ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71454— 2024/ IEC TR 63161:2022

НАЗНАЧЕНИЕ ТРЕБОВАНИЙ К ПОЛНОТЕ БЕЗОПАСНОСТИ

Обоснование

(IEC TR 63161:2022, IDT)

Издание официальное

Москва
Российский институт стандартизации
2024

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии 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 14 июня 2024 г. № 790-ст

4 Настоящий стандарт идентичен международному документу IEC TR 63161:2022 «Назначение требований к полноте безопасности. Обоснование» (IEC TR 63161:2022 «Assignment of a safety integrity requirements — Basic rationale», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им межгосударственные стандарты, сведения о которых приведены в дополнительном 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 ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

Введение

В настоящем стандарте представлен пример базовой логики обоснования при назначении требований к полноте безопасности для функции управления, связанной с безопасностью, в случае подхода, основанного на рисках, пояснены параметры назначения и описано, как эти параметры могут быть связаны с оценкой риска, выполненной в соответствии с ИСО 12100, и с требованиями безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

НАЗНАЧЕНИЕ ТРЕБОВАНИЙ К ПОЛНОТЕ БЕЗОПАСНОСТИ

Обоснование

Assignment of a safety integrity requirements.
Basic rationale

Дата введения — 2025—07—01

1 Область применения

Настоящий стандарт может быть использован в тех случаях, когда для машины или производственного предприятия выполнена оценка рисков в соответствии с ИСО 12100 и выбрана связанная с безопасностью функция управления, реализующая меры защиты от определенных опасностей. В настоящем стандарте описан пример базовой логики обоснования при назначении требования полноты безопасности для выбранной функции.

С одной стороны, представленное описание является общим и, насколько это возможно, не зависит от какого-либо конкретного инструментального средства или метода, который может быть использован для определения требования полноты безопасности. Это требование может быть выражено как уровень полноты безопасности (SIL) или уровень эффективности защиты (PL).

В качестве примера приведено обоснование, которое реализуется методами и средствами, использующими количественный подход, основанный на управлении рисками.

С другой стороны, логика, описанная в настоящем стандарте, может быть использована в качестве эталонной для оценки конкретных методов или средств при назначении полноты безопасности. Это позволяет определить, в какой степени рассматриваемое(ый) средство/метод соответствует количественному подходу, основанному на управлении рисками, и в каких случаях отклонения от этого подхода обусловлены другими причинами. Часто в реальных приложениях могут существовать веские основания, которые приводят к тому, что количественный подход, базирующийся на управлении рисками, может быть изменен или отменен. Обсуждение или оценка подобных оснований не входит в область применения. Как правило, причины отклонений рассматриваемого средства или метода от логики количественного подхода приводятся и обсуждаются в соответствующем разделе настоящего стандарта.

Примеры такого анализа приведены для общеиспользуемых методов и средств в форме графов рисков и матриц рисков.

Настоящий стандарт может быть использован для функций управления, связанных с безопасностью, во всех режимах применения: в непрерывном режиме, режиме с высоким уровнем запросов и режиме с низким уровнем запросов.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения к нему)]:

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

Издание официальное

3 Термины и определения

В настоящем стандарте применены следующие термины и определения.

ИСО и МЭК для применения в стандартизации поддерживают терминологические базы данных:

- Электропедия МЭК, доступная по адресу: http://www.electropedia.org/
- платформа онлайн-просмотра ИСО, доступная по адресу: https://www.iso.org/obp.

3.1 **вероятность** (probability): Вещественное число в интервале от 0 до 1, связанное со случайным событием и количественно выражающее вероятность возникновения этого события.

Примечание 1 — Для получения дополнительной информации см. 5.2.2.

[МЭК 60050-103:2009, 103-08-02, изменено — примечания 1 и 2 удалены и заменены новым примечанием]

3.2 **интенсивность события** (event rate): Частота с размерностью время$^{-1}$, обычно задаваемая в единицах час$^{-1}$ или год$^{-1}$, связанная со случайным событием и выражающая количественно частоту этого события.

Примечание 1 — Для получения дополнительной информации см. 5.2.3.

3.3 **допустимый риск** (tolerable risk): Риск, приемлемый при данных обстоятельствах на основании существующих в обществе ценностей.

Примечание 1 — Для целей ИСО/МЭК Руководство 51:2014 термины «приемлемый риск» и «допустимый риск» считают синонимами.

[ИСО/МЭК Руководство 51:2014, 3.15]

3.4 **предел допустимого риска** (tolerable risk limit): Риск, принимаемый в контексте данной опасности машины или технологического оборудования и определяемый количественно как интенсивность возникновения вреда с определенным уровнем существенности вследствие этой опасности.

Примечание 1 — Для получения дополнительной информации см. 5.9.5.

Примечание 2 — Вред с указанным уровнем существенности является необходимым атрибутом предела допустимого риска, однако он не выражается непосредственно в пределе.

Примечание 3 — Это определение добавляет элемент количественной оценки к общему определению допустимого риска, которое необязательно подразумевается в термине «допустимый риск» без модификатора «предел».

3.5 **опасное событие** (hazardous event): Событие, в результате которого может быть причинен вред.

Примечание 1 — Для получения дополнительной информации см. 4.3.2.

[ИСО 12100:2010, 3.9, изменено — примечание удалено и заменено новым]

3.6 **опасная ситуация** (hazardous situation): Обстоятельства, при которых люди подвергаются одной или нескольким опасностям.

Примечание 1 — Согласно ИСО 12100:2010, определение 3.10.

Примечание 2 — Для получения дополнительной информации см. 4.3.2.

[ИСО 12100:2010, 3.10, изменено — примечание удалено и заменено новым]

3.7 **запрос** (demand) <к функции управления безопасностью>: Событие, которое инициирует систему управления безопасностью выполнять свою функцию управления безопасностью.

Примечание 1 — Для получения дополнительной информации см. 5.9.2.

[МЭК 62061:2005, 3.2.25, изменено — сокращения SRECS и SRCF заменены словосочетаниями «система управления безопасностью» и «функция управления безопасностью» соответственно]

3.8 **инициирующее событие** (initiating event) <для функции управления безопасностью>: Ситуация, которая без функции безопасности приведет к повреждению или ущербу любого вида или уровня существенности.

Примечание 1 — Для получения дополнительной информации см. 5.9.3.

3.9 **запрос функции безопасности** (safety demand) <для функции управления безопасностью>: Ситуация, при которой произойдет авария с определенным уровнем вреда для людей, если она не будет предотвращена запрашиваемой функцией управления безопасностью.

Примечание 1 — Для получения дополнительной информации см. 5.9.4.

3.10 **уровень опасности** (hazard rate): Интенсивность аварий определенной степени тяжести в сочетании с конкретной возникающей опасностью при условии, что для предотвращения такого типа аварий установлена функция управления безопасностью.

