Российские железные дороги

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»
(ОАО «РЖД»)

РАСПОРЯЖЕНИЕ

«02» марта 2010г. Москва № 416р

Об изменении порядкового номера стандарта ОАО «РЖД» «Системы и устройства железнодорожной автоматики и телемеханики. Выбор и общие правила задания требований по безопасности»

Во изменение распоряжения ОАО «РЖД» от 04 декабря 2009 г. № 2472р присвоить стандарту СТО РЖД 1.19.008-2009 «Системы и устройства железнодорожной автоматики и телемеханики. Выбор и общие правила задания требований по безопасности» новый порядковый номер - СТО РЖД 1.19.010-2009.

Вице-президент
ОАО «РЖД» В.Б. Воробьев

Открытое акционерное общество «Российские железные дороги» Департамент управления делами Отдел документационного обеспечения №5 ОАО «РЖД»

Исп. Кудрявцев Виктор Вадимович, ЦШ
2-77-59

gost.e-ecolog.ru

Российские железные дороги

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»
(ОАО «РЖД»)

РАСПОРЯЖЕНИЕ

04 декабря 2009г. Москва № 2472р

Об утверждении стандарта ОАО «РЖД»
«Системы и устройства железнодорожной автоматики и телемеханики. Выбор и общие правила задания требований по безопасности»

В целях повышения безопасности, определения понятия и назначения процесса доказательства безопасности, установления состава, порядка и общих правил задания требований по безопасности для включения их в нормативную документацию систем автоматики и телемеханики:

1. Утвердить и ввести в действие с 1 января 2010 г. стандарт СТО РЖД 1.19.008-2009 «Системы и устройства железнодорожной автоматики и телемеханики. Выбор и общие правила задания требований по безопасности».

2. Начальнику Департамента автоматики и телемеханики Кайнову В.М. обеспечить выполнение требований настоящего стандарта при утверждении технических заданий на разработку и приемке систем автоматики и телемеханики.

3. Начальникам железных дорог – филиалов ОАО «РЖД» организовать изучение требований настоящего стандарта работниками причастных структурных подразделений.

4. Начальнику Департамента автоматики и телемеханики Кайнову В.М. подготовить в установленном порядке обращение в Министерство транспорта Российской Федерации с предложением о необходимости отмены ОСТ 32.18-92 «Безопасность железнодорожной автоматики и телемеханики. Выбор и общие правила нормирования показателей безопасности».

Вице-президент
ОАО «РЖД» В.Б. Воробьев



Исп. Кудрявцев Виктор Вадимович, ЦШ
2-77-59

Российские железные дороги

Стандарт ОАО «РЖД»

СТО РЖД 1.19.010— 2009

СИСТЕМЫ И УСТРОЙСТВА ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Выбор и общие правила задания требований по безопасности

Москва
2009

Предисловие

1 РАЗРАБОТАН Государственным образовательным учреждением высшего профессионального образования «Петербургский государственный университет путей сообщения» (ПГУПС)

2 ВНЕСЕН Департаментом автоматики и телемеханики ОАО «РЖД»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ распоряжением ОАО «РЖД» от 02 марта 2010 г. № 416р

4 ВВЕДЕН ВПЕРВЫЕ

Учетный регистрационный номер _____

© «РЖД», 2009

Воспроизведение и/или распространение настоящего стандарта, а также его применение сторонними организациями осуществляется в порядке, установленном ОАО «РЖД»

Содержание

1 Область применения 1
2 Нормативная ссылка 1
3 Основные положения 2
4 Порядок задания требований безопасности на различных стадиях жизненного цикла изделий железнодорожной автоматики и телемеханики 5
5 Выбор номенклатуры задаваемых требований безопасности 6
6 Выбор и обоснование значений показателей безопасности 7
Приложение А (справочное) Примеры определения количественных показателей безопасности . 11
Приложение Б (рекомендуемое) Примеры построения и изложения разделов «Требования по безопасности» в ТЗ, ТУ изделий ЖАТ 12
Приложение В (справочное) Примеры возможных модификаций и определений стандартизованных показателей 14
Приложение Г (рекомендуемое) Примеры критериев опасных отказов 15
Приложение Д (рекомендуемое) Примеры расчета нормированных значений показателей безопасности 17
Библиография 20

Стандарт ОАО «РЖД»

СИСТЕМЫ И УСТРОЙСТВА ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Выбор и общие правила задания требований по безопасности

Дата введения - 02 марта 2010г.

1 Область применения

Настоящий стандарт распространяется на все виды систем и устройств (в дальнейшем - изделий) железнодорожной автоматики и телемеханики (ЖАТ), к которым предъявляются требования безопасности, и устанавливает состав, порядок и общие правила задания требований по безопасности для включения их в нормативную (НД) документацию.

Требования настоящего стандарта могут быть конкретизированы в нормативной документации по видам систем и устройств железнодорожной автоматики и телемеханики.

Настоящий стандарт предназначен для применения подразделениями аппарата управления ОАО «РЖД», филиалами ОАО «РЖД» и иными структурными подразделениями ОАО «РЖД».

Помимо настоящего стандарта следует руководствоваться нормативными документами федеральных органов исполнительной власти, в том числе, государственными стандартами, другими нормами и правилами, которые регулируют вопросы систем и устройств ЖАТ.

Применение настоящего стандарта сторонними организациями оговаривается в договорах (соглашениях) с ОАО «РЖД».

2 Нормативная ссылка

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ 27.003-90 Надежность в технике. Состав и общие правила задания требований по надежности.

3 Основные положения

3.1 Стандартом определяются количественные и качественные требования к системам и устройствам железнодорожной автоматики и телемеханики, реализация которых должна обеспечивать необходимый уровень безопасности, и устанавливается выбор и общие правила задания требований безопасности.

Примечание – Примеры задания количественных показателей безопасности приведены в приложении А.

3.2 Требования безопасности должны быть включены:
- в технические задания (ТЗ) на разработку или модернизацию изделий ЖАТ;
- в технические условия (ТУ) на изготовление опытной и серийной продукции;
- в стандарты общих технических условий (ОТУ);
- программу обеспечения безопасности;
- документ «Доказательство безопасности».

Примечание – Примеры построения и изложения разделов «Требования по безопасности» в ТЗ, ТУ изделий ЖАТ приведены в приложении Б.

3.3 При задании требований безопасности определяют (обосновывают) и согласовывают между заказчиком (потребителем) и разработчиком (изготовителем) изделия ЖАТ:
- типовую модель (модели) эксплуатации, применительно к которой (которым) устанавливают требования безопасности;
- критерии опасных отказов;
- перечень и значения показателей безопасности (ПБ);
- методы контроля соответствия изделий ЖАТ заданным требованиям безопасности;
- требования и (или) ограничения по конструкционным, производственным и эксплуатационным способам обеспечения безопасности (при необходимости - с учетом экономических ограничений);
- программу обеспечения безопасности.

3.4 Типовая модель эксплуатации изделия ЖАТ определяется по ГОСТ 27.003 (п. 1.3) и дополнительно с учетом специфики изделий ЖАТ должна быть дополнена проведением периодического контроля, подтверждающего безопасность в процессе эксплуатации.

3.5 Требования безопасности изделий ЖАТ подразделяют на количественные и качественные.

3.5.1 Номенклатура задаваемых ПБ выбирается в соответствии с положениями настоящего стандарта и согласовывается в установленном порядке между заказчиком (потребителем) и разработчиком (изготовителем). Показатели должны выбираться из числа тех, которые определены в настоящем стандарте и приведены в таблице 1. Допускается применять показатели, термины и определения которых кон-

кретизируют соответствующие термины, установленные отраслевым стандартом [1], с учетом особенностей изделия ЖАТ и (или) специфики его применения, но не противоречащие стандартизированным терминам.

Примечание – Примеры возможных модификаций стандартизированных показателей приведены в приложении В.

Таблица 1

Номенклатура показателей безопасности

Наименование показателя	Обозначение
Вероятность безопасной работы	$P_б(t)$
Вероятность опасного отказа	$Q_{оп}(t)$
Средняя наработка до опасного отказа	$T_{оп}$
Средняя наработка на опасный отказ	$T_{б\,ср}$
Интенсивность опасных отказов	$\lambda_{оп}(t)$
Параметр потока опасных отказов	$\omega_{оп}(t)$
Коэффициент безопасности	$K_б$
Примечание – Примеры численных значений показателей безопасности приведены в [2].	

3.5.2 Качественные требования регламентируют конструкционные, производственные и эксплуатационные способы обеспечения безопасности изделий ЖАТ.

3.5.2.1 Конструкционные способы обеспечения безопасности предъявляют требования:

- к способам и кратности резервирования;
- к способам снижения интенсивности опасных отказов составных частей и комплектующих изделий;
- к ограничению номенклатуры комплектующих изделий и материалов;
- к аппаратуре индикации и фиксации отказов, тестового и функционального контроля.

3.5.2.2 Производственные способы обеспечения безопасности предъявляют требования:

- к стабильности технологических процессов, к свойствам сырья, материалов, к комплектующим изделиям;
- к способам и средствам контроля уровня безопасности в ходе производства;
- к способам и продолжительности технологического прогона изделий;
- к периодичности, объемам и методам испытаний на безопасность серийно изготавливаемых или разрабатываемых опытных изделий ЖАТ.

3.5.2.3 Эксплуатационные способы обеспечения безопасности ЖАТ предъявляют требования:

- к системе технического обслуживания (ТО) и ремонта в части числа видов, периодичности, объемов ТО и плановых ремонтов;
- к средствам материально-технического оснащения ТО и ремонтов;
- к системе учета, сбора, обработки и представления информации о безопасно-

сти ЖАТ, если контроль нормируемых показателей осуществляется в условиях эксплуатации;

- к способам устранения отказов и повреждений, к правилам регулировок;
- к численности и квалификации обслуживающего персонала;
- к порядку действий оперативного персонала при опасных и защитных отказах системы, и т.п.

3.6 Критерии опасных отказов устанавливают при задании требований безопасности с целью однозначного определения опасного состояния изделий ЖАТ при разработке, испытаниях, эксплуатации и ремонте.

Критерии опасных отказов устанавливают по одному или по совокупности отличительных признаков опасного состояния.

Определения критериев опасных отказов должны быть четкими, конкретными, не допускающими неоднозначного толкования.

3.6.1 При определении критериев опасных отказов следует учитывать:

- вид, назначение и структуру изделий ЖАТ;
- требования безопасности, предъявляемые к изделиям ЖАТ;
- концепцию безопасности, принятую при разработке изделия ЖАТ;
- последствия опасных отказов изделий ЖАТ;
- возможные отказы, сбои и ошибки программ, присутствующие в программном обеспечении системы.

3.6.2 Для аналоговых и части дискретных изделий ЖАТ формальным критерием опасного отказа является выход значений показателей качества функционирования, влияющих на безопасность, за пределы установленных норм (см. приложение Г).

3.6.3 Формальным критерием опасного отказа дискретного изделия ЖАТ следует считать выполнение условий, изложенных в приложении Г.

3.6.4 Признаками опасных отказов изделий ЖАТ являются:

- нарушение положений концепции безопасности, в соответствии с которой построено изделие ЖАТ;
- отклонение хотя бы одного показателя безопасности изделия ЖАТ за пределы установленных норм;
- выход показателей качества функционирования, влияющих на безопасность изделия ЖАТ, за пределы установленных норм в результате его перехода в предельное состояние;
- выработка изделием ЖАТ ложных контрольных и управляющих сигналов, переводящих его в опасное состояние.

Примечание – Примеры критериев опасных отказов приведены в приложении Г.

3.6.5 Для изделий ЖАТ, построенных на элементах с симметричными отказами, признаками опасных отказов являются, кроме вышеуказанных, следующие:

- искажение ответственной информации, переводящее изделие ЖАТ в опасное состояние;

- возникновение в течение периода диагностирования такого количества эквивалентных отказов, которое больше или равно кратности резервирования;
- возникновение и накопление необнаруживаемых отказов хотя бы в одном резервированном канале изделия ЖАТ.

3.7 Под методами контроля безопасности изделия ЖАТ понимается проверка его характеристик на соответствие качественным и количественным требованиям по безопасности. Виды контроля можно разделить:

- по объему контролируемых изделий: сплошной и выборочный (статистический);
- по стадии производственного процесса: входной, текущий, выходной;
- по используемым методам и средствам: экспертный, расчетный, экспериментальный и расчетно-экспериментальный;
- по времени проведения: циклический (периодический), одноразовый, плановый, внеплановый (инспекционный).

3.8 Для выполнения и подтверждения выполнения заданных требований безопасности изделий ЖАТ разрабатывается программа обеспечения безопасности (ПОБ), которая является организационно-техническим документом, определяющим перечень работ и мероприятий, проводимых на всех стадиях создания и эксплуатации систем ЖАТ. Результатом выполнения ПОБ является документ «Доказательство безопасности».

4 Порядок задания требований безопасности на различных стадиях жизненного цикла изделий железнодорожной автоматики и телемеханики

4.1 Требования безопасности, включаемые в ТЗ, первоначально определяют на стадии исследования и обоснования разработки путем выполнения следующих работ:

- анализа требований заказчика (потребителя), назначения и условий эксплуатации изделия (или его аналогов), ограничений по всем видам затрат, в том числе по конструктивному исполнению, технологии изготовления и стоимости эксплуатации;
- выработки и согласования с заказчиком (потребителем) критериев опасных отказов;
- выбора рациональной номенклатуры задаваемых ПБ;
- установления значений (норм) ПБ изделий ЖАТ и их составных частей.

4.2 На стадии разработки изделия по согласованию между заказчиком (потребителем) и разработчиком допускается уточнять (корректировать) требования безопасности при соответствующем технико-экономическом обосновании путем:

- рассмотрения возможных вариантов построения изделия и расчета для каждого из них ожидаемого уровня безопасности, а также показателей, характеризующих виды затрат, включая эксплуатационные, и возможности выполнения других заданных ограничений;
- уточнений значений ПБ изделия и его составных частей.

4.3 При формировании ТУ на серийные изделия в него включают, как правило, те требования к ПБ из заданных в ТЗ, которые предполагается контролировать на этапе изготовления изделия ЖАТ (например, для микроэлектронных систем качественными требованиями могут быть независимость отказов в резервированных элементах структуры, исключение возможности накопления отказов, контроль правильности функционирования ПО).

4.4 На стадиях серийного производства и эксплуатации допускается по согласованию между заказчиком и разработчиком (изготовителем) корректировать значения отдельных ПБ по результатам испытаний или подконтрольной эксплуатации.

4.5 Для сложных изделий ЖАТ при их разработке, опытном и серийном производстве допускается по согласованию между заказчиком и разработчиком поэтапное задание значений ПБ с учетом накопленных статистических данных по предшествующим изделиям-аналогам.

5 Выбор номенклатуры задаваемых требований безопасности

5.1 Выбор номенклатуры ПБ осуществляется на основе классификации изделий ЖАТ по признакам, характеризующим их назначение, особенности режимов эксплуатации и др.

5.2 Определение классификационных признаков изделий ЖАТ осуществляют путем анализа ТЗ на разработку изделия в части характеристик его назначения, условий эксплуатации и данных о безопасности изделий-аналогов.

5.3 Основными признаками, по которым классифицируют изделия ЖАТ по безопасности, являются:

- определенность назначения изделия;
- режим функционирования;
- возможные последствия отказов;
- возможность восстановления работоспособного состояния после защитного отказа;
- возможность и способ восстановления технического ресурса;
- характер основных процессов, определявших переход изделия в предельное состояние;
- возможность и необходимость технического обслуживания;
- возможность и необходимость контроля перед применением;
- наличие в составе изделия микроэлектронных схем и средств вычислительной техники.

По этим признакам изделия ЖАТ классифицируются следующим образом.

5.3.1 По определенности назначения:

- объекты конкретного назначения, имеющие один основной вариант применения по назначению;
- объекты общего назначения, имеющие несколько вариантов применения.

5.3.2 По режимам функционирования:

- изделия непрерывного длительного применения;

- изделия многократного циклического применения.

5.3.3 По последствиям отказов:

- изделия, отказы которых приводят к снижению эффективности функционирования или уменьшения порога резервирования;
- изделия, отказы которых могут привести к последствиям катастрофического характера (к угрозе для жизни и здоровья людей, значительным экологическим и экономическим потерям).

5.3.4 По возможности восстановления работоспособного состояния после опасного отказа в процессе эксплуатации:

- восстанавливаемые;
- невосстанавливаемые.

5.3.5 По характеру основных процессов, определяющих переход в опасное и предельное состояния.

- стареющие;
- изнашиваемые;
- стареющие и изнашиваемые одновременно.

5.3.6 По возможности и способу восстановления технического ресурса путем проведения плановых ремонтов:

- ремонтируемые;
- неремонтируемые.

5.3.7 По возможности технического обслуживания в процессе эксплуатации:

- обслуживаемые;
- необслуживаемые.

5.3.8 По возможности (необходимости) проведения контроля:

- контролируемые перед применением;
- непрерывно кочтролируемые при применении;
- периодически контролируемые в процессе функционирования;
- периодически контролируемые с отключением от технологического процесса;
- неконтролируемые,

5.3.9 Из-за сбоев и отказов в изделиях ЖАТ, содержащих в своем составе микроэлектронные элементы и средства вычислительной техники, такие изделия ЖАТ относят к объектам с опасными отказами. При отсутствии в составе изделий ЖАТ микроэлектронных элементов и средств вычислительной техники – к объектам без опасных отказов сбойного характера.

6 Выбор и обоснование значений показателей безопасности

6.1 Значения (нормы) ПБ изделий устанавливают в ТЗ, ТУ с учетом назначения, достигнутого уровня и выявленных тенденций повышения безопасности изделий ЖАТ, технико-экономического обоснования, возможностей изготовителей и заказчика.

6.2 Расчетные (оценочные) ПБ изделия ЖАТ и его составных частей, полученные после завершения очередного этапа (стадии) работ, принимают в качестве норм

безопасности, действующих на последующем этапе (стадии), после завершения которого эти нормы могут быть уточнены (откорректированы).

6.3 Расчет норм безопасности производится на основе концепции приемлемого риска. Частными случаями применения данной концепции являются:

а) расчет норм безопасности на основе достигнутого уровня безопасности. В этом случае норма безопасности считается приемлемой, если ее значение соответствует достигнутому уровню безопасности, признанному обществом или специалистами достаточным на данный момент;

б) расчет норм безопасности на основе соотношения между затратами на обеспечение безопасности и ее эффективностью. В этом случае должны быть известны перечень мероприятий по повышению (обеспечению) безопасности, значение прироста безопасности и затраты на его обеспечение, вид зависимости *эффективность – безопасность*;

в) расчет норм безопасности на основе концепции замещения рисков. В этом случае показатели безопасности вновь разрабатываемых изделий ЖАТ не должны быть ниже аналогичных показателей замещаемых изделий.

Примечание – Пример расчета норм безопасности приведен в приложении Д.

6.4 Для обоснования значений ПБ используют экспертные, расчетные, экспериментальные (статистические) или расчетно-экспериментальные методы.

6.4.1 Экспертные методы применяют в тех случаях, когда затруднительно использовать более объективные методы, например при разработке принципиально новых изделий ЖАТ, когда отсутствуют статистические данные, нет апробированных методик расчета ПБ, а также отсутствуют исходные данные и средства для определения ПБ экспериментальным методом.

Примечание – Пример расчета норм безопасности экспертным методом приведен в приложении Д.

6.4.2 Расчетные методы используют для изделий ЖАТ, по которым отсутствуют достоверные статистические данные, полученные в ходе испытаний (эксплуатации) аналогов (прототипов).

Примечание – Материалы по расчету норм безопасности расчетным методом приведены в приложении Д.

6.4.3 Экспериментальные методы применяют для изделий, по которым возможно получение статистических данных в процессе испытаний или имеющих аналоги (прототипы), позволяющие оценить их ПБ, а также тенденции изменения ПБ от одного аналога к другому. Такие оценки ПБ могут быть получены в результате сбора статистических данных об эксплуатации или при имитационном моделировании существующих аналогичных изделий ЖАТ.

Сущность экспериментальной оценки норм безопасности состоит в том, что на основании полученных при эксплуатации ограниченных по объему исходных статистических данных по разработанным методам определяют фактические значения норм безопасности с заданной точностью и достоверностью.

За норму безопасности может быть принято ее точечное и (или) интервальное (границы доверительного интервала, который с заданной вероятностью содержит истинное значение показателя) значение.

Исходными данными для расчета норм безопасности являются:

- число изделий;
- число отказов изделий;
- время наработки на отказ;
- время наблюдения.

Для оценки значений норм безопасности задаются следующими величинами:

- доверительной вероятностью q соответствующего значения нормы безопасности;
- предельной относительной ошибкой оценки соответствующего значения нормы безопасности:

$$\varepsilon = \max\left\{\frac{\hat{R}-\underline{R}}{\hat{R}};\frac{\overline{R}-\hat{R}}{\hat{R}}\right\}, \qquad (1)$$

где $\hat{R}$ - точечная оценка нормы безопасности R;

$\underline{R}$ - нижняя доверительная граница значения нормы безопасности R;

$\overline{R}$ - верхняя доверительная граница значения нормы безопасности R.

Значения относительной ошибки и доверительной вероятности q для показателей безопасности рекомендуется принимать следующими: $\varepsilon = 0{,}05$; $q = 0{,}95 \div 0{,}99$.

Получение достоверной экспериментальной оценки норм безопасности требует наличия достаточной по объему исходной статистической информации, получение которой связано с большими затратами времени в связи с тем, что опасные отказы ЖАТ – редкое событие.

При ограниченности статистических данных для расчета норм безопасности используется параметрический метод оценки, предполагающий известный закон распределения. Для систем ЖАТ справедлив экспоненциальный закон распределения.

Параметр закона распределения – интенсивность опасных отказов – определяется экспериментальным путем, остальные значения норм безопасности устанавливаются расчетными формулами соответствующих показателей.

Точечные и интервальные значения норм безопасности рассчитываются согласно формулам, приведенным в руководящем документе [3], в зависимости от вида исходной экспериментальной информации и соответствующего ему плана испытаний.

6.4.4 Расчетно-экспериментальные методы представляют комбинацию расчетных и экспериментальных методов. Их применяют в тех случаях, когда по отдель-

ным составным частям имеются статистические данные о безопасности, а по другим - результаты расчетов или когда предварительные результаты испытаний изделий, полученные в ходе разработки, позволяют уточнить расчетные значения ПБ.

Примечание – Пример применения расчетно-экспериментального метода приведен в приложении Д.

6.4.5 Расчет норм безопасности методом замещения рисков применяется в случае, когда новое изделие ЖАТ включается в структуру системы ЖАТ, замещая частично или полностью менее совершенные изделия. Нормы безопасности данного изделия ЖАТ рассчитываются с учетом норм безопасности замещаемых изделий.

Примечание – Пример применения метода замещения рисков приведен в приложении Д.

6.4.6 В целях уточнения норм безопасности допускается совместное использование нескольких методов.

Приложение А
(справочное)

Примеры определения количественных показателей безопасности

При задании количественных показателей безопасности систем ЖАТ необходимо учитывать функциональные возможности и число объектов управления в этих системах. Поэтому целесообразно ввести условные измерители, по отношению к которым необходимо производить задание требований. В таблице приведены условные измерители для различных систем управления.

Таблица А.1

Система автоматики	Условный измеритель нормирования
1. Электрическая и горочная централизации	Централизованная стрелка, станция
2. Диспетчерская централизация, станционная кодовая централизация	Управляемый, контролируемый объект, контрольный пункт
3. Центры диспетчерского управления	Пункт управления или контроля
4.Автоблокировка	Сигнальная точка
5. Полуавтоматическая блокировка	Перегон
6. Переездная сигнализация	Переезд
7. Автоматическая локомотивная сигнализация	Дешифратор или локомотивные устройства

Таким образом, если известны аппаратурные затраты на условный измеритель (стрелку, перегон, управляемый объект), показатели безопасности элементов и число таких элементов в разрабатываемой системе, то можно получить значения заданных показателей системы.

Приложение Б
(рекомендуемое)

Примеры построения и изложения разделов «Требования по безопасности» в ТЗ, ТУ изделий ЖАТ

Б.1 Требования безопасности оформляют в виде подраздела "Требований надежности".

Б.2 В первом пункте подраздела приводят перечень требований, номенклатуру и значения ПБ, которые записываются в следующей последовательности:

- качественные требования;
- количественные требования общие и при необходимости частные.

Рекомендуемая формулировка:

"Безопасность (наименование изделия) в условиях и режимах эксплуатации, установленных п.п._____ настоящего ТЗ, ТУ, должна характеризоваться качественными и количественными ПБ ...(приводятся эти показатели)."

Пример – Безопасность микроэлектронной автоматической локомотивной сигнализации определяется:

- ***аппаратурным резервированием 2Л2;***
- ***мягкой синхронизацией резервированных вычислительных каналов;***
- ***периодическим тестированием и сравнением работы вычислительных каналов (период диагностирования $t_д \leq 300$ мс);***
- ***несимметричными отказами внешнего интерфейса;***
- ***интенсивностью необнаруживаемых (опасных) отказов***

$\lambda \leq 1{,}2 * 10^{-10}$ 1/ч.

Примечания

1 В стандартах ОТТ требования безопасности приводят в виде предельно допустимых значений ПБ для изделий данной группы.

2 В стандартах видов ОТУ и в ТУ требования по безопасности устанавливаются в виде предельно допустимых значений тех показателей, которые контролируют при изготовлении изделий ЖАТ данной группы, и приводят в качестве справочных значения показателей, заданных в ТЗ на разработку изделия, но в процессе изготовления не контролируемых.

Б.3 Во втором пункте приводят определения (критерии) опасных отказов.

Пример – Опасным отказом реле первого класса надежности является создание цепи через замыкающий контакт при отсутствии тока в обмотке.

Опасным отказом схемы управления светофором является более разрешающее показание сигнала (вместо красного - желтый или зеленый, вместо желтого - зеленый и т. п.).

Б.4 В третьем пункте приводят общие требования к методам оценки безопасности и исходные данные для оценки каждым из методов соответствия изделий требованиям безопасности.

Рекомендуемая формулировка:

"Соответствие (наименование изделия) требованиям безопасности, установленным в п.п. _____, на этапе проектирования оценивают расчетным методом на основании данных; об интенсивности отказов комплектующих по (наименование НД), о достоверности используемых мер контроля; на этапе предварительных испытаний методом имитационного моделирования по (наименование НД); на этапе серийного производства контрольными испытаниями на стендах, физическим моделированием отказов по (наименование НД) с использованием следующих исходных данных для проведения испытаний: ... (перечисляются состав и значения исходных данных для испытаний).

Б.5 В четвертом пункте раздела при необходимости приводят ограничения по способам и средствам обеспечения заданного уровня безопасности.

Приложение В
(справочное)

Примеры возможных модификаций и определений стандартизованных показателей

В.1 При задании ПБ для многих видов изделий ЖАТ возникает потребность конкретизации их определений и наименований с учетом:

- специфики функций обеспечения безопасности;
- этапа эксплуатации, применительно к которому задан ПБ;
- принятой для рассматриваемых изделий классификации отказов и сбоев.

В.2 Изделия ЖАТ имеют различные функции по регулированию движения поездов, связанные с обеспечением безопасности:

- поддержание безопасного интервала между поездами на перегонах в системах интервального регулирования движения поездов;
- регулирование скорости движения путем задания допустимой скорости на путевых и локомотивных светофорах;
- управление маршрутами движения подвижных единиц на станции;
- управление переездной сигнализацией и т.п.

Примерами ПБ для ЖАТ с различными функциями могут быть:

- вероятность безопасной работы за поездку, рейс;
- вероятность опасного искажения ответственной команды;
- вероятность искажения информации о сохранении безопасного интервала между поездами;
- вероятность искажения информации о непревышении скорости, допустимой по соображениям безопасности;
- вероятность своевременного обнаружения автотранспортного средства на переезде и т. п.

В.3 Для некоторых изделий ЖАТ следует задавать ПБ применительно к отдельным этапам их эксплуатации (создания) или применительно к отдельным составным частям:

- вероятность обнаружения опасного отказа при предрейсовом (послерейсовом) контроле локомотивных устройств;
- вероятность появления опасного отказа в программном (аппаратном) обеспечении;
- вероятность появления опасных отказов (ошибок) в процессе включения изделия ЖАТ в эксплуатацию.

В.4 Для многих изделий ЖАТ (в основном микроэлектронных) разделяют ПБ из-за отказов и сбоев:

- вероятность опасного искажения ответственной команды в телемеханическом канале связи;
- вероятность появления сбоя, приводящего к опасному отказу;
- средняя наработка на сбой, приводящий к опасному нарушению алгоритма.

Приложение Г
(рекомендуемое)

Примеры критериев опасных отказов

Г.1 К пункту 3.6.2:

Для норм, ограниченных снизу, признаком опасного состояния является выполнение соотношения

$$K_б < K_{бн}, \qquad (Г.1)$$

где $K_б$ – значение показателя качества функционирования, влияющего на безопасность изделия ЖАТ;

$K_{бн}$ – нормированное значение показателя качества функционирования, влияющего на безопасность.

Для норм, ограниченных сверху, признаком опасного состояния является выполнение соотношения

$$K_б > K_{бн}, \qquad (Г.2)$$

где $K_б$ – значение показателя качества функционирования, влияющего на безопасность изделия ЖАТ;

$K_{бн}$ – нормированное значение показателя качества функционирования, влияющего на безопасность.

Г.2 К пункту 3.6.3:

Г.2.1 Для комбинационных дискретных элементов или устройств

$$f' f_{оп} \neq 0, \qquad (Г.3)$$

где f' – функция, реализуемая элементом или устройством ЖАТ при возникновении отказа;

$f_{оп}$ – функция опасного отказа, равная единице на опасных входных наборах;

Г.2.2 Для дискретных устройств с памятью

$$E' E_{оп} \neq 0, \qquad (Г.4)$$

где E' – событие, реализуемое устройством или системой ЖАТ при возникновении в них отказа;

$E_{оп}$ – событие, определяющее условия перехода устройства или системы в опасное состояние;

Г.2.3 Для изделий ЖАТ, выполненных в виде функциональных преобразователей (ФП),

$$Y \cap Z = 0, \qquad (Г.5)$$

где Y – множество значений выходных переменных ФП при исправности его элементов;

Z – множество значений выходных переменных ФП при отказе его элементов.

Примечание - Изделия ЖАТ, выполненные в виде функциональных преобразователей (ФП) с несимметричными отказами, характеризуются зависимостью во времени t

множества значений выходных параметров Y от множества значений входных (рабочих $X_р$, тестовых $X_т$) и внутренних переменных A, т.е. системой передаточных функций вида:

$$Y = F(X_р, X_т, A, t).$$

Множество возможных неисправностей, возникающих в преобразователе, приводит к искажению передаточных функций, а появление запрещенных входных наборов – к искажению выходных переменных.

Следовательно, появляется множество значений выходных переменных Z, которые должны вызывать переход системы в защитное состояние.

Таким образом, критерием опасного отказа для изделий ЖАТ, выполненных в виде функциональных преобразователей, следует считать выполнение условия (Г.5).

Г.3 К пункту 3.6.4

Г.3.1 Создание цепи через замыкающий контакт при отсутствии тока в обмотке реле первого класса надежности.

Г.3.2 Уменьшение сопротивления изоляции между соседними контактами реле (блока, статива) до величины, меньшей, чем указана в нормативных документах на реле (блок, статив).

Г.3.3 Уменьшение переходного сопротивления между соседними рельсовыми цепями ниже установленной нормы в случае, если изолирующие стыки этих рельсовых цепей не расположены в створе.

Г.3.4 Для системы электрической централизации опасным отказом будет ложная свободность рельсовой цепи, т.к. при этом возможна передача ложных управляющих приказов, например, разрешения на прием или отправление поезда через занятый участок пути.

Г.3.5 Ложное получение согласия в системах полуавтоматической блокировки; ложный контроль положения стрелки в системе электрической централизации.

Г.4 К пункту 3.6.5

Г.4.1 Искажение предметных, функциональных или предикатных символов программы в результате ошибок, допущенных программистом при ее создании, или в результате дефектов либо сбоев аппаратных средств при ее выполнении изделием ЖАТ, приводящее к реализации опасного отказа.

Г.4.2 Возникновение отказов в течение периода диагностирования в двух или более каналах изделия ЖАТ с троированной мажоритарной структурой.

Приложение Д
(рекомендуемое)

Примеры расчета нормированных значений показателей безопасности

Д.1 К пункту 6.3 - Расчет норм безопасности на основании достигнутого уровня безопасности

Пример - При замене существующей системы электрической централизации (ЭЦ) на систему микропроцессорной централизации (МПЦ) нормы безопасности МПЦ рассчитывают на основании норм ЭЦ следующим образом.

В качестве условного измерителя для систем ЭЦ принимают число K_O используемых реле, приходящихся на один стрелочный электропривод. В настоящее время $K_O = 60 \div 80$, в том числе для наборной группы $K_H = 12 \div 16$, а для исполнительной - $K_И = 48 \div 64$.

Собрать достоверную статистику об опасных отказах реле затруднительно, т.к. эти события происходят крайне редко. Поэтому ряд исследователей расчетным путем и на основе экспертных оценок определили интенсивность опасных отказов реле первого класса надежности $\lambda_р < 10^{-12}\ 1/ч$.

На основании этого можно определить укрупненный показатель интенсивности потока опасных отказов постовой аппаратуры, приходящейся на одну стрелку:

$$\lambda_{0стр} = \lambda_{0р} \cdot K_и = 5 \cdot 10^{-11}\ 1/ч.$$

Таким образом, зная число стрелок N на станции, оборудованной МПЦ, можно определить нормированное допустимое значение $\lambda_{0доп}$ для данной системы следующим образом:

$$\lambda_{0доп} = N \cdot \lambda_{0стр}.$$

Д.2 К пункту 6.4.1 - Определение норм безопасности с помощью экспертного метода

Пример - Вероятность опасных отказов микропроцессорной системы централизации стрелок и сигналов по результатам совещания экспертов стран-членов СЭВ (Румыния, 1984) должна удовлетворять условию:

$Qоп < 10^{-11}$.

Допустимая интенсивность опасных отказов реле первого класса надежности, определенная на основе экспертных оценок, должна быть не выше 10^{-13} 1/ч.

Д.3 К пункту 6.4.2 - Использование расчетного метода

Расчет норм безопасности производится исходя из условия, что данное изделие ЖАТ с заданной вероятностью будет иметь не более одного опасного отказа за весь срок эксплуатации. Вероятность опасного отказа рассчитывается по следующей формуле:

$$Q_{оп}(t) = \frac{1}{N}, \qquad (Д.1)$$

где N – количество изделий ЖАТ, находящихся в эксплуатации.

Формула (Д.1) справедлива для N > 100000.

Интенсивность опасных отказов для данного изделия ЖАТ с учетом срока эксплуа-

тации

$$\lambda_{оп}(t) = \frac{1}{NT}\ , \qquad (Д.2)$$

где Т – предполагаемый срок эксплуатации изделия ЖАТ.

Наработка до опасного отказа определяется по формуле

$$T_{оп}(t) = \frac{1}{\lambda_{оп}}\ . \qquad (Д.3)$$

Пример - Интенсивность опасных отказов схем управления стрелочными переводами при условии, что их количество по сети железных дорог составляет 230000 и срок эксплуатации 15 лет (131400 часов), рассчитывается следующим образом:

$$\lambda_{оп}(t) = \frac{1}{230000 \cdot 131400} = 3{,}31 \cdot 10^{-11} \qquad 1/ч.$$

Наработка до опасного отказа определяется по формуле (Д.3):

$$T = \frac{1}{3{,}31 \cdot 10^{-11}} = 3{,}02 \cdot 10^{10} \qquad ч.$$

Вероятность опасного отказа при t = 43800 ч (5 лет) рассчитывается по формуле:

$$Q_{оп} = \lambda_{оп} \cdot t = 3{,}31 \cdot 10^{-11} \cdot 4{,}38 \cdot 10^{4} = 1{,}45 \cdot 10^{-7}.$$

К пункту 6.4.4 - Применение расчетно-экспериментального метода

Пример - Расчетно-экспериментальный метод может быть использован для расчета норм безопасности изделия ЖАТ, построенных на реле первого класса надежности.

Предположим, что на основании экспериментального метода получены нормы вероятности $q_{оп}$ интенсивности опасных отказов для реле первого класса надежности.

Тогда, зная количество реле первого класса надежности, входящих а состав данного изделия ЖАТ, можно определить нормы вероятности и интенсивности опасных отказов всего изделия в целом:

$$q_{изд} = K_р \cdot q_{оп}\ , \qquad (Д.1)$$

$$\lambda_{изд} = K_р \cdot \lambda_{оп}\ , \qquad (Д.2)$$

где $K_р$- количество реле первого класса надежности в данном изделии ЖАТ.

Для сложных изделий ЖАТ, включающих N составляющих, содержащих m элементов, интенсивность опасных отказов может быть определена следующим образом:

$$\lambda_{изд} = \sum_{i=1}^{N} m_i \cdot \lambda_i\ , \qquad (Д.3)$$

где m_i- количество элементов i -й составляющей изделия ЖАТ;

λ_i - интенсивность опасных отказов первого элемента составляющей изделия ЖАТ.

Д.4 К пункту 6.4.5 - Использование метода замещения рисков

Пример - Метод замещения рисков может быть использован для расчета норм показателей безопасности при модернизации изделия ЖАТ.

Рассмотрим случай, когда в результате модернизации системы автоматической переездной сигнализации часть релейной схемы управления замещается микропроцессорным управляющим модулем. В соответствии с концепцией замещения рисков норма вероятности безопасной работы модуля должна удовлетворять следующему условию:

$$P_{БМ}(t) = P_{БР}(t) \quad , \qquad (Д.4)$$

где $P_{БМ}(t)$ ***и*** $P_{БР}(t)$, ***- соответственно нормы вероятности безопасной работы модуля и замещаемой части релейной схемы управления.***

В случае, если выполняется условие

$$P_{БМ}(t) > P_{БМН}(t) \quad , \qquad (Д.5)$$

где $P_{БМ}(t)$ ***- собственная вероятность безопасной работы модуля, возможно повышение нормы вероятности безопасной работы всей системы в целом или перераспределение норм между другими составляющими схемы управления автоматической переездной сигнализацией.***

Библиография

[1]	Отраслевой стандарт ОСТ 32.17-92	Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения.
[2]	Памятка ОСЖД Р-807	Количественные требования и средства контроля обеспечения безопасности систем и устройств СЦБ. Организация сотрудничества железных дорог (ОСЖД): совещание экспертов V комиссии
[3]	Руководящий документ РД 50-690-89	Методические указания. Надежность в технике. Методы оценки показателей надежности по экспериментальным данным.

gost.e-ecolog.ru