ВОЕННЫЕ СРЕДСТВА СВЯЗИ И РАДИОЧАСТОТНАЯ БЕЗОПАСНОСТЬ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Левицкий Ю.Ю

Горбачев К.Л – к.т.н., доцент

В работе рассматриваются основные факторы, влияющие на качество и безопасность радиосвязи. Рассматриваются подходы и решения для реализации наиболее эффективных средств связи с точки зрения габаритов, потребления, технических характеристик и безопасности.

Разработка военных средств коммуникации, в частности радиостанций, по-прежнему направлена на расширение рабочей полосы частот, уменьшение веса, габаритов и потребления. Тем не менее, ключевой компонент, который также должен усовершенствоваться для повышения эффективности работы радиостанции – это безопасность радиосвязи. Обеспечение защиты и безопасности радиосвязи, является основным требованием любых спецслужб, вплоть до того что в архитектурах многих радиостанций, используется несколько процессоров для обеспечения разделения между безопасной и незащищенной обработкой сигналов.

Усовершенствование средств связи для вооруженных сил, в частности радиостанций, по-прежнему направлено на расширение рабочей полосы частот, уменьшения размера, веса и потребления. Однако ключевой компонент, который также должен быть рассмотрен, чтобы максимизировать операционную эффективность - это безопасность связи. Безопасная связь является основой любой военной отрасли, также во многих радиостанциях в архитектуре может доминировать решение безопасности, не смотря на то что для обеспечения разделения между безопасной и незащищенной обработкой требуется несколько процессоров. Для достижения наиболее эффективных результатов, необходимо совмещать как высокотехнологичные средства обеспечения безопасности, так и современные технологические решения по части приемопередатчика.

Традиционно, военные радиостанции обычно состоят из четырех или пяти ключевых блоков обработки. Каскад радиочастоты используется для предварительной обработки принятого сигнала с антенны, обеспечения соответствующей фильтрации, усиления и преобразования частоты. Этап оцифровки преобразует высокочастотные данные в цифровой вид. В рамках цифровой обработки ряд специализированных этапов используется для выполнения модуляции и демодуляции до того, как стадия криптографии обеспечит безопасность принятых и переданных данных. Последним этапом обработки является пользовательский интерфейс, который может включать голосовые кодеки или обработку видео. В некоторых случаях используются до пяти этапов цифровой обработки, как показано на рисунке 1.

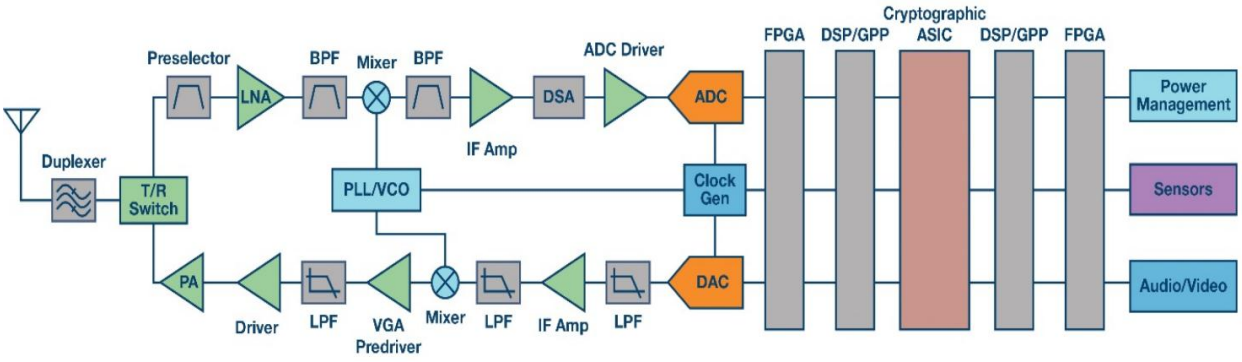

Рисунок 1 –Структурная схема современной радиостанции

Несмотря на превосходное функционирование, количество этапов обработки может сделать радиостанции громоздкими. В последние годы основное внимание уделялось сокращению дискретных компонентов на этапах приема и передачи данных путем их интеграции в микросхемы, а также увеличению функциональности цифровых блоков с учетом преимуществ обработки ПЛИС. Обработка на основе FPGA была ключевым фактором в течение последних двух десятилетий для программируемых радиостанций, особенно с учетом выделенных процессорных блоков в FPGA-матрице. FPGA предоставили конфигурируемые, обновляемые и более модульные архитектуры. Однако, учитывая требования безопасности, все еще существуют ограничения для данной архитектуры. Например, наличие криптографического процессора, ограничивает любое возможное сокращение габаритов, и потребления.

В последние годы произошла революция в новых технологиях интеграции микросхем для оцифровки и компонентов, реализующих функцию приемопередатчика. Новые технологии в области приемопередатчиков прямого преобразования, обеспечили возможность интеграции МШУ, модуляторов I / Q и демодуляторов, ФАПЧ, АЦП и ЦАП. Использование прямого преобразования было реализовано с помощью встроенной калибровки и алгоритма квадратурной коррекции ошибок (QEC), который преодолел ограничения использования этой архитектуры вместо супергетеродинного решения. В качестве альтернативы, новые высокоскоростные преобразователи теперь могут напрямую обрабатывать или генерировать сигналы в приемопередатчике на частотах от 6 ГГц и выше.

Не смотря на то что FPGA обеспечивают дальнейшую оптимизацию для программируемых радиостанций, необходим новый подход для использования криптографического процессора и поддержки инфраструктуры безопасности. Криптографические подходы на основе программного обеспечения предлагают решение проблемы интеграции. С помощью этого метода криптография может быть совмещена с обработкой модуляции и демодуляции и потенциальными функциями пользователя, такими как обработка голоса или изображений.

Путем перенастройки или обновления FPGA, могут быть применены различные уровни безопасности, что уменьшает необходимость в аппаратных изменениях. Легко поддерживаются обновления для исправления ошибок и добавление функций.

Используя вышеописанные варианты, возможно высоко интегрированное решение. Например, тот, который обеспечивает значительные преимущества для приложений с малой потребляемой мощностью и размерами. Структурная схема изображена на рисунке 2.

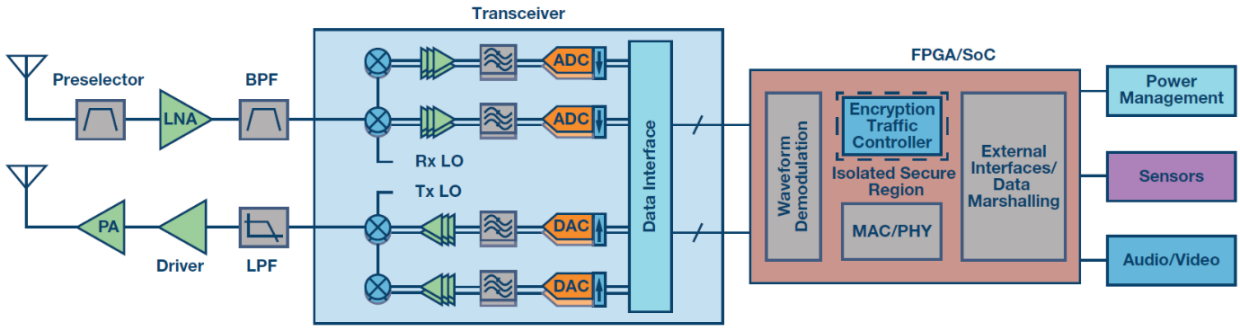

Рисунок 1 –Оптимальная структура радиостанции

Блок приемопередатчика, такой как AD9371, обеспечивает почти полный функционал радиочастотной части, за исключением усилителя с низким уровнем шума (LNA) и усилителя мощности передатчика (HPA). Полоса пропускания до 100 МГц может обрабатываться и передаваться в устройства обработки сигналов. Для этого Xilinx Zynq-7000 можно комбинировать с технологией Sypher ™, для криптографической обработки на основе программного обеспечения.

Такое решение уменьшает количество активных элементов с потенциально двух или трех десятков, до менее чем полудюжины. Это уменьшает размер и потребление, а также уменьшает сложность соединения между устройствами, что часто является проблемой для отладки.

Благодаря новым техническим решениям, радиостанции достигают беспрецедентных уровней интеграции, причем обработка радиосигналов и их оцифровки сводится к одной или нескольким устройствам. Элементы цифровой обработки сигналов также достигают аналогичных уровней интеграции с возможностью реализации необходимой безопасности с помощью программного обеспечения. Это приводит к масштабируемому подходу с компромиссами в реализации уровней защиты данных и желаемой производительности, применимых к широкому спектру устройств.

Список использованных источников:

14. Duncan Bosworth, Analog Devices Inc., Norwood, Mass. Military Communications and RF Security, August 15, 2017

15. Duncan Bosworth, Analog Devices Inc, Multiband military communications challenges overcome by software-defined radio, October 3, 2014