Обнаружение кибервторжений в сетях подстанций

Как повысить безопасность подстанций стандарта IEC 61850

Общие сведения

Многоуровневая защита необходима для обеспечения кибербезопасности подстанций. Криптография позволяет проверить подлинность устройств, но не все атаки могут быть предотвращены этими мерами. Брандмауэры и «воздушные зазоры» возможно обойти через существующие туннели удаленного доступа или через обслуживающие компьютеры, напрямую связанные с IED или станционной шиной. Поэтому необходимо принять меры в целях выявления угроз на подстанции для обеспечения быстрого реагирования и минимизации последствий.

В этой статье будут описаны требования безопасности подстанций МЭК 61850 и различные подходы для обнаружения угроз в этих сетях. Также будет описан подход, специально разработанный для подстанции МЭК 61850 и технологической шины.

Векторы атак на подстанцию

Определим кибератаку на подстанцию как событие, в ходе которого злоумышленник изменяет, ухудшает или отключает работу как минимум одного защитного, автоматического или управляющего устройства в пределах подстанции. Типичная подстанция может быть атакована через все пути, отмеченные номером (рис. 1). Взломщик может войти через соединение центра управления (1), как это произошло в ходе одной из кибератак в Украине, когда была изменена прошивка шлюзов (вызвав их разрушение).

Другая точка входа возможна через инженерные ПК (3), подключенные к оборудованию подстанции. Когда инженер подключает свой ПК к реле для изменения (защитных) настроек, вредоносные программы, размещенные на ПК, могут в свою очередь установить вредоносное ПО на реле аналогичным образом, как это произошло с ПЛК в ходе кибератаки вируса Stuxnet. Ноутбуки, используемые для тестирования системы МЭК 61850, часто напрямую подключаются к станционной шине, что также является потенциальным вектором для заражения интеллектуальных электронных устройств (IED) (4).

По этой причине предлагается использовать новые инструменты тестирования МЭК 61850, обеспечивающие кибербезопасное разделение между тестовым ПК и сетью подстанции. Само тестирующее устройство (5) также является потенциальным путем проникновения. Важно, чтобы производители тестовых комплектов вкладывали средства в усиление защиты своих устройств, чтобы злоумышленник не смог воспользоваться этим путем входа. Хранилище настроек (3a) и тестовых документов (4a) также может быть направлением для атаки. Этот сервер хранения данных, таким образом, также принадлежит к критическому периметру. Поэтому также имеет смысл реализовать отдельное, изолированное и защищенное решение дляуправления такими данными.

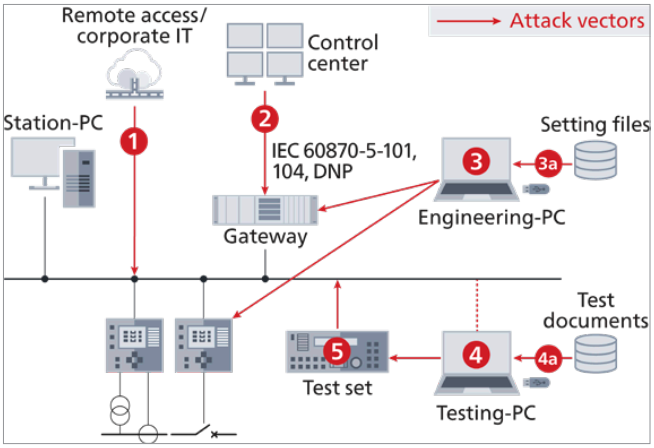

Рис. 1. Векторы атаки на подстанцию

Безопасность и МЭК 61850

Частым вопросом о кибербезопасности на цифровых подстанциях является: «Что случится, если злоумышленник подаст GOOSE-сообщение с командой отключения в станционную шину, как я могу предотвратить это?» Отвечая на этот вопрос мы не должны сосредотачиваться только на случае, когда злоумышленник имеет физический доступ к сети подстанции. Существует другой возможный сценарий: зараженный инженерный или тестовый ПК, подключенный к станционной шине, или даже зараженное IED может начать выдачу протокола GOOSE. Такие механизмы, как статус и порядковые номера в GOOSE-сообщении часто рассматриваются, как «механизмы безопасности».Однако, такие меры едва ли могут быть названы «механизмами безопасности», так как любой злоумышленник может перехватить текущий статус и порядковый номер и внедрить подходящие значения. Кроме того, MAC-адрес источника GOOSE пакета может быть легко подделан взломщиком. IED, получающее GOOSE сообщение, не имеет другого выбора, как отреагировать на первое GOOSE сообщение, полученное с корректным MAC адресом источника, и правильным

статусом/порядковым номером. То же самое, конечно, относится к счетчику отсчетов в выборочных значениях. Единственная реальная мера для предотвращения таких инъекционных атак – обеспечение подлинности и целостности сообщения, используя аутентификационные коды в конце GOOSE-сообщения, в соответствии со стандартами МЭК 62351-6. Благодаря этой мере отправляющее IED четко идентифицируется, и становится невозможным манипулировать содержимым GOOSE-сообщения. Следует отметить, что не требуется шифровать сообщение, чтобы воспользоваться этими возможностями. Для доставки и обслуживания этих аутентификационных ключей для каждого IED требуется наличие инфраструктуры управления ключами внутри подстанции. По этой причине эти механизмы безопасности GOOSE-протокола пока не получили широкого применения, но получат в будущем. То же самое относится к MMS и управлению доступом на основе ролей (RBAC).

Шифрование

Шифрование часто воспринимается как серебряная пуля в безопасности. Стандартом МЭК 62351 также предусматривается шифрование для GOOSE и MMS сообщений. Тем не менее, в среде подстанции существует только несколько приложений, где важна конфиденциальность сообщений. Если сообщения не могут быть подделаны (целостность) и отправитель может быть проверен (проверка подлинности), что достигается с помощью аутентификации в GOOSE и MMS протоколах, то нет необходимости шифровать сообщение. Одним из примеров, когда шифрование может быть необходимо, является передача маршрутизируемых GOOSE-сообщений (R-GOOSE) через незашифрованный канал связи. Шифрование только создает дополнительную нагрузку процессора IED, увеличивает время передачи GOOSE-сообщений и затрудняет сценарии тестирования, но в большинстве случаев не увеличивает защиту, уже обеспечиваемую кодами аутентификации. Шифрование также затрудняет последующий анализ записей трафика и препятствует применению таких подходов к мониторингу, как описанные ниже.

Защита в глубину

Большинство подстанций МЭК 61850, построенных до сих пор, не внедрили МЭК 62351. Даже на подстанциях, где применяются протоколы GOOSE и MMS с кодами аутентификации, зараженные устройства в сети могут по-прежнему заражать другие устройства или влиять на уровень работоспособности, нарушая систему связи. Поэтому в большинстве инфраструктурах безопасности рекомендуется использовать «системы обнаружения вторжений» (СОВ), термин, известный в классических ИТ системах, для обнаружения угроз и злонамеренных действий в сети. Такие системы обнаружения вторжений сейчас становятся все более распространенными в области систем электроснабжения.

Требования к СОВ на подстанциях

На подстанции МЭК 61850 система обнаружения вторжений должны быть подключена, как показано на рис. 1. Порты зеркалирования на всех соответствующих коммутаторах пересылают копию всего сетевого трафика в СОВ. СОВ проверяет весь сетевой трафик, передаваемый через эти коммутаторы. Чтобы иметь возможность анализировать наиболее важный трафик между шлюзом и IED, СОВ как минимум должна быть подключена к коммутатору рядом со шлюзом и всеми остальными критическими точками входа в сеть. Коммутаторы уровня ячейки, как правило, не нужно закрывать, так как обычно оттуда исходит только

