Ключевые особенности ПЛИС для взаимосвязанного мира

Пауль ПИКЛЕ (Paul PICKLE)

Программируемые логические интегральные схемы (ПЛИС, Field Programmable Gate Array — FPGA) совершенствуются и все больше удовлетворяют требованиям разработчиков, но до сих пор существуют актуальные проблемы, касающиеся вопросов безопасности, энергопотребления и надежности.

Новые идеи и разработки, новые продукты и приложения непрерывно меняют все грани нашей повседневной жизни. Наш взаимосвязанный мир постоянно определяет новые способы общения, коллективного взаимодействия, сотрудничества и обмена информацией. Пока новаторские подходы порождают очередные парадигмы, появляется множество новых бизнес-возможностей с огромным потенциалом.

Как показывает практика, каждый последующий виток технологического прогресса не только открывает другие возможности, но и создает ряд острых проблем технологического и инфраструктурного характера. Защита интеллектуальной собственности, безопасность, киберпреступность, защита окружающей среды и надежность — лишь небольшая часть тех сложных вопросов, которые стоят перед компаниями, работающими в сфере информационных технологий.

Компании, проектирующие изделия для взаимосвязанного мира, обычно опираются на одну из трех фундаментальных методологий разработки устройств с высокой степенью интеграции для реализации требуемой функциональности в одном или более устройствах:

- Стандартная часть специализированной ИС (Application specific standard products — ASSP) часто является идеальным решением для новой разработки. Однако инженеры не всегда могут найти такую ИС, которая могла бы охватить все необходимые функции целевого устройства. Также компании, создающие последние ASSP, больше всего заинтересованы в крупномасштабных приложениях из-за крайне высокой стоимости разработки. Это лишает множество проектов доступных ASSP-решений.
- ИС специального назначения (Application specific integrated circuit — ASIC) считались отличным вариантом для компаний, которым необходимо интегрировать множество функций в один кристалл. При общей миниатюризации устройств проблемы, связанные с использованием ASIC, такие как время полного цикла разработки и непомерно большая общая стоимость (включая средства САПР), вынуждают специалистов отказываться от применения ASIC и искать иные пути создания сложных устройств.
- За минувшие два десятилетия ПЛИС прошли долгий путь; активно совершенствовались такие характеристики, как возможности интеграции и ввода/вывода, объем, встроенные функции, память, встроенные процессоры и математические блоки. ПЛИС, бесспорно, являются самым быстрым способом разработки цифровых устройств с интеграцией на одном кристалле, хотя традиционно и стоят дороже, чем ASSP и ASIC, но они предоставляют пользователю огромные возможности для поддержки и упрощения перепрограммирования в процессе функционирования, гибкости разрабатываемого устройства и ускорения выпуска готового продукта. Сегодня ПЛИС предоставляют превосходные возможности для системных инженеров, а в перспективе значительно сократят издержки дальнейших поколений разработок.

Технологические компании, проектирующие новые изделия, часто выбирают средства ПЛИС для решения сложных задач в условиях строгих ограничений. Это значительный шаг вперед и огромное преимущество для тех, кто занимается созданием сложных изделий на основе ПЛИС. Текущие предложения основных поставщиков ПЛИС отличаются превосходными инновационными решениями с расширенными встроенными функциями, такими как математические блоки, высокоскоростные последовательные интерфейсы, различные процессорные ядра и решения для цифровой обработки сигналов, когда-то доступные только в ASIC-решениях.

Прогнозы по рынку ПЛИС показывают, что системные инженеры, которые разрабатывают сложные устройства для взаимо-связанного мира, все так же будут нуждаться в уникальных встроенных функциях и различных возможностях, необходимых для новых приложений в сферах связи, промышленности, медицины и обороны. Такие системы должны обладать большей безопасностью, меньшим суммарным энергопотреблением, высоким уровнем надежности и системной интеграцией, зависящей от приложения и предназначенной для конечного пользователя.

Вот почему поставщик ПЛИС, который может предложить средства безопасности, низкое энергопотребление, надежность и высокий уровень интеграции в пределах одного устройства, предоставляет наилучшее решение для системного инженера. Безопасность, низкое энергопотребление, высокая надежность и системная интеграция — ключевые особенности, позволяющие создать действительно незаменимое устройство для конечного потребителя.

Безопасность

Сегодня сложные проекты для ПЛИС содержат множество встроенных решений, являющихся интеллектуальной собственностью (Intellectual Property, IP) их владельцев, а потому достаточно остро стоит вопрос защиты ПЛИС от обратного инжиниринга (Reverse engineering), клонирования и несанкционированного доступа. Также ПЛИС должна стать доверенным модулем (Root-of-trust, RoT) в сложных системах.

Большой шаг вперед в области безопасности ПЛИС — наделение базового уровня безопасности простым интерфейсом и возможностью адаптации. Идеальное решение — предоставить ПЛИС со встроенной системой безопасности, выполненной по передовой технологии и функционирующей независимо.

Одна из проблем с ПЛИС, выполненных по SRAM-технологии, — необходимость конфигурировать ее каждый раз после очередной подачи питания, что делает конфигурацию ПЛИС крайне уязвимой к обратному инжинирингу. В том случае если конфигурационная информация хранится во внутренней энергонезависимой памяти, ее невозможно считать, а значит, таким образом удается предотвратить обратный инжиниринг и преднамеренное искажение конфигурации злоумышленниками. В нынешних поколениях ПЛИС предусмотрены средства защиты

исключительно для конфигурации системы, однако для полной безопасности в процессе функционирования необходимо защитить и прикладные данные.

Функции защиты данных в новых приложениях в мире, где доступ к сети имеет практически каждое устройство, содержат:

- Аппаратную защиту от дифференциального анализа потребляемой мощности (differential power analysis, DPA).
- Недетерминированный генератор случайных последовательностей (Non-deterministic random bit (number) generator, NRBG).
- Аппаратные межсетевые экраны для защиты интегрированного процессора ARM Cortex-M3.

Низкое энергопотребление

В последние два десятилетия самые продвинутые процессоры и микроконтроллеры, как правило, имели различные режимы энергосбережения. Делалось это для того, чтобы решить проблему высокого потребления энергии, вызванную возрастающей тактовой частотой и высокой степенью интеграции. Только наиболее прогрессивные ПЛИС были спроектированы таким образом, чтобы предоставить разработчику подобные средства сокращения потребления для устройств, работающих на более высоких частотах. Сейчас разработчики впервые имеют возможность использовать режимы низкого энергопотребления, реализованные в ПЛИС по технологии энергонезависимой памяти.

Высокая надежность

Разработка и исполнение систем специального назначения ведутся в соответствии со строгими регламентами, которые существуют в различных областях применения. Так, множество систем, предназначенных для военного и аэрокосмического использования, создано согласно требованиям по таким параметрам, как размер, вес, потребляемая мощность (Size Weight and Power, SWaP), а также срок службы изделия. Ведь военные системы должны функционировать безупречно, в том числе и после долгого времени простоя. К системам же, предназначенным для других сфер деятельности, предъявляются и иные требования: в частности, промышленные системы должны отвечать высоким стандартам безопасности, а необходимость в наивысшей надежности всегда была приоритетом в медицинской промышленности.

Проблемы надежности ПЛИС чаще всего относятся к одиночным сбоям (Single event upset, SEU), при которых изменяется содержимое конфигурационной SRAM-памяти. Поскольку эта память отвечает за конфигурацию устройства, любое ее изменение может вызвать ошибку. Это обстоятельство в значительной степени игнорируется или даже скрывается от покупателей поставщиками ПЛИС, выполненных по SRAM-технологии.

Flash ПЛИС устойчивы к SEU, таким образом, предотвращается возможность искажения конфигурации и исключается наиболее частая причина отказа системы. Также нет необходимости в применении специальных подходов к уменьшению влияния SEU, которые вынуждены применять специалисты, работающие с SRAM ПЛИС.

Системная интеграция

Интеграция встроенного процессорного ядра исключает необходимость использования софт-процессора в матрице ПЛИС и сводит на нет все трудности, связанные с этим подходом. Таким же образом встроенные периферийные модули и такие подсистемы, как контроллеры памяти, аналоговые блоки, математические блоки и высокоскоростные средства ввода/вывода, исключают применение в системе лишних компонентов. Используя ПЛИС, выполненную по флэш-технологии, разработчику не понадобится хранить конфигурацию во внешней памяти. Интеграция ПЛИС с такими компонентами, как память, микропроцессоры и интерфейсы DDR, уменьшает количество компонентов и увеличивает надежность системы в целом.

Будущее

В течение следующего десятилетия основные достижения и ключевые особенности в технологиях ПЛИС станут решающими факторами в обеспечении жизнеспособности проектов, которые служат взаимосвязанному миру.