

PRIVATE LTE и системы связи и управления уровня Mission Critical

Е.Трифонов, директор по развитию ГК "ТРИАЛИНК" / e.trifonov@trialink.ru

DOI: 10.22184/2070-8963.2022.102.2.30.38

Рассматривается применение сетей LTE для профессиональных целей на объектах критически важной инфраструктуры. Обосновывается целесообразность использования для решения задач класса Mission Critical технологии Private (частной) сети LTE. Даются рекомендации по выбору диапазонов частот и набора оборудования для создания частных сетей LTE. Описывается комплексное решение для систем Mission Critical на базе технологии Private LTE от компании "ТРИАЛИНК".

БЕЗОПАСНОСТЬ НА ПРОМЫШЛЕННЫХ ОБЪЕКТАХ И ОБЪЕКТАХ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Объекты критически важной инфраструктуры (КВИ) (транспорт, энергетика, связь и др.) всегда имели стратегическое значение для экономики и повседневной жизни. Кроме непосредственного влияния на экономику, бесперебойная работа таких объектов связана с безопасностью и сохранением жизни людей.

Обеспечение надежности функционирования таких объектов и их безопасности имеют высший приоритет. В связи с этим организацию работы данных объектов относят к критически важным операциям (Mission Critical Operations), а систему управления и связи на этих объектах, необходимую для выполнения указанных операций, – к критически важным средствам коммуникации (Mission Critical Communications). Уровень Mission Critical (MC) означает повышенные требования к системе связи, в частности наивысший уровень доступности, надежности и безопасности. Внедрение цифровых технологий открывает новые возможности в создании систем связи уровня Mission Critical.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И "ИНДУСТРИЯ 4.0"

Программы цифровой трансформации и перехода на решения "Индустрии 4.0" приняты к настоящему времени как на федеральном уровне, так и в большинстве компаний и организаций самого различного профиля, в том числе на объектах КВИ. "Индустрия 4.0", или 4-я промышленная революция в управлении современным предприятием – это:

- широкое применение информационных технологий и облачных решений;
- переход к полной автоматизации бизнес-процессов и созданию киберфизических систем;
- создание "цифрового образа" предприятия;
- цифровизация всех сфер деятельности и роботизация;
- широкое внедрение Интернета вещей (IoT) и средств искусственного интеллекта (ИИ);
- аналитика и работа с собранными данными (Data Lake).

Внедрение новых цифровых технологий на объектах критически важной инфраструктуры позволяет добиться новых экономических результатов и качественно повысить уровень безопасности.

Рассмотрим, какие основные задачи должна решать система управления и обеспечения безопасности, удовлетворяющая требованиям "Индустрии 4.0". В первую очередь это задачи управления работой предприятия, в частности:

- внедрение современных систем управления;
- использование технологий промышленного Интернета вещей (IIoT);
- мониторинг состояния объектов транспорта, систем обеспечения, логистики, экологических и климатических параметров;
- видеонаблюдение (с возможностями видеоаналитики);
- использование средств искусственного интеллекта (ИИ);
- управление работой персонала, в том числе с функциями "мобильный работник" и "дополненная реальность", возможностями голосовой технологической связи и работой в специализированных IT-приложениях;
- управление технологическими процессами;
- управление парком транспортных средств, в частности задача "беспилотный транспорт".

Цифровизация работы предприятия позволяет повысить уровень надежности и безопасности, успешно выполняя следующие задачи:

- 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, решающей перечисленные выше задачи, невозможно без создания единой информационной среды, состоящей из опорной сети и центральной инфраструктуры, системы беспроводной связи, оконечного оборудования различного типа (камеры,

датчики, контроллеры и т.д.), универсальных абонентских устройств и специального ПО.

Создание единой информационной среды дает возможность внедрения и интеграции различных IT-решений, обеспечивая их совместимость, возможности необходимых апгрейдов, модернизации, будущего 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.

Рассмотрим подробнее выбор решения для создания единой информационной среды и системы беспроводной связи, которая является ее основной частью. Системы голосовой технологической радиосвязи используются на критически важных объектах десятки лет. Данные системы построены на базе узкополосных протоколов радиосвязи, что не позволяет обеспечивать передачу данных с высокой скоростью и, как следствие, передавать "живое" видео в высоком качестве или использовать многие современные IT-решения. В связи с этим при выборе технологии системы связи с перспективой будущего использования и развития следует ориентироваться на новые современные стандарты.

Одним из таких стандартов является протокол LTE, разработанный партнерством 3GPP. Решения данного стандарта используются по всему миру уже несколько лет и хорошо себя зарекомендовали. Изначально стандарт разрабатывался для использования операторами, предоставляющими услуги связи частным лицам, но позже в его спецификации были добавлены функции, необходимые для профессиональных пользователей, таких как полиция, транспорт, энергетика, промышленность. Целью было поставлено создание на базе LTE систем Mission Critical с уровнем надежности 99,999% (т.е. допускается отсутствие связи не более 5 мин 16 с в течение года), а также обеспечивающих такие специальные функции, как MC PTT (MC Push-To-Talk), MC Video и MC Data. Данные функции означают выполнение голосовых вызовов, передачу видео и данных с заданным уровнем надежности как индивидуально, так и в группе абонентов с минимальными задержками.

При использовании технологии LTE уровня MC обеспечивается выполнение следующих важных требований:

- необходимая надежность работы системы, в том числе в случае ЧС;
- возможность использования различных IT-решений, использующих протокол Ethernet;
- функции связи PTT;

- обеспечение необходимой пропускной способности для передачи данных (в том числе поддержка передачи видео в высоком разрешении с необходимого числа видеокамер);
- возможность подключения мобильных и стационарных объектов (видеокамеры, датчики, контроллеры и др.);
- возможность расширения и модернизации;
- поддержку необходимого количества объектов и абонентов (с учетом будущего развития);
- необходимый охват территории предприятия системой беспроводного доступа (как вне помещений, так и внутри зданий, сооружений и туннелей);
- защита информации и контроль доступа к системе;
- возможность интеграции с другими системами (интернет, ТфОП, системы радиосвязи и др.);
- возможность подключения облачных сервисов и стыковки с внешними ЦОДами;
- возможность подключения диспетчерских и центров управления.

ВАРИАНТЫ ИСПОЛЬЗОВАНИЯ СЕТЕЙ LTE НА ОБЪЕКТАХ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Есть несколько вариантов создания и использования опорной сети и системы LTE:

- использовать полностью или частично сеть и инфраструктуру оператора связи (например, одного из сотовых операторов);
- строить собственную систему связи в составе опорной беспроводной или оптоволоконной сети и частной системы LTE (Private LTE, pLTE);
- смешанная модель, когда часть системы принадлежит и контролируется заказчиком и используются элементы сети оператора связи.

В первом случае расходы на создание корпоративной системы связи будут ниже. Операторы связи предлагают корпоративным заказчикам не только низкие тарифы на телефонную связь и мобильный интернет, но и дополнительные услуги, такие как РТТ для технологической радиосвязи или решения NB-IoT для подключения через сотовую инфраструктуру различных датчиков. Однако надежность работы операторской системы связи, особенно в случае кризисной ситуации, невысока. Ни один коммерческий оператор не может гарантировать предоставления необходимого сервиса (и голосовых вызовов, и интернета) в 100% случаев. При работе через оператора также нужно осуществлять ему регулярные платежи за услуги.

Во втором случае расходы на создание инфраструктуры будут выше, но при этом можно построить систему связи с заданным уровнем надежности, в том числе систему, удовлетворяющую требованиям МС. Можно заранее предусмотреть близкую к 100% надежность работы 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 системы связи и управления предпочтительна для предприятий и организаций, относящихся к критически важной инфраструктуре.

При реализации второго варианта (частная сеть) 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 они будут подключаться через сеть оператора. Но надежная связь будет обеспечена только в зоне покрытия собственной сети.

Выбор бизнес-модели зависит от специфики работы конкретной организации. Но мы рекомендуем строить и использовать собственную систему связи, что обеспечит более высокий уровень управления и безопасности, соответствующий уровню МС.

ВЫБОР ДИАПАЗОНОВ ДЛЯ РАЗВЕРТЫВАНИЯ СЕТИ pLTE

Для работы сети LTE требуется разрешение на использование частот. Частотные диапазоны сетей LTE определены 3GPP. В России такие сети в основном строятся в диапазонах, принятых для Европы: 2600, 2300, 2100, 1900, 1800, 900, 800 и 450 МГц. В ряде стран регуляторы предусмотрели наличие частотного диапазона, предназначенного специально для создания частных сетей LTE, обслуживающих организации охраны общественной безопасности и критически важную инфраструктуру. В России таких "зарезервированных" для сетей pLTE диапазонов нет, имеющийся частотный ресурс распределен между крупными коммерческими операторами.

Сказанное не означает, что строительство сетей pLTE в России невозможно. При создании частной сети LTE необходимо сотрудничество с сотовым оператором, позволяющее развернуть такую сеть на частотах, выделенных ему.

В крупных городах операторы активно используют спектр для коммерческой сотовой сети, в связи с чем развертывание сети pLTE там может оказаться невозможным или трудно реализуемым. Но за пределами крупных агломераций, там, где у оператора нет коммерческой LTE-сети, создание частных сетей вполне возможно. Впрочем, и в крупных городах

может оказаться реальным создание сети рLTE в диапазонах В38 (2570–2620 МГц) или В40 (2300 МГц), отделив таким образом частные сети от общедоступных операторских, работающих в "массовых" диапазонах LTE (В3, В7, В20).

Выбор оборудования для создания сети рLTE

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

При планировании сети рLTE следует учитывать необходимую ее функциональность и размеры (количество БС и абонентских устройств). В сетях LTE операторов используется ядро, позволяющее поддерживать очень большое количество БС и имеющее широкий набор функций, например VoLTE. Данная функция позволяет абонентам выполнять телефонные звонки через сеть LTE. Заметим, ни один из российских операторов не работает только через сеть LTE. Сотовые сети сегодня состоят из сегментов различных типов (2G (GSM), 3G и 4G/LTE). Эти сегменты объединяются в единую сеть на уровне ядра, что требует наличия в его составе большого количества серверов, делая ядро технически сложным и дорогим. Отдельной сложной задачей оператора является тарификация (биллинг).

В случае организации технологической связи на базе рLTE не требуется поддержка сегментов 2G и 3G. В такой сети не нужны тарификация и поддержка большого количества базовых станций (eNB). Функция VoLTE в частной сети не является обязательной, поскольку голосовая связь РТТ может быть реализована с помощью специального РТТ-сервера, работа которого построена на мобильной передаче данных.

В случае если в сети рLTE функция VoLTE отсутствует, но нужны обычные дуплексные телефонные звонки, то это можно реализовать с помощью решений VoIP, иногда называемых SoftPhone, которые работают на базе передачи данных через сеть LTE.

Таким образом все необходимые в сети рLTE функции могут быть обеспечены с помощью ядра, имеющего только базовые функции. Такое ядро будет технически значительно проще и следовательно дешевле, чем ядро операторского класса. Сравнение топологии сетей операторского класса и рLTE показано на рис.1.

Следует отметить также, что операторская сеть будет удовлетворять требованиям МС только, если

в сети реализованы функции QCI (Quality Class Indicator) и обеспечены необходимые значения QoS (Quality Of Service), позволяющие предоставлять определенной части абонентов сервисы МС РТТ, МС Data и МС Video с наивысшим приоритетом. Это позволит гарантировать данным абонентам надежную работу в кризисной ситуации, когда сеть перегружена. Функции QCI технически доступны в ядре операторских сетей, но ни один из операторов на сегодняшний день их не использует и не планирует использовать, поскольку это не соответствует реализуемой оператором бизнес-модели.

Как в операторской, так и в частной сети LTE для достижения уровня МС требуется обеспечить резервирование всех элементов, включая электропитание, опорную сеть, через которую подключаются БС, сами базовые станции (обеспечение "двойного" покрытия) и ядро.

Таким образом операторские и частные сети, хотя и используют одинаковую технологию LTE, строятся для совершенно различных целей и на разных принципах. Для достижения необходимой функциональности, надежности и приемлемой стоимости в сети рLTE можно использовать оборудование (в первую очередь ядро), не имеющее избыточных функций.

Дальность связи (покрытие) сети LTE зависит от используемого диапазона, рельефа, наличия препятствий, типа антенн и высоты их подвеса и других факторов. Наиболее выгодным с точки зрения дальности является диапазон В31 (450 МГц), однако возможности получения этого диапазона в России для сетей рLTE очень ограничены.

Более вероятно получение разрешений на развертывание частных сетей LTE, как упоминалось выше, в диапазонах В38 или В40. Дальность связи в этом случае будет значительно меньше по сравнению с диапазоном В31. Но в случае применения направленных антенн с высотой подвеса 15–20 м дальность связи рLTE в данных диапазонах может быть около 1,5–2 км, что позволяет построить сеть с гарантированным покрытием достаточно большой территории, используя 3–4 БС.

Центр управления системы

Центр управления и безопасности (Control Room), кроме собственно функций управления, обеспечивает интеграцию отдельных подсистем, сбор и хранение информации, визуализацию данных различного типа на экранах дежурного или диспетчера, подключение различных внешних модулей и возможность интеграции с системой верхнего уровня. Обычно центр управления имеет возможность подключения следующих подсистем:

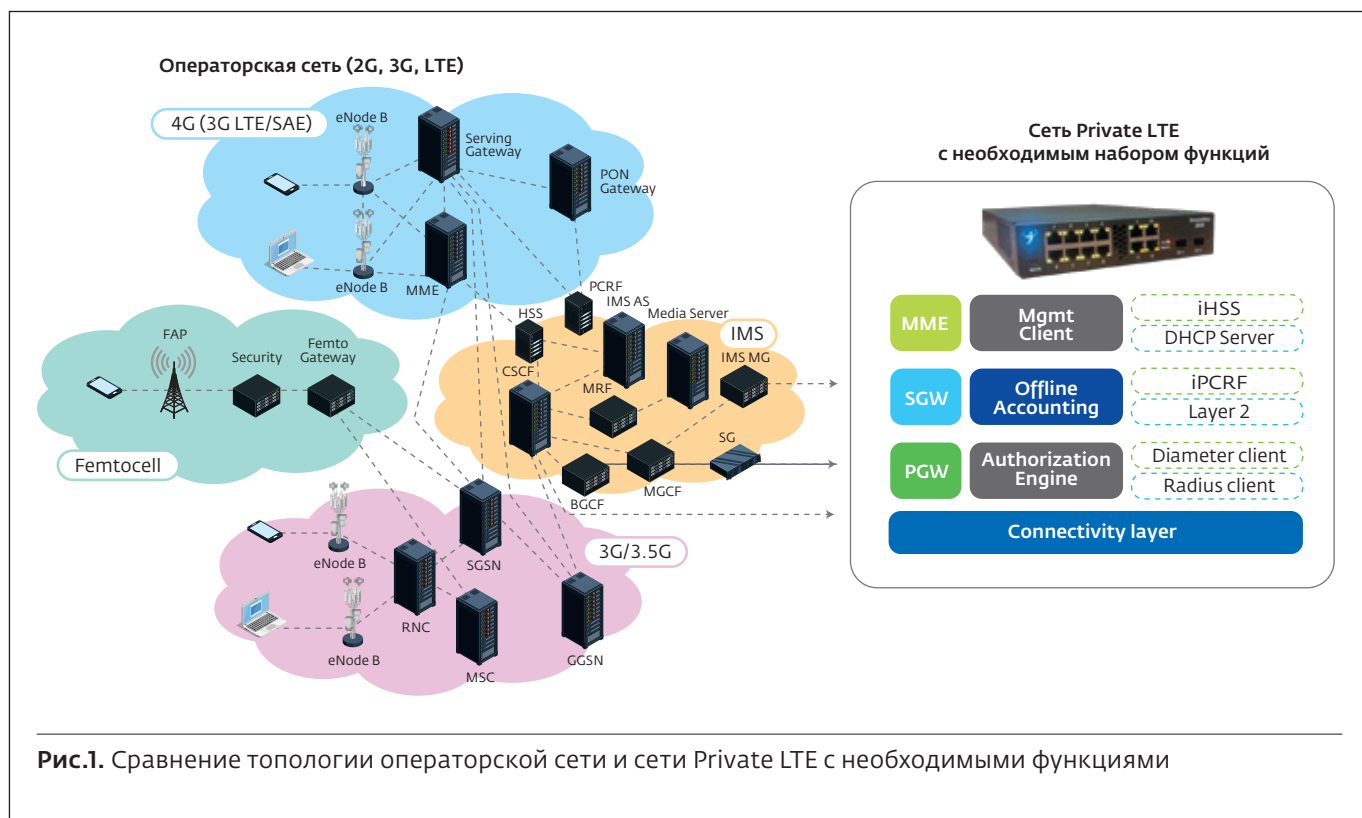


Рис.1. Сравнение топологии операторской сети и сети Private LTE с необходимым набором функциями

- управления работой предприятия;
- управления технологическими процессами;
- мониторинга технологических процессов, экологических и климатических параметров;
- видеонаблюдения;
- управления парком транспортных средств;
- мониторинга транспортных средств и отдельных сотрудников с возможностью отображения местоположения на карте;
- обеспечения безопасности (контроль доступа, охрана периметра, противопожарная система и др.);
- специализированных IT-решений;
- РТТ – голосовой технологической связи с мобильными абонентами.

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

АБОНЕНТСКИЕ ТЕРМИНАЛЫ В СИСТЕМАХ рLTE

Система управления и обеспечения безопасности будет соответствовать уровню МС только, если использовать специальные абонентские терминалы, также удовлетворяющие требованиям Mission Critical.

Для работы в частных сетях LTE имеется достаточно большой выбор абонентских устройств. Это мобильные терминалы (предназначены для установки на транспортное средство) и носимые терминалы (для оснащения сотрудников).

Носимые терминалы, в свою очередь, можно разделить на две группы. Это простые устройства (типа "радиостанция"), имеющие только функции РТТ (голосовые вызовы) и возможности позиционирования. Второй группой являются смартфоны и планшеты, которые, кроме РТТ-связи и позиционирования, могут выполнять самые различные функции. Общим требованием для работы в сети рLTE является необходимость установки в терминал SIM-карты.

Как правило, для работы в сети МС следует использовать специальные (промышленные) смартфоны и планшеты, которые имеют повышенные характеристики защищенности, прочности и надежности, батареи повышенной емкости и специальную кнопку РТТ. Конечно, возможно использование в сети рLTE обычного смартфона, не имеющего физической кнопки РТТ. Для этого задействуется "виртуальная кнопка", появляющаяся на дисплее. Однако, на таком терминале невозможно обеспечить вызов одним нажатием: требуется сначала перевести смартфон из спящего состояния, разблокировав его, вывести на экран необходимое приложение (с "виртуальной кнопкой")

и только затем нажать на нее. Лишь наличие физической кнопки РТТ позволяет обеспечить вызов действительно одним нажатием, как это происходит в системах PMR. И только такие терминалы удовлетворяют требованиям МС.

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

Надежность работы абонентских терминалов определяется не только прочностью корпуса. В профессиональных абонентских устройствах обычно используются аккумуляторы большей мощности, возможность замены батареи и зарядки в настольном зарядном устройстве (типа "стакан"), что не требует постоянного использования USB-C или Micro-USB разъема, а также использование с терминалом различных аксессуаров: наушников, гарнитур, выносных микрофонов (в том числе с кнопкой РТТ). Важной особенностью профессиональных терминалов является громкость внешнего динамика. Специальные смартфоны, имеющие кнопку РТТ, оснащаются динамиком повышенной мощности (2–2,5 Вт), что обеспечивает уровень звука, сравнимый с профессиональными радиостанциями.

Сегодня большинство терминалов работают под управлением ОС Android, но уже есть абонентские устройства, работающие под управлением российской ОС "Аврора". Возможность использования смартфонов и планшетов российского производства с ОС "Аврора" особенно важно для государственных организаций и предприятий с высокими требованиями по информационной безопасности.

Некоторые абонентские устройства типа "радиостанция" работают под управлением ОС Linux. Использование Linux в терминалах может дать преимущество по скорости соединения и надежности. Открытый код Linux и использование российского ПО (приложение РТТ на данном терминале) позволяет получить для данных устройств статус ТОРП (телекоммуникационное оборудование российского производства), что также важно с точки зрения использования в государственных организациях.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Сегодня требования к информационной безопасности (ИБ) повышаются не только в органах охраны общественной безопасности, но и в различных государственных структурах и на объектах КВИ. Для обеспечения ИБ предлагается предусмотреть выполнение следующих принципов:

- использование собственной IT-инфраструктуры системы управления и безопасности для обеспечения контроля доступа к системе и защите данных;
- собственные протоколы обмена, обеспечивающие защиту от несанкционированного доступа к информации;
- в случае необходимости могут применяться средства шифрования и криптографии;
- использование российского ПО и аппаратных средств обеспечат более высокий уровень информационной безопасности;
- специальные средства идентификации абонентов исключают возможность появления "двойников" и несанкционированного подключения;
- средства работы администратора системы защищают от несанкционированных изменений в ПО и IT-инфраструктуре;
- средства мониторинга IT-инфраструктуры обеспечивают оперативный контроль за работой системы.

Все перечисленные средства защиты информации могут успешно применяться в системах рLTE.

КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ СИСТЕМ MISSION CRITICAL НА БАЗЕ ТЕХНОЛОГИИ рLTE ОТ КОМПАНИИ "ТРИАЛИНК"

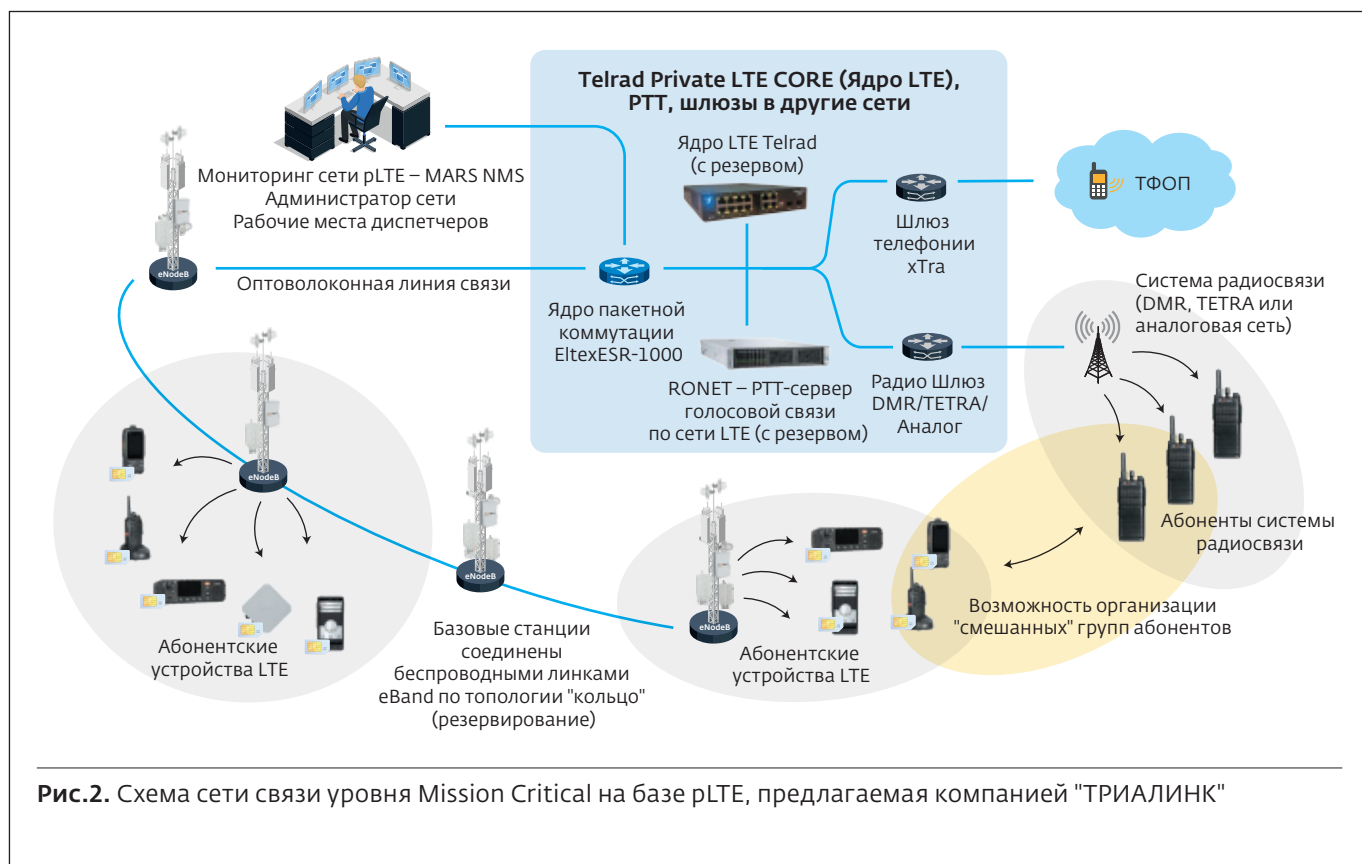
Рассмотрим пример построения сети уровня Mission Critical на основе технологии рLTE, предлагаемое компанией "ТРИАЛИНК".

Требуемый уровень надежности предлагаемой сети обеспечен резервированием всех основных элементов, включая ядро сети (Core), базовые станции, сервер РТТ, опорную сеть и систему электропитания.

Кроме указанного, надежность работы гарантируется расчетом необходимого количества каналов связи для 100%-ной работы абонентских устройств всех типов даже в случае кризисной ситуации с предоставлением необходимых функций (голос, видео и данные по требованиям МС). Доступность связи в протоколе LTE обеспечивается расчетом зоны покрытия с развертыванием необходимого количества базовых станций (eNodeB) и применением специальных направленных антенн.

Схема рассматриваемой системы связи представлена на рис.2.

Как видно из схемы, предлагаемая система Private LTE, кроме поддержки LTE-абонентов, позволяет подключать существующие сети радиосвязи (аналоговые и стандартов DMR и TETRA), а также обеспечивать стыковку с ТфОП. Таким образом внедрение новой технологии может осуществляться постепенно, используя существующие сети и системы связи.



В рассматриваемом решении используются ядро и БС производства компании Telrad. Такой выбор обусловлен тем, что ядро Telrad имеет оптимальную для сети pLTE структуру и доступно по цене. Обеспечиваются все необходимые в частной сети функции (такие как передача голоса с использованием специального РТТ-сервера RONET, разработанного компанией "ТРИАЛИНК", передача видео и данных).

Данное ядро предназначено для поддержки абонентов только LTE (связь по стандартам GSM и 3G в системе не предусмотрена). Хотя ядро не поддерживает функции VoLTE, но телефонные вызовы, в том числе дуплексные, выполняются с помощью приложения Softphone. Не предусмотрен также биллинг, не требующийся в частной сети.

В системе используются БС eNodeB различных типов (в зависимости от необходимого для подключения абонентских терминалов количества каналов), производимые также компанией Telrad. Базовые станции работают в диапазонах В38 и В40, которые в большинстве случаев используются для строительства сетей pLTE.

Вместе с eNodeB в составе комплексного решения pLTE компания "ТРИАЛИНК" предлагает сервисный блок (SB LTE), с помощью которого обеспечиваются

функции коммутации и выполняется резервирование электропитания.

Опорную сеть (для подключения eNodeB к ядру) предлагается строить с использованием оборудования "точка-точка" eBand, работающего в нелицензируемом частотном диапазоне, обеспечивающем необходимую пропускную способность и надежность. Состав базовой станции pLTE представлен на рис.3.

В качестве абонентских устройств сети pLTE предлагается использовать носимые терминалы различных типов, мобильные терминалы для установки на транспортные средства, а также датчики и видеокамеры. Возможно подключение любых стандартных LTE-устройств, работающих в диапазонах В38 и В40.

Информационная безопасность предлагаемого решения обеспечивается применением абонентских устройств, работающих под управлением ПО российского производства, таких как терминал RONET P102 (рис. 4.), работающий под управлением ОС Linux, или смартфоны и планшеты, работающие под управлением ОС "Аврора".

Чтобы предоставить комплексное решение, компания "ТРИАЛИНК" предлагает в составе сети pLTE средства для организации Центра управления на основе диспетчерского приложения системы PoC (Push-To-Talk over Cellular) RONET. Другие IT-подсистемы,

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



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)
- РТТ Сервер RNET собственного производства (включен в реестр российского ПО)

ПОДСИСТЕМЫ В СОСТАВЕ СЕТИ PRIVATE LTE НА ОСНОВЕ СОБСТВЕННЫХ РАЗРАБОТОК:

- РТТ-связь (Push-To-Talk) с функциями позиционирования и передачи данных и видео RNET
- Мониторинг и управление объектами и процессами MARS MONITORING
- Видеонаблюдение и аналитика
- Оповещение и ГТС (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



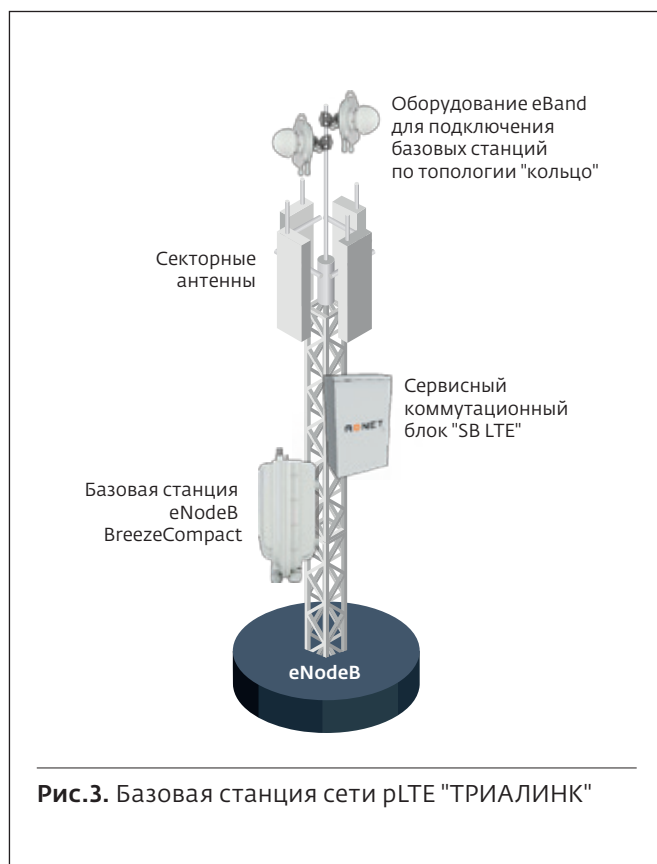


Рис.3. Базовая станция сети рLTE "ТРИАЛИНК"



Рис.4. Абонентский терминал сети рLTE RONET P102

работающие через сеть LTE, такие как видеонаблюдение, мониторинг различных объектов и процессов, оповещение, контроль доступа и др., могут быть интегрированы в единую систему связи и управления с помощью коммуникационной платформы MAGIS, разработанной и поставляемой также "ТРИАЛИНК".

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ УРОВНЯ МС

Цифровая трансформация и внедрение решений "Индустрии 4.0" не являются самоцелью. Такие решения открывают новые возможности и в случае успешного внедрения дают следующие практические результаты:

- создание собственной инфраструктуры системы управления и обеспечения безопасности на базе решений рLTE в рамках перехода на решения "Индустрии 4.0" обеспечит более высокий уровень безопасности, эффективности, доступности и производительности;
- 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;

- выбор оборудования для создания сети рLTE (в первую очередь ядра), имеющего только необходимые функции и не обладающего избыточностью позволит значительно снизить затраты на создание и эксплуатацию собственной системы LTE;
- внедрение систем ИИ и аналитики с использованием Big Data дает возможность прогнозировать кризисные ситуации, а также оперативно менять модель управления и повысить общую эффективность работы предприятия;
- внедрение комплексной системы связи и управления, кроме обеспечения безопасности объектов КВИ, позволит сократить число нарушений техники безопасности и понизить уровень травматизма, исключить возможные хищения и нарушения регламента работы;
- на базе системы связи и управления может быть развернута система экологического контроля, которая позволит избежать серьезных инцидентов в области экологии и связанных с ними штрафов и дополнительных расходов;
- система управления персоналом позволит более эффективно использовать кадры и повысить производительность. ■

XXVIII Международный форум по информационно-коммуникационным технологиям







6-10.06.2022

пр. Победителей, 111а
г. Минск, Республика Беларусь

ЗАО «Техника и коммуникации»
Тел.: (375-17) 306 06 06
E-mail: tibo@tc.by

tibo.by



XXVIII Международный форум по информационно-коммуникационным технологиям

tibo





6-10.06.2022

пр. Победителей, 111а
г. Минск, Республика Беларусь

ЗАО «Техника и коммуникации»
Тел.: (375-17) 306 06 06
E-mail: tibo@tc.by
tibo.by





XXVIII Международный форум
по информационно-коммуникационным
технологиям

tibo





6-10.06.2022
 пр. Победителей, 111а
 г. Минск, Республика Беларусь

ЗАО «Техника и коммуникации»
 Тел.: (375-17) 306 06 06
 E-mail: tibo@tc.by



tibo.by

XXVIII Международный форум
по информационно-коммуникационным
технологиям

tibo





6-10.06.2022
пр. Победителей, 111а
г. Минск, Республика Беларусь

ЗАО «Техника и коммуникации»
Тел.: (375-17) 306 06 06
E-mail: tibo@tc.by

tibo.by



XXVIII Международный форум по информационно-коммуникационным технологиям

tibo

6-10.06.2022
пр. Победителей, 111а
г. Минск, Республика Беларусь

ЗАО «Техника и коммуникации»
Тел.: (375-17) 306 06 06
E-mail: tibo@tc.by
tibo.by

