ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54899— 2012

СИСТЕМЫ ДИСПЕТЧЕРСКОЙ ЦЕНТРАЛИЗАЦИИ И ДИСПЕТЧЕРСКОГО КОНТРОЛЯ ДВИЖЕНИЯ ПОЕЗДОВ

Требования безопасности и методы контроля

Издание официальное

Москва
Стандартинформ
2012

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным образовательным учреждением высшего профессионального образования «Петербургский государственный университет путей сообщения» (ФГОУ ВПО «ПГУПС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 45 «Железнодорожный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 апреля 2012 г. № 58-ст

4 В настоящем стандарте реализованы требования технического регламента «О безопасности инфраструктуры железнодорожного транспорта» в части требований к системам диспетчерской централизации и диспетчерского контроля движения поездов:

- подразделы 4.1—4.7 содержат минимально необходимые требования безопасности;
- подразделы 5.2—5.4 устанавливают методы проверки минимально необходимых требований безопасности для осуществления оценки соответствия

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2012

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины, определения и сокращения . . . 1
3.1 Термины и определения . . . 1
3.2 Сокращения . . . 2
4 Требования безопасности . . . 2
4.1 Функции, реализуемые системами диспетчерской централизации и диспетчерского контроля . . . 2
4.2 Требования к реализации функций телесигнализации в системах диспетчерской централизации и диспетчерского контроля . . . 3
4.3 Требования к реализации функций телеуправления диспетчерской централизации . . . 4
4.4 Ответственные команды телеуправления диспетчерской централизации . . . 4
4.5 Требования к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля . . . 5
4.6 Требования к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля . . . 6
4.7 Критерии опасных отказов систем диспетчерской централизации и диспетчерского контроля . . . 6
5 Методы контроля . . . 7
5.1 Общие положения . . . 7
5.2 Контроль требований безопасности к функциям, реализуемым диспетчерской централизацией и диспетчерским контролем . . . 8
5.3 Контроль требований безопасности к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля . . . 9
5.4 Контроль требований безопасности к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля . . . 9
Библиография . . . 11

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ДИСПЕТЧЕРСКОЙ ЦЕНТРАЛИЗАЦИИ И ДИСПЕТЧЕРСКОГО КОНТРОЛЯ ДВИЖЕНИЯ ПОЕЗДОВ

Требования безопасности и методы контроля

Centralised traffic and dispatching control systems movement of trains.
Safety requirements and methods of checking

Дата введения — 2013—01—01

1 Область применения

Настоящий стандарт распространяется на системы диспетчерской централизации и диспетчерского контроля движения поездов.

Настоящий стандарт устанавливает функции и условия безопасного функционирования систем диспетчерской централизации и диспетчерского контроля движения поездов, значения параметров, обеспечивающих их безопасность, критерии опасных отказов, а также требования к аппаратно-программным средствам диспетчерской централизации и диспетчерского контроля.

Настоящий стандарт применяют при разработке, проектировании и изготовлении аппаратных и программных средств диспетчерской централизации и диспетчерского контроля движения поездов и оценке соответствия вновь разрабатываемых и импортируемых систем диспетчерской централизации и диспетчерского контроля требованиям безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 8.563—2009 Государственная система обеспечения единства измерений. Методики (методы) измерений

ГОСТ Р 8.654—2009 Государственная система обеспечения единства измерений. Требования к программному обеспечению средств измерений. Основные положения

ГОСТ Р 53431—2009 Автоматика и телемеханика железнодорожная. Термины и определения

ГОСТ 26.005—82 Телемеханика. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 53431, ГОСТ 26.005, а также следующие термины с соответствующими определениями:

Издание официальное

3.1.1 **комбинированное управление станцией:** Режим управления железнодорожной станцией на участке диспетчерской централизации, при котором поездной диспетчер управляет движением железнодорожных поездов по главным и боковым путям для безостановочного пропуска поездов, а по остальным железнодорожным путям, изолированным охранным положением стрелок, управление движением осуществляет дежурный по железнодорожной станции (маневровый диспетчер).

