ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)

II издание

Разработано экспертами Комиссии ОСЖД
по инфраструктуре и подвижному составу 21-24 сентября
2010 г., Словацкая Республика, г. Кошице

Утверждено совещанием Комиссии ОСЖД по инфраструктуре
и подвижному составу 22 октября 2010 г.,
Комитет ОСЖД, г. Варшава

Дата вступления в силу: 22 октября 2010 г.

Примечание: теряет силу I издание от 7 ноября 2000 г.

Р
807

КОЛИЧЕСТВЕННЫЕ ТРЕБОВАНИЯ И СРЕДСТВА КОНТРОЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ И УСТРОЙСТВ СЦБ

СОДЕРЖАНИЕ

Стр.

1. Область применения

Настоящая Памятка распространяется на все виды систем и устройств (в дальнейшем - систем) сигнализации, централизации и блокировки (СЦБ), к которым в нормативной и конструкторской документации предъявляются требования безопасности.

Памятка распространяется на системы, разрабатываемые по заказам железных дорог – членов ОСЖД. Памятка может быть использована при сертификации.

Памятка определяет количественные требования к основным системам СЦБ и к средствам контроля обеспечения безопасности.

2. Основные понятия и определения

Безопасность систем СЦБ (Signalling systems safety) – свойство систем сигнализации, централизации и блокировки непрерывно сохранять исправное, работоспособное или защитное состояние в течение некоторого времени или наработки.

Защитный отказ (Protective failure) – событие, заключающееся в нарушении работоспособного состояния системы при сохранении защитного состояния.

Опасный отказ (Hazardous failure) – событие, заключающееся в нарушении работоспособного и защитного состояний системы.

Критерий опасного отказа (Hazardous failure criterion) – признак или совокупность признаков опасного состояния системы, установленных в нормативной или конструкторской документации.

Концепция безопасности (Safety conception) – совокупность положений, в соответствие с которыми осуществляется построение безопасной системы.

Уровень безопасности (Safety level) – совокупность требований к системе, определяемая предельными значениями показателей безопасности и удовлетворяющая определенным требованиям безопасности.

Нормируемый показатель безопасности (Specified safety measure) – показатель безопасности, значение которого регламентировано нормативной или конструкторской документацией на систему.

Вероятность опасного отказа (Hazardous failure probability) – вероятность того, что в пределах заданной наработки опасный отказ наступает хотя бы один раз.

Интенсивность опасных отказов (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.

Средняя наработка до опасного отказа (Mean operating time to hazardous failure) – математическое ожидание наработки системы до первого опасного отказа.

3. Общие положения

3.1. Основным направлением всех работ и исследований при создании системы управления, связанной с безопасностью движения поездов, является принцип исключения возможности появления потенциально опасной ситуации (или сведению вероятности появления этого события к минимально допустимой величине). Поэтому достижение безопасности функционирования устройств и систем управления движением поездов должно базироваться на следующих основополагающих принципах:

- обеспечение безопасного функционирования системы управления;
- обеспечение качественного изготовления устройств системы и ее программного обеспечения;
- принцип допущения худшего случая, при котором система даже при маловероятном сочетании поражающих факторов должна исключать появление потенциально опасной ситуации;
- организация непрерывного контроля функционирования устройств в процессе эксплуатации;
- осуществление непрерывного мониторинга состояния устройств системы методами диагностики.

3.2. Методы обеспечения безопасности весьма разнообразны, но могут быть сведены к двум основным принципам.

Первый принцип связан с созданием систем и устройств СЦБ, их узлов и элементов, с введением в них избыточности. Избыточность может быть параметрической (запас прочности), схемной (так называемые безопасные логические элементы, компараторы, ключи и т.д.), структурной или аппаратной (дублирование, троирование и т.д. аппаратных средств, функциональных узлов и элементов), программной (решение задачи двумя независимыми программными продуктами), информационной (кодирование информации внутри системы с последующим декодированием и проверкой ее безошибочности перед использованием), временной (увеличение времени восприятия или выдачи воздействия), комбинированной (при использовании нескольких из перечисленных методов). Требования безопасности накладывают дополнительные условия на комплектующие изделия и материалы, на конструкцию, на схемные решения и структуру системы, на представление информации в ней и т.д.

В соответствии со **вторым принципом** обеспечение безопасности достигается применением средств, локализующих развитие неблагоприятных процессов, защищающих систему от выдачи неправильных воздействий, предупреждающих о возможном наступлении экстремальных ситуаций, управляющих функционированием объекта в критических случаях (парирующих развитие отказа и переводящих объекты управления в защитное состояние). Для этих целей используются контролирующие и диагностирующие устройства, которые оценивают значения выходных параметров системы и значения специальных диагностических признаков, а в необходимых случаях и окружающей среды (вибрации, температура, электромагнитная обстановка и др.). Сравнение измеренных сигналов с их заданными значениями, обработка информации и принятие решения о необходимых действиях для предотвращения аварийной ситуации должны осуществляться устройствами, которые сами

обладают высокой достоверностью, т.е., в данном случае, отвечающих требованиям безопасности.

Естественно, возможно и одновременное использование обоих методов реализации требований безопасности при построении одной системы.

3.3. Требования к средствам управления движением поездов с учетом безопасности должны заключаться в следующем:

- вероятность появления потенциально опасной ситуации, а тем более аварии, по вине самих технических средств должна быть минимальной, не выше заданной;
- при возникновении потенциально опасной ситуации система должна парировать ее (переходить в защитное состояние).

3.4. Проблемы безопасного функционирования систем и устройств управления, к которым можно отнести и системы и устройства СЦБ, рассматриваются в международных стандартах, в соответствии с которыми вводится следующие понятия:

- система, связанная с безопасностью;
- функция безопасности и полнота безопасности;
- уровень полноты безопасности;
- состояния безопасности;
- отказы.

Система, связанная с безопасностью, обеспечивает выполнение функций безопасности, необходимых для достижения или поддержания безопасного состояния объекта управления, и предназначена для достижения необходимой полноты безопасности – самостоятельно или совместно с другими связанными с безопасностью средствами, как встроенными в систему, так и внешними по отношению к ней, в том числе средствами снижения риска. Необходимо отметить, что система, связанная с безопасностью, включает в себя не только аппаратные средства, но и программное обеспечение, кроме того, человек – оператор также может являться частью такой системы. При этом под средствами снижения риска понимаются специальные меры, предпринимаемые без использования систем, связанных с безопасностью.

Функция, реализуемая связанной с безопасностью системой, целью которой является обеспечение или поддержание безопасного состояния применительно к конкретному опасному состоянию называется *функцией безопасности*.

Полнота безопасности – это уровень удовлетворительного выполнения системой, связанной с безопасностью, требуемых функций безопасности при всех заданных условиях в течение заданного периода времени. Чем выше *уровень полноты безопасности* систем, связанных с безопасностью, тем меньше вероятность отказа этих систем при выполнении ими требуемых функций безопасности. При определении полноты безопасности учитываются все причины отказов, ведущих к опасному состоянию (отказы аппаратуры, программного обеспечения, электромагнитное влияние и др.), многие из них могут быть оценены количественными показателями, но для ряда факторов возможна лишь их качественная оценка.

Состояния безопасности включают исправное (выполняются все требования нормативно-технической документации), неисправное (не обеспечивается выполнение хотя бы одного требования нормативно-

технической документации), работоспособное (выполняются все требования нормативно-технической документации, характеризующие способность выполнять заданные функции), неработоспособное (значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно-технической документации), защитное (выполняются все предусмотренные функции безопасности, реализуемые, например, путем отключения от объекта управления), опасное (неработоспособное состояние, при котором не выполняется хотя бы одна функция безопасности), неопасное (работоспособное и защитное состояния). Естественно, защитное состояние может быть только в системах, связанных с безопасностью.

Отказ – это событие, заключающееся в нарушении работоспособного состояния системы. Отказы в свою очередь могут быть защитными (при попадании системы в защитное состояние), опасными (при нарушении работоспособного или защитного состояний).

В стандарте МЭК 61508 (аналогично стандартам CENELEC EN50126, EN 50128, EN50129) приводятся четыре уровня полноты безопасности (УПБ, Safety Integrity Level – SIL), приведенные в табл. 3.1. УПБ 1 достигается относительно при применении на всех стадиях разработки и производства требований стандартов качества. Для обеспечения УПБ 2 требуется большее число проверок и испытаний, что приводит к повышению стоимости системы. Для достижения УПБ 3 требуются более существенные усилия и более высокая компетенция разработчиков, чем в случаях УПБ 1 и УПБ 2. УПБ 4 требует проведения разработки с применением специальных правил и формальных методов доказательства безопасности. Стоимость проекта будет предельно большой и при создании потребуется исключительно высокая компетентность. В ряде случаев удается избегать применения УПБ 4, дополнительно используя уровни защиты.

Таблица 3.1

Уровень полноты безопасности	При высокой интенсивности запросов (опасных отказов в час)	При низкой интенсивности запросов (вероятность отказа)
УПБ 4	$\geq 10^{-9}$ до $< 10^{-8}$	$\geq 10^{-5}$ до $< 10^{-4}$
УПБ 3	$\geq 10^{-8}$ до $< 10^{-7}$	$\geq 10^{-4}$ до $< 10^{-3}$
УПБ 2	$\geq 10^{-7}$ до $< 10^{-6}$	$\geq 10^{-3}$ до $< 10^{-2}$
УПБ 1	$\geq 10^{-6}$ до $< 10^{-5}$	$\geq 10^{-2}$ до $< 10^{-1}$

3.5. Для систем и устройств СЦБ безопасность выступает как одно из основных свойств этих систем, характеризующих их качество наряду с понятиями, составляющими характеристики надежности: безотказность, долговечность, ремонтопригодность и сохраняемость.

В данной Памятке безопасность рассматривается как свойство системы или устройства СЦБ, связанное с их поведением при отказах технических средств, входящих в них. Безопасность движения поездов является более широким понятием, поскольку она может быть нарушена и при исправном состоянии систем и устройств СЦБ в результате неправильных действий человека-оператора, отказов других объектов железнодорожного транспортного

комплекса, катастрофических природных явлений и по другим внешним по отношению к системе СЦБ причинам.

В опасное состояние система может перейти в результате воздействия электромагнитных помех, возникновения внезапных, постепенных и перемежающихся отказов аппаратных и программных средств. При этом происходит нарушение работоспособного и защитного состояния, 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/или от действий человека оператора.

3.6. Для систем, связанных с безопасностью, применяют несколько количественных показателей безопасности. На железнодорожном транспорте распространены следующие показатели: интенсивность опасных отказов, вероятность опасных отказов, вероятность безопасной работы за заданное время, средняя наработка до опасного отказа и другие. Определение значений этих параметров возможно на основе статистической обработки результатов экспериментов, расчетным путем или с помощью моделирования. Необходимо учитывать, что появление опасного отказа – редкое событие, и для определения его вероятностных параметров экспериментальными методами потребуется время, значительно превышающее время жизни исследуемого устройства. Кроме того, появление такого редкого события, как опасный отказ, нельзя описывать известными законами распределения случайных событий, поддающимися аналитическим исследованиям, а, следовательно, расчетные методы для получения всех перечисленных характеристик безопасности не могут быть адекватны фактическим параметрам устройства.

Математическое моделирование процессов появления опасных отказов является мощным инструментом исследования устройств и систем управления на соответствие требованиям безопасности, но для его реализации необходимо создание соответствующего математического описания объекта исследования – процесса появления опасных отказов, что не может быть реализовано в силу высказанных выше причин.

При выборе значений 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 желательно, 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.

Таким образом, показателем безопасности технических средств, достаточно полно отражающим количественные характеристики, является интенсивность опасных отказов. На практике этот показатель может быть получен расчетным путем, при этом, как правило, получается верхняя оценка этой величины.

3.7. Требования безопасности систем и устройств СЦБ подразделяют на количественные и качественные. Количественные требования могут быть детерминированными и вероятностными. Количественные требования задают в

виде групповых и индивидуальных норм. Групповые нормы устанавливаются для совокупности устройств СЦБ данного типа (вида, марки, модели), индивидуальные – для единичного устройства СЦБ данного типа (вида, марки, модели).

3.8. Определение нормируемых показателей безопасности производится на основе концепции приемлемого риска. Частными случаями применения данной концепции являются:

- 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;
- расчет норм безопасности на основе соотношения между затратами на обеспечение безопасности и ее эффективностью;
- расчет норм безопасности на основе концепции замещения рисков; в этом случае показатели безопасности вновь разрабатываемых систем и устройств СЦБ не должны быть ниже аналогичных показателей замещаемых устройств.

3.9. Методы контроля показателей безопасности в зависимости от способа получения исходных данных подразделяют на расчетные, экспериментальные и расчетно-экспериментальные.

3.10. Организация-разработчик системы или устройства СЦБ должна представить документ «Доказательство безопасности» (Safety Case), который подготавливается при разработке системы и на стадии ее проектирования. Этот документ является основой для разработки конструкции системы, ее структуры и схем отдельных узлов, алгоритмического и программного обеспечения, т.е. разработки безопасной системы, устойчивой к возникновению «нештатных» ситуаций. Для этого необходимо:

- провести анализ возможности возникновения аварийной ситуации, рассмотреть и описать сценарии их развития, классифицировать возможные последствия аварий, установить вероятности получения каждой степени поражения;
- установить перечень выходных параметров системы, которые претерпевают существенные изменения в процессе аварии. По возможности выявить те показатели, изменение которых предшествует критическому состоянию и по изменению значения которых можно предотвратить (прогнозировать) возможность аварии;
- установить потенциально опасные узлы и элементы системы, нарушение работоспособности которых может иметь недопустимые последствия;
- установить предельно допустимые условия эксплуатации и режимы работы системы. Оценить возможную продолжительность работы системы в экстремальных условиях, в том числе при потере работоспособности ее отдельных узлов и элементов;
- рассмотреть возможные действия пользователей системы и обслуживающего ее персонала и проработать способы защиты от их ошибок (как умышленных, так и неумышленных), которые могли бы привести к недопустимым последствиям.

В документе «Доказательство безопасности» разработчиком в письменной

форме обосновываются показатели безопасности, удовлетворяющие требованиям, предъявляемым к системам и устройствам СЦБ данного класса или определенным в нормативных документах. Согласование и оценка документа «Доказательство безопасности» производится независимым аккредитованным органом.

3.11. Процесс доказательства безопасности, а следовательно, и документ «Доказательство безопасности», отражающий результат этого процесса, должен состоять из теоретической и экспериментальной частей, являющихся результатом мероприятий, проводимых в процессе разработки, изготовления, проектирования, монтажа и эксплуатации системы или устройства СЦБ.

3.12. Перед введением в эксплуатацию системы или устройства СЦБ необходимо провести проверку выполнения требований условий безопасности.

4. Количественные требования безопасности

4.1. На основании обработки статистических данных о безопасности систем и устройств СЦБ получены значения вероятностных показателей безопасности основных систем СЦБ на условный измеритель, которые в соответствии с концепцией замещения рисков принимаются за нормированные.

В качестве критерия допустимости риска для технических средств систем и устройств СЦБ устанавливается допустимая интенсивность опасных отказов с нормой (уровнем) не более $1x10^{-9}$ 1/ч (в степени минус девятой за час эксплуатации для случайных отказов) на каждую составную часть системы управления движением поездов.

Значение критерия допустимости риска для технических средств систем ЖАТ является граничным, т.е. риски с более высокой частотой появления угроз или с более высокой значимостью их последствий должны считаться недопустимыми.

Критерий допустимости риска принят равным эталонному значению критерия допустимости риска для технических систем RAC-TS (Risk Acceptance Criterion for Technical Systems), принятому на железных дорогах Европейского Сообщества. Критерий RAC-TS определен следующим образом: любой функциональный отказ, обладающий вероятным потенциалом непосредственного несчастного случая с катастрофическими последствиями, не должен происходить чаще указанного значения. Под вероятным потенциалом понимается то, что возникновение данного функционального отказа должно сопровождаться вероятностью непосредственного несчастного случая с катастрофическими последствиями, т.е. отсутствуют или почти отсутствуют какие-либо препятствия, способные предотвратить несчастный случай.

Единица измерения критерия – один час эксплуатации, непосредственно связанная с функцией составной части, в которой происходит отказ.

4.2. В качестве порога пренебрежимости риска для технических средств систем и устройств СЦБ устанавливается величина не более $5x10^{-12}$ 1/ч (в степени минус двенадцатой за час эксплуатации для случайных отказов) на каждую составную часть системы управления движением поездов.

4.3. Для технических средств систем и устройств СЦБ на станциях и перегонах железнодорожных линий должна быть установлена категория опасности (угрозы) в зависимости от потенциальных последствий транспортных

происшествий и иных, связанных с нарушением правил безопасности движения, событий в соответствии с табл. 4.1.

Таблица 4.1

Категория опасности (угрозы)	Потенциальные последствия:	
	для людей и экологии	другие
Катастрофическая	Крушение поездов	
Критическая	Авария 1	Авария 2
Граничная	Авария 3	Авария 4
Незначительная	Событие 1	Событие 2

В табл. 4.1. приняты следующие понятия:

Крушение поездов – транспортное происшествие (например, сходы, столкновение поездов, наезды на препятствия и др.), в результате которого погибли и/или получили тяжкие телесные повреждения люди и/или нанесен значительный ущерб экологии.

Авария 1 – транспортное происшествие, в результате которого погиб человек и/или получили тяжкие телесные повреждения пять и более человек и/или пострадало здоровье десяти и более человек и/или нарушены условия жизнедеятельности ста и более человек и/или нанесен существенный ущерб экологии.

Авария 2 – транспортное происшествие, в результате которого повреждены жизненно важные системы и/или локомотивы и вагоны до степени исключения их из инвентаря.

Авария 3 – транспортное происшествие, в результате которого есть легкораненые и/или пострадавшие люди и/или возникла существенная угроза экологии.

Авария 4 – транспортное происшествие, в результате которого повреждены железнодорожные системы и/или локомотивы и вагоны до степени, когда для восстановления их исправного состояния требуется капитальный ремонт и/или допущены события, связанные с нарушением правил безопасности движения (столкновение или сход поезда без трагических последствий; перевод стрелки под поездом; проезд запрещающего сигнала светофора; прием поезда на занятый путь; отправление встречного поезда на занятый перегон; прием или отправление поезда по неустановленному и незамкнутому маршруту).

Событие 1 – транспортное происшествие, в результате которого возможны незначительные ранения и/или угрозы здоровью людей и/или допущены действия, вводящие в заблуждение граждан (пассажиров, пешеходов, работников, водителей других транспортных средств и т.п.).

Событие 2 – транспортное происшествие, в результате которого возможны нарушения конструкций инфраструктуры и/или поезда, перерывы движения на один час и более и/или допущены события, связанные с нарушением правил безопасности движения (несанкционированный или не единоличный доступ к управлению самоходным подвижным составом или объектом инфраструктуры; превышение установленной скорости движения на участке постоянного или временного ограничения скорости; отсутствие

замкнутого маршрута для поезда на расстоянии меньшем его тормозного пути экстренного торможения при максимальной установленной скорости; самопроизвольный выход подвижного состава на маршруты следования поездов; несанкционированная принудительная остановка или отмена принудительной остановки поезда; ложное появление на светофоре (локомотивном или напольном) более разрешающего показания; смена направления движения на пути перегона при его фактической занятости; установка враждебного маршрута или открытие светофора враждебного маршрута; открытие светофора для неустановленного и незамкнутого маршрута; перевод стрелки, замкнутой в маршруте; размыкание маршрута или части маршрута во время его фактического использования; взрез стрелки.

4.4. Взаимосвязь вероятностных показателей безопасности определяется следующими формулами:

наработка до опасного отказа

$$T_{оп} = \frac{1}{\lambda_{оп}};$$

вероятность безопасной работы

$$P_{б(t)} = e^{-\lambda_{оп} \cdot t}.$$

4.5. Для систем ДЦ вероятность трансформации и возникновения ложной ответственной команды телеуправления должна быть не более 10^{-14}.

4.6. Интенсивность опасных отказов аппаратуры передачи и реализации ответственных команд должна быть не более $\lambda = 3 \cdot 10^{-11}$ 1/ч на одну команду.

5. Средства контроля обеспечения безопасности

5.1. Контроль обеспечения безопасности должен осуществляться в виде организационных и технических мероприятий, проводимых на всех стадиях жизненного цикла системы и устройства СЦБ (при разработке, изготовлении, проектировании, монтаже и эксплуатации).

5.2. В процессе разработки систем и устройств СЦБ параллельно с разработчиками проводится экспертиза на безопасность предлагаемых технических решений независимыми экспертными организациями (испытательными лабораториями, органами по сертификации).

5.3. Для подтверждения (контроля) безопасности в испытательных лабораториях проводятся испытания на функциональную безопасность образцов или моделей систем и устройств СЦБ, а также в условиях воздействия электромагнитных помех.

5.4. Испытания систем и устройств СЦБ проводятся при воздействии:

- климатических факторов;
- механических факторов;
- отказов аппаратных средств и ошибок в программных средствах;
- электромагнитных помех:
  - наносекундных, действующих в сети электропитания, в цепях заземления и ввода-вывода;
  - микросекундных, большой энергии в цепях электропитания;
  - динамических изменений (провалов и выбросов) напряжения

в сети электропитания;

- электростатических разрядов;
- других видов помех, установленных в нормативной и конструкторской документации на изделие.

Испытания систем и устройств СЦБ на безопасность проводят с помощью стандартных (измерительные приборы, вибростенды, камеры тепла и холода и т.п.) и нестандартных средств (имитаторы отказов, электромагнитных помех, технологических ситуаций и т.п.).

До начала испытаний средства проведения испытаний подлежат проверке, паспортизации и аттестации.

Применяемые нестандартные средства имитации должны удовлетворять следующим требованиям: адекватности моделируемому объекту, процессу или источнику информации; инструментальной точности средств, реализующих имитатор внешней среды; статистической точности процесса имитации и объему тестовых данных, учитываемых при статистическом обобщении результатов тестирования; точности дискретизации имитатором непрерывных процессов моделируемых объектов.

5.5. Испытания систем и устройств СЦБ проводят на основании утвержденных установленным образом программ и методик, а результаты испытаний оформляются в виде протоколов для каждого вида испытания. На основании протоколов испытаний составляется общее заключение о соответствии системы или устройства СЦБ предъявляемым к ней требованиям.

6. Состав документа «Доказательство безопасности»

6.1. Результаты контроля обеспечения безопасности при разработке фиксируются в документе «Доказательство безопасности», представляемым разработчиком или изготовителем системы или устройства.

6.2. Доказательство безопасности систем и устройств СЦБ основывается на:

- экспертных методах;
- расчетных методах;
- испытаниях на машинных моделях;
- стендовых испытаниях;
- испытаниях систем СЦБ в условиях эксплуатации;
- сборе и обработке статистических данных об отказах в условиях эксплуатации (корректируется и учитывается при последующей эксплуатации).

6.3. Документ «Доказательство безопасности» должен содержать:

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

- заключение по безопасности;
- список использованных источников.

6.4. 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.

6.5. В разделе «Нормативные документы, используемые для доказательства безопасности» приводится перечень международных, национальных или отраслевых документов, которые регламентируют содержание и структуру доказательства безопасности.

6.6. Характеристика объекта должна содержать:

- концепцию обеспечения безопасности;
- требования и нормы безопасности;
- критерии опасных отказов;
- краткое описание принципов построения и работы;
- описание конструктивного оформления.

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

6.8. В разделе «Методы доказательства безопасности» приводится перечень используемых методов доказательства безопасности и определяются цели их использования.

Применяемые методы используются для доказательства:

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

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

6.10. В разделе "Программа и методика испытаний" приводится описание нетиповых (оригинальных) программ и методик. При использовании типовых

или ранее утвержденных программ и методик допускается не приводить их в доказательстве безопасности, а привести ссылку на них.

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

6.12. В разделе "Подтверждение безопасности, результаты испытаний и экспертизы" приводятся протоколы и акты различных видов испытаний и экспертные заключения. В этом разделе требуется доказать, что соблюдается основной принцип безопасности систем и устройств СЦБ – одиночный отказ не должен приводить систему в опасное состояние. Это доказательство осуществляется на основании перечня отказов, возможных в данном типе аппаратуры.

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

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

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

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

6.16. Доказательство безопасности содержит оценку адекватности испытаний условиям эксплуатации, которая зависит от реальных ограничений (класс рассматриваемых отказов, время испытаний, точность измерений и т.д.). В доказательстве безопасности отдельных частей системы допускается делать ссылки на известные доказательства безопасности при условии полной идентичности части устройства и ее связей этому доказательству.

6.17. С учетом специфики систем и устройств СЦБ возможно исключение некоторых видов доказательства безопасности. При этом должно быть приведено обоснование, которое является составной частью доказательства безопасности.