Практический обзор внедрения уровней безопасности МЭК 62443 в приложениях промышленных систем управления

Автор: Daniel DesRuisseaux (Даниель ДеРюсо)
Директор отраслевой программы кибербезопасности
Schneider Electric

Сводная информация

Требования современных приложений промышленного Интернета вещей (IIoT) увеличивают сложность системной инфраструктуры и оказывают дополнительное воздействие на безопасность IT и OT.
С возрастанием частоты и сложности кибератак предприятия должны использовать отраслевые стандарты для обеспечения постоянной защиты.
В этом документе будет рассмотрен вопрос о том, как МЭК 62443 может быть применен к промышленным системам управления и поможет читателям понять различные приоритеты и шаги, необходимые для противодействия киберугрозам.

Содержание

Введение

За последнее десятилетие промышленные системы управления (ICS) пережили экспоненциальный рост кибератак. Отрасль отреагировала на угрозы кибербезопасности, разработав стандарты для содействия конечным пользователям и поставщикам оборудования в процессе обеспечения безопасности промышленных систем управления. Сегодня на рынке существует ряд ключевых стандартов. МЭК 62443 был разработан комитетами ISA99 и МЭК для повышения безопасности, доступности, целостности и конфиденциальности компонентов или систем, используемых в промышленной автоматизации и управлении. Стандарты серии МЭК 62443 могут использоваться во всех сегментах промышленного управления и одобрены многими странами. МЭК 62443 развился до ключевого стандарта отрасли, и Schneider Electric строит свою стратегию кибербезопасности на его основе.

Этот документ предназначен для тех, кто не имеет специальных знаний в области кибербезопасности промышленных систем управления.
Данный документ – руководство по применению с практическими примерами. Обратите внимание, что это общий документ, предназначенный для понимания концепций – приведенные здесь рекомендации не должны использоваться для защиты промышленных систем управления без подробного изучения конкретных сетей.

EcoStruxure

EcoStruxure™ – это открытая, интероперабельная, IoT-совместимая системная архитектура и платформа Schneider Electric. EcoStruxure использует достижения в области Интернета вещей (IoT), мобильных, сенсорных и облачных технологий, аналитики и кибербезопасности для инноваций на всех уровнях. В нее входят подключенные продукты, управление в реальном времени, приложения, аналитика и службы. EcoStruxure имеет более чем 450 000 инсталляций при поддержке 9000 системных интеграторов, и более одного миллиарда подключенных устройств.

Рисунок 1

Одним из ключевых требований архитектуры EcoStruxure является обеспечение сквозной кибербезопасности. В этой информационной статье мы рассмотрим, как Schneider Electric использует основанные на стандартах методы для обеспечения безопасности своих решений EcoStruxure.

Понятия кибербезопасности

В этом разделе будут представлены понятия, которые необходимы для понимания рекомендаций, представленных ниже в документе.

Уровни обеспечения безопасности

Стандарт МЭК 62443 содержит понятие уровней безопасности. Понятие определяется как ряд требований, предназначенных для обеспечения безопасности системы на одном из четырех определенных уровней. Сводка по каждому уровню в сочетании с характеристикой типа атакующего, для защиты от которого разработан каждый уровень безопасности, представлена в таблице ниже.

Таблица 1

Уровень безопасности	Цель	Навыки	Мотивация	Средства	Ресурсы
SL1	Случайное нарушение или по совпадению	Нет навыков атак	Ошибки	Непреднамеренные	Один человек
SL2	Киберпреступление, хакерство	Общие	Низкая	Простые	Недостаточные (отдельный человек)
SL3	Хактивист, террорист	Знаниие специфики ICS	Средняя	Изощренные (атака)	Умеренные (хакерская группа)
SL4	Национальное государство	Знание специфики ICS	Высокая	Изощренные (кампания)	Расширенные (многопрофильная команда)

Конечные пользователи, заинтересованные в предоставлении решения, которое предназначено для борьбы с атаками от обычных хакеров или киберпреступников, должны, например, реализовать систему с функциями, указанными в уровне обеспечения безопасности 2. Обратите внимание, что характеристики, представленные в таблице, являются общей классификацией для обеспечения общего уровня понимания клиентов. Внедрение SL2 не гарантирует, что система может остановить атаку любых хакеров или киберпреступников.

Многоуровневая защита

Многоуровневая защита – это скоординированное использование контрмер безопасности для защиты целостности информационных активов в сети. Правильная реализация стратегии многоуровневой защиты предполагает реализацию шести шагов. Ниже приводится краткое описание каждого шага.

- *Создание плана обеспечения безопасности* – важнейшим шагом в процессе многоуровневой защиты является создание плана обеспечения безопасности. В плане безопасности персонал проводит детальный аудит всего оборудования, подключенного к сети промышленного управления, сопоставляет, как подключено оборудование, проверяет конфигурацию безопасности оборудования и оценивает потенциальные уязвимости системы. План безопасности включает в себя влияние продуктов, архитектуры, людей и корпоративных процессов. Прежде чем предпринимать какие-либо дополнительные шаги для повышения безопасности системы, необходимо составить план обеспечения безопасности. В противном случае персонал может ошибочно подумать, что система безопасна, не зная о потенциальных векторах атаки.

- *Отдельные сети* – после того как в плане безопасности будет создана подробная карта сети, сети могут быть разделены по основной функции. Примером может быть разделение сети на корпоративную, заводскую, технологическую и полевую зоны. Должны быть определены все каналы передачи данных между зонами.

- *Защита периметра* – на этом этапе надежно защищаются каналы передачи данных между зонами. Важной частью этого шага является защита удаленного доступа.

- *Сегментация сети* – на этом этапе зоны, созданные на втором шаге, можно разделить на более мелкие зоны по местоположению или функции. Периметры этих сегментированных зон должны быть защищены. Важно отметить, что уровень безопасности, присвоенный каждой зоне, может варьироваться. Например, уровень безопасности зоны, связанной с мониторингом оборудования, может быть установлен на уровень 1, тогда как уровень безопасности зоны, связанной с системой защиты, может быть установлен на уровень 3. Уровень каждой сегментированной зоны не обязательно должен совпадать с уровнем соседних зон.

- *Повышение защищенности устройств* – добавление функций на устройства ICS для повышения их способности противостоять кибератакам. Это уменьшает вероятность того, что сетевые элементы будут скомпрометированы, если хакер получит доступ к сети.

- *Мониторинг и обновление* – активный мониторинг активности в сети для обнаружения потенциальных угроз и установка исправлений в продукты по мере доступности нового программного обеспечения/прошивки для устранения уязвимостей или для добавления функций безопасности.

Многим заказчикам промышленных систем управления не хватает знаний в области кибербезопасности. Schneider Electric создала практику оказания услуг кибербезопасности, чтобы помочь этим клиентам. Специалисты по безопасности Schneider могут оказать содействие клиентам в разработке и внедрении стратегии многоуровневой защиты.

