбоев.

Устройства *автоматизации*, такие как персональные компьютеры (ПК), маршрутизаторы, неуправляемые/управляемые коммутаторы, программируемые логические контроллеры (ПЛК) и человеко-машинные интерфейсы (ЧМИ), обычно используются для координации работы защитных и контрольных устройств, а также для поддержки других необходимых функций, таких как сетевой обмен данными. Все эти устройства содержат в себе аппаратную часть для осуществления управления; кроме того, на них нередко установлено программное обеспечение для выполнения различных операций.

В идеальном случае все эти устройства должны быть совместимыми со стандартными протоколами IEC 61850, со службой связи, объединяющей все эти устройства на уровне 0, с серверами на уровне 1 и с клиентами на уровне 2. Однако это идеальное условие выполняется не всегда; но даже когда оно выполняется, остаются другие проблемы, связанные с коммуникацией и интеграцией.

Стандартная распределительная подстанция оснащена многими из перечисленных устройств, поставляемых различными производителями, при этом каждое из них содержит собственную фирменную аппаратную часть, а также нередко свои собственные операционные системы и установленное программное обеспечение, что приводит к множеству операционных и управленческих ошибок.

Управление множеством устройств

На каждой подстанции установлены сотни отдельных устройств. Для правильной работы подстанции эти устройства должны быть установлены надёжным и безопасным способом; они должны соединяться друг с другом посредством цифровых каналов связи и иметь чётко определённые схемы передачи данных. Даже если каждое устройство соответствует требованиям отраслевых стандартов (что бывает далеко не всегда), нередко возникают трудности при настройке таких коммуникационных каналов. После того как каналы связи налажены и работают в соответствии с проектом, встаёт вопрос их технического обслуживания, поскольку обновления программно-аппаратного и программ-

ного обеспечения устройства могут привести к случайному отключению связи.

Каждое из устройств может быть поставлено отдельным производителем, имеющим свои собственные представления об электропитании, механическом устройстве, разъёмах для обмена данными и температурных режимах, то есть об охлаждении устройства летом и обогреве зимой при работе под максимальной нагрузкой.

Кроме того, есть и другие проблемы: график технического обслуживания, а именно, процедуры замены повреждённых, изношенных или неисправных компонентов.

Техническое обслуживание не только влияет на работу или требует отключения электронного устройства. Оно сопряжено с рядом логистических операций, таких как обнаружение неисправного компонента, его демонтаж, возврат на завод-изготовитель, подбор подходящего компонента на замену и установка нового компонента – и всё это должно выполняться с уверенностью в том, что устройство будет правильно функционировать без необходимости дополнительного испытания перед тем, как подстанция будет снова включена в работу.

Даже если компоненты оборудования исправны, может потребоваться обновление их программно-аппаратного обеспечения и установка корректировок (патчей) к программному обеспечению. Поставщики могут придерживаться различного порядка выполнения этих работ, при этом сетевые операторы вынуждены работать с каждым поставщиком в отдельности при обновлении конкретного устройства.

Устройства могут быть встроены в другое оборудование или смонтированы отдельно в защитных шкафах, поставляемых вместе со вспомогательными источниками питания. Уже само количество таких устройств делает их установку сложной и дорогостоящей, а также требует немало места для установки каждого шкафа.

Программирование некоторых устройств осуществляется со встроенного контроллера – для этого нужно иметь под рукой руководство по эксплуатации и определённый уровень технических знаний. При этом интерфейсы устройства могут быть различными в зависимости от поставщика, что увеличивает время выполнения этой операции и повышает риск ошибки со стороны оператора. Работы также усложняются из-за необходимости принимать меры обеспечения кибербезопасности.

Виртуализация подстанций позволяет решить все эти проблемы, а также предлагает ряд других преимуществ.

Преимущества виртуализации

Самым значительным преимуществом виртуализации является само отсутствие необходимости использовать множество устройств от различных поставщиков. Теоретически все ИЭУ могут работать на одной аппаратной платформе от одного или двух утверждённых поставщиков с использованием единых стандартов на аппаратную часть, электромагнитную совместимость, соединения и электропитание. Аппаратная часть может быть стандартизована на уровне серверов центра обработки данных, при этом программное обеспечение может быть установлено только на сервере-гипервизоре, с виртуальными ИЭУ, установленными на каждой ВМ.

