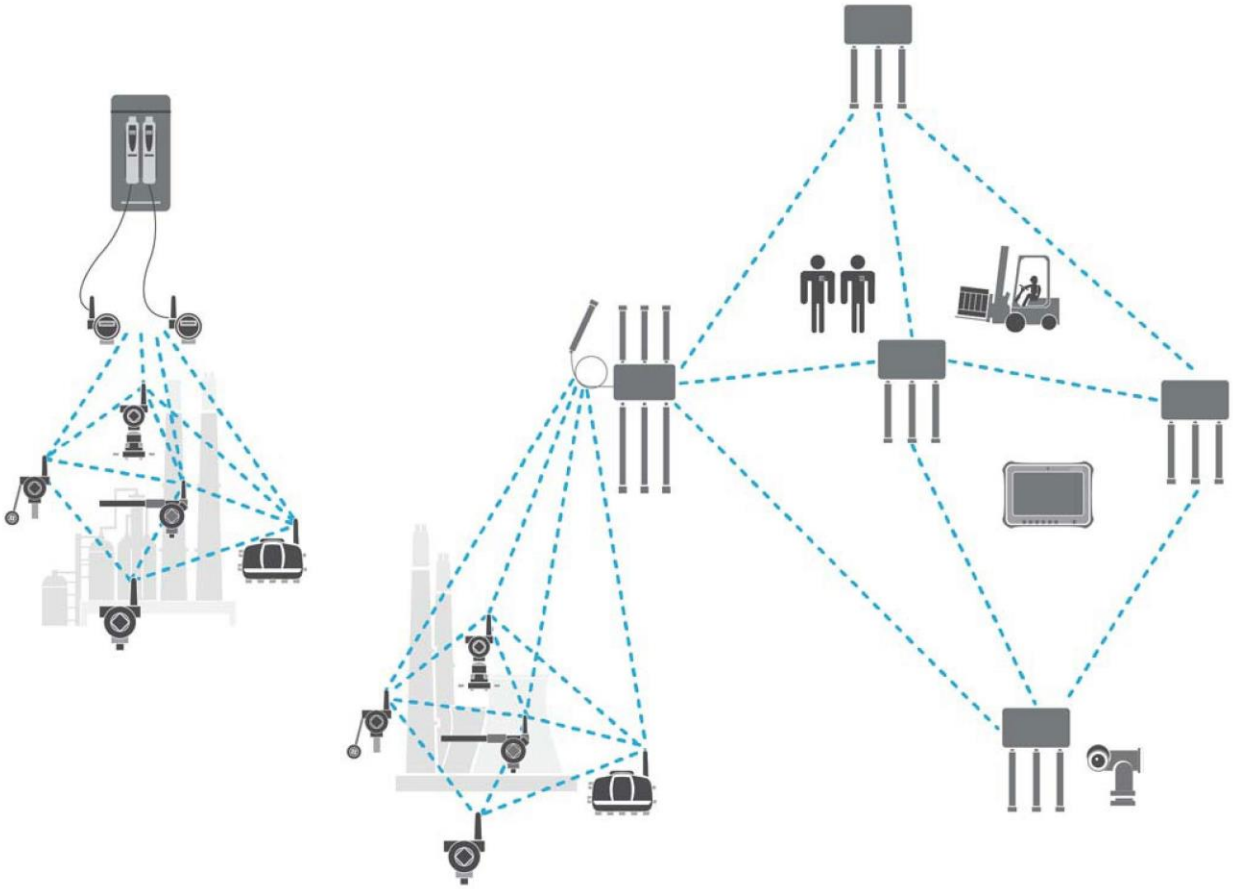
Безопасность беспроводных сетей Emerson™

Безопасность протоколов *Wireless*HART® и Wi-Fi®



Безопасность беспроводных сетей имеет первостепенное значение для успешного внедрения как сетей для полевых устройств, так и решений на уровне предприятия. Настоящий документ описывает возможности Emerson по внедрению безопасных, надежных и функциональных беспроводных решений для полевых устройств и производственных применений.

EMERSON.

1 Введение

Цель настоящего документа заключается в комплексном описании стратегии компании Emerson по обеспечению глубокой защиты (Defense in Depth) беспроводных сетей, соответствующих стандартам IEC 62591 *(Wireless*HART*)* и Wi-Fi. В нем также описаны:

- программа Emerson Wireless;
- стандарт *WirelessHART*;
- общая топология беспроводной сети предприятия;
- прикладные решения (включая описание безопасной и беспрепятственной интеграции беспроводных полевых приборов Emerson).

Кроме того, описаны функции обеспечения безопасности как полевых приборов *Wireless*HART, так и решений для беспроводных сетей предприятия.

2 Беспроводные решения Emerson Wireless

Несколько лет назад компания Emerson в сотрудничестве с поставщиками перерабатывающей промышленности и заказчиками начала внедрять новые беспроводные полевые КИП. В результате был создан стандарт *Wireless*HART (на базе протокола HART® 7), в полном соответствии с которым началось производство различных полевых контрольно-измерительных приборов Emerson Wireless.

Технология *Wireless*HART является частью стандарта HART 7, поэтому все устройства *Wireless*HART обладают такими же характеристиками и функциями, что и проводные приборы на базе протокола HART, миллионы которых установлены сегодня по всему миру. Для вас это значит, что все программные продукты, инструменты и навыки ваших сотрудников могут быть использованы для ввода в эксплуатацию, технического обслуживания и интеграции беспроводных приборов в современные хост-системы. Перед установкой таких приборов не требуется проводить радиочастотное (РЧ) исследование объекта, а их конструкция обеспечивает простоту монтажа в соответствии с несколькими несложными эффективными методами.

Стандарт *Wireless*HART представляет собой специализированный стандарт, который позволяет КИП выполнять измерения параметров технологического процесса, передавать результаты по ячеистой сети и легко интегрировать данные в существующие хост-системы. Одним из ключевых показателей при разработке устройств и стандарта было снижение энергопотребления и обеспечение срока службы от 4 до 10 лет при работе на батарейном питании.

В дополнение к беспроводным решениям для полевых приборов компания Emerson стала предлагать решения на уровне предприятия, которые основываются на технологии Wi-Fi и предназначены для таких применений, как:

- беспроводные технологии для выездного персонала;
- мобильная голосовая и видеосвязь;
- удаленное видеонаблюдение;
- отслеживание местонахождения;
- сбор по тревоге;

- транспортная сеть передачи полевых данных;
- мост сети управления.

Все решения, относящиеся к беспроводным сетям предприятия (WPN), базируются на группе стандартов для беспроводного оборудования IEEE 802.11-2007 (стандарты технологии Wi-Fi), которые продвигаются ИТ-сообществом.

Есть существенное различие между полевыми решениями и решениями на уровне предприятия: протокол *Wireless*HART создан представителями промышленности для полевых КИП, тогда как стандарт Wi-Fi сформирован ИТ-сообществом для широкого круга применений и решений. Оба стандарта широко применимы в рамках надежных решений, установленных на предприятиях заказчиков по всему миру.

2.1 Сетевые коммуникации *Wireless*HART

*Wireless*HART — это беспроводной коммуникационный протокол ячеистой сети, предназначенный для решений по автоматизации технологических процессов. Он добавляет беспроводные функции в протокол HART, сохраняя при этом совместимость с существующими HART-устройствами, командами и инструментами.

- Каждая сеть *Wireless*HART состоит из трех основных элементов.
- Беспроводные полевые устройства, подсоединенные к технологическому или заводскому оборудованию.
- Шлюзы, которые обеспечивают обмен данными между этими устройствами и хост-приложениями, подсоединенными к высокоскоростной магистральной или другой имеющейся на предприятии коммуникационной сети.
- Администратор сети, ответственный:

  за конфигурирование сети;

  - планирование обмена данными между устройствами;
  - управление маршрутизацией сообщений;
  - мониторинг состояния сети.

Примечание

Администратор сети может быть встроен в шлюз, хост-приложение или контроллер автоматизации технологического процесса.

Сеть включает совместимые с IEEE 802.15.4 радиопередатчики, работающие на частоте 2,4 ГГц. В них реализованы технология широкополосного сигнала с прямой последовательностью (DSSS) и переключение каналов для обеспечения коммуникационной безопасности и надежности, а также технология синхронизированного многостанционного доступа с временным разделением каналов (TDMA) и контролируемой задержкой для передачи данных между устройствами в сети.

Каждое устройство ячеистой сети может служить маршрутизатором для сообщений от других устройств, что позволяет расширить сетевой диапазон и организовать резервные маршруты передаваемых данных для повышения надежности до 99,9 %.

Как и проводной протокол HART, WirelessHART поддерживает полный диапазон применений для мониторинга и контроля технологических процессов:

- мониторинг состояния оборудования и параметров технологического процесса;
- мониторинг загрязнения окружающей среды, управление энергопотреблением, соблюдение нормативных требований;
- управление активами, профилактическое обслуживание, расширенная диагностика;
- замкнутая система управления (при необходимости).

Беспроводные решения дополняют, а не заменяют проводные КИП, и, как правило, работают на предприятиях параллельно с ними. Сегодня практически каждому применению, подразумевающему автоматизацию технологического процесса, соответствует минимум один прибор, поддерживающий проводной протокол HART. WirelessHART — дополнительный способ обмена данными с HART-приборами [1].