3.1.2 **полигон диспетчерского управления:** Зона управления перевозочным процессом, интегрированная в диспетчерском центре по технологическим соображениям.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

АБ — автоматическая блокировка;

ДК — диспетчерский контроль;

ДЦ — диспетчерская централизация;

ЖАТ — железнодорожная автоматика и телемеханика;

ТС — телесигнализация;

ТУ — телеуправление;

ЭЦ — электрическая централизация стрелок и сигналов.

4 Требования безопасности

4.1 Функции, реализуемые системами диспетчерской централизации и диспетчерского контроля

4.1.1 Системы ДЦ и ДК должны обеспечивать выполнение следующих функций телесигнализации:

- сбор и отображение для поездного диспетчера в реальном времени данных о состоянии всех объектов, контролируемых системами ЭЦ и АБ участка железнодорожной линии;
- автоматизированная передача информации, преобразованной в нужную форму, операторам вышестоящего и смежного уровней управления движением железнодорожных поездов (далее — поезда);
- фиксация и выдача актуальной информации по объектам путевого развития и железнодорожному подвижному составу (далее — подвижной состав);
- двустороннее информационное взаимодействие с локомотивными устройствами безопасности по индуктивному каналу или радиоканалу;
- обеспечение требуемой достоверности при передаче информации и защиты от внешних влияний;
- автоматическое ведение графика исполненного движения поездов и приложения к нему;
- расчет ожидаемого времени проследования поездов по станциям участка железнодорожной линии;
- выявление возможных конфликтных ситуаций в организации движения поездов;
- расчет и корректировка прогнозного графика движения поездов;
- формирование диспетчерских приказов и предупреждений;
- ведение диспетчерского журнала;
- протоколирование эксплуатационных событий с возможностью воспроизведения архивированных данных;
- логический анализ эксплуатационных событий и действий персонала;
- диагностирование и оценка состояния технических средств ЖАТ;
- автоматизированный учет показателей движения поездов и производимых работ;
- контроль выполнения технологических этапов перевозочного процесса на участке железнодорожной линии;
- слежение за перемещениями подвижных средств и организация динамических моделей поездного, локомотивного, вагонного положений на участке железнодорожной линии;
- формирование и выдача сведений о поезде:
  - номер поезда,
  - местоположение,
  - длина состава,
  - вес поезда,
  - натурные листы,
  - разложение по дорогам назначения и плану формирования,

- история поезда;
- формирование и выдача сведений о локомотиве:
  - серия и номер,
  - депо приписки,
  - фактическое местоположение,
  - история,
  - учет времени по прибытию и отправлению,
  - расчет простоя,
  - подвязка бригад локомотивов к ниткам графика движения поездов,
  - плановые сроки обслуживания и ремонта;
- формирование и выдача сведений о вагонах:
  - идентификационный номер,
  - местоположение,
  - состояние,
  - вагонный лист;
- формирование нормативно-справочной информации и запросов в смежные системы;
- продвижение по участку номера поезда после ввода в систему с пульта поездного диспетчера, со средств идентификации или трансляции со смежного участка;
- фиксация изменений в состоянии контролируемых объектов и формирование соответствующих сообщений;
- контроль единого времени и актуальности используемой информации.

4.1.2 Системы ДЦ должны обеспечивать выполнение следующих функций телеуправления:

