ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

ОСНОВНЫЕ ПОНЯТИЯ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ОСТ 32.17—92

Издание официальное

САНКТ-ПЕТЕРБУРГ

УДК 656.25 Группа Д50

ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ Основные понятия. Термины и определения

ОСТ 32.17-92

ОКСТУ 4201

Дата введения 1.01.1993 г.

Настоящий отраслевой стандарт устанавливает термины и определения основных понятий в области безопасности железнодорожной автоматики и телемеханики, которые обязательны для применения в проектной и конструкторской документации, научно-технической, учебной и справочной литературе.

Все термины и определения, которые используются в данном стандарте и не устанавливаются им, соответствуют ГОСТ 27.002-89 "Надежность в технике. Основные понятия. Термины и определения".

Понятия, определяемые стандартом, даются применительно к техническому объекту - элементу, устройству или системе железнодорожной автоматики и телемеханики (в дальнейшем просто - система). Железнодорожная автоматика и телемеханика - это комплекс технических систем, предназначенных для управления движением поездов и обеспечения безопасности движения.

Стандарт состоит из пяти разделов: общие понятия; показатели безопасности; безопасность дискретных систем; нормирование безопасности; обеспечение, определение и контроль безопасности.

Стандарт следует применять совместно с ГОСТ 27.002-89.

Термин	Определение

I. ОБЩИЕ ПОНЯТИЯ

1.1. Надежность E.Dependability, reliability	Свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования (по ГОСТ 27.002-89)
1.2. Безопасность системы железнодорожной автоматики E.Railroad automatic system safety	Свойство системы непрерывно сохранять исправное, работоспособное или защитное состояние в течение некоторого времени или наработки
1.3. Защитное состояние E.Protective state	Неработоспособное состояние системы, при котором значения всех параметров, характеризующих способность выполнять заданные функции по обеспечению безопасности движения поездов, соответствуют требованиям нормативно-технической и(или) конструкторской документации
1.4. Опасное состояние E.Hazardous state	Неработоспособное состояние системы, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции по обеспечению безопасности движения поездов, не соответствует требованиям нормативно-технической и(или) конструкторской документации
1.5. Защитный отказ E.Protective	Событие, заключающееся в нарушении работоспособного состояния системы при сохранении защитного состояния

Термин	Определение
failure	
I.6. Опасный отказ E.Hazardous failure	Событие, заключающееся в нарушении работоспособного и защитного состояний системы
I.7. Критерий опасного отказа E.Hazardous failure criterion	Признак или совокупность признаков опасного состояния системы, установленные в нормативно-технической и (или) конструкторской документации
I.8. Показатель безопасности E.Safety measure	Количественная характеристика свойства безопасности
I.9. Наработка до опасного отказа E.Operating time to hazardous failure	Наработка системы от начала ее эксплуатации до возникновения первого опасного отказа
I.IO. Наработка между опасными отказами E.Operating time between hazardous failures	Наработка системы от окончания восстановления ее работоспособного состояния из опасного состояния до возникновения следующего опасного отказа
I.II. Концепция безопасности E.Safety conception	Совокупность положений, в соответствии с которыми осуществляется построение системы, отвечающей требованиям безопасности

Термин	Определение
I.I2. Уровень безопасности E.Safety level	Совокупность требований к системе, определяемая предельными значениями показателей безопасности и удовлетворяющая определенным требованиям безопасности
I.I3. Безопасная система E.Safety system	Система, построенная в соответствии с определенной концепцией безопасности и удовлетворяющая заданному уровню безопасности
	2. ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ
2.I. Вероятность безопасной работы E.Safety function	Вероятность того, что в пределах заданной наработки опасный отказ системы не наступает
2.2. Вероятность опасного отказа E.Hazardous failure probability	Вероятность того, что в пределах заданной наработки опасный отказ наступит хотя бы один раз
2.3. Средняя наработка до опасного отказа E.Mean operating time to hazardous failure	Математическое ожидание наработки системы до первого опасного отказа
2.4 Средняя наработка на опасный отказ	Отношение суммарной наработки восстанавливаемой системы к математическому ожиданию числа опасных отказов в течение этой наработки

Термин	Определение
E.Mean operating time between hazardous failures	
2.5. Интенсивность опасных отказов E.Hazardous failure rate	Условная плотность вероятности возникновения опасного отказа невосстанавливаемой системы, определяемая для рассматриваемого момента времени при условии, что до этого момента отказ не возник
2.6. Параметр потока опасных отказов E.Hazardous failure intensity	Отношение математического ожидания числа опасных отказов восстанавливаемой системы за произвольно малую ее наработку к значению этой наработки
2.7. Коэффициент безопасности E.Safety factor	Вероятность того, что система окажется в работоспособном или защитном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается

3. НОРМИРОВАНИЕ БЕЗОПАСНОСТИ

3.I. Нормирование безопасности E.Safety specification	Установление в нормативно-технической и(или) конструкторской (проектной) документации количественных и качественных требований к безопасности
3.2. Нормируемый показатель безопасности	Показатель безопасности, значение которого регламентировано нормативно-технической и(или) конструкторской (проектной) докумен-

Термин	Определение
E.Specified safety measure	тацией на систему

4. ОБЕСПЕЧЕНИЕ, ОПРЕДЕЛЕНИЕ И КОНТРОЛЬ БЕЗОПАСНОСТИ

4.1. Программа обеспечения безопасности E.Safety support programm	Документ, устанавливающий комплекс взаимосвязанных организационно-технических требований и мероприятий, подлежащих проведению на всех стадиях жизненного цикла системы и направленных на обеспечение заданного уровня безопасности
4.2. Безотказность E.Reliability, failure-free operation	Свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки (по ГОСТ 27.000-89)
4.3. Отказоустойчивость E.Fault-tolerance	Свойство системы продолжать выполнение заданных функций при наличии отказов ее элементов за счёт резервных возможностей
4.4. Безопасное поведение при отказе E.Safety failure behavior	Переход системы в защитное необратимое состояние при появлении отказа
4.5. Гарантоспособность E.Dependability	Свойство системы, позволяющее обоснованно полагаться на выполнение функций, для которых она предназначена.
4.6. Деградация системы автоматики E.Degradation	Свойство системы при появлении отказов отключать неисправные резервные элементы структуры
4.7. Реконфигурация системы	Свойство системы изменять структуру путем отключения неисправных или включения ре-

Термин	Определение
автоматики E.Reconfiguration	зервных (восстановленных) элементов
4.8. Контроль безопасности E.Safety verification	Проверка соответствия системы заданным требованиям к безопасности
4.9. Расчетный метод определения безопасности E.Analytical safety assessment	Метод, основанный на вычислении показателей безопасности по справочным данным о надежности компонентов и комплектующих изделий ЖАТ, по используемым мерам резервирования и контроля, по данным о безопасности объектов-аналогов и другой информации, имеющейся к моменту оценки безопасности
4.10. Расчетно-экспериментальный метод определения безопасности E.Analytical-experimental safety assessment	Метод, при котором показатели безопасности всех или некоторых составных частей объекта определяют по результатам испытаний и(или) эксплуатации, а показатели безопасности системы в целом рассчитывают по математической модели
4.11. Экспериментальный метод определения безопасности E.Experimental safety assessment	Метод, основанный на статистической обработке данных, получаемых при имитационных испытаниях или эксплуатации системы

Примечание к терминам 4.9 - 4.11. Аналогично определяют соответствующие методы контроля безопасности

Термин	Определение
4.13. Сертификация безопасности E.Safety certification	Действия третьей стороны, направленные на определение степени соответствия параметров системы конкретному стандарту и(или) нормативному документу по безопасности
4.13. Сертификат безопасности E.Safety certificate	Документ, удостоверяющий, что должным образом идентифицированная система соответствует заданному на основании стандартов уровню безопасности
4.14. Испытание на безопасность E.Safety test	Испытания, проводимые с целью исследования безопасности системы **Примечание.** В отличие от испытаний на надежность по ГОСТ 27.002-89 при испытаниях на безопасность не проводятся определительные испытания, так как появление опасных отказов - событие редкое и для получения достоверных результатов требуется подвергнуть испытаниям большое число систем ЖАТ в течение длительного времени. Ускоренные испытания на безопасность проводятся, как правило, с помощью специализированных программно-аппаратных имитационных комплексов, позволяющих значительно сократить сроки испытаний при различных режимах и условиях эксплуатации

5. БЕЗОПАСНОСТЬ ДИСКРЕТНЫХ СИСТЕМ

5.1. Ответственный объект управления E.Responsible controlled device	Объект управления, технология работы которого не допускает ложного включения или выключения
5.2. Защитное состояние дискретной системы E.Protective state of digi-	Неработоспособное состояние системы, при котором не происходит опасного искажения алгоритма функционирования

Термин	Определение
tal system	
5.3. Опасное состояние дискретной системы E.Hazardous state of digital system	Неработоспособное состояние системы, при котором происходит опасное искажение алгоритма функционирования
5.4. Ответственная информация E.Responsible information	Информация, используемая в дискретной системе, искажение которой переводит систему в опасное состояние
5.5. Ответственная телемеханическая команда E.Responsible telemechanic command	Команда телеуправления или телесигнализации, несущая ответственную информацию
5.6. Безопасная система телемеханики E.Safety telemechanic system	Безопасная система, передающая ответственные телемеханические команды
5.7. Вид отказа дискретной системы E.Failure kind of digital system	Изменение логических сигналов 0→1 или 1→0 на выходе дискретной системы в результате отказа ее элементов

Термин	Определение
5.8. Элемент с несимметричными отказами E.Nonsymmetrical failure component	Элемент, у которого интенсивность отказов разного вида различается на порядок и более
5.9. Элемент с симметричными отказами E.Symmetrical failure component	Элемент, у которого интенсивность отказов разного вида имеет один порядок
5.IO. Безопасный элемент E.Safety component	Элемент с несимметричными отказами, у которого интенсивность возникновения менее вероятного вида отказов не более предельного значения при заданном уровне безопасности
5.II. Коэффициент асимметрии отказов E.Failure asymmetric factor	Отношение интенсивности опасных отказов к интенсивности защитных отказов дискретной системы
5.I2. Опасный входной набор E.Hazardous input set	Множество значения переменных на входах комбинационной схемы, при наличии которых отказ вида 0→I на его выходах приводит к опасному искажению алгоритма функционирования
5.I3. Функция опасного отказа E.Hazardous failure function	Функция алгебры логики, равная I на опасных входных наборах
5.I4. Опасный	Отказ, при котором функция, реализуемая

Термин	Определение
отказ в комбинационной схеме E.Hazardous failure in combinational scheme	неисправной комбинационной схемой, и функция опасного отказа равны I хотя бы на одном общем входном наборе
5.I5. Безопасная комбинационная схема E.Safety combinational scheme	Комбинационная схема, у которой с заданным уровнем безопасности отсутствуют опасные отказы
5.I6. Опасная входная последовательность E.Hazardous input sequence	Упорядоченное множество входных наборов, после поступления которых на вход автомата отказы вида 0→I на его выходах приводят к опасному искажению алгоритма функционирования
5.I7. Реализация входной последовательности E.Input sequence realization	Появление логического сигнала I на выходе автомата после поступления на его входы данной входной последовательности
5.I8. Опасное событие E.Hazardous event	Множество опасных входных последовательностей
5.I9. Опасный отказ	Отказ, при котором событие, реализуемое неисправным автоматом, и опасное событие со-

Термин	Определение
в автомате E.Hazardous failure in automaton	держат хотя бы одну общую входную последовательность
5.20. Ложный переход E.False transition	Переход автомата из одного состояния в другое под действием отказа
5.21. Опасный ложный переход E.Hazardous false transition	Ложный переход, в результате которого в автомате реализуется хотя бы одна опасная входная последовательность
5.22. Безопасный ложный переход E.Safety false transition	Ложный переход, в результате которого в автомате не реализуется ни одна опасная входная последовательность
5.23. Граф безопасных ложных переходов E.Safety false transition graph	Ориентированный граф, вершины которого суть состояния автомата, а дуги соединяют одну вершину с другой, если соответствующий ложный переход безопасен
5.24. Граф безопасных искажений E.Safety perversion graph	Ориентированный граф, определяющий множество допустимых ложных переходов в автом

Термин	Определение
5.25. Граф возможных ложных переходов E.Possible false transition graph	Ориентированный граф, определяющий множество возможных ложных переходов в схеме дискретного автомата
5.26. Безопасное кодирование автомата E.Automaton safety encoding	Кодирование состояний автомата, при котором граф возможных ложных переходов является суграфом графа безопасных искажений
5.27. Безопасный автомат E.Safety automaton	Автомат, у которого с заданным уровнем безопасности отсутствуют опасные отказы
5.28. Отказ программы E.Programm failure	Искажение символа программы, проявляющееся в процессе ее исполнения в вычислительной системе
5.29. Опасный отказ программы E.Hazardous programm failure	Отказ программы, переводящий систему в опасное состояние
5.30. Безопасная программа E.Safety programm	Программа, у которой с заданным уровнем безопасности отсутствуют опасные отказы

Алфавитный указатель терминов на русском языке

Термин	Номер термина
Наработка до опасного отказа	I.9
Наработка между опасными отказами	I.I0
Нормирование безопасности	3.I
Нормируемый показатель безопасности	3.2
Опасная входная последовательность	5.I6
Опасное событие	5.I8
Опасное состояние	I.4
Опасное состояние дискретной системы	5.3
Опасный входной набор	5.I2
Опасный ложный переход	5.2I
Опасный отказ	I.6
Опасный отказ в автомате	5.I9
Опасный отказ в комбинационной схеме	5.I4
Опасный отказ программы	5.29
Ответственная информация	5.4
Ответственный объект управления	5.I
Ответственная телемеханическая команда	5.5
Отказоустойчивость	4.3
Отказ программы	5.28
Параметр потока опасных отказов	2.6
Показатель безопасности	I.8
Программа обеспечения безопасности	4.I
Расчетный метод определения безопасности	4.9
Расчетно-экспериментальный метод определения безопасности	4.I0
Реализация входной последовательности	5.I7
Реконфигурация	4.7
Сертификат безопасности	4.I3
Сертификация безопасности	4.I2
Средняя наработка до опасного отказа	2.3
Средняя наработка на опасный отказ	2.4
Уровень безопасности	I.I2
Функция опасного отказа	5.I3

Алфавитный указатель терминов на английском языке

Термин	Номер термина
Hazardous programm failure	5.29
Hazardous state	I.4
Hazardous state of digital system	5.3
Input sequence realization	5.I7
Mean operating time between hazardous failures	2.4
Mean operating time to hazardous failure	2.3
Nonsymmetrical failure component	5.8
Operating time between hazardous failures	I.IO
Operating time to hazardous failure	I.9
Possible false transition graph	5.25
Programm failure	5.28
Protective failure	I.5
Protective state	I.3
Protective state of digital system	5.2
Reconfiguration	4.7
Reliability	I.I, 4.2
Responsible controlled device	5.I
Responsible information	5.4
Responsible telemechanic command	5.5
Railroad automatic system safety	I.2
Safety automaton	5.27
Safety certificate	4.I3
Safety certification	4.I2
Safety component	5.IO
Safety combinational scheme	5.I5
Safety conception	I.II
Safety factor	2.7
Safety false transition	5.22
Safety false transition graph	5.23
Safety fault behavior	4.4
Safety function	2.I
Safety level	I.I2

Термин	Номер термина
Safety measure	I.8
Safety perversion graph	5.24
Safety programm	5.30
Safety specification	3.I
Safety support programm	4.I
Safety system	I.I3
Safety telemechanic system	5.6
Safety test	4.I4
Safety verification	4.8
Specified safety measure	3.2
Symmetrical failure component	5.9

ПРИЛОЖЕНИЕ
Справочное

ПОЯСНЕНИЯ К НЕКОТОРЫМ ТЕРМИНАМ

К термину "Безопасность системы железнодорожной автоматики" (п. I.2)

Для систем железнодорожной автоматики безопасность выступает как одна из составляющих надежности совместно с безотказностью, долговечностью, ремонтопригодностью и сохраняемостью, которые определены в ГОСТ 27.002-89 (рис.I).

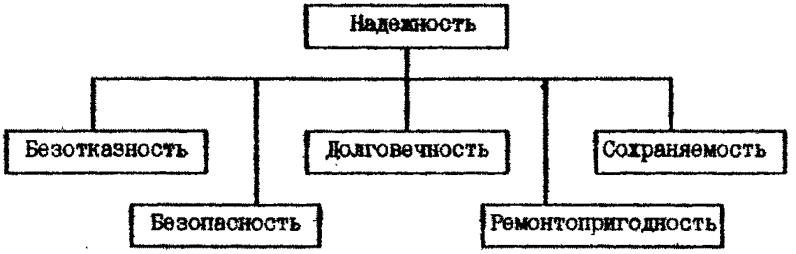

Рис.I. Составляющие надежности систем ж.-д. автоматики

Таким образом, в данном стандарте безопасность рассматривается как безопасность технических средств, т.е. свойство системы, связанное с ее поведением при отказах. Безопасность движения поездов является более широким понятием, поскольку она может быть нарушена и при исправном состоянии системы ЖАТ в результате неправильных действий человека-оператора, отказов других объектов ж.-д. комплекса, катастрофических природных явлений и по другим внешним по отношению к системе ЖАТ причинам.

К терминам "Защитное состояние" и "Опасное состояние" (пп. I.3 и I.4)

В опасное состояние система может перейти в результате возникновения внезапных, постепенных и перемежающихся отказов аппаратных и программных средств. При этом происходит нарушение работоспособного и защитного состояний, что может привести к возникновению угрозы для жизни и здоровья людей, сохранности

грузов, а также для окружающей среды. Переход системы в опасное состояние не означает, однако, что при этом обязательно возникает какая-либо авария. Она может произойти в зависимости еще от двух условий: от существующей в данный момент поездной ситуации и от действий человека-оператора.

На рис.2 показана диаграмма состояний систем железнодорожной автоматики и телемеханики. Все множество состояний S разбивается на подмножества исправных $S_и$, работоспособных $S_р$, неработоспособных защитных $S_з$ и неработоспособных опасных $S_о$ состояний.

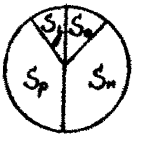

Рис.2. Диаграмма состояний систем ж.-д. автоматики

Безотказность систем характеризуется множеством состояний

$$S_н = S_и \cup S_р,$$

безопасность - множеством состояний

$$S_б = S_и \cup S_р \cup S_з.$$

Из сравнения множеств $S_н$ и $S_б$ следует, что в общем случае имеет место неравенство:

БЕЗОПАСНОСТЬ > БЕЗОТКАЗНОСТЬ.

В частном случае, когда $S_о = S_з$, имеем:

БЕЗОПАСНОСТЬ = БЕЗОТКАЗНОСТЬ.

К терминам "Защитный отказ" и "Опасный отказ" (пп. I.5 и I.6)

Разделение отказов на опасные и защитные устанавливает определенное неравноправие отказов. Это дает возможность при построении системы сконцентрировать внимание прежде всего на защите от опасных отказов, что в целом способствует повышению уровня безопасности и уменьшению объема избыточной аппаратуры. На рис.3 приведена схема основных состояний и событий в системе железнодорожной автоматики.

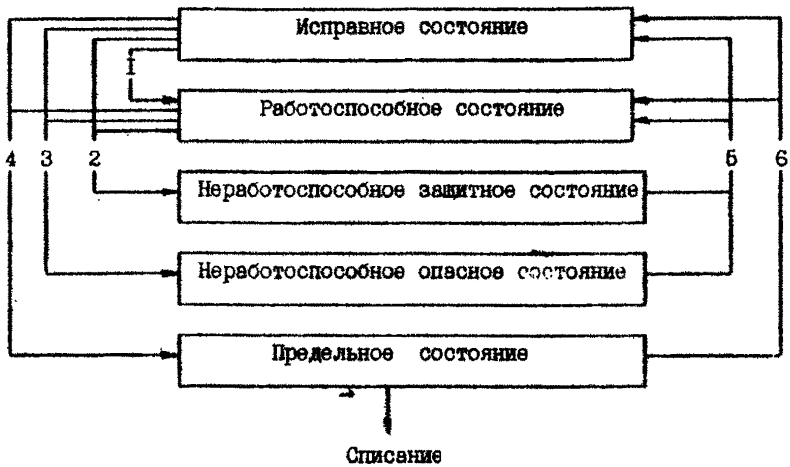

Рис.3. Схема основных состояний и событий:
I - повреждение; 2 - защитный отказ; 3 - опасный отказ; 4 - переход системы в предельное состояние из-за неустранимого нарушения требований безопасности, снижения эффективности эксплуатации, морального старения и других факторов; 5 - восстановление; 6 - ремонт

К термину " Критерий опасного отказа " (п. I.7)

Данный критерий должен устанавливаться для конкретной системы железнодорожной автоматики и ее элементов (реле, рельсовых цепей, стрелочных электроприводов и др.). Например, для электромагнитного реле железнодорожной автоматики в качестве критерия опасного отказа может служить следующий признак: замыкание замыкающего контакта при отсутствии тока в обмотке реле; для микроэлектронной системы автоматики, выполненной с использованием структурного резервирования $2 \wedge 2$ или $2 \vee 3$, в качестве критерия опасного отказа может выступать следующий признак: появление независимых отказов в двух резервированных элементах структуры, не обнаруженных средствами встроенного или внешнего контроля.

К термину "Показатель безопасности" (п. 1.8)

По своим свойствам показатель безопасности относится к показателю надежности, определенному ГОСТ 27.002-89. В соответствии с последним, при рассмотрении показателя безопасности следует различать наименование показателя, его численное значение, формулировку сущности показателя и его размерность.

К показателям безопасности относят количественные характеристики, которые могут иметь две формы представления: вероятностную и статистическую. Так как объекты железнодорожной автоматики и телемеханики, как правило, являются уникальными, то применение методов статистической теории надежности ограничено. Это ограничение связано также с высокими требованиями к количественным значениям показателей безопасности, которым должны отвечать СЖАТ. Статистическая оценка показателей безопасности таких систем возможна на стадии экспериментальной отработки и испытаний методами имитационного моделирования. На стадии проектирования и конструирования показатели безопасности трактуют как характеристики вероятностных математических моделей создаваемых систем.

Показатели безопасности вводят по отношению к определенным режимам и условиям эксплуатации, установленным в нормативно-технической и(или) конструкторской документации.

К термину "Концепция безопасности" (п. 1.11)

Концепция безопасности имеет фундаментальное значение, поскольку на ее основе устанавливается критерий опасного отказа системы. Концепция безопасности зависит в основном от свойств элементной базы, используемой для построения системы. В качестве примера сформулируем одну из распространенных концепций для безопасных микроэлектронных систем: одиночные дефекты аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться с заданной вероятностью на рабочих или тестовых воздействиях не позднее, чем в системе возникнет второй дефект.

К терминам "Вероятность безопасной работы" и "Вероятность опасного отказа" (пп. 2.I и 2.2)

Величина вероятности безопасной работы рассчитывается для заданной наработки - интервала времени t. При этом предполагается, что в начальный момент времени система находится в исправном или работоспособном состоянии (в множестве $S_и = S_и \cup S_р$), но не находится в защитном состоянии $S_з$.

Вероятность безопасной работы $P_б(t)$ за время t определяется по формуле

$$P_б(t) = I - F_{оп}(t) ,$$

где $F_{оп}(t)$ - функция распределения наработки до опасного отказа.

Вероятность опасного отказа определяется при тех же условиях по формуле

$$Q_{оп}(t) = F_{оп}(t) = I - P_б(t).$$

К термину "Средняя наработка до опасного отказа" (п. 2.3)

Величина средней наработки до опасного отказа определяется по формуле

$$T_{оп} = \int_0^\infty [I - F_{оп}(t)]\, dt.$$

К термину "Интенсивность опасных отказов" (п. 2.5)

Вероятностный смысл интенсивности опасных отказов $\lambda_{оп}(t)$ поясняется на рис.4. Пусть система проработала безотказно в течение времени t, т.е. не имела не только опасных, но и защитных отказов. Тогда

$$\lambda_{оп}(t) = \frac{dz(t)}{dt} ,$$

где dz(t) - условная вероятность опасного отказа системы за время dt, найденная в предположении, что она безотказно проработала за время (0,t).

Рис.4. К вероятностному смыслу $\lambda_{оп}(t)$

Если известна функция распределения $F_{оп}(t)$ и ее плотность распределения $f_{оп}(t)$, то интенсивность опасных отказов

определяют по формуле

$$\lambda_{оп}(t) = \frac{f_{оп}(t)}{P_{б}(t)} .$$

Статистически величину $\lambda_{оп}(t)$ определяют в результате испытаний по формуле (рис.5), 1/ч:

$$\lambda_{оп}(t) = \frac{n(\Delta t)}{N_{ср} \times \Delta t} ,$$

где $n(\Delta t)$ - число образцов системы, имевших опасный отказ за интервал времени Δt ; $N_{ср} = \frac{N_i + N_{i+1}}{2}$ - среднее число работоспособных образцов системы, не имевших опасных отказов в интервале Δt (при условии, что образцы системы, которые имели защитный отказ, немедленно заменялись новыми); N_i - число работоспособных образцов системы в момент времени $t - \frac{\Delta t}{2}$; N_{i+1} - число работоспособных образцов системы, не имевших опасных отказов к моменту времени $t + \frac{\Delta t}{2}$.

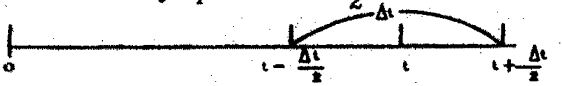

Рис.5. Схема расчета $\lambda_{оп}(t)$

К термину "Параметр потока опасных отказов" (п. 2.6)

Параметр потока опасных отказов $\omega_{оп}(t)$ характеризует безопасность восстанавливаемых систем. Статистически его определяют в результате испытаний по формуле (рис.6), 1/ч:

$$\omega_{оп}(t) = \frac{n(\Delta t)}{N_{о} \times \Delta t} ,$$

где $N_{о}$ - число образцов системы, поставленных на испытание в момент времени $t - \frac{\Delta t}{2}$; $n(\Delta t)$ - число образцов системы, имевших опасный отказ в интервале Δt при условии, что образцы системы, которые имели опасный или защитный отказы, немедленно заменялись новыми (таким образом, в течение всего интервала Δt работает $N_{о}$ образцов системы).

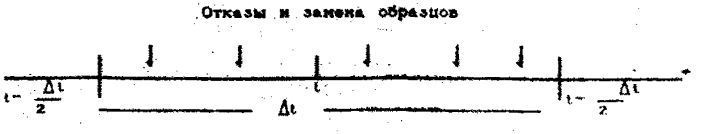

Рис.6. Схема расчета $\omega_{оп}(t)$

При экспоненциальном законе распределения времени безопасной работы

$$\omega_{оп}(t) = \lambda_{оп} = const .$$

К термину "Коэффициент безопасности" (п. 2.7)

Коэффициент безопасности является комплексным показателем безопасности системы,

$$K_б = \frac{T_{б\ ср}}{T_{б\ ср} + T_{в\ ср}} ,$$

где $T_{б\ ср}$ – средняя наработка на опасный отказ;

$T_{в\ ср}$ – среднее время восстановления.

К терминам "Нормирование безопасности" и "Нормируемый показатель безопасности" (пп. 3.1 и 3.2)

При выборе номенклатуры нормируемых показателей безопасности необходимо учитывать назначение системы, уровень безопасности, условия и режимы эксплуатации, характер возникновения опасных отказов (внезапные, перемежающиеся, постепенные и т.п.). При этом необходимо, чтобы общее число нормируемых показателей безопасности было минимально; нормируемые показатели имели простой физический смысл и допускали бы возможность расчетной оценки на этапе проектирования и подтверждения по результатам ускоренных испытаний.

Длительность ускоренных (как правило, имитационных) испытаний должна быть достаточной для выявления и устранения скрытых дефектов и определяться соглашением между потребителем (заказчиком) и поставщиком (изготовителем).

К терминам "Программа обеспечения безопасности", "Сертификация безопасности" и "Сертификат безопасности" (пп. 4.1, 4.12 и 4.13)

Программа обеспечения безопасности является документом, служащим организационно-технической основой для создания систем ЖАТ, удовлетворяющих заданному уровню безопасности. Программа обеспечения безопасности должна охватывать все стадии жизненного цикла системы ЖАТ. Она является составной частью программы

обеспечения надежности или самостоятельным документом.

Программа обеспечения безопасности определяет стратегию, методы и средства обеспечения безопасности, порядок проведения нормирования безопасности, необходимый объем и виды испытаний, методы расчетов показателей безопасности на различных стадиях жизни системы ЖАТ. Программа служит одним из оснований сертификации безопасности системы ЖАТ. На основе результатов выполнения программы устанавливается соответствие показателей безопасности системы ЖАТ заданному уровню.

К терминам "Безотказность", "Отказоустойчивость", "Безопасное поведение при отказе" (пп. 4.2, 4.3 и 4.4)

Для достижения требуемого уровня безопасности используются три стратегии: безотказность (система, которая не отказывает, – безопасна), отказоустойчивость и безопасное поведение при отказах.

Отказоустойчивость базируется на резервировании, остальные средства (диагностика, восстановление и реконфигурация) только повышают ее эффективность. Система обладает отказоустойчивостью, если можно выделить непустой набор элементов, неисправность которых не приведет к отказу.

Отказоустойчивость в зависимости от вида используемого резерва может быть функциональной, структурной (аппаратной и(или) программной), временной и информационной. Если в результате отказов система ЖАТ исчерпала свои резервные возможности для маскирования отказов, т.е. в результате деградации структура перестала быть отказоустойчивой, то при появлении еще одного отказа она должна перейти в необратимое защитное (отключенное от объектов управления) состояние. Автоматический выход из этого состояния должен быть маловероятен.

К терминам "Деградация системы автоматики" и "Реконфигурация системы автоматики" (пп. 4.6 и 4.7)

При деградации происходит уменьшение кратности резервирования и может изменяться вид резервирования. При реконфигурации производится изменение структуры отказоустойчивой системы при отключении неисправных элементов, при переключении на

резервные элементы и включении восстановленных элементов.

К разделу 5. "Безопасность дискретных систем"

В данном разделе определяются основные понятия, связанные с безопасностью дискретных систем, которые составляют большинство устройств железнодорожной автоматики. Приведенные далее термины должны использоваться при составлении нормативно-технической документации, в формулировках концепций безопасности, при доказательствах безопасности и разработке сертификатов на аппаратуру. Элементами дискретных систем являются комбинационные схемы, автоматы (с памятью) и программы. Относительно этих объектов и даются последующие определения.

К терминам "Защитное состояние дискретной системы" и "Опасное состояние дискретной системы" (пп. 5.2 и 5.3)

Для дискретных систем целесообразно ввести определения защитного и опасного состояний, которые будут частными случаями определений, данных в пп. I.3 и I.4. Это связано с тем, что функции, которые выполняет дискретная система, обычно формулируются как алгоритм ее функционирования. При этом используются формальные способы записи алгоритмов, такие как язык временных диаграмм, функции алгебры логики, язык граф-схем алгоритмов, логических схем алгоритмов, язык регулярных выражений и др. Поэтому далее вместо термина "функция" будет использоваться термин "алгоритм функционирования".

Под опасным искажением алгоритма функционирования понимается искажение, в результате которого происходит опасное воздействие на объект управления (неправильное включение разрешающего показания светофора, самопроизвольное включение стрелочного электродвигателя и т.п.).

Под защитным искажением алгоритма функционирования понимается искажение, в результате которого либо не происходит необходимого воздействия на объект, либо происходит защитное воздействие на объект управления (неправильное включение запрещающего показания светофора, невключение стрелочного электродвигателя и т.п.).

К терминам "Ответственная телемеханическая команда" и "Безопасная система телемеханики" (пп. 5.5 и 5.6)

Примерами ответственных команд телеуправления являются передачи по телемеханическому каналу на промежуточную станцию команд на открытие пригласительного сигнала и на аварийный перевод стрелки. Особенностью таких команд является то, что технологические условия безопасности при их выполнении уже не проверяются на контрольном пункте, а должны полностью обеспечиваться на пункте управления. Если в системе телемеханики передаются подобные команды, то такая система должна быть безопасной.

К терминам "Элемент с несимметричными отказами" и "Коэффициент асимметрии отказов" (пп. 5.8 и 5.11)

У элемента с несимметричными отказами имеют различную вероятность возникновения отказы типов 0→1 и 1→0. Это следует либо из самой физической природы и принципа действия элемента, либо достигается специальными мерами. Например, элемент, у которого отказ типа 1→0 имеет интенсивность отказов 10^{-6} 1/ч, а отказ типа 0→1 - интенсивность 10^{-7} 1/ч, является элементом с коэффициентом асимметрии отказов, раьным 10.

К терминам "Опасный входной набор" и "Функция опасного отказа" (пп. 5.12 и 5.13)

Работа комбинационной схемы описывается функцией алгебры логики f. Областью определения функции f является множество двоичных наборов, которое разбивается на два подмножества: подмножество разрешенных наборов (f = 1) и подмножество запрещенных наборов (f = 0). На выходе комбинационной схемы из-за отказов возможны трансформации сигналов двух видов: 0→1 и 1→0. Пусть, как это обычно считается, к опасному искажению алгоритма функционирования приводит ошибка 0→1. Тогда опасным является запрещенный набор, на котором происходит трансформация сигнала 0→1. Функция опасного отказа $f_{оп}$ определяет условия возникновения всех опасных искажений алгоритма функционирования.

К термину "Опасный отказ в комбинационной схеме" (п. 5.I4)

Неисправная комбинационная схема реализует некоторую ошибочную функцию f'. Для опасного отказа выполняется условие

$$f'f_{оп} \neq 0 .$$

К термину "Безопасная комбинационная схема" (п. 5.I5)

У безопасной комбинационной схемы для всех отказов, вероятность возникновения которых необходимо учитывать исходя из заданного уровня безопасности, выполняется условие

$$f'f_{оп} = 0.$$

Термины пп. 5.I2 - 5.I5 используются для доказательства отсутствия опасных отказов в комбинационной схеме.

К терминам "Опасная входная последовательность", "Реализация входной последовательности" и "Опасное событие" (пп. 5.I6, 5.I7 и 5.I8)

Дискретный автомат с памятью функционирует в дискретном времени. Поэтому опасные ситуации в алгоритме его работы связаны с последовательностями входных наборов, которые сменяют друг друга во времени. Такие последовательности определяют предысторию автомата к данному моменту времени и реализуются путем появления на выходе логического сигнала I и активного воздействия на ответственный объект управления. Опасная входная последовательность задает опасное искажение алгоритма, а опасное событие - множество всех опасных искажений.

К термину "Опасный отказ в автомате" (п. 5.I9)

Алгоритм работы автомата задается в той или иной форме указанием множества входных слов (события E), которые реализуются в автомате. Неисправный автомат реализует некоторое ошибочное событие E'. Для опасного отказа выполняется условие

$$E' \cap E_{оп} \neq 0 ,$$

где $E_{оп}$ - опасное событие.

К терминам "Ложный переход", "Опасный ложный переход" и "Безопасный ложный переход" (пп. 5.20, 5.2I и 5.22)

Ложный переход $S_i \rightarrow S_f$ из состояния S_i в состояние S_f

является автоматной моделью отказа логической сети схемы с памятью. Эта модель отражает искажение функции переходов, которая задает алгоритм функционирования автомата. На рис.7 приведен граф переходов релейной электрической централизации, смысл состояний S которой приведен в табл.I. В таблице применены обозначения С, З, IМ и 2М соответственно для сигнального, замыкающего, первого маршрутного и второго маршрутного реле.

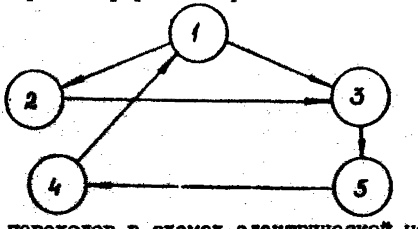

Рис.7. Граф переходов в схемах электрической централизации

Пусть, например, при открытии сигнала в результате отказа вместо предварительного замыкания ложно происходит окончательное замыкание маршрута. Тогда возникает ложный переход 2 → 3. Опасный ложный переход отражает опасное искажение алгоритма функционирования. Так, ложный переход 2 → 3 в схемах электрической централизации является безопасным, а ложный переход 3 → 2 - опасным.

Таблица I

S	Состояние реле				Смысл состояний
	С	З	IМ	2М	
I	0	I	I	I	Сигнал закрыт, замыкание отсутствует
2	I	0	I	I	Сигнал открыт, предварительное замыкание
3	I	0	0	0	Сигнал открыт, окончательное замыкание
4	0	0	I	0	Сигнал закрыт, поезд вступил на маршрут
5	0	0	0	0	Сигнал закрыт, окончательное замыкание

К терминам "Граф безопасных ложных переходов" и "Граф безопасных искажений" (пп. 5.23 и 5.24)

Все безопасные ложные переходы автомата задаются с помощью графа безопасных ложных переходов. На рис.8 изображен этот граф для электрической централизации. При структурном синтезе автомата с требуемой вероятностью должны быть исключены все опасные ложные переходы и некоторое множество безопасных ложных переходов. Это связано с тем, что несколько безопасных ложных переходов в совокупности могут вызвать опасное искажение алгоритма функционирования. По этой причине граф безопасных искажений является суграфом графа безопасных ложных переходов, т.е. множество дуг первого является подмножеством множества дуг второго. Для электрической централизации граф безопасных искажений совпадает с графом безопасных ложных переходов (рис.8).

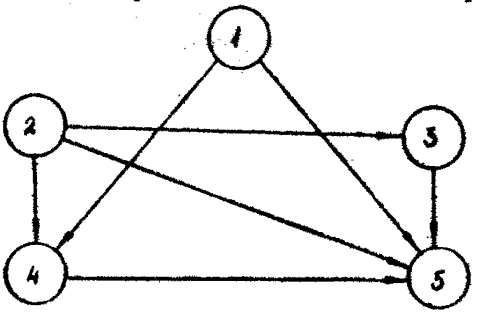

Рис.8. Граф безопасных ложных переходов электрической централизации

К терминам "Граф возможных ложных переходов" и "Безопасное кодирование автомата" (пп. 5.25 и 5.26)

При построении схемы автомата на безопасных элементах вероятность возникновения некоторых ложных переходов оказывается настолько малой, что ею можно пренебречь. Например, если в схемах электрической централизации считать отказ реле типа 0 → 1 маловероятным событием, то при кодировании состояний, указанном в табл.1, можно считать невозможными ложные переходы 5 → 4, 4 → 3 и др. Все возможные ложные переходы в реальной схеме задаются

графом возможных ложных переходов. Последний для электрической централизации совпадает с графом на рис.8 Таким образом, кодирование состояний в табл.I является безопасным, поскольку допускает существование только безопасных ложных переходов, включенных в граф безопасных искажений.

Термины пп. 5.25 и 5.26 используются для доказательства отсутствия опасных отказов в автоматах.

К термину "Отказ программы" (п. 5.28)

Отказ программы возникает либо из-за ошибки, допущенной программистом при ее написании, либо в результате воздействия "компьютерного вируса" или отказа аппаратных средств. Во всех случаях моделью отказа является искажение символов программы. Например, в программе, записанной на языке Ассемблер, возможно искажение символов: ANA → ORA. Первой причиной этого может явиться ошибка программиста, который вместо символа ANA напишет символ ORA. Второй причиной может быть искажение объектных кодов этих команд в результате сбоев или отказов в аппаратуре в процессе вычисления. В восьмиразрядном микропроцессоре код команды ANA (IOIOOOOO) и код команды ORA (IOIIOOOO) отличаются только в одном разряде, искажение которого приведет к тому, что вместо операции логического умножения микропроцессор выполнит операцию логического сложения.

К термину "Опасный отказ программы" (п. 5.29)

Понятие опасного отказа конкретизируется для программ определенного класса. Например, если управляющая программа вычисляет некоторую функцию алгебры логики f, а отказавшая программа f', то отказ опасен при $f'f_{оп} \neq 0$.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Надежность и эффективность в технике: Справочник /Ред. совет: В.С.Авдуевский (пред.) и др.

Т.I: Методология. Организация. Терминология/
Под ред. Рембезы. - М.: Машиностроение, I989. - 224 с.

2. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. - М.: Изд. стандартов, I989 - 37 с.

3. Сапожников В. В., Сапожников Вл. В. О синтезе конечных автоматов с исключением опасных отказов //Автоматика и телемеханика.- I972.- N 8. -С. 93-99.

4. Переборов А. С., Трохов В. Г., Василенко М. Н. Определение основных показателей надежности систем железнодорожной автоматики и телемеханики//Автоматическое управление на железнодорожном транспорте: Сб. науч. тр.- Л.: ЛИИЖТ, I977.- С. 47-56.

5. Христов Х. А. Електронизация на осигурителната техника.- София: Техника, I984. - 355 с.

6. Лисенков В. М. Теория автоматических систем интервального регулирования. - М.: Транспорт, I987. - I50 с.

7. Сапожников В. В., Кравцов Ю. А., Сапожников Вл. В. Дискретные устройства железнодорожной автоматики и телемеханики. - М.: Транспорт, I988.- 255 с.

8. Руденко Ю., Ушаков И. О безопасности как одном из свойств надежности систем энергетики//Известия АН СССР. Сер. Энергетика и транспорт.- I985.- N 2.- С.5-II.

9. Справочник по безопасности космических полетов/Г.Т. Береговой, В.И. Ярополов, И.И. Баранецкий и др. - М.: Машиностроение, I989.- 336 с.

ИНФОРМАЦИОННЫЕ ДАННЫЕ

1. РАЗРАБОТАН И ВНЕСЕН Управлением сигнализации, связи и вычислительной техники МПС и Петербургским институтом инженеров железнодорожного транспорта.

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**, **Д. С. Марков**, канд. техн. наук, **М. А. Новиков**, **В. А. Гладков**, канд. техн. наук, **Е. В. Самонина**, **Д. М. Котельников**.

2. УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Указанием МПС РФ от 22 июля 1992 г. № Г-640у.

3. СРОК ПРОВЕРКИ 1997 г.

4. ВВЕДЕН ВПЕРВЫЕ.

5. ССЫЛОЧНЫЕ НОРМАТИВНО-ТЕХНИЧЕСКИЕ ДОКУМЕНТЫ.

Обозначение НТД, на который дана ссылка	Номер пункта
ГОСТ 27.002—89	1.1 4.2 4.4

ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Основные понятия. Термины и определения

Редакторы А.И. Жук, Н.В. Фролова

Подписано в печать с оригинала-макета 27.10.92

Формат 60 х 84 1/16. Бумага для множ. апп. Печать офсетная.

Усл.печ.л. 2,25 Уч.-изд.л. 2,25 Тираж 1000.

Заказ 1051

Петербургский институт инженеров железнодорожного транспорта. 190031, СПб, Московский пр.,9.

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