УДК 629.7.05

ВЫЧИСЛИТЕЛЬНЫЙ МОДУЛЬ ПОВЫШЕННОЙ НАДЁЖНОСТИ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ КОСМИЧЕСКИМИ АППАРАТАМИ

А.В. Есиновский, А.В. Леонтьев, А.Б. Уманский
(ОАО «Научно-производственное объединение автоматики им. академика Н.А. Семихатова», г. Екатеринбург)

Рассматриваются вопросы разработки структур на отечественной элементной базе и алгоритмов работы сбоеустойчивого управляющего вычислителя для систем автоматического управления малогабаритных космических аппаратов (МКА). Отмечается, что использование традиционных магистрально-модульных структур для МКА с учётом предъявляемых жёстких требований по объёмно-массовым характеристикам и энергопотреблению становится невозможным и требует новых подходов. Представлен ряд аппаратно-программных решений как основы для разработки управляющей цифровой вычислительной системы для малогабаритной системы управления МКА.

Ключевые слова: *система управления, космический аппарат, вычислительный модуль, факторы космического пространства, резервирование.*

Введение. В ОАО «НПО автоматики» (НПОА) выполняются работы по созданию малогабаритных бортовых цифровых вычислительных систем (БЦВС), с использованием отечественной микроэлектроники, работающих в режиме жёсткого реального времени и устойчивых к факторам космического пространства (ФКП).

Основной опасностью для аппаратуры СУ являются дозовые и одиночные радиационные эффекты, вызываемые потоками протонов, электронов и тяжёлых заряженных частиц, вызывающие сбои в работе аппаратуры СУ, в том числе и тиристорный эффект (ТЭ), который может приводить к выводу из строя микроэлектроники в составе СУ [1]. Помимо этого, воздействие радиационных ФКП на аппаратуру СУ длительное время вызывает деградацию параметров и характеристик используемой элементной базы.

Первый вид воздействия – дозовый эффект – можно парировать только на этапе создания конструкции КА, путём варьирования толщин корпуса КА, материала его изготовления и применения стойкой к дозовым нагрузкам элементной базы.

Другим видом воздействия на аппаратуру СУ являются одиночные радиационные эффекты, вызывающие сбои и катастрофические отказы в работе СУ. Сбои являются обратимыми, т. е. имеется возможность их парирования программно-аппаратными методами, например «залипание» транзистора в одно устойчивое состояние парируется снятием питания. Катастрофические отказы – необратимые эффекты, например вторичный пробой *p–n*-перехода, приводящий к его разрушению.

В части парирования ТЭ замечено [1], что он является обратимым: при своевременном снятии питания тиристорная структура выключается, и при повторном включении питания ожидается полное восстановление работоспособности и параметров изделия. Несвоевременное снятие питания при возникновении ТЭ может привести к отказу микросхемы. В случае отсутствия возможности своевременного обнаружения ТЭ программными способами, для защиты интегральных схем от необратимого повреждения, могут применяться токоограничивающие резисторы или аппаратные решения, осуществляющие контроль потребления тока интегральными схемами прибора. На этих принципах построено большинство технических решений для парирования ТЭ.

Данные эффекты могут приводить к нарушению штатного функционирования аппаратуры и её отказу, если в ней не применены необходимые пассивные схемотехнические и программно-алгоритмические методы парирования одиночных сбоев и защиты элементной базы от одиночных катастрофических отказов. При этом основным принципом проектирования сбоеотказоустойчивой системы является временная, информационная и аппаратная избыточность.

Технические требования к БЦВС для СУ КА. Были определены следующие требования, предъявляемые к разрабатываемой БЦВС: 1) жёсткое ограничение по массогабаритным характеристикам, обусловленное использованием СУ на микро- и наноспутниках; 2) функционирование в условиях воздействия ФКП в течение длительного времени; 3) самовосстановление после сбоев в работе без вмешательства извне; 4) корректопригодность программного обеспечения; 5) использование только отечественной элементной базы. Современные вычислительные системы разработки НПОА ориентированы на построение БЦВС с магистрально-модульной структурой, работающих под управлением центрального резервированного вычислителя малой разрядности. Модули собираются в вычислительную систему по-

средством установки на общесистемной магистрали требуемого для данной системы управления набора базовых модулей.

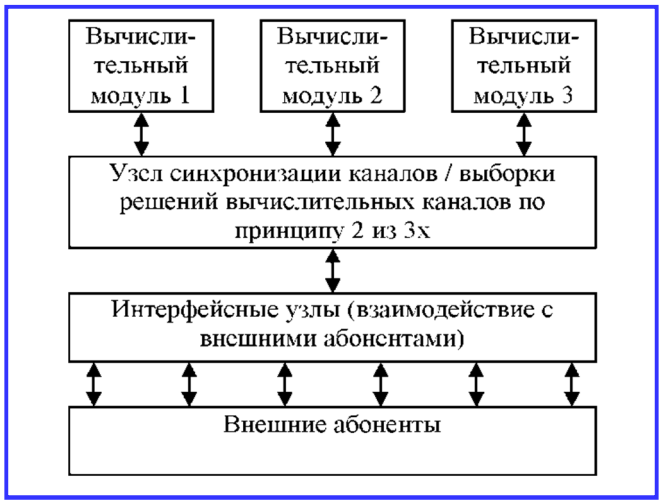

Рис. 1. Структура типовой трёхканальной БЦВС

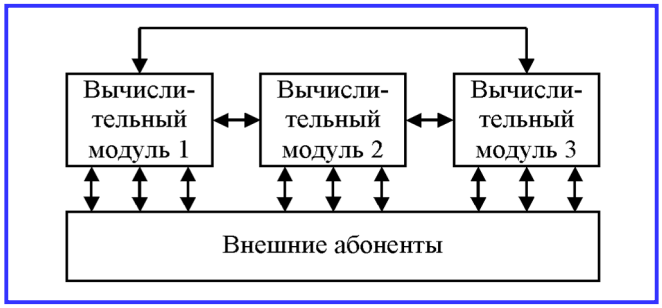

Рис. 2. Стуктура управляющего трёхканального ВМ

Традиционно в разработках БЦВС предприятия используются троированные вычислительные структуры, что обусловлено необходимостью обеспечения высоких показателей надёжности функционирования системы управления в целом (например, для СУ ракеты-носителя семейства Союз-2) [2].

Применение БЦВС данной структуры для КА затруднительно из-за относительно высоких массогабаритных характеристик. Поэтому необходимы современные подходы к построению архитектур малогабаритных надёжных СУ.

Особенности реализации требований к БЦВС СУ КА. В ходе работ по реализации вышеобозначенных требований было установлено, что для обеспечения гарантированного обнаружения сбоя и самовосстановления БЦВС оптимальным является использование трёхканального вычислительного модуля (ВМ). Наличие трёх синхронно работающих каналов ВМ позволяет осуществлять обнаружение канала с нарушенным функционированием по сравнению выдаваемой им информации в соседние каналы по принципу «два из трёх».

Типовая резервированная структура БЦВС разработки НПОА представлена на рис. 1.

В типовых схемах содержится, по меньшей мере, пять узлов – три вычислителя, узел синхронизации и выборки решений, интерфейсные узлы – реализованные в виде отдельных модулей [3]. Но из-за жёстких ограничений габаритных размеров и массы аппаратуры СУ необходимо предельно сократить количество используемых узлов и возложить их функции на программное обеспечение (ПО) трёхканального управляющего вычислителя. Упрощённая, с аппаратной точки зрения, схема представлена на рис. 2.

Требование по корректопригодности ПО обеспечивает возможность модернизации используемых алгоритмов работы КА без возвращения его на Землю, т. е. в СУ должна быть предусмотрена возможность корректировать ПО с Земли по радиоканалам. Однако это накладывает ограничения на спектр используемой элементной базы. В частности становится невозможным использование однократно прошиваемой памяти. А поскольку многие типы перепрограммируемой памяти подвержены искажениям своего содержимого вследствие воздействия ФКП, то необходимо использовать программные методы восстановления ПО управляющего вычислителя. Суть этих методов заключается в избыточном хранении кода программ с возможностью последующего его восстановления.

Оптимальным решением является хранение нескольких копий программного обеспечения в постоянном запоминающем устройстве (ПЗУ) и наличие специального загрузчика, функцией которого является восстановление ПО на основе нескольких его копий. При этом загрузчик должен храниться в отдельном неискажаемом, однократно прошиваемом ПЗУ.

Но в случае невозможности использования дополнительного ПЗУ, вследствие ограничений по массогабаритным характеристикам, необходимо использовать ПЗУ с переключаемыми банками, которые хранят полную копию программы. При этом переключение банков должно осуществляться из соседних каналов.

Другим решением могло быть использование самоконтролирующихся кодов, типа кодов Хэмминга, реализованных аппаратно. Но поскольку у имеющихся отечественных процессоров, поддерживающих код Хэмминга, заложено исправление только одного бита в слове, а искажения в памяти, вызываемые ФКП, чаще имеют блочный характер,

то данное решение является неэффективным. Кроме того, для хранения контрольных кодов требуются дополнительные микросхемы.

Аппаратная реализация управляющего вычислителя. Каждый канал управляющего вычислителя имеет собственный процессор (1892ВМ8Я), оперативную память, постоянную память, интерфейсную ПЛИС (рис. 3). Каждый процессор связан с двумя другими по интерфейсу SpaceWire. Взаимодействие с периферийными устройствами осуществляется с помощью: 1) кодовых линий связи (КЛС) RS-485, на основе порта UART; – КЛС типа «токовая петля» на основе порта UART; 2) дублированной КЛС на основе ГОСТ Р 52070 (MIL-STD-1553), реализованный на основе ПЛИС; 3) дискретных сигналов с портов ввода/ вывода общего назначения процессора, использующихся для: управления внешними устройствами; управления питанием процессоров 1, 2, 3, необходимого для перезапуска канала, имеющего отрицательный результат контроля работоспособности; переключения используемого банка ПЗУ каналом ВМ.

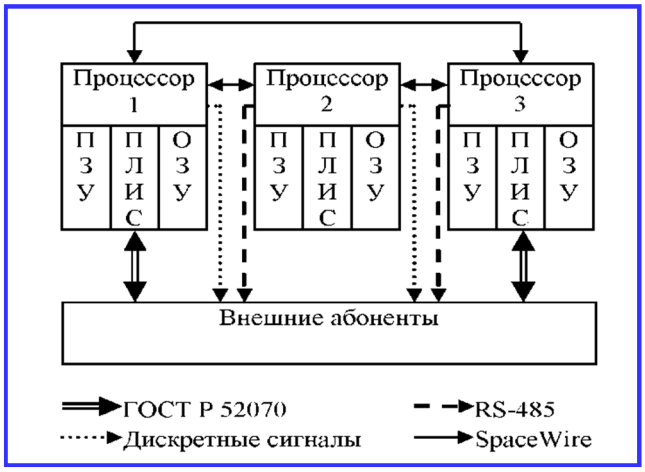

Рис. 3. Аппаратное устройство управляющего вычислителя

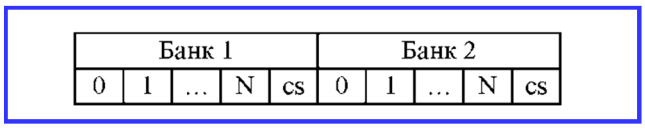

Рис. 4. Структура ПЗУ

Для защиты от ТЭ, который может приводить к резким скачкам потребления тока интегральными микросхемами, приводящим к отказам, в шину питания были установлены токоограничивающие резисторы. ПЗУ каждого канала разделено на два банка с возможностью переключения используемого в данный момент банка соседним или собственным каналом. Смена банка ПЗУ достигается путём манипулирования старшим разрядом шины адреса микросхемы ПЗУ. Для противодействия повреждениям памяти в обоих банках ПЗУ хранятся одинаковые программы. Каждая копия программы разбита на N блоков, снабжённые контрольными суммами которые хранятся в последнем блоке банка (с идентификатором «cs»), как показано на рис. 4.

В первых блоках ПЗУ хранится программный загрузчик, управление на который передаётся при подаче питания на процессорный канал. После запуска загрузчик проверяет свою целостность и отправляет соответствующие сообщения в соседние каналы. В случае неполучения соседними каналами данного сообщения они снимают питание с канала, не выдавшего данное сообщение, и производят смену используемого им банка ПЗУ.

В случае подтверждения целостности загрузчика им осуществляется копирование основной программы из ПЗУ в ОЗУ (оперативное запоминающее устройство). При копировании параллельно считается контрольная сумма блока. Если рассчитанная контрольная сумма не совпадает с контрольной суммой, хранящейся в ПЗУ, то блок считается испорченным и копируется по такому же принципу из другого банка. Копированием программы из ОЗУ в ПЗУ достигается ускорение выполнения программы, так как задержка обращения к ПЗУ многократно выше, чем к ОЗУ. Данная операция позволяет получить в ОЗУ исправную копию программы даже при множественном повреждении её блоков. Очевидно, что если повреждены два блока хранящих одну и ту же часть программы, то канал, к которому подключена сбившаяся память, отказывает. Исходя из этого, размер блоков выбирают наименьшим с целью снижения вероятности искажения блоков, хранящих одну и ту же часть программы.

Программное обеспечение управляющего вычислителя. При разработке СУ к программному обеспечению бортовых вычислительных систем предъявляются жёсткие требовании к надёжности функционирования, под которой понимается сбоеустойчивость, предсказуемость работы, автоматическое парирование расчётных нештатных ситуаций и другие характеристики, обеспечивающие максимально автономную, т. е. без участия наземных комплексов управления, работу СУ.

Сборка версий ПО для управляющего вычислителя осуществляется с использованием компилятора, обрабатывающего исходные коды бортовых модулей на языке программирования Си.

Мировая практика создания ПО для СУ определяет операционную систему реального времени (ОСРВ) важнейшим программным компонентом, лежащим в

основе функционирования. ОСРВ позволяет одновременно организовать работу нескольких подпрограмм с разными частотами включения и обеспечить взаимодействие между ними для решения одной общей задачи [4]. Основная проблема при создании ОСРВ – обеспечение одновременного решения функциональных задач и задач контроля правильности работы аппаратуры СУ, а также обеспечение решения задач нейтрализации отказов, вызванных дестабилизирующими воздействиями, возникающими в случайные моменты времени.

В частности, ПО управляющего вычислителя разбито на системное (СПО) и функциональное программное обеспечение (ФПО). Практически весь состав СПО является ОСРВ, а ФПО – абстракцией верхнего уровня, использующей API ОСРВ. СПО отвечает за обмен с внешними устройствами и исполнительными органами. ФПО отвечает за отработку логической части алгоритмов. Работа ФПО идентична во всех трёх каналах управляющего вычислителя, а работа СПО отличается в связи с тем, что набор внешних устройств, подключённый к каналам различен.

Взаимодействие СПО и ФПО производится с помощью системных вызовов. При каждом системном вызове СПО производит синхронизацию счёта времени во всех трёх каналах управляющего вычислителя. Также производится передача типа данного системного вызова и его параметров. Каждый канал проверяет, что ФПО во всех трёх каналах обратилось с одним и тем же типом и параметрами системного вызова, в одно и то же время. В случае прохождения данной проверки производится требуемое взаимодействие с внешним устройством, в том канале, который непосредственно подключён к нему, по завершению данного взаимодействия его результат передаётся в два других канала. В случае непрохождения данной проверки, канал, который её не прошёл, признаётся сбившимся.

Восстановление СУ после сбоя. Независимо от причины сбоя, сбившийся канал должен быть перезагружен. Сигнал снятия питания должны выставить оба соседних канала. Только в этом случае схема сброса питания активируется. Восстанавливаемый процессор инициализируется аналогично, как и при первой подаче питания. После инициализации процессор квитирует соседние процессоры об успешном запуске. При отсутствии квитанции в течение определённого времени соседний процессор меняет зону загрузки для восстанавливаемого процессора и заново перезапускает его. Если после перезапуска процессор не квитировал соседей, то считается, что канал СУ отказал. При успешном восстановлении, восстанавливаемый процессор должен получить из соседнего процессора данные для восстановления работоспособности (либо всё состояние ОЗУ и регистров процессора, либо только ключевые параметры для восстановления вычислительного процесса – на усмотрение разработчиков ПО). Также восстанавливается счёт времени и формируется определённый в зависимости от причины сбоя признак сбоя и восстановления (ПСВ). Наличие ПСВ означает, что был зафиксирован сбой и произведено восстановление. Этот признак необходим для того, чтобы в последующем определить причину и момент возникновения сбоя.

Заключение. Получена малогабаритная бортовая цифровая вычислительная система, позволяющая реализовать всю совокупность поставленных задач.

Заложенные аппаратно-программные средства защиты, контроля и восстановления позволяют обеспечить работоспособность космического аппарата в условиях возникновения кратковременных разовых сбоев, вызванных факторами космического пространства.

Литература

1. Тараксин А. С., Нигматуллин Р. Р, Савченков Д. В., Соловьёв С. А., Яненко А. В. Методики исследования и предотвращения развития катастрофического отказа вследствие одиночного тиристорного эффекта / А. С. Тараксин и др. // Проблемы разработки перспективных микро- и наноэлектронных систем: сборник докладов научн.-практич. конф. – М.: ИППМ РАН, 2012. – С. 628 – 633.

2. Антимиров В. М., Уманский А. Б., Шалимов Л. Н. Бортовые цифровые вычислительные системы семейства «Малахит» для работы в экстремальных условиях / В. М. Антимиров и др. // Вестник СГАУ. – 2013. – № 4(42). – С. 19 – 27.

3. Шейнин Ю., Солохина Т., Петрикович Я. Технология SpaceWire для параллельных систем и бортовых распределённых комплексов / Ю. Шейнин и др. // Электроника: Наука. Технология. Бизнес. – 2006. – № 5. – С. 64 – 75.

4. Соловьёва Н. В., Чебанов Е. Е., Дудин Н. В., Ханевский Д. А., Баженов А. И. К вопросу создания собственной операционной системы реального времени / Н. В. Соловьёва и др. РКТ. Сер. XI. Системы управления ракетных комплексов. – 2012. – Вып. 1. – С. 59 – 68.

Поступила в редакцию 24.07.2014

***Александр Валентинович Есиновский**, инженер-конструктор, e-mail: avt@npoa.ru, т. (343)263-76-89.*
***Алексей Викторович Леонтьев**, инженер-программист, e-mail: avt@npoa.ru, т. (343)263-76-89.*
***Алексей Борисович Уманский**, канд. техн. наук, начальник сектора, e-mail: avt@npoa.ru, т. (343)263-76-89.*