УДК 621.03

Ю. Б. ЮРЧЕНКО

НПП Хартрон-АРКОС, Украина

МЕТОДЫ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ ВСТРОЕННЫХ СИСТЕМ НА ОДНОКРИСТАЛЬНЫХ МИКРОКОМПЬЮТЕРАХ

Проведена оценка реализуемости заданных требований к вычислительной системе в рамках доступных аппаратных средств. Проанализированы пути оптимизации архитектур на базе применения параллельных систем при синтезе резервированных комплексов для особо тяжелых условий эксплуатации с длительным сроком активного функционирования. Обоснована целесообразность и проанализирована эффективность применения аппаратурной синхронизации для контроля в резервированных структурах вычислительных систем.

Ключевые слова: *встроенная система, отказоустойчивость, реконфигурируемая архитектура, уровень целостности.*

Введение

Одним из требований к системам управления (СУ) аэрокосмического назначения является обеспечение истинности функционирования в течение заданного периода времени управления. Оценка [1] истинности функционирования в СУ критичного применения возлагается на контролирующую систему (рис. 1а.), обычно включающую в себя программный и аппаратный уровень обеспечения (рис.1б.).

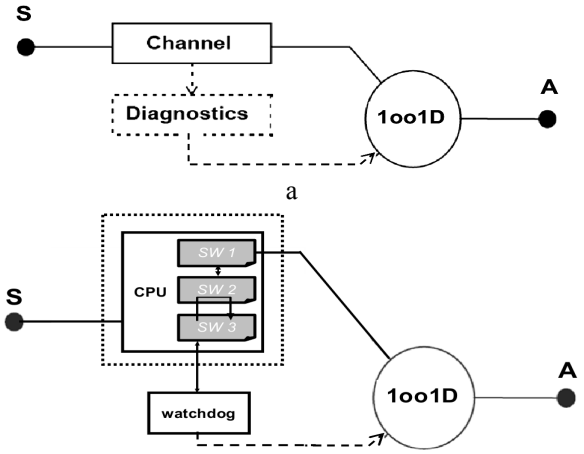

Рис. 1. Способы контроля состояния одноканальных систем

В функции контролирующей системы должны быть включены обнаружение факта отказа, его локализация и парирующее действие. Среди множества методов поддержания безотказного функционирования (рис. 2.) для построения системы под конкретные задачи немаловажным является требование обеспечения непрерывности процесса управления в течение некоторого периода времени, являющегося особо критичным, несмотря на возникающие отказы.

Такие периоды функционирования в управляющих системах существуют, как при обеспечении аварийной защиты и недопущении лавинообразного развития событий с перерастанием в катастрофические последствия, так и при обеспечении планового завершения активного на данный период процесса. В частности, задача планового ведения процесса съемки характерна для СУ космических аппаратов (КА) зондирования Земли, при котором задействованы все системы спутника.

Цель – определить направления аппаратно-архитектурного построения системы управления и соответствующего выбора процессорных элементов для бортовых вычислительных комплексов перспективных КА.

Повышение скорости определения отказа

Анализ тенденций построения КА такого назначения показывает [2], что вне зависимости от класса спутника, аппаратура СУ представляет собой распределенную структуру оборудования с множеством периферийных процессоров, предназначенных для локального управления аппаратными средствами (рис. 3) при сохранении общей тенденции дублированной структуры аппаратуры КА. Поскольку периферийные контроллеры структурно одноканальные, то при таком подходе к построению СУ функционирование периферийного оборудования должно быть контролируемо центральным процессором.

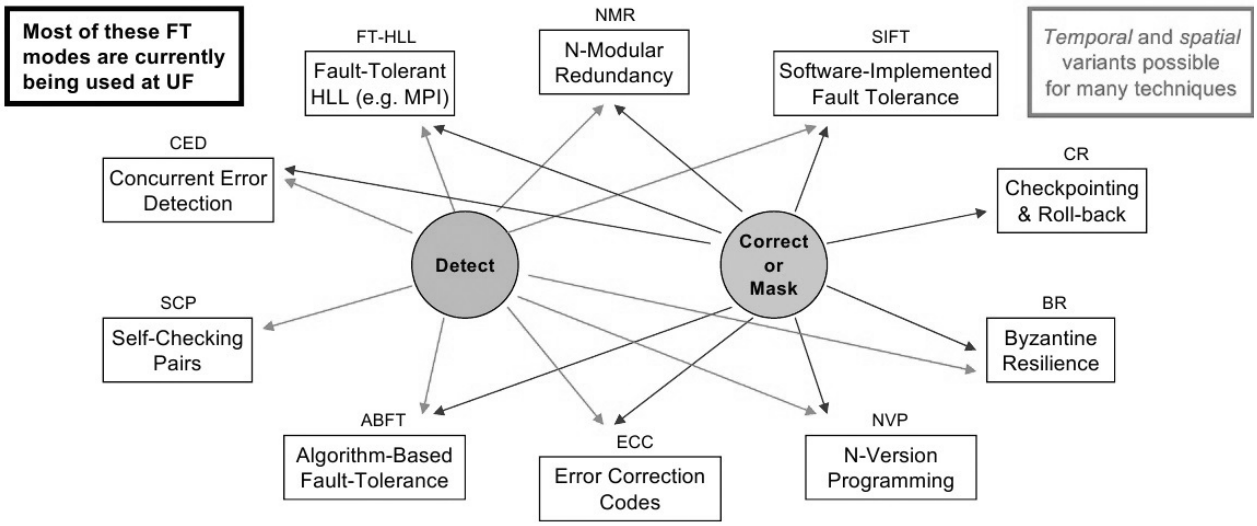

Рис. 2. Методы поддержания безотказного функционирования

При возникающих отказах в периферийных контроллерах для поддержания процесса без потери исполняемой функции время локализации дефектов должно быть достаточно малым, чтобы канал отказавшего оборудования безударно вывести из эксплуатации и оперативно включить резервный канал с параметрами данных на момент фиксации отказа. Таким образом, при построении канала периферийного оборудования необходимо вводить, как минимум, аппарат контроля [3].

Применение «faultRobust» технологии особенно эффективно для SoC- кристаллов [4] (рис. 4), поскольку есть необходимость и основную системную шину, и шину контроля, и память, и оборудование ввода-вывода, и аппарат «faultRobust» располагать только внутри кристалла. Данная технология предусматривает применение или очень емких кристаллов, или гибридных сэндвичей типа «процессор-на-памяти».

Взяв за основу структуру процессора «Delta-4» [5] корпорация ARM для контроллерных ядер разработала отказоопределяющую архитектуру [6], введя аппаратное сравнение внутренних сигналов функционирования двух идентичных ядер процессоров с регистрацией несовпадения информации в том или ином оборудовании. При воздействии суммарно на кристалл того или иного фактора в определенный момент времени, вероятность того, что сбой будет вызван в функционировании однотипного оборудования высока. Поэтому, для определения факта сбоя произошедшего в определенный момент контролирующее оборудование должно выполнять идентичную функцию со сдвигом во времени.

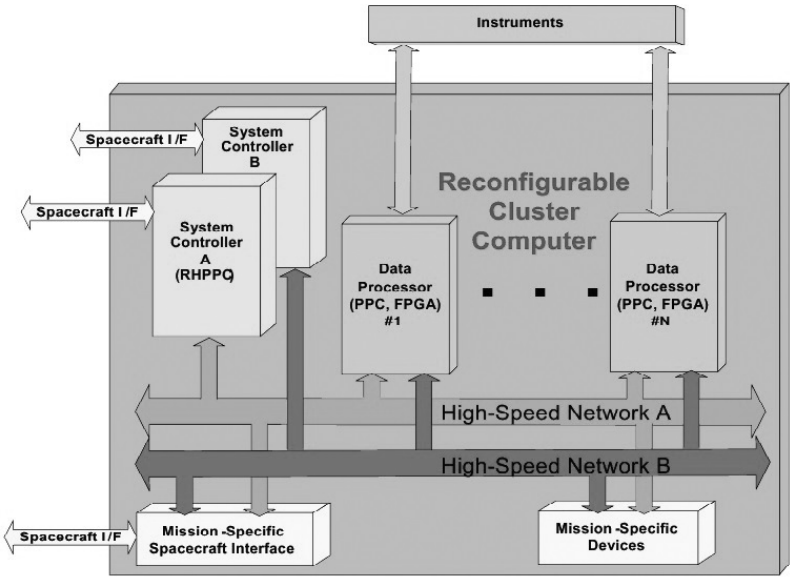

Рис. 3. Структура бортовых вычислительных комплексов КА

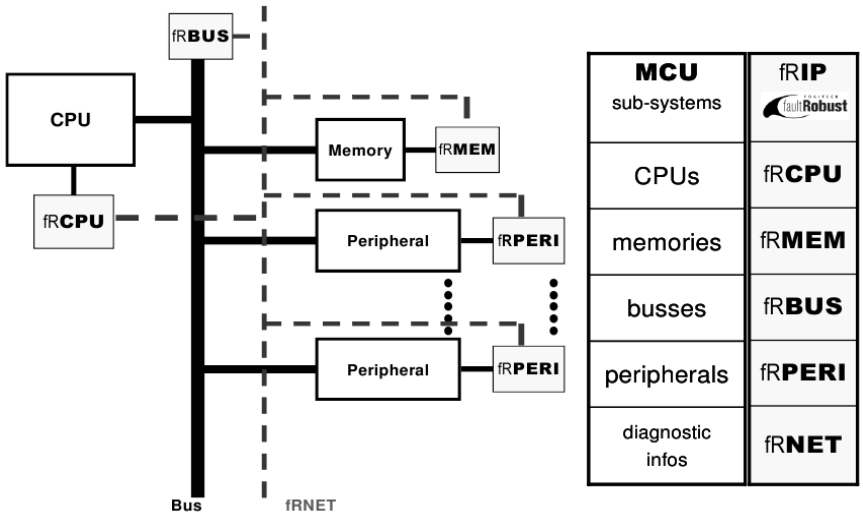

Рис. 4. Применение «faultRobust» технологии

Функционирование процессоров в таких системах должно быть аппаратно жестко связано по временным соотношениям, а временной сдвиг больше, чем длительность времени воздействия. Предложенный корпорацией Texas Instruments [7] временной сдвиг соответствует, в среднем, выполнению двух команд RISC процессора (рис. 5). Архитектура такого типа позволяет эффективно вести мониторинг узла собственными средствами.

Повышение скорости парирования отказов

Однако, при наличии зафиксированных сбоев отсутствует гарантия в достоверности информации, обрабатываемой данным контроллером и, как следствие, обычно предлагается для продолжения функционирования с подтверждением истинности решения о введении дополнительного канала «горячего» резервирования. При этом не рассматривается случай того, что резервный канал идентичного оборудования, который функционирует параллельно, также подвергается риску сбоя за время воздействий. Причем сбой будет зафиксирован вне зависимости от того, где он произошел в master или checker оборудовании основного или резервного каналов. Таким образом, есть вероятность получения результата фиксации сбоев в обоих каналах резервирования, что не обеспечит дальнейшего выполнения программы функционирования с подтверждением гарантии истинности. В итоге, применяемая архитектура, фактически являющаяся четырехканальной, обладает только свойством быстрой фиксации сбоев, в отличие от также четырехканальной, но с византийским алгоритмом обеспечения отказоустойчивости [8], которая гарантирует истинность продолжения функционирования.

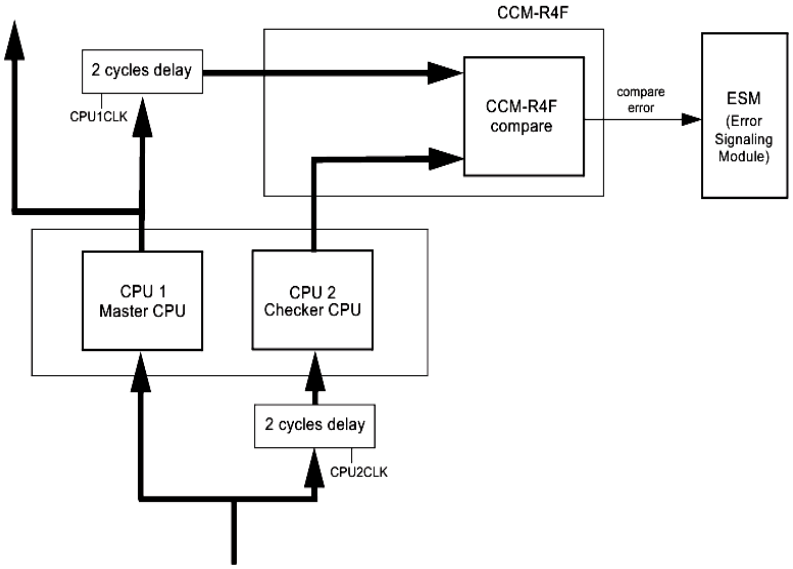

Рис. 5. Практическое применение «faultRobust» технологии

Следовательно, ни применение процессоров «faultRobust» технологии определения ошибок, ни наращивание канальности этих процессоров, при требовании ведения непрерывного вычислительного процесса с гарантией истинности в течение заданного времени нецелесообразно. При возникновении ошибки в такой системе требуется аппаратный рестарт ядра и последующее восстановление вычислительного процесса, что фактически прерывает постоянство функционирования на период времени превышающий допустимое. Исходя из оценочного анализа, следует вывод, что применение контроллеров «faultRobust» технологии в аппаратуре КА допустимо только в периферийных и сервисных модулях. При этом положительные стороны скоростного отказоопределения «faultRobust» используются в полной мере, и центральный управляющий модуль немедленно получает сигнал ошибки с указанием локализации.

Выбор структуры центрального процессорного блока в концепции [2] построения управления КА (рис. 6) состоит в обеспечении работоспособного состояния головной системы, а не только фиксации отказа и переключения на резервный канал, что обуславливает потерю управления в течение некоторого времени.

Практическое обеспечение устойчивости к отказам «на-лету», реализуется путём применения «византийского» принципа. Однако, классическая четырёхканальная византийская структура явно избыточна по всем техническим параметрам. В минимуме, применение принципа «голосования большинством» для исключения ложных состояний и сохранения работоспособности требует трёх взаимосвязанных информационных потоков или идентичных каналов. Данный подход достаточно сложен в реализации на независимых процессорах [8], особенно при обеспечении синфазности для выборки команд из памяти программ и прохождения через систему голосования в реальном темпе исполнения команд процессорами.

Применение технологии FPGA и возможности объёмов сверхбольших матриц к реализации в одном кристалле ядер процессоров позволило установить внутрисхемные модули голосования (рис.7а). Такой подход реализован в процессоре фирмы Atmel для военных и космических применений [9]. Защита от сбоев в регистрах и элементах фазирования сигналов после комбинаторных схем реализуется на основе мажоритарной логики, что позволяет исключить сбои, возникающие по причине ошибок SEU (Single Event Upset). Временной сдвиг импульсов стробирования может быть задан пользователем в программе начальной настройки оборудования в пределах периода максимальной частоты функционирования (рис. 7.б).

В последующем варианте исполнения данного процессора, со встроенным в корпус микросхемы дополнительного кристалла FPGA [10], предложенный способ применён по умолчанию также и для базовых ячеек кристалла программируемой пользователем логики. Это обеспечивает защиту от сбоев в аппаратуре интерфейсных модулей при построении сопряжения с периферийными блоками.

Однако, в отличие от контроллеров со встроенным «faultRobust» механизмом для всего кристалла, в вычислительных модулях на основе процессоров AT697 элементы памяти программ, памяти данных, периферийное оборудование устройств ввода-вывода располагаются вне кристалла. Учитывая требуемые для задач систем управления объёмы памяти в вычислительных модулях, получаем соотношение суммарной площади кристаллов элементов памяти к площади кристалла процессорного элемента, которое составляет более чем 3:1, а единственно доступным способом обеспечения отказоустойчивости на внешней магистрали есть встроенный в кристалл процессора механизм EDAC.