- диспетчерское управление поездной работой на участках, линиях, направлениях;
- диспетчерское управление движением высокоскоростных поездов на участках железнодорожных линий с совмещенным движением поездов;
- диспетчерское управление маневровой работой на железнодорожных станциях (далее — станции) диспетчерского участка;
- передачу управления станцией диспетчерского участка на автономное управление дежурным по станции как при исправных средствах телемеханики, так и в случае их отказа;
- передачу группы объектов ЭЦ станции диспетчерского управления на местное управление составителю поездов;
- перевод станции на комбинированное управление, когда на автономной станции главные пути и пути безостановочного пропуска остаются в управлении поездного диспетчера;
- изменение режимов управления станцией, районом, объектом участка (режимы управления: диспетчерское, станционное автономное, местное) с сохранением единоначалия в любой момент времени;
- изменение границ зоны управления с рабочего места (поездного диспетчера, дежурного по станции, оператора местного управления) с соблюдением принципа единоначалия;
- формирование команд управления объектами ЭЦ и АБ в разных эксплуатационных режимах (индивидуальное управление объектами, маршрутное управление, автоматическое управление по накопленной программе);
- передача и контроль реализации команд управления объектами ЭЦ и АБ;
- формирование управляющих команд с исключением использования устаревшей информации о состоянии объектов;
- формирование ответственных команд (по утвержденному перечню) с обеспечением их безопасной реализации системами ЭЦ и АБ;
- автоматическое двукратное реверсирование стрелочного электропривода и возвращение остряков централизованной стрелки в исходное состояние в случае отсутствия контроля требуемого положения этой стрелки в заданное время;
- формирование команды экстренной остановки движения локомотива;
- формирование команд управления заградительными сигналами.

4.2 Требования к реализации функций телесигнализации в системах диспетчерской централизации и диспетчерского контроля

Для организации безопасного движения поездов аппаратура каналов ТС в системах ДЦ и ДК должна обеспечивать:

- отображение для поездного диспетчера в реальном времени (не нарушая хронологии событий и с задержкой по времени не более 6 с) данных о состоянии всех объектов, контролируемых системами ЭЦ и АБ участка железнодорожной линии;
- автоматическое преобразование исходной информации в нужную форму при передаче сообщений операторам вышестоящего и смежного уровней системы управления перевозочным процессом;
- исключение использования поездным диспетчером неактуальной информации для управления движением в случае задержки передачи сообщений по каналу ТС более чем на 1 мин;
- протоколирование эксплуатационных событий с возможностью воспроизведения архивированных данных в течение 10 сут;
- контроль непрерывности связи по каналу ТС с требуемой достоверностью приема сообщений;
- гальваническую развязку входных цепей устройств сопряжения с контролируемыми устройствами ЖАТ;
- вероятность трансформации сигнала ТС более 10^{-8};
- вероятность потери информации в канале ТС не более 10^{-8};
- вероятность ложного контрольного сообщения при отсутствии передачи не более 10^{-12};
- время готовности системы ДЦ и ДК к работе при включении питания не более 3 мин.

4.3 Требования к реализации функций телеуправления диспетчерской централизации

В системах ДЦ при организации телеуправления объектами ЖАТ необходимо в целях обеспечения безопасности движения железнодорожных поездов обеспечивать:

- разграничение и изменение зон управления между операторами таким образом, чтобы в любой момент правом управления тем или иным объектом обладал только один оператор (соблюдение принципа единоначалия);
- передачу возможности управления тем или иным объектом другому оператору по установленной процедуре с регистрацией согласованных действий операторов;
- перевод железнодорожной станции со станционного управления на диспетчерское должен происходить при выполнении следующих условий:

а) наличие в замках аппаратов управления ключей-жезлов;

б) отсутствие начавшейся реализации ответственных команд;

в) отсутствие блокированных объектов;

г) отсутствие централизованных стрелок, выключенных из зависимостей;

- перевод железнодорожной станции с диспетчерского управления в режим станционного управления должен осуществляться дежурным железнодорожной станции по команде от поездного диспетчера;
- исключение использования устаревшей информации о состоянии объектов для формирования управляющих команд;
- использование режима накопления маршрутов и программного управления только для станций участка, оборудованных устройствами ЭЦ с защитой от преждевременного размыкания централизованной стрелки при кратковременном нарушении шунтирования рельсовой цепи стрелочной секции маршрута;
- время реакции системы ДЦ на управляющее воздействие оператора автоматизированного рабочего места должно быть не более 500 мс;
- время от момента ввода команды до начала ее реализации объектом управления должно быть не более 1 с;
- время хранения на контролируемом пункте предварительной части ответственной команды в ожидании исполнительной части команды управления объектом должно быть не более 30 с;
- длительность формирования серии посылок исполнительной части ответственной команды управления объектом (при спорадической передаче сигналов ТУ) должна быть не более 3 мин с интервалом между посылками серий не более 15 с;
- исключение формирования других команд ТУ во время посылки ответственной команды;
- вероятность трансформации сигнала ТУ не более 10^{-14};
- вероятность потери информации в канале ТУ не более 10^{-10};
- вероятность генерации ложной команды ТУ при отсутствии передачи 10^{-12};
- интенсивность опасных отказов технических средств передачи и реализации ответственных команд не более $3 \cdot 10^{-11}$ 1/ч на одну команду.

