Серия PacT

TransferPacT Active Automatic (с ЖКД)
TransferPacT Automatic (поворотный)

Руководство по кибербезопасности

Pact series — автоматические прерыватели и переключатели мирового класса.

DOCA0215RU-01
06/2022

www.se.com

Правовая информация

Установка, эксплуатация, сервисное и техническое обслуживание оборудования Schneider Electric должны осуществляться только квалифицированным персоналом.

Поскольку стандарты, спецификации и конструкции периодически изменяются, информация в данном руководстве может быть изменена без предварительного уведомления.

Являясь частью группы ответственных, инклюзивных компаний, мы обновляем наши средства связи, содержащие неинклюзивную терминологию. Однако, пока мы не завершим этот процесс, наш контент может по-прежнему содержать стандартизированные отраслевые термины, которые могут быть сочтены неприемлемыми для наших заказчиков.

Содержание

Информация по технике безопасности

Важная информация

ПРИМЕЧАНИЕ

До установки, эксплуатации, ремонта или обслуживания устройства тщательно изучите данные инструкции и осмотрите оборудование. В данной документации или на оборудовании могут использоваться следующие специальные сообщения с целью предупреждения о потенциальных опасностях или привлечения внимания к информации, которая разъясняет или упрощает выполнение различных процедур.

Добавление любого символа к предупреждающей табличке “Опасность” или “Предупреждение” предупреждает о риске поражения электрическим током, что может стать причиной несчастного случая при невыполнении данных инструкций.

Этот символ используется для обозначения опасности. Он используется для предупредения об опасности травм персонала. Чтобы избежать возможных травм или смертельного исхода, следуйте всем инструкциям, содержащимся в сообщениях о безопасности.

⚠⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ ПРЕДУПРЕЖДЕНИЕ

ПРЕДУПРЕЖДЕНИЕ обозначает опасную ситуацию, которая, если ее не избежать, **может привести к** смерти или тяжелому увечью.

⚠ ВНИМАНИЕ

ВНИМАНИЕ обозначает опасную ситуацию, которая, если ее не избежать, **может привести к** незначительной травме или травме средней тяжести.

УВЕДОМЛЕНИЕ

УВЕДОМЛЕНИЕ указывает на ситуации, не связанные с опасностью получения травм.

ОБРАТИТЕ ВНИМАНИЕ

Монтаж, эксплуатацию, ремонт и обслуживание электрического оборудования должны выполнять только квалифицированные электрики. Компания Schneider Electric не несет никакой ответственности за любые возможные последствия использования данной документации.

Квалифицированный специалист — это человек, обладающий навыками и знаниями, связанными с конструированием, монтажом и эксплуатацией электрооборудования и прошедший обучение по технике безопасности, которое позволяет распознавать и избегать связанные с этим опасности.

УВЕДОМЛЕНИЕ О КИБЕРБЕЗОПАСНОСТИ

⚠ОСТОРОЖНО

ПОТЕНЦИАЛЬНАЯ УГРОЗА ДЛЯ ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ И НАДЕЖНОСТИ СИСТЕМЫ

- Чтобы предотвратить несанкционированный доступ к настройкам устройства и его средствам управления, а также к информации, при первом использовании измените пароли, установленные по умолчанию.
- Отключите неиспользуемые порты/службы и учетные записи по умолчанию, чтобы помочь минимизировать возможные пути доступа для хакерских атак.
- Помещайте сетевые устройства за множественными эшелонами средств защиты информационной безопасности (наподобие брандмауэров, сегментации сети, средств обнаружения вторжений в сеть и защиты от них).
- Используйте отраслевые стандарты информационной безопасности (например, наименьшие привилегии, разделение обязанностей) для предотвращения несанкционированного доступа, потери или изменения данных и журналов, а также прерывания обслуживания.

Несоблюдение данных инструкций может привести к смерти, серьёзной травме или повреждению оборудования.

