# EcoStruxure Panel Server

## Руководство по кибербезопасности

**Беспроводной концентратор и шлюз Modbus, сервер регистрации данных и энергии**

**EcoStruxure** предоставляет архитектуру и платформу с поддержкой Интернета вещей.

**DOCA0211RU-02**
**11.2021**

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.

# Содержание

Информация по безопасности ..... 5
Об этой книге ..... 7
Введение в кибербезопасность ..... 8
Характеристики устройства ..... 10
Характеристики устройства ..... 12
Безопасность сети ..... 14
Физическая безопасность устройства ..... 16
Рекомендации по обеспечению безопасности при выполнении технического обслуживания ..... 17
Портал поддержки кибербезопасности Schneider Electric ..... 19
Глоссарий ..... 21

# Информация по безопасности

## Важная информация

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.

**⚠ ОПАСНОСТЬ**

**ОПАСНОСТЬ** обозначает опасную ситуацию, которая, если ее не избежать, **приведет к** смерти или тяжелому увечью.

**⚠ 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

Установка, эксплуатация, ремонт и обслуживание электрического оборудования может выполняться только квалифицированными электриками. Компания Schneider Electric не несет никакой ответственности за любые возможные последствия использования данной документации.

Квалифицированными электриками называются лица, обладающие соответствующими знаниями и навыками в области установки и эксплуатации электрического оборудования и систем и прошедшие обучение по технике безопасности с целью определения и устранения связанных с их работой опасностей.

# Уведомление о кибербезопасности

## ⚠ОСТОРОЖНО

**ПОТЕНЦИАЛЬНАЯ УГРОЗА ДЛЯ ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ И НАДЕЖНОСТИ СИСТЕМЫ**

- Отключайте неиспользуемые порты/службы, чтобы минимизировать возможные пути доступа для хакерских атак.
- Помещайте сетевые устройства за множественными эшелонами средств защиты информационной безопасности (наподобие брандмауэров, сегментации сети и 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 EcoStruxure Panel Server, 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 способах их устранения см. в разделе *How Can I Reduce Vulnerability to Cyber Attacks?*.

**Примечание:** В контексте данного руководства термин **безопасность** означает кибербезопасность.

## Примечание о применимости

Информация, представленная в данном руководстве, относится к EcoStruxure Panel Server.

## Информация в Интернете

Информация, представленная в этом руководстве, 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, описанных в этом руководстве, также доступны в режиме онлайн. Для доступа к информации в режиме онлайн перейдите на главную страницу компании Schneider Electric по адресу www.se.com.

## Соответствующие документы

| Наименование документации | Шифр документа |
|---|---|
| *EcoStruxure Panel Server - Руководство пользователя* | DOCA0172RU |
| *How Can I Reduce Vulnerability to Cyber Attacks?* | Cybersecurity System Technical Note |

Вы можете загрузить технические публикации и прочую техническую информацию на нашем веб-сайте www.se.com/ww/en/download.

# Введение в кибербезопасность

## EcoStruxure Основной диапазон

EcoStruxure компании Schneider Electric является открытой, полностью укомплектованной, готовой к работе и обладающей высокой функциональной совместимостью архитектурой и платформой на основе Интернета вещей, применяемой в жилых домах, зданиях, центрах обработки данных, инфраструктуре и различных отраслях промышленности. Инновации на каждом уровне – от подключенных продуктов до управления периферийным оборудованием, приложений, аналитики и услуг.

## Введение

Кибербезопасность предназначена для защиты вашей коммуникационной сети и всего подключенного к ней оборудования от атак, которые могут нарушить работу (обеспечивает готовность к работе), изменить информацию (обеспечивает целостность данных) или вызвать утечку конфиденциальной информации (обеспечивает конфиденциальность). Задача кибербезопасности — повышение уровня защиты информации и физических ресурсов от кражи, повреждения, неправильного использования или чрезвычайных происшествий при сохранении доступа к ним для назначенных пользователей. В кибербезопасности существует множество аспектов, включая, среди прочих, проектирование защищенных систем, ограничение доступа с использованием физических и цифровых методов, идентификацию пользователей, а также внедрение процедур обеспечения безопасности и инновационных политик.

## Рекомендации Schneider Electric

В дополнение к рекомендациям, приведенным в данном руководстве, которые относятся к Panel Server, следует придерживаться подхода Schneider Electric к кибербезопасности, основанного на концепции «глубоко эшелонированной защиты».

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

Кроме этого, много полезных ресурсов и актуальной информации представлено на портале поддержки кибербезопасности на глобальном веб-сайте Schneider Electric, стр. 19.

## Правила и политики компании Schneider Electric в сфере кибербезопасности

Компания Schneider Electric использует процесс Secure Development Lifecycle (SDL) (жизненный цикл безопасной разработки), который является основой для среды разработки продуктов и позволяет обеспечить соблюдение процессов безопасного проектирования на всех этапах жизненного цикла разработки продукта. Процесс SDL, внедренный в компании Schneider Electric, соответствует требованиям стандарта IEC 62443-4.1.

Процесс SDL включает:

- методы SDL, применяемые в рамках всей цепочки поставок в отношении внутренних действий, связанных с разработкой;
- обязательную завершающую проверку безопасности, предшествующую релизу проекта;

- обучение персонала, участвующего в разработке продукта, мерам обеспечения и соблюдения безопасности.

# Характеристики устройства

## Обзор

EcoStruxure Panel Server оснащен средствами обеспечения безопасности. Эти средства поставляются в предварительно настроенном состоянии, однако пользователь может изменить настройки в соответствии со специфическими требованиями к установке. Конфигурировать и настраивать EcoStruxure Panel Server должен только квалифицированный персонал, поскольку отключение или изменение настроек оказывает негативное влияние на общую отказоустойчивость системы обеспечения безопасности EcoStruxure Panel Server и сети пользователя.

Используйте это руководство в сочетании с DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*, где представлены подробные сведения касательно конфигурации функций и настроек EcoStruxure Panel Server.

## EcoStruxure Panel Server Интерфейсы

EcoStruxure Panel Server осуществляет обмен данными через следующие типы интерфейсов:

- Проводной, посредством использования:
  - двух портов Ethernet;
  - одного порта Modbus-SL.
- Радиоинтерфейс, посредством использования:
  - IEEE 802.15.4 (по умолчанию не активна).

## Поддерживаемые протоколы

EcoStruxure Panel Server поддерживает следующие протоколы:

- HTTPS (TLS v1.2) для выполнения настройки посредством использования средств конфигурирования и встроенных веб-страниц;
- VPN для удаленного доступа (открыт для центра поддержки клиентов компании Schneider Electric);
- Modbus TCP и Modbus-SL для связи с устройствами, поддерживающими операционную технологию (OT);
- DHCP для сетевой IP-адресации;
- DNS для отождествления сетевых имен;
- NTP для синхронизации времени;
- DPWS для обнаружения сети;
- IEEE 802.15.4 для беспроводной связи с использованием радиочастотной связи в диапазоне ISM 2,4 ГГц.

## Функции безопасности

EcoStruxure Panel Server поддерживает следующие функции безопасности:

- на EcoStruxure Panel Server можно установить только микропрограммное обеспечение, имеющее цифровую подпись компании Schneider Electric;
- при каждой загрузке, перед выполнением микропрограммы, ее цифровая подпись проверяется, обеспечивая целостность защиты;
- пароли пользователей хранятся в виде фиксированных и хешированных (SHA256) паролей;

- можно стереть всю информацию из EcoStruxure Panel Server с помощью кнопки перезапуска;
- устройство оснащено встроенными часами и хранит в памяти свою дату и время в течение нескольких месяцев без питания;
- код аутентификации EcoStruxure Panel Server хранится в высокозащищенной микросхеме, сертифицированной по стандарту CC EAL6+ Common Criteria (Общий уровень оценки критериев безопасности).

# Характеристики устройства

## Обновление микропрограммного обеспечения

Обновите EcoStruxure Panel Server до последней версии микропрограммного обеспечения и получите самые последние функции и актуальные обновления для системы безопасности. Все микропрограммное обеспечение, разработанное для EcoStruxure Panel Server, подписано инфраструктурой открытых ключей (PKI) компании Schneider Electric, что позволяет обеспечить целостность и аутентичность микропрограммного обеспечения, работающего на EcoStruxure Panel Server. Для правильной работы PKI синхронизируйте дату устройства (см. раздел Дата и время, стр. 12).

Для получения самой последней информации об обновлениях системы безопасности зарегистрируйтесь с помощью Security Notifications на портале поддержки кибербезопасности Schneider Electric.

## Дата и время

EcoStruxure Panel Server содержит сертификаты и цифровые подписи. Чтобы избежать ошибок, необходимо постоянно синхронизировать дату и время. Дополнительные сведения о дате и времени см. в DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*.

## Отключение неиспользуемых функций

В EcoStruxure Panel Server предусмотрена возможность деактивации неиспользуемых портов/служб, что позволяет минимизировать возможные пути доступа для хакерских атак.

Рекомендуется отключить:

- Wi-Fi (по умолчанию не активен, активация будет доступна в дальнейшем);
- IEEE 802.15.4 (по умолчанию не активна);
- шлюз Modbus (активен по умолчанию, деактивация будет доступна в дальнейшем);
- DPWS (протокол обнаружения по IP-адресу, версия 4/6) (активен по умолчанию);
- функцию PING (активна по умолчанию, деактивация будет доступна в дальнейшем).

Дополнительные сведения о функциях и настройках EcoStruxure Panel Server см. в DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*.

## TCP-порты

В EcoStruxure Panel Server используются следующие TCP-порты:

- Порт 443: HTTPS
- Порт 502: Modbus
- Порт 5357: DPWS (можно изменить)

# Журналы аудита

EcoStruxure Panel Server создает журналы аудита, которые записывают такие события, как неудачные попытки входа в систему и обновление микропрограммного обеспечения.

Журналы не содержат никаких персональных данных.

Рекомендуется регулярно просматривать журналы аудита (см. DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*), чтобы своевременно выявлять признаки непредвиденного поведения (например, частая перезагрузка, неправильное обновление микропрограммного обеспечения или неудачные попытки входа в систему).

# Утилизация устройства

EcoStruxure Panel Server содержит конфиденциальные данные, созданные в процессе ввода в эксплуатацию, значения новых данных и сведения журналов регистрации. Это могут быть, к примеру, сведения о топологии устройства Modbus, беспроводных сетях или измеренном энергопотреблении.

Перед утилизацией EcoStruxure Panel Server необходимо выполнить сброс до заводских настроек. Во время выполнения этой процедуры необходимо иметь физический доступ к циклу включения/выключения питания EcoStruxure Panel Server. Порядок сброса EcoStruxure Panel Server до заводских настроек см. в DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*.

# Безопасность сети

## Введение

EcoStruxure Panel Server не предназначен для прямого подключения к общедоступной сети Интернет. При его установке необходимо использовать, как минимум, технологию трансляции сетевых адресов Network Address Translation (NAT) либо, что является более предпочтительным вариантом, несколько брандмауэров. Дополнительные сведения см. на следующих веб-сайтах:

- Консультационные услуги Schneider Electric по кибербезопасности
- Национальный институт стандартов и технологий (NIST)
- Европейское агентство по кибербезопасности (ENISA)

## Сегментация сети

EcoStruxure Panel Server — это шлюз. Он создает мост между различными сетями. Сегментация сети предназначена для повышения уровня киберзащиты. Для оптимизации сегментации сети в EcoStruxure Panel Server предусмотрены два порта Ethernet. Их можно использовать в раздельном режиме, что позволит выделить один порт для информационных технологий (ИТ), и один порт — для операционных технологий (ОТ). Сетевая сегментация позволяет поддерживать ОТ- и ИТ-сети в разделенном состоянии, поскольку сетевые пакеты не передаются с одной стороны на другую.

Рекомендуется настроить сеть в отдельном режиме (дополнительную информацию о настройках сети см. в DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*).

Это позволит подключать EcoStruxure Panel Server к:

- нисходящим устройствам, поддерживающим ОТ, через Modbus TCP на одном порту Ethernet;
- восходящему ПК, поддерживающему ИТ, при помощи SCADA и программных приложений для ввода в эксплуатацию на другом порту Ethernet.

HTTPS и Modbus доступны на Ethernet-интерфейсах, то есть ETH1 и ETH2.

## Сертификат программы веб-сервера

Для обеспечения защищенной передачи данных по протоколу HTTP, EcoStruxure Panel Server по умолчанию оснащен X.509v3. Этот сертификат обеспечивает целостность и конфиденциальность данных при настройке связи по протоколу HTTPS.

Веб-браузеры распознают только сертификаты для общедоступных веб-сайтов. Поскольку EcoStruxure Panel Server устанавливается в локальной вычислительной сети (LAN), веб-браузеры не могут отличить один EcoStruxure Panel Server от другого. Поэтому при подключении EcoStruxure Panel Server в веб-браузере отображается сообщение, связанное с безопасностью.

Обеспечить защиту канала связи с EcoStruxure Panel Server можно с помощью прямого проводного соединения (дополнительную информацию о первом подключении к веб-страницам EcoStruxure Panel Server через ПК см. в DOCA0172RU *EcoStruxure Panel Server - Руководство пользователя*).

## Беспроводная сеть

Протоколы радиочастотной связи уязвимы для нарушений физической безопасности. Например, DOS-атака (отказ в обслуживании) может глушить радиосигнал мощным радипередатчиком, расположенным поблизости.

Поэтому рекомендуется адаптировать физическую безопасность устройств в зависимости от категории важности информации, передача которой осуществляется по протоколам радиочастотной связи.

Беспроводные устройства IEEE 802.15.4 рекомендуется вводить в эксплуатацию в местах, защищенных от неконтролируемых радиопередатчиков, таких как помещение администратора.

## Подключенные устройства

Рекомендуется регулярно проверять список устройств, подключенных к сети IEEE 802.15.4 Panel Server. В случае обнаружения неизвестного подключенного устройства найдите его и удалите. Можно также восстановить сеть и повторно подключить только идентифицированные устройства.

# Физическая безопасность устройства

## Метка с индикацией вскрытия

На EcoStruxure Panel Server предусмотрена метка с индикацией вскрытия, позволяющая обеспечить физическую безопасность устройства. Она должна быть неповрежденной, без признаков несанкционированного вскрытия (например, разрывы, прорези или царапины). Schneider Electric рекомендует не использовать устройство, которое имеет явно выраженные признаки вскрытия.

## Установка

С целью обеспечения физической безопасности устройства рекомендуется соблюдать следующий порядок установки:

- установите EcoStruxure Panel Server в шкаф, защищенный в соответствии с уровнем риска вашего оборудования (например, шкаф с навесным или врезным замком);
- при установке EcoStruxure Panel Server в распределительном щите необходимо разместить распределительный щит в защищенном помещении (например, оборудованном видеокамерой или дверью, запираемой на замок).

# Рекомендации по обеспечению безопасности при выполнении технического обслуживания

## Операции по техническому обслуживанию

В течение всего срока службы EcoStruxure Panel Server рекомендуется регулярно выполнять следующие операции:

- проверка физической безопасности EcoStruxure Panel Server (см. описание метки с индикацией вскрытия, стр. 16);
- проверка наличия последнего обновления микропрограммного обеспечения; необходимо зарегистрироваться для получения уведомлений безопасности, стр. 12;
- проверка подключенных устройств, стр. 15 с целью выявления неизвестных устройств;
- проверка журналов аудита, стр. 13 на наличие признаков непредвиденного поведения, таких как неудачные попытки входа в систему или частая перезагрузка;
- проверка даты и времени, стр. 12 с целью предотвращения отклонения от текущей даты.

## Проверка функций обеспечения безопасности

Ниже перечислены тесты, с помощью которых можно проверить работу функций обеспечения безопасности на предмет соответствия требованиям, предъявляемым для сертификации IEC 62443. Выполнять эти тесты можно на веб-страницах EcoStruxure Panel Server.

### Веб-аутентификация

1. Попробуйте войти на веб-страницы EcoStruxure Panel Server без пароля или введите неверный пароль.

   **Результат:** EcoStruxure Panel Server не предоставляет доступ к веб-страницам.
2. Повторите это действие еще 9 раз.

   **Результат:** EcoStruxure Panel Server блокирует доступ на 10 минут.
3. Повторите попытку 5 раз.

   **Результат:** EcoStruxure Panel Server блокирует доступ на 60 минут.

### Веб-авторизация

1. Войдите на веб-страницы EcoStruxure Panel Server.
2. Создайте закладку для любой веб-страницы (например, **Настройки**)
3. Откройте в браузере окно скрытой навигации, а затем откройте страницу, для которой ранее создали закладку.

   **Результат:** доступ к веб-странице запрещен, однако пользователь перенаправляется на страницу входа в систему.

### Аудит

1. Выполнив несколько или все тесты, представленные выше, перейдите на веб-страницу Logs (Журналы регистрации).
2. Загрузите файлы журнала.
3. Проверьте в журналах наличие неудачных попыток входа в систему.

## Обновление микропрограммного обеспечения

1. Перейдите на веб-страницу **Firmware Update** (Обновление микропрограммного обеспечения).
2. Загрузите любой файл, выбранный случайным образом (например, изображение или текстовый документ).

   **Результат:** EcoStruxure Panel Server сообщает о неправильной подписи.
3. Зайдите в журналы аудита.
4. Проверьте в журналах наличие ошибки обновления микропрограммного обеспечения.

## Отключение служб

1. Чтобы получить доступ к меню для отключения служб, выберите **Settings** (Настройки) **> Network Communication** (Передача данных по сети) **> DPWS**.
2. Подключите к той же локальной сети ПК с операционной системой Windows.
3. В проводнике нажмите пункт Network (Сеть).

   **Результат:** EcoStruxure Panel Server не обнаружен, поэтому не отображается в списке устройств, присутствующих в сети.

# Портал поддержки кибербезопасности Schneider Electric

## Обзор

На Schneider Electric cybersecurity support portal 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 своего оборудования.

Компания Schneider Electric внедрила корпоративный продукт CERT (CPCERT), который отвечает за управление уязвимостями, своевременное оповещение и принимает соответствующие меры для смягчения негативного воздействия 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 передать через веб-сайт Schneider Electric: Report a Vulnerability (Сообщить об уязвимости).

# Глоссарий

**OT — операционная технология:**

Означает аппаратные и программные системы, используемые компанией для непосредственного мониторинга и управления производственными процессами и оборудованием. Также называется сетью управления производством (IC). OT часто используется для обозначения операционной сети компании в качестве противопоставления ее информационно-телекоммуникационной сети.

**Политика обеспечения безопасности:**

Политика обеспечения безопасности системы — это параметры безопасности, применяемые ко всей защищенной системе. По общему правилу политика обеспечения безопасности означает использование неких стандартов. Она применяется для определения конфигурации любой системы обеспечения безопасности, совместно используемой всеми устройствами.

## D

**DPWS — профиль устройств для веб-служб:**

Минимальный набор ограничений ввода, который обеспечивает безопасный обмен сообщениями с веб-службами, выявление, описание и обработку событий на устройствах с ограниченными ресурсами.

## H

**HTTP — протокол передачи гипертекстовых файлов:**

Сетевой протокол, обеспечивающий передачу файлов и данных через Интернет.

**HTTPS — защищенный протокол передачи гипертекстовых файлов:**

Вариант стандартного протокола веб-передачи (HTTP), который добавляет уровень безопасности для передаваемых данных посредством использования соединения по протоколу уровня защищенных сокетов (SSL) или по протоколу безопасности на транспортном уровне (TLS).

## I

**IP — протокол Internet:**

IP-адреса используются для идентификации устройств, подключенных к внутрикорпоративной сети или Интернету.

**IT — информационная технология:**

Означает информационные системы и информационную сеть компании в отличие от ее сети OT (операционной технологии).

## L

**LAN — локальная вычислительная сеть:**

Означает внутрикорпоративную сеть на базе технологии intranet или информационно-телекоммуникационную сеть.

## M

**Modbus TCP/IP:**

Протокол, обеспечивающий обмен данными между устройствами по схеме «клиент-сервер», и TCP/IP, который обеспечивает связь через Ethernet.

## P

**PKI — инфраструктура открытых ключей:**

Определяет набор служб, используемых для создания и проверки подлинности цифровых подписей. Инфраструктура открытых ключей предназначена для обеспечения конфиденциальности, целостности и достоверности информации.

## S

**SCADA - Supervisory control and data acquisition:**

Означает системы, предназначенные для получения данных производственных процессов и оборудования в режиме реального времени с целью дистанционного мониторинга и управления такими процессами.

## T

**TCP/IP - Transmission control protocol/Internet protocol:**

Означает набор протоколов, используемых для передачи данных по сети Интернет.

## V

**VPN — виртуальная частная сеть:**

VPN используется для создания защищенного/частного «канала» между проверенной точкой доступа извне и доверенной корпоративной сетью.

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

+ 33 (0) 1 41 29 70 00

www.se.com

Стандарты, спецификации и схемы могут изменяться; обратитесь в компанию за подтверждением актуальности информации, опубликованной в данном руководстве.



DOCA0211RU-02