ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59981— 2022

СИСТЕМЫ И УСТРОЙСТВА БЕЗОПАСНОСТИ, УПРАВЛЕНИЯ И ДИАГНОСТИКИ МИКРОПРОЦЕССОРНЫЕ ЖЕЛЕЗНОДОРОЖНОГО ТЯГОВОГО ПОДВИЖНОГО СОСТАВА

Требования к типовой архитектуре, интерфейсам, функциям

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным автономным образовательным учреждением высшего образования «Российский университет транспорта (МИИТ)»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 045 «Железнодорожный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 января 2022 г. № 9-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (*gost.e-ecolog.ru

© Оформление. ФГБУ «РСТ», 2022

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Требования к типовой архитектуре микропроцессорных систем управления 4
5 Требования к типовым функциям бортовых систем 6
6 Требования к интерфейсам взаимодействия 11
Библиография 13

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ И УСТРОЙСТВА БЕЗОПАСНОСТИ, УПРАВЛЕНИЯ И ДИАГНОСТИКИ МИКРОПРОЦЕССОРНЫЕ ЖЕЛЕЗНОДОРОЖНОГО ТЯГОВОГО ПОДВИЖНОГО СОСТАВА

Требования к типовой архитектуре, интерфейсам, функциям

Microprocessor systems and devices for safety, control and diagnostics of railway traction rolling stock. Requirements for standard architecture, interfaces, functions

Дата введения — 2023—01—01

1 Область применения

Настоящий стандарт распространяется на вновь разрабатываемые и модернизируемые микропроцессорные системы и устройства безопасности, управления и диагностики тягового железнодорожного подвижного состава и устанавливает требования к их архитектуре, интерфейсам, функциям.

Настоящий стандарт предназначен для применения при разработке, производстве и эксплуатации микропроцессорных систем и устройств безопасности, управления и диагностики тягового железнодорожного подвижного состава, в т. ч. модернизируемых.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

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

ГОСТ Р МЭК 62280 Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации

ГОСТ IEC 61508-3—2018 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

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 ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **аппаратное обеспечение:** Материальная часть вычислительной системы, включающая в себя электрические и электронные элементы (например, приборы и схемы), электромеханические элементы (например, клапаны) и механические элементы (например, корпуса).

3.1.2

архитектура (системы) (architecture): Основные понятия или свойства системы в окружающей среде, воплощенной в ее элементах, отношениях и конкретных принципах ее проекта и развития.

[ГОСТ Р 57100—2016/ISO/IEC/IEEE 42010:2011, пункт 3.2]

3.1.3

аутентификация: Процесс подтверждения заявленной идентичности для гарантии того, что установленная идентичность пользователя корректна.

[ГОСТ Р 53632—2009, пункт 3.4]

3.1.4 **блок:** Элемент аппаратного обеспечения микропроцессорной системы управления, представляющий собой устройство или совокупность устройств, с уникальной блочной маркировкой (шифр блока и заводской номер), состоящий из электронных деталей или узлов, выполняющий свою (свои) собственную(ые) функцию(и).

3.1.5

виртуализация: Группа технологий, основанных на преобразовании формата или параметров программных, или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

[ГОСТ Р 56938—2016, пункт 3.1]

3.1.6

виртуальная машина; ВМ: Виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных, и которая дополнительно может содержать программное обеспечение и пользовательские данные.

Примечания

1 Виртуальная машина является простейшей формой виртуальных вычислительных систем.

2 Несколько виртуальных машин, объединенных для решения определенных задач, также составляют виртуальную вычислительную систему. В этом случае виртуальная машина выступает в качестве базового элемента при построении (сложных) виртуальных вычислительных систем.

3 Виртуальная машина скрывает настоящую реализацию находящихся в ней процессов и объектов от процессов, запущенных вне виртуальной машины. Верно и обратное — виртуальная машина скрывает настоящую реализацию находящихся вне нее процессов и объектов от процессов, запущенных внутри виртуальной машины.

[ГОСТ Р 56938—2016, пункт 3.4]

3.1.7 **вспомогательная функция системы:** Функция системы, потребность в которой возникает в связи с применяемыми техническими решениями, необходимостью диагностирования системы, ее обслуживания и ремонта.

3.1.8 **вычислитель:** Счетно-решающий элемент системы, предназначенный для выполнения математических операций.

3.1.9 **деградированное состояние:** Состояние системы, при котором она продолжает выполнять только часть своих функций.

3.1.10

инфраструктура железнодорожного транспорта общего пользования: Технологический комплекс, включающий в себя железнодорожные пути общего пользования и другие сооружения, железнодорожные станции, устройства электроснабжения, сети связи, системы сигнализации, централизации и блокировки, информационные комплексы, систему управления движением и иные обеспечивающие функционирование этого комплекса здания, строения, сооружения, устройства и оборудование.

[ГОСТ 34530—2019, статья 2.1.4]

3.1.11 **интерфейс (программный или аппаратный):** Совокупность средств, методов и правил взаимодействия (управление, обеспечение безопасности и т. д.) между элементами системы.

3.1.12 **коммутатор:** Активное сетевое устройство, которое соединяет две или несколько сетей, которые, в свою очередь, могут состоять из сегментов.

3.1.13 **микропроцессорная система управления (в том числе устройство безопасности/диагностики):** Система, реализованная на микропроцессорной элементной базе, выполняющая заданные функции управления, безопасности, контроля и диагностики железнодорожного тягового подвижного состава.

3.1.14 **модуль:** Независимый программный элемент системы, имеющий интерфейс, выполняющий основную или вспомогательную функцию системы (набор функций).

3.1.15 **мониторинг технического состояния:** Совокупность процедур, процессов и ресурсов, реализованных с использованием диагностических средств, позволяющая по результатам измерений заданных параметров в заданных точках и наблюдений за работой оборудования получить информацию о текущем техническом состоянии оборудования, опасностях и рисках, связанных с его применением.

3.1.16

надежность (железнодорожной техники) (dependability): Способность железнодорожной техники выполнять предусмотренные техническими требованиями функции в течение определенной наработки или периода эксплуатации при установленных в нормативной и (или) технической документации условиях применения, технического содержания, хранения и транспортирования.

Примечание — В зависимости от назначения железнодорожной техники и условий ее применения надежность может включать готовность, безотказность, ремонтопригодность, долговечность и сохраняемость или определенные сочетания этих свойств.

[ГОСТ 32192—2013, статья 2]

3.1.17

отказоустойчивость (железнодорожной техники) (fault tolerance): Способность железнодорожной техники сохранять работоспособное состояние при возникновении отказа одной или нескольких ее составных частей.

[ГОСТ 32192—2013, статья 9]

3.1.18 **принцип модульности:** Принцип, заключающийся в том, что система представляет собой совокупность отдельных элементов, являющихся независимыми модулями или блоками.

Примечание — Принцип независимости заключается в том, что замена и включение новых модулей и блоков не влечет изменений в других модулях и блоках системы.

3.1.19 **принцип расширяемости:** Принцип построения системы, при котором внесение изменений в элемент системы или дополнение системы новым элементом осуществляется без необходимости внесения изменений в другие элементы системы.

3.1.20 **программный контейнер:** Изолированная программная среда со специфическим набором компонентов операционной системы, обеспечивающим работу отдельных программ.

3.1.21 **синхронизация информации:** Устранение возможных различий между копиями.

3.1.22

тяговый (железнодорожный) подвижной состав: Совокупность видов железнодорожного подвижного состава, обладающего тяговыми свойствами для выполнения перевозочного процесса и включающая в себя локомотивы и моторвагонный подвижной состав.

Примечание — Моторвагонный подвижной состав включает в себя электропоезда, дизель-поезда и автомотрисы (рельсовые автобусы), предназначенные для перевозки пассажиров.

[ГОСТ 31539—2012, статья 3]

3.1.23 **функциональное состояние машиниста:** Наличный уровень активности функциональных систем организма машиниста, характеризуемый степенью адекватности конкретной деятельности, выполняемой машинистом.

3.1.24 **целевая функция:** Функция системы, которая прямо определяется заданием на разработку.

3.2 В настоящем стандарте применены следующие сокращения:

АРМ — автоматизированное рабочее место;
ББД — блок безопасности движения;
ББК — блок беспроводных коммуникаций;
БЖЦ — блок жизненного цикла;
БИЧМ — блок интерфейса «человек-машина»;
БК — блок коммутаторов;
БЦВ — блок центрального вычислителя;
МСУ — микропроцессорные системы и устройства безопасности, управления и диагностики железнодорожного тягового подвижного состава;
ПО — программное обеспечение;
СМЕ — система многих единиц;
ТЗ — техническое задание;
ТПС — тяговый железнодорожный подвижной состав;
ТЭД — тяговый электродвигатель;
УПБ4 — уровень полноты безопасности с интенсивностью опасных отказов от 10^{-8} до 10^{-9} в ч;.
ЭЦП — электронная цифровая подпись.

4 Требования к типовой архитектуре микропроцессорных систем управления

4.1 Микропроцессорные системы и устройства безопасности, управления и диагностики, устанавливаемые на тяговом железнодорожном подвижном составе, должны строиться по принципам модульности и расширяемости (кроме ББД и БК).

4.2 Количество блоков МСУ должно быть таким, чтобы не допускать дублирования функций в различных блоках. Типовыми блоками системы, исходя из этого принципа, должны являться:

- блок безопасности движения (ББД);
- блок центрального вычислителя (БЦВ);
- блок интерфейса «человек-машина» (БИЧМ);
- блок коммутаторов (БК);
- блок беспроводных коммуникаций (ББК);
- блок жизненного цикла системы (БЖЦ).

Допускается объединение блоков для снижения их количества. Точное количество каждого типа блоков МСУ и архитектура блоков должны быть определены в ТЗ на МСУ. Допускается вводить в МСУ дополнительные типы блоков, если невозможно реализовать новую функцию, предусмотренную в ТЗ на базе имеющихся типов блоков или модулей.

4.3 Модули МСУ должны быть выполнены в виде программы, программного контейнера, виртуальной машины, запущенных в блоках МСУ. Для типовой МСУ модуль должен иметь возможность замены на аналогичный без изменения программного обеспечения остальных модулей, если иное не отражено в ТЗ на МСУ, с учетом требований ГОСТ IEC 61508-3—2018 (приложения А и В).

4.4 ББД предназначен для обеспечения обработки первичной информации, от которой зависит безопасность движения, и выполнения функций безопасности движения с выполнением требований функциональной безопасности согласно ГОСТ 33435. Функции ББД не могут быть перераспределены между другими блоками.

4.5 БЦВ предназначен для выполнения модулей, которые отвечают за функции управления и диагностики оборудования и систем ТПС, диагностики поезда и железнодорожной инфраструктуры, функции управления режимами движения поезда, функции контроля и прочие функции. При реализации функций БЦВ предъявляются требования УПБ в соответствии с ГОСТ 34009. Для типовой МСУ к таким модулям относятся:

- модуль управления тяговым приводом;
- модуль управления вспомогательным оборудованием и системами ТПС;
- модуль оптимального управления движением поезда;
- модуль диагностики механической части, оборудования и систем ТПС;
- модуль хранения информации;
- модуль контроля функционального состояния машиниста и аутентификации персонала;
- модуль учета расхода топливно-энергетических ресурсов;
- модуль диагностики системы пожарной сигнализации и пожаротушения;
- модуль управления пневматическим и электропневматическим торможением.

Список модулей БЦВ не является исчерпывающим и может быть изменен в соответствии с ТЗ на МСУ.

Состав и количество одновременно исполняемых модулей устанавливают в ТЗ на МСУ в зависимости от типа ТПС и требований к производительности вычислителя.

4.6 БЦВ должен иметь независимый от основного источника питания ТПС резервный источник питания, обеспечивающий работоспособность модуля хранения информации для записи данных во время отключения питания и после отключения питания на время, установленное в ТЗ на МСУ.

4.7 БИЧМ предназначен для выполнения модуля ввода и вывода информации. Вывод информации следует осуществлять в комбинированной форме, включая вывод изображения на графический дисплей, светоизлучающие индикаторы и автоматически формируемые речевые сообщения.

4.8 Связь между блоками МСУ следует осуществлять посредством БК, либо напрямую при применении линий связи с топологией типа «шина».

4.9 ББК предназначен для выполнения модулей:

- беспроводной связи с железнодорожной инфраструктурой;
- межсекционной беспроводной связи (проводной, если беспроводная невозможна из-за ограничения пропускной способности передачи данных).

Для режима обслуживания в ББК должен быть реализован отдельный беспроводной интерфейс ближнего круга действия, чтобы исключить возможность действия этого интерфейса вне кузова ТПС, для сервисного соединения с АРМ обслуживающего персонала.

4.10 БЖЦ предназначен для выполнения модуля жизненного цикла МСУ. БЖЦ получает диагностическую информацию от БЦВ, ББК, БИЧМ, БК и может менять их состояние (включено/выключено), в зависимости от полученной информации. БЖЦ должен быть отказоустойчивым.

4.11 В зависимости от требуемых показателей надежности и отказоустойчивости МСУ следует применять резервирование.

4.12 Локализация функций МСУ может быть изменена относительно типовой, если это предусмотрено ТЗ.

4.13 Все блоки МСУ должны иметь собственные подсистемы, кроме ББД:

- электропитания;
- управления по командам БЖЦ (включение, отключение, обновление ПО).

4.14 Определение ведущего МСУ в случае совместной работы нескольких МСУ, например, при работе по СМЕ должно быть автоматическим, но должна быть предусмотрена возможность ручного выбора. Принцип автоматического определения ведущего комплекта должен определяться ТЗ на МСУ.

4.15 При работе в режиме распределенной тяги (для ТПС, поддерживающего такой режим работы) должно быть предусмотрено взаимодействие между МСУ «ведущий-ведомый», которое активизируется только при готовности МСУ всех единиц ТПС к указанному способу взаимодействия. Инициирование взаимодействия МСУ следует выполнять только вручную.

4.16 Обновление ПО модулей следует выполнять без необходимости выключения МСУ на стоянке. В случае резервированных модулей должно быть предусмотрено обновление ПО последовательно для каждого резервированного модуля. Допускается перезагрузка МСУ для применения обновлений.

4.17 Должны быть предусмотрены режимы работы МСУ, которые позволяют продолжать эксплуатацию системы в деградированном состоянии, то есть при наличии отказавших блоков или модулей, с обязательной передачей на железнодорожную инфраструктуру (в соответствии с ТЗ на МСУ) и машинисту (оператору) информации о работе в деградированном состоянии.

4.18 МСУ при необходимости (по согласованию между заказчиком и разработчиком МСУ) может дополняться блоками, обеспечивающими коммуникационные возможности между эксплуатирующимися МСУ или другими устройствами, которые построены без учета требований настоящего стандарта.

5 Требования к типовым функциям бортовых систем

5.1 Функции ББД

5.1.1 Функция интервального регулирования (автоматическая локомотивная сигнализация) должна обеспечивать распознавание (декодирование) сигнала, передаваемого по рельсовым цепям, по УПБ в соответствии с ГОСТ 33435—2015 (приложение А, таблица А.1), и передачу результатов распознавания потребителям (блокам и модулям).

5.1.2 Функция формирования сигнала управления экстренным торможением должна обеспечивать формирование сигнала для тормозной системы поезда на экстренное торможение при установленном нарушении безопасности движения (превышение ограничения по скорости, проезд светофора с запрещающим показанием и т. д.), с выдачей команды в модуль управления тяговым приводом на отключение режима тяги.

5.1.3 Функция формирования допустимой скорости должна обеспечивать формирование значения ограничений по скорости или групповых ограничений скоростей (по времени или пути), а также обеспечивать обновление информации об ограничениях скорости путем автоматической синхронизации через модуль беспроводной связи.

5.1.4 Функция проследования путевого светофора с запрещающим показанием должна обеспечивать:

- проследование путевого светофора с запрещающим показанием только после полной остановки поезда перед ним и получения по радиоканалу разрешения на проследование, за исключением проходных светофоров;
- безостановочное проследование грузовым поездом проходного светофора с запрещающим показанием, с установленным условно-разрешающим сигналом, на путях общего пользования со скоростью не более 20 км/ч, на путях необщего пользования со скоростью не более 15 км/ч.

5.1.5 Функция определения фактической скорости движения и координаты ТПС должны обеспечивать определение и формирование параметров движения поезда (полный перечень определяется в ТЗ на МСУ):

- фактическую скорость;
- текущее время;
- текущие географические координаты глобальных навигационных систем, запущенных в эксплуатацию на момент разработки МСУ;
- координату точки следующей остановки;
- номер пути следования на перегоне;
- номер пути и номер (признак) маршрута следования по станции;
- направление движения (ведущая кабина управления).

Точность и погрешность измерения фактической скорости движения и координат должны быть указаны в ТЗ.

5.1.6 Функция определения объектов на пути должна обеспечивать выявление потенциально опасных объектов на пути, которые могут создать аварийную ситуацию при движении поезда, с учетом условий ландшафта в случае оборудования ТПС соответствующими датчиками. Расстояния до объектов и размеры объектов устанавливают в ТЗ на МСУ.

5.1.7 Функция выдачи информации только для чтения, полученной ББД, другим блокам МСУ. Перечень информации определяется в ТЗ на МСУ.

5.2 Модуль управления тяговым приводом должен обеспечивать:

а) в режиме электрического торможения:

1) поддержание заданной тормозной силы с учетом ограничений тормозной характеристики до достижения заданной скорости с последующим ее поддержанием (на спусках);

2) ограничение токов ТЭД при достижении максимально допустимого значения;

3) выравнивание нагрузок ТЭД;

4) защиту от юза;

б) в тяговом режиме:

1) плавное или ступенчатое регулирование задаваемой величины силы тяги и скорости;

2) ограничение величины ускорения и замедления ТПС с поездом в соответствии с требованиями действующих нормативных документов (требования должны быть внесены в ТЗ на МСУ);

3) ограничение тока ТЭД при достижении максимально допустимого значения;

4) защита от боксования (путем автоматического регулирования тяги и/или подачи песка) с автоматическим выравниванием нагрузок ТЭД.

Модуль управления тяговым приводом должен выдавать информацию о режимах работы тягового оборудования потребителям, в том числе модулю диагностики механической части, оборудования систем ТПС для обнаружения нарушений работы тягового оборудования.

5.3 Модуль управления вспомогательным оборудованием и системами ТПС должен:

- обеспечивать управление вспомогательным оборудованием и системами ТПС с учетом ограничений в режимах работы этого оборудования для защиты от перехода в неисправное состояние;

- выдавать информацию о режимах работы вспомогательного оборудования и систем ТПС потребителям, в том числе модулю диагностики механической части, оборудования систем ТПС для обнаружения нарушений работы оборудования;

5.4 Модуль оптимального управления движением поезда должен:

- выполнять расчет траектории движения поезда на заданном участке пути с учетом условий движения и выбранной целевой функции: минимум расхода энергии при заданном времени движения, максимум скорости (список целевых функций устанавливают в ТЗ на МСУ);

- распознавать в автоматическом режиме цель оптимизации (время, энергия) или получать цель оптимизации от машиниста;

- проводить перерасчет траекторий движения поезда в случае значительных отклонений (величину отклонения указывают в ТЗ на МСУ) фактических значений параметров движения или ограничений за время, которое уточняется на этапе разработки ТЗ на МСУ.

5.5 Модуль диагностики механической части, оборудования и систем ТПС должен:

- выполнять мониторинг технического состояния механической части, тягового и вспомогательного оборудования, систем ТПС на основании получения информации с соответствующих модулей;

- выдавать на модуль ввода и вывода информации предупреждения машинисту в случае наступления отказа оборудования или в предотказном состоянии, влияющего на возможность продолжения движения и требующего вмешательства машиниста в работу оборудования или коррекции режимов работы локомотива с учетом его состояния;

- осуществлять синхронизацию информации с хранилищем данных для получения и обработки информации о техническом состоянии ТПС.

5.6 Модуль хранения информации должен:

а) обеспечивать сбор и регистрацию информации в энергонезависимом несъемном запоминающем устройстве или в энергонезависимом съемном запоминающем устройстве БЦВ (длительность хранения устанавливают в ТЗ на МСУ):

1) параметров движения поезда на маршруте движения в соответствии с перечнем регистрируемых параметров движения согласно ТЗ на МСУ;

2) диагностической информации о состоянии ТПС и всех модулей МСУ;

б) обеспечивать доступность данных, хранящихся в энергонезависимой внутренней памяти БЦВ в течение установленного периода времени (период хранения и число циклов перезаписи устанавливают для конкретных серий ТПС в ТЗ на МСУ);

в) выдавать другим модулям хранящуюся информацию о путевых объектах и условиях движения по участку (в соответствии с ТЗ на МСУ);

г) учитывать возможные реализации отказоустойчивых хранилищ данных и предусматривать программные механизмы восстановления информации при ее частичном повреждении;

д) обеспечивать хранение информации в стандартном открытом формате, если иное не предусмотрено ТЗ на МСУ.

В случае применения собственного формата хранения информации должно быть предоставлено ПО для расшифровки, либо преобразования к формату хранения данных заказчика.

5.7 Модуль контроля функционального состояния машиниста и аутентификации персонала должен:

а) проводить непрерывный контроль бодрствования и бдительности машиниста, при отрицательных (в соответствии с ТЗ на МСУ) результатах контроля формировать команду модулю управления пневматическим и электропневматическим торможением на остановку или запрет движения;

б) получать из хранилища данных информацию о машинисте (его биометрические параметры, данные предрейсового или непрерывного медицинского осмотра) и учитывать эту информацию при оценке функционального состояния машиниста;

в) обеспечивать проведение аутентификации персонала в штатном режиме или режиме обслуживания путем выполнения следующих действий:

1) предъявлением ЭЦП, содержащейся на съемном носителе, с последующей проверкой корректности этой ЭЦП в хранилище данных;

2) сравнением биометрической информации на съемном носителе и введенной биометрической информации через модуль ввода (отпечатки пальцев и/или пространственная модель лица, рисунок вен и прочее);

3) сравнением сертификата АРМ обслуживающего персонала и проверкой существования этого сертификата в центре сертификации;

4) путем получения разрешения на работу с системой при запросе в хранилище данных (в этом случае персонал должен располагаться лицом к видеофиксирующей аппаратуре, а оператор должен убедиться в том, что идентификационная информация в запросе соответствует изображению);

5) другими способами персональной идентификации, установленными в ТЗ на МСУ;

г) выполнять прогнозирование функционального состояния машиниста, а при переходе прогнозного функционального состояния в область недопустимых значений выдавать команду на запрет движения ТПС.

5.7.1 Информация о функциональном состоянии машиниста должна персонифицироваться и передаваться в хранилище данных для последующего анализа. Требования по защите персональных данных определены законодательством Российской Федерации [1]. Способ и порядок передачи информации определяются на этапе разработки ТЗ на МСУ.

5.7.2 При работе машиниста без помощника МСУ должна быть доукомплектована носимым блоком — для мониторинга физиологических показателей машиниста. В случае удаления машиниста от ТПС эти показатели должны передаваться в МСУ по беспроводному каналу. При потере связи МСУ с носимым блоком во время отсутствия машиниста в кабине ТПС более определенного промежутка времени (уточняют в ТЗ на МСУ) или в случае устойчивой передачи показателей, несовместимых с нормальным состоянием организма, МСУ должна передать информацию на железнодорожную инфраструктуру с указанием данных, однозначно идентифицирующих поезд и место остановки. Максимальное расстояние удаления машиниста от кабины управления определяется на этапе разработки ТЗ на МСУ.

5.8 Модуль учета расхода топливно-энергетических ресурсов должен:

а) обеспечивать с заданной точностью, которая определяется на этапе разработки ТЗ на МСУ, подсчет расхода энергоресурсов в течение заданного времени путем:

1) получения первичной информации от датчиков контроля энергоресурсов и расчета интегральных значений расхода;

2) подключения к системам ТПС, производящим самостоятельную обработку данных с таких датчиков, для получения интегральных значений расходов;

б) обеспечивать возможность учета типа энергоресурса в зависимости от типа ТПС: электрическую энергию, дизельное топливо, газ и прочее;

в) обеспечивать подключение к установленному на ТПС оборудованию коммерческого учета энергоресурсов посредством преобразователей интерфейсов или шлюзов;

г) хранить информацию о расходе энергоресурсов в течение времени, которое определяется на этапе разработки ТЗ на МСУ.

5.9 Модуль диагностики системы пожарной сигнализации и пожаротушения должен:

а) обеспечивать контроль состояния штатной системы пожарной сигнализации и пожаротушения;

б) при изменении состояния штатной системы пожарной сигнализации и пожаротушения обеспечивать:

1) во время поездки или подготовки к поездке — машиниста посредством передачи информации на БИЧМ;

2) во время поездки — работникам железнодорожной инфраструктуры посредством передачи сигнала через беспроводной интерфейс (порядок передачи данной информации уточняется в ТЗ на МСУ);

3) в режиме горячего или холодного отстоя ТПС — ответственного персонала депо посредством передачи информации через беспроводной интерфейс (порядок передачи данной информации уточняют в ТЗ на МСУ).

5.10 Модуль управления пневматическим и электропневматическим торможением должен:

- обеспечивать автоматическую остановку с точностью, указанной в ТЗ на МСУ, перед путевым светофором с запрещающим показанием;

- формировать допустимую скорость с учетом значения допустимой скорости, полученной от модуля автостопного торможения, и дополнительных ограничений, полученных из модулей, выполняющихся в БЦВ;

- осуществлять снижение текущей скорости ниже допустимой путем применения служебного пневматического или электропневматического торможения при превышении прогнозируемой скорости, определяемой путем решения уравнения движения поезда, экстраполяции ускорения или любым другим способом (конкретный способ устанавливают в ТЗ на МСУ) допустимого значения скорости;

- при каждом торможении автоматически определять эффективность тормозов (по замедлению и/или тормозному пути) поезда и ТПС при одиночном следовании или следовании в составе с группой локомотивов, сцепленных между собой;

- проводить контроль работы тормозной системы поезда, регистрировать и выдавать предупреждение через модуль ввода и вывода информации о нарушениях в работе пневматической тормозной системы;

- давать команду на отключение режима тяги в модуль управления тяговым приводом в случае перехода к режиму торможения;

- выполнять команды торможения поезда, поступающие от модуля оптимального управления движением поезда, и выполнять остановку поезда или ТПС с заданной точностью (определяют на этапе разработки ТЗ на МСУ);

- обеспечивать незамедлительно принудительную остановку поезда или ТПС служебным торможением при получении команды на остановку или запрет движения от модулей МСУ (модуля контроля функционального состояния машиниста, модуля диагностики механической части, оборудования и систем ТПС и другие. Полный перечень модулей приведен в ТЗ на МСУ).

5.11 Модуль ввода и вывода информации должен:

а) осуществлять подготовку визуальной и аудиоинформации для вывода машинисту через БИЧМ (перечень и формат информации уточняют в ТЗ на МСУ);

б) осуществлять вывод информации с учетом доступа после аутентификации по запросу пользователя МСУ;

в) обеспечивать ввод необходимой информации одним или сочетанием нескольких методов, таких как запись текстового сообщения, аудиозапись, передача в МСУ посредством любого из доступных устройств ввода, входящих в состав БИЧМ:

1) механической клавиатуры;

2) микрофона и распознавания голоса;

3) сенсорного экрана;

4) механических кнопок (рукоятка бдительности);

5.12 Модуль беспроводной связи с инфраструктурой должен:

а) выполнять функцию передачи данных в местах технического обслуживания с целью:

1) беспроводного чтения всей зарегистрированной информации и/или информации, полученной диагностическими модулями системы;

2) автоматической, а в случае отказа функции — ручной синхронизации данных из модуля хранения информации с данными систем железнодорожной инфраструктуры;

б) выполнять балансировку нагрузки при беспроводной передаче. При существенном объеме информации в автоматическом режиме на время передачи должна выполняться диверсификация используемых беспроводных интерфейсов по скорости и размерам зоны уверенного приема. Для передачи

информации, прогнозируемое время доставки которой превышает установленное в ТЗ на МСУ, должен быть использован интерфейс с максимальной пропускной способностью из готовых к передаче на текущий момент;

в) выполнять сжатие информации без потерь для снижения передаваемого объема. Алгоритм сжатия и степень сжатия информации должны быть установлены в ТЗ;

г) использовать в режиме обслуживания отдельный беспроводной интерфейс ближнего круга действия, исключающий возможность действия вне кузова ТПС, для сервисного соединения с АРМ обслуживающего персонала.

5.13 Объем синхронизируемой информации и системы железнодорожной инфраструктуры, с которыми должна быть обеспечена синхронизация данных модуля хранения информации, уточняют в ТЗ на МСУ. В обязательном порядке синхронизируемый объем информации должен содержать:

а) во время следования в составе поезда — информацию для передачи в хранилище данных:

1) номер поезда;

2) серию и номер ТПС;

3) время МСУ;

4) оперативную информацию от модуля контроля функционального состояния машиниста и аутентификации персонала;

5) аварийные сообщения и диагностические предупреждения (длительность периода поиска сообщений для передачи определяют в ТЗ на МСУ);

б) во время захода в депо (пункт технического осмотра локомотивов):

1) аварийные сообщения и диагностические предупреждения за время, прошедшее с последней синхронизации;

2) зарегистрированную в соответствии с ТЗ на МСУ информацию о поездке;

3) информацию от модуля контроля функционального состояния машиниста и аутентификации персонала;

4) информацию от модуля учета расхода топливно-энергетических ресурсов.

5.14 Модуль межсекционной беспроводной связи должен обеспечивать двухсторонний обмен информацией между секциями локомотива, в том числе передачу управляющей, диагностической и другой информации.

5.15 Модуль жизненного цикла должен обеспечить выполнение следующих функций:

- локализацию отказов блоков/модулей (кроме ББД) с выключением отказавшего блока/модуля из рабочего состава МСУ во время работы с возможной реконфигурацией или восстановлением исправного состояния отказавшего модуля (зависит от причин отказа), с передачей на железнодорожную инфраструктуру соответствующей информации;
- отслеживание периодичности выполнения регламентных работ, связанных с технической диагностикой МСУ;
- инициализация модулей;
- автоматический перевод модулей в режим обслуживания;
- автоматический перевод модулей в рабочий режим, если до этого перевод в режим обслуживания был выполнен модулем жизненного цикла;
- тестирование исправности блоков и модулей МСУ;
- обновление ПО модулей;
- формирование предупреждений, аварийных сообщений для протоколирования в модуле хранения информации, в собственной памяти за последние 24 ч или более (определяют на этапе разработки ТЗ на МСУ);
- ведение электронного журнала, в котором регистрируется время работы модулей и МСУ с дифференциацией по режимам работы, история уникальных идентификаторов блоков в составе МСУ, история обновления ПО модулей;
- определение состояния МСУ в текущий момент времени;
- ввод и вывод из работы блоков и их модулей по требованию авторизованного пользователя в сервисном режиме;
- автоматическое формирование рекомендаций (инструкций) персоналу о порядке локализации отказа и восстановления исправного состояния МСУ или оборудования локомотива, либо о возможности продолжения и порядке работы с ним при наличии частичных отказов.

6 Требования к интерфейсам взаимодействия

6.1 Межмодульное взаимодействие ББД для выполнения функций, требующих УПБ4, должно использовать интерфейсы, которые выполнены с учетом требований ГОСТ Р МЭК 61508-1. При этом может быть применен интерфейс или набор интерфейсов, отличающийся от интерфейса межблочного взаимодействия.

6.2 Интерфейсы взаимодействия между блоками должны соответствовать следующим требованиям:

- вся информация из ББД должна быть доступна для БЦВ в режиме чтения;
- протокол взаимодействия между модулями ББД и БЦВ должен быть гармонизирован в части обмена информацией, чтобы уменьшить избыточность и повторную обработку;
- протоколы должны предусматривать инструменты для снижения служебного трафика;
- обеспечивать сетевое взаимодействие между получателем и отправителем информации;
- должны быть дифференцированы в соответствии с уровнем функциональной безопасности той функции МСУ, которая реализуется посредством этого интерфейса.

6.3 Межблочное и межмодульное взаимодействие в рамках БЦВ следует осуществлять с помощью открытого промышленного стандартизованного интерфейса, использующего открытые и стандартные протоколы.

6.4 Интерфейсы связи между структурными блоками могут быть:

- проводными, соответствующими 6.5;
- беспроводными, соответствующими 6.6.

6.5 Проводные интерфейсы связи между структурными блоками должны:

- предусматривать возможность резервирования в виде кольца (двойного кольца), двойной магистрали (шинная топология);
- обеспечивать передачу данных в режиме реального времени, что подразумевает гарантированные и предсказуемые задержки во времени между их отправкой и получением и удовлетворительную нормированную вариацию этого времени;
- иметь возможность гарантированной доставки пакетов данных;
- иметь пропускную способность, достаточную для выполнения функций МСУ (уточняется на этапе разработки ТЗ);
- допускать сопряжение блоков с различными пропускными способностями интерфейса;
- иметь определенное время реакции на отказ маршрута передачи данных для последующего перенаправления трафика, которое уточняется на этапе ТЗ на разрабатываемую систему;
- иметь возможность создания сетевых структур;
- иметь возможность автоматической адресации в случае изменения конфигурации сети;
- поддерживать виртуализацию.

6.6 Беспроводные интерфейсы связи должны:

- удовлетворять требованиям ГОСТ Р МЭК 62280;
- иметь резервную частоту или несколько частот и автоматически переключаться на них при возникновении проблем с передачей данных для используемой частоты;
- обеспечивать автоматический поиск соседних беспроводных устройств, готовых к обмену информацией.

Гигиенические требования к размещению и эксплуатации средств сухопутной подвижной радиосвязи приведены в [2].

6.7 При работе машиниста без помощника должен быть предусмотрен дополнительный резервируемый канал связи для возможности поддержания связи между МСУ и машинистом. Радиус работы такого канала должен быть достаточным для реализации связи у хвостового вагона поезда. В случае соединенных поездов второй и последующий локомотивы должны выступать в роли повторителей, увеличивающих зону действия радиоканала.

6.8 При реализации интерфейсов необходимо соблюдать следующие требования к защите информации:

- применяют меры защиты информации в автоматизированной системе. К документам, определяющим требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами, относится приказ Федеральной службы по техническому и экспортному контролю [3];

- применяют сертифицированные методы криптозащиты информации, передаваемой по беспроводным и проводным интерфейсам. Необходимость применения средств криптозащиты в проводных линиях связи оценивается и согласуется на этапе определения класса защищенности МСУ;

- производят классификацию ПО интерфейсов по уровню контроля отсутствия в нем недекларированных возможностей. К документам, определяющим требования по безопасности информации, относится приказ Федеральной службы по техническому и экспортному контролю [4];

- проводят сертификацию средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации;

- подтверждают выполнение требований функциональной и информационной безопасности к ПО МСУ (путем проведения оценки соответствия).

Для оценки соответствия должна быть разработана программная и конструкторская документация.

Библиография

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[2] СанПиН 2.1.8/2.2.4.1190-03 Гигиенические требования к размещению и эксплуатации средств сухопутной подвижной радиосвязи

[3] Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

[4] Приказ ФСТЭК России от 15 марта 2021 г. № 46 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31»

УДК 656.2:006.354 ОКС 45.020

Ключевые слова: тяговый подвижной состав, микропроцессорная система управления, устройство безопасности, интервальное регулирование, виртуализация, принцип модульности, принцип расширяемости, межсекционная беспроводная связь, программный контейнер, виртуальная машина

Редактор *Е.В. Якубова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 19.01.2022. Подписано в печать 07.02.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,90.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru