МИНИСТЕРСТВО ПУТЕЙ СООБЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

РТМ 32 ЦШ 1115842.01—94

РУКОВОДЯЩИЙ ТЕХНИЧЕСКИЙ МАТЕРИАЛ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Методы и принципы обеспечения безопасности микроэлектронных СЖАТ

Издание официальное

САНКТ-ПЕТЕРБУРГ
1994

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАН И ВНЕСЕН Управлением сигнализации, связи и вычислительной техники МПС, Петербургским государственным университетом путей сообщения

РАЗРАБОТЧИКИ: Вл. В. Сапожников, академик АТ РФ, д-р техн. наук (руководитель), В. В. Сапожников, академик АТ РФ, д-р техн. наук, Д. В. Гавзов, канд. техн. наук (ответственный исполнитель), В. И. Талалаев, О. А. Наседкин, канд. техн. наук, М. В. Илюхин, Д. М. Котельников

2 УТВЕРЖДЕН начальником Управления сигнализации, связи и вычислительной техники МПС РФ Г. Ф. Лекутой 10 февраля 1994 г.

3 ВВЕДЕН ВПЕРВЫЕ

СОДЕРЖАНИЕ

РУКОВОДЯЩИЙ ТЕХНИЧЕСКИЙ МАТЕРИАЛ

Методы и принципы обеспечения безопасности микроэлектронных СЖАТ

Дата введения 1994-06-01

ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий руководящий технический материал рассчитан на работников научно-исследовательских, проектно-конструкторских и испытательных организаций. Он распространяется на дискретные устройства, системы железнодорожной автоматики и телемеханики (СЖАТ), а также определяет основные правила и методы обеспечения безопасности микроэлектронных схем. В данном документе под микроэлектронными схемами подразумеваются схемы, построенные на электронных элементах, микросхемах, микропроцессорах и микроЭВМ.

Требования настоящего руководящего технического материала должны использоваться разработчиками с учетом специфики области применения конкретных устройств (например для обработки аналоговых сигналов и т.д.).

Данный руководящий документ является открытым для дополнений и изменений, связанных со спецификой устройств и с расширением области его распространения, а также с появлением новых технических решений, элементов и совершенствованием известных схем, отвечающих требованиям безопасности.

Все дополнения и изменения осуществляются установленным для нормативных документов порядком.

Использование данного документа не отменяет общего порядка проведения испытаний на безопасность в соответствии с ОСТ 32.19, РД ЦШ 1115842.01-93 и РД 32 ЦШ 1115842.02-93.

Термины и определения, используемые в данном документе, соответствуют ОСТ 32.17 и ГОСТ 27.002.

НОРМАТИВНЫЕ ССЫЛКИ

В настоящем руководящем техническом материале использованы ссылки на следующие стандарты:

- ГОСТ 27.002-83. Надежность в технике. Термины и определения;
- ОСТ 32.17-92. Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения;
- ОСТ 32.19-92. Безопасность железнодорожной автоматики и телемеханики. Общие требования к программам обеспечения безопасности.

1 МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И БЕЗОТКАЗНОСТИ МИКРОЭЛЕКТРОННЫХ СЖАТ

Выбор методов достижения требуемых показателей безотказности и безопасности осуществляется на основе анализа возможных отказов (рисунок 1.1) элементов СЖАТ [1.1], [1.2].

В релейных системах железнодорожной автоматики отказы разделяются на защитные и опасные. Появление сложных микроэлектронных элементов привело к выделению нового класса отказов - маскируемых.

Дефекты технических средств, которые не приводят к нарушению функционирования системы, называются маскируемыми и могут быть обнаруживаемыми и необнаруживаемыми. Последние могут приводить к накоплению неисправностей и, как следствие, к возможности появления опасных отказов.

В отличие от релейных СЖАТ проблема безотказности и безопасности комплексно может быть решена не за счет применения более надежных элементов, а за счет использования различных методов резервирования и контроля.

Это в значительно большей степени относится к безопасности, которая обеспечивается определенным комплексом мероприятий, устанавливаемых концепцией безопасности.

Для реализации концепций безопасности микроэлектронных СЖАТ используются три стратегии (рисунок 1.2): безотказность

РТМ 32 ЦШ 1115842.01-94

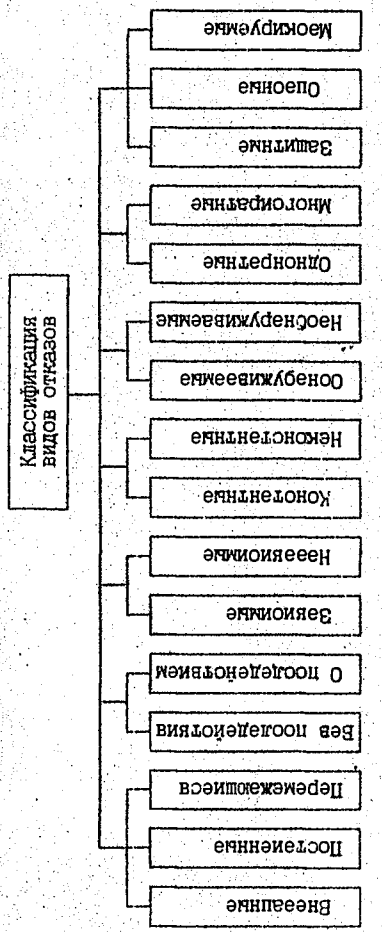


Рисунок 1.1

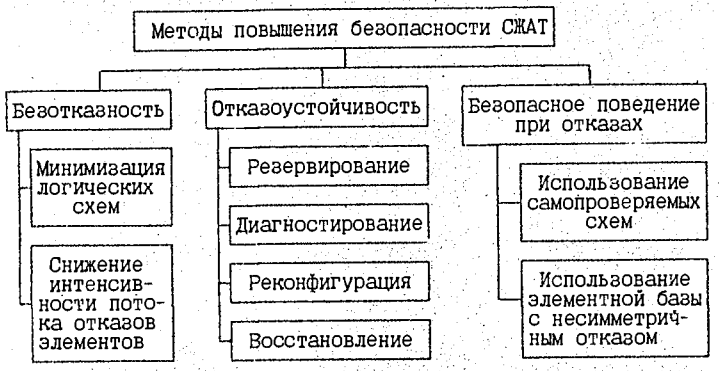


Рисунок 1.2

(reliability), отказоустойчивость (fault-tolerance) и безопасное поведение при отказах (fail-safe) [1.1], [1.9], [1.11], [1.13]. Первые две стратегии подразумевают, что система, которая правильно выполняет свой алгоритм функционирования, безопасна. Третья стратегия используется специально для безопасных систем и заключается в переводе системы в защитное необратимое состояние при появлении отказа (рисунок 1.3). Обратный переход в работоспособное состояние исключается (маловероятен) и производится искусственным путем (обычно с участием человека).

Графическая интерпретация взаимодействия этих стратегий между собой при построении безопасных систем отображена на рисунке 1.4. Безопасность технических средств в значительной степени определяется влиянием человеческого фактора на всех стадиях жизненного цикла (разработки, изготовления и эксплуатации). Поэтому для создания безопасных технических средств должна дополнительно использоваться стратегия безошибочности.

С широким внедрением полупроводниковых и микроэлектронных элементов появилась необходимость в разработке и исследовании дополнительных мер по защите от опасных отказов устройств, выполненных на их основе [1.2], [1.6]-[1.9].

Первоначально в электронных системах автоматики [1.10]-[1.13] необходимый уровень безопасности достигался за счет выполнения их на элементах с несимметричным отказом, не требующих специальных мер защиты от опасных отказов, - на электронных аналогах реле 1 класса надежности.

Более перспективным является реализация сложных СЖАТ на интегральных микросхемах большой степени интеграции (БИС). При использований такой элементной базы для достижения необходимых показателей безопасности применяют сочетание различных видов резервирования (рисунок 1.5) с контролем и диагностикой появления сбоев и отказов элементов. Контроль осуществляется устройством с несимметричной характеристикой отказов.

Классификации методов диагностики приведена на рисунке 1.6.

При разработке СЖАТ на основе микроэлектронных элементов большой степени интеграции (например микропроцессоров) необходимо учитывать, что многие их элементы используются многократно в

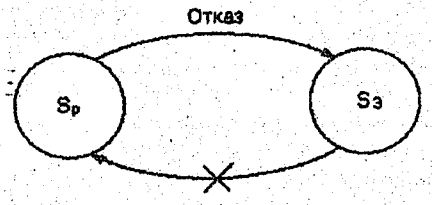


Рисунок 1.3

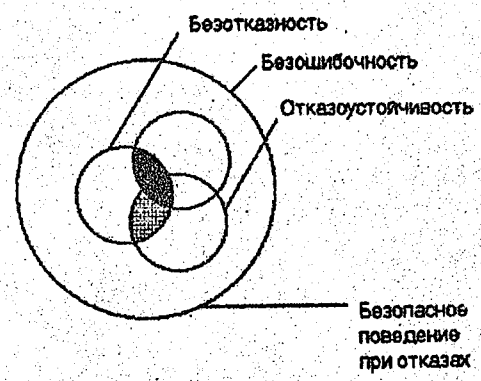


Рисунок 1.4

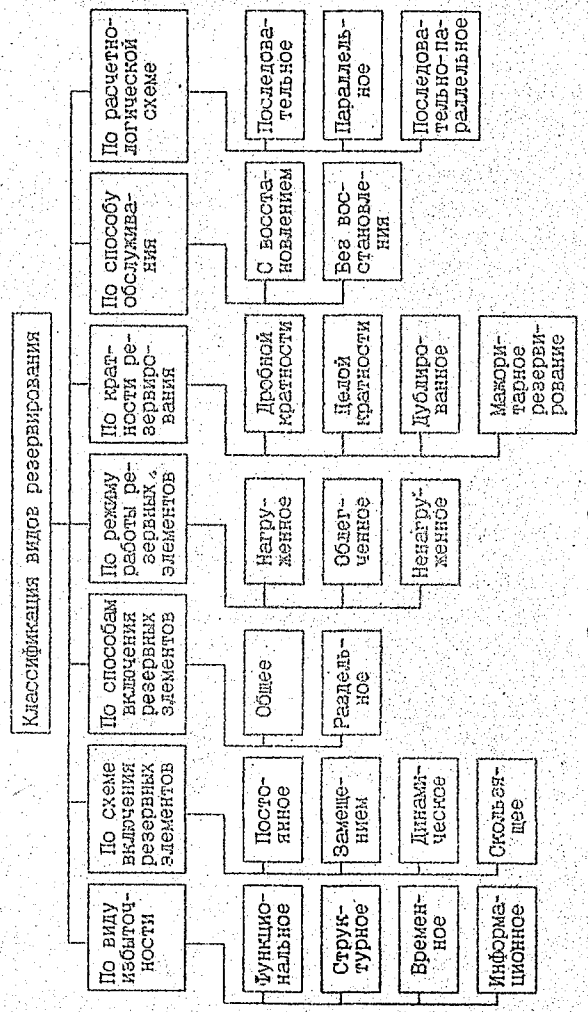


Рисунок 1.5

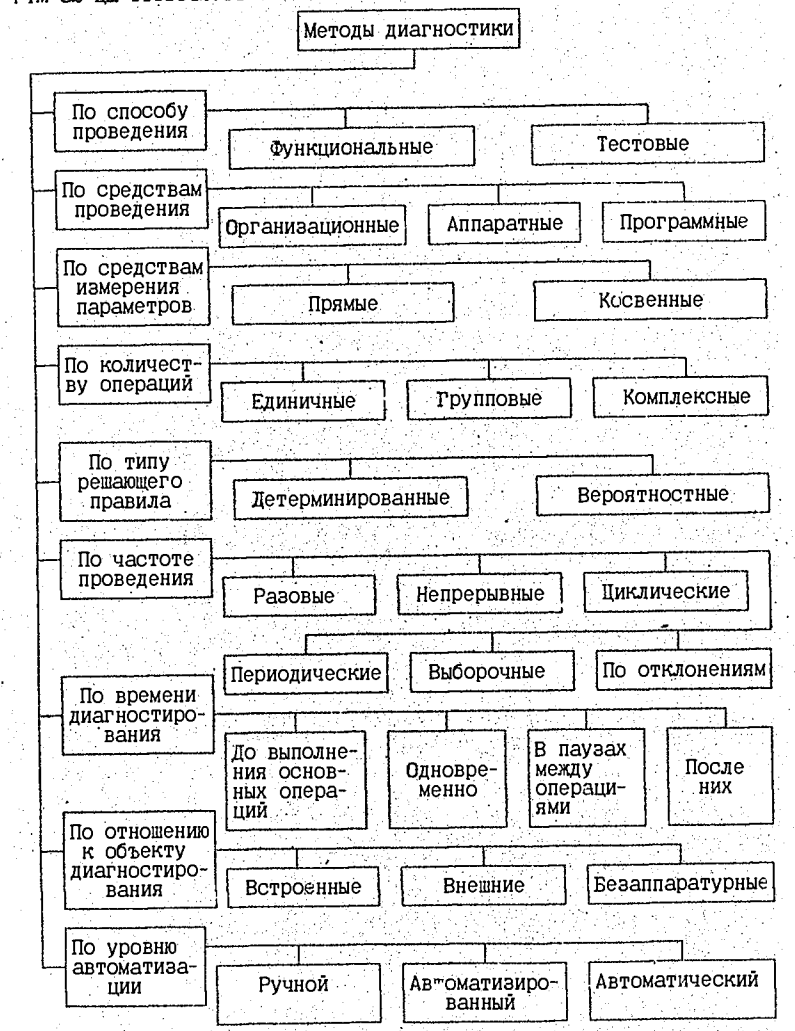


Рисунок 1.6

ходе выполнения программы. Кроме того, отдельные отказы БИС могут быть многократными. Например, отказы в питающих выводах приводят к искажениям в работе многих элементов БИС, к появлению новых связей и элементов (паразитных элементов). Последствия этого могут проявляться в различных частях ВИС, даже косвенно связанных с первоначальными обстоятельствами.

Поэтому при синтезе СЖАТ на основе микропроцессоров (МП) необходимо считаться с многократными отказами. Современные МП характеризуются высокой степенью интеграции и малым числом выводов, поэтому их полная проверка требует значительного времени и практически невозможна.

Необходимые показатели безотказности, контролепригодности и безопасности микропроцессорных систем автоматики достигаются за счет использования структурного резервирования, которое можно подразделить на аппаратное и программное, т.е. используется способ параллельной обработки информации в нескольких микроЭВМ или с помощью нескольких программ в одной микроЭВМ.

Для контроля правильности работы каналов обработки информации используется аппаратное или программное сравнение результатов выполнения отдельных команд или решения отдельных задач.

Используемые методы резервирования и контроля в СЖАТ, отвечающие требованиям безопасности, должны обеспечивать:

- независимость отказов в однотипных элементах функционально избыточных структур;
- защиту системы от сбоев и отказов, исключение возможности накопления отказов;
- контроль правильности функционирования программного обеспечения.

При структурном резервировании критическими узлами с точки зрения независимости отказов в различных вычислительных каналах являются входная и выходная информация, питание, достоверность работы устройств контроля, однотипные ошибки программного обеспечения.

Для защиты от искажений входную информацию вводят в МП СЖАТ в виде последовательного избыточного кода или по нескольким параллельным гальванически разделенным цепям. Питание различных

микроЭВМ должно быть автономным, а управляющие воздействия на исполнительные органы должны осуществляться по методу накопления выходных сигналов, т.е. по интегральной оценке избыточной информации, что позволит также обеспечить необходимый уровень помехоустойчивости СЖАТ [1.12].

Программные методы резервирования и контроля требуют большего, чем аппаратные, времени обнаружения отказов, и при их использовании трудно обеспечить требование независимости отказов в различных программах обработки информации [1.13].

Для обеспечения независимости отказов программных модулей создаются разные коллективы программистов, используются инверсные данные и т.п. Все эти меры приводят к увеличению стоимости разработки МП СЖАТ, т.к. затраты на создание программного обеспечения достигают 70% [1.14]. Кроме того, в настоящее время не существует теоретического подтверждения обеспечения безопасности МП-средств, использующих только программные методы резервирования и контроля. Таким образом, в МП СЖАТ для обеспечения безопасности необходимо использовать сочетание программных и аппаратных методов [1.1], [1.2].

2 СТРУКТУРНЫЕ МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ СЖАТ

2.1 Анализ резервированных структур

В большинстве существующих микроэлектронных систем (МЭС), отвечающих за безопасность, используются аппаратные методы резервирования и контроля [2.1]-[2.4].

В общем виде резервированная структура МЭС приведена на рисунке 2.1. Резервироваться может как все устройство, так и его отдельные узлы.

Величина n, называемая кратностью резервирования, характеризует число идентичных каналов или элементов, обеспечивающих соответственно получение или обработку информации.

Неотъемлемой частью избыточных устройств являются восстанавливающие органы (ВО), осуществляющие коррекцию ошибок, возникающих при сбоях и отказах аппаратуры, и реализующие в большинстве случаев пороговую функцию.

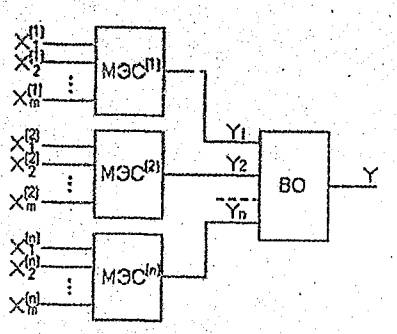
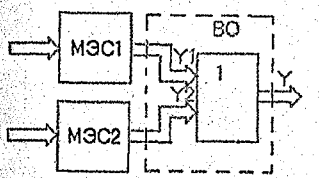
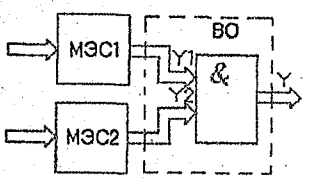


Рисунок 2.1



$Y=M_2^1=Y1 \vee Y2$

Рисунок 2.2



$Y=M_2^2=Y1 \cdot Y2$

Рисунок 2.3

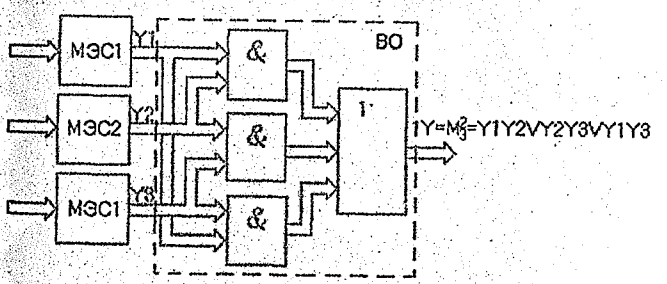


Рисунок 2.4

При неисправности какого-либо из обрабатывающих каналов МЭС на его выходе может появиться ложная 1 или ложный 0. Правильный сигнал на выходе избыточной структуры появляется только при определенном числе ложных сигналов 0 и 1 на выходах y_i МЭС.

Естественно, чем выше кратность резервирования n, тем больше ошибок на выходах логических блоков будет корректироваться.

В общем виде пороговая функция ВО с равными весами может быть записана [2.5]:

$$y = M_n^{\rho} = f(y_1, y_2, \ldots, y_n) = \begin{cases} 1, \text{ если } \sum_{i=1}^{n} y_i - \rho > 0 \\ 0, \text{ если } \sum_{i=1}^{n} y_i - \rho < 0, \end{cases} \qquad (2.1)$$

где ρ - порог восстанавливающего органа.

В таблице 2.1 указано количество ошибок, исправляемых ВО с различными пороговыми функциями $y = M_n^{\rho}$.

Таблица 2.1

Кратность резервирования n	Функция ВО	Количество корректируемых ошибок	
		Ложный 0	Ложная 1
1	2	3	4
1	M_1^1	0	1
2	M_2^1	1	0
	M_2^2	0	1
3	M_3^1	2	0
	M_3^2	1	1
	M_3^3	0	2
4	M_4^1	3	0
	M_4^2	2	1
	M_4^3	1	2

Продолжение таблицы 2.1

1	2	3	4
	M_4^4	0	3
5	M_5^1	4	0
	M_5^2	3	1
	M_5^3	2	2
	M_5^4	1	3
	M_5^5	0	4
n	M^{ρ}_n	n-ρ	ρ-1

На рисунках 2.2-2.4 приведены примеры МЭС с ВО, реализующими функции M_1^1, M_2^2, M_3^2.

Из таблицы 2.1 видно, что симметричной способностью корректировать ошибки типа "ложный 0" и "ложная 1" обладают ВО, реализующие мажоритарную функцию M_3^2, M_5^3 и т.п.; ошибки типа "ложный 0" лучше всего исправляют ВО, реализующие функцию ИЛИ, а ошибки типа "ложная 1" - ВО, реализующие функцию И.

Таким образом, зная вероятности появления ложных сигналов 0, 1 и предпочтительное значение выходных сигналов, выбирают тип ВО. С точки зрения обеспечения безопасности наилучшим является ВО типа И, но по сравнению с неизбыточными такие МЭС обладают худшими показателями безотказности.

МЭС с мажоритарными ВО позволяют найти компромиссное решение для достижения необходимых показателей безотказности и безопасности.

Анализ различных видов структурного резервирования показывает, что всем им, кроме мажоритарного, присущи следующие недостатки: сложность коммутации и перерыв в работе системы по основной программе при замене отказавшего элемента или комплекта исправным.

Необходимо отметить, что мажоритарное резервирование позволяет защититься не только от постоянных отказов, но и от переме-

жающихся, в том числе и от воздействия помех, т.к. они обычно проявляются неодинаково в резервированных каналах обработки информации [2.6].

2.2 Применение мажоритарного резервирования для повышения показателей надежности МЭС

При мажоритарном резервировании организуется нечетное число каналов обработки информации МЭС, выходные сигналы которых объединяются с помощью восстанавливающего органа (мажоритарного элемента МЭ).

Сигнал на выходе МЭ определяется большинством ($p > \frac{m+1}{2}$) входных сигналов. Отказ или сбой $\frac{n-1}{2}$ каналов обработки информации не приводит к отказу системы в целом. Поэтому работоспособность отдельных каналов можно восстанавливать без прерывания работы системы, что позволяет значительно увеличить ее коэффициент готовности.

Низкая надежность отдельных блоков аппаратуры, а также значительное время восстановления неисправных узлов и элементов может быть скомпенсировано повышением кратности мажоритарного резервирования. Однако при обычном использовании таких резервированных устройств используются не все достоинства высокой кратности.

С увеличением кратности число резервируемых блоков n растет быстрее, чем величина K+1 - число блоков, при выходе из строя которых вся резервируемая группа прекращает работу, а значит растет число исправных блоков, остающихся незадействованными после отказа мажоритарно-резервированной группы.

При изменении структуры мажоритарного элемента (снижении кратности резервирования) возможно использование оставшихся исправных блоков, т.е. можно увеличить время наработки на отказ всей резервированной группы. Например, при работе МЭ по принципу 3v5 отказ наступает при неисправной работе любых трех блоков, а два блока остаются работоспособными. Если в момент исправности трех блоков преобразовать схему МЭ 3v5 в 2v3, то работоспособность всей системы будет сохранена до тех пор, пока остаются исправными

два блока.

Такого рода преобразование может быть выполнено путем понижения порога в МЭ. В этом случае мажоритарность сохраняется до полного отказа; но он применим только при высокой кратности (n>3) резервирования системы.

Возможно перестроение структуры с переходом к другому виду резервирования - дублированию. Этот способ является частным случаем адаптивных МЭ с цикловой адаптацией [2.7]. Если длительное время (несколько циклов) на одном из входов существовал ложный сигнал, то вес этого входа постепенно уменьшается до нуля, данный блок отключается от МЭ, а оставшиеся два переходят в режим работы по схеме И.

В этом случае общая надежность МЭ и его защищенность от появления ложного сигнала 1 на выходе повышается с сохранением общих параметров работоспособности. Это возможно либо подачей на отключаемый вход ВО логического 0 (в логических МЭ), либо снижением до нуля веса неисправного входа (для пороговых МЭ).

Граф возможных состояний адаптивной мажоритарно-резервированной системы (МРС) 3v5 приведен на рисунке 2.5. Средняя наработка на отказ такой адаптивной системы Tp ≈ 1,28 To [2.7].

Таким образом, адаптивные мажоритарные системы позволяют значительно повысить показатели безотказности аппаратуры даже без восстановления отказавших каналов обработки информации.

Практическую реализацию адаптивных МЭ наиболее целесообразно выполнять программно, т.к. в аппаратном выполнении они получаются довольно сложными и, следовательно, имеют не очень высокие показатели безотказности, что соответственно понижает эффективность резервирования.

На рисунке 2.6 приведены зависимости вероятности безотказной работы МРС 2v3 и 3v5 (без восстановления) от вероятности безотказной работы резервируемого канала при Pм-const. Они имеют S-образный характер, и можно сделать вывод, что в избыточных структурах 2v3, 3v5 с однократной связью [2.5], [2.6] возможен выигрыш в надежности при наличии высоконадежного МЭ (Pмэ → 1), если вероятность безотказной работы неизбыточного канала обработки информации P_o>0,5. Недостатком таких структур является то, что вероят-

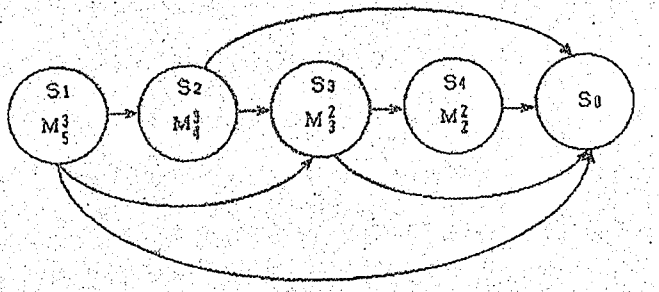


Рисунок 2.5

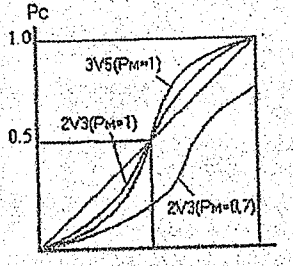


Рисунок 2.6

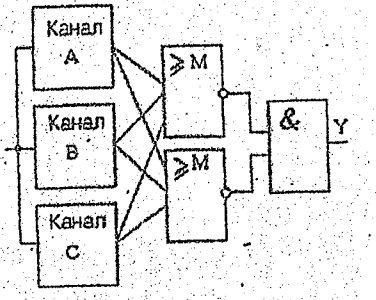


Рисунок 2.7

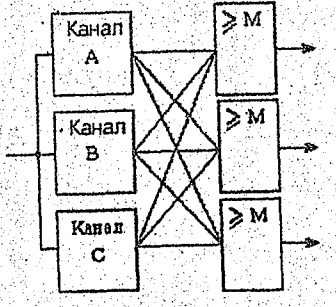


Рисунок 2.8

ность их безотказной работы не превосходит вероятности безотказной работы МЭ и в случае отказа последнего отказывает вся избыточная структура.

С этой точки зрения еще более высокие требования предъявляются к надежности МЭ при дублировании его по схеме И (рисунок 2.7) [2.8].

Больший эффект от повышения надежности избыточной структуры МЭС можно получить, используя мажоритарное резервирование с многократными связями (рисунок 2.8) [2.6].

3 СТРУКТУРЫ БЕЗОПАСНЫХ МИКРОЭЛЕКТРОННЫХ И МИКРОПРОЦЕССОРНЫХ СИСТЕМ

Безопасность функционирования МП-систем зависит в основном от интенсивности потока отказов элементов микроЭВМ, длительности периода контроля МП-модуля ($\tau_д$), закона формирования выходных воздействий системы (конъюнкции, пороговой или мажоритарной функции) и глубины (дискретизации) контроля.

Наиболее широко распространенная концепция безопасности микроэлектронных СЖАТ требует, чтобы одиночные дефекты аппаратных и программных средств не приводили к опасным отказам и обнаруживались с заданной вероятностью на рабочих или тестовых воздействиях не позднее, чем в системе возникнет второй дефект. Проблема осложняется, если не все одиночные дефекты обнаруживаются. Тогда новый отказ может привести к нарушению безопасности. Поэтому необходимо предъявлять высокие требования по достоверности контроля программно-аппаратных средств и уменьшать время тестирования аппаратуры. Обнаружение отказа должно происходить в течение заданного интервала времени. Эту задачу решают внутрипроцессорный и межпроцессорный контроль.

Наиболее эффективно внутрипроцессорный контроль осуществляется путем тестирования в отведенные для этого промежутки времени или путем применения принципов самоконтроля (самопроверяемости) и сигнатурного анализа. Межпроцессорный контроль состоит во взаимной проверке работы процессоров на уровне системных шин, памяти и выходов (контроль с сильными связями). При контроле с умеренными

связями производится проверка выходов. Применяется также вариант, когда один процессор реализует вычисления, а другой их проверяет (контроль со слабыми связями).

Далее рассматриваются реально используемые на практике восемь основных типов безопасных структур.

3.1 Структуры безопасных микропроцессорных модулей

Одноканальная система с одной программой (тип 1) может быть применена при организации достаточно полной проверки микроЭВМ с помощью самопроверяемых средств внутреннего контроля (ССВК) и наличии (см. рисунок 3.1) безопасных выходных схем (ВВС) для включения управляемых объектов [3.2], [3.3]. При возникновении отказа ССВК формирует сигнал Y, с помощью которого система может быть переведена в защитное состояние по выходу (например отключено питание) и (или) выходы микроЭВМ Z отключаются от управляемых объектов УО (с помощью ВВС). Безопасность данной структуры зависит от эффективности способа самопроверки. Тестовые программы должны выполняться достаточно часто. Прикладные программы должны быть свободны от ошибок при загрузке. Целесообразно применение самопроверяемого программного обеспечения [3.3].

Одноканальная система с дублированной программой (тип 2) использует две различные и независимые программы (рисунок 3.2) для реализации одних и тех же функций [3.4], [3.5]. Результаты выполнения программ Z1 и Z2 сравниваются внешней безопасной схемой сравнения (БСС). Уровень безопасности зависит от степени различия двух программ и от интервала времени обращения к данным. Целесообразно, чтобы программы были написаны разными бригадами программистов и по разным алгоритмам.

Дублированная система со слабыми связями (тип 3) состоит из двух микроЭВМ (рисунок 3.3), в которых процессоры и программы могут быть неодинаковыми [3.6], [3.7]. Процессор микроЭВМ 1 реализует основные вычисления, микроЭВМ 2 их проверяет. Для этого осуществляется обмен информацией по шине W. Синхронизация каналов необязательна. Контроль работы микроЭВМ осуществляется либо за счет тестовых программ, либо за счет параллельных вычислений и

РТМ 32 ЦШ 1115842.01-94

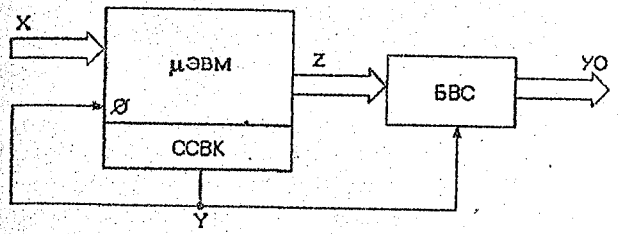


Рисунок 3.1

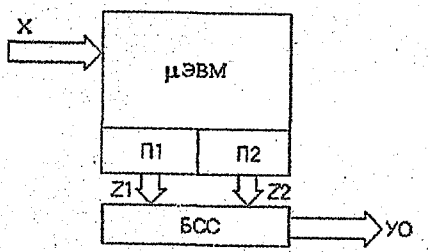


Рисунок 3.2

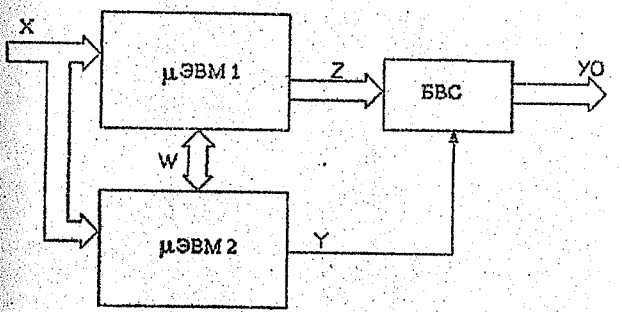


Рисунок 3.3

сравнения результатов. При обнаружении ошибки микроЭВМ 2 формирует сигнал Y и выходы микроЭВМ 1 отключаются от УО. В таких структурах возникают проблемы с обеспечением необходимой достоверности контроля.

Дублированная система с умеренными связями (тип 4) включает в себя две одинаковые микроЭВМ (рисунок 3.4) с одинаковыми программами [3.8], [3.9]. Работа обоих каналов синхронизирована. Сравнение результатов обработки информации осуществляется на уровне выходов Z1 и Z2 с помощью БСС. Это одна из наиболее распространенных на практике безопасных структур. Минимальная кратность необнаруживаемых отказов в ней равна 2 - по одному отказу в каждой микроЭВМ, которые одинаковым образом искажают выходные сигналы Z1 и Z2. Прикладные программы должны быть свободны от ошибок при загрузке. Одиночные отказы не опасны. Кратные независимые отказы могут не учитываться, если время обнаружения отказа достаточно мало.

Дублированная система с сильными связями (тип 5) использует одинаковые программы в двух одинаковых микроЭВМ (рисунок 3.5), но в отличие от структуры типа 4 контроль работы двух каналов осуществляется здесь не только на уровне выходов, но и на уровне шин и памяти [3.7], [3.10]-[3.12]. Работа каналов синхронизирована. В наиболее сильном случае производится потактовая проверка совпадения сигналов W1 и W2 на внутренних контрольных точках (шинах) с помощью БСС 1. При возникновении ошибки сигнал Y воздействует на БСС 2 и отключает УО, т.е. переводит оба канала в защитное состояние. Структура обладает высоким уровнем безопасности. Проблему могут составить одинаковые программные ошибки в каналах.

Самопроверяемая дублированная система (тип 6) состоит из двух каналов (рисунок 3.6), построенных в виде самопроверяемых устройств [3.3], [3.13], [3.14]. Сигналы контроля W1 и W2, формируемые с помощью ССВК 1 и ССВК 2, сравниваются с ССВК 3. Последняя вырабатывает сигнал ошибки Y. Минимальная кратность необнаруживаемых отказов равна 4 - по два отказа в каждом канале, которые не обнаруживаются ССВК и одинаковым образом искажают выходные сигналы Z1 и Z2. Самоконтроль каналов может быть аппаратный и

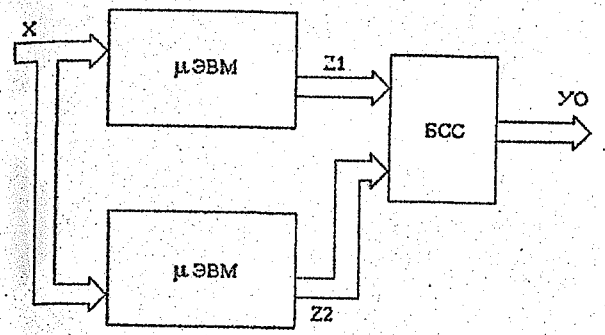


Рисунок 3.4

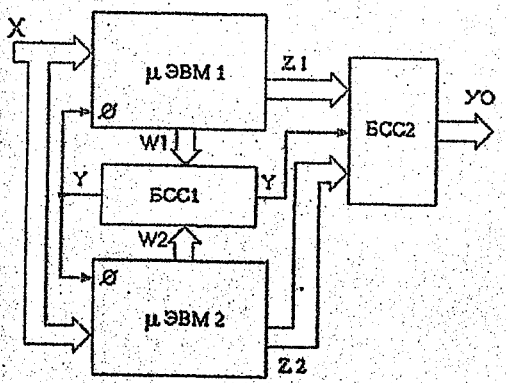


Рисунок 3.5

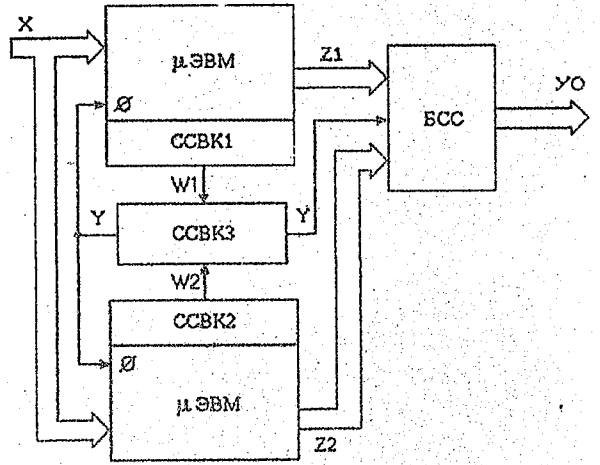


Рисунок 3.6

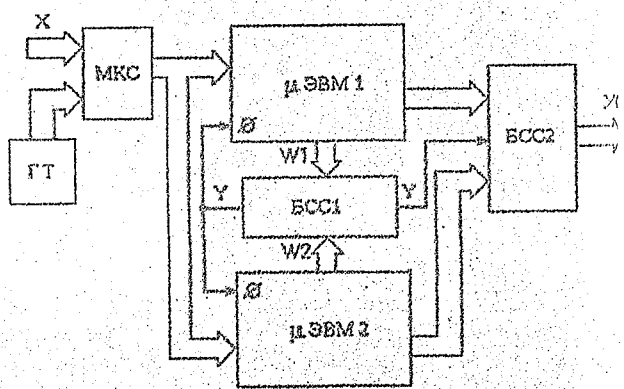


Рисунок 3.7

программный. Возможно использование независимых программ в каждом процессоре.

Дублированная система с тестированием и сильными связями (рисунок 3.7) содержит в дополнение к структуре типа 5 генератор тестов (ГТ) и мультиплексор (МКС) й применяется, если множество входных воздействий X не обеспечивает необходимой глубины проверки каналов обработки информации [3.15]. В этом случае в процессе рабочего функционирования периодически выделяются отрезки времени, в течение которых с помощью мультиплексора сигналы X отключаются от входов системы и к последним подключается генератор тестов. Результаты тестирования обоих каналов сравниваются БСС 1. При обнаружении ошибки система переводится в защитное состояние. Данный принцип используется также тогда, когда система большую часть рабочего функционирования находится в ждущем режиме (при этом сигналы X длительное время не изменяются).

Троированная мажоритарная система (тип 8, рисунок 3.8) имеет три независимых канала обработки информации [3.2]-[3.7], [3.16], [3.17]. Работа каналов синхронизирована и сравнивается с помощью безопасного мажоритарного элемента (БМЭ). Безопасность сравнима с безопасностью дублированной структуры (рисунок 3.4), но отказоустойчивость увеличивается.

С применением в СЖАТ средств вычислительной техники появились специфичные структуры мажоритарно-резервированных МП на уровне двунаправленных шин (рисунок 3.9) [3.18]. Такой подход в построении МП СЖАТ требует разработки сложного специализированного модуля.

Рассмотренные структуры и принципы построения безопасных систем могут использоваться в сочетании, дополняя друг друга. При этом базовыми обычно являются дублированная (тип 4) и троированная (тип 8) структуры. Перспективным, на наш взгляд, является принцип построения самопроверяемых безопасных систем (тип 6).

3.2 Аппаратный контроль и способы локализации отказов микропроцессорных систем автоматики

Как уже отмечалось, в СЖАТ, выполненных на основе МП и мик-

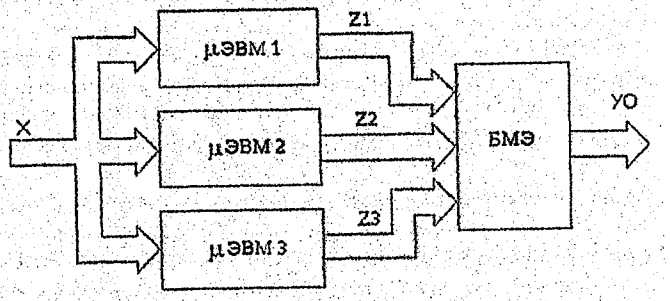


Рисунок 3.8

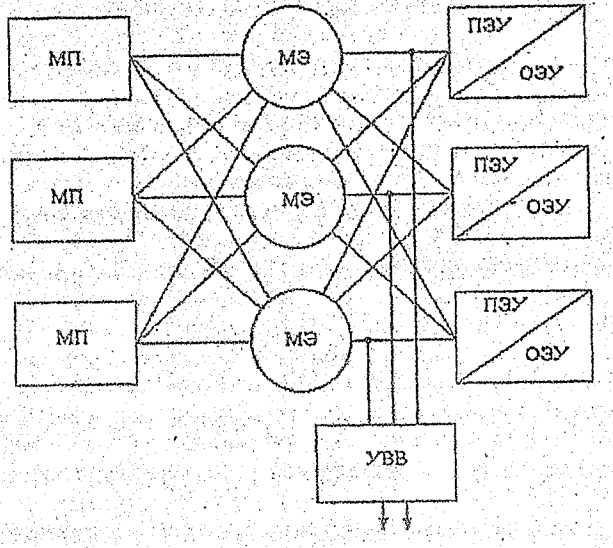


Рисунок 3.9

роЭВМ, необходимо использовать структурное резервирование и аппаратный контроль [3.19].

Обмен информацией между отдельными узлами микроЭВМ, входящих в состав микроэлектронных систем (МЭС), осуществляется через шины внутреннего интерфейса, поэтому при контроле совпадения сигналов на этих шинах можно утверждать, что они в процессе выполнения рабочих и тестовых алгоритмов функционируют без отказов, т.е. таким образом можно контролировать исправность внутренних функциональных узлов микроЭВМ [3.20]. Для сравнения результатов обработки информации используют компараторы с несимметричной характеристикой отказов.

Устройство сравнения и n-резервированные каналы обработки информации выполняются в виде конструктивно законченного безопасного модуля.

В большинстве случаев устройство контроля шин внутреннего интерфейса МП не определяет, какой узел отказал, а просто фиксирует расхождение в работе каналов обработки информации и первоначально, для того чтобы отличить сбой от отказа, осуществляет перезапуск искаженного участка программы во всех n микроЭВМ. При повторном обнаружении неравнозначности кодовых векторов на шинах микроЭВМ осуществляется реконфигурация безопасного МП-модуля или устройство контроля обеспечивает безопасное (выключенное) состояние модуля. Причем отключение должно осуществляться необратимо даже в случае нового отказа в системе.

При выполнении рабочих алгоритмов МП СЖАТ некоторые элементы микроЭВМ могут использоваться с малой интенсивностью (например области ОЗУ и ПЗУ), поэтому для обеспечения большей глубины контроля и исключения возможности накопления отказов необходимо предусмотреть их циклическую тестовую проверку. Одним из видов такой проверки в паузах между эксплуатационными событиями является использование имитационных программ для тестового моделирования поездной обстановки на станции или перегоне. Таким образом, длительность периода контроля элементов МП-модуля определяется рабочими и тестовыми алгоритмами системы.

Как было показано в п. 3.1, для обеспечения безопасности МЭС достаточно дублирование структуры устройства. На рисунке 3.10

приведена обобщенная структура дублированного МП-модуля. Шины внутреннего интерфейса контролируются компаратором с несимметричной характеристикой отказов (УК МП) [3.20].

Выходная информация на внешнем интерфейсе может формироваться схемами сравнения (вых.1) или с выхода одной из микроЭВМ (вых.2). Во втором случае необходимо дополнительное устройство, контролирующее идентичность состояния выходов обоих микроЭВМ.

УК выходов МП-модуля может быть также общим, но при этом отказ любого выходного элемента приводит к отказу всего модуля. Поэтому в ряде случаев целесообразно выходы внешнего интерфейса разделять на группы, имеющие свое устройство контроля, или внешний интерфейс организовывать на элементах И, ИЛИ с несимметричной характеристикой отказов. В этих случаях МЭС, выполненная на основе дублированной микроЭВМ, обладает функциональной отказоустойчивостью, т.к. при отказе некоторых выходов она частично сохраняет свою работоспособность.

В настоящее время известно довольно много безопасных схем сравнения с несимметричной характеристикой отказа, исключающих ложный логический сигнал 1 на выходе [3.10], [3.20]. Классификация безопасных компараторов приведена на рисунке 3.11.

В компараторах на основе функциональных преобразователей, получивших наибольшее распространение, несимметричность отказов достигается за счет того, что при отказе их элементов нарушается закон преобразования сигналов из одного вида в другой. В этом случае на их выходе сигнал отсутствует или появляется в виде, не воспринимаемом последующим элементом.

На основе анализа показателей надежности известных компараторов [3.20], применяемых для сравнения кодовых векторов на шинах интерфейса в параллельном виде, можно сделать вывод, что одними из лучших являются самопроверяемые тестеры 2/4 [3.3].

На рисунке 3.12а приведена функциональная схема устройства контроля шин дублированного МП-модуля. Сигналы от второго МП поступают в инверсном виде. При нарушении согласованной работы МП на выходах контрольных схем 2/4 (рисунок 3.12б) появляется непарафазный сигнал, что регистрируется фиксирующим элементом (ФЭ).

Для того чтобы отличать сбои и отказы аппаратуры, ФЭ состоит

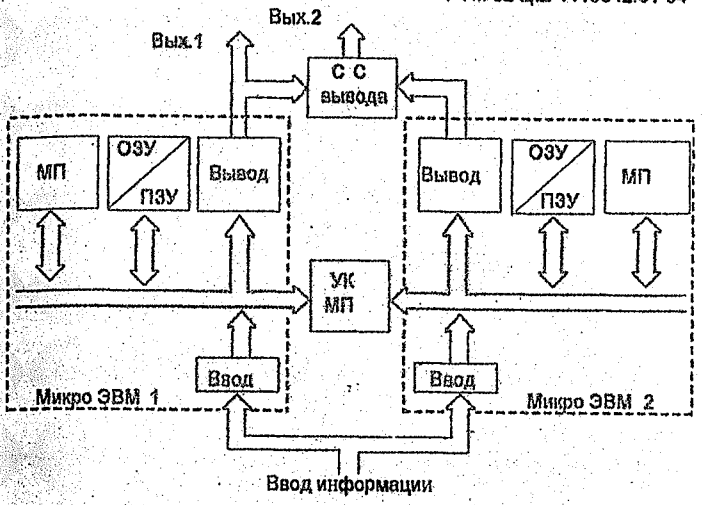


Рисунок 3.10

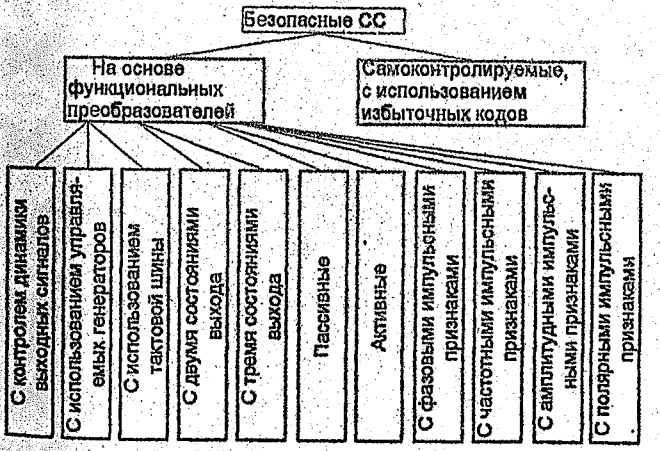


Рисунок 3.11

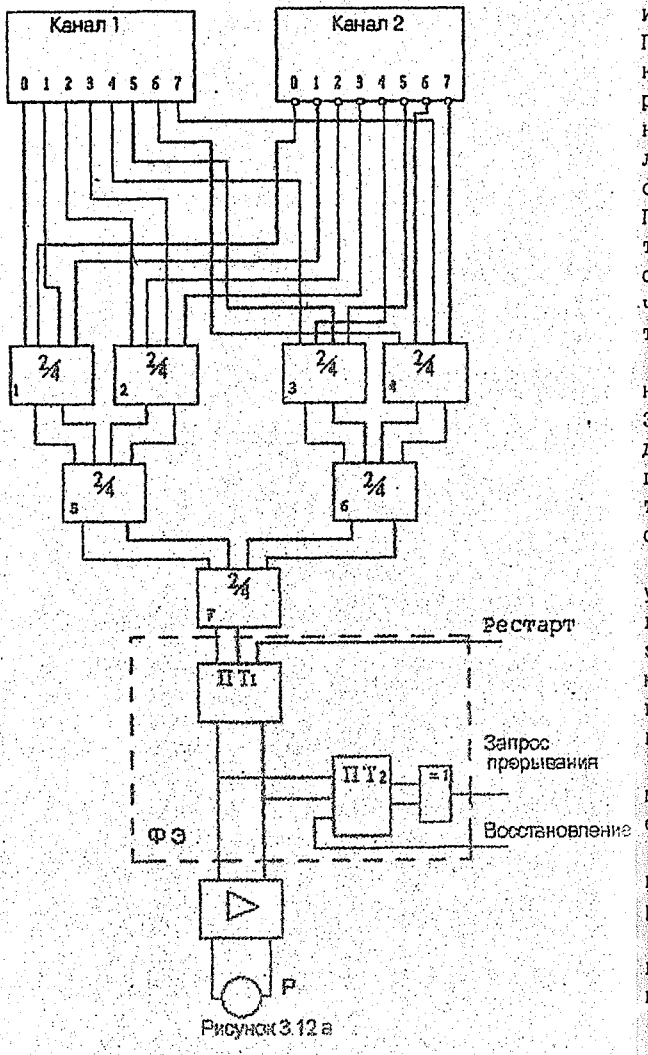


Рисунок 3.12 а

из двух последовательно соединенных парафазных триггеров $ПТ_1$ и $ПТ_2$ [3.21]. При первоначальном нарушении парафазности на выходах контрольных схем оба ПТ блокируются и в МП поступает запрос прерывания. По этому сигналу в МП осуществляется возврат в программе на несколько шагов назад (рестарт), формируется сигнал восстановления $ПТ_1$ и искаженный участок программы повторяется вновь. Если снова фиксируется нарушение идентичности выполнения программы, то $ПТ_1$ окончательно блокируется и контактами реле Р выключается питание МП-модуля, т.е. обеспечивается защитное состояние МЭС. При отсутствии повторного сбоя, т.е. при полном прохождении первоначально искаженного программного блока, МП формируют сигнал восстановления $ПТ_2$.

