ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

ОСТ 32.19—92

Издание официальное

САНКТ-ПЕТЕРБУРГ

gost.e-ecolog.ru

УДК 656.25 Группа Д50

ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Общие требования к программам обеспечения безопасности

ОСТ 32.19-92

ОКСТУ 4202

Дата введения I.0I.I993 г.

Содержание

I. ОБЩИЕ ПОЛОЖЕНИЯ	2
2. ОСНОВНЫЕ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ПРОГРАММЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ	–
3. СОДЕРЖАНИЕ РАЗДЕЛОВ ПРОГРАММЫ	4
3.I. Введение	–
3.2. Состав и основные характеристики системы железнодорожной автоматики и телемеханики	–
3.3. Требования технического задания к безопасности функционирования СЖАТ	5
3.4. Основная концепция, методы и средства обеспечения безопасности СЖАТ	–
3.5. Мероприятия по обеспечению безопасности СЖАТ	–
3.6. Порядок отчетности	I3
3.7. Организация контроля выполнения программы обеспечения безопасности	–
3.8. Порядок корректировки программы обеспечения безопасности	–
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	I4
ИНФОРМАЦИОННЫЕ ДАННЫЕ	I5

1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа обеспечения безопасности представляет собой организационно-технический документ, определяющий перечень и взаимосвязь необходимых работ и мероприятий, проводимых на всех стадиях разработки (в соответствии с ГОСТ 34.602-89, РД 50-680), серийного изготовления и эксплуатации системы железнодорожной автоматики и телемеханики (СЖАТ), направленных на обеспечение заданного уровня безопасности.

Все термины и определения, которые используются в данном стандарте, соответствуют ОСТ 32.17-92 "Безопасность железнодорожной автоматики. Основные понятия. Термины и определения".

Программа должна содержать список исполнителей и определять состав, последовательность, организацию, методические основы, содержание и этапы выполнения мероприятий, обеспечивающих заданный уровень безопасности системы.

Программа обеспечения безопасности представляет собой составную часть программы разработки, изготовления и эксплуатации конкретной СЖАТ. Она является необходимым документом для сертификации безопасности СЖАТ.

Отчетные материалы по обеспечению безопасности должны быть оформлены в виде специального раздела документации на СЖАТ, соответствующей этапу создания системы.

2. ОСНОВНЫЕ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ПРОГРАММЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

2.1. Программа должна представлять собой совокупность организационных, конструктивных, технологических и методических мероприятий, увязанных со всеми этапами жизненного цикла СЖАТ (разработки, производства и эксплуатации).

2.2. Программа должна содержать следующие разделы:

2.2.1. введение;

2.2.2. состав программы;

2.2.3. состав и основные характеристики СЖАТ;

2.2.4. требования ТЗ по безотказности и безопасности функционирования СЖАТ;

2.2.5. основная концепция, методы и средства обеспечения безопасности;

2.2.6. мероприятия по обеспечению безопасности, проводимые на всех этапах разработки, серийного производства и эксплуатации СЖАТ;

2.2.7. порядок отчетности;

2.2.8. организация контроля выполнения программы;

2.2.9. порядок корректировки программы.

2.3. Программа обеспечения безопасности может быть оформлена в виде отдельного документа, увязанного с программами обеспечения надежности и испытаний, или в виде составной части программы обеспечения надежности.

2.4. В программе должны быть отражены основные пути решения задач обеспечения безопасности:

2.4.1. достижение требуемого уровня безопасности системы (структурные и конструктивные решения, методы резервирования элементов и составных частей системы и т.п.);

2.4.2. выведение системы из состояния защитного и опасного отказов.

2.5. Программа должна охватывать все этапы жизненного цикла СЖАТ и распространяться на все технические средства, влияющие на безопасность функционирования системы (средства прогнозирования, обнаружения и распознавания опасных отказов, оповещения о них обслуживающего персонала и т.п.).

2.6. Программа обеспечения безопасности должна предусматривать определение требований по безопасности к СЖАТ в целом и к ее составным частям.

2.7. Программа должна предусматривать моделирование и всесторонние испытания системы в целом и ее элементов.

2.8. Программа обеспечения безопасности СЖАТ должна содержать три взаимосвязанные частные программы, а именно:

2.8.1. программу обеспечения безопасности для этапа разработки, включая эксплуатационные испытания и постановку на производство;

2.8.2. программу обеспечения безопасности для этапа серийного производства;

2.8.3. программу обеспечения безопасности для этапа эксплуатации.

2.9. Программа обеспечения безопасности должна разрабатываться независимой организацией, аттестованной на проведение сертификационных работ по безопасности СЖАТ, совместно с разработчиком, изготовителем и заказчиком системы соответственно на каждом этапе ее жизненного цикла.

3. СОДЕРЖАНИЕ РАЗДЕЛОВ ПРОГРАММЫ

3.1. Введение

В разделе указываются нормативно-технические документы (ГОСТы, ОСТы, ОТТ и др.), в соответствии с которыми разработана программа обеспечения безопасности СЖАТ, а также методические документы (руководства, инструкции, методические указания и т.п.), подлежащие использованию в процессе реализации программы обеспечения безопасности.

Приводится название органа сертификации, разработавшего программу, и перечень организаций и предприятий, которые участвовали в разработке и согласовании программы.

Приводится список организаций, которые принимают участие в реализации программы.

Указываются сроки выполнения этапов программы обеспечения безопасности и сроки утверждения частных программ (см. п. 2.9).

3.2. Состав и основные характеристики системы железнодорожной автоматики и телемеханики

В разделе следует привести состав и основные функциональные, информационные, конструктивные и эксплуатационные характеристики системы, которые являются определяющими для безопасности функционирования, описать и провести анализ поведения системы в работоспособном состоянии и в состояниях защитного и опасного отказов. В этом разделе дается характеристика предполагаемых условий эксплуатации и технического обслуживания.

При необходимости дается характеристика подсистем СЖАТ, влияющих на безопасность движения поездов.

3.3. Требования технического задания к безопасности функционирования СЖАТ

В разделе должны быть указаны количественные и качественные показатели безопасности системы, заданные в ТЗ на разработку СЖАТ и нормируемые действующими нормативно-техническими документами (ОСТ 32.18-92 "Выбор и основные правила нормирования показателей безопасности").

Указываются определенные в ТЗ критерии опасных и защитных отказов системы.

Приводятся исходные условия (например, число стрелок на станции, наработка на отказ и др.), при которых должны определяться и подтверждаться показатели безопасности.

Приводится требования ТЗ и нормативно-технических документов о порядке выполнения и подтверждения требований по безопасности.

3.4. Основная концепция, методы и средства обеспечения безопасности СЖАТ

В разделе должны быть сформулированы общая концепция, основные принципы и необходимые условия обеспечения безопасности принимаемые для системы в целом и ее составных частей. Описывается общая (укрупненная) модель безопасного функционирования СЖАТ.

Дается качественная оценка используемых методов и средств обеспечения безопасности.

3.5. Мероприятия по обеспечению безопасности СЖАТ

3.5.1. Разработка технических предложений

На данной стадии должны быть осуществлены следующие мероприятия.

3.5.1.1. Предварительный анализ СЖАТ, ее основных характеристик, решаемых ею задач и процесса безопасного функционирования системы на всех этапах ее эксплуатации.

3.5.1.2. Анализ требований руководящих и нормативно-технических документов по обеспечению безопасности функционирования СЖАТ.

3.5.1.3. Анализ опыта обеспечения безопасности аналогичных систем и достигнутого в них уровня безопасности.

3.5.1.4. Анализ различных вариантов построения СЖАТ и их сравнительная оценка с точки зрения безопасности.

3.5.1.5. Разработка концепции, основных принципов и способов обеспечения безопасности функционирования проектируемой СЖАТ.

3.5.1.6. Определение предварительных требований по безопасности СЖАТ, вносимых в техническое задание.

3.5.1.7. Распределение требований по обеспечению безопасности между составными частями системы исходя из требований руководящих и нормативно-технических документов на систему в целом.

3.5.1.8. Анализ возможных опасных отказов СЖАТ с предварительной оценкой вероятности их возникновения и задаваемого уровня безопасности.

3.5.1.9. Разработка способов вывода системы из состояния опасного отказа.

3.5.1.10. Предварительное обоснование методов и средств обеспечения безопасности СЖАТ на этапе эксплуатации.

3.5.1.11. Предварительная оценка возможности технической реализации заданного уровня безопасности СЖАТ.

3.5.1.12. Предварительное обоснование требований по безопасности к конструктивной схеме СЖАТ.

3.5.1.13. Разработка принципиальных технических решений по способам и средствам предупреждения опасных отказов.

3.5.1.14. Разработка плана программы обеспечения безопасности СЖАТ в целом.

3.5.1.15. Составление проекта программы обеспечения безопасности СЖАТ на этапе разработки.

3.5.2. Техническое задание

На этой стадии в программе обеспечения безопасности должны быть предусмотрены следующие мероприятия.

3.5.2.1. Анализ степени выполнения требований по безопасности СЖАТ по материалам, изложенным в технических предложениях.

3.5.2.2. Обобщение материалов по отечественному и зарубежному опыту обеспечения безопасности СЖАТ, сравнительная оценка

уровней безопасности аналогичных систем.

3.5.2.3. Анализ возможных опасных отказов на всех этапах функционирования СЖАТ и определение:

3.5.2.3.I. возможных источников возникновения опасных отказов;

3.5.2.3.2. количественных характеристик опасных отказов (вероятности возникновения, времени, необходимого на выход СЖАТ из состояния опасного отказа и т.д.);

3.5.2.3.3. способов и алгоритмов выхода системы из состояния опасного отказа;

3.5.2.3.4. списка возможных опасных отказов и их распределения по причинам возникновения, характеру проявления и т.п.;

3.5.2.3.5. способов прогнозирования, обнаружения и распознавания опасных отказов и оповещения обслуживающего персонала об их возникновении.

3.5.2.4. Разработка вариантов технических решений, направленных на предупреждение (или уменьшение вероятности) появления опасных отказов в процессе функционирования.

3.5.2.5. Разработка (уточнение) методик:

3.5.2.5.I. анализа и определения параметров опасных отказов;

3.5.2.5.2. определения значений показателей безопасности системы в целом и ее подсистем, проектной оценки уровня безопасности по выбранным показателям;

3.5.2.5.3. классификации и перечня опасных отказов;

3.5.2.5.4. сравнительной оценки технико-экономической эффективности различных вариантов средств обеспечения безопасности;

3.5.2.5.5. имитационного моделирования функционирования СЖАТ в состояниях отказа;

3.5.2.5.6. исследования динамики развития опасных отказов, оценки основных характеристик функционирования средств безопасности при опасных отказах, анализа предложенных ранее способов вывода системы из состояния опасного отказа и выбора оптимального;

3.5.2.5.7. подтверждения заданных значений показателей и уровня безопасности.

3.5.2.6. Разработка и обоснование необходимого состава оборудования комплекса имитаторов моделирования поведения СЖАТ в

состояниях: исправном, работоспособном, защитном.

Предварительное определение необходимого объема моделирования исходя из требований по обеспечению безопасности.

3.5.2.7. Разработка имитационной модели СЖАТ.

3.5.3. Эскизное проектирование

На данном этапе должны быть выполнены следующие мероприятия.

3.5.3.1. Разработка предварительных технических решений по выбранному варианту средств обеспечения безопасности СЖАТ.

3.5.3.2. Оценка проектного уровня безопасности выбранного варианта системы в целом и ее подсистем, а также степени их соответствия ТЗ.

3.5.4. Разработка технического проекта

На данной стадии в программе обеспечения безопасности должны быть проведены следующие мероприятия.

3.5.4.1. Анализ и обобщение замечаний и предложений по обеспечению безопасности, высказанных при рассмотрении технического задания. Разработка плана мероприятий по устранению выявленных недоработок и реализации предложений.

3.5.4.2. Анализ окончательных решений по составу СЖАТ и степени выполнения требований по безопасности, разработанных на предыдущей стадии работ.

3.5.4.3. Анализ процесса функционирования СЖАТ для определения (уточнения) возможных опасных отказов. Разработка уточненного списка опасных отказов с определением их количественных характеристик и способов вывода системы из состояний опасного отказа.

3.5.4.4. Детальная разработка технических проектов средств обеспечения безопасности СЖАТ в соответствии с требованиями, отработанными на стадии технического задания, в том числе средств прогнозирования, обнаружения и распознавания опасных отказов и оповещения обслуживающего персонала об их возникновении, вывода системы из состояний опасного отказа.

3.5.4.5. Уточнение методик оценки значений показателей безопасности.

3.5.4.6. Разработка перечня инструкций по обеспечению безопасности СЖАТ в процессе эксплуатации.

3.5.4.7. Доработка имитационной модели СЖАТ с учетом уточненных критериев опасных отказов.

3.5.4.8. Проведение количественной и качественной оценки уровня безопасности и эффективности средств и мероприятий по обеспечению безопасности СЖАТ в процессе эксплуатации.

3.5.4.9. Анализ и обобщение замечаний и предложений по результатам рассмотрения технического проекта, разработка плана мероприятий по устранению отмеченных недостатков по вопросам безопасности.

3.5.5. Разработка рабочей документации

На данной стадии в программе должны быть предусмотрены следующие мероприятия.

3.5.5.I Уточнение причин появления опасных отказов и их вероятности.

3.5.5.2. Оценка возможных последствий каждого опасного отказа.

3.5.5.3 Разработка мероприятий по прогнозированию и предупреждению опасных отказов и выводу системы из них.

3.5.5.4. Составление списка защитных отказов системы в целом и ее составных частей.

3.5.5.5. Выделение элементов и узлов, влияющих на безопасность СЖАТ.

3.5.5.6. Определение характера поведения СЖАТ в состоянии защитного отказа.

3.5.5.7. Составление списка защитных отказов, которые необходимо исследовать на имитационной модели.

3.5.5.8. Составление перечня элементов с ограниченным сроком службы.

3.5.5.9. Оценка (экспертиза) достигнутого проектного уровня безопасности.

3.5.5.IO. Разработка методик подтверждения количественных требований по безопасности системы.

3.5.5.II. Проверка рабочей документации на соответствие

требованиям по обеспечению безопасности.

3.5.5.12. Разработка инструкции по входному контролю материалов, комплектующих элементов и узлов на соответствие требованиям по безопасности.

3.5.5.13. Создание и испытание имитационной модели СЖАТ.

3.5.5.14. Оценка эффективности имитационной модели и разработка методик по отработке процесса функционирования СЖАТ в состояниях защитного отказа и способов вывода системы из этих состояний.

3.5.5.15. Изготовление макетных образцов средств обеспечения безопасности.

3.5.5.16. Разработка планов, технических условий, программ и методик испытаний элементов СЖАТ и средств безопасности.

3.5.5.17. Разработка планов, программ и методик эксплуатационных испытаний средств безопасности.

3.5.5.18. Разработка методик оценки результатов испытаний, а также достигнутого уровня безопасности по результатам испытаний.

3.5.5.19. Разработка планов, программ и методик испытаний СЖАТ и средств обеспечения безопасности с имитацией защитных и опасных отказов.

3.5.5.20. Обоснование объема эксплуатационных испытаний, необходимого для обеспечения заданного уровня безопасности системы.

3.5.5.21. Разработка рекомендаций для обслуживающего персонала по выводу системы из состояния опасного отказа.

3.5.6. И з г о т о в л е н и е о п ы т н о г о о б р а з ц а. Э к с п л у а т а ц и о н н ы е и с п ы т а н и я

На этих стадиях в программе обеспечения безопасности должны планироваться следующие мероприятия.

3.5.6.1. Уточнение программ и объемов эксплуатационных испытаний средств обеспечения безопасности.

3.5.6.2. Контроль опытных изделий средств безопасности на соответствие предъявляемым к ним требованиям.

3.5.6.3. Проведение эксплуатационных испытаний технических средств безопасности, в том числе:

3.5.6.3.1. проверки функционирования средств безопасности с

имитацией опасных отказов;

3.5.6.3.2. определения рациональных режимов и предельных условий работы средств безопасности;

3.5.6.3.3. проверки и оценки технических характеристик СЖАТ на соответствие предъявляемым к ним требованиям безопасности.

3.5.6.4. Испытания элементов, входящих в состав СЖАТ, на соответствие требованиям по обеспечению безопасности.

3.5.6.5. Анализ и уточнение характеристик и списка опасных отказов по результатам испытаний.

3.5.6.6. Оценка эффективности средств обеспечения безопасности и достигнутого уровня безопасности по результатам испытаний. Определение степени соответствия СЖАТ предъявляемым требованиям по безопасности.

3.5.6.7. Разработка плана мероприятий по устранению выявленных в ходе испытаний недостатков, разработка предложений по доработке системы и средств безопасности.

3.5.6.8. Уточнение рабочей документации по безопасности в соответствии с результатами эксплуатационных испытаний.

3.5.6.9. Разработка планов, программ и методик заводских испытаний на безопасность СЖАТ.

3.5.6.10. Обоснование объема заводских испытаний, необходимого для обеспечения заданного уровня безопасности системы.

3.5.6.11. Разработка отчета по выполнению программы обеспечения безопасности на стадии эксплуатационных испытаний.

3.5.6.12. Разработка, согласование и утверждение программы обеспечения безопасности на этапе серийного производства.

3.5.6.13. Разработка инструкций для обслуживающего персонала по безопасной эксплуатации системы (по выводу из опасного отказа).

3.5.7. Серийное производство

На данном этапе должны быть осуществлены следующие мероприятия.

3.5.7.1. Разработка методических документов (руководств, положений, инструкций) по обеспечению безопасности в процессе серийного производства.

3.5.7.2. Систематизация, обработка и анализ данных эксплуатационных испытаний и серийного производства, влияющих на безопасность функционирования СЖАТ.

3.5.7.3. Уточнение программ и объемов заводских испытаний СЖАТ.

3.5.7.4. Организация качественного технологического контроля выполнения особо ответственных операций.

3.5.7.5. Контроль и оценка влияния на безопасность функционирования СЖАТ изменений (отступлений) в конструкторской и технологической документации.

3.5.7.6. Систематический контроль за испытаниями деталей, узлов и систем, направленный на достижение максимального соответствия режимов испытаний фактическим условиям и нагрузкам.

3.5.7.7. Проведение заводских сертификационных испытаний.

3.5.7.8. Разработка отчета о выполнении программы обеспечения безопасности на этапе серийного производства.

3.5.7.9. Разработка, согласование и утверждение программы обеспечения безопасности на этапе эксплуатации.

3.5.8. Эксплуатация

На этом этапе должны быт предусмотрены следующие мероприятия.

3.5.8.1. Систематический сбор, обработка и всесторонний анализ данных о всех защитных отказах, имевших место в процессе эксплуатации.

3.5.8.2. Внесение изменений в конструкторскую и рабочую документацию по вопросам обеспечения безопасности.

3.5.8.3. Определение фактических значений количественных показателей безопасности и общего ее уровня с учетом данных, накопленных в процессе эксплуатации, а также оценка соответствия этих показателей заданным значениям.

3.5.8.4. Разработка и реализация конструкторско-технологических мероприятий по совершенствованию (устранению недостатков, выявленных в процессе эксплуатации) системы.

3.5.8.5. Разработка и реализация мероприятий по совершенствованию методов и средств технического обслуживания для обеспечения безопасности.

3.5.8.6. Оценка эффективности проводимых мероприятий по обеспечению безопасности.

3.6. Порядок отчетности

В разделе приводятся отчетные материалы о результатах выполнения каждого мероприятия программы обеспечения безопасности, список исполнителей работ и сроки их выполнения.

Результаты выполнения программы фиксируются в сертификате безопасности СЖАТ.

3.7. Организация контроля выполнения программы обеспечения безопасности

В разделе приводится название органа сертификации, ответственного за контроль выполнения программы, и определяются сроки проведения сертификационных испытаний на безопасность СЖАТ.

3.8. Порядок корректировки программы обеспечения безопасности

В разделе указываются основание, исполнители и сроки корректировки программы.

Основанием для коррекции могут служить:

3.8.1. выявление новых путей обеспечения безопасности, связанных с совершенствованием технических средств;

3.8.2. изменение структуры СЖАТ и конструкции ее составных частей, узлов и элементов;

3.8.3. изменение в технологии изготовления элементов аппаратуры и узлов системы в связи с использованием новых материалов и технических решений;

3.8.4. неудовлетворительные результаты оценки достигнутого уровня безопасности на предыдущем этапе;

3.8.5. получение новых данных об опасных отказах и их характеристиках в процессе испытаний элементов системы и средств обеспечения безопасности.

В разделе также должен быть определен порядок обмена информацией между заинтересованными организациями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Г о л и н к е в и ч Т.А. Прикладная теория надежности. - М.: Высшая школа, 1985. - 168 с.

2. Я с т р е б е н е ц к и й М.А., И в а н о в в Г.М. Надежность автоматизированных систем управления технологическими процессами - М.: Энергоатомиздат, 1989.- 264 с.

3. Безопасность полетов летательных аппаратов: Методические основы/Под ред. А.И.Старикова. - М.: Транспорт, 1988.- 159 с.

4. Я г у д и н Р.Ш. Надежность устройств железнодорожной автоматики и телемеханики. - М.: Транспорт, 1989.- 159 с.

5. Справочник по безопасности космических полетов/ Г.Т. Береговой, В.И. Ярополов, И.И. Баранецкий и др. - М.: Машиностроение, 1989.- 336 с.

6. ГОСТ 24.602. Автоматизированные системы управления. Состав и содержание работ по стадиям создания.- М.: Изд-во стандартов, 1986.- 12 с.

И Н Ф О Р М А Ц И О Н Н Ы Е Д А Н Н Ы Е

I. 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, А.В. Крылатов, Е.В. Самонина.

2. УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Указанием МПС РФ от 22 июля 1992 г. N Г-640у.

3. СРОК ПРОВЕРКИ - 1997 г.

4. ВВЕДЕН ВПЕРВЫЕ.

5. ССЫЛОЧНЫЕ НОРМАТИВНО-ТЕХНИЧЕСКИЕ ДОКУМЕНТЫ.

Обозначение НТД, на который дана ссылка	Номер пункта
ГОСТ 34.602-89	I
РД50-680-88	I
ОСТ 32	I, 3.3, 3.5.6.9

ОТРАСЛЕВОЙ СТАНДАРТ

БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Общие требования к программам обеспечения безопасности

Редакторы А.И. Жук, Н.В. Фролова

Подписано в печать с оригинала - макета 21.11.92.
Формат 60 х 84 1/16. Бумага для множ.апп. Печать офсетная.
Усл.печ.л. 1,0. Уч.-изд.л. 1,0. Тираж 1000.
Заказ 1059

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

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

gost.e-ecolog.ru