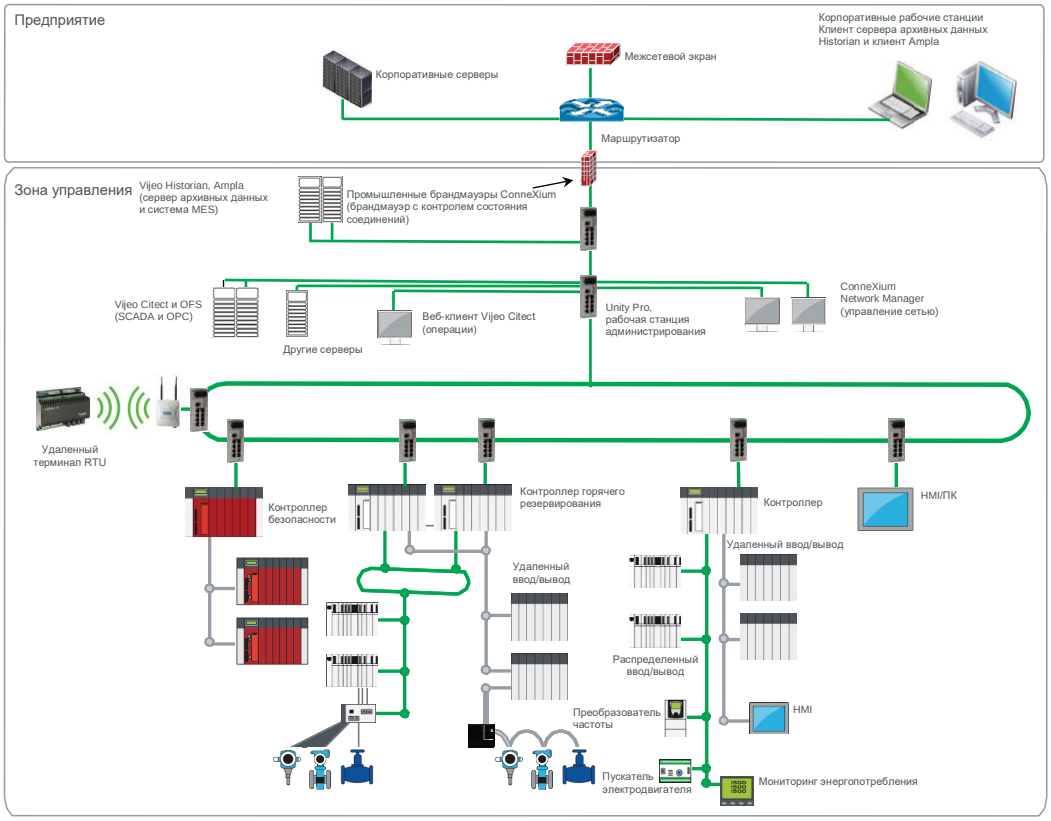
Компенсирующие меры

Еще одно важное понятие – компенсирующие меры. Если продукт не имеет требуемых функций безопасности, система все равно может соответствовать требованиям, если необходимая функциональность обеспечивается другим компонентом в системе. Например, предположим, что система использует старый ПЛК. ПЛК не имеет некоторых необходимых функций безопасности, но размещение межсетевого экрана перед ПЛК обеспечивает необходимую функциональность для защиты ПЛК.

Формат обзора

Пример сети будет использоваться для иллюстрации изменений, необходимых для повышения безопасности на каждом из целевых уровней безопасности. Пример сети представлен ниже.

Рисунок 2



Компоненты ICS размещаются по всей сети, включая контроллеры, системы безопасности, преобразователи частот и HMI. Сеть из примера представляет собой общую систему промышленного управления, которая может использоваться в различных промышленных сегментах.

В этом документе будут рассмотрены требования кибербезопасности для сетей на базе Ethernet. В рамках документа не рассматриваются элементы, связанные с использованием последовательных интерфейсов.

Далее в статье сеть из примера, приведенного выше, будет видоизменяться для демонстрации изменений, которые позволят ей соответствовать требованиям каждого из уровней безопасности МЭК 62443. Основное внимание в документе будет уделено первым трем уровням безопасности, поскольку они охватывают основную часть промышленных применений. Мы сосредоточимся на системных требованиях, указанных в стандарте МЭК 62443-3-3. Каждый из уровней безопасности будет представлен вместе с описанием изменений. Для упрощения в документе предполагается, что повышение уровня безопасности относится ко всей сети в целом (все сегменты сети имеют один и тот же уровень безопасности).

Предлагаемые изменения будут минимально необходимыми для того, чтобы система могла достичь целевого уровня безопасности. Например, простой брандмауэр можно использовать для сегментирования сетей на уровне безопасности 1. Более продвинутый брандмауэр с глубокой проверкой пакетов или однонаправленный шлюз обеспечит большую безопасность, чем простой брандмауэр, но дополнительные возможности безопасности не указаны на этом уровне, они могут быть указаны на следующих уровнях. Клиенты всегда могут использовать методы, указанные на более высоких уровнях, для повышения безопасности в своих системах.

Статья также будет посвящена продуктам и архитектурам. Другие аспекты, которые могут быть определены в плане безопасности (обучение персонала, корпоративные политики безопасности и т. д.) не будет обсуждаться.

Уровень безопасности 1

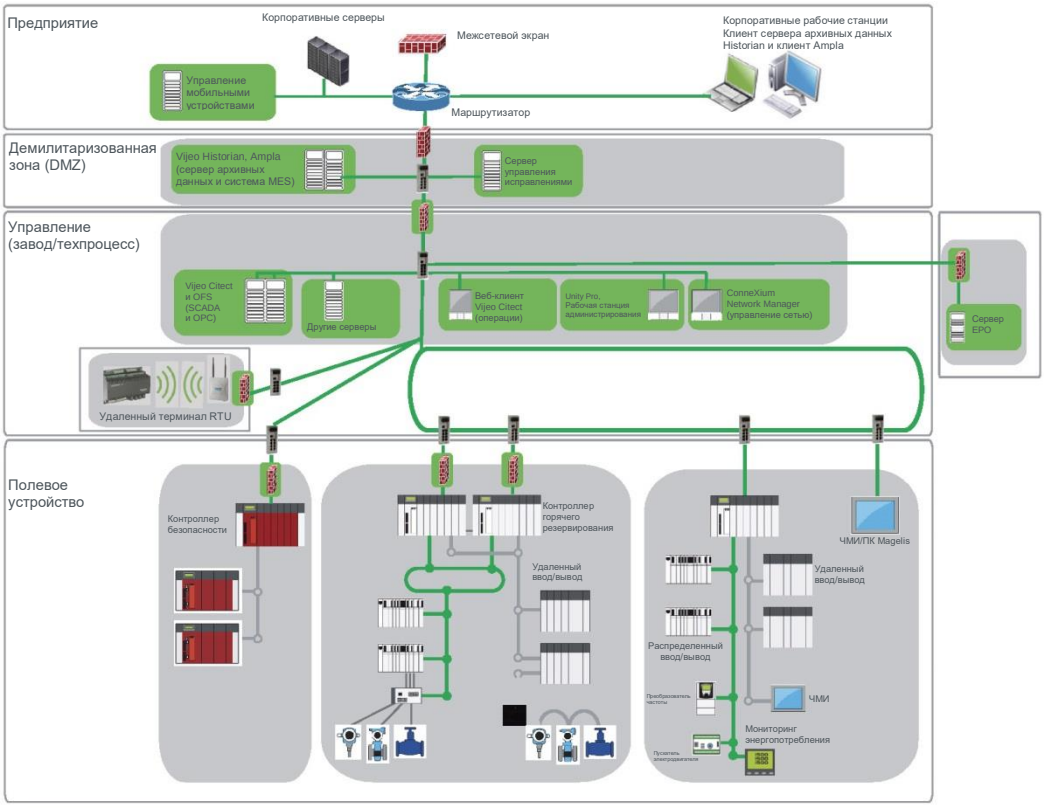
Уровень обеспечения безопасности 1 (SL1) предназначен для защиты от непреднамеренных или случайных нарушений. Спецификации МЭК 62443-3-3 определяют широкий перечень требований, необходимых для обеспечения соответствия этому уровню безопасности. В приведенной ниже таблице приведены ключевые требования SL1. Обратите внимание, что в МЭК 62443-3-3 указано 37 индивидуальных требований. В таблице ниже предпринимается попытка дать общий обзор 14 основных требований. Желающие получить более подробную информацию, должны обратиться к стандартам МЭК.

Таблица 2

№	Требование	Способ выполнения
1	Аутентификация и авторизация пользователей в системе. Создание и управление учетными записями пользователей. Конфигурирование сложности пароля. Отслеживание неудачных попыток входа.	Учетные записи пользователей, созданные на устройствах или централизованном сервере аутентификации.
2	Аутентификация и авторизация пользователей в беспроводных сетях.	Аутентификация пользователей на мобильных устройствах и в сетевой инфраструктуре.
3	Система управления должна обеспечивать возможность мониторинга и контроля доступа из недоверенных сетей.	Брандмауэры отслеживают трафик из недоверенных сетей.
4	Система управления должна быть способна ограничивать код, встроенный в электронную почту или на носитель информации.	Сервер EPO может ограничивать взаимодействие с мобильными устройствами.
5	Системы управления должны обеспечивать возможность составления аудиторских отчетов.	Записи/журналы аудитов, генерируемых оборудованием.
6	Система управления должна защищать целостность передаваемой информации.	Оборудование поддерживает зашифрованные протоколы, надежные контрольные суммы/хеширование.
7	Система управления должна обнаруживать, предупреждать и сообщать о вредоносном коде.	Включение «Белого списка» приложений на конечных устройствах.
8	Система управления должна обеспечивать конфиденциальность информации при ее хранении и передаче.	Оборудование поддерживает имена пользователей и пароли для авторизации
9	Система управления должна сегментировать сети и защищать периметр.	Брандмауэры сегментируют сети и защищают периметр.
10	Система управления должна быть способна предотвращать получение сообщений от внешних пользователей или систем.	Брандмауэр может фильтровать сообщения из внешних сетей.
11	Система управления должна обеспечивать поддержку разделения данных, приложений и служб по критичности для реализации модели зонирования.	Сети должны быть сегментированы путем построения зон и каналов связи.
12	Система управления должна работать в режиме ограниченной функциональности в случае DoS-атаки	Сетевые элементы (коммутаторы, маршрутизаторы и т. д.) поддерживают ограничение скорости передачи.
13	Запрет неиспользуемых функций, портов, протоколов и служб.	Устройства ICS имеют возможность отключать неиспользуемые функции.
14	Система управления должна выполнять резервное копирование пользовательской и системной информации.	Резервные файлы располагаются на выделенных устройствах.

Реализация требований SL1 влияет на архитектуру сети. SL1 требует осуществления определенных шагов многоуровневой защиты, в частности, сегментирования сетей и защиты периметров зон. Ниже перечислены изменения архитектуры сети.

Рисунок 3



В этом примере сеть управления была разбита на семь меньших зон, выделенных серым цветом. Новые элементы выделены зеленым цветом. Зоны:

- *демилитаризованная зона (DMZ)* – подсеть, которая содержит и предоставляет внешние сервисы из зоны управления для корпоративной сети. Серверы в корпоративной зоне никогда не должны быть напрямую подключены к элементам в зоне управления. Тем не менее бизнес-системам необходим доступ к данным из зон управления, а элементам в зонах управления необходим доступ к файлам из недоверенных сетей (например, обновления прошивок). DMZ обеспечивает связь зоны управления с зоной предприятия;
- *зона завода/процесса* – зона, в которой содержатся продукты и приложения, позволяющие управлять технологическими процессами;
- *зона систем безопасности* – централизованная зона, в которой размещаются различные системы обеспечения безопасности;
- *беспроводная зона* – беспроводная инфраструктура отнесена в отдельную зону;

- *зоны контроллеров* – в данном примере область полевых устройств была разбита на три зоны: 2 стандартные зоны управления и одна зона контроллера противоаварийной защиты. Сегментирование зон является результатом плана безопасности и будет меняться в зависимости от применения – это просто пример.

Для сегментирования сети добавлены брандмауэры промышленного уровня (выделены также зеленым цветом). Кроме того, в схему были добавлены сервер EPO и сервер управления мобильными устройствами вместе с ПО по созданию белых списков для серверов, на которых размещено ПО ICS.

Уровень безопасности 2

Спецификация уровня безопасности 2 включает требования, указанные для уровня безопасности 1, плюс следующие требования. Заметьте, что МЭК 62443-3-3 определяет 23 индивидуальных требования. Мы упростили список до 11 основных требований. Желающие получить более подробную информацию, должны обратиться к стандартам МЭК.

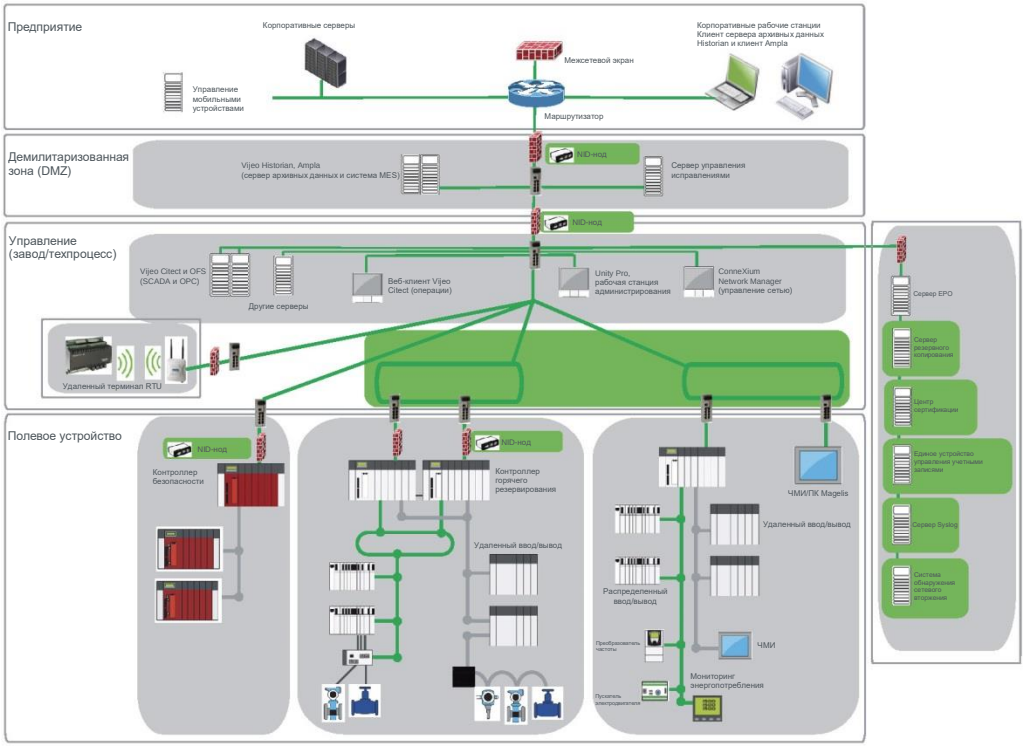
Таблица 3

№	Требование	Способ выполнения
1	Аутентификация и авторизация программных процессов и устройств.	Программное обеспечение и устройства проходят аутентификацию с помощью сертификатов.
2	Аутентификация в системе управления пользователей и пользователей программного обеспечения, использующих беспроводное соединение.	Мобильные устройства и сетевая инфраструктура аутентифицируют пользователей через централизованный сервер аутентификации.
3	Система управления должна поддерживать стандартную инфраструктуру открытых ключей PKI и аутентификацию на основе сертификатов при ее использовании.	Орган сертификации добавлен в сеть управления для выдачи сертификатов.
4	Система управления должна иметь возможность отклонять запросы доступа из недоверенных сетей, если они не одобрены назначенной ролью.	Функция включается на конечных устройствах.
5	Система управления должна позволять авторизованным пользователям определять и изменять права доступа для ролей.	Роли и права доступа разрешены на устройствах или на едином устройстве управления учетными записями.
6	Система управления должна использовать защиту от вредоносного кода во всех точках входа и выхода.	Поддержка системы обнаружения вторжений в сети обеспечивает защиту от вредоносного кода. Централизованный сервер с удаленными узлами защищает сети.
7	Система управления должна защищать целостность сеансов	Оборудование поддерживает зашифрованные протоколы.
8	Система управления должна защищать информацию аудита	Сервер событий, используемый в качестве централизованного хранилища для записей оборудования. Конечные устройства пересылают записи на сервер событий.
9	Система управления должна защищать конфиденциальность в удаленном доступе, проходящем через недоверенную сеть.	VPN, инициированный с брандмауэра, обеспечивает защиту соединения удаленного доступа.
10	Система управления должна обеспечивать возможность физически сегментировать сети систем управления от сетей, не относящихся к системам управления.	Передача сообщений от критически важных систем по сетям, отличным от сетей некритических систем.
11	Система управления должна иметь список установленных компонентов с соответствующими свойствами.	Данные могут быть предоставлены системой обнаружения вторжений.

Важно отметить, что некоторые из требований – это усовершенствования требований, указанных в уровне безопасности 1, а некоторые – новые. Например, на уровне безопасности 1 система должна аутентифицировать и авторизовать пользователей. На уровне безопасности 2 система также должна аутентифицировать и авторизовать программные процессы и устройства. На уровне безопасности 1 система должна обнаруживать, сообщать и предотвращать действия вредоносного ПО. На уровне безопасности 2 система должна обнаруживать, сообщать и предотвращать действия вредоносного программного обеспечения на всех точках входа и выхода зон. В некоторых случаях добавляются новые требования, такие как возможность поддержки сертификатов для аутентификации.

Некоторые из спецификаций требуют добавления продуктов в сеть. Добавлены в сеть и выделены зеленым цветом: унифицированное устройство управления учетными записями, сервер сертификации, сервер резервного копирования, сервер событий и система обнаружения вторжений в сеть. Кроме того, сеть управления была разделена на две отдельные сети. Обратите внимание, что потенциальное устройство ICS, замененное для поддержки новых функций, требуемых в SL2 (необходимость обновления до нового ПЛК, который поддерживает безопасные протоколы, например), не отображается на диаграмме.

Рисунок 4



Уровень безопасности 3

Спецификация уровня безопасности 3 включает требования, указанные для уровня безопасности 2, плюс следующие требования. Заметьте, что МЭК 62443-3-3 определяет 30 индивидуальных требований. Мы упростили список до 12 основных требований. Желающие получить более подробную информацию, должны обратиться к стандартам МЭК.

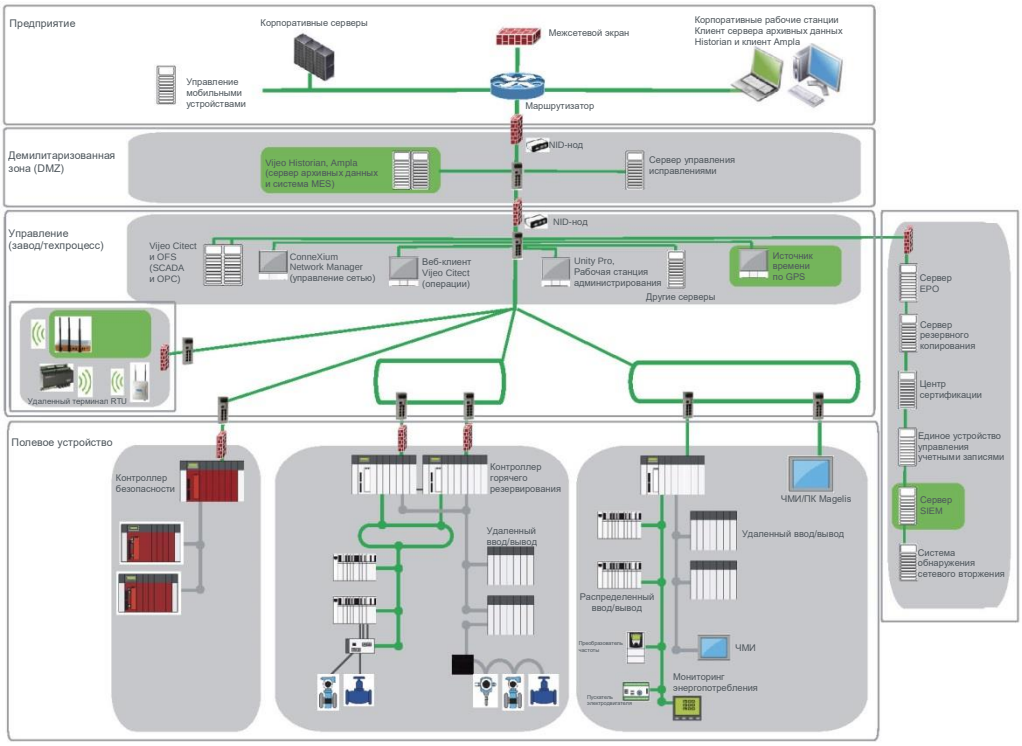
Таблица 4

№	Требование	Способ выполнения
1	Система управления должна поддерживать многофакторную аутентификацию для недоверенных интерфейсов.	Функция работает через централизованное устройство управления учетными записями и конечные устройства.
2	Система управления должна однозначно идентифицировать и аутентифицировать процессы программного обеспечения.	Функция поддерживается через центр сертификации. Также можно использовать защищенные протоколы.
3	Система управления должна поддерживать единое управление учетными записями.	Единое управление учетными записями обеспечивается централизованным управлением учетными записями.
4	Система управления должна защищать приватные ключи с помощью аппаратных механизмов.	Защищенные элементы в оборудовании ICS.
5	Система управления должна идентифицировать и сообщать о несанкционированных беспроводных устройствах	Идентификация несанкционированных беспроводных устройств путем добавления устройства обнаружения беспроводных угроз.
6	Система управления должна проверить целостность мобильного кода, прежде чем разрешить его выполнение.	Целостность мобильного кода проверяется с сервера EPO и центра сертификации.
7	Система управления должна обеспечивать журнал аудита с системой централизованного управления.	Конечные устройства пересылают файлы журналов на SIEM-сервер.
8	Система управления должна синхронизировать внутренние системные часы с определенным периодом.	В сеть добавлен источник времени на основе GPS.
9	Система управления должна поддерживать криптографические механизмы для распознавания изменений информации во время соединения.	Включено с помощью защищенных протоколов.
10	Система управления должна централизованно управлять механизмами защиты от вредоносного кода.	Защита от вредоносного кода осуществляется через серверы EPO и SIEM. Все обнаруженные результаты перенаправляются на сервер SIEM.
11	Система управления должна поддерживать автоматическое резервное копирование с заданным периодом.	Функция автоматического резервного копирования поддерживается на сервере резервного копирования.
12	Система управления должна сообщать о текущих настройках безопасности на конечных устройствах.	Сервер EPO в сочетании с системами управления сетью сообщает о настройках безопасности.

Ряд требований SL3 реализован в компонентах ICS. Примеры включают обязательные защищенные протоколы и использование защищенных элементов для защиты ключей.
На уровне обеспечения безопасности 2 необходимые функции могут быть реализованы с помощью нового программного обеспечения.
На уровне обеспечения безопасности 3 оборудование, скорее всего, придется заменить/перепроектировать.

Некоторые из спецификаций требуют добавления продуктов в сеть. Например, сервер событий, добавленный на уровне безопасности 2, необходимо обновить до SIEM-сервера, чтобы он соответствовал требованиям уровня безопасности 3. Кроме того, необходимо добавить источник времени по GPS и устройство обнаружения угроз в беспроводных сетях.

Рисунок 5



Сертификация продукции и системы

Стандарт МЭК 62443 определяет требования к уровням безопасности продукта и системы. Эти требования представляют ценность как для конечных пользователей, так и для поставщиков оборудования.

- *Конечные пользователи* – конечные пользователи традиционно оценивают продукты поставщиков на основе критериев, включая содержание функций, цену и условия поставки. Определение требуемых функций может быть сложным процессом. МЭК 62443 упрощает процесс определения требований к кибербезопасности, позволяя конечным пользователям указать целевой уровень безопасности вместо определения огромного списка отдельных функций. Конечные пользователи будут знать точные функции, доступные в оборудовании, на основании соответствия требованиям стандартов МЭК 62443.

- *Поставщики оборудования* – поставщики оборудования могут дифференцировать свои решения от конкурентов посредством стандартов МЭК 62443. Традиционно было трудно четко показать, что одно решение является более безопасным, чем другое, поскольку каждое из них имело различный набор функций кибербезопасности. Поставщики, которые разрабатывают и сертифицируют решения для уровней безопасности, как определено в стандарте МЭК 62443, могут четко различать возможности кибербезопасности, продавая продукт, сертифицированный по стандартам уровня 2, и конкурирующие продукты с уровнем безопасности 1.

Поставщики могут проводить сертификацию как конечных устройств (как указано в МЭК 62443-4-2), так и систем (как указано в МЭК 62443-3-3). В обоих случаях соответствие стандартам должно быть подтверждено независимой третьей стороной. Конечные пользователи должны учитывать сертификаты кибербезопасности при составлении своих требований к приобретению оборудования.

Заключение

Стандарт МЭК 62443 содержит руководящие указания для конечных пользователей, которые ищут безопасные промышленные решения. Структура уровней безопасности помогает группировать требования кибербезопасности для успешной реализации. Повышение безопасности системы может привести к необходимости модернизации устаревшего оборудования ICS и приобретению новых устройств кибербезопасности. Требуемые расходы и сложность внедрения будут возрастать с повышением целевого уровня безопасности.

Перед началом любой работы по защите промышленного решения необходим детальный план безопасности. Защищенные продукты и архитектуры являются лишь частью решения. Обучение персонала в сочетании с обдуманными корпоративными политиками безопасности имеет большое значение для обеспечения безопасности промышленных систем управления.

Об авторе

Даниель ДеРюсо обладает более чем 25-летним опытом в областях разработки, продаж и маркетинга в высокотехнологичных компаниях. В настоящее время г-н ДеРюсо является директором по кибербезопасности промышленного подразделения Schneider Electric. На этой должности он работает над обеспечением правильной и последовательной реализации функций безопасности в разнообразном портфеле промышленных продуктов Schneider Electric.

Свяжитесь с нами

Более подробную информацию можно найти на нашем сайте:
https://www.schneider-electric.com/en/work/solutions/cybersecurity/

Программное обеспечение Schneider Electric
26561 Rancho Pkwy South, Lake Forest, CA 92630 Тел.: +1 (949) 727-3200 Факс: +1 (949) 727-3270 software.schneider-electric.com
© 2018 Schneider Electric Software, LLC. Все права защищены.

PN SE-998-20186845_GMA-US Ред. 01/18