МИНИСТЕРСТВО ПУТЕЙ СООБЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСТ 32.41-95

ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

МЕТОДЫ ДОКАЗАТЕЛЬСТВА БЕЗОПАСНОСТИ СИСТЕМ И УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Издание официальное

САНКТ-ПЕТЕРБУРГ
1995

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, **А. Б. Никитин,** канд. техн. наук, **Е. Н. Розенберг,** канд. техн. наук

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Указанием МПС РФ № Г-519-у от 28 июня 1995 г.

3 ВВЕДЕН ВПЕРВЫЕ

Содержание

ОТРАСЛЕВОЙ СТАНДАРТ

Безопасность железнодорожной автоматики и телемеханики

Методы доказательства безопасности систем и устройств железнодорожной автоматики и телемеханики

Дата введения 1995-10-01

1 Область применения

Настоящий стандарт распространяется на все виды систем и устройств (в дальнейшем - систем) железнодорожной автоматики и телемеханики (ЖАТ), к которым в нормативной (НД) и конструкторской (КД) документации предъявляются требования безопасности в соответствии с ОСТ 32.17 и ОСТ 32.18. Стандарт может быть использован при проведении сертификационных работ.

Стандарт распространяется на системы, разрабатываемые по заказам Министерства путей сообщения РФ и поставляемые другими ведомствами и организациями для железнодорожного транспорта.

Стандарт устанавливает виды и методы доказательства безопасности систем, порядок их применения и определяет структуру документа "Доказательство безопасности".

Термины, применяемые в настоящем стандарте, и их определения приводятся в соответствии с Руководством ИСО/МЭК 2, ГОСТ 27.002 и ОСТ 32.17.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты и руководящие документы:

- Руководство ИСО/МЭК 2 Общие термины и определения в области стандартизации и смежных видов деятельности;
- ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения;
- ОСТ 32.17-92 Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения;

- ОСТ 32.18-92 Безопасность железнодорожной автоматики и телемеханики. Выбор и общие правила нормирования показателей безопасности;

- ОСТ 32.19-92 Безопасность железнодорожной автоматики и телемеханики. Общие требования к программам обеспечения безопасности;

- ОСТ 32.27-93 Безопасность железнодорожной автоматики и телемеханики. Организация сбора и обработки информации о безопасности систем железнодорожной автоматики и телемеханики;

- РТМ 32 ЦШ 1115842.01-94 Безопасность железнодорожной автоматики и телемеханики. Методы и принципы обеспечения безопасности микроэлектронных СЖАТ;

- РТМ 32 ЦШ.1115843.02-94 Безопасность железнодорожной автоматики и телемеханики. Методы расчета показателей безотказности и безопасности СЖАТ;

- РТМ 32 ЦШ 1115842.03-94 Безопасность железнодорожной автоматики и телемеханики. Правила и методы обеспечения безопасности релейных схем;

- РД 32 ЦШ.1115842.01-93 Безопасность железнодорожной автоматики и телемеханики. Методы испытаний на безопасность;

- РД 32 ЦШ 1115842.02-93 Безопасность железнодорожной автоматики и телемеханики. Порядок и методы контроля показателей безопасности, установленных в нормативно-технической документации;

- РД 32 ЦШ 1115842.03-93 Безопасность железнодорожной автоматики и телемеханики. Критерии опасных отказов;

- РД 32 ЦШ 1115842.04-93 Безопасность железнодорожной автоматики и телемеханики. Методы расчета норм безопасности;

- РД 32 ЦШ 03.07-90 Аппаратура железнодорожной автоматики и связи. Общие технические условия;

- РД 32 ЦШ 03.08-90 Аппаратура железнодорожной автоматики и связи. Технические условия (ТУ). Методика испытаний (МИ). Типовая форма построения и изложения.

3 Общие положения

3.1 Доказательство безопасности должно состоять из теоретической и экспериментальной частей. Оно является результатом ме-

роприятий, проводимых в соответствии с программой обеспечения безопасности. Требования к программе обеспечения безопасности определены в ОСТ 32.19-92.

3.2 Доказательство безопасности осуществляется на всех стадиях разработки, сертификационных испытаний, пусконаладочных работ и эксплуатации системы железнодорожной автоматики и телемеханики (СЖАТ).

3.3 Целями доказательства безопасности являются:

- проверка выполнения концепции обеспечения безопасности;

- проверка соответствия СЖАТ качественным требованиям безопасности, сформулированным в нормативной и конструкторской документации;

проверка соответствия показателей безопасности заданным в соответствии с РД 32 ЦШ 1115842.02-93 нормам.

3.4 Проверка выполнения концепции обеспечения безопасности системы должна быть направлена на доказательство

выполнения алгоритмических условий обеспечения безопасности движения поездов;

- выполнения конструктивных требований безопасности,

- защищенности от перехода в опасное состояние при ошибках в программном обеспечении, появлении отказа в аппаратных средствах или воздействии электромагнитных помех;

- защищенности от механических и климатических воздействий;

- защищенности от ошибочных и несанкционированных действий обслуживающего и оперативного персонала;

- защищенности от опасного искажения ответственной информации.

3.5 В документе "Доказательство безопасности" следует в письменной форме обосновать, что устройство или система являются безопасными в соответствии с ОСТ 32.17-92, 32.18-92.

3.6 Разработка документа "Доказательство безопасности" осуществляется организацией-разработчиком системы и устройств. Документ утверждается руководителем этой организации и представляется для независимого экспертного заключения в организацию, которая будет производить сертификационные испытания. При наличии положительного экспертного заключения система может быть допущена к эксплуатационным испытаниям.

3.7 "Доказательство безопасности" является обязательным документом при проведении сертификации соответствия требованиям безопасности.

4 Виды доказательства безопасности

4.1 Доказательство безопасности основывается на шести видах доказательства, применяемых на различных стадиях создания, испытаний и эксплуатации системы:

- экспертных методах;
- расчетных методах,
- испытаниях на машинных моделях;
- стендовых испытаниях,
- испытаниях системы в условиях эксплуатации;
- сборах статистических данных об отказах в процессе эксплуатации.

4.2 Последовательность применения видов доказательства безопасности, используемые методы и программы испытаний по РД 32 ЦШ 1115842.01-93, РД 32 ЦШ 03.08-90 включаются в программу обеспечения безопасности, выполненную в соответствии с ОСТ 32.19-92.

4.3 Указанные в 4.1 виды доказательства должны носить законченный характер для подтверждения показателей безопасности или являться промежуточными этапами интегральной оценки показателей безопасности по результатам нескольких видов испытаний (см. приложение Б).

4.4 С учетом специфики устройств ЖАТ возможно исключение некоторых видов доказательства безопасности. При этом должна быть приведена мотивировка, которая является составной частью доказательства безопасности.

5 Экспертные методы

5.1 Экспертные методы применяются на всех этапах разработки системы: при разработке технических предложений и технического задания, при эскизном и техническом проектировании, составлении рабочей документации [6].

5.2 Экспертами являются, как правило, сотрудники независимой

организации, выполняющей сертификационные испытания систем и устройств. Независимые эксперты должны оценить: концепцию обеспечения безопасности, принятую разработчиками данной системы; критерии опасных отказов, определенные в соответствии с РД 32 ЦШ 1115842.03-93; требования и нормируемые показатели безопасности, их значения и методы расчета по РД 32 ЦШ 1115842.04-93; предлагаемые программно-технические решения. Эксперты проверяют технические решения на соответствие утвержденным правилам и методам построения безопасных схем (например РТМ 32 ЦШ 1115842.01-94, РТМ 32 ЦШ 1115842.03-94) с учетом возможных отказов. Объективность экспертизы определяется личным опытом экспертов, их знаниями в соответствующей области техники.

Для работы экспертам предоставляются научно-исследовательские отчеты, выпущенные разработчиками, ТЗ, ТУ, техническое описание, инструкции по обслуживанию и эксплуатации, рабочие программы и методики испытаний и т.п.

5.3 Основные задачи, которые должны решать эксперты на различных стадиях разработки и проектирования системы, приведены в таблице 1.

6 Расчетные методы

6.1 Расчетные методы реализуются на основе утвержденных методик, например РТМ 32 ЦШ 1115842.02-94, и используются для обоснования предполагаемого уровня безопасности на разных этапах разработки системы.

6.2 В зависимости от требуемой точности при расчетах уровня безопасности должны учитываться [7]:

- отказы (сбои) основной и резервной аппаратуры;
- отказы и сбои внешних контрольных устройств;
- эффективность средств контроля;
- процессы восстановления и реконфигурации;
- ошибки программного обеспечения при написании и загрузке программ;
- ошибки аппаратных средств при изготовлении.

6.3 Группы методов расчета безопасности и используемые в них модели приведены на рисунке 1.

Таблица 1

Этап	Задача
Технические предложения	Оценка концепции безопасности
Техническое задание	Оценка принятых норм и требований безопасности
Эскизное проектирование	Оценка уровня безопасности выбранного варианта системы
Технический проект	Оценка принятых технических решений и списка опасных отказов
Рабочая документация	Оценка результатов испытаний имитационной модели СЖАТ и достигнутого проектного уровня безопасности

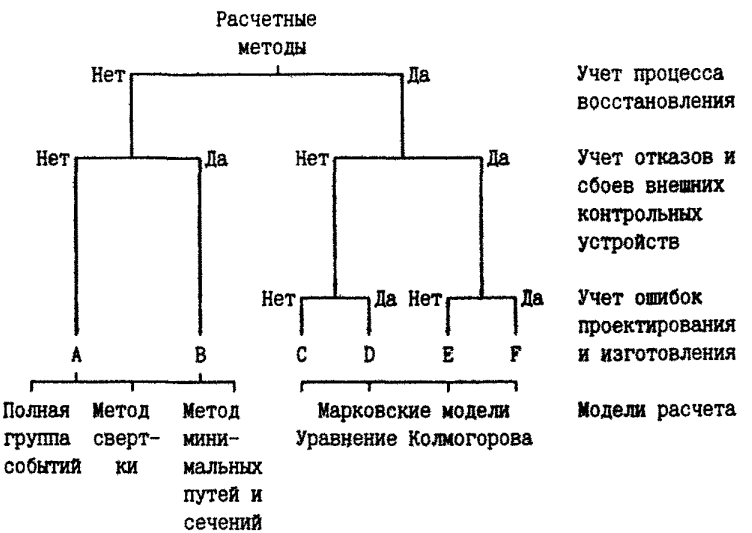
Расчетные методы
Нет
Да
Учет процесса восстановления
Нет
Да
Нет
Да
Учет отказов и сбоев внешних контрольных устройств
Нет
Да
Нет
Да
Учет ошибок проектирования и изготовления
A
B
C
D
E
F
Полная группа событий
Метод сверт-ки
Метод мини-мальных путей и сечений
Марковские модели
Уравнение Колмогорова
Модели расчета

Рисунок 1

6.3.1 На этапе технических предложений выполняется первый оценочный расчет безопасности выбранной структуры для построения системы (метод группы А).

6.3 2 На этапе технического задания и эскизного проектирования выполняется расчет безопасности с учетом безопасности внешних контрольных устройств (метод группы В).

6.3.3 Для восстанавливаемых систем на этапе технического проекта выполняется расчет безопасности с учетом процессов восстановления, реконфигурации и обслуживания (методы групп С или Е).

6.3.4 При наличии данных по ошибкам проектирования и изготовления производится наиболее точный расчет безопасности (методы групп D или F).

6.3.5 После имитационных и эксплуатационных испытаний системы, а также сбора статистических данных по отказам, возникающим в процессе эксплуатации, указанные расчеты безопасности уточняются.

7 Испытания безопасности с помощью моделирования

7.1 Моделирование является одной из основных методологических концепций, играющей ведущую роль в процессе анализа безопасности СЖАТ. При исследовании безопасности сложных технических систем моделирование является одним из основных средств ее оценки. Моделирование предполагает формирование условного образа (модели) реальной системы и изучение его свойств с целью получения информации о реальной системе. Однако по сравнению с реальной системой (оригиналом) модель может иметь совершенно иную природу. Реальная система и ее модель должны быть адекватны, т.е. соответствовать друг другу. Классификация возможных методов моделирования приведена в приложении В

7.2 Имитационное моделирование

7.2.1 Основной формой системного анализа безопасности сложных технических систем является имитационное исследование, проводимое в рамках имитационных моделей, реализуемых на ЭВМ. При этом необходимо стремиться к наиболее полному учету всех существенных факторов. При имитации события разворачиваются во времени, как правило, в том порядке, в каком они следуют в реальной системе, но в измененной временной шкале.

7.2.2 Действие случайных факторов учитывается с помощью специальных датчиков случайных чисел (имитаторов), настроенных на соответствующие вероятностные распределения. В определенном месте процесс имитации на ЭВМ может быть приостановлен для проведения, например, операционной игры, экспертного опроса или натурного эксперимента с использованием промежуточных данных, полученных при машинной имитации. Результаты игры, экспертизы или эксперимента могут быть использованы для продолжения имитации на ЭВМ.

7.2.3 Имитационное моделирование объединяет имитацию исследуемого явления и планирование эксперимента. Теория планирования эксперимента позволяет организовать имитационный эксперимент рациональным образом применительно к целенаправленному получению информации.

7.2.4 При имитационном моделировании сложных систем главным требованием является адекватность модели. Однако при высокой сложности реальной системы ее адекватная имитационная модель также становится довольно сложной. Одна реализация имитируемого явления (прогон модели) может быть весьма продолжительной, а сделать какие-либо содержательные выводы о свойствах системы по одной реализации, как правило, не удается. Проведение статистических имитаций в рамках модели при различных исходных данных может оказаться неприемлемым по времени. В этих условиях эффективными являются методы планирования эксперимента.

7.2.5 Имитационный эксперимент планируют либо с целью получения оптимальных значений факторов (задача оптимизации по определенным критериям), либо с целью получения аналитической зависимости выходной переменной (отклика) от контролируемых переменных (факторов) в достаточно широкой области изменения последних (задача аппроксимации). Достоинством имитационного моделирования является возможность фиксации промежуточных значений различных показателей в процессе имитации подобно тому, как это имеет место при съеме данных в процессе функционирования реальной системы.

7.3 Для ускорения проведения испытаний с помощью различных видов моделирования используют вычислительную технику (машинное моделирование).

7.3.1 Испытания безопасности на машинных моделях производятся на этапе разработки рабочей документации и делятся на пять ви-

дов:

испытания технологических алгоритмов;

- моделирование работы дискретных и аналоговых аппаратных средств при сбоях и отказах;

- испытание имитационной модели программно-технических средств;

- испытания прикладного программного обеспечения;

- испытания системных функций.

7.3.2 Испытания безопасности на машинных моделях имеют следующие основные цели:

- производство ускоренных испытаний в машинном времени;

- создание во время испытаний всего множества возможных технологических ситуаций;

- имитация заданного класса (вида) отказов аппаратных и программных средств;

- организация процедуры верификации прикладного программного обеспечения;

- корректировка списка опасных отказов;

- организация вероятностных экспериментов с машинными моделями систем большой размерности;

- сбор статистических данных по влиянию отказов и сбоев на безопасность.

7.3.3 Испытания технологических алгоритмов проверяют выполнением всех условий безопасности в данном технологическом процессе.

7.3.3.1 При испытаниях с помощью ЭВМ создаются все штатные и возможные нештатные технологические ситуации и сравнивается реакция системы с эталонной реакцией.

7.3.3.2 При испытаниях предусматриваются отказы внешних датчиков и неправильные действия человека-оператора.

7.3.4 Моделирование используется для испытаний дискретных и аналоговых аппаратных средств, ответственных за безопасность (схем сравнения и контроля, мажоритарных схем, фиксаторов ошибок (отказов), тестеров, фильтров, усилителей и др.).

7.3.4.1 При испытаниях схемы представляются в ЭВМ и организуются эксперименты двух видов:

- внесение отказов из заданного списка и определение реакции

схемы на эти отказы;

- анализ работы схемы при разбросе временных параметров.

7.3.4.2 Доказательство отсутствия опасных отказов осуществляется прямым методом перечисления анализируемых ситуаций.

7.3.5 Испытания безопасности программно-технических комплексов, содержащих микропроцессорные БИС и другие интегральные схемы большой сложности, проводятся на имитационных машинных моделях.

7.3.5.1 Имитационная модель представляет программно-технический комплекс с определенной точностью (на уровне шин данных, регистровых передач, ячеек памяти и т.п.).

7.3.5.2 Испытания производятся с внесением отказов в машинную модель при выполнении прикладных программ.

7.3.5.3 Данный вид испытаний позволяет оценить выбранную концепцию безопасности.

8 Стендовые испытания

8.1 Цель стендовых испытаний - проверка безопасности функционирования всех составных элементов системы в комплексе, в их взаимодействии.

8.2 Стендовые испытания проводятся с помощью генератора входных технологических ситуаций и имитаторов объектов управления и контроля по специальным программам.

Длительность испытаний колеблется обычно от одного месяца до года. Это позволяет собрать определенные статистические данные об отказах и сбоях, которые используются для уточнения аналитических расчетов безопасности. Стендовые испытания проводятся с учетом влияния на безопасность опытного образца колебания питающего напряжения, электромагнитных, климатических и механических воздействий, возможных в условиях эксплуатации.

8.3 Программы стендовых испытаний предусматривают:

- физическое моделирование отказов;
- проверку электромагнитной совместимости (с учетом перенапряжений);
- колебания питающего напряжения;
- испытания на электрическую прочность;
- климатические испытания;

- испытания на воздействие механических факторов;
- специальные измерения.

9 Испытания в условиях эксплуатации

9.1 Система допускается к опытной эксплуатации при наличии выданного независимой организацией, проводящей сертификационные испытания, положительного экспертного заключения по всем предшествующим этапам экспертизы, определенным программой обеспечения безопасности.

9.2 Данный вид испытаний проводится после пусконаладочных работ и имеет целью доказательство безопасности в реальных условиях и режимах эксплуатации, технического обслуживания и ремонта.

9.3 Длительность и характер испытаний устанавливаются в программе испытаний.

9.4 При наличии на объекте старой системы управления целесообразно включить новую систем' последовательно или параллельно со старой. Это позволяет путем сравнения работы двух систем гарантированно зафиксировать случаи возникновения опасных отказов.

9.5 В течение всего срока испытаний фиксируются защитные и опасные отказы системы. Полученные данные используются для уточнения аналитических расчетов безопасности, выявления конструктивных и технологических недостатков систем, снижающих их безопасность.

10 Сбор статистических данных в процессе эксплуатации

10.1 Сбор статистических данных об опасных отказах при длительной эксплуатации большого числа экземпляров систем и устройств ЖАТ позволяет оценить эффективность проводимых мер по обеспечению безопасности и является наиболее объективным методом доказательства безопасности.

10.2 Основные принципы сбора и обработки данных об отказах установлены в ОСТ 32.27-93.

10.3 Полученные данные об опасных отказах систем и устройств ЖАТ используются для:

- анализа уровня безопасности эксплуатируемых технических

средств и тенденции его изменения;

- установления элементов, ограничивающих безопасность изделий;

- выполнения окончательных расчетов показателей безопасности.

11 Структура документа "Доказательство безопасности"

11.1 Документ "Доказательство безопасности" должен содержать:

- вводные замечания;
- нормативные документы, используемые для доказательства безопасности;
- характеристику объекта;
- доказательство работоспособности;
- методы доказательства безопасности;
- реальные ограничения;
- программу и методику испытаний;
- характеристику испытательной аппаратуры;
- подтверждение безопасности, результаты испытаний и экспертизы;
- заключение по безопасности;
- список использованных источников.

11.1.1 Вводные замечания должны содержать:

- назначение объекта в системе обеспечения безопасности движения поездов;
- описание взаимодействия объекта с другими средствами и уровнями обеспечения безопасности;
- условия эксплуатации и технического обслуживания.

11.1.2 В разделе "Нормативные документы, используемые для доказательства безопасности" приводится перечень международных (при необходимости), государственных и отраслевых документов, которые регламентируют содержание и структуру доказательства безопасности.

11.1.3 Характеристика объекта должна содержать:

- концепцию обеспечения безопасности;
- требования и нормы безопасности;

- критерии опасных отказов;
- краткое описание принципов построения и работы;
- описание конструктивного оформления.

11.1.4 Доказательство работоспособности удостоверяет, что система соответствует требованиям ТЗ или иных нормативных документов и что в разработанных приборах, устройствах, системах и программных продуктах отсутствуют систематические ошибки при эксплуатации их в заданных режимах и условиях.

11.1.5 В разделе "Методы доказательства безопасности" приводится перечень используемых методов доказательства безопасности и определение целей использования применяемых методов доказательства безопасности. Применяемые методы используются для доказательства:

- выполнения концепции безопасности разработанной системы;
- выполнения количественных и качественных требований безопасности, установленных в нормативной документации;
- перехода системы в защитное состояние при появлении отказов или сбоев;
- независимости отказов в структурно-резервированных каналах;
- полноты диагностирования заданного класса отказов с заданной достоверностью (отсутствия накопления отказов);
- обеспечения необратимого защитного (выключенного) состояния отказавших (неисправных) элементов, блоков или каналов системы;
- требуемой эффективности программных и аппаратных средств контроля;
- защищенности от опасных отказов системы при неисправности источников питания, отказах программного обеспечения, отказах и сбоях входных и выходных элементов, при перенапряжениях, при влиянии климатических и механических факторов. Примерная форма анализа защищенности от отказов приведена в приложении Г.

11.1.6 В разделе "Реальные ограничения" определяются границы применения каждого из используемых методов доказательства безопасности, например: используемые допущения при расчете показателей безопасности, учитываемый класс повреждений, полнота и достоверность испытаний.

11.1.7 В разделе "Программа и методика испытаний" приводится описание нетиповых (оригинальных) программ и методик. При использовании типовых или ранее утвержденных МПС РФ программ и методик допускается не приводить их в доказательстве безопасности, а привести ссылку на них.

11.1.8 В разделе "Характеристика испытательной аппаратуры" приводится перечень используемой типовой испытательной аппаратуры, а также при необходимости перечень нестандартных средств (комплексов программных средств, имитаторов и измерительных приборов) с параметрами, характеризующими достоверность проведения испытаний.

11.1.9 В разделе "Подтверждение безопасности, результаты испытаний и экспертизы" приводятся протоколы и акты различных видов испытаний и экспертные заключения.

В этом разделе требуется доказать, что соблюдается основной принцип безопасности железнодорожной автоматики и телемеханики - одиночный отказ не должен приводить систему в опасное состояние.

Это доказательство осуществляется на основании перечня отказов, возможных в данном типе аппаратуры.

После первого отказа может возникнуть второй, третий и т д. В зависимости от концепции обеспечения безопасности безопасная реакция системы в целом может обеспечиваться даже в случае отказа двух или более конструктивных элементов, например в системах, выполненных на реле I класса надежности. В микроэлектронных системах, как правило, используют концепцию быстрого обнаружения (за допустимый интервал времени) отдельного отказа. Возникновение двух и более отказов за рассматриваемый интервал времени должно иметь вероятность не выше установленной в НД на конкретный тип аппаратуры. Вероятность такого события определяется на основании расчетов или моделирования.

При анализе влияния на систему одиночных отказов важным свойством для безопасности является независимость отказов. Если это требование нарушается, то необходимо считаться с множественными отказами, которые не обнаруживаются средствами контроля (тестовыми программами, компараторами, контрольными схемами и т.п.). В приложении D приведен пример анализа на независимость отказов критических мест в двухканальной системе.

В данном разделе также должно быть подтверждено, каким образом и за счет чего обеспечивается безопасное состояние системы при возникновении отказов, при изменении параметров элементов в допустимых пределах, при воздействии электромагнитных помех, климатических и механических факторов. В разделе приводятся требования по эксплуатации, относящиеся к обеспечению безопасности.

11.2 Доказательство безопасности сложной системы может быть подразделено на доказательства безопасности ее отдельных подсистем. Структура доказательства безопасности по 2.1 должна повторяться для каждой из подсистем.

11.3 Электрические и информационные связи отдельных подсистем должны быть подвергнуты самостоятельному анализу на безопасность.

11.4 Доказательство безопасности проходит экспертизу в независимых испытательных лабораториях. При положительных результатах экспертизы выдается заключение (свидетельство) о безопасности системы. После выдачи заключения доказательство безопасности не может быть изменено. Изменения, которые в дальнейшем вносятся в систему и могут влиять на ее безопасность, должны сопровождаться новым доказательством безопасности.

11.5 Доказательство безопасности содержит оценку адекватности испытаний условиям эксплуатации, которая зависит от реальных ограничений (класс рассматриваемых отказов, время испытаний, точность измерений и т.д.).

11.6 В доказательстве безопасности отдельных частей системы допускается делать ссылки на известные доказательства безопасности при условии полной идентичности части устройства и ее связей этому доказательству.

11.7 Доказательство безопасности хранится у разработчиков и в испытательной лаборатории, выдававшей заключение о безопасности системы. Срок хранения заканчивается не ранее чем через 10 лет после прекращения производства системы.

Приложение А
(справочное)

Библиография

1. Голинкевич Т. А. Прикладная теория надежности. - М.: Высшая школа, 1985. - 168 с.

2. Дружинин Г. В. Надежность автоматизированных систем - М.: Энергия, 1977. - 536 с.

3. Чуа Л. О., Лин П. М. Машинный анализ электронных схем (алгоритмы и вычислительные методы). - М.: Энергия, 1980. - 600 с.

4. Судаков Р. С. Испытания технических систем. - М.: Машиностроение, 1988. - 272 с.

5. Надежность и эффективность в технике. Т.6. Экспериментальная обработка и испытания: Справочник / Под ред. Р.С. Судакова. - М.: Машиностроение, 1988. - 376 с.

6. Гавзов Д. В. Методика проведения экспертизы на безопасность устройств железнодорожной автоматики и телемеханики // Автоматика, телемеханика и связь. - 1994. - N 6. - С. 26 - 27.

7. Гавзов Д. В., Самонина Е. В. Методика расчета количественных показателей безопасности микропроцессорных систем железнодорожной автоматики и телемеханики // Вестник ВНИИЖТа. - 1992. - N 5. - С. 21 - 25.

8. Надежность и эффективность в технике. Т.3. Эффективность технических систем: Справочник /Под ред. В.Ф. Уткина, Ю.В. Крючкова. - М.: Машиностроение, 1988. - 328 с.

9. Гавзов Д. В., Сапожников В. В., Сапожников Вл.В. Методы обеспечения безопасности дискретных систем // Автоматика и телемеханика. - 1994. - N 8. - С. 3 - 50.

10. Чжоу Ч. Модели надежности и безопасности микропроцессорных систем управления // Железные дороги мира. - 1981. - N 10. - С. 51 - 57.

Приложение Б
(справочное)
Взаимосвязь методов доказательства безопасности программного обеспечения

Указанные в 4.1 методы доказательства безопасности в отношении программного обеспечения более ограниченны, чем при анализе и испытании на безопасность аппаратных средств. Это обусловлено неоднородностью характеристик программ, влияющих на безопасность функционирования систем. В таких случаях используют результаты различных методов доказательства. Основными целями такого подхода являются:

- получение последовательных с поэтапным повышением полноты и достоверности оценок требуемых показателей безотказности и безопасности;

- получение промежуточных данных оценки безотказности и безопасности по результатам различных подходов доказательства;

- выявление и локализация мест наиболее вероятных опасных отказов для обоснования принятия решения об объемах и степени детализации имитационных или стендовых испытаний.

Взаимосвязь методов можно проиллюстрировать на следующем примере. Если экспериментально определены возможные искажения программы в результате сбоев или отказов аппаратных средств и их влияние на параметры вычислительного процесса (структуру, данные, временные параметры), то при заданных значениях интенсивности отказов аппаратуры и известной эффективности средств контроля можно аналитически оценить вероятность опасного отказа.

Приложение В
(справочное)

Классификация моделей и методов моделирования

В теории безопасности методы математического моделирования занимают ведущее место. Однако при моделировании в технике [8] дело в значительной мере осложняется тем, что наряду с чисто физическими процессами функционирования разнообразных технических подсистем, агрегатов, устройств приходится моделировать поведение людей в различных формах их взаимодействия между собой, что вынуждает обращаться к неформальным методам интуитивного моделирования, экспертного оценивания, анализа рефлексий и т.д.

Различают материальное (предметное) и идеальное моделирование (рисунок П.В.1). В первом случае в качестве модели предполагается использование некоторого материального предмета. По природе аналогии материальное моделирование делят на физическое (макетирование, обеспечивающее аналогию физической природы оригинала и модели) и аналоговое (обеспечивающее сходство процессов, протекающих в оригинале и модели). Идеальное моделирование основывается на мысленной идеализированной аналогии реального объекта и его модели, а по способу отражения реального объекта (или по глубине формализации) делится на знаковое (семиотическое) и интуитивное моделирование.

По способу представления семиотических моделей различают математическое, логическое и графическое моделирование. Математическое моделирование играет определяющую роль среди других форм знакового моделирования. Однако довольно трудно четко отделить логическое и графическое моделирование от математического ввиду их тесного переплетения (например в форме логико-математического моделирования и т.п.).

По определению различных показателей, отношений и т.п. методы математического моделирования делят на аналитические и алгоритмические. Аналитическое моделирование предполагает использование математической модели реального объекта в форме алгебраических, дифференциальных, интегральных и других уравнений, связывающих выходные переменные с входными, дополненных системой ограни-

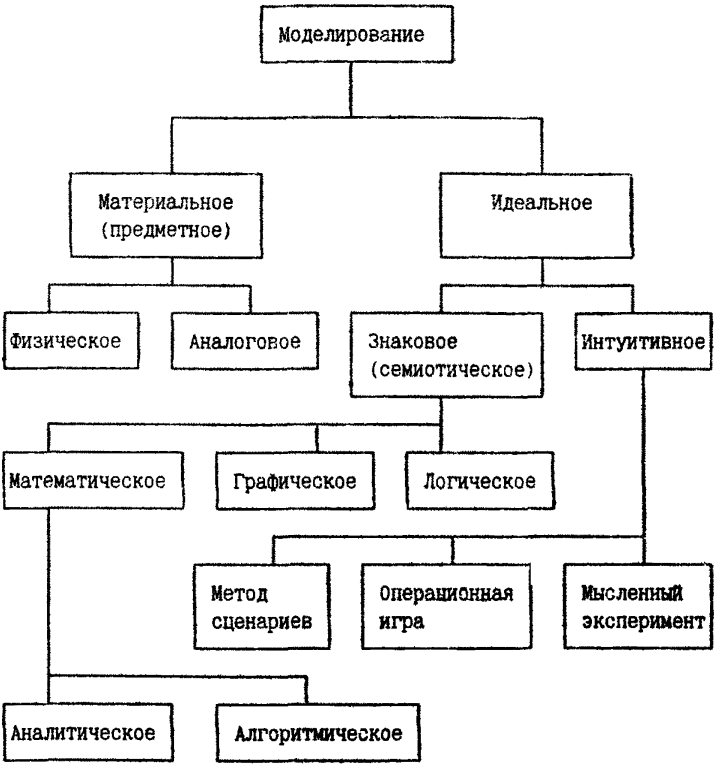

Рисунок П.В.1 Классификация методов моделирования

чений (в виде равенств или неравенств). При этом предполагается наличие однозначной вычислительной процедуры получения точного решения уравнения. При алгоритмическом подходе используемая математическая модель не допускает точного решения и вынуждает обращаться к различным рекуррентным методам, интерактивным процедурам поиска приближенного решения. Такой подход при моделировании сложных систем является типичным.

Интуитивное моделирование проводится на вербальном (описательном) уровне. При этом методе не устанавливают строгие количественные соотношения между моделируемыми явлениями, ограничиваясь лишь анализом качественных обобщенных понятий, отражающих общие тенденции развития явлений, направления изменения свойств изучаемых объектов и т.п. Такой подход осуществляется с целью выдвижения различного рода гипотез поведения субъектов сложных систем, формирования эвристик относительно взаимоотношений между активными элементами системы и их развития.

По способу формирования эвристик различают следующие формы интуитивного моделирования: метод сценариев, операционные игры, мысленный эксперимент и др. Интуитивное моделирование является основным методом моделирования деятельности метасистемы. Концептуальные модели метасистемы часто представляют в аналитическом виде, учитывая лишь некоторые существенные связи и отношения между моделируемыми явлениями.

Имитационное моделирование, являясь своеобразным экспериментированием с моделью реальной системы, синтезирует знаковое и интуитивное (иногда и материальное) моделирование. Таким образом, в имитационном моделировании используются практически все методы моделирования, отображенные на рисунке П.В.1.

Имитационное моделирование не следует противопоставлять методам математического программирования. При исследовании операций типичным является следующий подход. Путем различного рода допущений реальную задачу идентифицируют с одной из стандартного класса задач математического программирования (линейного программирования, динамического программирования и т.п.). Для каждого класса задач разработаны алгоритмы решения, воспользовавшись которыми исследователь (при интересующих его исходных данных) может получить решение своей задачи. Этот путь решения оптимизационных за-

дач известен в практике исследования систем на уровне *структура - функция* [8]. Однако такой подход не всегда приводит к успеху при исследовании сложных систем уровня *организация - поведение*. Упрощенное описание сложной системы, выполненное с целью сведения ее к одному из классов моделей математического программирования, часто приводит к утрате адекватности модели и, как следствие этого, к обесцениванию получаемых результатов.

Приложение Г
(рекомендуемое)

Форма записи классификатора отказов

Вид отказа	Последствия отказа	Обнаружение отказа
1	2	3

Приложение Д
(рекомендуемое)

Независимость отказов и сбоев

После подтверждения безопасности каждого отдельного отказа необходимо доказать, что данный произошедший отказ не вызывает дополнительно одного или группы отказов, приводящих систему в опасное состояние, т.е. необходимо подтвердить, что отказы, возникающие в системе, независимы. Это требование относится как к релейным, так и к микроэлектронным системам.

На рис. П.D.1 показаны критические места в двухканальной установке, которые могут оказать влияние на независимость отказов (1 - предыдущая схема; 2 - источник питания; 3 - блок опорного сигнала; 4 - устройство синхронизации и начального запуска; 5 - блок межканального обмена информацией; 6 - компаратор; 7 - выходная схема).

Для обеспечения независимости отказов каналы обработки информации питают от разных источников напряжения, используют элементы гальванической развязки, состоящей из конструктивных элементов, короткое замыкание между которыми можно не учитывать. Для обеспечения независимости отказов при вводе информации и при обмене информацией между каналами часто используют информационную избыточность (обнаруживающие коды).

Система (рисунок П.D.1) должна быть защищена от возникновения одинаковых сбоев при воздействии электромагнитных помех. С этой целью используются различные фильтры, элементы гальванической развязки, различные конструктивные решения, обеспечивающие независимость сбоев в каналах обработки информации.

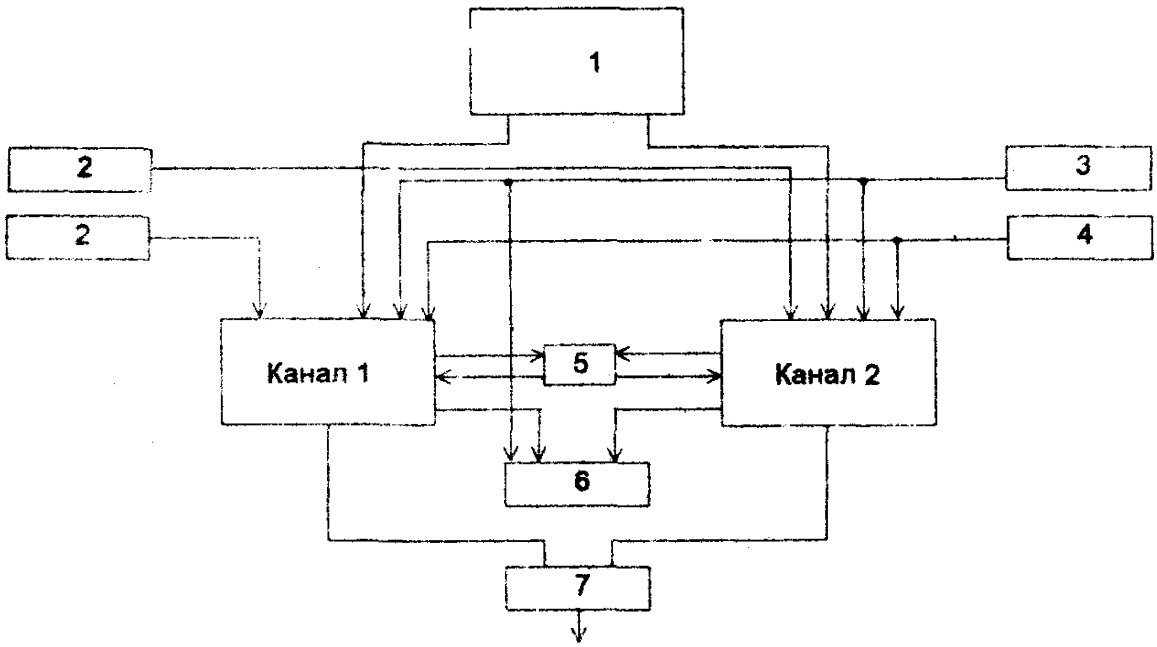

Рисунок П.D.1

УДК 656.25 Д 50

Ключевые слова: доказательство безопасности, испытания на безопасность, имитационное моделирование, опасный отказ, критерии опасного отказа, количественные и качественные требования безопасности

ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Методы доказательства безопасности систем и устройств железнодорожной автоматики и телемеханики

Редактор Н.Е.Фролова

Подписано в печать с оригинала-макета 25.09.95.
Формат 60 х 84 1/16. Бумага для множ. апп. Печать офсетная.
Усл.-печ. л. 2,0. Уч.-изд. л. 2,0. Тираж 1000. Заказ *911*.

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

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