УДК 004.27 : 004.052

ФУНКЦИОНАЛЬНЫЕ МОДЕЛИ И СРЕДСТВА ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ НА ОСНОВЕ DA-ТЕХНОЛОГИИ

В.С. Харченко, Ю.Н. Прохорова, Ф.А. Асидех
(Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков)

Анализируются принципы обеспечения отказоустойчивости на базе Stratus-архитектур и пути их совершенствования на основе DA (Dependable Availability)-технологии – третьего этапа развития технологий высокой готовности. Предлагаются функциональные модели многоканальных компьютерных систем (КС), на основе которых возможно создание средств реализации данной технологии.

отказоустойчивость, DA-технология, много канальная система

Введение. Проблема обеспечения отказоустойчивости КС. Несмотря на увеличение избыточности каналов и введение специальных средств поддержки отказоустойчивости, в Stratus-структурах имеют место недостатки [1 – 4]. Это, прежде всего, недостаточная защита от отказов, обусловленных дефектами программного обеспечения (ПО), потеря работоспособности при наложении отказов двух каналов. Они связаны с невозможностью парирования части дефектов проектирования прикладных программ и потерей работоспособности при возникновении сбоев или отказов элементов каналов, принадлежащих разным подсистемам. Решением этих проблем может стать внедрение встроенных средств контроля и реконфигурации резервированной системы на основе *DA-технологии* [3].

Проанализировав последние публикации в сфере отказоустойчивых систем можно прийти к выводу, что уже существующие *HA-* и *CA-технологии* высокой готовности отказоустойчивых систем [2] не решают проблему выявления отказов программных версий. Хотя существуют решения, способные парировать последовательности из двух подряд идущих отказов аппаратных средств [5], отсутствуют методы и средства (в рамках Stratus-структур) обнаружения отказов программных версий.

Целью статьи является анализ технологий высокой готовности на базе отказоустойчивых Stratus-систем и разработка усовершенствованных архитектур и алгоритмов функционирования.

Эволюция технологий высокой готовности. Применительно к бизнес-критическим компьютерным системам можно выделить следующие этапы эволюции технологий высокой готовности, исходя из процентного соотношения плановых и неплановых простоев для устранения отказов и обслуживания [2, 6, 7] (рис.1).

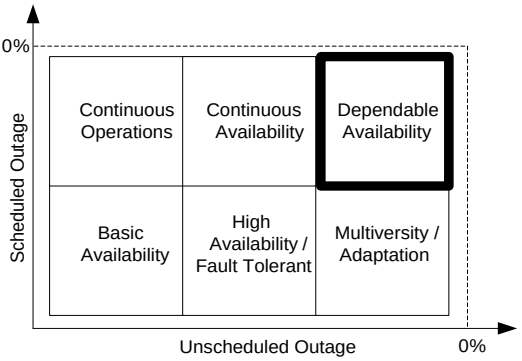

Рис. 1. Эволюция технологий высокой готовности

Первый из них основывается на переходе от обычного дублирования (принципа “Достоверное обнаружение”) к мажоритированию (принципу “Надежное парирование”). Он получил название “*High Availability”* (высокая готовность) или *HA-технологии* Недостатки дублированных и мажоритарных структур хорошо известны: дублирование – потери времени на восстановление, так как невозможно восстановление без прерывания; требуются дополнительные программные средства реконфигурации; низкая надежность защиты от отказов ПО; мажоритирование – проблемы рассинхронизации каналов; трудности при программировании; потеря работоспособности при наложении сбоев; усложнение средств мажоритирования.

Второй этап эволюции связывают с появлением и развитием многоканальных дублированных структур, в рамках *CA-технологии* (“*Continuous Availability”* – постоянная готовность). В этих структурах каждая из подсистем построена по дублированной схеме и отключается при отказе любого из блоков. Примером реализации такой технологии является архитектуры многоканальных дублированных систем (МДС) семейства Stratus (ftServer и Continuum). При этом обеспечивается возможность оперативного ремонта каналов при отказе одной из подсистем.