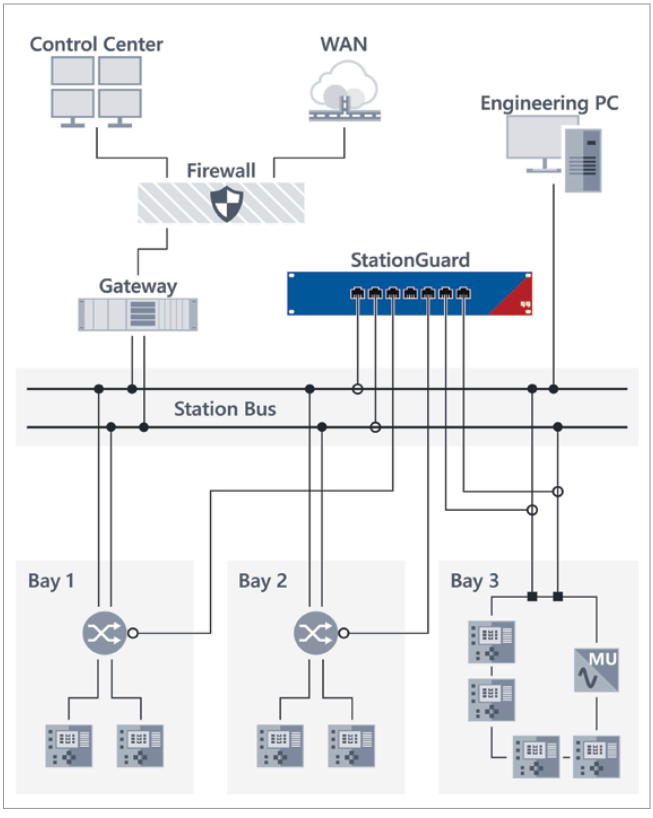

Рис. 2. Структура подстанции с подключенной IDS

многоадресный трафик (GOOSE, Sampled Values). Чтобы обеспечить анализ всего одноадресного трафика во всех ветвях сети необходимо, чтобы все коммутаторы были отзеркалены в СОВ, что не всегда возможно, если используются чипы коммутаторов, встроенные в IED.

Киберугрозы могут быть обнаружены путем детального функционального мониторинга. Однако, системы обнаружения вторжений из классического IT не подходят для подстанции. В то время как классическая ITбезопасность связана с высокопроизводительными серверами с миллионами одновременных подключений, IT безопасность подстанции имеет дело с устройствами с ограниченными ресурсами, специализированными операционными системами, требованиями в реальном времени и специализированными протоколами резервирования. Например, атака типа «отказ в обслуживании» на службу связи IED зачастую требует только 10 подключений, т.е. 10 Ethernet пакетов, чтобы быть успешной. Просто потому, что сценарии «отказа в обслуживании» не учитывались в старые добрые времена, когда эти устройства и протоколы были разработаны. Кроме того, известно лишь небольшое количество кибератак на подстанции, но даже первый случай новой атаки может иметь серьезные последствия. Таким образом, СОВ подстанции должна быть в состоянии обнаружить атаки без каких-либо предварительных знаний о том, как атака может выглядеть. Этот подход значительно отличается от подхода антивирусного сканера, у которого есть список вирусных сигнатур для поиска.

Системы, основанные на обучении

Чтобы быть в состоянии обнаружить неизвестные атаки, многие поставщики используют подход «стадии обучения». Такие системы обращают внимание на частоту и время определенных маркеров протокола, чтобы попытаться изучить обычное поведение системы. После завершения этапа изучения сработает сигнализация, если один из маркеров значительно выходит за пределы ожидаемого диапазона. Это приводит к тому, что ложные сигналы тревоги появляются при каждой ситуации, которая не возникла во время обучения, например, при срабатывании защит или автоматики, необычных действиях по переключению или при текущем обслуживании и тестировании. Так как эти системы не понимают семантику протоколов, сообщения о тревоге выражаются в терминах деталей технического протокола. Следовательно, сигнализации

Рис. 3. Система StationGuard импортирует файл SCL с описанием подстанции для создания полной модели системы

могут быть проверены только инженером, разбирающимся в деталях протокола МЭК 61850 и знакомым с IT-безопасностью сети. Инженер, проверяющий сигнализацию, также должен знать об эксплуатационной ситуации, чтобы оценить, соответствует ли определенное протокольное событие МЭК 61850 правильному поведению. Поэтому, возникает большое количество ложных сигналов тревоги, каждый из которых нуждаются в проверке высококвалифицированным персоналом. Это часто приводит к тому, что сигналы тревоги игнорируются или отклоняются без их изучения, и в конечном итоге СОВ отключается.

Подход

Для подстанций МЭК 61850 вся система автоматизации, включая все устройства, их модели данных и их шаблоны коммуникации описаны в стандартизованном формате SCL (язык системной конфигурации). Файлы описания конфигурации системы (SCD), как правило, также содержат информацию о первичном оборудовании и, всё чаще, в них присутствует даже однолинейная схема подстанции.Эта информация позволяет применить иной подход для обнаружения вторжений: Система мониторинга может создавать полную системную модель системы автоматизации и энергоснабжения и может сравнивать каждый пакет в сети с моделью действующей системы. Даже переменные, содержащиеся в переданных (GOOSE, MMS, SV) сообщениях, могут быть оценены с учетом ожидаемых значений, определенных на основе системной модели. Этот процесс возможен без необходимости этапа изучения, просто путем конфигурации из SCL. Этот подход реализован в новой системе мониторинга функциональной безопасности StationGuard от OMICRON.

