ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52980— 2008

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИХ ИНТЕГРАЦИЯ. СИСТЕМЫ ПРОГРАММИРУЕМЫЕ ЭЛЕКТРОННЫЕ ЖЕЛЕЗНОДОРОЖНОГО ПРИМЕНЕНИЯ

Требования к программному обеспечению

Издание официальное

БЗ 10—2008/374

Москва
Стандартинформ
2009

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 Открытым акционерном обществом «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 459 «Информационная поддержка жизненного цикла изделий»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 13 октября 2008 г. № 243-ст

4 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

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИХ ИНТЕГРАЦИЯ. СИСТЕМЫ ПРОГРАММИРУЕМЫЕ ЭЛЕКТРОННЫЕ ЖЕЛЕЗНОДОРОЖНОГО ПРИМЕНЕНИЯ

Требования к программному обеспечению

Functional safety of electrical, electronic, programmable electronic safety-related systems applications for railways. Software requirements

Дата введения — 2009—05—01

1 Область применения

1.1 Настоящий стандарт устанавливает требования к программному обеспечению (ПО) устройств и систем, связанных с безопасностью на железнодорожном транспорте, в том числе используемому для разработки систем, связанных с безопасностью. Такое ПО, например, устанавливают на следующие устройства и системы: автоматическая локомотивная сигнализация; аппаратно-программные комплексы железнодорожной автоматики и телемеханики; аппаратно-программный комплекс диспетчерского контроля; диспетчерская централизация; комплексные бортовые системы обеспечения безопасности движения; локомотивные устройства системы автоматизированного управления торможением поезда; система маневровой автоматической локомотивной сигнализации и др.

1.2 Программное обеспечение, связанное с безопасностью, включает в себя операционные системы, системное программное обеспечение, программное обеспечение в коммуникационных сетях, функции интерфейса человек-машина, инструментальные средства поддержки и программно-аппаратные средства, а также прикладные программы.

1.3 Настоящий стандарт устанавливает требования для этапов жизненного цикла обеспечения безопасности и деятельности, которая должна проводиться при проектировании и разработке программного обеспечения, обеспечивающего безопасность.

Эти требования включают в себя применение методов и мер, классифицированных по уровням полноты безопасности, для исключения отказов и ошибок в программном обеспечении и принимать необходимые меры при их возникновении.

1.4 Настоящий стандарт устанавливает требования:

к информации, которая должна передаваться организациям, проводящим интеграцию программируемых электронных систем (ПЭС);

к подготовке информации и процедур, относящихся к программному обеспечению, необходимому пользователю для эксплуатации и обслуживания ПЭС безопасности, которые должны выполнять организации, проводящие модификацию программного обеспечения, обеспечивающего безопасность;

к инструментальным средствам поддержки, например, инструментальным средствам проектирования и разработки, языковым трансляторам, инструментальным средствам тестирования и отладки, инструментальным средствам управления конфигурацией.

1.5 Настоящий стандарт предназначен для заказчиков, поставщиков, разработчиков, потребителей, а также персонала сопровождения систем, ПО и услуг.

В настоящем стандарте термин «должны» используется для выражения соглашения между двумя или более сторонами; «должна» — для выражения объявления решения или намерения одной из сторон; «следует» — для выражения выбора одного из имеющихся возможных вариантов; «может» — для обозначения действий, допускаемых в рамках требований настоящего стандарта.

1.6 Настоящий стандарт применяется совместно с ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-3 и ГОСТ Р МЭК 61508-4.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р МЭК 61508-1—2006 Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-3—2006 Функциональная безопасность систем электрических /электронных/программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р МЭК 61508-4—2006 Функциональная безопасность систем электрических/ электронных/программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

ГОСТ Р МЭК 61508-5—2006 Функциональная безопасность систем электрических/ электронных/программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровня соответствия комплексу требований безопасности

ГОСТ Р ИСО/МЭК 12207—99 Информационная технология. Процессы жизненного цикла программных средств

ГОСТ Р ИСО 9001—2001 Системы менеджмента качества. Требования

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 и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **автоматическая локомотивная сигнализация:** Устройства, обеспечивающие автоматическую передачу с пути и прием на локомотиве сигналов, соответствующих показаниям путевого светофора, к которому приближается поезд.

3.2 **аппаратно-программный комплекс:** Комплекс, состоящий из аппаратного и программного обеспечения системы, позволяющий осуществлять сбор, обработку, хранение и отображение информации о состоянии объектов в реальном масштабе времени.

3.3 **аппаратно-программные комплексы железнодорожной автоматики и телемеханики (АПК ЖАТ):** Сложные разветвленные технические системы, содержащие автоматизированные рабочие места, каналы передачи информации, локальные вычислительные сети, контроллеры, преобразователи информации и др. АПК ЖАТ решают задачи диспетчерского контроля и централизации, автоматической локомотивной централизации, автоблокировки, передачи информации оперативно-технологического назначения и т.д.

3.4 **аппаратно-программный комплекс диспетчерского контроля (АПК-ДК):** Аппаратно-программный комплекс, предназначенный для централизованного контроля, диагностики и регистрации состояния устройств железнодорожной автоматики и телемеханики, диагностики их технического состояния, а также организации управления движением поездов в пределах диспетчерского круга. АПК-ДК позволяет осуществлять сбор, обработку, хранение и отображение информации о состоянии объектов контроля в реальном масштабе времени.

3.5 **встроенная система:** Система, погруженная во внешнюю среду, управляется вычислительной системой и представляет собой взаимодействующую совокупность программных и аппаратных элементов.

3.6 **диспетчерская централизация (ДЦ):** Комплекс устройств, включающий в себя автоматическую блокировку на перегонах, электрическую централизацию на станциях и телемеханическую систему, предназначенную для передачи и приема управляющих и информационных сигналов.

Примечание — Основными задачами ДЦ являются:

- управление из одного пункта стрелками и светофорами ряда станций и перегонов;
- непрерывный контроль в автоматическом режиме за поездной ситуацией — положением и занятостью стрелок, занятостью перегонов, путей на станциях и прилегающих к ним блок-участках, а также повторение показаний входных маршрутных и выходных светофоров;

- возможность передачи станций на резервное управление стрелками и светофорами по приему, отправлению поездов и производству маневров или передачи стрелок на местное управление для производства маневров;
- автоматическая запись графика выполнения движения поездов;
- документирование действий поездного диспетчера;
- обмен необходимой информацией с устройствами ДЦ соседних участков и с информационно-управляющими системами «верхнего» уровня.

3.7 **комплексные бортовые системы обеспечения безопасности движения:** Аппаратно-программные системы, выполняющие следующие основные функции:
- прием сигналов от путевых устройств станционной и перегонной автоматики о местонахождении идущего впереди поезда, допустимой скорости движения и о другой информации;
- измерение скорости движения, определение местоположения локомотива, положение органов управления локомотива, состояние тормозной системы;
- обработка принятых сигналов и измеренных параметров движения, формирование допустимой скорости, при превышении допустимой скорости — принудительное торможение поезда;
- индикация и сигнализация машинисту информации, формируемой системой;
- контроль бдительности и бодрствования машиниста и принудительное торможение поезда при их недопустимом снижении;
- регистрация информации, формируемой системой, параметров движения, местоположения локомотива и времени действия в энергонезависимую память системы.

3.8 **локомотивные устройства системы автоматизированного управления торможением поезда:** Размещенный на локомотиве аппаратно-программный комплекс, предназначенный для управления автоматическим торможением в соответствии с заложенными алгоритмами.

3.9 **система маневровой автоматической локомотивной сигнализации:** Система, предназначенная для использования при выполнении маневровых работ на станциях. Система обеспечивает повышение безопасности при маневрах, увеличение перерабатывающей способности станций, оборудованных электрической централизацией, за счет повышения эффективности средств управления локомотивами.

3.10 **функциональная безопасность:** Способность системы, связанной с безопасностью, выполнять все предусмотренные в системе функции безопасности с сохранением остаточного риска возникновения опасных событий на допустимом уровне.

3.11 **функция безопасности:** Функция, реализуемая связанной с безопасностью системой или внешними средствами снижения риска, предназначенная для обеспечения или поддержания безопасного состояния применительно к конкретному опасному событию.

3.12 **безопасность:** Отсутствие неприемлемого риска.

4 Требования к управлению качеством программного обеспечения

4.1 Цель управления качеством программного обеспечения безопасности

Целью управления качеством программного обеспечения является определение:

а) управления и технической деятельности на всех этапах цикла обеспечения безопасности: общей; электрических, электронных, программируемых электронных систем (Э/Э/ПЭС) и программного обеспечения, необходимых для достижения требуемой функциональной безопасности;

б) ответственности лиц, подразделений и организаций за каждый этап цикла обеспечения безопасности (за деятельность на каждом этапе).

Примечание — Организационные меры, оговоренные в данном подразделе, обеспечивают эффективную реализацию технических требований по достижению и сохранение функциональной безопасности Э/Э/ПЭ систем безопасности.

Технические требования, необходимые для сохранения функциональной безопасности, обычно являются частью информации, предоставляемой поставщиком Э/Э/ПЭ систем безопасности.

4.2 Требования к управлению качеством ПО ПЭС безопасности

4.2.1 Организации или лица, несущие ответственность на этапах цикла обеспечения безопасности, должны на этапах, за которые они несут ответственность, определять управленческую и техническую деятельность, необходимую для гарантии достижения и сохранения требуемой функциональной безопасности Э/Э/ПЭ систем безопасности. Должны быть рассмотрены:

а) способы достижения функциональной безопасности и средства оценки ее достижения, а также средства информирования внутри организации для обеспечения безопасной работы;

б) определение лиц, подразделений и организаций, ответственных за осуществление и проверку достижения безопасности на выполняемых этапах цикла обеспечения общей безопасности;

в) способ организации и объем информации, которая должна быть внесена в документацию;

г) выбранные методы и средства, используемые для соответствия требованиям безопасности;

д) деятельность по оценке функциональной безопасности;

е) процедуры, способствующие обеспечению последовательного и полного выполнения рекомендаций, имеющих отношение к Э/Э/ПЭС и ПО, и связанных с:

анализом опасности и риска,

оценкой функциональной безопасности,

деятельностью по верификации,

деятельностью по аттестации,

конфигурацией управления;

ж) процедуры, обеспечивающие гарантию того, чтобы участники любой деятельности, относящейся к циклу обеспечения безопасности, были подготовлены для выполнения деятельности, которая является сферой их компетентности, т.е. должны быть предусмотрены:

подготовка персонала в области диагностики и устранения отказов в испытуемых системах,

обучение операторов,

переподготовка персонала через определенные промежутки времени;

и) процедуры, обеспечивающие анализ опасных случаев (или случаев, способных создать опасность), а также выработку рекомендаций для уменьшения вероятности повторения таких случаев;

к) процедуры анализа процессов эксплуатации и сопровождения, в том числе процедуры для:

выявления систематических отказов, которые могут понизить уровень функциональной безопасности, включая процедуры, используемые во время плановых обслуживаний в случае обнаружения повторяющихся отказов,

оценки того, что интенсивность запросов системы и интенсивность отказов во время эксплуатации и обслуживания соответствуют допущениям, принятым при проектировании системы;

л) требования по периодической проверке функциональной безопасности, включая:

частоту проверки функциональной безопасности,

рассмотрение уровня независимости, необходимого для лиц, ответственных за такую проверку,

деятельность по доведению проверки до конца и составлению документации;

м) процедуры по инициации процесса модификации систем, обеспечивающих безопасность и процедуры одобрения и разрешения на модификацию;

н) процедуры сохранения точной информации о потенциальных опасностях и системах, обеспечивающих безопасность;

п) процедуры управления конфигурацией ПО систем безопасности на всех этапах цикла обеспечения безопасности, в том числе должны быть оговорены:

стадия, на которой должна быть произведена официальная проверка конфигурации,

процедуры, используемые для однозначного определения частей, составляющих объект (аппаратура и программное обеспечение),

процедуры по предотвращению попадания в эксплуатацию опасных объектов.

4.2.2 Результаты деятельности, выполняемой в соответствии с 4.2.1, должны документироваться в процессе ее выполнения.

4.2.3 Требования, разработанные по результатам 4.2.1, должны быть официально рассмотрены заинтересованными организациями, и между ними должно быть достигнуто соглашение.

4.2.4 Лица, ответственные за управление деятельностью по обеспечению функциональной безопасности, должны быть проинформированы о возложенной на них ответственности.

4.2.5 Поставщики продукции или услуг организациям, несущим общую ответственность на одном или нескольких этапах цикла обеспечения безопасности, должны поставлять эту продукцию или услуги в соответствии с тем, как оговорено этими организациями и иметь соответствующую систему управления качеством.

4.2.6 Планирование функциональной безопасности должно определять порядок получения, разработки, компоновки, верификации, аттестации и модификации программного обеспечения в той мере, которая необходима для требуемого уровня соответствия Э/Э/ПЭ системы безопасности уровню полноты безопасности.

4.2.7 При управлении конфигурацией программного обеспечения должно выполняться:

а) применение административного и технического контроля на всем протяжении цикла обеспечения безопасности для управления изменениями программного обеспечения и подтверждение того, что требования, предъявляемые к безопасности программного обеспечения, продолжают выполняться;

б) обеспечение выполнения операций, необходимых для подтверждения достижения заданного уровня полноты безопасности программного обеспечения [1];

в) точное сохранение с однозначной идентификацией всех элементов конфигурации, необходимых для сохранения заданного уровня полноты безопасности.

Примечание — Элементы конфигурации должны включать в себя, по меньшей мере:
- анализ и требования безопасности,
- спецификацию программного обеспечения и проектную документацию,
- исходный текст программного обеспечения,
- план и результаты тестирования,
- разработанные компоненты и модули ПО, которые должны быть интегрированы в Э/Э/ПЭ систему безопасности,
- инструментальные средства и среду разработки, используемые при создании, тестировании или выполнении любых других действий с программным обеспечением Э/Э/ПЭ системы безопасности;

г) использование процедуры управления изменениями ПО для предотвращения несанкционированных модификаций, в том числе для:
- составления заявки на модификацию,
- анализа влияния предлагаемой модификации и одобрения или отказа от заявки,
- составления документации на модификацию и разрешение всех утвержденных модификаций,
- установления базовых положений конфигурации на соответствующих этапах разработки программного обеспечения и составления документации на (частичные) компоновочные испытания, которые подтверждают эти базовые положения,
- гарантирование объединения и компоновки всех подсистем программного обеспечения.

