инженерия программного обеспечения

Кривошеин Борис Николаевич

УДК 004.414.2

ПРОЕКТИРОВАНИЕ СЕТЕВЫХ КОМПЬЮТЕРНЫХ СИСТЕМ ПО ТРЕБОВАНИЯМ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Аннотация

Электронные устройства, обладающие высоким уровнем функциональной безопасности, могут быть построены только на основе избыточных аппаратных архитектур. Для сложных систем с высокоскоростными сетевыми интерфейсами предпочтительной является архитектура «2 из 3» (2oo3, TMR) и её модификации. Решения с применением мажорирующих элементов обеспечивают высокую надёжность сетевого вычислителя без ущерба для производительности. В статье рассмотрены методики расчётов показателей надёжности сетевых вычислителей и практические примеры их реализации.

Ключевые слова: отказоустойчивый вычислитель, мажорирование, тройная модульная избыточность, TMR, 2oo3, функциональная безопасность.

Компьютерные системы всё чаще используются для решения задач, связанных с обеспечением безопасности. В большинстве ситуаций безопасность достигается за счет использования систем защиты, включающих датчики, исполнительные механизмы и электронные системы управления. Подходы к построению систем, гарантирующих функциональную безопасность, подробно исследованы и изложены в серии стандартов IEC 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». В России адаптированный вариант IEC 61508 был принят как национальный стандарт ГОСТ Р МЭК 61508 [1].

Вне всякого сомнения, данный стандарт может применяться в отношении любых компьютерных систем, отказ которых может быть опасен для людей, окружающей среды или дорогостоящих объектов управления. В то же время разнообразие реальных систем управления и обработки данных очень велико и не всегда соответствует традиционной модели «датчики – контроллер – схема защиты». Современные технологии передачи данных позволяют строить распределенные системы со сложной сетевой топологией на базе компьютеров и оконечных устройств с сетевыми интерфейсами. Для таких систем требуется специальная интерпретация положений стандарта [1] для обеспечения требуемого уровня надежности.

Стандарт [1: часть 4, п. 3.3.2] определяет программируемую электронную систему как систему для управления, защиты или мониторинга, основанную на использовании одного или нескольких программируемых электронных устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магист-

рали данных и другие каналы связи, устройства привода и другие устройства вывода.

В данной работе мы будем рассматривать сетевую распределенную систему, которая полностью соответствует данному определению и при этом обладает следующими особенностями:

– программируемые электронные устройства системы связаны между собой, а также с устройствами ввода и вывода посредством одного или нескольких высокоскоростных каналов пакетной передачи данных (для определенности в данной работе рассматривается сеть стандарта Ethernet 100 со стеком протоколов TCP/IP, но все выводы могут быть применены и к альтернативным сетевым технологиям);

– каждое электронное устройство системы в непрерывном режиме выполняет функции приема, обработки и передачи данных по сети Ethernet во взаимодействии с другими сетевыми устройствами;

– система имеет высокие требования по уровню производительности, что приводит к применению сложных инженерно-технических решений при проектировании её узлов;

– система в целом реализует функции безопасности, и любой сбой в процессах обработки и передачи данных от источника до конечного получателя является потенциально опасным событием.

Опасным отказом на уровне системы в этом случае следует считать любое из двух событий:

– получение оконечным устройством недостоверных результатов обработки, таких что ошибка не будет обнаружена средствами внутренней диагностики;

– неполучение оконечным устройством достоверных результатов обработки в течение заданного времени.

Достижение требуемого уровня полноты безопасности зависит как от надежности каждого элемента, так и от архитектуры системы в целом. Мы рассмотрим оба этих аспекта в части аппаратных средств для систем с требованиями по уровню полноты безопасности SIL3/SIL4 *(SIL = Safety Integrity Level – Уровень Полноты Безопасности)*. Надежность программных средств является важной составляющей безопасности системы, но этот вопрос выходит за рамки данной статьи.

