ПРОЕКТИРОВАНИЕ И ВВОД В ЭКСПЛУАТАЦИЮ АРХИТЕКТУРЫ ЗАЩИТЫ СЕТИ ПОДСТАНЦИИ

Андреас Клин (Andreas Klien)[1], Янн Гостели (Yann Gosteli)[2], Штефан Маттман (Stefan Mattmann)[3]

[1]OMICRON electronics GmbH, Клаус, Австрия (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Люцерн, Швейцария (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Люцерн, Швейцария (stefan.mattmann@ckw.ch)

Ключевые слова: КИБЕРБЕЗОПАСНОСТЬ, IEC 61850, СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, СИСТЕМА АВТОМАТИЗАЦИИ ПОДСТАНЦИЙ

Краткое изложение

Кроме центров управления, традиционно считающихся главным объектом атак киберпреступников, пристальное внимание аудиторов инженерных сетей и систем кибербезопасности все чаще направлено на подстанции — потенциальные «точки входа» для кибератак. Слабым звеном в системе безопасности являются процессы, связанные со вводом в эксплуатацию систем защиты и управления, а также реализацией удаленного доступа при проведении технического обслуживания. Исходя из вышеизложенного, именно архитектура системы защиты и управления нуждается в самой тщательной проверке на предмет устойчивости к угрозам. В связи с этим Centralschweizer Kraftwerke AG (CKW), швейцарская компания по производству и распределению электроэнергии, в 2016–2017 годах запустила проект по разработке новой эталонной архитектуры для своих вторичных систем. Эта архитектура предусматривает создание активных помех на том участке, на который направлена кибератака, и обеспечивает высокий уровень защиты систем, никоим образом не влияя на их эксплуатационные качества. Дизайн архитектуры отличается многоэтапной проверкой безопасности, в том числе несколькими уровнями межсетевой защиты. В обеспечении безопасности участвует также система обнаружения вторжений (IDS). Выбрать подходящую IDS для подстанций оказалось непростой задачей, поскольку многие системы не соответствуют требованиям сетей подстанций. В начале данной статьи перечисляются наиболее важные векторы атак на подстанции, после чего следует описание архитектуры безопасности, впервые реализованной компанией CKW в совершенно новом проекте подстанции на 110 кВ. В заключительной части приводится пример выбора надлежащей IDS для подстанции, а также излагаются выводы по результатам заводских приемочных испытаний в рамках данного проекта.

1. Общие сведения

1.1. Векторы кибератак на подстанции

Здесь и далее под кибератакой на подстанцию подразумевается событие, в ходе которого злоумышленник изменяет, ухудшает или прерывает работу как минимум одного защитного, автоматического или управляющего устройства в пределах подстанции. Чтобы добиться такого эффекта, злоумышленник прибегает к направленной атаке и делает это одним из способов, изображенных ниже на рис. [1].

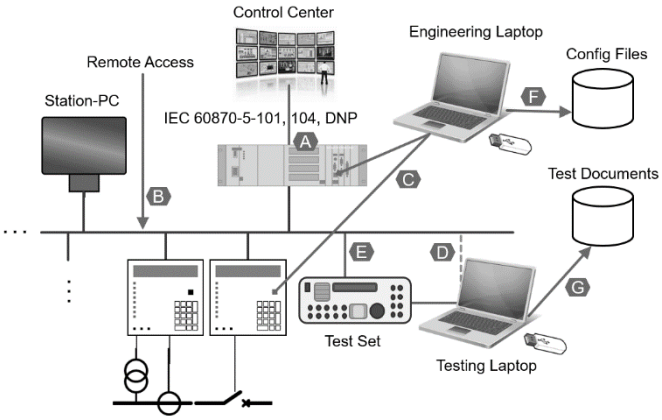

Рис. 1 Векторы кибератак на подстанции [1]

Атака может осуществляться по следующей схеме: сначала злоумышленник старается подключиться к центру управления (**A**). Так, например, произошло в Украине во время первой кибератаки, когда санкционированная извне модификация встроенного ПО шлюзов

вызвала серьезные сбои в их работе [2]. Кроме того, взломщик может действовать через удаленное подключение (**B**), что случилось в Украине во время второй кибератаки в 2016 г. [3] и при 'TRITON' кибератаке на PLC критической инфраструктуры [4].

Другая точка входа — через инженерные ПК (**C**), подключенные напрямую к оборудованию либо сети подстанции. Когда инженер РЗА подключает свой ПК к реле для изменения уставок (защиты), вредоносная программа на ПК может, в свою очередь, установить вредоносную программу на реле так, как это было сделано с PLC в ходе нашумевшей кибератаки Stuxnet в 2010 г. [5].

Ноутбуки, используемые для испытания систем IEC 61850 (**D**), часто подключаются к станционной шине напрямую, что также является возможным способом заражения интеллектуальных электронных устройств (IED). По этой причине были созданы новые, удовлетворяющие требованиям IEC 61850 испытательные установки, которые обеспечивают кибербезопасное разделение между испытательным ПК и сетью подстанции. При этом возможным путем входа также остается сама испытательная устрановка (**E**). В связи с этим важно, чтобы производители испытательного оборудования инвестировали в обеспечение кибербезопасности своих устройств. Это снизит вероятность использования злоумышленниками данного пути входа.

Хранилище настроек (**F**) и документов испытаний (**G**) также является потенциальным объектом заражения. Следовательно, сервер или хранилище также являются важными и уязвимыми элементами, поэтому они не должны размещаться в ИТ-зоне офиса. Поэтому имеет смысл внедрить отдельное, изолированное и защищенное решение для управления данными такого рода.

2. Новая версия архитектуры подстанции

2.1. Самые современные наработки в области кибербезопасности эксплуатационных технологий

Швейцарская ассоциация производителей электроэнергии VSE создала рабочую группу по безопасности эксплуатационных технологий (ЭТ). По результатам своей деятельности эта группа опубликовала документ, содержащий отраслевые инструкции, — «Справочник по основной защите эксплуатационных технологий в энергосистемах». Его авторы ссылаются на «Концепцию кибербезопасности для важнейших объектов инфраструктуры», разработанную Национальным институтом стандартов (NIST) [7]. Данный документ постоянно адаптируется и дополняется новыми материалами, а последняя обновленная редакция была выпущена в 2018 году. Концепция NIST основана на предположении, что обеспечить киберзащиту на 100 % невозможно в принципе. Приложив достаточно усилий, осведомленный злоумышленник способен обойти все предпринятые меры безопасности. Соответственно в концепции NIST изложена схема выявления вторжений, состоящая из пяти этапов: распознавания, защиты, выявления, реагирования и восстановления. Итак, первоочередным этапом является идентификация векторов атаки (распознавание). Об этом речь шла в предыдущем разделе данной статьи. На следующем этапе (защита) уже можно принимать меры противодействия атаке. Если это не остановит злоумышленника, следует перейти к более радикальным действиям, а именно: выявить атаку (выявление) и — в идеале — предпринять ответные шаги (реагирование) с тем, чтобы система как можно быстрее восстановилась до нормального состояния (восстановление). Опыт, приобретенный на этапах выявления и реагирования, позволяет идентифицировать новые векторы атак, принять новые ответные меры — и таким образом пройти всю процедуру заново.

В руководстве с отраслевыми инструкциями, выпущенном в Швейцарии, большое внимание уделяется взаимодействию людей, технологий и процессов внутри организации. Например, постоянный мониторинг или обнаружение вторжения (выявление) имеют смысл лишь в том случае, если на сообщения об аварийной

ситуации реагируют надлежащим образом. Поэтому такие сообщения должны быть понятны всем, кто задействован в процессе реагирования, — инженерам по эксплуатационным технологиям (operation technology, OT) и специалистам ИТ-безопасности. В противном случае реагирование будет неэффективным. Кроме того, если IDS слишком часто издает сигналы ложной тревоги, со временем на них просто перестанут обращать внимание.

2.2. Проекты компании CKW в области кибербезопасности эксплуатационных технологий [6]

В последние годы компания CKW уделяет особое внимание вопросу обеспечения безопасности систем управления и защиты подстанций. Выбор приоритетов обусловлен не только упомянутыми выше швейцарскими отраслевыми инструкциями, но и, прежде всего, уровнем безопасности OT согласно исследованиям, проведенным компанией CKW в течение последних лет. В ходе таких исследований были обнаружены уязвимые участки как в сетях, так и в технологиях управления, используемых на подстанциях. К примеру, было обнаружено использование незащищенных переходов между зонами и весьма ненадежных методов удаленного подключения к управляющим компьютерам. Кроме того, не было возможности установить, подвергается ли сеть подстанции кибератаке сейчас или присутствуют ли в сети подозрительные действия, которые могут предшествовать атаке.

Основываясь на этих выводах, компания CKW задалась целью устранить наиболее существенные уязвимости и ужесточить требования к дальнейшим наработкам в области архитектуры подстанций. Таким образом результаты исследований нашли воплощение в новом стандарте, разработанном CKW для проектирования подстанций.

Помимо работы над стандартом, компания CKW нашла возможность принять участие в швейцарской рабочей группе по составлению упомянутого выше руководства по безопасности OT. Такой обмен данными позволил CKW последовательно внедрить выводы рабочей группы в свои собственные стандарты проектирования.

В 2016–2017 гг. проектная группа компании CKW начала работы по созданию абсолютно новой подстанции US Rothenburg, которую введут в эксплуатацию в 2020 г. В этом проекте был применен новый стандарт архитектуры защиты, разработанный CKW, а также реализованы новейшие рекомендации из руководства по безопасности OT (Швейцария). Чтобы эти комплексные меры безопасности можно было внедрить на практике, компания CKW решила самостоятельно реализовать сетевую архитектуру и настроить конфигурацию коммутатора.

2.3. Сетевая архитектура

Архитектура сети подстанции US Rothenburg предполагает установку в каждой зоне барьеров, задача которых — затруднить атаку на рабочую сеть. На рис. Figure 2 показана схема сети подстанции US Rothenburg.

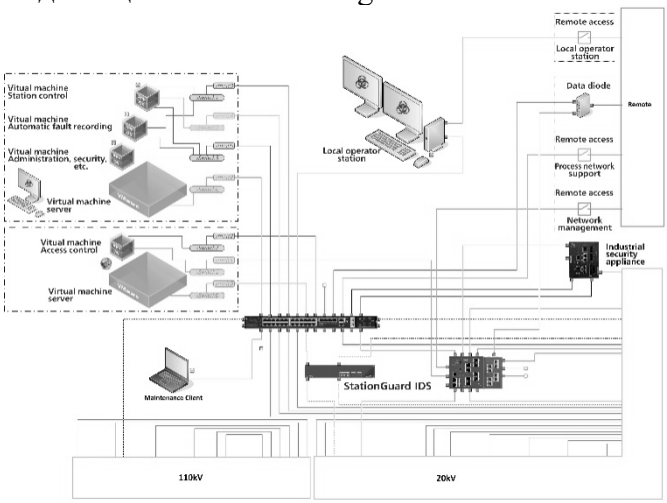

Рис. 2 Архитектура сети подстанции US Rothenburg [6]

Данная архитектура предусматривает полный комплект защитных мер в ответ на все векторы атаки, описанные в разделе 1.1 данного документа. Самое пристальное внимание было уделено вопросу удаленного подключения к сетям предприятия. Это удаленное подключение не только защищено с помощью брандмауэров и туннелирования, но и отключено по умолчанию. Оно активируется лишь в случае возникновения объективной необходимости в таком подключении. Это означает, что для

обеспечения удаленного доступа требуется несколько человек, так же как и для двухуровневой авторизации.

Связь системы диспетчерского контроля и сбора данных (SCADA) с центром управления осуществляется с помощью последовательного протокола по стандарту IEC 60870-5-101. Вся процедура доступа к устройствам подстанции для их технического обслуживания проводится исключительно через специальные, должным образом защищенные рабочие станции. Эти станции виртуализированы и расположены в пункте централизованного управления. Активация удаленного доступа также осуществляется удаленно.

Серверы системы SCADA, системы регистрации повреждений и системы безопасности виртуализируются и функционируют на центральном компьютере, расположенном локально на подстанции. Даже локальная станция с интерфейсом «человек-машина» (ИЧМ) может получить доступ к этим системам только за счет подключения к удаленному рабочему столу через дополнительный локальный брандмауэр. Используется механизм управления доступом на основе ролей (RBAC). Это означает, что пароль является индивидуальным не в отношении конкретного устройства, а в отношении конкретного пользователя. Преимущество заключается в том, что инженер может использовать свой пароль для подключения ко всем подстанциям. Если сотрудник компании увольняется, его учетную запись пользователя можно легко удалить, при этом пароль менять не нужно. Такая система управления пользователями функционирует на базе центрального сервера Active Directory (AD) и локального сервера RADIUS, расположенных на подстанции. Вход пользователей в систему осуществляется с помощью AD, которая дает необходимые разрешения. При необходимости доступ к центральному серверу AD можно активировать на главном компьютере. Кроме того, ко всем IED следует подключаться отдельно, вводя индивидуальные имя пользователя и пароль. Таким образом, IED используют локальный сервер RADIUS для авторизации пользователя, проверки пароля и получения разрешений, данных этому пользователю. Это правило касается доступа как к устройствам, оснащенным средствами разработки, так и к операциям, выполняемым на дисплее IED. Стандартные пароли не используются.

Все подключения ПК к сети подстанции защищены. Это достигается, в частности, путем настройки брандмауэра Windows в соответствии с матрицей связи подстанции, а также — в зависимости от роли этого клиента — посредством блокирования функций неиспользуемых операционных систем.

Для повышения уровня безопасности управление доступом к сети осуществляется через обход аутентификации по MAC-адресу, а значит, к сетевому коммутатору можно подключить только зарегистрированные устройства.

Кроме того, в случае неисправности коммутатор должен распознавать поставляемые со склада резервные устройства и давать разрешение на их подключение. Списки контроля доступа в сетевых коммутаторах подстанции и в брандмауэре настроены так, что позволяют определить, какому устройству разрешено подключаться к тому или иному устройству той же сети посредством используемого протокола и порта коммутатора.

Сеть станционных шин, а также сеть для конфигурации и техобслуживания разделены как логически (VLAN), так и физически. Это означает, что на каждом IED обмен сообщениями MMS и GOOSE по стандарту IEC 61850 осуществляется в сетевом интерфейсе, отличном от интерфейса доступа, предназначенного для выполнения технического обслуживания. Помимо этого, вся сеть станционных шин разделена на сегменты посредством брандмауэра. Это такие сегменты:

- 110 кВ (GOOSE и MMS)
- 20 кВ (GOOSE и MMS)
- Локальный интерфейс «человек-машина»
- Шлюз протокола
- Вспомогательные системы
- Сети техобслуживания для IED и клиентов
- Управляющая сеть, виртуальная машина, RADIUS

Связь между подстанцией и зонами высокоуровневой сети дополнительно

защищена шлюзом однонаправленной передачи данных. Благодаря этому шлюзу однонаправленной передачи данных осуществляется запуск только исходящих сеансов связи, что позволяет достичь более высокого уровня безопасности.

Система обнаружения вторжений (IDS) отслеживает весь сетевой трафик в системе с помощью белого списка. При выявлении неизвестного трафика, отсутствующего в белом списке, по умолчанию выдается аварийный сигнал. IDS передает этот сигнал в центр управления через RTU и в центр управления безопасностью - посредством специализированных протоколов для регистрации аварийных сигналов.

3. Обнаружение вторжений

В основе разработанной компанией CKW архитектуры безопасности лежит создание сегментов сети, разделенных при помощи брандмауэра. Конфигурация брандмауэра определяет с точностью, какие именно протоколы могут использоваться для связи между всеми сегментами сети. Однако для атаки на устройства и их заражения могут быть использованы также протоколы, разрешенные брандмауэром, например упомянутые в стандарте IEC 61850 MMS/GOOSE, и определяемые производителями инженерные протоколы. При таком сценарии событий несанкционированные действия необходимо выявлять на ранней стадии. Для этой цели в эталонной архитектуре CKW было решено использовать IDS.

Для анализа наиболее важного трафика, осуществляемого, например, при обмене данными между шлюзом и IED, в IDS должен отображаться как минимум трафик шлюза (полностью). Коммутаторы на уровне ячейки обычно не нуждаются в защите, так как они передают только многоадресный трафик (GOOSE, SV). Кроме того, для анализа всего одноадресного трафика во всех ветвях сети желательно, чтобы все коммутаторы были зеркально отображены в IDS.

В разработанной CKW архитектуре IDS подключается к зеркальным портам на всех сетевых коммутаторах. Это означает, что IDS анализирует трафик на станционной шине, а также трафик, поступающий извне до и после прохождения через брандмауэры.

3.1. Требования к IDS подстанций

Выбор подходящей для подстанции IDS оказался нетривиальной задачей. Одним из важных требований, выдвигаемых к IDS, было то, чтобы с этими системами могли без труда взаимодействовать как инженеры РЗА и управления, отвечающие за все IED, так сетевые инженеры, которые несут ответственность за сетевое оборудование. Чтобы процесс реагирования на аварийные сигналы осуществлялся должным образом, следует наладить связь между аварийными сигналами IDS с событиями на подстанции и журналами событий в ИЧМ. Следовательно, IDS должна обеспечивать обзор конкретных аспектов работы подстанций, а не только терминологии информационной безопасности.

До недавнего времени IDS использовали только два основных метода: сигнатурный и метод, основанный на обучении.

В основе сигнатурного метода лежит работа с черным списком так, как это делает стандартный компьютерный сканер вирусов. Система сканируется на предмет шаблонов известных вирусов и вредоносных программ. Трудность состоит в том, что известно лишь небольшое количество кибератак на подстанции, тогда как даже первая атака может иметь серьезные последствия. IDS подстанции должна быть способна обнаруживать атаки без каких-либо предварительных сведений о том, как может выглядеть атака.

Поэтому большинство IDS используют метод, основанный на обучении. IDS просматривает общие параметры различных протоколов и вычисляет усредненные значения и частоту для каждого параметра.

После этого в нормальном режиме работы система издает сигнал тревоги каждый раз, когда уровень обмена данными в сети значительно отклоняется от усредненного, полученного путем обучения системы. В результате операторы получают сигналы ложной тревоги в связи с каждым событием, которое отсутствовало на этапе обучения системы. В их числе, к примеру, срабатывания РЗА, операции переключения или плановые

испытания защиты. Поскольку система не знает значения телеграмм в сети, сообщения об аварийной ситуации относятся к общим параметрам протокола, таким как MMS confirmed-write-response failed. В итоге возникает большое количество сигналов ложной тревоги, каждый из которых требует проверки ИТ-специалистами и специалистами по IEC 61850. Для компании CKW столь трудоемкий процесс реагирования оказался неприемлемым.

3.2. Применяемый метод работы IDS

Вся система автоматизации подстанций стандарта IEC 61850 со всеми IED, моделями данных и схемами связи описана в стандартизированном формате SCL. Эта информация позволяет использовать другой подход для обнаружения вторжений: система мониторинга может смоделировать систему автоматизации подстанции и сравнить каждый пакет в сети с моделью действующей системы. Даже переменные, содержащиеся в сообщениях (GOOSE, MMS, SV), можно оценить в соответствии с ожидаемыми переменными из модели системы. Таким образом формируется белый список для данной модели системы. После этого обнаружение пакетов, не соответствующих ей, вызовет сигнал тревоги. Выбранная компанией CKW модель IDS работает именно по такому принципу (OMICRON StationGuard).

Преимущество данного принципа заключаются в том, что он обеспечивает выявление не только киберугроз, таких как искаженные пакеты и запрещенные действия MMS-управления, но и сбоев связи, проблем синхронизации во времени и, следовательно, определенных неполадок в работе оборудования. В случае обнаружения этих дефектов система издает сигнал тревоги.

На основе сведений из раздела файла SCL, посвященного подстанции, можно автоматически создать обзорную диаграмму подстанции с отображением аварийных сигналов. Такой способ отображения позволяет определить, было ли действие, вызвавшее аварийный сигнал, намеренным. Например, данное событие может быть вызвано действиями инженера при проведении испытания или же вредоносной активностью на зараженном ноутбуке, с помощью которого проводится тестирование.

На момент написания этой статьи в Ротенбурге (США) уже прошли заводские приемочные испытания и начат запуск архитектуры в действие. На стадии заводских приемочных испытаний конфигурация сети должна быть практически завершена. Это дает возможность проверить, выполняет ли архитектура свои задачи. Кроме того, выяснилось, что IDS нужна поддержка маршрутизации, выполняемой на нескольких уровнях брандмауэров. Многократное дублирование трафика до и после прохождения брандмауэров может усложнить отображение сигналов в IDS. Корректное выполнение такого сценария зависит от того, правильно ли выбрана IDS. Создание матрицы связи для конфигурации брандмауэра также требует больших усилий, поскольку это можно сделать исключительно вручную. Однако благодаря тому, что в IDS уже используется импортированный из файла SCL белый список, в будущем создание матрицы связи, возможно, удастся автоматизировать.

4. Выводы и перспективы

Если действия злоумышленника затронут одну или несколько подстанций, это может серьезно сказаться на работе всей сети. Существует ряд способов обойти брандмауэр и, соответственно, несколько векторов атаки на подстанции. Разработанная компанией CKW архитектура защиты подстанций позволяет реализовать многочисленные ответные меры, направленные против векторов атак, описанных в этой статье. Указанные меры обеспечивают высокий уровень безопасности, в то же время позволяя эффективно проводить процедуры по техническому обслуживанию и проектированию с использованием удаленного доступа. В основе данной архитектуры лежит обнаружение вторжений в ядре сети. На подстанциях стандарта IEC 61850 для обнаружения вторжений можно использовать файл SCL, служащий для автоматического создания белого списка всего разрешенного сетевого трафика. Кроме того, такой метод позволяет отображать обнаруженные события в формате, понятном инженерам систем защиты, автоматизации и

управления. Совместно со специалистами по безопасности они смогут эффективнее определить причину того или иного события.

Чем совершеннее архитектура, тем, естественно, выше уровень кибербезопасности. Так, в частности, в систему можно встроить функцию управления доступом к сети на основе сертификатов в соответствии со стандартом 802.1X [8] вместо применяемого в настоящее время метода на основе MAC-адреса. Однако для этого нужно, чтобы большее количество IED поддерживало стандарт 802.1X. На данный момент число таких устройств весьма незначительно. В последующих статьях, как ожидается, будут отображены итоги ввода данного проекта в эксплуатацию и результаты выполненных в будущем на этой подстанции исследований, касающихся уровня безопасности и проницаемости.

5. Литература

[1] Klien, A.: New approach for detecting cyber intrusions in IEC 61850 substations, PAC World Conference Europe, Глазго, 2019 г.

[2] Analysis of the Cyber Attack on the Ukrainian Power Grid, SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, по состоянию на ноябрь 2019 г.

[3] WIN32/INDUSTROYER – A new threat for industrial control systems, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, по состоянию на ноябрь 2019 г.

[4] Threat Research – Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, по состоянию на ноябрь 2019 г.

[5] D. Kushner: The Real Story of Stuxnet
How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program, IEEE Spectrum, февраль 2013 г.

[6] Gosteli, Y., Klien, A.: Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg, bulletin.ch, 2019 г., № 6, стр. 50–52.

[7] NIST: Framework for improving critical infrastructure cybersecurity, version 1.1, Национальный институт стандартизации и технологии, апрель 2018 г.

[8] IEEE: 802.1X-2010 – IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control, международный стандарт, февраль 2010 г.

OMICRON — ведущий мировой производитель высокотехнологичного испытательного и диагностического оборудования для предприятий электроэнергетической отрасли. Устройства OMICRON позволяют с высокой точностью оценивать состояние первичного и вторичного оборудования энергосистем. Компания также предоставляет услуги по вводу устройств в эксплуатацию, тестированию и диагностике оборудования, консультированию и обучению персонала.

Клиенты из более чем 160 стран доверяют опыту компании OMICRON, используя высококачественное передовое оборудование ее производства. Сервисные центры компании расположены по всему миру, что позволило создать обширную базу знаний и обеспечить всестороннюю поддержку клиентов. Благодаря всем этим преимуществам, а также развитой дистрибьюторской сети компания прочно занимает лидирующие позиции в области электроэнергетики.

Посетите наш веб-сайт, чтобы узнать больше о компании и получить контактную информацию по региональным офисам.

www.omicronenergy.com