Примечание — Дополнительную информацию об управлении конфигурацией см. в ГОСТ Р ИСО/МЭК 12207.

4.3 Требования к жизненному циклу программного обеспечения, связанного с безопасностью

4.3.1 Жизненный цикл ПО, связанного с безопасностью представляет собой определенные этапы и процессы, выполняемые в течение периода времени, начиная с момента замысла программного обеспечения и до того момента, когда использование программного обеспечения полностью прекращается (см. рисунок 1 и приложение А).

Рисунок 1 — Жизненный цикл программного обеспечения, связанного с безопасностью (V-модель)

4.3.2 Жизненный цикл при разработке программного обеспечения, связанного с безопасностью должен быть выбран и задан при планировании безопасности в соответствии с разделом 6 [2].

Примечание — Модель жизненного цикла обеспечения безопасности, которая соответствует требованиям [2] раздела 7, может быть приспособлена для практических нужд проекта или организации.

4.3.3 В деятельность, связанную с жизненным циклом обеспечения безопасности, должны быть включены процедуры гарантирования качества и безопасности ПО.

4.3.4 Каждый этап жизненного цикла обеспечения безопасности ПО должен быть подразделен на элементарные действия. Должны быть определены входные и выходные данные для каждого этапа жизненного цикла.

Примечание — При разработке некоторых Э/Э/ПЭ систем безопасности выходные данные отдельных этапов жизненного цикла обеспечения безопасности могут представлять собой различные документы, которые по выходным данным нескольких этапов могут быть объединены. Основным требованием для объединения является соответствие выходных данных этапа цикла обеспечения безопасности поставленной перед этапом цикла цели. В случае простых разработок некоторые этапы цикла обеспечения безопасности ПО также могут быть объединены.

4.3.5 Жизненный цикл программного обеспечения, связанного с безопасностью, создается с учетом уровня полноты безопасности и сложности проекта.

Примечание — Полный перечень этапов цикла обеспечения безопасности (см. приложение А) используется для очень больших вновь разрабатываемых систем. В некоторых случаях может оказаться целесообразным, например, объединить этапы проектирования системы программного обеспечения и архитектурного проектирования.

4.3.6 Проект ПО может быть изложен не в соответствии с требованиями настоящего стандарта (т. е. допускается использовать другую модель жизненного цикла) при условии, что все цели и требования подпунктов 4.3.1—4.3.5 будут удовлетворены.

4.3.7 Для каждого этапа цикла обеспечения безопасности должны использоваться соответствующие методы и меры (см. ГОСТ Р МЭК 61508-3, приложения А и В).

4.3.8 По результатам деятельности на этапах жизненного цикла ПО, связанного с безопасностью, должна быть составлена документация.

4.3.9 Если на любом этапе цикла обеспечения безопасности ПО потребуется изменение, относящееся к более раннему этапу цикла обеспечения безопасности, то более ранний этап цикла обеспечения безопасности и последующие этапы должны быть повторены.

5 Уровни полноты безопасности программного обеспечения

5.1 Определение уровней полноты безопасности ПО для систем железнодорожного применения основываются на сведениях:

а) обо всех возможных опасных состояниях в системе, при всех режимах эксплуатации, технического обслуживания и состояниях окружающей среды;

б) о показателях каждого опасного состояния, выражающих тяжесть его последствий;

в) о безопасности и отказах, связанных с безопасностью, основанных на:

- всех видах системных отказов, которые могут приводить к опасному состоянию,
- вероятности возникновения вида отказа, связанного с безопасностью,
- последовательности и (или) одновременности событий, отказов, режимов работы, условий окружающей среды и т. д. применения, которые могут привести к аварии,
- вероятности, с которой каждое из этих событий, отказов, режимов работы, условий окружающей среды и т.д. применения происходит;

г) о ремонтопригодности всех связанных с безопасностью частей системы, основывающейся на:

- простоте, с которой может проводиться техническое обслуживание части системы или ее компонентов, связанных с опасным состоянием,
- вероятности ошибки при техническом обслуживании частей системы, связанных с безопасностью,
- времени, которое необходимо для восстановления безопасного состояния;

д) о процессе эксплуатации системы и техническом обслуживании связанных с безопасностью частей системы, основывающихся на:

- влиянии человеческого фактора на эффективное техническое обслуживание всех связанных с безопасностью частей системы и безопасную эксплуатацию системы,
- средствах и методах для эффективного технического обслуживания,

- всех, связанных с безопасностью, частях системы и ее безопасной эксплуатации,
- контроле и мероприятиях исключения опасных состояний и уменьшению их последствий.

5.2 Отказы в системе, эксплуатируемой в заданных условиях применения и окружающей среды, оказывают воздействие на поведение системы. Все отказы отрицательно сказываются на надежности системы, однако только некоторые специфические отказы оказывают отрицательный эффект на безопасность при конкретном применении. Окружающая среда может влиять как на работоспособность системы, так и на безопасность применения на железной дороге.

5.3 На основании результатов процедуры оценки риска для системы, связанной с безопасностью, должны быть определены требования к уровню полноты безопасности [1]. Уровень полноты безопасности может рассматриваться как комбинация статистически исследуемых элементов, принципиально связанных с аппаратным обеспечением (т. е. случайные отказы) и статистически не исследуемых элементов (принципиально связанных с систематическими отказами в программном обеспечении).

Внешние средства и средства собственно системы, предназначенные для снижения риска, должны обеспечивать требуемое снижение риска для системы, чтобы обеспечивать заданный уровень полноты безопасности.

5.4 Уверенность в достижении уровня полноты безопасности может достигаться посредством эффективной комбинации специальных систем, методов, средств и технических приемов. Полнота безопасности ПО относится к вероятности отказа, которая обеспечивает достижение требуемой достоверной работоспособности (надежности). Высокие требования относительно безопасности могут осуществляться, как правило, только с дополнительными издержками.

5.5 Полнота безопасности специфицируется для функций безопасности. Эти функции должны быть назначены системе безопасности и/или внешним средствам для снижения риска. Данное назначение происходит итеративно, принимая во внимание оптимизацию разработки и стоимости всей системы.

5.6 Необходимый уровень полноты безопасности ПО должен быть определен на основе уровня риска, связанного с использованием ПО в системе и уровнем безопасности системы.

Риск может быть определен как численно определенная вероятность или комбинация численно определенных вероятностей, но уровень безопасности ПО не может быть определен подобным образом, так как отказы ПО имеют систематический характер (см. 5.3).

6 Спецификация требований по безопасности программного обеспечения

6.1 Требования безопасности ПО должны быть определены:

- в терминах функций безопасности и полноты безопасности;
- к функциям безопасности программного обеспечения для каждой Э/Э/ПЭ системы безопасности, необходимых для выполнения требуемых функций безопасности;
- к уровню полноты безопасности для каждой Э/Э/ПЭ системы безопасности (для каждой функции безопасности, адресованной этой Э/Э/ПЭ системе безопасности).

6.2 Требования, приводимые в 6.2.1—6.2.11, должны достигаться комбинацией общего, встроенного ПО и специального прикладного ПО. Разделение между общим и специальным прикладным ПО зависит от выбранной архитектуры ПО.

6.2.1 Требования к функциям безопасности ПО могут быть определены в требованиях к Э/Э/ПЭ системе безопасности (см. подраздел 7.2) [3]. В этом случае спецификацию требований по безопасности ПО повторять не надо.

6.2.2 Спецификация требований к безопасности ПО должна основываться на заданных требованиях к безопасности Э/Э/ПЭ системы безопасности железнодорожного применения и требованиях планирования безопасности. Эта информация должна быть доступной разработчику ПО.

Примечание — Это требование (см. 6.2.2) не означает, что не должно быть взаимодействия между разработчиком Э/Э/ПЭС и разработчиком ПО [3]. Требования к безопасности ПО и архитектура ПО постоянно уточняются в процессе реализации цикла безопасности и могут оказать влияние на архитектуру аппаратуры Э/Э/ПЭС, поэтому необходимо тесное сотрудничество между разработчиками аппаратуры и ПО.

6.2.3 Спецификация требований к безопасности ПО должна быть достаточно подробной для того, чтобы на этапах разработки и реализации достигался требуемый уровень полноты безопасности, и можно было провести оценку функциональной безопасности.

Примечание — Уровень детализации спецификации может изменяться в зависимости от сложности применения ПО.

6.2.4 Разработчик ПО для подтверждения адекватного задания требований должен учитывать:

а) функции безопасности;

б) конфигурацию или архитектуру системы;

в) требования по полноте безопасности программируемой электроники, датчиков и исполнительных механизмов;

г) требования к полноте безопасности ПО;

д) производительность и время срабатывания;

е) взаимодействие между оборудованием и оператором.

6.2.5 Разработчик ПО должен установить процедуры устранения любых разногласий, выходящих за пределы допустимых, при задании уровня полноты безопасности ПО.

6.2.6 В пределах, требуемых уровнем полноты безопасности, заданные требования к безопасности ПО должны быть выражены и структурированы так, чтобы они были:

а) ясными, точными, недвусмысленными, проверяемыми, сохраняемыми и осуществимыми, соответствующими уровню полноты безопасности;

б) определяемыми в спецификации требований по безопасности Э/Э/ПЭ системы безопасности;

в) содержащими четкие, недвусмысленные термины, понятные для тех, кто будет использовать этот документ на любом этапе цикла обеспечения безопасности ПО.

6.2.7 Все ответственные режимы эксплуатации аппаратуры [4] должны быть определены в требованиях к Э/Э/ПЭ системе безопасности и в требованиях по безопасности ПО (см. 6.2.2).

6.2.8 Спецификация требований безопасности ПО должна определять и документировать любые связи, относящиеся к обеспечению безопасности между аппаратурой и программным обеспечением.

6.2.9 В пределах, требуемых проектом архитектуры аппаратных средств Э/Э/ПЭС, спецификация требований безопасности ПО должна содержать:

а) самоконтроль ПО;

б) мониторинг аппаратных средств Э/Э/ПЭС, датчиков и исполнительных механизмов программируемой электроники;

в) периодическую проверку функций безопасности в процессе работы системы;

г) возможность проверки функций безопасности во время эксплуатации аппаратных средств Э/Э/ПЭС.

6.2.10 В случаях, если Э/Э/ПЭ система безопасности должна выполнять функции, не связанные с обеспечением безопасности, требования безопасности ПО должны четко определять такие функции.

6.2.11 Спецификация требований безопасности ПО должна определять требуемые свойства безопасности ПО, но не проекта. В соответствии с 6.2.1—6.2.10 спецификации должны содержать:

а) требования:

- к функциям, обеспечивающим достижение и поддержание безопасного состояния аппаратных средств Э/Э/ПЭС,
- к функциям, относящимся к выявлению отказов, извещению об их наличии и устранению отказов в аппаратных средствах программируемой электроники,
- к функциям, относящимся к выявлению отказов, извещению об их наличии и устранению отказов датчиков и исполнительных механизмов,
- к функциям, относящимся к выявлению отказов, извещению об их наличии и обработке ошибок в самом ПО (самоконтроль ПО),
- к функциям, относящимся к периодической проверке функций безопасности в режиме эксплуатации,
- к функциям, относящимся к периодической проверке функций безопасности в режиме автономного контроля,
- к функциям, позволяющим безопасно проводить модификацию ПЭС,
- к функциям, не относящимся к обеспечению безопасности,
- производительности и времени срабатывания,
- взаимодействию между ПО и ПЭС.

Примечание — Взаимодействие включает в себя средства программирования как в режиме эксплуатации, так и в прочих состояниях (например, при модификации ПО);

б) требования к полноте безопасности ПО, т. е. к уровню полноты безопасности для каждой функции безопасности [см. 6.2.1, перечисление а)].

Примечание — Информация, относящаяся к адресному распределению функций по безопасности между компонентами ПО, приведена в ГОСТ Р МЭК 61508-5, приложение А.

7 Порядок подтверждения безопасности программного обеспечения

7.1 Настоящий раздел содержит требования, которые должны выполняться, чтобы ПО, связанное с безопасностью, могло быть признано обеспечивающим требуемый уровень полноты безопасности для его применения по назначению.

Должен быть разработан план подтверждения соответствия безопасности ПО (см. ГОСТ Р МЭК 61508-3, подраздел 7.3).

7.2 Должны быть выполнены и задокументированы процедуры доказательства:

а) эффективности управления качеством (см. ГОСТ Р ИСО 9001);

б) эффективности мер обеспечения безопасности [4];

в) функциональной и технической безопасности (см. ГОСТ Р МЭК 61508-1).

Документальные доказательства выполнения указанных требований [см. перечисление а) — в)] должны быть включены в документ по обоснованию безопасности («Доказательство соответствия требованиям безопасности») [5]. Документ [5] образует часть общего комплекта документальных доказательств, который должен быть представлен в орган сертификации, отвечающему за безопасность, с целью получения сертификата безопасности ПО.

7.2.1 Данный документ должен иметь следующую структуру:

1 Раздел «Определение системы программного обеспечения» должен содержать точные определения или описания ПЭС и ПО, к которому относится данное доказательство соответствия требованиям безопасности, включая номера версий и состояние изменений для всех требований проектной и рабочей документации.

2 Раздел «О мерах по управлению качеством» должен содержать доказательства эффективности управления качеством в соответствии с разделом 4.

3 Раздел «О мерах по обеспечению безопасности» должен содержать доказательства эффективности мер обеспечения безопасности в соответствии с разделами 6, 9 и 10.

4 Раздел «Оценка функциональной безопасности» должен содержать оценку и подтверждение функциональной безопасности в соответствии с разделом 13.

5 Раздел «Подтверждение соответствия требованиям безопасности для устройств и систем, связанных с данной системой», т. е. систем, от которых зависит работа основной системы. В данном разделе необходимо продемонстрировать, что условия применения ПЭС и ПО, связанных с обеспечением безопасности, требования к которым определены в каждом из доказательств соответствия требованиям безопасности устройств и систем, выполняются в основном доказательстве соответствия требованиям безопасности или включены в состав условий применения ПО.

6 Заключение, которое должно содержать обобщение доказательств, представленных в предшествующих разделах, и окончательное доказательство того, что ПЭС и ПО обеспечивают необходимую безопасность и соответствуют требованиям конкретных условий применения.

7.3 Первым условием для приемки ПО безопасности, которое обязательно должно выполняться, является наличие эффективной системы управления качеством в течение всего жизненного цикла ПО.

Назначение системы управления качеством заключается в том, чтобы свести к минимуму вероятность человеческих ошибок (ошибок персонала) на всех этапах жизненного цикла ПО, связанного с безопасностью, и снизить риск возникновения систематических отказов в ПО.

В раздел «О мерах по управлению качеством» нет необходимости включать большие объемы подробной доказательной и вспомогательной информации при условии, что на документы, содержащие такую информацию, будут приведены ссылки.

Требования к управлению качеством являются обязательными для уровней полноты безопасности 1—4 включительно. Точность представленных доказательств должна соответствовать уровню полноты безопасности проверяемой системы. Требования к уровню полноты безопасности 0 (изделие не связано с обеспечением безопасности) в настоящем стандарте не рассматриваются.

7.4 Вторым условием подтверждения безопасности, которое обязательно должно выполняться, является наличие эффективного процесса управления безопасностью (комплекса мер по обеспечению безопасности) в течение всего жизненного цикла ПО, который должен соответствовать требованиям к процессу управления надежностью устройств и систем железнодорожного применения (показателей надежности, оперативной готовности, пригодности к техническому обслуживанию и безопасности) [4]. Цель данного процесса состоит в обеспечении дальнейшего снижения вероятности человеческих ошибок (ошибок персонала), связанных с безопасностью (т. е. способных повлиять на безопасность), в течение всего жизненного цикла ПО и тем самым свести к минимуму остаточный риск систематических отказов, способных повлиять на безопасность.

Процесс управления безопасностью должен состоять из этапов и действий, связанных между собой, образующих жизненный цикл безопасности ПО. Данный процесс должен соответствовать жизненному циклу, заданному в 4.3 и приложении А.

7.5 Доказательство функциональной безопасности ПО должно быть проведено в обязательном порядке. Раздел «О мерах по обеспечению безопасности» должен содержать разъяснение принципов, положенных в основу обеспечения безопасности проекта ПО, включая все подтверждающие доказательства (например, спецификации и результаты испытаний, анализ безопасности).

Данный раздел должен содержать:

1 Введение, в котором должно содержаться общее описание проекта, включая обзор технических принципов обеспечения безопасности ПО, положенных в основу проекта с указанием степени, в которой устройства и система, обеспечивающие безопасность на железных дорогах, могут считаться безопасными при отказах в соответствии с требованиями настоящего стандарта.

Во введении должны также быть ссылки на международные и национальные стандарты, использованные в качестве оснований для обеспечения функциональной безопасности проекта ПО.

В случае внесения изменений (модификации) или расширения ПО, уже находящегося в эксплуатации или после завершения разработки (в порядке исключения), в качестве оснований могут быть использованы стандарты, примененные для первоначального проекта (разработки) и послужившие основой для его сертификации. Должны быть приведены причины, являющиеся обоснованием для использования данных стандартов при внесении изменений (модификации) или расширения ПО.

2 Подраздел «Обеспечение правильности выполнения функций», который должен содержать доказательства, необходимые для демонстрации правильности действия ПО в нормальных условиях и при отсутствии неисправностей в соответствии с заданными спецификацией эксплуатационными требованиями и требованиями безопасности.

Данный подраздел должен содержать:

а) описание архитектуры ПО;

б) выполнение требований спецификации на ПО;

в) выполнение требований спецификации по безопасности;

г) обеспечение правильного действия ПЭ систем;

д) выполнение заданных требований в части условий окружающей среды;

е) обеспечение правильного действия ПО.

3 Подраздел «О влиянии неисправностей» должен содержать доказательства, что ПО выполняет заданные в спецификации требования по безопасности, включая значения целевых показателей безопасности, в случае возникновения случайных неисправностей в ПЭ системах.

В данном подразделе должны быть указаны меры, принятые с целью снижения риска до практически возможного минимального уровня в случае наличия ошибок в ПО.

Подраздел должен содержать:

а) последствия одиночных отказов;

б) независимость компонентов;

г) обнаружение одиночных отказов;

д) действия при обнаружении отказа (включая сохранение безопасного состояния);

е) последствия множественных отказов;

ж) защиту от систематических отказов.

4 Подраздел «О работе при наличии внешних воздействий» должен содержать подтверждение, что системы ПО и ПЭ, подверженные внешним воздействиям, заданным в спецификации требований, продолжают выполнять:

требования, заданные в спецификации;

заданные требования по безопасности (в том числе при наличии отказа).

Доказательство соответствия требованиям безопасности (приведенное в настоящем подразделе) является действительным только в пределах заданных в спецификации требований к системе диапазона внешних воздействий. Вне этих пределов без принятия специальных дополнительных мер безопасность не обеспечивается.

Методы, применяемые для обеспечения устойчивости к заданным внешним воздействиям, должны быть полностью описаны и обоснованы.

5 В подразделе «Условия применения, связанные с обеспечением безопасности» должны быть определены или приведены ссылки на правила, условия и ограничения, которые должны соблюдаться в процессе применения ПО и ПЭ систем. В их число должны входить условия применения, содержащиеся в документе [5] (см. 7.2) любой подсистемы, относящейся к системе, связанной с безопасностью.

6 В подразделе «О квалификационных испытаниях по безопасности» должны содержаться доказательства успешного завершения квалификационных испытаний по безопасности при условиях, соответствующих условиям эксплуатации ПО.

7.6 Должны быть определены процедуры приемки и сертификации по безопасности программного обеспечения ПЭС, связанного с безопасностью. В настоящем стандарте не определяется, кто должен проводить работы на каждом этапе, поскольку это может зависеть от конкретных обстоятельств.

7.6.1 Для признания ПО ПЭС, обеспечивающими адекватную безопасность для применения по назначению, должны быть приведены следующие доказательства (см. 7.2):

- эффективности управления качеством;
- эффективности мер обеспечения безопасности;
- функциональной безопасности.

Данные доказательства должны быть включены в документ «Доказательство соответствия требованиям безопасности».

7.6.2 Перед рассмотрением заявки на сертификацию по безопасности должна быть проведена независимая оценка и процедура доказательства соответствия ПО требованиям безопасности с целью получения дополнительной гарантии обеспечения требуемого уровня безопасности. Результаты данной процедуры должны быть представлены в отчете об оценке (экспертизе) безопасности.

Данный отчет должен служить дополнением к процедурам, проведенным экспертом по безопасности с целью определения методов и средств, с помощью которых при разработке программного обеспечения были выполнены заданные требования, а также, при необходимости, содержать некоторые дополнительные требования к эксплуатации ПО. Степень оценки безопасности и степень независимости ее проведения определяют на основании результатов классификации рисков в соответствии с ГОСТ Р МЭК 61508-1 и ГОСТ Р МЭК 61508-5. Для повышения степени доверия к результатам оценки эксперт может потребовать проведения конкретных испытаний.

7.6.3 Полный комплект документов, обосновывающих доказательство соответствия ПО требованиям безопасности, должен включать в себя:

- спецификацию требований к ПО;
- спецификацию требований к безопасности ПО;
- доказательство соответствия требованиям безопасности;
- отчет об оценке безопасности.

7.6.4 «Сертификат соответствия требованиям безопасности» выдается на основании документов, перечисленных в 7.6.3, и в соответствии с протоколом «О результатах сертификационных испытаний», проведенных независимым органом оценки безопасности.

Выдача сертификата может зависеть также от выполнения дополнительных требований (временных или постоянных), выдвинутых экспертом по безопасности.

7.7 После того как ПО получит сертификат безопасности, любую последующую модификацию контролируют с использованием тех же критериев управления качеством, управления безопасностью и функциональной и технической безопасности, что и для новой разработки. Вся необходимая документация, включая [5] (см. 7.2), должна быть обновлена или дополнена добавочной документацией, а модифицированный проект должен быть представлен на сертификацию.

8 Порядок разработки программного обеспечения

Порядок разработки ПО, связанного с безопасностью, должен соответствовать требованиям ГОСТ Р МЭК 61508-3, подраздел 7.4.

9 Требования к методам интеграции программного и аппаратного обеспечения

Требования к методам интеграции программного и аппаратного обеспечения должны соответствовать требованиям ГОСТ Р МЭК 61508-3, подраздел 7.5.

10 Порядок верификации программного обеспечения

10.1 Целью данного раздела является определение, испытание и оценка выходных данных этапа верификации в пределах, требуемых уровнем полноты безопасности, для подтверждения правильности и согласованности с выходными данными предыдущих этапов, используемых в качестве входных данных на данном этапе.

Примечание — В зависимости от архитектуры программного обеспечения, ответственность за проведение верификации может быть возложена на организации, участвующие в разработке и модификации ПО.

10.2 Верификация ПО должна планироваться одновременно с разработкой каждого цикла обеспечения безопасности ПО, и эта информация должна быть задокументирована.

План верификации ПО должен содержать описание процедур верификации. Данные процедуры могут варьироваться в зависимости от уровня безопасности ПО. План верификации ПО должен включать в себя, как минимум, следующие разделы:

а) «Распределение организационной ответственности при проведении верификации ПО и интерфейсы с другими процессами жизненного цикла ПО»;

б) «Описание методов для обеспечения независимости верификации» (если это требуется);

в) «Описание методов верификации», т.е. методов, которые будут использованы на каждом этапе процесса верификации ПО, в том числе описание методов:

- просмотра программных документов, включающего в себя просмотр контрольных листов и другие средства поддержки;
- анализа, включающего в себя методы анализа трассируемости и оценки полноты покрытия;
- тестирования, включающего в себя рекомендации для выбора тестовых вариантов, используемых тестовых процедур, генерации тестовых данных.

г) «Описание среды: оборудования для тестирования, инструментальных средств тестирования и анализа, а также руководств по применению этих средств и аппаратного тестового оборудования»;

д) «Критерии перехода к процессу верификации ПО» (определяемому в этом плане);

е) «Описание метода верификации целостности», если используют разбиение на части;

ж) «Описание соглашений относительно корректности применения компилятора, редактора связей или загрузчика»;

и) «Описание методов идентификации модифицируемых областей ПО и измененных частей исполняемого объектного кода» (повторная верификация ПО должна гарантировать, что ранее зарегистрированные ошибки или классы ошибок были устранены).

Если для ранее разработанного ПО требования к процессу верификации не согласуется с требованиями настоящего стандарта, приводят описание методов верификации, соответствующих этим требованиям.

11 Правила аттестации программного обеспечения

11.1 Аттестация ПО представляет собой проверку и анализ интегрированной программной системы для обеспечения согласованности с требованиями безопасности, функционирования производительности и взаимодействия ПЭ систем, связанных с безопасностью.

Должно быть проведено планирование процесса аттестации для определения шагов (как процедурных, так и технических), которые должны быть сделаны для подтверждения того, что ПО соответствует требованиям безопасности.

11.1.1 План аттестации программного обеспечения должен содержать:

а) подробные указания о сроках проведения аттестации;

б) подробные указания о том, кто должен проводить аттестацию;

в) определение ответственных режимов эксплуатации технических средств, включая:

- подготовку к использованию, в том числе наладку и регулировку ПЭС,
- запуск, обучение, эксплуатацию ПЭС,
- переналадку, выключение, обслуживание ПЭС,
- предсказуемые нештатные ситуации;

г) определение относящегося к обеспечению безопасности ПО, безопасность которого необходимо подтверждать на каждом этапе эксплуатации технических средств перед запуском в эксплуатацию;

д) техническую стратегию аттестации (например, аналитические методы, статистические испытания и т. п.);

е) меры (методы) и процедуры, которые должны использоваться для подтверждения того, что каждая функция безопасности соответствует заданным требованиям к функциям безопасности программного обеспечения и заданным требованиям полноты безопасности программного обеспечения;

ж) требования к условиям окружающей среды, в которой должна проводиться аттестация;

и) критерии прохождения / непрохождения аттестации;

к) политику и процедуры оценки результатов аттестации.

Примечание — Данные требования основаны на общих требованиях [2], подраздел 7.8.

11.1.2 План аттестации относящегося к обеспечению безопасности ПО должен включать в себя выбор методов:

а) с ручным или автоматическим управлением ПЭС (или тех и других);

б) статических или динамических (или тех и других);

в) аналитических или статистических (или тех и других).

11.1.3 Область и содержание планирования аттестации ПО должны быть рассмотрены совместно с экспертом, проводящим оценку безопасности, если этого требует уровень полноты безопасности (см. [2], пункт 8.2.12). Данная процедура должна также предусматривать присутствие эксперта во время испытаний.

11.1.4 Критерий прохождения/непрохождения при проведении аттестации ПО должен включать в себя последовательность и значения:

- требуемых входных сигналов;
- ожидаемых выходных сигналов, а также
- другие критерии приемки, например, используемую память.

11.2 Целью требований настоящего подраздела является обеспечение соответствия заданным требованиям безопасности ПО при заданном уровне безопасности.

11.2.1 Если соответствие требованиям безопасности ПО уже установлено в качестве части Э/Э/ПЭ системы безопасности (см. [3], подраздел 7.7), то аттестацию не повторяют.

11.2.2 Аттестация ПО должна проводиться в соответствии с планом аттестации ПО.

11.2.3 По результатам аттестации ПО должна быть составлена документация.

11.2.4 Для каждой функции безопасности в документации по аттестации ПО должны быть указаны:

а) хронологические записи о выполненных в процессе аттестации процедурах;

б) план, по которому проводилась аттестация ПО;

в) наименование (идентификация) функции, проходившей аттестацию (анализ или испытания) вместе со ссылками на план аттестации;

г) инструментальные средства и оборудование;

д) результаты аттестации;

е) расхождение между ожидаемыми и полученными результатами.

11.2.5 По обнаруженным расхождениям между ожидаемыми и полученными результатами оформляют документацию о проведенном анализе и принятом решении, продолжать ли аттестацию или сделать заявку на изменения и вернуться к предшествующим этапам жизненного цикла обеспечения безопасности.

Примечание — Требования 11.2.2 и 11.2.5 основаны на общих требованиях ГОСТ Р МЭК 61508-1, подраздел 7.14.

11.2.6 Аттестация ПО, относящегося к обеспечению безопасности, должна соответствовать следующим требованиям:

а) основным методом аттестации ПО должны быть испытания [синтез динамических изображений (анимация) и моделирование могут использоваться дополнительно];

б) ПО должно быть проверено имитацией:

1) входных сигналов, существующих при нормальной эксплуатации,

2) ожидаемых происшествий,

3) нежелательных условий, требующих вмешательства системы;

в) поставщик и/или разработчик должны представить документацию о результатах аттестации ПО и всю относящуюся к делу документацию разработчику системы с тем, чтобы он мог выполнить требования ГОСТ Р МЭК 61508-1 и [3].

11.2.7 Требования к квалификации инструментальных средств ПО заключаются в следующем:

а) оборудование, используемое при аттестации, должно быть квалифицировано в соответствии со спецификацией, согласующейся с национальным стандартом Российской Федерации (при наличии), или общепринятой процедурой;

б) должно быть подтверждено, что все использованные при аттестации инструментальные средства, аппаратура или программное обеспечение, соответствуют поставленной цели.

Примечание — В настоящем стандарте под «квалификацией» подразумевается деятельность, подтверждающая, что все конкретные требования спецификаций безопасности к инструментальным средствам ПО удовлетворены.

11.2.8 К результатам аттестации ПО предъявляются следующие требования:

а) испытания должны показать, что все заданные требования к безопасности ПО правильно выполняются и что ПО не выполняет непредназначенных ему функций;

б) по каждому испытанию и его результатам должна быть составлена документация для проведения последующего анализа и независимой оценки в соответствии с требуемым уровнем полноты безопасности (см. ГОСТ Р МЭК 61508-1, пункт 8.2.12);

в) внесенные в документацию результаты должны подтверждать, что ПО прошло аттестацию либо объяснять причины непрохождения аттестации.

12 Правила модификации программного обеспечения

12.1 Целью настоящего раздела является установление информации и относящихся к ПО процедур, необходимых для подтверждения того, что безопасность Э/Э/ПЭ системы безопасности сохраняется в процессе эксплуатации и модификации.

Требования к модификации ПО приведены в [3], подраздел 7.6 и подраздел 12.2 настоящего стандарта.

Примечание — В [3] определено, что ПО (в отличие от аппаратной части ПЭС) не обслуживается, но только модифицируется.

12.2 Перед проведением любой модификации ПО (корректировки, улучшения или приспособления) должен быть составлен план применяемых процедур модификации (см. ГОСТ Р МЭК 61508-1, подраздел 7.16).

Примечания

1 Требования настоящего подраздела применяют, прежде всего, для изменений, проводимых на этапе эксплуатации ПО. Изменения могут также применяться в процессе компоновки ПЭ и на этапах общей установки и ввода в эксплуатацию ПЭ систем (см. [2], подраздел 7.13).

2 Пример модели процедуры модификации представлен в [2], рисунок 9.

12.2.1 Модификацию допускается проводить только при наличии утвержденной заявки на модификацию ПО в соответствии с процедурами, установленными при планировании безопасности, в которой подробно описаны:

а) опасности, на которые может оказать влияние предлагаемая модификация ПО;

б) предлагаемое изменение в ПО;

в) причины изменения.

Примечание — Причиной подачи заявки на модификацию может служить, например:

- функциональная безопасность ниже заданной;
- систематические отказы;
- модификация технических средств или его использование;
- модификация требований к общей безопасности;
- анализ производительности ПО при эксплуатации и обслуживании, который показал производительность ниже заданной;
- контрольная проверка функциональной безопасности ПО.

12.2.2 Должен проводиться анализ, выявляющий влияние предложенной модификации ПО на функциональную безопасность Э/Э/ПЭ системы безопасности, для определения:

а) необходимости проведения анализа опасности и риска;

б) этапа цикла обеспечения безопасности ПО, который необходимо повторить.

12.2.3 По результатам анализа влияния, полученным в соответствии с 12.2.2, должна быть составлена документация.

12.2.4 После модификации, оказавшей влияние на безопасность Э/Э/ПЭ системы безопасности, необходимо вернуться к соответствующему этапу цикла обеспечения безопасности ПО. Все последующие этапы жизненного цикла ПО должны быть повторены в соответствии с процедурами, установленными настоящим стандартом для конкретных этапов жизненного цикла ПО (см. приложение А).

Примечание — Может оказаться необходимым проведение полного анализа опасности и риска, который может вызвать необходимость установления уровней безопасности, отличных от ранее оговоренных для систем обеспечения безопасности и внешних средств снижения риска.

12.2.5 Планирование безопасности для модификации ПО, относящегося к обеспечению безопасности, должно включать в себя:

а) перечень персонала требуемой компетентности ([2], приложение В);

б) детальную спецификацию модификации;

в) планирование верификации;

г) повторную аттестацию и испытание модифицированного ПО в соответствии с уровнем полноты безопасности.

12.2.6 Модификация должна проводиться в соответствии с планом.

12.2.7 Все подробности модификации ПО должны быть изложены в документации, включая ссылки на:

а) заявку на модификацию и повторную настройку ПЭС;

б) результаты анализа влияния на функциональную безопасность, предложенной модификации ПО, а также принятые решения с соответствующими обоснованиями;

в) предысторию управления конфигурацией ПО;

г) отклонения от условий нормальной эксплуатации ПО.

12.2.8 Подробная информация о подробностях всех модификаций должна быть внесена в документацию (например, журнал регистрации). Документация должна включать в себя повторные проверку и подтверждение данных и результатов.

12.2.9 Оценка модификации или повторной настройки должна зависеть от результатов анализа влияния и уровня полноты безопасности ПО.

13 Правила оценки функциональной безопасности программного обеспечения

13.1 Требования [2], раздела 8 применимы для оценки ПО, относящегося к обеспечению безопасности.

13.2 Если иное не оговорено в национальных стандартах Российской Федерации, минимальный уровень независимости экспертов, оценивающих функциональную безопасность, должен соответствовать указанному в [2], 8.2.12.

13.3 При оценке функциональной безопасности допускается использовать результаты деятельности по ГОСТ Р МЭК 61508-3, приложение А, таблица А.10.

Примечание — Выбор методов по ГОСТ Р МЭК 61508-3, приложения А и В, не гарантирует, что будет достигнут требуемый уровень полноты безопасности. При проведении оценки должны также учитываться:

- обоснованность и согласованность выбранных методов, языков программирования и инструментальных средств со всем циклом разработки;
- степень понимания разработчиками используемых ими методов;
- соответствуют ли методы, языки программирования и инструментальные средства разрешению проблем, возникающих при разработке.

Приложение А
(справочное)

Жизненный цикл безопасности программного обеспечения

Таблица А.1 — Этапы жизненного цикла безопасности ПО

Этап цикла обеспечения безопасности ПО	Цель	Входные данные	Выходные данные
1 Спецификация требований по безопасности программного обеспечения	Составить спецификацию требований безопасности ПО в отношении требуемых функций безопасности и соответствия уровню полноты безопасности ПО. Составить спецификацию требований к функциям безопасности ПО для каждой ПЭС безопасности для выполнения требуемых функций безопасности. Составить спецификацию требований соответствия ПО уровню полноты безопасности для каждой ПЭС, необходимой для достижения уровня полноты безопасности, заданного для каждой функции безопасности, адресованной этой ПЭС безопасности	Спецификация требований по безопасности Э/Э/ПЭС [2]	Спецификация требований безопасности ПО
2 Планирование аттестации ПО	Разработать план аттестации программного обеспечения	Спецификация требований безопасности ПО	План аттестации программного обеспечения
3 Проектирование и разработка программного обеспечения	Архитектура: - создать архитектуру ПО, отвечающую заданным требованиям безопасности ПО в отношении требуемого уровня полноты безопасности; - рассмотреть и оценить требования, возлагаемые на ПО архитектурой ПЭС безопасности, включая значение взаимодействия аппаратуры и ПО ПЭС для безопасности контролируемых технических средств (КТС)	Спецификация требований безопасности ПО. Конструкция архитектуры аппаратуры ПЭС [3]	Описание конструкции архитектуры ПО. Спецификация компоновочных испытаний архитектуры ПО. Спецификация компоновочных испытаний ПО ПЭС [3]
4 Проектирование и разработка ПО	Средства инструментальной поддержки и языки программирования: выбрать подходящий комплект инструментальных средств, включая языки и компиляторы, на протяжении всего цикла обеспечения безопасности ПО, который способствует верификации, аттестации, оценке и модификации	Спецификация требований безопасности ПО. Описание конструкции архитектуры ПО	Инструментальные средства разработки и стандарты кодирования. Выбор инструментальных средств разработки
5 Проектирование и разработка ПО	Рабочий проект и разработка системы ПО. Спроектировать и изготовить ПО, соответствующее заданным требованиям безопасности ПО в отношении заданного уровня полноты безопасности, поддающееся анализу и верификации, которое можно безопасно модифицировать	Описание архитектуры ПО. Средства инструментальной поддержки и стандарты кодирования	Спецификация конструкции системы программного обеспечения. Спецификация компоновочных испытаний системы ПО

Продолжение таблицы А.1

Этап цикла обеспечения безопасности ПО	Цель	Входные данные	Выходные данные
6 Проектирование и разработка ПО	Рабочий проект и разработка отдельных модулей ПО: спроектировать и изготовить ПО, соответствующее заданным требованиям по безопасности ПО в отношении заданного уровня полноты безопасности, которое поддается анализу и верификации и которое можно модифицировать	Спецификация конструкции системы ПО. Средства инструментальной поддержки и стандарты кодирования	Спецификация конструкции модуля ПО. Спецификация испытаний модуля ПО
7 Проектирование и разработка ПО	Детальное кодирование: спроектировать и изготовить ПО, соответствующее заданным требованиям безопасности ПО в отношении заданного уровня полноты безопасности, которое поддается анализу и верификации и может быть безопасно модифицировано	Спецификация конструкции модуля ПО	Перечень исходных кодов. Отчет с обзором кодов
8 Проектирование и разработка ПО	Испытания модуля ПО: верификацией установить, что требования по безопасности ПО (в отношении требуемых функций безопасности ПО) достигнуты, показать, что каждый модуль ПО выполняет предназначенные функции и не выполняет непредназначенные	Спецификация испытаний модуля ПО. Перечень исходных кодов. Отчет с обзором кодов	Результаты испытаний модуля ПО. Проверенные и испытанные модули ПО
9 Проектирование и разработка ПО	Компоновочные испытания ПО: верификацией установить, что требования по безопасности ПО (в отношении требуемых функций безопасности ПО) достигнуты — показать, что все модули, компоненты и подсистемы ПО взаимодействуют правильно и выполняют предназначенные им функции и не выполняют непредназначенные функции	Спецификация компоновочных испытаний системы ПО	Результаты компоновочных испытаний системы ПО. Поверенная и испытанная система ПО
10 Компоновка ПЭС (аппаратуры и ПО)	Установить ПО на аппаратуру ПЭ. Объединить ПО и аппаратуру в ПЭС, обеспечивающую безопасность, для подтверждения их совместимости и соответствия требованиям заданного уровня полноты безопасности	Спецификация компоновочных испытаний архитектуры ПО. Спецификация компоновочных испытаний ПЭС. Скомпонованная ПЭС	Результаты компоновочных испытаний архитектуры ПО. Результаты компоновочных испытаний ПЭ. Поверенная и испытанная ПЭС
11 Процедуры эксплуатации и модификации ПО	Обеспечить информацию и процедуры, относящиеся к ПО, обеспечивающему поддержание функциональной безопасности ПЭС при эксплуатации и модификации	Поверенная и испытанная ПЭС	Процедуры эксплуатации и обслуживания ПО
12 Аттестация ПО	Убедиться, что скомпонованная система соответствует заданным требованиям безопасности ПО при заданном уровне полноты безопасности	План аттестации ПО	Результаты аттестации ПО. Аттестованное ПО
13 Модификация ПО	Провести исправление, улучшение или адаптацию аттестованного ПО для обеспечения поддержания заданного уровня полноты безопасности	Процедуры модификации ПО. Заявка на модификацию ПО	Результаты анализа влияния модификации ПО. Журнал регистрации модификации ПО

Окончание таблицы А.1

Этап цикла обеспечения безопасности ПО	Цель	Входные данные	Выходные данные
14 Верификация ПО	В объеме, соответствующем уровню полноты безопасности, испытать и оценить выходные данные этапа цикла обеспечения безопасности ПО для проверки их правильности и согласованности с выходными данными и стандартами, являвшимися входными данными на этом этапе	Соответствующий план верификации (зависит от этапа)	Отчет о верификации (зависит от этапа)
15 Оценка функциональной безопасности ПО	Исследовать и прийти к заключению о функциональной безопасности, достигнутой ПЭС безопасности	План оценки функциональной безопасности ПО	Отчет об оценке функциональной безопасности ПО

Библиография

[1] МЭК 61508-6:2000 Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3

[2] МЭК 61508-1:1998 Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

[3] МЭК 61508-2:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам электрическим/электронным/программируемым электронным, связанным с безопасностью

[4] ЕН 50126:1999 Применения на железнодорожном транспорте. Спецификации и доказательства надежности, эксплуатационной готовности, ремонтопригодности и безопасности для использования на железных дорогах

[5] ЕН 50128:1999 Применения на железнодорожном транспорте. Программное обеспечение для систем управления и обеспечения безопасности на железнодорожном транспорте

УДК 62-783:614.8:331.454:006.354 ОКС 25.040.40 ОКСТУ 4002 П87

Ключевые слова: безопасность функциональная, жизненный цикл систем, электрические компоненты, электронные компоненты, программируемые электронные компоненты и системы, системы, связанные с безопасностью, планирование функциональной безопасности, программное обеспечение, уровень полноты безопасности

Редактор *В.Н. Копысов*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 18.08.2009. Подписано в печать 14.09.2009. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 2,79. Уч.-изд. л. 2,40. Тираж 121 экз. Зак. 582.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.