ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57300— 2016/ ISO/TS 15998-2: 2012

Машины землеройные

СИСТЕМЫ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ КОМПОНЕНТОВ

Часть 2

Применение ИСО 15998

**(ISO/TS 15998-2:2012,
Earth-moving machinery — Machine control systems (MCS)
using electronic components — Part 2: Use and application of ISO 15998, IDT)**

Издание официальное

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии международного документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2016 г. № 1868-ст

4 Настоящий стандарт идентичен международному документу ISO/TS 15998-2:2012 «Машины землеройные. Системы управления с использованием электронных компонентов. Часть 2. Применение ИСО 15998» (ISO/TS 15998-2:2012 «Earth-moving machinery — Machine control systems (MCS) using electronic components — Part 2: Use and application of ISO 15998», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного документа для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им межгосударственные стандарты, сведения о которых приведены в справочном приложении ДА

5 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 ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2017

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Общие положения 4
4.1 О средствах управления в других стандартах 4
4.2 Методы оценки риска 4
5 Дополнительные руководящие указания для связанных с безопасностью систем управления машинами 5
6 Документация 6
7 Проверка связанной с безопасностью системы управления машиной 6
Приложение А (справочное) Руководящие указания по оценке риска 7
Приложение В (справочное) Руководство по формированию концепции безопасности в соответствии с ИСО 15998 44
Приложение С (справочное) Соответствие с ИСО 15998 46
Приложение D (справочное) Соответствие с ИСО 15998 на примере землеройной машины 48
Приложение Е (справочное) Качественный подход к управлению случайными отказами аппаратных средств 52
Приложение F (справочное) Архитектура 56
Приложение G (справочное) Реализуемый проект, удовлетворяющий определенным значениям УПБ или $УЭЗ_т$ 57
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам 61
Библиография 62

Введение

Сложность стандартов, посвященных электронным системам управления, затрудняет определение даже основных требований к уровням безопасности. Настоящий стандарт был разработан, чтобы помочь пользователю ИСО 15998 определить общие характеристики землеройных машин и возможные виды отказов с разумно обоснованными и согласованными требованиями к уровням безопасности. Настоящий стандарт поможет пользователю понять, что другие пользователи будут принимать аналогичные требования для подобных опасных условий.

В то время как первая часть ИСО 15998 и документы, на которые она ссылается, изложены кратко, настоящий стандарт описывает процессы, непосредственно связанные с землеройным оборудованием. С помощью большого количества примеров пользователь сможет достаточно легко определить, как применить ИСО 15998 к различным типам землеройных машин.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Машины землеройные

СИСТЕМЫ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ КОМПОНЕНТОВ

Часть 2

Применение ИСО 15998

Earth-moving machinery. Machine control systems using electronic components.
Part 2. Application of ISO 15998

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт помогает интерпретировать и применять критерии эффективности и методы испытаний функциональной безопасности системы управления машиной (далее — СУМ), использующей электронные компоненты, для землеройных машин и их оборудования, представленные в первой части ИСО 15998, с помощью:

- демонстрации альтернативного метода оценки опасности;
- рассмотрения информации и прикладных примеров для демонстрации соответствия требованиям ИСО 15998;
- рассмотрения определений, требований и применения ИСО 15998 при анализе риска опасных движений машины, выполняемых под управлением, связанных с безопасностью СУМ;
- предоставления руководства по использованию и взаимосвязи с нормативными ссылками, перечисленными в первой части ИСО 15998.

Электронные СУМ — это такие системы управления, которые непосредственно воздействуют на движение машины, т. е. приводят в движение (выполняют механическое перемещение), выполняют торможение, управляют приспособлениями и рабочими инструментами. ИСО 15998 применим к механическим отказам выключателей, датчиков и других электронных устройств, а также к механическому отказу клапанов соленоидов, такому как заедание, вызванное инородными элементами (может использоваться электронный контроль ошибки функции клапана соленоида, если оценка степени риска определит, что это необходимо).

Системы и электрические/электронные сборочные узлы (ESA), которые являются вспомогательными для эксплуатации машины и не влияют на управление машиной, такие как мониторы, средства выдачи сигналов тревоги, панель приборов, внешние световые приборы и дворники, а также те части систем, которые обеспечивают обратную связь оператору, не входят в область применения ИСО 15998, так как являются чисто гидравлическими, пневматическими и/или механическими СУМ, не использующими электронные/электрические компоненты, и в которых происходят механические отказы, такие как разрушение осей, чисто механических клапанов, автопокрышек и другие подобные отказы.

2 Нормативные ссылки

В настоящем стандарте используются нормативные ссылки на следующие документы или на их части, незаменимые для применения данного документа. В случае датированных ссылок действует

Издание официальное

только цитируемое издание. Для недатированных ссылок действует самое позднее издание документа, на который производится ссылка (включая любые внесенные в него поправки).

ISO 13766, Earth-moving machinery — Electromagnetic compatibility (Машины землеройные. Электромагнитная совместимость)

ISO 13849-1:2006, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for desing — lehnical Corrigenolom 1 (Безопасность машин. Детали систем управления, связанные с обеспечением безопасности. Часть 1. Общие принципы проектирования. Механическая поправка)[1)]

ISO 15998:2008, Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety[1)] (Землеройные машины. Системы управления с использованием электронных компонентов. Критерии эффективности и испытания на функциональную безопасность)

Примечание — При использовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальной 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 принять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте используются термины, определения и сокращения, данные в первой части ИСО 15998, а также следующие термины и определения:

3.1 **базовая машина** (base machine): Машина с кабиной или крытым кузовом и при необходимости с защищающими оператора конструкциями, без рабочего оборудования или приспособлений, но обладающая необходимыми средствами установки для такого рабочего оборудования и приспособлений.

[ИСО 6016]

3.2 **рабочее оборудование** (equipment): Набор компонентов, устанавливаемых на базовую машину, которые позволяют приспособлению выполнять основную предназначенную для машины функцию.

[ИСО 6016]

3.3 **приспособление** (attachment): Сборка компонентов, которая может быть установлена на базовую машину или рабочее оборудование для конкретного использования.

[ИСО 6016]

3.4 **уровень полноты безопасности**; УПБ [safety integrity level (SIL)]: Дискретный уровень (принимающий одно из трех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 3, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.

[МЭК 61508-4:2010, определение 3.5.8, модифицированное]

Примечания

1 Меры целевых отказов (см. таблицу 1).

2 Уровни полноты безопасности используют при определении требований полноты безопасности для функций безопасности, которые должны быть распределены по электрическим/электронным/программируемым электронным системам, связанным с безопасностью.

3 Уровень полноты безопасности (УПБ) не является свойством системы, подсистемы, элемента или компонента. Правильная интерпретация фразы «УПБ системы, связанной с безопасностью, равен n» (где n = 1, 2 или 3) означает, что система потенциально способна к реализации функций безопасности с уровнем полноты безопасности до значения, равного n.

[1)] ИСО 15988-1.

4 УПБ является самым полезным для производителей, применяющих IEC 61508 или граф риска, представленный в первой части ИСО 15998.

5 УПБ 4 не применяется для СУМ (землеройных машин).

6 УПБ Θ означает «Нет требований» или «Конкретное требование по безопасности отсутствует» (см. таблицу 1 и рисунок 1).

3.5 **уровень эффективности защиты**; УЭЗ (performance level; PL): Дискретный уровень, используемый для определения способности элементов систем управления, связанных с безопасностью, осуществлять функцию безопасности в предсказуемых условиях.

[ИСО 13849-1:2006, определение 3.1.23]

Примечания

1 УЭЗ является самым полезным для производителей, применяющих ИСО 13849.

2 См. таблицу 2.

3.6 **требуемый уровень эффективности защиты**; $УЭЗ_т$ (required performance level; PL_r): Уровень эффективности защиты (PL), применяемый для установления предела требуемого снижения риска для каждой функции безопасности (см. рисунок 1 и А.1).

[ИСО 13849-1:2006, определение 3.1.24]

3.7 **электрический/электронный сборочный узел**; ЭСУ (electrical/electronic subassembly; ESA): Электрические и/или электронные компоненты или набор компонентов, предназначенный для применения в землеройной машине, вместе со всеми соответствующими электрическими связями и проводными соединениями, который выполняет одну или несколько специализированных функций.

[ИСО 13766:2006, определение 3.10]

3.8 **функциональная безопасность** (functional safety): Часть общей безопасности, которая зависит от системы или оборудования, корректно реагирующего на его входные сигналы.

[МЭК 61508-0, определение 3.1]

Примечания

1 Например, устройство тепловой защиты, использующее тепловой датчик в обмотках электродвигателя, чтобы обесточить двигатель до его перегрева, является реализацией функциональной безопасности. Но применение специализированной изоляции, чтобы противостоять высоким температурам, не является примером функциональной безопасности (хотя и является средством безопасности и может защитить от точно такой же опасности).

2 Ни безопасность, ни функциональная безопасность не могут быть определены, не рассматривая систему как единое целое с окружающей средой, с которой они взаимодействуют.

3.9 **элемент системы управления, связанный с безопасностью** (safety-related part of a control system; SRP/CS): Часть системы управления, которая реагирует на входные сигналы, связанные с безопасностью, и вырабатывает выходные сигналы, связанные с безопасностью.

[ИСО 13849-1:2006, определение 3.1.1, модифицированное]

Примечание — Связанные с безопасностью элементы, соединенные с системой управления, появляются там, где возникают сигналы, связанные с безопасностью (включая, например, включающий кулачок и ролик переключателя позиции), и заканчиваются на выходе силовых управляющих элементов (например, главные контакты электромагнитного пускателя).

3.10 **система управления машиной**; СУМ (machine control system): Система, которая отвечает на входные сигналы, поступающие от элементов оборудования, операторов, оборудования внешнего контроля или любой их комбинации, и генерирует выходные сигналы, приводящие машину в действие предусмотренным способом.

[ИСО 13849-1:2006, определение 3.1.32]

Примечание — Система управления машиной может использовать любую технологию или любую комбинацию различных технологий (например, электрическую/электронную, гидравлическую, пневматическую, механическую).

3.11 **интервал диагностических проверок** (diagnostic time interval): Интервал между неавтономными проверками, предназначенными для обнаружения отказов в системе управления, связанной с безопасностью, или в ее части (СУСБ/Ч).

3.12 **время реакции на сбой** (fault reaction time): Время, необходимое для выполнения заданного действия, обеспечивающего достижение или поддержку безопасного состояния.

3.13 **режим высокой интенсивности запросов/режим с непрерывным запросом** (high/continuous mode): Режим работы, где частота запросов на обслуживание к СУСБ/Ч больше, чем один в год, или больше удвоенной частоты выполнения функции самопроверки системы управления.

3.14 **время безопасности процесса** (process safety time): Промежуток времени между моментом появления отказа в СУСБ/Ч и моментом возникновения опасного события, если функция безопасности не была выполнена.

4 Общие положения

4.1 О средствах управления в других стандартах

Строго рекомендуется, чтобы пользователь ИСО 15998 применял по крайней мере один из стандартов, рассматривающих средства управления, на которые ссылается настоящий стандарт. В частности, это МЭК 61508-1 или ИСО 13849-1, которые предоставляют общую информацию и теорию безопасности электронной системы управления:

- рисунок 1 МЭК 61508-1:2010 представляет в общих чертах процесс применения стандартов МЭК 61508 для обеспечения безопасности систем управления;
- рисунок 1 ИСО 13849-1:2006 представляет альтернативную блок-схему для демонстрации безопасности системы управления, на рисунке 3 ИСО 13849-1:2006 показаны методы снижения риска (которые раскрыты в приложении А ИСО 13849-1:2006) для определения УПБ и $УЭЗ_Т$.

В приложении В представлено руководство по формированию концепции безопасности.

Производители могут также применять ИСО 26262 (дорожно-транспортные средства) или ИСО 25119 (сельскохозяйственные машины), выполняя соответствующие изменения, учитывающие отличия этих машин от землеройных. Это различие должно помочь передаче технологий в различные отрасли. Производители должны полностью поддерживать один реализуемый на практике метод, заменяя или добавляя соответствующие положения МЭК 61508.

4.2 Методы оценки риска (см. 4.4 первой части ИСО 15998)

4.2.1 УПБ и УЭЗ

Пользователи могут выбрать методы определения УПБ между представленными в МЭК 61508-5 и ИСО 15998 или методы определения УЭЗ между представленными в ИСО 13849-1, ИСО 25119-2 и ИСО 26262-3. Независимо от того, выбрана ли методология для определения УПБ или УЭЗ, интенсивность отказов для режима работы с высокой частотой запросов/с непрерывным запросом должна продемонстрировать соответствующий уровень безопасности, полученный по таблице 1.

Примечания

1 Таблица 1 используется для систем, работающих в режиме с высокой частотой запросов/с непрерывным запросом. Интенсивность отказов в режиме с низкой частой запросов также рассмотрена в МЭК 61508-1:2010, раздел 7 и таблица 2. Инструкция по использованию таблицы 1 дана в МЭК 61508-1:2010, раздел 7, и в ИСО 13849-1:2006, подраздел 4.5.

2 Значение УПБ 4 не используются для машин, рассматриваемых в настоящем стандарте, поскольку не разумно оценивать землеройные машины, удовлетворяющие системному требованию УПБ, равному 4.

Таблица 1 — Таблица соответствия значений УПБ и УЭЗ

УПБ	Средняя вероятность опасных отказов в час (1/ч)	$УЭЗ_Т$	Средняя вероятность опасных отказов в час (1/ч)
—	Нет требования безопасности	—	Нет требования безопасности
—	Нет конкретных требований безопасности	A	От $> 10^{-5}$ до $< 10^{-4}$
1	От $> 10^{-6}$ до $< 10^{-5}$	B	От $> 3 \cdot 10^{-6}$ до $< 10^{-5}$
		C	От $> 10^{-6}$ до $< 3 \cdot 10^{-6}$
2	От $> 10^{-7}$ до $< 10^{-6}$	D	От $> 10^{-7}$ до $< 10^{-6}$
3	От $> 10^{-8}$ до $< 10^{-7}$	E	От $> 10^{-8}$ до $< 10^{-7}$
4	Не используется для землеройных машин	—	Не применяется

4.2.2 Варианты оценки риска

Поскольку упоминаемые средства оценки риска предназначены в качестве общего руководства по определению УПБ, допустимо и иногда необходимо «подогнать» средства оценки риска, выполнив такие изменения, которые показаны на рисунке 1, чтобы обеспечить более близкое соответствие между упоминаемыми используемыми методами оценки риска.

Из-за сложности использования параметра *W* согласно приложению А первой части ИСО 15998 также допустимо предположить, что параметр *W* всегда равен *W*2.

Примечания

1 УПБ Θ означает «Нет требований» или «Конкретное требование по безопасности отсутствует».

2 C_4 в ИСО 15998:2008, приложение А не применимо к землеройным машинам, поскольку вероятность смерти большого количества людей от землеройной машины незначительна.

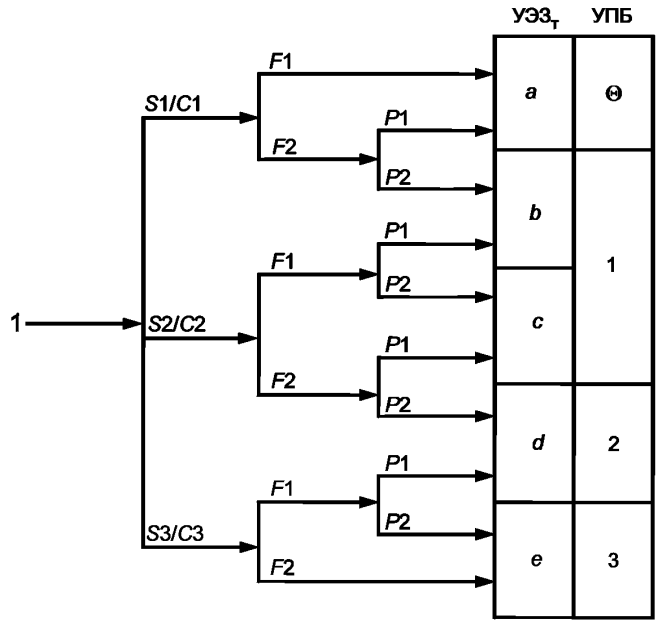


Рисунок 1 — Граф риска

4.2.3 Согласование различных методов

Независимо от используемого метода определения УПБ, УЭЗ$_т$ или эквивалентной характеристики интенсивность отказов, приведенная в таблице 1, должна использоваться для систем, работающих с высокой частотой запросов/с непрерывным запросом. Незначительные корректировки могут быть внесены, если интенсивность отказов, приведенная в таблице 1, точно не соответствует интенсивности отказов в других стандартах. Для определенных систем управления машины были установлены общие значения УПБ/УЭЗ и рассмотрены в приложении А. Для определения УПБ/УЭЗ$_т$ или подобных требований безопасности для конкретной функции безопасности необходимо выполнить оценку риска. Если результаты оценки риска значительно отличаются от общих значений УПБ, то пользователь ИСО 15998 должен их тщательно исследовать, чтобы гарантировать, что были сделаны надлежащие предположения.

5 Дополнительные руководящие указания для связанных с безопасностью систем управления машинами

В приложении Е представлены руководящие указания по реализации пункта 5.2 ИСО 15998:2008.

Никаких дополнительных руководящих указаний не дается для оставшихся подразделов раздела 5 первой части ИСО 15998.

6 Документация

В таблице В.1 (см. приложение В) представлен метод, объединяющий результаты оценки риска, снижения риска и формирования концепции безопасности в единой электронной таблице для организации документации.

7 Проверка связанной с безопасностью системы управления машиной

Тестирование аппаратных средств в соответствии с требованиями раздела 7 первой части ИСО 15998 может быть выполнено на уровне машины, уровне системы, уровне датчика, уровне коммутатора, уровне жгутов проводов, уровне соленоидных клапанов, уровне монтажной платы или подобном уровне в зависимости от того, на каком уровне тестирование является наиболее практичным или предпочтительным для пользователя ИСО 15998. Должно быть рассмотрено, как на уровень машины влияет электрическая система при ее испытании на воздействие окружающей среды, например, температуры в моторном отсеке, жесткой и мягкой подвески и т. д.

В отсутствие подтверждения тестирования первоначального производителя оборудования (OEM) поставщик должен предоставить приемлемую документацию, относящуюся к работе компонентов.

Приложение А
(справочное)

Руководящие указания по оценке риска

А.1 Типовые методы оценки риска, подобные методам оценки ИСО 13849-1

Метод ИСО 13849-1, описанный в настоящем приложении, дает представление, как определяется УЭЗ и соответствующий УПБ, связанный с конкретными видами землеройных машин и их СУСБ/Ч. Примеры других методологий оценки риска представлены в приложение А первой части ИСО 15998, ИСО/ТО 14121-2, ИСО 25119-2, ИСО 26262-3 или МЭК 61508-5.

Анализ опасности должен рассматривать только разумно предсказуемые сценарии. Например, бульдозер на стальном гусеничном ходу на шоссе не должен рассматриваться (если цель не состоит в том, чтобы ответить некоторому уникальному требованию потребителя). Просто установлено, что в обычных условиях использовать бульдозер на стальном гусеничном ходу на шоссе незаконно из-за того, что может произойти серьезное повреждение дороги. Каждый разумно предсказуемый сценарий должен быть оценен с точки зрения оператора машины и серьезности раны, частоты и возможности предотвращения опасности для постороннего свидетеля.

А.1.1 Использование графов риска

Начальное определение параметров риска делается без рассмотрения каких-либо СУМ или любых параметров безопасности, включенных в СУМ, чтобы проанализировать риск исключительно для соответствующей опасности. Дополнительное указание, как выполнить оценку риска, рассмотрено ниже, в инструкции по параметрам риска. Оценка риска первоначально предполагает существование видов отказов, которые вызовут опасное поведение машины. Средства ослабления таких опасностей рассматривают ниже.

А.1.2 Тяжесть травмы — *S*1, *S*2 и *S*3

Тяжесть имеет 3 уровня: *S*1 (небольшая — обычно незначительная травма), *S*2 (серьезная — обычно серьезное увечье или смерть одного человека) и *S*3 (катастрофическая — большое количество погибших). При выборе уровня тяжести для опасности выбирается уровень, который соответствовал бы наихудшему вероятному результату для этой опасности, а не наихудшему возможному результату, поскольку это может всегда приводить к *S*3. При выборе уровня также необходимо рассматривать непосредственный результат без учета присутствующих дополнительных условий для возможных последствий. Например, можно представить бульдозер на гусеничном ходу, который управляется самопроизвольно и поражает газовый трубопровод, что приводит к взрыву и многочисленным жертвам среди посторонних свидетелей. Этот сценарий учитывает наличие многих условий и не является вероятным результатом опасности самопроизвольного управления. Чтобы принять решение, при определении *S*1 и *S*2 должны быть учтены обычные последствия несчастных случаев и нормальные процессы лечения. Например, избиение и/или рваная рана без осложнений будут классифицированы как *S*1, тогда как ампутация или смерть будут классифицированы как *S*2.

*S*3 эквивалентно C_3 согласно первой части ИСО 15998. Данная тяжесть/последствие определена как «смерть нескольких человек».

Другое условие, которое необходимо рассмотреть, состоит в том, будет ли землеройная машина двигаться по общественным дорогам, и в этом случае вероятный сценарий может привести к многочисленным жертвам (*S*3), тогда как опасности, связанные с движением на ограниченной стройплощадке, могут быть на один (1) уровень менее серьезны (*S*2). На бездорожье машины находятся в условиях намного меньшего трафика автотранспорта, поэтому машины, которым запрещено движение по дороге, могут уменьшить уровень серьезности на единицу (1), по сравнению с подобной «дорожной» версией в случае потери управления или функции торможения, и соответствующие риски столкновений с движущимся автотранспортом.

Пример — Полноприводной погрузчик, который используется на дороге, может иметь S3 при полной потере управления. Для подобного погрузчика, но слишком большого для использования на дороге, при том же условии потери управления может быть определен более низкий уровень тяжести S2.

Машины меньшего размера из-за их меньшей массы при столкновении оказывают воздействие друг на друга с меньшей силой. Поэтому уровень тяжести для компактной машины при посторонних свидетелях и движении автотранспорта мог быть понижен на 1 по сравнению с более тяжелой версией машины в тех же самых условиях.

А.1.3 Частота и/или время нахождения в опасной зоне (F_1 и F_2)

При выборе между F_1 и F_2 бывает трудно определить процент времени нахождения персонала в опасной зоне. Однако следующее пояснение может упростить принятие правильного решения, если существует сомнение.

F_2 должен быть выбран, если человек часто или непрерывно находится в опасной зоне, т. е. ≥ 10 % времени. И не важно, находятся ли в опасной зоне те же самые или другие люди, например, при использовании лифтов. Параметр F должен быть выбран в соответствии с частотой и продолжительностью нахождения в опасной зоне.

Если проектировщику известны характеристики запросов к функции безопасности, то частота и продолжительность этих запросов могут быть выбраны в качестве частоты и продолжительности нахождения в опасной зоне. В настоящем приложении предполагается, что частота запросов к функции безопасности больше одного раза в год.

Период нахождения в опасной зоне должен быть оценен на основе отношения среднего значения нахождения в опасной зоне к полному промежутку времени, когда используется оборудование. Например, если необходимо иметь рабочих в непосредственной близости от землеройной машины во время повторяющейся операции, чтобы подать заготовку и забрать готовую деталь, то должен быть выбран F_2. Если нахождение в опасной зоне требуется только время от времени, то должен быть выбран F_1.

В случае отсутствия какого-либо другого обоснования должен быть выбран F_2, если частота выше чем один раз в час, или нахождение в опасной зоне больше чем 10 % времени.

Примеры

1 Работая около края обрыва, оператор, скорее всего, будет находиться в опасной зоне (на краю обрыва) меньше чем 10 % времени, таким образом, уровень частоты будет F_1.

2. Если у работающего грейдера выходит из строя система рулевого управления, а для самоходного грейдера это большей частью происходит, то уровень частоты будет F_2.

А.1.4 Возможность предотвращения опасности (P_1 и P_2)

Когда возникает опасная ситуация, то должен быть выбран P_1, только если существует реальный шанс предотвращения несчастного случая или значительного сокращения его последствий. P_2 выбирается, если нет почти никакого шанса предотвращения опасности.

Пример — Полная потеря тормозов на колесном автопогрузчике может первоначально оцениваться значением P_2. Ковш можно опустить, чтобы остановить машину, таким образом, возможный уровень будет снижен до P_1. Урок: если в качестве средств предотвращения опасности используются внешние источники, то в проекте должна быть обеспечена независимость оцениваемой системы. В этом случае пока органы управления оборудованием независимы от тормозной системы (т. е. нет общих компонентов), опустив ковш, можно снизить риск опасности.

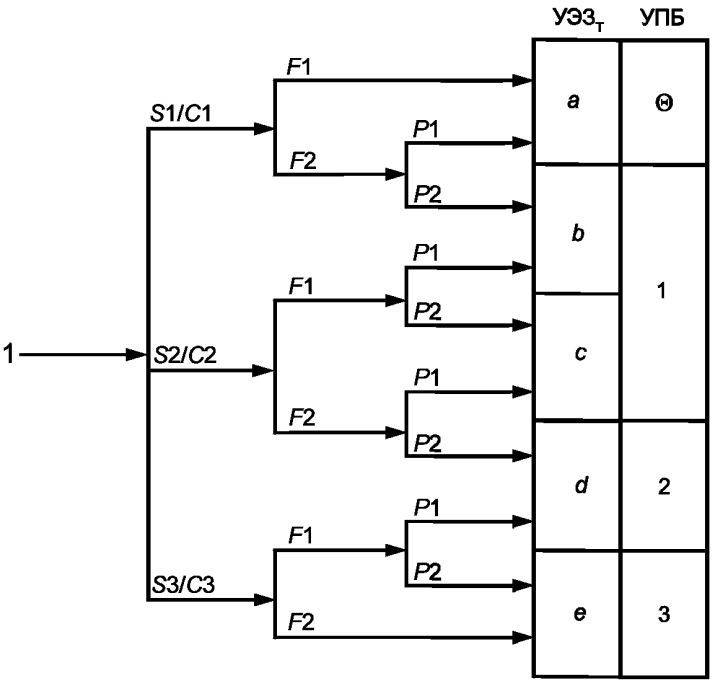
Важно знать, можно ли опасную ситуацию признать и предотвратить до реализации несчастного случая. Например, важно знать, может ли быть опасность определена непосредственно ее физическими характеристиками или признана только техническими средствами, например, индикаторами. Другие важные аспекты, которые влияют на выбор параметра P, включают:

- действие выполняется с или без контроля рабочего места;
- действие выполняется экспертами или непрофессионалами;
- скорость развития опасности (например, быстро или медленно);
- возможности для предотвращения опасности (например, убежать);
- практический опыт в области безопасности, касающийся процесса.

«Возможность предотвращения» не должна учитывать архитектуру проекта при обращении к проанализированной функции безопасности, т. е. при анализе рисков, связанных с электронной системой рулевого управления, архитектура проекта электронной системы рулевого управления не может способствовать возможности предотвращения опасности, но другие независимые системы (такие как тормоза или механическая система рулевого управления) могут.

На рисунке А.1 представлен пример графа рисков, применяемый для определения требуемых $УЭЗ_т$ для различных сценариев, используя параметры анализа риска для тяжести, частоты и/или времени нахождения в опасной зоне и возможности предотвращения опасности. Данный граф (или альтернативный граф риска, упомянутый в 4.1.2) должен использоваться для оценки всех разумно предсказуемых сценариев для каждой функции безопасности. Метод оценки риска основывается на ИСО/ТО 14121-2 (см. также ИСО 13849-1:2006, приложение А) и должен применяться в соответствии с ИСО 12100.

Если используются методы из ИСО 13849, то в приложениях, где СУСБ/Ч можно считать простой и требуемый уровень эффективности защиты не превышает значения c, качественная оценка УЭЗ может быть подтверждена в обосновании принятых проектных решений. Дополнительные разъяснения по непосредственному применению методов ИСО 15998 см. также в приложении Е.



1 — стартовая точка для предварительной оценки риска;
*S*1/*C*1 — небольшая (обычно незначительная травма);
*S*2/*C*2 — серьезная (обычно серьезное увечье или смерть);
*S*3/*C*3 — смерть нескольких людей;
*F*1 — от редко до реже и/или короткого времени нахождения в опасной зоне;
*F*2 — от частого к продолжительному и/или длительному времени нахождения в опасной зоне;
*P*1 — возможно при определенных условиях;
*P*2 — почти невозможно;
a—*e* — требуемый уровень эффективности защиты (УЭЗ$_т$) для СУМ

Рисунок А.1 — Граф риска для определения УЭЗ$_т$ для функции безопасности

А.2 Руководство и примеры анализа рисков для землеройных машин, оснащенных системами управления поворотом, движением, торможением и работой приспособлений, выполняемого для ИСО 15998, ИСО 13849-1 или других подобных оценок риска

В данном подразделе для иллюстрации идентификации опасности и распределения параметров риска представлены опасности для четырех основных рабочих функций примеров землеройной машины. Настоящий подраздел не относится к конкретной системе управления, но основывается на типовых видах землеройной машины с учетом возможного отказа, который заставляет землеройную машину вести себя непреднамеренным способом.

Графы риска, представленные в ИСО 13849-1, в первой части ИСО 15998 и полученные другими методами оценки риска, могут дать в некоторых случаях более высокие значения УПБ/УЭЗ$_т$, чем полученные в примерах и представленные в настоящем приложении обобщенные УПБ/УЭЗ$_т$. Однако эти примеры и обобщенные УПБ/УЭЗ$_т$ действительно отражают современный уровень, доступный для каждого типа функции. Кроме того, опыт (например, истории инцидентов) показывает, что они адекватны и доказаны для каждой функции.

При выполнении оценки риска и использовании таблиц А.1—А.5 для землеройных машин необходимо рассмотреть следующее.

А.2.1 Тяжесть травмы

Тяжесть не должна быть «искажена» крайне маловероятными событиями. Если бы, например, в 999 случаях из 1000, ожидаемая рана в результате несчастного случая была бы очень легкой, но в одном случае предсказана смерть, то последствие должным образом оценивается *S*1 или C_1.

А.2.2 Частота пребывания в опасной зоне

В некоторых случаях машины могут быть очень низкие частоты нахождения в опасной зоне, так что F_1 неадекватно описал бы частоты как низкие. Тогда более разумно не оценивать такой сценарий.

Пример — Движение бульдозера на стальном гусеничном ходу по шоссе осуществляется очень редко и обычно недопустимо. Поэтому нет необходимости оценивать связанные с этим риски.

А.2.3 Общая оценка

Значения *S/C*, *P* и *F* обычно зависят от анализа набора влияющих факторов, каждый из которых либо повышает, либо понижает, либо оценивает их частично.

Таблица А.1 представляет некоторые ключевые факторы, используемые при определении этих значений. После того как влияющие факторы определены, выбирается наиболее близкое значение, например, P_1 или P_2. Оценки риска могут иметь большее разрешение (например, ИСО 25119-2), чем в примерах, рассмотренных в настоящем стандарте.

Рассматриваются примеры для двух из различных методов оценки риска. Пользователь должен выбрать один метод оценки риска для всех оцениваемых систем управления, чтобы избежать конфликтов в результатах.

С увеличением скорости значения УПБ/УЭЗ$_т$, связанные с системами рулевого управления и торможения, увеличиваются из-за ограничений возможностей оператора в обеспечении управления после отказа (*P*). Также увеличивается тяжесть последствий из-за более высоких скоростей во время столкновения (*S/C*).

Количество посторонних свидетелей существенно отличается в различных сценариях. В шахтах обычно мало или нет посторонних свидетелей, присутствие которых ограничено в большинстве шахт. У малых и средних экскаваторов и всех одноковшовых экскаваторов с обратной лопатой чаще всего есть посторонние свидетели около мест их работы. Частота (*F*) должна соответственно изменяться при наличии свидетелей.

Столкновения между землеройными машинами, как правило, вызывают менее тяжелые травмы, и их число мало, что приводит к более низким значениям *S/C* и уменьшает значения УПБ/УЭЗ$_т$. Столкновения землеройной машины с автотранспортом имеют более высокие значения *S/C* для пассажиров транспортного средства.

О частичной потере. Легче обеспечить управление машиной при отказах систем рулевого управления и торможения, чем при отказах всех систем (*P*). Системы торможения и рулевого управления при работоспособности 90 % работают почти нормально. Системы торможения и рулевого управления, функциональность которых менее 5 %, не могут предотвратить большинства несчастных случаев.

Кнопка аварийного отключения/гидроусилитель тормозов/гидравлическое включение/клавишный переключатель: их эффективность управления отключением для предотвращения несчастного случая (*P*) существенно зависит от скорости машины. Они более эффективны при выполнении внезапной остановки медленно двигающейся гусеничной машины или остановки приспособления, когда присутствует посторонний свидетель в зоне работы. Но они не столь эффективны при отказе системы рулевого управления на более высоких скоростях.

В условиях бездорожья машины оказываются в менее интенсивном дорожном движении и имеют соответственно более низкое значение *S/C*. Поэтому машины, использование которых на дороге запрещено, могут иметь значение УПБ/УЭЗ$_т$ на один уровень меньше, чем подобная версия машин, использование которых на дороге разрешено, при отказе всей функциональности рулевого управления и соответствующих рисках столкновений в процессе дорожного движения. Например, полноприводный погрузчик, использование которого на дороге разрешено, имеет УПБ 3/УЭЗ$_т$ *e* при полном отказе рулевого управления, когда нет никакого предшествующего предупреждения. Для подобного погрузчика, но слишком большого для использования на дороге, требование будет на один уровень меньше или УПБ 2/УЭЗ$_т$ *d* при условии такого же отказа рулевого управления.

Таблица А.1 — Обобщенные значения УПБ/УЭЗ$_т$ оценок риска при идентификации опасности и определении значений параметров риска для землеройных машин с и без СУМ, используя метод оценки риска, подобный представленному в ИСО 13849-1 или ИСО 15998

Опасности для оператора	Тяжесть травмы, *S* или *C*	Частота и/или время нахождения в опасной зоне, *F*	Возможность предотвращения опасности, *P*	Требуемый уровень эффективности защиты, УЭЗ$_т$	УПБ
1 Бульдозер на гусеничном ходу, двигающийся со скоростью ≤ 12 км/ч	Н/п (не применимо)	F_2	P_1	Нет требования	Θ
Самопроизвольное срабатывание тормоза. Машина очень резко останавливается	Оператор вряд ли будет травмирован	Машина часто двигается со скоростями, соответствующими нанесению минимальных травм	Машина оснащена ремнем безопасности, который при использовании значительно уменьшает риск получения травмы. Оператор может использовать ноги, чтобы себя поддержать. У передней части кабины нет острых краев в зоне досягаемости. Так как машина останавливается, у нее, как		

Продолжение таблицы А.1

Опасности для оператора	Тяжесть травмы, *S* или *C*	Частота и/или время нахождения в опасной зоне, *F*	Возможность предотвращения опасности, *P*	Требуемый уровень эффективности защиты, $УЭЗ_Т$	УПБ
			правило, пробуксовывает гусеничная лента, уменьшая внезапность остановки		
2 Самосвал с шарнирно-сочлененной рамой, двигающийся со скоростью ≤ 60 км/ч	$S2/C_2$	F_2	P_1	*c*	1
Самопроизвольное срабатывание тормоза. Машина очень резко останавливается	Оператор может пострадать от серьезной травмы во время опрокидывания	Машина часто двигается со скоростями и полезным грузом, достаточными, чтобы вызвать опрокидывание	Машина оснащена ремнем безопасности, который при использовании значительно уменьшает риск получения травмы. Оператор может использовать руки и ноги, чтобы себя поддержать. У передней части кабины нет острых краев в зоне досягаемости. Как правило, полезный груз смягчает резкую остановку. Удаленные панели управления машины предотвращают оператора от осколочных травм		
3 Траншеекопатель на резиновом ходу, двигающийся со скоростью < 12 км/ч	Н/п	F_2	P_1		Θ
Машина начинает движение *F/N/R* на нейтральной передаче. Или машина начинает двигаться в противоположном от задаваемого направления. - Оператор вынужден находиться в кабине оператора. - Оператор имеет по крайней мере один главный орган управления, чтобы остановить движение	Оператор вряд ли будет травмирован	Оператор обычно находится в кабине оператора. Машина часто находится на нейтральной передаче	Оператор может нажать основной тормоз, чтобы остановиться. Машина оснащена ремнем безопасности, который при использовании значительно уменьшает риск получения травмы. У передней части кабины нет острых краев в зоне досягаемости. Скорость машины обычно очень низкая, что дает оператору больше времени на ответную реакцию		
4 Одноковшовый экскаватор с обратной лопатой, двигающийся со скоростью ≤ 40 км/ч	$S2/C_2$	F_2	P_1	*a*	Θ
Машина начинает движение *F/N/R* на нейтральной передаче. Или машина начинает двигаться в	Оператор может пострадать от легкой излечимой раны. Наиболее вероятны удары и	Оператор обычно присутствует. Машина часто находится на нейтральной передаче	Оператор может нажать основной тормоз, чтобы остановиться. Машина оснащена ремнем безопасности, который при использовании		

Продолжение таблицы А.1

Опасности для оператора	Тяжесть травмы, *S* или *C*	Частота и/или время нахождения в опасной зоне, *F*	Возможность предотвращения опасности, *P*	Требуемый уровень эффективности защиты, $УЭЗ_т$	УПБ
противоположном от задаваемого направления. - Оператор вынужден находиться у пульта оператора. - Оператор имеет по крайней мере один главный орган управления, чтобы остановить движение	ушибы. В очень редких случаях машина может покатиться, и оператор может выпасть из кабины оператора и получить более тяжелые травмы		значительно уменьшает риск получения травмы. У передней части кабины нет острых краев в зоне досягаемости. Скорость машины обычно очень низкая, что дает оператору больше времени на ответную реакцию		
5 Шарнирно-соединенный колесный погрузчик, слишком большой для использования на дороге, двигающийся со скоростью меньше 40 км/ч	$S2/C_2$	F_1	P_1	*b*	1
Полный отказ всех остановочных тормозов. - Оператор может только позволить машине двигаться по инерции до остановки или использовать приспособления для остановки. - Рулевое управление остается работоспособным	Оператор может быть травмирован в результате столкновения машины с другими машинами. Машина может быть вовлечена в одновременное опрокидывание	Погрузчики, как правило, работают вблизи препятствий, включая землеройные машины, которые могут быть сбиты	Оператор может управлять машиной, объезжая вокруг препятствий. Машина оснащена ремнем безопасности, который при использовании значительно уменьшает риск получения травмы		
6 Шарнирно-соединенный колесный погрузчик	$S2/C_2$	F_1	P_2	*c*	1
Грузовая стрела машины, ковш или другое приспособление перемещаются самопроизвольно. Оборудование или приспособление не отключается из-за повреждения рычага управления, устройства переключения или подобной причины	Оператор может смазывать машину или же быть около движущихся деталей	Оператор, как правило, находится в опасной ситуации, существенно меньше 10 % времени	Если оператор находится вблизи движущейся части, то ему достаточно трудно очень быстро уйти, чтобы предотвратить травму		
Опасности для случайных свидетелей	*S/C*	*F*	*P*	$УЭЗ_т$	УПБ1
7 Компактные машины, двигающиеся со скоростью ≤ 20 км/ч	$S2/C_2$	F_1	P_1	*b*	1

Продолжение таблицы А.1

Опасности для оператора	Тяжесть травмы, *S* или *C*	Частота и/или время нахождения в опасной зоне, *F*	Возможность предотвращения опасности, *P*	Требуемый уровень эффективности защиты, $УЭЗ_Т$	УПБ
Машина начинает движение *F/N/R* на нейтральной передаче. - Оператор вынужден находиться в кабине оператора. - Оператор может воспользоваться основным тормозом	Случайный свидетель может быть размозжен между машиной и твердой поверхностью	Случайные свидетели закрывают машину и находятся в пути меньше 10 % времени	Оператор может остановить машину в нормальном рабочем положении. Оператор инстинктивно применит торможение. Случайный свидетель может отойти и освободить путь движения машины		
8 Бульдозер на гусеничном ходу, двигающийся со скоростью ≤ 12 км/ч	$S2/C_2$	F_1	P_2	*c*	1
Полный отказ всех тормозных устройств. - Оператор может только позволить машине двигаться по инерции до остановки или использовать лезвие для остановки. - Рулевое управление не будет работать	Случайный свидетель может быть размозжен между машиной и твердой поверхностью. Случайный свидетель может попасть под машину	Случайный свидетель не часто находится на возможном пути машины	Машиной невозможно управлять. В некоторых случаях случайный свидетель может отойти и освободить путь движения машины. Скорость машины сначала ниже, чем у большинства землеройных машин		
9 Одноковшовый экскаватор с обратной лопатой, двигающийся со скоростью ≤ 40 км/ч	$S2/C_2$	Н/п	Н/п		Θ
Самопроизвольное срабатывание тормоза. Машина очень резко останавливается и может возникнуть проскальзывание	Случайный свидетель может быть размозжен между машиной и твердой поверхностью. Случайный свидетель может попасть под машину	Частота незначительна, потому что для случайного свидетеля крайне маловероятно оказаться на пути машины, которая останавливается быстрее, чем это делает оператор, даже в случае переворачивания	В дальнейшей оценке нет необходимости	Н/т	
10 Минипогрузчик	$S2/C_2$	F_1	P_2	*c*	1
Грузовая стрела машины, ковш или другое приспособление перемещаются самопроизвольно. - Оператор вынужден находиться у пульта оператора. - Оператор может остановить двигатель, чтобы остановить движение	Случайный свидетель может быть размозжен между машиной и твердой поверхностью. Случайный свидетель может попасть под машину	Оператор, как правило, находится в опасной ситуации, существенно меньше 10 % времени	Если оператор находится вблизи движущейся части, то может быть достаточно трудно очень быстро уйти, чтобы предотвратить травму		

Продолжение таблицы А.1

Опасности для оператора	Тяжесть травмы, *S* или *C*	Частота и/или время нахождения в опасной зоне, *F*	Возможность предотвращения опасности, *P*	Требуемый уровень эффективности защиты, $УЭЗ_т$	УПБ
Опасности для движения автотранспорта	*S/C*	*F*	*P*	$УЭЗ_т$	УПБ
11 Шарнирно-сочлененный грейдер, двигающийся со скоростью ≤ 50 км/ч. Машина приспособлена для движения по дорогам	$S3/C_3$	F_2	P_2	*e*	3
Полная потеря основного рулевого управления и аварийной системы рулевого управления (или управление самопроизвольное, или вовсе отсутствует при движении). - Оператор для остановки машины может ее застопорить. - Оператор не предупрежден заранее о потере рулевого управления	Несчастный случай при движении автотранспорта может привести к многократным смертельным случаям	Самоходный, пригодный для движения по дорогам грейдер часто обладает повышенной проходимостью	Машиной невозможно управлять. В некоторых случаях движущийся транспорт может уступить дорогу машине		
12 Шарнирно-сочлененные колесные погрузчики, двигающиеся со скоростью < 40 км/ч	$S3/C_3$	F_1	P_2	*e*	3
Полная потеря основного рулевого управления и аварийной системы рулевого управления (или управление самопроизвольное, или вовсе отсутствует при движении). - Оператор для остановки машины может ее застопорить. - Оператор не предупрежден заранее о потере рулевого управления	Существует возможность столкновения с более высокоскоростным транспортным средством с большим количеством пассажиров	Нахождение транспортного средства с большим количеством пассажиров на пути машины составляет существенно меньше 10 % времени	Машиной невозможно управлять. Оператор может остановить машину. Транспортное средство может избежать столкновение с погрузчиком		
13 Карьерный самосвал с жесткой рамой, двигающийся по шоссе, на котором установлена минимальная скорость 60 км/ч	$S3/C_3$	Н/п	Н/п		

Окончание таблицы А.1

Опасности для оператора	Тяжесть травмы, *S* или *C*	Частота и/или время нахождения в опасной зоне, *F*	Возможность предотвращения опасности, *P*	Требуемый уровень эффективности защиты, $УЭЗ_т$	УПБ
Полная потеря основного рулевого управления и аварийной системы рулевого управления (или управление самопроизвольное, или вовсе отсутствует при движении). - Оператор для остановки машины может ее застопорить. - Оператор не предупрежден заранее о потере рулевого управления	Существует возможность столкновения с более высокоскоростным транспортным средством с большим количеством пассажиров	Карьерному самосвалу и не разрешено, и он не использует шоссе. Автобус очень редко бывает на территории карьера, поэтому риск незначителен	В дальнейшей оценке нет необходимости		

А.3 Формирование уровней полноты безопасности (УПБ)/уровней эффективности защиты ($УЭЗ_т$) из обобщенных значений УПБ/$УЭЗ_т$, полученных в процессе оценок риска

А.3.1 В таблицах А.2—А.5 сравниваются значения УПБ/$УЭЗ_т$ для различных видов машин и выполняемых ими функций, полученные из примеров оценки рисков и назначения УПБ/УЭЗТ. Эти примеры представляют обобщенные значения УПБ/$УЭЗ_т$, которые являются консервативными значениями для СУСБ/Ч.

А.3.2 Опасности разделены на категории для: оператора (Оп), случайного свидетеля (Св) и автотранспорта (Ат). К автотранспорту относятся автомобили, грузовики и автобусы, с которыми сталкиваются землеройные машины при транспортировке или в процессе работы на шоссейных дорогах. К автотранспорту не будем относить другие землеройные машины, находящиеся на месте выполнения работ.

Примечания

1 Региональные требования к движению по дороге не обязательно совпадают с указанными в таблицах А.2—А.5.

2 Под максимальной скоростью понимают максимальную скорость по ровной дороге.

В зависимости от ситуации обслуживающий персонал может быть или операторами, или случайными свидетелями в таблице обобщенных значений УПБ/$УЭЗ_т$. Если специалист по ремонту находится у пульта оператора, то опасности оператора (Оп) из этой таблицы обычно относятся к опасностям, связанным с обслуживанием машины. Если специалист по ремонту покидает пульт оператора, то его все еще считают оператором. Если два человека обслуживают машину и один находится у пульта оператора, а другой находится вне пульта оператора, то специалист по ремонту, находящийся вне пульта оператора, подвергается опасностям как случайный свидетель (Св).

Таблица А. 2 — Обобщенные значения УПБ/$УЭЗ_т$

Тип отказа	Категория опасности	Бульдозер на гусеничном ходу, погрузчик, трубоукладчик, скрепер, ≤ 12 км/ч	Шарнирно-соединенный бульдозер на резиновом ходу или погрузчик, ≤ 40 км/ч	Одноковшовый экскаватор с обратной лопатой, ≤ 40 км/ч	Шарнирно-соединенные колесные погрузчики, ≤ 40 км/ч	Шарнирно-соединенный колесный погрузчик, слишком большой для использования на дороге/ подземный горный погрузчик/сва-лочный уплотнитель, ≤ 40 км/ч	Шарнирно-соединенный, компактный, колесный погрузчик, ≤ 40 км/ч
СТАЦИОНАРНАЯ МАШИНА							
Любые движения машины, такие как в шарнирном соедине-	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*

Продолжение таблицы А.2

Тип отказа	Категория опасности	Бульдозер на гусеничном ходу, погрузчик, трубоукладчик, скрепер, ≤ 12 км/ч	Шарнирно-соединенный бульдозер на резиновом ходу или погрузчик, ≤ 40 км/ч	Одноковшовый экскаватор с обратной лопатой, ≤ 40 км/ч	Шарнирно-соединенные колесные погрузчики, ≤ 40 км/ч	Шарнирно-соединенный колесный погрузчик, слишком большой для использования на дороге/подземный горный погрузчик/сваточный уплотнитель, ≤ 40 км/ч	Шарнирно-соединенный, компактный, колесный погрузчик, ≤ 40 км/ч
нии, продвижение вперед, ее стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, функции подъема и спуска и другие подобные функций вращения, например, бурение, разрезка, скашивание и подобные, начинают выполняться самопроизвольно. - Машина стационарная. - Оператор отсутствует. - Применено неисправное устройство/стояночный тормоз. - Двигатель может работать. - Приспособления на земле в соответствующих случаях для машин не используются	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*
Двигатель запускается самопроизвольно во время обслуживания. - Устройство отключения аккумулятора блокировано в положении отключено	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ УЭЗт *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
ДЕЙСТВУЮЩАЯ МАШИНА							
Продвижение, движение стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, выполнение функции подъема и спуска и другие подобные функции вращения, такие как сверление, отрезание, скашивание и аналогичные, не реализуются, если подается команда на их включение	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т
ПРОДВИЖЕНИЕ/ТОРМОЖЕНИЕ							
Скорость движения/ускорения намного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как *F*/*N*/*R*.	Оп	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*

Продолжение таблицы А.2

Тип отказа	Категория опасности	Бульдозер на гусеничном ходу, погрузчик, трубоукладчик, скрепер, ≤ 12 км/ч	Шарнирно-сочлененный бульдозер на резиновом ходу или погрузчик, ≤ 40 км/ч	Одноковшовый экскаватор с обратной лопатой, ≤ 40 км/ч	Шарнирно-сочлененные колесные погрузчики, ≤ 40 км/ч	Шарнирно-сочлененный колесный погрузчик, слишком большой для использования на дороге/подземный горный погрузчик/сваложный уплотнитель, ≤ 40 км/ч	Шарнирно-сочлененный, компактный, колесный погрузчик, ≤ 40 км/ч
- Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения							
Скорость хода/ускорения немного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как *F/N/R*. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т
Полная потеря всех средств торможения для остановки. - Оператор может только позволить машине двигаться по инерции до остановки или в некоторых случаях для остановки использовать приспособление. - Для большинства колесных машин рулевое управление остается работоспособным, но не для машин с управлением направлением движения и гусеничных машин	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	Н/п	УПБ 1/ $УЭЗ_т$ *b*
Полная потеря рабочего и вспомогательного торможения. - Оператор все еще имеет по крайней мере один основной орган управления, чтобы остановить машину, такой как стояночный тормоз	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*
Полная потеря замедлителя двигателя/передачи/электрического. - Поддержка функций рабочего, вспомогательного, и стояночного тормоза. Без предупреждения	Оп	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Св	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п

Продолжение таблицы А.2

Тип отказа	Категория опасности	Бульдозер на гусеничном ходу, погрузчик, трубоукладчик, скрепер, ≤ 12 км/ч	Шарнирно-сочлененный бульдозер на резиновом ходу или погрузчик, ≤ 40 км/ч	Одноковшовый экскаватор с обратной лопатой, ≤ 40 км/ч	Шарнирно-сочлененные колесные погрузчики, ≤ 40 км/ч	Шарнирно-сочлененный колесный погрузчик, слишком большой для использования на дороге/подземный горный погрузчик/сваточный уплотнитель, ≤ 40 км/ч	Шарнирно-сочлененный, компактный, колесный погрузчик, ≤ 40 км/ч
Любой тормоз применяется оператором самопроизвольно, возможно при движении на максимальной скорости. - Машину заносит до остановки в большинстве случаев. - Рулевое управление очень неэффективное	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Св	УПБ Θ/ Н/т	УПБ Θ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Ат	Н/п	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	Н/п	УПБ 1/ $УЭЗ_т$ *b*
Растормаживание тормоза поворота без команды. - Машина может перемещаться только очень медленно из-за утечки в гидравлической системе. - Оператор отсутствует	Оп	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Св	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
РУЛЕВОЕ УПРАВЛЕНИЕ							
Полная потеря всего рулевого управления (или рулевое управление выполняется самопроизвольно или совсем не выполняется при движении). - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*
	Ат	Н/п	УПБ 3/ $УЭЗ_т$ *e*	УПБ 3/ $УЭЗ_т$ *e*	УПБ 3/ $УЭЗ_т$ *e*	Н/п	УПБ 3/ $УЭЗ_т$ *e*
Потеря нормального рулевого управления при поддержке рулевого управления другой системой (или рулевое управление выполняется отчасти самопроизвольно, или чувствительность автомобиля к действиям водителя ограничена при всех движениях автомобиля). - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления. - Оператор может переключиться на альтернативное управление, например, с помощью джойстика	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	Н/п	УПБ 2/ $УЭЗ_т$ *d*

Продолжение таблицы А.2

Тип отказа	Категория опасности	Бульдозер на гусеничном ходу, погрузчик, трубоукладчик, скрепер, ≤ 12 км/ч	Шарнирно-соединенный бульдозер на резиновом ходу или погрузчик, ≤ 40 км/ч	Одноковшовый экскаватор с обратной лопатой, ≤ 40 км/ч	Шарнирно-соединенные колесные погрузчики, ≤ 40 км/ч	Шарнирно-соединенный колесный погрузчик, слишком большой для использования на дороге/подземный горный погрузчик/сваложный уплотнитель, ≤ 40 км/ч	Шарнирно-соединенный, компактный, колесный погрузчик, ≤ 40 км/ч
ОБОРУДОВАНИЕ/ПРИСПОСОБЛЕНИЯ							
Нож дорожного струга, самосвальный контейнер, дорожный рыхлитель, ковш и другое оборудование начинает перемещаться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ Θ/ $УЭЗ_т$ *a*	Н/п	УПБ Θ/ $УЭЗ_т$ *a*
Вращение приспособления, функции экскаватора-погрузчика/экскаватора с обратной лопатой, поворот платформы экскаватора, движение стрелы экскаватора, рукояти экскаватора, ковшов экскаватора, которые могут достаточно далеко выдвинуться, стабилизаторов или функции мачты минипогрузчика начинают выполняться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *c*. Рассмотреть УПБ 2/ $УЭЗ_т$ *d*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*
	Ат	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*
Функция автоматического управления ножом/ковшом/ накопителем потеряна. Нож/ ковш/ накопитель перемещается беспорядочно или оказываются в нежелательном местоположении. - Предполагается, что оператор находится на рабочем месте, так как, уходя, он вынужден отключить функцию приспособления. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, перемещение и т. д.	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*

Окончание таблицы А.2

Тип отказа	Категория опасности	Бульдозер на гусеничном ходу, погрузчик, трубоукладчик, скрепер, ≤ 12 км/ч	Шарнирно-сочлененный бульдозер на резиновом ходу или погрузчик, ≤ 40 км/ч	Одноковшовый экскаватор с обратной лопатой, ≤ 40 км/ч	Шарнирно-сочлененные колесные погрузчики, ≤ 40 км/ч	Шарнирно-сочлененный колесный погрузчик, слишком большой для использования на дороге/подземный горный погрузчик/сваелочный уплотнитель, ≤ 40 км/ч	Шарнирно-сочлененный, компактный, колесный погрузчик, ≤ 40 км/ч
Функция автоматического управления ножом потеряна. Нож/ковш не будет двигаться автоматически. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, боковое перемещение и т. д.	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т
Быстроразъемное соединение позволяет приспособлению непроизвольно срываться	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*
	Ат	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т
ДВИГАТЕЛЬ							
Помпаж двигателя с незначительным воздействием на: скорость продвижения, рулевое управление, торможение или приспособления	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБΘ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т

Таблица А.3 — Обобщенные значения $УПБ/УЭЗ_т$

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
СТАЦИОНАРНАЯ МАШИНА							
Любые движения машины, такие как в шарнирном соединении, продвижение вперед, ее стрелы, ковша,	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*

Продолжение таблицы А.3

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
рукояти, ножа, опрокидывателя бункера, поворот экскаватора, функции подъема и спуска и другие подобные функций вращения, например, бурение, разрезка, скашивание и подобные, начинают выполняться самопроизвольно. - Машина стационарная. - Оператор отсутствует. - Применено неисправное устройство/ стояночный тормоз. - Двигатель может работать. - Приспособления на земле в соответствующих случаях для машин не используются	Ат	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	Н/п (УПБ1/ $УЭЗ_т$ *b)*	Н/п (УПБ 1/ $УЭЗ_т$ *b)*	Н/п
Двигатель запускается самопроизвольно во время обслуживания. - Устройство отключения аккумулятора блокировано в положении отключено	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
ДЕЙСТВУЮЩАЯ МАШИНА							
Продвижение, движение стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, выполнение функции подъема и спуска и другие подобные функции вращения, такие как сверление, отрезание, скашивание и аналогичные, не реализуются, если подается команда на их включение	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ Θ/ Н/т	Н/п	Н/п	Н/п УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п

Продолжение таблицы А.3

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
ДВИЖЕНИЕ/ТОРМОЖЕНИЕ							
Скорость хода/ускорения намного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как *F*/*N*/*R*. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Оп	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*
	Ат	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	Н/п (УПБ Θ/ УЭЗ$_т$ *a*)	Н/п (УПБ Θ/ УЭЗ$_т$ *a*)	Н/п
Скорость хода/ускорения немного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как *F*/*N*/*R*. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п
Полная потеря всех средств торможения для остановки. - Оператор может только позволить машине двигаться по инерции до остановки или в некоторых слу-	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Св	УПБ 2/ УЭЗ$_т$ *d*	УПБ 2/ УЭЗ$_т$ *d*	УПБ 2/ УЭЗ$_т$ *d*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*

Продолжение таблицы А.3

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
чаях для остановки использовать приспособление. - Для большинства колесных машин рулевое управление остается работоспособным, но не для машин с управлением направления движения и гусеничных машин	Ат	УПБ 2/ УЭЗ$_т$ *d*	Н/п	Н/п	Н/п (УПБ 1/ УЭЗ$_т$ *b*)	Н/п (УПБ 1/ УЭЗ$_т$ *b*)	Н/п
Полная потеря рабочего и вспомогательного торможения. - Оператор все еще имеет по крайней мере один основной орган управления, чтобы остановить машину, такой как стояночный тормоз	Оп	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	Н/п	Н/п	Н/п
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	Н/п	Н/п	Н/п
	Ат	УПБ 1/ УЭЗ$_т$ *b*	Н/п	Н/п	Н/п	Н/п	Н/п
Полная потеря замедлителя двигателя/передачи/электрического. - Поддержка функций рабочего, вспомогательного, и стояночного тормоза. Без предупреждения	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п	Н/п
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п	Н/п
	Ат	УПБ Θ/ Н/т	Н/п	Н/п	Н/п	Н/п	Н/п
Любой тормоз применяется оператором самопроизвольно, возможно при движении на максимальной скорости. - Машину заносит до остановки в большинстве случаев. - Рулевое управление очень неэффективное	Оп	УПБ 1/ УЭЗ$_т$ *c*	УПБ 1/ УЭЗ$_т$ *c*	УПБ 1/ УЭЗ$_т$ *c*	УПБ Θ/ УЭЗ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ 1/ УЭЗ$_т$ *b*	Н/п	Н/п	Н/п УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п
Растормаживание тормоза поворота без команды. - Машина может перемещаться только очень медленно, из-за утечки в гидравлической системе. - Оператор отсутствует	Оп	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п

Продолжение таблицы А.3

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
РУЛЕВОЕ УПРАВЛЕНИЕ							
Полная потеря всего рулевого управления (или рулевое управление выполняется самопроизвольно или совсем не выполняется при движении). - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления	Оп	УПБ 1/ УЭЗ$_т$ *b a*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*
	Св	УПБ 2/ УЭЗ$_т$ *d*	УПБ 2/ УЭЗ$_т$ *d*	УПБ 2/ УЭЗ$_т$ *d*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*
	Ат	УПБ 3/ УЭЗ$_т$ *e*	Н/п	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п УПБ Ѳ/ УЭЗ$_т$ *a*	Н/п
Потеря нормального рулевого управления при поддержке рулевого управления другой системой (или рулевое управление выполняется отчасти самопроизвольно, или чувствительность автомобиля к действиям водителя ограничена при всех движениях автомобиля) - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления. - Оператор может переключиться на альтернативное управление, например, с помощью джойстика	Оп	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	Н/п	Н/п	Н/п
	Св	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	Н/п	Н/п	Н/п
	Ат	УПБ 2/ УЭЗ$_т$ *d*	Н/п	Н/п	Н/п	Н/п	Н/п
ОБОРУДОВАНИЕ/ПРИСПОСОБЛЕНИЯ							
Нож дорожного струга, самосвальный контейнер, дорожный рыхлитель, ковш и другое оборудование	Оп	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т
	Св	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ Ѳ/ УЭЗ$_т$ *a*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*

Продолжение таблицы А.3

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
начинает перемещаться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Ат	Н/п	Н/п	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п
Вращение приспособлений, функции экскаватора-погрузчика/ экскаватора с обратной лопатой, поворот платформы экскаватора, движение стрелы экскаватора, рукояти экскаватора, ковшов экскаватора, которые могут достаточно далеко выдвинуться, стабилизаторов или функции мачты минипогрузчика начинают выполняться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	Н/п	Н/п	Н/п	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т	УПБ Ѳ/ Н/т
	Св	Н/п	Н/п	Н/п	УПБ 1/ УЭЗ$_т$ *c.* Рассмотреть УПБ 2/ УЭЗ$_т$ *d*	УПБ 1/ УЭЗ$_т$ *c.* Рассмотреть УПБ 2/ УЭЗ$_т$ *d*	УПБ 1/ УЭЗ$_т$ *c* УПБ Ѳ/ Нет требования для рукояти и стрелы экскаватора, если он не используется как кран
	Ат	Н/п	Н/п	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п
Функция автоматического управления ножом/ковшом/накопителем потеряна. Нож/ковш/накопитель перемещаются беспорядочно или оказываются в нежелательном местоположении. - Предполагается, что оператор находится в рабочей кабине, так как, уходя, он вынужден отключить функцию приспособления.	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ Ѳ/ УЭЗ$_т$ *a* или УПБ 1/ 1/ УЭЗ$_т$ *b*, если есть опасность возможного касания кабины оператора или другого рабочего места	УПБ Ѳ/ УЭЗ$_т$ *a* или УПБ 1/ УЭЗ$_т$ *b*, если есть опасность возможного касания кабины оператора или другого рабочего места	УПБ Ѳ/ УЭЗ$_т$ *a* или УПБ 1/ УЭЗ$_т$ *b*, если есть опасность возможного касания кабины оператора или другого рабочего места