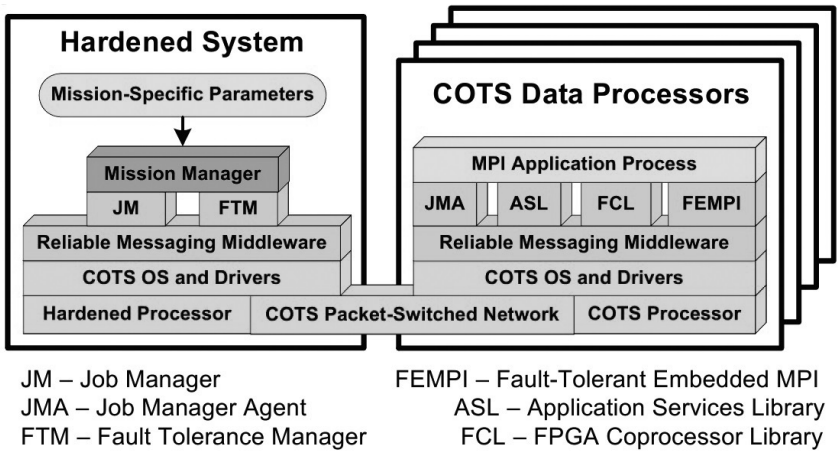

Рис. 6. Типовая концепция построения системы управления КА

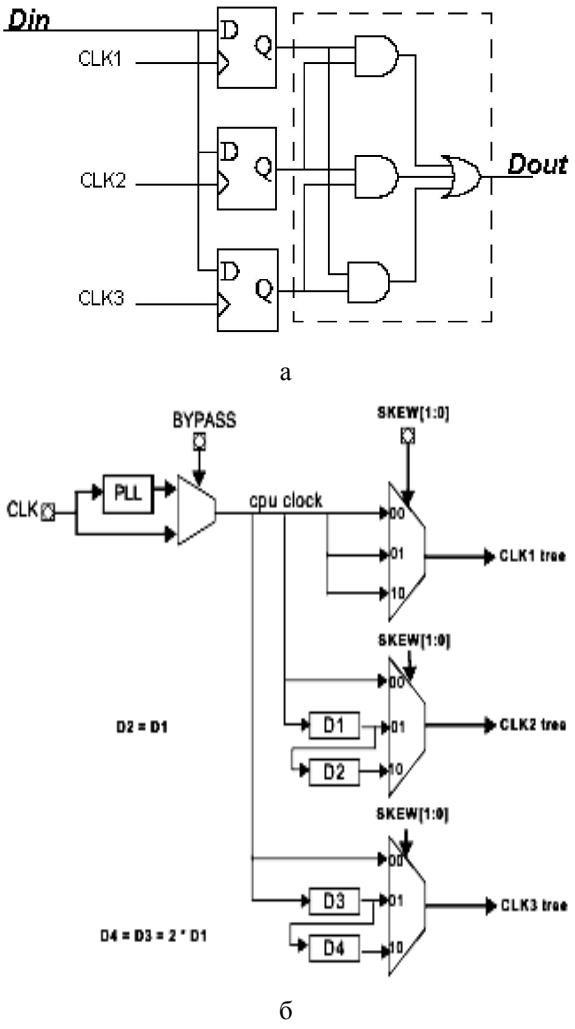

Рис. 7. Схема парирования сбоев в процессоре AT697F на основе византийского подхода с внутрикристальным трёхканальным резервированием

Таким образом, обеспечение отказоустойчивости в модулях памяти выделяется в самостоятельную задачу, влияющую на выбор элементов и архитектуры периферийных устройств вычислительного модуля канала головного процессорного блока системы.

Заключение

Структурное представление бортового комплекса аппаратуры (рис. 3) подчиняется только общей концепции функционально-алгоритмического обеспечения отказоустойчивости системы управления.

Задача выбора структуры надёжности для каждого функционального узла в представляемой концепции должна решаться не только исходя из интегрального показателя надёжности узла, но и включать временные параметры реакции на аппаратный отказ или сбой в его оборудовании.

Процесс выбора электронных компонент, планируемых к применению в аппаратуре бортовых систем управления, должен учитывать возможности и особенности функционирования встроенных средств определения и парирования отказов, представляемых производителями интегральных схем.

Комбинирование средств определения и парирования отказов при реализации каждого модуля, в пределах выбранной концепции, способствует улучшению характеристик надёжности.

Литература

1. Mariani, R. Comparing fail-safe microcontroller architectures in light of IEC 61508 [Electronic resource] / R. Mariani, P. Fuhrmann. – Access mode: http://cadal.cse.nsysu.edu.tw/seminar/seminar_file_ pclee/ pdf_1350895329.pdf. – 4.02.2014.