3 Общая топология беспроводной сети предприятия

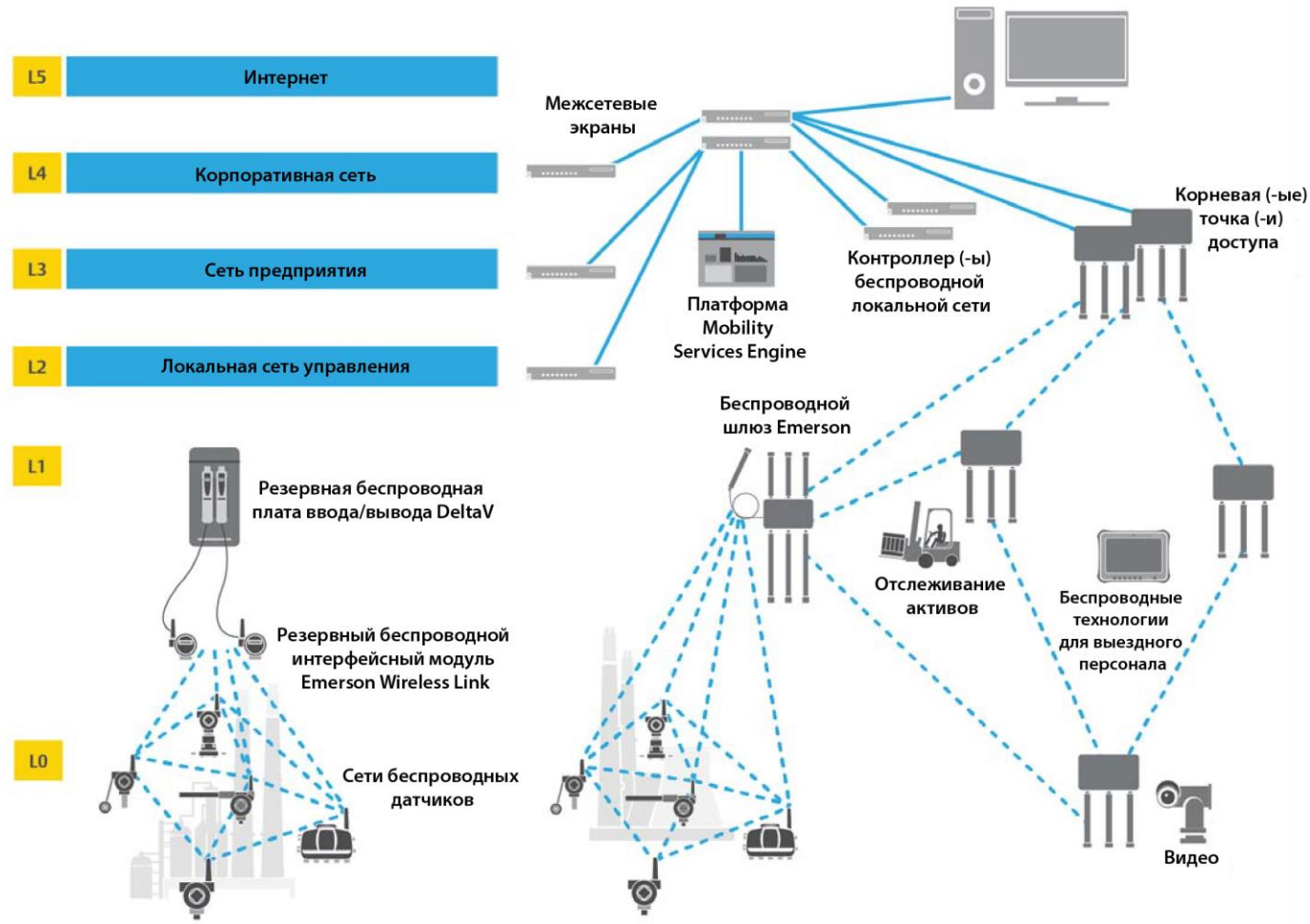
3.1 Модель Purdue (ISA95)

В то время как полевые приборы, поддерживающие WirelessHART, находятся только на сетевом уровне 0, беспроводная сеть предприятия должна охватывать все остальные уровни сетевой модели, разработанной в университете Пердью (Purdue) (ISA95). См. сопутствующие схемы сети. Было бы нерентабельно устанавливать отдельную беспроводную сеть для каждого сетевого уровня, поэтому каждый уровень беспроводной сети виртуализирован в рамках общего аппаратного обеспечения. Реализованные на базе общего аппаратного обеспечения безопасные виртуальные сети полностью изолированы друг от друга на программном уровне.

Кроме того, беспроводная сеть предприятия поддерживает «Дифференцированные службы», что необходимо для выделения частот и определения приоритета для каждой виртуальной сети, которая использует общую полосу пропускания. Это обеспечивает наивысший приоритет передачи данных от полевых измерительных приборов (для которых нужна полоса пропускания очень малой ширины) по беспроводной сети предприятия.

[1] *HART Communication Foundation, “Why WirelessHART: The Right Standard at the Right Time”, октябрь 2007г.*

Рисунок 1-1. Архитектура беспроводной сети предприятия



Каждый прибор беспроводной сети (карманные компьютеры, ноутбуки, RFID-метки или беспроводные шлюзы для полевых приборов) направляет данные на одну из точек доступа ячеистой сети предприятия. Из точек доступа информация передается обратно по ячеистой сети до корневой точки доступа. Далее информация поступает напрямую на управляемый сетевой коммутатор, где виртуальные ЛВС разделяются на разные физические ЛВС. В результате данные проходят на каждый сетевой уровень через межсетевой экран для гарантии того, что на каждый уровень поступает только предназначенный для него трафик. Заключительным этапом является передача данных на соответствующий прибор в сети.

При наличии беспроводных приборов данные направляются на беспроводной шлюз Emerson, после чего передаются по описанному выше маршруту на контроллер DeltaV™ (версии 10.3 или более поздней), устройство на базе Modbus® TCP/IP, OPC-сервер или в AMS Suite.

Данные устройств видеосвязи передаются на сервер цифровой видеозаписи, который может находиться на сетевых уровнях 3 или 4. Как правило, устройства видеонаблюдения соединены проводами с точками доступа ячеистой сети. Видеокамеры имеют сертификат подлинности, что гарантирует наличие в сети только авторизованных камер.

Данные с мобильных устройств могут быть переданы на любой (модель Пердью) сетевой уровень (например, на уровни 2–4), но только на одну подсеть с присвоенным идентификатором SSID в единицу времени (чтобы предотвратить

пересечение трафика). Пользователь сетевого устройства подключается к сети SSID (подтверждает подлинность), куда будут передавать данные портативные устройства. Существует несколько правомерных способов аутентификации пользователей и предоставления им доступа к конкретной беспроводной виртуальной ЛВС. Как правило, для этого используют RADIUS-сервер, где выполняется как аутентификация, так и авторизация пользователей через Active Directory. Пользователь заходит в операционную систему устройства и, указывая те же самые учетные данные, запрашивает доступ к конкретной SSID-сети, чтобы осуществлять обмен данными с приложениями в составе проводной сети.

Для обмена данными с клиентским устройством могут использоваться следующие приложения 3-го уровня:

- терминальные серверы — для удаленных офисных приложений;
- серверы удаленного доступа к DeltaV — для устройств с установленной системой DeltaV;
- серверы архивных данных;
- OPC-серверы;
- программный комплекс прогностической диагностики AMS Suite.

Серверные решения 4 уровня:

- ERP;
- приложения для транспортировки и смешивания нефтепродуктов;
- приложения для транспортировки и смешивания нефтепродуктов;
- прочие пользовательские или закрытые приложения.

4 Интеграция полевых приборов

Беспроводные полевые приборы Emerson интегрируются в систему управления верхнего уровня через беспроводной шлюз Emerson одним из шести способов.

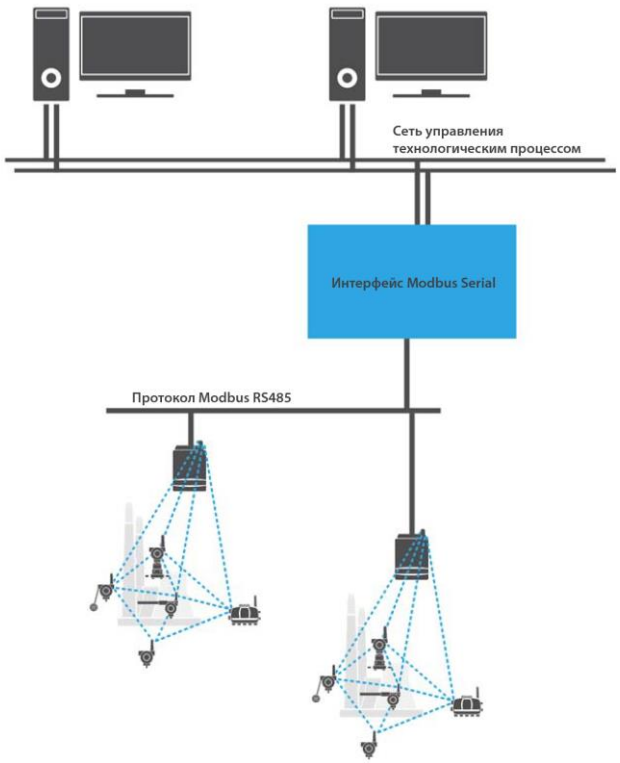
1. Собственный узел DeltaV, начиная с версии 10.3.
2. Соединение с OPC-сервером.
3. Подключение к протоколу Modbus TCP/IP.
4. ПО AMS по протоколу HART TCP/IP.
5. Порт HART.
6. Соединение EtherNet/IP™.
7. Соединение с протоколом последовательной передачи данных Modbus Serial.

Первые шесть методов интеграции через Ethernet могут быть беспрепятственно реализованы в беспроводной сети предприятия, при условии, что хост-система поддерживает соответствующий протокол. Протокол последовательной передачи Modbus Serial поддерживают практически все существующие системы управления, но для этого, как правило, требуется проводное соединение.

4.1 Интеграция в беспроводную полевую сеть Emerson

Беспроводная полевая сеть включает несколько устройств, поддерживающих WirelessHART, которые передают данные на беспроводной шлюз Emerson по самоорганизующейся ячеистой сети. Те хост-системы, которые не поддерживают естественную интеграцию WirelessHART, напрямую подключаются к беспроводному шлюзу Emerson тремя различными способами: протоколы Modbus Serial, Modbus TCP/IP, EtherNet/IP и OPC DA. Данные протоколы позволяют обеспечить достаточную гибкость при внедрении беспроводной полевой сети Emerson в соответствии с производственными нуждами.

Рисунок 1-2. Подключения к плате Modbus Serial в многоточечном режиме



На рисунке 1-2 представлен один из трех способов проводного подключения беспроводного шлюза Emerson к системе управления и интеграции данных, которые передаются полевыми приборами.

Во многих случаях может быть неудобно тянуть провод к шлюзу, если он расположен далеко от основного технологического процесса. Тогда шлюз можно подключить к центральной операторской через беспроводную сеть предприятия либо использовать беспроводной шлюз Emerson 1552WU, который действует как точка доступа ячеистой сети для сети Wi-Fi и шлюза WirelessHART и обеспечивает более простой и экономичный способ развертывания повсеместного измерения.

Для всех хост-систем, которые поддерживают Modbus TCP/IP или OPC, существует два возможных метода интегрирования беспроводной полевой сети Emerson в беспроводную сеть предприятия Emerson, как показано на рисунках 1-3 и 1-4.

Рисунок 1-3. Интеграция беспроводной полевой сети Emerson через OPC DA

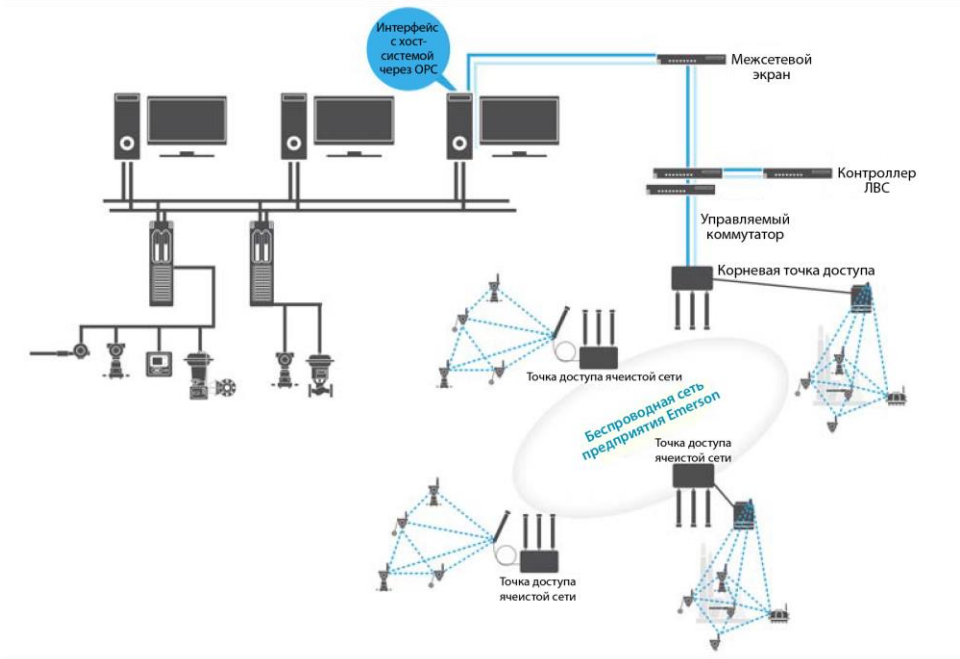
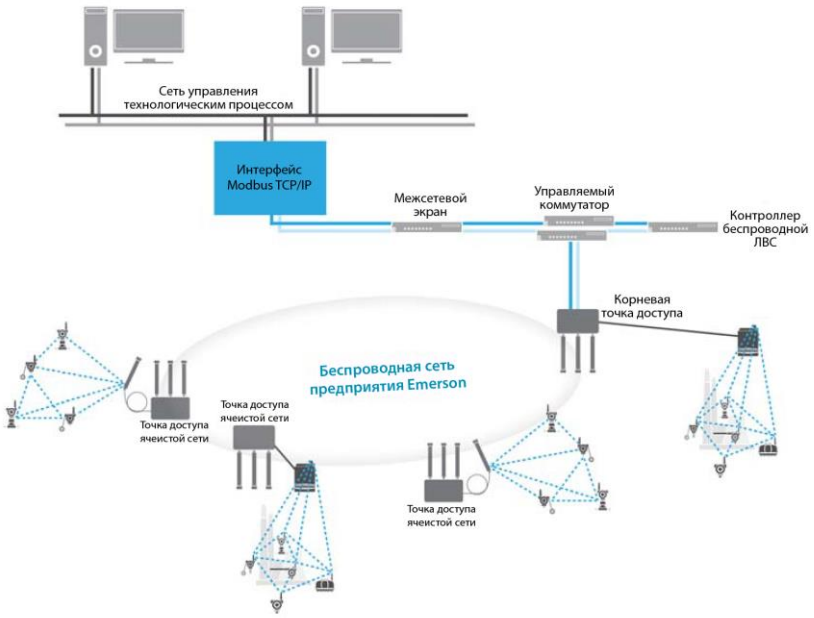


Рисунок 1-4. Интеграция беспроводной полевой сети Emerson через интерфейс Modbus TCP/IP



4.2 Беспроводная сеть предприятия

Все решения Emerson по организации беспроводной сети предприятия предлагаются в качестве готовых решений, включая ряд услуг, подробно описанных в предыдущем разделе:

- оценка площадок и консультирование;
- проектирование сетевой системы;
- развертывание системы;
- обучение;
- поддержка после реализации проекта.

Беспроводная сеть предприятия Emerson может состоять из следующих сетевых компонентов Cisco® (см. рисунок «Архитектура беспроводной сети» в разделе «Архитектура сети»):

- точка доступа серии 1550;
- контроллеры беспроводной ЛВС (WLAN);
- первостепенная инфраструктура (опция);
- платформа Mobility Services Engine (MSE) с беспроводной системой предотвращения вторжений(wIPS) (опция);
- управляемый коммутатор;
- межсетевые экраны.

5 Решения на уровне предприятия

5.1 Беспроводная сеть передачи полевых данных

Для беспроводных полевых сетей (например, в резервуарных парках), расположенных далеко от центральной операторской, в рамках беспроводной сети предприятия обеспечивается надежная, масштабируемая и экономически выгодная беспроводная транспортная сеть, для того чтобы данные от беспроводных полевых устройств могли быть переданы на любую хост-систему управления. Благодаря характеристике «Класс услуг» (*Class of Service*) полевым данным могут быть назначены приоритеты с целью минимизации периода ожидания. При наличии беспроводной сети предприятия данные дистанционных беспроводных приборов могут быть экономично и оперативно интегрированы в системы управления технологическими процессами.

5.2 Беспроводные технологии для мобильного персонала

Решения «Мобильный рабочий» позволяют полевым операторам и специалистам по техническому обслуживанию работать более эффективно, получая всю необходимую информацию в нужном месте и в нужное время.

Приложения для портативных устройств, как правило, могут работать одним из следующих двух способов.

- В качестве клиент-серверного веб-приложения — пользователи подключаются к основному приложению, которое запускается на сервере проводной сети, через браузер портативного устройства. Это может быть веб-приложение, которое у вас уже внедрено.
- Терминальный сервер установлен в сети, и клиент удаленно подключается к индивидуальной сессии Windows, где размещены все программные приложения, к которым необходим доступ, как в случае с распределенной системой управления DeltaV™.

После внедрения беспроводной сети предприятия сотрудники могут передвигаться по всему объекту, не теряя соединения с технологическим процессом по сети Wi-Fi.

Типичные примеры соединений

- DeltaV Remote Client — удаленный доступ ко всем функциям АСУТП DeltaV с коммуникатора или ноутбука. Это позволит мобильным операторам или специалистам по техническому обслуживанию получить возможность видеть тревожные сигналы и оповещения, а также отслеживать состояние технологического процесса при совершении обходов.
- Удаленный клиент AMS Suite позволяет работникам воспользоваться всеми возможностями программного комплекса AMS Suite, включая функции диагностики и ведения журнала аудита (Audit Trail), которые могут понадобиться для выявления и устранения неисправностей прибора.

Более того, благодаря подключению к беспроводной сети пользователь получает доступ к компьютеризированной системе управления техническим обслуживанием (CMMS), заводским чертежам или документам, что может обеспечить более эффективное, оперативное и безопасное устранение проблемы, чем при выполнении работ без возможности незамедлительного получения таких данных.

Решения для мобильных сотрудников представлены неограниченным количеством клиентских устройств в разных исполнениях и с разными функциональными возможностями. Выбор портативного устройства, соответствующего внедряемому решению, определяется требованиями к конкретному проекту.

5.3 Удаленное видеонаблюдение

Видеонаблюдение становится неотъемлемой частью безопасной работы производственного предприятия. Сегодня с помощью беспроводных технологий критически важные видеоданные могут быть переданы универсальным методом в операторскую, офисные здания и на другие участки предприятия, что невозможно при использовании проводных решений. Решение Wireless от Emerson для беспроводной передачи видео — экономически выгодный и оперативный способ следить за безопасностью и рабочими процессами предприятия. Для передачи видео используется ячеистая сеть с высокой пропускной способностью.

5.4 Сбор по тревоге/отслеживание местонахождения

Беспроводные технологии позволяют наблюдать за сотрудниками и оборудованием на территории предприятия, что обеспечивает множество преимуществ, включая повышенный уровень безопасности. Таким образом, можно оперативно получать точную информацию о том, кого учли или не учли в случае чрезвычайной ситуации. Кроме того, за счет усовершенствованных функций отслеживания человеческих и капитальных ресурсов вы можете более эффективно использовать

своих сотрудников и оборудование, а также оперативнее реагировать на возникшие ситуации в случае необходимости. Такие технологии также позволяют справиться с угрозами безопасности, связанными с перемещением людей и оборудования.

Предприятия с неблагоприятными условиями окружающей среды, такие как НПЗ и нефтехимические заводы, нуждаются в специализированных технологиях для защиты персонала. Полная видимость местонахождения людей в аварийных ситуациях крайне необходима для безопасной эвакуации или оперативного принятия необходимых мер в экстренных случаях. Например, при включенной станции промывки глаз важно знать, кто использует станцию и кто находится поблизости для оказания помощи.

5.5 Беспроводной мост сети управления

В некоторых случаях необходимо дистанционное управление распределенной системой управления DeltaV: например, если между операторской и местом расположения контроллера проходит автомагистраль или водный канал или же устройство ввода/вывода необходимо установить в резервуарном парке/ на удаленном объекте. Прокладка оптоволоконного кабеля стоит дорого. Вместо этого компоненты системы DeltaV можно подключить беспроводным способом, который является надежным и экономически эффективным.

Компания Emerson в рамках предложения Wireless поддерживает распределенные системы управления DeltaV, которые имеют беспроводные мосты в локальной управляющей сети. Согласно договору на оказание услуг специалисты Emerson помогут вам при проектировании, монтаже, а также проведении приемочных испытаний на заводе/на месте установки моста беспроводной управляющей сети.

6 Безопасность беспроводной сети предприятия

6.1 Возможные направления атаки

При отсутствии физических препятствий для беспроводной передачи данных по сети предприятия крайне важно обеспечить глубокую защиту сети от несанкционированного доступа. Ниже представлено краткое описание возможных направлений атак.

Неавторизованные точки доступа

Несанкционированные точки доступа, подключенные к проводной сети, через которые беспроводной доступ к данным получают (не)санкционированные клиенты. Такие точки доступа могут быть открытыми или защищенными (чтобы ограничить число [не]санкционированных пользователей, которые могут подключаться и не попасть в поле зрения администраторов). Неавторизованные точки доступа могут использоваться как санкционированными, так и несанкционированными клиентами. Неавторизованные точки доступа могут быть добавлены в сеть злоумышленниками или же правомочными сотрудниками, чтобы лучше реализовать возможности беспроводного подключения в пределах своего офиса. В последнем случае доступ к беспроводной сети предприятия разрешен, но сотрудник при этом подключает точку доступа, представляющую потенциальную угрозу безопасности сети, пытаясь «улучшить» беспроводную связь в своем офисе. Кроме того, к неавторизованной точке доступа могут подключаться и санкционированные клиенты.

Беспроводные мосты в режиме Ad-hoc

Определенная разновидность протокола 802.11 позволяет устанавливать соединение между двумя равноправными узлами, что называется построением самоорганизующейся сети (ad-hoc). Основная опасность, которую представляют такие сети, заключается в том, что конфигурация устройств проводной сети позволяет им тоже стать узлом ad-hoc соединения. Тогда две сети могут быть соединены посредством моста, что открывает несанкционированный беспроводной доступ к ресурсам проводной сети.

Атаки с перехватом (Evil Twin, Honeypot AP и т. д.)

Существует множество типов атак такого рода, однако все они основаны на одном и том же эксплойте. Атакующий вторгается между легальным клиентом и ресурсами, к которым клиент пытается получить доступ. Такая атака может произойти между клиентом и санкционированной инфраструктурой или путем убеждения клиента подключиться к неавторизованной точке доступа, имитирующей допустимую сеть. Используемый эксплойт меняется с течением времени, поскольку выявляются новые неисправленные уязвимости протокола.

Атака типа «отказ в обслуживании» (DoS)

Существует несколько способов, к которым прибегают злоумышленники для перекрытия легальным пользователям доступа к беспроводной сети. Атакующие отправляют сообщения или ложные запросы, вследствие чего ресурсы точки доступа используются для неблагоприятных коммуникаций, при этом пропускной способности становится недостаточно для обслуживания легального пользователя.

Преднамеренное создание радиопомех (считается DoS-атакой)

В спектре частот беспроводной сети могут быть созданы радиопомехи путем целенаправленного нарушения связи с каким-либо беспроводным датчиком в определенной зоне за счет создания «шума».

Разведывательные атаки и взлом

Большое количество существующих активных и пассивных разведывательных инструментов позволяет как администраторам, так и хакерам получать данные о конфигурации и топологии сети. Инструменты взлома обладают еще большими возможностями и могут расшифровывать беспроводной трафик в режиме реального времени или автономно.

6.2 Глубокая защита беспроводной сети

В основе модели глубокой защиты беспроводной сети лежат три ключевых аспекта.

1. Контроль доступа к беспроводной сети.
2. Защита инфраструктуры беспроводной сети.
3. Защита клиентских устройств.

В большинстве беспроводных сетей реализован только контроль доступа, но для предотвращения вторжения в сеть этого недостаточно. Даже при использовании всех инструментов, которые предлагает Emerson, необходимо контролировать соблюдение внутренней политики безопасности и периодически проверять журнал событий, что позволит отслеживать попытки злоумышленников взломать сеть.

Контроль доступа к сети

Для осуществления контроля сетевого доступа нужно, чтобы каждый пользователь или каждое устройство прошли проверку подлинности через единый центр защиты сетевых доменов. В рамках предлагаемого решения Emerson использует сервер аутентификации, авторизации и учета (AAA) на базе протокола RADIUS для управления доступом к ресурсам беспроводной сети в условиях существующей инфраструктуры информационной безопасности. Благодаря этому обеспечивается централизованный контроль доступа пользователей в беспроводную сеть, а также контроль прав на использование ресурсов проводных сетей. Проверка пользователей в рамках решения Emerson осуществляется с помощью технологии защиты WPA2 для предприятий, которая поддерживает расширяемый протокол проверки подлинности.

Сертификаты безопасности могут быть установлены на всех одобренных мобильных устройствах, а доступ к сети Wi-Fi может быть разрешен только для устройств с утвержденными сертификатами.

Вся беспроводная передача данных между клиентским устройством и беспроводной сетью шифруются с помощью алгоритма блочного шифрования AES (размер блока 128 бит), который предотвращает несанкционированные действия по перехвату информации или манипулированию передаваемыми данными.

Система отслеживает и регистрирует сетевые операции (как авторизованные, так и незаконные), тем самым позволяя администраторам контролировать попытки взлома сети или получения доступа к устройствам без предварительной авторизации.

Защита сети

Каждая точка доступа ячеистой беспроводной сети имеет цифровой идентификатор, который отождествляет ее с беспроводным контроллером и подтверждает статус узла безопасной сети. Таким образом, предотвращается имитация подлинных точек доступа неавторизованными.

Передача данных (в пределах, допустимых законом) в беспроводной сети шифруется с помощью алгоритма блочного шифрования AES (размер блока 128 бит), который предотвращает несанкционированные действия по перехвату информации или манипулированию пакетами данных. Неавторизованные точки доступа не могут стать частью беспроводной инфраструктуры или каким-либо иным способом подвергнуть сеть опасности. Emerson также рекомендует организовывать беспроводные сети с возможностью беспроводного доступа пользователей в комплексе с системой предотвращения вторжений, описанной ниже.

Защита клиентских устройств

Даже в самые безопасные проводные и беспроводные сети может проникнуть вирус или «червь» от подключенного зараженного устройства. Решение Emerson включает установку антивирусного ПО на беспроводное клиентское устройство с целью предотвращения его первичного заражения. Должны быть реализованы методы эффективной защиты для обеспечения своевременного обновления антивирусных программ наряду с регулярным обновлением системы безопасности ОС. Emerson настоятельно рекомендует, чтобы устройства (проводные или беспроводные), которые являются частью системы управления, не имели доступа к почтовым приложениям или Интернету, поскольку это самые крупные источники вирусов.

Таблица 1-1. Атаки на беспроводную сеть предприятия и способы защиты

Атаки	Способы защиты					
	w IPS	Проверка подлинности	Целостность данных	Кодирование	Первостепенная инфраструктура	Агент клиента
Отказ в обслуживании	✔				✔	
MAC-спуфинг		✔		✔		
Атаки с перехватом	✔	✔	✔	✔		
Беспроводные мосты в режиме Ad-hoc			</		✔	
Неавторизованные точки доступа	✔	✔			✔	
Инструменты взлома		✔		✔	✔	✔
Атаки, не нацеленные на протокол 802.11				✔	✔	
Клиентское ad-hoc-соединение	✔	✔				✔
Разведывательные атаки на сеть	✔			✔	✔	
Взлом аутентификации и кодирования	✔	✔	✔	✔	✔	
Маскировка под законного пользователя	✔	✔	✔	✔	✔	

Система предотвращения вторжений в беспроводную сеть

Наконец, Emerson может внедрить систему предотвращения вторжений в беспроводную сеть, которая позволяет контролировать передачу данных в пределах беспроводной сети предприятия. Процессы сетевых коммуникаций проверяются на наличие нестандартных наборов данных, а в случае обнаружения подозрительных операций администратор получает предупредительный сигнал. Кроме того, точки доступа проверяют радиоволны с целью обнаружения неавторизованных клиентов и точек доступа и в случае необходимости направляют администратору соответствующие уведомления. Кроме того, систему wIPS можно настроить на активную атаку неавторизованных точек доступа в пределах зоны покрытия беспроводной сети, чтобы исключить возможность случайного подключения к ним со стороны пользователей. На случай преднамеренных помех предусмотрены ответные меры по триангуляции положения источника с целью перекрытия радиосигнала и максимально возможного сокращения времени простоя. Система предотвращения вторжений в беспроводную сеть непрерывно мониторит радиоволны и коммуникационный трафик, защищая сеть от атак, представленных в таблице 1-1.

7 Функции обеспечения безопасности сети полевых приборов WirelessHART

Примечание

Функции кибербезопасности, встроенные в беспроводной шлюз Smart Wireless от Emerson версии 4 или более поздней, сертифицированы Национальным институтом стандартов и технологий (NIST) на соответствие требованиям Федерального стандарта по обработке информации 197 (FIPS-197) и имеют сертификат Achilles 1 уровня, что дает заказчикам еще большую уверенность в надежности и безопасности беспроводных сетей.

Функции безопасности полевой сети WirelessHART для беспроводного шлюза Emerson, беспроводной платы ввода/вывода DeltaV и канала связи Field Link, а также для приборов любого другого поставщика практически идентичны и включают следующие.

- Шифрование AES-128 (в соответствии с Национальным институтом стандартов и технологии и стандартом IEEE) для всех коммуникаций между ячеистой сетью КИП и шлюзом.
- Ключи для отдельных сеансов приборов для непрерывного обеспечения подлинности передаваемых сообщений, достоверности данных, подтверждения получении информации и сохранения ее секретности (исключение возможности перехвата другими приборами в ячеистой сети) за счет шифрования.
- Расчет циклических избыточных кодов (CRC) и кода проверки целостности сообщения (MIC) для каждого транзитного узла также обеспечивает достоверность сообщений и проверку источника и получателя информации.
- На каждом приборе должен быть предварительно настроен ключ подключения (join key). Это может быть либо единый ключ на беспроводную полевую сеть, либо индивидуальный ключ для каждого устройства.

Примечание

Не используйте коды подключения, установленные по умолчанию.

- Технология «белых списков» (по спискам контроля доступа ACL) — при использовании индивидуальных ключей подключения приборам открыто присваивается разрешение на присоединение к сети через шлюз или устройство управления сетью и запись ACL, которая включает их глобальный уникальный адрес HART. «Белый список» является рекомендуемым режимом работы для беспроводного шлюза. «Белый список» не поддерживается беспроводной платой ввода/вывода системы DeltaV.

Совокупность таких функций обеспечения безопасности создает высокий уровень надежности коммуникационной системы, которая при этом остается удобной в использовании и управлении. Несмотря на то что технология WirelessHART выполняет полное шифрование информации, передаваемой в полевых условиях, и гарантирует присутствие в сети только авторизованных приборов, этого недостаточно для обеспечения безопасности сети КИП. Помимо этого, необходима защита соединения между шлюзом полевой сети и хост-системой.

Способы защиты соединения между беспроводным шлюзом Emerson и хост-системой

- Внутренний межсетевой экран, который можно легко настроить на то, чтобы в процессе коммуникации использовались только те протоколы и порты, которые необходимы для полевого решения.
- Все протоколы на базе Ethernet (Modbus, OPC, EtherNet/IP, AMS, HART Port, https) поддерживают обмен данными, защищенный протоколом SSL.
- Внутренний двунаправленный межсетевой экран шлюза имеет настройку по умолчанию «отклонить все», при этом определенные пользователем протоколы и порты открываются на экране настройки протоколов безопасности (*Setup-Security-Protocols*S).
- Межсетевой экран не требует активного управления.

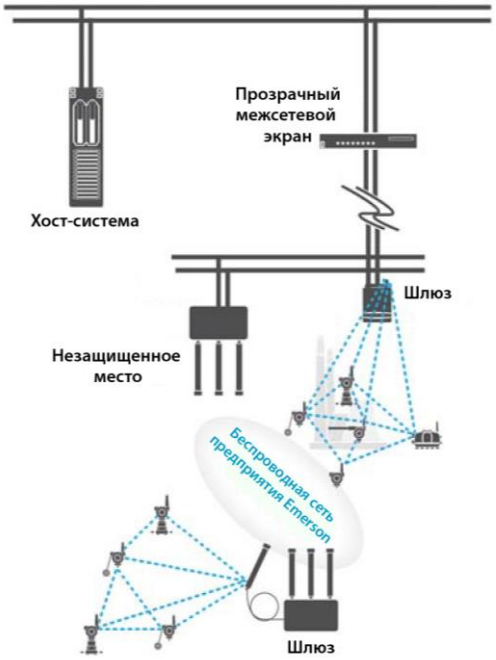
Таблица 1-2. Атаки на беспроводную сеть предприятия и способы защиты

Атаки	Способы защиты				
	Защита от преднамеренных помех	Проверка подлинности	Проверка	Кодирование	Управление ключами
Отказ в обслуживании	✓				✓
Спуфинг		✓		✓	
Атаки с перехватом		✓	✓	✓	
Повторить			✓		✓
Атаки HELLO-Flood	✓	✓	✓		✓
Атака «бездонная воронка»		✓		✓	✓
Перехват информации				✓	✓

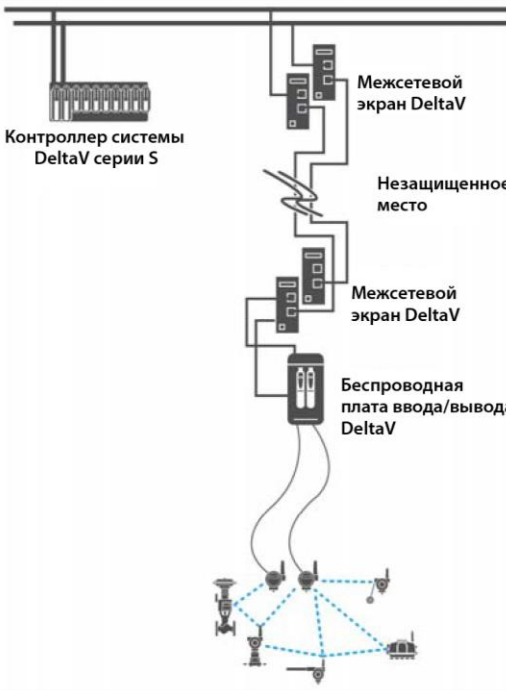
С целью защиты от хакеров, пытающихся взломать сеть предприятия через Ethernet-соединение между шлюзом и узлом на объекте, особенно если шлюз расположен в незащищенном месте, со стороны узла объекта в безопасной зоне можно установить межсетевой экран.

Рисунок 1-5. Межсетевые экраны

Прозрачный межсетевой экран между шлюзом и хост-системой



Межсетевой экран DeltaV между беспроводной платой ввода/вывода и системой DeltaV



Плата беспроводного ввода/вывода системы DeltaV

Помимо беспроводного шлюза, Emerson имеет резервированную беспроводную плату ввода/вывода (WIOC) и беспроводной антенный модуль Field Link 781 с целью естественной интеграции в систему DeltaV версии 11 или более поздней.

Соединение между WIOC и контроллером DeltaV защищено следующим образом.

- Внешний межсетевой экран DeltaV, который настроен на разрешение только протоколов и портов DeltaV для обмена данными.
- WIOC отклоняет любой обмен данными, который не соответствует собственному протоколу DeltaV.
- Конфигурирование и управление работой WIOC осуществляется с помощью программного обеспечения DeltaV.

8 Требования к безопасности беспроводной сети

В следующем разделе приведены распространенные угрозы безопасности, связанные с существующими технологиями. В связи с тем, что такие угрозы все еще дают о себе знать, решения по борьбе с ними продолжают совершенствоваться.

8.1 Беспроводные полевые приборы Emerson

Поскольку шлюз беспроводной сети полевых КИП Emerson связан с производственной зоной посредством Ethernet-соединения, многие заказчики запрашивают установку межсетевого экрана в месте подключения шлюза к производственной IP-сети. Очевидно, что это обусловлено стремлением защитить соединение между шлюзом и сетью управления технологическим процессом от уязвимостей. Компания Emerson выполнила данное требование, разработав шлюз, который одновременно служит беспроводной точкой доступа для КИП и специализированным межсетевым экраном, что позволяет устранить произвольные и сопутствующие затраты на установку дополнительного сетевого устройства.

Межсетевой экран шлюза легко настраивать, он не требует активного управления после установки и направляет весь обмен данными только на порты, соответствующие выбранным протоколам, по которым передаются данные о технологическом процессе и контролируются настройки шлюза.

Для защиты сети предприятия или РСУ от вторжения Emerson может предложить отдельный межсетевой экран, который открывает для коммуникаций и доступа только те порты, которые требуются шлюзу или РСУ.

В разделах ниже описаны способы защиты беспроводной сети Emerson от различного вида атак.

Преднамеренное создание радиопомех

Помимо технологии широкополосного сигнала с прямой последовательностью (DSSS), *Wireless*HART использует радиопередатчики стандарта IEEE 802.15.4 (2,4 ГГц) с функцией переключения каналов. Как показала практика, совокупность таких средств обеспечивает высокую устойчивость к помехам в разнообразных суровых условиях эксплуатации. Сеть WirelessHART — самоорганизующаяся и самовосстанавливающаяся ячеистая сеть, которая позволяет приборам передавать данные на шлюз через другие приборы по нескольким маршрутам, что повышает уровень надежности сетевых коммуникаций до 99,9 %.

Ряд тестирований на совместимость, проведенных компанией Emerson, доказали возможность совместного функционирования WirelessHART и Wi-Fi без блокирования каналов и существенного повреждения данных протоколов связи.

Перехват информации

Каждый прибор имеет собственный ключ сеанса связи со шлюзом, выполняющим шифрование передаваемых данных, так что они не могут быть декодированы даже другим устройством WirelessHART, направляющим сообщение от имени исходного прибора.

Раскрытие передаваемых данных

Несмотря на то что приборы в сети WirelessHART передают данные при гораздо меньшем энергопотреблении, чем приборы на базе протокола 802.11, угроза раскрытия информации все же существует. Поэтому технология WirelessHART обладает большим количеством защитных механизмов, благодаря которым неавторизованный пользователь может только обнаружить факт осуществления беспроводного обмена данными, но не может получить к ним доступ, перехватить информацию или повредить сеть каким-либо иным способом.

Атака повторного воспроизведения (или временные задержки)

Шлюз WirelessHART управляет безопасностью сети приборов. После присоединения к сети каждому прибору присваивается сетевой ключ и уникальный ключ сеанса связи для шифрования обмена данными со шлюзом. Поскольку для каждого сообщения используется одноразовый крипто-графический код, который никогда не распространится на другие сообщения, в изменении сетевых или сеансовых ключей не возникает необходимости. Использование одноразового кода в совокупности с надежным криптоалгоритмом и ключом достаточной длины приводит к тому, что даже повторно отправляемые сообщения передаются в виде уникальной зашифрованной последовательности.

Одноразовый код канального уровня состоит из 8-октетного адреса отправителя и полного 5-октетного номера ASN (счетчик времени увеличивается каждые 10 мс). При интервале дискретизации в 1 с номер ASN не повторяется как минимум 300 лет, т. е. одноразовый код канального уровня никогда не будет использован повторно, что предотвращает атаки повторного воспроизведения. Поскольку одноразовый код включает индикацию времени, атаки, основанные на временных задержках, также блокируются. Одноразовый код сетевого уровня, который используется для управления сетью WirelessHART, является единым для всех устройств. WirelessHART также поддерживает 8-октетный адрес отправителя плюс счетчик на 4 октета, плюс 1 октет со значением 0. При интервале дискретизации в 1 с одноразовый код не будет повторяться более 136 лет.

Атаки с перехватом (обход системы защиты)

Защита устройств от атак с перехватом осуществляется с помощью одноразового кода канального уровня и кода проверки целостности сообщений, которые рассчитываются на каждом транзитном участке. Несмотря на то что технология WirelessHART выполняет полное шифрование информации, передаваемой в полевых условиях, и гарантирует присутствие в сети только авторизованных приборов, этого недостаточно для обеспечения безопасности сети КИП. Также важно отметить, что WirelessHART намеренно не подразумевает присвоения IP-адресов периферийным устройствам, что предотвращает риск применения многочисленных вредоносных программ в качестве атак на беспроводную полевую сеть. Однако для комплексной защиты сквозной коммуникации между полевым устройством и потребителем данных необходимо также защитить соединение между шлюзом полевой сети и хост-системой.

Атака Сибиллы

При атаке Сибиллы злоумышленник подрывает систему репутации одноранговой сети, создавая большое количество идентификаторов и используя их для получения непропорционально большого влияния. Прежде всего, все устройства в сети WirelessHART должны проходить проверку подлинности, чтобы неавторизованные устройства не могли подключаться к сети. Использование уникального кода подключения для каждого устройства создает список контроля доступа (ACL) на беспроводном шлюзе. Каждое устройство имеет свой уникальный идентификатор, который контролируется и поддерживается шлюзом и виден пользователю. Списки контроля доступа указаны в технических характеристиках WirelessHART (IEC-62591) и гарантируют, что одно устройство может иметь только один идентификатор. Технические характеристики WirelessHART также предусматривают либо автоматическое чередование ключей, либо чередование по запросу. Чередование ключей осуществляется через веб-интерфейс шлюза для систем WirelessHART от Emerson или доступно в качестве функции через проводник системы DeltaV для карты беспроводного ввода-вывода DeltaV.

Управление беспроводной сетью Emerson

Для обеспечения защиты сети пользователь должен выполнять ряд передовых практик, однако большинство сложных задач выполняются самой сетью автоматически.

Управление ключами подключения

В зависимости от настроек, выполняемых администратором шлюза, ключ подключения может быть единым для всех сетевых устройств или же уникальным для каждого из них. Единый ключ подключения виден только администратору шлюза. Индивидуальные ключи подключения всегда скрыты от всех. Изменить ключ (-и) подключения может только администратор.

Единый (или уникальный для каждого устройства) ключ подключения можно изменить в настройках беспроводного шлюза Wireless в любое время. Такое изменение безопасным способом распространяется по всей ячеистой сети WirelessHART, при этом старый (-е) ключ (-и) подключения становится (становятся) недействительным (-и). Использование коммуникаторов моделей 375 и 475 для настройки ключей подключения позволяет выполнить масштабное развертывание устройств и последующее изменение ключа подключения для защиты сети от злонамеренного или неосторожного инсайдера.

Для обеспечения более строгой системы безопасности, которую удобнее использовать, перед монтажом и подключением приборов в сеть WirelessHART технические специалисты могут настроить их с помощью приложения AMS Device Manager и модема HART. При использовании графического интерфейса AMS Device Manager пользователь не видит присваиваемый прибору ключ подключения в шестнадцатеричном представлении.

Отсутствие необходимости в планировании частот

Сети WirelessHART не требуют планирования частот. Согласно проектным характеристикам, протокол использует каждый канал в пределах диапазона 2,4 ГГц, выполняя переключение каналов в ходе нормальной передачи данных. Испытания на совместимость между приборами с поддержкой *WirelessHART* и Wi-Fi описаны в отдельном информационном документе Emerson. До тех пор, пока расстояние между приборами Wi-Fi и средствами измерения WirelessHART не превышает одного метра, проблем, связанных с несовместимостью, в процессе передачи данных по сети не возникает.

Предотвращение несанкционированного доступа

Надежность пароля для доступа к шлюзу контролируется на локальном уровне. Заводские учетные записи теперь не могут быть активированы локальным администратором **без** ключа опции для встроенного ПО, предоставленного поставщиком. Этот ключ присваивается индивидуально каждому конкретному шлюзу. Впоследствии администратор может отозвать данную опцию.

В это время функция определения местоположения КИП недоступна. Внутренние функции шлюза защищены с помощью управления доступом на основе ролей, настроенном на шлюзе. Пользователям должны быть присвоены роли и предоставлены соответствующие пароли на основании привилегий на доступ.

Для предотвращения вмешательств в настройки шлюза при работе пользователя со шлюзами предусмотрены эффективные процессы и процедуры управления паролями.

Физический доступ

Физическая безопасность является важной частью любой программы обеспечения безопасности и играет важную роль для защиты вашей системы. Ограничьте физический доступ неуполномоченному персоналу для защиты активов конечных пользователей. Это относится не только к системам WirelessHART, но ко всем системам, используемым на данном предприятии. Несанкционированный персонал может стать причиной серьезного повреждениям оборудования конечных пользователей. Это может быть сделано намеренно или непреднамеренно, но оборудование должно быть защищено от этого.

Безопасность на основе ролей

Шлюз защищен по принципу распределения ролей, что позволяет обеспечить четыре уровня доступа к функциям, которые конечные пользователи могут настроить.

Роль	Имя пользователя	Доступ через веб-интерфейс
Руководитель	exec	Доступ только для чтения
Оператор	oper	Доступ только для чтения
Обслуживание	maint	Конфигурирование настроек устройства HART Конфигурирование протокола связи Modbus Настройка для отображения реестров Modbus Настройка древовидного меню OPC Конфигурирование пользовательских трендов
Administartor	admin	Включает все права, необходимые для технического обслуживания Конфигурирование настроек сети Ethernet Настройка сетевых параметров WirelessHART® Установка паролей Установка настроек времени Установка опций начальной страницы Конфигурирование страниц пользовательских точек Повторный запуск приложений

Программы DeltaV и AMS имеют защиту на основании разрешений, что позволяет определять возможный уровень доступа пользователя к беспроводным устройствам и плате WIOC.

«Ключ» разрешения	Доступ к системе управления
Конфигурирование или запись в память устройства	Запуск платы WIOC Назначение беспроводного устройства каналу Изменение параметров устройства
Эксплуатация	Доступ только для чтения
Диагностика	Переключение платы WIOC на резервное устройство

8.2 Решения «Мобильный сотрудник». Wi-Fi и WLAN 802.11

Беспроводные решения Emerson предлагаются с использованием технологии ячеистой Wi-Fi-сети Cisco, основанной на группе стандартов 802.11-2007.

По мнению Emerson, стандартизация применения технологии Wi-Fi и доступность оборудования на рынке имеют огромную ценность, поскольку это обеспечивает возможность выбора из широкого ассортимента продуктов и приложений, которые легко интегрируются в новые приложения и решения, а также обмениваются данными с ними.

Опасения, представленные в настоящем разделе, относятся к стандарту 802.11, который подвержен угрозе безопасности, поскольку передаваемые беспроводные сигналы могут быть получены любым имеющимся на рынке прибором с поддержкой данного стандарта.

Чтобы преодолеть такие риски, необходимы решения, основанные на данной группе стандартов и обеспечивающие выполнение ряда механизмов, защищающих от угроз безопасности и атак, которые уже происходили с общедоступным ПО.

Предотвратить вторжение хакеров в сеть можно как минимум путем аутентификации пользователей перед предоставлением доступа к беспроводной сети. Кроме того, решение Emerson шифрует все беспроводные данные, которые передаются в пределах ячеистой Wi-Fi-сети, а также между такой сетью и всеми клиентскими устройствами, что предотвращает перехват данных и манипулирование информацией несанкционированными пользователями.

В разделе ниже описаны способы защиты беспроводной сети предприятия от различного вида атак.

Преднамеренное создание радиопомех

Беспроводная сеть предприятия, которую разворачивает Emerson, представляет собой систему с точками доступа ячеистой технологии на базе контроллера, а не простую совокупность автономных точек доступа.

Автономные точки доступа настроены на обмен данными по одному каналу, и в случае обнаружения помех на близлежащих частотах такие точки необходимо менять вручную.

Решение Emerson, основанное на контроллере, имеет многочисленные преимущества.

- Точки доступа ячеистой сети мониторят радиоволны и сигналы, поступающие от других точек доступа, и выполняют динамическую корректировку силы сигнала и канала, с которым взаимодействуют, чтобы минимизировать помехи как вне ячеистой сети, так и внутри нее.
- В то время как все точки доступа ячеистой сети могут передавать данные по разным каналам, клиентское устройство легко переключается с одной точки доступа на другую, при этом пользователю не нужно выполнять какие-либо операции по управлению каналами связи.
- В совокупности с системой предотвращения вторжений в беспроводную сеть ячеистая сеть одновременно проверяет радиоволны на наличие сигналов, создающих преднамеренные помехи в сети, направляет администратору предупредительный сигнал при возникновении проблемы и выполняет триангуляцию местоположения источника помех.

Неавторизованные точки доступа

Подключение к ячеистой сети неавторизованных точек доступа (или ноутбуков) предотвращается с помощью процедуры аутентификации устройств. Каждая точка доступа ячеистой сети имеет уникальный сертификат X.509 с цифровой подписью. Цифровой сертификат подтверждает подлинность точки доступа для всей ячеистой сети. Точки доступа, которые пытаются подключиться к сети или имитировать сетевую среду, помечаются системой предотвращения вторжений.

На предприятии устанавливается минимум одна точка доступа Wi-Fi, которая прослушивает используемые частоты. Аномальные коммуникации помечаются системой WIPs, установленной в первостепенной инфраструктуре.

Оценка площадок

Предлагая услуги для организации беспроводных сетей на предприятиях, Emerson выполняет оценку соответствующих площадок предприятия, чтобы определить существующие радиочастотные сигналы и возможные помехи от близлежащих зон. Инженер по беспроводным решениям спроектирует сеть так, чтобы расположение точек доступа ячеистой сети и тип антенны максимально уменьшили возможные помехи. Для полевых установок WirelessHART оценка площадок не требуется.

Для клиентского доступа к ячеистой сети используется протокол 802.11 b/g/n, а протокол 802.11a применяется для беспроводной транспортировки клиентских данных в проводную сеть. Сеть позволяет выбирать класс обслуживания, за счет чего клиентские устройства в единой беспроводной ячеистой сети могут иметь доступ к нескольким сконфигурированным виртуальным ЛВС. Таким образом, пользователи группы офисных ресурсов могут работать в той же самой физической ячеистой сети, что и пользователи ресурсов по управлению технологическим процессом, оставаясь при этом совершенно изолированными друг от друга. Благодаря этому нет необходимости в организации нескольких Wi-Fi-сетей. На предприятии будет функционировать только одна общая беспроводная ячеистая сеть.

Раскрытие передаваемых данных

Emerson рекомендует заказчикам всегда транслировать идентификатор SSID. Отключение функции трансляции или скрытие SSID не обеспечивает полноценную защиту и затрудняет связь в сети. SSID передается в составе зондирующего фрейма запроса и фрейма запроса на ассоциацию. Эти фреймы не шифруются, а отправляются прямым текстом, поэтому идентификатор SSID легко узнать, даже если не осуществляется его трансляция.

Перехват информации

На разрешенных участках развернутой Emerson беспроводной сети предприятия реализуется технология криптографической защиты WPA2 (алгоритм AES на блоки длиной 128 бит).

Сеть WPN предполагает объединение с сервером аутентификации, авторизации и учета с использованием протокола RADIUS, для того чтобы безопасно подтверждать подлинность пользователей по их стандартным сетевым учетным данным, что обеспечивает динамическое управления ключами защиты и устраняет угрозу безопасности для пользователя при выборе гибкого метода проверки подлинности EAP (протокол расширенной проверки подлинности).

Изоляция беспроводной сети

Сеть WPN поддерживает большое количество виртуальных беспроводных ЛВС, которые в конечном итоге должны быть соединены с одной проводной сетью или несколькими. Такую структуру обеспечивает управляемый коммутатор. Несмотря на то что управляемого коммутатора достаточно для изоляции каждой виртуальной ЛВС таким образом, чтобы она передавала данные **только** подключенной к ней проводной сети, Emerson также устанавливает межсетевые экраны, которые гарантируют поступление трафика на соответствующий уровень с целью предотвращения перекрестных сетевых коммуникаций.

Emerson поддерживает возможность конфигурации назначения адресов пользователей, для того чтобы отключить DHCP-сервер и при необходимости выполнять назначение только статических IP-адресов.

8.3 Возможности управления и обслуживания

Обучение

Поскольку беспроводные решения Emerson относительно сложны в сравнении с беспроводными полевыми КИП, специалисты компании совместно с вами составят программу обучения в соответствии с конкретными потребностями, включив в нее в качестве одного из аспектов работу с беспроводными сетями.

- Управление сетью

  Контроль оборудования и конфигурации

  Конкретная информация о местоположении и установке

  Управление общим беспроводным доступом в корпоративную сеть и сеть предприятия

- Управление защитой доступа к данным

  Доступ и авторизация пользователей

  Управление паролями по стандартной процедуре ИТ-службы

  Риски и угрозы нарушения безопасности

- Конкретные приложения в составе решения

Цель обучения — формирование способности к самостоятельным действиям в соответствии с потребностями.

Поддержка

Emerson предлагает комплексную поддержку при решении проблем в ходе ежедневной работы. Поддержка сети WPN осуществляется в соответствии с договором о локальном сервисном обслуживании. Такие договоры составляются индивидуально путем выбора программы обслуживания из пакета сервисных модулей SureService™ в соответствии с вашими потребностями и задачами. Услуги по сервисному обслуживанию оказывают как эксперты по технической поддержке Emerson, так и местная сервисная служба. Если заказчики работают в системе DeltaV при развернутой сети WPN, они могут обратиться в глобальный сервисный центр за экспертной технической поддержкой.

Для комплексного беспроводного решения от Emerson разработан портфель услуг по поддержке после реализации проекта:

- экспертная техническая поддержка специалистов;
- экстренное обслуживание на месте эксплуатации;
- программа управления запасными частями;
- плановое техническое обслуживание на месте эксплуатации — обновление ПО;
- сопровождение приложений и управление сроком службы оборудования.

Предотвращение несанкционированного доступа

В рамках решения Emerson предусмотрен AAA-сервер, который может быть расположен в пределах сети и настроен на работу с системами информационной безопасности вашего предприятия, для того чтобы пользователи оперировали одними и теми же уникальными учетными данными для доступа как к офисным, так и к производственным ресурсам. Благодаря этому пользователям не нужно заводить отдельные учетные записи для беспроводной, производственной и корпоративной сетей. Служба ИТ может управлять доступом к беспроводной

сети тем же способом, что и к проводной сети. Такое управление осуществляется с помощью RADIUS-серверов, которые могут быть расположены в разных сетях и выполнять аутентификацию пользователей, которым разрешен доступ к конкретной сети (производственной или офисной).

Сеть WPN поддерживает функцию предоставления административных прав и привилегий отдельным пользователям или группам пользователей, чтобы ограничить доступ, разрешающий управление критически важными сетевыми настройками.

В сети WPN реализована технология управления ключами WPA2 Enterprise, что устраняет необходимость управления ключами каждого отдельного пользователя. Защита сертификатов сетевой безопасности (ключей) обеспечивается программой по управлению WPN так, что только авторизованные пользователи могут иметь права на расширение сети или изменение ключей.

Сеансовые ключи для пользователей беспроводной сети (используемые для шифрования передаваемых данных между клиентским устройством и точкой доступа) обновляются каждый раз, когда клиентское устройство выполняет ассоциирование с точкой доступа ячеистой сети, поэтому нет необходимости управлять чередованием ключей.

Двухфакторная аутентификация, совместимая с интерфейсом CryptoAPI операционной системы Microsoft® Windows™, может быть использована для проверки подлинности устройства, подключаемого к беспроводной сети, а также для того, чтобы начать работу с приложениями или серверами производственной и офисной сети.

8.4 Беспроводная сеть как специализированное техническое решение

Услуги Emerson по организации сети WPN представляют собой специализированное решение под ключ, которое включает следующее.

Анализ площадок и консультирование

Инженеры по беспроводным технологиям компании Emerson совместно с заинтересованными лицами вашего предприятия разработают комплексный план работы в соответствии с текущими и долгосрочными потребностями. Исходя из конкретных требований, инженеры Emerson проведут радиочастотное исследование на объекте и соберут прочие сведения о месте эксплуатации, необходимые для определения количества и месторасположения точек доступа ячеистой сети.

Проектирование и планирование сети и архитектуры системы

Согласно результатам исследования объекта и особенностям внедряемого решения, соответствующего требованиям бизнеса, инженеры выполняют комплексное проектирование архитектуры системы, включая сетевую инфраструктуру, механизмы обеспечения безопасности и приложения. На этапе проектирования и планирования сети формируется рабочий проект сетевой инфраструктуры, который может быть проанализирован производственными специалистами и сотрудниками службы ИТ на предмет соответствия всем требованиям.

Управление на этапе монтажа физической сети и ввод системы в эксплуатацию

Emerson предоставляет подробные указания относительно схемы размещения и способа установки каждой точки доступа ячеистой сети на производственном предприятии. Вы можете установить беспроводное оборудование силами Emerson или путем привлечения других ресурсов. После монтажа компонентов сети Emerson выполнит их конфигурирование и запуск в эксплуатацию всей сети.

Внедрение приложений

Основываясь на конкретных требованиях, инженеры разработают и включат приложения в состав беспроводного решения, после чего установят их на предприятии.

9 Беспроводные сетевые мосты

Беспроводные мосты от Emerson обладают всеми функциями обеспечения безопасности, подробно описанными в предыдущем разделе, самой важной из которых является полное шифрование всех беспроводных коммуникаций между устройствами, объединенными беспроводным мостом. Emerson предлагает следующие дополнительные инструкции по монтажу.

- Установите управляемые коммутаторы, для того чтобы обеспечить мониторинг беспроводной сети и проводной сети с внутрисистемной коммутацией.
- По возможности используйте полосу на 5 ГГц (зависит от мирового региона), поскольку полоса на 2,4 ГГц может быть перегружена.
- Контролируйте узлы канала беспроводной коммуникационной сети с помощью приложения на базе простого протокола сетевого управления (SNMP). WhatsUp® Gold — одна из возможных программ для мониторинга, а также выявления и устранения проблем, которые могут возникнуть при передаче данных.
- Настройте функцию мониторинга SNMP на выполнение периодических проверок, чтобы предотвратить ухудшение характеристик беспроводных коммуникаций с течением времени вследствие изменения условий окружающей среды.

9.1 Преднамеренное создание радиопомех

См. «Преднамеренное создание радиопомех» на стр. 22.

9.2 Раскрытие передаваемых данных

Сети, которые соединены с помощью беспроводного моста, как правило, настроены на отсутствие клиентского доступа, то есть так, чтобы не было анонсированного сетевого доступа, который могут обнаружить несанкционированные клиенты.

9.3 Перехват информации

Сетевой мост полностью шифруется с помощью личных сертификатов AES. Доступ к таким личным кодам есть только у ограниченного круга лиц.

10 Сертификаты

Если на вашем предприятии предъявляются особые требования по обеспечению безопасности беспроводных решений, специалисты Emerson могут совместно с вами проработать все необходимые аспекты.

11 Архитектура сети

В следующем разделе представлено описание компонентов беспроводной сети предприятия, приведенной на рисунке 1-6 на странице 32. Несмотря на то что все приложения от компании Emerson функционируют на одном и том же оборудовании беспроводной сети предприятия, коммуникации между ними надежно изолированы друг от друга. Для всех наиболее важных компонентов беспроводной сети предприятия существуют резервные элементы.

A. Беспроводной шлюз Emerson1

Управление конфигурацией беспроводной полевой сети осуществляется с помощью системы DeltaV (начиная с версии 10) или приложений AMS Intelligent Device Manager. Автоматический опрос шлюза начинается сразу после его подключения к управляющей сети DeltaV. Достаточно перетащить (Drag and drop) свободный шлюз в подсистему беспроводного ввода/вывода, и ему будет автоматически присвоен IP-адрес. Информация о беспроводных передатчиках, подключенных к сети шлюза, автоматически заносится в базу данных. Пользователю нужно просто перетащить новый беспроводной преобразователь, закрепив его за назначенным каналом. После этого с точки зрения конфигурации беспроводной преобразователь будет выглядеть так же, как любое проводное устройство. Ввод/вывод через шлюз можно связать с одним контроллером. Управление шлюзом и всеми его коммуникациями выполняется через систему DeltaV и сопутствующие приложения. Emerson 1420 и 1552WU — это беспроводные шлюзы, которые могут быть интегрированы в систему DeltaV, тогда как Emerson 1552WU также включает в себя возможность подключения по Wi-Fi.

B. Плата беспроводного ввода/вывода

Версия 11 системы DeltaV дополнена резервированной беспроводной платой ввода/вывода (WIOC), что позволяет реализовать решение DeltaV по стандарту автоматической настройки конфигурации с функцией полного резервирования. Плата WIOC управляет сетью устройств WirelessHART по радио через устройство Rosemount 781 Field Link. Сетевое управление и управление безопасностью беспроводных устройств WirelessHART осуществляется платой WIOC аналогично управлению беспроводным шлюзом Emerson.

Автоматический опрос платы WIOC начинается сразу после ее подключения к управляющей сети DeltaV. Достаточно перетащить (Drag and drop) свободную плату WIOC в подсистему беспроводного ввода-вывода, и ей будет автоматически присвоен IP-адрес. Информация о беспроводных передатчиках, подключенных к сети WIOC, автоматически заносится в базу данных. Пользователю нужно просто перетащить новый беспроводной преобразователь, закрепив его за назначенным каналом. После этого с точки зрения конфигурации беспроводной преобразователь

будет выглядеть так же, как любое проводное устройство. Ввод/вывод с платы WIOC можно связать с несколькими контроллерами (до 4 контроллеров). Управление платой WIOC и всеми ее коммуникациями выполняется через систему DeltaV и сопутствующие приложения.

C. Беспроводной DMZ

Сегмент DMZ дополнительно отделяет приложения беспроводной сети от сетей предприятия и корпоративных сетей путем изолирования коммуникаций сервера приложений с помощью межсетевого экрана в рамках отдельного диапазона сетевых IP-адресов, а также посредством контроля доступа со всех сторон. Механизм обеспечения защиты реализуется внутри домена, но управлять DMZ можно из различных сетей.

D. Коммутатор уровня распределения

Это управляемый сетевой коммутатор в центре беспроводной и проводной связи. В общей беспроводной сети конфигурируются виртуальные локальные сети, после чего каждая из них подключается к соответствующим проводным сетям. Все компоненты беспроводного сегмента DMZ подключаются к беспроводной сети через коммутатор. Коммутатор выполняет базовые функции межсетевого экрана, но при необходимости для повышения качества функционирования можно использовать дополнительный межсетевой экран.

E. Контроллер беспроводной локальной сети

Контроллер — это компонент, который автоматически выполняет активное управление точками доступа ячеистой технологии в рамках беспроводной сети предприятия. Контроллер управляет безопасностью передачи данных внутри самой сети и разрешает присоединение к сети только санкционированных точек доступа ячеистой технологии. Контроллер беспроводной локальной сети — это устройство, которое отвечает за выполнение беспроводных функций в пределах сети, включая политики безопасности, обнаружение вторжений, управление радиочастотами, качество обслуживания (QoS) и мобильность. Информация от клиентов Wi-Fi поступает через контроллер беспроводной локальной сети в туннельный протокол CAPWAP (протокол управления и инициализации беспроводных точек доступа) и затем — в проводную сеть. Информация с устройств, аппаратно подключенных к Mesh-точкам доступа, поступает не на контроллер беспроводной локальной сети, а непосредственно в корневую точку доступа.

F. Первостепенная инфраструктура

Первостепенная инфраструктура представляет собой графический инструмент, с помощью которого администратор может легко настраивать конфигурацию и управлять всей беспроводной сетью, а сетевые менеджеры — проектировать, управлять и вести мониторинг беспроводных сетей предприятий из одной точки, что упрощает работу. Система WCS выполняет мониторинг работы контроллеров беспроводной локальной сети. Эта программа осуществляет управление сетью, включая диагностику и устранение неисправностей, а также обеспечивает бесперебойную работу сети.

G. Первостепенная инфраструктура с системой предотвращения вторжений в беспроводную сеть (wIPS)

Беспроводная система предотвращения вторжений добавляет еще один уровень «глубокой защиты» (Defense in Depth) от потенциальных беспроводных атак. Кроме управления доступом к сети, wIPS защищает беспроводную сеть от атак

и обеспечивает целостность всех беспроводных клиентов, получивших доступ к сети. Точка доступа Cisco серии 3600 конфигурируется для мониторинга радиочастотного спектра и передачи данных об аномалиях в первостепенную систему с помощью wIPS.

H. Система Mobility Services Engine (MSE)

MSE необходима для wIPS и решений по определению местоположения. В комплексе с первостепенной системой платформа выполняет все математические расчеты и операции для передачи данных об аномалиях, обнаруженных в беспроводной сети.

I. Межсетевой экран системы DeltaV

Прозрачный межсетевой экран системы DeltaV можно сконфигурировать так, чтобы по обе стороны от него располагалась одна и та же подсеть, при этом обмен информацией будет разрешен только между устройствами с определенными IP-адресами, а доступ будет предоставлен только к тем портам, которые необходимы системе DeltaV для обмена информацией между шлюзом и управляющей сетью через беспроводную сеть предприятия.

J. OPC-сервер интеллектуального беспроводного шлюза

Шлюз может обмениваться данными с OPC-клиентами (например, с OPC Mirror) через OPC-сервер шлюза, установленный на ПК проводной сети. OPC-сервер шлюза обменивается данными со шлюзом через защищенные линии связи SSL. Полностью поддерживаются версии 2 и 3 стандарта OPC DA. OPC-сервер используется, если в распределенной хост-системе управления (DCS) нет собственного интерфейса WirelessHART.

K. OPC-сервер системы DeltaV

Самый простой способ организации связи между шлюзом и системой DeltaV (до версии 9 включительно) — через OPC-сервер системы DeltaV, который может быть лицензирован на рабочих станциях DeltaV «Интеграционная» (Application Station) или «Базовая» (Base Station).

L. Точка доступа ячеистой сети

Точки доступа ячеистой технологии обеспечивают соединение с беспроводными портативными устройствами, которые используют мобильные сотрудники, или со стационарными Wi-Fi-ресурсами (например, видеокамерами). Кроме того, неподвижные активы, такие как беспроводной полевой шлюз, могут иметь проводное соединение с точкой доступа ячеистой технологии, которая обеспечивает беспроводное транзитное соединение с корневой точкой доступа и далее с проводной сетью. Таким образом, шлюз подключается к хост-системе управления. Беспроводной шлюз Emerson 1552WU также является ячеистой точкой доступа для сети Wi-Fi.

M. Видеокамеры

Решение для удаленного видеонаблюдения позволяет использовать различные камеры: стационарная камера, «панорама-наклон-зум» (PTZ), беспроводные и тепловизионные камеры. Большинство камер подключается к точкам доступа ячеистой сети для транзитной связи.

M. Видеосервер

Все видеоизображения централизованно регистрируются, хранятся и предоставляются на другие рабочие станции и приложения с сервера цифровой видеозаписи. Пользователи могут дистанционно просматривать и сохранять видеозаписи с различных IP-камер, просматривать сохраненные видеозаписи и моментальные снимки, управлять PTZ-камерами способом click-to-point через интерфейс интернет-браузера. Все видеоизображения централизованно регистрируются, хранятся и предоставляются на другие рабочие станции и приложения с сервера цифровой видеозаписи, который может находиться в пределах сегмента DMZ беспроводной сети.

O. Видеоклиент

Видеоклиент обеспечивает настраиваемый интерфейс для связи с сетевыми камерами. Являясь клиентом видеосервера, видеоклиент может управлять несколькими камерами, подключенными к нескольким видеосерверам. Пользователь может определить, как использовать пространство экрана при наличии неограниченного количества режимов просмотра с отображением нескольких пунктов списка и функций. В этих режимах пользователь может просматривать сохраненное видео и видео в режиме реального времени, управлять PTZ-камерами, планировать порядок просмотра изображений скоростной видеокамеры и управлять предупредительными сигналами.

P. RFID-метки беспроводного оборудования

RFID-метки передают информацию о своем местонахождении по беспроводной ячеистой сети. Можно использовать множество меток, включая метки с кнопками вызова для сигнализации об аварийной ситуации для объекта-носителя.

Q. Сервер определения местоположения

На данном сервере выполняются все правила предупредительной сигнализации о местоположении, а также хранятся настройки данных о пользователях и оборудовании.

R. Клиент определения местоположения

Это веб-приложение позволяет любому пользователю получить визуальное представление о местоположении оборудования и персонала, которое выводится на экран в виде карты. На графическом дисплее можно отслеживать перемещения конкретных сотрудников в режиме реального времени. Операторы могут легко получить доступ к контактной информации о сотруднике или физическим характеристикам физических активов: для этого достаточно щелкнуть мышью экранную пиктограмму.

S. Резервные точки доступа с функциями моста

Существует несколько моделей беспроводных точек доступа, которые можно установить в качестве беспроводного моста в зависимости от требований к сети. Есть точки доступа для установки в помещениях и вне помещений, а также оборудование, сертифицированное на соответствие классу I, разделу 2 или зоне 2 ATEX. Применяемый радиоприемник может соответствовать стандартам IEEE 802.11 a/b/g/n в зависимости от местных норм и конкретных требований к решению.

T. Мобильные устройства

Хотя компания Emerson и продвигает ноутбуки Panasonic® Toughbook® CF-19 и CF-31 и Panasonic Toughpad® FZ-G1, обладающие высокой надежностью и способные выполнять приложения PlantWeb™ компании Emerson с беспроводным подключением к процессу, компания поддерживает и другие беспроводные ноутбуки и карманные компьютеры, указанные и затребованные пользователем. По требованию заказчика Emerson может предоставлять специализированные программные решения.

U. Служба удаленного доступа (RAS)

Мобильные устройства DeltaV Operate подключаются к серверу приложений DeltaV, который управляет службой удаленного доступа и находится внутри сегмента DMZ беспроводной сети. Посредством непрямой маршрутизации все данные о технологическом процессе в системе DeltaV направляются из службы RAS, расположенной в сети управления или сети предприятия, через беспроводную DMZ в службу RAS, находящуюся в пределах беспроводной DMZ. Таким образом, еще эффективнее реализуется отделение безопасных коммуникаций.

V. Терминальный сервер

В традиционных системах управления можно использовать сервер терминала, при условии что они поддерживают сервер терминала корпорации Microsoft или иных разработчиков. Компания Emerson готова помочь заказчикам определить жизнеспособность такого решения и сформулировать требования к нему.

W. Сервер RADIUS

RADIUS-сервер выполняет аутентификацию и авторизацию пользователей для доступа к беспроводной сети и конкретным SSID-сетям (виртуальным ЛВС). Это упрощает управление доступом пользователей с помощью настройки локальных групповых политик.

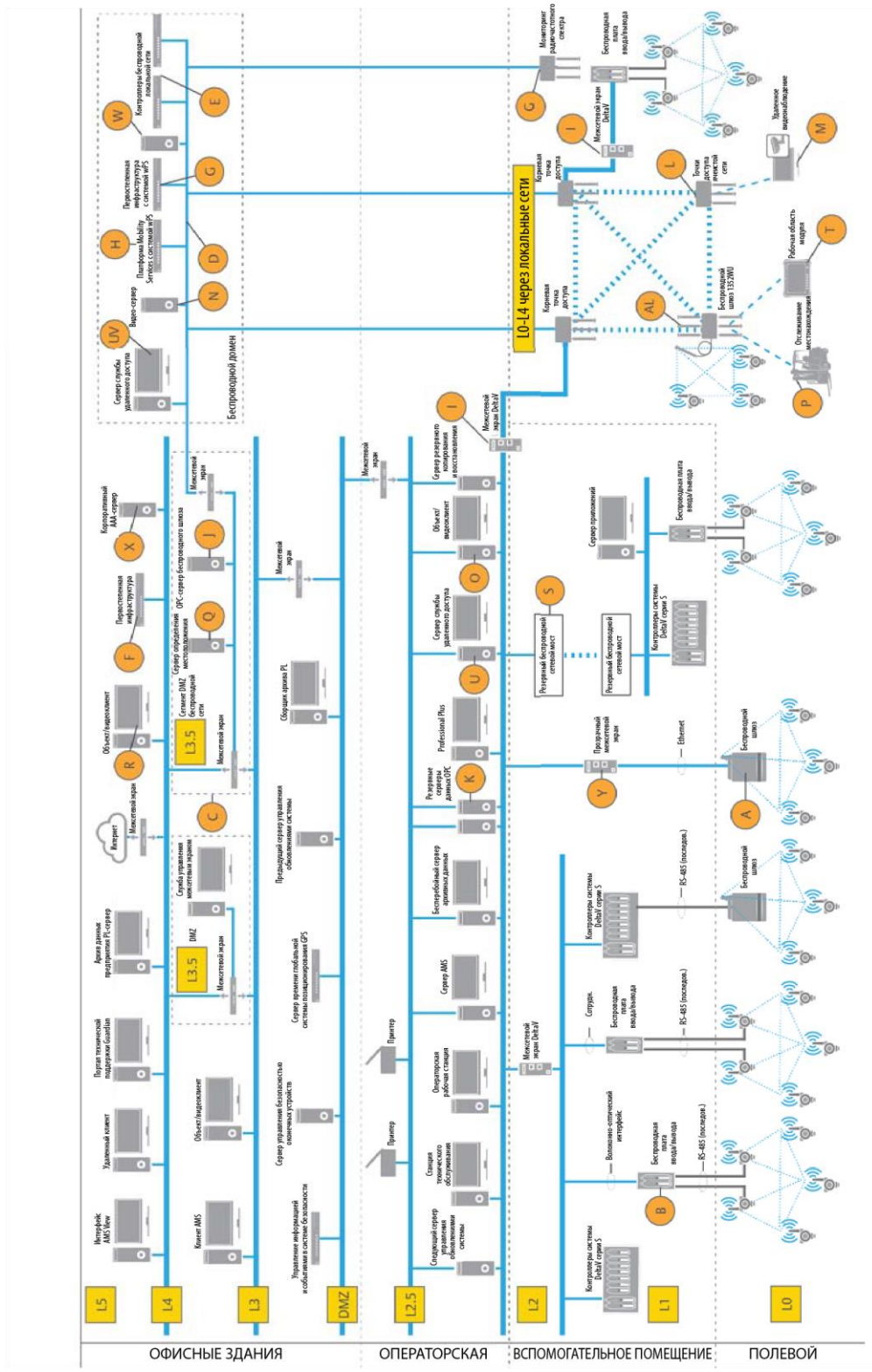
X. Контроллер домена предприятия (AAA)

RADIUS-сервер конфигурируется для аутентификации пользователей с помощью сервера аутентификации, авторизации и учета (AAA-сервера), имеющегося у пользователя. Учетные данные пользователей хранятся здесь, а не локально в беспроводной DMZ.

Y. Прозрачный межсетевой экран

Прозрачный межсетевой экран можно сконфигурировать так, чтобы по обе стороны от него располагалась одна и та же подсеть, при этом обмен информацией будет разрешен только между устройствами с определенными IP-адресами, а доступ будет предоставлен только к тем портам, которые необходимы системе DeltaV или AMS для обмена данными между шлюзом (или WIOC) и локальной управляющей сетью.

Рисунок 1-6. Архитектура сети



12 Выводы

Безопасность беспроводных сетей имеет первостепенное значение для успешного внедрения как сетей для полевых устройств, так и решений на уровне предприятия. Настоящий документ описывает возможности Emerson по внедрению безопасных, надежных и функциональных беспроводных решений для полевых устройств и производственных применений.

Специалисты Emerson являются экспертами по технологиям обеспечения безопасности и могут внедрить их совместно с вами для более эффективного мониторинга технологических процессов, повышения производительности сотрудников и снижения производственных расходов.

Обладая практическим опытом и профессионализмом в сфере беспроводных технологий, компания Emerson предлагает готовые решения для беспроводных полевых КИП и беспроводных решений на уровне предприятия.

Техническое примечание
00840-0200-6129, ред. AA
Сентябрь 2017 г.

Emerson Automation Solutions

Россия, 115054, г. Москва,
ул. Дубининская, 53, стр. 5
Телефон: +7 (495) 995-95-59
Факс: +7 (495) 424-88-50
Info.Ru@Emerson.com
www.emerson.ru/automation

Азербайджан, AZ-1025, г. Баку
Проспект Ходжалы, 37
Demirchi Tower
Телефон: +994 (12) 498-2448
Факс: +994 (12) 498-2449
e-mail: Info.Az@Emerson.com

Казахстан, 050060, г. Алматы
ул. Ходжанова 79, этаж4
БЦ Аврора
Телефон: +7 (727) 356-12-00
Факс: +7 (727) 356-1 2-05
e-mail: Info.Kz@Emerson.com

Украина, 04073, г. Киев
Куреневский переулок, 12,
строение А, офис А-302
Телефон: +38 (044) 4-929-929
Факс: +38 (044) 4-929-928
e-mail: Info.Ua@Emerson.com

Промышленная группа «Метран»

Россия, 454003, г. Челябинск,
Новоградский проспект, 15
Телефон: +7(351)799-51-52
Факс: +7 (351) 799-55-90
Info.Metran@Emerson.com
www.metran.ru

Технические консультации по выбору и применению продукции осуществляет Центр поддержки Заказчиков
Телефон: +7 (351) 799-51-51
Факс: +7 (351) 799-55-88

Актуальную информацию о наших контактах смотрите на сайте www.emerson.ru/automation