Все ВМ и функции сетевого обмена данными по виртуальной сети могут быть поставлены и управляться единым организатором для обеспечения глобальной масштабируемости и быстрой поставки даже высокоспециализированных решений, разработанных по индивидуальному заказу.

Пара взаимодополняющих виртуальных серверов потребляет намного меньше электроэнергии по сравнению с гораздо бóльшим количеством отдельных устройств, которые эти серверы заменяют, особенно с тех пор, как многие промышленные ПК (ППК) были оптимизированы с целью снижения энергопотребления и, соответственно, вырабатываемого ими тепла. С внедрением ЦПУ высокой плотности пара серверов способна заменить до 24 ИЭУ. Требуется меньше места для их физического размещения, что упрощает проектирование подстанций, монтируемых в шкафах, контейнерах, под землёй или под водой – в условиях крайне ограниченного пространства.

Наконец, виртуализация позволяет легко внедрять и обновлять передовые аналитические методы, машинное обучение и искусственный интеллект без существенного переустройства физической сетевой инфраструктуры. Эта дополнительная функция объединения возможностей программного обеспечения открывает новую эру прогнозных и нормативных методов анализа, отсутствующих в сегодняшней весьма проблемной инфраструктуре ИЭУ электрических подстанций.

По мнению ведущего инженера отдела стратегии защиты и контроля в рамках проекта Солт-Ривер Энтони Сайвсинда (Anthony Sivesind), благодаря виртуализации устройств в масштабах всей энергетической системы, вплоть до функций релейной защиты, построенной на базе единой платформы, коммунальные предприятия, в конечном счёте, смогут наверстать упущенное как в части изменения топологии и технологии принадлежащих им участков сетей, так и в части планирования жизненного цикла оборудования.

Виртуальные подстанции позволят уменьшить на 50% или более число аппаратных устройств и снизить на 76% расходы на эксплуатацию и техническое обслуживание.

Виртуализация функций автоматизированного управления и контроля

Виртуализацию подстанций можно реализовать посредством установки промышленных серверов для подстанций, сертифицированных согласно стандарту IEC 61850-3. Как правило, такие серверы устанавливаются парами в целях взаимного дублирования, при этом каждый из них оснащён многоядерными микропроцессами (рис. 3). Достигнутое в последнее время повы-

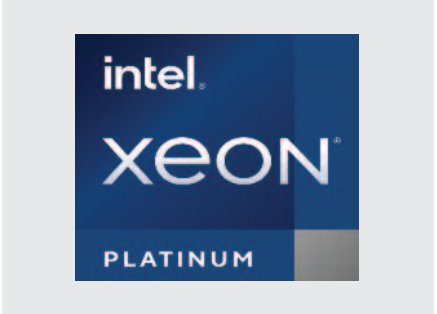
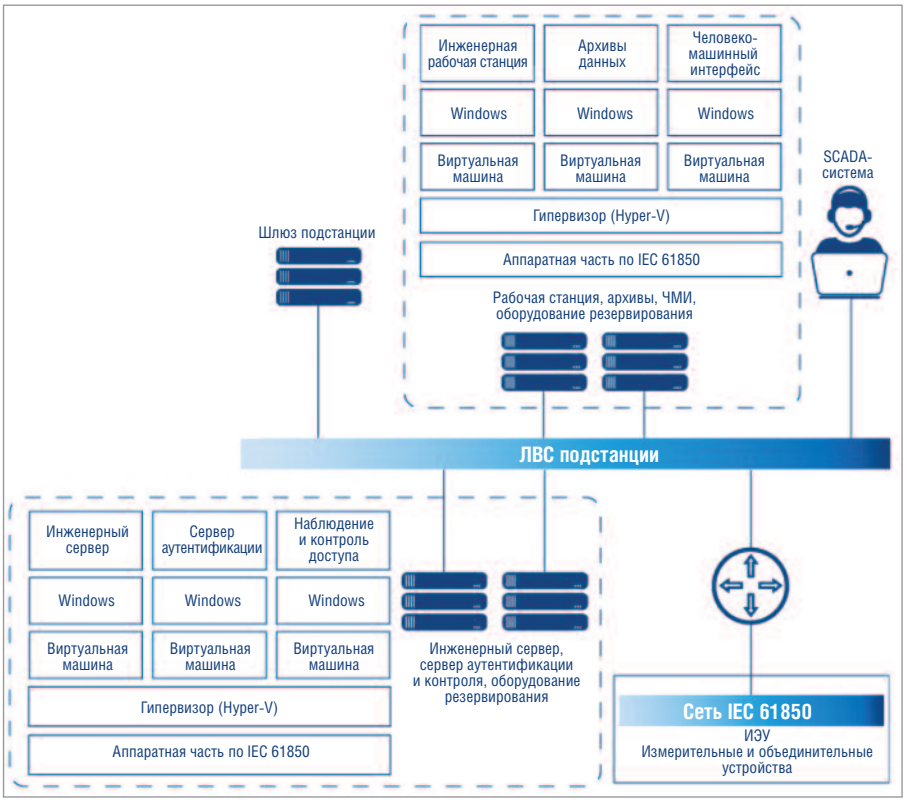


Рис. 3. Многоядерные процессоры обеспечивают вычислительную мощность и работу в режиме реального времени, которые необходимы для виртуальных машин, используемых на подстанциях



Условные обозначения:

ЧМИ – человеко-машинный интерфейс; ИЭУ – интеллектуальные электронные устройства.

Рис. 4. Архитектура виртуальной локальной сети для виртуальной системы автоматизации подстанции

шение производительности со временем ожидания, близким к режиму реального времени, делает возможным обеспечить с использованием таких серверов работу ВМ, выполняющих наиболее критичные функции защиты и управления подстанцией, такие как функции релейной защиты. Каждое виртуальное реле может работать на своём собственном ядре, гарантируя уровень производительности и защиты, аналогичный возможностям специализированного аппаратного устройства.

Функции автоматизированного управления и контроля чуть менее требовательны, поэтому несколько устройств можно заменить одной или несколькими ВМ, образующими виртуальную систему автоматизации подстанции (рис. 4).

На одном сервере виртуальной подстанции, соответствующем стандарту IEC 61850, могут быть установлены все операционные системы и связанные с ними приложения, которые ранее запускались на отдельных серверах, что значительно уменьшает количество ИЭУ, а также позволяет уменьшить сопутствующие расходы на приобретение и техническую поддержку оборудования (рис. 5).

Два сервера виртуальной подстанции можно настроить на работу в качестве дублирующих устройств, при этом оба сервера соединяются по дублирующему сетевому протоколу HSR/PRP, который обеспечивает полную работоспособность в случае отказа одного из серверов. При такой архитектуре дублирующие серверы обеспечивают намного более высокую надёжность по сравнению с множеством отдельных устройств, поскольку каждое такое устройство представляет собой единственную критическую точку для работающих на нём приложений.

Рис. 5. Надёжный и компактный сервер Advantech ECU-570, сертифицированный по стандарту IEC 61850, можно настроить в качестве сервера-гипервизора системы автоматизации подстанции

Кроме того, виртуальные системы могут заменять ПЛК и другие контроллеры, которые нередко устанавливаются на подстанциях с ВМ. Устройства ввода-вывода подключаются напрямую к серверам виртуальной подстанции по сети Ethernet, в то время как программные ПЛК запускаются на ВМ.

Виртуализация функций защиты и контроля

Стандартная распределительная подстанция может включать в себя до 10 устройств автоматизации; при этом такая подстанция, как правило, оснащена намного большим количеством защитных и контрольных устройств – их количество нередко превышает 100. Защитные устройства должны работать в непрерывном режиме в течение длительного периода времени (от 10 до 20 лет). Однако обновление таких устройств после их установки с добавлением новых функций является сложной процедурой в силу регуляторных и физических причин.

Разделение функциональности на две части – на электрическую и на цифровую, или электронную, часть – позволяет архитекторам системы перенести вторую часть на ВМ, работающую на сервере виртуальной подстанции. В любой момент времени, когда оператор пожелает обновить ВМ с добавлением новых функций защиты либо добавить ещё одну ВМ, в которой используется такая же электрическая релейная защита, он может сделать это без внесения физических изменений в локальную сеть и даже без необходимости посещать объект.

На фоне ускоренного развития функций защиты и постоянно совершенствующихся алгоритмов уже существующих функций возможность быстро и эффективно вносить изменения в систему представляет собой огромное преимущество при управлении защитой подстанции.