Стандарт [1: часть 2, п. 7.4.3] содержит требования к полноте безопасности аппаратных средств и определяет архитектурные ограничения. По положениям стандарта, уровень полноты безопасности ограничивается отказоустойчивостью аппаратных средств и долей безопасных отказов подсистем, которые выполняют функцию безопасности. По определению, отказоустойчивость аппаратных средств уровня N означает, что отказ $N + 1$ подсистемы может привести к потере функции безопасности. Для определения архитектурных ограничений стандарт разделяет аппаратные средства на типы A и B. По стандарту [1: часть 2, п. 7.4.3.1.2] конкретная подсистема может быть отнесена к типу A, если для ее компонентов, необходимых для реализации функции безопасности:

a) виды отказов всех составляющих компонентов определены,

b) поведение системы в условиях отказа может быть полностью определено,

c) имеются достоверные эксплуатационные данные, показывающие, что частоты, требуемые для обнаруженных отказов и необнаруженных опасных отказов, реализованы.

Если хотя бы одно из этих условий не выполняется, то подсистема должна быть отнесена к типу B.

Мы будем рассматривать системы типа B, так как поведение сложных программируемых электронных устройств в условиях отказа не может быть полностью определено, и это

Табл. 3. Полнота безопасности аппаратных средств: архитектурные ограничения подсистем, связанных с безопасностью типа B

Доля безопасных отказов	Отказоустойчивость аппаратных средств		
	$N = 0$	$N = 1$	$N = 2$
< 60 %	Не оговаривается	SIL1	SIL2
60–90 %	SIL1	SIL2	SIL3
90– 99%	SIL2	SIL3	SIL4
≥ 99 %	SIL2	SIL4	SIL4

является критерием для их классификации по данному типу. Ограничения для аппаратных средств типа B приведены в следующей таблице ([1: часть 2, п. 7.4.3.1.4, табл. 3].

Как следует из приведенной таблицы, для систем с требованиями к уровню полноты безопасности SIL3 или SIL4 необходимо иметь уровень отказоустойчивости не менее 1. Другими словами, любой одиночный отказ аппаратуры не должен приводить к опасному событию в системе. Кроме того, для уровня SIL4 необходимо обеспечить долю безопасных отказов не ниже 99 % для отказоустойчивости $N = 1$ и не ниже 90 % для $N = 2$.

Требование по минимальному уровню отказоустойчивости $N = 1$ ограничивает выбор возможных архитектур при разработке аппаратной платформы. Стандарт [1: часть 6, приложение B] рассматривает следующие базовые архитектуры аппаратных средств: 1oo1, 1oo2, 2oo2, 1oo2D, 2oo3 (запись XooY означает, что в составе устройства имеется Y каналов, и для нормального функционирования устройства достаточно корректной работы X из них, запись XooYD используется для архитектуры XooY со встроенной диагностикой). Архитектуры 1oo1 и 2oo2 не удовлетворяют критерию устойчивости к одиночным отказам. Для архитектуры 1oo2 без диагностики её реализация в рамках системы, основанной на сетевых компьютерных технологиях, представляется в общем случае невозможной. По определению стандарта [1], данная архитектура представляет собой два канала, соединенных параллельно, так что любой из каналов может выполнить функцию безопасности. Следовательно, для нарушения функции безопасности опасные отказы должны возникнуть в обоих каналах. Обычно данная архитектура применяется в системах с двумя независимыми схемами защиты, подключенными к каждому из каналов, при том что срабатывание любой из этих схем означает выполнение функции безопасности. Для рассматриваемой нами системы одной из разновидностей опасного отказа является выдача в канал управления информационного пакета, содержащего искаженные данные. Получатель такого пакета не сможет диагностировать ошибку даже в случае получения по параллельному каналу правильного пакета. При возникновении ошибки в вычислениях до фазы защиты данных избыточным кодированием для передачи в канал связи получатель примет два различных набора данных без каких-либо критериев выбора одного правильного. Блокировка обоих информационных пакетов будет означать неполучение оконечным устройством достоверных результатов, что в нашем случае также относится к потенциально опасным событиям.

Таким образом, выбор базовой архитектуры для сетевой аппаратуры уровней SIL3/4 ограничен вариантами 1oo2D и 2oo3. Рассмотрим оба этих варианта.

Согласно стандарту [1: часть 6, прил. B, п. 2.2.4], архитектура 1oo2D представляет собой два канала, соединенных параллельно. При нормальной работе для выполнения функции безопасности необходимы оба канала. Кроме того, если диагностическое тестирование обнаруживает отказ в любом канале, то результаты анализа устанавливаются так, чтобы общее выходное состояние совпадало с результатом, выдаваемым другим каналом.

В применении к сетевому устройству данное определение означает, что при нормальной работе каждый из каналов устройства передает идентичные информационные пакеты. При отказе одного из каналов его средства внутренней диагностики препятствуют передаче искаженной информации, и на выход передаётся только пакет из исправного канала. Данную схему можно рассматривать как соединение двух архитектур: в исходном состоянии система работает, как 2oo2, однако частичный отказ любого из каналов приводит не к общему отказу, а к деградации к архитектуре 1oo1. Таким образом, отказоустойчивость системы 1oo2D равна 1, и этого достаточно для уровней полноты безопасности SIL3/4 при обеспечении должного соотношения опасных и безопасных отказов.

Архитектура 2oo3, согласно стандарту [1: часть 6, прил. B, п. 2.2.5], состоит из трех каналов, соединенных параллельно с мажо-

рированием выходных сигналов, так что выходное состояние не меняется, если результат, выдаваемый одним из каналов, отличается от результата, выдаваемого двумя другими каналами. Для сетевого устройства в роли «выходных сигналов» выступают информационные пакеты, генерируемые каждым из каналов, а мажорирование может выполняться путем сравнения их содержимого. В случае любой одиночной ошибки происходит деградация системы к архитектуре 2oo2, следующая ошибка приводит к общему отказу. Отказоустойчивость архитектуры 2oo3 равна 1, как и для 1oo2D.

Оценка полноты безопасности зависит от нескольких характеристик, таких как полнота диагностического покрытия, интервал между контрольными испытаниями, среднее время ремонта, доля отказов с общей причиной. Отказ с общей причиной определён в стандарте [1: часть 4, п. 3.6.10] как «Отказ, который является результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной системе, ведущие к отказу системы». В этой же части стандарта можно найти формальные определения всех терминов, используемых в других частях стандарта [1].

Оценим интенсивности отказов и потенциальный уровень полноты безопасности систем с архитектурами 1oo2D и 2oo3, исходя из следующих предположений:

– непрерывный режим работы;

– диагностическое покрытие (уровень обнаруживаемых опасных отказов) DC = 99 %;

– интенсивность отказов для 1 канала подсистемы $\lambda = 1 \cdot 10^{-5}$ (данный параметр выбран как типичный для современных программируемых контроллеров промышленного назначения без встроенной избыточности);

– доля отказов, обнаруженных диагностическими тестами и имеющих общую причину, равна $\beta_D = 1$ %;

– доля необнаруженных отказов по общей причине равна $\beta = 2$ %;

– интервал между контрольными испытаниями – 1 мес.;

– среднее время ремонта – 8 час.

Для данных параметров вероятность отказа в час составляет [1: часть 6, прил. B.3.3, табл. B.10]:

– архитектура 1oo2D: $\lambda = 5{,}1 \cdot 10^{-8}$;

– архитектура 2oo3: $\lambda = 5{,}2 \cdot 10^{-8}$.

В соответствии со стандартом [1: часть 1, п. 7.6.2.9., табл. 3], данная интенсивность отказов соответствует уровню полноты безопасности SIL3 для обеих архитектур.

Для принятия решения о выборе архитектуры разработчику необходимо ответить на ряд вопросов:

1. Если уровня полноты безопасности SIL3 достаточно для разрабатываемой системы, то:

- Какие технические решения необходимы для безопасного перехода от полной конфигурации системы к частичной при отказе одного из каналов, и обратно – после ремонта?
- Как реализовать систему диагностики, гарантирующую нужный уровень диагностического покрытия?
- Как снизить до требуемого уровня долю отказов по общей причине?
- Как гарантировать независимость работы каналов и не допустить отказа по общей причине вследствие внутренней ошибки в одном из них?

2. Если необходим уровень полноты безопасности SIL4, то какие существуют возможности достижения этого уровня, кроме увеличения надежности аппаратуры каждого из каналов?

Решение этих задач в значительной степени зависит от архитектуры, для которой они предназначены. Первый вопрос, относящийся к любой архитектуре, – как обеспечить соответствие реализации тому определению архитектуры, которое используется при расчетах надежности? Для архитектуры 1oo2D критичной является диагностика канала. Некорректная работа схемы диагностики может привести к выдаче каналом искаженной информации с последующим общим отказом, как в схеме 2oo2. При высокой сложности аппаратуры канала схемы контроля, основанные на механизмах сторожевых таймеров, косвенных проверках и периодическом внутреннем тестировании,

не могут гарантировать отсутствие одиночного сбоя при выполнении арифметических или логических операций. Высокая достоверность диагностики в сложных устройствах может быть достигнута лишь одним способом – проведением вычислений параллельно на нескольких аппаратных блоках с последующим сравнением результатов. Различные результаты вычислений при этом интерпретируются как обнаружение отказа при диагностике и приводят к блокировке канала. Системы с такой организацией иногда объявляются разработчиками, как системы «архитектуры 2oo4», однако следует признать, что такая характеристика не соответствует стандарту [1]. Во-первых, общее число каналов такой системы – 2, а не 4, и, во-вторых, корректной работы 2 из имеющихся 4 вычислителей такой системы будет недостаточно, если они находятся в разных каналах. Более правильно будет отнести данную архитектуру к классу 1oo2D, в которой каждый из составляющих каналов, в свою очередь, имеет внутреннюю архитектуру 2oo2. Данная внутренняя архитектура обеспечивает необходимый уровень достоверности диагностики канала, но в то же время она обладает рядом недостатков. Дублирование вычислений в каждом канале на практике приводит к удвоению аппаратных ресурсов. При том же уровне надежности каждого комплекта аппаратуры, вероятность отказа канала удваивается (см. [1: часть 6, п. 3.2.3]). Итоговая интенсивность отказов в час для всей системы 1oo2D при тех же входных параметрах может быть оценена на уровне $\lambda = 1 \cdot 10^{-7}$. Данное значение является пограничным между уровнями полноты безопасности SIL3 и SIL2 [1: часть 1, п. 7.6.2.9., табл. 3]. Кроме того, при построении такой системы следует обратить особое внимание на схему сравнения подканалов и блокировки модуля, обеспечивающую переход модуля в безопасное состояние в случае ошибки. Отказ подсистемы контроля может привести к опасному отказу всей системы, поэтому в общей схеме надежности она должна рассматриваться как отдельный последовательный элемент и ее интенсивность отказов должна быть не выше, чем задано для полной системы. На практике такой уровень надежности потребует введения избыточности на уровне схем контроля, решения для этой подсистемы проблем, связанных с возможными отказами общего характера, и в целом доказательство соответствия системы нужному уровню SIL может оказаться очень затруднительным.

Архитектуры 2oo3, как было показано выше, обеспечивают тот же порядок надежности, что и 1oo2D при одинаковых расчетных параметрах, однако, с точки зрения реализации сетевых компьютерных систем, они обладают рядом преимуществ. Определение архитектур в стандарте [1: часть 6, прил. B] не содержит никаких сведений о природе объекта, объединяющего каналы в единое выходное состояние, описаны лишь абстрактные свойства такого объединения. Для архитектуры 2oo3 таким свойством является выдача результата, совпадающего с двумя каналами из трёх. На практике эта схема реализуется простым сравнением трёх входных каналов с выбором совпадающей пары, и для работы такой системы не требуется никаких внешних условий. Кроме этого, обеспечивается мгновенная диагностика отказавшего канала. Архитектура 1oo2D таким свойством не обладает. Для реализации необходимой функции объединения требуется внешняя схема диагностики, определяющая правильный канал в случае расхождения данных. Как было показано выше, построение такой диагностической схемы может быть сопоставимо по сложности с разработкой функциональной аппаратуры канала.

Для архитектур 2oo3 мажорирующий узел также не является абстрактным идеальным элементом и обладает определенной интенсивностью отказов, влияющей на общую надежность. В то же время возможна реализация модели архитектуры 2oo3, которая исключает распространение отказа любого элемента аппаратуры, включая схемы мажорирования, на выходную функцию системы и поддерживает все основные принципы отказоустойчивости.

Стратегии реализации систем с аппаратной избыточностью основаны на нескольких базовых принципах, которые просто форму-

лируются, но точно им следовать бывает весьма непросто. Рассмотрим эти принципы и механизмы их влияния на вероятность отказов целевой системы с архитектурой 2oo3. Для расчета вероятности отказа в час будем пользоваться методикой, определенной в стандарте [1: часть 6, прил. В, п. 3.2.5]:

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC),\ \lambda_{DD} = \frac{\lambda}{2} DC\ ; \quad (1)$$

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}; \quad (2)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DU}}{\lambda_D} MTTR; \quad (3)$$

$$PFH_G = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)]\lambda_{DU}]^2 t_{CE} + \\ + \beta_D \lambda_{DD} + \beta\lambda_{DU}\ , \quad (4)$$

где:

T_1 – интервал времени между процедурами тестирования, ч,

$MTTR$ – среднее время восстановления, ч,

DC – диагностическое покрытие, дробь,

β – доля необнаруженных отказов по общей причине,

β_D – доля обнаруженных отказов по общей причине,

λ – интенсивность отказов для канала подсистемы, отказ/ч,

PFH_G – вероятность отказа для группы голосующих каналов, отказ/ч,

λ_D – интенсивность опасных отказов для канала подсистемы, отказ/ч,

λ_{DD} – интенсивность обнаруженных опасных отказов для канала подсистемы, отказ/ч,

λ_{DU} – интенсивность необнаруженных опасных отказов для канала подсистемы, отказ/ч,

t_{CE} – эквивалентное среднее время простоя канала (это объединенное время простоя для всех компонентов канала подсистемы), ч.

Базовые принципы реализации систем с аппаратной избыточностью:

- Нет одинарных точек отказа: функции любого элемента системы резервируются;

Данный принцип обеспечивает соответствие реализации системы типам архитектур XooY, где X < Y. Как было показано выше, все решения, обеспечивающие высокие уровни полноты безопасности, относятся к этим типам архитектуры.

- Нет одинарных точек восстановления: возможна «горячая замена» любого компонента системы без остановки ПО.

Обеспечивается возможность ремонта в оперативном режиме, что позволяет снизить среднее время восстановления и показатель эквивалентного среднего времени простоя канала t_{CE}. Кроме того, остановка управляющего ПО в системах с постоянной готовностью требует переключения на резервную систему. Это является дополнительным фактором риска, так как при передаче управления возможен отказ общего характера вследствие человеческой ошибки. В формуле (4) данное обстоятельство пришлось бы учесть, увеличив параметр β.

- Восстановление после ошибки: система обеспечивает автоматическое реконфигурирование без остановки ПО.

Данный принцип позволяет резко сократить эквивалентное среднее время простоя t_{CE} за счет быстрого восстановления полной конфигурации системы после ошибок, не связанных с постоянным отказом аппаратуры.

- 100 % обнаружение ошибок: все транзакции внутри системы защищены схемами контроля.

Обеспечивается уровень диагностического покрытия (DC), близкий к 1, и, соответственно, – близкая к 0 интенсивность необнаруженных опасных отказов λ_{DU}, что, в свою очередь, уменьшает эквивалентное среднее время простоя t_{CE}.

- 100 % локализация ошибок: обеспечивается идентификация вызвавшего ошибку компонента и его восстановление либо изоляция.

Является необходимым условием для безопасного проведения ремонта в оперативном режиме. Неточная локализация отказавшего узла может привести к ошибочным операциям при ремонте с возможным отказом рабочего канала и системы в целом.

- Ограничение распространения последствий: сбой или отказ компонента не блокирует работу других компонентов и системы в целом.

Влияние отказа канала на работу всей системы может привести к возникновению отказа по общей причине и должно быть учтено путем увеличения параметра β, что приведет к резкому увеличению интенсивности отказов.

При строгом следовании данным принципам можно реализовать систему архитектуры 2oo3, для которой значения параметров β, β_D и $(1 - DC)$ пренебрежимо малы. В этом случае, принимая их равными нулю в формуле (4), а также принимая $\lambda_D = \lambda$ (все отказы являются опасными), получим следующую оценку вероятности отказа системы, связанного с аппаратными средствами:

$$PFH_G = 6\lambda^2 \cdot MTTR . \qquad (5)$$

Эта же формула для систем с архитектурой 2oo3 приведена в таблице «Приближенные формулы для определения интенсивности отказов восстанавливаемых параллельных систем» стандарта [2: табл. B.2]. В терминах стандарта [2] система с архитектурой 2oo3 может быть выражена следующей диаграммой состояний и переходов.

На рис. 1 обозначения состояний 3, 2 соответствуют количеству исправных каналов системы в работоспособном состоянии и 0 – состоянию отказа.

Подставив в (5) значения интенсивности отказов в час одного канала $\lambda = 1 \cdot 10^{-5}$ и среднего времени ремонта $MTTR \equiv \mu = 8$ ч, получаем оценку для $PFH_G = 4{,}8 \cdot 10^{-9}$.

В соответствии со стандартом [1: часть 1, п. 7.6.2.9., табл. 3], данная интенсивность отказов соответствует уровню полноты безопасности SIL4.

Компьютерные системы на основе архитектуры 2oo3 широко используются разработчиками оборудования ответственного назначения. Компания RTP Corporation (США) поставляет системы 3000 SIS с архитектурой ядра 2oo3, сертифицированные по уровню функциональной безопасности SIL3. По данным производителя, среднее время наработки на отказ данной системы (MTBF) составляет не менее 2500 лет [3], что соответствует вероятности отказа $PFH_G = 4{,}56 \cdot 10^{-8}$. Система 3000 SIS содержит 3 узловых процессора (Node Processors), обеспечивающих мажорированную обработку информации и до 16 периферийных процессоров (Chassis Processors), выполняющих операции обмена данными по входным и выходным каналам системы. Периферийные процессоры могут контролировать целостность данных на внешних каналах за счет объединения в логические группы с архитектурой 1oo2D.

Другая известная компания на рынке систем, критичных для безопасности – Rockwell Automation, Inc. (США, подразделение ICS Triplex) выпускает отказоустойчивые вычислительные комплексы Trusted™, в составе которых могут быть установлены 2 вычислительных модуля T8110D, каждый из которых имеет архитектуру 2oo3 [4, 5]. Во время работы системы один из модулей является активным, а другой находится в горячем резерве и автоматически принимает на себя управление в случае частичного отказа первого. Система с такой архитектурой может быть выражена следующей упрощённой диаграммой состояний и переходов (рис. 2).

В случае частичного отказа активного модуля (переход из исходного состояния $3 + R$ в $2 + R$) управление передаётся на резервный модуль автоматически. На диаграмме этому событию соответствует переход из состояния $2 + R$ в состояние 3 с интенсивностью τ. После этого блок с частичным отказом может быть заменен ремонтной бригадой на исправный блок (переход с интенсивностью μ), и исходное состояние системы будет восстановлено. В предположении, что $\tau >> \mu >> \lambda$, вероятность отказа данной системы может быть приближенно оценена, как $6\lambda^2\tau$. Данная схема позволяет снизить требования к времени восстановления $MTTR$ и использовать вычислители с архитектурой 2oo3, конструктивно выполненные в едином аппаратном модуле. Даже при до-

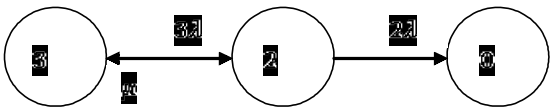

Рис. 1. Диаграмма состояний и переходов для системы 2oo3

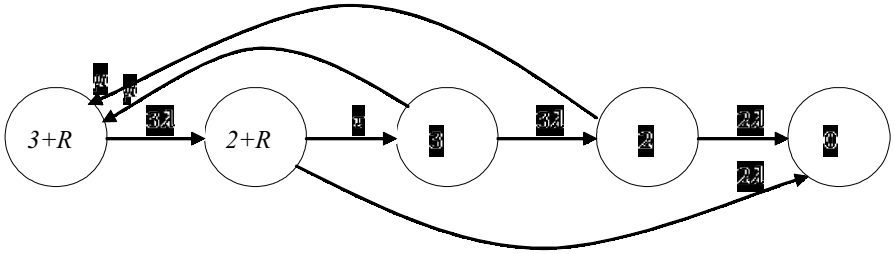

Рис. 2. Диаграмма состояний и переходов для системы 2oo3 + *R*

статочном уровне надежности такого вычислителя с архитектурой 2oo3 без дублирующего модуля он будет являться одиночной точкой восстановления, и его резервирование необходимо для обеспечения ремонтопригодности системы.

Ещё один пример системы на базе архитектуры 2oo3 – отказоустойчивый вычислительный комплекс (ОВК), разработанный совместно компаниями ФГУП «НИИ автоматики» и ЗАО «Ланит-Терком» в 2008–2011 годах [6]. ОВК является частью распределенной системы обработки данных, построенной на основе компьютерной сети Ethernet и обслуживающей критичные с точки зрения безопасности приложения. Структура ОВК позволяет проводить ремонт неисправного модуля без остановки прикладного программного обеспечения, в соответствии с классической моделью системы 2oo3 (рис. 1). В то же время условия применения ОВК могут накладывать ограничения на время восстановления полной конфигурации в случае частичного отказа. В этом случае возможно построение резервированной сетевой структуры с двумя ОВК, для которой диаграмма состояний и переходов будет соответствовать рис. 2.

ЗАКЛЮЧЕНИЕ

Проектирование отказоустойчивых систем с высокой степенью функциональной безопасности требует применения аппаратных структур 2oo3, 1oo2D, либо их комбинаций. Для сетевых компьютерных систем с высокой интенсивностью запросов построение ядра на основе архитектуры 2oo3 является наиболее практичным выбором для разработчика. Системы с архитектурой 2oo3 обеспечивают выполнение всех базовых принципов отказоустойчивости с возможностью формального доказательства соответствия уровням функциональной безопасности SIL3/SIL4. Практика создания систем, сертифицированных по требованиям стандарта [1], подтверждает высокую эффективность синхронных аппаратных решений с использованием мажорирующих схем голосования «2 из 3».

Литература

1. ГОСТ Р МЭК 61508-2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»:

Часть 1: Общие требования.

Часть 2: Требования к системам.

Часть 3: Требования к программному обеспечению.

Часть 4: Термины и определения.

Часть 5: Рекомендации по применению методов определения уровней полноты безопасности.

Часть 6: Руководство по применению ГОСТ Р МЭК 61508-2-2007 и ГОСТ Р МЭК 61508-3-2007.

Часть 7: Методы и средства.

2. ГОСТ Р 51901.15 – 2005 (МЭК 61165:1995) «Менеджмент риска. Применение Марковских методов».

3. Critical control and safety system 3000 SIS. RTP Corp., 2009 / http://www.rtpcorp.com.

4. Trusted^{TM} Fault Tolerant Technology. Rockwell Automation, Inc., 2011 / http://www.rockwellautomation.com.

5. Trusted^{TM} Industrial Control System SDS-8110. Trusted^{TM} TMR Processor-T8110B. Rockwell Automation, Inc., 2006 / http://www.rockwellautomation.com.

6. *Бондарев А.В., Короткий Н.В., Кривошеин Б.Н.* Построение отказоустойчивых вычислительных комплексов по принципу троирования // Труды второй научно-технической конференции молодых специалистов, посвящённой 50-летию полёта Ю.А. Гагарина в космос. ОАО «КБСМ», СПб., 2011.

Abstract

High level of functional safety for electronic systems can be reached using redundant hardware architectures only. For the complex systems with high-performance network interfaces the architecture 2oo3 (TMR) with optional modifications is a preferable choice. Solutions based on voting nodes provide high reliability level of the network computers not compromising the performance. This article describes the techniques of network system reliability analysis and practical implementation examples.

Keywords: fault-tolerant computer, voting, triple modular redundancy, TMR, 2oo3, functional safety.

Кривошеин Борис Николаевич,
директор департамента
Радиоэлектронной Аппаратуры
ЗАО «Ланит-Терком»,
Boris.Krivoshein@lanit-tercom.com