ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71615— 2024

Машины землеройные

МАШИНЫ ВЫСОКОАВТОМАТИЗИРОВАННЫЕ ЗЕМЛЕРОЙНЫЕ И ДОРОЖНО-СТРОИТЕЛЬНЫЕ

Технические требования и методы испытаний

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «ДСТ-УРАЛ» (ООО «ДСТ-УРАЛ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 267 «Строительно-дорожные машины и оборудование»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 сентября 2024 г. № 1253-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 «Институт стандартизации», 2024

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

Введение IV
1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Требования к безопасности рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин 8
5 Технические требования к уровню автоматизации рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин 9
6 Требования безопасности при испытании рассматриваемых землеройной и дорожно-строительной машин 10
7 Заключение об уровне полноты безопасности РВАЗДСМ 39
8 Условия испытаний 40
Приложение А (обязательное) Методы испытаний рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин 42
Приложение Б (обязательное) Метод определения уровня полноты безопасности рассматриваемых землеройной и дорожно-строительной машин — оценка риска 47
Приложение В (справочное) Классификация опасностей 53
Приложение Г (обязательное) Виды препятствий (целевых объектов) 56
Библиография 58

Введение

Безопасность является одним из приоритетов современного машиностроения. Усложнение технологий, программного обеспечения и мехатронных устройств увеличивает риски, связанные с систематическими и случайными отказами аппаратных средств, рассматриваемыми в рамках функциональной безопасности и безотказности. Расширение числа функциональных возможностей землеройных и дорожно-строительных машин вызывает необходимость нормирования технических параметров аппаратно-программного комплекса высокоавтоматизированных землеройных и дорожно-строительных машин с применением методик по их верификации.

Настоящий стандарт разработан в соответствии с программой по разработке национальных стандартов в области машиностроения, в том числе направленных на сокращение зависимости от импортной продукции и технологий, в результате применения которых на добровольной основе обеспечивается соблюдение требований к безопасности рассматриваемых высокоавтоматизированных землеройных и дорожно-строительных машин.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Машины землеройные

МАШИНЫ ВЫСОКОАВТОМАТИЗИРОВАННЫЕ ЗЕМЛЕРОЙНЫЕ И ДОРОЖНО-СТРОИТЕЛЬНЫЕ

Технические требования и методы испытаний

Earth moving machines. Highly automated earth-moving and road-building machines. Technical requirements and test methods

Дата введения — 2025—01—01

1 Область применения

Настоящий стандарт устанавливает требования и методы испытаний в отношении безопасности работы автоматизированной системы управления в совокупности с исполнительными механизмами землеройных и дорожно-строительных машин, в зависимости от их уровня автоматизации, путем анализа отказов и составления матрицы рисков.

Настоящий стандарт не относится к области испытаний землеройной и дорожно-строительной техники на соответствие ее технических параметров выполнению дорожно-строительных работ.

Требования настоящего стандарта не распространяются на испытание тракторов и самоходных машин с целью определения соблюдения их соответствия требованиям дорожно-строительной технологии.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO 12100 Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска

ГОСТ Р 12.2.011 Система стандартов безопасности труда. Машины строительные, дорожные и землеройные. Общие требования безопасности

ГОСТ Р 27.302 Надежность в технике. Анализ дерева неисправностей

ГОСТ Р 27.607 Надежность в технике. Управление надежностью. Условия проведения испытаний на безотказность и статистические критерии и методы оценки их результатов

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

ГОСТ Р 57612 Эргономика. Система звуковых и визуальных сигналов опасности и информационных сигналов

ГОСТ Р 58837 Автомобильные транспортные средства. Системы автоматизированного управления. Общие принципы проектирования

ГОСТ Р 70850 Тракторы и машины сельскохозяйственные. Высокоавтоматизированные машинно-тракторные агрегаты. Технические требования и методы испытаний

ГОСТ Р 70851 Тракторы и машины сельскохозяйственные. Полигон для испытания высокоавтоматизированных машинно-тракторных агрегатов. Технические требования

ГОСТ Р 70852 Тракторы и машины сельскохозяйственные. Аппаратно-программный комплекс для управления высокоавтоматизированными машинно-тракторными агрегатами. Технические требования и методы испытаний

Издание официальное

ГОСТ Р ИСО 7731 Эргономика. Сигналы опасности для административных и рабочих помещений. Звуковые сигналы опасности

ГОСТ Р ИСО 20474-1 Машины землеройные. Безопасность. Часть 1. Общие требования

ГОСТ Р 59898 Оценка качества систем искусственного интеллекта. Общие положения

ГОСТ ISO 15998 Машины землеройные. Системы управления с использованием электронных компонентов. Критерии эффективности и испытания на функциональную безопасность

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.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **дорожно-строительные машины;** ДСМ: Группа машин (автомобильной техники), предназначенных для дорожного строительства, а также для ремонта и очистки дорог, которую в зависимости от выполняемых функций разделяют на группы: машины для подготовительных работ, землеройные машины, машины для укладки и обслуживания дорожных покрытий и пр. [1]

3.1.2 **высокоавтоматизированные землеройная и дорожно-строительная машины;** ВАЗДСМ: Землеройная и дорожно-строительная машины с оператором на борту или без него с возможностью высокоавтоматизированной работы, в том числе с установленным прицепным и навесным оборудованием, сконструированные специально для применения автоматической системы управления, которая активна в работе в пределах ограничений условий эксплуатации.

Примечание — Уровни автоматизации 1—5 — согласно ГОСТ Р 58823—2020. ВАЗДСМ, предназначенные для АСУ рассматриваемых ВАЗДСМ: высокоавтоматизированные самоходные землеройные и дорожно-строительные машины с оператором на борту или без него с возможностью высокоавтоматизированной работы, в том числе с установленным навесным оборудованием, сконструированный специально для применения автоматической системы управления, которая активна при выполнении заданий, в пределах ограничений условий эксплуатации.

3.1.3 **рассматриваемые высокоавтоматизированные землеройная и дорожно-строительная машины;** РВАЗДСМ: Высокоавтоматизированные землеройная и дорожно-строительная машины, оснащенные аппаратно-программным комплексом и исполнительными механизмами.

3.1.4

система [технология] автоматизации управления движением (driving automation system or technology): Аппаратные и программные средства систем автоматического управления движением 1-го — 5-го уровней, которые в совокупности способны выполнять всю задачу управления движением или ее часть в длительном режиме.

Примечание — В отличие от этого общего термина, характеризующего системы 1-го — 5-го уровней, термин «Автоматическая система управления движением» (АСУД) используется только для систем 3-го — 5-го уровней. Ввиду сходства между общим термином «система автоматизации управления движением» и термином «автоматическая система управления движением», применяемым для уровней 3—5, второй термин предпочтительнее использовать в виде аббревиатуры АСУД.

[ГОСТ Р 58823—2020, пункт 2.8]

3.1.5

задача управления движением, ЗУД [dynamic driving task (DDT)]: Совокупность выполняемых в реальном времени функций управления и планирования действий (тактические функции), которые требуются для управления транспортным средством в условиях дорожного движения, исключая стратегические функции, такие как планирование поездок, выбор пунктов назначения и промежуточных точек маршрутов.

[ГОСТ Р 58823—2020, пункт 2.13]

3.1.6 **препятствие:** Окружающие объекты, находящиеся в неподвижном состоянии, затрудняющие выполнение операций эксплуатационного задания.

3.1.7

исполнительное устройство; ИУ: Элементы конструкций высокоавтоматизированных землеройной и дорожно-строительной машин, выполняющие функции управления машинами и их агрегатами с помощью механизмов (двигатель, трансмиссия, органы управления, система подачи топлива, тормозная система, электрическая система, гидравлическая система).

[Адаптировано из ГОСТ Р 70850—2023, пункт 3.1.28]

3.1.8

высокоавтоматизированная работа: Функция, контролируемая системой автоматического управления без непосредственного вмешательства локального или удаленного оператора.

[ГОСТ Р 70850—2023, пункт 3.1.3]

3.1.9 **управление траекториями землеройной и дорожно-строительной машин:** Подзадача задания работы, включающая действия, необходимые для длительного управления в реальном времени движением высокоавтоматизированных землеройной и дорожно-строительной машин.

Примечания

1 Управление траекторией РВАЗДСМ включает определение положения РВАЗДСМ относительно границ полосы движения и воздействие на управление направления движения при уровнях автоматизации 0—3 или на исполнительные органы при уровнях автоматизации 3—5.

2 Движение РВАЗДСМ идентифицируется прямолинейным: в направлении оси Y и его поворотом вправо или влево относительно оси X (см. рисунок 1).

3.1.10 **управление скоростями землеройной и дорожно-строительной машин:** Подзадача управления, включающая действия, необходимые для длительного управления в реальном времени движением землеройной и дорожно-строительной машин.

Примечание — Управление скоростями землеройной и дорожно-строительной машин включает поддержание заданной скорости, а также обнаружение идущего впереди попутного целевого объекта, поддержание необходимой дистанции до идущего впереди целевого объекта и создание тягового или тормозного усилия для поддержания требуемой траектории, скорости или дистанции.

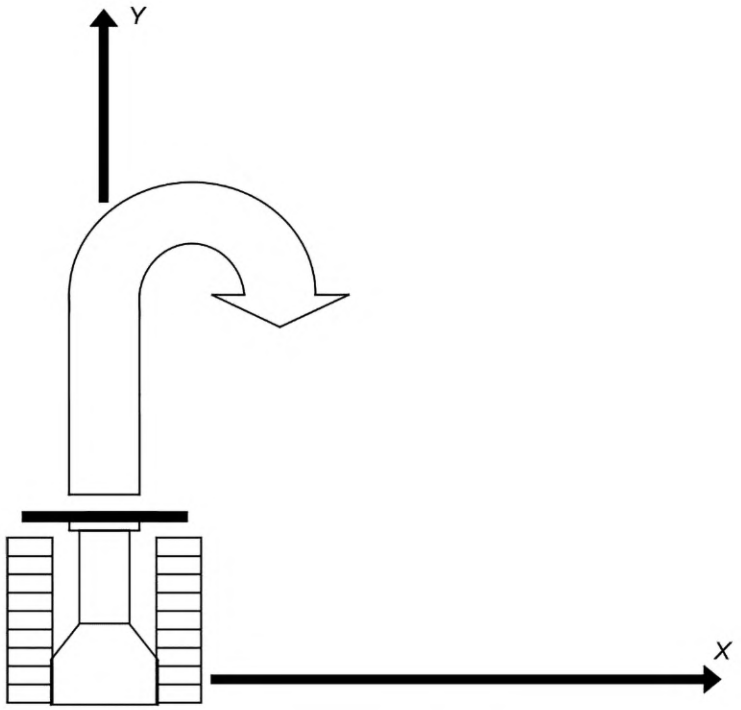


Рисунок 1 — Управление траекторией РВАЗДСМ

3.1.11

мониторинг: Набор функций, которые выполняются человеком или высокоавтоматизированными землеройной и дорожно-строительной машинами в реальном времени и включают наблюдение и обработку данных, используемых для управления транспортным средством или для обеспечения возможности управления им.

Примечание — Управление скоростями землеройной и дорожно-строительной машин включает поддержание заданной скорости, а также обнаружение идущего впереди попутного целевого объекта, поддержание необходимой дистанции до идущего впереди целевого объекта и создание тягового или тормозного усилия для поддержания требуемой траектории, скорости или дистанции.

[Адаптировано из ГОСТ Р 58823—2020, пункт 2.19]

3.1.12

мониторинг оператора: Действия и (или) автоматизированные операции, предназначенные для оценки степени, в которой оператор выполняет предписанную ему роль (функцию).

Примечание — Мониторинг оператора актуален в основном на УА 2 и УА 3. В отношении систем более низкого УА нет свидетельств неправильного использования или злоупотребления технологией автоматизации управления движением. АСУ более высокого УА всегда способны выполнять условие минимизации рисков.

[ГОСТ Р 70850—2023, пункт 3.1.8]

3.1.13 **управление землеройной и дорожно-строительной машинами:** Действия, выполняемые оператором с применением одной или более функций уровней автоматизации 1 и 2 или без них или системы автоматизации управления; уровней автоматизации 1, 2 и 3 для выполнения задания во время движения данных землеройной и дорожно-строительной машин.

3.1.14 **уровень эксплуатации**; УЭ: Конкретные условия для выполнения задания РВАЗДСМ, включая (но не ограничиваясь) условия окружающей среды, метеоусловия, географический регион, ограничения, связанные со временем суток, наличие или отсутствие специальных требований.

3.1.15

вред: Причинение ущерба здоровью человека, окружающей среде, имуществу, экономические потери.

[ГОСТ Р 54124—2010, пункт 3.2]

3.1.16

опасность (hazard): Потенциальная угроза нанесения физической травмы или причинения вреда здоровью человека.

[ГОСТ ISO 12100—2013, пункт 3.6]

3.1.17

риск (risk): Сочетание вероятности нанесения и степени тяжести возможных травм или другого вреда здоровью.

[ГОСТ ISO 12100—2013, пункт 3.12]

3.1.18

предварительная оценка риска (risk estimation): Определение возможности и вероятности нанесения физической травмы или причинения вреда.

[Адаптировано из ГОСТ ISO 12100—2013, пункт 3.14]

3.1.19

оценка риска (risk assessment): Процесс, включающий анализ и оценку степени риска.

[Адаптировано из ГОСТ ISO 12100—2013, пункт 3.17]

3.1.20

анализ риска (risk analysis): Изучение технических характеристик машины в части ограничений, идентификации опасности и предварительная оценка степени риска.

[ГОСТ ISO 12100—2013, пункт 3.15]

3.1.21

защитная мера (protective measure): Мера, предпринимаемая для адекватного снижения степени риска:

- конструктором (разработка безопасной конструкции машины, средств защиты, дополнительных защитных мер и информации для пользователя);
- пользователем (осуществление безопасной эксплуатации, технический контроль, система допуска к работе; применение дополнительных защитных ограждений; использование средств индивидуальной защиты; обучение персонала).

[ГОСТ ISO 12100—2013, пункт 3.19]

3.1.22

неожиданный/непреднамеренный пуск: (unexpected/unintended start-up): Любой пуск, который вследствие своего неожиданного характера может привести к возникновению опасности для оператора.

Примечание 1 — Причиной такого пуска могут быть, например:

- команда пуска, выдаваемая в результате неисправности системы управления или внешнего воздействия на нее,
- команда пуска, выдаваемая в результате несвоевременного воздействия на орган управления пуском или на другие части машины, например датчик или элемент силового управления,
- возобновление энергоснабжения после его прерывания,
- внешнее или внутреннее воздействие на элементы машины (например, действие силы тяжести, ветра, самовоспламенения в двигателе внутреннего сгорания).

Примечание 2 — Пуск машины в режиме выполнения автоматического цикла не следует считать непреднамеренным, но он может оказаться неожиданным для оператора. Для предотвращения таких случаев следует принимать соответствующие защитные меры.

Примечание 3 — Рекомендации по предотвращению неожиданных пусков см. ISO 14118, пункт 3.2.

[ГОСТ ISO 12100—2013, пункт 3.31]

3.1.23

неисправность, отказ в работе (fault): Состояние машины, характеризующееся ее неспособностью выполнять заданную функцию. Исключение составляет остановка машины для профилактического технического обслуживания или других плановых действий подобного вида, а также из-за отсутствия внешних ресурсов (например, отключение энергоснабжения).

Примечание 1 — Отказ в работе часто является результатом повреждения машины, но может произойти и без этого.

Примечание 2 — Для машин и оборудования термин «fault» обычно применяется в соответствии с определениями IEV 191-05-01.

Примечание 3 — На практике термины «повреждение» и «отказ в работе» часто употребляются как синонимы.

[ГОСТ ISO 12100—2013, пункт 3.33]

3.1.24

тестирование: Проверка соответствия выполнения процессов действий рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин при опытной эксплуатации между ожидаемым и реальным поведением техники в специально заданных условиях.

[Адаптировано из ГОСТ Р 70850—2023, пункт 3.1.21]

3.1.25

программа испытаний (test program): Проверка соответствия выполнения процессов действий рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин при опытной эксплуатации между ожидаемым и реальным поведением техники в специально заданных условиях.

[Адаптировано из ГОСТ Р 16504—81, статья 13]

3.1.26

оператор: Физическое лицо, активирующее автоматизированную систему вождения высокоавтоматизированных землеройной и дорожно-строительной машин и контролирующее действия этих высокоавтоматизированных землеройной и дорожно-строительной машин в автоматизированном режиме управления, а также осуществляющее ручное управление в период опытной эксплуатации.

[Адаптировано из ГОСТ Р 70850—2023, пункт 3.1.22]

3.1.27

локальный оператор: Человек, осуществляющий основное управление при опытной эксплуатации посредством бортовых органов управления или посредством пульта управления.

[ГОСТ Р 70850—2023, пункт 3.1.23]

3.1.28

удаленный оператор: Человек, осуществляющий основное управление при опытной эксплуатации посредством системы диспетчерского управления при УА 3—5, получающий данные в целях контроля работы машины и находящийся не в машине, а в зоне тестирования.

[ГОСТ Р 70850—2023, пункт 3.1.24]

3.1.29

пульт управления: Беспроводной или проводной ручной (переносной) блок управления с интерфейсами к системе управления и с возможностью исключительно локальной или удаленной эксплуатации.

[ГОСТ Р 70850—2023, пункт 3.1.25]

3.1.30 **подсистема управления:** Программно-аппаратные средства, осуществляющие воздействие на исполнительные механизмы высокоавтоматизированных землеройной и дорожно-строительной машин без физического воздействия со стороны оператора, с возможностью автоматического отключения при воздействии самого оператора на органы управления для перехода в режим ручного управления при необходимости, в том числе для предотвращения опасной ситуации.

3.1.31

пульт управления: Беспроводной или проводной ручной (переносной) блок управления с интерфейсами к системе управления и с возможностью исключительно локальной или удаленной эксплуатации.

[ГОСТ Р 70850—2023, пункт 3.1.25]

3.1.32

включенное состояние: Состояние высокоавтоматизированных землеройной и дорожно-строительной машин, при котором осуществляется высокоавтоматизированная работа.

[Адаптировано из ГОСТ Р 70850—2023, пункт 3.1.26]

3.1.33

отключенное состояние: Состояние высокоавтоматизированных землеройной и дорожно-строительной машин, в котором высокоавтоматизированная работа не активирована.

[Адаптировано из ГОСТ Р 70850—2023, пункт 3.1.27]

3.1.34 **препятствие:** Объект или состояние поверхности, которые могут причинить ущерб или быть повреждены в случае соприкосновения (контакта) или столкновения с высокоавтоматизированным машинным оборудованием.

3.1.35 **активация двигателя:** Включение автоматизированного управления двигателем рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин в зоне тестирования.

3.1.36 **автоматизированное управление двигателем:** Управление движением и скоростью высокоавтоматизированных землеройной и дорожно-строительной машин.

3.1.37

цифровая топографическая карта: Цифровая картографическая модель, содержание которой соответствует содержанию топографической карты определенного масштаба.

[ГОСТ Р 51605—2023, пункт 3.1]

3.1.38

собственник: Юридическое лицо, которому на праве собственности принадлежат высокоавтоматизированные землеройная и дорожно-строительная машины и которое участвует в проведении тестирования на добровольной основе.

[Адаптировано из ГОСТ Р 70850—2023, пункт 3.1.31]

3.1.39

испытательный полигон: Подготовленный участок земли с элементами инфраструктуры с использованием цифровых систем, оснащенный испытательным оборудованием и обеспечивающий проведение испытаний высокоавтоматизированных землеройной и дорожно-строительной машин, их аппаратно-программного комплекса или компонентов отдельных подсистем, а также элементов инфраструктуры в сфере строительно-дорожного комплекса в условиях, близких к условиям их штатной эксплуатации, установленных в рамках нормативной и технической документации.

[Адаптировано из ГОСТ Р 70851—2023, пункт 3.1]

3.1.40 **уровень полноты безопасности высокоавтоматизированных землеройной и дорожно-строительной машин;** УПБ: Комбинация четырех уровней рисков, используемых для определения соответствия уровня безопасности рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин необходимым требованиям, заложенным в конструкции.

3.1.41

компонент обнаружения; КО: Исполнительные элементы подсистем системы автоматизированного управления (видеокамеры, радары, лидары, датчики и т. п.).

[ГОСТ Р 70852—2023, пункт 3.5]

3.2 В настоящем стандарте применены следующие сокращения:

- АПК — аппаратно-программный комплекс;
- АСУ — автоматизированная система управления;
- БУ — блок управления;
- ГНСС — глобальная навигационная спутниковая система;
- ДСМ — дорожно-строительные машины;
- ЗВД — запасной вариант действия;
- ИМ — исполнительные механизмы;
- КО — компонент обнаружения;
- ПО — программное обеспечение;
- ПС — подсистема системы автоматизированного управления;
- УА — уровень автоматизации;
- УЭ — условия эксплуатации;
- ЦТС — целевое транспортное средство;
- ЭЗ — эксплуатационное задание.

4 Требования к безопасности рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин

4.1 Подсистема безопасности, входящая в состав АСУ РВАЗДСМ, должна подать предупредительный визуальный и (или) звуковой сигнал в случае возникновения риска при неисправности или обнаружении препятствия в предупредительной зоне (например, человека, животного или другой машины) и отключить все высокоавтоматизированные функции, а РВАЗДСМ должна перейти в свой заданный безопасный режим работы (функции движения и работы).

Примечание — Значения индикаторов (обозначений), а также все требуемые действия должны быть прописаны в техническом задании рассматриваемой РВАЗДСМ и соответствовать ГОСТ Р 57612, ГОСТ Р ИСО 7731.

4.2 Визуальный предупредительный сигнал

Визуальный предупредительный сигнал, воспринимаемый людьми, находящимися рядом с РВАЗДСМ, должен подаваться непрерывно в случае выбора высокоавтоматизированной работы. Режимы состояния РВАЗДСМ обозначаются визуально (см. таблицу 1).

Таблица 1 — Визуальное сопровождение режимов РВАЗДСМ

Режимы состояния РВАЗДСМ	Визуальный сигнал
Высокоавтоматизированная работа	Желтый
Приостановлена работа АСУ после обнаружения неисправности или объекта в предупредительной зоне	Зеленый
Ручное управление удаленного оператора	Зеленый
Режим ошибки	Красный

4.3 Звуковой предупредительный сигнал

Максимальная частота повторения не должна превышать 2 Гц. Интервал включения предупредительного сигнала должен быть равен интервалу отключения предупредительного сигнала в пределах 20 %.

Частотные и временные характеристики режимов сигнала должны соответствовать требованиям ГОСТ Р ИСО 7731.

5 Технические требования к уровню автоматизации рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин

5.1 Оценку соответствия высокоавтоматизированных самоходных землеройных и дорожно-строительных машин в соответствии с уровнем автоматизации управления следует производить согласно таблице 2.

Примечание — Уровни автоматизации рассматриваемой РВАЗДСМ устанавливаются согласно требованиям [2].

Таблица 2 — Выбор УА РВАЗДСМ

Уровень автоматизации	Описание
УА0 (отсутствует автоматизация)	Отсутствуют функции автоматического выполнения задания
УА1 (помощь оператору)	Управление скоростью или поддержание траектории РВАЗДСМ. Автоматическое выполнение некоторых операций
УА2 (частичная автоматизация выполнения задания)	Поддержание оптимальной траектории движения и скорости РВАЗДСМ, автоматическое выполнение некоторых рабочих операций. Оператор полностью контролирует работу РВАЗДСМ
УА3 (условная автоматизация выполнения задания)	Полное выполнение ЗУД без функции ЗВД в пределах, ограниченных УЭ. Оператор задает ограничения УЭ и выполняет ЗВД
УА4 (высокая автоматизация управления функциями)	Полное выполнение ЗУД и ЗВД в пределах, ограниченных УЭ. Оператор задает ограничения УЭ
УА5 (полная автоматизация управления)	Полное выполнение ЗУД и ЗВД без ограничения УЭ и вмешательства оператора в течение смены

5.2 Требования к САУ. Структура САУ РВАЗДСМ

В процессе проектирования РВАЗДСМ АСУ в зависимости от уровней автоматизации должна состоять из функциональных подсистем, приведенных на рисунке 2.

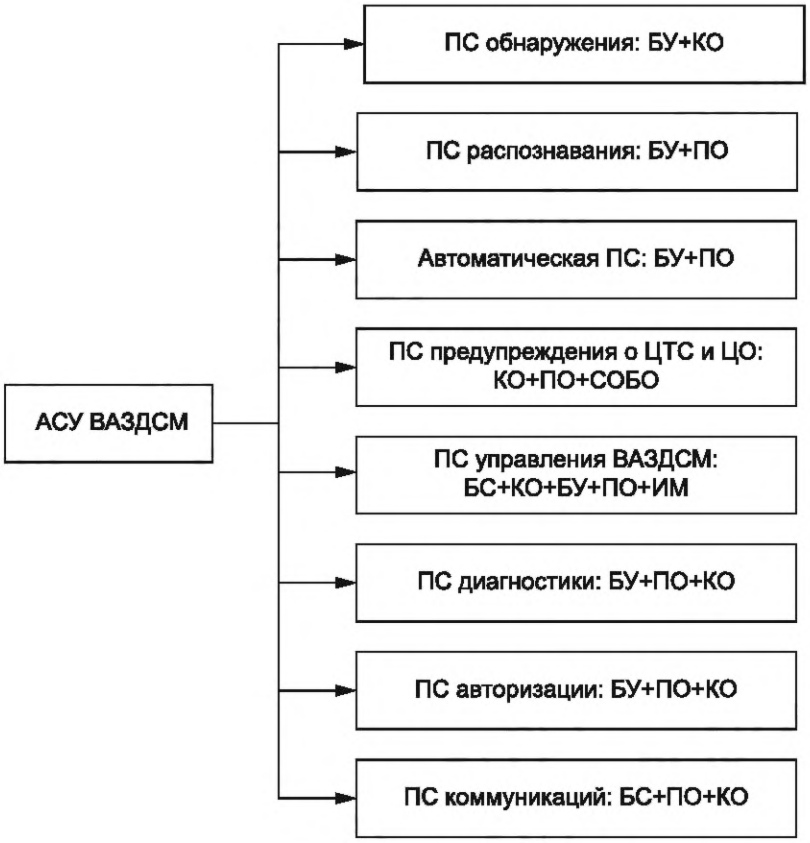


Рисунок 2 — Структура АСУ РВАЗДСМ

Требования к АСУ РВАЗДСМ — в соответствии с ГОСТ Р 58837.

6 Требования безопасности при испытании рассматриваемых землеройной и дорожно-строительной машин

6.1 Тестирование системы

Тестирование на соответствие заявленным параметрам выполнения операций задания РВАЗДСМ на УА 1—5 проводится на испытательном полигоне с использованием методов испытаний в соответствии с приложением А. УПБ РВАЗДСМ определяют в соответствии с приложением Б и ГОСТ ISO 12100.

В процессе испытаний фиксируются произошедшие опасности и опасные ситуации. На основе полученных данных составляется матрица рисков и на ее основе делается заключение об УПБ РВАЗДСМ.

6.2 Уровень автоматизации 1

6.2.1 Роль оператора и АСУ

Локальный оператор выполняет часть оперативных и тактических функций в режиме реального времени, необходимых для безопасного управления РВАЗДСМ, контролирует работу АСУ РВАЗДСМ и при необходимости вмешивается в технологический процесс для поддержания работоспособности машины. АСУ (при включенном состоянии) обеспечивает адаптивную помощь для эффективности работы ДСМ.

6.2.2 Принципы защиты

Для обеспечения соответствующего уровня безопасности:

- РВАЗДСМ должны быть оснащены средствами, позволяющими локальному оператору останавливать или запускать АСУ;

- для системы основного доступа к операторскому посту должно быть предусмотрено освещение, если платформа операторского поста находится на высоте более 3 м. Включение огней должно быть возможно с земли и локального поста оператора;
- локальный оператор должен осуществлять контроль работы РВАЗДСМ.

6.2.3 Коммуникации и сети

Во время всего рабочего процесса РВАЗДСМ осуществляется постоянный мониторинг и подтверждение наличия связи между локальным оператором и РВАЗДСМ.

6.2.3.1 Виды рисков и отказов

а) Риски

Сбои в работе связи и сети могут привести к следующим рискам для безопасности:
- невозможности остановить машину в аварийной ситуации;
- отсутствию доступа к информации об осведомленности о ситуации;
- потере или задержке ввода команд;
- потере устаревшей информации;
- утерянной или задержанной информации об опасности.

б) Режимы отказа

Режимы сбоев связи включают:
- потерю связи;
- ухудшение качества связи;
- задержку связи.

в) Потенциальные причины

Режимы сбоя могут быть результатом любой из следующих причин:
- проблемы с шумом (непреднамеренные помехи);
- физические изменения в сети;
- изменения конфигурации сети;
- проблемы с оборудованием;
- проблемы с питанием;
- преднамеренный взлом или подмена;
- преднамеренное заклинивание.

6.2.3.2 Требования к системам связи

При любом сбое связи РВАЗДСМ должны поддерживать безопасный режим работы с помощью безотказных средств (например, с помощью активного мониторинга, нескольких независимых каналов связи).

Там, где этого требует оценка риска, РВАЗДСМ должны иметь средства обнаружения потери связи, ухудшения качества связи или повреждения коммуникаций. Машины должны иметь средства приведения в действие регулируемой остановки и должны поддерживать безопасное состояние в случае потери, повреждения или задержки связи. Скорость работы устройства и текущие условия эксплуатации следует использовать в сочетании с оценкой риска для определения максимально допустимой продолжительности потери связи или ухудшения качества связи.

Должны быть предусмотрены средства для предотвращения несанкционированного контроля и подмены или саботажа РВАЗДСМ.

Приемлемость таких средств должна быть определена на основе оценки риска. Подходящие средства включают ограничение физического доступа, аутентификацию, использование брандмауэра, шифрование данных и ограничение внешнего подключения за пределами сайта.

6.2.4 Включение/отключение АСУ РВАЗДСМ

Средство включения/отключения АСУ должно быть на каждой РВАЗДСМ.

Средства включения/отключения АСУ обязаны быть:
- идентифицируемыми;
- доступными для локального оператора;
- установленными в кабинах РВАЗДСМ и защищенными от непреднамеренного приведения в действие.

Индикация состояний АСУ должна быть однозначной (четкой) и легко опознаваемой (идентифицируемой).

Доступные состояния управления должны включать в себя:
- отключенное состояние АСУ;
- включенное состояние АСУ.

Примечание — В отключенном состоянии все подсистемы АСУ должны быть остановлены и отключены. Возможность запускать работу АСУ осуществляет только локальный оператор.

Работа АСУ осуществляется до моментов:

- отключения системы управления оператором;
- возникновения неисправного состояния машины и ее оборудования.

6.2.5 Правила эксплуатации

Перед запуском АСУ должна запрашивать разрешение локального оператора.

После отключения АСУ (независимо от причины) запуск повторного включения АСУ осуществляется локальным оператором.

6.2.6 Управление двигателем

6.2.6.1 Запуск двигателя

РВАЗДСМ должны производить запуск двигателя исключительно в ответ на запрос локального оператора о запуске двигателя.

Перед запуском (прокруткой) двигателя должен быть подан звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и запуском двигателя (предстартовое предупреждение), длительность предупреждения после запуска двигателя должны быть достаточными для избегания опасностей с учетом характеристик РВАЗДСМ.

Запуск двигателя допускается исключительно после истечения периода предстартового предупреждения.

Локальный оператор должен выключить двигатель при попадании препятствия в опасную зону вокруг РВАЗДСМ в течение периода предупреждения или во время запуска двигателя.

В случае остановки запуска двигателя на более чем 1 с процесс предупреждения о запуске двигателя должен быть запущен заново.

6.2.6.2 Проверка эксплуатационной опасности

Локальным оператором должен осуществляться постоянный мониторинг опасной зоны вокруг РВАЗДСМ с целью обнаружения препятствий при работающем двигателе во время работы АСУ.

6.2.6.3 Остановка работы двигателя

АСУ РВАЗДСМ должна выключить двигатель при получении запроса от оператора на остановку двигателя.

При повторном запуске двигателя АСУ должна послать запрос локальному оператору на подтверждение пуска.

6.2.6.4 Неисправность (отказ) двигателя

В случае неисправности (отказа) двигателя, препятствующей безопасной эксплуатации РВАЗДСМ в соответствии с проектной спецификацией, РВАЗДСМ должны перейти в заданный безопасный режим работы, а АСУ РВАЗДСМ должна быть отключена автоматически до устранения неисправности.

6.2.6.5 Автоматический контроль состояния двигателя РВАЗДСМ

Должен быть обеспечен постоянный автоматический контроль состояния двигателя с информированием оператора о его состоянии.

Для обеспечения безопасной работы необходимо постоянное подтверждение связи с АСУ в соответствии с проектной документацией. В случае потери связи РВАЗДСМ должны оповестить локального оператора и перейти в заданный безопасный режим работы.

6.2.7 Автоматизированное управление двигателем

Автоматизированное управление двигателем допускается только при активизации АСУ. Автоматизированные системы управления двигателем должны обеспечить номинальные режимы траектории и скорости РВАЗДСМ при непосредственном контроле локального оператора.

Опасная зона вокруг РВАЗДСМ должна контролироваться локальным оператором с целью обнаружения препятствий в течение всего предстартового периода и времени работы.

6.2.7.1 Начало движения

РВАЗДСМ должны начинать движение исключительно при подтверждении оператором запроса об активации двигателя и отсутствия препятствий в зоне перемещения.

Активация двигателей допускается исключительно после истечения предстартового периода предупреждения. Она не должна приводить к возникновению опасных ситуаций (см. ГОСТ Р 70850).

До начала движения подается звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреж-

дения и движением и продолжительность предупреждения после активации двигателей должны быть достаточными для предотвращения соответствующих опасностей с учетом технических характеристик РВАЗДСМ.

Движение РВАЗДСМ допускается исключительно после истечения предстартового периода предупреждения.

Локальный оператор должен прервать запуск движения при попадании РВАЗДСМ в опасную зону в течение периода предупреждения.

Если движение затрудняется по причине отсутствия связи, РВАЗДСМ должны перейти в заданный безопасный режим работы, а локальный оператор должен быть оповещен автоматически, либо звуковым сигналом, либо с помощью уведомления на дисплее, установленном в машине.

6.2.7.2 Остановка движения

Локальный оператор должен остановить движение при попадании в опасную зону. РВАЗДСМ должны останавливать движение в ответ на запрос, полученный от оператора.

Если во время работы в АСУ возникнет неисправность, РВАЗДСМ должны автоматически остановить движение, не создавая опасной ситуации, а АСУ должна быть отключена до устранения неисправности (см. ГОСТ Р 70852).

Если может возникнуть опасность, необходимо предотвратить самопроизвольный перезапуск машины при ее повторном включении после отключения питания (например, с помощью автономного реле, контактора или клапана).

6.2.8 Блокировка автоматизированной системы управления

Блокировка АСУ РВАЗДСМ, включая возобновление (перезапуск) режима помощи, не должна создавать опасных ситуаций.

В руководстве для оператора РВАЗДСМ должен быть описан порядок действий оператора при отключении и включении АСУ РВАЗДСМ.

Должны быть предусмотрены доступные локальному оператору средства [такие, как клавишные (кнопочные) переключатели, пароли или подобные средства] для возобновления работы АСУ, автоматическое управление которой было заблокировано, и для дальнейшей передачи управления оператору.

Если ни один подобный пользовательский интерфейс не применим, РВАЗДСМ должны быть переведены в заданный безопасный режим работы до момента, пока высокоавтоматизированная работа не будет возобновлена, а оператор — уведомлен автоматически о блокировке АСУ, либо звуковым сигналом, либо с помощью уведомления на дисплее, установленном в машине.

6.2.9 Контроль неисправностей

Неисправности, вызванные проблемами надежности (в результате отказа оборудования в системе), и сбой, вызванный несоответствием техническому заданию или ПО (например, функционирует ли система должным образом в исправном состоянии при различных параметрах окружающей среды), не должны создавать опасных условий.

6.2.10 Эксплуатационное состояние РВАЗДСМ

Соответствующая информация об эксплуатационном состоянии РВАЗДСМ и информация по безопасности должны быть доступны оператору в любой момент рабочего процесса и осуществления сервисных работ.

Локальный оператор самостоятельно задает параметры работы РВАЗДСМ.

6.2.11 Бортовая электрическая мощность

РВАЗДСМ должны реагировать на сбои в работе электропитания, в том числе на потерю питания всех контроллеров, которые влияют на движение машины.

Источник электропитания должен обеспечивать подачу питания на системы машины для достижения остановленного состояния и поддержания безопасного состояния.

РВАЗДСМ должны иметь достаточный источник электроэнергии во время работы в автономном режиме, включая:

- достаточный запас заряда батареи для предполагаемых условий окружающей среды;
- достаточную мощность генератора переменного тока для дополнительной электроники, связанной с дистанционным управлением;
- проводку с достаточными размерами для увеличения токоведущей способности.

Аккумуляторы РВАЗДСМ должны иметь достаточную емкость для обслуживания всей электроники машины при отключенном двигателе или генераторе для поддержания безопасного состояния и завершения упорядоченного отключения машины при любых предполагаемых условиях окружающей среды.

При непреднамеренной потере электропитания машины во время работы РВАЗДСМ должны перейти в безопасное состояние.

РВАЗДСМ должны обладать достаточной электрической мощностью, чтобы выдерживать дополнительные нагрузки, требуемые автономной электроникой (в дополнение к общим требованиям к машине) для всех предполагаемых условий эксплуатации и окружающей среды (например, низкий холостой ход или ночное время).

6.3 Уровень автоматизации 2

6.3.1 Роль оператора

Локальный оператор выполняет часть оперативных и тактических функций в режиме реального времени, необходимых для безопасного управления РВАЗДСМ, контролирует работу АСУ РВАЗДСМ и при необходимости вмешивается в рабочий процесс для поддержания работоспособности машины. АСУ (при включенном состоянии) обеспечивает адаптивную помощь для эффективности работы РВАЗДСМ.

6.3.2 Принципы защиты

Для обеспечения соответствующего уровня безопасности:

- РВАЗДСМ должны быть оснащены средствами, безопасно позволяющими локальному оператору останавливать или запускать высокоавтоматизированную работу;
- для системы основного доступа к операторскому посту должно быть предусмотрено освещение, если платформа операторского поста находится на высоте более 3 м. Включение огней должно быть возможно с земли и поста оператора;
- в случае обнаружения или попадания в опасную зону препятствия РВАЗДСМ система должна оповестить звуковым или визуальным предупредительным сигналом и перейти в заданное безопасное состояние;
- локальный оператор должен иметь полный доступ для осуществления соответствующего контроля работы АСУ РВАЗДСМ.

6.3.3 Коммуникация и сети

Во время всего рабочего процесса РВАЗДСМ осуществляются постоянный мониторинг и подтверждение наличия связи между локальным оператором и РВАЗДСМ.

6.3.3.1 Виды рисков и отказов

а) Риски

Сбои в работе связи и сети могут привести к следующим рискам для безопасности:

- невозможности остановить машину в аварийной ситуации;
- отсутствию доступа к информации об осведомленности о ситуации;
- потере или задержке ввода команд;
- потере устаревшей информации;
- утерянной или задержанной информации об опасности;

б) Режимы отказа

Режимы сбоев, связанных со связью, включают:

- потерю связи;
- ухудшение качества связи;
- задержку связи;
- неверно направленную связь;
- измененную связь;
- связь с нарушением последовательности.

в) Потенциальные причины

Режимы сбоя могут быть результатом:

- проблемы с шумом (непреднамеренные помехи);
- физических изменений в сети;
- изменения конфигурации сети;
- проблемы с оборудованием;
- проблемы с питанием;
- преднамеренного взлома или подмены;
- преднамеренного заклинивания.

6.3.3.2 Требования к системам связи

РВАЗДСМ должны поддерживать безопасный режим работы в случае любого сбоя, связанного со связью. Где оценка риска показывает необходимость, РВАЗДСМ должны иметь безотказные средства (например, с помощью активного мониторинга, нескольких независимых каналов связи) для поддержания безопасного состояния.

Там, где этого требует оценка риска, РВАЗДСМ должны иметь средства обнаружения потери связи, ухудшения качества связи или повреждения коммуникаций. Машины должны иметь средства приведения в действие регулируемой остановки и должны поддерживать безопасное состояние в случае потери, повреждения или задержки связи. Скорость работы устройства и текущие условия эксплуатации следует использовать в сочетании с оценкой риска для определения максимально допустимой продолжительности потери связи или ухудшения качества связи.

Должны быть предусмотрены средства для предотвращения несанкционированного контроля и подмены или саботажа РВАЗДСМ.

Приемлемость таких средств должна быть определена на основе оценки риска. Подходящие средства включают ограничение физического доступа, аутентификацию, использование брандмауэра, шифрование данных и ограничение внешнего подключения за пределами сайта.

6.3.4 Включение/отключение РВАЗДСМ

Средство включения/отключения АСУ должно быть на каждой РВАЗДСМ.

Средство включения/отключения АСУ обязано быть:

- идентифицируемым;
- доступным для локального оператора;
- установленным в кабине и снаружи РВАЗДСМ, защищенным от непреднамеренного приведения в действие.

Индикация состояний АСУ должна быть однозначной (четкой) и легко опознаваемой (идентифицируемой).

Доступные состояния управления должны включать в себя:

- отключенное состояние АСУ;
- включенное состояние АСУ.

Примечание — В отключенном состоянии все подсистемы АСУ должны быть остановлены и отключены. Возможность запускать работу АСУ осуществляет только локальный оператор.

Работа АСУ осуществляется до моментов:

- отключения системы управления оператором;
- возникновения неисправного состояния.

Оператор определяет, является ли целесообразным включение/отключение АСУ.

Высокоавтоматизированная работа РВАЗДСМ осуществляется до моментов отключения АСУ оператором или при возникновении неисправного состояния.

6.3.5 Проверка эксплуатационной опасности

Локальным оператором должен осуществляться постоянный мониторинг опасной зоны вокруг РВАЗДСМ с целью обнаружения препятствий при работающем двигателе во время работы АСУ.

Если может возникнуть опасность, необходимо предотвратить самопроизвольный перезапуск машины при ее повторном включении после отключения питания (например, с помощью автономного реле, контактора или клапана).

6.3.6 Управление двигателем

6.3.6.1 Запуск двигателя

РВАЗДСМ должны производить запуск двигателя исключительно в ответ на запрос локального оператора о запуске двигателя.

Перед запуском (прокруткой) двигателя должен быть подан звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и запуском двигателя (предстартовое предупреждение), длительность предупреждения после запуска двигателя должны быть достаточными для избегания опасностей с учетом характеристик РВАЗДСМ.

Запуск двигателя допускается исключительно после истечения периода предстартового предупреждения.

Локальный оператор должен выключить двигатель при попадании препятствия в опасную зону вокруг РВАЗДСМ в течение периода предупреждения или во время запуска двигателя.

В случае остановки запуска двигателя на более чем 1 с процесс предупреждения о запуске двигателя должен быть запущен заново.

6.3.6.2 Остановка работы двигателя

АСУ РВАЗДСМ должна выключить двигатель при получении запроса от оператора на остановку двигателя.

При повторном запуске двигателя АСУ должна послать запрос локальному оператору на подтверждение пуска.

6.3.6.3 Неисправность (отказ) двигателя

В случае неисправности (отказа) двигателя, препятствующей безопасной эксплуатации РВАЗДСМ в соответствии с проектной спецификацией, РВАЗДСМ должны перейти в заданное безопасное состояние, а АСУ РВАЗДСМ должна быть отключена автоматически до устранения неисправности.

6.3.6.4 Автоматический контроль состояния двигателя РВАЗДСМ

Должен быть обеспечен постоянный автоматический контроль состояния двигателя с информированием оператора о его состоянии.

Для обеспечения безопасной работы необходимо постоянное подтверждение связи с АСУ в соответствии с проектной документацией. В случае потери связи РВАЗДСМ должны оповестить оператора и перейти в заданное безопасное состояние.

6.3.7 Автоматизированное управление двигателем

Автоматизированное управление двигателем допускается только при активизации АСУ. Системы управления двигателем должны обеспечить номинальные режимы траектории и скорости РВАЗДСМ при непосредственном контроле оператором.

Опасная зона вокруг РВАЗДСМ должна контролироваться локальным оператором с целью обнаружения препятствий в течение всего предстартового периода и времени работы.

6.3.7.1 Начало движения

РВАЗДСМ должны начинать движение исключительно при подтверждении оператором запроса об активации двигателя и отсутствия препятствий в зоне перемещения.

Активация двигателей допускается исключительно после истечения предстартового периода предупреждения и не должна приводить к возникновению опасной ситуации (см. ГОСТ Р 70850).

До начала движения подается звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и движением и продолжительность предупреждения после активации двигателей должны быть достаточными для предотвращения соответствующих опасностей с учетом технических характеристик РВАЗДСМ.

Движение РВАЗДСМ допускается исключительно после истечения предстартового периода предупреждения.

Локальный оператор должен прервать запуск движения при попадании РВАЗДСМ в опасную зону в течение периода предупреждения.

Если движение затрудняется по причине отсутствия связи, система должна перейти в заданное безопасное состояние, а локальный оператор должен быть оповещен автоматически.

6.3.7.2 Остановка движения

Локальный оператор должен остановить движение при попадании в опасную зону. РВАЗДСМ должны останавливать движение в ответ на запрос, полученный от оператора.

Если во время работы в АСУ возникнет неисправность, РВАЗДСМ должны автоматически остановить движение, не создавая опасной ситуации, а АСУ должна быть отключена до устранения неисправности (см. ГОСТ Р 70852).

6.3.8 Блокировка автоматизированной системы управления

Блокировка АСУ РВАЗДСМ, включая возобновление (перезапуск) режима помощи, не должна создавать опасных ситуаций.

В руководстве для оператора РВАЗДСМ должен быть описан порядок действий оператора при отключении и включении АСУ РВАЗДСМ.

Должны быть предусмотрены доступные локальному оператору средства [такие, как клавишные (кнопочные) переключатели, пароли или подобные средства] для возобновления работы АСУ, автоматическое управление которой было заблокировано, и для дальнейшей передачи управления оператору.

Если ни один подобный пользовательский интерфейс не применим, функция должна быть переведена в заданное безопасное состояние до момента, пока высокоавтоматизированная работа не будет возобновлена, а оператор — уведомлен автоматически о блокировке АСУ.

6.3.9 Контроль неисправностей

Неисправности, вызванные проблемами надежности (в результате отказа оборудования в системе), и сбой, вызванный несоответствием техническому заданию или программному обеспечению (например, функционирует ли система должным образом в исправном состоянии при различных параметрах окружающей среды), не должны создавать опасных условий.

6.3.10 Эксплуатационное состояние РВАЗДСМ

Соответствующая информация об эксплуатационном состоянии РВАЗДСМ и информация по безопасности должны быть доступны оператору в любой момент рабочего процесса и осуществления сервисных работ.

Локальный оператор самостоятельно задает параметры работы РВАЗДСМ.

6.3.11 Бортовая электрическая мощность

РВАЗДСМ должны реагировать на сбои в работе электропитания, в том числе на потерю питания всех контроллеров, которые влияют на движение машины.

Источник электропитания должен обеспечивать подачу питания на системы машины для достижения остановленного состояния и поддержания безопасного состояния.

РВАЗДСМ должны иметь достаточный источник электроэнергии во время работы в автономном режиме, включая:

- достаточный запас заряда батареи для предполагаемых условий окружающей среды;
- достаточную мощность генератора переменного тока для дополнительной электроники, связанной с дистанционным управлением;
- проводку достаточных размеров для увеличения токоведущей способности.

Аккумулятор РВАЗДСМ должен иметь достаточную емкость для обслуживания всей электроники машины при отключенном двигателе или генераторе, для поддержания безопасного состояния и завершения упорядоченного отключения машины при любых предполагаемых условиях окружающей среды.

При непреднамеренной потере электропитания машины во время работы РВАЗДСМ должны перейти в безопасное состояние.

РВАЗДСМ должны обладать достаточной электрической мощностью, чтобы выдерживать дополнительные нагрузки, требуемые автономной электроникой (в дополнение к общим требованиям к машине) для всех предполагаемых условий эксплуатации и окружающей среды (например, низкий холостой ход или ночное время).

6.4 Уровень автоматизации 3

6.4.1 Роль оператора и АСУ

Локальный оператор проводит проверку эксплуатационной готовности РВАЗДСМ, оснащенных АПК непосредственно перед его работой. По запросу АСУ РВАЗДСМ локальный оператор может управлять процессом работы машин. В течение всего периода выполнения задания локальный оператор контролирует рабочий процесс посредством подсистемы оповещения АСУ, находясь в кабине. РВАЗДСМ возможно управлять удаленно длительное время в течение смены с помощью дистанционного пульта управления.

6.4.2 Принципы защиты

Для обеспечения соответствующего уровня безопасности РВАЗДСМ должны соответствовать требованиям защиты, при которых:

- для системы основного доступа к операторскому посту должно быть предусмотрено освещение, если платформа операторского поста находится на высоте более 3 м. Включение огней должно быть возможно с земли и поста оператора.
- все РВАЗДСМ должны иметь бортовые средства управления (кнопки, джойстики и т. д.) для их остановки;
- РВАЗДСМ должны быть оснащены системой распознавания, позволяющей обнаруживать и определять местоположение людей или прочих препятствий относительно РВАЗДСМ, предотвращать непреднамеренные перемещения за пределы рабочей зоны;
- перед каждым перемещением РВАЗДСМ система безопасности должна обеспечить (подтвердить) отсутствие препятствий в опасной зоне;
- при выполнении высокоавтоматизированных операций в случае обнаружения или попадания в опасную зону препятствия РВАЗДСМ должны подать звуковой или визуальный предупредительный сигнал и перейти в заданное безопасное состояние;

- РВАЗДСМ должны быть оснащены средствами, позволяющими локальному или удаленному оператору останавливать или запускать высокоавтоматизированную работу;
- в РВАЗДСМ должны быть предусмотрены системы управления, обеспечивающие достижения безопасных рабочих температур и давлений в тормозной и рулевой системах (например, колесный погрузчик), а также в системах управления направлением движения (например, бульдозер) до запуска РВАЗДСМ в автономном режиме;
- РВАЗДСМ должны позволять осуществление соответствующего контроля локальным или удаленным оператором.

6.4.3 Коммуникации и сети

Во время всего рабочего процесса РВАЗДСМ осуществляется постоянный мониторинг и подтверждение наличия связи между системой дистанционного управления и РВАЗДСМ.

При рассмотрении пропускной способности будут учитываться требования к вспомогательным машинам и взаимодействию с оператором. Важной эксплуатационной проблемой является необходимость осведомленности о зонах с потенциально высоким уровнем помех (например, местах расположения очередей).

6.4.3.1 Виды рисков и отказов

а) Риски

Сбои в работе связи и сети могут привести к следующим рискам для безопасности:
- невозможности дистанционно остановить машину или к аварийной ситуации;
- отсутствию доступа к информации об осведомленности о ситуации;
- потере или задержке ввода команд;
- потере устаревшей информации;
- утерянной или задержанной информации об опасности.

б) Режимы отказа

Режимы сбоев, связанных со связью, включают:
- потерю связи;
- ухудшение качества связи, включая потерю одного направления;
- задержку связи;
- неверно направленную связь;
- измененную связь;
- связь с нарушением последовательности.

в) Потенциальные причины

Режимы сбоя могут быть результатом:
- проблемы с шумом (непреднамеренные помехи);
- физических изменений в сети;
- изменений конфигурации сети;
- проблемы с оборудованием;
- экологических проблем, например связанных с погодой, солнечными пятнами;
- изменения топологии;
- проблемы с питанием;
- преднамеренного взлома или подмены;
- преднамеренного заклинивания.

6.4.3.2 Требования к системам связи

РВАЗДСМ должны поддерживать безопасный режим работы в случае любого сбоя, связанного со связью. Где оценка риска показывает необходимость, РВАЗДСМ должны иметь безотказные средства (например, с помощью активного мониторинга, нескольких независимых каналов связи) для удаленной остановки и поддержания безопасного состояния.

Там, где этого требует оценка риска, РВАЗДСМ должны иметь средства обнаружения потери связи, ухудшения качества связи или повреждения коммуникаций. Машина должна иметь средства приведения в действие регулируемой остановки и должна поддерживать безопасное состояние в случае потери, повреждения или задержки связи. Скорость работы устройства и текущие условия эксплуатации следует использовать в сочетании с оценкой риска для определения максимально допустимой продолжительности потери связи или ухудшения качества связи.

Должны быть предусмотрены средства для предотвращения несанкционированного контроля и подмены или саботажа РВАЗДСМ.

Приемлемость таких средств должна быть определена на основе оценки риска. Подходящие средства включают ограничение физического доступа, аутентификацию, использование брандмауэра, шифрование данных и ограничение внешнего подключения за пределами сайта.

6.4.4 Включение/отключение РВАЗДСМ

Средство включения/отключения АСУ должно быть на каждой из РВАЗДСМ.

Средство включения/отключения АСУ обязано быть:

- идентифицируемым;
- доступным для локального оператора;
- установленным в кабине и снаружи РВАЗДСМ, в том числе удаленно, защищенным от непреднамеренного приведения в действие.

Индикация состояний АСУ должна быть однозначной (четкой) и легко опознаваемой (идентифицируемой).

Доступные состояния управления должны включать в себя:

- отключенное состояние АСУ;
- включенное состояние АСУ.

Примечание — В отключенном состоянии все подсистемы АСУ должны быть остановлены и отключены. Возможность запускать работу АСУ осуществляет только локальный оператор.

Работа АСУ осуществляется до моментов:

- отключения системы управления оператором;
- возникновения неисправного состояния.

В отключенном состоянии все высокоавтоматизированные операции РВАЗДСМ должны быть остановлены и отключены. Во включенном состоянии выполнение высокоавтоматизированных операций должно быть разрешено.

Должна быть предусмотрена возможность отключения высокоавтоматизированной работы в любое время либо на позиции локального оператора, либо при удаленном контроле — на позиции удаленного управления.

Запуск РВАЗДСМ в режиме высокоавтоматизированной работы осуществляется автоматически.

Высокоавтоматизированная работа РВАЗДСМ осуществляется до моментов:

- отключения системы управления оператором;
- обнаружения препятствия, создающего опасность;
- возникновения неисправного состояния АСУ или ИМ.

6.4.5 Проверка эксплуатационной опасности

Возможность запуска высокоавтоматизированной работы без подтверждения системой распознавания отсутствия препятствий в опасной зоне должна быть исключена. Запуск высокоавтоматизированной работы должен запрашивать разрешение оператора РВАЗДСМ, кроме тех случаев, когда оценка рисков показывает отсутствие рисков потери безопасности.

В случае прекращения высокоавтоматизированной работы (независимо от причины) для процедуры повторной активации высокоавтоматизированного режима должен требоваться запуск АСУ оператором РВАЗДСМ.

Должен осуществляться постоянный мониторинг опасной зоны вокруг РВАЗДСМ с целью обнаружения препятствий при работающем двигателе во время высокоавтоматизированной работы.

6.4.6 Управление двигателем

6.4.6.1 Запуск двигателя

РВАЗДСМ должны производить запуск двигателей исключительно в ответ на запрос оператора о запуске двигателя.

Перед запуском (прокруткой) двигателя должен быть подан звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и запуском двигателя (предстартовое предупреждение), длительность предупреждения после запуска двигателя должны быть достаточными для избегания опасностей с учетом характеристик РВАЗДСМ.

Запуск двигателя допускается исключительно после истечения периода предстартового предупреждения.

Оператор должен выключить двигатель при попадании препятствия в опасную зону вокруг двигателя в течение периода предупреждения или во время запуска двигателя.

В случае остановки запуска двигателя на более чем 1 с процесс предупреждения о запуске двигателя должен быть запущен заново.

6.4.6.2 Остановка работы двигателя

АСУ РВАЗДСМ должны выключить двигатели при получении запроса от оператора на остановку двигателя.

При повторном запуске двигателя АСУ должна послать запрос локальному оператору на подтверждение пуска.

6.4.6.3 Неисправность (отказ) двигателя

В случае неисправности (отказа) двигателей, препятствующей безопасной эксплуатации РВАЗДСМ в соответствии с проектной спецификацией, РВАЗДСМ должны перейти в заданное безопасное состояние, а АСУ РВАЗДСМ должна быть отключена автоматически до устранения неисправности.

6.4.6.4 Автоматический контроль состояния двигателей РВАЗДСМ

Должен быть обеспечен постоянный автоматический контроль состояния двигателя с информированием оператора о его состоянии.

Для обеспечения безопасной работы необходимо постоянное подтверждение связи с АСУ в соответствии с проектной документацией. В случае потери связи РВАЗДСМ должны оповестить оператора и перейти в заданное безопасное состояние.

6.4.7 Автоматизированное управление двигателем

Автоматизированное управление двигателем допускается только при активизации АСУ. Системы управления двигателем должны обеспечить номинальные режимы траектории и скорости РВАЗДСМ при непосредственном контроле оператором.

Опасная зона вокруг РВАЗДСМ должна сканироваться с целью обнаружения препятствий в течение всего предстартового периода и времени работы.

6.4.7.1 Начало движения

РВАЗДСМ должны начинать движение исключительно при подтверждении оператором запроса об активации двигателя и отсутствия препятствий в зоне перемещения.

Активация двигателей допускается исключительно после истечения предстартового периода предупреждения и не должна приводить к возникновению опасной ситуации (см. ГОСТ Р 70850).

До начала движения подается звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и движением и продолжительность предупреждения после активации двигателей должны быть достаточными для предотвращения соответствующих опасностей с учетом технических характеристик РВАЗДСМ.

Движение РВАЗДСМ допускается исключительно после истечения предстартового периода предупреждения.

Оператор должен прервать запуск движения при попадании РВАЗДСМ в опасную зону в течение периода предупреждения.

Если движение затрудняется по причине отсутствия связи, система должна перейти в заданное безопасное состояние, а удаленный оператор должен быть оповещен автоматически.

6.4.7.2 Остановка движения

Локальный оператор должен остановить движение при попадании в опасную зону. РВАЗДСМ должны останавливать движение в ответ на запрос, полученный от оператора. Отсутствие препятствий в опасной зоне должно постоянно подтверждаться при движении РВАЗДСМ в режиме высокоавтоматизированной работы (см. ГОСТ Р 70852).

Если во время работы в АСУ возникнет неисправность, РВАЗДСМ должны автоматически остановить движение, не создавая опасной ситуации, а АСУ должна быть отключена до устранения неисправности.

В случае, если движение РВАЗДСМ затрудняется (например, при обнаружении препятствия), РВАЗДСМ должны перейти в заданное безопасное состояние. Дальнейшее движение должно осуществляться по команде оператора.

6.4.8 Блокировка автоматизированной системы управления

Блокировка АСУ РВАЗДСМ, включая возобновление (перезапуск) режима помощи, не должна создавать опасных ситуаций.

Намеренная активация органов управления, предусмотренных на бортовой рабочей станции оператора, дистанционном пульте управления или на станции удаленного оператора для управления функциями движения [например, контроль направления, торможение, остановка (отключение) рабочих

органов], должна блокировать высокоавтоматизированную работу. Такая блокировка автоматического управления, включая возобновление (перезапуск) высокоавтоматизированной работы, не должна создавать опасных ситуаций.

Руководство для оператора РВАЗДСМ должно описывать, как перевести управление РВАЗДСМ с высокоавтоматизированной работы на управление оператором и с управления оператором на высокоавтоматизированную работу.

Должны быть предусмотрены доступные локальному оператору средства [такие, как клавишные (кнопочные) переключатели, пароли или подобные средства] для возобновления работы АСУ, автоматическое управление которой было заблокировано, и для дальнейшей передачи управления оператору.

Если ни один подобный пользовательский интерфейс не применим, функция должна быть переведена в заданное безопасное состояние до момента, когда высокоавтоматизированная работа не будет возобновлена, а оператор уведомлен автоматически о блокировке АСУ.

6.4.9 Удаленная остановка высокоавтоматизированной работы

Когда оценка риска показывает необходимость, РВАЗДСМ должны быть оснащены системой удаленной остановки. Механизм остановки высокоавтоматизированной работы должен быть легкодоступным для оператора на всех позициях управления.

После остановки машины должно потребоваться вмешательство оператора для возобновления движения машины.

Для оператора РВАЗДСМ, не требующего бортовой станции или удаленной станции оператора, должен быть предусмотрен дистанционный пульт управления.

6.4.10 Подсистема распознавания

Подсистема распознавания содержит датчики восприятия, используемые для сбора информации об окружении РВАЗДСМ и последующей передачи информации алгоритмам обнаружения, локализации и распознавания (классификация) потенциального объекта, представляющего интерес. Целью системы машинного восприятия является предоставление информации, необходимой для безопасного управления РВАЗДСМ, без необходимости взаимодействия с оператором.

Если для обеспечения того, чтобы подсистема распознавания работала в соответствии с системными требованиями, требуется возможность тестирования и калибровки, интегратор РВАЗДСМ должен предоставить такую возможность.

6.4.10.1 Виды рисков и отказов

а) Неспособность обнаружить объект или несвоевременное обнаружение объекта.

Примерами неспособности обнаружить препятствие или позднего обнаружения объекта являются:

- объекты, скрытые из-за пыли, тумана, снега, дождя или других затемняющих факторов;
- результаты восприятия, которые становятся ненадежными из-за плохого освещения;
- препятствия, которые скрыты из-за наклона РВАЗДСМ;
- неровный грунт, приводящий к изменению плоскости сканирования; например, лазерный луч может попадать на землю или указывать в небо, когда машина наклоняется вниз или вверх;
- вибрация или движение машины, приводящие к смещению датчиков;
- объекты, движущиеся слишком быстро, чтобы их можно было обнаружить;
- слишком маленькие объекты;
- объекты, которые не отражаются обратно в направлении приемника; например, способность радиолокационной технологии идентифицировать объект может зависеть от эффективного поперечного сечения радара объекта;
- прозрачные или темные объекты, не отражающие лазерный луч;
- не обнаруживающиеся отрицательные объекты (дыры в рельефе);
- увеличение задержки из-за других приложений или вычислительной нагрузки на процессор, используемый для подсистемы распознавания или классификации объектов.

б) Ложное обнаружение несуществующего объекта

Примерами ложного обнаружения являются:

- пыль или другие затемняющие вещества, которые отражают достаточно энергии, чтобы быть классифицированными как объект;
- материал на передатчике или приемнике, ошибочно распознаваемый как объект.

в) Ошибочное местоположение обнаруженного объекта

Примерами ошибочного местоположения являются:

- смещение датчика, приводящее к неточной оценке положения;

- системные ошибки, приводящие к неточному положению или ориентации машины;
- вибрация крепления датчика, вызывающая движение датчика, которое не учитывается системой восприятия;
- пыль или затемняющие вещества, размывающие края.

г) Неправильная классификация объекта

Примерами неправильной классификации объекта являются:
- пыль или затемняющие вещества, размывающие края;
- неадекватное обучение или валидация классификатора.

6.4.10.2 Требования

Системные требования к бортовой системе РВАЗДСМ или подсистеме РВАЗДСМ должны основываться на оценке риска, характеристиках машины (например, скорость, видимость, нормальная работа) и местности эксплуатации (например, поверхность, подземелье, открытая местность, туннель).

Подсистема распознавания должна поддерживать безопасное состояние РВАЗДСМ во время любого взаимодействия с предполагаемой рабочей средой (например, рельефом местности, пылью, погодными условиями, условиями освещения).

Подсистема распознавания должна быть способна обнаруживать объекты в требуемой области (например, ожидаемая траектория движения), которые находятся либо на положительном, либо на отрицательном склоне, как требуется на основе оценки риска.

РВАЗДСМ должны быть способны обнаруживать, когда подсистема распознавания не функционирует в соответствии с минимальными требованиями, основанными на оценке риска, и поддерживать машину в безопасном состоянии.

При нефункционировании подсистемы необходимо уведомить оператора или систему контроля РВАЗДСМ.

При необходимости на основе оценки риска эксплуатационные пределы подсистемы распознавания в руководстве пользователя должны быть указаны, например размер мишени, форма и отражательная способность, дальность восприятия, угловой охват.

6.4.10.3 Поведение системы распознавания в исправном состоянии

Система должна функционировать надлежащим образом в условиях и при ограничениях, предусмотренных для эксплуатации, включая предусмотренное ненадлежащее использование. Ограничения системы распознавания должны быть описаны в руководстве оператора.

Ограничения могут быть вызваны: несоответствующими условиями окружающей среды, такими как солнечное излучение, темнота, туман, температура, все типы атмосферных осадков и условий, особенности местности и участки, поросшие травой и кустарником; несоответствующими параметрами, связанными с препятствиями, например слишком малые размеры, слишком высокая скорость передвижения препятствий или низкая отражающая способность; несоответствующими параметрами, связанными с неисправностями или сбоями в работе РВАЗДСМ по таким причинам, как смещение датчика/датчиков, слишком высокая скорость работы, загрязнение на датчике, слишком сильные вибрации или слишком большая загрузка процессора вычислениями.

Если с удаленным оператором (при автономной работе) уровень достоверности датчиков системы распознавания опускается ниже минимального порога работоспособности, требуемого для безопасной эксплуатации, РВАЗДСМ должны перейти в безопасное состояние. Система диагностики РВАЗДСМ должна указать и зафиксировать причину, по которой было запущено безопасное состояние. Для РВАЗДСМ с оператором на борту запуск безопасного состояния может быть заменен звуковым предупреждением, если оценка рисков допускает, что этого достаточно.

6.4.11 Контроль неисправностей

Неисправности, вызванные проблемами надежности (в результате отказа оборудования в системе), и сбой, вызванный несоответствием техническому заданию или ПО (например, функционирует ли система должным образом в исправном состоянии при различных параметрах окружающей среды), не должны создавать опасных условий.

Контроль неисправностей и рабочие характеристики должны проверяться путем испытаний ПС распознавания на испытательном полигоне по методикам приложения А.

Все неисправные состояния систем распознавания и определения местонахождения/ориентирования РВАЗДСМ должны быть идентифицированы. Требуемый уровень эффективности и уровень полноты безопасности должны быть определены с учетом всех предусмотренных неисправных состояний, угроз, возникающих при использовании РВАЗДСМ в неисправном состоянии, прогнозируемой серьезности ущерба и вероятности нанесения ущерба, принимая во внимание вероятное присутствие

сторонних наблюдателей и возможности сторонних наблюдателей избежать опасности. При обнаружении остаточного опасного неисправного состояния РВАЗДСМ должны перейти в заданное безопасное состояние.

6.4.12 Управление с помощью удаленного оператора

Управление с помощью удаленного оператора должно позволять непрямой визуальный мониторинг (например, с помощью камеры) зоны вокруг РВАЗДСМ, если того требует оценка рисков.

Все предупреждения, требуемые для локального оператора, должны подаваться на станции управления удаленного оператора. Удаленный оператор должен иметь возможность вмешиваться (действовать) со станции удаленного управления для отключения высокоавтоматизированной работы.

6.4.13 Бортовая электрическая мощность

РВАЗДСМ должны реагировать на сбои в работе электропитания, в том числе на потерю питания всех контроллеров, которые влияют на движение машин.

Источник электропитания должен обеспечивать подачу питания на системы машины для достижения остановленного состояния и поддержания безопасного состояния.

РВАЗДСМ должны иметь достаточный источник электроэнергии во время работы в автономном режиме, включая:

- достаточный запас заряда батареи для предполагаемых условий окружающей среды;
- достаточную мощность генератора переменного тока для дополнительной электроники, связанной с дистанционным управлением;
- проводку достаточных размеров для увеличения токоведущей способности.

Аккумулятор РВАЗДСМ должен иметь достаточную емкость для обслуживания всей электроники машины при отключенном двигателе или генераторе, для поддержания безопасного состояния и завершения упорядоченного отключения машины при любых предполагаемых условиях окружающей среды.

При непреднамеренной потере электропитания машины во время работы РВАЗДСМ должны перейти в безопасное состояние.

РВАЗДСМ должны обладать достаточной электрической мощностью, чтобы выдерживать дополнительные нагрузки, требуемые автономной электроникой (в дополнение к общим требованиям к машине) для всех предполагаемых условий эксплуатации и окружающей среды (например, низкий холостой ход или ночное время).

6.5 Уровень автоматизации 4

6.5.1 Роль оператора и АСУ

Локальный оператор проводит проверку эксплуатационной готовности РВАЗДСМ, оснащенных АПК, непосредственно перед их работой. Оператор имеет возможность контролировать процесс выполнения задания РВАЗДСМ, находясь в кабине машины в качестве пассажира или удаленно, используя дистанционный пульт управления или приложение, устанавливаемое на мобильный телефон. В течение смены вмешательство оператора в работу РВАЗДСМ не требуется. АПК выполняет задание самостоятельно. РВАЗДСМ проводят работы и мониторинг технического состояния автономно. Оператор осуществляет работы лишь при построении задания АСУ и устранении неисправностей по запросу АСУ.

6.5.2 Принципы защиты

Необходимые требования для РВАЗДСМ УА 4 вследствие их тяжелых условий работы для обеспечения соответствующего уровня безопасности:

- для системы основного доступа к операторскому посту должно быть предусмотрено освещение, если платформа операторского поста находится на высоте более 3 м. Включение огней должно быть возможно с земли и поста оператора;
- все РВАЗДСМ должны иметь бортовые средства управления (кнопки, джойстики и т. д.) для их остановки;
- при работе РВАЗДСМ в заданных условиях эксплуатации АСУ должна обеспечивать торможение машины при сохранении безопасной работы (например, торможение в неблагоприятных условиях);
- в РВАЗДСМ должны быть предусмотрены системы управления, обеспечивающие достижения безопасных рабочих температур и давлений в тормозной и рулевой системах (например, колесный погрузчик), а также в системах управления направлением движения (например, бульдозер) до запуска РВАЗДСМ в автономном режиме;
- РВАЗДСМ должны быть оснащены системой распознавания, позволяющей обнаруживать и определять местоположение людей или прочих препятствий относительно РВАЗДСМ;

- РВАЗДСМ должны быть оснащены системой распознавания, позволяющей определять положение и ориентацию РВАЗДСМ так, как это требуется для соответствующих операций, а также предотвращать непреднамеренные перемещения за пределы рабочей зоны;
- перед каждым перемещением РВАЗДСМ система безопасности должна обеспечить (подтвердить) отсутствие препятствий в опасной зоне;
- при выполнении высокоавтоматизированных операций в случае обнаружения или попадания в опасную зону препятствия РВАЗДСМ должны подать звуковой или визуальный предупредительный сигнал и перейти в заданное безопасное состояние;
- РВАЗДСМ должны быть оснащены средствами, позволяющими локальному или удаленному оператору останавливать или запускать высокоавтоматизированную работу;
- РВАЗДСМ должны позволять осуществление соответствующего контроля локальным или удаленным оператором.

6.5.3 Коммуникации и сети

Во время всего рабочего процесса РВАЗДСМ осуществляется постоянный мониторинг и подтверждение наличия связи между системой дистанционного управления и РВАЗДСМ.

При рассмотрении пропускной способности будут учитываться требования к вспомогательным машинам и взаимодействию с оператором. Важной эксплуатационной проблемой является необходимость в осведомленности о зонах с потенциально высоким уровнем помех (например, местах расположения очередей).

6.5.3.1 Виды рисков и отказов

а) Риски

Сбои в работе связи и сети могут привести к следующим рискам для безопасности:
- невозможности дистанционно остановить машину или к аварийной ситуации;
- отсутствию доступа к информации об осведомленности о ситуации;
- неточным данным о местности;
- потере или задержке ввода команд;
- недостаточному контролю на перекрестке;
- потере координации машины;
- потере устаревшей информации;
- утерянной или задержанной информации об опасности;
- неточному местоположению (из-за потери коррекции ГНСС);
- неточной информации о планировании;
- неточному отслеживанию персонала;
- потере возможности дистанционного включения системы противопожарной защиты.

б) Режимы отказа

Режимы сбоев, связанных со связью, включают:
- потерю связи;
- ухудшение качества связи, включая потерю одного направления;
- задержку связи;
- неверно направленную связь;
- измененную связь;
- связь с нарушением последовательности.

в) Потенциальные причины

Режимы сбоя могут быть результатом:
- проблемы с шумом (непреднамеренные помехи);
- физических изменений в сети;
- изменения конфигурации сети;
- проблемы с оборудованием;
- экологических проблем (например, связанных с погодой, солнечными пятнами);
- изменения топологии;
- проблемы с питанием;
- преднамеренного взлома или подмены;
- преднамеренного заклинивания.

6.5.3.2 Требования к системам связи

РВАЗДСМ должны поддерживать безопасный режим работы в случае любого сбоя, связанного со связью. Где оценка риска показывает необходимость, РВАЗДСМ должны иметь безотказные средства

(например, с помощью активного мониторинга, нескольких независимых каналов связи) для удаленной остановки и поддержания безопасного состояния.

Там, где этого требует оценка риска, РВАЗДСМ должны иметь средства обнаружения потери связи, ухудшения качества связи или повреждения коммуникаций. Машина должна иметь средства приведения в действие регулируемой остановки и должна поддерживать безопасное состояние в случае потери, повреждения или задержки связи. Скорость работы устройства и текущие условия эксплуатации следует использовать в сочетании с оценкой риска для определения максимально допустимой продолжительности потери связи или ухудшения качества связи.

Должны быть предусмотрены средства для предотвращения несанкционированного контроля и подмены или саботажа РВАЗДСМ.

Приемлемость таких средств должна быть определена на основе оценки риска. Подходящие средства включают ограничение физического доступа, аутентификацию, использование брандмауэра, шифрование данных и ограничение внешнего подключения за пределами сайта.

6.5.4 Включение/отключение РВАЗДСМ

Средство включения/отключения АСУ должно быть на каждой из РВАЗДСМ.

Средство включения/отключения АСУ обязано быть:

- идентифицируемым;
- доступным для локального оператора;
- установленным в кабине, снаружи РВАЗДСМ и на станции удаленного оператора, защищенным от непреднамеренного приведения в действие.

Индикация состояний АСУ должна быть однозначной (четкой) и легко опознаваемой (идентифицируемой).

Доступные состояния управления должны включать в себя:

- отключенное состояние АСУ;
- включенное состояние АСУ.

Примечание — В отключенном состоянии все подсистемы АСУ должны быть остановлены и отключены. Возможность запускать работу АСУ осуществляет только локальный оператор.

В отключенном состоянии все высокоавтоматизированные операции РВАЗДСМ должны быть остановлены и отключены. Во включенном состоянии выполнение высокоавтоматизированных операций должно быть разрешено.

Должна быть предусмотрена возможность отключения высокоавтоматизированной работы в любое время либо на позиции локального оператора, либо при удаленном контроле — на позиции удаленного управления.

Запуск РВАЗДСМ в режиме высокоавтоматизированной работы осуществляется автоматически.

Высокоавтоматизированная работа РВАЗДСМ осуществляется до моментов:

- отключения системы управления оператором;
- обнаружения препятствия, создающего опасность;
- возникновения неисправного состояния АСУ или ИМ.

6.5.5 Проверка эксплуатационной опасности

Возможность запуска высокоавтоматизированной работы без подтверждения системой распознавания отсутствия препятствий в опасной зоне должна быть исключена. Запуск высокоавтоматизированной работы должен осуществляться с разрешения оператора РВАЗДСМ, кроме тех случаев, когда оценка рисков показывает отсутствие рисков потери безопасности.

В случае прекращения высокоавтоматизированной работы (независимо от причины) для процедуры повторной активации высокоавтоматизированного режима должен требоваться запуск АСУ оператором РВАЗДСМ.

Должен осуществляться постоянный мониторинг опасной зоны вокруг РВАЗДСМ с целью обнаружения препятствий при работающем двигателе во время высокоавтоматизированной работы.

6.5.6 Управление двигателем

6.5.6.1 Запуск двигателя

РВАЗДСМ должны производить запуск двигателя исключительно в ответ на запрос локального оператора о запуске двигателя.

Перед запуском (прокруткой) двигателя должен быть подан звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между пода-

чей звукового предупреждения и запуском двигателя (предстартовое предупреждение), длительность предупреждения после запуска двигателя должны быть достаточными для предотвращения опасностей с учетом характеристик РВАЗДСМ.

Запуск двигателя допускается исключительно после истечения периода предстартового предупреждения.

Локальный оператор должен выключить двигатель при попадании препятствия в опасную зону вокруг РВАЗДСМ в течение периода предупреждения или во время запуска двигателя.

В случае остановки запуска двигателя на более чем 1 с процесс предупреждения о запуске двигателя должен быть запущен заново.

6.5.6.2 Остановка работы двигателя

АСУ РВАЗДСМ должна выключить двигатель при получении запроса от оператора на остановку двигателя.

При повторном запуске двигателя АСУ должна послать запрос локальному оператору на подтверждение пуска.

6.5.6.3 Неисправность (отказ) двигателя

В случае неисправности (отказа) двигателя, препятствующей безопасной эксплуатации РВАЗДСМ в соответствии с проектной спецификацией, РВАЗДСМ должны перейти в заданное безопасное состояние, а АСУ РВАЗДСМ должна быть отключена автоматически до устранения неисправности.

6.5.6.4 Автоматический контроль состояния двигателей РВАЗДСМ

Должен быть обеспечен постоянный автоматический контроль состояния двигателя с информированием оператора о его состоянии.

Для обеспечения безопасной работы необходимо постоянное подтверждение связи с АСУ в соответствии с проектной документацией. В случае потери связи РВАЗДСМ должны оповестить оператора и перейти в заданное безопасное состояние.

6.5.7 Автоматизированное управление двигателем

Автоматизированное управление двигателем допускается только при активизации АСУ. Системы управления двигателем должны обеспечить номинальные режимы траектории и скорости РВАЗДСМ при непосредственном контроле оператором.

Опасная зона вокруг РВАЗДСМ должна сканироваться с целью обнаружения препятствий в течение всего предстартового периода и времени работы.

6.5.7.1 Начало движения

РВАЗДСМ должны начинать движение исключительно при подтверждении оператором запроса об активации двигателя и отсутствии препятствий в зоне перемещения.

Активация двигателей допускается исключительно после истечения предстартового периода предупреждения и не должна приводить к возникновению опасной ситуации (см. ГОСТ Р 70850).

До начала движения подается звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и движением и продолжительность предупреждения после активации двигателей должны быть достаточными для предотвращения соответствующих опасностей с учетом технических характеристик РВАЗДСМ.

Движение РВАЗДСМ допускается исключительно после истечения предстартового периода предупреждения.

Оператор должен прервать запуск движения при попадании РВАЗДСМ в опасную зону в течение периода предупреждения.

Если движение затрудняется по причине отсутствия связи, система должна перейти в заданное безопасное состояние, а удаленный оператор должен быть оповещен автоматически.

6.5.7.2 Остановка движения

Локальный оператор должен остановить движение при попадании в опасную зону. РВАЗДСМ должны останавливать движение в ответ на запрос, полученный от оператора. Отсутствие препятствий в опасной зоне должно постоянно подтверждаться при движении РВАЗДСМ в режиме высокоавтоматизированной работы (см. ГОСТ Р 70852).

Если во время работы в АСУ возникнет неисправность, РВАЗДСМ должны автоматически остановить движение, не создавая опасной ситуации, а АСУ должна быть отключена до устранения неисправности.

В случае, если движение РВАЗДСМ затрудняется (например, при обнаружении препятствия), РВАЗДСМ должны перейти в заданное безопасное состояние. Дальнейшее движение должно осуществляться по команде оператора.

6.5.8 Блокировка АСУ

Блокировка АСУ РВАЗДСМ, включая возобновление (перезапуск) режима помощи, не должна создавать опасных ситуаций.

Намеренная активация органов управления, предусмотренных на бортовой рабочей станции оператора, дистанционном пульте управления или на станции удаленного оператора для управления функциями движения [например, контроль направления, торможение, остановка (отключение) рабочих органов], должна блокировать высокоавтоматизированную работу. Такая блокировка автоматического управления, включая возобновление (перезапуск) высокоавтоматизированной работы, не должна создавать опасных ситуаций.

Руководство для оператора РВАЗДСМ должно описывать, как перевести управление РВАЗДСМ с высокоавтоматизированной работы на управление оператором и с управления оператором на высокоавтоматизированную работу.

Должны быть предусмотрены доступные локальному оператору средства [такие, как клавишные (кнопочные) переключатели, пароли или подобные средства] для возобновления работы АСУ, автоматическое управление которой было заблокировано, и для дальнейшей передачи управления оператору.

Если ни один подобный пользовательский интерфейс не применим, функция должна быть переведена в заданное безопасное состояние до момента, пока высокоавтоматизированная работа не будет возобновлена, а оператор — уведомлен автоматически о блокировке АСУ.

6.5.9 Удаленная остановка высокоавтоматизированной работы

Когда оценка риска показывает необходимость, РВАЗДСМ должны быть оснащены системой удаленной остановки. Механизм остановки высокоавтоматизированной работы должен быть легкодоступным для оператора на всех позициях управления.

После остановки машины должно потребоваться вмешательство оператора для возобновления движения машины.

Для оператора РВАЗДСМ, не требующего бортовой станции или удаленной станции оператора, должен быть предусмотрен дистанционный пульт управления.

6.5.10 Подсистема распознавания

Подсистема распознавания содержит датчики восприятия, используемые для сбора информации об окружении РВАЗДСМ и последующей передачи информации алгоритмам обнаружения, локализации и распознавания (классификация) потенциального объекта, представляющего интерес. Целью системы машинного восприятия является предоставление информации, необходимой для безопасного управления РВАЗДСМ, без необходимости взаимодействия с оператором.

Если для обеспечения того, чтобы подсистема распознавания работала в соответствии с системными требованиями, требуется возможность тестирования и калибровки, интегратор РВАЗДСМ должен предоставить такую возможность.

6.5.10.1 Виды рисков и отказов

а) Неспособность обнаружить объект или несвоевременное обнаружение объекта

Примерами неспособности обнаружить препятствие или позднего обнаружения объекта являются:

- объекты, скрытые из-за пыли, тумана, снега, дождя или других затемняющих факторов;
- результаты восприятия, которые становятся ненадежными из-за плохого освещения;
- препятствия, которые скрыты из-за наклонов рассматриваемых РВАЗДСМ;
- неровный грунт, приводящий к изменению плоскости сканирования; например, лазерный луч может попадать на землю или указывать в небо, когда машина наклоняется вниз или вверх;
- вибрация или движение машин, приводящие к смещению датчиков;
- объекты, движущиеся слишком быстро, чтобы их можно было обнаружить;
- слишком маленькие объекты;
- объекты, которые не отражаются обратно в направлении приемника; например, способность радиолокационной технологии идентифицировать объект может зависеть от эффективного поперечного сечения радара объекта;
- прозрачные или темные объекты, не отражающие лазерный луч;
- не обнаруживающиеся отрицательные объекты (дыры в рельефе);

- увеличение задержки из-за других приложений или вычислительной нагрузки на процессор, используемый для подсистемы распознавания или классификации объектов.

б) Ложное обнаружение несуществующего объекта

Примерами ложного обнаружения являются:

- пыль или другие затемняющие вещества, которые отражают достаточно энергии, чтобы быть классифицированными как объект;
- материал на передатчике или приемнике, ошибочно распознаваемый как объект.

в) Ошибочное местоположение обнаруженного объекта

Примерами ошибочного местоположения являются:

- смещение датчика, приводящее к неточной оценке положения;
- системные ошибки, приводящие к неточному положению или ориентации машины;
- вибрация крепления датчика, вызывающая движение датчика, которое не учитывается системой восприятия;
- пыль или затемняющие вещества, размывающие края.

г) Неправильная классификация объекта

Примерами неправильной классификации объекта являются:

- пыль или затемняющие вещества, размывающие края;
- неадекватное обучение или валидация классификатора.

6.5.10.2 Требования

Системные требования к бортовой системе РВАЗДСМ или подсистеме распознавания РВАЗДСМ должны основываться на оценке риска, характеристиках машины (например, скорость, видимость, нормальная работа) и местности эксплуатации (например, поверхность, подземелье, открытая местность, туннель).

Подсистема распознавания должна поддерживать безопасное состояние РВАЗДСМ во время любого взаимодействия с предполагаемой рабочей средой (например, рельефом местности, пылью, погодными условиями, условиями освещения).

Подсистема распознавания должна быть способна обнаруживать объекты в требуемой области (например, ожидаемая траектория движения), которые находятся либо на положительном, либо на отрицательном склоне, как требуется на основе оценки риска.

РВАЗДСМ должны быть способны обнаруживать, когда подсистема распознавания не функционирует в соответствии с минимальными требованиями, основанными на оценке риска, и поддерживать машину в безопасном состоянии.

При нефункционировании подсистемы необходимо уведомить оператора или систему контроля РВАЗДСМ.

При необходимости на основе оценки риска эксплуатационные пределы подсистемы распознавания в руководстве пользователя должны быть указаны, например размер мишени, форма и отражательная способность, дальность восприятия, угловой охват.

6.5.10.3 Поведение системы распознавания в исправном состоянии

Система должна функционировать надлежащим образом в условиях и при ограничениях, предусмотренных для эксплуатации, включая предусмотренное ненадлежащее использование. Ограничения системы распознавания должны быть описаны в руководстве оператора.

Ограничения могут быть вызваны: несоответствующими условиями окружающей среды, такими как солнечное излучение, темнота, туман, температура, все типы атмосферных осадков и условий, особенности местности и участки, поросшие травой и кустарником; несоответствующими параметрами, связанными с препятствиями (например, слишком малые размеры, слишком высокая скорость передвижения препятствий или низкая отражающая способность); несоответствующими параметрами, связанными с неисправностями или сбоями в работе РВАЗДСМ по таким причинам, как смещение датчика/датчиков, слишком высокая скорость работы, загрязнение на датчике, слишком сильные вибрации или слишком большая загрузка процессора вычислениями.

Если с удаленным оператором (при автономной работе) уровень достоверности датчиков системы распознавания опускается ниже минимального порога работоспособности, требуемого для безопасной эксплуатации, РВАЗДСМ должны перейти в безопасное состояние. Система диагностики РВАЗДСМ должна указать и зафиксировать причину, по которой было запущено безопасное состояние. Для РВАЗДСМ с оператором на борту запуск безопасного состояния может быть заменен звуковым предупреждением, если оценка рисков допускает, что этого достаточно.

6.5.11 Контроль неисправностей

Неисправности, вызванные проблемами надежности (в результате отказа оборудования в системе), и сбой, вызванный несоответствием техническому заданию или программному обеспечению (например, функционирует ли система должным образом в исправном состоянии при различных параметрах окружающей среды), не должны создавать опасных условий.

Контроль неисправностей и рабочие характеристики должны проверяться путем испытаний ПС распознавания на испытательном полигоне по методикам приложения А.

Все неисправные состояния систем распознавания и определения местонахождения/ориентирования РВАЗДСМ должны быть идентифицированы. Требуемые уровень эффективности и уровень полноты безопасности должны быть определены с учетом всех предусмотренных неисправных состояний, угроз, возникающих при использовании РВАЗДСМ в неисправном состоянии, прогнозируемой серьезности ущерба и вероятности нанесения ущерба, принимая во внимание вероятное присутствие сторонних наблюдателей и возможности сторонних наблюдателей избежать опасности. При обнаружении остаточного опасного неисправного состояния РВАЗДСМ должны перейти в заданное безопасное состояние.

6.5.12 Управление с помощью удаленного оператора

Управление с помощью удаленного оператора должно позволять непрямой визуальный мониторинг (например, с помощью камеры) зоны вокруг РВАЗДСМ, если того требует оценка рисков.

Все предупреждения, требуемые для локального оператора, должны подаваться на станции управления удаленного оператора. Удаленный оператор должен иметь возможность вмешиваться (действовать) со станции удаленного управления для отключения высокоавтоматизированной работы.

6.5.13 Адаптация к условиям окружающей среды

Основываясь на оценке риска, РВАЗДСМ должны быть способны адаптироваться к условиям окружающей среды до тех пор, пока любые изменения в условиях окружающей среды находятся в пределах установленных ограничений. РВАЗДСМ УА-4 могут включать использование людей-операторов или автоматизированных систем для регулировки скорости, отключения операций, перекрытия зон или других регулировок, необходимых для поддержания безопасной эксплуатации.

6.5.14 Бортовая электрическая мощность

РВАЗДСМ должны реагировать на сбои в работе электропитания, в том числе на потерю питания всех контроллеров, которые влияют на движение машины.

Источник электропитания должен обеспечивать подачу питания на системы машины для достижения остановленного состояния и поддержания безопасного состояния.

РВАЗДСМ должны иметь достаточный источник электроэнергии во время работы в автономном режиме, включая:

- достаточный запас заряда батареи для предполагаемых условий окружающей среды;
- достаточную мощность генератора переменного тока для дополнительной электроники, связанной с дистанционным управлением;
- проводку достаточных размеров для увеличения токоведущей способности.

Аккумуляторы РВАЗДСМ должны иметь достаточную емкость для обслуживания всей электроники машины при отключенном двигателе или генераторе, для поддержания безопасного состояния и завершения упорядоченного отключения машины при любых предполагаемых условиях окружающей среды.

При непреднамеренной потере электропитания во время работы РВАЗДСМ должны перейти в безопасное состояние.

РВАЗДСМ должны обладать достаточной электрической мощностью, чтобы выдерживать дополнительные нагрузки, требуемые автономной электроникой (в дополнение к общим требованиям к машине) для всех предполагаемых условий эксплуатации и окружающей среды (например, низкий холостой ход или ночное время).

6.5.15 Позиционирование и ориентация РВАЗДСМ

Система позиционирования и ориентации, способная при прогнозируемых условиях эксплуатации обнаруживать объекты, находящиеся в зоне распознавания, должна быть предусмотрена на всех РВАЗДСМ УА-4.

Системы позиционирования и ориентации могут включать в себя широкий спектр технологий, включая ГНСС, датчики, лазерные сканеры, псевдолиты, теодолиты, радары, сопутствующие алгоритмы, необходимые для идентификации и классификации значимых объектов относительно РВАЗДСМ, а также системы беспроводной триангуляции, системы безопасного контроля для управления и системы

технического зрения, не требующего вмешательства человека. Каждая из этих технологий может иметь уникальные характеристики. Требования также будут зависеть от приложения. Требуемая от таких систем точность позиционирования и ориентации или частота измерений также зависят от скорости и местоположения машины.

Режимы потенциального риска из-за неисправности или отказа включают:

- неточное абсолютное положение для систем, использующих глобальную систему координат;
- неточное относительное положение для систем, использующих локальную систему координат;
- неточную ориентацию;
- неточную регистрацию в цифровой модели местности;
- несуществующее положение, ориентацию или регистрацию.

6.5.16 Требования

Аналогичные системы позиционирования и ориентации должны иметь средства для определения состояния системы, например вероятности ошибки измерения, точности, разрешающей способности.

Когда состояние системы позиционирования и ориентации недостаточное для позиционирования с требуемой точностью, которая может динамически изменяться в зависимости от состояния РВАЗДСМ, РВАЗДСМ должны поддерживать безопасный режим работы.

РВАЗДСМ должны содержать достаточно независимых средств обнаружения систем позиционирования и ориентации, чтобы гарантировать, что данные средства могут поддерживать безопасный режим работы в случае отказа или износа одного из средств позиционирования/распознавания.

В приложениях, где цифровая карта местности используется для поддержания безопасных условий эксплуатации и отображения РВАЗДСМ, состояние системы позиционирования и ориентации должно контролироваться во время создания карты местности или обследования местности.

При составлении любого картографирования следует учитывать точность системы позиционирования и ориентации, чтобы гарантировать, что картографические данные должным образом взвешены во время создания и проверки цифровой карты местности.

6.5.17 Цифровая карта местности

В приложениях, где используется цифровая карта местности для поддержания безопасных условий эксплуатации, необходимо контролировать ее достоверность.

РВАЗДСМ должны поддерживать безопасное состояние в случае недостаточной точности цифровой карты местности. Сбои и ухудшения качества могут включать следующие причины:

- потерю или ухудшение точности цифровой карты местности из-за погодных условий на дороге (туман, дождь, снег, смог) или стройплощадке, изменения состояния дорог или других работ на стройплощадке;
- цифровая карта местности не была должным образом откалибрована или выровнена с учетом существующей местности;
- загружаемая или активная версия цифровой карты местности в РВАЗДСМ является устаревшей.

Примечание — РВАЗДСМ могут быть не в состоянии реагировать на внезапные изменения рельефа местности.

В приложениях, где используется цифровая карта местности для поддержания безопасных условий эксплуатации и отображается РВАЗДСМ, состояние системы позиционирования должно контролироваться во время создания карты или обследования местности.

При составлении любого картографирования следует учитывать точность системы позиционирования, чтобы гарантировать, что картографические данные рассчитаны верно во время создания и проверки цифровой карты местности.

6.5.18 Навигационная система

Навигационная система РВАЗДСМ может использовать либо абсолютное, либо относительное положение РВАЗДСМ для навигации по заранее заданному или динамически определяемому маршруту для достижения целей РВАЗДСМ. Системные требования будут зависеть от приложения и оценки рисков. Точность навигации также может зависеть от таких факторов, как скорость машины и ее местоположение.

6.5.18.1 Риски

Риски, связанные с навигацией РВАЗДСМ, включают столкновения с другими машинами, инфраструктурой и людьми в автономной рабочей зоне или повреждение РВАЗДСМ. Это может быть результатом неточной информации о местоположении, несовместимых систем координат, неточного управления навигацией, плохого планирования или неточной цифровой карты местности.

6.5.18.2 Требования

РВАЗДСМ должны поддерживать безопасный курс и скорость движения при эксплуатации в соответствии с их заданной рабочей средой и условиями.

При работе в пределах заданной среды навигационная система РВАЗДСМ должна иметь средства для обнаружения того, что она не соответствует заданным требованиям РВАЗДСМ и окружающей среде.

Если состояние системы недостаточное для обеспечения требуемой точности (это может быть динамическим требованием в зависимости от состояния РВАЗДСМ), РВАЗДСМ должны предпринять действия для поддержания безопасного режима работы.

Оператор должен быть уведомлен о любых ошибках в навигационной системе, которые могут привести к неприемлемому риску, определяемому оценкой риска.

Все пути или участки, используемые РВАЗДСМ, должны быть проверены для обеспечения их безопасного прохождения при всех разумно ожидаемых условиях эксплуатации. Валидация может быть завершена либо РВАЗДСМ, либо компетентным лицом.

6.5.19 Планировщик задач

Функции планировщиков задач, используемых в РВАЗДСМ, значительно различаются в зависимости от типа машины и ее применения. В этом подразделе определяются риски и излагаются общие требования к специалистам по планированию задач.

6.5.19.1 Риски

Планировщик может направить РВАЗДСМ куда-то, куда ему не следует, например пересекать несуществующий или опасный путь.

Планировщик может направить РВАЗДСМ куда-то, что может привести к опасным последствиям, таким как извлечение материала из хранилища или пункта выгрузки способом, создающим внезапный или непредвиденный поток материала, извлечение материала способом, который подрезает материал под другими машинами или конструкциями, или сброс материала способом, который создает опасность для других машин или персонала (например, экскаватор-драглайн, предназначенный для сброса материала поверх соседних машин).

6.5.19.2 Требования

Планировщик задач должен избегать направления РВАЗДСМ по заведомо опасному маршруту. Уровень опасности пути может определяться либо РВАЗДСМ, либо оператором. Если РВАЗДСМ несут ответственность за определение опасностей, связанных с маршрутом, то РВАЗДСМ должны самостоятельно определить все ожидаемые опасности и иметь средства для информирования планировщика задач об обнаруженных опасностях.

Планировщик задач не должен направлять РВАЗДСМ на создание опасных условий (например, извлечение материала из хранилища способом, который вызывает неожиданный поток материала, сброс материала способом, который создает опасность для других машин).

6.6 Уровень автоматизации 5

6.6.1 Роль оператора и АСУ

Локальный оператор проводит проверку эксплуатационной готовности РВАЗДСМ непосредственно перед его работой. Оператор имеет возможность контролировать процесс выполнения задания РВАЗДСМ, находясь в кабине машины в качестве пассажира или удаленно, используя дистанционный пульт управления или приложение, устанавливаемое на мобильный телефон. В течение дорожно-строительного процесса вмешательство оператора в работу РВАЗДСМ не требуется. АПК выполняет задание самостоятельно. РВАЗДСМ проводят работы и мониторинг технического состояния автономно. АСУ РВАЗДСМ самостоятельно выбирает параметры работы для выполнения задания в течение всего дорожно-строительного процесса. Оператор контролирует техническое состояние и работу РВАЗДСМ удаленно из диспетчерского пункта.

6.6.2 Принципы защиты

Необходимые требования для РВАЗДСМ УА-5 вследствие их тяжелых условий работы для обеспечения соответствующего уровня безопасности:

- для системы основного доступа к операторскому посту должно быть предусмотрено освещение, если платформа операторского поста находится на высоте более 3 м. Включение огней должно быть возможно с земли и поста оператора;
- все РВАЗДСМ должны иметь бортовые средства управления (кнопки, джойстики и т. д.) для их остановки;

- при работе РВАЗДСМ в заданных условиях эксплуатации АСУ должна обеспечивать торможение машины при сохранении безопасной работы (например, торможение в неблагоприятных условиях);
- в РВАЗДСМ должны быть предусмотрены системы управления, обеспечивающие достижения безопасных рабочих температур и давлений в тормозной и рулевой системах (например, колесный погрузчик), а также в системах управления направлением движения (например, бульдозер) до запуска РВАЗДСМ в автономном режиме;
- РВАЗДСМ должны быть оснащены системой распознавания, позволяющей обнаруживать и определять местоположение людей или прочих препятствий относительно РВАЗДСМ;
- РВАЗДСМ должны быть оснащены системой распознавания, позволяющей определять положение и ориентацию РВАЗДСМ так, как это требуется для соответствующих операций, а также предотвращать непреднамеренные перемещения за пределы рабочей зоны;
- перед каждым перемещением РВАЗДСМ система безопасности должна обеспечить (подтвердить) отсутствие препятствий в опасной зоне;
- при выполнении высокоавтоматизированных операций в случае обнаружения или попадания в опасную зону препятствия, РВАЗДСМ должны подать звуковой или визуальный предупредительный сигнал и перейти в заданное безопасное состояние;
- РВАЗДСМ должны быть оснащены средствами, позволяющими локальному или удаленному оператору останавливать или запускать высокоавтоматизированную работу;
- РВАЗДСМ должны позволять осуществление соответствующего контроля локальным или удаленным оператором.

6.6.3 Коммуникации и сети

Во время всего рабочего процесса РВАЗДСМ осуществляют постоянный мониторинг и подтверждение наличия связи между системой дистанционного управления и РВАЗДСМ.

При рассмотрении пропускной способности будут учитываться требования к вспомогательным машинам и взаимодействию с оператором. Важной эксплуатационной проблемой является необходимость быть осведомленным о зонах с потенциально высоким уровнем помех (например, местах расположения очередей).

6.6.3.1 Виды рисков и отказов

а) Риски

Сбои в работе связи и сети могут привести к следующим рискам для безопасности:
- невозможности дистанционно остановить машину или к аварийной ситуации;
- отсутствию доступа к информации о ситуации;
- неточным данным о местности;
- потере или задержке ввода команд;
- недостаточному контролю на перекрестке;
- потере координации машины;
- потере устаревшей информации;
- утерянной или задержанной информации об опасности;
- неточному местоположению (из-за потери коррекции ГНСС);
- неточной информации о планировании;
- неточному отслеживанию персонала;
- потере возможности дистанционного включения системы противопожарной защиты.

б) Режимы отказа

Режимы сбоев, связанных со связью, включают:
- потерю связи;
- ухудшение качества связи, включая потерю одного направления;
- задержку связи;
- неверно направленную связь;
- измененную связь;
- связь с нарушением последовательности.

в) Потенциальные причины

Режимы сбоя могут быть результатом любой из следующих причин:
- проблемы с шумом (непреднамеренные помехи);
- физические изменения в сети;
- изменения конфигурации сети;
- проблемы с оборудованием;

- экологические проблемы (например, связанные с погодой, солнечными пятнами);
- изменения топологии;
- проблемы с питанием;
- преднамеренный взлом или подмена;
- преднамеренное заклинивание.

6.6.3.2 Требования к системам связи

РВАЗДСМ должны поддерживать безопасный режим работы в случае любого сбоя, связанного со связью. Где оценка риска показывает необходимость, РВАЗДСМ должны иметь безотказные средства (например, с помощью активного мониторинга, нескольких независимых каналов связи) для удаленной остановки и поддержания безопасного состояния.

Там, где этого требует оценка риска, РВАЗДСМ должны иметь средства обнаружения потери связи, ухудшения качества связи или повреждения коммуникаций. Машины должны иметь средства приведения в действие регулируемой остановки, а также должны поддерживать безопасное состояние в случае потери, повреждения или задержки связи. Скорость работы устройства и текущие условия эксплуатации следует использовать в сочетании с оценкой риска для определения максимально допустимой продолжительности потери связи или ухудшения качества связи.

Должны быть предусмотрены средства для предотвращения несанкционированного контроля и подмены или саботажа РВАЗДСМ.

Приемлемость таких средств должна быть определена на основе оценки риска. Подходящие средства включают ограничение физического доступа, аутентификацию, использование брандмауэра, шифрование данных и ограничение внешнего подключения за пределами сайта.

6.6.4 Включение/отключение РВАЗДСМ

Средство включения/отключения АСУ должно быть на каждой РВАЗДСМ.

Средство включения/отключения АСУ обязано быть:

- идентифицируемым;
- доступным для локального оператора;
- установленным в кабине, снаружи РВАЗДСМ и на станции удаленного оператора, защищенным от непреднамеренного приведения в действие.

Индикация состояний АСУ должна быть однозначной (четкой) и легко опознаваемой (идентифицируемой).

Доступные состояния управления должны включать в себя:

- отключенное состояние АСУ;
- включенное состояние АСУ.

Примечание — В отключенном состоянии все подсистемы АСУ должны быть остановлены и отключены. Возможность запускать работу АСУ осуществляет только локальный оператор.

В отключенном состоянии все высокоавтоматизированные операции РВАЗДСМ должны быть остановлены и отключены. Во включенном состоянии выполнение высокоавтоматизированных операций должно быть разрешено.

Должна быть предусмотрена возможность отключения высокоавтоматизированной работы в любое время либо на позиции локального оператора, либо при удаленном контроле — на позиции удаленного управления.

Запуск РВАЗДСМ в режиме высокоавтоматизированной работы осуществляется автоматически.

Высокоавтоматизированная работа РВАЗДСМ осуществляется до моментов:

- отключения системы управления оператором;
- обнаружения препятствия, создающего опасность;
- возникновения неисправного состояния АСУ или ИМ.

6.6.5 Проверка эксплуатационной опасности

Возможность запуска высокоавтоматизированной работы без подтверждения системой распознавания отсутствия препятствий в опасной зоне должна быть исключена. Запуск высокоавтоматизированной работы должен запрашивать разрешение оператора РВАЗДСМ, кроме тех случаев, когда оценка рисков показывает отсутствие рисков потери безопасности.

В случае прекращения высокоавтоматизированной работы (независимо от причины) для процедуры повторной активации высокоавтоматизированного режима должен требоваться запуск АСУ оператором РВАЗДСМ.

Должен осуществляться постоянный мониторинг опасной зоны вокруг РВАЗДСМ с целью обнаружения препятствий при работающем двигателе во время высокоавтоматизированной работы.

6.6.6 Управление двигателем

6.6.6.1 Запуск двигателя

РВАЗДСМ должны производить запуск двигателя исключительно в ответ на запрос локального оператора о запуске двигателя.

Перед запуском (прокруткой) двигателя должен быть подан звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и запуском двигателя (предстартовое предупреждение), длительность предупреждения после запуска двигателя должны быть достаточными для предотвращения опасностей с учетом характеристик РВАЗДСМ.

Запуск двигателя допускается исключительно после истечения периода предстартового предупреждения.

Локальный оператор должен выключить двигатель при попадании препятствия в опасную зону вокруг РВАЗДСМ в течение периода предупреждения или во время запуска двигателя.

В случае остановки запуска двигателя на более чем 1 с процесс предупреждения о запуске двигателя должен быть запущен заново.

При использовании нескольких двигателей точную последовательность предупредительных сигналов дополнительных двигателей после пуска первого двигателя определяет локальный оператор после оценки степени опасностей.

6.6.6.2 Остановка работы двигателя

АСУ РВАЗДСМ должна выключить двигатель при получении запроса от оператора на остановку двигателя.

При повторном запуске двигателя АСУ должна послать запрос локальному оператору на подтверждение пуска.

6.6.6.3 Неисправность (отказ) двигателя

В случае неисправности (отказа) двигателя, препятствующей безопасной эксплуатации РВАЗДСМ в соответствии с проектной спецификацией, РВАЗДСМ должны перейти в заданное безопасное состояние, а АСУ РВАЗДСМ должна быть отключена автоматически до устранения неисправности.

6.6.6.4 Автоматический контроль состояния двигателей РВАЗДСМ

Должен быть обеспечен постоянный автоматический контроль состояния двигателя с информированием оператора о его состоянии.

Для обеспечения безопасной работы необходимо постоянное подтверждение связи с АСУ в соответствии с проектной документацией. В случае потери связи РВАЗДСМ должны оповестить оператора и перейти в заданное безопасное состояние.

6.6.7 Автоматизированное управление двигателем

Автоматизированное управление двигателем допускается только при активизации АСУ. Системы управления двигателем должны обеспечить номинальные режимы траектории и скорости РВАЗДСМ при непосредственном контроле оператором.

Опасная зона вокруг РВАЗДСМ должна сканироваться с целью обнаружения препятствий в течение всего предстартового периода и времени работы.

6.6.8 Начало движения

РВАЗДСМ должны начинать движение исключительно при подтверждении оператором запроса об активации двигателя и отсутствий препятствий в зоне перемещения.

Активация двигателей допускается исключительно после истечения предстартового периода предупреждения и не должна приводить к возникновению опасной ситуации (см. ГОСТ Р 70850).

До начала движения подается звуковой предупредительный сигнал, который должен оставаться активным в течение всего периода предупреждения. Задержка между подачей звукового предупреждения и движением и продолжительность предупреждения после активации двигателей должны быть достаточными для предотвращения соответствующих опасностей с учетом технических характеристик РВАЗДСМ.

Движение РВАЗДСМ допускается исключительно после истечения предстартового периода предупреждения.

Оператор должен прервать запуск движения при попадании РВАЗДСМ в опасную зону в течение периода предупреждения.

Если движение затрудняется по причине отсутствия связи, система должна перейти в заданное безопасное состояние, а удаленный оператор должен быть оповещен автоматически.

6.6.9 Остановка движения

Локальный оператор должен остановить движение при попадании в опасную зону. РВАЗДСМ должны останавливать движение в ответ на запрос, полученный от оператора. Отсутствие препятствий в опасной зоне должно постоянно подтверждаться при движении РВАЗДСМ в режиме высокоавтоматизированной работы (см. ГОСТ Р 70852).

Если во время работы в АСУ возникнет неисправность, РВАЗДСМ должны автоматически остановить движение, не создавая опасной ситуации, а АСУ должна быть отключена до устранения неисправности.

В случае, если движение РВАЗДСМ затрудняется (например, при обнаружении препятствия), РВАЗДСМ должны перейти в заданное безопасное состояние. Дальнейшее движение должно осуществляться по команде оператора.

6.6.10 Блокировка АСУ

Блокировка АСУ РВАЗДСМ, включая возобновление (перезапуск) режима помощи, не должна создавать опасных ситуаций.

Намеренная активация органов управления, предусмотренных на бортовой рабочей станции оператора, дистанционном пульте управления или на станции удаленного оператора для управления функциями движения [например, контроль направления, торможение, остановка (отключение) рабочих органов], должна блокировать высокоавтоматизированную работу. Такая блокировка автоматического управления, включая возобновление (перезапуск) высокоавтоматизированной работы, не должна создавать опасных ситуаций.

Руководство для оператора РВАЗДСМ должно описывать, как перевести управление РВАЗДСМ с высокоавтоматизированной работы на управление оператором и с управления оператором на высокоавтоматизированную работу.

Должны быть предусмотрены доступные локальному оператору средства [такие, как клавишные (кнопочные) переключатели, пароли или подобные средства] для возобновления работы АСУ, автоматическое управление которой было заблокировано, и для дальнейшей передачи управления оператору.

Если ни один подобный пользовательский интерфейс не применим, функция должна быть переведена в заданное безопасное состояние до момента, когда высокоавтоматизированная работа не будет возобновлена, а оператор уведомлен автоматически о блокировке АСУ.

6.6.11 Удаленная остановка высокоавтоматизированной работы

Когда оценка риска показывает необходимость, РВАЗДСМ должны быть оснащены системой удаленной остановки. Механизм остановки высокоавтоматизированной работы должен быть легкодоступным для оператора на всех позициях управления.

После остановки машины должно потребоваться вмешательство оператора для возобновления движения машины.

Для оператора РВАЗДСМ, не требующего бортовой станции или удаленной станции оператора, должен быть предусмотрен дистанционный пульт управления.

6.6.12 Подсистема распознавания

Подсистема распознавания содержит датчики восприятия, используемые для сбора информации об окружении РВАЗДСМ и последующей передачи информации алгоритмам обнаружения, локализации и распознавания (классификация) потенциального объекта, представляющего интерес. Целью системы машинного восприятия является предоставление информации, необходимой для безопасного управления РВАЗДСМ, без необходимости взаимодействия с оператором.

Если для обеспечения того, чтобы подсистема распознавания работала в соответствии с системными требованиями, требуется возможность тестирования и калибровки, интегратор РВАЗДСМ должен предоставить такую возможность.

6.6.12.1 Виды рисков и отказов

а) Неспособность обнаружить объект или несвоевременное обнаружение объекта

Примерами неспособности обнаружить препятствие или позднего обнаружения объекта являются:

- объекты, скрытые из-за пыли, тумана, снега, дождя или других затемняющих факторов;
- результаты восприятия, которые становятся ненадежными из-за плохого освещения;
- препятствия, которые скрыты из-за наклона РВАЗДСМ;

- неровный грунт, приводящий к изменению плоскости сканирования; например, лазерный луч может попадать на землю или указывать в небо, когда машина наклоняется вниз или вверх;
- вибрация или движение машины, приводящие к смещению датчиков;
- объекты, движущиеся слишком быстро, чтобы их можно было обнаружить;
- слишком маленькие объекты;
- объекты, не отражающиеся обратно в направлении приемника; например, способность радиолокационной технологии идентифицировать объект может зависеть от эффективного поперечного сечения радара объекта;
- прозрачные или темные объекты, не отражающие лазерный луч;
- не обнаруживающиеся отрицательные объекты (дыры в рельефе);
- увеличение задержки из-за других приложений или вычислительной нагрузки на процессор, используемый для подсистемы распознавания или классификации объектов.

б) Ложное обнаружение несуществующего объекта

Примерами ложного обнаружения являются:

- пыль или другие затемняющие вещества, которые отражают достаточно энергии, чтобы быть классифицированными как объект;
- материал на передатчике или приемнике, который ошибочно распознан как объект.

в) Ошибочное местоположение обнаруженного объекта

Примерами ошибочного местоположения являются:

- смещение датчика, приводящее к неточной оценке положения;
- системные ошибки, приводящие к неточному положению или ориентации машины;
- вибрация крепления датчика, вызывающая движение датчика, которое не учитывается системой восприятия;
- пыль или затемняющие вещества, размывающие края.

6.6.12.2 Неправильная классификация объекта

Примерами неправильной классификации объекта являются:

- пыль или затемняющие вещества, размывающие края;
- неадекватное обучение или валидация классификатора.

6.6.12.3 Требования

Системные требования к бортовой системе РВАЗДСМ или подсистеме распознавания РВАЗДСМ должны основываться на оценке риска, характеристиках машины (например, скорость, видимость, нормальная работа) и местности эксплуатации (например, поверхность, подземелье, открытая местность, туннель).

Подсистема распознавания должна поддерживать безопасное состояние РВАЗДСМ во время любого взаимодействия с предполагаемой рабочей средой (например, рельефом местности, пылью, погодными условиями, условиями освещения).

Подсистема распознавания должна быть способна обнаруживать объекты в требуемой области (например, ожидаемая траектория движения), которые находятся либо на положительном, либо на отрицательном склоне, как требуется на основе оценки риска.

РВАЗДСМ должны быть способны обнаруживать, когда подсистема распознавания не функционирует в соответствии с минимальными требованиями, основанными на оценке риска, и поддерживать машины в безопасном состоянии.

При нефункционировании подсистемы необходимо уведомить оператора или систему контроля РВАЗДСМ.

При необходимости на основе оценки риска эксплуатационные пределы подсистемы распознавания в руководстве пользователя должны быть указаны, например, размер мишени, форма и отражательная способность, дальность восприятия, угловой охват.

6.6.12.4 Поведение системы распознавания в исправном состоянии

Система должна функционировать надлежащим образом в условиях и при ограничениях, предусмотренных для эксплуатации, включая предусмотренное ненадлежащее использование. Ограничения системы распознавания должны быть описаны в руководстве оператора.

Ограничения могут быть вызваны: несоответствующими условиями окружающей среды, такими как солнечное излучение, темнота, туман, температура, все типы атмосферных осадков и условий, особенности местности и участки, поросшие травой и кустарником; несоответствующими параметрами, связанными с препятствиями (например, слишком малые размеры, слишком высокая скорость передвижения препятствий или низкая отражающая способность); несоответствующими параметрами, свя-

занными с неисправностями или сбоями в работе РВАЗДСМ по таким причинам, как смещение датчика/датчиков, слишком высокая скорость работы, загрязнение на датчике, слишком сильные вибрации или слишком большая загрузка процессора вычислениями.

Если с удаленным оператором (при автономной работе) уровень достоверности датчиков системы распознавания опускается ниже минимального порога работоспособности, требуемого для безопасной эксплуатации, РВАЗДСМ должны перейти в безопасное состояние. Система диагностики РВАЗДСМ должна указать и зафиксировать причину, по которой было запущено безопасное состояние. Для РВАЗДСМ с оператором на борту запуск безопасного состояния может быть заменен звуковым предупреждением, если оценка рисков допускает, что этого достаточно.

6.6.13 Контроль неисправностей

Неисправности, вызванные проблемами надежности (в результате отказа оборудования в системе), и сбой, вызванный несоответствием техническому заданию или программному обеспечению (например, система не функционирует должным образом в исправном состоянии при различных параметрах окружающей среды), не должны создавать опасных условий.

Контроль неисправностей и рабочие характеристики должны проверяться путем испытаний ПС распознавания на испытательном полигоне по методикам, приведенным в приложении А.

Все неисправные состояния систем распознавания и определения местонахождения/ориентирования РВАЗДСМ должны быть идентифицированы. Требуемый уровень эффективности и уровень полноты безопасности должны быть определены с учетом всех предусмотренных неисправных состояний, угроз, возникающих при использовании РВАЗДСМ в неисправном состоянии, прогнозируемой серьезности ущерба и вероятности нанесения ущерба, принимая во внимание вероятное присутствие сторонних наблюдателей и возможности сторонних наблюдателей избежать опасности. При обнаружении остаточного опасного неисправного состояния РВАЗДСМ должны перейти в заданное безопасное состояние.

6.6.14 Управление с помощью удаленного оператора

Управление с помощью удаленного оператора должно позволять непрямой визуальный мониторинг (например, с помощью камеры) зоны вокруг РВАЗДСМ, если того требует оценка рисков.

Все предупреждения, требуемые для локального оператора, должны подаваться на станции управления удаленного оператора. Удаленный оператор должен иметь возможность вмешиваться (действовать) со станции удаленного управления для отключения высокоавтоматизированной работы.

6.6.15 Адаптация к условиям окружающей среды

Основываясь на оценке риска, РВАЗДСМ должны быть способны адаптироваться к условиям окружающей среды до тех пор, пока любые изменения в условиях окружающей среды находятся в пределах установленных ограничений. РВАЗДСМ УА-5 могут включать использование людей-операторов или автоматизированных систем для регулировки скорости, отключения операций, перекрытия зон или других регулировок, необходимых для поддержания безопасной эксплуатации.

6.6.16 Бортовая электрическая мощность

РВАЗДСМ должны реагировать на сбои в работе электропитания, в том числе на потерю питания всех контроллеров, которые влияют на движение машины.

Источник электропитания должен обеспечивать подачу питания на системы машины для достижения остановленного состояния и поддержания безопасного состояния.

РВАЗДСМ должны иметь достаточный источник электроэнергии во время работы в автономном режиме, включая:

- достаточный запас заряда батареи для предполагаемых условий окружающей среды;
- достаточную мощность генератора переменного тока для дополнительной электроники, связанной с дистанционным управлением;
- проводку достаточных размеров для увеличения токоведущей способности.

Аккумуляторы РВАЗДСМ должны иметь достаточные емкости для обслуживания всей электроники машины при отключенном двигателе или генераторе, для поддержания безопасного состояния и завершения упорядоченного отключения машины при любых предполагаемых условиях окружающей среды.

При непреднамеренной потере электропитания машины во время работы РВАЗДСМ должны перейти в безопасное состояние.

РВАЗДСМ должны обладать достаточной электрической мощностью, чтобы выдерживать дополнительные нагрузки, требуемые автономной электроникой (в дополнение к общим требованиям к

машине) для всех предполагаемых условий эксплуатации и окружающей среды (например, низкий холостой ход или ночное время).

6.6.17 Позиционирование и ориентация РВАЗДСМ

6.6.17.1 Система позиционирования и ориентации должна быть предусмотрена на всех РВАЗДСМ УА-5, способная при прогнозируемых условиях эксплуатации обнаруживать объекты, находящиеся в зоне распознавания.

Системы позиционирования и ориентации могут включать в себя широкий спектр технологий, включая ГНСС, датчики, лазерные сканеры, псевдолиты, теодолиты, радары, сопутствующие алгоритмы, необходимые для идентификации и классификации значимых объектов относительно РВАЗДСМ, а также системы беспроводной триангуляции, системы безопасного контроля для управления и системы технического зрения, не требующего вмешательства человека. Каждая из этих технологий может иметь уникальные характеристики. Требования также будут зависеть от приложения. Требуемая от таких систем точность позиционирования и ориентации или частота измерений также зависят от скорости и местоположения машины.

Режимы потенциального риска из-за неисправности или отказа:

- неточное абсолютное положение для систем, использующих глобальную систему координат;
- неточное относительное положение для систем, использующих локальную систему координат;
- неточная ориентация;
- неточная регистрация в цифровой модели местности;
- несуществующее положение, ориентация или регистрация.

6.6.17.2 Требования

Аналогичные системы позиционирования и ориентации должны иметь средства для определения состояния системы, например вероятности ошибки измерения, точности, разрешающей способности.

Когда состояние системы позиционирования и ориентации недостаточное для позиционирования с требуемой точностью, которая может динамически изменяться в зависимости от состояния РВАЗДСМ, РВАЗДСМ должны поддерживать безопасный режим работы.

РВАЗДСМ должны содержать достаточно независимых средств обнаружения систем позиционирования и ориентации, чтобы гарантировать, что данные средства могут поддерживать безопасный режим работы в случае отказа или износа одного из средств позиционирования/распознавания.

В приложениях, где цифровая карта местности используется для поддержания безопасных условий эксплуатации и отображения РВАЗДСМ, состояние системы позиционирования и ориентации должно контролироваться во время создания карты местности или обследования местности.

При составлении любого картографирования следует учитывать точность системы позиционирования и ориентации, чтобы гарантировать, что картографические данные должным образом взвешены во время создания и проверки цифровой карты местности.

6.6.18 Цифровая карта местности

В приложениях, где используется цифровая карта местности для поддержания безопасных условий эксплуатации, необходимо контролировать ее достоверность.

РВАЗДСМ должны поддерживать безопасное состояние в случае недостаточной точности цифровой карты местности. Сбои и ухудшения качества могут включать:

- потерю или ухудшение точности цифровой карты местности из-за погодных условий на дороге (туман, дождь, снег, смог) или стройплощадке, изменений состояния дорог или других работ на стройплощадке;
- цифровая карта местности не была должным образом откалибрована или выровнена с существующей местностью;
- загружаемая или активная версия цифровой карты местности в РВАЗДСМ является устаревшей.

Примечание — РВАЗДСМ могут быть не в состоянии реагировать на внезапные изменения рельефа местности.

В приложениях, где используется цифровая карта местности для поддержания безопасных условий эксплуатации и отображается РВАЗДСМ, состояние системы позиционирования должно контролироваться во время создания карты или обследования местности.

При составлении любого картографирования следует учитывать точность системы позиционирования, чтобы гарантировать, что картографические данные рассчитаны верно во время создания и проверки цифровой карты местности.

6.6.19 Навигационная система

6.6.19.1 Навигационная система РВАЗДСМ может использовать либо абсолютное, либо относительное положение РВАЗДСМ для навигации по заранее заданному или динамически определяемому маршруту для достижения целей РВАЗДСМ. Системные требования будут зависеть от приложения и оценки рисков. Точность навигации также может зависеть от таких факторов, как скорость машины и ее местоположение.

6.6.19.2 Риски

Риски, связанные с навигацией РВАЗДСМ, включают столкновения с другими машинами, инфраструктурой и людьми в автономной рабочей зоне или повреждение РВАЗДСМ. Это может быть результатом неточной информации о местоположении, несовместимых систем координат, неточного управления навигацией, плохого планирования или неточной цифровой карты местности.

6.6.19.3 Требования

РВАЗДСМ должны поддерживать безопасный курс и скорость движения при эксплуатации в соответствии с их заданной рабочей средой и условиями.

При работе в пределах заданной среды навигационная система РВАЗДСМ должна иметь средства для обнаружения того, что она не соответствует заданным требованиям РВАЗДСМ и окружающей среде.

Если состояние системы недостаточное для обеспечения требуемой точности (это может быть динамическим требованием в зависимости от состояния РВАЗДСМ), РВАЗДСМ должны предпринять действия для поддержания безопасного режима работы.

Оператор должен быть уведомлен о любых ошибках в навигационной системе, которые могут привести к неприемлемому риску, определяемому оценкой риска.

Все пути или участки, используемые РВАЗДСМ, должны быть проверены для обеспечения их безопасного прохождения при всех разумно ожидаемых условиях эксплуатации. Валидация может быть завершена либо РВАЗДСМ, либо компетентным лицом.

6.6.20 Планировщик задач

Функции планировщиков задач, используемых в РВАЗДСМ, значительно различаются в зависимости от типа машины и ее применения. В этом подразделе определяются риски и излагаются общие требования к специалистам по планированию задач.

6.6.20.1 Риски

Планировщик может направить РВАЗДСМ куда-то, куда ему не следует, например, пересекать несуществующий или опасный путь.

Планировщик может направить РВАЗДСМ куда-то, что может привести к опасным последствиям, таким как извлечение материала из хранилища или пункта выгрузки способом, создающим внезапный или непредвиденный поток материала, извлечение материала способом, который подрезает материал под другими машинами или конструкциями, или сброс материала способом, который создает опасность для других машин или персонала, например экскаватор-драглайн, предназначенный для сброса материала поверх соседних машин.

6.6.20.2 Требования

Планировщик задач должен избегать направления РВАЗДСМ по заведомо опасному маршруту. Уровень опасности пути может определяться либо РВАЗДСМ, либо оператором. Если РВАЗДСМ несут ответственность за определение опасностей, связанных с маршрутом, то РВАЗДСМ должны самостоятельно определить все ожидаемые опасности и иметь средства для информирования планировщика задач об обнаруженных опасностях.

Планировщик задач не должен направлять РВАЗДСМ на создание опасных условий (например, извлечение материала из хранилища способом, который вызывает неожиданный поток материала, сброс материала способом, который создает опасность для других машин).

7 Заключение об уровне полноты безопасности РВАЗДСМ

После сбора информации об отказах и неисправностях, наступивших в ходе проведения испытаний ПО АСУ и ИМ РВАЗДСМ всех УА, проводится анализ риска (risk analysis), который включает изучение технических характеристик РВАЗДСМ в части ограничений, идентификации опасности и предварительной оценки степени риска, составления заключения об уровне полноты безопасности РВАЗДСМ путем оценки степени риска (risk evaluation) [сделанное на основе анализа риска заключение о дальнейшей его эксплуатации или возможности снижения уровня риска (adequate risk reduction)

при определении степени адекватности его снижения]. На основании проделанных работ составляется заключение о безопасности эксплуатации РВАЗДСМ или предписание о проведении дополнительных конструкторских работ. Собственник определяет допущение снижения степени риска путем проведения конструктивных изменений, в соответствии с требованиями действующего законодательства, с учетом оправданного вложения средств.

8 Условия испытаний

8.1 РВАЗДСМ должны выполнять заданные операции выполнения задания, которые тестируются на испытательном полигоне с применением методов испытаний работоспособности КО РВАЗДСМ в соответствии с приложением А при определении соответствия обеспечения уровня полноты безопасности в пределах его конструктивной составляющей, заложенной в КД, нормативных документах.

Самоходные дорожно-строительные и землеройные машины с высокой степенью автоматизации управления должны отвечать требованиям безопасности согласно ГОСТ Р 12.2.011, ГОСТ Р ИСО 20474, ГОСТ ISO 12100.

При необходимости проводят испытания на безотказность АПК РВАЗДСМ, в том числе с прицепными агрегатами.

Испытания РВАЗДСМ по безотказности АПК проводятся с учетом требований ГОСТ Р 27.607 на испытательном полигоне.

8.2 Общие принципы, применяемые при оценке риска и его снижения у РВАЗДСМ, которые состоят из мониторинга конструктивных ограничений РВАЗДСМ и (или) КО подсистем АСУ в процессе их использования по назначению: идентификация опасностей и связанных с ними опасных событий; определение степени риска для каждой идентифицированной опасности и опасного события; оценка степени риска и принятие решения о необходимости его снижения; принятие защитных мер по устранению опасности или уменьшению степени риска, связанного с этой опасностью.

Общие принципы, применяемые при решении задачи оценки риска и его снижения у РВАЗДСМ — в соответствии с ГОСТ Р ISO 12100.

8.3 Тестирование РВАЗДСМ следует проводить при целесообразности и эффективности применения имитаторов рисков, которыми являются испытательный полигон с предлагаемыми траекториями движения и макеты препятствий. Испытание с применением имитаторов (см. [3]) предполагается проводить с целью мониторинга процесса управления рисками, а именно в качестве анализа величины риска и принятия решений, направленных на снижение риска до пределов, соответствующих приемлемому уровню, заложенному в конструкции РВАЗДСМ.

8.4 В случае, если показания КО подсистемы обнаружения (расстояние от отбойников) вышли за предварительно заданные пределы или имеются расхождения в показаниях нескольких КО подсистемы обнаружения (измеряющих расстояние до внутреннего и внешнего отбойников), подсистема управления должна автоматически выполнить остановку, подав соответствующий сигнал на исполнительные механизмы, смонтированные на устройстве управления скоростью движения, и на педали сцепления.

8.5 Для обеспечения безопасности РВАЗДСМ должны быть оснащены клапанами отсечки подачи топлива, срабатывающими по данным КО, а также по сигналу оператора (переданному по радиоканалу).

8.6 Работоспособность и степень безопасности РВАЗДСМ проверяют при тестировании подсистем АСУ на обеспечение выполнения операций в зависимости от УА (1—5).

8.7 В процессе тестирования выявляют факты степени неработоспособности и возникновения опасных ситуаций АСУ РВАЗДСМ в соответствии с уровнями автоматизации УА 1—5.

8.8 Уровень автоматизации РВАЗДСМ определяется в зависимости от возможности выполнения функций задания (см. таблицу 2).

8.9 По окончании испытаний составляются матрицы риска с учетом идентификации потенциальных опасностей (см. приложение В) путем заключения об УПБ (см. приложение Б).

8.10 Из полученных данных с помощью составления дерева неисправностей, путем детального анализа совокупности событий/неисправностей в соответствии с ГОСТ Р 27.302 проводят выявление отклонений и их причин для каждого тестирования, которое, как правило, проводится по методикам «дерева неисправностей» (FTA), «дерева событий» (ETA) и «влияние человеческого фактора» (HRA).

8.11 Посредством мониторинга составляется заключение о степени безопасности РВАЗДСМ и безотказности конструкции, компонентов и подсистем или даются рекомендации по изменению конструкционных параметров в зависимости от уровня безотказности и степени безопасности.

Классификация типов и примеров опасностей — в соответствии с ГОСТ ISO 12100.

8.12 Мониторинг следует проводить путем анализа степени риска с помощью выявления типовых слоев защиты и средств снижения риска (см. рисунок 3).

При выявлении опасностей, возможных отклонений от выполнения задач процесса и их причин, исходных событий и потенциально опасных событий (инциденты) в используемых технических системах следует провести анализ опасностей самого процесса. Для этого могут быть использованы технологии качественного анализа с помощью:

- проведения анализа опасных ситуаций;
- составления контрольных листов;
- проведения анализа видов и последствий отказов;
- проведения анализа причин и последствий;
- проведения анализа гипотез («что произойдет, если»).

На основе полученных данных оценивается уровень полноты безопасности (см. приложение Б).

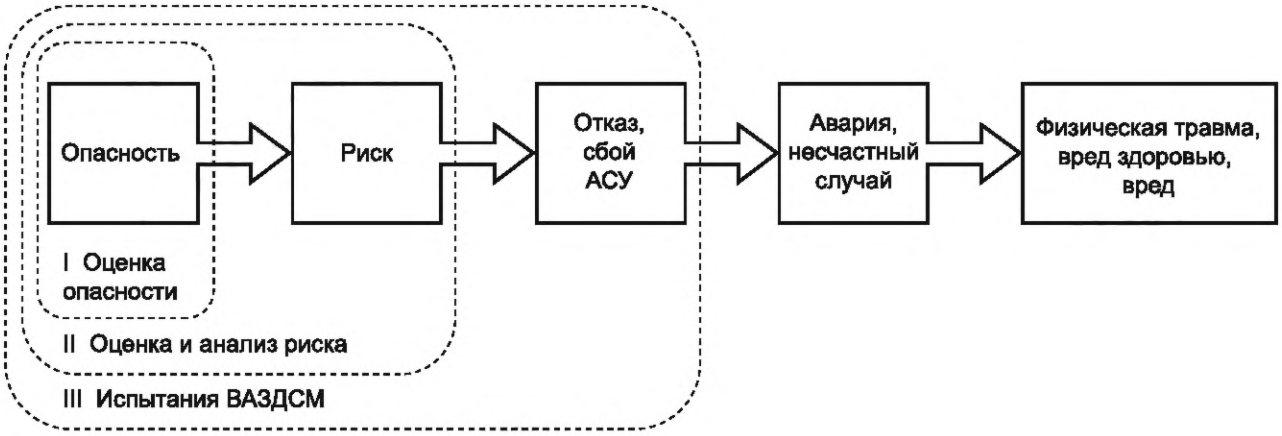


Рисунок 3 — Этапы мониторинга при определении УПБ РВАЗДСМ путем анализа степени риска

Приложение А
(обязательное)

Методы испытаний рассматриваемых высокоавтоматизированных землеройной и дорожно-строительной машин

А.1 Проверка функционирования РВАЗДСМ и работоспособности подсистем АСУ, входящих в состав РВАЗДСМ, проводится во время испытаний на соответствие нормативным требованиям технической документации РВАЗДСМ, ГОСТ ISO 15998 и ГОСТ Р 59898 (для подсистем АСУ с УА4 и УА5).

А.2 Условия эксплуатации системы автоматического управления

А.2.1 Спецификация полигона и оборудования

Испытания проводят на специальном огороженном испытательном полигоне, оборудованном для выполнения различных сценариев дорожно-строительного процесса, а именно:

- возведение насыпи;
- выемка грунта и расширение пространства выемки;
- засыпь каналов;
- перемещение и штабелирование сыпучих материалов и грунта;
- разработка грунта в каналах и канавах и пр.

А.2.2 Требование к сценариям испытаний

Из эксплуатационных испытаний РВАЗДСМ должна быть получена различная информация, которая имеет отношение к расчету показателей безопасности и качеству работы подсистем АСУ РВАЗДСМ. Испытания должны предоставлять данные об определенных условиях работы РВАЗДСМ, измеряемые датчиками, входящими в состав РВАЗДСМ.

Испытания РВАЗДСМ проводятся при следующих условиях эксплуатации (существенные факторы, влияющие на работу подсистем АСУ РВАЗДСМ):

- различные погодные условия (например, солнечно/пасмурно/облачно, дождь/туман/снег и пр.);
- различные виды ландшафта (например, скала, чернозем, щебень и др.);
- разметка дорожного полотна (для дорожных катков, фрез, асфальтоукладчиков) и/или грунта (для землеройных машин, погрузчиков и пр.) путем установки дорожных конусов и/или сигнальных лент;
- различные виды статических объектов (например, козловой кран, вагончик для рабочих, другая ВАЗДСМ в нерабочем состоянии, деревья, кустарники и т.д.);
- различные виды динамических объектов (например, рабочие, находящиеся на участке работы ВАЗДСМ, животные, другие РВАЗДСМ в рабочем состоянии и пр.).

Таким образом, объем информации сценариев испытаний должен быть достаточно обширным.

Сценарии дорожно-строительного процесса должны максимально отражать реальные ситуации технологического процесса.

Пределы рабочих скоростей при испытаниях РВАЗДСМ принимаются в соответствии с ЭЗ по специфике выполняемых работ для каждой из РВАЗДСМ, согласно таблице А.1.

Примечание — В случае, если показания КО подсистем обнаружения АСУ РВАЗДСМ (расстояние от препятствий) вышло за предварительно заданные пределы или имеется расхождение в показаниях разных КО, установленных на рассматриваемой РВАЗДСМ (измеряющих расстояние до внутреннего и внешнего препятствия) подсистема управления АСУ должна автоматически выполнить остановку, подав соответствующий сигнал на ИМ, смонтированные на устройстве управления скоростью движения и на педали сцепления в РВАЗДСМ АУ 1-3, или на диспетчерском пункте РВАЗДСМ АУ 4-5. Для обеспечения безопасности РВАЗДСМ должны быть оснащены клапанами отсечки подачи топлива, срабатывающими по данным системы обнаружения (независимых от работы подсистем системы управления), а также по сигналу удаленного оператора или в диспетчерский пункт.

А.2.3 Тестирование на управление по заданной траектории движения

При тестировании подсистем АСУ РВАЗДСМ с УА4 и УА5

Таблица А.1 — Пределы рабочих скоростей при дорожно-строительных работах

Вид работ	Скорость движения, км/ч
Бульдозер (максимальная скорость 11)	
Резание и перемещение грунта	2,3—6
Рыхление	1,8—2,1

Окончание таблицы А.1

Вид работ	Скорость движения, км/ч
Каток (максимальная скорость 9)	
Уплотнения насыпных и асфальтовых покрытий	2,63—8,6
Грейдер (максимальная скорость 38)	
Резание	До 2,5
Перемещение грунта	До 2,7
При отделочных проходах	До 3
Фронтальный погрузчик (максимальная скорость 34)	
Наполнение ковша грунтом	2,2—4

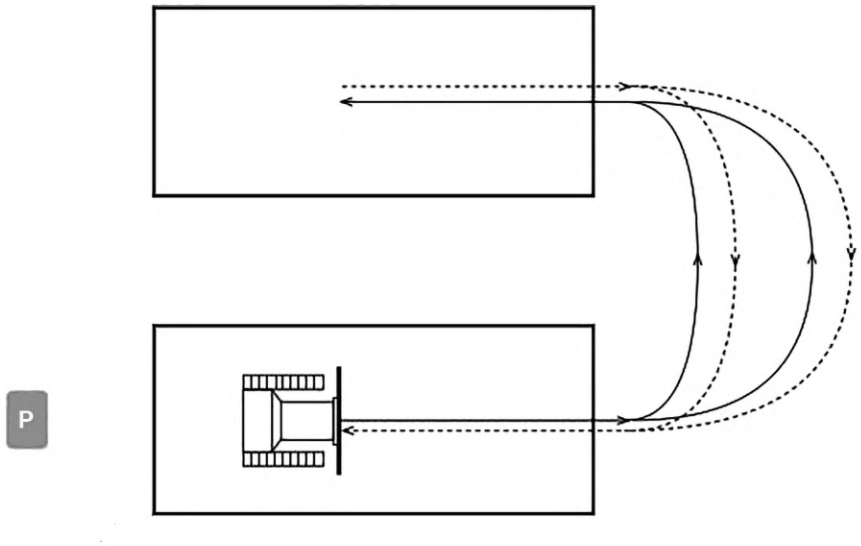
А.2.4 Тест на управляемость при имитации движения РВАЗДСМ по криволинейной траектории (перемещение грунта) (см. рисунок А.1)

Операции задания:

- движение с заданной точностью (при прямом и заднем ходе машины);
- прямолинейное движение (прямой и задний ход машины);
- авторазворот (прямым и задним ходом машины);
- автоматическая парковка;
- дистанционное управление скоростью.

Таблица А.2 — Минимальные размеры зоны движения РВАЗДСМ по криволинейной траектории

Название	Длина рабочей зоны, м	Ширина рабочей зоны, не менее, м	Длина зоны парковки, не менее, м	Длина зоны разворота, не менее, м
Зона криволинейного движения	20	16	5	8



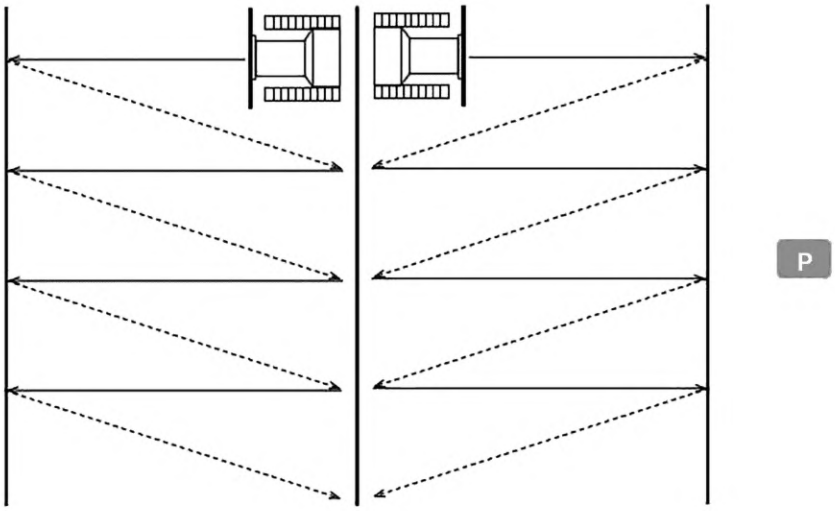
P — зона парковки

Рисунок А.1 — Схема работы РВАЗДСМ по кривой траектории

А.2.5 Тест на управляемость в групповом режиме по зигзагообразной схеме (выемка грунта и расширение пространства выемки) (см. рисунок А.2)

Операции задания:

- навигация с заданными параметрами точности для реализации параллельных проходок;
- прямолинейное движение с заданной точностью до назначенной точки;
- прямолинейное движение под углом к оси рабочего хода задним ходом;
- движение двух РВАЗДСМ.



P — зона парковки

Рисунок А.2 — Зона группового движения

Таблица А.3 — Минимальные размеры зоны группового движения

Название	Длина рабочей зоны, м	Ширина рабочей зоны, не менее, м	Длина зоны парковки, не менее, м
Зона зигзагообразного движения	32	20	4,5

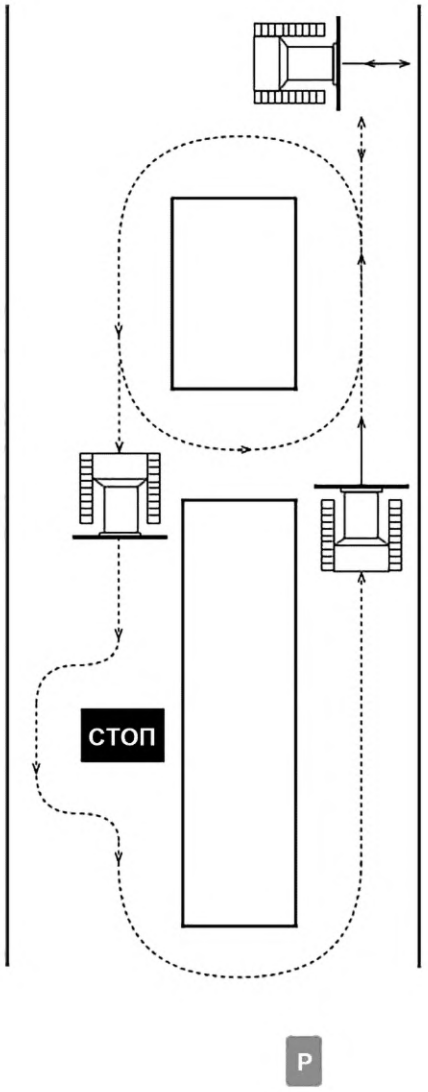
А.2.6 Тест систем управления в смешанном режиме (выемка грунта и расширение пространства выемки, перемещение грунта) (см. рисунок А.3)

Операции задания:

- групповая работа в смешанном парке;
- остановка перед препятствием;
- автоматический выбор скорости;
- объезд препятствия;
- авторазворот;
- контрвращение (для гусеничных РВАЗДСМ).

Таблица А.4 — Минимальные размеры зоны управления в смешанном режиме

Название	Длина рабочей зоны, м	Ширина рабочей зоны, не менее, м	Длина зоны парковки, не менее, м	Длина зоны разворота, не менее, м
Зона последовательно-кольцевого движения	90	34	16	12



P — зона парковки

Рисунок А.3 — Зона управления в смешанном режиме

А.2.7 Тест АСУ машины при объезде препятствия (см. рисунок А.4)

Примечание — Виды препятствий описаны в приложении Г (см. [3]), а также даны антропометрические размеры имитации препятствий.

Таблица А.5 — Минимальные размеры зоны объезда препятствий

Название	Длина рабочей зоны, не менее, м	Ширина рабочей зоны, не менее, м
Зона объезда препятствий	9	3

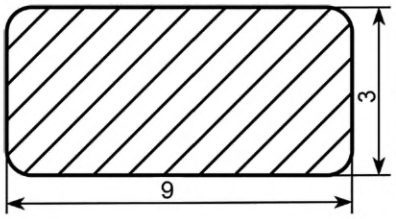


Рисунок А.4 — Зона объезда препятствий

Примечание — Метрические параметры предлагаемых форм искусственного полигона определены аналитическим путем, исходя из обеспечения безопасного коридора при проведении тестирования на выполнение задач безопасного управления РВАЗДСМ без агрегатирования прицепными машинами и агрегатами.

Приложение Б
(обязательное)

Метод определения уровня полноты безопасности рассматриваемых землеройной и дорожно-строительной машин — оценка риска

Б.1 Определение ограничений, налагаемых на РВАЗДСМ

Оценка риска начинается с определения ограничений, налагаемых на РВАЗДСМ. Это означает, что технические характеристики и эксплуатационные качества РВАЗДСМ или серии РВАЗДСМ в комплексном процессе, а также данные по обслуживающему персоналу, условиям эксплуатации и продукции, имеющие отношение к данному процессу, должны отражаться при составлении контрольных листов испытания.

Б.1.1 Эксплуатационные ограничения

Эксплуатационные ограничения распространяются как на использование РВАЗДСМ по назначению, так и на их прогнозируемое неправильное применение. Необходимо принимать во внимание следующие аспекты:

а) различные режимы работы РВАЗДСМ и разные процедуры вмешательства пользователя, в том числе и вмешательство, вызванное сбоем в работе;

б) арактер использования РВАЗДСМ;

в) предполагаемый уровень квалификации, опыта или способности пользователей, включая прогнозируемую возможность подверженности опасностям, связанным с данными РВАЗДСМ, других лиц, таких как:

- лиц, хорошо осведомленных об определенных опасностях;
- лиц, недостаточно осведомленных о специфических опасностях, но сведущих в технике безопасности, знающих дозволенные маршруты и т. д., например, административно-хозяйственных работников;
- лиц, очень мало осведомленных о специфических опасностях и технике безопасности, таких как представителей обычной публики, включая детей.

Б.1.2 Пространственные ограничения

Необходимо принимать во внимание вопросы пространственного ограничения, включая следующие:

а) диапазон перемещений РВАЗДСМ или их агрегатов;

б) пространственные требования для персонала, взаимодействующего с РВАЗДСМ как в процессе эксплуатации, так и при их техническом обслуживании;

в) взаимодействие человека с РВАЗДСМ (интерфейс «оператор-машина»);

г) алгоритм приведения в рабочее состояние.

Б.1.3 Временные ограничения

Необходимо принимать во внимание следующие аспекты временных ограничений:

а) предельный ресурс РВАЗДСМ и (или) некоторых их составляющих элементов (изнашиваемых частей, электромеханических и гидравлических компонентов) с учетом использования по назначению и прогнозируемого использования не по назначению (хранение, транспортировка);

б) рекомендуемый график технического обслуживания.

Необходимо принимать во внимание следующие аспекты прочих ограничений:

а) специфика дорожно-строительных работ;

б) уровень условий окружающей среды — рекомендуемые условия, для оптимальной работоспособности РВАЗДСМ (минимальную и максимальную температуру, пониженную и повышенную влажность, воздействие прямых солнечных лучей, пыли и т. п.).

Б.2 Идентификация опасностей

Б.2.1 После определения ограничений, налагаемых на РВАЗДСМ, следующим шагом в оценке риска, связанного с данным РВАЗДСМ, является идентификация прогнозируемых опасностей (постоянных опасностей, а также таких, которые могут возникнуть неожиданно), опасных ситуаций и (или) опасных случаев (см. таблица В.1).

Б.2.2 Предварительная оценка риска

После идентификации опасностей следует провести предварительную оценку риска для каждой опасной ситуации, определив элементы риска.

Б.2.3 Элементы риска

Риск, связанный с конкретной опасной ситуацией, выявляют в зависимости от следующих элементов:

а) серьезности возможного повреждения;

б) вероятности нанесения такого повреждения, которая, в свою очередь, является функцией:

- возможности лица (лиц) подвергнуться такой опасности;
- возникновения опасного случая;
- определяемой техническим или человеческим фактором возможности избежать повреждения или ограничить его последствия.

Элементы риска показаны на рисунке Б.1.



Рисунок Б.1 — Элементы риска

Таблица Б.1 — Идентификация опасностей

Категория	Тип	Примечание
Опасность	По квалификации	В соответствии с причиной его происхождения (например, механическая опасность, электрическая опасность)
		В соответствии с характером потенциального повреждения (например, опасность поражения электрическим током, удар, наезд и т. д.)
	По видам	Постоянно присутствующие в процессе использования РВАЗДСМ по назначению (например, опасное перемещение подвижных элементов, повышенный уровень шума, высокая температура, повышенная вибрация)
		Возникающие неожиданно (например, взрыв, опасность раздавливания вследствие неожиданного/непреднамеренного пуска, выбросы деталей вследствие аварии, падение вследствие ускорения или замедления)
	По характеру возникновения	Характерная опасность (relevant hazard): опасность, присущая РВАЗДСМ, неразрывно связанная с процессом ее эксплуатации
		Существенная опасность (significant hazard): опасность, которая определяется как характерная и требует от конструктора особых действий по устранению или снижению риска в соответствии с его оценкой
	По моменту возникновения	Опасный случай (hazardous event): неожиданный случай, который может стать причиной нанесения физической травмы или причинения вреда здоровью человека
		Опасная ситуация (hazardous situation): обстоятельства, при которых человек подвергается по меньшей мере одной или нескольким опасностям
	По месту	Опасная зона внутри РВАЗДСМ
		Опасная зона вокруг РВАЗДСМ
Риск	По характеру возникновения	Риск, вероятность нанесения и степени тяжести возможных травм или другого вреда здоровью
		Остаточный риск (residual risk): риск, остающийся после принятия защитных мер

Б.2.3.1 Серьезность причиняемого вреда здоровью

Предварительную оценку серьезности причиняемого вреда здоровью можно провести с учетом следующих факторов:

а) серьезности причиняемого вреда здоровью, например:

- легкий вред здоровью;
- тяжелый вред здоровью;
- летальный исход;

б) масштаба причинения вреда здоровью, например:

- одному человеку;
- нескольким лицам.

При проведении предварительной оценки риска необходимо рассматривать риск причинения наиболее вероятного и наиболее серьезного вреда здоровью для каждой идентифицированной опасности, а также учитывать прогнозируемое причинение наиболее серьезного вреда здоровью, даже если вероятность того, что оно произойдет, невысока.

Б.2.3.2 Вероятность причинения вреда здоровью

Б.2.3.2.1 Возможность лица (лиц) подвергнуться определенной опасности

Возможность лица (лиц) подвергнуться определенной опасности влияет на вероятность причинения вреда здоровью. В числе прочих для оценки такой возможности следует учитывать следующие факторы:

а) необходимость доступа в опасную зону (например, для нормальной работы, устранения неисправности, технического обслуживания или ремонта);

б) характер доступа (например, ручная подача материалов);

в) время, проводимое в опасной зоне;

г) число лиц, которым требуется доступ;

д) частоту доступа.

Б.2.3.3 Вероятность наступления опасного случая

Вероятность наступления опасного случая влияет на вероятность причинения вреда здоровью. В числе прочих для оценки вероятности наступления опасного случая следует учитывать следующие факторы:

а) данные по надежности и другие статистические данные;

б) статистику несчастных случаев;

в) статистику причинения вреда здоровью;

г) результаты сравнения рисков (см. 3.2).

Примечание — Наступление опасного случая может произойти по техническим причинам или из-за человеческого фактора.

Б.2.3.4 Возможность устранения или ограничения риска нанесения вреда здоровью

Возможность устранения или ограничения риска нанесения вреда здоровью влияет на вероятность такого результата. В числе прочих при оценке такой возможности следует учитывать следующие факторы:

а) категорию лиц, которые могут подвергаться опасности:

- квалифицированные;
- неквалифицированные;

б) скорость, с которой опасная ситуация может привести к причинению вреда здоровью:

- внезапно;
- быстро;
- медленно;

в) возможность распознавания риска:

- при помощи обычной информации, в частности, информации для пользователя;
- путем непосредственного наблюдения;
- при помощи предупреждающих сигналов и индикаторов, установленных, в частности, на РВАЗДСМ;

г) возможность человека избежать причинения вреда здоровью или ограничить риск (например, быстрота реакции, ловкость, возможность убежать);

д) практический опыт и уровень квалификации оператора:

- по данным РВАЗДСМ;
- по аналогичному РВАЗДСМ;
- не имеющий никакого опыта.

Б.2.4 Аспекты, которые следует учитывать для предварительной оценки риска

Б.2.4.1 Лица, подвергающиеся опасности

Предварительная оценка риска должна охватывать всех людей (операторов и других лиц), для которых существует вероятность подвергнуться рассматриваемой опасности.

Б.2.4.2 Тип, частота и продолжительность воздействия опасности

Б.2.4.2.1 Оценка воздействия конкретной опасности, включая долговременное расстройство здоровья, требует анализа, учитывающего все режимы работы РВАЗДСМ и способы обработки. В частности, этот анализ должен учитывать необходимость доступа к РВАЗДСМ во время установки, наладки, программирования, загрузки/выгрузки, корректировки или смены технологического процесса, чистки, обнаружения неисправностей и технического обслуживания.

Б.2.4.2.2 При предварительной оценке риска следует также принимать во внимание те работы, для выполнения которых требуется приостанавливать действие защитных мер.

Б.2.4.3 Соотношение воздействия опасности и ее последствий

Для каждой из рассматриваемых опасных ситуаций следует учитывать соотношение воздействия этой опасности и ее последствий. Необходимо также учитывать последствия от накапливаемых воздействий и совокупности опасностей. Если все эти воздействия учтены, предварительная оценка риска должна базироваться, насколько это возможно, на соответствующих общепризнанных данных.

Б.2.4.4 Человеческий фактор

Б.2.4.4.1 Человеческий фактор обязательно должен приниматься во внимание при оценке риска. В это понятие входят, например:

а) взаимодействие операторов с РВАЗДСМ, включая устранение сбоев;

б) взаимодействие между отдельными операторами;

в) аспекты, связанные со стрессом;

г) эргономические принципы;

д) способность людей оценивать риск в конкретной ситуации в зависимости от их обучения, опыта и способностей;

е) утомляемость;

ж) ограниченные возможности оператора (например, из-за физических недостатков или возраста).

Б.2.4.4.2 Обучение, опыт и способности оператора могут влиять на степень риска. Тем не менее ни один из этих факторов не должен использоваться вместо устранения опасности и снижения риска при помощи конструктивных или защитных мер, если есть возможность реализовать эти меры для обеспечения безопасности.

Б.2.4.5 Пригодность защитных мер

Б.2.4.5.1 Предварительная оценка риска должна учитывать пригодность защитных мер, для чего конструктору следует:

а) идентифицировать обстоятельства, которые могут привести к нанесению вреда здоровью;

б) использовать по возможности количественные методы сравнения альтернативных защитных мер.

Примечание — Сравнение альтернативных защитных мер проводят согласно ГОСТ Р 54124;

в) использовать информацию, способствующую выбору соответствующих защитных мер.

Б.2.4.5.2 При оценке риска особое внимание следует уделять компонентам и подсистемам АСУ, отказ которых может существенно увеличить степень риска.

Б.2.4.5.3 Возможность отключения защитных мер или действия, исключающие их

Для длительной безопасной эксплуатации РВАЗДСМ очень важно, чтобы защитные меры не мешали удобству их эксплуатации, не препятствовали их использованию по назначению. В противном случае возникает вероятность того, что пользователи могут отключать защитные меры или действовать в обход них, чтобы получить максимальную выгоду от использования РВАЗДСМ.

Предварительная оценка риска должна учитывать возможность отключения защитных мер или действия в обход них. Следует также принимать во внимание стимулы к отмене защитных мер или действию в обход них, например:

а) защитные меры замедляют производство, мешают какой-либо другой деятельности или противоречат предпочтениям пользователя;

б) защитные меры трудны в применении;

в) в производственный процесс вовлекаются другие лица, помимо оператора;

г) защитные меры пользователем не признаются или считаются непригодными для выполнения своих функций.

Возможность отключения защитных мер зависит как от наличия двух типов мер безопасности, таких как ограждение и программируемое выключающее устройство, так и от особенностей конструкции этих устройств.

Использование программируемых электронных систем дает возможность вывода из строя защитных мер или действия в обход них, если доступ к программному обеспечению, связанному с безопасностью, не ограничен и не контролируется должным образом. При предварительной оценке риска следует установить функции безопасности, неотделимые от технологических функций РВАЗДСМ, и определить, в какой мере доступ к ним возможен. Это особенно важно, когда требуется дистанционный доступ с целью диагностики или корректировки производственного процесса.

Б.2.4.6 Возможность поддержания защитных мер в рабочем состоянии

Б.2.4.6.1 При предварительной оценке риска необходимо рассмотреть возможность защитных мер для поддержания требуемого уровня безопасности.

Б.3 Методика оценка риска

Б.3.1 После того, как выполнена предварительная оценка риска, следует определить, требуется ли снижение риска. Если снижение риска необходимо, следует выбрать и применить соответствующие защитные меры. Неотъемлемой частью этого итеративного процесса является проверка возможности появления дополнительных опасностей или возрастания других рисков в результате применения новых защитных мер. Если дополнительные опасности все же появляются, они должны быть добавлены к перечню идентифицированных опасностей и против них следует применить соответствующие защитные меры.

По достижении поставленной цели и при благоприятном результате проведенного сравнения рисков снижение риска можно считать адекватным.

Б.3.2 Сравнение рисков

Б.3.2.1 Риски, как часть процесса оценки риска, связанные с РВАЗДСМ, могут сравниваться с рисками для подобных РВАЗДСМ при условии соблюдения следующих критериев:

Б.3.2.2 Аналогичные РВАЗДСМ удовлетворяют требованиям соответствующих стандартов типа С.

Б.3.2.3 У сравниваемых РВАЗДСМ сопоставимы:

- использование по назначению и прогнозируемое использование не по назначению, способы конструирования и изготовления;
- опасности и элементы риска;
- технические характеристики;
- условия эксплуатации.

Б.3.2.4 Применение сравнительного метода не устраняет необходимости соблюдения описанного в настоящем стандарте процесса оценки риска для конкретных условий эксплуатации. Не следует производить оценку рисков, связанных с разным применением функций. Например, не сравнивать РВАЗДСМ для погрузочных работ и РВАЗДСМ для укладки труб.

Б.3.2.5 При отклонении от выполнения функциональных задач все события и частота их возникновения заносятся в протокол испытаний.

Б.3.2.6 Для каждого конечного события в «дереве событий» моделируются аварии, характерные для этого конечного события.

Б.3.2.7 После сбора данных по итогам испытания проводится анализ событий, состоящий из анализа частот и анализа последствий:

Б.3.2.7.1 Анализ частот

Целью анализа частот является более детальное определение частоты каждого из нежелательных событий или сценариев аварий, идентифицированных на стадии идентификации опасности:

- использование соответствующих данных эксплуатации;
- прогнозирование частот событий с использованием таких технических приемов, как анализ диаграммы (а не составление) всех возможных последствий несрабатывания или аварии системы («дерева неисправностей») и анализ диаграммы возможных последствий данного события («дерева событий»). В том случае, когда статистические данные недоступны или не соответствуют требованиям, необходимо получить частоты событий посредством анализа системы и ее аварийных состояний;
- использование мнения экспертов;
- данные по надежности из литературных источников — из паспортов, ТУ на изделие, нормативной документации, справочников, статей, отчетов;
- данные по эксплуатационной надежности, собранные на предприятиях, где проводилась оценка риска или целенаправленный сбор данных для определения надежности.

Б.3.2.7.2 Анализ последствий

Проводя анализ последствий, испытатель предусматривает детальное определение результатов воздействия на людей, имущество или окружающую среду в случае наступления нежелательного события. Для расчетов рисков, касающихся безопасности (работающих или неработающих людей), анализ последствий представляет собой приблизительное определение количества людей, которые могут быть убиты, ранены или иметь серьезные поражения в том случае, если произойдет нежелательное событие.

Серьезность последствия определяется в соответствии с классификацией:

- катастрофическое — практически полная потеря объекта или системы. Большое количество смертельных исходов;
- значительное — крупный ущерб объекту или системе. Наличие смертельных исходов;
- серьезное — тяжелое ранение, увечье или вред здоровью, серьезное профессиональное заболевание, серьезный ущерб объекту или системе;
- незначительное — легкое ранение, незначительное повреждение объекта, отказ или неисправность подсистемы.

Б.3.3 Процесс оценки риска проводится в соответствии с классификацией:

В — высокая величина риска;

С — средняя величина риска;

М — малая величина риска;

Н — незначимая величина риска.

Б.3.4 На основе полученных данных и анализа для каждого вида испытаний составляется матрица рисков (см. таблицу Б.2).

Таблица Б.2 — Матрица риска (приведена только в качестве примера)

Качественная характеристика частоты событий	Частота события в год	Серьезность последствий			
		Катастрофическое	Значительное	Серьезное	Незначительное
Частое	> 1	В	В	В	С
Вероятное	$1 — 1^{-1}$	В	В	С	М
Случайное	$1^{-1} — 1^{-2}$	В	В	М	М
Маловероятное	$1^{-2} — {}^{-4}$	В	В	М	М
Неправдоподобное	$1^{-4} — 1^{-6}$	В	С	Н	Н
Невероятное	$< 10^{-6}$	С	С		Н

Б.3.5 По наличию численного количества обозначений уровней классификации рисков составляется вывод о УПБ РВАЗДСМ и делается заключение о безопасности ее конструкции при выполнении заданных функций или даются рекомендации собственнику по доработке ее конструкции.

Приложение В
(справочное)

Классификация опасностей

Параметры опасностей — в соответствии ГОСТ ISO 12100.

В таблице В.1 опасности объединены по типам: механические опасности, электрические опасности и т. п. Более подробные сведения приведены в колонках «Источник» и «Возможные последствия».

В зависимости от того, насколько подробное описание требуется при идентификации опасности, следует учитывать данные колонок таблицы В.1. В некоторых случаях данных, приведенных в одной из колонок таблицы В.1, достаточно, особенно когда опасности сконцентрированы в одной рабочей зоне и к ним могут применяться одинаковые защитные меры. При выборе учитываемой колонки следует помнить о том, что является более значимым для выбора подходящих защитных мер — источник опасности или ее последствия. Тем не менее все опасности должны быть внесены в документацию, даже если кажется, что риск, связанный с ними, в достаточной степени снижен при помощи защитных мер, предпринятых для снижения риска, связанного с другой опасностью. В противном случае опасность, не отраженная в документации, может быть не учтена, если ее риск существенно снижен при понижении риска другой опасности.

Если при описании опасности используется более одной колонки таблицы В.1, следует выбирать нужные значения, а не следовать таблице построчно. Следует подбирать и использовать в описании одно наиболее подходящее определение.

Например:

- раздавливание движущимися элементами;
- раздавливание из-за потери РВАЗДСМ или их частями устойчивости;
- электрошок или повреждение электрическим током из-за того, что части электрооборудования стали токоведущими в результате неисправности;
- долговременная потеря слуха из-за длительного шумового воздействия.

Таблица В.1 — Классификация типов и примеров опасностей

Тип или группа	Примеры опасностей	
	Источник*	Возможные** последствия
Механические опасности	- Резкое ускорение или замедление РВАЗДСМ; - заостренные части; - сближение движущихся частей с неподвижными; - режущие части; - пружинящие элементы; - падающие объекты; - сила тяжести; - высота от поверхности; - высокое давление жидкости и газа; - неустойчивое положение; - кинетическая энергия; - передвижение РВАЗДСМ; - движущиеся элементы; - вращающиеся элементы; - неровная или скользкая поверхность; - острые углы; - накопленная энергия; - вакуум	- Попадание под РВАЗДСМ; - отбрасывание в сторону; - раздавливание; - разрез или разрыв; - затягивание или захват; - запутывание; - повреждение от трения или абразивного воздействия; - удар; - впрыск давлением; - рассечение; - опасность падения из-за скольжения; - колотые раны, проколы; - удушье

Продолжение таблицы В.1

Тип или группа	Примеры опасностей	
	Источник*	Возможные** последствия
Электрические опасности	- Электрическая дуга; - электромагнитные возмущения; - электростатическое электричество; - токоведущие части; - приближение людей к токоведущим частям под высоким напряжением; - перегрузка; - части, ставшие токоведущими в результате неисправности; - короткое замыкание; - тепловое излучение	- Ожог; - химическое воздействие; - воздействие на медицинские импланты; - поражение электрическим током; - падение, отбрасывание; - пожар; - выброс расплавленных частиц; - шок
Термические опасности	- Взрыв; - пламя; - предметы либо материалы с экстремально высокой или низкой температурой; - излучение источников тепла	- Ожог; - обезвоживание; - неприятные ощущения; - обморожение; - воздействие излучения источников тепла; - ошпаривание
Опасности, создаваемые шумом	- Образование пустот; - система выброса отработанных газов; - быстрая утечка газа; - производственный процесс (штамповка, резка и т. п.); - движущиеся части; - трущиеся поверхности; - несбалансированные вращающиеся части; - пневматическое оборудование, работающее со свистом; - изношенные части	- Неприятные ощущения; - ослабление внимания; - падение из-за потери равновесия; - долговременная потеря слуха; - стресс; - звон в ушах; - усталость; - прочие последствия (например, в результате механических или электрических опасностей), наступившие из-за создания помех речевым сообщениям, восприятию звуковых сигналов
Опасности, создаваемые вибрацией	- Образование пустот; - нарушение центровки движущихся частей; - переносное оборудование; - трущиеся поверхности (продолжение); - несбалансированные вращающиеся части; - вибрация оборудования; - изношенные части	- Неприятные ощущения; - боль в поясничном отделе спины; - неврологические расстройства; - заболевания костей и суставов; - травма позвоночника; - сосудистые расстройства
Опасности, создаваемые излучением	- Источник ионизирующего излучения; - низкочастотное электромагнитное излучение; - оптическое излучение (инфракрасное, видимое и ультрафиолетовое), в том числе лазерное; - радиочастотное электромагнитное излучение	- Ожог; - повреждение глаз и кожи; - воздействие на репродуктивную систему; - мутации; - головная боль, бессонница и т. п.

Окончание таблицы В.1

Тип или группа	Примеры опасностей	
	Источник*	Возможные** последствия
Опасности, создаваемые материалами и веществами	- Аэрозоли; - биологические и микробиологические (вирусные или бактериальные) возбудители; - легковоспламеняющиеся материалы; - пыль; - взрывчатые вещества; - волокнистые материалы; - огнеопасные материалы; - жидкости; - испарения; - газ; - дымка; - окислители	- Затруднение дыхания; - удушье; - окисление; - воздействие на репродуктивную систему; - взрыв; - возгорание; - инфекция; - мутация; - отравление; - аллергические реакции
Опасности из-за несоблюдения конструктором эргономических принципов	- Затрудненный доступ; - некорректная конструкция или расположение устройств визуальной индикации; - некорректная конструкция, расположение или идентификация устройств ручного управления; - чрезмерные усилия; - мерцание, ослепление, затенение, стробоскопический эффект; - недостатки местного освещения; - избыточная мозговая нагрузка; - неудобная поза; - часто повторяющиеся монотонные движения; - недостаточный обзор	- Неприятные ощущения; - усталость; - скелетные и мускульные расстройства; - стресс; - прочие последствия как результат человеческого фактора (например, вследствие механических или электрических опасностей)
Опасности, связанные с окружающей средой, в которой эксплуатируется РВАЗДСМ	- Пыль и туман; - электромагнитные возмущения; - молния; - влажность; - загрязнение; - снег; - температура; - вода; - ветер; - недостаток кислорода	- Ожог; - легкое недомогание; - опасность падения из-за скользкой поверхности; - удушье; - все прочие последствия воздействия источников опасности на РВАЗДСМ или его части
Комбинация опасностей	Например, часто повторяющиеся действия + чрезмерные усилия + высокая температура окружающей среды и т.п.	

* Один потенциальный источник опасности может иметь множественные последствия.

** Возможные последствия, указанные в каждой группе или типе опасностей, могут быть связаны с несколькими источниками опасности.

Приложение Г
(обязательное)

Виды препятствий (целевых объектов)

Г.1 Параметры видов препятствий приведены в [3].

Препятствие для испытаний, предназначенное для имитации сидящего человека, должно соответствовать следующим требованиям и использоваться исключительно для достижения сходных (воспроизводимых) результатов (см. рисунок Г.1):

- препятствие для испытаний должно быть наполнено песком или щебнем;
- препятствие должно быть выполнено из пластика (например, полиэтилен с матовой поверхностью);
- цвет должен быть графитовый серый с матовой поверхностью.

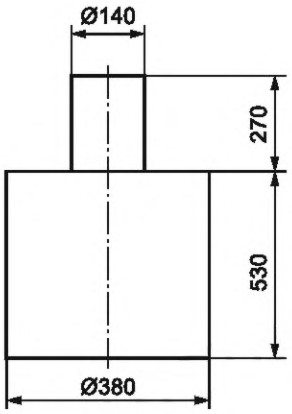


Рисунок Г.1 — Испытательный объект, имитирующий сидящего человека

Г.2 Препятствие, имитирующее габаритную неподвижную структуру

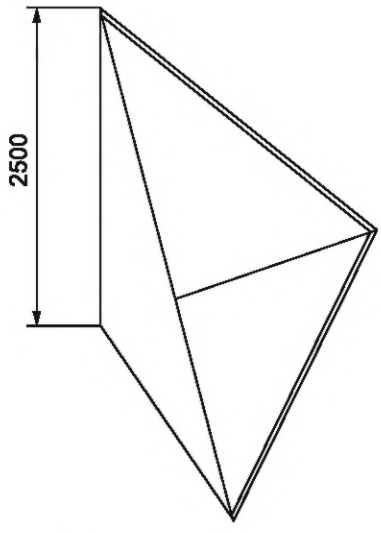


Рисунок Г.2 — Испытательный объект, имитирующий крупногабаритную структуру (размеры 2500×2500×2500 мм)

Примечание — Испытательные объекты соответствуют ГОСТ Р 70851.

Г.3 Для тестирования АСУ РВАЗДСМ используются движущиеся и неподвижные объекты (см. таблицу Г.1), которые представляют контуры и макеты возможных объектов при движении и работе РВАЗДСМ.

Таблица Г.1 — Движущиеся и неподвижные препятствия

Объекты		Размеры (Д × Ш × В), м
Неподвижные (муляж)	Человек сидящий	0,4 × 0,4 × 0,8
	Бульдозер	4,3 × 2,9 × 3,2
	Навесное оборудование	1,2 × 1,4 × 1
	Стационарный крупногабаритный объект	2,5 × 2,5 × 2,5
	Высокая трава	3 × 1 × 0,8
	Кустарник	1 × 1 × 1
	Камень	0,5 × 0,5 × 1
	Человек стоящий	0,4 × 0,4 × 1,6
	Дорожный каток	5,8 × 2,3 × 3
	Автомобиль	4,5 × 1,8 × 1,5
	Опора ЛЭП	9 × 9 × 6
	Низкая трава	3 × 1 × 0,2
	Дерево	0,2 × 0,2 × 2
	Животное	2,5 × 0,8 × 1,2
Движущиеся (контур)	Человек	2 × 0,4
	Животное	1,2 × 2,5
	Бульдозер	4,3 × 2,9 × 3,2
	Транспортное средство	2 × 2

Библиография

[1] Дорожно-строительные машины. Мигляченко В. П., Сергеев П. Г. — М.: Лесная промышленность, 1978. — 288 с.

[2] SAE J 3016-2018 Таксономия и определения терминов, относящихся к автоматизированным системам вождения автотранспортных средств на дорогах

[3] ISO 19206-2-2018 Транспорт дорожный. Контрольные приборы для оценки функций активной безопасности муляжей транспортных средств, уязвимых участников дорожного движения и других объектов. Часть 2. Требования к манекенам пешеходов

УДК 62.519:006.354 ОКС 19.060

Ключевые слова: высокоавтоматизированная землеройная и дорожно-строительная машина, целевой объект, автоматизированная система управления, риск, уровень полноты безопасности

Редактор *Е.Ю. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 20.09.2024. Подписано в печать 30.09.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,98. Уч.-изд. л. 5,58.

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.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru