УДК 621.03

ПОВЫШЕНИЕ НАДЕЖНОСТИ БОРТОВЫХ УПРАВЛЯЮЩИХ КОМПЛЕКСОВ ПУТЕМ ПОСТРОЕНИЯ МАЖОРИТИРОВАННЫХ СТРУКТУР НА ОСНОВЕ АППАРАТНОЙ СИНХРОНИЗАЦИИ ОДНОКРИСТАЛЬНЫХ МИКРОКОНТРОЛЛЕРОВ

© Ю. Б. Юрченко

Науково-виробниче підприємство ХАРТРОН-АРКОС

Досліджено структури відмовостійких багатоканальних бортових комп'ютерів критичного застосування. Відмічено зменшення часу виявлення прихованого дефекту при використанні елементів апаратної синхронізації процесів у каналах. Показано переваги побудови жорстко зв'язаних апаратно-мажоритованих структур з елементами міжканального порівняння для систем управління особливо критичного застосування.

Системы управления (СУ) критического назначения определяют особый подход к выбору структуры отказоустойчивых бортовых компьютеров (БК). Структура БК должна обеспечивать сохранение работоспособности в условиях одиночных сбоев и отказов (дефектов). Функционирование аппаратуры БК в условиях обратимых дефектов требует таких решений, которые в течение активного рабочего цикла выполняемой задачи либо обеспечивают парирование сбоев, либо их маскирование и восстановление процесса управления на борту. Полное тестирование и реконфигурация аппаратной части БК может происходить только в течение пассивного цикла выполняемой задачи [24]. Длительность активного рабочего цикла, соотношение его с пассивным и степень риска воздействия внешних факторов на аппаратуру СУ определяет требования при выборе структуры БК и его компонентов при проектировании СУ [4—6, 10, 22, 25].

Анализ рынка элементной базы показывает перспективы применения COTS- и IOTS-подходов для построения БК [5, 6, 11, 25], однако при построении СУ для особо критических применений необходимо иметь уверенность [3] в своевременном и гарантированном обнаружении возникающих дефектов, для последующих операций по их маскированию, изоляции и парированию.

Цели данной работы:

— анализ многоканальных структур бортовых управляющих компьютеров критичного применения;

— анализ времени состояния скрытого дефекта в структурах СУ с горячим резервированием каналов БК при применении аппаратной синхронизации процессов.

Многоканальные структуры с холодным и горячим резервом. В структурах БК такого типа за основу берется процессорный блок со встроенной системой обнаружения и коррекции ошибок. Для управления модулями в данной резервированной структуре вводится специальный блок контроля и управления реконфигурацией (БКУР). Такой блок должен функционировать как жесткий автомат с идеально отработанными алгоритмами управления резервом при всех возможных ситуациях. Это может быть либо разработка той же фирмы, что и БК, как, например, модуль резервирования 1785CHBM фирмы Allen Bradley для контроллеров семейства PCL-5, либо собственная разработка для проектируемой СУ.

Реальный показатель безотказной работы для всего БК сильно зависит от показателя безотказной работы собственно БКУР, величина которого должна быть гораздо выше, чем показатели для остальных резервированных модулей. Время жизни скрытого состояния потенциального сбоя в структуре с горячим резервом может быть сведено к нескольким десяткам тактов системной задачи СУ и зависит от построения алгоритмов работы интерфейса между каналом процессора и БКУР. Для случая с холодным резервом и аналогичными алгоритмами взаимодействия БКУР может позволить сократить по сравнению с одноканальной структурой БК время рестарта управляющей задачи СУ путем подключения резервного канала сразу после отсутствия сигнала нормы от активного канала. В обоих

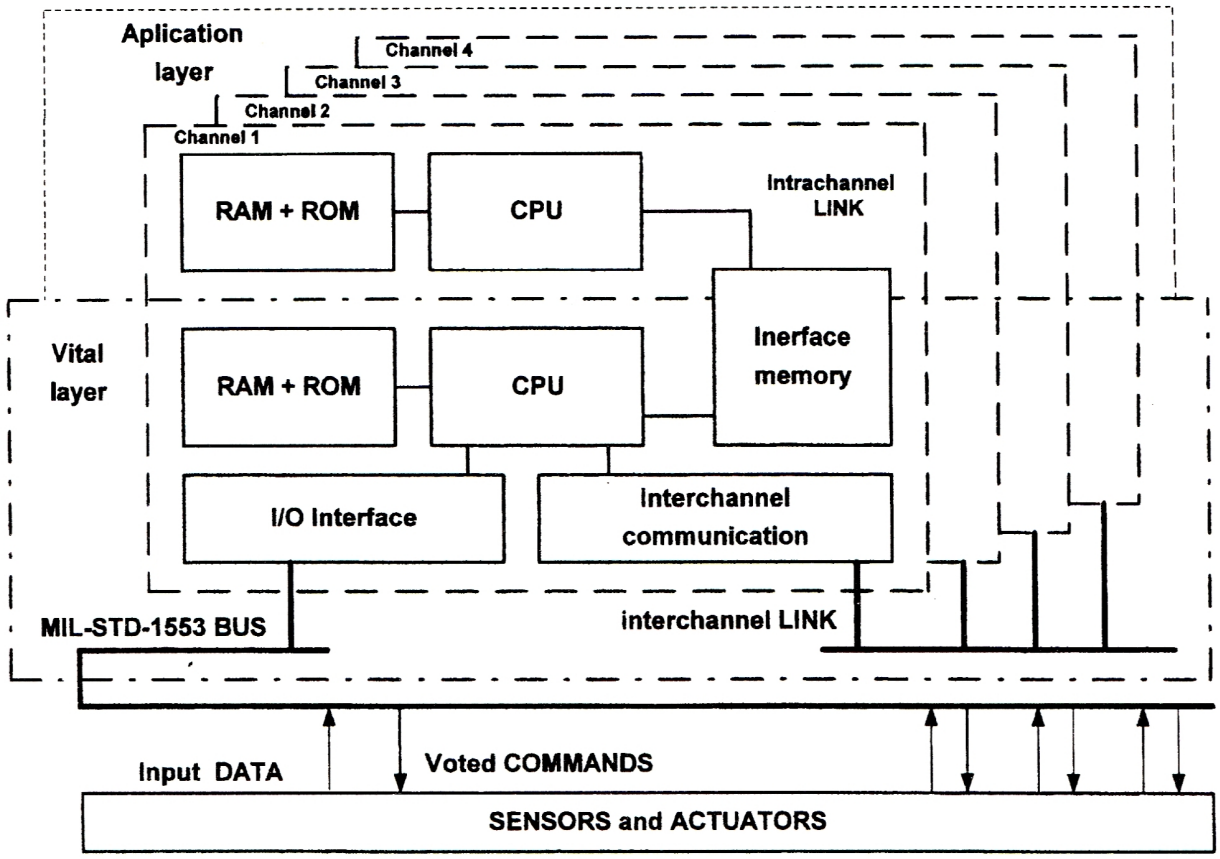


Рис. 1. Структурная схема БК с АМКВИ на основе двухпроцессорных канальных модулей

случаях управление передается на предварительно протестированный резервный канал, а подозреваемый канал переводится в режим тестирования с последующей маркировкой пригодности. Здесь также есть риск попадания на канал с неисправностью на момент включения [15].

Для выполнения задач, связанных с управлением процессами с быстро изменяющимися данными, например постоянного и точного поддержания ориентации и навигации кроме системной производительности, необходимо уменьшение времени реакции на дефект в оборудовании, что влечет дальнейшее усложнение структуры БК как в аппаратной, так и программной части. Кроме этого, необходимость развития функций БКУР превращает его в самостоятельный процессорный модуль с более жесткими требованиями по надежности.

Многоканальные структуры с программным обеспечением отказоустойчивости. Введение межканального обмена (МКО) в структуру БК позволяет повысить достоверность истинной работы каналов БК и сократить время обнаружения сбоя в одном из каналов БК. Предложено множество вариантов построения структуры с автоматом межканального контроля и восстановления информации (АМКВИ): SIFT [10, 19], MAFT [18], FTPP [16], DELTA-4 [21] и др., где за аппаратную основу взято более двух идентичных процессорных модулей с коммуникационным оборудованием для организации интерфейса программного межканального обмена (ПМКО).

Общая особенность БК с ПМКО состоит в практически полном переложении функций поддержания отказоустойчивости как БК, так и всей СУ на средства ПО. Теоретический показатель надежности оборудования высок, однако работоспособность БК на практике начинает зависеть от правильности алгоритмов обработки обнаружения и парирования дефектов. БК с такой структурой требуют выделения в такте задачи, кроме времени на самотестирование оборудования канала, дополнительного времени для организации ПМКО входной информа-

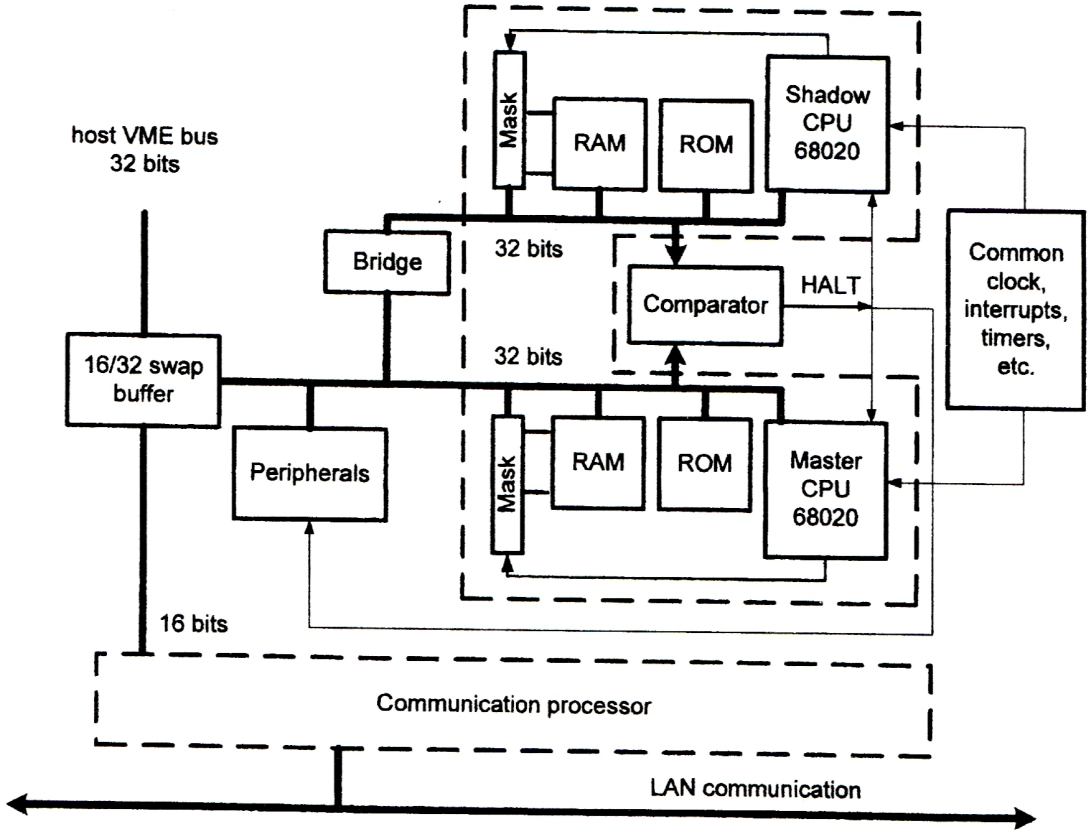


Рис. 2. Структурная схема базового процессорного модуля Delta-4

ции, данных вычислений, результатов самотестирования и обработки полученной информации для последующей выдачи [22]. Время на выполнение прикладной задачи уменьшается, и вследствие этого требуется повышение производительности процессорных модулей для покрытия вынужденных простоев и обслуживания задачи поддержания истинной работы БК для сохранения общей вычислительной мощности СУ [14]. Величина выделяемого времени зависит от количества анализируемой информации, пропускной способности интерфейса ПМКО [1, 22].

Однако ограниченная пропускная способность системной магистрали, интерфейса ПМКО, а также объем оборудования канала БК не обеспечивают малого времени на определение наличия дефекта. Время t, занимаемое задачей и затраченное на определение дефекта в СУ с k каналами, n внутренними параметрами, N входными-выходными данными и пропускной способностью ПМКО v можно определить как

$$t = k(n + N/)k/v.$$

Необходимо заметить, что данное выражение применимо только при условии охвата всех параметров n и данных N за один цикл ПМКО. При возрастании переменных n или N и сохранении прежней длительности такта задачи становится необходимым разделить функции управления и обеспечения надежности БК, а количество каналов k, активно задействованных в ПМКО желательно иметь минимальным, но достаточным для определения факта наличия дефекта (обычно $k = 3$) [1, 2, 5, 7, 10, 22].

Применение дополнительного коммуникационно-контролирующего процессора например, как в аппаратуре СУ с задачами ориентации и навигации КА [14, 24] или в контроллере SC300E фирмы ABB August Ltd для критических применений позволяет решить данную проблему. Такие построения БК представлены на рис. 1. Особенность БК такой структуры состоит в двухуровневом построении аппаратуры и программ [14, 18, 24]. Коммуника-

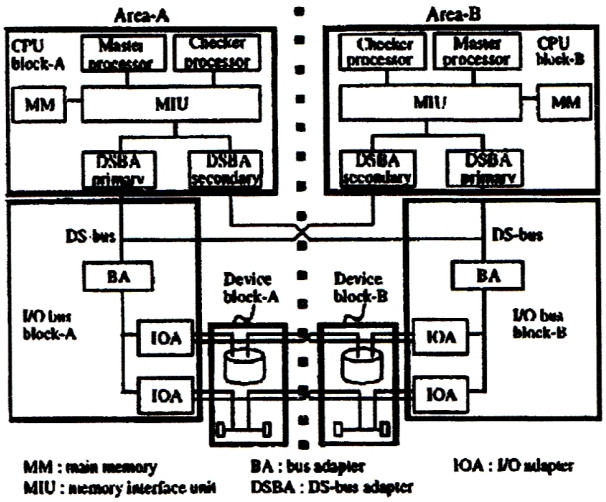


Рис. 3. Структурная схема QPR-БК с перекрестными связями

ционно-контролирующий процессор имеет возможность осуществлять межканальный обмен и контроль истинности работы приложений своего канала, во время работы каналов прикладного уровня. При этом разделение функций вызывает необходимость синхронизировать работу процессоров прикладного и жизненного уровня.

Коммуникационно-контролирующий процессор за время такта прикладной задачи может произвести более глубокий анализ поступающей и выдаваемой информации. Ожидаемое уменьшение времени обнаружения дефекта при разделении функций пропорционально высвобождаемой части такта задачи одноуровневой структуры.

Основными проблемами при построении АМКВИ структур становятся программная синхронизация процессов в каналах и поддержание планирования в интерфейсе ПМКО [1, 14, 22]. Частично решение этих проблем предлагается на программно-аппаратном уровне. В структуре DELTA 4 [21] синхронизация пары процессоров обеспечивается единством для пары каналов служб системной частоты, времени, прерываний, прямого доступа (рис. 2), в QPR-архитектуре [20] — перекрестными связями с периферийным оборудованием (рис. 3), в контроллере SC300E фирмы ABB, как и в микроконтроллере для космических применений [13] — аппаратным мажоритированием входной и выходной информации.

Применение элементов аппаратной синхронизации сокращает время простоев на период ожидания в коммуникационных программных модулях при выходе на точки ПМКО и задает жесткую циклограмму работы процессов как жизненного, так и прикладного уровня (рис. 4). Частное время локализации скрытого дефекта сокращается, однако количество внутренних параметров n может возрасти за счет дополнительного оборудования, что сказывается на общем времени принятия решения по локализации и парированию [15].

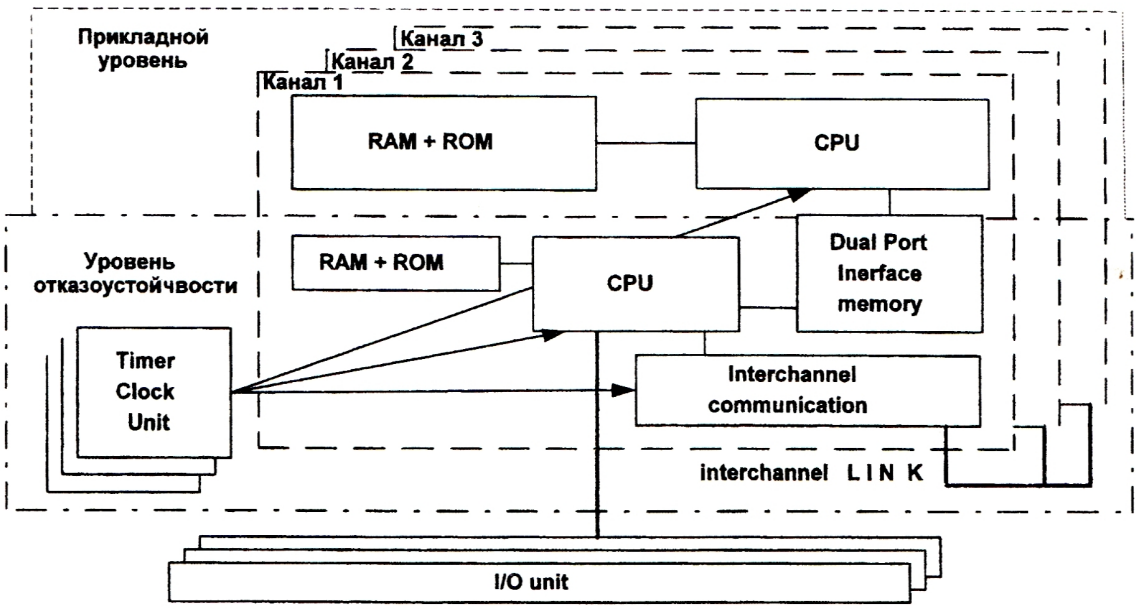


Рис. 4. Структурная схема двухуровневого БК с аппаратной синхронизацией каналов

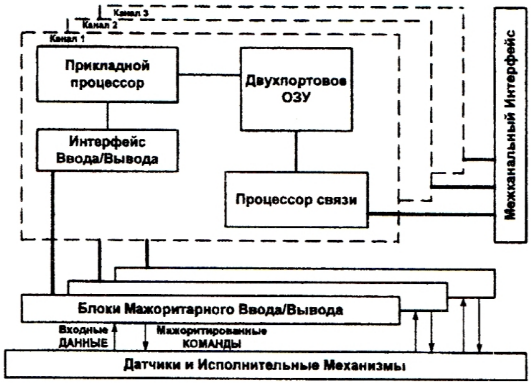


Рис. 5. Структура БК SIFT-CPU-HIFT-I/O

Многоканальные структуры с программным обеспечением отказоустойчивости и аппаратным мажоритированием входной и выходной информации каналов. Аппаратные решения по синхронизации процессов в каналах путем аппаратного межканального мажоритирования входной информации (Hardware Implement Fault-Tolerant Input-Output далее HIFTI/O) частично упрощают программную задачу определения наличия дефекта процессором (Software Implement Fault-Tolerant Central Processor Unit далее SIFTCPU). К таким решениям был проявлен интерес [13, 17], но при этом реализация проектов БК со структурой SIFTCPU-HIFTI/O вызывает необходимость проектирования уникального и достаточно сложного межканального оборудования. Такие решения позволяют повысить надежность всей СУ, так как узел мажоритирования между БК и периферийным оборудованием превращает надежностную структуру СУ из одноярусной в, как минимум, двухъярусную (рис. 5) с возможностью наращивания ярусов по периферийному оборудованию ввода-вывода.

Необходимо заметить, что в данной структуре БК отсутствуют потери времени на программное мажоритирование входной и выходной информации. Так же становится возможной реализация быстрого аппаратного межканального сравнения информации и определения наличия дефекта на момент чтения или выдачи. Время жизни скрытого состояния дефекта в каналах сокращается до:

$$t = k^2 n/v,$$

т. к. на срезе устройств ввода-вывода (УВВ) время обращения к внешним устройствам мене длительности такта ($1/v \to 0$). Соответственно на срезе БК t сокращается до нескольких тактов задачи СУ, определяемых количеством параметров n [15]. Показатели надежности, и особенно времени обнаружения дефекта, в такой структуре гораздо лучше, особенно при большом количестве N внешних параметров СУ. Следует заметить, что на этапе выдачи информации суммарная достоверность SIFT-истинности выдаваемой информации подтверждается межканальным HIFT-сравнением.

Интересное предложение по отказоустойчивости I/O HIFT БК предложено в [23]. Структурная схема соединения процессорных узлов (а) и архитектура единичного узла (б) представлена на рис. 6. В этой структуре БК решение вопросов отказоустойчивости состоит в аппаратном сетевом мажоритировании магистрали МКО и циклической передачи каналами прямого доступа предварительно программно подготовленной информации вычислительного процесса и состояния аппаратуры каждого из каналов. Это сочетание программно и аппаратно поддерживаемой отказоустойчивости для высокопроизводительных однокристальных сигнальных процессоров должно обеспечить время обнаружения возможных дефектов в пределах времени

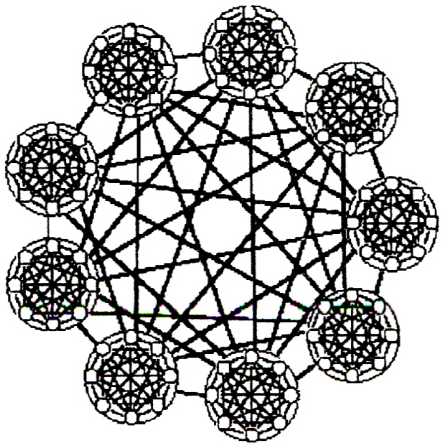
$$t = (n + N)/v.$$

БК с только HIFTI/O построением в структуре надежности процессорного модуля представляют одноярусную структуру и повышение показателя надежности возможно только путем наращивания количества каналов аппаратуры. Это ведет к соответствующим накладным аппаратным и временным расходам в СУ с сохранением самотестирования и обеспечения отказоустойчивости программными средствами.

Многоканальные структуры с аппаратным многоярусным мажоритированием. В отличие от одноярусных БК, где мажоритирование информации осуществляется (программно и аппаратно) только на входных и выходных сигналах, в многоярусной структуре БК (Multi-Level Hardware Implement Fault-Tolerant далее ML-HIFT) аппаратному межканальному мажоритированию подвергаются все основные магистральные сигналы процессора, памяти, блока сопряжения с УВВ и т. п. Такой подход позволяет определять и парировать возникающие дефекты в каждом цикле обращения по всем основным функциональным узлам БК [2, 7, 11, 12]. Типовая структура ML-HIFT БК представлена на рис. 7.

Применение решений по жесткой синхронизации однокристальных микроконтроллеров на аппаратном уровне дало возможность построения БК по принципу магистрального мажоритирования. Введение аппаратного межканального сравнения позволяет достичь уменьшения времени определения

а)



б)

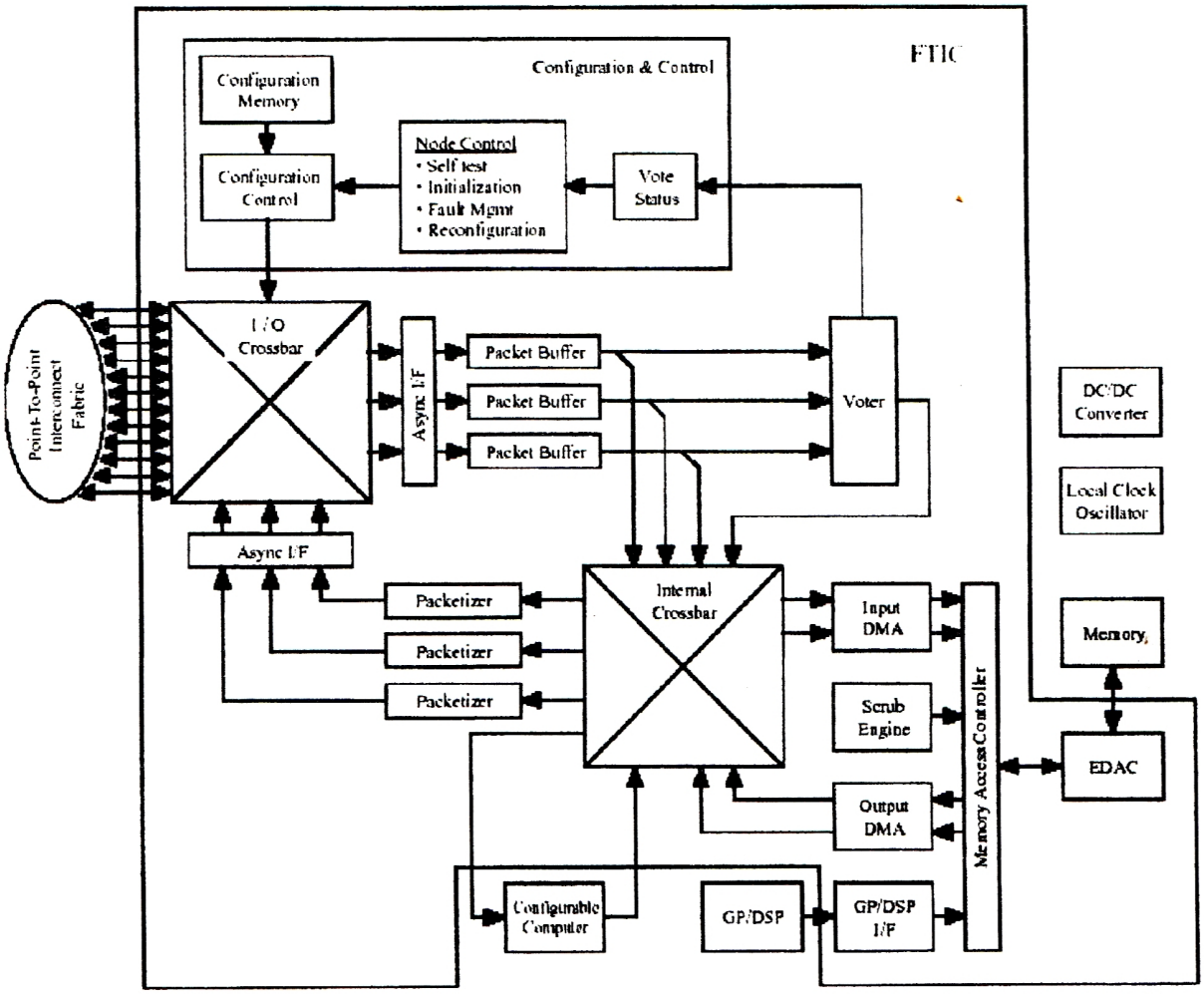


Рис. 6. БК на сигнальных процессорах с HPPS структурой узлов (*а*) и единичного узла (*б*)

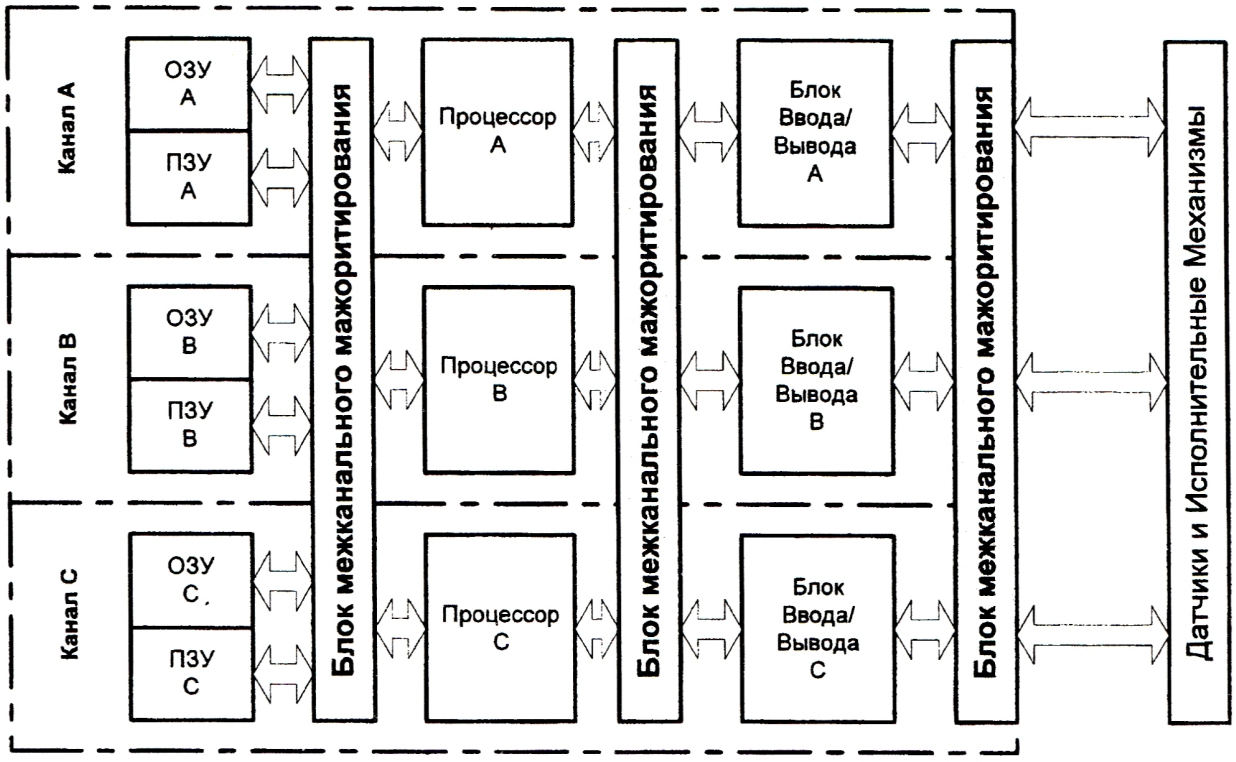


Рис. 7. Структура ML-HIFT БК

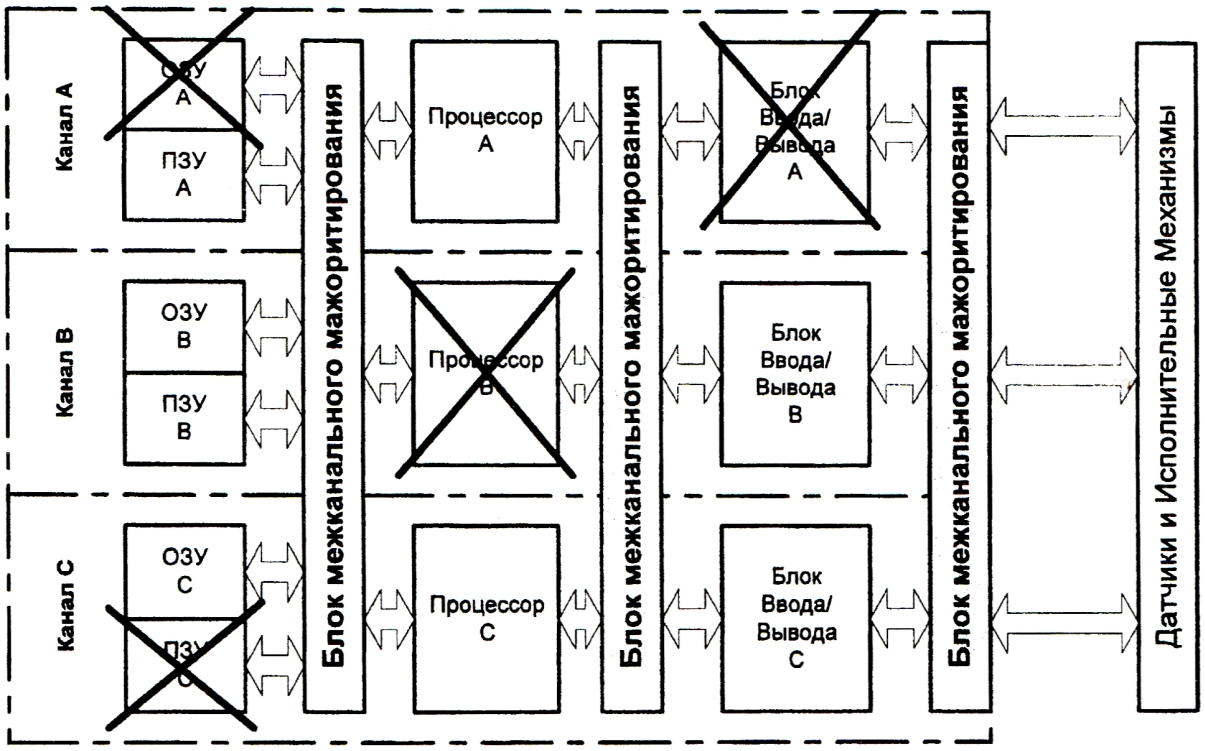


Рис. 8. Возможное накопление отказов блоков в ML-HIFT БК не приводящее к приостановке задачи процесса управления

дефекта оборудования до $t \leq 1$. Такое время реально достижимо, так как при ограниченном числе параметров $n + N$ пропускная способность v МКО резко возрастает, а мажоритирование и межканальное сравнение происходит аппаратно в каждом цикле процессорной шины. Даже грубая оценка показывает, что MLHIFT БК без адаптации структуры сохранит свое функционирование и без приостановок закончит задачу управления, находящуюся на активной фазе выполнения, при одном дефекте в ярусе каждого из каналов (рис. 8). При этом дефекты оборудования СУ определяются, изолируются и парируются на каждом цикле шины процессора. Для ранее рассматриваемых структур при одинаковом количестве каналов аналогичное распределение дефектов оборудования в соответствующих блоках и каналах БК приведет при сбоях — к необходимости приостановки процесса управления, реконфигурации на рабочий канал и быстрому истощению запасов резервного оборудования [22, 24], а при отказах — к полной потере работоспособности БК.

Применение многоярусного магистрального мажоритирования позволяет аппаратно фиксировать, изолировать и парировать возникающие дефекты не далее как к следующему циклу процессорной шины, а к концу такта задачи иметь четкую карту работоспособного состояния как БК, так и комплекса аппаратуры СУ [2, 7, 11]. Такая высокая скорость обнаружения и парирования отказов, с учетом опасений касающихся применения в системах управления цифровой обработки и применения элементов дальнего зарубежья [3], позволяет рекомендовать данную структуру БК для применения в необслуживаемых СУ с задачами, требующими очень жесткого регламента времени и требуемой [14, 22, 24] частотой дискретизации свыше 100 Гц.

Показатели надежности БК ML-HIFT структуры можно повышать и создавать ее требуемый запас, либо увеличением числа ярусов мажоритирования оборудования, либо применением методов адаптивного мажоритирования [2, 7, 11], что не вызывает необходимости увеличения каналов БК и роста сопутствующих накладных расходов, отмечаемых в [11]. Показатель прикладной вычислительной производительности к затраченному оборудованию для данной структуры БК лучше, по сравнению с SIFT-базированными структурами [11]. Очень важно, что обеспечение надежности происходит на аппаратном уровне и не зависит от скрытых дефектов в ПО.

Выводы. Время жизни скрытого состояния дефекта есть одним из ключевых параметров конечной архитектуры всего аппаратно-программного управляющего комплекса, величина которого зависит от структуры построения системы управления, и особенно бортового компьютера [15]. Данный показатель оказывает существенное влияние на достоверность принимаемой, обрабатываемой информации и последующих действий со стороны системы управления, особенно в системах критичного применения с жестким регламентом времени.

Уменьшение времени жизни скрытого состояния дефекта в структурах с автоматом программного межканального обмена и восстановления информации возможно путем применения средств принудительной аппаратной синхронизации процессов в каналах бортового компьютера. Данный факт особо важен в обслуживаемых системах управления с пространственно распределенными каналами бортового компьютера (например, [22]). Введение принудительной аппаратной синхронизации в обслуживаемых структурах с автоматом программного межканального обмена и восстановления информации бортового компьютера позволяет снизить время простоя процессоров на участках ввода в программный межканальный обмен, и за счет этого провести более глубокий анализ и программное мажоритирование поступающей, внутренней и выдаваемой информации.

Применение систем принудительной аппаратной синхронизации с жесткостью до цикла процессорной шины микроконтроллера [7, 11, 12] позволяет построить многоярусную, аппаратно-мажоритированную структуру бортового компьютера и системы управления, являющуюся лидером по показателю надежности среди систем с жестким регламентом времени [2, 7, 11]. Введение аппаратного межканального сравнения по всем сигналам в ярусах мажоритирования позволяет получить время обнаружения всевозможных дефектов, как бортового компьютера, так и всей системы управления не превышающее одного такта прикладной задачи.

1. Афонин В. В., Лисейкин В. А., Милютин В. В. и др. Синхронизация каналов троированных каналов ПЛК жесткого РВ // Промышленные АСУ и контроллеры.—2001.—№ 6.—С. 58—60.
2. Байда Н. К., Кривоносов А. И., Лысенко И. В. и др. Эволюция отказоустойчивых БЦВК и направления их развития на однокристальных микро-ЭВМ // Системи обробки інформації. — Харків, 2001.—Вип. 4(14).—С. 217—225.
3. Бурцев В. Возможности использования зарубежной элементной базы в системах военного применения // Живая электроника России.—2002.—С. 33—36.
4. Гобчанский О. Применение МісгоРС в вычислительных комплексах специального назначения // СТА.—1997.—№ 1.—С. 38—41.
5. Гобчанский О. Проблемы создания бортовых вычислительных комплексов малых космических аппаратов // СТА.—2001.—№ 4.—С. 28—35.

6. Гобчанский О., Попов В., Николаев Ю. Повышение радиационной стойкости индустриальных средств автоматики в составе бортовой аппаратуры // СТА.—2001.—№ 4.—С. 36—40.
7. Кривоносов А. И., Байда Н. К., Кулаков А. А. и др. Структурно-алгоритмическая организация и модели надежности мажоритарно-резервированных систем // Космічна наука і технологія.—1995.—**1**, № 1.—С. 69—77.
8. Тяпченко Ю., Безроднов В. ПЭВМ на борту пилотируемого космического аппарата // СТА.—1997.—№ 1.—С. 34—37.
9. Уэйкерли Дж. Повышение надежности микро-ЭВМ путем тройного резервирования модулей // ТИИЭР.—1976.—**64**, № 6.—С. 65—78.
10. Уэнсли Дж. Х., Лэмпорт Л., Голдберг Дж. и др. SIFT: Проектирование и анализ отказоустойчивой вычислительной системы для управления полетом летательного аппарата // ТИИЭР.—1978.—**66**, № 10.—С. 26—48.
11. Харченко В. С., Юрченко Ю. Б., Байда Н. К. Реализация проектов отказоустойчивых бортовых компьютеров космических аппаратов с использованием электронных компонент INDUSTRY // Технология приборостроения.—2002.—№ 1.—С. 74—80.
12. Харченко В. С., Юрченко Ю. Б. Повышение отказоустойчивости систем управления на основе мажоритированных вычислительных комплексов с аппаратной синхронизацией // Інформаційно-керуючі системи на залізничному транспорті.—2001.—№ 4.—С. 122—123.
13. Caldwell D. W., Rennels D. A. FTSM: A Fault-Tolerant Spaceborne Microcontroller // Department of Computer Science, 4731 Boelter Hall University of California, Los Angeles, CA 90024, ...http://www.chillarege.com/fastabstracts/ftcs98/382.html.
14. David Ph., Guidal Cl., Development of Fault Tolerant Computer System for the Hermes Space Shuttle // Fault-Tolerant Computing, 1993. FTCS-23. Digest of Papers., The Twenty-Third International Symposium on, Aug. 1993.—P. 641—646.
15. Hagbae Kim, Kang G. Shin Evaluation of Fault Tolerance Latency from Real-Time Application's Perspectives // IEEE Transactions on computers.—2000.—**49**, N 1.—P. 55—64.
16. Harper R. E. and Lala J. H. Fault-Tolerant Parallel Processor // Guidance, Control and Dynamics.—1990.—**14**, N 3.—P. 554—563.
17...http://www.cpm.ru/product/stratus.
18. Kieckhafer R. M., Walter C. J., Finn A. M., et al. The MAFT Architecture for Distributed Fault Tolerance // IEEE Trans. Computers.—1988.—**37**, N 4.—P. 398—405.
19. Melliar-Smith P. M. and Schwartz R. L. Formal Specification and Mechanical Verification of SIFT // IEEE Trans. Computers.—1982.—**31**, N 7.—P. 616—630.
20. Nakamikawa T., Morita Yu., Yamaguchi Sh., et al. High performance fault tolerant computer and its fault recovery // Fault-Tolerant Systems, 1997: Proc. Pacific Rim International Symp. 1997.—P. 2—6.
21. Powell D. Distributed Fault-Tolerance-Lessons from DELTA-4 // IEEE Micro.—1994.—**14**, N 1.—P. 36—47.
22. Powell D., Arlat J., Beus-Dukic L., et al. GUARDS: a generic upgradable architecture for real-time dependable systems // Parallel and Distributed Systems: IEEE Transactions.—1999.—**10**, N 6.—P. 580—599.
23. Prager K., Vahey M., Farwell W., et al. A fault tolerant signal processing computer // Dependable Systems and Networks, 2000. DSN 2000: Proc. Inter. Conf. 2000.—P. 169—174.
24. Roques R.,.Correge A, Boleat C.Fault-tolerant computer for the Automated Transfer Vehicle // Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symp. 1998.—P. 414—419.
25. Scott J. A., Preckshot G. G., Gallagher J. M. Using Commercial-Off-The-Shelf (COTS) Software in High-Consequence Safety Systems // Lawrence Livermore National Laboratory, UCRL122246, 1995.

RELIABILITY INCREMENT OF ONBOARD CONTROL COMPLEXES BY MEANS OF LOCKSTEPPED HARDWARE VOTING MAJORITY FRAMES CONSTRUCTION AT HARDWARE SYNCHRONIZATION OF SINGLE-CHIP MICROCONTROLLERS

Yu. B. Yurchenko

Multi-channel fault-tolerant onboard computer frames of critical application have investigated. Decreasing latent fault detection time at usage hardware synchronization components of processes in channels have defined. Advantage of lockstepped hardware voting majority frames construction with interchannel compare components for control system on top of critical application have demonstrated