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

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO 19014-1— 2024

МАШИНЫ ЗЕМЛЕРОЙНЫЕ

Функциональная безопасность

Часть 1

Методика определения элементов систем управления, связанных с обеспечением безопасности, и технические требования

(ISO 19014-1:2018, IDT)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Российской ассоциацией производителей специализированной техники и оборудования (Ассоциацией «Росспецмаш») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 267 «Строительно-дорожные машины и оборудование»

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 августа 2024 г. № 176-П)

За принятие проголосовали:

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

4 Приказом Федерального агентства по техническому регулированию и метрологии от 10 октября 2024 г. № 1416-ст межгосударственный стандарт ГОСТ ISO 19014-1—2024 введен в действие в качестве национального стандарта Российской Федерации с 1 января 2025 г.

5 Настоящий стандарт идентичен международному стандарту ISO 19014-1:2018 «Машины землеройные. Функциональная безопасность. Часть 1. Методика определения элементов систем управления, связанных с обеспечением безопасности, и технические требования» («Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements», IDT).

Международный стандарт разработан Техническим комитетом по стандартизации ISO/TC 127 «Машины землеройные» Международной организации по стандартизации (ISO).

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

6 ВВЕДЕН ВПЕРВЫЕ

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

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

© ISO, 2018
© Оформление. ФГБУ «Институт стандартизации», 2024



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 Метод определения MPLr для SRP/CS землеройных машин 4
5 Требования к индикаторам предупреждения о немедленных действиях 5
6 Процедуры определения уровня эффективности защиты 5
Приложение А (справочное) Блок-схема процесса оценки рисков машин 9
Приложение В (справочное) Таблица предупреждающих индикаторов и индикаторов работы 10
Приложение С (справочное) Пример MCSSA 11
Приложение D (справочное) Перечень возможных систем управления, связанных с обеспечением безопасности (SCS) землеройных машин 14
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам 15
Библиография 15

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

МАШИНЫ ЗЕМЛЕРОЙНЫЕ

Функциональная безопасность

Часть 1

Методика определения элементов систем управления, связанных с обеспечением безопасности, и технические требования

Earth-moving machinery. Functional safety.
Part 1. Methodology to determine safety-related parts of the control system and performance requirements

Дата введения — 2025—01—01

1 Область применения

Настоящий стандарт устанавливает методы определения уровней эффективности защиты, необходимых для землеройных машин (EMM) по ISO 6165.

Анализ безопасности системы управления машиной (MCSSA) определяет степень снижения риска опасностей, относящихся к связанным с обеспечением безопасности системам управления (SCS). Это снижение количественно определяется уровнем эффективности защиты машины (MPL), опасности идентифицируются с использованием принципов оценки риска, определенных в ISO 12100, или другими способами.

Примечание 1 — Шаг 2, как показано в приложении A, демонстрирует взаимосвязь между ISO 12100 и ISO 19014 в качестве дополнительной меры защиты.

Примечание 2 — ISO 19014 может также использоваться для оценки требований функциональной безопасности других внедорожных мобильных машин.

Для тех средств управления, которые определены как связанные с обеспечением безопасности, характеристики архитектуры, аппаратного обеспечения, требований к окружающей среде программного обеспечения и эффективности защиты рассмотрены в других частях ISO 19014.

ISO 19014 охватывает опасности, вызванные отказом связанных с обеспечением безопасности систем управления, и не рассматривает опасности, связанные с самим оборудованием (например, поражение электрическим током, пожар и т. д.).

Другие средства управления, которые не являются связанными с обеспечением безопасности системами управления (SCS), которые не уменьшают опасность или не выполняют функцию управления и о неисправности которых оператору было бы известно, исключены из настоящего стандарта (например, стеклоочистители, фары, освещение кабины и т. д.).

Примечание 3 — Список связанных с обеспечением безопасности систем управления приведен в приложении D.

Примечание 4 — Звуковые предупреждения исключены из требований диагностического охвата.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения)]:

Издание официальное

ISO 6165, Earth-moving machinery — Basic types — Identification and terms and definitions (Машины землеройные. Основные типы. Идентификация, термины и определения)

ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction (Безопасность машин. Основные понятия, общие принципы конструирования. Оценка и снижение рисков)

3 Термины и определения

В настоящем стандарте применены термины по ISO 6165 и ISO 12100, а также следующие термины с соответствующими определениями.

ISO и IEC ведут терминологические базы данных для использования в стандартизации по следующим ссылкам:

- онлайн-платформа ISO: gost.e-ecolog.ru ;
- электропедия IEC: gost.e-ecolog.ru .

3.1 **уровень эффективности защиты машины;** MPL (machine performance level): Дискретный уровень, используемый для определения способности элементов систем управления, связанных с обеспечением безопасности (3.3.2), осуществлять функцию безопасности в прогнозируемых условиях.

Примечание 1 к статье — Термин MPL используется для описания уровня эффективности защиты, требуемого от связанного с безопасностью элемента системы управления. Буква «M» относится к машине и обозначает землеройные машины, на которые распространяется действие настоящего стандарта, и используется для отличия от других стандартов функциональной безопасности (например, PL, AgPL, ASIL и т. д.).

3.1.1 **требуемый уровень эффективности защиты машины;** MPL_r (machine performance level required): Дискретный уровень, необходимый для достижения требуемой функциональной безопасности для каждой функции, связанной с обеспечением безопасности.

3.1.2 **достигнутый уровень эффективности защиты машины;** MPL_a (machine performance level achieved): Дискретный уровень, достигаемый аппаратными средствами, архитектурой и программным обеспечением систем управления безопасностью (3.3.1).

Примечание 1 к статье — Процесс определения MPL_a описан в ISO 19014-2 и ISO 19014-4.

3.2 **функциональная безопасность** (functional safety): Система, которая действует таким образом, что исключает неоправданный риск травмирования операторов или наблюдателей, и зависит от правильного функционирования систем управления, связанных с обеспечением безопасности (SCS) (3.3.1) и других мер по снижению риска.

3.3 **система управления машиной**; MSC (machine control system): Система, которая отвечает на входные сигналы от элементов оборудования, операторов (3.4.1), оборудования внешнего контроля или любой комбинации вышеприведенных элементов и генерирует сигналы, приводящие машину в действие в заданном порядке.

3.3.1 **система управления, связанная с обеспечением безопасности**; SCS (safety control system): Подсистема или система, используемая MCS (3.3) для достижения функциональной безопасности (3.2) путем воздействия на поведение машины или уменьшения опасности.

Примечание 1 к статье — Система, которая может выйти из строя таким образом, что это создаст опасность, считается SCS.

Примечание 2 к статье — Например, SCS для управления мощностью может включать дроссель, переключение передач, старт/стоп и т. д.

3.3.2 **элемент системы управления, связанный с обеспечением безопасности;** SRP/SC (safety-related part of the control system): Элемент или подсистема системы управления (3.3.1), которая реагирует на входные сигналы и вырабатывает выходные сигналы, связанные с обеспечением безопасности.

Примечание 1 к статье — Комбинированные элементы системы управления, связанные с обеспечением безопасности, начинают действовать в точке, где возникают сигналы, связанные с обеспечением безопасности (например, приводной кулачок или ролик путевого выключателя [переключателя] и заканчивают на выходе силовых элементов управления (например, главные контакты пускателя [контактора]).

Примечание 2 к статье — Если системы мониторинга используются для диагностического охвата, они также считаются SRP/CS.

Примечание 3 к статье — SRP/CS является частью или элементом конкретной MCS.

3.4 **группа лиц** (person group): Группы людей, проанализированные в MCSSA (3.14).

3.4.1 **оператор** (operator): Человек, эксплуатирующий машину и осведомленный о связанных рисках или опасностях.

3.4.2 **коллега по работе** (co-worker): Человек, работающий вблизи машины и осведомленный о связанных с ней опасностях.

3.4.3 **посторонний** (bystander): Человек, в том числе не являющийся коллегой по работе, ребенок или посторонний, мало осведомленный или не осведомленный об опасностях, связанных с работой машин, и не прошедший обучение.

3.4.4 **обслуживающий персонал** (maintainer): Человек, в обязанности которого входит выполнение работ по техническому обслуживанию машины.

Примечание 1 к статье — Обслуживающий персонал обучен соответствующим образом и знаком с особенностями и опасностями машины.

3.5 **управляемость** (controllability): Возможность избежать причинения вреда группе лиц (3.4), подверженной риску, за счет своевременной реакции оператора (3.4.1), в том числе с помощью альтернативных средств управления.

3.6 **время воздействия** (exposure): Процент времени, в течение которого группа лиц (3.4) подвергается опасности.

Примечание 1 к статье — Время воздействия является произведением следующих зависимых вероятностей: вариант использования (3.11), время опасности (3.12) и время воздействия на группу лиц (3.15).

3.7 **степень тяжести последствий** (severity): Мера оценки наиболее вероятного потенциального вреда здоровью человека, подвергающегося опасности.

3.8 **индикатор работы** (operation indicator): Средства, с помощью которых состояние оборудования или механизмов представляется наблюдателю.

3.8.1 **предупреждающий индикатор** (warning indicator): Визуальная, сенсорная или звуковая индикация в случае, когда требуется действие оператора (3.4.1) или системы управления.

3.8.2 **индикатор предупреждения о немедленных действиях** (immediate action warning indicator): Предупреждающий индикатор (3.8.1), требующий от оператора немедленных действий (3.4.1) для уменьшения опасности или отказа системы.

3.9 **область применения** (application): Различные отрасли, в которых используется машина, которые могут иметь разные опасные ситуации.

Примечание 1 к статье — Области применения могут включать общее строительство, строительство дорог, работу с отходами, разработку карьеров и т. д.

3.10 **вариант использования** (use case): Предполагаемое использование машины в области применения (3.9).

Примечание 1 к статье — Например, бульдозер может иметь варианты использования в режимах рыхления, перемещения грунта и обслуживания в рамках области применения.

3.11 **вариант использования в области применения** (application use case): Наибольший ожидаемый процент времени, в течение которого машина будет использоваться в варианте использования (3.10) в данной области применения (3.9) в течение предполагаемого жизненного цикла машины.

Примечание 1 к статье — Поскольку вариант использования в области применения представляет собой самый высокий процент времени, а не среднее значение, которое машина в совокупности тратит на вариант использования, сумма вариантов использования в области применения может превышать 100 %.

3.12 **время опасности** (hazard time): Процент времени в рабочем цикле области применения, когда разумно предвидеть, что может существовать опасность в случае отказа оцениваемой системы управления.

Примечание 1 к статье — Например, бульдозер, сталкивающий материал с обрыва, подвергается опасности падения с высоты только в то время, когда движется к обрыву в пределах тормозного пути.

3.13 **опасная зона** (hazard zone): Любое пространство внутри или вокруг машин, в котором человек может подвергаться опасности со стороны оцениваемой SCS (3.3.1).

3.14 **анализ безопасности системы управления машиной;** MCSSA (machine control system safety analysis): Оценка риска, используемая для определения MPLr (3.1.1) для SCS (3.3.1) на машине, как указано в настоящем стандарте.

3.15 **время воздействия на группу лиц** (person group exposure): Наибольший процент времени опасности (3.12), в течение которого кто-либо из оцениваемой группы лиц (3.4) находится в опасной зоне (3.13).

Примечание 1 к статье — Оценивается для всех людей, подвергшихся воздействию, а не для одного человека из группы лиц.

3.16 **тип отказа** (failure type): Описание типа отказа, который может произойти в SCS (3.3.1).

Примечание 1 к статье — Типы отказов, которые следует учитывать, включают в себя отказ применения или отключения, неуправляемое применение или отключение, неправильную скорость применения или отключения, неправильное направление и т. д.

3.17 **предполагаемый вред** (worst credible): Оценка степени тяжести последствий (3.7) наиболее серьезного вреда, который реально может возникнуть в результате одного опасного события.

Примечание 1 к статье — Предполагаемый вред не всегда является наихудшим возможным или наиболее вероятным, но он основан на рассмотрении истории прецедентов и потенциального исхода опасного события.

4 Метод определения MPLr для SRP/CS землеройных машин

4.1 Общее

Функциональная безопасность достигается с помощью одной или нескольких SCS, основанных на разных технологиях (например, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных). Любая стратегия безопасности должна учитывать все элементы SCS, такие как датчики, управляющие устройства и приводы.

Элементы SCS, обеспечивающие функции безопасности, называются элементами систем управления, связанными с безопасностью (SRP/CS). Они могут состоять из аппаратного или программного обеспечения, могут быть отдельными или интегрированными частями системы управления, которые должны быть включены в процесс MCSSA.

Цель состоит в том, чтобы уменьшить риск, связанный с конкретной опасностью (или опасной ситуацией) при использовании машины по назначению. Это достигается путем применения различных защитных мер (как SRP/CS, так и не-SRP/CS) для достижения безопасного состояния.

Исследование риска для функций безопасности сосредоточено на анализе вреда людям. Если при анализе потенциального вреда будет установлено, что ущерб однозначно ограничится имуществом и не влечет причинения вреда людям, то данная MCS не относится к SCS. Кроме того, пользователь (владелец) несет ответственность за выполнение конкретной оценки рисков на рабочей площадке, и эти оценки не являются частью процесса MCSSA.

4.2 Метод анализа безопасности систем управления машиной (MCSSA)

a) Определяют все MCS или функции оцениваемой машины.

b) Определяют возможные типы отказов для каждой MCS или функции.

c) Определяют риски для каждого типа отказа каждой MCS или функции:

1) Если риски не выявлены, MCS или функции не являются SCS, но могут подпадать под действие требований к показателям качества (QM) (см. 6.6).

2) Если выявлены риски, MCS или функции являются SCS.

d) Оценивают риски:

1) Оценивают ранее определенные риски с использованием оценок тяжести последствий, времени воздействия и управляемости с использованием метода, приведенного в разделе 6.

Примечание — ISO/TS 19014-5 содержит требования по анализу безопасности систем управления машинами (MCSSA) и уровням эффективности защиты; в настоящем стандарте будет подробно описан альтернативный метод для использования при определении соответствующего MPLr для некоторых распространенных MCS.

e) Определяют MPLr, используя графическое отображение рисков (см. 6.6 и рисунок 2) для каждого типа отказа каждой SCS, в соответствии с 6.3, 6.4 и 6.5:

1) Выбирают самый высокий MPLr для присвоения этой SCS в соответствии с 6.6.

f) Если MCSSA был выполнен для функции, а не для системы, то присваивают полученный MPLr соответствующей SCS.

g) Используют другие части ISO 19014 для определения MPLa SCS.

h) Проверяют, что MPLa ≥ MPLr.

Если добавляются дополнительные меры защиты, они должны соответствовать MPLr для SCS, к которой они относятся.

Примечание — Пример процесса MCSSA приведен в приложении С.

5 Требования к индикаторам предупреждения о немедленных действиях

5.1 Общее

Принципы настоящего стандарта также следует применять к индикаторам предупреждения о немедленном действии, предназначенным для предупреждения оператора о возможной опасности и требующим от оператора немедленных действий для исправления и предотвращения такой опасности.

Эти индикаторы не должны определяться как соответствующие уровню эффективности, поскольку выходной/диагностический охват зависит от реакции человека; индикаторы не обеспечивают управление системой и поэтому не могут являться связанными с безопасностью элементами системы управления.

Следует провести обзор доступных индикаторов, предупреждающих о немедленных действиях, чтобы убедиться, что разработчик машины понимает действия оператора, необходимые для уменьшения опасности.

В приложении В приведен неполный список предупреждающих индикаторов.

6 Процедуры определения уровня эффективности защиты

6.1 Общее

Требования настоящего раздела применяют, когда в соответствии с 4.2 требуется оценка рисков.

Архитектура (например, резервные каналы, дополнительные защитные устройства, блокировки, которые имеют общие компоненты с SCS и т. д.) SCS не должны рассматриваться в ходе MCSSA. Дополнительные защитные устройства и блокировки также могут быть SCS, и в таком случае требуется их оценка.

Если в течение жизненного цикла машины принимаются решения, которые изменяют базовые принципы, на основе которых были приняты более ранние решения, должны быть проведены новый MCSSA и оценка систем в соответствии со всеми частями ISO 19014.

6.2 Участники оценки риска

MCSSA должен быть проведен многофункциональной командой, например из числа разработчиков и испытателей электрических и электронных компонентов, гидравлики, конструкции машины, и оператора.

6.3 Оценка и классификация потенциального вреда

Наибольшая тяжесть предполагаемого вреда может быть определена с использованием как истории прошлых инцидентов, так и потенциального результата сбоев в работе анализируемой SCS. Потенциальная тяжесть вреда или травмы должна быть описана для каждого соответствующего сценария в MCSSA.

Примечание — Определение наибольшей тяжести предполагаемого вреда является сложной задачей. Наиболее серьезные последствия могут быть очень маловероятными, а наиболее вероятные могут быть несущественными, так что использование любого из них может привести к неправильной оценке риска.

При классификации тяжести вреда по категориям используются четыре категории: S0, S1, S2 и S3 (см. таблицу 1).

Оператор задействованной машины и другие участники события (например, люди, оказывающие помощь, другие операторы машин, посторонние люди, коллеги и т. д.) должны учитываться в подробном описании вреда.

Таблица 1 — Классификация тяжести вреда

S0	S1	S2	S3
Без существенных травм, требуется только первая медицинская помощь	Травмы, требующие медицинской помощи, полное выздоровление, обратимая травма без потери трудоспособности после выздоровления	Серьезные травмы, постоянная потеря трудоспособности	Смертельный исход

6.4 Оценка времени воздействия в наблюдаемой ситуации

Далее приведены последствия возможных отказов в конкретных условиях работы и эксплуатации.

Расчетное время воздействия E должно использоваться для классификации различных частот или продолжительности времени воздействия.

Оно рассчитывается по следующей формуле

$$E = A \cdot H \cdot P,$$

где A — вариант использования в области применения;

H — время опасности;

P — время воздействия на группу лиц.

Пример MCSSA приведен в приложении С.

Если вариант использования имеет цикл с переменными значениями, H и P, $H \times P$ можно рассчитать для каждого шага и просуммировать для цикла, чтобы получить общее значение $H \times P$ для цикла.

Машины должны быть спроектированы таким образом, чтобы снизить риски при любом предполагаемом использовании, даже если наихудший предполагаемый вариант использования составляет небольшой процент от вариантов использования. Области применения с опасностями, отличными от типичных для конкретной машины, например производная машина, разработанная с системами управления специально для конкретной области применения, могут рассматриваться как специализированные области применения, исключаться из анализа и рассматриваться в отдельной MCSSA.

Используются три категории, обозначенные E0, E1 и E2 (см. таблицу 2), где E служит для оценки того, как часто и как долго оператор или посторонний человек подвергается опасности, которая может привести к травме группы лиц. При проведении MCSSA следует использовать риск от наибольшего времени воздействия. Меньшие времена воздействия, которые имеют более высокий потенциальный вред, также должны быть рассмотрены при оценке, чтобы проверить, создается ли более высокий уровень эффективности защиты.

Время воздействия на обслуживающий персонал должно отражать время, затраченное на обслуживание машины, при этом в MCSSA должно учитываться, что работа SRP/CS может быть приостановлена во время обслуживания.

Примечание — Опасность может представлять собой комбинацию условий (например, условий окружающей среды и эксплуатации) машины.

Таблица 2 — Категории времени воздействия опасного события в зависимости от области применения

E0	E1	E2
$E < 1\ \%$	$1\ \% \le E < 10\ \%$	$E \ge 10\ \%$

6.5 Оценка возможности предотвращения вреда

Должна оцениваться управляемость для конкретной опасности, с учетом возможной реакции человека (например, паники, повторного воздействия на орган управления и т.д.), способности оператора реагировать на опасность и наличия средств для перехода в безопасное состояние. Альтернативные средства управления не учитываются, если они имеют общую причину отказа с анализируемой системой.

При рассмотрении нескольких альтернативных действий каждое из этих действий должно быть независимым друг от друга.

Следующие факторы используются для определения управляемости и рассчитываются с использованием рисунка 1.

Альтернативные элементы управления:

- AC0 — отсутствуют альтернативные элементы управления или возможные действия;
- AC1 — присутствует один или более альтернативный элемент управления или возможное действие.

Уровень осведомленности об опасности:

- AW3 — Высокий: известно до действия функции;
- AW2 — Средний: известно при действии функции, в течение всего времени;
- AW1 — Низкий: известно при действии функции, иногда;
- AW0 — Отсутствует: неизвестно при действии функции, например, система, которую никто не видит или о которой не знают, выполняет несанкционированные оператором действия.

Предупреждающие индикаторы должны учитываться при оценке осведомленности об опасности только в том случае, если они определены как индикаторы предупреждения о немедленных действиях, которые не имеют общих компонентов с SRP/CS анализируемой системы.

Возможность отреагировать:

- AR 3 — Оператор может отреагировать вовремя и естественным способом, без дополнительных движений рукой или ногой, например объехать препятствие при отказе тормозов;
- AR 2 — Оператор может отреагировать вовремя и естественным способом, с дополнительными движениями рукой или ногой, например включить стояночный тормоз при отказе рабочих тормозов;
- AR 1 — Оператор может отреагировать вовремя и неестественным способом, например, при отказе тормозов остановить машину ее рабочим органом;
- AR 0 — Оператор или система не могут отреагировать для предотвращения опасности вне зависимости от наличия другой системы для взаимодействия.

Действия включают ожидаемые, предполагаемые и/или интуитивные, и они должны быть задокументированы. Например, при отказе тормоза бульдозера ожидается и интуитивно предсказуемо, что оператор опустит отвал или рыхлитель.

Примеры других систем управления, связанных с безопасностью, приведены в приложении D.

Классификация управляемости:

- C0 — Высокая управляемость
- C1 — Средняя управляемость
- C2 — Низкая управляемость
- C3 — Отсутствие управляемости

		AR0	AR1	AR2	AR3
AC0		C3	C3	C3	C3
AC1	AW0	C3	C3	C3	C3
	AW1	C3	C3	C3	C2
	AW2	C3	C3	C2	C1
	AW3	C3	C2	C1	C0

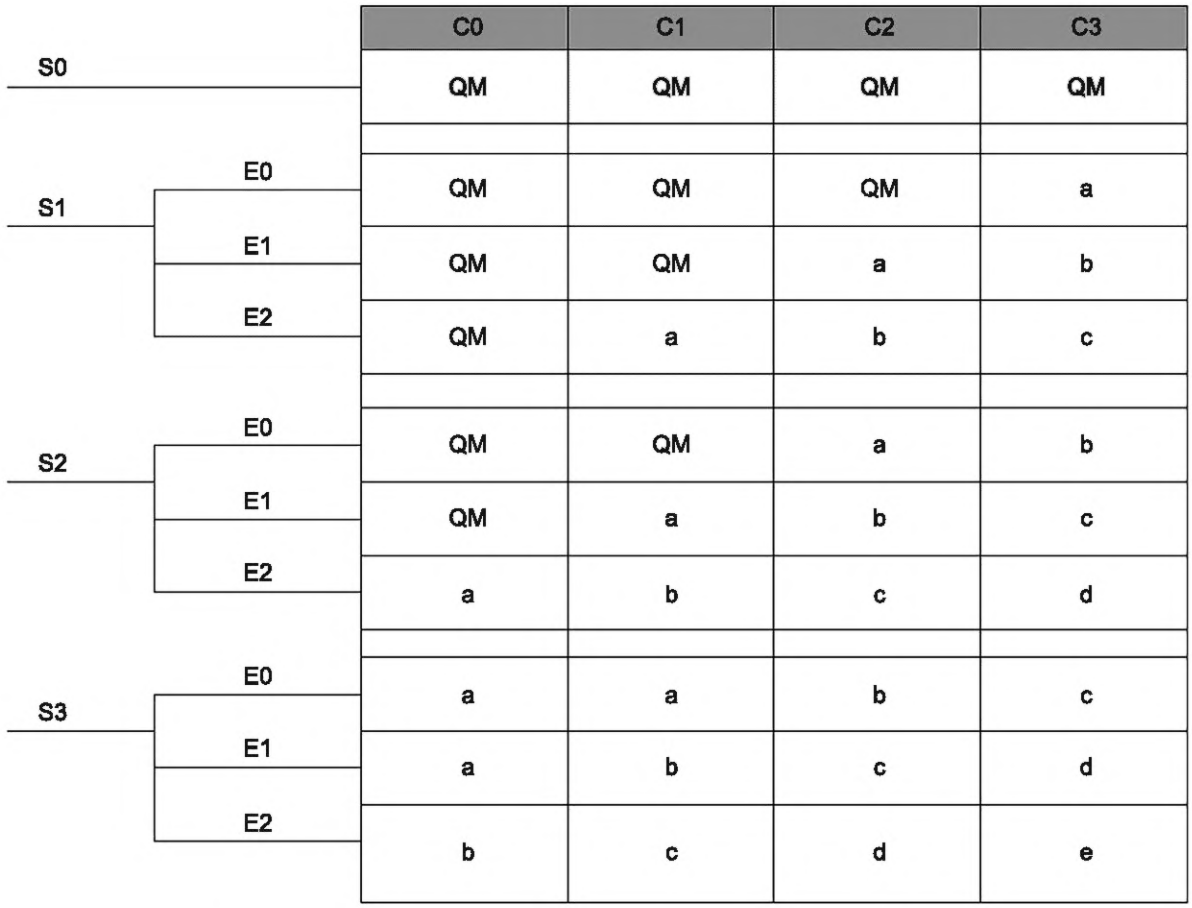
AC — альтернативные элементы управления; *AW* — осведомленность об опасности; *AR* — возможность отреагировать

Рисунок 1 — Классификация управляемости

6.6 Определение требуемого MPL

Требуемый MPLr определяется по рисунку 2 путем объединения значений тяжести вреда, времени воздействия и управляемости для каждой выявленной опасности при оценке риска. Если SCS используется в нескольких сценариях, где тяжесть вреда, время воздействия и управляемость могут отличаться, каждый сценарий должен быть рассмотрен. Для этой SCS должен использоваться наивысший уровень эффективности защиты, определенный MCSSA.

В дополнение уровням эффективности защиты существует мера качества (QM), неявным требованием которой является выполнение разработки системы в соответствии с инструментами управления качеством, соответствующими техническими требованиями и стандартами, если применимо.



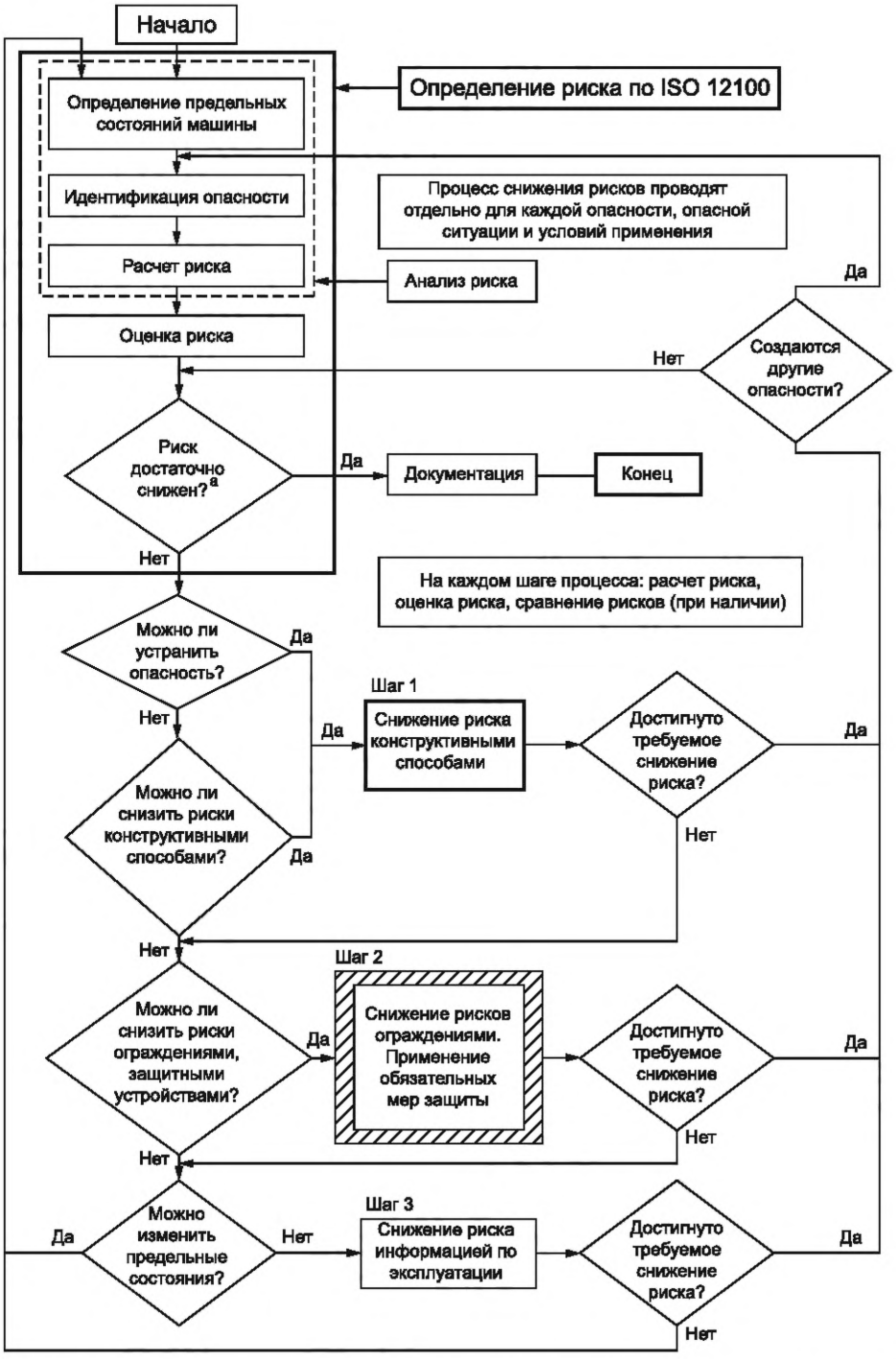
S — тяжесть последствий; E — время воздействия опасной ситуации; C — управляемость; QM — мера качества; a, b, c, d, e — требуемый уровень эффективности защиты машины, MPLr

Рисунок 2 — Определение MPLr

Приложение А
(справочное)

Блок-схема процесса оценки рисков машин

См. рисунок А.1.



— Взаимосвязь с ISO 19014 в случае, если снижение риска или защитные меры связаны с системой управления

[a] Раздел 6 ISO 12100:2010 дополнительно определяет, что можно считать адекватным снижением риска; конструктивные меры безопасности, ограждения и/или дополнительные защитные меры, информацию по эксплуатации.

Рисунок А.1 — Взаимосвязь между ISO 12100 и ISO 19014

Приложение В
(справочное)

Таблица предупреждающих индикаторов и индикаторов работы

Принципы настоящего стандарта в отношении оценки риска, архитектуры, аппаратного обеспечения, программного обеспечения, требований к окружающей среде и надежности должны применяться к индикаторам предупреждения о немедленных действиях, предназначенным для предупреждения оператора о возможной опасности, которая требует от оператора немедленных действий для устранения и предотвращения такой опасности.

В таблице В.1 приведен список общих индикаторов, используемых в ЕММ. Это не исчерпывающий список, и он применим не ко всем типам ЕММ. Другие индикаторы, специфичные для конкретного типа ЕММ, также могут соответствовать принципам ISO 19014, определенным изготовителем.

Примечание — Руководство приведено в ISO 6011:2003.

Таблица В.1 — Индикаторы ЕММ

Индикатор	Индикатор предупреждения о немедленных действиях	
	Да	Нет
Обороты двигателя		X
Давление масла в двигателе		X
Температура охлаждающей жидкости		X
Напряжение/ток в электросистеме	X	
Давление масла в гидротрансформаторе		X
Температура масла в гидротрансформаторе	X	
Давление масла в трансмиссии		X
Температура масла в трансмиссии		X
Запасенное давление в тормозной системе	X	
Давление гидравлической жидкости	X[a]	
Температура гидравлической жидкости		X
Мото-часы		X
Многофункциональный дисплей (ISO 20474-1:2017, 4.5.1)	X	
Датчик уровня топлива (ISO 20474-1:2017, 4.18.1)		X
Индикатор вместимости	X	
Система определения сближения с препятствием		X
Системы обзора		X
[a] При необходимости для зажима, удержания навесного оборудования или груза в нужном положении.		

Приложение С
(справочное)

Пример MCSSA

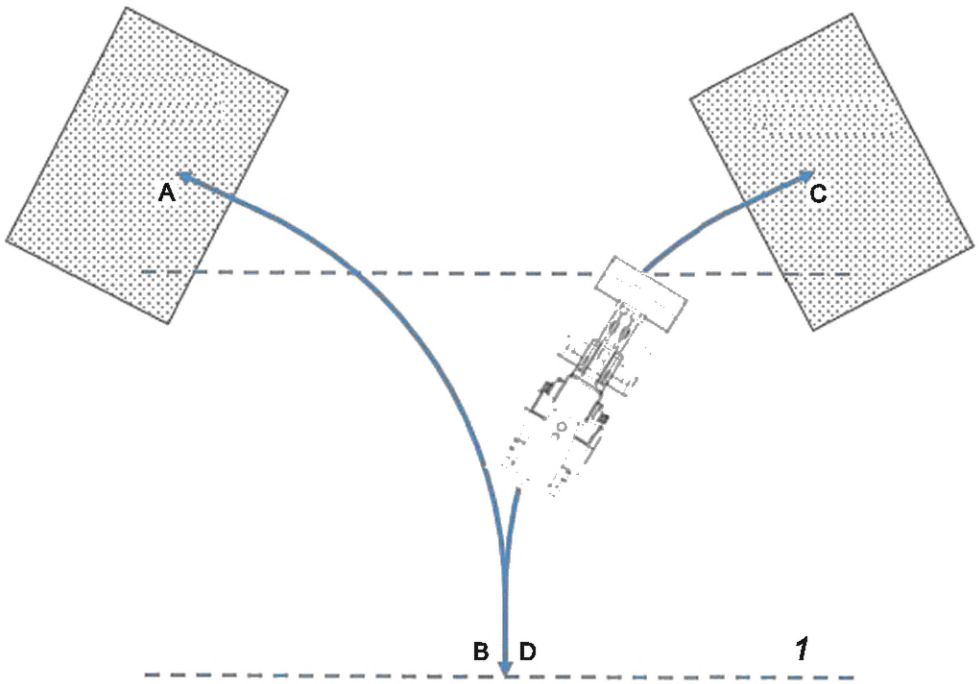
В настоящем приложении представлен пример MCSSA при соблюдении процедуры, описанной в 4.2, и при использовании изготовителем 4.2 d) 1), а не варианта 4.2 d), примечание. См. рисунок С.1.

Подпункт 4.2 Шаг 1

SCS — Тормозная система

Область применения: Общее использование на открытой местности (карьер)

Вариант использования: загрузка грузовика



A — погрузка; *C* — выгрузка; *1* — дорога; $P_{коллега}$ = 10 %; $P_{посторонний}$ = 5 %

Машина быстро перемещается по рабочей области, доступ людей к этой области обычно ограничен при работе с машинами такого размера. Плохой организацией рабочей площадки считается наличие людей на пути машины.

Рисунок С.1 — Вариант использования в области применения

Подпункт 4.2 Шаг 2

Тип отказа — отказ при попытке использования тормозов

Подпункт 4.2 Шаг 3

Опасный исход

Оператор: Столкновение с загружаемым грузовиком

Посторонний: Наезд (на пешехода)

Коллега по работе: Столкновение (С легкой техникой — хуже, чем для водителя грузовика при столкновении с грузовиком)

Подпункт 4.2 Шаг 4 a)

Тяжесть последствий

Оператор: S1 — незначительный удар

Посторонний: S3 — наезд

Коллега: S3 — на основе истории инцидентов

Время воздействия

A: 90 %.

Таблица С.1 — Время цикла, %

Применение	Погрузка/ разгрузка	V-образный цикл ковша (включая загрузку грузовика или бункера)	Передвижение (с грузом или без груза)	Низкая скорость, маневрирование, запуск, остановка	Рабочий орган низко над землей	Обслуживание, ремонт
Погрузчик на открытой площадке	90 %	90 %	80 %	6 %	90 %	6 %
Погрузчик скрыт за препятствием	90 %	90 %	80 %	6 %	90 %	6 %

H:

Простаивание: Грузовик присутствует до 90 % времени, поэтому машина может простаивать не более 10 %. При расчете H следует дополнительно умножать на (100 % – 10 %) = 90 %.

Таблица С.2 — Время воздействия опасности на оператора, % от общего

Стадия рабочего цикла (см. рисунок С.1)	Время, %	Время присутствия угрозы на стадии цикла, %	$H_{стадии}$ = Время, % × (Время присутствия угрозы на стадии)
A	25	0	0
B	25	0	0
C	25	10 % — Угроза присутствует только при приближении к грузовику. Погрузчик замедляется последние 10 % времени на стадии C	2,5
D	25	0	0
		Сумма	2,5

$H_{оператор} = H_{стадии}$ × (100 % — время простаивания) = 2,5 % × 90 % = 2,25 %.

Посторонний/коллега

В этом случае H для постороннего и коллеги одинакова, потому что опасная зона для этих групп лиц находится в одном и том же месте.

Таблица С.3 — Время воздействия опасности на коллегу/постороннего, в % от общего

Стадия рабочего цикла (см. рисунок С.1)	Время, %	Время присутствия угрозы на стадии цикла, %	$H_{Стадии}$ = Время, % × (Время присутствия угрозы на стадии)
A	25	0	0
B	25	10 % — Угроза присутствует только при приближении к области позади зоны работ. Погрузчик замедляется последние 10 % времени на стадии B	2,5
C	25	0	0
D	25	10 % — Угроза присутствует только при приближении к области позади зоны работ. Погрузчик замедляется последние 10 % времени на стадии B	2,5
		Сумма	5

$H_{посторонний/коллега} = H_{стадии}$ × (100 % — время простаивания) = 5 % × 90 % = 4,5 %.

P:

$P_{оператор}$: 100 % (всегда в колесном погрузчике);

$P_{посторонний}$: 5 % (определено по статистическим данным экспертов);

$P_{коллега}$: 10 % (определено по статистическим данным экспертов).

E:

A × H × P

$E_{оператор} = A \times H_{оператор} \times P_{оператор} = 90\ \% \times 2{,}25\ \% \times 100\ \% = 2\ \%$, категория времени воздействия E1;

$E_{посторонний} = A \times H_{посторонний} \times P_{посторонний} = 90\ \% \times 4{,}5\ \% \times 5\ \% = 0{,}2\ \%$, категория времени воздействия E0;

$E_{коллега} = A \times H_{коллега} \times P_{коллега} = 90\ \% \times 2{,}25{,}5\ \% \times 4{,}5\ \% = 0{,}4\ \%$, категория времени воздействия E0.

Управляемость

AC = AC1 — оператор может использовать рулевое управление, стояночный тормоз или иные системы, не имеющие общих компонентов с тормозной системой SRP/CS.

AW = AW2 — оператор узнает об отказе тормозов сразу же по отсутствию реакции машины на нажатие педали тормоза.

AR:

$AR_{оператор}$ = AR0 — оператор не смог вовремя среагировать до столкновения с грузовиком из-за необходимости найти альтернативные средства управления и не смог объехать грузовик

$AR_{посторонний/коллега}$ = AR3 — оператор может инстинктивно объехать (не снимая рук с руля) опасность и может сделать это вовремя (из-за большего расстояния между рабочей площадкой и дорогой)

Управляемость = C1 (согласно 6.5 и рисунку 1)

Пункт 4.2 Шаг 5

Выбор уровня эффективности защиты по 6.6 и рисунку 2.

(S1, E1, C3) -> $MPLr_{оператор}$ = b

(S3, E0, C1) -> $MPLr_{посторонний}$ = a

(S3, E0, C1) -> $MPLr_{коллега}$ = a

Примечание — Данный пример рассматривает только одну ситуацию для колесного погрузчика, оценка других вариантов использования при отказе тормозов может привести к гораздо более высоким MPLr.

Приложение D
(справочное)

Перечень возможных систем управления, связанных с обеспечением безопасности (SCS) землеройных машин

Далее приведен неполный перечень возможных SCS для землеройных машин. На любой конкретной машине эти системы могут считаться SCS, в зависимости от MCSSA и области применения машины. Системы, отмеченные *, почти всегда считаются SCS.

ТОРМОЗА
- *Рабочие тормоза (MCSSA и стандарты определяют дополнительные требования к тормозным системам)
- *Стояночный тормоз (ручной или автоматический)
- Зарядка аккумулятора
- Ретардер

РУЛЕВОЕ УПРАВЛЕНИЕ
- *Система рулевого управления (MCSSA и стандарты определяют дополнительные требования к рулевому управлению)
- Дополнительная подача гидравлической жидкости в рулевое управление (при наличии)

НАВЕСНОЕ ОБОРУДОВАНИЕ
- *Подъем, опускание и все перемещения навесного устройства
- Быстроразъемная муфта с силовым приводом

УПРАВЛЕНИЕ ТЯГОЙ
- *Управление оборотами двигателя
- *Трансмиссия
  - Направление движения
  - Выбор передач
- Выключение двигателя
- Контроль превышения скорости
- Система круиз-контроля

СИСТЕМЫ СНИЖЕНИЯ ОПАСНОСТЕЙ
- Аварийная остановка (при наличии)
- Системы контроля присутствия оператора на рабочем месте
- Блокировки дверей/отсеков

ДРУГИЕ
- *Системы управления автономных машин
- *Системы дистанционного управления
- *Системы предотвращения столкновений
- Автоматизированные системы доступа
- *Система поворота экскаватора
- Системы блокировки (для обслуживания)
- Блокировки

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 6165	IDT	ГОСТ ISO 6165—2015 «Машины землеройные. Основные типы. Идентификация, термины и определения»
ISO 12100:2010	IDT	ГОСТ ISO 12100—2013 «Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO 6011:2003 Earth-moving machinery — Visual display of machine operation

[2] ISO 13849-1:2015 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

[3] ISO 20474-1:2017 Earth-moving machinery — Safety — Part 1: General requirements

[4] ISO/TS 19014-5 Earth-moving machinery — Functional safety — Part 5: Tables of performance levels

УДК 631.3:006.354 МКС 53.100 IDT

Ключевые слова: машины землеройные, функциональная безопасность, методика определения элементов систем управления, связанных с безопасностью, технические требования

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 15.10.2024. Подписано в печать 25.10.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,90.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

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

gost.e-ecolog.ru