4.4 Ответственные команды телеуправления диспетчерской централизации

4.4.1 Для обеспечения непрерывности перевозочного процесса при возникновении некоторых неисправностей в устройствах ЖАТ должен использоваться вспомогательный режим управления

объектами путем передачи ответственных команд ТУ. Ответственная команда ТУ предполагает управляющее воздействие на объект ЖАТ с исключением схемной проверки отдельных блокировочных зависимостей, обеспечивающих безопасность движения железнодорожных поездов.

Использование вспомогательного режима допустимо только после проверки на месте работником службы перевозок или другим уполномоченным лицом фактического состояния соответствующего неисправного объекта ЖАТ (железнодорожного стрелочного перевода, изолированного участка, станционных железнодорожных путей, железнодорожного перегона, переезда, поезда и т. д.). Передача ТУ во вспомогательном режиме должна быть санкционирована ответственным лицом, назначенным руководителем единой диспетчерской смены дорожного центра управления перевозками. При этом ответственное лицо должно убедиться, что поездной диспетчер располагает достаточной информацией для безопасного применения вспомогательного режима.

4.4.2 Автоматизированная система диспетчерского управления движением поездов должна обеспечивать возможность передачи на контролируемые пункты станций зоны диспетчерского управления следующих ответственных команд:

- вспомогательная смена направления движения по пути перегона, оборудованного двухсторонней автоматической блокировкой (или автоматической блокировкой в одном направлении и автоматической локомотивной сигнализацией в другом), при занятом состоянии пути железнодорожного перегона;
- вспомогательный режим подачи сигнала прибытия железнодорожного поезда в полном составе на железнодорожную станцию на участках железнодорожных линий, оборудованных полуавтоматической блокировкой с устройством автоматического контроля свободности перегона, при ложно занятом состоянии пути железнодорожного перегона;
- вспомогательный перевод железнодорожных стрелок при ложно занятом состоянии изолированного участка железнодорожного пути;
- искусственное размыкание железнодорожных стрелок при разрешении движения железнодорожного поезда под запрещающее сигнальное показание железнодорожного светофора;
- искусственное размыкание замкнутых в маршруте изолированных участков железнодорожного пути;
- вспомогательное открытие железнодорожного переезда, расположенного в пределах железнодорожной станции;
- вспомогательное отключение устройства контроля схода подвижного состава из схемы включения разрешающего сигнального показания входного светофора при его ложном срабатывании;
- вспомогательная отмена режима пропуска скоростного и высокоскоростного поезда, размыкание железнодорожных блок-участков, участков удаления, принудительной остановки локомотива и отмены принудительной остановки.

4.5 Требования к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля

4.5.1 Конструкция аппаратных средств систем ДЦ и ДК, предназначенных для размещения около железнодорожных путей (напольное оборудование железнодорожной автоматики и телемеханики), должна отвечать требованиям габарита железнодорожного подвижного состава и габарита приближения строений.

4.5.2 Технические средства систем ДЦ и ДК должны выполнять свои функции во всех предусмотренных при их разработке и (или) проектировании условиях и режимах, не создавая при этом препятствий для функционирования как других технических средств ЖАТ, так и остальных объектов инфраструктуры железнодорожной линии.

4.5.3 Параметры быстродействия систем ДЦ и ДК должны обеспечивать выполнение всех предусмотренных функций в заданном диапазоне скоростей и характеристик железнодорожных подвижных составов.

4.5.4 В соответствии с проектом по оборудованию участка железнодорожной линии технические средства систем ДЦ и ДК должны быть функционально, информационно и технически совместимыми с системами:

- ЖАТ на станциях;
- ЖАТ на перегонах железнодорожных линий;
- контроля технического состояния подвижного состава (средства автоматического контроля технического состояния подвижного состава на ходу поезда, устройство контроля схода подвижного состава, контрольно-габаритные устройства);
- идентификации и определения местоположения железнодорожного подвижного состава;

- контроля состояния устройств ограждения и закрепления железнодорожного подвижного состава, устройств переездной, мостовой, тоннельной, обвальной и других сигнализаций;

- информационными системами смежных и более высоких уровней управления перевозочным процессом.

4.5.5 Технические средства систем ДЦ и ДК должны обеспечивать безопасный интерфейс с другими системами ЖАТ, действующими на данном участке железнодорожной линии или иметь возможность интегрировать функции этих систем.

4.6 Требования к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля

4.6.1 Аппаратные и программные средства ДЦ и ДК должны быть разработаны, спроектированы и изготовлены таким образом, чтобы во всех режимах работы при соблюдении всех требований, установленных в эксплуатационной документации, обеспечивалась реализация всех функций по обеспечению безопасности движения поездов (см. 4.1) в течение установленного срока службы.

4.6.2 Одиночный отказ, допустимая последовательность отказов аппаратных средств ДЦ и ДК должны обнаруживаться с заданной вероятностью на рабочих и тестовых воздействиях не позднее чем в системе возникнет последующий отказ.

После обнаружения отказа, допустимой последовательности отказов система ДЦ или ДК должна переходить в необратимое защитное состояние.

4.6.3 Если концепцией построения программно-аппаратных средств ДЦ и ДК допускается накопление отказов, которые не обнаруживаются в процессе эксплуатации, то вероятность возникновения опасного отказа по причине их накопления за период эксплуатации не должна превышать заданной вероятности опасного отказа.

4.6.4 Программно-аппаратные средства ДЦ и ДК должны обеспечивать восстановление работоспособного состояния из состояния защитного отказа только с участием эксплуатационного персонала.

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

4.6.6 Программные средства, применяемые в ДЦ и ДК, как встраиваемые в аппаратные средства, так и поставляемые на носителях записи, должны:

- обеспечивать корректное выполнение всех функций по обеспечению безопасности движения поездов (см. 4.1);

- быть тестируемыми и диагностируемыми;

- сохранять работоспособность после перезагрузок, вызванных сбоями и отказами аппаратных средств и источников электропитания;

- контролировать целостность программ и данных;

- быть защищены от несанкционированного доступа, от потерь и искажений при хранении, вводе, выводе, возникновении сбоев при обработке информации;

- не иметь свойств и характеристик, не описанных в технической документации на программные средства (недекларированные возможности).

4.7 Критерии опасных отказов систем диспетчерской централизации и диспетчерского контроля

4.7.1 Критериями опасного отказа систем ДЦ и ДК в процессе функционирования ТС являются следующие события:

- нарушение индикации на станционных устройствах отображения при отказах устройств съема информации. Потенциальная угроза безопасности движения поездов возникает при неправильном контроле состояния объектов во вспомогательных режимах управления, когда дежурный по железнодорожной станции пользуется показаниями средств отображения индикации;

- получение устаревших данных ТС после восстановления работоспособности контролируемого пункта или передачи по каналу передачи данных;

- сохранение устаревшей индикации на средствах отображения индикации у поездного диспетчера после прекращения поступления ТС;

- неправильная индикация состояния контролируемых объектов у поездного диспетчера при пользовании ответственными командами или при организации движения поездов по приказам.

4.7.2 Критериями опасного отказа систем ДЦ и ДК при выполнении ими функции ТУ являются:

- реализация на контролируемом пункте ответственной команды при отсутствии или передаче других команд;

- самопроизвольная (несанкционированная) генерация ответственной команды.

4.7.3 Критериями опасного отказа системы ДЦ при выполнении функции ТУ при разделении режимов управления между персоналом являются следующие события:

- возможность реализации команд ТУ (в т. ч. ответственных) от дежурного по железнодорожной станции и поездного диспетчера в случае, когда станция находится на комбинированном управлении, а также вследствие одновременного существования разных режимов управления станцией (диспетчерского и станционного, диспетчерского и резервного);
- возможность реализации команд ТУ (в т. ч. ответственных) от двух поездных диспетчеров при неправильном разграничении зон диспетчерского управления.

5 Методы контроля

5.1 Общие положения

5.1.1 Основными методами контроля систем ДЦ и ДК являются:

а) оценка соответствия системы ДЦ или ДК и ее составных частей требованиям безопасности в форме экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации.

Экспертная оценка на стадии разработки проводится с целью установления:

- полноты и корректности реализации системой функций по обеспечению безопасности движения поездов, установленных заданием на проектирование;
- достаточности и обоснованности технических приемов и мероприятий, которые применены в системе ДЦ или ДК, для реализации положений концепции обеспечения безопасности с целью исключения опасных отказов;
- полноты и корректности программ и методик испытаний;
- полноты и корректности результатов испытаний системы ДЦ или ДК и ее составных частей;
- обоснованности и корректности рассчитанных количественных показателей безопасности.

На стадии изготовления экспертиза проводится с целью оценки полноты и корректности выполнения требований разработчика при изготовлении системы ДЦ или ДК и ее составных частей.

Экспертиза на стадии эксплуатации проводится для оценки показателей безопасности функционирования системы в реальных условиях и режимах эксплуатации, технического обслуживания и ремонта;

б) оценка соответствия системы ДЦ или ДК и ее составных частей требованиям безопасности в форме испытаний.

На этапе разработки целью испытаний является:

- подтверждение соответствия требованиям безопасности элементов системы ДЦ или ДК и программных компонент в форме автономных испытаний. По результатам этих испытаний определяются соответствие полученных характеристик этих элементов требуемым значениям, а также готовность перехода к этапу комплексных проверок;
- проверка корректности взаимодействия между собой частей программ и аппаратуры, интегрированных на данном этапе разработки;
- оценка эффективности системы защиты от сбоев и отказов аппаратных средств;
- проверка работы системы контроля и локализации отказов;
- возможность реконфигурации системы и обеспечения защитного состояния;
- проверка работы системы на стойкость к внешним воздействующим факторам;
- процедуры адаптации системы ДЦ или ДК к полигону внедрения выполнены корректно.

На этапе изготовления испытания проводятся с целью установления возможности обеспечения стабильного качества выпускаемой продукции.

Эксплуатационные испытания проводятся с целью подтверждения заявленных требований безопасности в реальных условиях и режимах эксплуатации, технического обслуживания и ремонта системы ДЦ или ДК;

в) расчетные методы обоснования количественных показателей безопасности системы ДЦ или ДК.

На этапе разработки расчетные методы используются для определения предполагаемого уровня безопасности программно-аппаратных средств системы ДЦ или ДК.

На этапе эксплуатации на основании статистических данных об отказах системы определяется фактический уровень безопасности системы ДЦ или ДК.

5.1.2 Методы контроля выполнения требований безопасности систем ДЦ и ДК должны быть согласованы с этапами разработки, изготовления и эксплуатации систем ДЦ и ДК.

Методы контроля приведены в таблице 5.1.

Перечень контролируемых требований на каждом этапе должен быть отражен в программе обеспечения безопасности. Результаты выполнения методов контроля должны быть представлены в документе «Доказательство безопасности».

Таблица 5.1

Стадии жизненного цикла	Номера подразделов, пунктов требований, подлежащих контролю	Методы контроля
Разработка	4.1, 4.5, 4.6.5	Экспертиза технического задания на систему в части функциональных требований и требований безопасности
	4.2—4.5	Экспертиза алгоритмического обеспечения системы
	4.6.2, 4.6.3	Экспертиза концепции обеспечения безопасности системы
	4.2, 4.3, 4.4	Экспертиза проектной оценки безопасности системы
	4.6	Экспертиза аппаратных и программных средств системы на соответствие положений концепции безопасности
	4.5, 4.6	Экспертиза технических решений
	4.1—4.4, 4.6.6	Испытания технологического программного обеспечения
	4.6.1—4.6.5	Испытания программно-аппаратных средств
	4.1—4.4	Экспертиза документа «Доказательство безопасности»
	4.5	Экспертиза эксплуатационной документации
	4.1—4.4, 4.5.4, 4.6.2, 4.6.4	Проведение автономных испытаний системы
Изготовление	4.2—4.4	Проведение приемочных испытаний системы
	В соответствии с программой и методикой испытаний	Проведение заводских испытаний системы
	4.1—4.6	Экспертиза проекта
Эксплуатация	4.2—4.5	Систематический сбор, обработка и анализ данных об отказах и сбоях, имевших место в процессе эксплуатации. Определение фактических значений количественных показателей безопасности и данных, накопленных в процессе эксплуатации, а также оценка соответствия этих показателей заданным значениям

5.1.3 Если в составе систем ДЦ или ДК применяются аппаратные и (или) программные средства измерения, то

- все средства измерений должны быть утвержденного типа и поверены;
- применяемые методики измерений (кроме прямых измерений) должны быть аттестованы в соответствии с ГОСТ Р 8.563;
- программное обеспечение, связанное с измерениями, должно быть аттестовано в соответствии с ГОСТ 8.654 и [1].

5.2 Контроль требований безопасности к функциям, реализуемым диспетчерской централизацией и диспетчерским контролем

5.2.1 Контроль требований безопасности к функциям, реализуемым системами ДЦ и ДК, выполняется на основе проведения экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации, проверки наличия документации, подтверждающей выполнение проверяемых требований безопасности и испытаний.

5.2.2 На этапе разработки систем ДЦ и ДК организация-разработчик разрабатывает и согласовывает с организацией-заказчиком системы и испытательной лабораторией (центром), аккредитованной на проведение работ по оценке соответствия ЖАТ требованиям безопасности (далее — испытательная лаборатория (центр)), документацию с описанием функций, реализуемых системой ЖАТ.

5.2.3 Испытательная лаборатория (центр), при участии организации-разработчика, проводит экспертизу и испытания для подтверждения корректности реализации функций системами ДЦ и ДК.

5.2.4 При внесении изменений в программно-аппаратные средства систем ДЦ и ДК при добавлении функций, реализуемых этими системами, проводятся повторное согласование документации, повторная экспертиза и испытания в испытательной лаборатории (центре).

5.2.5 При проектировании участка железнодорожной линии организация-проектировщик на основе проектной, конструкторской, технологической, программной, эксплуатационной документации должна определить необходимый набор функций, реализуемых системами ДЦ и ДК для данного полигона управления, и при необходимости согласовать с организацией — заказчиком системы и организацией-разработчиком требуемый объем доработок.

5.2.6 При вводе в эксплуатацию полнота и корректность функций, реализуемых системами ДЦ и ДК, должна быть подтверждена при проведении приемочных испытаний в объеме, предусмотренном программой и методикой приемочных испытаний. Программа и методика приемочных испытаний должны покрывать все функции, реализуемые системами ДЦ и ДК. Программа и методика испытаний должна разрабатываться организацией — разработчиком системы ДЦ или ДК и согласовываться с организацией — заказчиком системы, организацией-проектировщиком и испытательной лабораторией (центром). В процессе эксплуатации системы ДЦ или ДК полнота и корректность реализуемых функций должна оцениваться по результатам мониторинга и статистических отчетов в соответствии с методическими указаниями по надежности в технике и сбору и обработке информации о надежности изделий в эксплуатации [2].

5.3 Контроль требований безопасности к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля

5.3.1 Контроль требований безопасности к эксплуатационной совместимости систем ДЦ и ДК выполняется на основе проведения экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации, проверки наличия документации, подтверждающей выполнение проверяемых требований безопасности и испытаний.

5.3.2 На этапе разработки систем ДЦ и ДК организация-разработчик разрабатывает и согласовывает с организацией-заказчиком документацию по увязке разрабатываемых систем ДЦ и ДК с другими системами ЖАТ, действующими на данном участке железнодорожной линии.

5.3.3 Испытательная лаборатория (центр) при участии организации-разработчика, проводит экспертизу и испытания для подтверждения корректности реализации увязки разрабатываемой системы с другими системами ЖАТ.

5.3.4 При внесении изменений в технические решения по увязке систем ДЦ и ДК с другими системами проводятся повторное согласование документации, повторная экспертиза и испытания в испытательной лаборатории (центре).

5.3.5 При проектировании железнодорожной линии в рамках экспертизы проекта проверяется выполнение требований к размещению аппаратных средств, функциональной, информационной и конструктивной совместимости систем ДЦ и ДК.

5.3.6 Для этапа эксплуатации станционной системы ЖАТ корректность размещения аппаратных средств систем ДЦ и ДК, а также соответствие проекту должны быть подтверждены при проведении приемочных испытаний.

5.4 Контроль требований безопасности к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля

5.4.1 Контроль требований безопасности к аппаратным и программным средствам систем ДЦ и ДК должен выполняться на основе проведения экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации, подтверждающей выполнение проверяемых требований безопасности, расчетных методов и испытаний.

5.4.2 На этапе разработки системы ДЦ или ДК организация-разработчик должна разработать и согласовать с испытательной лабораторией (центром) документ «Доказательство безопасности». В документе «Доказательство безопасности» должно быть представлено аргументированное обоснование того, что программно-аппаратные средства системы ДЦ или ДК соответствуют предъявляемым к ним требованиям безопасности. Материалы документа «Доказательство безопасности» должны позволять сделать следующие выводы:

- требования на систему заданы корректно и в полном объеме;
- требования, предъявляемые к системе, в полном объеме и корректно реализованы в программно-аппаратных решениях;
- программно-аппаратные решения не вносят дополнительных негативных свойств относительно первоначальных требований безопасности;
- представленные доказательства обоснованы и достоверны.

5.4.3 Испытательная лаборатория (центр), при участии организации-разработчика, должна провести экспертизу и испытания для подтверждения корректности доказательного материала, представленного в документе «Доказательство безопасности». Подтверждение обоснованности и корректности количественных показателей безопасности должно проводиться с использованием расчетных методов.

5.4.4 Система ДЦ или ДК должна допускаться в эксплуатацию только при наличии положительного заключения от испытательной лаборатории (центра).

5.4.5 На этапе эксплуатации системы корректность выполнения требований безопасности к аппаратным и программным средствам должна оцениваться экспертными и расчетными методами по результатам мониторинга и статистических отчетов об отказах системы. Сбор и обработка данных о безопасности и надежности эксплуатируемой системы ЖАТ осуществляются в соответствии с методическими указаниями по надежности в технике и сбору и обработке информации о надежности изделий в эксплуатации [2], с выделением при этом отказов (сбоев), вызванных отказами (сбоями) программного обеспечения. Анализ последствий отказов (сбоев), вызванных отказами (сбоями) программного обеспечения, осуществляется в соответствии с методическими указаниями по надежности в технике и методам оценки показателей надежности по экспериментальным данным [3].

Библиография

[1] Рекомендация МИ 2955—2010	Государственная система обеспечения единства измерений. Типовая методика аттестации программного обеспечения средств измерений и порядок ее проведения
[2] Методические указания РД 50-204—87	Надежность в технике. Сбор и обработка информации о надежности изделий в эксплуатации. Основные положения
[3] Методические указания РД 50-690—89	Надежность в технике. Методы оценки показателей надежности по экспериментальным данным

.

УДК 656.25:006.354 ОКС 45.020

Ключевые слова: железнодорожная автоматика и телемеханика, диспетчерская централизация, диспетчерский контроль, безопасность движения железнодорожных поездов, критерии опасных отказов, требования безопасности, методы контроля

Редактор *Е.С. Котлярова*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 19.09.2012. Подписано в печать 09.10.2012. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,35. Тираж 99 экз. Зак. 881.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru