УДК 004.2

ПЕРСПЕКТИВЫ РАЗРАБОТКИ СВЕРХБОЛЬШИХ ИНТЕГРАЛЬНЫХ СХЕМ УПРАВЛЕНИЯ ПЛАТФОРМОЙ С ПОДДЕРЖКОЙ СТАНДАРТА OPEN BMC

Тарасов И.Е.

«МИРЭА - Российский технологический университет», 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: tarasov_i@mirea.ru

В статье рассматривается перспективная архитектура специализированной сверх большой интегральной схемы (СБИС), предназначенной для реализации функций интеллектуального интерфейса управления вычислительной платформой. Актуальность разработки такой элементной базой обусловлена ростом парка вычислительной техники, в том числе серверов, центров обработки данных и подобных высокопроизводительных платформ. Мониторинг таких параметров, как напряжение питания, потребляемый ток, параметры системы охлаждения, состояние системных интерфейсов и подобных им, имеет существенную значимость с точки зрения процесса эксплуатации. В настоящее время СБИС, решающие эти задачи, относятся к типу Baseboard Management Controller (BMC) и представляют собой системы на базе процессора с набором периферийных контроллеров. Доступ таких СБИС к критически важным параметрам вычислительной системы требует реализации комплекса мер защиты от несанкционированного доступа с использованием недокументированных возможностей BMC зарубежного производства. В статье рассматриваются подсистемы СБИС управления платформой, предлагается реализация процессорной подсистемы для управления некоторыми параметрами, а также рассматриваются перспективы обеспечения поддержки библиотеки Open BMC.

Ключевые слова: процессор, микроконтроллер, система на кристалле, платформа, аппаратная архитектура.

PROSPECTS FOR DEVELOPING INTELLECTUAL PLATFORM MANAGEMENT VLSI SUPPORTING THE OPEN BMC STANDARD

Tarasov I. E.

«MIREA - Russian Technological University», 119454, Moscow, 78 Vernadskogo Avenue, Russia, e-mail: tarasov_i@mirea.ru

The article discusses a perspective architecture of a specialized VLSI for implementing the functions of an intelligent interface for managing a computing platform. The relevance of developing such an element base is due to the growth of the computer equipment fleet, including servers, data processing centers and similar high-performance platforms. Monitoring parameters such as supply voltage, current consumption, cooling system parameters, the status of system interfaces and the like is of significant importance from the point of view of the operation process. Currently, VLSI that solve these problems are of the Baseboard Management Controller (BMC) type and are processor-based systems with a set of peripheral controllers. The access of such VLSI to the critical parameters of the computer system requires the implementation of a set of measures to protect against unauthorized access using undocumented capabilities of foreign-made BMC. The article discusses platform management VLSI subsystems, proposes the implementation of a processor subsystem to control some parameters, and also considers the way for providing support for the Open BMC library.

Keywords: processor, microcontroller, system on chip, co-optimization, hardware architecture.

Введение

Усложнение современных вычислительных систем на базе высокопроизводительных многоядерных процессоров сопровождается интеграцией в такие системы большого количества сложных компонентов, выполняющих вспомогательные задачи. В частности, совместно с центральным процессором используются графические процессоры, системные контроллеры («наборы системной логики»), микросхемы динамической памяти и т.д. Для таких систем необходима реализация устройств мониторинга, включающих в себя как контроль предельно допустимых значений отдельных параметров (напряжения питания, потребляемого тока, температуры), так и мониторинг состояния системы с обеспечением интерфейсов удаленного управления. В настоящее время эти функции реализуются в составе СБИС «интеллектуального интерфейса управления платформой» (Intellectual Platform Management Interface), которая представляет собой систему на кристалле на базе процессора общего назначения, имеющего собственную подсистему памяти, цифровые интерфейсы для сопряжения с устройствами системной платы, а также аналоговые и цифровые периферийные модули для

контроля предельно допустимых значений критических параметров и управления исполнительными устройствами (вентиляторами и помпами системы охлаждения, системами сигнализации и аварийного отключения питания и т.д.). Распространенной программной библиотекой является Open BMC, используемая, в частности, корпорацией IBM [1].

Примерами СБИС систем мониторинга являются процессоры ASpeedTech AST2500 и AST2600 [2, 3]. Они основаны на процессорных ядрах ARM Cortex-A, причем в более современном процессоре AST2600 дополнительно присутствует вспомогательное процессорное ядро микроконтроллерного класса ARM Cortex-M. Также процессоры имеют собственную память DDR3, интерфейс PCI Express и автономный контроллер дисплея VGA с реализацией функций двумерной графики.