Следующим этапом развития можно назвать *DA-технологию* (*“Dependable Availability”* – надёжная готовность) [3], которая основана на сочетании *CA-технологии* с многоверсионностью, обеспечением устойчивости к двум и более отказам, введением подсистем парирования проявлений дефектов программных средств без принудительного выключения системы.

Проанализируем принципы обеспечения отказоустойчивости на основе Stratus-технологий (система может называться отказоустойчивой только в том случае, если ни один из ее компонентов не может привести к нарушению работоспособности системы в целом). Корпорация Stratus Technologies создала серии серверов ftServer и Continuum.

Семейство отказоустойчивых серверов ftServer. Каждый ftServer использует полностью дублированную, отказоустойчивую архитектуру для предотвращения сбоев и сохранения целостности данных [3, 4]. Сдвоенные процессоры и модули памяти работают параллельно, в жесткой связи, синхронно выполняя одни и те же инструкции в одно и то же время, не снижая производительность системы. При отказе какого-либо компонента обработка данных не прерывается, не происходит потерь данных или снижения производительности, так как предусмотрена горячая замена аппаратных компонент.

Серверы ftServer поставляются в двух конфигурациях: с двойной (Dual Modular Redundant, DMR) и тройной избыточностью (Triple Modular Redundant, TMR). В DMR-моделях используются два жестко связанных модуля процессор-память, а модели TMR содержат по три таких подсистемы. В обеих моделях резервированные системные платы выполняют все инструкции в жестком режиме синхронизации. Если специализированная цепь какой-либо системной платы обнаруживает ошибку, эта системная плата немедленно изолируется от системы и исключается из работы. На втором уровне обнаружения ошибок происходит сравнение выходной информации каждой подсистемы процессор-память для каждой операции ввода-вывода.

Семейство отказоустойчивых серверов Continuum. Компания Stratus Technologies позиционирует семейство Continuum как системы, обеспечивающие непрерывную доступность [3, 4]. Серверы Stratus Continuum делятся на 3 серии – 400, 600 и 1200, имеют высокую производительность и постоянную доступность. Дублированная архитектура Continuum 400 позволяет системе полностью сохранять работоспособность в случае единичных отказов. Серии 600 и 1200 являются отказоустойчивыми системами, в которых, прежде всего, следует отметить дублирование всех основных архитектурных блоков.

Компьютеры Stratus находят широкое применение в критических и бизнес-критических приложениях. Однако, применение *HA-* и *CA-технологии* в этой системе обуславливает необходимость:

– достижения более высоких показателей непрерывной безотказности с учетом аппаратных и программных компонент, в том числе обеспечением устойчивости к двум и более отказам;

– введения подсистем парирования проявлений дефектов программных средств без принудительного выключения системы.

С появлением *DA-технологии* становится возможным создание устройств, частично устраняющих перечисленные недостатки.

Структурно-функциональные модели многоканальных дублированных структур (МДС). Модели, позволяющие синтезировать множество отказоустойчивых архитектур [3], представлены на рис. 2 – рис. 5, где K_{ij} – каналы системы i = 1, ... , n (n – четное), j = 1, 2. Каналы K_{ij} объединяются в подсистемы B_j, φ_C, φ_U, φ_K – функции сравнения (контроля), управления реконфигурацией и коммутации выходов соответственно.

Модель (рис. 2) характеризуется тремя типами связей:

– информационные, по которым циркулируют данные на выходах каналов K_{ij} – I_{ij} и на выходах системы – I, показаны сплошными линиями;

– управляющие (сигналы U, пунктирные линии);

– диагностические (сигналы от схем сравнения c_i и диагноза D, точечные линии).

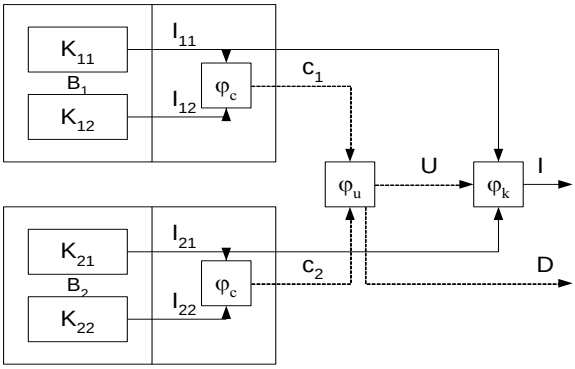

Рис. 2. Структурно-функциональная модель базовой МДС

Если внутриподсистемный контроль (ВПК) содержит все подсистемы, будем называть его полным. Элементы, реализующие функции φ_C, формируют сигналы c_1, c_2 (рис. 2) совпадения (c = 0) или несовпадения (c = 1) данных и выполняют функцию в данном случае внутриподсистемного контроля (ВПК). В соответствии с его результатами осуществляется реконфигурация структуры. В соответствии с управляющим сигналом U (функцией коммутации) реализуется и функция φ_K.

Сигнал диагноза D включает информацию о работоспособности (исправности) системы, отказавших подсистемах B_j и каналах K_{ij}, а также (при наличии средств самопроверки) о работоспособности части системы, выполняющей функции.

МДС, описываемая моделью на рис. 2, позволяет обнаружить любой единичный отказ в каждой подсистеме (отказ одного из каналов) и локализовать отказ любых подсистем. Если сравниваются данные только одной пары каналов подсистем B_i, B_k, будем называть такую МДС системой с минимальным межподсистемным контролем (МПК). Ее структурно-функциональная модель представлена на рис. 3.

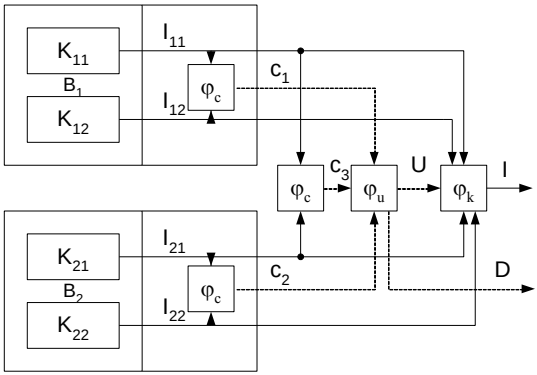

Рис. 3. Структурно-функциональная модель МДС
с минимальным межподсистемным контролем

Если сравниваются данные двух любых разных пар каналов подсистем B_i, B_k, (K_{i1}, K_{k1}, и K_{i2}, K_{k2}, или K_{i1}, K_{k2}, и K_{i2}, K_{k1}), такую систему будем называть МДС с базовым МПК. Если сравниваются данные всех пар каналов подсистем, такую систему будем называть МДС с полным МПК. Структурно-функциональные модели МДС с базовым и полным МПК представлены на рис. 4, 5.

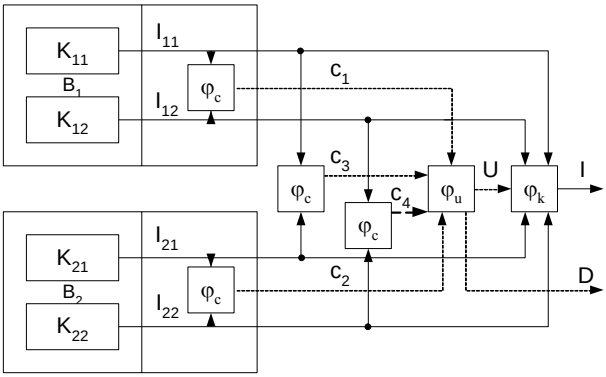

Рис. 4. Структурно-функциональная модель МДС
с базовым межподсистемным контролем

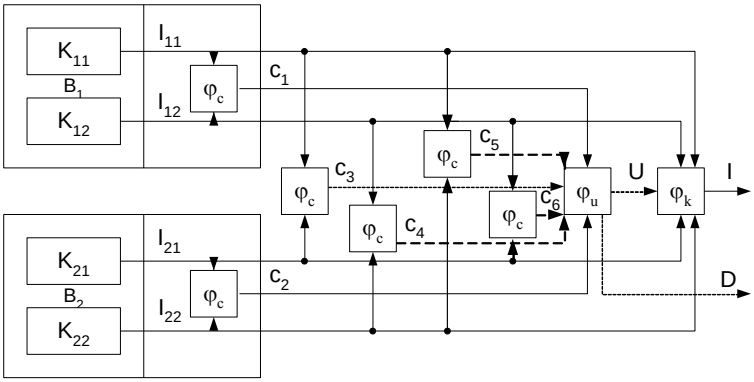

Рис. 5. Структурно-функциональная модель МДС
с полным межподсистемным контролем

Средства реализации *DA-технологии.* Существует возможность создания устройств для контроля и реконфигурации резервированной системы [5] на основе *DA-технологии* по структурно-функциональной схеме, показанной на рис. 3. Предполагается наличие четырех режимов работы (отсутствие отказов каналов системы, первого отказа одного из каналов, второго отказа, третьего отказа – отказа системы), введение межподсистемного контроля и обеспечение устойчивости к любой последовательности из двух одиночных отказов каналов. Использование многоверсионного (двухверсионного) ПО дает возможность обнаружить некоторые отказы ПО, но существует необходимость вводить встроенные средства контроля программных компонент.

Состояния резервированных блоков при различной последовательности отказов каналов и версий ПО показаны в табл. 1, табл. 2. Обозначения K_{11}, K_{12}, K_{21}, K_{22} соответствуют резервированным блокам, код отказа $<c_3\ c_2\ c_1>$ – выходам блоков сравнения. Код коммутации – $<w_4\ w_3\ w_2\ w_1>$, код диагностирования – $<d_4\ d_3\ d_2\ d_1>$. Обозначению НФ соответствует состояние неконтролированного функционирования, ПС 1, 2 – отказы первой и второй подсистем, которые состоят из первого 1, второго 2 и третьего 3, четвертого 4 резервированных блоков соответственно.

Из табл. 1 видно, что при первом отказе – отказ канала K_{11} (ситуация 1) система не прекращает своей работы, данные снимаются с канала K_{21}. Во второй момент времени происходит отказ канала K_{12}, система также не прекращает своей работы, данные снимаются с канала K_{21}. Так как отказавшие каналы находятся в одной подсистеме, то генерируется соответствующая комбинация, сигнализирующая об отказе первой подсистемы. В табл. 2 показан случай, когда в первый момент времени происходит от-

каз ПО. Обозначения A и B демонстрируют наличие различных версий ПО соответствующих каналов. Анализ показывает, что можно точно определить, что произошел отказ программного обеспечения, но установить отказавшую версию нельзя. Следовательно, в этом случае работа системы должна быть остановлена и зафиксирован ее отказ.

Таблица 1

Последовательность отказов: первый отказ HW, второй отказ HW

№ ситуации	Первый отказ				Второй отказ				Диагност. сигналы D
	Отказавший канал K_{ij}	Код отказа $<c_3c_2c_1>$	Код коммут. $<w_4w_3w_2w_1>$	Выход канала K_{ij}	Отказавший канал K_{ij}	Код отказа $<c_3c_2c_1>$	Код коммут. $<w_4w_3w_2w_1>$	Выход канала K_{ij}	
1	K_{11}	101	0010	K_{21}	K_{12}	101	0010	K_{21}	ПС1
2	K_{11}	101	0010	K_{21}	K_{21}	111	0100	K_{12}	НФ
3	K_{11}	101	0010	K_{21}	K_{22}	111	0100	K_{12}	НФ
4	K_{12}	001	0010	K_{21}	K_{11}	101	0010	K_{21}	ПС1
5	K_{12}	001	0010	K_{21}	K_{21}	111	0001	K_{11}	НФ
6	K_{12}	001	0010	K_{21}	K_{22}	011	0001	K_{11}	НФ
7	K_{21}	110	0001	K_{11}	K_{11}	111	1000	K_{22}	НФ
8	K_{21}	110	0001	K_{11}	K_{12}	111	1000	K_{22}	НФ
9	K_{21}	110	0001	K_{11}	K_{22}	110	0001	K_{11}	ПС2
10	K_{22}	010	0001	K_{11}	K_{11}	111	0010	K_{21}	НФ
11	K_{22}	010	0001	K_{11}	K_{12}	011	0001	K_{11}	НФ
12	K_{22}	010	0001	K_{11}	K_{21}	110	0001	K_{11}	ПС2

Таблица 2

Последовательность отказов (двухверсионное ПО): первый отказ SW

Тип системы	№ Ситуации	Первый отказ		Диагностические сигналы D
		Отказавший канал K_{ij}	Код отказа $<c_3c_2c_1>$	
AB; AB	1	K_{11}, K_{21}	011	Отказ SW
	2	K_{12}, K_{22}	011	Отказ SW
AA; BB	1	K_{11}, K_{12}	100	Отказ SW
	2	K_{21}, K_{22}	100	Отказ SW

Для таких систем невозможно идентифицировать случай, когда в первый момент времени происходит аппаратный отказ, а во второй момент времени – программный отказ. Поэтому должны быть введены до-

полнительные средства, позволяющие идентифицировать состояния системы (переход от структурно-функциональной модели МДС с минимальным межподсистемным контролем (рис. 3) к моделям с базовым (рис. 4) или полным (рис. 5) межподсистемным контролем). Другим возможным решением является переход к структурам с трехверсионным ПО.

Выводы. В статье предлагаются принципы и модели, используя которые становится возможным создание устройств для контроля и реконфигурации резервированной системы на основе *DA-технологии*, частично решающих проблему недостаточной защиты от отказов ПО, невозможности парирования дефектов проектирования прикладных программ и потери работоспособности при наложении сбоев или отказов элементов каналов, принадлежащих разным подсистемам. Подобные устройства могут быть встроены в стандартную архитектуру многоканальной дублированной вычислительной системы, выполненной на основе Stratus-технологии.

ЛИТЕРАТУРА

1. *[Электр. ресурс]. – Режим доступа: www.stratus.com.*
2. *Bartlett W., Spainhower L. Commercial Fault Tolerance: A Tale of Two Systems // IEEE Transactions on Dependable and Secure Computing. – 2004. – № 1. – P. 87 – 96.*
3. *Харченко В.С., Асидех Ф.А. STRATUS-системы для энергетических комплексов гарантированной готовности: компонентная модель, свойства и метод адаптации // Вісник Харківського державного технічного університету сільського господарства "Проблеми енергозбереження та енергозабезпечення в АПК України". – Х.: Міністерство аграрної політики України. – Вип. 27. – Т. 2. – С. 206 – 209.*
4. *Харченко В.С., Асидех Ф.А. Методы повышения отказоустойчивости бизнес-критических компьютерных систем с использованием многоверсионных STRATUS-технологий. //Открытые информационные и компьютерные интегрированные технологии. – Х.: НАКУ «ХАИ», 2003. – №19. – С. 45 – 54.*
5. *Харченко В.С., Асидех Ф.А. Устройство для контроля и реконфигурации резервированной системы. Патент. – G06F 11/18, HO5K10/00.*
6. *Littlewood B., Miller D.R., Conceptual Modeling of Coincident Failures in Multi-Version Software // IEEE Transactions on Software Engineering. – 1989. – SE-15 (12). – P. 596 – 614.*
7. *Dobson J.E., Randell B., Building Reliable Secure Computing Systems Out of Unreliable Insecure Components // in Proceedings of the Conference on Security and Privacy. – 1986. – P. 187 – 193.*

Поступила 12.11.2005

Рецензент: доктор технических наук, профессор В.М. Илюшко,

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ».