МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34673.3— 2022

ТЯГОВЫЙ ПОДВИЖНОЙ СОСТАВ ЖЕЛЕЗНОДОРОЖНЫЙ

Часть 3

Методы контроля выполнения функций устройствами, обеспечивающими безопасность движения

Издание официальное

Москва
Российский институт стандартизации
2022

Предисловие

Цели, основные принципы и общие правила проведения работ по международной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 РАЗРАБОТАН Акционерным обществом «Научно-исследовательский институт железнодорожного транспорта» (АО «ВНИИЖТ»)

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 524 «Железнодорожный транспорт»

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 22 ноября 2022 г. № 156-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Казахстан	KZ	Госстандарт Республики Казахстан
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 9 декабря 2022 г. № 1462-ст межгосударственный стандарт ГОСТ 34673.3—2022 введен в действие в качестве национального стандарта Российской Федерации с 1 мая 2024 г. с правом досрочного применения

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

Содержание

Введение

Установленные в настоящем стандарте методы контроля устройств, обеспечивающих безопасность движения, уточняют и дополняют методы по функциональной безопасности, приведенные в ГОСТ 33435.

Настоящий стандарт предоставляет основу методического обеспечения проверки уровня полноты безопасности, испытаний на функциональную безопасность программируемых устройств на тяговом железнодорожном подвижном составе, а также для применения разработанных методик к программно-аппаратным комплексам, с учетом влияния на безопасность как используемых программных средств, так и схемных и аппаратных решений.

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

ТЯГОВЫЙ ПОДВИЖНОЙ СОСТАВ ЖЕЛЕЗНОДОРОЖНЫЙ

Часть 3

Методы контроля выполнения функций устройствами, обеспечивающими безопасность движения

Railway tractive rolling stock.
Part 3. Inspection methods for devices ensuring traffic safety

Дата введения — 2024—05—01
с правом досрочного применения

1 Область применения

Настоящий стандарт распространяется на программируемые устройства, обеспечивающие безопасность движения тягового железнодорожного подвижного состава (ТПС), предназначенного для грузовых и пассажирских перевозок по железнодорожным путям шириной колеи 1520 мм.

Настоящий стандарт устанавливает методы контроля функциональной безопасности программируемых устройств, обеспечивающих безопасность движения ТПС на стадиях разработки (модернизации) и производства данных устройств.

Настоящий стандарт распространяется также на программируемые устройства, обеспечивающие безопасность движения самоходного специального подвижного состава.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие межгосударственные стандарты:

ГОСТ 12.0.004 Система стандартов безопасности труда. Организация обучения безопасности труда. Общие положения

ГОСТ 19.402 Единая система программной документации. Описание программы

ГОСТ 19.501 Единая система программной документации. Формуляр. Требования к содержанию и оформлению

ГОСТ 19.502 Единая система программной документации. Описание применения. Требования к содержанию и оформлению

ГОСТ 27.301 Надежность в технике. Расчет надежности. Основные положения

ГОСТ 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ 31814[1)] Оценка соответствия. Общие правила отбора образцов для испытаний продукции при подтверждении соответствия

ГОСТ 33432 Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта

ГОСТ 33433 Безопасность функциональная. Управление рисками на железнодорожном транспорте

ГОСТ 33435—2015 Устройства управления, контроля и безопасности железнодорожного подвижного состава. Требования безопасности и методы контроля

ГОСТ 34008 Железнодорожная техника. Правила подготовки обоснования безопасности

[1)] В Российской Федерации действует ГОСТ Р 58972—2020.

Издание официальное

ГОСТ 34009—2016 Средства и системы управления железнодорожным тяговым подвижным составом. Требования к программному обеспечению

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации (www.easc.by) или по указателям национальных стандартов, издаваемым в государствах, указанных в предисловии, или на официальных сайтах соответствующих национальных органов по стандартизации. Если на документ дана недатированная ссылка, то следует использовать документ, действующий на текущий момент, с учетом всех внесенных в него изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то следует использовать указанную версию этого документа. Если после принятия настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение применяется без учета данного изменения. Если ссылочный документ 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 **архитектура программного обеспечения:** Структура программы или вычислительной системы, которая включает программные компоненты, видимые снаружи свойства этих компонентов, а также отношения между ними.

3.2 **архитектура системы:** Конкретная конфигурация и принципы взаимодействия ее основных элементов.

3.3

буфер: Рабочая область памяти при пересылке данных.

Примечание — При операции ввода данные заносят в буферную область.

[ГОСТ 19781—90, статья 81]

3.4 **динамический анализ кода программы:** Вид работ по инструментальному исследованию программы, основанный на анализе кода программы в режиме непосредственного исполнения (функционирования) кода.

3.5

доказательство безопасности; ДБ: Документированное подтверждение того, что объект выполняет все заданные требования к функциональной безопасности.

[ГОСТ 33432—2015, пункт 3.1.5]

3.6 **защищенность информации от несанкционированного доступа:** Способность системы защитить информацию и данные от их несанкционированного прочтения или изменения другими системами и лицами, за исключением систем и лиц, допущенных к ним.

3.7 **защищенность от возможности случайных изменений информации:** Способность системы защитить информацию от несанкционированных и непреднамеренных воздействий (при отказах и сбоях аппаратной и программной частей системы).

3.8 **защищенность от компьютерных вирусов:** Способность системы предотвратить опасные состояния ТПС или его оборудования при появлении компьютерных вирусов.

3.9 **защищенность от ошибочных действий персонала:** Способность системы предотвратить опасные состояния ТПС или его оборудования при возможных ошибочных действиях персонала.

3.10 **канал:** Элемент или группа элементов системы управления, которые реализуют элемент функции безопасности.

Примечание — Канал используется для передачи информации при реализации функций безопасности.

3.11 **компьютерный вирус:** Программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области, оборудование сетей, а также осуществлять иные деструктивные действия.

3.12 **контур безопасности:** Совокупность технических и алгоритмических средств, реализующих конкретную функцию безопасности.

3.13 **несанкционированный доступ к программным средствам:** Доступ к программам, записанным в электронной памяти, а также к документации на эти программы, осуществленный с нарушением установленных правил.

3.14

обоснование безопасности; ОБ: Вид документа, содержащий анализ риска, а также сведения из конструкторской, эксплуатационной, технологической документации о минимально необходимых мерах по обеспечению безопасности, сопровождающий продукцию на всех стадиях жизненного цикла и дополняемый сведениями о результатах оценки рисков на стадии эксплуатации после проведения ремонта.

[ГОСТ 34008—2016, пункт 3.1.3]

3.15

опасный отказ (железнодорожной техники): Событие, в результате которого железнодорожная техника переходит из исправного, работоспособного или частично работоспособного состояния в опасное состояние.

[ГОСТ 32192—2013, статья 27]

3.16 **отсутствие дополнительных, непредусмотренных в документации возможностей:** Соответствие свойствам и характеристикам, описанным в сопроводительной документации.

3.17

политика обеспечения безопасности: Официально утвержденный руководством организации документ, в котором отражены общие намерения и направления деятельности организации в части обеспечения безопасности объекта железнодорожного транспорта от потенциальных опасностей.

[ГОСТ 33432—2015, пункт 3.1.18]

3.18

полнота безопасности: Степень уверенности в том, что объект железнодорожного транспорта будет выполнять заданные функции безопасности при данных условиях эксплуатации в заданный период времени.

Примечание — Различают полноту безопасности в отношении систематических отказов, которую чаще всего оценивают качественно, и полноту безопасности в отношении случайных отказов, характеризуемую количественными показателями безопасности (например, интенсивностью опасного отказа).

[ГОСТ 33432—2015, пункт 3.1.19]

3.19

программа обеспечения безопасности; ПОБ: Документ, устанавливающий комплекс взаимоувязанных организационных и технических мероприятий, методов, средств, требований и норм, направленных на выполнение установленных в документации на объект железнодорожного транспорта требований функциональной безопасности.

[ГОСТ 33432—2015, пункт 3.1.20]

3.20

программное обеспечение электронных систем подвижного состава; ПО: Продукт интеллектуальной деятельности, включающий программы, процедуры, данные, правила и информацию, имеющую отношение к работе системы обработки данных.

[ГОСТ 34056—2017, статья 3.2.141]

3.21

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ 33432—2015, пункт 3.1.22]

3.22

сбой (программного обеспечения): Самоустраняющийся отказ или однократный отказ, устраняемый вмешательством оператора.

[ГОСТ 34009—2016, пункт 3.10]

3.23 **статический анализ кода:** Совокупность методов контроля соответствия функциональных возможностей программного обеспечения требованиям документации, основанных на структурном анализе и декомпозиции исходных текстов программ, производимых без реального выполнения исследуемых программ.

3.24 **технические средства (железнодорожного транспорта):** Техническое средство или совокупность технических средств, предназначенные для обеспечения перевозочного процесса на железнодорожном транспорте.

Примечание — К железнодорожным техническим средствам относятся объекты инфраструктуры железнодорожного транспорта и железнодорожный подвижной состав, а также их составные части, представляющие собой функциональную единицу, которую можно рассматривать в отдельности.

3.25

техническое диагностирование: Определение технического состояния объекта.
[ГОСТ 20911—89, статья 4]

3.26

уровень полноты безопасности; УПБ: Обобщающий показатель безопасности, определяющий необходимую степень уверенности того, что объект будет выполнять заданные функции безопасности.

Примечания
1 УПБ включает:
- значение (диапазон значений) количественного целевого показателя безопасности;
- комплекс мероприятий, осуществляемых для достижения полноты безопасности в отношении систематических отказов.
2 Существует четыре УПБ — 1, 2, 3, 4. УПБ, равный 4, характеризует наибольшую полноту безопасности, уровень, равный 1, отвечает наименьшей полноте безопасности.

[ГОСТ 33432—2015, пункт 3.1.28]

3.27

уровень полноты безопасности программного обеспечения; УПБ: Дискретный уровень (принимающий одно из четырех возможных значений от 1 до 4), определяющий полноту безопасности программного обеспечения системы, связанной с безопасностью.
[ГОСТ 34009—2016, пункт 3.13]

3.28 **устройство, обеспечивающее безопасность движения (устройство):** Электрическая, электронная и программируемая (в т.ч. микропроцессорная) система, элемент или блок (программируемые электронные), от состояния которых зависит безопасность тягового подвижного состава и объектов инфраструктуры.

3.29 **функциональная безопасность (системы управления тяговым подвижным составом):** Свойство системы управления тяговым подвижным составом выполнять требуемые функции безопасности при всех возможных состояниях системы и условиях его использования.

3.30

функция безопасности: Функция, реализуемая объектом железнодорожного транспорта или его составными частями, которая предназначена для достижения или поддержания безопасного состояния по отношению к конкретному опасному событию.
[ГОСТ 33432—2015, пункт 3.1.30]

4 Проверяемые показатели

Контроль параметров устройства проводят в соответствии с ГОСТ 34009, ГОСТ 33435 по показателям, указанным в таблице 1.

Таблица 1 — Контролируемые показатели

Наименование показателя	Номер подраздела настоящего стандарта	Обозначение структурного элемента ГОСТ 34009—2016	Обозначение структурного элемента ГОСТ 33435—2015
1 Назначенный уровень полноты безопасности (составляющая функциональной безопасности)	7.1	4.4	4.1
2 Соответствие реализованного уровня полноты безопасности (составляющая функциональной безопасности)	7.2	4.4	4.1

Окончание таблицы 1

Наименование показателя	Номер подраздела настоящего стандарта	Обозначение структурного элемента ГОСТ 34009—2016	Обозначение структурного элемента ГОСТ 33435—2015
3 Реализация функций безопасности (составляющая функциональной безопасности)	7.3	4.4	А.2 (приложение А)
4 Соответствие свойствам и характеристикам, описанным в сопроводительной документации. Отсутствие дополнительных, непредусмотренных в документации возможностей	7.4	4.2	5.3.1
5 Защищенность информации от несанкционированного доступа	7.5	4.2, 7.1	А.4 (приложение А)
6 Защищенность от компьютерных вирусов	7.6	4.2, 7.3	А.4 (приложение А)
7 Защищенность от ошибочных действий персонала	7.7	4.4, таблица А.1	5.3.1
8 Защищенность от возможности случайных изменений информации, последствий сбоев и перезагрузок ПО	7.8	4.2, 6.5	5.3.1
9 Техническое диагностирование оборудования ТПС с наличием средств сигнализации и информирования о нарушении исправного состояния	7.9	4.2	А.2, А.3 (приложение А)

5 Общие требования и требования безопасности

5.1 Перед началом испытаний руководитель испытаний проводит целевой инструктаж по охране труда для персонала в соответствии с ГОСТ 12.0.004. По окончании инструктажа персонал расписывается в журнале регистрации целевого инструктажа.

5.2 Анализ исходного кода ПО, являющегося интеллектуальной собственностью разработчика, допускается проводить на территории разработчика или испытательного центра (лаборатории), или иной организации по согласованию сторон.

5.3 В процессе проведения испытаний при ошибочных действиях персонала или самопроизвольном нарушении функционирования устройства необходимо выключить его и прекратить испытания.

Испытания возобновляют после устранения выявленных нарушений.

6 Условия и порядок проведения испытаний и требования к средствам измерений

6.1 Перед началом контроля функциональной безопасности для устройства должны быть предъявлены документы, указанные в таблице 2.

Таблица 2 — Перечень документов

Наименование документа	Обозначение стандарта
1 ДБ	ГОСТ 33432, ГОСТ 33435
2 ОБ	ГОСТ 34008
3 ПОБ	ГОСТ 33432, ГОСТ 33435
4 Политика обеспечения безопасности (по требованию)	ГОСТ 33432
5 Описание применения	ГОСТ 19.502
6 Формуляр	ГОСТ 19.501
7 Описание программы	ГОСТ 19.402

В ДБ, ОБ, ПОБ и политике обеспечения безопасности должны быть определены функции безопасности и их УПБ.

6.2 Отбор образцов с установленным на них ПО и объем выборки для испытаний следует устанавливать в соответствии с ГОСТ 31814.

6.3 Идентификацию отобранного образца следует проводить по серийному или заводскому номеру устройства и номеру версии ПО (для программируемых устройств).

ПО должно соответствовать актуальной версии в соответствии с эксплуатационной документацией.

6.4 Исходные тексты программ должны содержать комментарии, максимально облегчающие понимание их логической работы.

6.5 Во время проведения испытаний запрещается вносить изменения в ПО и схемы подключения, если это не предусмотрено эксплуатационной документацией на устройство или порядком испытаний.

6.6 Испытания устройства возможно проводить на производственных площадках изготовителя, в лабораториях на специализированных стендах либо в эксплуатационных условиях (на стоянке и в движении) на подвижном составе. Место проведения испытаний для каждого устройства и вида испытаний (указывается в рабочей методике) определяют индивидуально, исходя из возможностей безопасного проведения испытаний и минимизации затрат.

6.7 Количество измерений, необходимое для обеспечения достоверности, должно устанавливаться программой и методикой испытаний исходя из конкретных условий и задач.

6.8 Средства измерений для контроля параметров устройства должны соответствовать законодательству в области единства измерений.

7 Методы контроля

7.1 Назначенный уровень полноты безопасности

7.1.1 Проверку правильности назначенного разработчиком УПБ допускается осуществлять на разных стадиях жизненного цикла при проведении испытаний ТПС в целом либо по требованию заказчика при выполнении оценки отдельных программируемых компонентов устройства, содержащего функции безопасности, для которых УПБ не установлен ГОСТ 33435.

7.1.2 УПБ для систем задают исходя из критичности последствий, которые могут возникнуть вследствие опасного отказа одной или нескольких функций безопасности и вероятности наступления данного события.

Если устройство выполняет набор функций безопасности, для которых определены разные УПБ, то значение вероятности (интенсивности) опасных отказов устройства следует устанавливать по наивысшему из этих уровней.

Диапазоны значений для назначения интенсивности опасных отказов для различных значений УПБ приведены в таблице 3.

Таблица 3 — Назначенное значение интенсивности опасных отказов для УПБ

УПБ	Максимально допустимая интенсивность опасных отказов $\lambda_р$, $ч^{-1}$
1	$10^{-6} \le \lambda_р < 10^{-5}$
2	$10^{-7} \le \lambda_р < 10^{-6}$
3	$10^{-8} \le \lambda_р < 10^{-7}$
4	$10^{-9} \le \lambda_р < 10^{-8}$

7.1.3 При контроле УПБ используют гипотезу, согласно которой интенсивность отказов компонента считается константной на протяжении всего срока службы системы.

7.1.4 Интенсивность опасного отказа для ТПС $\lambda_р$, $ч^{-1}$, с учетом эксплуатации ТПС только часть времени, вычисляют по формуле

$$\lambda_р = k_и \cdot \lambda_к, \quad (1)$$

где $k_и$ — коэффициент проявления риска, показывающий, какую часть времени ТПС находится в работе, вычисляемый по формуле

$$k_{и} = \frac{t}{T}, \quad (2)$$

где t — время пребывания ТПС в работе, ч;

T — общее время пребывания ТПС в эксплуатации, ч;

$\lambda_{к}$ — интенсивность опасного отказа в контуре безопасности, $ч^{-1}$.

Коэффициент проявления риска зависит от эксплуатационных показателей ТПС.

7.1.5 Блок-схема обобщенного алгоритма контроля УПБ приведена на рисунке 1. Система рассматривается как совокупность взаимосвязанных функций безопасности, каждой из которых присваивают требуемый УПБ.

Входными данными являются риски системы (блок 1). Для каждого риска определяют функции безопасности (блок 2). Каждой функции безопасности назначают свой УПБ (блок 3). Выходными данными являются УПБ для всех функций безопасности.

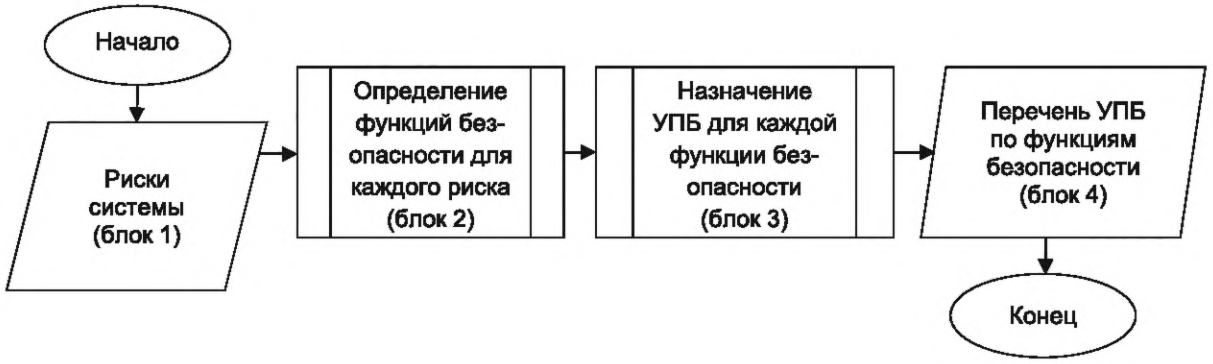
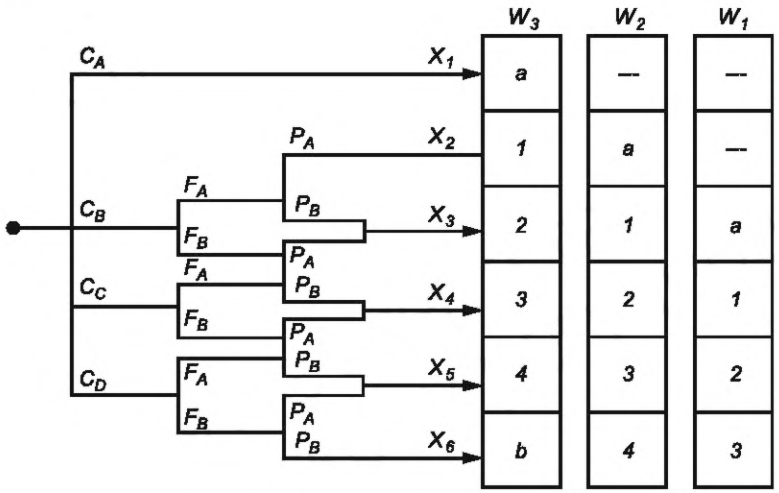


Рисунок 1 — Блок-схема обобщенного алгоритма контроля УПБ

7.1.6 Контроль правильности назначенного УПБ для устройства ТПС или отдельных систем проводят на базе оценки рисков у ТПС или по рискам, связанным с испытуемой системой в соответствии с ГОСТ 33433. УПБ определяют экспертно либо на основе подобных функций безопасности в аналогичных системах.

Пример — На рисунке 2 приведена схема определения УПБ в зависимости от имеющихся рисков и тяжести последствий.



C_A — C_D — параметры последствия риска с возможными последствиями сценария; F_A, F_B — параметры возможных сценариев событий; P_A, P_B — параметры возможности избежать риска; X_1 — X_6 — выходные параметры; W_1 — W_3 — параметры вероятности нежелательного события; --- — требования безопасности отсутствуют; a — специальные требования безопасности отсутствуют; b — требуются дополнительные устройства

Рисунок 2 — Схема определения УПБ в зависимости от имеющихся рисков и тяжести последствий

Параметры последствия риска С с индексами A, B, C, D показывают четыре возможных последствия сценария:

- C_A — один и более пострадавших с причинением средней тяжести и легкого вреда здоровью;

- C_B — один пострадавший с причинением тяжкого вреда здоровью;

- C_C — один погибший или от 2 до 10 пострадавших с причинением тяжкого вреда здоровью;

- C_D — два и более погибших;

- C_A — не требует УПБ.

C_B, C_C, C_D рассматривают при двух возможных сценариях событий:

- F_A — от редкого до частого пребывания в опасной зоне;

- F_B — от частого до постоянного пребывания в опасной зоне.

Эти события рассматривают по двум вариантам параметра возможности избежать опасного риска:

- P_A — возможно при определенных обстоятельствах избежать нежелательного события;

- P_B — практически невозможно избежать нежелательного события.

В результате выходные параметры X_1—X_6, соответствующие функциям безопасности, показывают требуемые УПБ с учетом вариативности:

- W_1 — вероятность нежелательного события весьма незначительная [понятие «незначительная вероятность» соответствует «либо не были вообще, либо о них все забыли» (λ_{W2}≈0,01 год$^{-1}$)];

- W_2 — небольшая вероятность нежелательного события [понятие «небольшая вероятность» соответствует выражению частоты события «такие случаи были» (λ_{W2}≈0,1 год$^{-1}$)];

- W_3 — относительно высокая вероятность наступления нежелательного события, вероятны частые повторения нежелательного события [понятие «относительно высокая вероятность» соответствует выражению частоты события «об этих случаях говорят» или в числовом эквиваленте: λ_{W3}≈1 год$^{-1}$ (один случай в год)].

В качестве примера рассмотрен случай риска неверных показаний датчика скорости при движении по ограничению скорости, например, на стрелочном переводе. Превышение скорости на 10 км/ч привело к динамическим усилиям по составу, в результате чего два человека сломали руку, упав с верхней полки, при этом был нанесен тяжкий вред здоровью одного человека (рисунок 2, ветвь C_B). Во время данного отказа в опасной зоне (на верхней полке) вероятно нахождение людей (рисунок 2, ветвь F_B), риска избежать практически невозможно (рисунок 2, ветвь P_B; выходная ветвь X_4), однако вероятность подобного отказа незначительна (вариативность W_1). Получен УПБ = 1.

7.1.7 При контроле УПБ проводят оценку правильности учета всех рисков, функций безопасности и назначенного УПБ для каждой функции безопасности в соответствии с 7.1.1—7.1.6.

7.1.8 На основании сопоставления полученных в ходе контроля данных с данными, предоставленными разработчиком, принимают решение о полноте назначенного УБП.

7.2 Соответствие реализованного уровня полноты безопасности

7.2.1 Контроль соответствия реализованного УПБ заданному допускается осуществлять на разных стадиях жизненного цикла при оценке функциональной безопасности ТПС в целом либо отдельных программируемых компонентов по требованию заказчика. Блок-схема контроля соответствия реализованного УПБ функции безопасности приведена на рисунке 3.

7.2.2 Оценку реализованного УПБ проводят на основании анализа проектной документации с использованием статистических данных по отказам, если они существуют. Определяют структуру реализации функций безопасности. На основе данных о принятых технических решениях проводят оценку ожидаемой интенсивности отказов всей системы. При наличии статистических данных по отказам значения ожидаемой интенсивности отказов могут быть уточнены. На основе интенсивности отказов определяют достигнутые УПБ устройств.

7.2.2.1 Для определения интенсивности опасных отказов оборудования необходимо провести анализ интенсивности отказов:

- определить возможные варианты развития ситуации в результате отказа;
- построить дерево событий для оценки вероятности опасных исходов;
- провести расчет вероятности опасных исходов на основе построенного дерева событий;
- провести расчет интенсивности опасных отказов на основе вероятности общей интенсивности отказов и вероятности опасных исходов.

7.2.2.2 Возможные варианты развития ситуации в результате отказа определяют экспертным методом для всей системы с функциями безопасности с учетом всех задействованных в ее работу компонентов, влияющих на исход события.

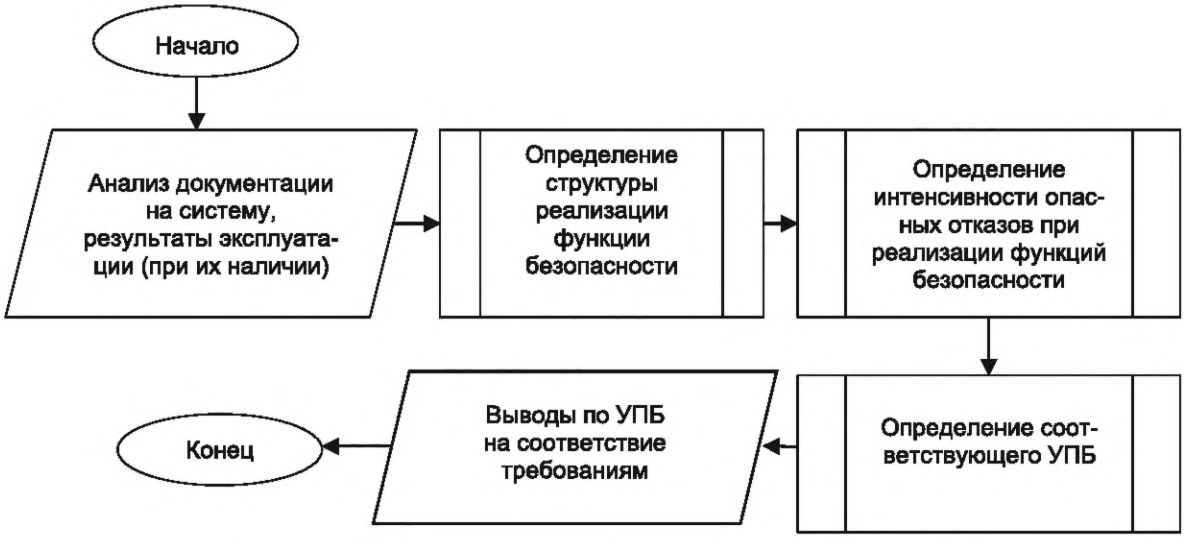


Рисунок 3 — Блок-схема оценки реализованного УПБ функций безопасности

7.2.2.3 Дерево событий строят для каждого вида отказа по следующим правилам:

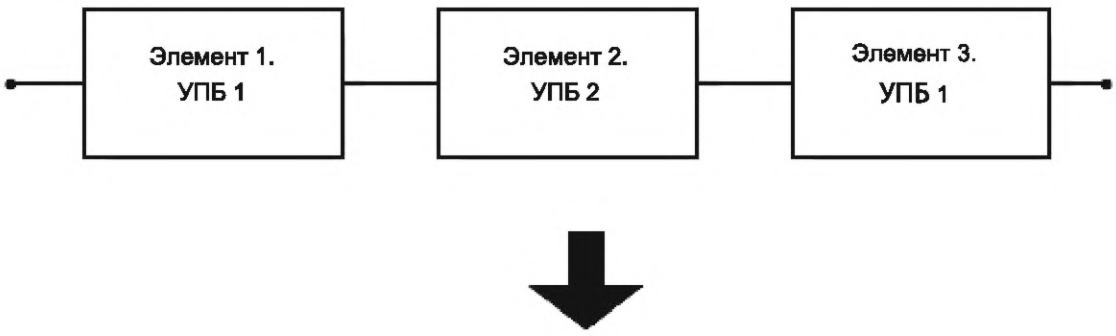
- вершину дерева ставят в соответствие исходной интенсивности отказов;
- каждая ветвь дерева соответствует цепочке последовательных событий;
- нижний уровень дерева соответствует множеству исходов;
- из одного узла дерева возможно перейти точно в два узла следующего уровня, один из которых соответствует наступлению следующего в цепочке события, второй — ненаступлению данного события;
- каждое ребро дерева помечают весом, равным вероятности наступления события.

Для определения вероятности того или иного события могут быть применены:

- экспертный метод;
- расчетный метод (например, структурные схемы надежности);
- комбинация экспертного и расчетного методов.

7.2.3 Для подтверждения УПБ устройства необходимо подтверждение соответствия УПБ аппаратных средств и ПО. При этом проводят разделение по отдельным устройствам или подсистемам, для которых могут быть определены показатели надежности.

7.2.4 На рисунке 4 приведен модуль, в котором некоторая часть контура безопасности реализуется с помощью последовательности из трех элементов. Максимально реализуемый УПБ определяют элементом, который имеет самый низкий УПБ.



Модуль соответствует функции безопасности с УПБ 1

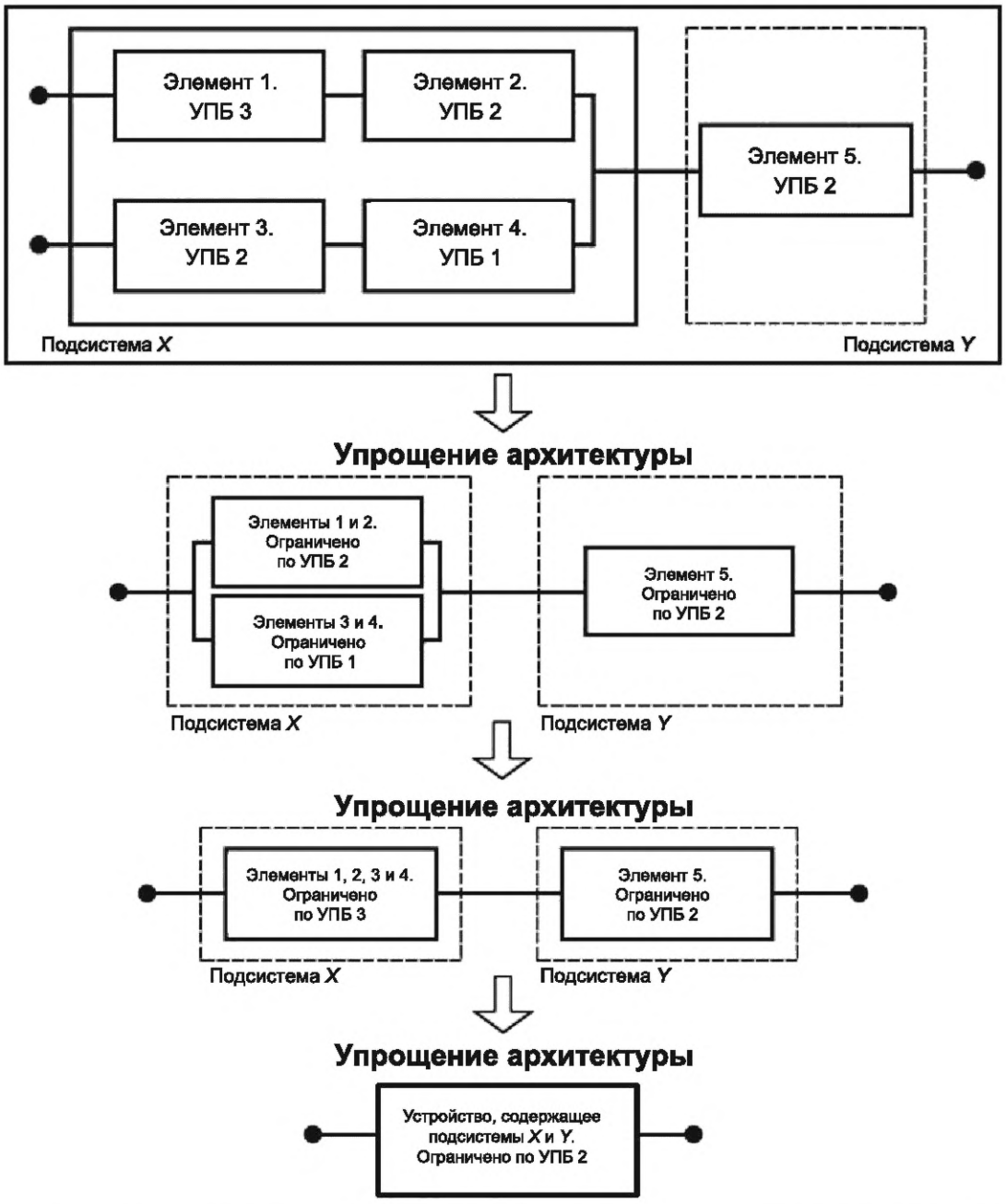
Рисунок 4 — Модуль, состоящий из последовательности трех элементов

7.2.5 В случае, когда функция безопасности реализуется в многоканальной архитектуре, изображенной на рисунке 5 (последовательно-параллельное соединение элементов подсистем *X* и *Y*), максимальный УПБ, который может быть достигнут для рассматриваемой функции безопасности, может быть определен:

- группированием последовательно соединенных элементов для каждого канала и затем определением максимального УПБ, который может быть достигнут для рассматриваемой функции безопасности для каждого канала;

- выбором канала с самым высоким УПБ, который может быть достигнут для рассматриваемой функции безопасности и определения максимальной полноты безопасности для полной подсистемы.

Примечание — Подсистемы, выполняющие функцию безопасности, считают полной системой, связанной с безопасностью, включая все элементы — от сенсоров до исполнительных устройств.



Примечание — Элементы 1 и 2 реализуют требуемую часть функции безопасности подсистемы X независимо от элементов 3 и 4 (резервирование).

Рисунок 5 — Определение максимального УПБ для смешанного соединения модулей

7.2.6 УПБ может быть повышен за счет введения технического диагностирования. При этом влияние на интенсивность отказов будет зависеть:

- от алгоритмов технического диагностирования;
- влияния системы обслуживания и восстановления после отказов.

При техническом диагностировании для каждого компонента оценивают долю опасных отказов, которые могут быть обнаружены с помощью диагностирования.

Общая интенсивность отказов λ суммарно равна интенсивности опасных отказов λ_S, которые могут быть выявлены при техническом диагностировании, и опасных отказов λ_D, которые не могут быть выявлены при техническом диагностировании.

7.2.7 Для аппаратных средств интенсивность отказов λ определяют с помощью средств теории надежности в соответствии с ГОСТ 27.301, а также в соответствии с нормативными документами, действующими на территории государства, принявшего стандарт[1)].

Если разработчик ПО использует готовые аппаратные средства с неизвестными параметрами надежности и схемными решениями, а также если функции системы реализуются на тех же аппаратных средствах, что и функции безопасности, могут быть использованы данные по гарантийному сроку используемых аппаратных средств с учетом времени пребывания в работе за время эксплуатации.

Пример — Если гарантийный срок $T_{гарант}$ = 1 год, а оборудование стоит на ТПС, т.е. коэффициент проявления риска в формуле (2) k_u = 0,5, то время наработки на отказ $T_{отк}$, ч, вычисляют по формуле

$$T_{отк} = \frac{T_{гарант}}{k_u} = \frac{8766}{0,5} = 17\ 532\ ч, \qquad (3)$$

тогда $\lambda_p = 0,57 \cdot 10^{-4}\ ч^{-1}$.

7.2.8 УПБ ПО считают достигнутым после получения положительных результатов при проверке:
- выполнения требований к архитектуре ПО;
- использования подходящего набора инструментальных средств, включая языки программирования и компиляторы;
- выполнения функций безопасности.

7.2.8.1 Подтверждение соответствия УПБ ПО устройства не допускается проводить отдельно от его аппаратных средств.

7.2.8.2 Основные требования к архитектуре и ПО в зависимости от УПБ приведены в таблице 4.

Таблица 4 — Основные требования к архитектуре и ПО в зависимости от УПБ

Метод (средство)	УПБ 1	УПБ 2	УПБ 3	УПБ 4
1 Программирование с проверкой ошибок	0	0	0	1
2 Постепенное отключение функций для парирования сбоев	0	0	1	1
3 Исправление ошибок методами искусственного интеллекта	0	1	1	1
4 Модульный подход	1	1	1	1
5 Использование доверительных/проверенных элементов ПО (при наличии)	1	1	1	1
6 Автоматизированные средства разработки спецификаций и проектирования	0	0	1	1
7 Циклическое поведение с гарантированным максимальным временем цикла	0	1	1	1
8 Архитектура с временным распределением	0	1	1	1
9 Статическое выделение ресурсов	0	0	1	1
10 Статическая синхронизация доступа к разделяемым ресурсам	0	0	0	1
11 Не использовать динамические объекты	0	1	1	1
12 Не использовать динамические переменные	0	0	1	1
13 Ограниченное использование прерываний	1	1	1	1
14 Ограниченное использование указателей	1	1	1	1
15 Ограниченное использование рекурсий	1	1	1	1

[1)] В Российской Федерации действует ГОСТ Р МЭК 61078—2021 «Надежность в технике. Структурная схема надежности».

Окончание таблицы 4

Метод (средство)	УПБ 1	УПБ 2	УПБ 3	УПБ 4
16 Не использовать неструктурированное управление в программах, написанных на языках высокого уровня	0	1	1	1
17 Не использовать автоматическое преобразование типов	0	1	1	1
Примечание — Цифрой 1 отмечены приемы и методы (средства), обязательные для данного УПБ; цифрой 0 — необязательные.				

7.2.8.3 С учетом имеющейся увеличенной сложности ПО системы безопасности должны обеспечивать:

- самоконтроль ПО;
- мониторинг программируемой электронной аппаратуры, датчиков и устройств привода.

7.2.8.4 Выполнение функций безопасности проверяют в соответствии с 7.3.

7.2.9 В целях достижения заданного УПБ контур безопасности может быть реализован в виде многоуровнего построения, содержащего системы, выполненные на различных принципах.

В контур безопасности могут входить:

- средства, программно выполняющие функции безопасности (1-й уровень);
- системы, контролирующие и предотвращающие нежелательные события (2-й уровень);
- защитные системы выявления опасности, способные с определенной долей вероятности не дать риску проявиться за счет использования автоматических или ручных защитных мер (3-й и последующие уровни).

Контуры безопасности приведены на рисунке 6.

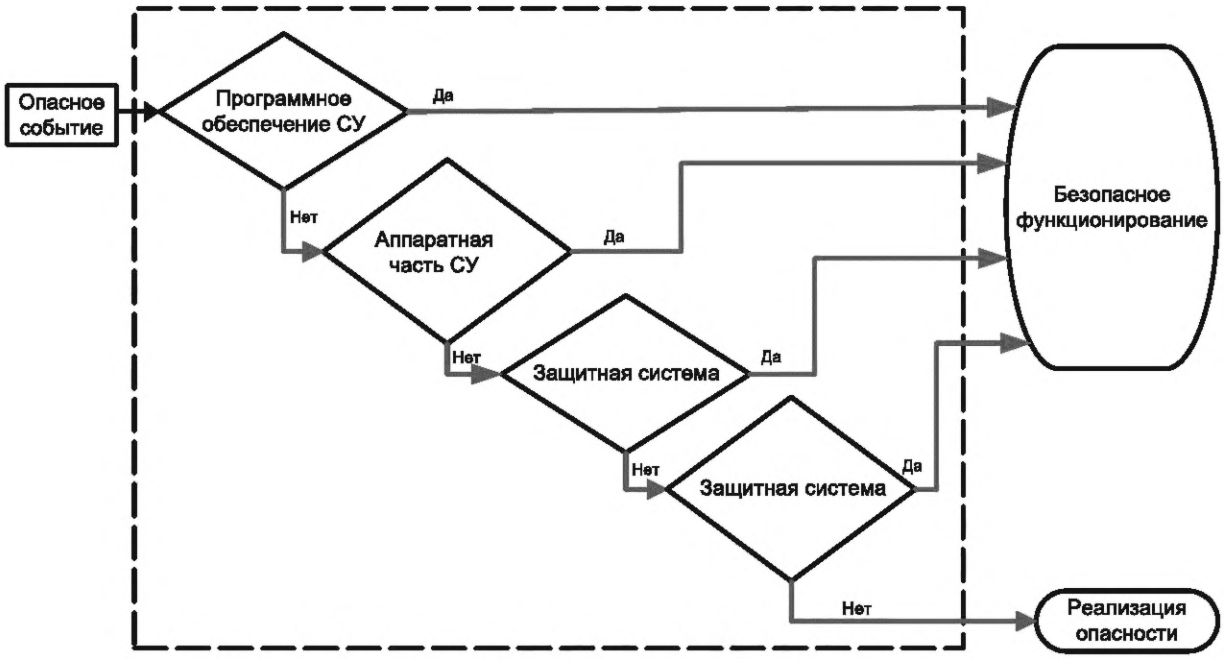


Рисунок 6 — Контуры безопасности

7.2.10 В качестве защитных систем могут быть использованы:

а) непрограммируемые электрические устройства:

1) главный (быстродействующий) выключатель;
2) блокировки шкафов с оборудованием;
3) блокировки дверей в электропоездах;
4) газовые реле и т.д.;

б) программируемые электрические устройства, при условии, что их система управления может функционировать без связи с центральной системой управления.

7.2.11 Дополнительным контуром безопасности является работа локомотивной бригады в случае ее своевременного уведомления об отказе в основном контуре, либо если ее работа не зависит от наличия такого отказа.

7.3 Реализация функций безопасности

7.3.1 Реализацию функций безопасности проверяют путем имитации функционирования в нормальных режимах работы, соответствующих технической документации и при наличии опасных ситуаций.

В нормальных режимах работы контролируют:

- входные и выходные сигналы, включая их последовательность и значения;
- другие критерии работы, например использование памяти, допустимые интервалы для значений рабочей информации и т.д.

При имитации опасных ситуаций, рассматривают случаи, связанные:

- с функционированием аппаратных средств программируемой электроники, не соответствующим технической документации;
- функционированием датчиков и устройств привода, не соответствующим технической документации;
- сбоями, происходящими вследствие ошибок в ПО, при нормальной эксплуатации устройства;
- сбоями, происходящими вследствие ошибок в ПО, при периодическом тестировании функций;
- несоответствием характеристик интерфейсов (производительность и время отклика);
- переполнением и потерей данных в памяти аппаратных средств программируемой электроники;
- недостаточной производительностью и временем отклика аппаратных средств программируемой электроники;
- ошибками управляющей деятельности локомотивной бригады.

7.3.2 Проверку выполнения функций безопасности осуществляют для следующих режимов работы устройства:

- проверки готовности к работе и/или запуска устройства;
- имитации нежелательных условий, требующих выполнения функций безопасности испытуемой системы.

7.3.3 В качестве основных приемов, имитирующих опасный отказ, может быть использовано, например одно из следующих имитационных воздействий:

- выключение аппаратуры во время функционирования ТПС;
- снятие напряжения питания с оборудования;
- отключение интерфейса устройства;
- короткое замыкание входных и выходных электрических цепей и т.д.

7.3.4 Решение о допустимости имитации отказов устройства путем короткого замыкания конкретной электрической цепи и необходимости применения при этом тех или иных вспомогательных средств принимают на основе анализа схемы электрических цепей и ее функционирования с учетом исключения повреждения оборудования вследствие замыкания, а также исключения опасных факторов для персонала при коротком замыкании (нагрев элементов электрической цепи или искрение, способные вызвать ожог, разлет частиц материалов электрооборудования и т. д.).

7.4 Соответствие свойствам и характеристикам, описанным в сопроводительной документации. Отсутствие дополнительных, непредусмотренных в документации возможностей

7.4.1 Проверяют описанные в сопроводительной документации алгоритмы работы.

7.4.2 Проводят проверку осуществления контроля в устройстве точности, полноты и правильности данных, как поступающих в программу, так и полученных в результате работы программы. Допускается использовать проверку функционирования ПО путем имитации событий в соответствии с 7.3.1.

7.4.3 В начале испытаний устройств проводят проверку контрольных сумм или результатов применения иного метода, применяемого для контроля правильности записи ПО на носитель, установленного в ГОСТ 34.11[1)] и нормативных документах, действующих на территории государства, принявшего стандарт.

7.4.4 Контроль на отсутствие дополнительных, непредусмотренных в документации возможностей может быть проведен с применением ручного, статического или динамического анализа кода ПО.

[1)] В Российской Федерации также действуют ГОСТ Р МЭК 61508-7—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства», ГОСТ Р 34.11—2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Выбор методов анализа осуществляет испытатель на основании сложности, объема объекта и неоднозначности результатов на каждом этапе испытаний. Для статического и динамического анализа кода ПО предпочтительно использовать специализированные программные средства.

7.4.5 При ручном анализе кода осуществляют:

- экспертизу исходного/восстановленного кода;
- выявление архитектурных уязвимостей определением неиспользуемых в алгоритмах участков кода;
- анализ участков кода, написанного с использованием языков программирования, отличных от заявленного в сопроводительной документации;
- проверку обоснованности применения операторов, не соответствующих алгоритмам;
- проверку осуществления контроля в устройстве точности, полноты и правильности данных, поступающих в программу.

Для проверки допускается использовать имитации событий в соответствии с 7.3.

7.4.6 При статическом анализе кода осуществляют выявление дополнительных возможностей по результатам исследования программы (анализа кода) в режиме, не предусматривающем реального выполнения программного кода объекта оценки.

7.4.7 При динамическом анализе кода осуществляют оценку дополнительных возможностей по результатам исследований программы (анализа кода) в режиме непосредственного исполнения (функционирования) кода. Возможно применение фаззинг-тестирования, при котором на вход подают неправильные, неожиданные или случайные данные.

7.4.8 Наиболее распространенными инцидентами в программе, вызывающими дополнительные, непредусмотренные в документации возможности, являются:

- переполнение буфера на стеке и куче;
- целочисленные переполнения;
- двойные освобождения памяти;
- использование памяти после ее освобождения;
- разыменовывание нулевого указателя;
- использование неинициализированных переменных;
- недостижимый код;
- утечка информации через сообщения об ошибках;
- использование присваивания вместо сравнения, функций поиска, вызова, уничтожение части кода и т.д.

7.5 Защищенность информации от несанкционированного доступа

7.5.1 Несанкционированный доступ может быть осуществлен как при наличии подключений к сетевым информационным ресурсам со стороны инфраструктуры, так и при использовании в протоколах эксплуатации, обслуживания и ремонта обращения к испытуемым объектам с помощью сервисной аппаратуры.

7.5.2 В начале испытаний проводят проверку идентификации и аутентификации при обращениях к программе, проверку контрольных сумм в соответствии с 7.4.3.

7.5.3 Путем анализа технической документации определяют наличие доступа к испытуемой системе со стороны инфраструктуры или элементов среды информационного взаимодействия и обмена данными.

7.5.4 При наличии доступа необходимо проверить (в соответствии с документацией на защищенный канал):

- наличие доверенного (защищенного) канала между взаимодействующими объектами (субъектами) с использованием выделенных каналов связи, защищенных линий связи и криптографических средств;
- возможность аутентификации взаимодействующих объектов (субъектов) и проверку подлинности отправителя и целостности передаваемых данных;
- возможность мониторинга состояния операционной среды систем в целях выявления уязвимостей и обнаружения сетевых атак.

7.5.5 При наличии в протоколах эксплуатации, обслуживания и ремонта программного обращения к испытуемым объектам:

- должно быть проверено выполнение принятых в документации протоколов доступа подключения аппаратных средств для считывания программ и данных;
- должен быть проведен контроль (анализ) возможности ввода ошибочной информации, копирования компьютерной информации или нейтрализации средств защиты информации.

7.6 Защищенность от компьютерных вирусов

7.6.1 В начале испытаний проводят проверку контрольных сумм в соответствии с 7.4.3.

7.6.2 Повторяют действия в соответствии с 7.5.3, 7.5.4. При наличии доступа проверяют наличие антивирусного контроля всей информации, получаемой при межсетевом взаимодействии.

7.6.3 При использовании дополнительного сервисного оборудования с возможностью подключения к поездным программируемым блокам необходимо проверить наличие антивирусной защиты в сервисном оборудовании, отсутствие возможности не лимитируемого технологией подключения сервисного оборудования к интернету, отсутствие в сервисной аппаратуре компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования программной информации.

7.7 Защищенность от ошибочных действий персонала

Проверяют действия персонала по управлению испытуемым объектом. Испытания осуществляют путем применения принципов функциональной безопасности. В соответствии с блоком 1 рисунка 1 рассматривают возможные риски из-за ошибочных действий персонала. В соответствии с блоком 2 рисунка 1 определяют функции безопасности, которые должны препятствовать реализации этих рисков. В соответствии с 7.3 проверяют реализацию данных функций безопасности.

7.8 Защищенность от возможности случайных изменений информации, последствий сбоев и перезагрузок программного обеспечения

7.8.1 В эксплуатационной документации устройства должна быть определена защитная стратегия, которая позволяет локализовать сбои и защитить систему управления от сбоев. В защитной стратегии также должна быть определена процедура действий для восстановления или обеспечения работоспособного и безопасного состояния системы управления после перезагрузок, вызванных сбоями или отказами технических средств.

7.8.2 Проводят испытания устройства, при которых контролируют его реакцию на случайные изменения информации, последствия отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, в том числе приводящих к перезагрузкам ПО, на различных этапах работы:

- при нахождении в состоянии отсутствия ввода, вывода и обработки информации;
- при вводе информации;
- при обработке и выводе информации.

При испытаниях используют приемы имитации сбоев в соответствии с испытаниями функций безопасности согласно 7.3.3.

7.8.3 После каждого этапа испытаний, связанного с имитацией сбоя, необходимо проверить целостность программы:

- данные не были изменены;
- все действия программы выполняются соответственно запрограммируемым алгоритмам;
- не произошло ошибочного расчета;
- не произошло выработки ошибочных управляющих сигналов на управляемое оборудование.

7.8.4 Проверяют, чтобы сбой системы управления при исправной работе бортовых устройств безопасности не приводил к остановке ТПС.

7.8.5 При сбоях ПО проверяют недопущение изменений характеристик и режимов работы оборудования, которые могут привести к нарушению безопасного состояния ТПС.

Проверку осуществляют путем применения принципов функциональной безопасности: в соответствии с блоками 1, 2 рисунка 1 определяют риски и соответствующие функции безопасности, в соответствии с 7.3 проверяют выполнение этих функций.

7.9 Техническое диагностирование оборудования тягового подвижного состава с наличием средств сигнализации и информирования о нарушении исправного состояния

7.9.1 При испытаниях проверяют систему контроля технического состояния ТПС, наличие информации о месте и причине отказа в работе оборудования на всех этапах эксплуатации:

- перед поездкой;
- в течение поездки;
- после окончания поездки.

7.9.2 Проводят техническое диагностирование основных узлов ТПС, подсистем и систем управления с выдачей информации о техническом состоянии локомотивной бригаде.

Испытания проводят в соответствии с эксплуатационной документацией на устройство.

7.9.3 Контроль функций устройств при неисправностях аппаратов электрической, гидравлической и/или пневматической частей, сбое ПО следует проводить с помощью имитации неисправностей согласно 7.3.3, 7.3.4.

8 Оформление результатов испытаний

По результатам испытаний формируют протокол, в котором каждый этап оформляют в виде отдельного пункта, с указанием условий, при которых проводились испытания, и результатов испытаний.

УДК 629.423:006.354 МКС 45.060.10

Ключевые слова: тяговый подвижной состав железнодорожный, методы контроля, функциональная безопасность, устройство, обеспечивающее безопасность движения

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 12.12.2022. Подписано в печать 28.12.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru