Masterpact MTZ

Руководство по кибербезопасности

www.schneider-electric.ru

Life Is On Schneider Electric

Информация, представленная в настоящем документе, содержит общее описание и/или технические характеристики указанных выше изделий. Настоящая документация не предназначена для определения пригодности или надежности применения данной продукции для конкретных целей. Пользователь или сборщик обязан выполнить надлежащий полный анализ рисков, а также провести оценку и испытание изделий с учетом соответствующей области применения или с учетом особенностей их использования. Компания Schneider Electric, а также любые ее филиалы и/или подразделения не несут ответственности и не берут на себя обязательства за неправильное использование информации, представленной в настоящем документе. Если у вас есть предложения по улучшению, корректировке, или если вы обнаружили ошибки в данной публикации, сообщите нам об этом.

При установке и эксплуатации настоящего изделия следует соблюдать все применимые государственные, региональные и местные правила безопасности. В целях безопасности и для обеспечения соответствия указанным в документации характеристикам системы ремонт компонентов оборудования должен выполняться только его производителем.

При использовании оборудования в приложениях, к которым предъявляются особые технические требования по безопасности, следует соблюдать соответствующие инструкции.

Отказ от использования программного обеспечения производства Schneider Electric или одобренного программного обеспечения других производителей с нашим оборудованием может привести к травмам, порче имущества или некорректной работе.

Несоблюдение приведенных инструкций может привести к травмам или повреждению оборудования.

Содержание

Требования безопасности 5
Об этом документе 7
Глава 1 Введение в кибербезопасность 9
Введение в кибербезопасность 10
Почему кибербезопасность важна для автоматических выключателей Masterpact MTZ 11
Глава 2 Рекомендации по кибербезопасности для проектирования, планирования и сборки систем 13
Определение и защита конфиденциальной информации и действий 14
Разработка политики паролей 15
Обучение 17
Глава 3 Рекомендации по кибербезопасности для доступа по месту 19
Ограничение доступа по месту к автоматическим выключателям Masterpact MTZ 20
Рекомендации по защите доступа по месту к интерфейсу блока Micrologic X 21
Рекомендации по защите доступа через NFC 22
Рекомендации по защите доступа через Bluetooth 23
Рекомендации по защите доступа к блоку управления Micrologic X через порт mini-USB 25
Глава 4 Рекомендации по кибербезопасности для удаленного доступа 27
Ограничение удаленного доступа к автоматическим выключателям Masterpact MTZ . . . 28
Отделение промышленной сети предприятия от корпоративной сети. 29
Рекомендации по защите удаленного доступа к блоку управления Micrologic X через Ethernet 30
Глава 5 Рекомендации по кибербезопасности при обновлении программного обеспечения и цифровых модулей 31
Установка обновлений программного обеспечения. 32
Покупка и установка цифровых модулей 34
Глоссарий терминов 37

Требования безопасности

Важная информация

УВЕДОМЛЕНИЕ

Прежде чем устанавливать, эксплуатировать или ремонтировать изделие, внимательно ознакомьтесь с ним и тщательно изучите настоящее руководство. На изделии и в тексте руководства имеются специальные знаки, предупреждающие о потенциальных опасностях или привлекающие внимание оператора или читателя к информации, которая поясняет или упрощает порядок действий.

Используется совместно с предупреждающей надписью ОПАСНОСТЬ (ОПАСНО ДЛЯ ЖИЗНИ!) или ПРЕДУПРЕЖДЕНИЕ (ОСТОРОЖНО!) и указывает на то, что несоблюдение предписанных требований может привести к поражению электрическим током.

Знак, предупреждающий обо всех остальных видах опасности. Знак используется для привлечения внимания к опасности получения травм. Строго соблюдайте все требования, указанные после этого знака. Несоблюдение этих требований может привести к получению травм или к смерти.

⚠ ОПАСНОСТЬ!

Предупреждает о наличии существующей опасной ситуации, которая может привести к тяжелой травме или к смертельному исходу.

⚠ ПРЕДУПРЕЖДЕНИЕ

Предупреждает о наличии потенциально опасной ситуации, которая, если ее не избежать, может стать причиной смерти или серьезных травм.

⚠ ВНИМАНИЕ

Предупреждает о наличии возможной потенциально опасной ситуации, которая, если ее не избежать, может привести к травмам легкой или средней тяжести.

УВЕДОМЛЕНИЕ

Предупреждает о наличии потенциальной опасности, не связанной с возможностью получения травмы.

ОБРАТИТЕ ВНИМАНИЕ

Установка, эксплуатация и обслуживание электрического оборудования должны осуществляться только квалифицированным персоналом. Компания Schneider Electric не несет ответственности за любые последствия использования настоящей документации.

Квалифицированный работник должен иметь навыки и знания в области конструкции, установки и эксплуатации электрического оборудования, а также пройти обучение технике безопасности для обнаружения и предотвращения возможных рисков.

УВЕДОМЛЕНИЕ ОБ ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ

⚠ ВНИМАНИЕ

ВОЗМОЖНЫЙ РИСК НАРУШЕНИЯ НЕПРИКОСНОВЕННОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

- Измените пароли по умолчанию, чтобы предотвратить несанкционированный доступ к настройкам и информации об устройстве.
- Отключите неиспользуемые порты/службы и учетные записи по умолчанию, чтобы свести к минимуму пути злоумышленников.
- Разместите сетевые устройства за несколькими уровнями киберзащиты (такими как межсетевые экраны, сегментация сети, обнаружение и защита от вторжения в сеть).
- Используйте передовые методы кибербезопасности (например, наименьшие привилегии, разделение обязанностей), чтобы помочь предотвратить несанкционированный доступ, потерю, изменение данных и журналов или перерыв в обслуживании.

Несоблюдение этих указаний может привести к смерти, серьезной травме или повреждению оборудования.

Об этом документе

Общая информация

Содержание документа

В данном руководстве представлена информация об аспектах кибербезопасности для автоматических выключателей Masterpact™ MTZ с блоками управления Micrologic™ X, чтобы помочь разработчикам и операторам системы обеспечить безопасную рабочую среду для оборудования.

В данном руководстве не рассматриваются общие вопросы обеспечения безопасности промышленной сети управления или сети Ethernet предприятия.

Для общего ознакомления с угрозами кибербезопасности и способов их устранения см. *«Как уменьшить уязвимость к кибератакам?»*.

ПРИМЕЧАНИЕ: В данном руководстве термин «безопасность» используется для обозначения кибербезопасности.

Область действия

Информация в данном руководстве относится к автоматическим выключателям Masterpact MTZ с блоками управления Micrologic X.

Документы, связанные с данным руководством

Название документа	№ по каталогу
Блок контроля и управления Micrologic X. Руководство пользователя	DOCA0102EN
	DOCA0102ES
	DOCA0102FR
	MKP-MAN-MTZXUG-17
Как уменьшить уязвимость к кибератакам?	System Technical Note V2.3

Указанные документы и другую техническую информацию можно загрузить с сайта http://www.schneider-electric.com/ww/en/download

ПРИМЕЧАНИЕ

Глава 1
Введение в кибербезопасность

Описание главы

Эта глава содержит общую информацию о политике в области кибербезопасности компании Schneider Electric и объясняет, почему кибербезопасность является важной для автоматических выключателей Masterpact MTZ с блоком управления Micrologic X.

Содержание главы

Эта глава содержит следующие части:

Наименование	Стр.
Введение в кибербезопасность	10
Почему кибербезопасность важна для автоматических выключателей Masterpact MTZ	11

Введение в кибербезопасность

Введение

Кибербезопасность предназначена для защиты сетей связи и подключенного к ним оборудования от кибератак, которые могли бы сорвать действия (возможность), изменение информации (целостности) или передачу информации (конфиденциальность).

Цель информационной безопасности – обеспечить повышенный уровень защиты информации и материальных ценностей от хищений, коррупции, злоупотреблений или несчастных случаев, сохраняя доступ для их предполагаемых пользователей.

Существует множество аспектов кибербезопасности, включая проектирование защищенных систем, ограничение доступа с помощью физических и цифровых методов идентификации пользователей, а также внедрение процедур по обеспечению безопасности и передовых методов работы.

Руководство Schneider Electric

В дополнение к рекомендациям, приведенным в данном руководстве, которые являются специальными для автоматических выключателей Masterpact MTZ, необходимо следовать всестороннему подходу Schneider Electric к кибербезопасности. Этот подход описан в следующем техническом документе:

- *Как я могу уменьшить уязвимость к кибератакам?*

Кроме того, множество полезных ресурсов по кибербезопасности размещено на специальной странице *Schneider Electric* глобального веб-сайта.

Почему кибербезопасность важна для автоматических выключателей Masterpact MTZ

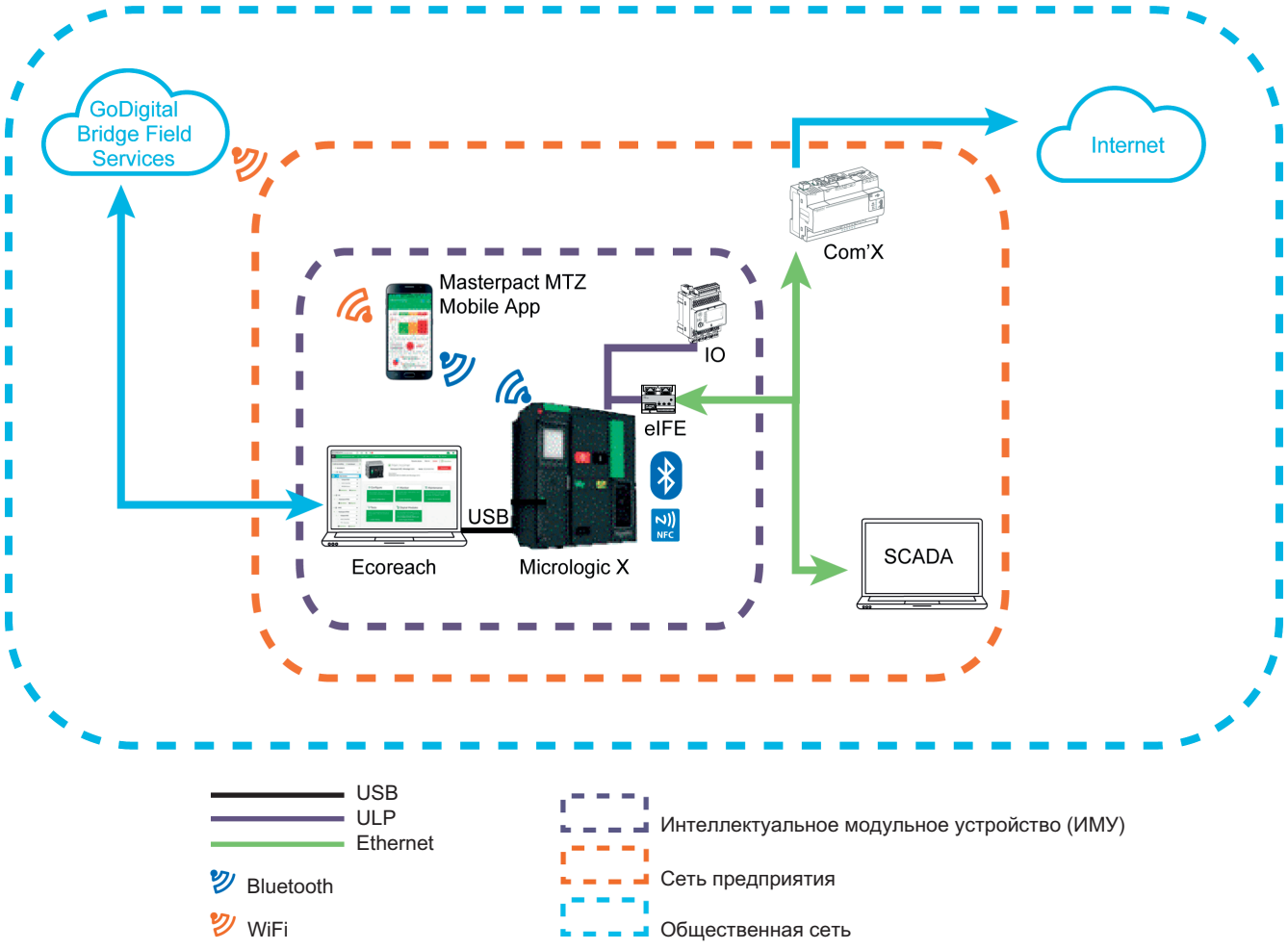
Обзор

Автоматические выключатели Masterpact MTZ являются ключевыми элементами любого распределительного щита или электроустановки в целом, поскольку они управляют электроснабжением системы, реализуют разного рода защиты и обеспечивают конфиденциальность информации.

Автоматические выключатели Masterpact MTZ с функциями связи также предоставляют доступ в режиме 24/7 к функциям управления в реальном времени и к мониторингу данных. Эти функции обеспечивают большую эффективность и гибкость в управлении электроустановкой. Но при этом, они также делают ее потенциально уязвимой для кибератак.

Автоматические выключатели Masterpact MTZ и рабочая среда

На рисунке ниже показаны различные способы связи с блоком управления Micrologic X, который взаимодействует с автоматическим выключателем Masterpact MTZ.



Интеллектуальное модульное устройство (ИМУ) представляет собой комбинацию автоматического выключателя Masterpact MTZ с блоком управления Micrologic X и соответствующих модулей ULP, интерфейсов IFE или EIFE, а также модуля ввода-вывода IO.

Для связи с автоматическим выключателем Masterpact MTZ через блок управления Micrologic X доступны следующие способы:

- Человеко-машинный интерфейс блока Micrologic X (HMI)
- Беспроводное соединение через NFC со смартфона
- Беспроводное соединение через Bluetooth со смартфона
- Подключение к порту mini-USB блока управления Micrologic X с ПК, на котором установлено программное обеспечение Ecoreach
- Ethernet-соединение через сеть предприятия при наличии интерфейса IFE или EIFE
- Ethernet-соединение из общедоступной сети при наличии сервера Com'X
- Ethernet-соединение с GoDigital, Bridge Field Services (облако Schneider Electric) при наличии ПК с программным обеспечением Ecoreach

Уязвимость системы для кибератак

Каждый из перечисленных выше способов связи представляет собой потенциально уязвимую точку в системе. В данном руководстве содержатся рекомендации по обеспечению безопасности этих способов связи во избежание преднамеренных атак или случайного злоупотребления.

Глава 2
Рекомендации по кибербезопасности для проектирования, планирования и сборки систем

Описание главы

В этой главе представлена важная информация, которую необходимо учитывать на этапах проектирования, планирования и сборки промышленного сетей, включающих в себя интеллектуальные модульные устройства (ИМУ) с Masterpact MTZ. Рекомендации и указания в этой главе помогают внедрять безопасную рабочую среду.

Содержание главы

Эта глава содержит следующие части:

Наименование	Стр.
Определение и защита конфиденциальной информации и действий	14
Разработка политики паролей	15
Обучение	17

Определение и защита конфиденциальной информации и действий

Обзор

При планировании и проектировании сети предприятия важно выделить информацию, которая имеет решающее значение для вашей деятельности. После определения эта конфиденциальная информация должна быть защищена.

Обычно такая информация включает в себя:

- Любые данные, которые могут быть использованы для доступа к электроустановке и сети предприятия
- Информацию об операциях, доступных через ИМУ с выключателем Masterpact MTZ

Вы несете ответственность за определение того, как эта информация может быть проанализирована и использована в интересах вашей организации.

Информация о корпоративной сети связи

Важная информация, которая может использоваться для доступа к сети предприятия, включает в себя:

- Архитектуру системы
- IP-адреса или MAC-адреса сетевых коммуникационных устройств
- Номера портов, используемые для связи по Ethernet
- Идентификаторы и пароли пользователей

Этот список не является полным, и необходимо учитывать всю информацию, важную для вашей организации, которая может облегчить доступ к ответственным системам.

Управление доступом

Важная часть кибербезопасности заключается в разработке эффективной политики контроля доступа. Контроль доступа состоит в определении групп пользователей или отдельных сотрудников в вашей организации и типа доступа, который им необходим для эффективного выполнения своих задач.

Объединение информации и действий, доступных разными способами

В зависимости от коммуникационного интерфейса или канала связи, используемого для доступа к ИМУ с выключателем Masterpact MTZ, доступные операции мониторинга и управления различны. В приведенной ниже сводной таблице представлены сведения и операции, доступные по разным каналам.

	Доступ по месту				**Удаленный доступ**
Операции мониторинга и управления	**ЧМИ Micrologic X**	**NFC**	**Bluetooth**	**USB**	**Ethernet**
Мониторинг данных	Да	Да	Да	Да	Да
Настройки защит	Да	Нет	Да	Да	Да
Прочие настройки	Да	Нет	Да	Да	Да
Отключение/Включение/ Сброс	Нет	Нет	Да	Да	Да

За информацией о защите каждого интерфейса и канала связи обратитесь к рекомендациям по доступу по месту (*см. стр. 19*) или, если это необходимо, по удаленному доступу (*см. стр. 27*).

Разработка политики паролей

Обзор

Профессионально разработанная политика паролей – это первая линия защиты от кибератак.

Для электроустановок, имеющих в составе автоматический выключатель Masterpact MTZ с блоком управления Micrologic X, пароли необходимы для:

- Выполнения определенных задач на блоке управления Micrologic X независимо от режима доступа (через Ethernet, USB-соединение или Bluetooth)
- Входа в компьютер, на котором установлено программное обеспечение Ecoreach

Пароль блока Micrologic X для важных настроек и управления

При доступе к блоку управления Micrologic X любые команды, которые изменяют состояние автоматического выключателя Masterpact MTZ, требуют пароля. Например, для внесения изменений в настройки защиты или для работы автоматического выключателя с блоком управления Micrologic X требуется пароль.

Пароли подразделяют на 4 уровня, каждый со своим доступом:

- Уровни 1, 2 и 3 используются для общего назначения, применяются операторами.
- Уровень 4 – уровень администратора. Администратор должен записывать настройки в блоки управления Micrologic X с использованием программного обеспечения Ecoreach.

При подключении через мобильное приложение Masterpact MTZ или ПО Ecoreach, или с веб-страниц интерфейсов IFE или EIFE пользователю предлагается ввести один из этих паролей.

При подключении к удаленному интерфейсу мониторинга и управления пароль должен быть частью запроса подключения к сети связи.

Пароль состоит из четырех символов ASCII. Пароль чувствителен к регистру, и должен содержать следующие допустимые символы:

- Цифры от 0 до 9
- Строчные буквы от a до z
- Прописные буквы от A до Z

Эти пароли необходимо поменять после первого подключения автоматического выключателя Masterpact MTZ к ПК с программным обеспечением Ecoreach и далее периодически их обновлять. Использовать их можно только ограниченному числу доверенных пользователей. Там, где возможно, следуйте рекомендациям политики паролей приведенной ниже.

Пароли и идентификаторы пользователей для сетевых ПК

Компьютеры, на которых запускается программное обеспечение Ecoreach или доступ к блоку управления Micrologic X с использованием любых других средств (например, веб-страниц SCADA, IFE или EIFE), должны запрашивать у пользователей логин и пароль. Необходимо убедиться, что пользователи задают надежные пароли и периодически меняют их. Кроме того, необходимо установить таймер для автоматического блокирования экрана ПК после периода бездействия.

Надежный пароль должен включать в себя прописные и строчные буквы, цифры и специальные символы, если они доступны. Пароль должен иметь длину не менее 10 символов.

Обратитесь к рекомендациям ниже в отношении политики паролей.

Пароли для веб-страниц IFE и EIFE

Пользователи веб-страниц IFE и EIFE имеют персональный идентификатор пользователя и пароль для входа на веб-страницы. При первом входе они должны изменить этот пароль.

Необходимо определить, каким пользователям в организации требуется вход на веб-страницы IFE и EIFE. Обратитесь к рекомендациям далее в отношении политики паролей.

Рекомендации по кибербезопасности в отношении политики паролей

Правильная политика паролей является одним из основных элементов политики кибербезопасности. Она заключается в:

- Использовании надежных паролей
- Регулярном изменении паролей
- Запрете повторного использования старых паролей
- Регулярном напоминании пользователям о лучших методах, касающихся паролей

Чтобы защитить компьютер и программное обеспечение, которое работает на нем, необходимо как минимум:

- Намеренно использовать надежные пароли
- Задавать длину пароля не менее до 10 символов
- Устанавливать срок действия пароля не менее 3 дней и не более 180 дней
- Хранить историю 8 последних паролей и запрещать их повторное использование

Все пользователи должны знать о следующих простых мерах, касающихся паролей:

- Не делиться личными паролями
- Не показывать пароли во время ввода пароля
- Не передавать пароли по электронной почте или любыми другими способами

Обучение

Обзор

Знание и обучение сотрудников являются чрезвычайно важной составляющей любой стратегии кибербезопасности. Необходимо убедиться, что всем пользователям, которым предоставлен доступ к сети управления электроустановкой, известно о корпоративной политике безопасности. Также нужно убедиться, что они прошли соответствующее обучение по выполнению своих задач в соответствии с этой политикой.

В частности, пользователи должны знать и помнить о том, что:

- Нельзя передавать секретную или конфиденциальную информацию, такую как пароли или коды доступа к оборудованию или помещениям с ограниченным доступом
- Компьютер необходимо блокировать, если он не используется
- Смартфоны, которые можно использовать для доступа к электроустановке, необходимо всегда контролировать, чтобы они не могли быть взломаны через Bluetooth или Интернет
- Нельзя игнорировать меры безопасности ради удобства применения

За дополнительной информацией о разработке и внедрении надежной политики кибербезопасности обратитесь к документу *«Как уменьшить уязвимость к кибератакам?»*.

Глава 3
Рекомендации по кибербезопасности для доступа по месту

Описание главы

В этой главе перечислены способы доступа к автоматическому выключателю Masterpact MTZ.
А также даны рекомендации по обеспечению безопасности при доступе.

Содержание главы

Эта глава содержит следующие части:

Наименование	Стр.
Ограничение доступа по месту к автоматическим выключателям Masterpact MTZ	20
Рекомендации по защите доступа по месту к интерфейсу блока Micrologic X	21
Рекомендации по защите доступа через NFC	22
Рекомендации по защите доступа через Bluetooth	23
Рекомендации по защите доступа к блоку управления Micrologic X через порт mini-USB	25

Ограничение доступа по месту к автоматическому выключателю Masterpact MTZ

Обзор

Интеллектуальное модульное устройство с Masterpact MTZ (ИМУ) предполагает доступ как по месту, так и удаленный. Доступ должен быть возможен только авторизованным пользователям.

Доступ по месту к автоматическому выключателю Masterpact MTZ

Доступ по месту к интеллектуальному модульному устройству Masterpact MTZ предоставляет различные каналы к информации об электроустановке и управлении ею.

Поэтому важно ограничить доступ по месту к Masterpact MTZ, установив его в помещении с ограниченным присутствием персонала, чтобы исключить:

- Несанкционированный доступ к ЧМИ Micrologic X с возможностью изменения настроек
- Несанкционированный доступ к беспроводной связи Bluetooth с возможностью изменения настроек через мобильное приложение Masterpact MTZ
- Несанкционированный доступ по беспроводной связи NFC с риском получения данных
- Несанкционированное подключение к порту mini-USB блока управления Micrologic X с возможностью изменения настроек из программного обеспечения Ecoreach
- Несанкционированный доступ к модулю ввода-вывода IO с возможностью изменения настроек коммутатора для используемого стандартного приложения

Это также важно для создания правил по управлению доступом в помещение, где установлено ИМУ с выключателем Masterpact MTZ.

В частности, необходимо убедиться, что:

- Помещение постоянно заперто.
- Территория оборудована системой аутентификации и авторизации.
- Только определенный персонал имеет ключи или коды доступа.
- Средства связи, сетевые кабели, входящие в помещение и порты подключения устройств связи за пределами помещения защищены.
- Все устройства, такие как ПК, смартфоны и планшеты, имеющие доступ к блоку управления Micrologic X, и установленное мобильное приложение Masterpact MTZ защищены соответствии с последними рекомендациями производителя.

Когда выключатели Masterpact MTZ установлены в помещении с ограниченным доступом, необходимо реализовать систему аварийного отключения. Например:

- Установить снаружи этого помещения по крайней мере одну доступную кнопку аварийного отключения
- Оснастить выключатель расцепителем минимального напряжения MN (отказоустойчивые системы)

Рекомендации по защите доступа по месту к интерфейсу блока Micrologic X

Функции, доступные через ЧМИ

Любой человек, имеющий доступ к распределительному щиту, в котором установлен автоматический выключатель Masterpact MTZ, имеет и доступ к интерфейсу блока управления Micrologic X.

Некоторые важные функции, такие как параметры защит оборудования, могут быть настроены с помощью интерфейса блока управления Micrologic X.

Рекомендации по защите доступа через ЧМИ Micrologic X

Интерфейс блока управления Micrologic X не защищен паролем и не может быть физически заблокирован, чтобы предотвратить несанкционированный доступ к экрану дисплея.

Поэтому, чтобы защитить доступ к Micrologic X необходимо:
- Устанавливать выключатели Masterpact MTZ в помещении с ограниченным доступом.
- Контролировать, чтобы это помещение было постоянно заперто.
- Выдавать ключи или коды доступа только авторизованному персоналу.

За дополнительной информацией о защите доступа к выключателям Masterpact MTZ обратитесь к рекомендациям по ограничению доступа (*см. стр. 20*).

Блокировка настроек защиты

Для предотвращения изменения настроек защиты автоматических выключателей Masterpact MTZ их можно заблокировать на ЧМИ.

По умолчанию, изменение параметров защиты с интерфейса разрешено.

Рекомендуется отключить изменение параметров защиты по месту на ЧМИ, если эта функция не используется. За дополнительной информацией, обратитесь к документу *«Блок контроля и управления Micrologic X. Руководство пользователя»*.

Рекомендации по защите доступа через NFC

Функции, доступные через NFC

Посредством беспроводной связи через NFC данные могут быть загружены из блока управления Micrologic X на смартфон, даже когда блок управления не работает.

Эта функция не может использоваться для изменения каких-либо настроек на блоке управления, отключения, включения или возврата в исходное положение автоматического выключателя Masterpact MTZ.

Предварительные условия для соединения через NFC

Чтобы установить беспроводное соединение через NFC с блоком управления Micrologic X, необходимы следующие условия:
- Необходимо иметь доступ в помещение, где установлен автоматический выключатель Masterpact MTZ.
- На смартфоне должно быть установлено мобильное приложение Masterpact MTZ.
- Подключаемый смартфон должен поддерживать связь через NFC.

Любой пользователь при выполнении вышеуказанных условий может загрузить данные, которые могут иметь важное значение при эксплуатации электроустановки. В блоке управления Micrologic X не сохраняются записи о соединениях, устанавливаемых через NFC.

За более подробной информацией о рекомендациях по установке соединения через NFC обратитесь к документу *«Блок контроля и управления Micrologic X. Руководство пользователя»*.

Основные рекомендации по защите доступа через NFC

Для защиты данных, доступных через NFC, рекомендуется:
- Устанавливать автоматические выключатели Masterpact MTZ в запираемых помещениях с ограниченным доступом, чтобы ограничить доступ к блоку управления Micrologic X неавторизованным пользователям.
- Постоянно контролировать доступ в это помещение.
- Предоставлять ключи или коды доступа только авторизованному персоналу.

За дополнительной информацией о защите доступа к выключателям Masterpact MTZ обратитесь к рекомендациям по ограничению доступа (*см. стр. 20*).

Рекомендации для связи через NFC

Для защиты доступа к функциям через NFC рекомендуется:
- Отключать смартфон от Интернета во время соединения через NFC с блоком управления Micrologic X.
- Отключать связь Bluetooth на смартфоне.
- Не вводить никаких кодов, даже если он запрашивается, потому что для подключения через NFC никаких кодов не требуется.

Рекомендации по использованию мобильного приложения Masterpact MTZ

Чтобы ограничить доступ к блоку управления Micrologic X со смартфона, рекомендуется для подключения к Masterpact MTZ использовать только официальное мобильное приложение Schneider Electric.

Рекомендации по использованию смартфонов

Для ограничения доступа к блоку управления Micrologic X со смартфона рекомендуется:
- Убедиться, что смартфоны, имеющие мобильное приложение Masterpact MTZ Mobile, защищены паролем и используются только для работы.
- Защитить смартфоны с мобильным приложением Masterpact MTZ, выполнив все функции по безопасности, рекомендованные продавцом или производителем смартфонов.
- Использовать современные антивирусные приложения для смартфонов.
- Не сообщать информацию о смартфоне (номер телефона, MAC-адрес) без необходимости.
- Отключать смартфон от Интернета во время соединения через NFC с блоком управления Micrologic X.
- Не хранить секретную или конфиденциальную информацию на смартфонах.

Рекомендации по защите доступа через Bluetooth

Функции, доступные через Bluetooth

По беспроводной связи через Bluetooth (BLE) возможно получить доступ к блоку управления Micrologic X с помощью смартфона, на котором установлено мобильное приложение Masterpact MTZ. Это приложение адаптировано под интерфейс блока управления Micrologic X. Передаваемые через Bluetooth данные шифруются с использованием 128-битного шифрования AES.

Предварительные условия для соединения через Bluetooth

Для беспроводного соединения через Bluetooth с блоком управления Micrologic X необходимо выполнить следующие условия:
- Блок управления Micrologic X должен быть включен.
- На блоке управления Micrologic X должна быть включена функция Bluetooth.
- Одновременно только один смартфон может подключаться к блоку управления.
- На смартфоне должно быть установлено мобильное приложение Masterpact MTZ.
- Смартфон должен поддерживать связь через Bluetooth (4.0 или выше).
- Необходимо иметь доступ к блоку управления Micrologic X для активации кнопки Bluetooth, т.е. физически находиться в радиусе действия (обычно от 20 до 30 метров) в течение всего времени соединения.

Любой человек, который выполнил эти условия и установил соединение, имеет доступ к важной информации об электроустановке.

За дополнительной информацией, обратитесь к документу *«Блок контроля и управления Micrologic X. Руководство пользователя»*.

Общие рекомендации по защите доступа через Bluetooth

Для защиты обращения к функциям, доступным через беспроводной Bluetooth, рекомендуется:
- Устанавливать автоматические выключатели Masterpact MTZ в запираемых помещениях с ограниченным доступом, чтобы ограничить доступ к блоку управления Micrologic X неавторизованным пользователям.
- Постоянно контролировать доступ в это помещение.
- Предоставлять ключи или коды доступа только авторизованному персоналу.

За дополнительной информацией о защите доступа к выключателям Masterpact MTZ обратитесь к рекомендациям по ограничению доступа (*см. стр. 20*).

Рекомендации по использованию Bluetooth

Для защиты обращения к функциям, доступным через Bluetooth, рекомендуется:
- Отключить функцию Bluetooth на блоке управления Micrologic X, как описано в документе *«Блок контроля и управления Micrologic X. Руководство пользователя»* и включать только тогда, когда необходимо установить соединение.
- Установить таймер отключения соединения через Bluetooth на 5 минут.
- За исключением сеансов установления соединения Bluetooth, не рекомендуется нажимать кнопку активации Bluetooth на передней панели блока управления Micrologic X. Связь по Bluetooth должна быть отключена, если она не используется.
- По окончании сеанса всегда нажимать кнопку Bluetooth для завершения связи.
- Выполнять соединение как можно реже и в безопасной зоне, чтобы злоумышленники не могли увидеть вводимый код соединения.
- Не вводить код соединения, если это соединение не оправдано.
- Во время соединения через Bluetooth держать смартфон как можно ближе к блоку управления Micrologic X.

Рекомендации по использованию мобильного приложения Masterpact MTZ

Чтобы ограничить доступ к блоку управления Micrologic X со смартфона, рекомендуется для подключения к Masterpact MTZ использовать только официальное мобильное приложение Schneider Electric.

Рекомендации по использованию смартфонов

Для ограничения доступа к блоку управления Micrologic X со смартфона рекомендуется:

- Убедиться, что смартфоны, имеющие мобильное приложение Masterpact MTZ Mobile, защищены паролем и используются только для работы.
- Защитить смартфоны с мобильным приложением Masterpact MTZ, выполнив все предписания по безопасности, рекомендованные продавцом или производителем смартфонов.
- Использовать современные антивирусные приложения для смартфонов.
- Не сообщать информацию о смартфоне (номер телефона, MAC-адрес) без необходимости.
- Отключать смартфон от Интернета во время соединения через NFC с блоком управления Micrologic X.
- Не хранить секретную или конфиденциальную информацию на смартфонах.

Рекомендации по защите доступа к блоку управления Micrologic X через порт mini-USB

Функции, доступные через порт mini-USB

При подключении компьютеру, на котором установлено программное обеспечение Ecoreach или другое программное обеспечение для блоков контроля и управления, через порт mini-USB блока управления можно получить доступ ко всем функциям блока Micrologic X.

Обратите внимание, что никакие носители информации не могут быть подключены к порту mini-USB блока управления Micrologic X. Поэтому никакие вредоносные программы с USB-носителей напрямую в блок управления не могут быть загружены.

Предварительные условия для соединения через порт mini-USB

Для соединения с блоком управления Micrologic X через порт mini-USB необходимо иметь:
- Физический доступ в помещение, в котором установлен автоматический выключатель Masterpact MTZ.
- Кабель с разъемом mini-USB для подключения компьютера к порту mini-USB на блоке управления Micrologic X.
- Компьютер с установленным программным обеспечением Ecoreach.

Общие рекомендации по защите доступа через порт mini-USB

Для защиты обращений к функциям, доступным через порт mini-USB, рекомендуется:
- Устанавливать автоматические выключатели Masterpact MTZ в запираемых помещениях с ограниченным доступом, чтобы ограничить доступ к блоку управления Micrologic X неавторизованным пользователям.
- Постоянно контролировать доступ в это помещение.
- Предоставлять ключи или коды доступа только авторизованному персоналу.

За дополнительной информацией о защите доступа к выключателям Masterpact MTZ, обратитесь к рекомендациям по ограничению доступа (*см. стр. 20*).

Рекомендации по использованию компьютеров с ПО Ecoreach

Для защиты доступа к блоку управления Micrologic X с компьютера, подключенного непосредственно к порту mini-USB на передней панели блока управления, рекомендуется:
- Хранить компьютер в безопасном месте, когда он не используется.
- Убедиться, что компьютеры, с которых запускается ПО Ecoreach, требуют ввода логина и пароля пользователя.
- Принудительно использовать надежные пароли (*см. стр. 16*)
- Контролировать регулярные изменения паролей пользователей.
- Запретить повторное использование устаревших паролей.
- Установить таймер блокировки экрана компьютера после определенного периода бездействия.
- Защитить компьютеры, выполнив все предписания по безопасности, рекомендованные продавцом или производителем компьютеров.
- Ограничить число пользователей, которым разрешено использовать ПО Ecoreach.

Глава 4
Рекомендации по кибербезопасности для удаленного доступа

Описание главы

В этой главе перечислены каналы удаленного доступа к автоматическим выключателям Masterpact MTZ. Также в ней приведены рекомендации по обеспечению безопасности доступа по различным каналам. Это важные соображения для управления аппаратом.

Содержание главы

Эта глава содержит следующие части:

Наименование	Стр.
Ограничение удаленного доступа к автоматическим выключателям Masterpact MTZ	28
Отделение промышленной сети предприятия от корпоративной сети	29
Рекомендации по защите удаленного доступа к блоку управления Micrologic X через Ethernet	30

Ограничение удаленного доступа к автоматическим выключателям Masterpact MTZ

Обзор

ИМУ с выключателями Masterpact MTZ имеют возможности доступа как по месту, так и дистанционно. Необходимо убедиться, что этот доступ имеют только авторизованные пользователи.

Удаленный доступ к автоматическим выключателям Masterpact MTZ

В зависимости от архитектуры сети возможно несколько способов удаленного доступа к автоматическим выключателям Masterpact MTZ. В частности, удаленный доступ через Ethernet может предоставлять полный контроль за электроустановкой. Поэтому крайне важно контролировать удаленный доступ к системе в целом.

В частности, необходимо контролировать:

- Доступ к системе с использованием различных доступных каналов связи (*см. стр. 11*)
- Информацию и элементы управления, доступные через каждый канал связи (*см. стр. 14*)

Управление дистанционным включением и отключением автоматического выключателя Masterpact MTZ

Дистанционное управление выключателем Masterpact MTZ предполагает возможность выполнения следующих действий:

- Отключение, включение и возврат в исходное состояние выключателя
- Изменение настроек автоматического выключателя

Если дистанционное управление выключателем Masterpact MTZ не является обязательным требованием, настоятельно рекомендуется отключить его с помощью интерфейса IFE или EIFE. По умолчанию дистанционное управление включено.

На интерфейсе IFE используйте блокировку на передней панели, чтобы включить или отключить удаленное управление по сети Ethernet.

Для интерфейса EIFE подключите компьютер с программным обеспечением Ecoreach к порту mini-USB на передней панели блока управления Micrologic X, чтобы включить или отключить возможность дистанционного управления выключателем Masterpact MTZ через сеть Ethernet.

Блокировка настроек защиты

Для предотвращения дистанционного внесения изменений настроек защиты автоматических выключателей Masterpact MTZ эту функцию нужно заблокировать.

По умолчанию, дистанционное изменение параметров защиты с интерфейса разрешено.

Рекомендуется отключить дистанционное изменение параметров защиты, если эта функция не используется. За дополнительной информацией, обратитесь к документу *«Блок контроля и управления Micrologic X. Руководство пользователя»*.

Отделение промышленной сети предприятия от корпоративной сети

Обзор

При проектировании и внедрении промышленной сети предприятия необходимо использовать механизмы разделения, чтобы содержать ее отдельно от корпоративной сети.

Это помогает ограничить доступ к ИМУ с выключателями Masterpact MTZ.

В частности, необходимо учитывать:
- Использование брандмауэров
- Создание безопасных зон
- Использование систем обнаружения вторжений (IDS) и / или систем предотвращения вторжений (IPS)
- Внедрение политики безопасности и программ обучения
- Создание механизмов реагирования на инциденты

Руководящие принципы создания промышленной сети предприятия и отделения ее от корпоративной интрасети выпускаются и обновляются специализированными организациями (например, NIST) и органами стандартизации (например, ISO, IEC / IEEE).

Обратитесь к этим публикациям для рассмотрения вышеперечисленных вопросов.

Рекомендации по защите удаленного доступа к блоку управления Micrologic X через Ethernet

Функции, доступные через Ethernet

Когда блок управления Micrologic X подключен к интерфейсу EIFE или IFE, все функции блока управления доступны с ПК, подключенного к сети Ethernet, и на нем запущено ПО Ecoreach или другое программное обеспечение для мониторинга и управления.

Предварительные условия для соединения через Ethernet

Для установления Ethernet-соединения с блоком управления Micrologic X необходимы следующие условия:

- Блок управления Micrologic X должен быть включен.
- Блок управления Micrologic X должен быть подключен к сети Ethernet через интерфейс EIFE или IFE.
- Необходим ПК или другое устройство (например, FDM128 или ПЛК), работающее с программным обеспечением мониторинга и управления (SCADA, Ecoreach), подключенным к сети Ethernet, обеспечивающей удаленный доступ.
- Необходимы ID пользователя и пароль с соответствующими правами доступа для входа в программное обеспечение Ecoreach.

Рекомендации для компьютеров, подключаемых к Ethernet

Для защиты доступа к блоку управления Micrologic X с сетевого компьютера, рекомендуется:

- Держать компьютеры безопасно закрытыми, когда они не используются.
- Убедиться, что на компьютерах, которые подключаются к блоку управления Micrologic X, используя Ethernet, например, через веб-страницы SCADA, IFE или EIFE, требуется логин и пароль пользователя
- Принудительно использовать надежные пароли (*см. стр. 15*).
- Контролировать регулярные изменения паролей пользователей.
- Запретить повторное использование устаревших паролей.
- Установить таймер блокировки экрана компьютера после определенного периода бездействия.
- Защитить компьютеры, выполнив все предписания по безопасности, рекомендованные продавцом или производителем компьютеров.
- Ограничить число пользователей, которым разрешено использовать ПО Ecoreach.

В дополнение к вышеуказанным мерам предосторожности также необходимо следовать общим рекомендациям и рекомендациям по защите установки, приведенным в документе *«Как уменьшить уязвимость к кибератакам?»*.

Глава 5
Рекомендации по кибербезопасности при обновлении программного обеспечения и цифровых модулей

Содержание главы

Эта глава содержит следующие части:

Наименование	Стр.
Установка обновлений программного обеспечения	32
Покупка и установка цифровых модулей	34

Установка обновлений программного обеспечения

Обзор

Все более распространенным видом кибератак становится распространение поддельного или противозаконного программного обеспечения, которое может содержать модифицированные или дополнительные приложения. Эти приложения могут ставить под угрозу целостность исходного программного обеспечения и его предполагаемое использование.

Для обеспечения целостности всех компонентов ИМУ с выключателем Masterpact MTZ, а именно блока управления Micrologic X, интерфейсов IFE или EIFE и модуля ввода-вывода IO, все оригинальные обновления прошивок Schneider Electric имеют цифровую подпись.

Необходимо убедиться, что любая устанавливаемая прошивка получена с официального центра загрузки Schneider Electric. Загруженное программное обеспечение может быть установлено только после проверки цифровой подписи Schneider Electric.

Рекомендации по кибербезопасности при обновлении программного обеспечения

Важно устанавливать все обновления прошивок, которые предназначены для повышения защиты и безопасности.

При установке обновлений прошивок для компонентов ИМУ с выключателем Masterpact MTZ рекомендуется:

- Устанавливать цифровые модули для «operational technology» (OT) сети предприятия с планированием последующего тестирования на неподключенной электроустановке перед включением аппаратов для дальнейшей эксплуатации.
- Для загрузки и обновления прошивок использовать только программное обеспечение Ecoreach.
- Перед установкой цифровых модулей убедитесь, что программное обеспечение Ecoreach использует последний официальный сертификат.
- Защитите компьютеры, используемые для загрузки цифровых модулей, в соответствии с последними рекомендациями разработчика операционной системы.

Защищенное программное обеспечение

Все программное обеспечение, предназначенное для ИМУ с выключатели Masterpact MTZ, использует инфраструктуру открытых ключей Schneider Electric. Цифровая подпись может быть проверена с помощью публичного сертификата, который находится в программном обеспечении Ecoreach.

При обновлении прошивок для ИМУ с выключателями Masterpact MTZ и блока управления Micrologic X автоматически проверяется цифровая подпись для всего пакета обновлений. Эта проверка осуществляется с помощью публичного сертификата, находящегося в блоке управления.

По соображениям безопасности публичные сертификаты могут меняться. Поэтому одним из основных требований безопасности является ответственность пользователя за проверку версий программного обеспечения Ecoreach, которое используется для загрузки и обновления прошивок.

Также пользователь отвечает за проверку сертификатов используемого оборудования на предмет их старения или отзыва, прежде чем загружать какие-либо обновления прошивки.

Сертификаты, которые больше недействительны, публикуются в списке отозванных сертификатов (CRL). Этот список доступен на официальном сайте Schneider Electric.

Преимущества использования программного обеспечения Ecoreach для обновления прошивок

Программное обеспечение Ecoreach выполняет важные функции, помогая обеспечить целостность сети предприятия во время обновления прошивки. Для загрузки и установки обновлений прошивок рекомендуется использовать только Ecoreach, потому что это единственное программное обеспечение, которое представляет следующие преимущества:

- При входе в ПО Ecoreach, появляется автоматическое уведомление, если публичный сертификат необходимо продлить.
- При скачивании обновлений прошивок с официального сайта Schneider Electric через ПО Ecoreach цифровая подпись прошивок проверяется автоматически.
- При подключении к блоку управления Micrologic X с помощью ПО Ecoreach цифровая подпись прошивки блока управления проверяется автоматически.
- При загрузке обновлений программного обеспечения для блока управления Micrologic X с помощью ПО Ecoreach через USB-соединение цифровая подпись обновлений проверяется автоматически.

Обратитесь к интерактивной справке ПО Ecoreach за подробными указаниями, как обновить публичный сертификат, а также для загрузки и установки обновлений прошивок.

Автоматические проверки, выполняемые ПО Ecoreach, полностью зависят от действия публичного сертификата, который оно использует.

⚠ ВНИМАНИЕ

ОПАСНОСТЬ НЕПРЕДВИДЕННЫХ ДЕЙСТВИЙ

Обновите публичный сертификат, хранящийся в программном обеспечении Ecoreach, как только вы получите уведомление о том, что текущий сертификат отменен.

Регулярно проверяйте список отозванных сертификатов, публикуемый на официальном сайте Schneider Electric.

Несоблюдение этих инструкций может привести к смерти, серьезной травме или повреждению оборудования.

Необновление отозванного сертификата лишает доверия к подлинности цифровых модулей.

Проверка списка отозванных сертификатов

Регулярно, не менее 1 раза в 3 месяца, необходимо проверять список отозванных сертификатов (CRL), публикуемый Schneider Electric, чтобы быть уверенным, что в нем нет сертификатов, используемых вашим оборудованием.

Для проверки списка отозванных сертификатов выполните следующие действия:

Шаг	Действие
1	Загрузите список сертификатов, публикуемый на веб-сайте Schneider Electric.
2	Если список пуст, это означает, что все используемые сертификаты действительны. Никаких дальнейших действий не требуется. Если же список не пуст, необходимо выполнить шаг 3.
3	С помощью ПО Ecoreach нужно получить серийные номера всех сертификатов, используемых оборудованием в электроустановке, и сравнить их с данными, указанными на официальном сайте Schneider Electric.
4	Если серийные номера отличаются, значит используемые сертификаты действительны. Никаких дальнейших действий не требуется. Если некоторые серийные номера одинаковы, значит, что в электроустановке есть устройства, использующие отозванные сертификаты. Эти сертификаты необходимо обновить. При необходимости обратитесь в Schneider Electric.

Покупка и установка цифровых модулей

Обзор

Цифровые модули – это дополнительные программы, которые расширяют возможности блоков управления Micrologic X. Их можно приобрести вместе с автоматическими выключателями Masterpact MTZ при заказе аппарата или позднее через цифровой онлайн-магазин Schneider Electric GoDigital.

Для обеспечения дополнительной безопасности все цифровые модули блоков управления Micrologic X снабжены цифровой подписью с использованием инфраструктуры открытых ключей – public key infrastructure (PKI) Schneider Electric. PKI помогает обеспечить подлинность и целостность загрузок цифровых модулей.

Цифровые модули устанавливаются в блок управления с помощью программного обеспечения Ecoreach.

Рекомендации по кибербезопасности при покупке цифровых модулей

Для покупки цифровых модулей к блоку управления Micrologic X пользуйтесь только официальным цифровым магазином Schneider Electric GoDigital.

При установке цифровых модулей для компонентов ИМУ с выключателем Masterpact MTZ рекомендуется:

- Устанавливать цифровые модули для «operational technology» (OT) сети предприятия с планированием последующего тестирования на неподключенной электроустановке перед включением аппаратов для дальнейшей эксплуатации.
- Использовать только программное обеспечение Ecoreach.
- Перед установкой цифровых модулей убедиться, что программное обеспечение Ecoreach использует последний официальный сертификат.
- Защитить компьютеры, используемые для загрузки цифровых модулей, в соответствии с последними рекомендациями разработчика операционной системы.

Рекомендации по кибербезопасности при установке цифровых модулей

Для установки цифровых модулей для блока управления Micrologic X необходимо использовать только программное обеспечение Ecoreach.

Программное обеспечение Ecoreach играет важную роль, помогая обеспечить целостность сети промышленного предприятия.

Для установки цифровых модулей необходимо использовать именно ПО Ecoreach, потому что это единственное программное обеспечение, которое предоставляет следующие преимущества:

- При входе в программное обеспечение Ecoreach пользователь автоматически уведомляется, если официальный сертификат должен быть продлен.
- При подключении к блоку управления Micrologic X с помощью ПО Ecoreach, цифровая подпись прошивки блока управления проверяется автоматически.
- При загрузке цифрового модуля управления Micrologic X с помощью ПО Ecoreach через USB-соединение цифровая подпись модуля проверяется автоматически.

Вход в ПО Ecoreach с компьютера, подключенного к сети Интернет, предоставляет подробные инструкции, объясняющие как продлить сертификат, как загрузить и установить цифровые модули. Автоматическая проверка ПО Ecoreach выполняется, полностью полагаясь на действие официального сертификата.

⚠ ВНИМАНИЕ

ОПАСНОСТЬ НЕПРЕДВИДЕННЫХ ДЕЙСТВИЙ

Обновите публичный сертификат, хранящийся в программном обеспечении Ecoreach, как только вы получите уведомление о том, что текущий сертификат отменен.

Регулярно проверяйте список отозванных сертификатов, публикуемый на официальном сайте Schneider Electric.

Несоблюдение этих инструкций может привести к смерти, серьезной травме или повреждению оборудования.

Необновление отозванного сертификата лишает доверия к подлинности цифровых модулей.

Проверка списка отозванных сертификатов

Регулярно, не менее 1 раза в 3 месяца, необходимо проверять список отозванных сертификатов (CRL), публикуемый Schneider Electric, чтобы быть уверенным, что в нем нет сертификатов, используемых вашим оборудованием.

Для проверки списка отозванных сертификатов выполните следующие действия:

Шаг	Действие
1	Загрузите список сертификатов, публикуемый на веб-сайте Schneider Electric.
2	Если список пуст, это означает, что все используемые сертификаты действительны. Никаких дальнейших действий не требуется. Если же список не пуст, необходимо выполнить шаг 3.
3	С помощью ПО Ecoreach нужно получить серийные номера всех сертификатов, используемых оборудованием в электроустановке, и сравнить их с данным, указанными на официальном сайте Schneider Electric.
4	Если серийные номера отличаются, значит используемые сертификаты действительны. Никаких дальнейших действий не требуется. Если некоторые серийные номера одинаковы, значит, что в электроустановке есть устройства, использующие отозванные сертификаты. Эти сертификаты необходимо обновить. При необходимости обратитесь в Schneider Electric.

Глоссарий терминов

B

BLE – Bluetooth low energy

Высокоскоростной протокол радиосвязи с низким энергопотреблением.

E

EIFE – Embedded Ethernet interface

Дополнительный встраиваемый модуль интерфейса Ethernet для выкатных автоматических выключателей Masterpact MTZ. Через этот модуль выключатель доступен через сеть Интранет компании.

G

GoDigital

Цифровой онлайн-магазин Schneider Electric для покупки цифровых модулей, предназначенных для блока управления Micrologic X.

H

HMI – Human-machine interface

Человеко-машинный интерфейс. Понятие применяется к экранам дисплея устройства, с помощью которых пользователь может прочитать информацию или посмотреть настройки устройства.

I

IC – Industrial control

Сеть промышленного предприятия. Она включает в себя аппараты и программное обеспечение, используемое для контроля и управления производственными процессами предприятия.

IFE – Ethernet interface

Модуль интерфейса Ethernet, который может быть подключен к автоматическому выключателю Masterpact MTZ. Через этот модуль выключатель доступен через сеть Интранет компании.

IMU – Intelligent modular unit

Интеллектуальное модульное устройство (ИМУ). ИМУ включает в себя автоматический выключатель Masterpact MTZ с его встроенными средствами связи (блок управления Micrologic) и внешние ULP-модули (модуль ввода/вывода IO), коммуникационные интерфейсы IFE или EIFE.

IP – Internet protocol

Интернет-протокол. IP-адреса используются для идентификации устройств, подключенных к корпоративной сети или к Интернету.

IT – Information technology

Информационная сеть предприятия. Понятие относится к информационным системам и сети компании, отделяет от сети предприятия (IC) и оперативно-технологической сети (OT).

L

LAN – Local area network

Локальная сеть. Относится к корпоративной сети.

N

NFC – Near field communication

Беспроводной протокол связи близкого действия.

O

OT – Operational technology

Оперативно-технологическая сеть предприятия. Понятие относится к аппаратному и программному обеспечению систем предприятия, используемому для непосредственного мониторинга и контроля производственных процессов и оборудования, синоним названия – сеть промышленного предприятия (IC). Название «OT» часто используется, чтобы обратиться к оперативной сети компании в отличие от информационной (IT) сети.

P

PIN – Personal identification number

Персональный идентификационный номер.

PKI – Public key infrastructure

Инфраструктура открытых ключей. Она представляет собой набор сервисов, используемых для создания и проверки подлинности электронной цифровой подписи. Инфраструктура открытых ключей предназначена для обеспечения конфиденциальности, целостности и аутентичности информации.

R

RAS – Remote access server

Удаленный сервер.

S

SCADA – Supervisory control and data acquisition

Диспетчерское управление и сбор данных. Относится к системам, предназначенным для получения данных в реальном времени по производственным процессам и оборудованию с целью контроля и управления ими дистанционно.

T

TCP/IP – Transmission control protocol/Internet protocol

Протокол данных /Интернет-протокол. Набор протоколов, используемых для обмена данными через Интернет.

V

VPN – Virtual private network

Виртуальные частные сети. VPN используют для создания защищенного / частного канала связи между авторизованными внешними точками доступа и надежной корпоративной сети.

Schneider Electric в странах СНГ

Пройдите бесплатное онлайн-обучение в Энергетическом Университете и станьте профессионалом в области энергоэффективности.

Для регистрации зайдите на www.MyEnergyUniversity.com

Беларусь

Минск
220007, ул. Московская, 22-9
Тел.: (37517) 236 96 23
Факс: (37517) 236 95 23

Казахстан

Алматы
050010, пр-т Достык, 38
Бизнес-центр «Кен Дала», этаж 5
Тел.: (727) 357 23 57
Факс: (727) 357 24 39
Центр поддержки клиентов: (727) 357 24 41
ccc.kz@schneider-electic.com

Астана
010000, ул. Достык, 20
Бизнес-центр «Санкт-Петербург», офисы 1503, 1504
Тел.: (7172) 42 58 20
Факс: (7172) 42 58 19
Центр поддержки клиентов: (727) 357 24 41
ccc.kz@schneider-electic.com

Атырау
060005, пр. Азаттык, 48
Бизнес-центр «Premier-Atyrau»
Тел.: (7122) 30 94 55
Центр поддержки клиентов: (727) 357 24 41
ccc.kz@schneider-electic.com

Россия

Владивосток
690091, ул. Пологая, 3, офис 306
Тел.: (4212) 40 08 16

Волгоград
400089, ул. Профсоюзная, 15, офис 12
Тел.: (8442) 93 08 41

Воронеж
394026, пр-т Труда, 65, офис 227
Тел.: (473) 239 06 00
Тел./факс: (473) 239 06 01

Екатеринбург
620014, ул. Б. Ельцина ,1 А
Бизнес-центр «Президент», этаж 14
Тел.: (343) 378 47 36
Факс: (343) 378 47 37

Иркутск
664047, ул. 1-я Советская, 3 Б, офис 312
Тел./факс: (3952) 29 00 07, 29 20 43

Казань
420107, ул. Спартаковская, 6, этаж 7
Тел./факс: (843) 526 55 84 / 85 / 86 / 87 / 88

Калининград
236040, Гвардейский пр., 15
Тел.: (4012) 53 59 53
Факс: (4012) 57 60 79

Краснодар
350063, ул. Кубанская набережная, 62 /
ул. Комсомольская, 13, офис 803
Тел./факс: (861) 214 97 35, 214 97 36

Красноярск
660021, ул. Горького, 3 А, офис 302
Тел.: (3912) 56 80 95
Факс: (3912) 56 80 96

Москва
127018, ул. Двинцев, 12, корп. 1
Бизнес-центр «Двинцев»
Тел.: (495) 777 99 90
Факс: (495) 777 99 92

Мурманск
183038, ул. Воровского, 5/23
Конгресс-отель «Меридиан», офис 421
Тел.: (8152) 28 86 90
Факс: (8152) 28 87 30

Нижний Новгород
603000, пер. Холодный, 10 А, этаж 8
Тел./факс: (831) 278 97 25, 278 97 26

Новосибирск
630132, ул. Красноярская, 35
Бизнес-центр «Гринвич»
Офис 1309
Тел./факс: (383) 227 62 53, 227 62 54

Омск
644043, ул. Герцена, 34
Бизнес-центр «Герцен Plaza», этаж 6
Тел.: (906) 197 85 31

Пермь
614010, Комсомольский пр-т, 98
Офис 11
Тел./факс: (342) 281 35 15, 281 34 13, 281 36 11

Ростов-на-Дону
344002, ул. Социалистическая, 74
Офис 1402
Тел./факс: (863) 218 65 88, 218 65 89

Самара
443080, пр-т Карла Маркса, 201 Б
БК «Башня», офисы 501, 505
Тел.: (846) 374 80 70
Факс: (846) 374 80 71

Санкт-Петербург
196158, Пулковское шоссе, 40, корп. 4,
литера А
Бизнес-центр «Технополис»
Тел.: (812) 332 03 53
Факс: (812) 332 03 52

Уфа
450098, пр-т Октября, 132/3 (бизнес-центр КПД)
Блок-секция № 3, этаж 9
Тел.: (347) 279 98 29
Факс: (347) 279 98 30

Хабаровск
680000, ул. Тургенева 26 А, офис 510
Тел.: (4212) 30 64 70
Факс: (4212) 30 46 66

Украина

Днепр
49000, ул. Глинки, 17, этаж 4
Тел.: (056) 79 00 888
Факс: (056) 79 00 999

Киев
04073, пр-т С. Бандеры, 13 В, литера А
Тел.: (044) 538 14 70
Факс: (044) 538 14 71

Львов
79015, ул. Героев УПА, 72, корп. 1
Тел./факс: (032) 298 85 85

Николаев
54030, ул. Никольская, 25
Бизнес-центр «Александровский»
Офис 5
Тел.: (0512) 58 24 67
Факс: (0512) 58 24 68

Центр поддержки клиентов
Тел.: 8 (800) 200 64 46 (многоканальный)
Тел.: (495) 777 99 88, факс: (495) 777 99 94
ru.ccc@schneider-electric.com
www.schneider-electric.com
Время работы: 24 часа 5 дней в неделю
(с 23.00 воскресенья до 23.00 пятницы)

MKP-MAN-MTZSG-17
09/2017