Система безопасности уровня Mission Critical на базе систем Private LTE

Евгений Трифонов
Директор по продажам
ГК "ТРИАЛИНК"

Транспортная инфраструктура – вокзалы, аэропорты, метро, железные и автомобильные дороги, морские и речные порты – всегда имела стратегическое значение для экономики страны. Надежная и бесперебойная работа транспорта связана также с безопасностью и сохранением жизни людей. Неслучайно отдельные объекты и транспорт в целом относятся к критически важной инфраструктуре. В связи с этим бесперебойную работу транспорта можно отнести к критически важным операциям (Mission Critical Operations), а систему управления и связи на транспорте, необходимую для выполнения этих операций, – к критически важным средствам коммуникации (Mission Critical Communications)

Уровень Mission Critical означает повышенные требования к системе связи, в частности более высокую доступность, надежность и безопасность. При этом новые возможности открывает внедрение цифровых технологий.

Цифровизация работы предприятия позволяет повысить уровень надежности и безопасности за счет успешного выполнения следующих задач:

- охрана периметра;
- контроль доступа;
- видеонаблюдение и видеоаналитика;
- управление сотрудниками службы безопасности;
- система оповещения и громкоговорящей связи (ГГС);
- контроль местоположения сотрудников и транспортных средств как внутри, так и вне помещений (Indoor/Outdoor Positioning);
- контроль использования средств индивидуальной защиты (СИЗ);
- мониторинг физического состояния сотрудников;
- распознавание лиц и объектов, в том числе на основе биометрических данных;
- прогнозирование и предотвращение кризисных ситуаций.

Единая информационная среда предприятия

Построение системы управления и безопасности, выполняющей перечисленные задачи, невозможно без создания единой информационной среды. Она состоит из опорной сети и центральной инфраструктуры, системы беспроводной связи, оконечного оборудования различного типа (камеры, датчики, контроллеры и т.д.), универсальных абонентских устройств и специального программного обеспечения.

Формирование единой информационной среды дает возможность внедрения и интеграции различных ИТ-решений, обеспечивая их совместимость, возможность необходимых апгрейдов, модернизации, будущего технического сопровождения и развития. Важно при этом предусмотреть необходимый уровень защиты информации и надежную работу системы в случае кризисной ситуации. Наконец, нельзя не учитывать стоимость строительства системы и ее использования.

Выбор решения для системы беспроводной связи

Системы голосовой технологической радиосвязи используются на транспорте десятки лет. Они построены на базе узкополосных протоколов радиосвязи, что не позволяет передавать данные с высокой скоростью (например, живое видео в высоком качестве) или использовать многие современные ИТ-решения.

При выборе системы связи с перспективой будущего использования и развития следует ориентироваться на новые современные стандарты. Один из них – протокол LTE (Long Term Evolution), созданный в рамках 3GPP (3rd Generation Partnership Project) – международной группы разработчиков стандартов в области телекоммуникаций. LTE-решения используются по всему миру уже несколько лет и хорошо себя зарекомендовали.

Изначально стандарт разрабатывался для операторов, предоставляющих услуги связи частным лицам, но позже в него были добавлены функции, необходимые для профессиональных потребителей, таких как полиция, транспорт, энергетика, промышленность. Основной целью было создание на базе LTE систем Mission Critical с уровнем надежности 99,999% (то есть допускается отсутствие связи не более 5 мин. 16 с в течение года), а также обеспечение таких специальных функций, как MC PTT (Mission Critical Push-To-Talk), MC Video и MC Data. Эти функции подразумевают выполнение голосовых вызовов, передачу видео и данных с заданным уровнем надежности как индивидуально, так и группе абонентов с минимальными задержками.

Соблюдение ключевых требований

Использование технологии LTE уровня Mission Critical удовлетворяет следующим важным требованиям:

1. Необходимая надежность работы системы, в том числе в случае чрезвычайной ситуации.
2. Применение различных ИТ-решений, использующих протокол пакетной передачи данных IEEE 802.3 (Ethernet).
3. Функция PTT (Push-To-Talk) связи.
4. Обеспечение необходимой пропускной способности при передаче данных, включая передачу видео в высоком качестве с необходимого числа видеокамер.
5. Подключение мобильных и стационарных объектов (видеокамеры, датчики, контроллеры и др.).
6. Возможность расширения и модернизации.
7. Поддержка необходимого количества объектов и абонентов (с учетом будущего развития).
8. Необходимый охват территории предприятия системой беспроводного доступа, в том числе внутри зданий, помещений и туннелей.
9. Защита информации и контроль доступа к системе.
10. Интеграция с другими системами (Интернет, телефонная сеть общего пользования (ТфОП), системы радиосвязи и др.).
11. Возможность подключения облачных сервисов и стыковки с внешними центрами обработки данных (ЦОД).
12. Возможность подключения диспетчерских и центров управления.

Выбор бизнес-модели

Существует три способа создания и применения опорной сети и системы LTE:

1. Использовать полностью или частично сеть и инфраструктуру оператора связи, предоставляющего услуги на данной территории (например, одного из сотовых операторов).
2. Строить и развивать собственную систему связи в составе опорной беспроводной или оптоволоконной сети и системы LTE (Private LTE).
3. Выбрать смешанную модель, когда часть системы принадлежит и контролируется заказчиком и используются элементы системы связи оператора.

В первом случае расходы на создание системы связи будут ниже. Операторы связи предлагают корпоративным заказчикам не только дешевые тарифы на телефонную связь и мобильный Интернет, но и дополнительные услуги, такие как PTT-связь для технологической голосовой связи или решения NB-IoT для подключения датчиков различных типов через сотовую инфраструктуру. Однако надежность работы операторской системы связи, особенно в случае кризисной ситуации, когда это особенно важно, невысока. Ни один коммерческий оператор не может гарантировать немедленное предоставление необходимого сервиса (и голосовых вызовов, и мобильного Интернета) в 100% случаев. При работе через оператора также нужно

предусмотреть регулярные платежи за получаемые услуги.

Во втором случае расходы на создание собственной инфраструктуры будут выше, но при этом можно построить систему связи с заданным уровнем надежности, в том числе систему, удовлетворяющую требованиям Mission Critical. Можно заранее предусмотреть на 100% надежную работу всех абонентов и подключенных устройств как в обычном режиме, так и в случае кризисной ситуации (природные или техногенные катастрофы, террористические атаки и т.д.). Такая модель применения системы управления предпочтительна для предприятий и организаций, относящихся к критически важной инфраструктуре, например транспортной.

В случае реализации второго варианта обеспечивается покрытие на определенной территории, за пределами которой связи с абонентами не будет. Работу абонентов за пределами частной сети можно обеспечить, используя третий вариант, когда вне зоны действия частной сети абоненты будут подключаться через сеть оператора. Но надежная работа будет обеспечена только в собственной сети.

Выбор бизнес-модели зависит от специфики работы конкретной организации. Мы рекомендуем строить и использовать собственную систему связи, что обеспечит более высокий уровень управления и безопасности, соответствующий классу Mission Critical.

Технический и функциональный состав операторской и частной сети

Сеть LTE состоит из ядра системы (Core) и базовых станций. В отдельных случаях сотовые операторы предлагают заказчику купить собственные базовые станции LTE и подключить их к ядру системы, находящемуся у оператора. Такую систему нельзя на 100% считать частной, поскольку ее работа зависит от ядра, находящегося у оператора. Сеть LTE будет полностью независимой, если и ядро сети, и базовые станции размещены на стороне заказчика и им контролируются.

При планировании частной сети LTE следует учитывать ее необходимую функциональность и размеры (количество базовых станций и абонентских устройств).

В сети LTE операторского класса, как правило, используется ядро (Core), позволяющее поддерживать очень большое количество базовых станций и имеющее широкий набор функций, таких как VoLTE (Voice Over LTE). Эта функция позволяет абонентам выполнять обычные телефонные звонки через сеть LTE.

Ни один из российских операторов не работает только через сеть LTE. Сотовые сети состоят из различных сегментов – 2G, 3G (GSM) и 4G (LTE). Эти сегменты объединяются в единую сеть на уровне ядра, что требует наличия в составе ядра большого количества дополнительных серверов и делает ядро технически сложным и дорогим. Отдельной задачей оператора является тарификация (биллинг), необходимая для учета предоставленных услуг и последующего оформления счетов абонентам.

При выборе системы связи с перспективой будущего использования и развития следует ориентироваться на новые современные стандарты. Один из них – протокол LTE, созданный в рамках 3GPP – международной группы разработчиков стандартов в области телекоммуникаций

Построение частной LTE-сети в России

Для работы сети LTE требуется разрешение на использование необходимых частотных диапазонов, которые определены самим стандартом. В России сети LTE в основном строятся на диапазонах, утвержденных для Европы, – 2100, 2300, 2600, 1800, 1900, 900, 800 и 450 МГц. В ряде стран регулирующие организации предусмотрели наличие частотного диапазона, предназначенного для создания собственных, частных, сетей LTE, обслуживающих организации охраны общественной безопасности и критически важную инфраструктуру. В России таких зарезервированных для частных сетей LTE диапазонов нет. Имеющийся частотный ресурс распределен между крупными коммерческими операторами. Однако это не означает, что строительство частных сетей LTE в России невозможно. Все крупные российские сотовые операторы предлагают заказчикам возможность построить частную LTE-сеть. Необходимо сотрудничество с оператором, позволяющее развернуть частную сеть на частотах, согласованных регулятором для работы данного оператора. В крупных городах операторы активно используют частотный спектр для коммерческой LTE-сети. Но возможно развертывание частных LTE-сетей для технологической связи в удаленных регионах, за пределами крупных городов – там, где у оператора нет своей коммерческой LTE-сети и частотный диапазон не используется.

В случае технологической частной сети LTE не требуется поддержка сегментов 2G и 3G (GSM). Не требуется тарификация и поддержка очень большого количества базовых станций (eNB). Функция VoLTE в частной сети не является необходимой, поскольку голосовая связь PTT (Push-To-Talk) реализуется с помощью специального PTT-сервера, работа которого построена на мобильной передаче данных. В случае если в частной сети требуются обычные дуплексные телефонные звонки, это можно реализовать с помощью решений VoIP (Voice Over IP), иногда называемых SoftPhone, которые также работают на базе функций передачи данных через сеть LTE. Таким образом, все необходимые в частной сети LTE функции могут быть обеспечены с помощью ядра (Core), имеющего только базовые функции. Такое ядро будет технически значительно проще и, соответственно, дешевле.

Операторская сеть будет удовлетворять требованиям Mission Critical, только если в сети будут реализованы функции QCI (Quality Class Indicator) и обеспечены необходимые значения QoS (Quality Of Service), позволяющие предоставлять определенной части абонентов сервисы MC PTT, MC Data, MC Video с наивысшим приоритетом. Это позволяет гарантировать определенным абонентам надежную работу в кризисной ситуации, когда сеть перегружена и обычные абоненты работать не могут. Функции QCI технически доступны в ядре (Core) операторских сетей, но ни один из операторов на сегодняшний день ее не использует и не планирует использовать.

И в операторской, и в частной сети LTE для достижения уровня Mission Critical требуется обеспечить резервирование всех элементов, включая электропитание, опорную сеть, через которую подключаются базовые станции, сами базовые станции (обеспечение двойного покрытия) и ядро (Core).

Таким образом, операторские и частные сети хотя и используют одну технологию LTE, но строятся для совершенно различных целей. Для достижения необходимой функциональности, надежности и приемлемой стоимости частной сети Private LTE можно использовать соответствующее оборудование (в первую очередь ядро), не имеющее избыточных функций.

Покрытие LTE-сети

Дальность связи (покрытие) сети LTE зависит от используемого диапазона, рельефа, наличия препятствий, типа антенн, высоты их подвеса и других факторов. Наиболее выгодным с точки зрения дальности является диапазон 450 МГц (B31), однако возможности получения этого диапазона для сетей Private LTE очень ограничены. Более вероятно получение разрешений на развертывание Private LTE в диапазонах B38 или B40 (2,3–2,4 ГГц). Дальность связи в этом случае будет значительно меньше. При использовании специальных направленных антенн с высотой подвеса 15–20 м дальность связи Private LTE в B38 или B40 может достигать 1,5–2 км, что позволяет построить сеть с необходимым покрытием достаточно большой территории с помощью 3–4 базовых станций.

Оценку стоимости решения Private LTE можно сделать, если провести расчеты радиопокрытия применительно к конкретному объекту, знать конкретные требования к беспроводной сети и определить, какой тип ядра (Core) будет использоваться в системе.

Центр управления системой (Control Room)

Центр управления и безопасности, кроме функций управления, обеспечивает интеграцию отдельных подсистем, сбор и хранение информации, визуализацию данных различного типа на экранах дежурного или диспетчера, подключение внешних модулей и возможность подключения к системе верхнего уровня. Обычно центр управления имеет возможность подключения подсистем для решения следующих задач:

- управление работой предприятия;
- управление технологическими процессами;
- мониторинг технологических процессов, экологических и климатических параметров;
- видеонаблюдение;
- управление парком транспортных средств;
- мониторинг транспортных средств и отдельных сотрудников с возможностью отображения местоположения на карте;

- обеспечение безопасности (контроль доступа, охрана периметра, противопожарная система и др.);
- специализированные ИТ-решения;
- PTT – голосовая технологическая связь с мобильными абонентами.

Кроме того, обеспечиваются интерфейсы с центром обработки данных (ЦОД) для сбора и хранения информации (Data Lake) и подключения внешних систем, таких как модули аналитики, системы радиосвязи (PMR), выход в телефонные сети (ТфОП), Интернет и др.

Абонентские терминалы в системах Private LTE

Система управления и обеспечения безопасности будет соответствовать уровню Mission Critical только при использовании специальных абонентских терминалов, также удовлетворяющих требованиям Mission Critical.

Существует достаточно большой выбор абонентских терминалов для работы в сетях Private LTE, к которым относятся мобильные (для установки на транспортное средство) и носимые терминалы (для работы сотрудников).

Носимые терминалы можно разделить на две группы:

1) простые устройства (типа "радиостанция"), имеющие только функции PTT (голосовые вызовы) и возможности позиционирования;

2) смартфоны и планшеты, которые, кроме PTT-связи и позиционирования, могут выполнять самые различные функции и представляют собой универсальные абонентские устройства.

Общей для обеих групп является необходимость установки в терминал СИМ-карты для работы в сети Private LTE.

Кнопка PTT

Для работы в сети Mission Critical следует использовать специальные (промышленные) смартфоны и планшеты, которые имеют повышенные характеристики защищенности, прочности и надежности, батареи повышенной емкости и специальную кнопку PTT.

В сети Private LTE возможно использование обычного смартфона, не имеющего физической кнопки PTT. При этом используется виртуальная кнопка на экране смартфона, нажатием на которую выполняется PTT-вызов. В этом случае невозможно обеспечить быстрый вызов одним нажатием. Требуется сначала вывести смартфон из спящего состояния, разблокировать его (введя ПИН-код), вывести на экран необходимое приложение с виртуальной кнопкой и только после этого нажать на нее. Наличие в смартфоне физической кнопки PTT позволяет обеспечить вызов действительно одним нажатием – так же, как это происходит в системах радиосвязи. Только такие терминалы удовлетворяют требованиям Mission Critical.

Повышенные характеристики прочности и надежности

Для работы в сложных условиях эксплуатации требуются абонентские устройства с повышенными характеристиками прочности и защищенности, в частности имеющие повышенную защиту от пыли и влаги (индекс IP) и ударопрочные корпус и экран, соответствующие требованиям военного стандарта MIL810.

Для работы на объектах с повышенным риском взрыва или пожара используются специальные смартфоны и планшеты, соответствующие требованиям стандарта ATEX (взрывозащита в пылевых или газовых средах).

Надежность работы абонентских терминалов определяется не только прочностью корпуса. В профессиональных абонентских устройствах обычно используются аккумуляторы большей мощности, имеется возможность замены батареи и зарядки в настольном зарядном устройстве (типа "стакан"), что не требует постоянного задействования разъема USB-C или micro-USB, а также доступно применение различных аксессуаров – наушников, гарнитур, выносных микрофонов (в том числе с кнопкой PTT).

Важной особенностью профессиональных абонентских устройств является громкость внешнего динамика. Большинство обычных смартфонов имеет внешний динамик, но громкость его работы значительно меньше, чем у радиостанций систем ПМР, и недостаточна для нормальной работы в системах Private LTE даже при невысоком уровне внешних шумов. Специальные смартфоны, имеющие кнопку PTT, комплектуются динамиком повышенной мощности (2–2,5 Вт).

Операционная система

Многие абонентские терминалы работают под управлением операционной системы Android, но есть и терминалы под управлением российской ОС для мобильных устройств "Аврора". Возможность использования смартфонов и планшетов российского производства с ОС "Аврора" (доверенная среда) особенно важна для государственных организаций и предприятий с высокими требованиями по информационной безопасности.

Некоторые абонентские терминалы типа "радиостанция" работают под управлением ОС Linux, что дает преимущество по скорости соединения и надежности. Открытый код Linux и наличие PTT российского приложения позволяют получить для данных терминалов статус ТОРП (телекоммуникационное оборудование российского производства), что также важно с точки зрения информационной безопасности.

Принципы информационной безопасности и защиты информации

Требования к информационной безопасности повышаются не только в организациях охраны общественной безопасности и государственных структурах, но и в коммерческих компаниях, в том числе транспортных. Защита персональных данных и коммерческой информации становится все более важной задачей.

Для обеспечения информационной безопасности предлагается предусмотреть выполнение следующих принципов:

1. Следует использовать собственную ИТ-инфраструктуру системы управления и безопасности для обеспечения контроля доступа к системе и защиты данных.
2. Собственные протоколы обмена обеспечивают защиту от несанкционированного доступа к информации.
3. В случае необходимости могут применяться средства шифрования и криптографии.
4. Использование программного обеспечения и аппаратных средств российского производства обеспечит более высокий уровень информационной безопасности.
5. Специальные средства идентификации абонентов исключают возможность двойников и несанкционированного подключения.
6. Средства работы администратора системы защищают от несанкционированных изменений в программном обеспечении и ИТ-инфраструктуре.
7. Средства мониторинга ИТ-инфраструктуры обеспечивают оперативный контроль работы системы.

7 практических эффектов внедрения

Цифровая трансформация и внедрение решений Индустрии 4.0 не являются самоцелью. Новые технологии открывают большие возможности и в случае успешного внедрения дают следующие практические результаты:

1. Создание собственной инфраструктуры системы управления и обеспечения безопасности на базе решений Private LTE в рамках перехода на решения Индустрия 4.0 обеспечит более высокий уровень безопасности, эффективности и производительности.
2. Использование собственной системы уровня Mission Critical обеспечит надежную работу системы управления и безопасности не только в обычных условиях, но и в случае кризисных ситуаций различного характера (террористические угрозы, техногенные и природные происшествия).
3. Выбор оборудования для создания сети Private LTE (в первую очередь ядра), имеющего необходимые функции и не обладающего избыточностью, позволит значительно снизить затраты на создание собственной системы LTE.
4. Внедрение искусственного интеллекта и аналитики с использованием больших данных (Big Data) позволяет прогнозировать возможные кризисные ситуации, оперативно менять модель управления и повысить общую эффективность работы предприятия.
5. Внедрение комплексной системы, помимо обеспечения безопасности объектов транспорта, позволит сократить число нарушений техники безопасности, понизить уровень травматизма, исключить возможные хищения и нарушения регламента работы.
6. Система экологического контроля позволит избежать серьезных инцидентов в области экологии и связанных с ними штрафов и дополнительных расходов.
7. Система управления персоналом позволит более эффективно задействовать имеющийся персонал и повысить производительность. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

ТРИАЛИНК

МУЛЬТИСЕРВИСНЫЕ СЕТИ, СИСТЕМЫ ОПОВЕЩЕНИЯ, РАДИОСВЯЗЬ

- Системы связи и передачи данных
- Системы оповещения населения
- Системы мониторинга природных и техногенных явлений и процессов

WWW.TRIALINK.RU

Проектирование и строительство систем Private LTE

для технологических сетей уровня Mission Critical, удовлетворяющих повышенным требованиям к надёжности, доступности и безопасности

СИСТЕМА ПРЕДНАЗНАЧЕНА ДЛЯ:

- Управления работой компании (повышение производительности и эффективности)
- Обеспечения охраны и безопасности

ВЫБОР ОПТИМАЛЬНОЙ КОНФИГУРАЦИИ СЕТИ PRIVATE LTE

- Базовые станции (eNodeB) и ядро сети (Core) от компании Telrad (оптимальное сочетание функций и цены)
- Широкий выбор оконечного оборудования и абонентских терминалов (в том числе смартфоны и планшеты, работающие на Linux или российской ОС АВРОРА)
- PTT Сервер RONET собственного производства (включен в реестр российского ПО)

ПОДСИСТЕМЫ В СОСТАВЕ СЕТИ PRIVATE LTE НА ОСНОВЕ СОБСТВЕННЫХ РАЗРАБОТОК:

- PTT-связь (Push-To-Talk) с функциями позиционирования и передачи данных и видео RONET
- Мониторинг и управление объектами и процессами MARS MONITORING
- Видеонаблюдение и аналитика
- Оповещение и ГГС (Громко-Говорящая Связь) MARS ARSENAL
- Открытая интеграционная платформа MAGIS для подключения отдельных подсистем и внешних модулей и организации Центров Управления и Командно-Контрольных Центров
- Интеграция с существующими системами ПМР (Профессиональная Радиосвязь), различными IT-приложениями, выход в Internet, ТФОП

www.ronet.one
www.mars-arsenal.ru
www.mars-mm.ru

+7 (495)232-11-32

РЕШЕНИЯ РАЗРАБОТАНЫ И ПРОИЗВОДЯТСЯ В РОССИИ