Об этой книге

Область действия документа

В данном руководстве представлена информация по аспектам кибербезопасности устройств, помогающая проектировщикам и операторам систем повышать безопасность рабочей среды для продукта. В этом руководстве не рассматривается более общая тема защиты операционной технологической сети или сети Ethernet компании. Общие сведения об угрозах кибербезопасности и их способах их устранения см. в разделе How Can I Reduce Vulnerability to Cyber Attacks

Примечание: В этом руководстве термин «безопасность» означает кибербезопасность.

Примечание о применимости

Информация, приведенная в данном руководстве, относится к устройствам, связанным с коммутационной аппаратурой Transfer**PacT** Automatic и Transfer**PacT** Active Automatic.

Информация в Интернете

Информация, содержащаяся в этом документе, может быть обновлена в любой момент. Компания Schneider Electric настоятельно рекомендует загрузить последнюю актуальную версию документа, доступную на сайте www.se.com/ww/en/download.

Технические характеристики устройств, описанные в настоящем руководстве, также представлены на веб-сайте. Для получения доступа к информации в Интернете перейдите на главную страницу компании Schneider Electric по адресу www.se.com.

Технические характеристики, представленные в настоящем руководстве, должны соответствовать характеристикам, опубликованным в Интернете. Если вы обнаружите разницу между информацией в данном руководстве и в Интернете, придерживайтесь информации, опубликованной в Интернете.

Информация о соответствии изделия экологическим директивам, таким как RoHS, REACH, PEP и EOLI, приводится на веб-сайте *www.se.com/green-premium*.

Дополнительная документация

Название документа	Номер документа
Руководство пользователя активной коммутационной аппаратуры TransferPacT Active Automatic	DOCA0214RU-01
How Can I reduce Vulnerability to Cyber Attacks	How Can I Reduce Vulnerability to Cyber Attacks

Введение в кибербезопасность

Введение

Кибербезопасность защищает коммуникационную сеть и устройства от любых сбоев в работе (обеспечивая доступность), изменения настроек (обеспечивая целостность) и раскрытия любой конфиденциальной информации (обеспечивая конфиденциальность).

Цели кибербезопасности:

- Повышение уровня защиты информации и физических активов от кражи, коррупции, неправильного использования или несчастных случаев при сохранении доступа к ним для назначенных пользователей.
- Разработка безопасных систем, ограничение доступа с использованием физических и цифровых методов, идентификация пользователей, а также внедрение процедур безопасности и передовых практик.

Рекомендации Schneider Electric

В дополнение к рекомендациям, приведенным в данном руководстве, которые относятся исключительно к устройствам, вам следует придерживаться подхода к кибербезопасности, основанного на концепции «глубокой обороны» компании Schneider Electric.

Этот подход описан в техническом примечании How Can I Reduce Vulnerability to Cyber Attacks к системе.

Кроме того, вы найдете много полезных ресурсов и актуальную информацию на портале поддержки кибербезопасности на всемирном веб-сайте Schneider Electric.

Характеристики устройства

Обзор

Коммутационная аппаратура автоматического переключения Tranfer**PacT** оснащена средствами обеспечения безопасности, которые находятся в предварительно заданном состоянии и могут быть изменены в соответствии с вашими требованиями к установке. Настраивать и устанавливать устройство должен только квалифицированный персонал, поскольку отключение или изменение настроек повлияет на общую безопасность устройства и сети связи.

Используйте это руководство в сочетании с руководством пользователя DOCA0214RU-01 для получения подробной информации о настройке функций и параметров устройства.

Характеристики связи

Связь с коммутационной аппаратурой автоматического переключения TransferPacT осуществляется через следующие типы интерфейсов:

- Проводная связь через:
  - Modbus-RTU
  - CANopen
- Человеко-машинный интерфейс (ЧМИ) через:
  - ЖКД с кнопками для отображения и управления.
  - Поворотные и DIP-переключатели со светодиодом для управления.

Поддерживаемые протоколы

- Modbus-RTU для связи с устройствами/системами, поддерживающими операционную технологию (OT).
- CANopen для внутренней связи между главным контроллером и вспомогательными устройствами (например, модуль DI/DO, модуль связи Modbus)

  Примечание: Modbus-RTU и CANopen являются устаревшими протоколами, которые имеют присущие им недостатки, связанные с безопасностью, и требуют компенсации для дополнительной физической защиты в каждом конкретном виде применения.

Функции безопасности

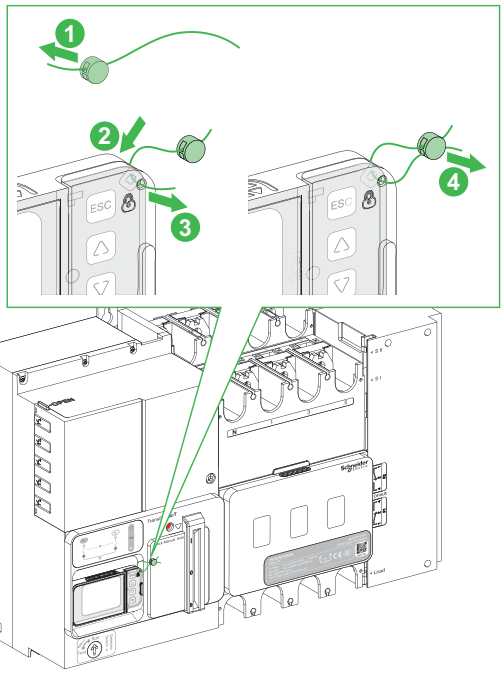
Поддерживаются следующие функции безопасности:

- Микропрограммное обеспечение может быть безопасно обновлено с установкой микропрограммного обеспечения, имеющего цифровую подпись от инфраструктуры открытых ключей (PKI) Schneider.
- Проверяется целостность данных, хранящихся в устройстве, для предотвращения несанкционированного изменения конфигураций, бизнес- и других данных.
- Выполняется надежная проверка входных данных для предотвращения удаленных атак из Modbus-RTU и/или CANopen.
- Любое изменение конфигурации защищено паролем.
- Пароль хранится в виде фиксированного хеша и может быть сброшен. Сброс пароля описан в руководстве пользователя DOCA0214RU-01.
- Функция управления связью по умолчанию отключена и может использоваться только после локальной активации. Отключайте ее, когда она не нужна.

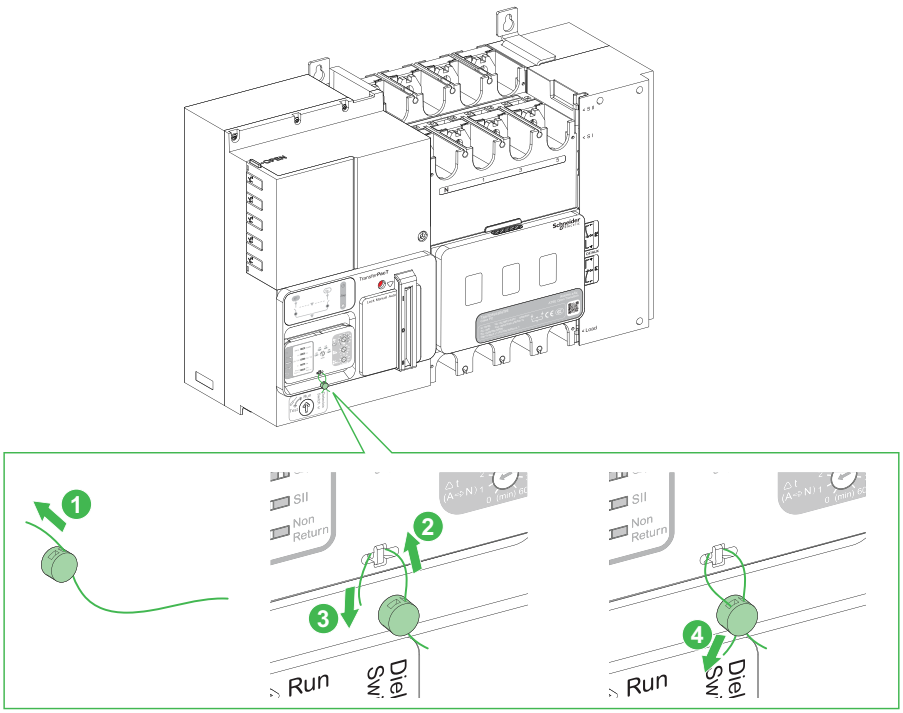
  Примечание: Функция управления связью поддерживается только в TransferPact Active Automatic. Для получения дополнительной информации см. руководство пользователя DOCA0214RU-01.
- Устройство будет заблокировано на 10 минут после 3 неудачных попыток ввода пароля для предотвращения атак методом подбора.
- Создаются журналы аудита для записи важных операций и бизнес-логики для анализа и прогнозирования, отслеживания после событий, расследования и сбора доказательств.

- Пластиковая крышка с отверстием упрощает пользователям наложение свинцовых пломб во избежание несанкционированного физического доступа к кнопкам (в устройствах TransferPact Active Automatic) или поворотным переключателям (в устройствах TransferPact Automatic).

TransferPacT Active Automatic



TransferPacT Automatic



Безопасность устройства

Обновление микропрограммного обеспечения

Микропрограммное обеспечение, разработанное для устройства, подписано инфраструктурой открытых ключей (PKI) компании Schneider Electric, что гарантирует целостность и аутентичность микропрограммного обеспечения, работающего на устройстве.

- Зарегистрируйтесь на портале поддержки кибербезопасности Schneider Electric.
- Обратитесь в службу технической поддержки компании Schneider Electric или к местному агенту, чтобы получить помощь в обновлении микропрограммного обеспечения устройства.

Пароль

Пароль по умолчанию: **0000**, его необходимо изменить при первом использовании.

Примечание: Не следует использовать старые пароли. Если вы забудете пароль, свяжитесь с выездной службой или обратитесь к руководству пользователя DOCA0214RU-01.

Дата и время

Сертификаты и цифровые подписи имеются в устройстве, а также в журналах аудита. Чтобы избежать ошибок, необходимо постоянно синхронизировать дату и время. Дополнительную информацию о дате и времени см. в руководстве пользователя DOCA0214RU-01.

Журналы аудита

Создавайте журналы аудита, записывающие события, такие как неудачные попытки входа в систему и обновление микропрограммного обеспечения.

Журналы аудита не содержат персональной и конфиденциальной информации.

Для обнаружения неожидаемых случаев поведения (например, частой перезагрузки, неправильного обновления микропрограммного обеспечения или неудачных попыток входа в систему) рекомендуется регулярно отслеживать журналы аудита.

Утилизация устройства

Устройство содержит конфиденциальную информацию, составленную во время ввода в эксплуатацию, последние значения данных и журналы. Например, эта информация может включать в себя пароль, топологию устройства Modbus и измеренное энергопотребление.

Перед утилизацией устройства необходимо выполнить сброс конфигурации и восстановить пароль по умолчанию. При включенном питании необходимо иметь физический доступ к устройству. Подробную процедуру возврата к заводским настройкам см. в руководстве пользователя DOCA0214RU-01.

Примечание: Крайне важно запланировать вывод устройства из эксплуатации еще до его утилизации, пока оно находится в работе.

Примечание: Перед выводом устройства из эксплуатации убедитесь, что экспортированы последние журналы событий.

Физическая безопасность устройства

При установке устройства необходимо учитывать важные моменты физической безопасности, указанные ниже.

- Рекомендуется устанавливать и использовать коммутационную аппаратуру в соответствии с концепцией «глубоко эшелонированной защиты», которую рекомендует Schneider Electronic для снижения риска атаки на коммутационное оборудование.
- Устанавливайте коммутационную аппаратуру автоматического переключения в шкафу, закрытом надлежащим образом, например с помощью навесного замка или ключа, во избежание рисков во время установки или риска несанкционированного физического доступа.
- Вспомогательные устройства ввода/вывода (если имеются) должны быть защищены от несанкционированного доступа, чтобы снизить риск изменения настроек переключателя для используемого, предварительно определенного варианта применения.
- Для вспомогательных устройств Modbus-RTU (если имеются), которые признаны в отрасли рисками для безопасности, рекомендуется использовать меры физической безопасности (например, специальные трубы) для защиты коммуникационных кабелей от несанкционированного доступа, обрыва связи, утечки и несанкционированного изменения данных и т. д.
- Для человеко-машинного интерфейса (если имеется) должна использоваться свинцовая пломба для предотвращения несанкционированного доступа к кнопкам или поворотным переключателям.
- Независимый ЧМИ (при наличии) настоятельно рекомендуется установить в одном шкафу с коммутационной аппаратурой автоматического переключения, чтобы обеспечить безопасность связи CANopen, или защитить коммуникационные кабели с помощью мер физической безопасности (например, с помощью специальных труб).

Рекомендуемые операции по техническому обслуживанию

В течение срока службы устройства требуется регулярное рекомендованное техническое обслуживание:

- Убедитесь, что микропрограммное обеспечение обновлено до последней версии.
- Проверьте в журналах аудита непредвиденные варианты поведения, такие как недопустимые попытки входа в систему или частая перезагрузка.
- Регулярно меняйте пароль администратора.
- Регулярно проверяйте кабели ввода-вывода, чтобы убедиться в их надлежащем подключении и отсутствии несанкционированного доступа.
- Регулярно проверяйте коммуникационные кабели Modbus-RTU и CANopen, чтобы убедиться в отсутствии несанкционированного доступа.
- Отключайте функцию управления связью, когда она не нужна. Для получения дополнительной информации см. руководство пользователя DOCA0214RU-01.

Портал поддержки кибербезопасности Schneider Electric

Обзор

На портале поддержки кибербезопасности Schneider Electric опубликована политика Schneider Electric по управлению уязвимостями.

Политика Schneider Electric по управлению уязвимостями направлена на устранение уязвимостей в кибербезопасности, влияющих на продукты и системы Schneider Electric, для защиты клиентов, окружающей среды и установленных решений.

Schneider Electric сотрудничает с исследователями, группами реагирования на киберпроисшествия (CERT) и владельцами активов, чтобы обеспечить своевременное предоставление точной информации для адекватной защиты установок.

Schneider Electric Corporate Product CERT (CPCERT) отвечает за управление и выдачу уведомлений об уязвимостях и смягчениях, влияющих на продукты и решения.

CPCERT координирует связь между соответствующими CERT, независимыми исследователями, менеджерами продукции и всеми клиентами, которых это затрагивает.

Информация, доступная на портале поддержки кибербезопасности Schneider Electric

Содержимое портала поддержки:

- Информация об уязвимостях продуктов в сфере кибербезопасности.
- Информация об инцидентах, связанных с кибербезопасностью.
- Интерфейс, с помощью которого пользователи могут сообщать об инцидентах или уязвимостях, связанных с кибербезопасностью.

Отчетность об уязвимостях и управление ими

Информацию об инцидентах, связанных с кибербезопасностью, и потенциальных уязвимостях можно получить на веб-сайте Report a Vulnerability (Сообщить об уязвимости) Schneider Electric.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France (Франция)

+33 (0) 1 41 29 70 00

www.se.com

DOCA0215RU-01