Поставщики также выигрывают от поставки операторам подстанций релейных устройств и ВМ, уже оснащённых всеми необходимыми техническими функциями. Если заказчик пожелает приобрести ту или иную функцию, поставщик одним нажатием кнопки может выдать лицензию на ее использование, и эта функция немедленно начинает работать. Таким образом, и поставщик, и оператор получают непосредственную выгоду от использования цифровой виртуальной подстанции.

AIM-75S+android 10

ПРОМЫШЛЕННЫЙ ПЛАНШЕТНЫЙ КОМПЬЮТЕР

Сканер штрих-кодов

Удобные аксессуары

Зарядная станция на несколько устройств

Считыватель магнитных карт

Зарядная станция на несколько батарей

Крепление VESA

ADVANTECH
Enabling an Intelligent Planet

Промышленный планшетный компьютер с проекционным емкостным сенсорным экраном с покрытием Gorilla Glass 3 на базе процессора Qualcomm SD660 под управлением операционной системы Android 10

- Диапазон рабочей температуры –10...+50°C
- Соответствует стандарту MIL-STD-810G по устойчивости к ударам и вибрации
- Защита IP65 от пыли и влаги по всему корпусу
- Питание от сети постоянного тока 5/9 В
- Автономная работа в течение 12 часов

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

Угрозы кибербезопасности и меры противодействия им

Добавление сервера для сбора данных подстанции к технологическому процессу и станционной шине влечёт за собой целый ряд проблем и рисков в области кибербезопасности и защиты данных. Речь идёт не всегда о новых рисках, связанных с данной технологией, а об определённом наборе уже известных угроз для кибербезопасности, с которыми необходимо бороться.

Энергетическая инфраструктура с учётом необходимой модернизации сетей представляет собой крайне привлекательную мишень для кибератак. Основные угрозы для энергетических сетей связаны со следующими пятью факторами.

1. Физический доступ к высокоавтоматизированным системам, не имеющим встроенных заводских элементов защиты, а также широкая зона атаки в связи с наличием множества точек доступа.
2. Возможность организовать атаки с устройств с участием сетевых роботов в целях манипулирования спросом на мощность в сети, что может привести к локальным отключениям и даже крупномасштабным блэкаутам.
3. Атаки, направленные на незащищённые системы контроля и сбора данных (SCADA) и другое программное обеспечение промышленных систем управления (ПСУ).
4. Системы выявления несанкционированного доступа (взлома) могут быть настроены на снижение количества ложных срабатываний, причём до такой степени, что становятся бесполезными.
5. В отличие от подхода к обеспечению ИТ-безопасности, при котором заражённые пользовательские рабочие станции (оконечные устройства) помещаются на карантин в рамках виртуальной локальной сети (ВЛС) благодаря принципу сегментирования сетей, действующие генерирующие и распределительные энергетические системы невозможно отключить, а помещение устройств на карантин во взаимосвязанных системах приводит к сбоям в работе и нежелательным отключениям.

Реагирование на выявление нарушений в работе сети и глубокая проверка прикладных протоколов на уровне пакетов данных могут осложниться в будущем из-за шифрования сетевого трафика (без технологической переделки приложений). Стратегия противодействия угрозам потребует по меньшей мере следующего (рис. 6).

- Обеспечение целостности сигналов, передаваемых между системами.
- Управление секретными цифровыми данными, используемыми для обеспечения безопасности, то есть паролями и ключами.
- Ротация секретных цифровых данных с использованием сертификатов X.509 в целях надёжной доставки данных в качестве стратегии смягчения последствий и восстановления устройств при нарушениях безопасности.
- Передача данных с защитой от несанкционированного доступа на протяжении всей логистической цепочки.
- Удалённое восстановление устройства в случае нарушения безопасности с использованием доверенного программного обеспечения и обновлений конфигурации, а также автоматическое обновление ключей.
- Встроенные средства контроля доступа в сеть для организации внутренней защиты.
- Контролируемость для выявления и оценки соответствия нормативным требованиям – во избежание штрафов за нарушения (например, технология защиты критической инфраструктуры Североамериканской корпорации по обеспечению надёжности электросистем – NERC CIP).

Модель нулевого доверия в киберзащите

Полевые устройства и ВМ в составе умных электрических сетей нуждаются в защите от кибератак на национальном уровне. Сервер-гипервизор требует наличия «корня доверия» на аппаратной основе, благодаря чему он может использоваться в качестве высоконадёжной платформы. ВМ и критические рабочие нагрузки, такие как «родные» и контейнерные приложения, требуют надёжного подтверждения правильного порядка загрузки, технического обслуживания, в зависимости от текущего состояния, с надёжной оценкой операционной целостности в процессе выполнения для аналитических систем искусственного интеллекта и машинного обучения, защиты с использованием криптографических ключей и ротации таких ключей, аутентификации на основе сертификатов, управления жизненным циклом сертификата, надёжной доставки данных с защитой логистической цепочки от несанкционированного доступа, а также встроенных средств контроля доступа к сети.

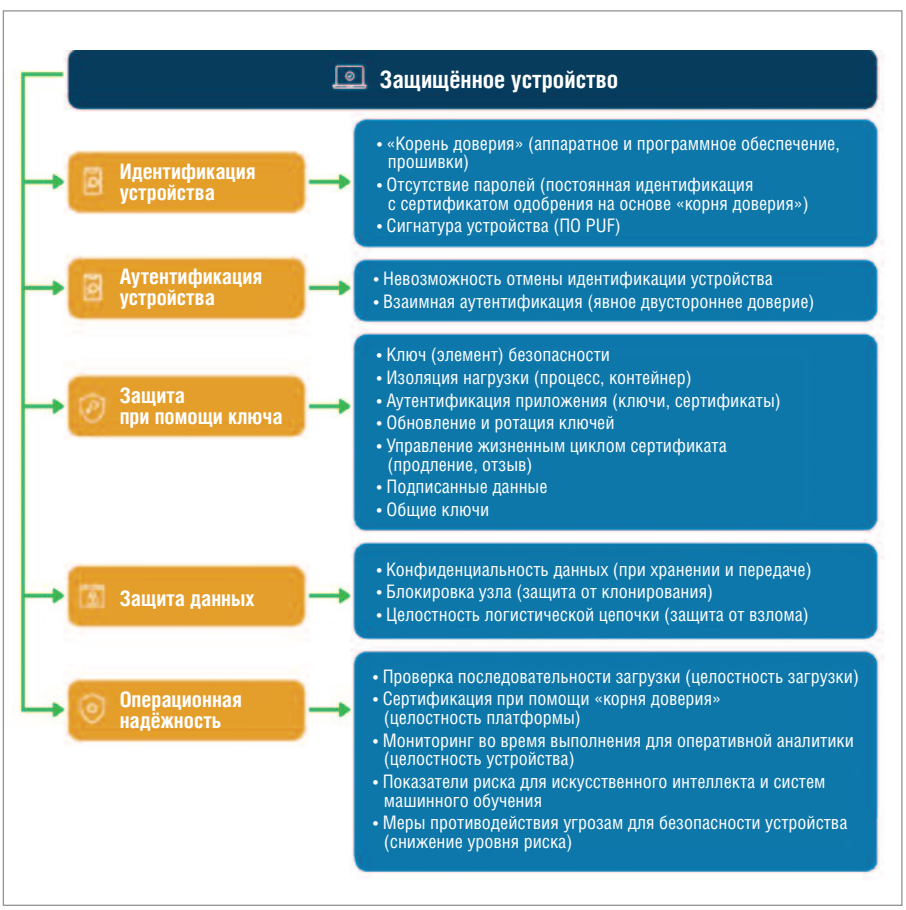


Рис. 6. Схема обеспечения многоуровневой защиты устройства

EtherWAN

SmartE — НОВАЯ СЕРИЯ
промышленных коммутаторов для решения базовых Ethernet-задач

Дано:

Необходимая функциональность:
(M) = VLAN, SNMP, RSTP, IGMP

Производительность:
(R) = 148,880 пакетов в секунду

Диапазон рабочих температур:
(T) = –40...+75°C

Исполнение:
(A) = промышленное, металлический корпус

Дополнительные условия:
(S) = крайне ограниченный бюджет

Найти:

***SW* – оптимальный Ethernet-коммутатор?**

Решение:

Условие равновесия сети

$$\sum_i F_i = 0$$

Здесь *F* – требования к оборудованию

$$\sum M + R + T + A = -S$$

$$\sum \vec{S} + \vec{M} + \vec{A} + \vec{R} + \vec{T} = SW$$

Ответ:

***SW* = SmartE**

Серия SF300 – Fast Ethernet

Серия SG300 – Gigabit Ethernet

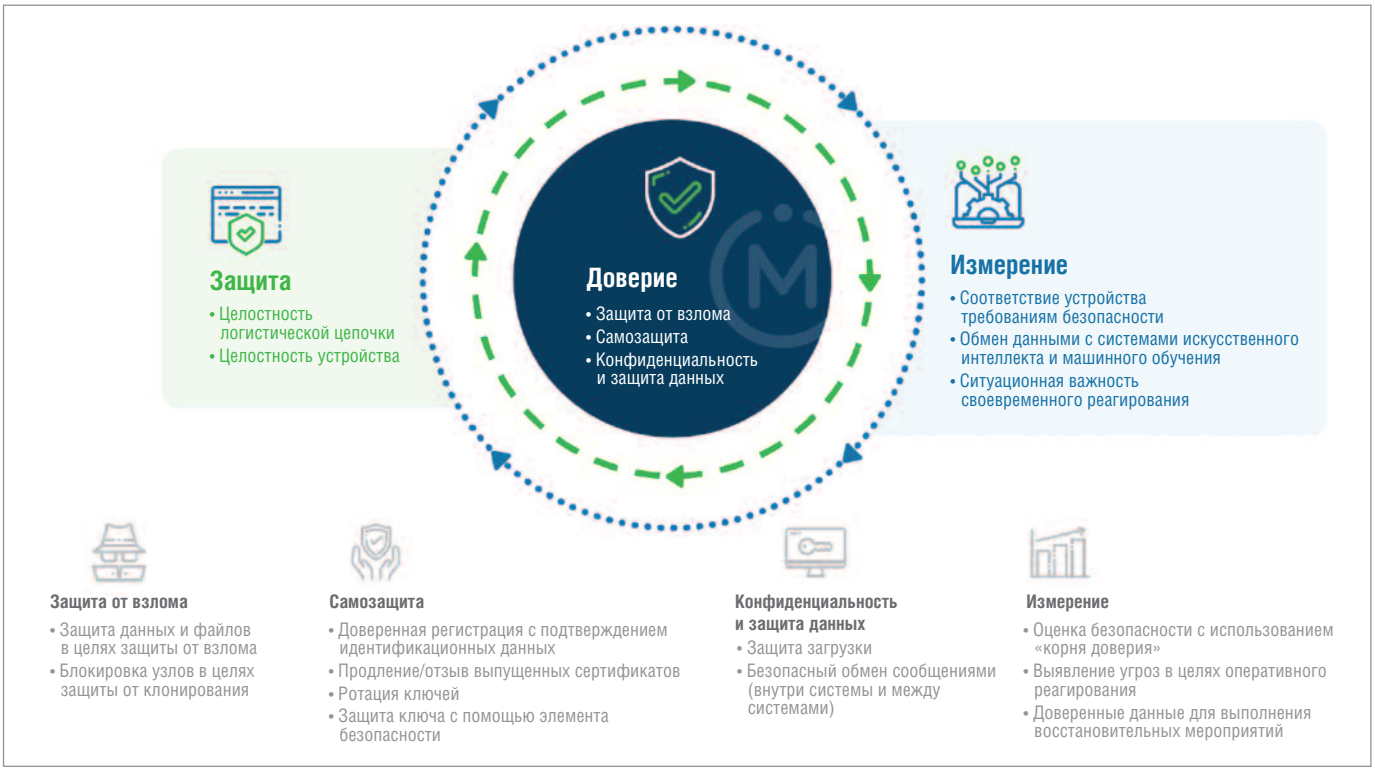


Рис. 7. Схема функциональных возможностей технологии TrustCenter™ компании Mocana

Сквозная киберзащита ВМ и критических рабочих нагрузок возможна благодаря сотрудничеству с компанией Mocana и использованию её технологии TrustCenter™. Эта технология обеспечивает конфиденциальность цифровой информации, защиту данных и обмен данными в глобальном масштабе (рис. 7). Она работает совместно с сервисом безопасного подключения устройств (SDO – Secure Device Onboarding) компании Intel, что значительно сокращает время подключения и передачи прав собственности на рабочие технологические устройства. Кроме того, эта технология интегрирована с доверенным платформенным модулем TPM 2.0 в составе системы Advantech ECU-579 в качестве аппаратного «корня доверия».

Технология TrustEdge™ «подключи и работай» от компании Mocana предоставляет доступ для «родных» и контейнерных приложений к возможностям модуля TPM, средствам защиты с использованием ключа, независимого от элементов безопасности доверенной абстрактной платформы (TAP – Trust Abstraction Platform), изоляции процессов, защиты на основе «корня доверия» и удалённого подтверждения доверия к платформе.

Заключение

Специальное оборудование подстанций позволяет воспользоваться преимуществами технологии виртуализации, благодаря которой коммунальные предприятия могут виртуализировать свои подстанции в любой точке мира. Многие компании выбирают этот подход, чтобы справиться с растущей сложностью и увеличивающимися потребностями интеллектуальной энергетической сети.

Эти технологические изменения можно внедрить только в тесном сотрудничестве с компаниями – поставщиками оборудования, систем безопасности, систем виртуализации, программного обеспечения и услуг системной интеграции.

Advantech – это центр сотрудничества, позволяющий осуществлять совместную разработку рассматриваемого решения в целях удовлетворения потребностей в надёжной, отказоустойчивой, резервированной двунаправленной электрической сети.●

Рекомендуемая литература

1. Dayabhai S. and Diamandis P. The Role of Virtualization in a Smart-Grid Enabled Substation Automation System [Электронный ресурс] // Режим доступа : https://www.concogrp.com/downloads/white-papers/The-role-of-virtualization-in-a-smart-grid-enabled-Substation-Automation.pdf.
2. Bose A. Grid Modernization: Opportunities and Obstacles [Электронный ресурс] // Режим доступа : https://www.tdworld.com/grid-innovations/article/20972284/grid-modernization-opportunities-and-obstacles.
3. Advantech Routers Secure Remote Data Upload for Oil and Gas Industry [Электронный ресурс] // Режим доступа : https://www.advantech.com/resources/case-study/advantech-routers-secure-remote-data-upload.
4. Helping Electrical Substation SCADA Systems Work Together [Электронный ресурс] // Режим доступа : https://www.advantech.com.my/resources/case-study/helping-disparate-scada-systems-work-together.
5. Enabling Digital Substations Through Passive Distributed Sensor Network [Электронный ресурс] // Режим доступа : https://www. tdworld.com/substations/whitepaper/21141827/enabling-digital-substations-through-passive-distributed-sensor-networks.
6. Group Domain of Interpretation [Электронный ресурс] // Режим доступа : https://en.wikipedia.org/wiki/Group_Domain_of_Interpretation.
7. Hanna S., Kumar S., Weber D. IIC Endpoint Security Best Practices [Электронный ресурс] // Режим доступа : https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf.
8. Foresight Review of Cyber Security for the Industrial IoT [Электронный ресурс] // Режим доступа : https://ocsiiot.web.ox.ac.uk/files/lrfforesightreviewofcybersecurityfortheiiotjuly2020pdf-0.
9. Contu R., Orans L. OT Security Best Practices [Электронный ресурс] // Режим доступа : https://www.gartner.com/en/documents/3889051/ot-security-best-practices.

Новости ISA

24 апреля 2021 года члены студенческой секции ISA ГУАП, студенты: Н.И. Мирошниченко, А.С. Раскопина и М.Д. Синкин приняли участие в региональной межвузовской олимпиаде по основам радиотехники и телекоммуникаций в составе команды ГУАП. Команда успешно проявила себя и заняла четвёртое место в общем зачёте.

19 мая в Мадриде (Испания) на заседании Исполкома округа 12 ISA объявлены итоги XVII Европейского конкурса на лучшую студенческую научную работу ISA (XVII ESPC-2021). Большого успеха добились студенты и аспиранты ГУАП. Золотыми медалями награждены: Ангелина Добровольская, Ксения Сердюк, Никита Степанов, Мария Рассыхаева, Виктория Гончарова, Мария Иванова. Серебряными медалями награждены: Белла Акопян, Анна Фоминых, Даниэле Казадио, Вениамин Китаев, Лилия Климочкина, Мария Создателева, Михаил Гордеев, Александра Щеголева. Бронзовыми медалями награждены: Владимир Кузьменко, Евгений Григорьев, Дарья Щукина, Алексей Тупицын, Александра Виниченко, Мария Белова, Виктория Афанасьева, Максим Русанов, Николай Реутов, Дмитрий Жданович. Команда университета стала победителем в общем медальном зачёте.