Окончание таблицы А.3

Тип отказа	Категория опасности	Самосвал с шарнирно-сочлененной рамой, скорость на котором ≤ 60 км/ч	Подземный горный самосвал не может двигаться по шоссе, минимальная скорость на котором 60 км/ч	Карьерный самосвал с жесткой рамой не может двигаться, по шоссе, минимальная скорость на котором 80 км/ч	Экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Компактный экскаватор на железных гусеницах (на резиновом гусеничном ходу) не может двигаться по дороге, минимальная скорость на которой 12 км/ч	Большой экскаватор на железных гусеницах или погрузчик > 45 т не может двигаться по дороге, минимальная скорость на которой 12 км/ч
- Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, перемещение и т. д.	Св	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ Θ/ УЭЗ$_т$ *a*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Ат	УПБ 1/ УЭЗ$_т$ *b*	Н/п	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п
Функция автоматического управления ножом потеряна. Нож/ковш не будет двигаться автоматически. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, боковое перемещение и т. д.	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ Θ/ Н/т	Н/п	Н/п	Н/п УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п
Быстроразъемное соединение: позволяет приспособлению непроизвольно срываться	Оп	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	Н/п	Н/п	Н/п	УПБ 1/ УЭЗ$_т$ *c*	УПБ 1/ УЭЗ$_т$ *c*	УПБ 1/ УЭЗ$_т$ *c*
	Ат	Н/п	Н/п	Н/п	Н/п УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п
ДВИГАТЕЛЬ							
Помпаж двигателя с незначительным воздействием на скорость продвижения, рулевое управление, торможение или приспособления	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ Θ/ УЭЗ$_т$ *a*	Н/п	Н/п	Н/п УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п

Таблица А.4 — Обобщенные значения УПБ/УЭЗ$_т$

Тип отказа	Категория опасности	Колесный экскаватор, приспособленный для движения по дорогам, ≤ 25 км/ч	Колесный экскаватор, приспособленный или не приспособленный для движения по дорогам, ≤ 40 км/ч	Колесный экскаватор, не приспособленный для движения по дорогам, ≤ 12 км/ч	Шарнирно-соединенный автогрейдер, приспособленный для движения по дорогам, ≤ 50 км/ч	Шарнирно-соединенный грейдер, слишком большой для общественных дорог, как правило, используется в горной промышленности, ≤ 50 км/ч	Минипогрузчикам и вездеходным погрузчикам на гусеничном ходу не позволено движение по дороге, а на резиновом ходу — позволено ≤ 25 км/ч
СТАЦИОНАРНАЯ МАШИНА							
Любые движения машины, такие как в шарнирном соединении, продвижение вперед, ее стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, функции подъема и спуска и другие подобные функций вращения, например, бурение, разрезка, скашивание и подобные, начинают выполняться самопроизвольно. - Машина стационарная. - Оператор отсутствует. - Применено неисправное устройство/стояночный тормоз. - Двигатель может работать. - Приспособления на земле в соответствующих случаях для машин не используются	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Ат	УПБ 1/ УЭЗ$_т$ *b*	Н/п (УПБ 1/ УЭЗ$_т$ *b)*	Н/п	(УПБ1/ УЭЗ$_т$ *b)*	Н/п	Н/п (УПБ 1/ УЭЗ$_т$ *b)*
Двигатель запускается самопроизвольно во время обслуживания. - Устройство отключения аккумулятора блокировано в положении отключено	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
ДЕЙСТВУЮЩАЯ МАШИНА							
Продвижение, движение стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, выполнение функции подъема и спуска и другие подобные функции вращения, такие как сверление, отрезание, скашивание и аналогичные, не реализуются, если подается команда на их включение	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т	Н/п	Н/п УПБ Θ/ Н/т
ДВИЖЕНИЕ/ТОРМОЖЕНИЕ							
Скорость хода/ускорения намного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели.	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*

Продолжение таблицы А.4

Тип отказа	Категория опасности	Колесный экскаватор, приспособленный для движения по дорогам, ≤ 25 км/ч	Колесный экскаватор, приспособленный или не приспособленный для движения по дорогам, ≤ 40 км/ч	Колесный экскаватор, не приспособленный для движения по дорогам, ≤ 12 км/ч	Шарнирно-соединенный автогрейдер, приспособленный для движения по дорогам, ≤ 50 км/ч	Шарнирно-соединенный грейдер, спишком большой для общественных дорог, как правило, используется в горной промышленности, ≤ 50 км/ч	Минипогрузчикам и вездеходным погрузчикам на гусеничном ходу не позволено движение по дороге, а на резиновом ходу — позволено ≤ 25 км/ч
- Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как *F*/*N*/*R*. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Ат	УПБ 1/ $УЭЗ_т$ *b*	Н/п УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п УПБ 1/ $УЭЗ_т$ *b*
Скорость хода/ускорения немного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как *F*/*N*/*R*. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	Н/п УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т	Н/п	Н/п УПБ Θ/ Н/т
Полная потеря всех средств торможения для остановки. - Оператор может только позволить машине двигаться по инерции до остановки или в некоторых случаях для остановки использовать приспособление. - Для большинства колесных машин рулевое управление остается работоспособным, но не для машин с управлением направлением движения и гусеничных машин	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	УПБ 1/ $УЭЗ_т$ *b*	Н/п УПБ 2/ $УЭЗ_т$ *d*	Н/п	УПБ 2/ $УЭЗ_т$ *d*	Н/п	Н/п УПБ 1/ У $УЭЗ_т$ ЭЗт *b*
Полная потеря рабочего и вспомогательного торможения. - Оператор все еще имеет по крайней мере один основной орган управления, чтобы остановить машину, такой как стояночный тормоз	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п УПБ 1/ $УЭЗ_т$ *b*

Продолжение таблицы А.4

Тип отказа	Категория опасности	Колесный экскаватор, приспособленный для движения по дорогам, ≤ 25 км/ч	Колесный экскаватор, приспособленный или не приспособленный для движения по дорогам, ≤ 40 км/ч	Колесный экскаватор, не приспособленный для движения по дорогам, ≤ 12 км/ч	Шарнирно-соединенный автогрейдер, приспособленный для движения по дорогам, ≤ 50 км/ч	Шарнирно-соединенный грейдер, слишком большой для общественных дорог, как правило, используется в горной промышленности, ≤ 50 км/ч	Минипогрузчикам и вездеходным погрузчикам на гусеничном ходу не позволено движение по дороге, а на резиновом ходу — позволено ≤ 25 км/ч
Полная потеря замедлителя двигателя/передачи/электрического. - Поддержка функций рабочего, вспомогательного, и стояночного тормоза. Без предупреждения	Оп	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Св	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
Любой тормоз применяется оператором самопроизвольно, возможно при движении на максимальной скорости. - Машину заносит до остановки в большинстве случаев. - Рулевое управление очень неэффективное	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*
	Ат	УПБ Θ/ $УЭЗ_т$ *a*	Н/п УПБ Θ/ $УЭЗ_т$ *a*	Н/п	УПБ Θ/ $УЭЗ_т$ *a*	Н/п	Н/п УПБ Θ/ $УЭЗ_т$ *a*
Растормаживание тормоза поворота без команды. - Машина может перемещаться только очень медленно, из-за утечки в гидравлической системе. - Оператор отсутствует	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п	Н/п
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п	Н/п
	Ат	УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п	Н/п	Н/п	Н/п
РУЛЕВОЕ УПРАВЛЕНИЕ							
Полная потеря всего рулевого управления (или рулевое управление выполняется самопроизвольно или совсем не выполняется при движении). - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ Θ/ $УЭЗ_т$ *a*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 2/ $УЭЗ_т$ *d*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	УПБ 2/ $УЭЗ_т$ *d*	Н/п УПБ 3/ $УЭЗ_т$ *e*	Н/п	УПБ 3/ $УЭЗ_т$ *e*	Н/п	Н/п УПБ 2/ $УЭЗ_т$ *d*
Потеря нормального рулевого управления при поддержке рулевого управления другой системой (или рулевое управление выполняется отчасти самопроизвольно, или чувствитель-	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/Н/т	УПБ Θ/Н/т
	Св	УПБ Θ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*

Продолжение таблицы А.4

Тип отказа	Категория опасности	Колесный экскаватор, приспособленный для движения по дорогам, ≤ 25 км/ч	Колесный экскаватор, приспособленный или не приспособленный для движения по дорогам, ≤ 40 км/ч	Колесный экскаватор, не приспособленный для движения по дорогам, ≤ 12 км/ч	Шарнирно-соединенный автогрейдер, приспособленный для движения по дорогам, ≤ 50 км/ч	Шарнирно-соединенный грейдер, спишком большой для общественных дорог, как правило, используется в горной промышленности, ≤ 50 км/ч	Минипогрузчикам и вездеходным погрузчикам на гусеничном ходу не позволено движение по дороге, а на резиновом ходу — позволено ≤ 25 км/ч
ность автомобиля к действиям водителя ограничена при всех движениях автомобиля). - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления. - Оператор может переключиться на альтернативное управление, например, с помощью джойстика	Ат	УПБ 1/ УЭЗ$_т$ *b*	Н/п УПБ 2/ УЭЗ$_т$ *d*	Н/п	УПБ 2/ УЭЗ$_т$ *d*	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*
ОБОРУДОВАНИЕ/ПРИСПОСОБЛЕНИЯ							
Нож дорожного струга, самосвальный контейнер, дорожный рыхлитель, ковш и другое оборудование начинает перемещаться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Ат	УПБ 1/ УЭЗ$_т$ *b*	Н/п УПБ 1/ УЭЗ$_т$ *b*	Н/п	УПБ 1/ УЭЗ$_т$ *b*	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*
Вращение приспособлений, функции экскаватора-погрузчика/экскаватора с обратной лопатой, поворот платформы экскаватора, движение стрелы экскаватора, рукояти экскаватора, ковшов экскаватора, которые могут достаточно далеко выдвинуться, стабилизаторов или функции мачты минипогрузчика начинают выполняться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п	УПБ Θ/Н/т. УПБ 1/ УЭЗт *c* для стрелы во время съезда с дороги
	Св	УПБ 1/ УЭЗ$_т$ *c*. Рассмотреть УПБ 2/ УЭЗ$_т$ *d*	УПБ 1/ УЭЗ$_т$ *c*. Рассмотреть УПБ 2/ УЭЗ$_т$ *d*	УПБ 1/ УЭЗ$_т$ *c*. Рассмотреть УПБ 2/ УЭЗ$_т$ *d*	Н/п	Н/п	УПБ 1/ УЭЗ$_т$ *c*
	Ат	УПБ 1/ УЭЗ$_т$ *c*	Н/п УПБ 1/ УЭЗ$_т$ *c*	Н/п	Н/п	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*

Окончание таблицы А.4

Тип отказа	Категория опасности	Колесный экскаватор, приспособленный для движения по дорогам, ≤ 25 км/ч	Колесный экскаватор, приспособленный или не приспособленный для движения по дорогам, ≤ 40 км/ч	Колесный экскаватор, не приспособленный для движения по дорогам, ≤ 12 км/ч	Шарнирно-соединенный автогрейдер, приспособленный для движения по дорогам, ≤ 50 км/ч	Шарнирно-соединенный грейдер, слишком большой для общественных дорог, как правило, используется в горной промышленности, ≤ 50 км/ч	Минипогрузчикам и вездеходным погрузчикам на гусеничном ходу не позволено движение по дороге, а на резиновом ходу — позволено ≤ 25 км/ч
Функция автоматического управления ножом/ковшом/ накопителем потеряна. Нож/ковш/ накопитель перемещаются беспорядочно или оказываются в нежелательном местоположении. - Предполагается, что оператор находится в рабочей кабине, так как, уходя, он вынужден отключить функцию приспособления. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, перемещение и т. д.	Оп	УПБ Θ/ $УЭЗ_т$ *a* или УПБ 1/ УЭЗт *b*, если есть опасность возможного касания кабины оператора или другого рабочего места	УПБ Θ/ $УЭЗ_т$ *a* или УПБ 1/УЭЗт *b*, если есть опасность возможного касания кабины оператора или другого рабочего места	УПБ Θ/ $УЭЗ_т$ *a* или УПБ 1/ УЭЗт *b*, если есть опасность возможного касания кабины оператора или другого рабочего места	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ b	УПБ Θ/ Н/т. УПБ 1/ $УЭЗ_т$ *c* для стрелы во время съезда с дороги
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п УПБ/ $УЭЗ_т$ *b*
Функция автоматического управления ножом потеряна. Нож/ковш не будет двигаться автоматически. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, боковое перемещение и т. д.	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т	Н/п	Н/п УПБ Θ/ Н/т
Быстроразъемное соединение позволяет приспособлению непроизвольно срываться	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	Н/п	УПБ Θ/ Н/т
	Св	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *c*
	Ат	УПБ Θ/ Н/т	Н/п УПБ Θ/ Н/т	Н/п	Н/п	Н/п	Н/п УПБ Θ/ Н/т
ДВИГАТЕЛЬ							
Помпаж двигателя с незначительным воздействием на скорость продвижения, рулевое управление, торможение или приспособления	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	УПБ Θ/ $УЭЗ_т$ *a*	Н/п УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т	Н/п	Н/п УПБ Θ/ Н/т

Таблица А.5 — Обобщенные значения УПБ/УЭЗ$_т$

Тип отказа	Категория опасности	Гусеничный траншеекопатель, ≤ 12 км/ч	Траншеекопатель на резиновом ходу, ≤ 12 км/ч	Машина горизонтально направленного бурения, управляемая сзади идущим оператором, ≤ 12 км/ч	Самоходная машина горизонтально направленного бурения, ≤ 12 км/ч	Колесный самоходный скрепер, приспособленный для движения по дорогам ≤ 40 км/ч	Самоходный каток, приспособленный для движения по дорогам ≤ 12 км/ч
СТАЦИОНАРНАЯ МАШИНА							
Любые движения машины, такие как в шарнирном соединении, продвижение вперед, ее стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, функции подъема и спуска и другие подобные функций вращения, например, бурение, разрезка, скашивание и подобные, начинают выполняться самопроизвольно. - Машина стационарная. - Оператор отсутствует. - Применено неисправное устройство/стояночный тормоз. - Двигатель может работать. - Приспособления на земле в соответствующих случаях для машин не используются	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Ат	Н/п	УПБ 1/ УЭЗ$_т$ *b*	Н/п	Н/п УПБ 1/ УЭЗ$_т$ *b*	УПБ1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
Двигатель запускается самопроизвольно во время обслуживания. - Устройство отключения аккумулятора блокировано в положении отключено	Оп	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Св	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*	УПБ 1/ УЭЗ$_т$ *b*
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
ДЕЙСТВУЮЩАЯ МАШИНА							
Продвижение, движение стрелы, ковша, рукояти, ножа, опрокидывателя бункера, поворот экскаватора, выполнение функции подъема и спуска и другие подобные функций вращения, такие как бурение, разрезка, скашивание и аналогичные, не реализуются, если подается команда на их включение	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т
ДВИЖЕНИЕ/ТОРМОЖЕНИЕ							
Скорость хода/ускорения намного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ 1/ УЭЗт *b*	УПБ Θ/ Н/т

Продолжение таблицы А.5

Тип отказа	Категория опасности	Гусеничный траншеекопатель, ≤ 12 км/ч	Траншеекопатель на резиновом ходу, ≤ 12 км/ч	Машина горизонтально направленного бурения, управляемая сзади идущим оператором, ≤ 12 км/ч	Самоходная машина горизонтально направленного бурения, ≤ 12 км/ч	Колесный самоходный скрепер, приспособленный для движения по дорогам ≤ 40 км/ч	Самоходный каток, приспособленный для движения по дорогам ≤ 12 км/ч
присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как F/N/R. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
Скорость хода/ускорения немного выше, чем задана командой. - Вождение вблизи мест, где может быть столкновение или присутствуют случайные свидетели. - Оператор может остановить движение, используя основную тормозную систему или другое подобное устройство, такое как F/N/R. - Мощность основной тормозной системы достаточна для необходимого увеличения силы торможения	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т
Полная потеря всех средств торможения для остановки. - Оператор может только позволить машине двигаться по инерции до остановки или в некоторых случаях для остановки использовать приспособление. - Для большинства колесных машин рулевое управление остается работоспособным, но не для машин с управлением направления движения и гусеничных машин	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*
Полная потеря рабочего и вспомогательного торможения. - Оператор все еще имеет по крайней мере один основной орган управления, чтобы остановить машину, такой как стояночный тормоз	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*

Продолжение таблицы А.5

Тип отказа	Категория опасности	Гусеничный траншеекопатель, ≤ 12 км/ч	Траншеекопатель на резиновом ходу, ≤ 12 км/ч	Машина горизонтально направленного бурения, управляемая сзади идущим оператором, ≤ 12 км/ч	Самоходная машина горизонтально направленного бурения, ≤ 12 км/ч	Колесный самоходный скрепер, приспособленный для движения по дорогам ≤ 40 км/ч	Самоходный каток, приспособленный для движения по дорогам ≤ 12 км/ч
Полная потеря замедлителя двигателя/передачи/электрического. - Поддержка функций рабочего, вспомогательного, и стояночного тормоза. Без предупреждения	Оп	Н/п	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	Н/п	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	Н/п	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т
Любой тормоз применяется оператором самопроизвольно, возможно при движении на максимальной скорости. - Машину заносит до остановки в большинстве случаев. Рулевое управление очень неэффективное	Оп	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ Θ/ $УЭЗ_т$ *a*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
Растормаживание тормоза поворота без команды. - Машина может перемещаться только очень медленно из-за утечки в гидравлической системе. - Оператор отсутствует	Оп	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Св	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
РУЛЕВОЕ УПРАВЛЕНИЕ							
Полная потеря всего рулевого управления (или рулевое управление выполняется самопроизвольно или совсем не выполняется при движении). - У оператора есть средства торможения для остановки машины. - Оператор не предупрежден заранее о потере рулевого управления	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	УПБ 3/ $УЭЗ_т$ *e*	УПБ 3/ $УЭЗ_т$ *e*
Потеря нормального рулевого управления при поддержке рулевого управления другой системой (или рулевое управление выполняется отчасти самопроизвольно, или чувствительность автомобиля к действиям водителя ограничена при всех движениях автомобиля). - У оператора есть средства торможения для остановки машины.	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ 2/ $УЭЗ_т$ *d*	УПБ 2/ $УЭЗ_т$ *d*

Продолжение таблицы А.5

Тип отказа	Категория опасности	Гусеничный траншеекопатель, ≤ 12 км/ч	Траншеекопатель на резиновом ходу, ≤ 12 км/ч	Машина горизонтально направленного бурения, управляемая сзади идущим оператором, ≤ 12 км/ч	Самоходная машина горизонтально направленного бурения, ≤ 12 км/ч	Колесный самоходный скрепер, приспособленный для движения по дорогам ≤ 40 км/ч	Самоходный каток, приспособленный для движения по дорогам ≤ 12 км/ч
Оператор не предупрежден заранее о потере рулевого управления. - Оператор может переключиться на альтернативное управление, например, с помощью джойстика							
ОБОРУДОВАНИЕ/ПРИСПОСОБЛЕНИЯ							
Нож дорожного струга, самосвальный контейнер, дорожный рыхлитель, ковш и другое оборудование начинают перемещаться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	Н/п
	Ат	Н/п	Н/п	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п
Вращение приспособления, функции экскаватора-погрузчика/экскаватора с обратной лопатой, поворот платформы экскаватора, движение стрелы экскаватора, рукояти экскаватора, ковшов экскаватора, которые могут достаточно далеко выдвинуться, стабилизаторов или функции мачты минипогрузчика начинают выполняться без команды. - Оператор находится на рабочем месте и может реагировать. - Оборудование или приспособления отключают рычагом отключения, выключателем или подобным средством	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	Н/п	УПБ Θ/ Н/т
	Св	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	УПБ 1/ $УЭЗ_т$ *c*	Н/п	Н/п
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	Н/п	Н/п
Функция автоматического управления ножом/ковшом/накопителем потеряна. Нож/ковш/накопитель перемещается беспорядочно или оказываются в нежелательном местоположении.	Оп	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Св	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*
	Ат	Н/п	УПБ 1/ $УЭЗ_т$ *b*	Н/п	Н/п	УПБ 1/ $УЭЗ_т$ *b*	УПБ 1/ $УЭЗ_т$ *b*

Окончание таблицы А.5

Тип отказа	Категория опасности	Гусеничный траншеекопатель, ≤ 12 км/ч	Траншеекопатель на резиновом ходу, ≤ 12 км/ч	Машина горизонтально направленного бурения, управляемая сзади идущим оператором, ≤ 12 км/ч	Самоходная машина горизонтально направленного бурения, ≤ 12 км/ч	Колесный самоходный скрепер, приспособленный для движения по дорогам ≤ 40 км/ч	Самоходный каток, приспособленный для движения по дорогам ≤ 12 км/ч
Предполагается, что оператор находится на рабочем месте, так как, уходя, он вынужден отключить функцию приспособления. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, перемещение и т. д.							
Функция автоматического управления ножом потеряна. Нож/ковш не будет двигаться автоматически. - Функцией является только движение вверх и вниз или поворот. - Функцией не является колебание, вращение, боковое перемещение и т. д.	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т
Быстроразъемное соединение позволяет приспособлению непроизвольно срываться	Оп	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Св	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
	Ат	Н/п	Н/п	Н/п	Н/п	Н/п	Н/п
ДВИГАТЕЛЬ							
Помпаж двигателя с незначительным воздействием на скорость продвижения, рулевое управление, торможение или приспособления	Оп	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Св	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т	УПБ Θ/ Н/т
	Ат	Н/п	УПБ Θ/ Н/т	Н/п	Н/п	УПБ Θ/ Н/т	УПБ Θ/ Н/т

Значения УПБ/УЭЗ$_т$ были определены при оценках риска для опасностей в наихудших случаях, связанных с данным видом машины. Рекомендуется, чтобы конкретное выполнение оценки риска для различных видов машин, специальных применений или других конкретных особенностей проводилось с использованием приложения А первой части ИСО 15998.

А.3.3 Схемы на рисунках А.2—А.5 являются примерами, демонстрирующими конфигурации систем, которые согласуются с обобщенными значениями УПБ/УЭЗ$_т$ таблиц А.2—А.5. Конечно, возможны другие конфигурации.

Пример блок-схемы системы для бульдозера на гусеничном ходу.

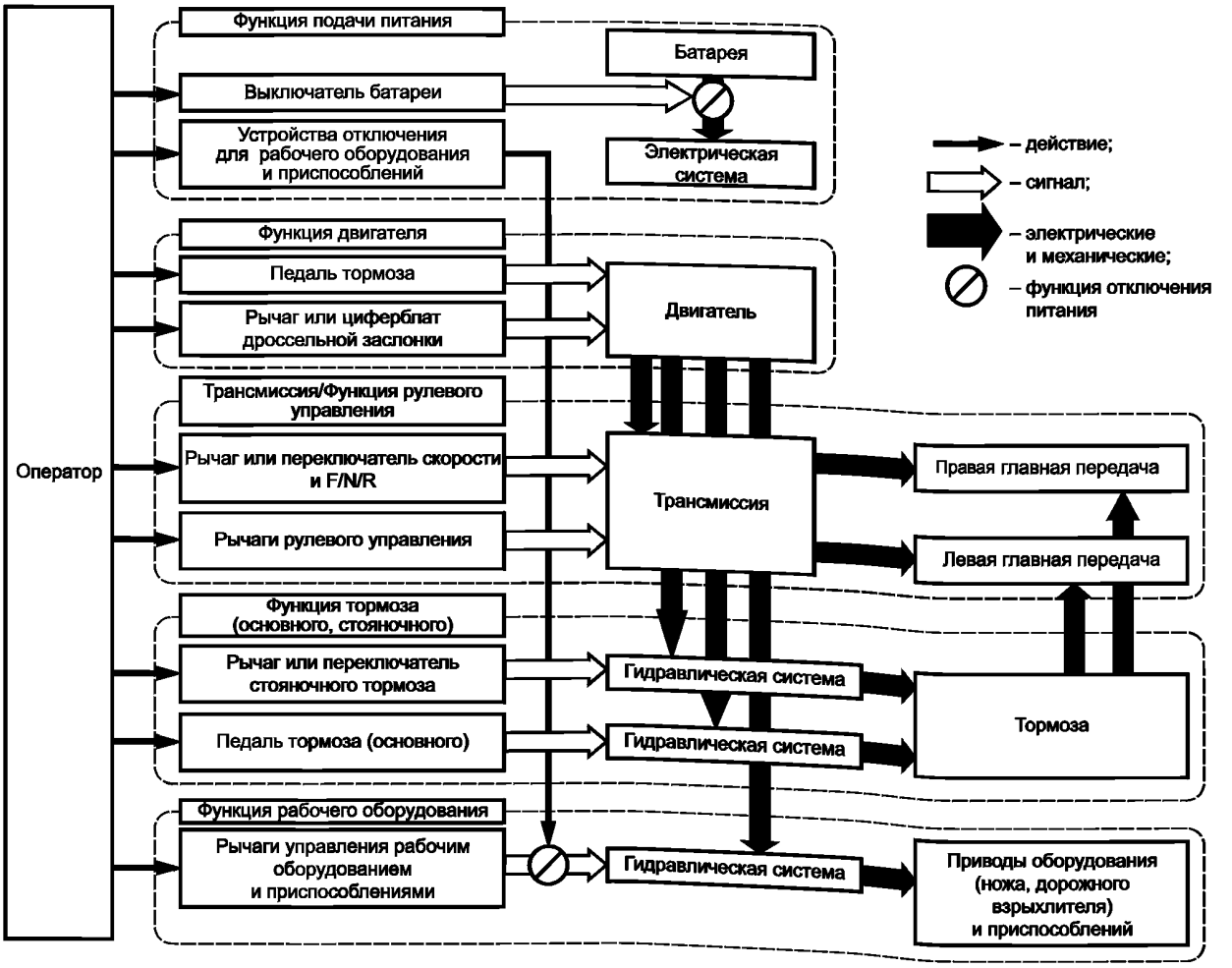


Рисунок А.2 — Бульдозер на гусеничном ходу

Пример блок-схемы системы для экскаватора на гусеничном ходу.

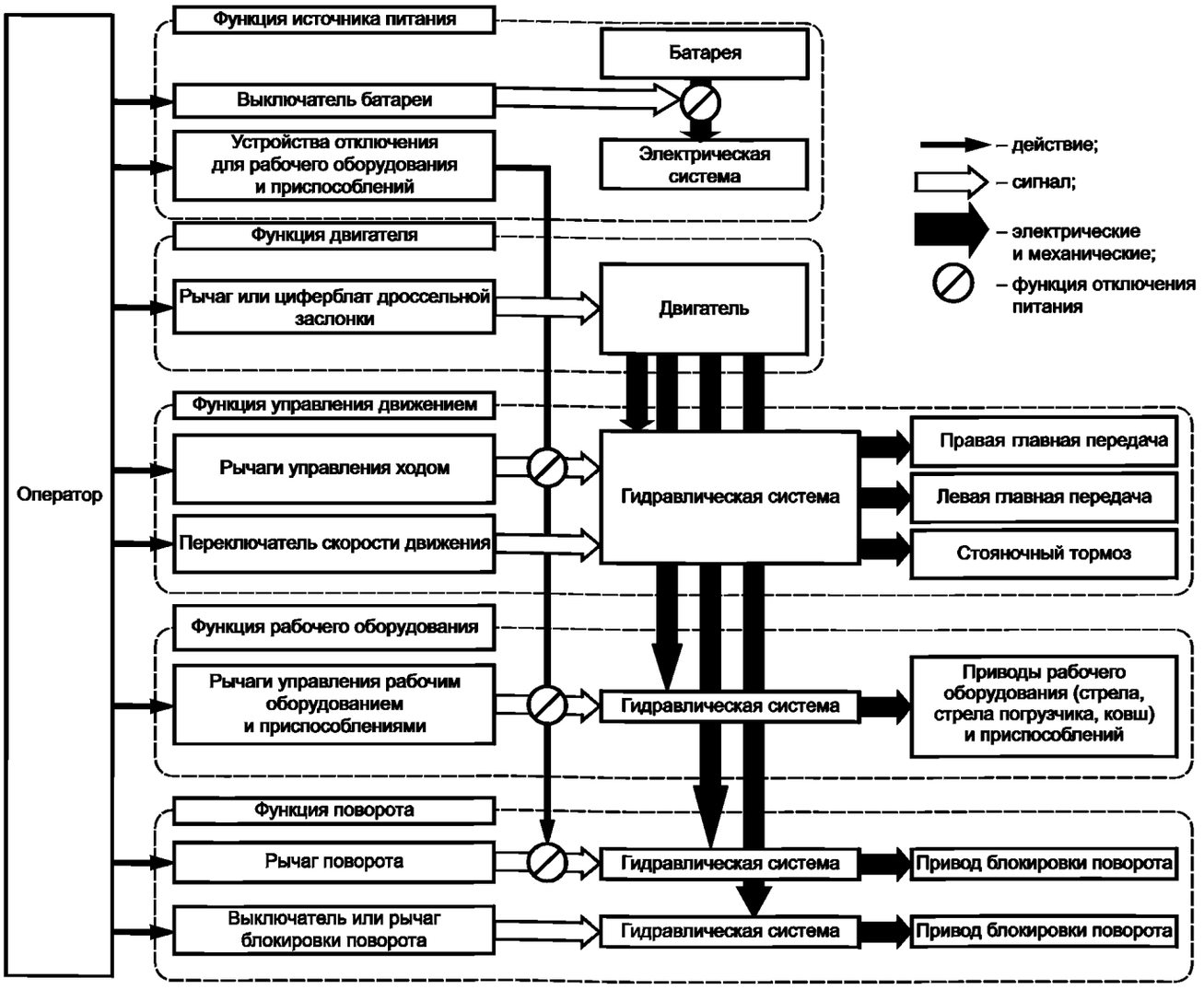


Рисунок А.3 — Экскаватор на гусеничном ходу

Пример блок-схемы системы для самосвала с шарнирно-сочлененной рамой/карьерного самосвала на жесткой раме.

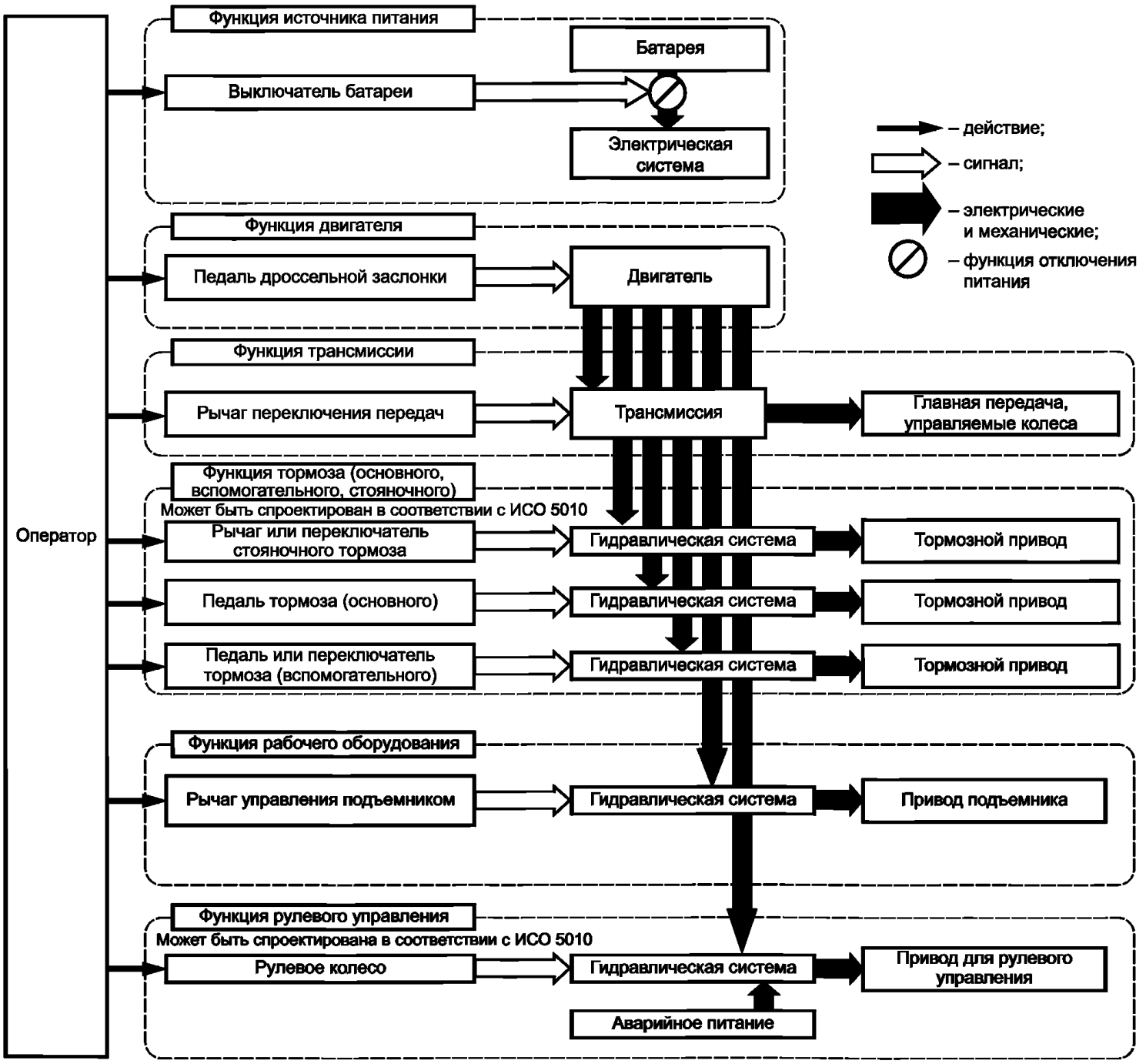


Рисунок А.4 — Самосвал с шарнирно-сочлененной рамой/карьерный самосвал на жесткой раме

Пример блок-схемы системы для шарнирно-сочлененного колесного погрузчика.

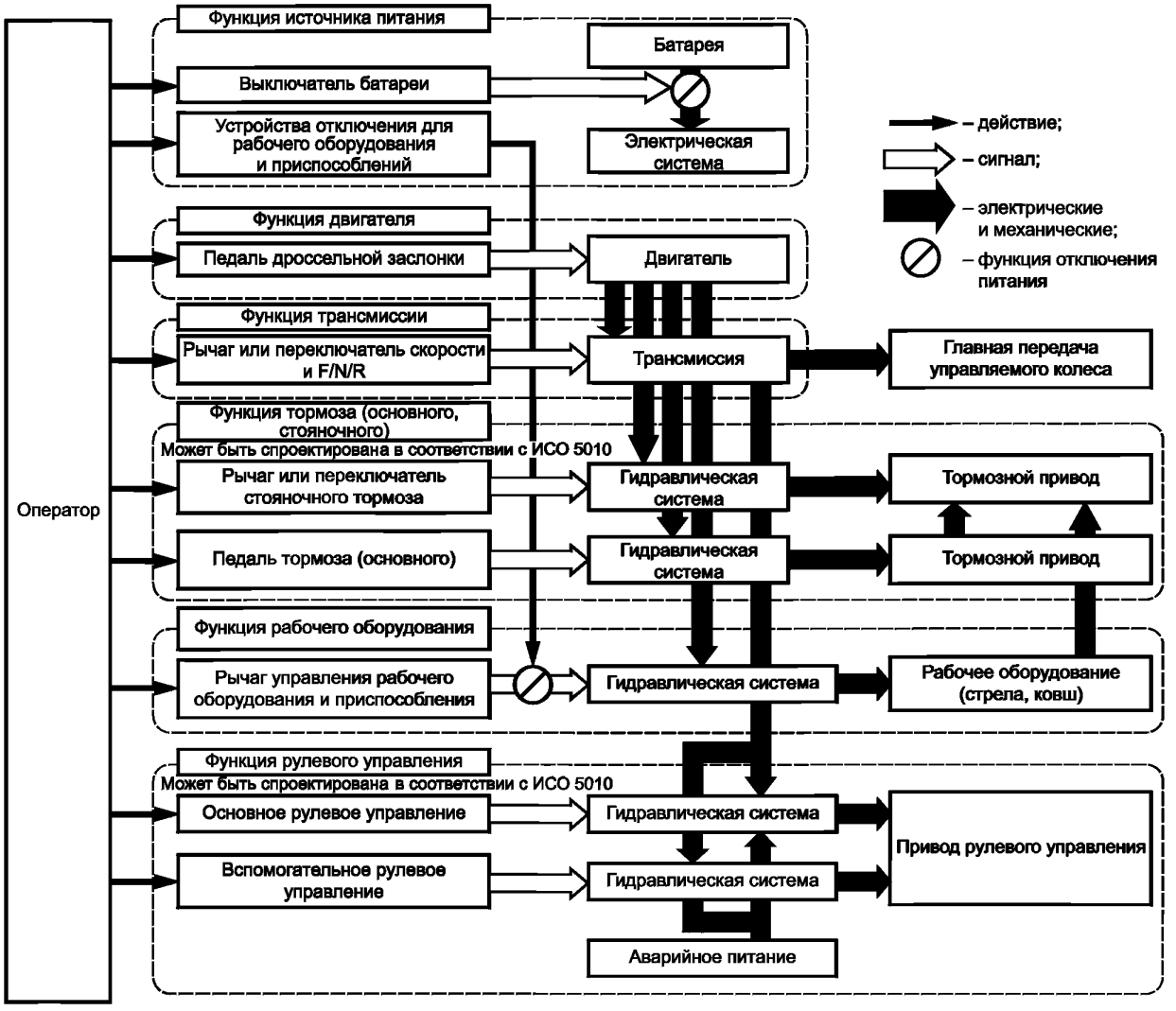


Рисунок А.5 — Шарнирно-сочлененный колесный погрузчик

А.4 Снижение риска СУМ

Для снижения опасностей могут использоваться различные методы (см., например, ИСО 13849-1:2006, 4.2). Для оценки риска строительных машин могут непосредственно использоваться рассмотренные ниже методы, но может потребоваться и дальнейший анализ. Неисправные части системы управления, такие как система торможения, рулевое управление, ходовая система или управление приспособлением, могут иметь риски, ослабляемые при помощи рассмотренных ниже методов. При этом общее значение УПБ/УЭЗ$_т$ остается на прежнем высоком уровне, но определенные комбинации характеристик позволяют для частей системы иметь более слабые требования.

Примечания

1 Комбинации систем с более низкими значениями УПБ/УЭЗ$_т$, которые могут быть объединены электронными способами, ниже не описаны. В МЭК 61508-6:2010, приложение В, рассматривается этот случай, когда вся система управления остается с высоким значением УПБ/УЭЗ$_т$.

2 Различие между системой с УПБ 1/УЭЗ$_т$ *b* и с УПБ 2/УЭЗ$_т$ *d* состоит в том, что надежность системы с УПБ 2 в 10 раз выше относительно определенного вида нежелательных отказов.

А.4.1 Избыточные системы управления

Операторы могут менять управляющие приводы, чтобы предотвратить несчастные случаи. Для машин с избыточными средствами управления, которые приблизительно воспроизводят функции друг друга, можно понизить значение УПБ/УЭЗ$_т$ на 1 для каждой из подсистем, составляющих полную систему (при условии, что конкретный рассматриваемый вид отказа не приводит к одновременному сбою в обоих основных органах управления).

Примеры

1 Полная потеря функций основной и вспомогательной системы торможения соответствует значению УПБ 2/УЭЗ$_т$ d для самосвала с шарнирно-сочлененной рамой. Если есть стояночный тормоз со способностью динамической остановки согласно ИСО 3450, то требование для основного тормоза может быть понижено до УПБ 1/УЭЗ b.

2 Полная потеря всей системы рулевого управления (например, рабочих и аварийных источников питания системы рулевого управления) соответствует значению УПБ 3/УЭЗ$_т$ e для большинства колесных машин, двигающихся по дороге со скоростью > 25 км/ч. Машина может быть оснащена механической/гидравлической системой управления в качестве основной системы рулевого управления и электрогидравлической ручкой (джойстиком) управления в качестве дополнительной системы рулевого управления. В этом случае для электрической системы управления с помощью джойстика приемлемо требование УПБ 2/УЭЗ d, если эти системы рулевого управления удовлетворяют ИСО 5010. Это комбинация отдельных систем рулевого управления с меньшими значениями УПБ/УЭЗ, работающих вместе, которая обеспечивает для всей системы значение УПБ 3/УЭЗ$_т$ e.

3 Если есть дополнительный способ рулевого управления, например, если электрогидравлическая система рулевого управления с помощью джойстика и механическая/гидравлическая система рулевого управления являются основными системами рулевого управления, то для электрической системы управления с помощью джойстика приемлемо требование УПБ 2/УЭЗ d, если эти системы рулевого управления удовлетворяют ИСО 5010. Это комбинация отдельных систем рулевого управления с меньшими значениями УПБ/УЭЗ, работающих вместе, которая обеспечивает для всей системы значение УПБ 3/УЭЗ$_т$ e.

А.4.2 Заблаговременное предупреждение

Виды отказов, которые происходят с соответствующим заблаговременным предупреждением, чтобы безопасно остановить машину, уменьшая тем самым опасность, дают возможность уменьшить значение УПБ/УЭЗ$_т$ на один уровень для системы управления (при условии, что конкретный рассматриваемый вид отказа не приводит к одновременному сбою и в основной функции, и в функции предупреждения).

Пример — Полная потеря основной и аварийной системы управления соответствует значению УПБ 3/УЭЗ$_т$ e для колесных машин, двигающихся по дороге. Если предупреждение появилось заблаговременно настолько, чтобы обеспечить оператору безопасное управление машиной до ее остановки, то сама система рулевого управления должна быть разработана только в соответствии с требованием УПБ 2/УЭЗ d.

А.4.3 Вывод из эксплуатации

Управление выводом из эксплуатации (автоматически или принудительно) оператором может значительно снизить риск неуправляемого движения, когда оператор покидает пульт оператора. Поэтому значение УПБ/УЭЗ$_т$ основного управления может быть меньше на 1 в отношении травм людей, стоящих на земле, и риска от неуправляемого движения.

Пример — Если неисправность в основной ходовой системе со значением УПБ 1/УЭЗ$_т$ b обнаружена другой системой мониторинга, которая способна безопасно перевести основную ходовую систему в нейтральное состояние, то вся система будет иметь УПБ 1, но «основная» часть ходовой системы и систем мониторинга могут каждая иметь УПБ Θ / УЭЗ a (где интенсивность отказов каждой системы меньше 10^{-4}/ч).

А.4.4 Противодействие

Некоторые виды отказов системы управления таковы, что оператор может остановить неуправляемое движение в одном направлении, применив команду для встречного направления. Противодействие может значительно снизить риск неуправляемого движения, если дополнительно есть метод управления принудительной блокировкой, такой как стояночный тормоз или использование гидравлических средств.

Пример — Если положение нейтрального состояния органа управления сдвигается от центральной точки для переменного входного устройства, то оператор может переместить устройство ввода во встречное направление, чтобы противостоять неисправности. Более конкретный пример — на вилочный погрузчик, где ходовая система может качаться в зависимости от входного сигнала датчика (или наклона рабочего места). Это может вызвать необходимость небольшого увеличения тяги машины, чтобы удержать ее в неподвижном состоянии. Движение машины, когда управление ходовой системой находится в нейтральном положении, все еще характеризуется значением УПБ 1/УЭЗ$_т$ b для всей системы средств управления, но режим отказа датчика не рассматривают со значением УПБ 1/УЭЗ$_т$ b, а, скорее, со значением УПБ Θ/УЭЗ a. Точно так же, если стрела крана на машине

дрейфует вниз из-за дрейфа датчика (или гидравлической утечки), то это также значение УПБ Θ/УЭЗ а. В обоих случаях предполагается, что оператор будет в состоянии приспособиться к этим ситуациям и имеет возможность блокировки машины, чтобы предотвратить их появление.

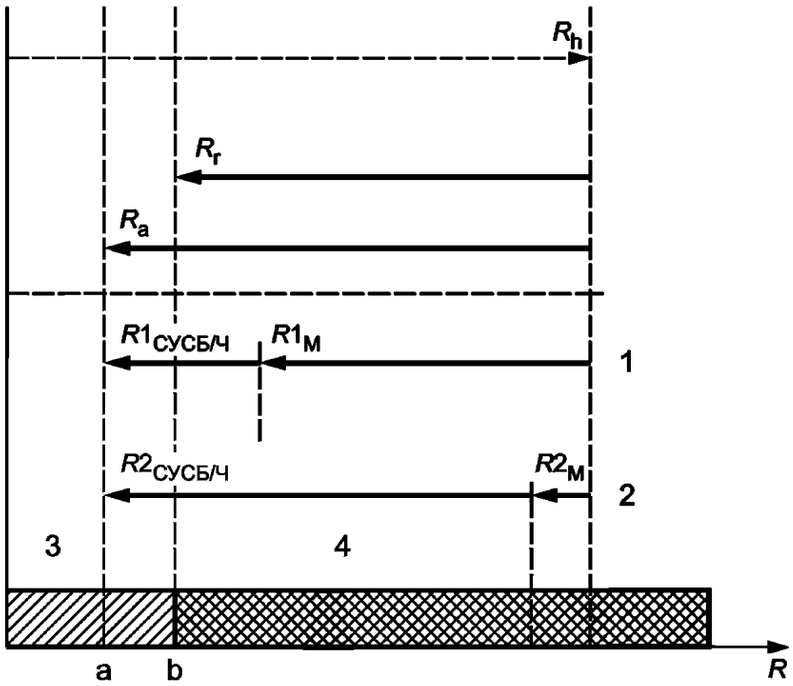
А.5 Схема снижения риска

Можно использовать несколько методов, чтобы определить, удовлетворяют ли технические требования СУСБ/Ч концепции безопасности, определенной для УПБ и связанного с ним $УЭЗ_т$. Эти методы описаны подробно в нормативных ссылках ИСО 15998.

Стратегия снижения риска для СУСБ/Ч охватывает весь жизненный цикл машины и включает концепцию безопасности. Процесс анализа опасностей и снижения риска для машины требует, чтобы опасности были устранены или уменьшены с помощью иерархии следующих мер.

А.5.1 Процесс снижения риска, используемый для достижения допустимого риска (адекватное снижение риска)

Один важный метод, связанный с концепцией безопасности, основан на реализации процесса снижения риска. Снижение риска может быть достигнуто применением различных мер защиты (и для СУСБ/Ч, и для не СУМ) с конечным результатом достижения условия безопасности (см. рисунок А.6).

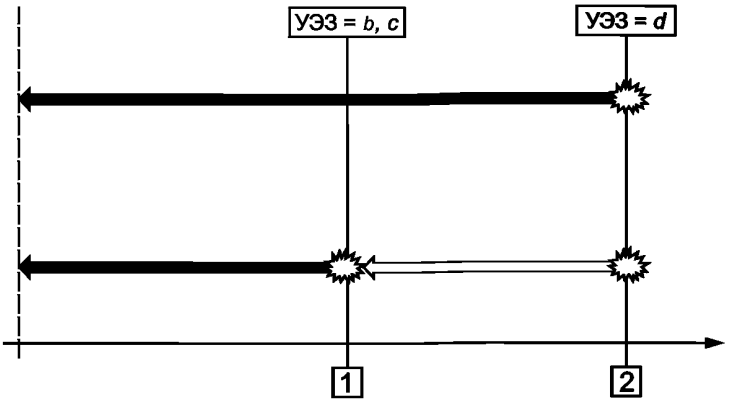


R_h — для конкретной опасной ситуации значение риска до применения мер защиты;
R_r — снижение риска, требуемое от мер защиты;
R_a — фактическое снижение риска, достигнутое с использованием мер защиты;
1 — решение 1: наибольшая часть снижения риска из-за мер защиты, отличных от СУМ (например, механических мер), и небольшая часть снижения риска из-за СУСБ/Ч;
2 — решение 2: наибольшая часть снижения риска из-за СУСБ/Ч (например, блокировки) и небольшая часть снижения риска из-за мер защиты, кроме СУМ (например, механических мер);
3 — достаточно сниженный риск;
4 — недостаточно сниженный риск;
R — риск;
$R1_{СУСБ/Ч}$, $R2_{СУСБ/Ч}$ — снижение риска от функции безопасности, выполненное с помощью СУСБ/Ч;
$R1_М$, $R2_М$ — снижение риска от защитных мер, кроме СУСБ/Ч (например, механических мер);
a — остаточный риск получен, используя решения 1 или 2;
b — достаточно сниженный риск.

Рисунок А.6 — Анализ процесса снижения риска для каждой опасной ситуации

Другой способ проиллюстрировать эту концепцию для неэлектрической тормозной системы СУМ и для объединенной тормозной системы с механической и электрогидравлической СУМ см. в таблице А.6.

Таблица А.6 — Примеры снижения риска для систем торможения

Допустимый риск	
	**Примеры**
	Неэлектрическая(ие) тормозная(ые) система(ы)
	Полностью избыточная вспомогательная тормозная система с дополнительным динамическим стояночным тормозом как резерв к вспомогательным тормозам
	Комбинация электрогидравлических стояночной и вспомогательной тормозных систем и основной неэлектрической тормозной системы
	Проверенные общие компоненты для электрогидравлической стояночной/ вспомогательной тормозной системы
	Риск представлен через УПБ

На иллюстрации таблицы А.6 показано, что в результате оценки риска было получено, что независимо от типа СУМ требуется уровень УПБ 2/УЭЗ$_т$ *d*. Машина оснащена традиционной неэлектрической тормозной системой в соответствии с уровнем типа С стандарта безопасности, в данном случае ИСО 3450 (отображено серым цветом). Неэлектрическая тормозная система является трехканальной и обеспечивает безопасное состояние для любого одиночного отказа, что дает значение УЭЗ, которое превышает УПБ 2/УЭЗ$_т$ *d*.

Вторая система (в черно-белых тонах) включает электрогидравлическую вспомогательную и стояночную тормозные системы и неэлектрическую основную тормозную систему. Эта комбинация также является трехканальной и обеспечивает безопасное состояние для любого одиночного отказа, что дает значение УЭЗ$_т$, которое превышает УПБ 2/УЭЗ$_т$ *d*. Электрогидравлическая часть системы оценена как имеющая значение УПБ 1/УЭЗт *b* и состоит из проверенных на практике компонентов.

Землеройные машины обычно оснащены подобными многоканальными системами рулевого управления. В качестве аналогичного примера можно предложить объединенную систему рулевого управления, состоящую из электрогидравлической системы рулевого управления, имеющей УПБ 1/УЭЗ *b*, и механической гидравлической многоканальной системы рулевого управления, имеющей УПБ 2/УЭЗ *d*. Комбинация обеих этих систем обладает адитивностью и привела бы к значению УПБ 3/УЭЗ$_т$ *e*.

А.5.2 Снижение риска с помощью защитного устройства оператора

Риски, связанные с тем, что оператор покинул пульт управления минипогрузчика с опущенной стрелой, оцениваются значением УПБ 1/УЭЗ$_т$ *c*. Если есть блокировочное приспособление, имеющее рычаг управления, которое принудительно блокирует гидросистему (т. е. блокирует положение стрелы независимо от основной системы управления, когда оператор покидает пульт управления), то комбинация двух отдельных систем основной и рычагом управления блокировочной может удовлетворять требованиям УПБ 1/УЭЗ$_т$ *c*. Основное управление стрелой оператором может тогда иметь более низкое значение УПБ Θ / Н/т.

Примечание — Риск получения травмы сторонним свидетелем не уменьшается этим рычагом управления и оценивается значением УПБ 1/УЭЗ *b*. Поэтому полное снижение риска для основного управления не может быть реализовано до тех пор, пока для снижения опасностей стороннего свидетеля в проекте не будут предусмотрены другие меры.

Приложение В
(справочное)

Руководство по формированию концепции безопасности в соответствии с ИСО 15998

В таблице В.1 представлен пример, описывающий концепцию безопасности для коробки передач ходовой системы колесного погрузчика, управляемой одним из блоков СУМ и рычагом оператора электронного управления переключением передач. Как одна из частей процесса эта информация может быть использована, чтобы продемонстрировать соответствие связанных с безопасностью блока трансмиссии СУМ и переключателя электронного управления требованиям ИСО 15998:2008 пункты 4.2, первый абзац, 4.3, 4.4, 4.5, 4.7, 5.2, 5.3, 5.4 и 5.5 (и соответствующим подразделам ИСО 15998-1). Каждая СУСБ/Ч для колесного погрузчика нуждается в подобном описании концепции безопасности. Для большинства реальных систем требуются диаграммы и схемы, но в данном случае ради краткости они опущены.

Таблица В.1 — Колесный погрузчик. Подсистема управления переключением направления хода машины. Пример

Элементы описания концепции безопасности из ИСО 15998:2008 [ИСО 15998-1]	Э/Э/ПЭ система. Пример. Подсистема управления коробкой передач машины	
4.2 (первый пункт маркированного списка) Список всех устройств системы, используемых функциями, связанными с безопасностью	Коробка передач: с сервоприводом переключения, с гидротрансформатором. Соленоиды для управления передаточным механизмом и направлением передачи. *F*/*N*/*R* (вперед/нейтральное положение/назад) рычаг включения направления, выполненный на трех переключателях. Жгуты проводов для электрического соединения в системе. Электропитание. Генератор переменного тока и аккумулятор	
4.3 Описание основных функций	Для направлений *F*/*N*/*R* реализовано три цифровых входа:	
	a) сигнал «вперед» (*F*)	0,0 – 0,5 V = не в *F*, 4,5 – 5,0 V = *F*
	b) сигнал «нейтральное положение» (*N*)	0,0 – 0,5 V = не в *N*, 4,5 – 5,0 V = *N*
	c) сигнал «назад» (*R*)	0,0 – 0,5 V = не в *N*, 4,5 – 5,0 V = *N*
	Соленоиды направления выхода	
	Соленоид движения вперед Соленоид движения назад	0,0 V = *N* или *R*, 24 V = *F*, 0,0 V = *N* или *F*, 24 V = *R*
	Незамкнутая система. Погрузчик может двигаться вперед, назад и быть в нейтральном положении. Он имеет четыре передних скорости и три задних. Максимальная скорость составляет 40 км/ч	
4.4 Анализ и оценка риска	Оценка риска движения машины, когда оператор установил положение *N*, указывает на значение УПБ 1/*УЭЗ*$_{т}$ *b*	
4.5 Рабочие характеристики для концепции безопасности	Избыточность. Входные датчики *F*/*N*/*R* должны иметь следующие допустимые значения: - если вход *F* = 4,5 – 5,0 В, то *N* и *R* должны оба быть в диапазоне 0,0—0,5 В; - если вход *N* = 4,5 – 5,0 В, то *F* и *R* должны оба быть в диапазоне 0,0—0,5 В; - если вход *R* = 4,5 – 5,0 В, то *N* и *F* должны оба быть в диапазоне 0,0—0,5 В.	

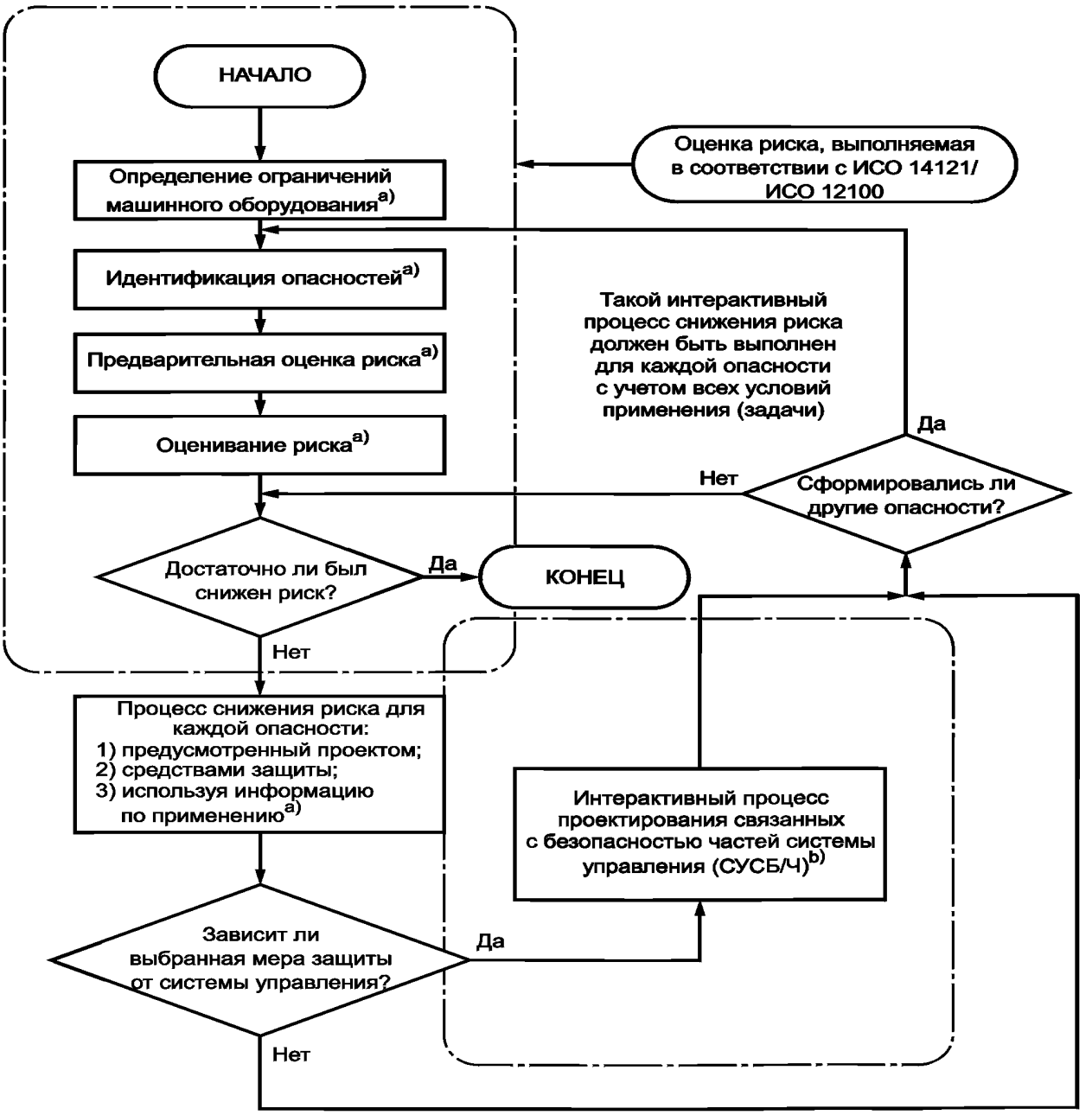
Окончание таблицы В.1

Элементы описания концепции безопасности из ИСО 15998:2008 [ИСО 15998-1]	Э/Э/ПЭ система. Пример. Подсистема управления коробкой передач машины
	Обнаружение сбоев. Если входные сигналы *F/N/R* не находятся в диапазоне допустимых значений более 50 мс, то считается, что обнаружен сбой. Каждый раз, когда на любом из входов *F/N/R* значение < 0,0 В, или между 0,5 В и 4,5 В, или > 5,0 В, то фиксируется обнаружение сбоя. Безопасное состояние Если обнаружен сбой *F/N/R*, то контроллер коробки передач полностью отключает соленоиды, отвечающие за движение вперед и назад. Потеря питания всей машины, контроллера коробки передач, *F/N/R* или в соленоидах приводит к возвращению машины в нейтральное положение. Оценки FTA/FMEA/рисков (не рассматриваются) показывают, что автоматическое возвращение к *N* на погрузчике обладает низким риском. У оператора все еще будут в распоряжении полностью функционирующие тормозные системы. Комплект измерительных кабелей, подсоединенный к *F/N/R*, может моделировать все допустимые условия и условия сбоев, связанные с многоканальностью и некорректными диапазонами напряжения. Оценки FTA/FMEA/рисков (не рассматриваются) показывают, что немедленное переключение передачи в положение *N* на погрузчике обладает низким риском. Никакой переход не нужен. У оператора все еще будут в распоряжении полностью функционирующие тормозные системы. Для удаления машины от места работы в руководстве по эксплуатации представлены буксирующие приспособления
4.7 Функции аварийной остановки	Аварийная остановка не требуется в концепции безопасности. Тем не менее машина обеспечена функцией аварийной остановки с помощью клавишного переключателя, который обладает способностью возвращать машину в состояние *N* в любых условиях в любое время
5.2 Предотвращение сбоев и управление сбоями	Должен быть выполнен анализ согласно 5.2, поскольку система с контроллером коробки передач характеризуется значением УПБ 1/УСЗ$_т$ *b*.
5.3 Требования к программируемым электронным системам (ПЭС)	Порограммное обеспечение в соответсвии со значением УПБ 1/УСЗ$_т$ *b*
5.4 Ошибки и отказы электронных компонентов, учитываемые в СУМ	Безопасное состояние Если обнаружен сбой *F/N/R*, то контроллер коробки передач полностью отключает соленоиды, отвечающие за движение вперед и назад. Потеря питания всей машины, контроллера коробки передач, *F/N/R* или в соленоидах приводит к возвращению машины в нейтральное положение. Оценки FTA/FMEA/рисков (в настоящем стандарте не рассматриваются) показывают, что немедленное переключение передачи в положение *N* на погрузчике обладает низким риском. Никакой переход не нужен. У оператора все еще будут в распоряжении полностью функционирующие тормозные системы
5.5 Процедура повторного запуска	Как только машина вошла в *N* из-за нарушенного условия, она остается в *N* до тех пор, пока из контроллера коробки передач не получена реальная команда *N*. После того как реальная команда *N* получена, машина способна еще раз перейти к *F* или *R* по команде оператора

Приложение С
(справочное)

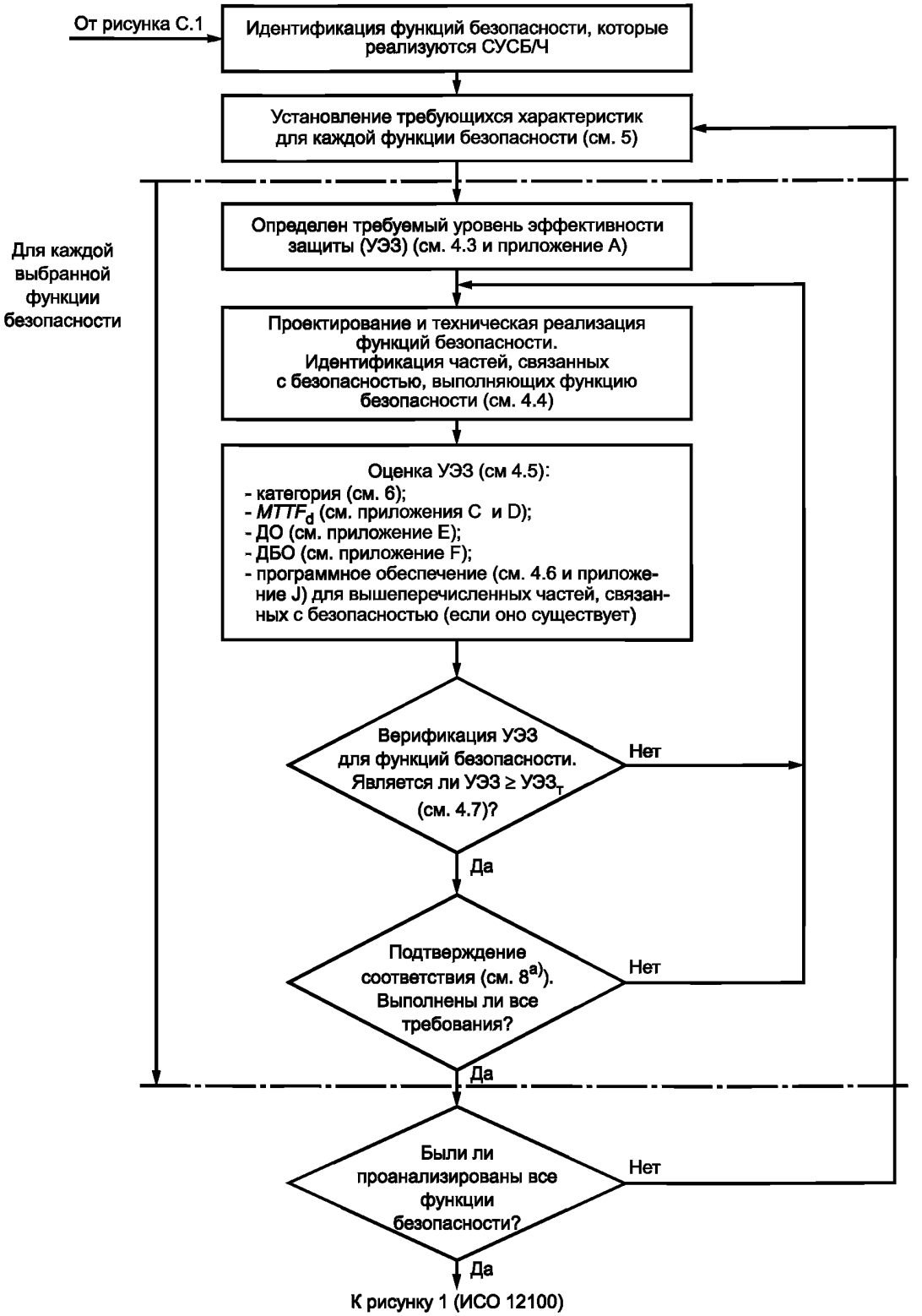
Соответствие с ИСО 15998

В настоящем приложении кратко изложен один из способов выполнения соответствия землеройных машин требованиям ИСО 15998, используя блок-схемы из ИСО 13849-1. См. также ИСО 12100 (другой способ представлен в МЭК 61508-1:2010, рисунок 2).



[a)] См. ИСО 12100.
[b)] См. рисунок С.2 (ИСО 13849-1:2006, рисунок 3).

Рисунок С.1 — Блок-схема обобщенного процесса обеспечения соответствия с ИСО 15998 (ИСО 13849-1:2006, рисунок 1)



[a] Все ссылки в диаграмме указывают на ИСО 13849-1:2006.

Рисунок С.2 — Блок-схема обобщенного процесса. Итеративный процесс проектирования связанных с безопасностью частей систем управления (СУСБ/Ч) (ИСО 13849-1:2006, рисунок 3)

Приложение D
(справочное)

Соответствие с ИСО 15998 на примере землеройной машины

Таблица D.1 — Карта контрольных проверок по ИСО 15998. Пример

ИСО 15998-1:2008/ИСО 15998-1. Общие требования	Функция	Выполнено (Да/Нет/%)	Критерии соответствия требованиям и критерии верификации
Описание СУСБ/Ч содержит следующее:			
4.2.1 Список всех системных блоков (т. е. блок управления передачей), используемых связанными с безопасностью функциями	Разработка изделия		Список всех связанных с безопасностью контроллеров для машины. Использовать электронную спецификацию машины
4.2.2 Схема связи устройств (т. е. монтажная схема) и системных блоков (контроллеров), представляющая связанные с безопасностью функции, реализуемые СУМ	Разработка изделия		Техническое руководство. Гидравлические и электрические схемы машины
4.2.3 Электрические соединения системы изображаются соотвествующим способом (т. е. принципиальной схемой) и должны однозначно классифицировать каждое соединение устройства (например, провода) с системными блоками (например, маркировкой выводов)	Разработка изделия		Техническое руководство. Электрические и монтажные схемы машины
4.2.4 Системные блоки (блоки управления, маркируются идентификаторами (например, числами, символами, знаками) так, чтобы могло быть проверено соответствие между принципиальной схемой системы и СУМ, установленной в машине	Разработка изделия		Монтажные схемы машины
4.2.5 Для соответствия системных блоков документации, описывающей основную функцию, концепцию безопасности и интерфейсы, используются идентификаторы	Разработка изделия		Монтажные схемы с идентифицированными соединениями
4.2.6 Описание системы также включает требования к условиям окружающей среды, в которой предполагается эксплуатация машины: - климатические условия (температура, влажность); - механические условия (вибрация, удар); - коррозийные условия (солевой туман, загазованность); - электрические условия (не под напряжением, под напряжением линий передач); - электромагнитные условия; - скачки напряжения питания	Разработка изделия		Технические требования на машину, программное обеспечение, аппаратные средства и требования к СУМ

Продолжение таблицы D.1

ИСО 15998-1:2008/ИСО 15998-1. Общие требования	Функция	Выполнено (Да/Нет/%)	Критерии соответствия требованиям и критерии верификации
4.3 Основная функция СУМ определена в кратком описании, которое может сопровождаться графическим материалом, таким как функциональные схемы или блок-схемы, и оно содержит следующее:			Технические требования на машину, программное обеспечение, аппаратные средства и требования к СУМ. Блок-схема с описаниями функции каждого блока. Принципиальная схема для внешних соединений и описание внешних сигналов
4.3.1 Перечень типов и значений входных сигналов СУМ	Разработка изделия		Требования к СУМ
4.3.2 Перечень типов и значений управляемых выходных сигналов СУМ	Разработка изделия		Требования к СУМ
4.3.3 Управление по замкнутому/разомкнутому контуру, используемые данные/датчики	Разработка изделия		Требования к СУМ
4.3.4 Допустимый рабочий и регулируемый диапазоны	Разработка изделия		Требования к СУМ
4.4 Чтобы оценить опасности, должны быть выполнены анализ и оценка рисков СУМ, используя описание систем в соответствии с 4.2	Разработка и верификация изделия		Используйте ИСО 13849-1:2006, таблицы А.2—А.5, в которых представлены обобщенные значения УПБ/УЭЗ$_т$, полученные из оценок риска, или эквивалентные им
4.5 Критерии эффективности базовой концепции и функции системы, определенные производителем для концепции безопасности машины, учитываются при разработке и производстве СУМ. Концепция безопасности включает в себя все меры, которые предусматривают безопасное функционирование при ненормальном режиме работы. Они должны быть перечислены общепринятым способом, как в следующих примерах: - резервирование; - процедуры выявления сбоев; - безопасное состояние, которое может инициироваться, например, функцией аварийного движения [функцией(ями) снижения производительности системы или замещающей(ими) функцией(ми), функцией замещения для автоматической коробки переключения передач вместе с сообщением оператору: например сигналом тревоги, индикатором, снижением номинальных рабочих характеристик]	Разработка и верификация изделия		Документально оформленные требования к СУМ, включающие концепцию безопасности. Все соответствующие методы FMEA для проверки концепции безопасности Документально оформленные требования к СУМ Документально оформленные требования к СУМ Документально оформленные требования к СУМ
4.6.1 Условия окружающей среды, в которых используются машины, являются основой для спецификации СУМ	Верификация изделия		Общие технические условия для машины, программного обеспечения, аппаратных средств и требования к СУМ
4.6.2 Температура и влажность окружающей среды	Верификация изделия		Соответствие внутренним методам и процедурам испытаний компании при проверке изделий с электрическими и электронными компонентами и систем, которые не хуже указанных в ИСО 15998-1

Продолжение таблицы D.1

ИСО 15998-1:2008/ИСО 15998-1. Общие требования	Функция	Выполнено (Да/Нет/%)	Критерии соответствия требованиям и критерии верификации
4.6.3 Степень защиты (IP-код)	Верификация изделия		Соответствие внутренним тестам при верификации электрических и электронных компонентов и систем
4.6.4 ЭМС	Верификация изделия		Соответствие с ИСО 13766 и внутренними критериями компании при тестировании на ЭМС, которые превышают критерии из ИСО 15998-1 и ИСО 1376
4.6.5 Механическая вибрация	Верификация изделия		Соответствие внутренним тестам при верификации электрических и электронных компонентов и систем
4.6.6 Механический удар	Верификация изделия		Соответствие внутренним тестам при верификации электрических и электронных компонентов и систем
5.1 СУМ с минимальным значением УПБ 1/УЭЗ$_т$ *b*, а также с УПБ 1—3/УЭЗ$_т$ *b*—*e* должны удовлетворять следующим дополнительным требованиям в соответствии с оценкой риска:	Разработка и верификация изделия		Соответствие обеим частям ИСО 15998
5.2 Предотвращение сбоев и управление сбоями	Разработка и верификация изделия		Спецификация MSC, включающая предотвращение сбоев и управление сбоями, как определено в разделе 5 (согласно 5.3, 5.4 и 5.5 настоящей таблицы). Сертификация программы обеспечения качества для изготовителя на соответствие требованиям от ИСО 9001 до ИСО 9004 или аналогичных
5.3 Согласно требованиям к программируемым электронным системам (PES) разработка и оценка соответствия программного обеспечения должны быть выполнены соответствующими мерами (см., например, МЭК 61508-3 или ИСО 13849-1:2006)	Разработка и верификация изделия		Соответствие внутренним требованиям компании — документально оформленной спецификации встроенного программного обеспечения для спецификации требований к программному обеспечению; внутри компании — оценка для подтверждения соответствия системного программного обеспечения машины
5.4 Сбои или отказы электронных компонентов, используемых в СУМ. В случае сбоя или отказа электронных компонентов, используемых в СУМ, переход в безопасное состояние осуществляется в соответствии с оценкой риска	Разработка и верификация изделия		Документально оформленные требования к СУМ, включающие концепцию безопасности и безопасное состояние (примеры погрузчика в таблице D.1)
5.5 Процедуры перезапуска. Автоматический перезапуск в случае исчезающей ошибки не разрешен, если с помощью оценки риска показано, что обеспечивается безопасный режим работы	Разработка и верификация изделия		Документально оформленные требования к СУМ, включающие описание концепции безопасности и безопасного состояния
6 Документация. Изготовитель хранит согласно своим правилам регистрации и хранения данных всю соответствующую документацию с общими требованиями по безопасности СУМ согласно требованиям первой части ИСО 15998, раздел 4	Разработка и верификация изделия		Упомянуто выше в 4.2—4.6.5

Окончание таблицы D.1

ИСО 15998-1:2008/ИСО 15998-1. Общие требования	Функция	Выполнено (Да/Нет/%)	Критерии соответствия требованиям и критерии верификации
7.1 Тесты, представленные в 7.2, предназначены для удовлетворения общим требованиям к СУСБ/Ч в соответствии с первой частью ИСО 15998, раздел 4. Однако также разрешены альтернативные средства проверки. Тесты могут быть выполнены последовательно на уровне блоков СУМ (например, для сборочных узлов)	Верификация изделия		Тестовая проверка согласно разделу 7 первой части ИСО 15998 (см. специфические особенности ниже)
7.2 Тесты СУСБ/Ч. Содержание тестов: проверка основных функций согласно 4.2 и 4.3; проверка перехода в безопасное состояние (см. 5.4); функциональные испытания на температуру и влажность в соответствии с 4.6.2 и 7.2.2; испытания на ЭМС согласно 4.6.4; испытания на удар и вибрацию согласно 4.6.5, 7.2.3, 7.2.4	Верификация изделия		Собственные проверочные тесты компании и требования к формальным испытаниям для электрических деталей и электронных компонентов и систем; внутренние процедуры компании для электрических функциональных испытаний на уровне машины; внутренние процедуры компании оценки системного программного обеспечения машины; безопасность изделия и соблюдение функциональной проверки обеспечиваются соответствием с ИСО 13766 и первой части ИСО 15998
7.2.2 Испытания на функционирование СУСБ/Ч при температуре и влажности, заданных в 7.2.2, на соответствие эксплуатационным требованиям, представленным в 4.6.2 первой части ИСО 15998	Верификация изделия		Соответствие внутренним для компании методам и процедурам проверочных испытаний изделий для электрических и электронных компонентов и систем, которые превышают критерии из первой части ИСО 15998-1. Испытательные тесты, которые «прошли», сохраняются
7.2.3 Вибрационные испытания должны быть выполнены для компонентов СУМ в той же самой позиции и с тем же самым способом крепления, который применяется в машине	Верификация изделия		См. выше
7.2.4 Испытания на удары должны быть выполнены либо в соответствии с техническими требованиями изготовителя, либо в соответствии с руководством МЭК 60068-2-27	Верификация изделия		См. выше
7.2.5 Дополнительные функциональные тесты для СУСБ/Ч. Должны быть выполнены основной функциональный тест программного обеспечения и расширенный функциональный тест в соответствии с МЭК 61508-7. Примечание — Допускаются альтернативные средства для проверки, кроме представленных в МЭК 61508	Верификация изделия		Соответствие проверочным тестам для изделия и формальным отчетам испытаний при электрических функциональных испытаний на уровне машины

Приложение Е
(справочное)

Качественный подход к управлению случайными отказами аппаратных средств

Е.1 Цель

Цель данного приложения — описать, как можно использовать МЭК 61508-2:2010, приложение А, чтобы продемонстрировать соответствие с 5.2 первой части ИСО 15998, где рассматриваются предотвращение отказов и управление случайными отказами аппаратных средств, происходящими во время срока службы/эксплуатации машины.

Предложенный метод основан главным образом на качественных аргументах и не требует вычисления диагностического охвата (ДО) или доли безопасных отказов (ДБО), как определено в ИСО 61508-2:2010, приложение С, так как это не является нормативным требованием в ИСО 15998.

Настоящее приложение применяется к СУСБ/Ч, реализующей функцию безопасности, работающей в режиме высокой интенсивности запросов или в непрерывном режиме.

Е.2 Доля безопасных отказов

Для определения ДБО подсистемы необходимо знать:

- тип подсистемы (тип А или тип В согласно МЭК 61508-2:2010):

«7.4.4.1.2 Элемент может быть отнесен к типу А, если для его компонентов, необходимых для реализации функции безопасности, одновременно выполняются следующие условия:

a) виды отказов всех составляющих компонентов определены;

b) поведение элемента в условиях отказа может быть полностью определено;

c) есть достаточно надежные данные об отказах, чтобы показать, что требуемые интенсивности отказов для обнаруженных и необнаруженных опасных отказов достигнуты (см. 7.4.9.3—7.4.9.5).

7.4.4.1.3 Элемент может быть отнесен к типу В, если для его компонентов, необходимых для реализации функции безопасности, выполняется хотя бы одно из следующих условий:

a) вид отказа по крайней мере одного составляющего компонента не определен;

b) поведение подсистемы в условиях отказа не может быть полностью определено;

c) имеются недостаточно надежные данные об отказах, чтобы показать, что требуемые интенсивности отказов для обнаруженных и необнаруженных опасных отказов достигнуты (см. 7.4.9.3—7.4.9.5).

Примечание — Если по крайней мере один из компонентов конкретного элемента соответствует условиям для типа В, то такой элемент должен быть отнесен к типу В, а не к типу А».

[МЭК 61508-2:2010]

- требуемое значение УПБ для связанной с безопасностью функции;
- уровень избыточности архитектуры аппаратных средств, который определяет отказоустойчивость аппаратных средств.

Пример — Для СУСБ/Ч: УПБ 1/УЭЗ$_т$ b, безопасное состояние с отключенным питанием, время безопасности процесса 500 мс. Подсистема: последовательность программ (микроконтроллера). Тип подсистемы: В (электронный комплекс). Отказоустойчивость аппаратных средств подсистемы: 0 (одиночный микроконтроллер без избыточности в СУСБ/Ч). Минимальная необходимая доля безопасных отказов: 60 % (низкий охват).

Е.3 Управление сбоями

Е.3.1 Документация

Чтобы применить данный метод, должно быть доступно следующее:

- описание системы управления машиной согласно 4.2 из первой части ИСО 15998;
- описание базовой функции согласно 4.3 из первой части ИСО 15998;
- результаты анализа и оценки риска согласно 4.4 из первой части ИСО 15998, включая необходимые УПБ для функций безопасности СУСБ/Ч;
- описание «безопасных состояний» для функций безопасности СУСБ/Ч согласно 4.5 из первой части ИСО 15998, включая информацию о «времени безопасности процесса» функций безопасности.

Данный метод дает указания по выбору мер управления случайными отказами аппаратных средств, возникающими во время срока службы/эксплуатации машины. Это способствует документальному оформлению концепции безопасности согласно 4.5 и 5.2 из первой части ИСО 15998.

Е.3.2 Архитектура аппаратных средств

Чтобы применить данный метод, список всех устройств СУСБ/Ч системы согласно 4.2 из первой части ИСО 15998 должен быть детализирован до подсистем, соответствующих МЭК 61508-2:2010, таблицы А.2—А.14 (см. таблицу Е.1).

Таблица Е.1 — Архитектура аппаратных средств

Таблицы МЭК 61508-2:2010	Подсистемы
Таблица А.2	Электрические компоненты
Таблица А.3	Электронные компоненты
Таблица А.4	Устройства обработки
Таблица А.5	Постоянная память
Таблица А.6	Память с произвольным доступом (ОЗУ)
Таблица А.7	Устройства ввода/вывода и интерфейс
Таблица А.8	Информационные каналы
Таблица А.9	Источник питания
Таблица А.10	Последовательность выполнения программ
Таблица А.11	Генератор тактовой частоты
Таблица А.12	Устройство связи и запоминающее устройство большой емкости
Таблица А.13	Датчики
Таблица А.14	Исполнительные элементы

Е.3.3 Ограничения архитектуры

Для каждой подсистемы из списка устройств СУСБ/Ч должны использоваться архитектурные ограничения согласно МЭК 61508-2:2010, таблица 2 и таблица 3 (см. таблицы Е.2 и Е.3), чтобы определить минимальное значение доли безопасных отказов, требуемое для подсистемы.

Таблица Е.2 — Максимальный допустимый уровень полноты безопасности для функции безопасности, реализуемой элементом или подсистемой типа А, связанной с безопасностью

Доля безопасных отказов элемента	Отказоустойчивость аппаратных средств		
	N = 0	*N* = 1	*N* = 2
Менее 60 %	УПБ 1/УЭЗ$_т$ *b/c*	УПБ 2/УЭЗ$_т$ *d*	УПБ 3/УЭЗ$_т$ *e*
От 60 до 90 %	УПБ 2/УЭЗ$_т$ *d*	УПБ 3/УЭЗ$_т$ *e*	
От 90 до 99 %	УПБ 3/УЭЗ$_т$ *e*		
Более и равно 99 %	уПБ 3/УЭЗ$_т$ *e*		

[МЭК 61508-2:2010]

Таблица Е.3 — Максимальный допустимый уровень полноты безопасности для функции безопасности, реализуемой элементом или подсистемой типа В, связанной с безопасностью

Доля безопасных отказов элемента	Отказоустойчивость аппаратных средств		
	N = 0	*N* = 1	*N* = 2
Менее 60 %	Не оговаривается	УПБ 1/УЭЗ$_т$ *b/c*	УПБ 2/УЭЗ$_т$ *d*
От 60 до 90 %	УПБ 1/УЭЗ$_т$ *b/c*	УПБ 2/УЭЗ$_т$ *d*	УПБ 3/УЭЗ$_т$ *e*

Окончание таблицы Е.3

Доля безопасных отказов элемента	Отказоустойчивость аппаратных средств		
	$N = 0$	$N = 1$	$N = 2$
От 90 до 99 %	УПБ 2/УЭЗт *d*	УПБ 3/УЭЗт *e*	
Более и равно 99 %	УПБ 3/$УЭЗ_т$ *e*		

Примечания

1 Требования настоящей таблицы совместно с требованиями 7.4.4.2.1 и 7.4.4.2.2 применяются для определения максимального значения УПБ, который может быть предъявлен к подсистеме, задавая отказоустойчивость подсистемы и долю безопасных отказов используемых элементов.

Для общего применения к любой подсистеме см. 7.4.4.2.1.

Для применения к подсистемам, включающим в себя элементы, отвечающие требованиям 7.4.4.2.2. Для того чтобы утверждать, что подсистема соответствует указанному УПБ непосредственно из данной таблицы, необходимо, чтобы для нее были выполнены все требования 7.4.4.2.2.

2 Требования настоящей таблицы совместно с требованиями 7.4.4.2.1 и 7.4.4.2.2 применяются для определения:

- требований отказоустойчивости аппаратных средств подсистемы, задавая необходимый УПБ функции безопасности и долю безопасных отказов используемых элементов;
- требований к значению доли безопасных отказов элементов, задавая необходимый УПБ функции безопасности и отказоустойчивость аппаратных средств подсистемы.

3 Требования 7.4.4.2.3 и 7.4.4.2.4 основаны на данных, определенных в настоящей таблице и в таблице 3.

4 Расчет доли безопасных отказов см. в приложении С.

5 Если используются требования 7.4.4.2.1 для комбинации элементов типа В, с отказоустойчивостью аппаратных средств, равной 1, в которой у обоих элементов доля безопасных отказов менее 60 %, то максимальным допустимым уровнем полноты безопасности для функции безопасности, выполняемой этой комбинацией, является УБП 1.

[МЭК 61508-2:2010]

Е.3.4 Выбор методов и мер для управления случайными отказами аппаратных средств в процессе эксплуатации

Методы и меры для управления случайными отказами аппаратных средств после установки системы должны быть выбраны из МЭК 61508-2:2010, приложение А, для каждой подсистемы СУСБ/Ч.

Методы и меры должны быть выбраны так, чтобы максимальный достижимый диагностический охват, который рассматривается в МЭК 61508-2:2010, таблицы А.2—А.14, был равен или превышал минимально необходимую долю безопасных отказов из-за архитектурных ограничений.

Методы и меры должны быть выбраны в соответствии с определением безопасных состояний функций безопасности, а интервал диагностических проверок должен удовлетворять требованиям 4.5.

Пример — Для СУСБ/Ч: УПБ 1/$УЭЗ_т$ b, безопасное состояние с отключенным питанием, время безопасности процесса 500 мс. Подсистема: последовательность программ (микроконтроллера). Тип подсистемы: В (электронный комплекс). Отказоустойчивость аппаратных средств подсистемы: 0 (одиночный микроконтроллер без избыточности в СУСБ/Ч). Минимальная необходимая доля безопасных отказов: 60 % (низкая). Выбранные методы и меры диагностики: контрольный датчик времени с отдельной временной базой и временным окном. Максимально достижимый диагностический охват считается: 90 % (средний). Дополнительное временное требование: интервал диагностических проверок + реакция на сбой < 500 мс.

Таблица Е.4 — Управляющая программа (контрольный датчик времени)

Диагностический метод/средство	См. МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Контрольный датчик времени с отдельной временной базой без временного окна	А.9.1	Низкий	—
Контрольный датчик времени с отдельной временной базой и временным окном	А.9.2	Средний	—
Логический контроль последовательности выполнения программ	А.9.3	Средний	Зависит от качества контроля

Окончание таблицы Е.4

Диагностический метод/средство	См.МЭК 61508-7	Максимально достижимый рассматриваемый охват диагностикой	Примечания
Комбинация временного и логического контроля последовательности выполнения программ	А.9.4	Высокий	—
Первоначальный тест при включении	А.9.5	Средний	—
Примечания 1 Требования настоящей таблицы не отменяют требований, приведенных в приложении С. 2 Для определения охвата диагностикой применяют требования приложения С. 3 Общие сведения, касающиеся настоящей таблицы, см. в таблице А.1.			

Так как:

a) максимально достижимый диагностический охват — 90 % (средний) превышает минимально необходимую долю безопасных отказов: 60 % (низкая);

b) выбранный метод позволяет достигать «безопасного состояния» с отключенным питанием;

c) временные требования 4.5 определены,

то выбранный метод «Контрольный датчик времени с отдельной временной базой и временным окном» подходит для управления случайными отказами аппаратных средств во время эксплуатации подсистемы «Управляющая программа».

Е.3.5 Интервал диагностических проверок и реакция на сбой

Е.3.5.1 Отказоустойчивость аппаратных средств больше нуля

Требования из МЭК 61508-2:2010:

«7.4.5.4 Диагностический испытательный интервал любой подсистемы которая:

- имеет значение отказоустойчивости аппаратных средств больше нуля и которая осуществляет функцию безопасности или часть функции безопасности, действуя в режиме высокой частоты запросов или с непрерывными запросами, или

- осуществляет функцию безопасности или часть функции безопасности, работая в режиме с низкой частотой запросов,

должен быть таким, чтобы суммарное время диагностического испытательного интервала и время выполнения ремонта обнаруженного отказа было меньше среднего времени восстановления MTTR, используемого в вычислении при определении достигаемой полноты безопасности для этой функции безопасности».

[МЭК 61508-2:2010]

заменяются следующим требованием:

диагностический испытательный интервал любой подсистемы, имеющей отказоустойчивость аппаратных средств больше нуля, должен составлять менее 24 ч.

Е.3.6 Отказоустойчивость аппаратных средств равна нулю

Применимы требования из МЭК 61508-2:2010:

«7.4.5.3 При количественной оценке случайных отказов аппаратных средств подсистемы со значением отказоустойчивости аппаратных средств, равным нулю, которая осуществляет функцию безопасности или часть функции безопасности, действующей в режиме высокой частоты запросов или с непрерывными запросами, доверие (предпочтение) должно быть отдано только диагностике, если:

- суммарное время диагностического испытательного интервала и время выполнения определенного действия для достижения или поддержания безопасного состояния меньше времени безопасности процесса;

- при работе в режиме высокой частоты запросов отношение частоты диагностических испытаний к частоте запросов равно или более 100».

[МЭК 61508-2:2010]

Приложение F
(справочное)

Архитектура

Архитектура системы управления должна быть выбрана на основе метода, выбранного пользователем ИСО 15998. Например, при рассмотрении среднего времени наработки на отказ можно использовать следующие международные стандарты:

- ИСО 13849-1:2006, раздел 6;
- МЭК 61508-6:2010, приложение В;
- ИСО 25119-2:2010, приложение А;
- ИСО 26262;
- МЭК 62061:2005, раздел 6.

Приложение G
(справочное)

Реализуемый проект, удовлетворяющий определенным значениям УПБ или $УЭЗ_т$

G.1 Общие положения

В настоящем приложении показано, как определить, удовлетворяет ли реализуемый проект определенному для него значению УПБ или $УЭЗ_т$. Значения УПБ должны быть пересчитаны в значения УЭЗ, чтобы иметь возможность воспользоваться ИСО 13849-1. Для реализуемого проекта должны быть определены следующие количественные характеристики:

- $MTTF_d$, см. ИСО 13849-1:2006, приложение С;
- диагностический охват, см. ИСО 13849-1:2006, приложение Е;
- результаты анализа отказов по общей причине, см. ИСО 13849-1:2006, приложение F;
- категория системы.

G.2 Определение $MTTF_d$

$MTTF_d$ = *MTTF* % опасных отказов.

Использование данных производителя.

Использование данных из справочников, например:

- MIL-HDBK-217F;
- МЭК/ТО 62380 (ранее RDF 2000);
- Руководство FIDES;
- средства расчета *MTBF* фирмы ALD;
- EPRD — данные о надежности электронных компонентов (RAC-STD-6100), Центр анализа надежности;
- NNPRD-95 — данные о надежности неэлектронных компонентов (RAC-STD-6200), Центр анализа надежности;
- программные инструменты, разработанные для доступа к вышеупомянутым базам данных;
- производитель (OEM или поставщик ЕКА), чтобы определить $MTTF_d$, может использовать практические данные вместо вычислений, предлагаемых в настоящем разделе;
- Siemens SN 29500, Интенсивность отказов компонентов.

Обычно при вычислении надежности и в стандартах MIL предполагается, что $MTTF_d = 2 \cdot MTTF$, т. е. если среднее время наработки на отказ составляет 50 лет, то среднее время наработки на опасный отказ составляет 100 лет. Поэтому можно оценить вид отказа каждого компонента и определить процент опасных отказов.

$MTTF_d$ = *MTTF*/ % опасных отказов.

Если известна величина B10, то снова может быть использовано предположение о 50 % количестве опасных отказов, поэтому:

$B10_d \approx 2 \cdot B10$.

$MTTF_d = B10_d / (0{,}1\ nop)$.

$nop = dop \cdot hop \cdot 3600$ с/ч / *tcycle*,

где *nop* — число циклов в год;

hop — средняя наработка (час/день);

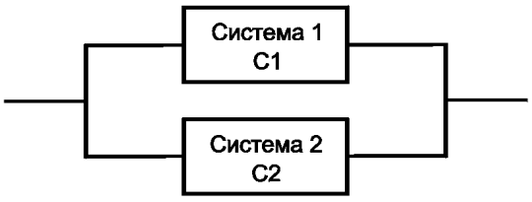
dop — средняя наработка (день/год);

tcycle — среднее время между началами двух последующих циклов для компонента (секунда/цикл).

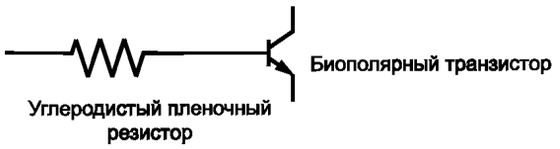
Рассмотрим, как вычислить $MTTF_d$ для последовательных и параллельных систем:



$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{dj}}$$



$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$



Компонент	*MTTF* (годы)	$MTTF_d$ (годы)	$1/MTTF_d$
Биполярный транзистор	34247	68494	1.46E-05
Резистор	114155	228310	4.380E-06

$1/MTTF_d$ = 1/ $MTTF_d$(резистора) + $1/MTTF_d$(транзистора),
$1/MTTF_d$ = 1/68494 + 1/228310,
$MTTF_d$ = 52687 лет.

Такие вычисления потребуются при анализе для каждого из компонентов и связанных с ними устройств в системе.

Таблица G.1 представляет обозначение для каждого канала на основе разбиения диапазона значений $MTTF_d$ на три уровня. В предыдущем простом примере значение $MTTF_d$ было бы определено как «высокое».

Таблица G.1 — Среднее время наработки на опасный отказ каждого канала ($MTTF_d$)

$MTTF_d$	
Обозначение каждого канала	Диапазон времени каждого канала
Низкое	3 года ≤ $MTTF_d$ < 10 лет
Среднее	10 лет ≤ $MTTF_d$ < 30 лет
Высокое	30 лет ≤ $MTTF_d$ < 100 лет

Примечания

1 Выбор диапазонов $MTTF_d$ каждого канала основан на интенсивности (частоте) отказов, определенной для области современной технологии, формируя своего рода логарифмическую шкалу, соответствующую логарифмической УЭЗ-шкале. Значение $MTTF_d$ каждого канала менее трех лет для реальной СУСБ/Ч считается невозможным, поскольку это означало бы, что после одного года около 30 % всех систем на рынке сломались, и их необходимо бы было заменить. Значение $MTTF_d$ каждого канала более 100 лет не приемлемо, так как СУСБ/Ч для крупных рисков не будет зависеть от надежности только одних компонентов. Чтобы защитить СУСБ/Ч от систематических и случайных отказов, должны использоваться дополнительные средства, такие как резервирование. На практике количество диапазонов было сокращено до трех. Ограничение $MTTF_d$ каждого канала максимальным значением, равным 100 лет, относится к одноканальной связанной с безопасностью системе управления, которая выполняет функцию безопасности. Более высокие значения $MTTF_d$ могут использоваться для одиночных компонентов (см. таблицу D.1).

2 Указанные в данной таблице границы имеют точность 5 %.

[ИСО 13849-1:2006, таблица 5]

G.3 Диагностический охват

Среднее значение диагностического охвата (ДО) определено как отношение между количеством обнаруженных опасных отказов и общим количеством опасных отказов следующим образом ($ДО_{ср}$ должен быть вычислен для всего канала):

$$ДО_{ср} = \frac{\frac{ДО1}{MTTF_{d1}} + \frac{ДО2}{MTTF_{d2}} + ... + \frac{ДОN}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + ... + \frac{1}{MTTF_{dN}}}.$$

В ИСО 13849-1:2006, приложение Е, рассмотрены примеры и оценки ДО.

После завершения анализа $ДО_{ср}$ должна использоваться таблица G.2, чтобы установить обозначение для каждого канала.

Таблица G.2 — Мера диагностического охвата

ДО	
Обозначение	Диапазон
Никакой	ДО < 60 %
Низкий	60 % ≤ ДО < 90 %
Средний	90 % ≤ ДО < 99 %
Высокий	99 % ≤ ДО

Примечания

1 Для СУСБ/Ч, состоящего из нескольких частей, используется средний диагностический охват $ДО_{ср}$ вместо ДО, изображенного на рисунке 5, раздел 6 и Е.2.

2 Выбор диапазонов ДО основан на ключевых значениях 60, 90 и 99 %, также используемых в других стандартах (например, МЭК 61508), имеющих дело с тестами оценки диагностического охвата. (1 — ДО) для ключевых значений 60, 90 и 99 %, формируя своего рода логарифмическую шкалу, соответствующую логарифмической УЭЗ-шкале. Значение ДО менее 60 % оказывает лишь небольшое влияние на надежность тестируемой системы и, следовательно, называется «никакое». Значение ДО свыше 99 % для сложных систем очень сложно достичь. Из практических соображений количество диапазонов было сокращено до четырех. Указанные в данной таблице границы имеют точность 5 %.

[ИСО 13849-1:2006, таблица 6]

G.4 Отказ по общей причине

Отказ по общей причине (ООП) — одиночный отказ, который приводит к отказу в двух или более каналах. В МЭК 61508-6:2010, приложение D, рассмотрена полная процедура по реализации мер против ООП. В ИСО 13849-1 рассмотрен общий метод для количественного определения ООП (см. таблицу G.3).

Таблица G.3 — Количественная оценка мер предотвращения ООП

№	Меры предотвращения ООП	Оценка
1	Разделение/Отделение	
	Физическое разделение между каналами сигналов: - разделение в проводке/трубопроводе; - достаточный зазор и расстояние между проводниками на печатных платах	15
2	Разнообразие	
	Используются разные технологии или физические принципы: - первый канал электронный с возможностью программирования, а второй канал оптико-проводной; - способ запуска; - давление и температура. Измерение расстояния и давления: цифровое и аналоговое. Компоненты от разных производителей	20
3	Проектирование/Приложение/Опыт	
3.1	Защита от скачков напряжения, перепадов давления и скачков тока и т. д.	15

Окончание таблицы G.3

№	Меры предотвращения ООП	Оценка
3.2	Используемые компоненты тщательно проверены	5
4	Оценка/анализ	
	Учтены ли все результаты анализа видов и последствий сбоев, чтобы избежать сбоев по общей причине?	5
5	Компетентность/обучение	
	Были ли проектировщики/операторы обучены, чтобы понимать причины и последствия сбоев по общим причинам?	5
6	Окружающая среда	
6.1	Предотвращение загрязнения и электромагнитная совместимость согласно соответствующим стандартам. Жидкостные системы: фильтрация рабочей среды под давлением, предотвращение попадания грязи, дренаж сжатого воздуха, например, в соответствии с требованиями разработчиков к компоненту, касающихся чистоты рабочей среды под давлением. Электрические системы: проверена ли система на электромагнитную устойчивость согласно соответствующим стандартам? Для комбинированных систем жидкостных и электрических — оба аспекта должны быть учтены	25
6.2	Другие влияния Соответствует ли требования к устойчивости от всех соответствующих влияний окружающей среды, таких как температура, ударная нагрузка, вибрация, влажность? (согласно соответствующим стандартам)	10
	Сумма	[максимально достижимая — 100]

Общая оценка	Меры предотвращения ООП[a)]
65 и более	Соответствует требованиям
Менее 65	Процесс не удался –> выберите дополнительные меры

[a)] Если технические меры не подходят, то баллы в этой колонке могут быть получены в результате полного расчета.

G.5 Категория системы

После завершения анализа УПБ или УЭЗ необходимо воспользоваться таблицей G.4. Реализация проекта может выполняться на основе опыта, а категория каждого канала может быть выбрана на основе начальных ожиданий проекта.

Из таблицы G.4 можно определить максимально достижимое значение УЭЗ для проекта, задав категорию системы, $ДО_{ср}$ и $MTTF_d$. Так как значения УПБ и УЭЗ известны, то это поможет определить категорию реализуемого проекта. Более подробно о возможностях каждой категории проекта см. также в ИСО 13849-1:2006, 6.2.

Таблица G.4 — Связь категорий системы со значениями УЭЗ, $ДО_{ср}$ и $MTTF_d$ для каждого канала

Категория	B	1	2	2	3	3	4
$ДО_{ср}$	Никакой	Никакой	Низкий	Средний	Низкий	Средний	Высокий
$MTTF_d$ для каждого канала:							
Низкий	a	Не рассматривается	a	b	b	C	Не рассматривается
Средний	B	Не рассматривается	b	c	c	d	Не рассматривается
Высокий	Не рассматривается	c	c	d	d	d	e

[ИСО 13849-1:2006, таблица 7]

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO 13766	IDT	ГОСТ ISO 13766:2006 «Машины землеройные. Электромагнитная совместимость»
ISO 13849-1:2006	IDT	ГОСТ ISO 13849-1:2015 «Безопасность машин. Детали систем управления, связанные с обеспечением безопасности. Часть 1. Общие принципы проектирования»
ISO 15998:2008	IDT	ГОСТ ISO 15998:2008 «Землеройные машины. Системы управления с использованием электронных компонентов. Критерии эффективности и испытания на функциональную безопасность»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO 3450:2011, Earth-moving machinery — Wheeled or high-speed rubber-tracked machines — Performance requirements and test procedures for brake systems
[2] ISO 5010:2007, Earth-moving machinery — Rubber tyred machines — Steering requirements
[3] ISO 9001:2008, Quality Management Systems — Requirements
[4] ISO 9004:2009, Managing for the sustained success of an organization — A quality management approach
[5] ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction
[6] ISO 13849-2:2003, Safety of machinery — Safety-related parts of control systems — Part 2: Validation
[7] ISO/TR 14121-2:2007, Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods
[8] ISO 25119-1, 2010, Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development
[9] ISO 25119-3:2010, Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software
[10] ISO 25119-4:2010, Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes
[11] ISO 26262:2011 (all parts), Road vehicles — Functional safety
[12] IEC 60068-2-27:2008, Environmental testing — Part 2-27: Tests — Test Ea and guidance: Shock
[13] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safetyrelated systems
[14] IEC 62061:2005, Safety of Machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems
[15] MIL-HDBK-217F: 1995, Reliability Prediction of Electronic Equipment
[16] IEC/TR 62380:2004, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment
[17] Guide FIDES 2009, Issue A
[18] Advanced Logistics Development MTBF calculator

ГОСТ Р 57300—2016

УДК 62-783:614.8:331.454:006.354 ОКС 13.110 Т51

Ключевые слова: машины землеройные, риск, защитные устройства, управляющее устройство, элементы систем управления, принципы конструирования, полнота безопасности

Редактор *А.Ф. Колчин*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 02.12.2016. Подписано в печать 25.01.2017. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 7,44.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Набрано в ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru
Издано во ФГУП «СТАНДАРТИНФОРМ», 123995, Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru