Сбоеустойчивый микроконтроллер на базе ядра ARM Cortex-M4F

для систем с повышенными требованиями надежности, разработанный ЗАО «ПКК Миландр»

Одним из основных способов обеспечения надежности аппаратуры является применение высококачественной элементной базы. В результате предъявляются новые требования к показателям надежности и элементной базы. В статье рассматривается архитектура нового микроконтроллера, разрабатываемого в ходе ОКР «Обработка-13», и способы повышения таких показателей. Для обеспечения стойкости к факторам космического пространства микроконтроллер выполнен по технологии «кремний-на-изоляторе» с проектными нормами 180 нм. Использование кольцевых транзисторов повышает уровень накопленной дозы до 500 крад. Применение триггеров типа DICE и контрольных сумм ECC (SECDED) для блоков памяти и регистровых файлов способствует снижению интенсивности одиночных сбоев, вызванных, например, ТЗЧ. Схемы аппаратной диагностики ключевых элементов системы «процессор-память», построенные на принципах дублирования в режиме Lock-Step, обеспечивают высокий уровень безопасности. Для улучшения качества ПО, разрабатываемого для данного микроконтроллера, реализованы вспомогательные аппаратные блоки, сокращающие нагрузку с процессорного ядра при выполнении функций диагностики. Благодаря расширенным возможностям отладки ПО проводится качественная его подготовка, в том числе системы диагностики, с учетом программного внесения ошибок. Обширный функционал, наличие различных интересов (UART, SPI, CAN, USB, Ethernet, SpaceWire), мощная аналоговая подсистема (АЦП, ЦАП, встроенные приемопередатчики Ethernet, SpaceWire) и много другое позволяют получить высокие функциональные возможности при обеспечении самых строгих требований надежности.

Сергей ШУМИЛИН
Михаил КАКОУЛИН

Компания ЗАО «ПКК Миландр» является отечественным разработчиком и поставщиком микроэлектронной элементной базы для различных отраслей, начиная от бытовой техники и заканчивая сложными системами ВПК и аэрокосмической отрасли. В настоящее время серийно поставляются различные микросхемы статической памяти, микропроцессоры и микроконтроллеры, интерфейсные схемы и многое другое. Постоянный рост сложности и важности систем, построенных на базе микросхем производства ЗАО «ПКК Миландр», диктует новые требования к надежности, такие как достоверность, сбоеустойчивость, безопасность и т. д. В новой разработке компании реализованы различные механизмы по повышению надежности и обеспечению новых, повышенных требований, предъявляемых потребителями.

Надежность может быть охарактеризована рядом параметров, в частности, безотказностью, готовностью, ремонтопригодностью. В последнее время стали формироваться дополнительные требования к надежности, в том числе безопасность (вероятность возникновения аварийных ситуаций в результате различного рода неисправностей и сбоев) и достоверность (возможность несанкционированной манипуляции критически важной информацией, используемой при работе системы). При этом факторами угрозы надежности могут выступать различные неисправности (сбои), ошибки и отказы. Также учитываются не только факторы, вызванные естественными причинами (тяжелые заряженные частицы, ТЗЧ в космосе, сбои питания, общие отказы элементов системы), но и недочеты в программном обеспечении, конструкции системы и даже ошибочное поведение операторов (человеческий фактор). Современные средства анализа и расчета надежности позволяют провести тщательную проверку новых разрабатываемых систем на предмет качества как функции затраченных средств на обеспечение качества, полученной надежности и допустимых рисков при эксплуатации этой системы. Очевидно, что к микроэлектронной элементной базе, используемой для создания важных систем, тоже предъявляются повышенные требования. Однако здесь должна обеспечиваться и максимальная гибкость в применяемости данных микросхем, чтобы они не стали по-настоящему золотыми для разработчиков аппаратуры. Следует отметить, что предприятия различной направленности зачастую выдвигают противоречащие друг другу требования: например, разработчики авиационной техники заинтересованы в наличии

множества различных интерфейсов связи и, как следствие, большого числа выводов, в то время как для создателей космической техники остро стоит вопрос габаритных размеров и им, наоборот, интересны компактные маловыводные микроконтроллеры. Кроме того, для космической индустрии весьма актуален вопрос устойчивой (пусть и более медленной) работы микросхем в условиях космической радиации и потока тяжелых заряженных частиц, а для разработчиков наземной аппаратуры прежде всего важно создание средств связи, где на первый план выходит высокая производительность.

Анализируя потребности предприятий, выпускающих аппаратуру, в новых микросхемах и новые предъявляемые к ним требования, компания ЗАО «ПКК Миландр» начала разработку универсального 32-разрядного микроконтроллера на базе процессорного ядра ARM Cortex-M4F с повышенными характеристиками надежности и стойкости к специальным факторам космического пространства. Обеспечение стойкости микросхемы к накопленной дозе радиации в космическом пространстве оказывает существенное влияние на ее потребительские свойства в космических системах, но для наземной техники в большинстве случаев абсолютно не требуется соблюдение столь жестких условий, при этом накладываемые ограничения (повышенное потребление и стоимость) зачастую ограничивают ее широкое применение. В результате было принято решение о разработке двух версий микроконтроллера:

- Rad Hard (RH-версия) — радиационно-стойкий МК для космических систем;
- Rad Tolerance (RT-версия) — радиационно-устойчивый МК для авиационных и наземных систем.

Характеристики RT- и RH-версий микросхемы представлены в таблице 1.

Главным различием между версиями микросхемы является разное топологическое исполнение элементов микросхемы. В RH-версии применяются «кольцевые» транзисторы, которые более устойчивы к накопленной дозе, но и занимаемая ими площадь на кристалле больше чем в 2,5 раза. Кроме того, для уменьшения интенсивности сбоев от ТЗЧ все триггеры RH-версии выполнены в виде DICE (специальная дублированная схема триггера). Все это приводит к росту общей площади кристалла и, как следствие, его стоимости. Увеличение размеров кристалла пагубно сказывается и на характеристиках потребляемой энергии. Во всем остальном обе версии кристаллов полностью совместимы и имеют общие механизмы повышения надежности.

Основное отличие новых микросхем состоит в возможности осуществления аппаратной диагностики сбоев при работе. Для этого основные узлы микросхемы, такие как процессорные ядра, контроллеры внутренних блоков памяти, контроллер внешней системной шины и многие другие, дублированы и работают в режиме Lock-Step. Принцип действия режима Lock-Step представлен на рис. 1.

В режиме Lock-Step второе ядро повторяет все действия первого ядра с отставанием на два такта — таким образом при возникновении сбоя в одном из ядер на блоке сравнения будет обнаружено расхождение в их поведении и выработан специальный флаг ошибки. При необходимости оба процессорных ядра могут быть выведены из режима Lock-Step и переведены в режим Dual-Core (рис. 2). В данном

Таблица 1. Основные параметры разрабатываемых микросхем

Параметр	Описание
Процессорное ядро	2 ядра ARM Cortex-M4F: – режим Lock-Step – режим Dual Core
Тактовая частота	До 100 МГц
Напряжение питания	3–5,5 В
Корпус	До 240 выводов, планарный металлокерамический
Память программ	Однократно программируемая (antifuse) 128 кбайт (SECDED) Статическая память 128 кбайт (SECDED)
Память данных	Статическая память 64 кбайт (SECDED)
Производительность	2,1 CoreMark/МГц в Lock-Step 4 CoreMark/МГц в Dual-Core
Контроллер Ethernet	2×MAC 10/100 Мбит/с 2×PHY 10 Мбит
Контроллер SpaceWire	2×MAC 2×PHY
Внешняя системная шина	8/16/32/64 бита, с различными возможностями организации ECC
Интерфейс UART	4 штуки
Интерфейс SPI	4 штуки
Интерфейс CAN	5 штук
Блок таймеров	6 штук 32-разрядных таймеров с 4 каналами ШИМ/регистрации
Контроллер DMA	2 штуки, 32 физических канала, 96 виртуальных каналов
Контроллер МКПД	2 штуки, согласно ГОСТ 52070-2003
Контроллер ARINC	16 приемников, 8 передатчиков, согласно ГОСТ 18977-79
Интерфейс USB	Device и Host до 12 Мбит/с
Блок вычисления ECC	До 64 бит данных, по программируемой матрице
Блок вычисления CRC	С произвольным полиномом со степенью от 4 до 64
Блок шифрации	По ГОСТ 28147-89
АЦП	2 штуки с разрядностью 12 бит, до 16 внешних каналов
ЦАП	2 штуки с разрядностью 12 бит
Число выводов	До 160 выводов общего назначения
Технология	180 нм, кремний-на-изоляторе
Накопленная доза*	RH-версия до 500 крад (Si) RT-версия до 100 крад (Si)
Устойчивость к сбоям*	Иммунитет к тиристорному эффекту SEL LET_{SEL} > 120 МэВ·см^2/мг Порог одиночных сбоев от ТЗЧ: – RH-версия — LET_{SEU} > 20 МэВ·см^2/мг – RT-версия — LET_{SEU} > 2 МэВ·см^2/мг Сечение насыщения одиночных сбоев от ТЗЧ: – RH-версия — 10^{-9} см^2/бит – RT-версия — 10^{-6} см^2/бит

Примечание. * Предварительные данные, будут уточнены в ходе испытаний.

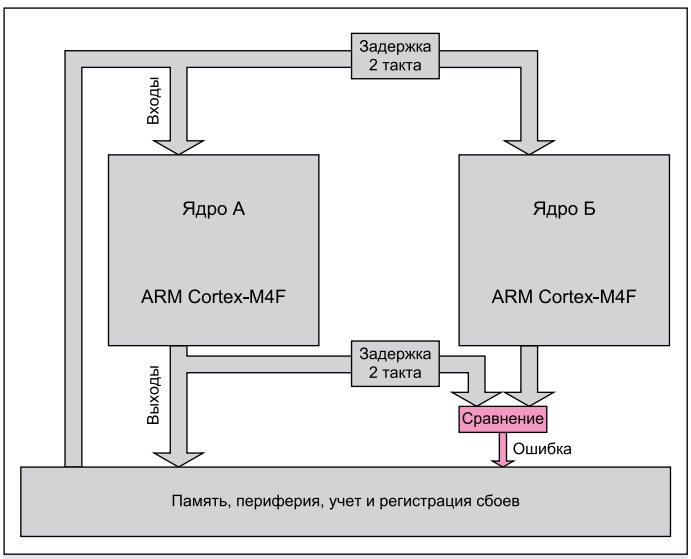

Рис. 1. Организация режима Lock-Step

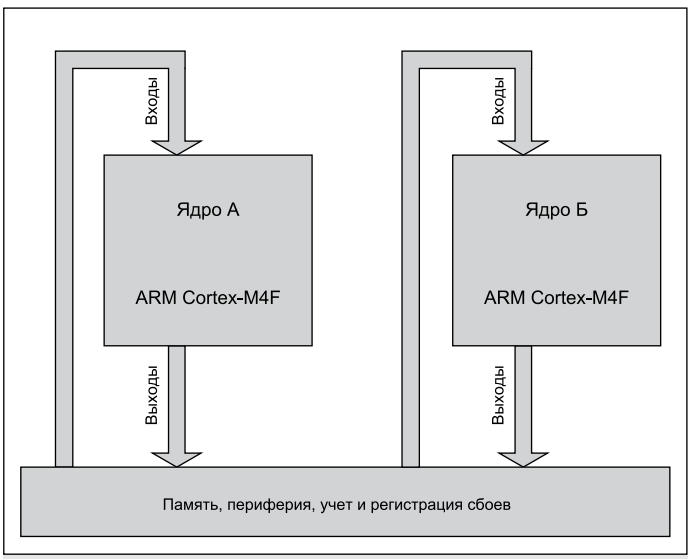

Рис. 2. Организация режима Dual-Core

режиме ядра способны выполнять полностью независимые задачи, обеспечивая увеличение производительности. Следующий метод повышения устойчивости к сбоям — применение корректирующих кодов (ECC) в памяти, позволяющих исправлять одиночные и обнаруживать двойные ошибки (SECDEC). Также с помощью ECC, кодов защищены основные настройки микросхемы. Кроме того, благодаря ECC-кодам имеют защиту и внутренние системные шины, но в отличие от памяти они позволяют лишь обнаруживать ошибки. Некоторые элементы микросхемы, такие как сторожевые таймеры, счетчики часов реального времени, счетчик отложенного сброса и другие, выполнены в виде троированной схемы с мажоритарным элементом. Таким образом обеспечивается высокая степень аппаратной диагностики и исправления различных сбоев. Также в микросхеме реализованы различные аналоговые блоки диагностики уровней напряжения питания, качества сигналов тактирования и многое другое. Но, к сожалению, обеспечение аппаратных методов диагностики для всех узлов микросхемы невозможно. И для периферийных блоков основная роль в обнаружении и исправлении сбоев ложится на программное обеспечение. Для облегчения работы программного обеспечения по повышению надежности в микросхеме реализовано и несколько вспомогательных блоков. В первую очередь это блок управления сбоями (FT_CNTR), в котором обрабатываются все сигналы ошибок микросхемы, в зависимости от критичности ошибки в данном блоке может быть настроена различная реакция на эти события, начиная от аппаратного сброса и заканчивая минимальной программной обработкой для набора статистики или игнорированием. Характеристики блоков поддержки программного обеспечения сбоеустойчивости приведены в таблице 2.

Важный элемент повышения надежности программного обеспечения — легкая и всесторонняя отладка ПО на этапе разработки. Средства отладки микросхемы позволяют выполнять пошаговое исполнение, отображение внутренних ресурсов микросхемы, трассировку выполнения ПО в реальном масштабе времени и многое другое. Кроме того, в микросхеме присутствуют специальные механизмы программного внесения ошибок, предназначенные для отладки подсистемы диагностики сбоев.

Таблица 2. Блоки поддержки программной диагностики сбоев

Блок	Описание
FT_CNTR	Блок фиксации флагов сбоев и ошибок в микросхеме, позволяет настроить различную реакцию на те или иные события, от сброса до игнорирования
MPU	Блок защиты памяти, позволяет ограничить адресное пространство и права доступа для подзадач и обеспечивает защиту памяти других задач при сбое в одной из них
SCR_CNTR	Блок «чистильщик» памяти, позволяет в фоновом режиме без участия процессора осуществлять чтение массивов памяти для ускорения обнаружения ошибок по ECC-сумме
CRC_CNTR	Блок аппаратного вычисления CRC-сумм с произвольным полиномом со степенью от 4 до 64, позволяет обеспечить защиту от сбоев передаваемых массивов информации
ECC_CNTR	Блок аппаратного вычисления ECC-сумм по произвольной матрице до 64 бит, позволяет обеспечить защиту от сбоев хранимой информации
COST_CNTR	Блок аппаратной поддержки шифрования согласно ГОСТ 28147-89, позволяет осуществить криптографическую защиту информации

Реализация всех этих элементов, аппаратная и программная диагностики, широкие функциональные возможности и высокая производительность позволяют обеспечить как классические параметры надежности, так и новые (безопасность и достоверность), и значительно повысить качество новой аппаратуры.

В настоящее время микросхемы находятся на стадии изготовления экспериментальных образцов, но для заинтересованных потребителей имеется возможность протестировать FPGA-макет проекта. Доступ к макету осуществляется через сеть Интернет. На макете можно оценить общие показатели производительности и качество средств разработки ПО.

Образцы микросхем будут доступны в начале 2014 года, окончание ОКР и серийные поставки намечены на 2015 год.