Президент Российской Санкт-Петербургской секции ISA профессор Галина Юрьевна Пешкова и президент-элект секции профессор Андрей Михайлович Тюрликов приняли участие в работе онлайн-заседания Исполкома ISA округа 12, которое провёл вице-президент округа 12 господин Франсиско Диас Андреу (Francisco Diaz Andreu, Испания).

С 31 мая по 4 июня в ГУАП была проведена XXIV Международная научная конференция «Волновая электроника и инфокоммуникационные системы». В работе конференции приняли участие более 350 учёных из России и зарубежных стран (Беларусь, Азербайджан, Франция, Италия, Алжир, Великобритания, Казахстан, Болгария). Было представлено 134 доклада в 8 секциях. По итогам работы конференции материалы 129 докладов были рекомендованы оргкомитетом к опубликованию в сборнике трудов конференции на платформе IEEE с индексацией в SCOPUS. В программе конференции были предусмотрены заседания 8 секций: акустооптика, акустоэлектроника, методы и устройства обработки информации, обработка и передача информации в инфокоммуникационных системах, контрольно-измерительные приборы и интеллектуальные транспортные системы, электромеханика и системы управления, моделирование и ситуационное управление качеством в электронике и приборостроении, встроенные микроэлектронные системы. Работа секций прошла в смешанном формате: участники представляли доклады как очно, так и в онлайн-формате с использованием платформы Zoom. По традиции оргкомитет отметил наиболее интересные доклады молодых участников конференции. В этом году среди обладателей дипломов и ценных подарков отмечен член Российской Санкт-Петербургской секции ISA Александр Чабаненко за лучшее фундаментальное исследование, секция «Моделирование и ситуационное управление качеством в электронике и приборостроении». Члены Российской Санкт-Петербургской секции ISA: Ю.А. Антохина, А.А. Оводенко, В.Ф. Шишлаков, А.Р. Бестугин, К.В. Лосев, Н.Н. Майоров, А.М. Тюрликов, В.И. Казаков, И.А. Киршина, С.В. Селёный приняли активное участие в организации и проведении конференции.

Один из старейших членов Российской Санкт-Петербургской секции ISA профессор, доктор технических наук Евгений Дмитриевич Соложенцев преподнёс в дар центру знаний ISA свою фундаментальную монографию «Основы событийного управления качеством экономики, государства и жизни человека», изданную в 2021 году в издательстве «Наука». Событийное управление качеством является методом искусственного интеллекта на основе алгебры логики и логико-вероятностного исчисления и создаёт новое научное направление в экономике.

22 июня в демонстрационном зале НИТ ГУАП профессор университета штата Индиана (США), президент ISA 2008 года, почётный доктор ГУАП Джеральд Кокрелл (Gerald Cockrell) принял участие в заключительном

занятии интернет-семинара «Управление проектами». Профессор Кокрелл уже в 16-й раз провёл семинар. За эти годы около 450 студентов, аспирантов, преподавателей ГУАП и членов регулярной и студенческой секций ISA приняли в нём участие. Традиционно директор института технологий предпринимательства ГУАП Артур Суренович Будагов вручил от имени профессора Джеральда Кокрелла сертификаты университета штата Индиана слушателям семинара, успешно завершившим программу.

30 июня в Атриуме Комендантского дома Петропавловской крепости в Санкт-Петербурге состоялась 19-я церемония награждения лучших выпускников петербургских вузов. Вчерашним студентам вручили благодарственные письма от губернатора и бронзовые статуэтки. Статуэтка сфинкса символизирует интеллект, сильный характер и мудрость. Этот почётный знак получили 60 лучших выпускников Санкт-Петербурга. Их поздравили вице-губернатор Владимир Княгинин и председатель Совета ректоров вузов Санкт-Петербурга и Ленинградской области Алексей Демидов. Среди награждённых выпускница магистратуры Института аэрокосмических приборов и систем ГУАП, активный член студенческой секции ISA ГУАП Ангелина Добровольская. На счету девушки 13 научных публикаций и зарегистрированная программа для ЭВМ.

Объявлены имена победителей международного конкурса грантов ISA для студентов (ISA Educational Foundation Scholarship) в 2021 году. Среди победителей президент студенческой секции ISA ГУАП 2021 года, аспирантка кафедры проблемно-ориентированных вычислительных комплексов ГУАП Белла Акопян и аспирант кафедры вычислительных систем и сетей ГУАП Евгений Григорьев.