Мониторинг функциональной безопасности

По сути, для обнаружения киберугроз в сети производится очень подробный функциональный мониторинг. Благодаря высокому уровню детализации мониторинга выявляются не только угрозы кибербезопасности, такие как искаженные пакеты и недопустимые управляющие воздействия, но также и сбои связи, проблемы синхронизации времени и, следовательно, также (определенные) повреждения оборудования. Если однолинейная схема известна системе и значения измерений можно наблюдать в сообщениях MMS (или даже через Sampled Values), то возможности того, что можно проверить, безграничны.

Например, только для GOOSE протокола предусмотрены 33 кода тревоги для случаев, когда что-то может пойти не так. Они варьируются от простых сбоев stNum / sqNum (как описано выше) до более сложных проблем, таких как превышение времени передачи. Последнее обнаруживается путем точного измерения разницы между отметкой времени входа (EntryTime) в сообщении и моментом времени входа в StationGuard. Если это время передачи по сети значительно превышает 3 мс для защитных GOOSE (см. МЭК 618505), это указывает на проблему в IED, сети или синхронизации времени. Что сделано для коммуникаций MMS? Из модели системы (из SCL) известно, какие логические узлы управляют каким основным оборудованием. Таким образом, можно различить правильные/неправильные и критические/некритические действия. При переключении выключателя и переключении в тестовый режим МЭК 61850 используется та же последовательность в протоколе MMS (выбор перед исполнением), но воздействие на оборудование подстанции совсем другое. Поэтому, если тестовый ПК из рис. 2 включает тестовый режим в реле, это возможно законное действие во время технического обслуживания, но, скорее всего, тестовый ПК не имеет прав на управление выключателем. Этот пример будет более подробно рассмотрен в следующих параграфах.

Разработано вместе с инженерами РЗА

Исследование этого подхода началось в 2011 году. Спин-оффы этой концепции, круглосуточный функциональный контроль SV, GOOSE и PTP синхронизации времени, применяются в распределенном гибридном анализаторе (OMICRON DANEO 400) с 2015 года. Более того, обратная связь от многих других энергокомпаний по всему миру, а также некоторые экспериментальные установки нашли свое отражение в нашей разработке. В 2018 году одна из первых экспериментальных установок была установлена на подстанции 110 кВ швейцарской генерирующей и распределительной электростанции CKW и работает с тех пор. На рис. 4 показана установка на новой подстанции в 2019 году. В этом случае весь трафик «основного» коммутатора был отзеркален на StationGuard. Это обеспечивает, что весь обмен данными между шлюзом и всеми устройствами ИЭУ является видимым. Поскольку удаленные сервисные соединения также проходят через этот коммутатор, StationGuard также проверяет весь этот трафик. Поскольку связь GOOSE является многоадресной, а сетевая настройка позволяет это, все GOOSE сообщения из IED в ячейках подстанции также видны для StationGuard.

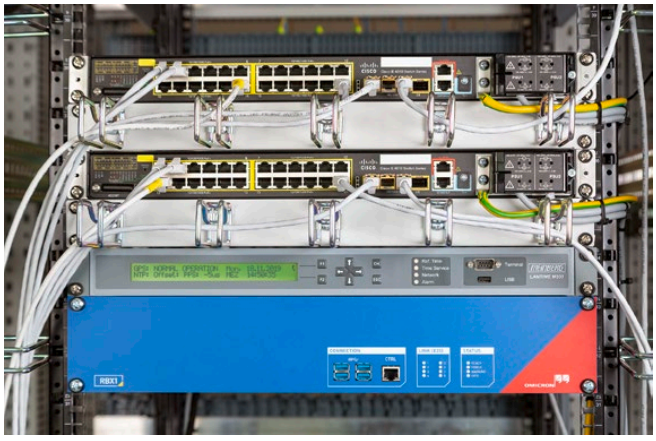

Рис. 4. StationGuard установлена на новой подстанции 110 кВ, 2019

Дисплей тревожной сигнализации

Помимо избежания ложных срабатываний, также крайне важно, чтобы доставленные сообщения о тревоге были понятны для инженеров, которые отвечают за работу систем защиты, автоматики и сети на подстанции. Это позволяет сократить время реакции, поскольку часто эти аварийные сигналы запускаются инженерами, работающими на подстанции (или удаленно). Кроме того, это позволяет инженерам по безопасности и PAC-инженерам сотрудничать при отслеживании событий на подстанции.