Необходимость использования зарубежной компонентной базы создает ряд угроз, как с точки зрения нарушения поставок, так и возникновения непосредственных угроз безопасности данных и физической целостности вычислительной техники, в составе которых находятся СБИС, имеющие доступ к функциям управления электропитанием, охлаждением, а также способные осуществлять удаленный доступ к данным. Следовательно, замена таких СБИС аналогичными изделиями российской разработки является важной задачей, решение которой снижает риски в области информационной безопасности, способствует повышению надежности вычислительной техники и ее устойчивости к внешним воздействиям, направленным на нарушение нормальной работы и разрушение оборудования путем манипулирования параметрами, к которым имеет доступ СБИС управления платформой.

Архитектура СБИС управления платформой

Ввиду того, что в составе применяемых в настоящее время СБИС присутствуют разнородные по сложности системы (процессорные ядра, сложнофункциональные блоки, простые цифровые интерфейсы), для эффективного импортозамещения необходимо выделить подсистемы, которые при низких технических рисках разработки способны обеспечить управление процессами, имеющими критическое значение для функционирования вычислительной платформы.

Предлагается реализация подсистемы внешнего управления (Out-Of Band Management) на основе гетерогенной подсистемы специализированных управляющих процессоров. Основанием для такого решения являются следующие факторы:

1. Концентрация функций в одном процессорном ядре усложняет разработку программного обеспечения, создавая единственную точку уязвимости; кроме того, при наличии множества независимых процессов в контролируемых устройствах возможно возникновение ситуаций, когда единственное процессорное ядро будет объективно не в состоянии обеспечить своевременное обслуживание одновременно возникающих запросов. Вместе с тем, более простые задачи не требуют использования сложного процессорного ядра, и реализации симметричной многопроцессорной системы. Косвенным подтверждением необходимости введения вспомогательных процессорных ядер является добавление ядра ARM Cortex-M к основному ядру ARM Cortex-A при переходе от AST2500 к AST2600.

2. Положительный опыт реализации системы мониторинга параметров и управления подсистемой охлаждения способствует снижению рисков разработки оригинальной процессорной подсистемы измерений и мониторинга. В рамках выполнения работ по созданию контроллера вентиляторов и измерения скорости их вращения была подтверждена возможность автономной работы подобной системы и ее положительное влияние на эксплуатационные характеристики вычислительной платформы [4, 5].

3. Базовые функции управления, такие как измерение напряжения питания, температуры, скорости вращения вентиляторов, могут быть реализованы на базе относительно простых процессорных ядер, однако способствуют существенному снижению рисков выхода из строя вычислительной платформы.

Таким образом, датчики контроля электропитания, температуры и скорости вращения вентиляторов целесообразно подключить к специализированным процессорным ядрам микроконтроллерного класса, которые могли бы работать автономно в составе СБИС, обеспечивая базовые функции контроля без необходимости выполнять запуск всей вычислительной подсистемы СБИС, в составе которой может присутствовать процессорное ядро уровня ARM или RISC-V. В то же время, при реализации функций управления в соответствии со стандартом Open BMC возможности специализированного процессора окажутся недостаточными. Поэтому центральный процессор, роль которого может играть лицензируемое IP-ядро, поддержанное библиотекой Open BMC, также должен иметь доступ к периферийным контроллерам. Параметры этого доступа и условия его предоставления могут контролироваться отдельными инструментами, вплоть до физической блокировки доступа со стороны центрального процессора, если требования информационной безопасности не могут быть гарантированно выполнены. Взаимодействие процессорных подсистем и периферийных контроллеров в составе СБИС управления платформой показано на рис. 1.

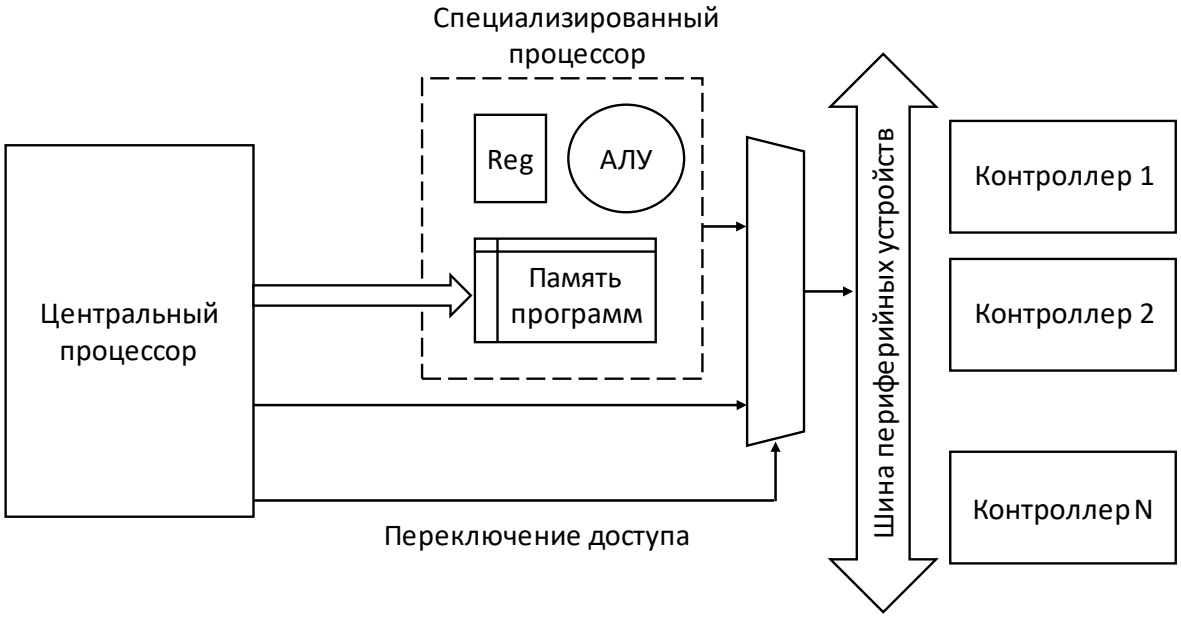

Рис.1. Взаимодействие процессорных подсистем и периферийных контроллеров в составе СБИС управления платформой

В представленной системе центральный процессор имеет возможность динамического обновления программного обеспечения специализированного процессора. Таким образом, управление периферийными устройствами может выполняться как централизованно, так и автономно, с возможностью изменения алгоритмов. Такой подход расширяет возможности программного обеспечения, упрощая требования к аппаратной составляющей СБИС и позволяя сконцентрироваться на реализации относительно несложной подсистемы специализированного процессора.

Архитектура специализированных процессоров и алгоритмы управления периферийными устройствами мониторинга

В процессе работы вычислительной платформы ряд параметров, такие как напряжение питания, потребляемый ток и температура, являются критически важными для физической целостности оборудования. Выход этих параметров за допустимые пределы требует немедленной реакции соответствующих аппаратных систем защиты. Также может оказаться полезным дублирование функций контроля, в том числе отслеживание приближения к критическим значениям работы при определенных режимах эксплуатации. Можно отметить подход комбинированного управления, известный из теории систем автоматического управления, который основан на упреждающем изменении параметров работы исполнительных устройств, основанном не на сигнале обратной связи, а на входном сигнале. Применительно к управлению платформой такой подход может быть использован для увеличения оборотов вентилятора системы охлаждения, если произведен запуск программного обеспечения, которое в ближайшее время приведет к повышению температуры компонентов системы. Упреждающее включение системы охлаждения будет в данном случае способствовать предупреждению перерегулирования температуры.

Приведенный сценарий работы является примером, обуславливающим необходимость подключения к специализированному процессорному ядру различных периферийных контроллеров, а также обеспечение автономной работы такого ядра с относительно небольшим объемом программного кода. Пример подключения периферийных устройств мониторинга критических параметров платформы к специализированным процессорным ядрам показан на рис. 2.

Система мониторинга может быть дополнена устройствами, специфичными для области применения или отрасли. Например, датчики нарушения целостности корпуса, контроллеры активности цифровых интерфейсов и передаваемых коммуникационных пакетов могут быть также интегрированы в СБИС в качестве периферийных устройств специализированных процессорных ядер.

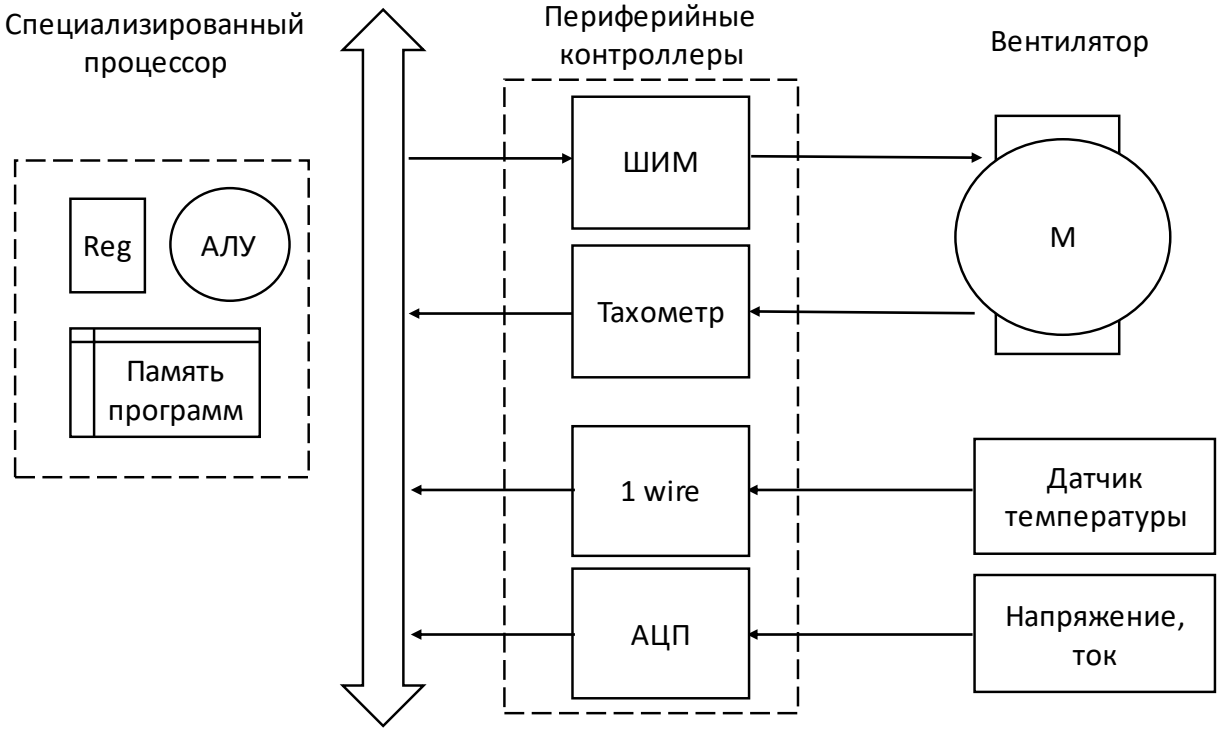

Рис.2. Подключение периферийных устройств мониторинга критических параметров платформы к специализированным процессорным ядрам

Сочетание набора периферийных устройств, специализированных процессорных ядер и подсистемы центрального процессора позволяют обеспечить базовые возможности мониторинга и управления на базе только вновь разрабатываемых специализированных ядер. При этом адаптация к стандарту Open BMC может быть проведена впоследствии, предположительно без коррекции аппаратной составляющей СБИС.

Заключение

Рассмотренная архитектура СБИС предназначена для реализации импортозамещающей компонентной базы, которая играет вспомогательную роль в вычислительных платформах, однако в силу сложности алгоритмов реализуется в настоящее время на базе высокопроизводительных процессорных ядер, что усложняет процесс замены микросхем данного класса. Предложенный в статье подход к разработке СБИС предполагает раннюю реализацию базовых функций мониторинга и управления с последующей адаптацией к промышленным стандартам, в том числе распространенной библиотеке Open BMC.

Список литературы

1. https://www.ibm.com/docs/ru/power10/7063-CR2?topic=cr2-managing-system-by-using-openbmc-tool (дата обращения 12.04.2023)
2. https://www.aspeedtech.com/server_ast2500/ (дата обращения 12.04.2023)
3. https://www.aspeedtech.com/server_ast2600/ (дата обращения 12.04.2023)
4. Тарасов И.Е., Потехин Д.С., Хренов М.А., Советов П.Н. Автоматизация проектирования многопроцессорной системы на базе ПЛИС для управления во встраиваемых приложениях // Экономика и менеджмент систем управления, 2017, №3.1(25) с. 179 — 184.
5. П. Н. Советов, И. Е. Тарасов Разработка многопоточного софт-процессора со стековой архитектурой на основе совместной оптимизации программной модели и системной архитектуры // Многоядерные процессоры, параллельное программирование, ПЛИС, системы обработки сигналов. – 2017. – Т. 1, № 7. – С. 8-19.

References

1. https://www.ibm.com/docs/ru/power10/7063-CR2?topic=cr2-managing-system-by-using-openbmc-tool (access date 12.04.2023)

2. https://www.aspeedtech.com/server_ast2500/ (access date 12.04.2023)
3. https://www.aspeedtech.com/server_ast2600/ (access date 12.04.2023)
4. Tarasov I.E., Potekhin D.S., Khrenov M.A., Sovetov P.N. Automation of the design of a multiprocessor system based on FPGA for control in embedded applications // Economics and Management of Control Systems, 2017, No. 3.1(25) p. 179 - 184.
5. P. N. Sovetov, I. E. Tarasov Development of a multi-threaded soft processor with a stack architecture based on joint optimization of the software model and system architecture // Multicore processors, parallel programming, FPGAs, signal processing systems. - 2017. - V. 1, No. 7. - S. 8-19.