ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)

I издание

Разработано экспертами Комиссии ОСЖД
по инфраструктуре и подвижному составу 5-7 сентября 2006 г.,
г.Варшава, Республика Польша

Утверждено совещанием Комиссии ОСЖД
по инфраструктуре и подвижному составу 6-9 ноября 2006 г.

Дата вступления в силу: 9 ноября 2006 г.

Р
858

ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И БЕЗОТКАЗНОСТИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

СОДЕРЖАНИЕ

Стр.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Памятка распространяется на дискретные устройства и системы железнодорожной автоматики и телемеханики (ЖАТ) на основе микропроцессорных систем и определяет основные правила и методы обеспечения безопасности систем. Под микропроцессорными подразумеваются системы, построенные на электронных элементах, микросхемах и микроЭВМ.

Данный 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 совершенствования известных схем, отвечающих требованиям безопасности.

Рекомендации распространяются на СЖАТ, разрабатываемые по заказам железных дорог стран-членов ОСЖД, и используются для целей сертификации.

2. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И БЕЗОТКАЗНОСТИ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ И СИСТЕМ ЖАТ

В релейных системах железнодорожной автоматики отказы разделяются на защитные и опасные. Появление сложных микропроцессорных систем 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 отказов и, как следствие, к нарушению функционирования и к возможности появления опасных отказов.

В отличие от релейных систем железнодорожной автоматики и телемеханики (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.

Для реализаций концепций безопасности микроэлектронных СЖАТ используются три стратегии ***(рис.2.1):*** безотказность (reliability), отказоустойчивость (fault-tolerance) и безопасное поведение при отказах (fail-safe).

Рис.2.1

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. Обратный переход в работоспособное состояние исключается (маловероятен) и производится искусственным путем (обычно с участием персонала).

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.

Перспективным направлением является реализация сложных СЖАТ на интегральных микросхемах большой степени интеграции (БИС). При использовании такой элементной базы для достижения необходимых показателей безопасности применяют сочетание различных видов резервирования ***(рис.2.2)*** с контролем и диагностикой появления сбоев и отказов элементов.


Классификация видов резервирования
По виду избыточности
Функциональное
Структурное
Временное
Информационное
По схеме включения резервных элементов
Постоянное
Замещением
Динамическое
Скользящее
По способам включения резервных элементов
Общее
Раздельное
По режиму работы резервных элементов
Нагруженное
Облегченное
Ненагруженное
По кратности резервирования
Дробной кратности
Целой кратности
Дублированное
Мажоритарное резервирование
По способу обслуживания
С восстановлением
Без восстановления
По расчетно-логической схеме
Последовательное
Параллельное
Последовательно-параллельное

Рис.2.2

Контроль осуществляется устройством с несимметричной характеристикой отказов.

Классификация методов диагностики приведена на ***рис.2.3.***

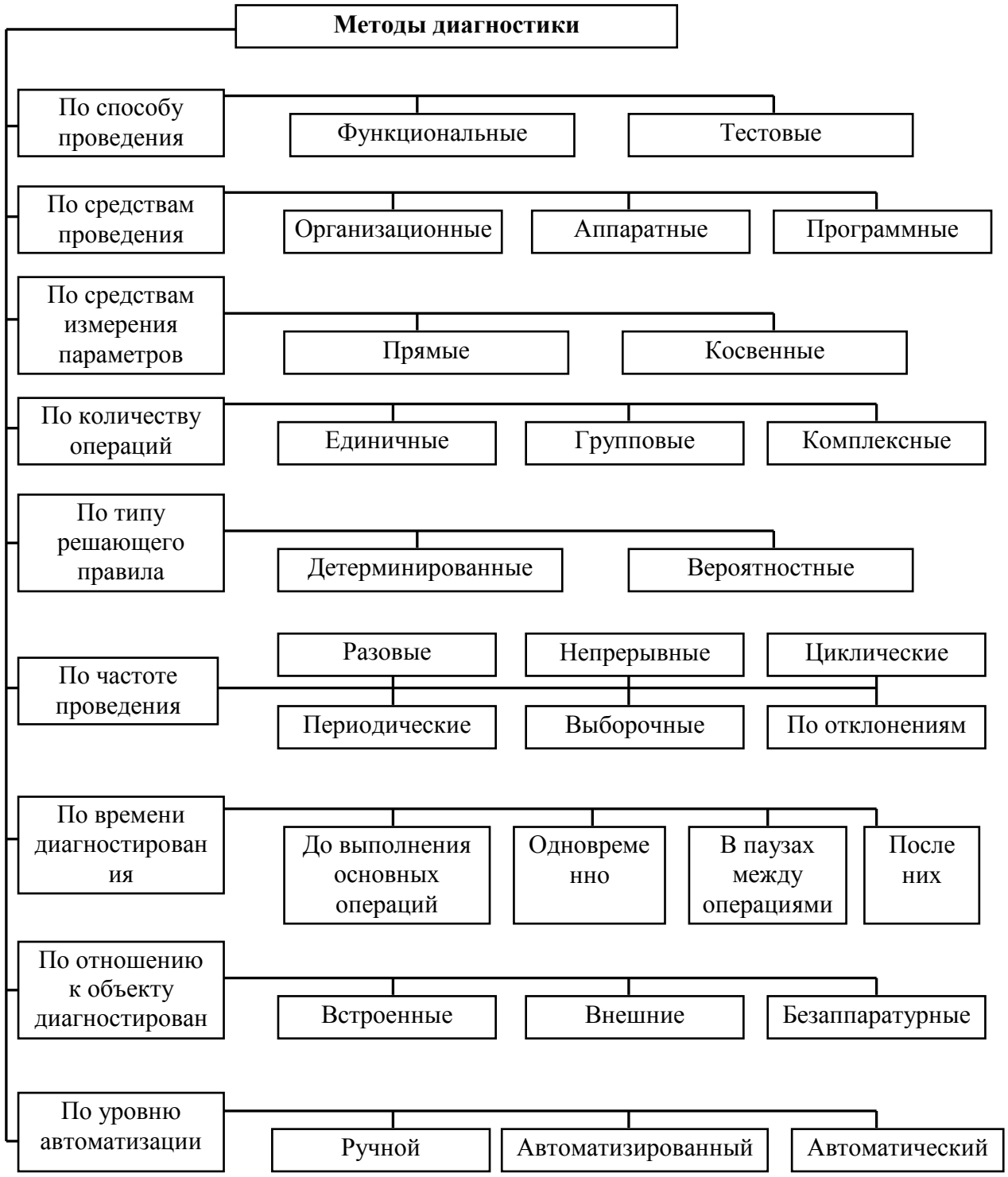

Рис.2.3

При разработке СЖАТ на основе БИС (например, микропроцессоров) необходимо учитывать, что многие их элементы используются многократно в ходе выполнения программы. Кроме того, отдельные отказы могут быть многократными. Например, отказы в питающих выводах приводят к искажениям в работе многих элементов БИС, к появлению новых связей и элементов (паразитных). Последствия этого могут проявляться в различных частях БИС, даже косвенно связанных с первоначальным обстоятельством. 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 в ритме реального времени функционирования СЖАТ.

Необходимые показатели безотказности, контролепригодности и безопасности МП СЖАТ достигаются за счет использования структурного резервирования, которое можно подразделять 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 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 (ПО).

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 позволяет также обеспечить необходимый уровень помехоустойчивости СЖАТ. Программные методы резервирования и контроля требуют большего, чем аппаратные, времени обнаружения отказов, и при их использовании трудно обеспечить принципы независимости отказов в различных программах обработки информации.

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 ПО достигают 70%. Кроме того, в настоящее время не существует теоретического подтверждения обеспечения безопасности МП СЖАТ, использующих только программные методы резервирования и контроля. Таким образом, в МП СЖАТ для обеспечения безопасности движения поездов необходимо использовать сочетание программных и аппаратных методов.

3. СТРУКТУРНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ СЖАТ

3.1. Анализ резервированных структур

В большинстве существующих микроэлектронных систем (МЭС), отвечающих за безопасность, используются аппаратные методы резервирования и контроля.

В общем виде резервированная структура МЭС приведена на ***рис.3.1.*** Резервироваться может как все устройство, так и его отдельные узлы.

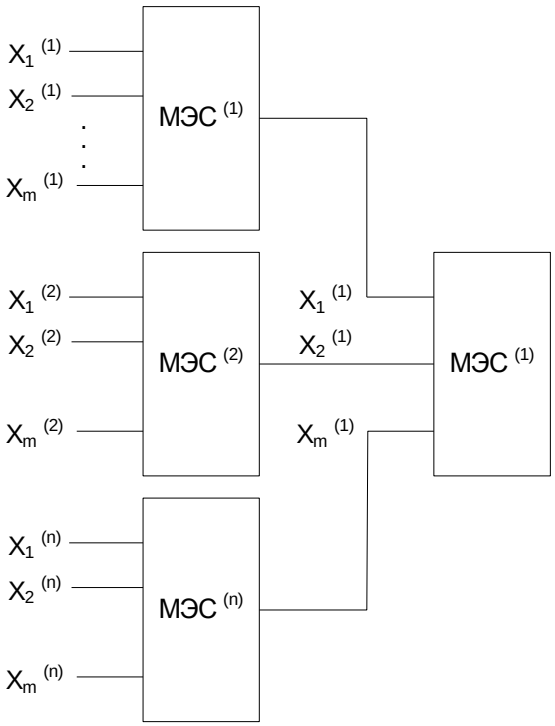

Рис.3.1

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

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

При неисправности какого-либо из обрабатывающих каналом МЭС на его выходе может появится ложная 1 или ложный 0. Правильный сигнал на выходе избыточной структуры появляется только при определенном числе ложных сигналов 0 или 1 на выходах $У_1$ МЭС.

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

Мажоритарное резервирование позволяет защититься не только от постоянных отказов, но и от перемежающихся, в том числе от воздействия помех, т.к. они обычно проявляются неодинаково в резервированных каналах обработки информации.

3.2. Применение мажоритарного резервирования для повышения показателей надежности МЭС

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

Сигнал на выходе МЭ определяется большинством $\left(\rho > \frac{m+1}{2}\right)$ выходных 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 (снижения 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 неисправно 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. 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 ***рис.3.2.*** Средняя наработка на отказ такой адаптивной системы Тр -1,28 То.

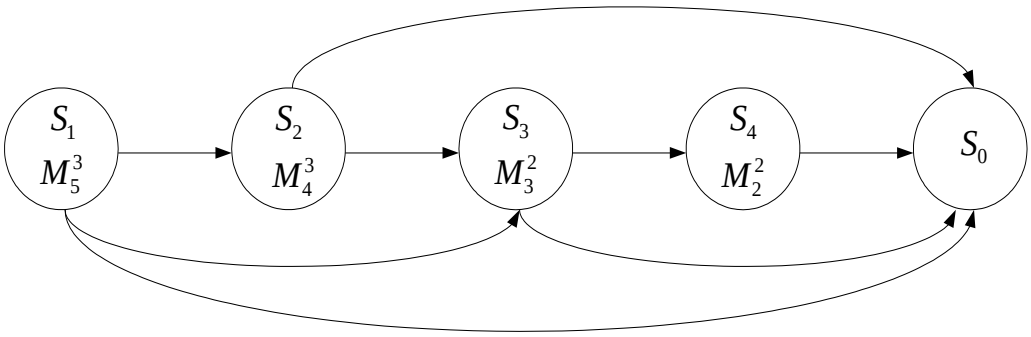

Рис.3.2

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 снижает эффективность

На ***рис.3.3*** приведены зависимости вероятности безотказной работы МРС 2v3 и 3v5 (без восстановления) от вероятности безотказной работы резервируемого канала при Рм=const. Они имеют S-образный характер, и можно сделать вывод, что в избыточных структурах 2v5, 3v5 с однократной связью возможен выигрыш в надежности при наличии высоконадежного МЭ (Рмэ->1), если вероятность безотказной работы неизбыточного канала обработки информации Ро>0.5. Недостатком таких структур является то, что вероятность их безотказной работы не превосходит вероятности безотказной работы МЭ и в случае отказа последнего отказывает вся избыточная структура.

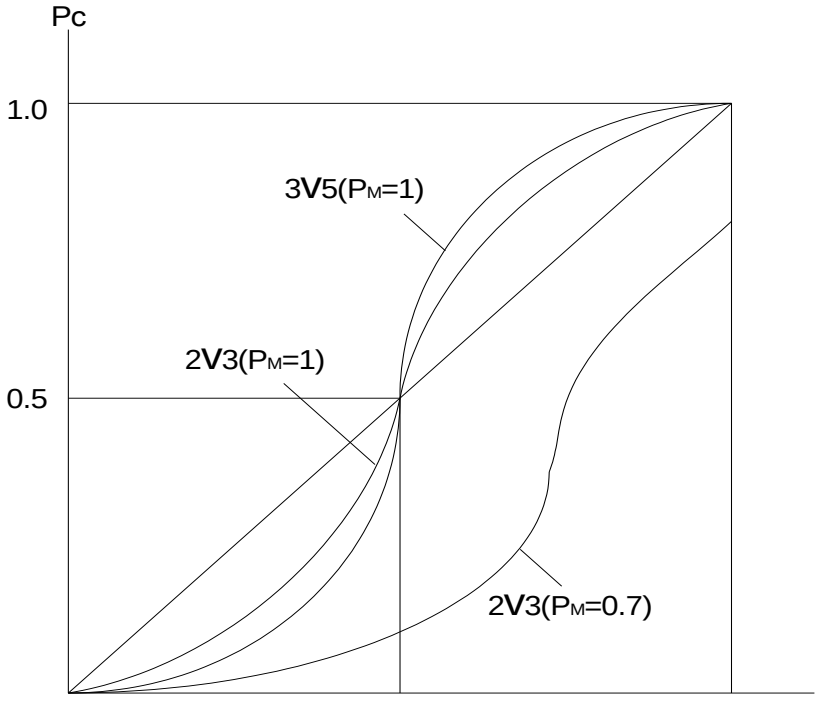

Рис. 3.3

С этой точки зрения, еще более высокие требования предъявляются к надежности МЭ при дублировании его по схеме И ***(рис. 3.4).***

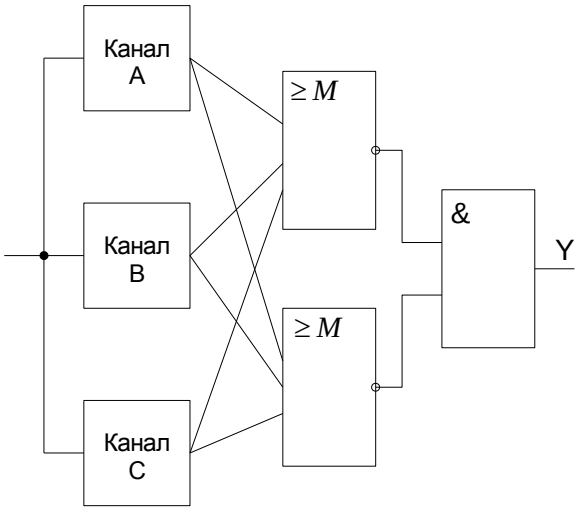

Рис. 3.4

Больший эффект от повышения надежности избыточной структуры МЭС можно получить, используя мажоритарное резервирование с многократными связями ***(рис 3.5).***

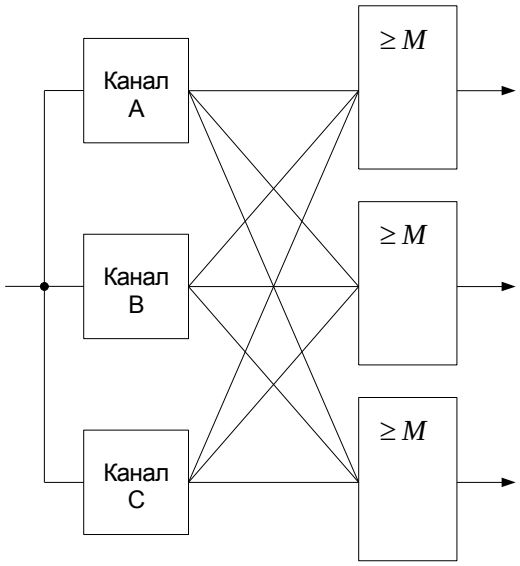

Рис. 3.5

4. 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.

4.1. 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 безопасных выходных схем (БВС) для включения управляемых объектов ***(рис.4.1).*** 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 БВС). 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. Данная архитектура применяется на Французских железных дорогах при реализации станционных систем управления.

Одноканальная система с дублированной программой (тип 2) использует две различные и независимые программы ***(рис.4.2)*** для реализации одних и тех же функций. 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. Диверситетное программное обеспечение применяется в архитектуре объектных контроллеров системы Ebilock-850 (950).

Дублированная система со слабыми связями (тип 3) состоит из двух микроЭВМ ***(рис.4.3),*** в которых процессоры и программы могут быть неодинаковыми. 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 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. Такая архитектура была применена фирмой SIEMENS в первых устройствах микропроцессорной централизации.

Дублированная система с умеренными связями (тип 4) включает в себя две одинаковые микроЭВМ ***(рис. 4.4)*** с одинаковыми программами. Работа обоих каналов синхронизирована.

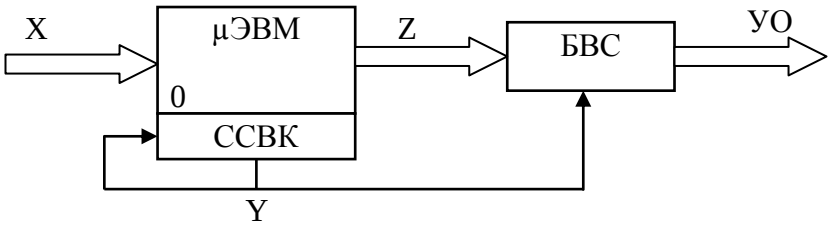

Рис.4.1

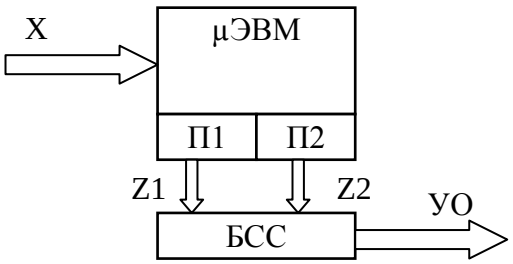

Рис.4.2

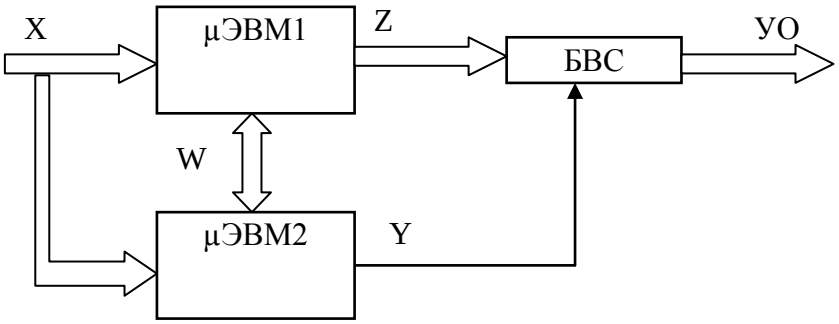

Рис.4.3

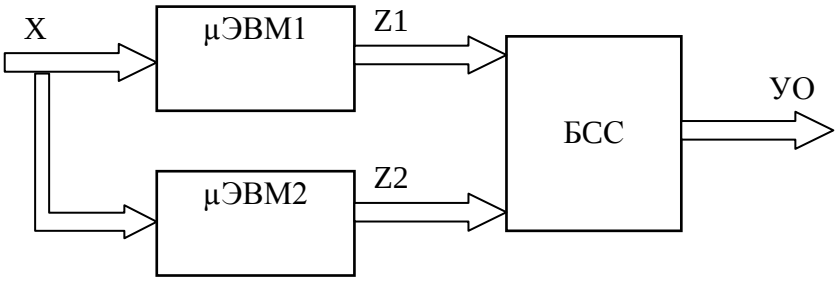

Рис.4.4

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. Данная архитектура используется в бортовых локомотивных устройствах, а для обеспечения надежности реализуется структура (2v2 «ИЛИ» 2v2).

Дублированная система с сильными связями (тип 5) использует одинаковые программы в двух одинаковых микроЭВМ ***(рис.4.5),*** 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. Работа каналов синхронизирована. В наиболее сильном случае производится потактовая проверка совпадения сигналов W1 и W2 на внутренних контрольных точках (шинах) с помощь 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.

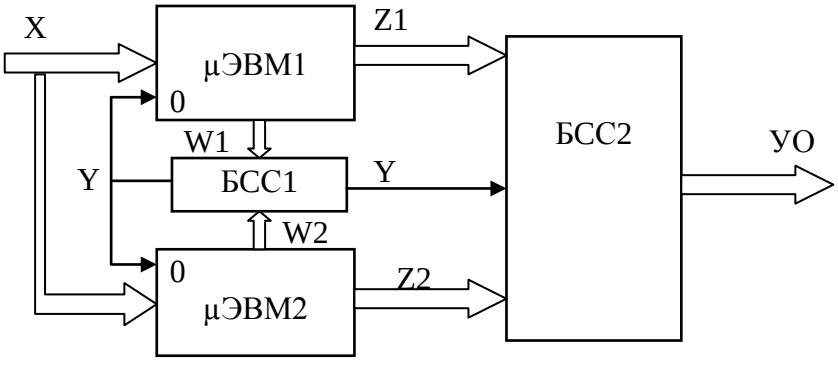

Рис.4.5

Самопроверяемая дублированная система (тип 6) состоит из двух каналов ***(рис. 4.6),*** построенных в виде самопроверяемых устройств. 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 программный. Возможно использование независимых программ в каждом процессоре.

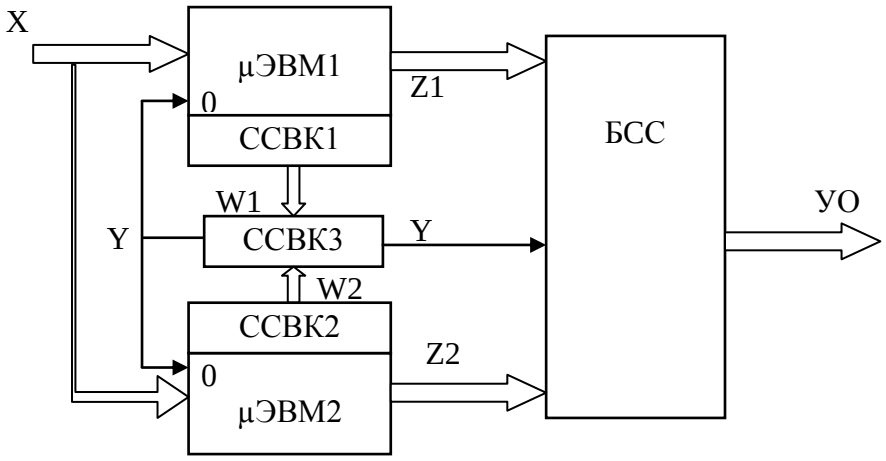

Рис.4.6

Дублированная система с тестированием и сильными связями ***(рис. 4.7)*** содержит в дополнение к структуре типа 5 генератор тестов (ГТ) и мультиплексор (МКС) и применяется, если множество входных воздействий X не обеспечивает необходимой глубины проверки каналов обработки информации. 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 имеет три независимых канала обработки информации. Работа каналов синхронизирована и сравнивается с помощью безопасного мажоритарного элемента (БМЭ). Безопасность сравнима с безопасностью дублированной структуры (рис.4.4), но отказоустойчивость увеличивается.

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

Функционирование таких систем осуществляется в ритме жесткого реального времени и применяется в современных разработках ЖАТ (SIMIS W, ЭЦ-ЕМ, МПЦ-2).

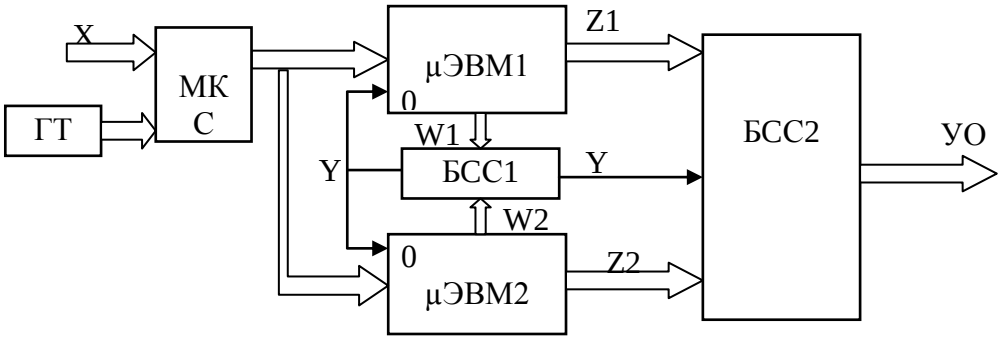

Рис.4.7

4.2. Аппаратный контроль и способы локализации отказов микропроцессорных систем автоматики

В СЖАТ, выполненных на основе МП и микроЭВМ, необходимо использовать структурное резервирование и аппаратный контроль.

Обмен информацией между отдельными узлами микроЭВМ, входящих в состав 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 узлом микроЭВМ. 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.

Для обеспечения безопасности МЭС достаточно дублирование структуры устройства. Выходная информация на внешнем интерфейсе может формироваться схемами сравнения или с выхода одной из микроЭВМ. Во втором случае необходимо дополнительное устройство, контролирующее идентичность состояния выходов обоих микроЭВМ.

Устройство контроля выходов (УК) МП-модуля может быть 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. 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, применяемых для сравнения кодовых векторов на шинах интерфейса в параллельном виде, можно сделать вывод, что одними из лучших являются самопроверяемые тестеры 2/4.

Для примера рассмотрим функциональную схему 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 появляется непарафазный сигнал, что регистрируется фиксирующим элементом (ФЭ).

Для того чтобы отличать сбои и отказы аппаратуры, ФЭ состоит из двух последовательно соединенных парафазных триггеров $ПТ_1$ и $ПТ_2$. 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 формирует сигнал восстановления $ПТ_2$.

На основе самопроверяемых тестеров может быть выполнено устройство контроля шин трехканального микропроцессорного модуля. 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 за счет сравнения кодовых векторов на шинах не в параллельном виде, а в последовательном. С этой целью для мультиплексирования сигналов на шинах МП используются универсальные сдвиговые регистры.

С целью повышения отказоустойчивости МЭС в УК мажоритарный элемент контроля может выполняться 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 возможность последовательно во времени сравнивать сигналы всех узлов вычислительных каналов.

5. ПРИНЦИПЫ ПОСТРОЕНИЯ БЕЗОПАСНЫХ СХЕМ НА ЭЛЕМЕНТАХ С НЕСИММЕТРИЧНЫМИ ОТКАЗАМИ

С точки зрения 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 $0 \rightarrow 1$ и $1 \rightarrow 0$ 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 ($\lambda_{кр}= 10^{-8} – 10^{-14}$ 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 $0 \rightarrow 1$ (h_1-надежные);

элементы, надежные относительно отказов вида $1 \rightarrow 0$ (h_o-надежные).

На практике обычно используются h_1-надежные элементы. Методы построения безопасных схем на h_1-надежных и h_o-надежных элементах одни и те же.

6. ИСПОЛЬЗОВАНИЕ САМОПРОВЕРЯЕМЫХ СХЕМ ПРИ ПОСТРОЕНИИ БЕЗОПАСНЫХ СИСТЕМ

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

Самопроверяемые ДУ содержат два блока ***(рис. 6.1).*** Первый блок (собственно ДУ) реализует функции переходов и выходов. Второй блок (КС) представляет собой контрольную схемы, 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.

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

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

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

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 $1 \rightarrow 0$, либо $0 \rightarrow 1$).

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 называется m/n-тестером.

Для обеспечения возможности прогнозирования предотказных состояний система дополняется внешними устройствами диагностирования напольного оборудования ЖАТ.

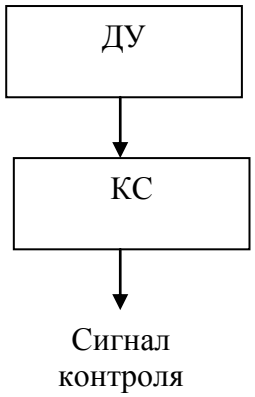

Рис. 6.1

7. МЕТОДЫ ДОСТИЖЕНИЯ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

7.1. Специфика программного обеспечения как средства контроля

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 производятся программным способом. ПО в этом случае являются определяющими в реализации системой требуемых функций.

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, 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 системой могут 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 последствий отказов.

Опыт разработки программных средств систем управления технологическими процессами, критичными к вопросам безопасности, показывает, что проблема обеспечения надежности ПО охватывает все этапы жизненного цикла программ ***(рис. 7.1).*** 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, таких как:

разработка методологической теории надежности ПО, 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 сложного ПО с заданной надежностью, применение структурных подходов к созданию ПО, 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 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.

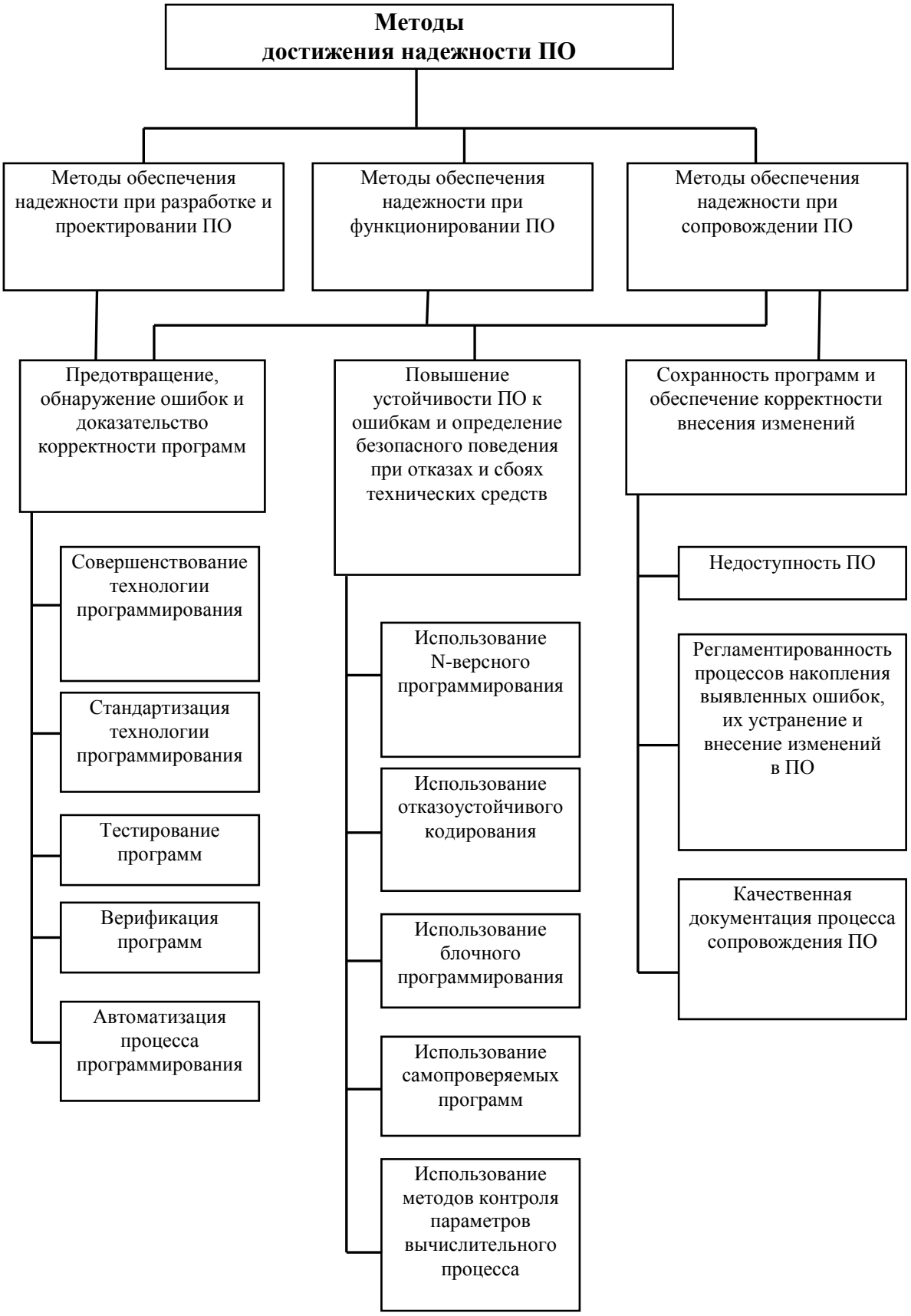
Методы
достижения надежности ПО
Методы обеспечения надежности при разработке и проектировании ПО
Методы обеспечения надежности при функционировании ПО
Методы обеспечения надежности при сопровождении ПО
Предотвращение, обнаружение ошибок и доказательство корректности программ
Повышение устойчивости ПО к ошибкам и определение безопасного поведения при отказах и сбоях технических средств
Сохранность программ и обеспечение корректности внесения изменений
Совершенствование технологии программирования
Стандартизация технологии программирования
Тестирование программ
Верификация программ
Автоматизация процесса программирования
Использование N-версного программирования
Использование отказоустойчивого кодирования
Использование блочного программирования
Использование самопроверяемых программ
Использование методов контроля параметров вычислительного процесса
Недоступность ПО
Регламентированность процессов накопления выявленных ошибок, их устранение и внесение изменений в ПО
Качественная документация процесса сопровождения ПО

Рис.7.1

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 и требует контроля ПО ***(рис.7.2).***

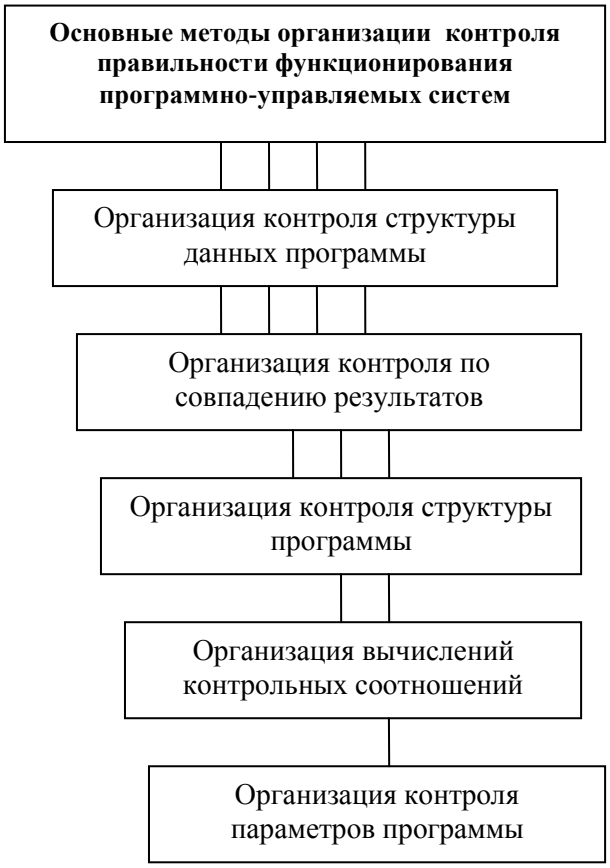

Рис.7.2

Основной функцией с точки зрения обеспечения безопасности СЖАТ является функция контроля правильности функционирования, качество которой определяется возможностью средств контроля адекватно оценивать состояние технических средств в заданный промежуток времени.

7.2. Программные методы обеспечения безопасности

7.2.1. 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 базируется на результатах синтеза самопроверяемых конечных автоматов ***(рис.7.3).*** 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).

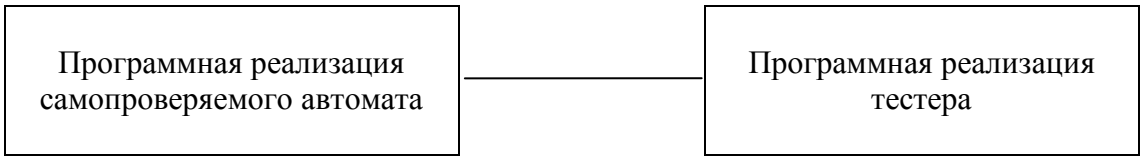

Рис.7.3

7.2.2. 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, один из которых преследует цель уменьшить, по возможности, разрушающее влияние ошибок на программу. 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 не желательных команд);

ограничении использования команд определенного типа;

введении в структуру программы команд, выполняющих функцию компенсаторов, пассивных с алгоритмической точки зрения, но активных с точки зрения контроля.

7.2.3. Тестирование

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

Область применения: микропроцессорные вычислительные системы.

Описание: Процесс контроля методом тестирования предусматривает поочередное выполнение тестовых и программных процедур. При этом их взаимное чередование может быть произвольным и определяется объектом теста. Так, например, в методе блоков восстановления 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).

7.2.4 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 программы;

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