На рис. 5 показан снимок экрана с графическим отображением тревоги: Сигнал тревоги отображается в виде стрелки от активного участника (ноутбук 1), выполняющего запрещенное действие, к «жертве» действия – контроллеру ячейки в ячейке Q01.

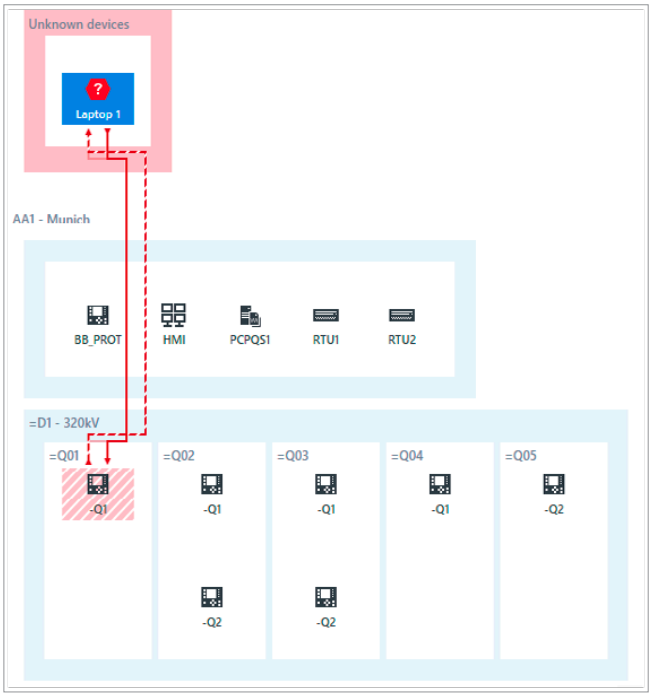

Рис. 5. Графическое отображение сигнала тревоги IDS вместо списка событий

На рис. 6 показаны подробности об этом сигнале тревоги: Недопустимая операция управления (с использованием MMS последовательности) силовым выключателем от неизвестного ПК. Кроме того, этот ноутбук также подключается по протоколу производителя и загружает файлы через MMS. Детали сообщения раскрывают дополнительную информацию, например, имя загруженного файла.

Рис. 6. Детали для рисунка 5: неизвестный ноутбук несанкционированно контролировать силовой выключатель

Реестр оборудования

Все устройства, взаимодействующие в сети, обнаруживаются и отображаются. Для каждого обнаруженного устройства информация из перехваченного сетевого трафика агрегируется с информацией из SCL. Это позволяет показать производителя, модель и версию микропрограммного обеспечения там, где это возможно. На рисунке 7 показана агрегированная информация для объекта сети, включая описание и имя устройства из файла SCD проекта.

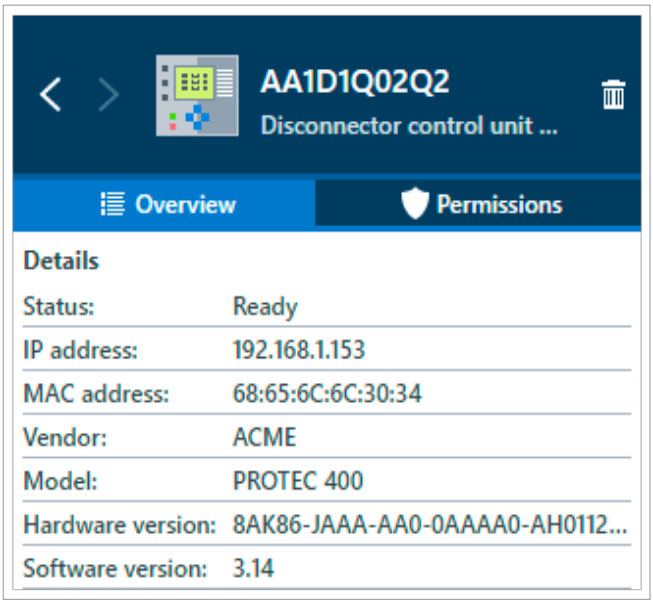

Рис. 7. Объединение информации об активах из сетевого трафика и SCL

Конфигурация

Как упоминалось ранее, этап обучения не требуется. Обнаружение начинается сразу с момента включения системы и не может быть выключено по соображениям безопасности. До тех пор, пока не будет загружен SCD-файл подстанции, все IED будут обнаружены и представлены как неизвестные устройства. После загрузки SCD-файла IED будут обозначены как известные устройства, а структура подстанции собрана в схему «нулевой линии» (‘zero-line’ diagram) термин, введенный для описания способа отображения коммуникаций на подстанции в StationScout от OMICRON. Конфигурация также может быть подготовлена в офисе, а затем поочередно установлена на местах вместе с быстрым вводом в эксплуатацию. Если не все IED были объединены в один файл (такое происходит), дополнительные устройства IED также можно импортировать по одному. После завершения импорта пользователь может добавить роли, такие как «Тестовый ПК», «Инженерный ПК» и т. д. любым оставшимся неизвестными устройствам.

Что происходит в случае сигнала тревоги?

Важно отметить, что StationGuard является полностью пассивной. Если действие «не разрешено», она просто запустит тревогу. Этот сигнал тревоги может быть передан шлюзу/RTU и центру управления или отдельной системе, собирающей оповещения о безопасности, известной как система управления информацией о безопасности и событиями безопасности (SIEM), использующую протокол Syslog. StationGuard активно не реагирует и не вмешивается в работу подстанции. В зависимости от выбранного аппаратного варианта, определяемые пользователем двоичные выходы могут быть подключены непосредственно к RTU. В этом случае сигнализация тревоги происходит без сетевой связи, и сигналы тревоги могут быть интегрированы в обычный список сигналов SCADA, как и любой другой проводной сигнал станции.

Кибербезопасность самой СОВ

Как мы знаем из кинофильмов, грабители всегда сначала атакуют систему охранной сигнализации. Так как насчет безопасности этой системы сигнализации? Важным аспектом является то, что используется автономная защищенная аппаратная платформа, а не виртуальная машина. Оба варианта аппаратного обеспечения StationGuard, мобильный (MBX1) и 19-дюймовый вариант для постоянной установки (RXB1), имеют одинаковую защиту платформы. Они оба имеют защищенный чип криптопроцессора в соответствии с ISO/МЭК 11889. Это позволяет хранить криптографические ключи не на флэш-накопителе , а в отдельном чипе, защищенном от подделки. Установка сертификатов OMICRON в этот чип во время производства создаёт безопасную измеряемую цепь загрузки. Это означает, что каждый шаг в процессе загрузки прошивки проверяет подписи следующего модуля или драйвера для загрузки и гарантирует, что в устройстве может выполняться только подписанное OMICRON программное обеспечение.

Внутренняя память устройства зашифрована ключом, уникальным для этой единицы оборудования, и защищено внутри крипточипа. Поскольку никто (включая OMICRON) не знает этот ключ, все данные на устройстве будут потеряны при замене оборудования при ремонте. Многие другие механизмы гарантируют, что процессы на устройстве не могут быть атакованы или использованы не по назначению, поэтому подход «защиты в глубину» также применяется глубоко в программном обеспечении, работающем на устройстве. Рассмотрение всех этих механизмов было бы полноценной темой для другой статьи.

Рис. 8. StationGuard, вид спереди, 48 см стационарный вариант RBX1

Краткие выводы

Подстанции являются потенциальным объектом для кибератак. Если злоумышленник может повлиять на одну или несколько подстанций, это может иметь серьезные последствия для сети. Поэтому эффективные меры кибербезопасности должны быть реализованы не только в центрах управления, но и на подстанциях. В системе обнаружения вторжений для подстанций МЭК 61850 StationGuard реализован подход, который обеспечивает небольшое количество ложных срабатываний тревоги и все еще низкие издержки конфигурации благодаря возможностям SCL.Эта система обнаруживает не только угрозы безопасности, но и функциональные проблемы IED и коммуникаций МЭК 61850, что также полезно на этапах FAT и SAT. Система обнаружения вторжений, которая отображает обнаруженные события на языке инженеров по защите, автоматизации и управлению, имеет преимущество в том, что инженеры РЗА и инженеры по безопасности могут работать вместе, чтобы найти причину событий.

Рис. 9. StationGuard, вид сзади, 48 см стационарный вариант RBX1

Более подробная информация доступна на сайте: www.omicronenergy.com/stationguard