Российские железные дороги

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

РАСПОРЯЖЕНИЕ

04 декабря 2009г. Москва № 2471р

**Об утверждении стандарта ОАО «РЖД»
«Системы и устройства железнодорожной автоматики и телемеханики. Доказательство безопасности»**

В целях повышения безопасности, определения понятия и назначения процесса доказательства безопасности, установления структуры, содержания и порядка разработки документа «Доказательство безопасности» для систем автоматики и телемеханики:

1. Утвердить и ввести в действие с 1 января 2010 г. стандарт СТО РЖД 1.19.009-2009 «Системы и устройства железнодорожной автоматики и телемеханики. Доказательство 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 32.41-95 «Безопасность железнодорожной автоматики и телемеханики. Методы доказательства безопасности систем и устройств железнодорожной автоматики и телемеханики».

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

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

gost.e-ecolog.ru

Российские железные дороги

Стандарт	СТО РЖД
ОАО «РЖД»	1.19.009—
	2009

СИСТЕМЫ И УСТРОЙСТВА ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Доказательство 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 04 декабря 2009г. №2471р

4 ВВЕДЕН ВПЕРВЫЕ

Учетный регистрационный номер

© ОАО «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 Основные положения 1
3 Общие требования 2
4 Структура документа “Доказательство безопасности” 3
5 Содержание документа “Доказательство безопасности” 3
Библиография 6

Стандарт ОАО «РЖД»

СИСТЕМЫ И УСТРОЙСТВА ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Доказательство безопасности

Дата введения 04 декабря 2009г.

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 отраслевым стандартом [1] и СТО РЖД 1.19.008-2009 «Системы и устройства железнодорожной автоматики и телемеханики. Выбор и общие правила задания требований по безопасности».

Настоящий стандарт определяет понятие и назначение процесса доказательства безопасности и устанавливает структуру, содержание и порядок разработки документа "Доказательство безопасности".

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 железнодорожной автоматики и телемеханики.

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

2 Основные положения

2.1 Доказательство безопасности системы железнодорожной автоматики и телемеханики (СЖАТ) – это базирующееся на актуальных, объективных и достоверных данных аргументированное обоснование того, что должным образом идентифицированная система соответствует предъявляемым к ней требованиям по безопасности при работе в заданных режимах и условиях эксплуатации.

2.2 Доказательство безопасности является результатом мероприятий, проводимых в соответствии с программой обеспечения безопасности.

2.3 Документ «Доказательство безопасности» предназначен для аккумулирования всей совокупности материалов доказательного характера и отражения результатов работ по обеспечению требований безопасности, проводимых на всех этапах жизненного цикла СЖАТ. В документе "Доказательство безопасности" следует в письменной форме обосновать, что система является безопасной.

2.4 Документ "Доказательство безопасности" является обязательным при оценке соответствия системы требованиям безопасности, установленным в технических регламентах.

2.5 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 системы заданным нормам.

2.6 Выводы доказательства безопасности должны позволять судить о следующем:

– требования на систему заданы корректно и в полном объёме;

– требования, предъявляемые к системе, в полном объеме и корректно реализованы в программно-аппаратных решениях;

– программно-аппаратные решения не привносят дополнительных негативных свойств относительно первоначальных требований безопасности;

– представленные доказательства обоснованы и достоверны.

3 Общие требования

3.1 Разработка документа "Доказательство безопасности" осуществляется организацией-разработчиком системы. Документ утверждается руководителем этой организации и представляется для независимого экспертного заключения в организацию, которая будет производить оценку соответствия системы заданным требованиям безопасности.

3.2 Обязательным условием для допуска системы в опытную и постоянную эксплуатацию является наличие положительного экспертного заключения по документу "Доказательство безопасности" для данного этапа.

3.3 Должна быть предусмотрена следующая последовательность (этапность) разработки документа «Доказательство безопасности» в жизненном цикле системы:

– формирование проекта документа для этапа технического проектирования;

– выпуск первой редакции документа для этапа опытной эксплуатации;

– формирование второй редакции для этапа постоянной эксплуатации;

– при необходимости корректировка документа по результатам постоянной эксплуатации.

3.4 Документ «Доказательство безопасности» системы может быть разделен на документы «Доказательства безопасности» ее отдельных подсистем. Структура документа «Доказательства безопасности» должна повторяться для каждой из подсистем. Электрические и информационные связи отдельных подсистем должны быть подвергнуты самостоятельному анализу на безопасность.

3.5 В документе «Доказательство безопасности» отдельных частей системы допускается делать ссылки на известные документы «Доказательство безопасности» при условии полной идентичности части устройства, ее связей этому доказательству, а также принятым в доказательстве ограничениям, режимам и условиям эксплуатации и технического обслуживания.

3.6 Для технических средств различного применения допускается разработка документа «Доказательство безопасности», отражающего универсальные характеристики изделия, свойственные различным условиям применения. При этом для каждого конкретного применения данных технических средств должен быть разработан новый документ «Доказательство безопасности», обосновывающий возможность использования данного изделия в условиях данного конкретного применения.

3.7 Представленные в документе «Доказательство безопасности» материалы должны отражать актуальное положение дел. Изменение требований, условий эксплуатации или программно-технических решений должно приводить к корректировке документа с необходимостью проведения его повторной экспертизы.

3.8 Документ «Доказательство безопасности» хранится у разработчиков и в организации, выдавшей заключение о безопасности системы. Срок хранения заканчивается не ранее чем через 10 лет после прекращения производства системы.

4 Структура документа “Доказательство безопасности”

4.1 Документ «Доказательство безопасности» должен содержать следующие разделы:

- вводные замечания;
- нормативные документы;
- характеристика объекта;
- доказательство работоспособности;
- методы доказательства безопасности;
- подтверждение безопасности;
- заключение по безопасности;
- список использованных источников.

5 Содержание документа “Доказательство безопасности”

5.1 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.

5.2 В разделе "Нормативные документы" приводится перечень международных, государственных и отраслевых документов, которые регламентируют содержание и структуру доказательства безопасности.

5.3 Характеристика объекта должна содержать:

– концепцию обеспечения безопасности;

– требования и нормы безопасности;

– критерии опасных отказов;

– краткое описание принципов построения и работы;

– описание конструктивного оформления.

5.4 В подразделе «Концепция безопасности» приводится совокупность положений в соответствии с которыми осуществляется построение безопасной системы.

5.5 В подразделе «Требования и нормы безопасности» должны быть приведены все качественные и количественные требования безопасности, предъявляемые к системе.

5.6 Описание системы должно быть приведено в объёме, позволяющем однозначно идентифицировать систему (её версию и (или) конфигурацию), оценить её функциональность, определить её состав, границы и интерфейсы взаимодействия с другими системами, объектами контроля и управления.

5.7 Раздел «Доказательство работоспособности» должен содержать доказательный материал, подтверждающий, что система соответствует заданным техническим требованиям при эксплуатации в заданных условиях и режимах. В данном разделе приводятся результаты испытаний и результаты расчёта показателей надежности системы. Протоколы испытаний и расчёт надежности должны быть приведены в приложениях к документу. Также в приложениях должны быть представлены программы и методики, в соответствии с которыми выполнялись испытания системы.

5.8 В разделе "Методы доказательства безопасности" приводится перечень используемых методов доказательства безопасности с указанием целей их использования и ограничениями применения каждого из методов доказательства. Ограничения должны отражать условия, определяющие степень достоверности доказательств, получаемых каждым из используемых методов доказательства, например: используемые допущения при расчете показателей безопасности, учитываемый класс повреждений, полнота и достоверность испытаний, степень адекватности используемых машинных моделей, квалификация экспертов и т.п.

5.9 В разделе "Подтверждение безопасности" приводится аргументированное обоснование соответствия программно-технических решений заданным требованиям безопасности.

В данном разделе обосновывается полнота и корректность требований, предъявляемых к системе, и приводится аргументация, базирующаяся на представленных свидетельствах того, что программно-технические решения системы соответствуют

данным требованиям безопасности. Весь материал раздела должен быть ориентирован на поддержку данной аргументации. Аргументированное обоснование должно быть хорошо структурировано и содержать ссылки на свидетельства, полученные с использованием различных методов доказательства и представленные в документированном виде в приложениях к документу.

В данном разделе должно быть подтверждено, что в системе обеспечивается корректность выполнения алгоритмических условий обеспечения безопасности, обосновано, каким образом и за счет чего обеспечивается выполнение заданных требований и концепции безопасности при возникновении сбоев и отказов, при изменении параметров элементов в допустимых пределах, при искажении информации в каналах связи, при воздействии электромагнитных помех, климатических и механических факторов, приведены результаты расчёта количественных показателей безопасности. Также в разделе приводятся требования по эксплуатации и техническому обслуживанию, относящиеся к обеспечению безопасности.

Любые выводы и используемые для их формирования исходные данные должны быть обоснованы. В качестве обоснования могут выступать аналитические материалы (теоретический анализ), экспертные заключения, расчет, ссылка на справочную или научную (научно-техническую) литературу, протоколы моделирования и/или испытаний.

Обоснования (свидетельства), используемые при аргументации, должны быть приведены в приложениях «Доказательства безопасности». Также в приложениях к документу должны быть представлены программы и методики, в соответствии с которыми выполнялись испытания системы на безопасность.

5.10 В разделе «Заключение по безопасности» приводятся общие выводы по результатам доказательства безопасности, представленного в документе.

Библиография

[1] Отраслевой стандарт ОСТ 32.17-92 — Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения.

gost.e-ecolog.ru