На основе самрпроверяемых тестеров выполнено устройство контроля шин трехканального микропроцессорного модуля (рисунок 3.13). Сигналы на шинах МП попарно сравниваются, так же как и в дублированной структуре, с помощью тестеров 2/4. При отказе одного из МП выключаются два контрольных реле и с помощью их контактов осуществляется дешифрация номера неисправного канала и его отключение.

Сократить число элементов и значительно повысить надежность устройства контроля МП-модулей можно ва счет сравнения кодовых векторов яа шинах не в параллельном виде, а в последовательном. С этой целью для мультиплексирования сигналов на шинах МП используются универсальные сдвиговые регистры. На рисунках 3.14-3.16 предлагаются структурные схемы устройств контроля шин дублированных и мажоритарно-резервированных МП-модулей.

В УК, приведенных на рисунках 3.15, 3.16, не требуется дешифратор неисправного канала, т.к. контрольное реле подключено к соответствующему каналу обработки информации.

С целью повышения отказоустойчивсти МЭС в УК, предлагаемом на рисунке 3.16, мажоритарный элемент контроля выполнен резервированным.

Таким образом, можно сделать вывод, что УК шин внутреннего интерфейса обеспечивает большую глубину диагностирования по сравнению с контролем внешнего интерфейса микроЭВМ, т.е. дает возмож-

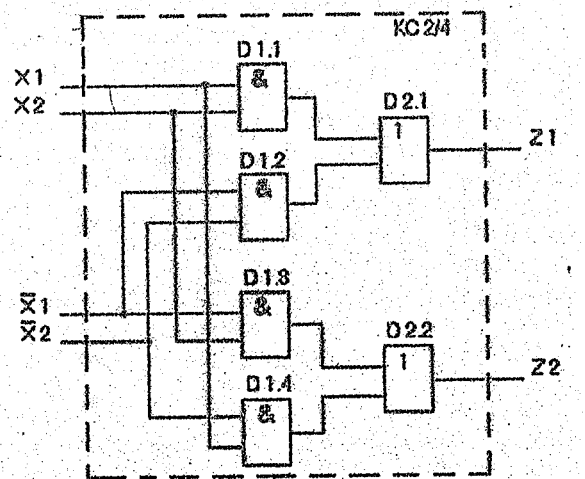


Рисунок 3.12 б

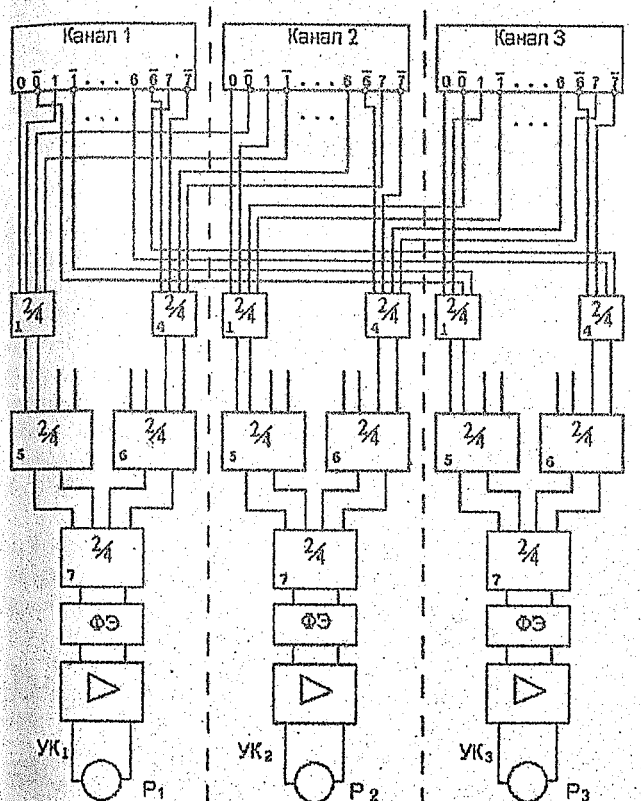


Рисунок 3.13

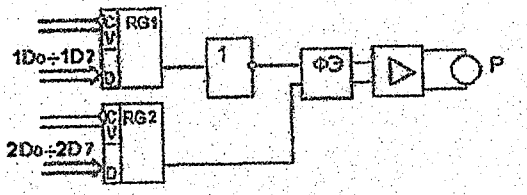


Рисунок 3.14

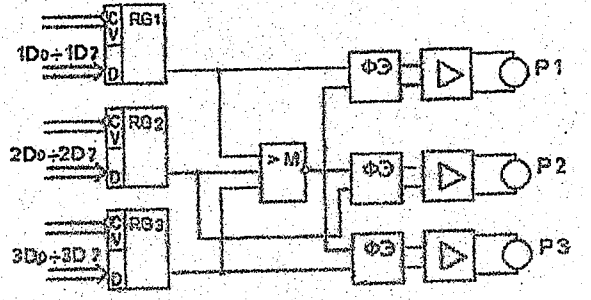


Рисунок 3.15

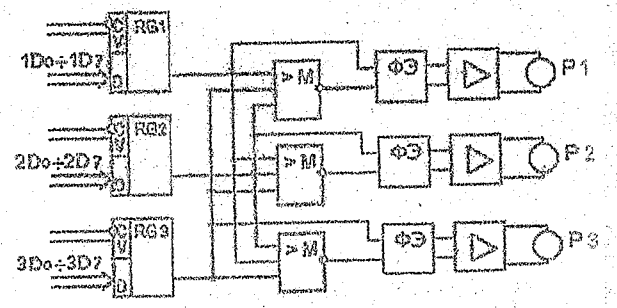


Рисунок 3.16

ность последовательно во времени сравнивать сигналы всех узлов вычислительных каналов.

4 ПРИНЦИПЫ ПОСТРОЕНИЯ БЕЗОПАСНЫХ СХЕМ НА ЭЛЕМЕНТАХ С НЕСИММЕТРИЧНЫМИ ОТКАЗАМИ

4.1 Элементы с несимметричными отказами

С точки врения безопасности элементы, на которых осуществляется построение безопасных систем, делятся на элементы с симметричными отказами и элементы с несимметричными отказами. У элементов с симметричными отказами вероятности возникновения отказов видов $0 \to 1$ и $1 \to 0$ примерно равны (имеют один порядок). К ним относятся большинство элементов, используемых в микроэлектронной и микропроцессорной технике. У элементов с несимметричными отказами интенсивности отказов разного вида различаются на порядок и более. Если при этом интенсивность отказов не более некоторого критического значения при заданном уровне безопасности ($\lambda_{кр} = 10^{-8} \div 10^{-14}$ 1/ч), то элемент называют безопасным.

Безопасные элементы разрабатываются специально для построения безопасных систем. Несимметричность отказов достигается сочетанием следующих основных методов: соответствующим физическим представлением логических сигналов; резервированием деталей и узлов; специальными конструктивными мерами; импульсным кодированием логических сигналов; использованием генераторных и резонансных режимов работы; гальванической развязкой входных и выходных цепей.

Безопасные элементы бывают двух типов: элементы, надежные относительно отказов вида $0 \to 1$ (h_1-надежные), и элементы, надежные относительно отказов вида $1 \to 0$ (h_0-надежные). На практике обычно используются h_1-надежные элементы. Методы построения безопасных схем на h_1-надежных и h_0-надежных элементах одни и те же.

4.2 Принципы построения безопасных комбинационных схем

Безопасная комбинационная схема задается с помощью двух

функций алгебры логики (ФАЛ): функции f, которую схема должна реализовать, и функции опасного отказа f_{on}, равной единице на опасных входных наборах. Опасным входным набором называется множество значений входных переменных, при наличии которых отказ вида 0 → 1 на выходе схемы приводит к опасному искажению алгоритма функционирования. Отказ, при котором функция f', реализуемая неисправной комбинационной схемой, и f_{on} равны 1 хотя бы на одном общем входном наборе, называется опасным отказом.

Таким образом, для опасного отказа выполняется условие:

$$f' \cdot f_{on} \neq 0. \qquad (4.1)$$

В большинстве практических случаев считается, что f_{on}=f. Тогда безопасной называется комбинационная схема, которая вполне надежна относительно отказов вида 0 → 1 (h_1-надежная схема). В дальнейшем рассматриваются именно такие схемы.

Сформулируем требования к безопасным комбинационным схемам. Пусть имеется произвольная схема, содержащая безопасные логические элементы $Э_1, Э_2, .., Э_5$ (рисунок 4.1), каждый из которых реализует некоторую функцию $f_1, f_2, ..., f_5$. Присвоим каждому элементу свой ранг. Первый ранг имеют элементы, соединенные только со входами схемы. Ранг r имеют элементы, входы которых соединены с выходами элементов с рангом не выше r-1. В схеме (рисунок 4.1) первый ранг имеют элементы $Э_1$ и $Э_2$, второй ранг - $Э_3$, третий - $Э_4$, четвертый - $Э_5$ и т.д.

Следующая теорема определяет способ построения безопасных схем.

ТЕОРЕМА 4.2.1. Неизбыточная комбинационная схема, построенная на безопасных элементах, является безопасной тогда и только тогда, когда все ее элементы ранга K ⩾ 2 реализуют монотонные функции алгебры логики.

Функция называется монотонной, если для двух любых двоичных наборов $a = (\alpha_1, \alpha_2, ..., \alpha_n)$ и $b = (\beta_1, \beta_2, ..., \beta_n)$ из условия a ⩽ b следует, что f(a)·f(b). Особенностью монотонной функции является то, что ее минимальная дизъюнктивная форма (МДНФ) не содержит переменных с отрицанием. Это в свою очередь определяет следующее свойство схемы, реализующей монотонную функцию (рисунок 4.2): если на входе схемы произошла смена сигнала 1 → 0, то на выходе

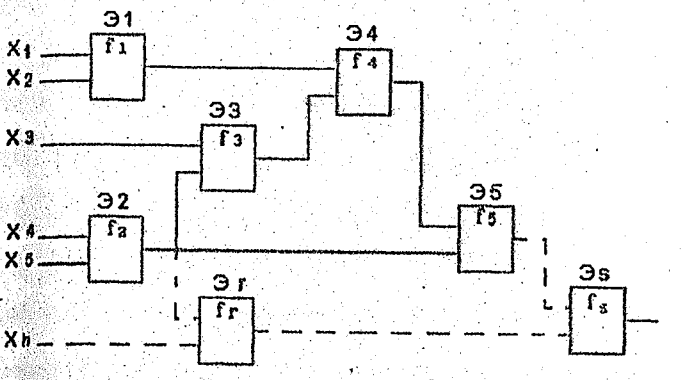


Рисунок 4.1

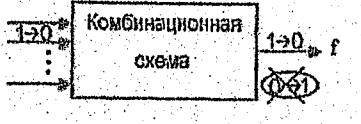


Рисунок 4.2

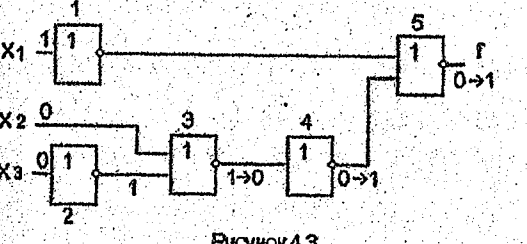


Рисунок 4.3

схемы может произойти смена сигналов 1 → 0, но не может произойти смена сигналов 0 → 1.

Рассмотрим схему (рисунок 4.3) на безопасных элементах И, ИЛИ, НЕ, для которой не выполняется требование теоремы 4.2.1. В ней элемент 4 третьего ранга реализует немонотонную ФАЛ (инверсию). Схема вычисляет функцию

$$f=x_1 \vee x_2 \vee x_3. \qquad (4.2)$$

Рассмотрим работу схемы на двоичном наборе 100, f(100)=0. Пусть происхоит отказ элемента 3 вида 1 → 0. Элемент 4 инвертирует вид отказа, т. е. на его выходе будет происходить изменение сигнала 0 → 1. Это же изменение сигнала будет и на выходе схемы. Следовательно, схема не является безопасной (h_1-надежной).

Для выполнения требования теоремы 4.2.1 надо преобразовать формулу (4.2), применив правило де Моргана:

$$f=x_1 \vee x_2 x_3. \qquad (4.3)$$

Формула (4.3) имеет знаки отрицания только над переменными. Это означает, что в соответствующей ей схеме элементы НЕ являются только элементами первого ранга (см. рисунок 4.4). Поэтому изменение сигнала вида 1 → 0 на какой-либо внутренней линии схемы не может перейти в изменение вида 0 → 1 на выходе, и схема является h_1-надежной. При этом сами входные датчики, формирующие сигналы x, должны быть h_1-надежными и не давать ложной информации вида 0 → 1.

Теорема 4.2.1 накладывает весьма жесткие ограничения на способы построения безопасных комбинационных схем. Это следует из того, что единственными формами представления функций алгебры логики, у которых немонотонная операция применяется только к переменным функции, являются дизъюнктивная нормальная форма (ДНФ), конъюнктивная нормальная форма (КНФ) и их скобочные формы СДНФ, СКНФ. Поэтому имеет место:

ТЕОРЕМА 4.2.2. Схемная реализация функции алгебры логики является безопасной тогда и только тогда, когда она осуществлена по одной из четырех форм представления функции: ДНФ, КНФ, СДНФ и СКНФ.

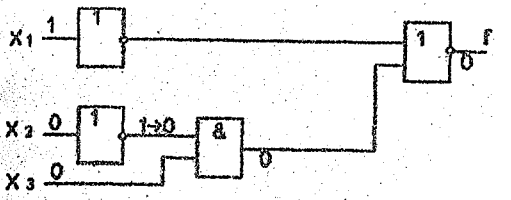


Рисунок 4.4

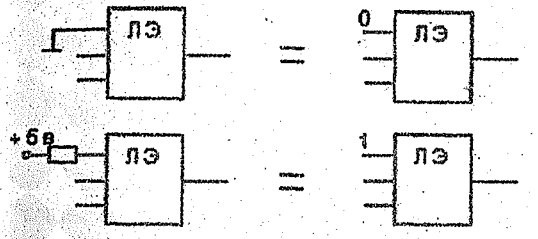


Рисунок 4.5

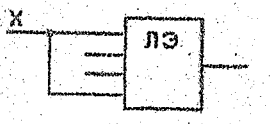


Рисунок 4.6

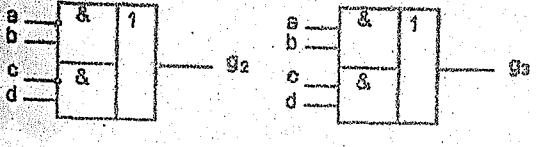


Рисунок 4.7

4.3 Функциональная полнота безопасных элементов

Рассмотрим вопрос о функциональной полноте безопасных элементов. Пусть имеется система функций $A = \{g_1, g_2, \ldots, g_k\}$.

Определение 4.3.1. Система функций A называется безопасно полной (безопасным базисом), если с помощью логических элементов, реализующих безопасно функции этой системы, можно реализовать безопасно любую функцию алгебры логики.

Система A может содержать и константы 0 и 1. Они реализуются соединением входов элементов с полюсами источников питания (рисунок 4.5). Надежность реализации констант определяется надежностью монтажных соединений. Это же относится к надежности реализации функции X (повторения), которая осуществляется за счет отождествления входов элементов монтажным соединением их между собой (рисунок 4.6).

Условия функциональной полноты безопасных элементов определяет следующая теорема.

ТЕОРЕМА 4.3.1. При наличии вполне надежных констант и надежного отождествления входов система A является безопасно полной тогда и только тогда, когда выполняются следующие условия: 1) система A содержит хотя бы одну немонотонную функцию; 2) система A содержит: а) монотонную функцию, которая не является дизъюнкцией или конъюнкцией, или б) конъюнкцию и дизъюнкцию.

Пусть задана система, которая удовлетворяет условиям теоремы: $A = \{0, 1, g_1, g_2, g_3\}$, где $g_1 = a$, $g_2 = ab \vee cd$, $g_3 = ab \vee cd$. Функция g_2 является немонотонной, а функция g_3 - монотонной и отличной от дизъюнкции и конъюнкции.

Функции g_2 и g_3 реализуются безопасными элементами (рисунок 4.7). Построим на этих элементах безопасную схему, вычисляющую функцию $f = (a \vee b)c \vee abd$. На рисунке 4.8,а,б,в показана реализация соответственно функций НЕ, ИЛИ, И. Они образуют безопасно полный набор элементов. Искомая реализация функции приведена на рисунке 4.9.

Если монтажные соединения не являются вполне надежными, то справедлива следующая теорема.

ТЕОРЕМА 4.3.2. При отсутствии вполне надежных констант и на-

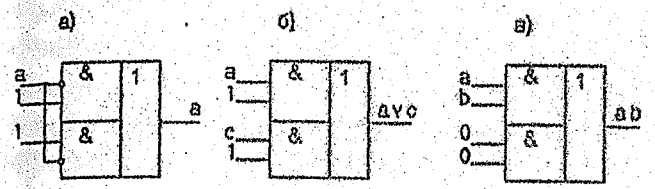


Рисунок 4.8

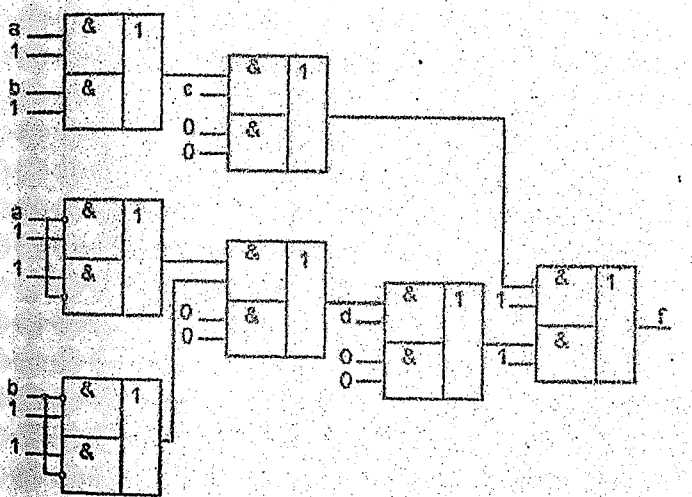


Рисунок 4.9.

дежного отождествления входов система А является безопасно полной тогда и только тогда, когда она содержит функции И, ИЛИ, НЕ.

4.4 Принципы построения безопасных схем с памятью на безопасных элементах

Исходными данными для синтеза безопасного автомата (схемы с памятью) являются таблица переходов и граф безопасных ложных переходов.

Принципы построения рассмотрим на примере синтеза синхронного автомата, заданного таблицей 4.4.1 и рисунком 4.10. В таблице 4.4.2 приведена кодированная таблица переходов, использующая один из вариантов безопасного кодирования состояний.

Таблица 4.4.1

S	a		Z
	0	1	
1	(1)	2	0
2	3	(2)	0
3	(3)	4	0
4	(4)	(4)	1

Таблица 4.4.2

S	y y	x		Z
		0	1	
1	00	(00)	01	0
2	01	10	(01)	0
3	10	(10)	11	0
4	11	(11)	(11)	1

Граф возможных ложных переходов для этого варианта (рисунок 4.11) является суграфом графа безопасных ложных переходов (рисунок 4.10).

Построим безопасный автомат, используя безопасные элементы И, ИЛИ, НЕ и безопасный D-триггер (в качестве элемента памяти). По таблице 4.4.2 находим логические функции, описывающие схему автомата:

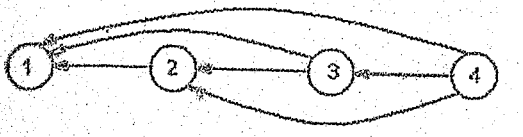


Рисунок 4.10

Рисунок 4.11

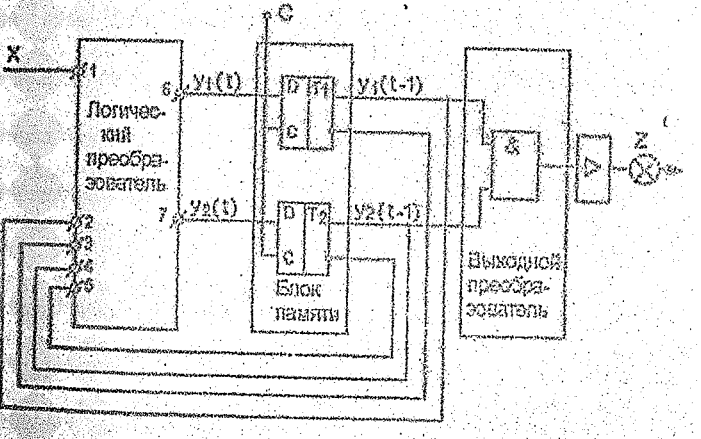


Рисунок 4.12

$y_1 = xy_1 \vee xy_2 \vee xy_1y_2 \vee y_1y_2$;

$y_2 = x \vee y_1y_2$;

$z = y_1y_2$.

На рисунках 4.12 и 4.13 показана реализация данной системы функций. При этом логический и выходной преобразователи построены как h_1-надежные схемы. Покажем, что в схеме автомата отсутствуют опасные отказы. Необходимо рассмотреть три типа отказов:

1) отказы D-триггеров вида 1 → 0 не опасны, т. к. применено безопасное кодирование;

2) отказы элементов логического преобразователя вида 1 → 0 приводят к изменению сигналов на выходах логического преобразователя в такте вида 1 → 0, что вызывает ложное переключение D-триггеров вида 1 → 0; это не опасно по п.1;

3) отказы элементов выходного преобразователя вида 1 → 0 не опасны, поскольку последний построен как h_1-надежная схема.

Часто для получения безопасного кодирования необходимо вводить избыточность по числу элементов памяти. Например, если из графа безопасных ложных переходов (рисунок 4.10) исключить ложный переход 3 → 1 (рисунок 4.14), то в этом случае нельзя найти безопасное кодирование с использованием элементов памяти.

Введем третий дополнительный элемент памяти и применим вариант безопасного кодирования, показанный в таблице 4.4.3. Граф возможных искажений показан на рисунке 4.15. При этом возникает проблема доопределения неосновных состояний таким образом, чтобы исключить опасные отказы.

В таблице 4.4.3 приведен наиболее простой из возможных способов доопределения: во всех клетках неосновных состояний проставляется код 000...00 и значение выхода Z=0. При таком кодировании любой отказ вида 1 → 0, который переводит схему из основного состояния в неосновное, в конце концов переводит схему в защитное необратимое состояние 000...00. На рисунке 4.16 показан процесс перехода схемы в необратимое состояние, если она находилась в устойчивом состоянии (0,110) и произошел отказ элемента памяти y_1 вида 1 → 0.

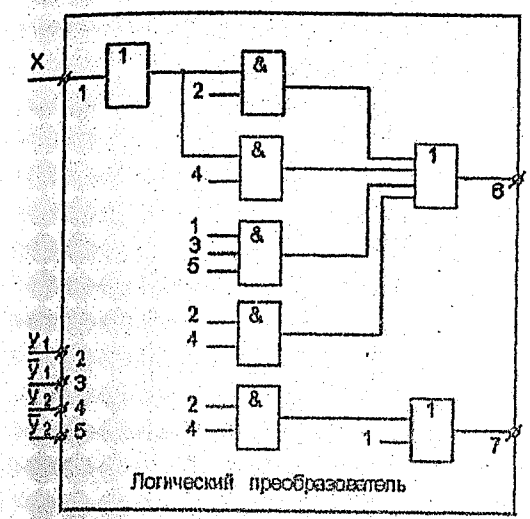


Рисунок 4.13

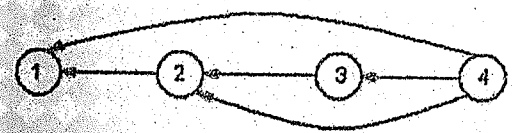


Рисунок 4.14

Рисунок 4.15

Таблица 4.4.3

	S	y y y	x		Z
			0	1	
Основные состояния	1	0 0 1	(001)	101	0
	2	1 0 1	110	(101)	0
	3	1 1 0	(110)	011	0
	4	0 1 1	(011)	(011)	1
Неосновные состояния	5	0 0 0	(000)	(000)	0
	6	0 1 0	000	000	0
	7	1 0 0	000	000	0
	8	1 1 1	000	000	0

Любой ложный переход в защитное необратимое состояние
опасен, т. к. в этом состоянии отключаются все выходы. Вывод сх
мы из него в основное начальное состояние производится искусс
твенным путем по цепям установки. Защитное необратимое соотоян
может находиться и среди основных состояний схемы. Примером тако
го состояния является окончательное замыкание стрелок и сигнал
в схемах электрической централизации. Выход из него осуществляет
ся с помощью искусственной разделки маршрутов.

В итоге можно сформулировать следующие основные принци
построения безопасных автоматов на безопасных элементах: 1) дл
кодирования состояний автомата выбирается один из вариантов без
пасного кодирования; 2) для всех неосновных состояний автома
определяется переход в защитное необратимое состояние; 3) все

неосновным состояниям приписываются значения выходов Z=0; 4) логический и выходной преобразователи строятся как безопасные схемы в соответствии с условиями теоремы 4.2.1.

5 ИСПОЛЬЗОВАНИЕ САМОПРОВЕРЯЕМЫХ СХЕМ ПРИ ПОСТРОЕНИИ БЕЗОПАСНЫХ СИСТЕМ

5.1 Структура самопроверяемого дискретного устройства

Самопроверяемые дискретные устройства (ДУ) относятся к классу систем с контролем в процессе функционирования.

Самопроверяемые ДУ содержат два блока (рисунок 5.1). Первый блок (собственно ДУ) реализует функции переходов и выходов. Второй блок (КС) представляет собой контрольную схему, назначение которой состоит в выработке сигнала контроля при возникновении неисправностей во внутренней структуре ДУ.

Контрольная схема рассматривается как элемент собственно структуры ДУ, выход контрольной схемы - как контрольный выход ДУ.

5.2 Принципы использования самопроверяемых ДУ в безопасных системах

Сигнал контроля используется для отключения объектов управления (ОУ) с помощью специальных устройств переключения (УП), которые должны иметь несимметричные отказы (рисунок 5.2).

В резервированных системах (дублированных, троированных) сигнал контроля используется для определения отказавшего комплекта аппаратуры (рисунок 5.3) и/или для дополнительного отключения выходов (рисунок 5.4), что позволяет увеличить кратность обнаруживаемых неисправностей (в дублированных системах - до четырех).

5.3 Принципы контроля ДУ

Основной принцип состоит в кодировании состояний ДУ кодом с обнаружением ошибок. Свойства ДУ определяются свойствами кода, использованного для кодирования внутренних состояний.

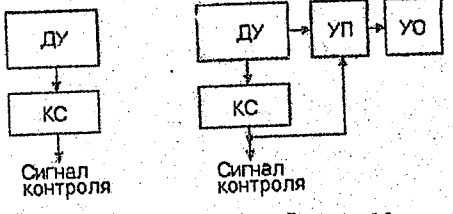


Рисунок 5.1 Рисунок 5.2

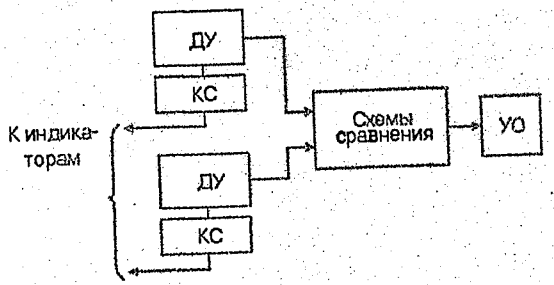


Рисунок 5.3

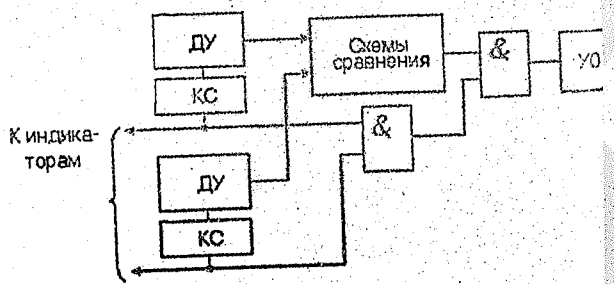


Рисунок 5.4

Эффективным является использование для кодирования кода с постоянным весом m (nCm-кода, n - число разрядов кодовых слов). В этом случае обеспечивается обнаружение в схеме ДУ всех одиночных неисправностей, а также всех сочетаний однонаправленных одиночных неисправностей (т.е. неисправностей одного вида: либо 1 → 0, либо 0 → 1).

Контроль ДУ может осуществляться либо по внутреннему состоянию, либо по выходному состоянию. При использовании nCm-кода КС фиксирует все состояния и вырабатывает сигнал контроля при нарушении веса. В этом случае КС называют m/n-тестером.

5.4 ДУ с контролем по внутреннему состоянию

Структура ДУ представлена на рисунке 5.5. На входы m/n-тестера подаются внутренние переменные $Y_1, Y_2, .., Y_n$ (выходы элементов памяти).

ДУ обладает следующим свойством. При нормальном функционировании ДУ и отсутствии в нем неисправности на его основных выходах $Y_1, Y_2, \ldots, Y_r$ присутствует рабочее выходное состояние, а на контрольных выходах $Y_1, Y_2, \ldots, Y_n$ - вектор с весом m. При возникновении неисправности во внутренней структуре ДУ на основных выходах $Y_1, Y_2, \ldots, Y_r$ устанавливается некоторое (отличное от рабочего) защитное состояние, а на контрольных выходах $Y_1, Y_2, \ldots, Y_n$ - вектор с весом, не равным m. При этом на выходе m/n-тестера формируется сигнал контроля.

5.5 ДУ с контролем по выходному состоянию

Структура ДУ представлена на рисунке 5.6. Выходные состояния кодируются кодом nCm. При необходимости вводятся дополнительные контрольные выходы $Y_{r+1}, \ldots, Y_{r+q}$.

На входы m/n-тестера подаются выходные переменные ДУ. ДУ обладает следующим свойством. При нормальном функционировании ДУ и отсутствии в нем неисправностей на основных выходах $Y_1, Y_2, \ldots, Y_r$ присутствует рабочее выходное состояние, на основных и контрольных выходах $Y_1, Y_2, \ldots, Y_r, Y_{r+1}, \ldots, Y_{r+q}$ - вектор с весом m. При

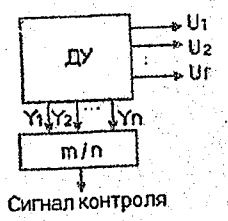


Рисунок 5.5

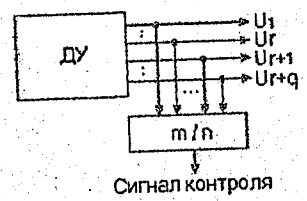


Рисунок 5.6

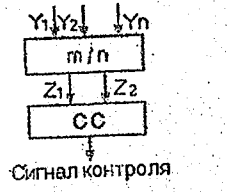


Рисунок 5.7

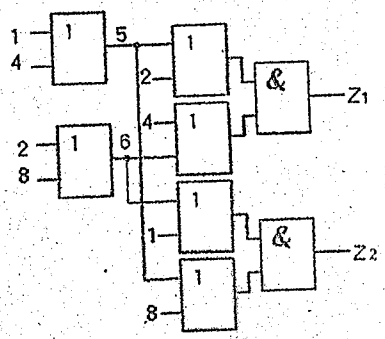


Рисунок 5.8

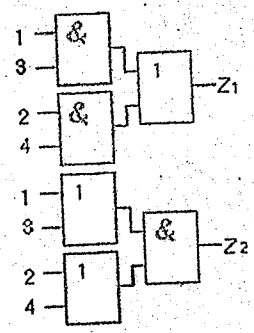


Рисунок 5.9

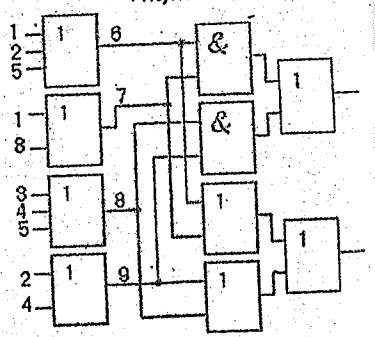


Рисунок 5.10

возникновении неисправности на основных выходах устанавливается защитное состояние, на основных и контрольных выходах - вектор с весом, не равным m. При этом на выходе m/n-тестера формируется сигнал контроля.

5.6 Самопроверяемое ДУ со свойством блокировки

Свойство блокировки связано с определением момента появления и длительности присутствия сигнала контроля.

ДУ обладает свойством блокировки, если при возникновении в его структуре неисправности на основных и контрольных выходах устанавливается защитное состояние не позднее того такта, в котором неисправность в первый раз проявляется на выходе, после чего защитное состояние сохраняется до тех пор, пока в ДУ не возникает новая неисправность. Соответственно в указанные моменты времени на выходе контрольной схемы присутствует сигнал контроля.

Принцип построения ДУ с блокировкой состоит в следующем. Внутреннее состояние ДУ кодируется кодом nCm. Это позволяет выделить на всем множестве внутренних состояний подмножество S основных состояний и подмножество R ошибочных (защитных) состояний. Логическая сеть ДУ строится таким образом, что любая одиночная неисправность или любая комбинация одиночных однонаправленных неисправностей переводит ДУ из множества S в множество R. После этого ДУ блокируется в множестве R, т.е. оно может выйти из множества R только искусственным путем (по цепям установки элементов памяти) или при возникновении новых отказов. Состояниям из множества R ставятся в соответствие защитные значения выходов. Переход автомата в множество R фиксируется контрольной схемой.

5.7 Определение самопроверяемого ДУ

Сформулируем указанные свойства самопроверяемых ДУ в терминах теории автоматов. Выделим на полном множестве выходных $\hat{Z}$ и внутренних $\hat{S}$ состояний ДУ множества основных (рабочих) состояний Z и S и некоторые множества защитных (ошибочных) состояний Z_r и S_r таких, что $Z \vee Z_r \subseteq \hat{Z}$, $Z \wedge Z_r = \varnothing$, $S \vee S_r \subseteq \hat{S}$, $S \wedge S_r = \varnothing$.

Определение 5.7.1. ДУ называется защищенным от неисправностей, если при возникновении любой неисправности из заданного класса на любой рабочей входной последовательности выходные состояния либо вычисляются правильно, либо принадлежат множеству защитных состояний Z_r.

Определение 5.7.2. ДУ называется самотестируемым, если для каждой неисправности из заданного класса существует хотя бы одна рабочая входная последовательность, на которой появляется хотя бы одно выходное состояние, принадлежащее множеству защитных состояний Z_r.

Определение 5.7.3. ДУ называется полностью самоуправляемым (ПСП), если оно защищено от неисправностей и является самотестируемым.

Защищенность от неисправностей исключает неправильные воздействия со стороны управляющего ДУ на объекты управления. Это есть основное требование к безопасным системам (fail safe system). Свойство самотестируемости исключает наличие в схеме ДУ необнаруживаемых неисправностей из заданного класса и устраняет возможность их накопления. При этом рабочие входные воздействия составляют одновременно и проверяющий тест. Таким образом, ДУ, удовлетворяющее определениям 5.7.1 - 5.7.3, в указанном смысле само себя контролирует.

5.8 Самопроверяемые тестеры

Тестеры в самопроверяемых ДУ рассматриваются как элементы структуры ДУ, поэтому в них также должны обнаруживаться неисправности. Тестеры строятся в виде самопроверяемых устройств с двумя выходами Z_1 и Z_2 (рисунок 5.7) и обозначаются m/n-СПТ. Они обладают двумя свойствами:

- свойством контроля входного вектора: выходы Z_1 и Z_2 принимают значение (1,0) или (0,1), если на входе тестера присутствует вектор кода nCm, и значение (0,0) или (1,1), если на вход поступает вектор с весом, отличным от m;
- свойством самопроверки: для любой единичной неисправности или любой комбинации одиночных однонаправленных неисправностей

тестера существует входной вектор с весом m, на котором выходы Z_1 и Z_2 принимают значения (0,0) или (1,1).

Тестер дополняется вполне надежной схемой сравнения (СС), которая непосредственно вырабатывает сигнал контроля при равенстве входных сигналов Z_1 и Z_2 (рисунок 5.7).

Тестеры характеризуются двумя оценками:

- сложностью L, которая равна суммарному числу входов логических элементов, принадлежащих структуре тестера;
- длиной проверяющего теста t, которая равна числу слов кода nCm, подача которых на вход тестера обеспечивает обнаружение всех одиночных и однонаправленных неисправностей.

5.9 Способ описания тестеров

Тестеры описываются системами функций алгебры логики. При этом используется принцип суперпозиции функций. Входные переменные тестера обозначаются цифрами от 1 до n, соответствующими индексам этих переменных. Для обозначения промежуточных функций, реализуемых на внутренних линиях схемы, также используются цифры от n+1 и далее. Логическая операция дизъюнкции обозначается знаком "+", а операция конъюнкции - знаком "×". Если с помощью конъюнкции связываются два скобочных выражения, то знак "×" опускается.

Промежуточные функции выделяются с таким расчетом, чтобы получаемая при этом система функций полностью отражала структуру схемы тестера. Для этого каждый промежуточный узел разветвления в схеме обозначается отдельной цифрой. Проверяющий тест T указывается в виде множества слов кода nCm, заключенных в фигурные скобки.

5.10 Каталог тестеров для равновесных кодов

Приведем описание наиболее часто используемых тестеров.

5.10.1 1/4-СПТ

Система функций (рисунок 5.8): 5=1+4, 6=2+3, Z_1=(2+5)×

×(4+6), Z_2=(1+6)(3+5). Оценки: L=16, t=4. Тест: T={1000,0100,
0010,0001}.

5.10.2 2/4-СПТ

Система функций (рисунок 5.9): Z_1=1×3+2×4, Z_2=(1+3)(2+4).
Оценки: L=12, t=4. Тест: T={0101,1001,0110,1010}.

5.10.3 1/5-СПТ

Система функций (рисунок 5.10): 6=1×2×5, 7=1+3, 8=3+4+5,
9=2+4, Z_1=6×7+8×9, Z_2=(6+7)(8+9). Оценки: L=22, t=5. Тест:
T={10000, 01000,00100,00010,00001}.

5.10.4 2/5-СПТ

Система функций (рисунок 5.11): 6=1+2, 7=3+4, 8=1×2, 9=3×4,
10=7+6, 11=5×7, 12=9+10, 13=8+11, Z_1=(11+12)(9+13), Z_2=(10+13)×
×(8+12). Оценки: L=30, t=6. Тест: T={10100,01010,01001,00101,
11000,00110}.

5.10.5 1/6-СПТ

Система функций: 7=1+2+5, 8=1+3+6, 9=3+4+5, 10=2+4+6,
Z_1=7×8+9×10, Z_2=(7+8)(9+10). Оценки: L=24, t=6. Тест:
T={100000,010000,001000,000100,000010,000001}.

5.10.6 2/6-СПТ

Система фукций: 7=2+3, 8=5+6, 9=(1+7)(4+8), 10=1×
11=2×3+5×6, 12=4×8, 13=9+12, 14=10+11, Z_1=(10+13)(12+14),
Z_2=(9+14)(11+13). Оценки: L=36, t=7. Тест: T={100100,01001,
001001,110000,011000,000011,000110}.

5.10.7 3/6-СПТ

Система функций: 7=1×2, 8=1+2, 9=4×5, 10=4+
Z_1=(3+8)(9+6×10)+3×7, Z_2=(6+10)(7+3×8)+6×9. Оценки: L=32, t=
Тест: T={111000,011100,001110,110001,100011,000111}.

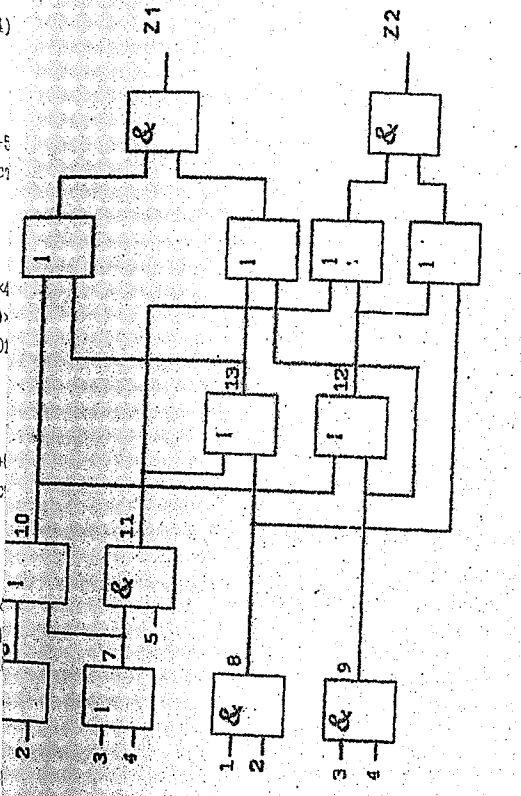


Рисунок 5.11

5.11 1/3-СПТ

Тестер для кода "1 из 3" представляет собой особый случай, т. к. он не может быть реализован в виде комбинационной схемы. На рисунке 5.12 представлена схема 1/3-СПТ, построенная в виде схемы с памятью, с характеристиками: L = 18, t = 5.

5.12 Самопроверяемый фиксатор ошибок

Фиксатор ошибок (ФО) представляет собой устройство (рисунок 5.13), имеющее два входа x_1 и x_2 и два выхода q_1 и q_2. Вход ФО является парафазным, т.е. допустимыми являются следующие комбинации сигналов (x_1,x_2): (1,0) - (0,1). Свойства ФО:

- если на вход ФО поступает парафазный сигнал и сама схема ФО исправна, то на его выходе (q_1,q_2) также присутствует парафазный сигнал - (0,1) или (1,0);
- если на вход ФО в некотором такте его работы поступают одинаковые сигналы x_1=x_2, то схема ФО блокируется в защитном состоянии и в том же такте на выходе устанавливаются одинаковые сигналы q_1=q_2 (0,0 или 1,1), которые сохраняются во всех последующих тактах работы независимо от состояния входов;
- при возникновении в схеме ФО одиночных неисправностей или любых комбинаций однонаправленных неисправностей схема также блокируется в защитном состоянии;
- вывод схемы ФО из защитного состояния возможен только по цепям установки.

В качестве ФО используются самопроверяемые парафазные триггеры. На рисунке 5.14 представлена схема парафазного асинхронного Т-триггера. Он имеет парафазный вход T^1T^0, парафазный выход Q^1Q^0 и работает в соответствии с таблицей переходов 5.12.1.

Схема состоит из четырех биотабильных ячеек и описывается формулами:

$$y_1 = T^0y_1 \vee T^1y_1;$$

$$y_2 = T^0y_2 \vee T^1y_2;$$

$$y_3 = T^0y_2 \vee T^1y_3;$$

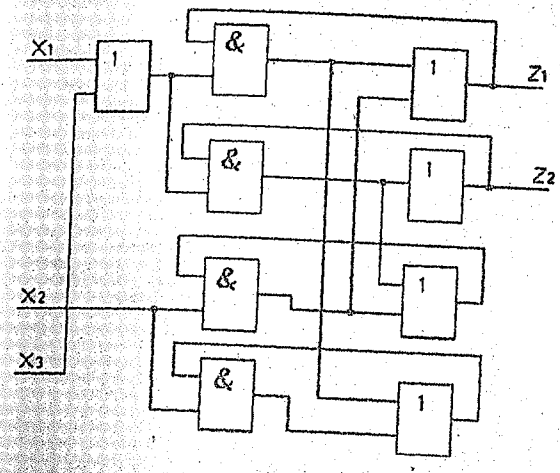


Рисунок 5.12

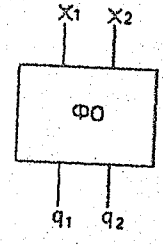


Рисунок 5.13

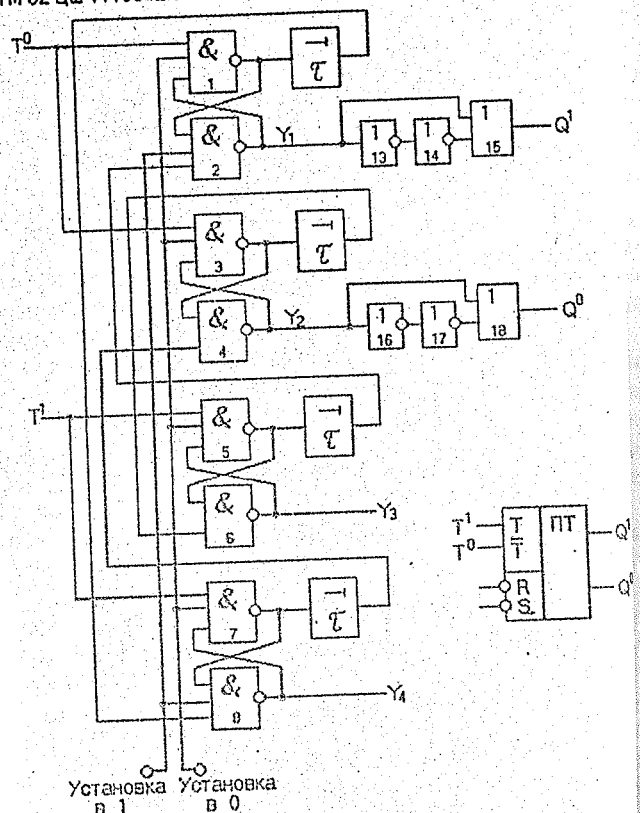


Рисунок 5.14

Таблица 5.12.1

$y_1y_2y_3y_4$	T^1T^0	
	01	10
0 1 1 0	0110,01	1010
1 0 1 0	1001	(1010),10
1 0 0 1	(1001),10	0101
0 1 0 1	0110	(0101),01

$y_4 = T^0y_1 \vee T^1y_4;$

$Q^1 = y_1; \quad Q^0 = y_2.$

Элементы 13, 14, 15 и 16, 17, 18 образуют несимметричные линии задержки, которые исключают непарафазность сигналов Q^1 и Q^0.

При кратковременной подаче логического нуля на вход "Установка в 0" и наличии сигналов T^1T^0=01 схема приходит в устойчивое состояние 0110 (состояние "0" триггера). При подаче нулевого сигнала на вход " Установка в 1" и наличии сигналов T^1T^0 - 01 схема приходит в устойчивое состояние 1001 (состояние "1" триггера). Полный цикл работы триггера происходит на входной последовательности сигналов T^1T^0 вида 01,10,01,10,01. При этом схема триггера последовательно проходит все свои состояния: 0110→1010→1001→0101→0110.

5.13 Внутренняя структура самопроверяемого ДУ

Структура ДУ состоит в общем случае из пяти блоков (рисунок 5.15). Блок входного преобразователя ВхП предназначен для реализации наборов входных переменных. Блок логического преобразователя ЛП вычисляет функции включения элементов памяти. Блок памяти

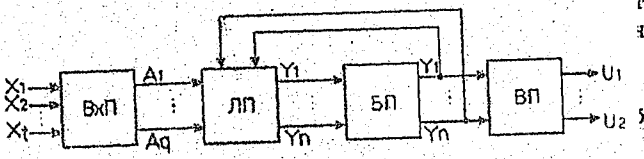


Рисунок 5.15

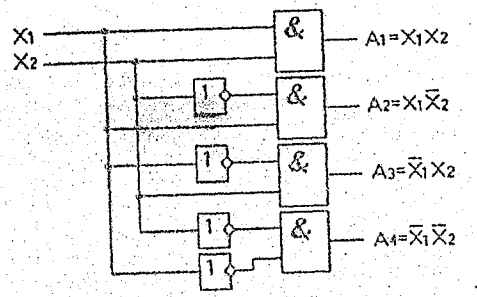


Рисунок 5.16

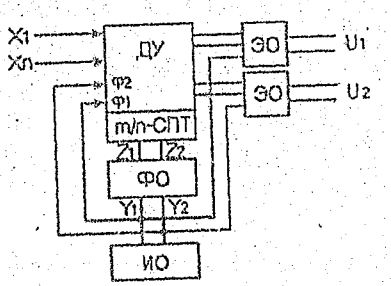


Рисунок 5.17

БП содержит все множество элементов памяти (реле, линии задержки, триггеры различного типа). Выходной преобразователь (ВП) предназначен для вычисления выходных функций.

5.13.1 Особенности построения блока ВхП

На выходах блока реализуются наборы входных переменных $a_1,\ldots,a_q$. Каждый набор $a_1,\ldots,a_q$ реализуется отдельной схемой. Пример такого построения приведен на рисунке 5.16 для ДУ, имеющего две входные переменные. В каждый момент времени только на одном выходе блока ВхП может быть сигнал 1.

Возможны три случая проявления одиночных неисправностей на выходах блока ВхП. В первом случае для всех выходов выполняется равенство $a_j = 0$ ($j\in\{1,2,\ldots,q\}$). Данная неисправность фиксируется блоками ЛП и БП, т. к. при этом на вход блока ЛП поступает вектор с весом V = 0, тогда как при исправном блоке ВхП поступает вектор с весом V = 1. Во втором случае имеют место равенства: $a_j = 1$ и $a_t = 1$ ($j \neq t$, $j,t\in\{1,2,\ldots,q\}$). Данная неисправность также инспируется блоками ЛП и БП, т.к. при этом на вход блока ЛП поступает вектор с весом V = 2.

Третий случай имеет место тогда, когда на выходе исправного блока выполняются соотношения $x_j = 1$, $x_t = 0$, а на выходе неисправного блока - соотношения $x_j = 0$, $x_t = 1$. Данная неисправность не фиксируется блоками ЛП и БП, т. к. при этом на вход ЛП поступает вектор с весом V = 1, как и в случае исправного блока ВхП. Такая неисправность возникает при дефектах схемы типа "обрыв входа". В этом случае защита осуществляется введением избыточности по входную информацию. Если входные состояния ДУ закодировать кодом с постоянным весом, то из структуры ВхП исключаются инверторы. Если такое кодирование невозможно, то целесообразно уменьшить вероятность возникновения неисправностей вида "обрыв входа" конструктивными методами или с помощью резервирования.

5.13.2 Особенности построения блока БП

Блок БП представляет собой совокупность элементов памяти.

Число элементов памяти определяется длиной кода nCm, принятого для кодирования внутренних состояний ДУ. Неисправность любого элемента памяти и любое сочетание их одноправленных отказов приводит к искажению принятого веса кода состояния, что обнаруживается контрольной схемой m/n-СПТ.

5.13.3 Особенности построения блока ЛП

В блоке ЛП реализуются функции включения элементов памяти. При кодировании состояний ДУ кодом nCm функции включения являются монотонными. Реализация блока ЛП может быть двух видов - раздельная и совместная. Раздельная реализация предусматривает использование каждого логического элемента в схеме включения только одного элемента памяти. При совместной реализации данное условие может не выполняться. Неисправности блока ЛП оказывают непосредственное влияние на работу элементов памяти и поэтому обнаруживаются из-за искажения вектора состояния внутренних переменных.

5.13.4 Особенности реализации блока ВП

В блоке ВП вычисляются выходные функции ДУ. В общем случае отказы элементов ВП не оказывают влияния на работу остальных блоков ДУ и поэтому не могут быть зафиксированы на основании искажения кода внутреннего состояния. Это следует из рисунка 5.15.

Наиболее просто контроль ВП осуществляется по выходному состоянию. В этом случае выходные состояния ДУ доопределяются (если это необходимо) путем введения дополнительных контрольных выходов так, чтобы они оказались закодированы кодом с постоянным весом. Функции выходов при этом будут монотонными. Любые комбинации однонаправленных неисправностей элементов ВП искажают вес выходного состояния.

Второй подход к контролю ВП состоит в полном его совмещении с блоком ЛП. В этом случае элементы блока ВП включаются в цепи обратных связей ДУ, в результате чего их отказы искажают вес кода внутреннего состояния.

5.14 Стратегии поведения самопроверяемых дискретных систем

На рисунке 5.17 представлена общая структура самопроверяемого ДУ с внешними схемами контроля. Дискретное устройство имеет рабочие входы $X_1,\ldots,X_n$, рабочие выходы $Y_1,\ldots,Y_n$ и контрольные выходы Z_1 и Z_2, которые формируются самопроверяемым тестером m/n-СПТ. Нарушение парафазности выходов Z_1 и Z_2 регистрируется ПСП-схемой фиксатора ошибок (ФО), играющей роль "последнего сторожа". При нарушении парафазности входов ФО блокируется в защитном состоянии, при котором нарушается парафазность его выходов и которое не зависит от последующего изменения входов. ФО включает индикатор отказа системы (ИО). После восстановления исправности ДУ фиксатор ошибки переводится по цепи установки в рабочее состояние. В качестве ФО может быть использован любой ПСП-триггер.

В безопасных системах при возникновении отказа и блокировке ФО возможны три стратегии в поведении ДУ:

- отключение всей системы;
- повторный запуск фиксатора ошибок;
- отключение рабочих выходов.

В первом случае организуется самопроверяемая обратная связь, когда выходы ФО подключаются к специальным тактовым входам Ф1 и Ф2 дискретного устройства. При нарушении парафазности на входах Ф1 и Ф2 отключается тактовое питание системы и ДУ преводится в защитное состояние. Другой способ отключения системы состоит в коммутации цепей питания на контактах специального контрольного реле, обмотка которого подключается к выходам ФО через самопроверяемые схемы включения реле ССВР (они описаны в разделе 7).

Рисунок 5.18 иллюстрирует вторую стратегию поведения ДУ при отказе - повторный запуск ФО. Эта стратегия применяется для повышения устойчивости дискретной системы относительно сбоев. Для включения реле К используется схема формирования импульсных сигналов. В ней выходы m/n-СПТ, на которых может длительно сохраняться статический парафазный сигнал, подключаются ко входам 2/4-СПТ. На другие входы 2/4-СПТ поступают парафазные импульсы от тактового генератора. При этом на выходе 2/4-СПТ формируется импульсный парафазный сигнал. Если в результате случайного сбоя на

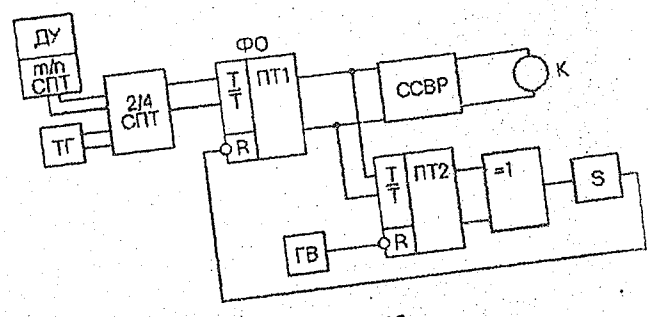


Рисунок 5.18

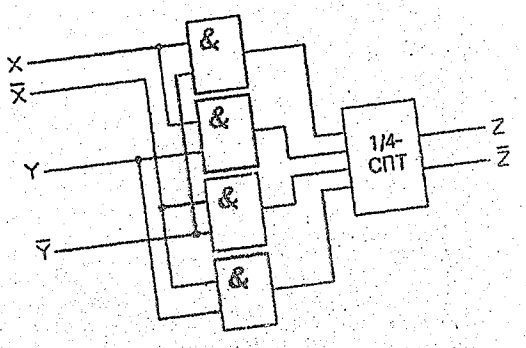


Рисунок 5.19

выходе m/n-СПТ нарушается парафазность сигналов, то блокируются триггеры Т1 и Т2. На выходах Т2 устанавливаются одинаковые сигналы и происходит запуск одновибратора S, который через некоторое время вырабатывает сигнал на установку ФО в рабочее состояние. Это время меньше, чем время отпускания реле К, поэтому в момент установки ФО питание системы еще не отключено.

Если действие сбоя было кратковременным и парафазность сигналов на выходе m/n-СПТ восстановилась, то после окончания сигнала установки триггер Т1 остается в рабочем состоянии, продолжает работу ССВР и реле К снова получает питание. Нормальное функционирование ДУ продолжается. В противном случае после окончания сигнала установки триггер Т1 снова блокируется, реле К отпускает якорь и выключает питание системы. Установка триггера Т2 в рабочее состояние происходит уже после завершения описанных процессов, что обеспечивается специальным генератором восстановления (ГВ) с низкой частотой работы.

Третья стратегия поведения ДУ при отказах состоит в отключении рабочих выходов. При этом парафазные выходные сигналы ДУ (рисунок 5.17) транслируются через специальные самопроверяемые элементы сравнения ЭО (рисунок 5.19). Схема ЭО имеет парафазный информационный вход (X, $\bar{X}$), который подключается к выходу $ДУ^{v}$, и парафазный контрольный вход (Y, $\bar{Y}$), связанный с выходами ФО. Парафазный выход (Z, $\bar{Z}$) повторяет значение сигнала (X, $\bar{X}$), если на входе (Y, $\bar{Y}$) имеется парафазный сигнал. В противном случае парафазность на выходе нарушается. Таким образом, при возникновении отказа и блокировке ФО в защитном состоянии схемы ЭО отключают выходы ДУ от нагрузки. Все три описанные стратегии могут быть использованы и одновременно, что обеспечивает высокий уровень безопасности, т. е. высокую вероятность отсутствия неправильного воздействия на объекты управления.

6 ПРОГРАММНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

6.1 Методы обеспечения надежности программных средств

Требование высокой надежности является первостепенным при проектировании систем железнодорожной автоматики. Построение таких систем на базе программно-управляемой аппаратуры (ПУА) порождает свою специфику в постановке и решении задач обеспечения высокой надежности. Эта специфика определяется тем, что специализация ПУА под конкретные технологические задачи производится программным способом. Программные средства в этом случае являются определяющими в реализации системой требуемых функций.

Согласно [6.1], под надежностью понимают свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность системы выполнять требуемые функции в заданных режимах и условиях применения. Применительно к безопасным СЖАТ под выполнением заданных функций следует понимать комплекс:

- функций, обеспечивающих реализацию технологических алгоритмов с учетом проверки условий обеспечения безопасности движения поездов;
- функций, определяющих поведение системы в условиях возникновения отказов и сбоев технических средств или проявления программных ошибок.

Таким образом, создание безопасных систем, логика функционирования которых отражена в виде программы, охватывает два аспекта (рисунок 6.1), в соответствии с которыми процесс создания безопасного программного обеспечения предусматривает комплекс мероприятий, направленных на:

- корректную постановку целевых функций системы;
- корректную программную интерпретацию целевых функций системы.

С точки зрения обеспечения безопасности актуальным является решение как первой, так и второй задачи. Например, правильно сформулированные функции программно-управляемой системы могут

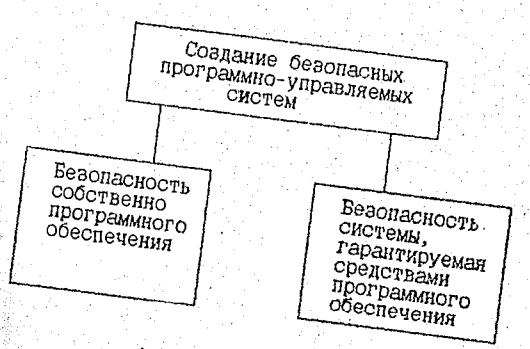


Рисунок 6.1

быть небезопасными в результате ошибки программиста или ошибочных средств трансляции. И наоборот, корректно выраженные в виде программы функции системы могут содержать ошибки функционального характера или быть функционально неполными в охвате последействий откавов.

Опыт разработки программных средств систем управления технологическими процессами, критичными к вопросам безопасности, показывает, что проблема обеспечения надежности программных средств (ПС) охватывает все этапы жизненного цикла программ (рисунок 6.2). Такое разнообразие методов определяется тем, что существует принципиальное различие в причинах нарушения работоспособности программных средств.

Одной из причин нарушения работоспособности программных средств является отклонение исходного текста программ от формализованного эталона и требований заказчика. Ошибки такого рода в практике программирования получили название ошибок программирования, возникающих в основном при разработке ПО и его сопровождения. В литературе рассматривается широкий спектр организационных и технических мероприятий по их предотвращению и обнаружению, которые позволяют выделить основные пути повышения надежности функционирования программных средств [6.2], такие как:

- разработка методологической теории надежности ПС, включающая исследование методов анализа надежности, выбор и обоснование критериев, исследование видов ошибок, причин их проявления и законов распределения, динамику изменения ошибок при отладке и модернизации программ, создание методов и методик измерения надежности программ;

- разработка и внедрение прогрессивных методов проектирования сложных ПС с заданной надежностью, применение структурных подходов к созданию ПС, позволяющих существенно снизить сложность программ, своевременно обнаруживать, локализовывать и предупреждать ошибки в программах;

- переход на широкое использование языков высокого уровня, учитывающих требования систем реального времени;

- разработка методов оценки и прогнозирования характеристик надежности, особенно на ранних этапах создания программ, методов

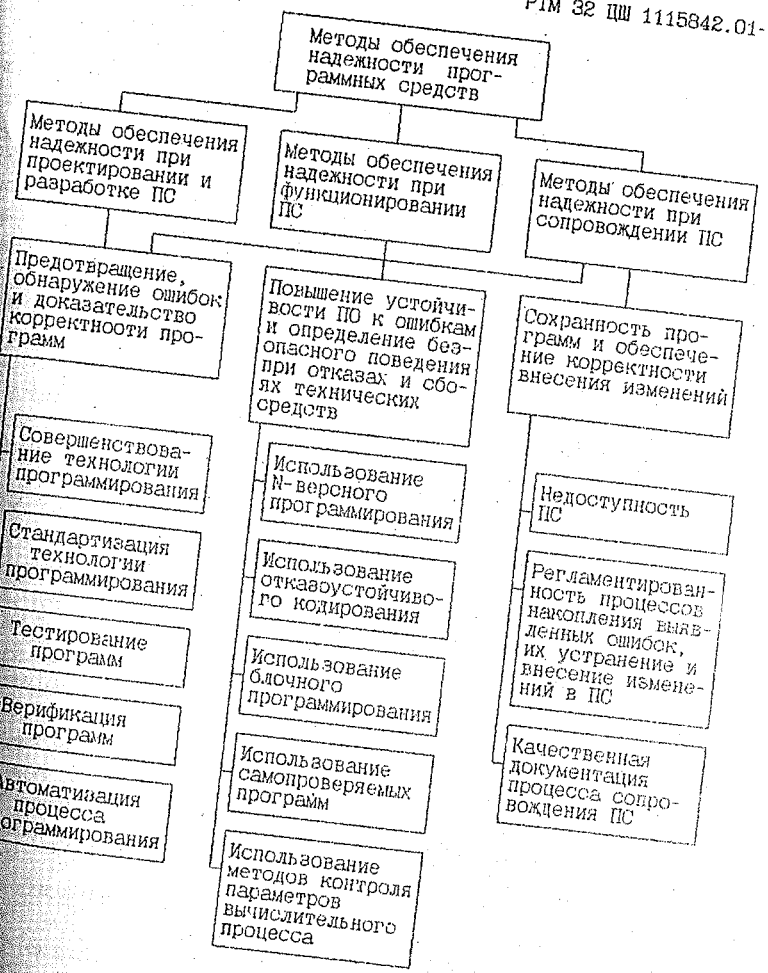


Рисунок 6.2

своевременного предупреждения и локализации ошибки, методов измерения статистических характеристик, определяющих устойчивость функционирования и надежность программ;

- разработка методов сопровождения программ и их модернизации в условиях длительного периода эксплуатации и массового тиражирования систем управления;

- существенное повышение уровня автоматизации процессов создания сложных комплексов программ на разных стадиях их жизненного цикла, разработка методов автоматизации управления процессами проектирования программ и целенаправленного планирования технико-экономических показателей разработки.

Основным методом обнаружения ошибок программ является их тестирование, в основе которого лежит тот факт, что программа любой сложности при строго фиксированных исходных данных и абсолютно надежной аппаратуре исполняется по однозначно определенному алгоритму. Исполнение всех маршрутов программ является сложной комбинаторной задачей, объем которой определяется произведением:

ПОЛНЫЙ ПЕРЕБОР ВХОДНЫХ СИТУАЦИЙ × ЧИСЛО СОСТОЯНИЙ ВЫЧИСЛЕНИЙ.

С целью оптимизации этого процесса необходимо использовать методы упорядочения и систематизации процесса, а также методы тестирования по различным стратегиям и параметрам. Метод тестирования (рисунок 6.3) базируется на выделении факторов и параметров, позволяющих эффективно распределять ресурсы тестирования на разных стадиях разработки программ [6.3].

Ошибки второго вида определяются прежде всего отказами и сбоями аппаратных средств. Эффективность методов их обнаружения определяется качеством подхода к синтезу функций безопасности:

- полнотой анализа поведения системы при возникновении ошибок аппаратуры и программных средств;

- полнотой охвата конкретного метода или совокупности методов реализации функций безопасности;

- способностью функций безопасности к обнаружению собственных ошибок;

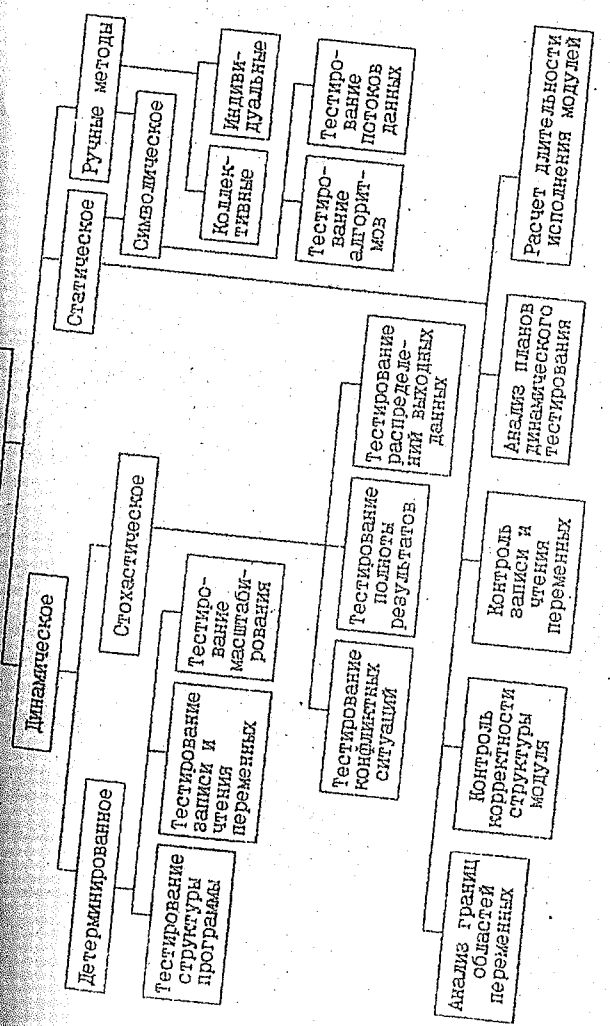


Рисунок 6.3

- степенью независимости функций безопасности от исправности аппаратных средств.

6.2 Специфика программного обеспечения как средства контроля

Основной функцией с точки зрения обеспечения безопасности СЖАТ является функция контроля правильности функционирования, качество которой определяется вовможностью средств контроля адекватно оценить состояние технических средств в заданный промежуток времени. Необходимость применения ПО для процедур контроля определяется прежде всего особенностями аппаратуры (МП, микроЭВМ) как объекта контроля [6.4]:

- неразделимостью аппаратуры и ПО;
- функциональной замкнутостью;
- высокой сложностью БИС.

Использование ПО как средства контроля правильности функционирования имеет свою специфику, которую необходимо учитывать при создании безопасных программно-управляемых систем.

С одной стороны, привлечение программных средств к процессу контроля позволяет повысить разрешающую способность контроля и полноту диагностирования системы. С другой стороны, такие особенности программ, как последовательный характер обработки команд программы и аппаратная зависимость программных процедур контроля, оказывают существенное влияние на достоверность, оперативность, покрытие неисправностей средств контроля.

Последовательный характер обработки приводит к необходимости чередования процедур основной программы с контрольными. При таком варианте контроля, тем более, если он ориентирован на состояние технических средств, можно выделить два негативных момента, влияющих на достоверность контроля:

- отказ (сбой) технических средств приходится на момент реализации основной программы или ее части;
- отказ технических средств приходится на момент выполнения контрольной процедуры.

По этой же причине при реализации контроля средствами ПО в значительной мере увеличивается латентность ошибки, т.е. период

времени между возникновением неисправности и ее обнаружением. В существующих методах программного контроля оперативность контроля обычно соизмерима с некоторыми заданными значениями программных единиц (элемента, модуля, блока, программы).

Аппаратная зависимость процедур контроля подразумевает тот факт, что в целях реализации основной программы и программ контроля используются одни и те же технические средства. Поэтому ошибки, искажающие основной алгоритм, ставят под сомнение результат работы контрольной программной процедуры.

Анализ существующих методов контроля показывает, что использование в этих целях только программных средств в значительной мере сужает класс выявляемых неисправностей. В основном программные методы ориентированы на содержательную проверку результатов вычислений. В этом смысле целесообразным является дополнение их методами контроля формальной составляющей процесса вычисления (динамики процесса вычисления, фактической последовательности команд, структуры программы).

6.3 Основные понятия и критерий оценки методов контроля

Возможность использования программного обеспечения как средства контроля основывается на следующем положении. С программно-аппаратной точки зрения модель вычислительной системы может быть представлена:

- на функциональном уровне

Мф=(X,Y,Q,S,F),

где X,Y - множество состояний входов-выходов объекта;
Q - множество внутренних состояний;
S - размеченная принципиальная схема;
F - множество функций переходов и функций выходов всех функциональных узлов схемы;

- на программном уровне

Мп=(X,Y,T,N,P),

где T - граф-схема алгоритма;
N - множество линейных участков;
P - множество предикатов.

Из свойства преемственности модели имеем тождественное отображение Мп на Мф и соответственно (T, N, P) на (S, F). Определим тройку (T, N, P) как программный блок. Между программным блоком и схемным представлением может быть установлено прямое соответствие. Каждому программному блоку соответствуют элементы схемы, которые активизируются при выполнении данного программного блока. В результате с каждым программным блоком отождествляется реализующая его подсхема функциональной схемы объекта.

Важнейшим следствием данного утверждения является вывод о том, что любая ошибка в аппаратной части (ошибка, при которой продолжается процесс функционирования) может быть описана как ошибка программы, т.е. ошибка аппаратуры может быть смоделирована и обнаружена программным способом.

В микропроцессорных вычислительных системах аналогом программного представления аппаратных отказов является схемная система команд. Это позволяет установить однозначное соответствие между отказами аппаратных средств и их интерпретацией в виде команды или группы команд конкретной вычислительной системы, т.е. определить программную модель отказа. Такое соответствие может быть задано в виде таблицы покрытия, где в столбцах перечислены ошибки Q, а в строках результат их интерпретации вычислительной системой. Дадим определение возможных ошибок. При этом введём следующие обозначения: N - линейный оператор, A - управляющий оператор, P - предикатный оператор.

1. Ошибкой первого типа Q_1 называется ошибка, заключающаяся в замене одного линейного оператора другим:

$$Q_1: N_i - N_j.$$

2. Ошибка типа Q_2 - замена одного предикатного оператора другим:

$$Q_2: P_i - P_j.$$

3. Ошибка типа Q_3 - замена одного управляющего оператора другим:

$$Q_3: A_i - A_j.$$

4. Ошибка типа Q_4 - замена линейного оператора предикатным:

$$Q_4: N - P.$$

5. Ошибка типа Q_5 - замена линейного оператора управляющим:

$$Q_5: N - A.$$

6. Ошибка типа Q_6 - замена предикатного оператора линейным:

$$Q_6: P - N.$$

7. Ошибка типа Q_7 - замена предикатного оператора управляющим:

$$Q_7: P - A.$$

8. Ошибка типа Q_8 - замена управляющего оператора предикатным:

$$Q_8: A - P.$$

9. Ошибка типа Q_9 - замена управляющего оператора линейным:

$$Q_9: A - N.$$

В таблице 6.1 приведены результаты возможных программных интерпретаций перечисленных ошибок, которые обычно приводят к искажению логики программы; искажению структуры программы; разрушению

Таблица 6.1

Результат последействия	Вид ошибки								
	Q_1	Q_2	Q_3	Q_4	Q_5	Q_6	Q_7	Q_8	Q_9
Искажение данных программы	+	+	+			+		+	+
Невывод результата		+	+	+	+		+	+	+
Изменение временных параметров программы	+		+	+		+			
Прерывание процесса вычисления			+		+		+		

программы и проявляются в искажении данных программы (промежуточных, выходных) S; искажению параметров программы K; нарушению контрольных соотношений M.

Поведение вычислительной системы однозначно определяется последовательностью состояний, которые она проходит и которые характеризуются определенными значениями (S, K, M). Если поставить в соответствие этим значениям правильную интерпретацию программы техническими средствами, то, контролируя значения этих параметров, можно определить наличие искажения в алгоритме функционирования программно-управляемых средств. С учетом сказанного можно выделить следующие методы контроля правильности функционирования (рисунок 6.4).

При определенной ориентации программных методов контроля такой подход позволяет количественно оценить эффективность конкретного метода контроля. В качестве критерия эффективности программных методов контроля можно ввести вероятность обнаружения отказов K, которая зависит от вероятности появления ошибок каждого из типов, указанных в таблице 6.1, и обнаруживающей способности выбранного метода контроля:

$$K = \sum_{i=1}^{9} W_i \cdot K_{об},$$

где $K_{об}$ - вероятность обнаружения ошибок данным методом контроля;

W_i - относительная доля ошибок i-го типа.

6.4 Программные методы обеспечения безопасности

6.4.1 Самопроверяемые программы

Цель: получить программы, удовлетворяющие свойствам защищенности и самотестируемости относительно определенного класса неисправностей.

Область применения: локальные микропроцессорные автоматы сбора и обработки информации, части программ, критичные к вопросам безопасности.

Описание. Метод построения самопроверяемых программ базиру-

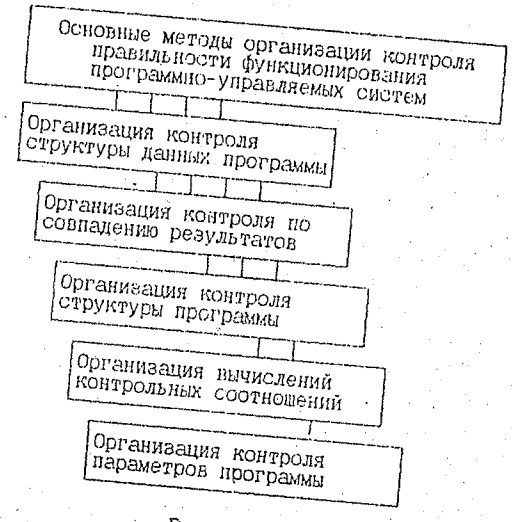


Рисунок 6.4

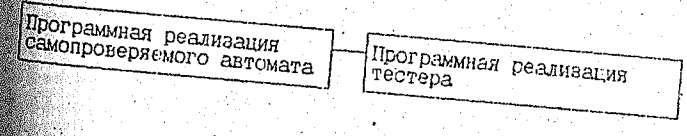


Рисунок 6.5

ется на результатах синтеза самопроверяемых конечных автоматов [6.5]. Идея метода заключается в следующем. Для заданного алгоритма управления находится функциональное описание выполняющего этот алгоритм автомата. Кодирование состояний автомата производится равновесным кодом nCm, по результатам которого строится система функций, монотонных относительно переменных кодового вектора. Данное свойство позволяет контролировать состояние переменных системы функций и вычислять защитный вектор (вектор, отличный от кодового слова nCm) в результате их искажений (одиночных искажений или любой комбинации однонаправленных искажений переменных слова состояния автомата). При этом контроль принадлежности слова состояния автомата множеству векторов с весом nCm производится программной реализацией самопроверяемой комбинационной схемы. Таким образом, самопроверяемая программа представляет собой последовательность программных модулей (рисунок 6.5), один из которых выполняет собственно алгоритм управления, а второй контролирует правильность этого вычисления.

Основные преимущества

1. Показанная на рисунке 6.5 структура хорошо согласуется с понятием программного модуля, облегчая процесс контроля, локализации и восстановления процесса вычисления.

2. Структура самопроверяемых программ обладает свойством блокировки в защитном состоянии.

3. Способ представления информации в синтезируемой программной системе (кодирование входных, выходных, внутренних переменных) позволяет сочетать программный контроль с аппаратными средствами контроля, основанными на использовании парафазной логики.

Проблемы и недостатки. Данный метод приводит к увеличению кода программы. Покрывает только класс неисправностей, эквивалентных искажению кодового вектора слова состояния автомата, что затрудняет количественную оценку покрытия. Охватывает только класс логических алгоритмов управления.

Взаимосвязь с другими методами. В комбинации с методами защищенного программирования дает хорошие результаты.

6.4.2 Защищенное программирование

Цель: получить программы, которые обнаруживают ошибки, проявляющиеся в аномальных передачах управления, передачах данных, разрушении части объектного кода, и реагируют на них заранее определенным образом.

Область применения: микропроцессорные вычислительные системы.

Описание. При реализации защищенного программирования можно выделить несколько технических приемов, одни из которых преследуют цель уменьшить, по возможности, разрушающее влияние ошибок на программу [6.6]. Эти методы основаны на:

- детальном анализе команд конкретной вычислительной системы с целью прогнозирования поведения системы при возможной их модификации из-за возникновения неисправностей аппаратных средств (искажения байтности команд, возникновения нежелательных команд);
- ограничении использования команд определенного типа;
- введении в структуру программы команд, выполняющих функции компенсаторов, пассивных с алгоритмической точки зрения, но активных с точки зрения контроля.

Второй подход связан с диагностической модификацией основной программы, позволяющей отслеживать фактическое выполнение последовательности команд, целостность структуры программы [6.7].

Основные преимущества. Данный метод хорошо формализуем, что позволяет автоматизировать процесс модификации исходного текста программы с учетом конкретной спецификации команд, видов программ, учитываемого классов отказов.

Проблемы и недостатки. Приводит к увеличению объектного кода программы. Накладывает определенные ограничения на процесс программирования. Не контролирует искажения данных программы.

Взаимосвязь с другими методами. См. п. 6.4.1.

6.4.3 Тестирование

Цель: обнаружение отказов аппаратных средств с целью предотвращения их влияния на выполнение основного алгоритма.

Область применения: микропроцессорные вычислительные систе-

мы.

Описание. Процесс контроля методом тестирования предусматривает поочередное выполнение тестовых и программных процедур. При этом их взаимное чередование может быть произвольным и определяется объемом теста. Так, например, в методе блоков восстановления [6.8] выполнение приемочного теста производится после реализации определенной программной процедуры. В методе программирования утверждений предусматривается проверка предусловий (проводится тестирование исходных условий на достоверность) и постусловий (тестируется результат выполнения последовательности операторов).

В МП-системах нашло широкое применение тестирование технических средств методом раскрутки, т.е. сначала тестируется ядро системы (при этом используется способность МП к самотестированию), а затем МП принимает участие в процессе тестирования окружений.

При этом разработка теста может быть ориентирована на любой уровень модели программно-аппаратных средств МП-системы.

Основные преимущества. Увеличивается глубина контроля. Упрощается процесс создания программ технологических алгоритмов, т.к. процесс создания тестового программного обеспечения может рассматриваться как процесс независимый, ограниченный только параметрами управляемого технологического процесса.

Проблемы и недостатки. Процесс тестового контроля не обнаруживает неисправностей типа "сбой аппаратных средств".

Взаимосвязь с другими методами. Может рассматриваться как дополнительное средство контроля. Например, для обеспечения заданной глубины контроля достаточно сочетать тестирование элементов программы с контролем данных и фактического завершения программы.

6.4.4 N-версионное программирование

Цель: обнаружение оставшихся ошибок проектирования программного обеспечения, отказов аппаратных средств с целью предотвращения критических отказов, влияющих на безопасность системы.

Описание. N-версионное программирование предусматривает N-разовую реализацию данной программы различными способами. Эффективность данного метода определяется прежде всего степенью непохожести программных компонент, сводящих к минимуму появление одинаковой реакции при нарушении работы технических средств или наличии программных ошибок. Если выделить в ПО две составляющие - логическую структуру и данные, то для первой из них имеется несколько вариантов достижения определенной степени неповторимости:

а) создание версий программы разными программистами или коллективами программистов;

б) использование упрощенной модели программы в качестве другой версии;

в) использование разных методов логической организации программ;

г) использование различных версий языков или разных версий компиляторов с одного и того же языка.

Основные преимущества. Данный подход позволяет контролировать как состояние технических средств, так и наличие программных ошибок.

Проблемы и недостатки. Приводит к значительному увеличению объектного кода программы и затрат на разработку.

Взаимосвязь с другими методами. В целях корректного сравнения результатов работы вариантов программ могут использоваться самопроверяемые программы.

7 БЕЗОПАСНЫЙ ИНТЕРФЕЙС

Важной проблемой при построении безопасных систем является организация сопряжения микроэлектронной аппаратуры железнодорожной автоматики и телемеханики с исполнительными объектами. Известны два основных подхода к организации сопряжения (интерфейса) различных частей управляющего комплекса:

- жесткая унификация и стандартизация входных и выходных параметров элементов комплекса;
- использование специализированных функциональных блоков, обладающих в той или иной мере адаптивными характеристиками по входам-выходам.

В настоящее время производится и эксплуатируется много различных исполнительных объектов железнодорожной автоматики и теле-

механики с разнообразными характеристиками по входам-выходам, унифицировать которые не представляется возможным. Поэтому чаще используется второй путь построения устройств сопряжения с объектами (УСО). Кроме того, специфичные для ответственных дискретных систем требования безопасности, как правило, не позволяют использовать выпускаемые промышленностью УСО для управляющих ЭВМ.

7.1 Требования к специализированным УСО

Структура безопасной системы в общем виде приведена на рисунке 7.1. Она состоит из управляющего вычислительного комплекса УВК (обычно дублированного или мажоритированного), восстанавливающего органа ВО, управляющего выходного преобразователя ВП, исполнительных объектов ИО и контрольного входного преобразователя ВхП.

Задачей ВО является формирование сигналов управления при совпадении всех или большинства выходных сигналов УВК. ВП обеспечивает энергетическое согласование электронных элементов с ИО, а также исключает воздействие на ИО при повреждении элементов ВО. В ряде случаев разделить управляющую часть УСО на ВО и ВП затруднительно, т.к. в их состав входят одни и те же элементы. Блок ВхП обеспечивает формирование и передачу в управляющий вычислительный комплекс достоверных сигналов о состоянии ИО.

К УСО САТ предъявляются следующие основные требования [7.1]-[7.6]:

1) обеспечение временного и энергетического согласования электронных схем и ИО;

2) обеспечение минимально допустимой вероятности возникновения ложного сигнала включения ИО на выходе УСО при любом отказе его элементов;

3) обеспечение максимально допустимой чувствительности к электромагнитным помехам и влияниям;

4) сохранение временных и энергетических параметров УСО в заданных пределах в течение всего срока эксплуатации;

5) высокая технологичность в производстве в сочетании с низкой стоимостью.

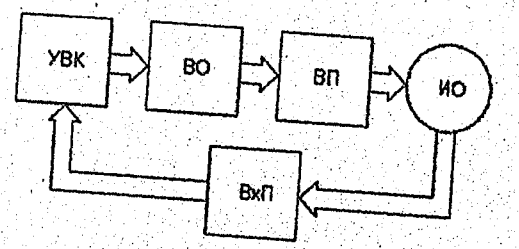


Рисунок 7.1

Схемные решения УСО не должны иметь опасных отказов, т. е. с определенной вероятностью должны исключать ложное включение ИО на выходе УСО при любом отказе его элементов. Обычно учитываются отказы, выражающиеся в появлении следующих событий: короткого замыкания, обрыва элементов или соединений; трансформации одного типа полупроводникового элемента в другой; самовозбуждения электронных схем; кратковременного или длительного отключения источника питания; повреждения источника питания, при котором на его шинах появляется значительная переменная составляющая; изменения параметров элементов или режимов их работы в установленных пределах; появления двух и более отказов элементов или соединений между точками схемы, не выявленных за время нахождения схемы в статическом состоянии.

Для исключения опасных отказов в УСО необходимо диагностировать полупроводниковые (электронные) элементы путем периодического переключения их из состояния логической 1 в 0 и из 0 в 1.

7.2 Классификация элементов сопряжения

УСО условно можно разделить на две части: элементы вывода управляющей информации и элементы ввода контрольной информации о состоянии исполнительных объектов. В цепях железнодорожной автоматики и телемеханики, к которым не предъявляются требования безопасности, как правило, применяют стандартные УСО, выпускаемые промышленностью в составе управляющих ЭВМ и контроллеров. Специализированные (безопасные) УСО разрабатываются на основе вышеперечисленных требований, а также методов, которые будут рассмотрены ниже. В зависимости от используемой элементной базы их можно разделить на релейные и электронные (бесконтактные) УСО.

На рисунке 7.2 приведена классификация методов построения безопасных УСО [7.5], [7.6]. Наиболее часто их выполняют в виде функциональных преобразователей (ФП) с несимметричным отказом, у которых при появлении неисправности искажаются передаточные функции. Возникающие в этом случае выходные сигналы неисправного ФП не должны приводить к ложному включению ИО, т.е. при возникновении отказа ФП должны переходить в защитное состояние.

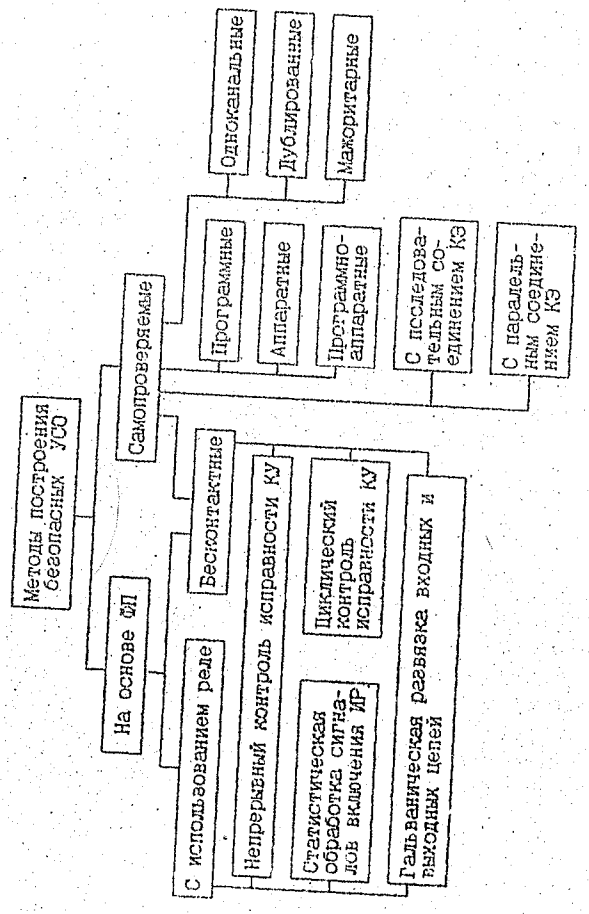


Рисунок 7.2

Наиболее широко в настоящее время применяются ФП с использованием безопасных реле, контакты которых коммутируют рабочие цепи ИО. Такие ФП иногда называют устройствами включения исполнительных реле (УВИР) [7.1]-[7.6].

Преимущества такого решения в том, что реле имеют высокую устойчивость к электромагнитным помехам и перенапряжениям, являются элементами идеальной гальванической развязки с несимметричным отказом. Недостатками являются ограниченный ресурс реле и потребность в профилактическом обслуживании релейно-контактных схем, а также специфичность производства релейных приборов.

Второй путь реализации УСО - построение полностью бесконтактных схем [7.7]. В этом случае не требуется профилактического обслуживания, УСО более технологичны в изготовлении, не содержат специализированных элементов. Однако проблема безопасности при этом решается более сложными методами, что определяет и более высокую сложность УСО и затрудняет доказательство достижения требуемого уровня безопасности. В настоящее время этот путь менее исследован, но он является наиболее перспективным для безопасных систем, особенно в тех случаях, когда применение релейных приборов затруднено.

7.3 Устройства включения исполнительных реле

Для того чтобы обеспечить безопасность устройств включения исполнительных реле при повреждении электронных коммутирующих элементов, в релейных УСО используются элементы контроля их динамической работы, играющие роль функциональных преобразователей. С этой целью, как правило, применяют трансформаторную и конденсаторную гальванические развязки. Однако импульсные трансформаторы являются нетехнологичными элементами, поэтому усилия разработчиков в последнее время направлены на выполнение УВИР без намоточных элементов.

УВИР являются ФП, работа которых в общем виде описывается выражениями:

$$y = F(x), \quad F(x) = \begin{cases} 0 \text{ при } x=0; \ A_i=0 \\ U < U_{n2} \text{ при } A_i=1 \\ U > U_{n1} \text{ при } x=1; \ A_i=0 \end{cases}, \quad (7.1)$$

где $F(x)$ - закон преобразования входных сигналов;

x - входная переменная ФП;

A_i=0; 1 - переменная, отражающая отсутствие или наличие отказов в ФП;

U - значение сигнала на выходе ФП;

U_{n1}, U_{n2} - значение напряжения срабатывания и отпускания ИР соответственно.

Анализ поведения УВИР при отказах его элементов заключается в проверке выполнения условий (7.1).

На рисунке 7.3 приведена схема УВИР, выполненная с динамическим контролем работоспособности коммутирующих элементов. Принцип ее работы основан на поочередном включении перекрестно установленных пар транзисторов VT1 и VT4, VT2 и VT3. Этим обеспечивается защита схемы от появления однократной неисправности типа "пробой" цепи *коллектор-эмиттер* всех транзисторов. Данная схема может использоваться для включения реле, контролирующих исправность микроэлектронной аппаратуры, т.к. они постоянно включены и выключаются при любой однократной неисправности. Данную схему нельзя использовать для включения исполнительных реле, которые могут в процессе работы находиться в выключенном состоянии, т.к. в это время возможно накопление неконтролируемых неисправностей, приводящих к ложному включению реле (например пробой транзисторов VT1 и VT4 или VT2 и VT3).

На рисунке 7.4 приведена схема УВИР [7.3], защищенного от двукратных неисправностей, в котором используется конденсаторная гальваническая развязка, выполняющая функции дифференцирования и интегрирования:

$$i_{C_1} = \frac{C_1 \, dU_{C_1}}{dt}; \quad U_C = U_C(0) + \frac{1}{C_2} \int_0^t i_{C_2} \, dt. \quad (7.2)$$

В данной схеме возможно накопление отказов в течение ее эксплуатации (в период между профилактиками). При пробое C1, VD2 и

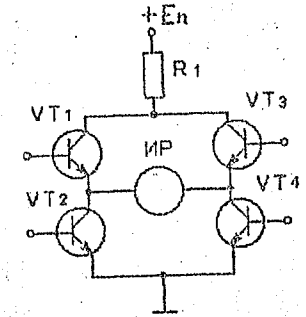


Рисунок 7.3

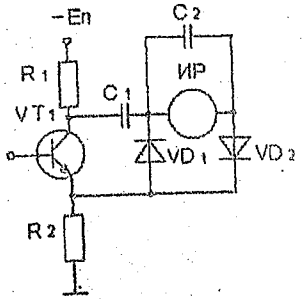


Рисунок 7.4

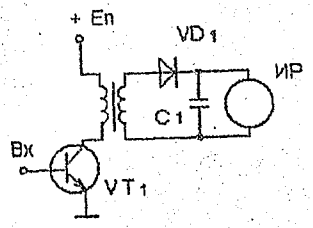


Рисунок 7.5

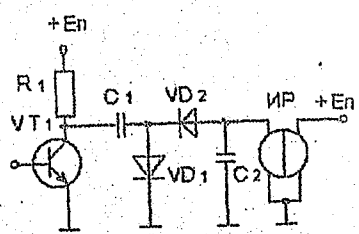


Рисунок 7.6

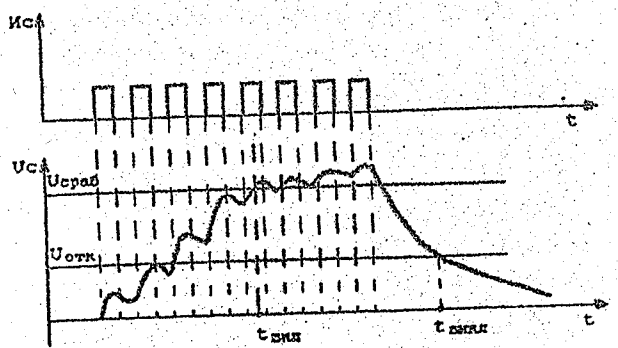


Рисунок 7.7

обрыве VD1 условие (7.1) не соблюдается, значит использовать эту схему в УСО, отвечающем требованиям безопасности, не рекомендуется.

На рисунке 7.5 изображена наиболее распространеная схема УВИР [7.2]. Безопасное поведение этой схемы при отказах обеспечивается за счет двойного преобразования входных импульсных сигналов - дифференцирования с помощью трансформатора и интегрирования с помощью диода и конденсатора:

$$U_T = M\frac{di_T}{dt}\ ;\quad U_C = U_C(0) + \frac{1}{C}\int_0^t i_C dt\ , \qquad (7.3)$$

где U_T, U_C - напряжения соответственно на выходе трансформатора и на конденсаторе;

M - взаимная индуктивность обмоток трансформатора;

$U_C(0)$ - напряжение на конденсаторе в момент времени t=0;

C - величина емкости конденсатора;

i_T, i_C - ток в цепи соответственно трансформатора и конденсатора.

При нарушении любого из этих двух законов преобразования сигналов на выходе схемы либо отсутствует напряжение, либо оно меньше напряжения выключения, поэтому ИР отпустит свой якорь.

При использовании в схеме (рисунок 7.4) в качестве выходного устройства поляризованного реле с несимметричным отказом (например ПЛ-3) при отказе ее элементов будет соблюдаться условие (7.1), т.е. она будет переходить в защитное состояние. Это достигается за счет того, что с помощью дополнительного полярного признака проверяется исправность элементов схемы. Такой вариант УВИР приведен на рисунке 7.6.

Для защиты от ложного включения исполнительных реле при появлении сбоев аппаратуры в большинстве УВИР используют принцип статистической обработки (накопления) импульсных сигналов включения, что иллюстрируется рисунком 7.7. При этом кратковременные случайные сбои в работе СЖАТ не приводят к ложному выключению или включению ИР. Во включенном состоянии реле будет находиться до тех пор, пока будут поступать импульсные сигналы. Каждый импульс подтверждает исправное состояние элементов, формирующих его.

Известны схемные решения релейных УСО, принцип работы кото-

рых основан на преобразовании импульсных сигналов малой амплитуды в рабочее напряжение ИР с помощью выпрямителей с умножением напряжения (рисунок 7.8) [7.7], а также использующих эффект формирования ЭДС самоиндукции при коммутации индуктивности [7.8].

В схеме, показанной на рисунке 7.8, входные сигналы в виде последовательности импульсов поступают на прямой и инверсный входы двухполюсного ключа (ДПК) на транзисторах VT1-VT3. При парафазности сигналов, поступающих от разных вычислительных каналов, на входе выпрямителя с умножением напряжения (ВУН), выполненного на элементах С1-С6, VD1-VD6, появляется переменное напряжение прямоугольной формы с амплитудой Е, которое выбирается меньше, чем напряжение отпускания ИР. ВУН производит выпрямление и умножение исходного напряжения до уровня, необходимого для работы ИР при поступлении нескольких импульсов, т.е. в этом устройстве также осуществляется статистическая обработка (накопление) сигналов.

Повреждение любого элемента УВИР ведет к прекращению умножения напряжения или к снижению выходного напряжения ВУН и исключает возможность ложного притяжения или удержания якоря реле. В случае повреждения трех и более элементов к обмотке реле может быть подключен один из источников ДПК, но уровня его напряжения недостаточно не только для включения, но и для удержания реле во включенном состоянии.

УВИР (рисунки 7.4-7.6) имеют один вход и, следовательно, могут использоваться в микроэлектронных системах, достоверность выходных сигналов которых контролируется специальными средствами. УВИР (рисунки 7.3, 7.7) могут использоваться в дублированных микроэлектронных системах, причем данные элементы сопряжения контролируют правильность работы резервированных каналов, выполняя роль выходных компараторов.

В микроэлектронных системах, выполненных по мажоритарной структуре 2У3, можно использовать УВИР, изображенный на рисунке 7.9 [7.9]. При синхронном поступлении импульсных сигналов на входы 1, 2, 3 происходит заряд конденсаторов C_1, C_2, C_3 в течение времени действия входных импульсов. Во время паузы они разряжаются на светодиоды оптопар VO_1 и VO_2 через резисторы R_1, R_2; при этом напряжение, воздействующее на них, равно сумме напряжений на

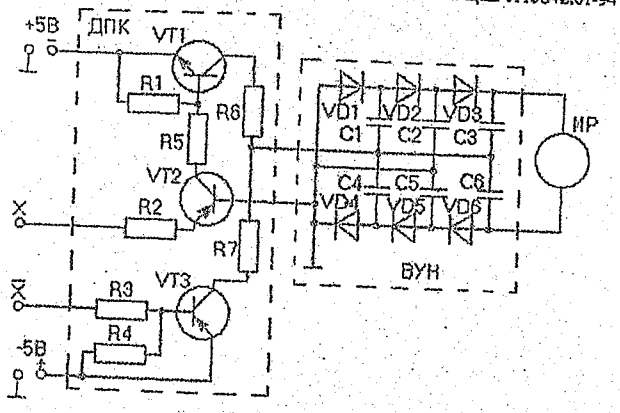


Рисунок 7.8

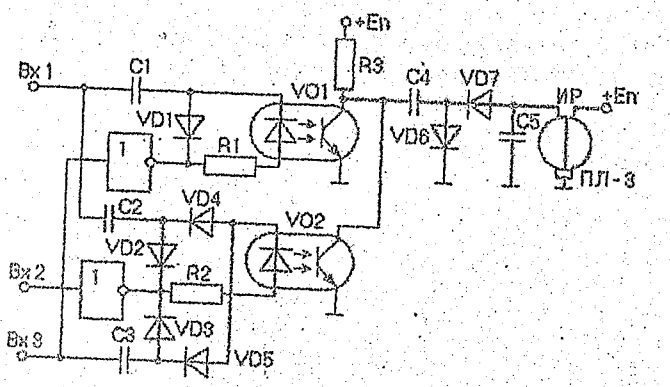


Рисунок 7.9

конденсаторе и источнике питания. В результате этого фототранзисторы оптопар VO_1, VO_2 переключаются и формируют импульсы, поступающие на вход преобразователя полярности (элементы C_4, C_5, VD_6, VD_7). Поляризованное реле ИР притягивает якорь.

При отсутствии импульсов на двух входах из трех (например на 1-м и 2-м) на светодиоды воздействует только напряжение заряда конденсаторов, т.е. приблизительно в два раза меньшей величины, чем в случае синхронного поступления импульсных сигналов на эти входы. В результате оптроны не переключаются и ИР отпустит свой якорь. В данной схеме для обеспечения ее безопасного функционирования используются функции дифференцирования, удвоения напряжения и гальванической развязки.

Обобщая анализ описанных схемных решений, можно сформулировать основные принципы построения УСО, отвечающих требованиям безопасности и выполненных с использованием реле 1 класса надежности:

1) обеспечение непрерывного контроля исправности электронных элементов путем периодического изменения их состояния (принцип контроля динамической работы);

2) статистическая обработка сигналов включения ИР;

3) гальваническая развязка входных и выходных цепей;

4) частотная или амплитудная защита схемы от неисправностей источника питания;

5) отсутствие обратных связей, приводящих к самовозбуждению схем;

6) амплитудная, полярная или частотная защита ФП от ложного включения ИР.

7.4 Бесконтактные УСО.

Все многообразие известных способов построения устройств бесконтактной коммутации цепей ИО в зависимости от используемых методов обеспечения безопасности можно разделить на три вида [7.10]:

- с периодическим программным тестовым контролем дублированных коммутирующих элементов УСО;

- с аппаратным контролем исправности дублированных коммутирующих элементов и программным тестированием контрольного устройства;

- в виде бесконтактных ФП с несимметричным отказом.

Исправность коммутационных устройств (КУ) первой группы проверяется с помощью параллельно или последовательно соединенных с ними контрольных элементов (КЭ).

При параллельном соединении КУ и КЭ (рисунок 7.10) с целью предотвращения последовательных во времени отказов типа "пробой" обоих ключей $КУ_1$ и $КУ_2$ ЭВМ периодически опрашивает входы, на которые поступают сигналы от КЭ. Если $КУ_1$ и $КУ_2$ закрыты, то на выходах $КЭ_1$ и $КЭ_2$, выполненных на оптронах VO_1-VO_2, появляются импульсные последовательности (рисунок 7.11); в состоянии пробоя КУ на вход ЭВМ поступает сигнал 1 (рисунок 7.12).

При последовательном соединении КУ и КЭ (рисунок 7.13) также осуществляется периодическая тестовая проверка их исправности путем поочередного включения одного из двух КУ. В этом случае с помощью КЭ проверяется отсутствие тока в рабочей цепи ИО. Считается, что вероятность пробоя обоих КУ за время $\tau_д$ мала, однако необходимо учитывать такую возможность одновременного пробоя полупроводниковых ключей, например при воздействии перенапряжений. При этом возникает ложный сигнал активизации ИО в течение времени $t_л < \tau_д$, что может привести к опасной ситуации до выявления отказа.

Этот вывод подтверждается результатами эксплуатации полупроводниковых приборов и тем, что внешние (рабочие и контрольные) цепи ИО СЖАТ наиболее подвержены воздействию перенапряжений.

Таким образом, для обеспечения безопасности функционирования такого рода коммутационных устройств длительность периода диагностирования (тестирования) $\tau_д$ должна быть меньше времени включения (инерции) ИО. Но т.к. в обоих вариантах (рисунки 7.10, 7.13) первого способа построения устройств коммутации контроль исправности полупроводниковых элементов осуществляется программным способом, такое диагностирование снижает полезную производительность ЭВМ.

Поэтому специалисты многих стран контроль исправности УСО

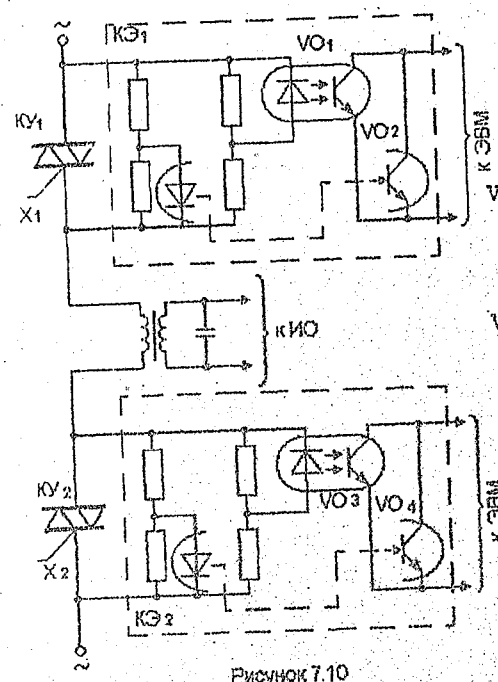


Рисунок 7.10

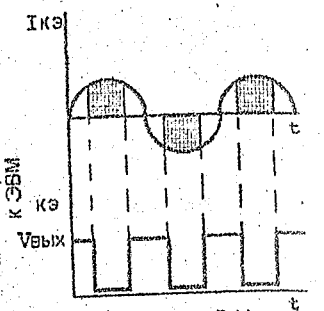


Рисунок 7.11

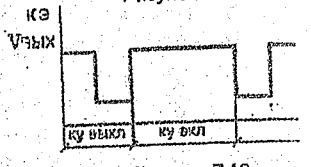


Рисунок 7.12

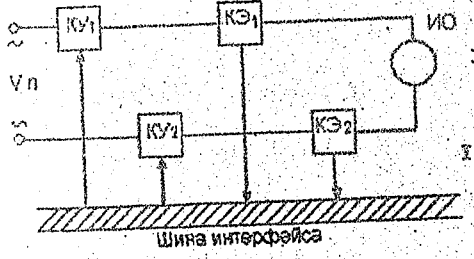


Рисунок 7.13

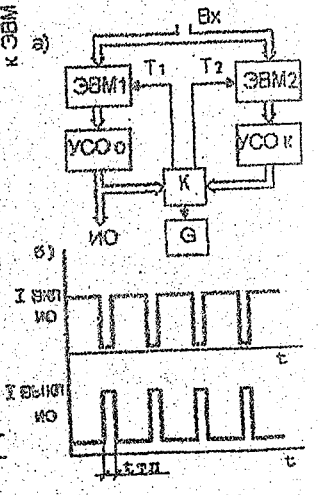


Рисунок 7.14

осуществляют с помощью аппаратных или программно-аппаратных средств.

Например, в системе Simis [7.11], выполненной на основе дублированной микроЭВМ, специальным компаратором (К) осуществляется сравнение сигналов, поступающих от основного (УСОо) и контрольного (УСОк) устройств сопряжения (рисунок 7.14,а).

Одноименные сигналы от УСОо и УСОк поступают на входы К в парафазном виде, для того чтобы можно было обнаруживать такое повреждение, как короткое замыкание его входов.

При повреждении КУ нарушается парафазность и К блокирует поступление тактовых сигналов Т1 и Т2 в ЭВМ. Можно отметить, что КУ, УСОо и УСОк работают в разных условиях, т.к. вторые не подключены к внешним цепям и, следовательно, значительно меньше подвержены воздействию перенапряжений. Поэтому при пробое КУ из-за воздействия перенапряжений вероятность появления ложного парафазного сигнала, поступающего на входы К от УСОо и УСОк, мала.

Для исключения возможности накопления дефектов в К необходимо периодически его тестировать путем программного изменения состояния каждого из выходов УСО (рисунок 7.14,б) независимо от того, включена или выключена рабочая цепь ИО.

Такой программно-аппаратный контроль позволяет при возникновении неисправности сразу же обеспечить выключенное состояние системы, поэтому тестирование компаратора можно осуществлять относительно редко, т.е. производительность ЭВМ снижается меньше, чем в первом случае. Длительность сигналов тестовой проверки tтп должна оставаться меньше времени инерции ИО.

Рассмотрим вариант УСО с программно-аппаратным контролем для мажоритарно-резервированного УВК (рисунок 7.15) [7.12].

Под действием тактовых импульсов ЭВМ 1, 2, 3 по определенной программе производят обработку поступающей на их входы X_1- X_n информации, при этом на выходах Z_1- Z_k и Z_1'- Z_k' мажоритарных элементов M_1 – M_k и M_1'- M_k' появляются парафазные импульсные сигналы, которые поступают к исполнительным устройствам.

При повреждении одной из ЭВМ ее выходные сигналы будут отличаться от сигналов двух исправных ЭВМ. При этом на входе одной или нескольких контрольных схем (КС) 2/4 соответствующего блока

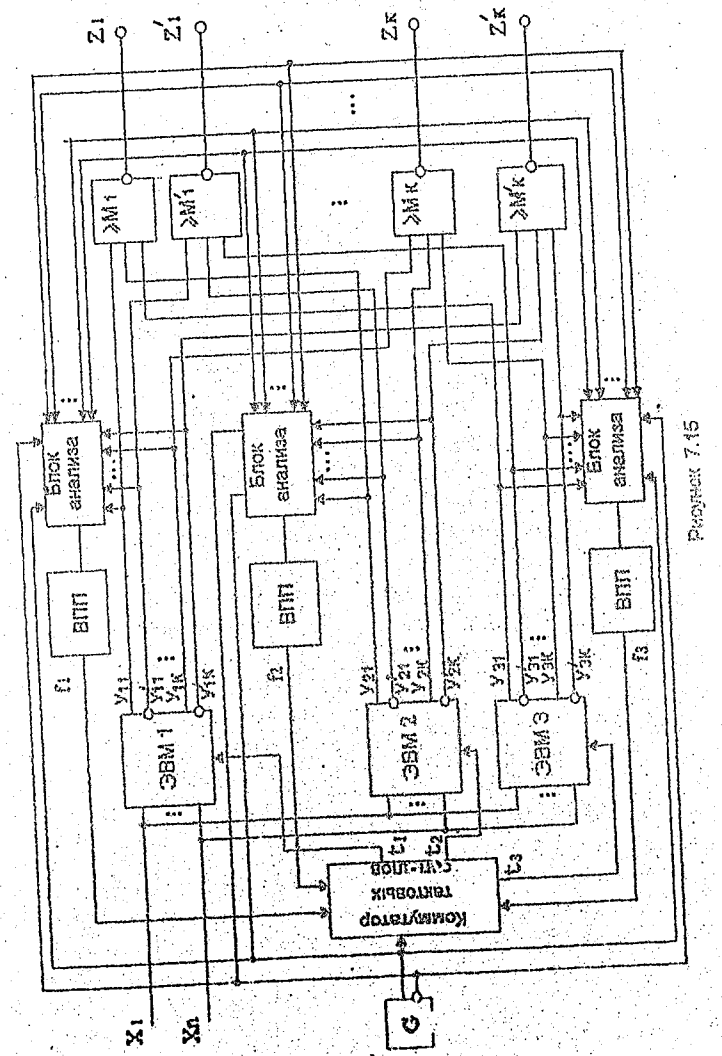


Рисунок 7.15

анализа нарушается код 2 из 4, т.к. сигналы на выходе поврежденной ЭВМ не соответствуют выходным сигналам мажоритарных элементов (не являются парафазными). В этом случае на выходе каскадно соединенных КС появляется непарафазный код, что фиксируется самопроверяемыми элементами памяти [7.13], которые блокируются.

При этом на выходе f схемы контроля динамики (ВПП) отсутствует напряжение. Если произойдет отказ еще одной ЭВМ, то будет отсутствовать напряжение на выходах f двух ВПП и в этом случае с помощью электронных контактов прерывается цепь поступления тактовых сигналов, необходимых для работы вычислительных каналов УВК.

Таким образом обеспечивается защитное статическое состояние выходных сигналов МЭ. При контроле их динамического характера с помощью специальных схем исключается возможность ложной активизации ИО.

Рассмотренные схемы УСО являются в значительной степени универсальными для коммутации контрольных и рабочих цепей различных ИО, но возможно построение узко специализированных УСО на основе ФП или самоконтролируемых.

Примерами таких УСО могут быть преобразователи постояннго тока в переменный. На рисунке 7.16 предлагается схема мостового преобразователя, управляемого двумя парафазными импульсными последовательностями X_1 и X_2 (01 или 10). Под действием X_1=1 открываются ключи K_1, K_4, и через цепь ИО протекает ток одного направления, а под действием X_2=1 открываются ключи K_2 и K_3, и через цепь ИО протекает ток другого направления.

Таким образом в рабочей цепи ИО формируется переменный ток. Ложная активизация ИО невозможна, т.к. при пробое ключей через рабочую цепь протекает постоянный ток, который не приводит к изменению состояния ИО.

Если ИО работает как от переменного, так и от постоянного тока, например лампа светофора, то в состав преобразователя должен входить элемент гальванической развязки - трансформатор (рисунок 7.17), защищающий ИО от воздействия постоянного тока при повреждении элементов УСО.

Если используется трансформатор с прямоугольной петлей гистерезиса, то схема защищена от таких отказов, как появление зна-

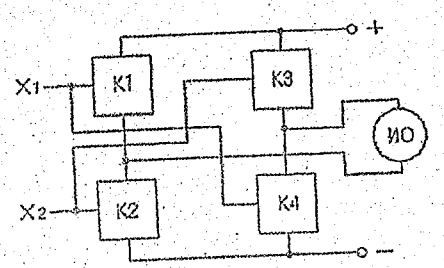


Рисунок 7.16

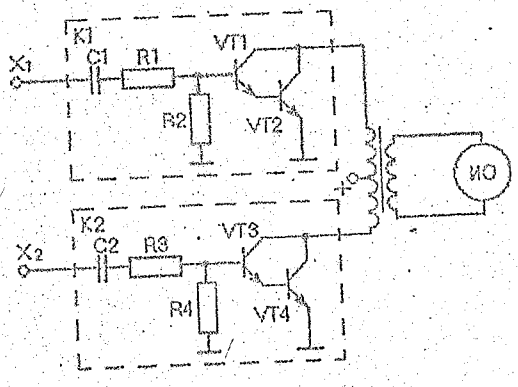


Рисунок 7.17

чительной переменной составляющей на шинах питания и самовозбуждение ключей K_1 и K_2.

Примером ИО, защищенного от воздействия постоянного тока (при повреждении ключей преобразователя), может служить применяемый на железных дорогах стрелочный электропривод переменного тока.

Для управления таким электроприводом требуется три мостовых преобразователя, управляемых импульсными последовательностями, сдвинутыми друг относительно друга на 120^0. Такой преобразователь называется инвертором.

Преимуществом данной схемы является возможность тестирования обмоток электродвигателя и полупроводниковых ключей в паузах между установкой и замыканием маршрутов. С этой целью последовательно с обмотками двигателя включаются контрольные элементы (токовые трансформаторы или оптроны), с помощью которых можно диагностировать исправность цепи ИО. Мостовые преобразователи тестируются по одному, что позволяет исключить возможность ложного перевода стрелочного электропривода.

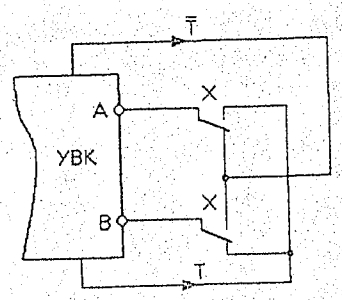
7.5 Безопасный ввод информации

Построению устройств ввода, отвечающих требованиям безопасности, посвящено значительно меньше работ, чем безопасности устройств вывода.

Для обеспечения необходимой достоверности контрольной информации о состоянии исполнительных объектов в безопасных системах используются различные виды избыточного кодирования последовательного или параллельного вида.

Наиболее широко применяется парафазное импульсное представление информации. На рисунках 7.18,а и 7.18,б приведены примеры построения устройств ввода информации в УВК [7.14]. В этих случаях значение переменной X отображается парафазными импульсными последовательностями $\overline{T}T$ или $T\overline{T}$, поступающими на входы A и B УВК. При неисправности нарушается парафазность или импульсный характер сигналов на входах A и B, что фиксируется с помощью программных или аппаратных средств контроля УВК.

а)



б)

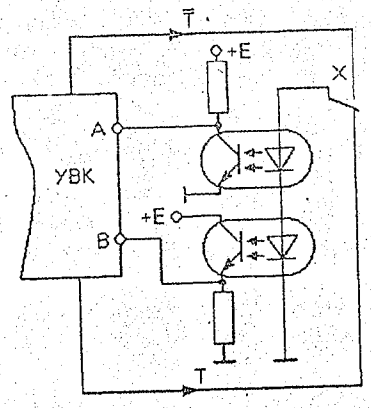


Рисунок 7.18

По аналогичному принципу выполняется контроль исправности нити лампы светофора (рисунок 7.19). При переключении транзистора VT_1 в цепи лампы HL протекает переменный ток, который приводит к поочередному переключению оптронов VO_1, VO_2. Таким образом, при поступлении сигналов управления светофором исправность нити его лампы в горячем состоянии контролируется за счет динамического характера парафазных сигналов на вых.1, вых.2.

8 БЕЗОПАСНЫЕ ЛОГИЧЕСКИЕ ЭЛЕМЕНТЫ

Логические элементы (ЛЭ) играют важную роль при синтезе безопасных дискретных систем. От их свойств и особенностей зависит концепция обеспечения безопасности. Классификация безопасных элементов приведена на рисунке 8.1. Они делятся на две группы: с несимметричным отказом и самопроверяемые.

Элементы с несимметричным отказами разрабатываются специально для построения безопасных систем. Очевидно, что безопасную (h_1-надежную) схему на h_1-надежных элементах построить легче и она будет реализована с меньшей избыточностью. Степень асимметрии характеризуется коэффициентом асимметрии отказов [8.7] - отношением интенсивностей отказов типа 1->0 и 0->1.

Несимметричность отказов ЛЭ достигается сочетанием следующих основных методов [8.1], [8.2]: специальным физическим представлением логических сигналов, резервированием деталей и узлов, импульсным кодированием сигналов, использованием генераторных и резонансных режимов работы, гальванической развязкой входных и выходных цепей, избыточным кодированием внутренней и внешней информации, специальными конструктивными мерами.

В самопроверяемых элементах используется троичное представление логических сигналов, при котором вводится третье защитное состояние ø. Элемент строится таким образом, что при всех вероятных повреждениях происходит только трансформация сигналов 0->ø или 1->ø. Наиболее просто это достигается при двухфазном (парафазном) кодировании. Сигнал X представляется с помощью единичной X и нулевой $\bar{X}$ фаз ($X\bar{X}$). Сигнал 0 кодируется в этом случае как 01, сигнал 1 - как 10, сигнал ø - как 00 или 11.

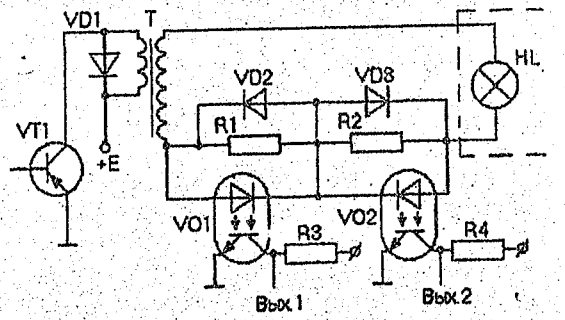


Рисунок 7.19

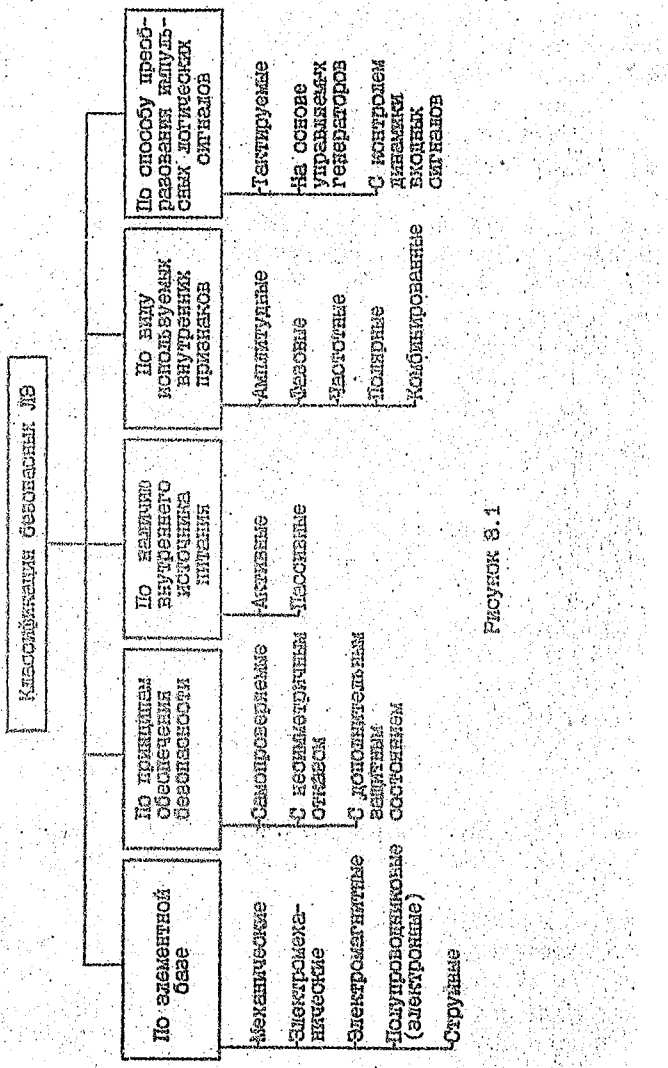


Рисунок 8.1

В зависимости от используемой элементной базы применялись механические, магнитные, электромеханические, электромагнитные, полупроводниковые, оптические безопасные ЛЭ и элементы, работа которых основана на процессах, имеющих неэлектрическую природу.

В 60-х годах появились первые безопасные бесконтактные элементы - магнитные, трансформаторные, феррит-транзисторные. В магнитных элементах роль надежного источника энергии, которая не исчезает, так же как и сила тяжести якоря реле, играет постоянный магнит [8.8] или электромагнит [8.9]. В трансформаторных [8.10], [8.11] и феррит-транзисторных [8.12], [8.13] элементах для достижения h_1-надежности используется импульсный характер работы ЛЭ. В этом случае логический сигнал 1 представляется последовательностью импульсных сигналов, а сигнал 0 - отсутствием их. Это позволяет легко контролировать обрывы в схемах (наиболее вероятные повреждения).

В современных системах широко используется безопасный элемент *исключающее ИЛИ* с импульсным характером работы, построенный на базе диодного моста (рисунок 8.2) [8.19], [8.20]. Если сигналы X1 и X2 взаимно инверсны, то транзистор VT, включенный в диагональ диодного моста, получает питание. При наличии тактовых импульсов на входе Т на выходе Y также формируется импульсный сигнал. При неисправности или при нарушении парафазности сигналов на входах X1 и X2 транзистор VT не имеет питания и импульсный сигнал на выходе отсутствует (Y=0).

Новые возможности при построении импульсных безопасных ЛЭ появились с развитием оптоэлектроники. Ценным качеством здесь является высоконадежная оптронная гальваническая развязка [8.1], [8.14]. На рисунке 8.3 представлен безопасный элемент И, состоящий из транзисторного ключа, диода, конденсатора и оптрона [8.1]. При совпадении импульсных сигналов на входах X1 и X2 на выходе оптрона формируется импульсный сигнал У.

Большое число безопасных ЛЭ построено с использованием генераторных и резонансных режимов работы. В этом случае все вероятные повреждения должны приводить к срыву генерации или нарушению резонанса. Генераторные ЛЭ строятся на микрозлектронной базе

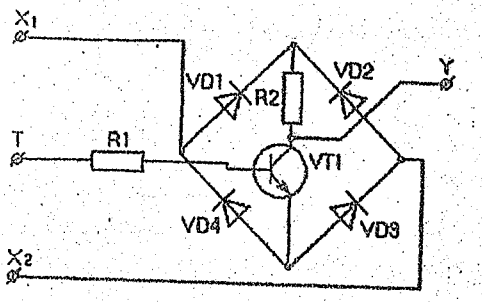


Рисунок 8.2

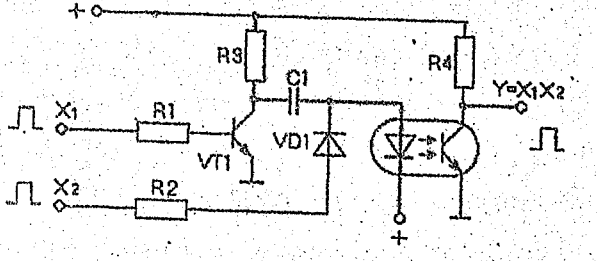


Рисунок 8.3

[8.8]-[8.17] с использованием трансфлюксоров [8.14] и параметронов [8.18].

На рисунке 8.4 представлена принципиальная схема генераторного элемента И из системы безопасных электронных модулей LOGISAFE [8.15], [8.16], состоящая из блокинг-генератора с трансформаторной обратной связью (VT1), выходного усилителя (VT2) и входных каскадов. Если в результате повреждений параметры отдельных деталей элемента выходят за пределы допусков, процесс генерации прекращается. Система LOGISAFE имеет безопасные модули типов И, ИЛИ, И-НЕ, ПАМЯТЬ, ВРЕМЯ. Развитием системы LOGISAFE стала система дискретных логических схем с безопасными отказами LOGISAFE-GS [8.16].

При наличии функционально полного набора самопроверяемых логических элементов с дополнительным защитным состоянием на способ построения внутренней структуры безопасных дискретных систем не накладывается никаких ограничений. Вопросы применения элементов данного типа рассмотрены в [8.13]. Там же описаны безопасные ЛЭ, реализованные на феррит-транзисторных модулях и работающие во временном парафазном коде. В [8.17] разработан самопроверяемый элемент И, имеющий разнополярные логические 1; 0 и третье состояние - отсутствие напряжения на выходе, что сигнализирует об отказе в схеме ЛЭ.

В [8.3] разработаны схемы типовых полностью самопроверяемых цифровых устройств, выполненных на элементах с симметричными отказами (триггеров различных типов, двоичных счетчиков и регистров, распределителей, дешифраторов, генераторов и др.). В основу устройств с памятью положена элементарная ячейка памяти - самопроверяемый асинхронный парафазный Т-триггер, обладающий свойствами контроля входного вектора, самопроверки и блокировки. Там же исследованы принципы самопроверяемой парафазной схемотехники, в которой используются парафазная логика, указанные типовые ПСП, цифровые устройства и специальная контрольная парафазная логика (КПЛ).

КПЛ отличается от обычной парафазной логики представлением логических сигналов 0 и 1. Логический сигнал 1 представляется значением двух фаз парафазного сигнала 01 или 10, а логический

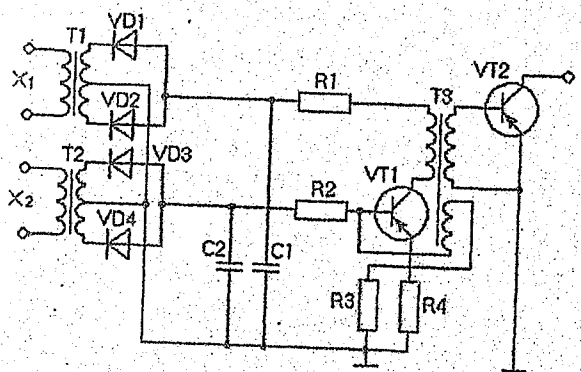


Рисунок 8.4

сигнал 0 - значениями 00 или 11. Описаны ПСП-элементы И, ИЛИ, НЕ, *исключающее ИЛИ*, мажоритарные элементы, работающие в КПЛ, с помощью которых можно строить разнообразные схемы контроля самопроверяемых дискретных систем.

На рисунке 8.5 приведена схема парафазного D-триггера, который используется как фиксатор ошибок (ФО) в безопасных системах, выполняя роль "последнего сторожа". При нарушении парафазности сигнала (Z_1,Z_2) и возникновении неисправностей из заданного класса в структуре ФО его схема переходит в защитное состояние и блокируется со значениями выходов (V_1,V_2), равными (0,0) или (1,1). Вывод схемы ФО из защитного состояния по входным цепям невозможен. Это возможно только по цепи установки. Практические схемы ФО предложены в [8.4]-[8.6].

Безопасные элементы, действие которых основано на процессах, не имеющих электрической природы (например струйные элементы [8.2]) при построении СЖАТ имеют ограниченное применение.

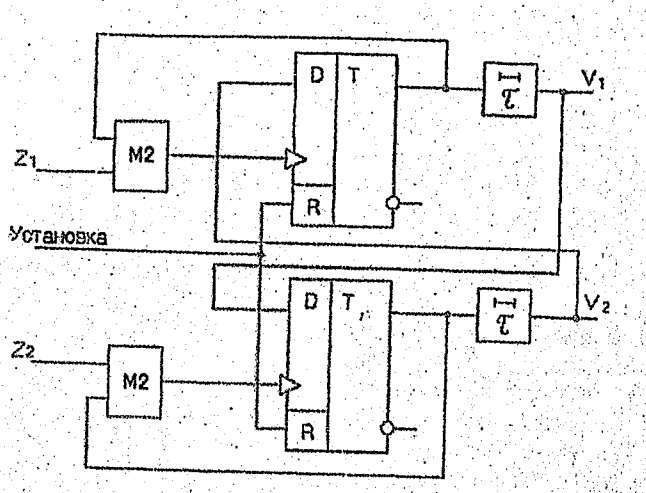


Рисунок 8.5

Прилож ние А
Справочное

Библиография

А.1 Список использованной литературы к разделу 1

1.1. Методы и средства оценки обеспечения безопасности систем железнодорожной автоматики / Сапожников В.В., Сапожников Вл.В., Гавзов Д.В. и др. // Автоматика, телемеханика и связь. - 1992. - N 1. - С.4-7.

1.2. Дрейман О.К. и др. Способы обеспечения и методика расчета показателей надежности и безопасности микропроцессорных систем железнодорожной автоматики / Дрейман О.К., Гавзов Д.В., Илюхин М.В.; Ленингр. ин-т инж. ж.-д. трансп. - Л., 1988. - Деп. в ЦНИИ ТЭИ МПС 28.01.88, N 4320. - 18 с.

1.3. Сотсков Б.С. Основы теории и расчета надежности элементов и устройств автоматики и вычислительной техники. - М.: Высшая школа, 1970. - 270 с.

1.4. Велецкий В.В. Теория и практические методы резервирования радиоэлектронной аппаратуры. - М.: Энергия, 1977. - 360 с.

1.5. Доманицкий С.М. Построение надежных логических устройств. - М.: Энергия, 1971. - 280 с.

1.6. Сапожников В.В., Сапожников Вл.В. Методы синтеза надежных автоматов. - Л.: Энергия, 1980. - 96 с.

1.7. Ефимов В.Ю. Об оценке безопасности действия устройств железнодорожной автоматики и телемеханики и способах достижения заданной величины безопасности // Тр. Ленингр. ин-та инж. ж.-д. трансп. - Л.: Транспорт, 1973. - Вып.367. - С.118-125.

1.8. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов. - Л.: Энергоатомиздат, 1984. - 112 с.

1.9. Гавзов Д.В. Аппаратные способы повышения надежности систем железнодорожной автоматики на основе микропроцессоров //Автоматика и вычислительная техника на железнодорожном

транспорте: Сб. трудов Ленингр. ин-та инж. ж.-д. трансп. - Л.: ЛИИЖТ, 1986. - С.79-87.

1.10. Телеуправление стрелками и сигналами: Учебник для вузов ж.-д. трансп. / А.С. Переборов, А.М. Брылеев, В.Ю. Ефимов и др.; Под ред. А.С. Переборова. - 3-е изд., перераб. и доп. - М.: Транспорт, 1981. - 390 с.

1.11. Христов Х.А. Електронизация на осигурителната техника. - София: Техника, 1984. - 355 с.

1.12. Дрейман О.К. Помехоустойчивость методов передачи информации в телемеханических устройствах электрической централизации: Дис. ... канд. техн. наук. - Л.: ЛИИЖТ, 1970. - 177 с.

1.13. Швир В. Надежность электронных схем в устройствах СЦБ //Железные дороги мира. - 1986. - N 1. - С.59-67.

1.14. Балашов Е.П., Пузанков Д.В. Проектирование информационно-управляющих систем. - М.: Радио и связь, 1987. - 255 с.

А.2 Список использованной литературы к разделу 2

2.1. Христов Х.А. Електронизация на осигурителната техника. - София: Техника, 1984. - 355 с.

2.2. Балашов Е.П., Пузанков Д.В. Проектирование информационно-управляющих систем. - М.: Радио и связь, 1987. - 255 с.

2.3. Стрелов Х., Уэбел Х. Надежная система микроЭВМ//Экспресс-информация. Организация перевозок. Автоматизированные системы управления транспортом. - 1978. - N 45. - С.1-4.

2.4. Masao Jadi Fail-safe Digital Date Transmission Sistem //JRE. - 1981. - Vol.21. - N2. - P.12-16.

2.5. Доманицкий С.М. Построение надежных логических устройств. - М.: Энергия, 1971. - 280 с.

2.6. Пакулов Н.И. и др. Мажоритарный принцип построения надежных узлов и устройств ЦВМ / Н.И. Пакулов, В.Ф. Уханов, П.Н. Чернышов. - М.: Сов. радио, 1974. - 184 с.

2.7. Гавзов Д.В., Илюхин М.В. Анализ и класси-

фикация мажоритарных элементов и способов их адаптации / Ленингр. ин-т инж. ж.-д. трансп. - Л., 1987. - Деп. в ЦНИИ ТЭИ МПС 14.09.87, N 4258. - 16 с.

2.8. Федотов А.Е. Исследование вопросов надежности систем электрической централизации стрелок и сигналов: Дис. ... канд. техн. наук. - Л.: ЛИИЖТ, 1976.

А.3 Список использованной литературы к разделу 3

3.1. Сапожников В.В., Сапожников Вл.В. Принципы построения безопасных микропроцессорных систем//Автоматика, телемеханика и связь. - 1989. - N11.- С.22-24.

3.2. Rutherford D.B. Fail-safe microprocessor interlocking - an application of numerically - integrated safety assurance logic //Int. Conf. Railway Safety Cintrol and Automation towards the 21st century. - London, 1984. - P.72-76.

3.3. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов. - Л.: Энергоатомиздат, 1984.- 112 с.

3.4. Berg von Linde O. Computers can now perform vital functions safety//Railway Gazette International. - 1979. - N 11. - P.1004-1007.

3.5. Jonasen A.A., Siggard N. Microcomputers take over the interlocking function//Railway Gazette International. - 1981. - N 12. - P.1028-1030.

3.6. Stadler O. Computer gesteuerter Rangierbalnhof: Geschwlndigkeits und Laufwegsteurung von ablaufende Eisenbahnwagen//Technlsche Rundschau. - Bern, 1975. - Vol. 67. - P.16-21.

3.7. Акита К., Накамура Х. Безопасность и отказоустойчивость микропроцессорных систем сигнализации // Железные дороги мира. - 1991. - N 6. - С.29-34.

3.8. Wobig K.-H., Horder A., Strelov H. Prozessrechner systeme mit Fail-Safe-Verhalten // Signal und Draht. - 1974. - N 11. - S.211-218.

3.9. Cribbens A.H. The solid state interlocking// International Conference "Railway Safety Control and Automation towards the 21st century". London, 1984. - P.24-29.

3.10. Lohmann H.-J., Zillmer A. Safety principale and fail-safe analysis of electronic interlocking devices and practical realization of electronic interlocking // International Conference "Railway Safety Control and Automation towards the 21st century". London, 1984. - P.41-48.

3.11. Strelow H., Uebel H. Das Sichere Microkomputersystem SIMIS // Signal and Draht. - 1978. - N 4. - P.82-86.

3.12. Wobig K.-H. Failsafe microcomputer systems for railway signalling - problems and posslbilites//International Conference "Railway in the electronic age". - 1981. - P.164-168.

3.13. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. - М.: Радио и связь, 1989. - 208 с.

3.14. Sapoznikov V., Sapoznikov VI., Wytulany A. Realization of fail- safe discrete systems by using principales of self-checking and standby//Proc. of Second. International Conference on Reliability and Exploitation of Computer systems. RELCOMEX'81. - Wroclaw, 1981. - P.67-71.

3.15. Гессель М., Согомонян Е.С. Построение самотестируемых и самопроверяемых комбинационных устройств со слабонезависимыми выходами // Автоматика и телемеханика. - 1992. - N 8. - С.150-160.

3.16. Gayen T.-T., Reinhold G., Wojanowskl E. Mogllchkeiten zur Gewahrleistung eines sicheren Betriebs bel spurgebundenen Verkchrsmitteln//Slgnal and Draht. - 1976. - N 10. - S.203-207.

3.17. А.с. СССР N1609510 МКИ Н05К 10/00. Устройство контроля и реконфигурации реверсированной вычислительной системы /Гавзов Д.В., Дрейман О.К., Кукушкин А.В. - N 4467114/24; Заявл. 29.07.88; Опубл.15.11.90, Бюл. N41.

3.18. Окимура И. Разработка электронной системы централизации // Железные дороги мира. - 1983. - N 2. - С.44-52.

3.19. Шибалов Г.П. Контроль функционирования больших

систем. - М.: Машиностроение, 1977. - 356 с.

3.20. Гавзов Д.В., Самонина Е.В. Принципы построения и анализ надежности схем сравнения дублированных микропроцессорных систем железнодорожной автоматики /Ленингр. ин-т инж. ж.-д. трансп. - Л., 1988. - Деп. в ЦНИИ ТЭИ МПС 14.06.88, N 4525. - 16 с.

3.21. Гавзов Д.В. Методика расчета показателей надежности микропроцессорных модулей, используемых в системах обеспечения безопасности движения поездов / Ленингр. ин-т инж. ж.-д. трансп. - Л., 1989. - Деп. в ЦНИИ ТЭИ МПС 30.11.89, N 4848. - 12 с.

А.4 Список рекомендуемой литературы к разделу 4

4.1. Сапожников В.В. О построении логических схем на элементах с несимметричными отказами // Сб. трудов Ленингр. ин-та инж. ж.-д. трансп. - Л.: Транспорт, 1976. - Вып. 391. - С.52-63.

4.2. Сапожников В.В. Исследование и разработка методов надежностного синтеза дискретных систем железнодорожной автоматики и телемеханики: Дис, ... д-ра техн. наук. - Д.: ЛИИЖТ, 1979. - 353 с.

4.3. Сапожников В.В. и др. Дискретные устройства железнодорожной автоматики, телемеханики и связи / В.В. Сапожников, Ю.А. Кравцов, Вл.В. Сапожников. - М.: Транспорт, 1988. - 255 с.

4.4. Сапожников Вл.В. Исследование принципов построения электрической централизации малых станций с исключением опасных отказов: Дис. ... канд. техн. наук. - Л.: ЛИИЖТ, 1969. - 238 с.

А.5 Список рекомендуемой литературы к разделу 5

5.1. Пархоменко П.П., Согомонян Е.С. Основы технической диагностики. - М.: Энергоатомиздат, 1981. - 320 с.

5.2. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов. - Л.: Энергоатомиздат, 1984. - 112 с.

5.3. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. - М.: Радио и связь, 1989. - 208 с.

5.4. Сапожников В.В., Сапожников Вл.В. Самопроверяемые дискретные устройства. - Л.: Энергоатомиздат, 1992. - 224 с.

5.5. Anderson D.A., Metze G. Design of Totally Self-Checking Chek Circuits for M - out - of - N Codes // IEEE Trans. Computer. - 1973.-V. 22. - N 3. - P.77-79.

5.6. Reddy S.M. A Note on Self-Checking Checkers // IEEE Trans. Computer. - 1974.-V. 23. - N 10. - P.58-62.

5.7. Marouf M.A., Friedman A.D. Efficient Desing of Self-Checking Checkers any m - out - of - n Codes // IEEE Trans. Computer. - 1974.-V. 23. - N 10. - P.482-490.

5.8. Сапожников В.В., Рабара В. Универсальный алгоритм синтеза 1/п-тестеров // Проблемы передачи информации. - 1982. - Т. 18. - N 3. - С.64-73.

5.9. Сапожников В.В., Сапожников Вл.В. Универсальный алгоритм синтеза самопроверяющихся тестеров для кодов с постоянным весом // Проблемы передачи информации. - 1984. - Т. 20. - N 2. - С.65-76.

5.10. Сапожников В.В., Сапожников Вл.В. О синтезе самопроверяемых тестеров для кода "1 из 3" // Автоматика и телемеханика. - 1992. - N 2. - С.178-188.

5.11. Nanya T., Kawamura T. On Error Indication for Totully Self-Checking Systems // IEEE Trans. Comput. - 1987. - V. 36. - N 11. - P.1389-1392.

5.12. Gaitanis N. A Totally Self-Checking Error Indicator // IEEE Trans. Comput. - 1985. - V. 34. - N 8. - P.758-761.

5.13. Сапожников В.В., Сапожников Вл.В. Самопроверяемый фиксатор ошибок для парафазных сигналов // Автоматика и телемеханика. - 1992. - N 2. - С.197-200.

5.14. Сапожников В.В., Сапожников Вл.В. Синтез полностью самоконтролирующихся асинхронных автоматов // Автоматика и телемеханика. - 1979. - N 1. - С.154-166.

А.6 Список использованной литературы к разделу 6

6.1. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. - М.: Изд-во отандартов. - 1989. - 37 с.

6.2. Штрик А.А. и др. Структурное проектирование надежных программ встроенных ЭВМ / А.А. Штрик, Л.Г. Осовецкий, И.Г. Мессин. - Л.: Машиностроение, 1989. - 295 с.

6.3. Gawzow D.W., Lewinski A. Programove metody zapewnienia bezpieczenstwa dla mikroprocesorowych systemov strerowania ruchem kolejowym//Nauka I Practika w transporcie/ Materialy na V konferencje naukowa. - Warszawa, 1990. - P.82-87.

6.4. Микропроцессоры и системы программирования и отладки / В.А. Мясников, М.В. Игнатьев, А.А. Кошин, Ю.Е. Шейнин. - М.: Энергоиздат, 1985. - 272 с.

6.5. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов.- Л.: Энергоатомиздат, 1984. - 112 с.

6.6. Построение защитных программ для микропроцессорных систем / Сапожников В.В., Сапожников Вл.В., Харитонов А.В., Чухонин В.М. // Тез. докл. VI Всесоюзн. совещ. по техн. диагностике. - М., 1987. - С.23-25.

6.7. Тышкевич В.Г., Зиборова М.Э., Тышкевич А.И. Методы контроля программ // Зарубежная радиоэлектроника. - 1990. - N 1. - С.32-45.

6.8. Brenda M. Ozaki, Eduardo B. Fernandez, Ehud Gudes. Software Fault Tolerance in Architektures with Hierarchical Protection Levels // IEEEMICRO. - 1989. - N 8. - С.30-42.

А.7 Список использованной литературы к разделу 7

7.1. Дрейман О.К., Гавзов Д.В., Илю-

хин М.В. Сопряжение микропроцессорных систем железнодорожной автоматики с напольными объектами//Автоматика, телемеханика и связь. - 1990. - N 12. - С.14-17.

7.2. Христов Х.А., Иванов Э.В. Специфичен интерфейс на микрокомпютърни гарови централивации // Железопътен транспорт. - 1985. - N 6. - С.18-22.

7.3. Принципы построения электронных устройств включения исполнительных реле в бесконтактных системах железнодорожной автоматики и телемеханики / Гавзов Д.В., Молодцов В.П., Савельев А.Н., Песков И.А.; Ленингр. ин-т инж. ж.-д. трансп. - Л., 1982. - Деп. в ЦНИИ ТЭИ МПС 20.10.82, N 2024. - 14 с.

7.4. Переборов А.С., Лисовский М.П., Прокофьев А.А. Построение устройств согласования электронных схем управления с исполнительными реле//Автоматика, телемеханика и связь. - 1982. - N 5. - С.7-11.

7.5. Кошевой С.В. Устройство сопряжения микропроцессорной техники с исполнительными реле железнодорожной автоматики и телемеханики // Межвуз. сб. науч. тр. - Харьков: ХЭИТ, 1986. - С.42-45.

7.6. Цымбал А.Л. Структура выходного элемента устройств связи микроЭВМ с объектами управления и контроля // Идентификация систем интервального регулирования движения поездов: Тр. Омского ин-та инж. трансп. - Омск: ОмИИТ, 1987. - С.64-67.

7.7. А.с. СССР N 1017570 МКИ В61L 23/16. Устройство для включения исполнительного реле железнодорожной автоматики / Дрейман О.К., Гавзов Д.В., Бодров А.А. - N 3244130/27-11; Заявл. 3.02.81; Опубл. 14.01.83, Бюл. N 1.

7.8. А.с. СССР N 1017571 МКИ В61L 23/16. Устройство для включения исполнительного реле / Гавзов Д.В., Дрейман О.К., Молодцов В.П., Песков И.А. - N 3364194/27-11; Заявл. 11.12.81; Опубл. 14.01.83, Бюл. N 1.

7.9. А.с. СССР N 1528815 МКИ В61L 19/14. Мажоритарное устройство управления включением исполнительного реле железнодорожной автоматики и телемеханики / Гавзов Д.В., Илюхин М.В., Сос-

новская Е.Г. - N 4289412/11; Заявл. 27.06.87; Опубл. 25.10.90, Бюл. N 32.

7.10. Дрейман О.К., Гавзов Д.В., Илюхин М.В. Бесконтактные устройства сопряжения микропроцессорных систем железнодорожной автоматики с напольными объектами // Автоматика, телемеханика и связь. - 1991. - N 1. - С.12-14.

7.11. Стрелов Х., Уэбел Х. Надежная система микроЭВМ // Экспресс-информация. Организация перевозок. Автоматизированные системы управления транспортом. - 1978. - N 45. - С.1-4.

7.13. А.с. СССР N 921048 МКИ Н03К 3/037. Парафазное триггерное устройство со счетным входом / Сапожников В.В., Сапожников Вл.В., Трохов В.Г.- N 2951560/18-21; Заявл. 04.07.80; Опубл. 15.04.82, Бюл. N 3.

7.14. Христов Х.А. Електронизация на осигурителната техника. - София: Техника, 1984. - 355 с.

А.8 Список использованной литературы к разделу 8

8.1. Христов Х.А. Електронизация на осигурителната техника. - София: Техника, 1984. - 355 с.

8.2. Сапожников В.В. и др. Дискретные устройства железнодорожной автоматики, телемеханики и связи / В.В. Сапожников, Ю.А. Кравцов, Вл.В. Сапожников. - М.: Транспорт, 1988. - 255 с.

8.3. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов. - Л.: Энергоатомиздат, 1984. - 112 с.

8.4. Nanya T., Kawamura T. On error indication for totally self-checking systems // IEEE Trans. Computer.- 1987. - V. 36. - N 11. - P.1389-1392.

8.5 Gaitanis N. A totally self-checking error indicator // IEEE Trans. Computer. - 1985. - V.34. - N 8. - P.758- 761.

8.6. Сапожников В.В., Сапожников Вл.В. Самопроверяемый фиксатор ошибок для парафазных сигналов // Автоматика и телемеханика. - 1992. - N 2. - С.197-200.

8.7. ОСТ 32.17-92. Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения. - СПб: ПИИТ, 1992. - 34 с.

8.8. Weber O. Les elements statiques de securite// Revue generale des chemins de fer. - 1973. - N 6. - P.382-391.

8.9. Duckitt H. Solid state switching for safety circuits // The Railway Gazette. - 1965. - Vol. 121. - N 15. P.610-613.

8.10. Патент Франции, 1973, N2.147.481. 8.11 Nara A., Fukinuki T. A failsafe logik system utilizing core transistor logik elements // IEEE Trans. Ind. Electron. and Control Instrum. - 1971. - V. 18. - N 3. - P.77-85.

8.12. Stancinlesco F. La conception et la realisation electronique deshemas loglque a grande fiabilite // Automatisme. - 1966. - V. X1. - N 11. - P.11-13.

8.13. Принципы построения схем электрической централизации на феррит-транзисторных модулях / Переборов А.С., Сапожников В.В., Сапожников Вл.В. и др. // Автоматика, телемеханика и связь. - 1976. - N 5. - С.5-8.

8.14. Лисенков В.Н., Шалягин Д.В., Бестемьянов П.Ф. Автоматическая локомотивная сигнализация АЛС-ЕН // Автоматика телемеханика й связь. - N 11. - 1988. - С.7--10.

8.15. Ientsch A.A., Lots A., Schlwek W. Das Slcherhelts baus sustem Loglsafe // Signal and Draht. - 1978. - N 12. - S.82-86.

8.16. Sohlwek L.-W. Failsafe - Schaltungen mlt LOGISAFE - Technik // Signal and Draht. - 1986. - 78. - N 9. - S.192-197.

8.17. А.с. СССР N 915238 МКИ Н 03 К 19/42. Логический элемент, исключающий ложный сигнал на выходе / Лисенков В.М., Аркатов В.С., Терентьев С.А. - N 2951549/18-21; Заявл. 03.05.80; Опубл. 15.03.82, Бюл. N 2.

8.18. Окумура И., Ватанабэ Т. Использование ЭВМ в устройствах централизации // Ежемесячный бюллетень Междуна-

родной ассоциации железнодорожных конгрессов. - 1970. - N 3.- С.54-58.

8.19. Lohmann H. I. Sicherheit von Mikrocomputern fiir die Eisenbahnsicherungs technik // Elektronische Rechenanlager. - 1980. - N 5. - P.229.

8.20. Strelow H., Uebel H. Das Sichere Microkomputersystem SIMIS // Signal and Draht. - 1978. - N 4. - P.82-86.

УДК 656.25 Д 50

Ключевые слова: безопасные микроэлектронные системы, безопасные микропроцессорные системы, методы повышения надежности, структуры безопасных систем, принципы построения безопасных систем, самопроверяемые схемы, безопасный интерфейс.

РУКОВОДЯЩИЙ ТЕХНИЧЕСКИЙ МАТЕРИАЛ
БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Методы и принципы обеспечения безопасности
микроэлектронных СЖАТ

Редактор Н.В. Фролова

Подписано в печать с оригинала-макета 20.05.94.
Формат 60 х 84 1/16. Бумага для множ.апп. Печать офсетная.
Усл.печ.л. 7,5. Уч.-изд.л. 7,5. Тираж 1000.
Заказ 508.

Петербургский государственный университет путей сообщения.
190031, СПб, Московский пр.,9.

Типография ПГУПС. 190031, СПб, Московский пр.,9.