2. Advanced Space Computing with System System-Level Fault Tolerance [Electronic resource] / Grzegorz Cieslewski, Adam Jacobs, Chris Conger, Alan D. George. – Access mode: http://www.cs.sandia.gov/CSRI/Workshops/2008/FaultTolerantSpaceborne/presentations/Cieslewski-UF-FTWorkshop-final2.pdf. – 4.02.2014.

3. faultRobust technology [Electronic resource]. – Access mode: http://www.fr.yogitech.com. – 4.02.2014.

4. A single channel, fail-safe microcontroller to simplify SIL3 safety architectures in automotive applications [Electronic resource] / Dr. M. Baumeister, Dipl.-Ing. P. Fuhrmann, Philips, Aachen; Dr. R. Mariani, Yogitech, Pisa. – Access mode: http://home.arcor.de/mbaumeister/veroeff/BadenBaden 2007-Final.pdf. – 4.02.2014.

5. Speirs, N. A. Using Passive Replicates in Delta-4 to provide Dependable Distributed Computing [Text] / N. A. Speirs, P. A. Barrett // Proc. 19th Int. Symp. on Fault-Tolerant Computing Systems (FTCS-19), (Chicago, MI, U.S.A). IEEE Computer Society Press. – 1989. – P. 184–190.

6. Lyons, W. Enabling Increased Safety with Fault Robustness in Microcontroller Applications ARM [Electronic resource] / W. Lyons. – Access mode: http://www.arm.com/files/pdf/Enabling_Increased_Safety_with_Fault_Robustness_in_MCU_Applications.pdf. – 4.02.2014.

7. TMS570LS3137 16/32-Bit RISC Flash Microcontroller [Electronic resource]. – Access mode: http://www.ti.com/lit/ds/symlink/tms570ls3137.pdf. – 4.02.2014.

8. Харченко, В. С. IOTS-подход: анализ вариантов структур отказоустойчивых бортовых

комплексов при использовании электронных компонент Industry [Текст] / В. С. Харченко, Ю. Б. Юрченко // Chip News инженерная микроэлектроника. – 2003. - № 7. – С. 28-39.

9. Rad-Hard 32 bit SPARC V8 Processor AT697F [Electronic resource]. – Access mode: http://www.atmel.com/Images/doc7703.pdf. – 4.02.2014.

10. ATF697FF Rad- hard 32 bit SPARC V8 Re-configurable Processor DATASHEET [Electronic resource]. – Access mode: http://www.atmel.com/ Images/doc41000.pdf. – 4.02.2014.

Поступила в редакцию 6.02.2014, рассмотрена на редколлегии 12.02.2014

Рецензент: д-р техн. наук, проф., зав. каф. компьютерных систем и сетей В. С. Харченко, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ВБУДОВАНИХ СИСТЕМ НА ОДНОКРИСТАЛЬНИХ МІКРОКОМП'ЮТЕРАХ

Ю. Б. Юрченко

Проведено оцінку реалізуємості заданих вимог до обчислювальної системи в межах доступних апаратних засобів. Проаналізовано шляхи оптимізації архітектур на базі застосування паралельних систем при синтезі резервованих комплексів для особливо тяжких умов експлуатації з тривалим строком активного функціювання. Обгрунтовано доцільність та проаналізовано ефективність застосування апаратної синхронізації для контролю в резервованих структурах обчислювальних систем.

Ключові слова: вбудована система, відмовостійкість, переконфігуруєма архітектура, рівень цілісності.

FAIL SAFETY SUPPORT METHODS IN EMBEDDED SYSTEMS ON SINGLE-CHIP MICROCOMPUTERS

Yu. B. Yurchenko

The estimation of a realizability of the given requirements to the computing system within the limits of accessible hardware is investigated. Ways of architecture optimization on the basis of application of parallel systems at synthesis of redundant complexes for especially severe conditions of maintenance with long term of the active functioning is analyzed,. The expediency is justified and efficiency of application of hardware synchronization for control in redundant structures of computing systems is analyzed.

Keywords: embedded system, the fail safety, reconfigured architecture, integrity level.

Юрченко Юрий Борисович - канд. техн. наук, старший научный сотрудник, НПП Хартрон-Аркос, Харьков, Украина.