3.11 **вероятность предотвращения или ограничения вреда** (probability of avoiding or limiting harm): Вероятность того, что потенциально подверженным воздействию лицам не будет причинен вред указанного уровня тяжести во время опасного события.

Примечание 1 — Для получения дополнительной информации см. 5.8.

3.12 **предотвратимость** (avoidability): Вероятность того, что потенциально подверженные воздействию сотрудники избегают воздействия опасности во время опасного события.

Примечание 1 — Для получения дополнительной информации см. 5.8.

3.13 **уязвимость** (vulnerability): Вероятность того, что подвергшимся воздействию лицам в опасной ситуации будет причинен вред определенного уровня тяжести.

Примечание 1 — Для получения дополнительной информации см. 5.8.

3.14 **скрытый отказ [сбой]** (hidden failure, hidden fault): Отказ или сбой в аппаратном средстве или программном обеспечении, который не проявляет себя и не обнаруживается специальными методами, когда он происходит.

Примечание 1 — Термин «скрытый» в данном смысле является дополнением к термину «обнаруженный» согласно МЭК 61511-1: 2016, 3.2.13.

Примечание 2 — Отказ или сбой в аппаратном средстве или программном обеспечении проявляет себя сам, например нарушением работы управляемого оборудования или его окружения.

Примечание 3 — Статус «скрытый» для отказа или сбоя в аппаратном средстве или программном обеспечении отменяется, когда этот отказ или сбой обнаруживается с помощью специальной(ого) проверки или метода или когда он становится обнаруженным из-за нарушения работы управляемого оборудования или его окружения. Это может быть связано, например, с изменением рабочего состояния или с сотрудником, приближающимся к оборудованию. Отказы, которые остаются скрытыми и не прекращают действие, не рассматривают.

4 Количественный подход, основанный на оценке риска

4.1 Общие положения

При подходе, основанном на риске, может быть задана функция управления безопасностью, позволяющая удерживать риск, вызванный машиной или процессом, ниже определенного максимального уровня — «предела допустимого риска».

С одной стороны, понятие «риск» определено в ИСО 12100, 3.12, как «сочетание вероятности нанесения и степени тяжести возможных травм или другого вреда здоровью». Хотя оба элемента определения могут быть оценены количественно, риск в контексте ИСО 12100 необязательно понимается как параметр, поддающийся количественной оценке. Это в еще большей степени относится к допустимому риску, т. е. к риску, который считается приемлемым в данном контексте на основе принятой в обществе системы ценностей.

С другой стороны, эффективность функции управления безопасностью для снижения риска, часто определяющая безотказность системы управления, представлена термином «полнота безопасности». Этот термин отражает степень доверия к функции управления безопасностью. Термин «полнота безопасности» имеет количественный аспект, который в полной мере описывается количеством отказов функции управления безопасностью. Такие отказы определяют количественно как целевую меру отказов, т. е. либо как среднюю вероятность отказа функции по запросу PFD_{avg}, либо как частоту опасных отказов функции в час PFH.

Назначение SIL — это процесс получения целевого значения для меры безопасности функции управления безопасностью на основе оценки риска. Если для определения требуемого уровня пол-

ноты безопасности использована оценка риска, то подразумевается, что элементы этой оценки риска установлены количественно. Таким образом, количественное значение выводится как результат выполнения процедуры, и обычно предполагается, что оно логически связано с допущениями, которые использовались в качестве входных данных.

Следовательно, существует базовая логика обоснования обеспечения функциональной безопасности, которая отражает все соответствующие аспекты применения функции управления безопасностью в количественных параметрах и устанавливает их логическую связь с пределом допустимого риска и целевой мерой отказов для функции.

Примечание — Информация об управлении рисками приведена в ИСО 31000:2018.

4.2 Последовательность шагов по обеспечению функциональной безопасности

Для обеспечения функциональной безопасности в контексте анализа рисков для машины или процесса могут быть использованы нижеприведенные шаги. В данном контексте SIL применяют в качестве условного обозначения для любого типа показателя полноты безопасности.

1) В результате анализа выявляется опасность.

2) С этой опасностью могут быть разработаны сценарии аварий: с указанием, какие лица могут пострадать от какого вида вреда, от каких узлов или функций машины, в каких режимах работы машины или процесса и т. д. — элементы сценария аварии приведены в 4.3.2.

3) Меры по смягчению последствий могут быть разработаны концептуально. В соответствии с 6.1 ИСО 12100:2010 приоритет мер снижается от безопасных по своей сути мер проектирования (шаг 1), далее рассматриваются защитные мероприятия и/или дополнительные меры защиты (шаг 2) и затем информация для использования (шаг 3). Функции безопасности — это форма «защитных мероприятий и/или дополнительных мер защиты».

4) Повторное обращение к общему проектному решению машины или технологического процесса приводит к решению о том, что будет реализована приборная функция управления. Не позднее данного этапа определяют функциональные возможности функции управления.

5) Можно определить связанные с безопасностью части приборной функции управления. Что касается опасности, описанной на шаге 1, то эта функция будет использована с целью предотвратить причинение вреда вследствие данной опасности, если эта функция работает так, как было задумано.

Примечание 1 — Требуемое значение SIL имеет отношение к функциональности, описанной на шаге 5. На этом шаге могут быть заданы предварительные условия для назначения SIL. Следующие шаги представляют собой более жесткое задание SIL. Обычно это можно сделать с помощью инструментария, основанного на графах, таблицах или системах баллов. Настоящее описание предполагает, что такого заранее разработанного инструмента не существует, но основную логику процесса можно реализовать, используя количественный подход. Это означает, что параметрам присвоены числовые значения и их связь с целевой мерой отказов выражена уравнениями в явном виде.

6) Можно определить класс существенности типичного сценария аварии (см. 4.3.4).

7) Можно определить интенсивность инициирующих событий для аварийных сценариев (см. 5.9.3).

8) Как только будет задано инициирующее событие, с помощью анализа рисков могут быть сформированы обстоятельства, которые могли бы предотвратить аварию заданного уровня существенности или более высокого, но без учета функции безопасности. Эти обстоятельства и условия могут быть обозначены параметрами $P_г$, $F_г$ или A_v и оценены количественно (см. 5.6, 5.7 и 5.8). Каждый из приведенных параметров является вероятностью в соответствии с 5.2.2, следовательно, будет определен количественно как действительное число в диапазоне от 0 до 1.

Примечание 2 — В методах, основанных на графах, и методах подсчета баллов числовой диапазон обычно является дискретным. Это означает, что используют только дискретные значения, каждое из которых представляет определенный диапазон непрерывного диапазона от 0 до 1.

9) Ожидаемая интенсивность несчастных случаев без учета влияния функции безопасности — «интенсивность запросов к функции безопасности» — может быть определена в соответствии с формулой (4).

10) Ожидаемая интенсивность аварий с учетом функции безопасности — «уровень опасности» — может быть определена в соответствии с формулой (6).

11) Допустимую интенсивность отказов функции безопасности PFH можно определить по формуле (7). Это означает, что ожидаемая интенсивность аварий сравнивается с допустимым пределом $L_{(S)}$ для данного класса существенности.

12) Назначение режима запросов. До этого момента функцию безопасности рассматривают как функцию, работающую в режиме с высокой частотой запросов от приложения. Соответственно, интенсивность инициирующих событий до этого не использована при формировании требования [см. формулу (7) и приведенное в 6.2 объяснение]. Тем не менее можно определить интенсивность инициирующих событий l_R и интенсивность запросов к функции безопасности D_R:

- l_R и D_R являются исходными данными для принятия решения о выборе между режимом работы с высокой частотой запросов и режимом работы с низкой частотой запросов;
- l_R необходима для определения и/или оценки интенсивности и времени реакции на диагностические меры.

При наличии данных об интенсивности инициирующих событий l_R, интенсивности запросов к функции безопасности D_R и других особенностях приложения, таких как возможность проведения регулярных контрольных испытаний, можно решить, следует ли рассматривать эту функцию как функцию, работающую в режиме с низкой частотой запросов (см. раздел 7).

Примечание 3 — Более подробная информация об интенсивности запросов и определении требуемого уровня SIL приведена в IEC TR 63039:2016.

Блок-схема на рисунке 1 описывает вышеперечисленные шаги.

Примечание 4 — Более подробная информация о тех методах, которые следует применять для отдельных этапов, представленных на рисунке 1, приведена в ИСО 31010:2019.

4.3 Справочная информация

4.3.1 Общие положения

Количественные параметры при оценке риска неизменно связаны со справочной информацией, которая не является количественной, т. е. эта информация при оценке риска и назначении SIL не представлена в форме параметров, имеющих значение. Тем не менее, являясь справочной, она обеспечивает обоснование для тех параметров, которые могут быть определены количественно.

4.3.2 Сценарий аварии

Функцию безопасности можно определить как защиту от конкретных аварий. Сценарий аварии можно представить как краткое обобщенное описание, связывающее в простом понятном изложении все аспекты, общие для рассматриваемых аварий. Сценарий аварии может выявить:

- какой тип машин или оборудования задействован в аварии;
- какой аспект оборудования или его работы вызывает аварию; что такое опасность; примеры того, как опасности могут быть описаны с указанием их происхождения, последствий и ситуационных зарисовок, приведены в ИСО 12100:2010, приложение В;
- на кого может воздействовать, в каком режиме работы оборудования;
- каким образом могут быть затронуты люди — какой ущерб они понесут, какой уровень существенности;
- какие исходные события могут привести к аварии: отказы деталей, ошибки человека, внешние воздействия;
- каким образом событие будет развиваться от начальных событий до конечных аварий. Существуют ли конкретные промежуточные этапы, которые можно было бы определить как типичные этапы? Существуют ли особые граничные условия, влияющие на ход событий?

В последовательности событий сценария аварии две стадии имеют конкретные определения в ИСО 12100 (см. также таблицу 1 в 5.10);

опасный случай: событие, которое может причинить вред (см. ИСО 12100:2010, 3.9). Это означает, что оборудование оказывает потенциально опасное воздействие на опасную зону, при этом доступ людей в такую опасную зону не предотвращается;

опасная ситуация: обстоятельство, при котором человек подвергается как минимум одной опасности (см. ИСО 12100:2010, 3.10). Это опасный случай с дополнительным условием, при котором сотрудник действительно полностью или частично находится в опасной зоне.

Рисунок 1 — Последовательность действий по обеспечению функциональной безопасности

4.3.3 Опасная зона

В контексте сценария аварии опасная зона может быть задана как объем и/или поверхность внутри или вокруг машины, где сотрудники могут подвергаться опасности, создаваемой машиной. Опасная зона может быть определена в качестве параметра воздействия (см. также ИСО 12100:2010, 3.11).

4.3.4 Существенность вреда

Риск определен в ИСО 12100:2010, 3.12, как «сочетание вероятности причинения вреда и существенности этого вреда». Существенность вреда обычно выражается в классах существенности: S1, S2 и т. д. Каждый из этих классов определен примерным описанием вреда, например:

- класс существенности S1: легкие травмы, включая царапины и незначительные ушибы, требующие оказания первой помощи без медицинского вмешательства;
- класс существенности S2: обратимые травмы, в том числе тяжелые рваные раны, колотые раны и значительные ушибы, требующие внимания практикующего врача;

и т. д.

Обычно избегают количественного выражения существенности с помощью числового значения и единицы измерения. Соответственно, выражение риска в конкретных единицах также не является установившейся практикой. Вместо этого оценка опасности и риска определяет применимый класс существенности как качественный показатель риска. Таким образом, существенность является граничным условием количественной оценки, но явно в нее не включена.

4.3.5 Функция управления безопасностью

Чтобы установить значение SIL, необходимо определить, какие типы аварий может предотвратить оцениваемая функция. Присвоение значения SIL функции безопасности связано с риском, который функция безопасности может снизить. Поэтому в качестве граничного условия для задания будет использовано краткое функциональное описание этой функции, например: какие сигналы, при каких уровнях или значениях запускают функцию (сигналы процесса), что она делает (останавливает определенное движение, прерывает линию электропередачи, закрывает линию передачи данных, устанавливает что-либо в определенное положение и т. д.).

5 Количественные параметры, описывающие функциональную безопасность

5.1 Общие положения

Параметры, рассмотренные в настоящем разделе, описывают либо частоту определенных событий во времени, либо вероятность событий при заданных начальных условиях. Эти элементы могут быть количественно оценены по числовой шкале.

5.2 Типы параметров

5.2.1 Общие положения

Количественные параметры при оценке риска можно разделить на два различных типа представления:

- как точное значение вероятности;
- как интенсивность событий.

Для количественной оценки риска и присвоения значения SIL это различие можно рассматривать как значимое.

5.2.2 Вероятность

Точное значение вероятности количественно определяет математическое ожидание того, что данное утверждение истинно при заданных условиях. Это может быть выражено действительным безразмерным числом от 0 до 1.

Пример — Насколько вероятно, что сотрудник получит серьезную травму, когда будет находиться внутри здания, когда оно рухнет?

Утверждение: получит, как минимум, серьезную травму.

Условие: находится внутри здания, когда оно рушится.

Ответ будет дан в терминах значения вероятности:

- 0 будет означать, что обрушение здания никогда не приведет к более серьезным травмам сотрудника, находящегося внутри здания;

- 1 будет означать, что обрушение вызовет, по крайней мере, серьезную травму.

В этом примере наличия доступной информации будет недостаточно, чтобы принять решение о значении вероятности с какой-либо уверенностью. Ответ будет критически зависеть, например, от характеристик здания и местонахождения сотрудника внутри него.

5.2.3 Интенсивность событий

Интенсивность событий может быть использована для количественной оценки ожидаемой частоты возникновения данного события в данное время и в заданной системе отсчета. Это выражается как отношение ожидаемого количества событий к продолжительности времени. Размерность интенсивности событий равна времени$^{-1}$, обычно в единицах 1/ч или 1/год.

Интенсивность отказов, например, представляет собой интенсивность событий, которая количественно определяет ожидаемое число отказов для заданного комплекта оборудования за время использования этого комплекта. Системой отсчета в этом случае является один комплект указанного оборудования. Для интенсивности отказов оборудования система отсчета самоочевидна — один комплект

исследуемого оборудования. Интенсивность событий при оценке риска связана с аварийными событиями. В них могут участвовать разные люди и разное оборудование. Интенсивность событий может быть определена количественно и актуальна только в том случае, если в этих случаях система отсчета описана достаточно точно.

5.3 Вероятность причинения вреда

Вероятность причинения вреда обычно выражается в формате «количество событий, связанных с заданной существенностью, в единицу времени». Это может быть применено к определенному объему оборудования или к процессу. Подобный формат может принимать характеристики интенсивности событий, как определено в 5.2.3. Соответственно, вероятность причинения вреда — это не вероятность, а скорее, интенсивность событий. Таким образом, вероятность причинения вреда является функцией от других параметров (см. раздел 8 для соотношений).

5.4 Количественная оценка риска

При понимании существенности вреда и вероятности возникновения вреда, как описано в 4.3.4 и 5.3, определение риска в ИСО 12100 может быть выражено в количественной форме следующим образом:

$$R = S \cdot E_R, \quad (1)$$

где R — риск;

S — существенность;

E_R — коэффициент для рассматриваемых событий с учетом вреда заданной существенности.

При существенности в качестве граничного условия риск, соответственно, количественно определяют как интенсивность событий.

Для отдельной оценки риска могут быть определены различные уровни риска в зависимости от мер по снижению риска и предполагаемых факторов. Если такие допущения не связаны с различными уровнями существенности, то они могут быть количественно выражены различными значениями интенсивностей событий. Поэтому различные виды риска могут быть представлены следующим образом: каждый по отношению к соответствующей интенсивности событий:

- риск до его снижения любыми факторами: интенсивность инициирующих событий I_R (см. 5.10);
- риск без учета функции безопасности: интенсивность запросов к функции безопасности D_R (см. 5.9.4);
- риск с учетом функции безопасности: уровень опасности H_R (см. 3.10);
- допустимый риск: предел допустимого риска $L_{(S)}$ (см. 5.10).

См. также рисунок 2.

5.5 Целевая мера отказа

Целевая мера отказа для функции безопасности может быть задана как количественная мера вероятности отказа, приписываемая функции.

Примечание 1 — Следующее определение целевой меры отказа дано в МЭК 61508-4:2010, 3.5.17: заданная вероятность отказов в опасном режиме, которая должна быть достигнута в соответствии с требованиями к полноте безопасности.

В зависимости от режима применения, непрерывного, с высокой частотой запросов или низкой частотой запросов, целевая мера отказа может быть определена либо как интенсивность событий, либо как вероятность следующим образом:

- режим с высокой частотой запросов или непрерывный режим работы — интенсивность отказов функции безопасности, PFH.

PFH — это интенсивность опасных отказов функции безопасности, которые не распознаются и не устраняются диагностикой до того, как может произойти авария;

- режим с низкой частотой запросов — средняя вероятность опасного отказа при выполнении функции безопасности по запросу, PFD_{avg}.

PFD_{avg} — это вероятность обнаружения опасного сбоя функции как среднее значение по времени. Вероятность отказа PFD является функцией времени и изменяется в период проведения диагностических испытаний и контрольных проверок. Если средние периоды между запросами функции безопасности достаточно большие по сравнению с ритмом проверок и испытаний, то PFD может быть представлена ее средним значением во времени, т. е. PFD_{avg}.

На шкале целевой меры отказов SIL или PL представляют собой интервалы между дискретными уровнями: SIL1, SIL2, SIL3 или PLa, PLb и т. д. Основанные на графах методы обеспечения функциональной безопасности обычно дают только требуемое значение SIL или PL, которое в этом случае понимается как предельное значение соответствующего интервала, т. е. допустимый максимум.

Для режима с низкой частотой запросов, с высокой частотой запросов или непрерывного режима работы целевая мера отказов для функции безопасности может быть определена количественно с учетом мер или условий по снижению риска, отличных от функции безопасности. Подобные меры или условия могут быть представлены параметрами P_r, F_r или A_v или могут быть учтены в интенсивности инициирующих событий l_R (см. 5.6, 5.7 и 5.8).

Примечание 2 — Дополнительную информацию об интенсивности запросов можно найти в IEC TR 63039:2016 «Вероятностный анализ риска технических систем. Оценка интенсивности конечного события для заданного начального состояния».

5.6 Вероятность возникновения опасного события P_r

Опасное событие — это «событие, которое может причинить вред» (см. 3.5). Опасная ситуация может быть предотвращена, если действует функция безопасности. Опасный отказ функции безопасности является необходимой предпосылкой возникновения опасной ситуации. Однако не каждый отказ функции безопасности обязательно приводит к опасному событию. Если, например, установка заготовки в механообрабатывающем станке рассмотрена как функция безопасности, то отказ этой функции во многих случаях может привести к выбросу деталей только в пределах пространства защитного ограждения. В этих случаях отсутствует опасное воздействие в опасной зоне, в которой могут находиться люди.

Определение «Опасное событие не может произойти» заменяют на определение «Опасная ситуация будет предотвращена».

Пример вопроса для оценки.

Если предположить, что функция безопасности отказала, какая вероятность того, что произойдет опасное событие?

Пример ответа для оценки.

Вероятность возникновения опасного события — параметр P_r. Он выражает вероятность как действительное число от 0 до 1:

- 0 означает, что опасное событие никогда не произойдет вследствие отказа функции безопасности;
- 1 означает, что опасное событие обязательно произойдет при каждом опасном отказе функции безопасности.

Отказ функции безопасности может быть обнаружен до возникновения опасной ситуации. Можно предположить, что после этого опасная работа машины будет прекращена и ее функционирование не возобновится до тех пор, пока функция безопасности не будет восстановлена. В этом случае отказ функции безопасности не приводит к возникновению опасной ситуации. Вероятность этого события равна $1 – P_r$, т. е. дополнению к P_r.

Параметр P_r включает в себя диагностику процесса отказа функции безопасности. Это означает, что отказ функции безопасности может быть обнаружен при нарушении технологического процесса и машина переводится в безопасное состояние до того, как произойдет опасное событие. Как правило, это относится к функциям безопасности, которые также выполняют функции в обычном рабочем процессе. Если функция безопасности может выйти из строя без явных признаков, то отказ является скрытым. Для скрытых отказов параметр P_r обычно равен 1.

5.7 Параметр воздействия F_r

Наличие опасного события еще не означает, что человек действительно подвергается опасности. Только в опасной ситуации человек действительно подвергается потенциально опасным воздействиям, т. е. опасности. Это дополнительное условие может быть определено количественно с помощью параметра воздействия F_r.

Пример вопроса для оценки.

Предполагая, что опасное событие прогнозируется в опасной зоне, какая вероятность того, что в опасной зоне одновременно находится по крайней мере один сотрудник?

Пример ответа для оценки.

Параметр воздействия F_r определен как вероятность F_r и выражен действительным числом от 0 до 1:

- 0 означает, что в опасной зоне не может быть персонала в то время, когда происходит опасное событие;
- 1 означает, что каждый раз, когда происходит опасное событие, в опасной зоне рано или поздно окажется сотрудник, но в любом случае с перекрытием во времени.

Для количественной оценки параметра F_r рабочая ситуация может быть оценена с учетом таких факторов, как:

- необходимость доступа в опасную зону, связанную с режимом работы (настройка/автоматический/ручной/специальный режим);
- характер доступа (загрузка материалов, устранение неисправности, техническое обслуживание или ремонт);
- время, проведенное в опасной зоне, t_F, ч;
- частота посещения опасной зоны f_F, $ч^{-1}$.

Если ожидается, что в отдельно взятый момент времени произойдет опасное событие, например взрыв, то параметр F_r эквивалентен вероятности того, что опасная зона в этот момент занята. В этом случае параметр F_r можно определить по частоте присутствия персонала в опасной зоне и по средней продолжительности его присутствия по формуле

$$F_r = f_F \cdot t_F. \quad (2)$$

Для опасных событий, которые длятся в течение продолжительного периода времени, параметр воздействия не будет равен временной доле пребывания в опасной зоне. В типичном примере опасностью может быть контакт между сотрудником и движущимися частями оборудования во время нормальной работы машины. Такие опасности могут быть защищены световыми завесами, защитными дверями или аналогичными устройствами. Если функция безопасности подобного типа выходит из строя в опасном режиме и это не обнаруживается (диагностика отсутствует), то машина может продолжать работать в обычном режиме. Отказ функции безопасности не влияет на рабочие функции машины. Отказ — скрытый (см. 5.6). Опасное событие может перерасти в опасную ситуацию, как только сотрудник войдет в опасную зону, не будучи защищенным функцией безопасности. В этих и аналогичных случаях параметр воздействия F_r может быть установлен равным 1 независимо от частоты доступа f_F и времени, проведенного в опасной зоне, t_F.

Другими словами, если опасное событие может длиться в течение продолжительного периода времени в той зоне, которую персонал регулярно посещает, то в определенный момент сотрудник, получивший доступ после отказа функции безопасности, будет подвержен опасности. При этих граничных условиях отсутствие персонала в момент отказа функции безопасности не снижает риск. (Еще существует вероятность того, что отказ будет обнаружен и двигатель будет остановлен до того, как сотрудник войдет в опасную зону. Это может быть учтено в параметре P_r, вероятности возникновения опасного события.)

5.8 Вероятность предотвращения или ограничения вреда A_v

5.8.1 Общие положения

Опасная ситуация подразумевает, что сотрудник действительно подвергается опасности, однако это еще не означает, что ему действительно причинен вред. Подвергшийся воздействию сотрудник мог бы распознать ситуацию и избежать вреда собственными целенаправленными действиями. Подвергшийся воздействию персонал также может случайно избежать опасности. Эти дополнительные условия могут быть количественно определены с помощью вероятности предотвращения или ограничения вреда — параметра A_v.

Пример вопроса для оценки.

Если предположить, что сотрудник подвергается опасному событию в опасной зоне, то какая вероятность того, что ему действительно будет причинен вред?

Пример ответа для оценки параметра A_v.

Вероятность предотвращения или ограничения вреда определена как вероятность и выражена действительным числом от 0 до 1:

- 1 означает, что сотрудник, подвергшийся воздействию, будет избегать опасного воздействия и таким образом не пострадает;
- 0 означает, что пострадавший понесет ущерб в каждом случае.

Следует отметить, что по отношению к риску полярность параметра A_v может быть противоположной по отношению к полярности параметров P_r и F_r. В то время как для P_r и F_r значение 1 указывает на окончание шкалы высокого риска, для параметра A_v все наоборот. Соответственно, для конечной оценки можно использовать дополнение к A_v: $1 - A_v$.

Параметр A_v согласно настоящему подразделу сочетает в себе два аспекта предотвращения:

- предотвращение вреда целенаправленными действиями лица, подвергающегося опасности;
- предотвращение вреда благодаря благоприятным обстоятельствам или благоприятному стечению обстоятельств.

Эти два аспекта могут быть выражены отдельно. Первый аспект можно обозначить параметром «предотвратимость» (A), а второй аспект — параметром «уязвимость» (V).

Если уязвимость используется как отдельный параметр в назначении SIL, то параметр A_v в соответствии с 5.7 будет заменен на A и V следующим образом:

$$(1 - A_v) = (1 - A) \cdot V. \quad (3)$$

5.8.2 Уязвимость *V*

Уязвимость может быть задана как вероятность того, что лицам, подвергшимся воздействию опасной ситуации, нанесен вред определенного уровня.

Параметр уязвимости V может представлять собой предотвращение вреда благодаря благоприятным обстоятельствам или благоприятному стечению обстоятельств.

Для следующих аспектов опасной ситуации может быть уместно использовать уязвимость в качестве конкретного параметра:

- токсичность и/или концентрация выброса вредных веществ, например дымовых газов при сценарии пожара, или общехимических веществ при сценарии аварии на химическом производстве;
- вероятность поражения осколками в сценариях, предусматривающих механическое разрушение быстро движущихся механизмов.

Пример вопроса для оценки.

Если сотрудник подвергается опасному событию в опасной зоне и не предпринимает действий для предотвращения или смягчения воздействия, то какая вероятность того, что ему действительно будет причинен вред?

Пример ответа для оценки.

Параметр V «Уязвимость» определен как вероятность и выражен действительным числом от 0 до 1:

- 0 означает, что подвергающемуся воздействию лицу не будет нанесен вред указанного уровня, даже если оно будет подвержено опасности;
- 1 означает, что подвергающемуся воздействию лицу будет причинен вред указанного уровня в каждом случае воздействия опасности.

5.8.3 Предотвратимость *A*

Предотвратимость A может быть определена как вероятность того, что потенциально подверженные опасности лица избегают воздействия опасности во время опасного события.

Пример ответа для оценки.

Параметр A «Предотвратимость» определен как вероятность и выражен действительным числом от 0 до 1:

- 1 означает, что сотрудник, подвергшийся воздействию, неизменно будет избегать опасной ситуации;
- 0 означает, что пострадавший не сможет избежать опасной ситуации.

Для случая скрытых отказов значение, которое можно принять для параметра A, подчиняется аналогичному граничному условию, как и для P_r и F_r: предотвращение вреда может быть рассмотрено как снижение риска только при допущении того, что отказ функции безопасности распознается, и ситуация восстанавливается до безопасного уровня вследствие определенного воздействия. Если оценка приводит к такому результату, при котором вреда можно было бы избежать по благоприятному стечению обстоятельств, даже не будучи замеченным, то для параметра A невозможно определять соответствующую вероятность.

Тот факт, что отказ скрыт, не будет автоматически означать, что значение параметра A равно 0, если последующее опасное событие будет способствовать его выявлению.

Пример — Случай превышения скорости предотвратить невозможно, так как событие, связанное с причинением вреда, происходит так быстро, что, как правило, ни само событие, ни его последствия не могут быть предотвращены действиями сотрудника. Таким образом, вероятность избежать опасного события будет равна 0.

5.9 Типы запросов и соответствующие интенсивности событий

5.9.1 Классы событий

Термин «запрос функции безопасности» может описывать различные классы событий. Описаниями событий могут быть, например, нижеприведенные.

1) Могут быть заданы предварительно определенные условия для срабатывания функции безопасности. В примере световой завесы, защищающей от контакта с движущимися частями металлорежущего оборудования, это описание события будет относиться к проникновению предмета или части тела в плоскость завесы, достаточной по ширине и по продолжительности для срабатывания функции.

2) Заранее определенные условия для срабатывания функции безопасности могут быть заданы в той ситуации, когда функция безопасности необходима для предотвращения ущерба или вреда любого характера. В рассматриваемом примере это применимо, если предмет или часть тела настолько глубоко проникают в плоскость завесы, что фактически вступают в контакт с движущимися частями машины. В отличие от условий по перечислению 1 прежде всего исключаются запасы безопасности.

3) Заранее определенные условия для срабатывания функции безопасности могут быть заданы в той ситуации, когда функция безопасности необходима для предотвращения причинения вреда персоналу, и вред будет не ниже уровня существенности, принятой при назначении SIL. В данном примере это применимо к той ситуации, когда рука сотрудника протягивается к движущимся частям, так что рука или ее части будут отрублены, если машина не будет вовремя остановлена.

Приведенные выше описания событий становятся более конкретными при последовательности событий от перечисления 1 к событиям по перечислению 3. Каждый класс событий в приведенной последовательности может быть включен как подмножество в предыдущий класс событий. Соответственно, как правило, интенсивность событий уменьшается для типов событий в последовательности от 1 до 3. В настоящем стандарте для каждого из следующих событий на примере дается конкретное определение:

- запрос по 3.7 и 5.9.2;
- исходное событие по 3.8 и 5.9.3;
- требование безопасности по 3.9 и 5.9.4.

5.9.2 Запрос и интенсивность запросов

Запрос и интенсивность запросов могут быть применены к любой ситуации, которая вызывает срабатывание функции безопасности в данном приложении. Интенсивность запросов таким образом не является непосредственной мерой фактического риска несчастных случаев в этом приложении. Интенсивность срабатывания функции управления безопасностью также может быть определена ограничениями аппаратуры и запасами безопасности, которые могут быть использованы в отношении пределов срабатывания. Следовательно, интенсивность запросов согласно 3.7 обычно не подходит в качестве входных данных для присвоения SIL.

5.9.3 Инициирующие события и интенсивность инициирующих событий l_R

Инициирующее событие может быть задано как ситуация, которая приведет к ущербу или вреду любого вида, если она не будет предотвращена функцией безопасности. К таким видам относят все случаи потенциального повреждения оборудования и продукции, а также все незначительные повреждения, которые необходимо предотвратить с помощью функции безопасности, но которые не рассматриваются конкретно при задании SIL.

Инициирующие события могут быть связаны со следующими причинами:

- помехи или отказы: механические отказы оборудования, отказы исполнительных механизмов, таких как двигатели или пневматические/гидравлические приводы, внешние воздействия (например, колебания электропитания), ошибки сотрудника при управлении оборудованием;

- характер рабочего процесса машины: движение режущих или прессующих частей, непосредственное взаимодействие частей машины с сотрудником в рабочем цикле машины, непосредственное взаимодействие частей машины с человеком при загрузке/разгрузке, настройке эксплуатации или обслуживании;

- отказ функции непрерывного управления, которая необходима для предотвращения немедленного создания опасной ситуации в процессе работы машины.

Вышеперечисленные причины инициирующих событий типичны для приложений, работающих в режиме с низкой частотой запросов, приложений с высокой частотой запросов и в режиме с непрерывными запросами, в последовательности перечислений. Частота возникновения может быть описана интенсивностью событий, интенсивностью инициирующих событий, обозначаемой как I_R.

Функция безопасности, как правило, предназначена для распознавания инициирующих событий и реагирования на них. Предполагается, что каждое инициирующее событие будет запускать реакцию функции безопасности, пока эта функция работоспособна.

Если последствия инициирующих отказов смягчаются факторами, которые считаются присущими машине и/или ее рабочему процессу, то эти факторы также можно учитывать в интенсивности инициирующих событий. Например, если сотрудник, подвергающийся воздействию, не является оператором машины (обычно в перерабатывающих производствах), то действия оператора, предотвращающие опасные события, обычно могут быть учтены в интенсивности инициирующих событий I_R, а не в параметре предотвратимости A_v.

Если функция безопасности предназначена для предотвращения контакта персонала с движущимися механизмами, то исходное событие может быть определено либо опасными движениями машины, либо опасными движениями незащищенного сотрудника — в зависимости от того, какое из них может привести к срабатыванию функции безопасности.

5.9.4 Запросы функции безопасности и интенсивность запросов функции безопасности D_R

Запрос функции безопасности можно определить как ситуацию, в которой авария с определенным уровнем вреда для персонала может произойти, если только эта функция управления безопасностью ее не предотвратит. Соответственно, интенсивность соответствующих событий D_R может быть определена как интенсивность аварий указанного типа с заданным уровнем вреда для персонала, которые бы происходили при отсутствии функции безопасности.

Запрос функции безопасности и интенсивность запросов функции безопасности могут иметь особое значение в контексте оценки риска, которая используется в качестве основы для назначения SIL и которая предполагает заданный уровень вреда людям как элемент сценария аварии. В данном контексте функция запрашивается с такой же интенсивностью, с какой она фактически должна предотвращать указанную аварию.

Интенсивность запросов функции безопасности D_R может быть получена из интенсивности инициирующих причин путем применения любого снижения риска, которое может быть заявлено для параметров P_r, F_r или $1 - A_v$. Другими словами, интенсивность запросов D_R к функции безопасности будет представлять собой интенсивность инициирующих событий I_R, уменьшенную на общую вероятность того, что указанный вред сотрудникам будет предотвращен и что машина будет переведена в безопасное состояние, не предполагая вмешательства со стороны функции безопасности. Это можно определить по формуле

$$D_R = I_R \cdot P_r \cdot F_r \cdot (1 - A_v). \quad (4)$$

В формуле (4) I_R представляет собой интенсивность инициирующих событий. В случае возникновения инициирующего события аварию можно было бы предотвратить факторами, представленными в $P_r \cdot F_r \cdot (1 - A_v)$. Если авария не предотвращена этими факторами, то ее предотвратит функция безопасности.

Риск, который остается в интенсивности запросов D_R в качестве интенсивности событий, представляет собой риск, который можно снизить с помощью функции безопасности.

На рисунке 2 представлены инициирующие события и запросы с соответствующими интенсивностями событий в модели риска.

Отдельные слои защиты показаны слева направо в той последовательности, в которой они рассмотрены при назначении SIL. В реальной последовательности событий функция безопасности занимала бы первое место слева, немедленно реагируя на исходные события (см. 3.10 для I_R, 4.3.2 для опасного события и опасной ситуации и 5.10 для уровня опасности H_R).

5.9.5 Предел допустимого риска — параметр $L_{(S)}$

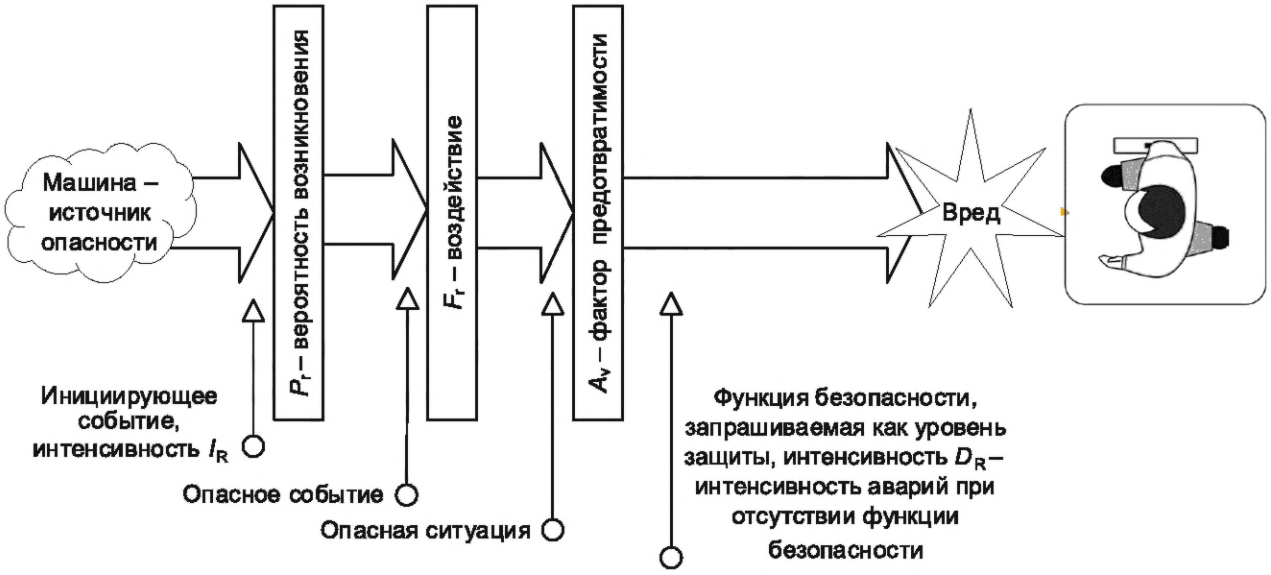
Для аварий определенного уровня существенности применяют максимальную интенсивность событий, которая допускается при оценке риска. Она соответствует максимально допустимому риску:

$$L_{(S)} = S \cdot E_{RMAX}, \quad (5)$$

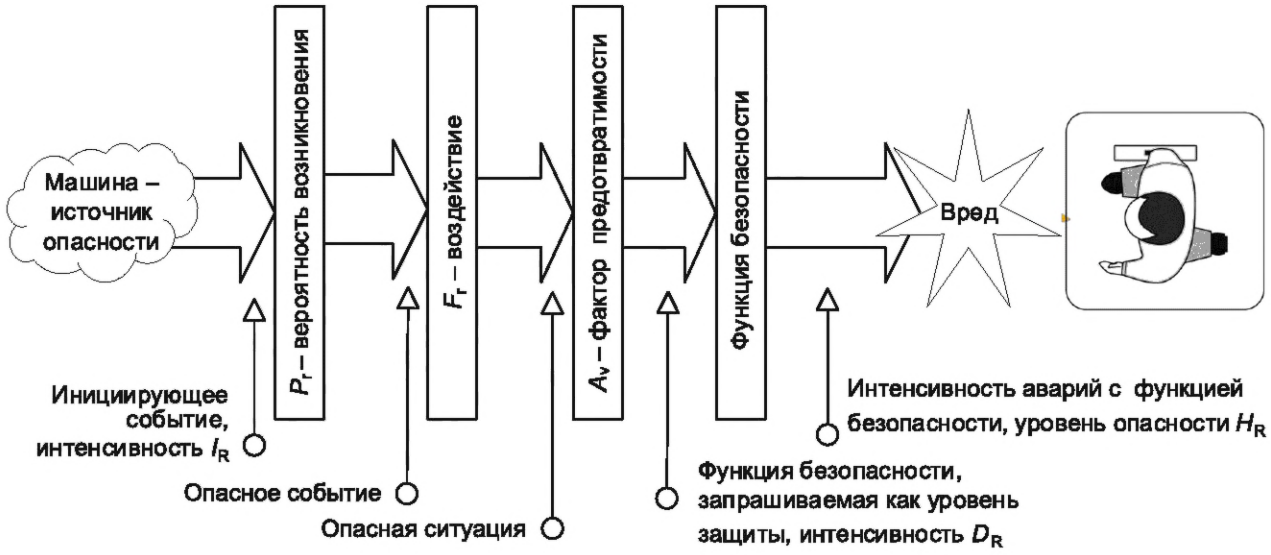
где $L_{(S)}$ — предел допустимого риска для данной существенности;

S — существенность;

E_{RMAX} — максимально допустимая интенсивность событий для данной существенности.



a) Ситуация без функции безопасности



b) Ситуация с функцией безопасности

Рисунок 2 — Слои защиты, интенсивности событий и их взаимосвязь

Для каждого уровня существенности аварийного события необходим предел допустимого риска. Его можно определить по формуле (5). $L_{(S)}$ может быть задан как интенсивность событий с числом событий за единицу времени (время$^{-1}$), обычно в единицах 1/год.

Чем выше класс существенности аварии, тем ниже может быть численное значение соответствующего предела допустимого риска $L_{(S)}$. Как правило, значения $L_{(S)}$ для ряда классов существенности располагаются равными шагами по десятичной логарифмической шкале, например 10 в год для существенности S1, 10^{-1} в год для существенности S2 и т. д. Менее существенные аварии допускаются чаще, чем аварии более существенные.

Предел допустимого риска обычно не указывают явно в основанных на графах методах при назначении SIL, хотя его часто можно вывести из таких графов. Логически невозможно вывести требование по снижению риска из оценки риска, не подразумевая предела допустимого риска.

5.10 Дополнительные параметры

Следующие определения дополнительных параметров могут быть целесообразны для описания логики назначения SIL в форме уравнений, т. е. логически точным образом:

H_R — интенсивность несчастных случаев, даже если функция установлена. В соответствующей литературе это часто называют «уровень опасности»;

T_R — интенсивность контрольной проверки функции безопасности;

T_I — интервал контрольных проверок функции безопасности, обратная величина интенсивности контрольных проверок $T_R = 1/T_I$;

D_I — среднее время между запросами функции безопасности;

PFD_{avg} — вероятность отказа функции безопасности по запросу;

RRF — коэффициент снижения риска. Отношение интенсивности тех аварий, которые произошли бы без функции безопасности, к тем, которые произошли бы с функцией безопасности. RRF также можно определить как требование RRF_{req}. В этом случае знаменатель может быть задан пределом допустимого риска: $RRF_{req} = D_R/L_{(S)}$.

Если функция безопасности работает в режиме с низкой частотой запросов, так что ей может быть присвоена PFD_{avg} (средняя вероятность отказа при запросе), коэффициент снижения риска также может быть выражен как значение, обратное PFD_{avg}: $RRF = 1/PFD_{avg}$.

Эти определения представлены для полноты, однако далее они не использованы в настоящем стандарте.

Таблица 1 — Обзор параметров

Обозначение	Параметр	Значение	Размерность
PFH	Вероятность опасного отказа в час	Интенсивность опасных отказов функции безопасности в режиме с высокой частотой запросов или в непрерывном режиме работы, что приводит к увеличению оцениваемого риска (см. 5.5)	Интенсивность событий, *n*/время
PFD_{avg}	Средняя вероятность отказа по запросу	Применимо к функции безопасности только в режиме работы с низкой частотой запросов: вероятность нахождения функции безопасности в состоянии отказа, как среднее значение по времени (см. 5.5)	Безразмерная, действительное число от 0 до 1
P_r	Вероятность возникновения опасного события	Вероятность того, что опасное событие произойдет в результате отказа функции безопасности (см. 5.6)	Безразмерная, действительное число от 0 до 1
F_r	Воздействие	Вероятность того, что в момент опасного события человек находится в опасной зоне (см. 5.7)	Безразмерное, действительное число от 0 до 1
A_v	Вероятность предотвращения или ограничения вреда	Вероятность того, что потенциально подвергшиеся воздействию лица не получат вреда определенного уровня существенности во время опасного события (см. 5.8)	Безразмерная, действительное число от 0 до 1
A	Предотвратимость	Вероятность того, что потенциально подверженные опасности лица избегают воздействия опасности во время опасного события (см. 5.8.3)	Безразмерная, действительное число от 0 до 1
V	Уязвимость	Вероятность того, что лица, подвергшиеся воздействию опасной ситуации, действительно понесут вред определенного уровня существенности (см. 5.9)	Безразмерная, действительное число от 0 до 1
I_R	Интенсивность инициирующих событий	Интенсивность событий, которые запускают функцию безопасности, поскольку состояние машины или положение персонала по отношению к машине несут потенциальную опасность (см. 5.9.3)	Интенсивность событий, *n*/время

Окончание таблицы 1

Обозначение	Параметр	Значение	Размерность
D_R	Интенсивность запросов безопасности	Интенсивность событий, при которых вред может быть причинен без вмешательства функции безопасности (см. 5.9.4)	Интенсивность событий, *n*/время
D_I	Интервал запроса функции безопасности	Средний период времени между двумя запросами функции безопасности	Время
S	Класс существенности	S является показателем величины вреда, причиняемого единичным типичным несчастным случаем с рассматриваемой опасностью (см. 4.3.4)	Безразмерный, только качественное описание
$L_{(S)}$	Предел допустимого риска	Максимально допустимая средняя интенсивность события существенности S рассматриваемой опасности (см. 5.9.5)	Интенсивность события, *n*/время
H_R	Уровень опасности	Интенсивность фактических несчастных случаев с ожидаемым ущербом (см. 3.10)	Интенсивность события, *n*/время
T_I	Интервал проверки	Интервал контрольных проверок функции безопасности, актуальный только в режиме с низкой частотой запросов (см. 5.10)	Время
T_R	Интенсивность проверки	Интенсивность контрольных проверок функции безопасности, применимая только в режиме с низкой частотой запросов (см. 5.10)	Интенсивность события, *n*/время
RRF	Коэффициент снижения риска	Отношение интенсивности аварий, которые произошли бы без функции безопасности, к интенсивности аварий, которые произошли бы с функцией безопасности, применимое только в режиме с низкой частотой запросов (см. 5.10)	Безразмерный, положительное действительное число >1

6 Общие принципы обеспечения функциональной безопасности

6.1 Основные положения

6.1.1 Применимость к полным функциям

Обеспечение функциональной безопасности, выполняемое на основе оценки риска, неизменно применяется ко всей функции безопасности. Только вся функция, включая все подсистемы, способна снизить риск. Чтобы присвоить значение SIL подсистеме всей системы безопасности, необходимо рассмотреть максимально допустимую вероятность отказов для всей системы и, разделив ее на части, для каждой подсистемы.

6.1.2 Связь с риском

Чем выше риск, который может быть определен для функции безопасности в качестве целевого снижения, тем выше требования к полноте безопасности для функции безопасности. Соотношение между покрываемым риском и требуемой полнотой безопасности может быть определено пределом допустимого риска $L_{(S)}$.

Требование полноты безопасности к функции безопасности становится более высоким с увеличением вероятности опасного события P_r и с увеличением параметра воздействия F_r. Требования становятся менее жесткими с возрастанием значения вероятности предотвращения или ограничения вреда A_v и значения допустимого предела риска $L_{(S)}$. [$L_{(S)}$ является менее жестким с численно более высоким значением.] Это проще и точнее выразить простыми формулами (см. 6.2, 6.3 и раздел 7).

6.1.3 Логическая независимость параметров

Отдельный фактор или отдельное обстоятельство учитывают только один раз в общей оценке. Это также часто выражено как требование независимости уровней защиты.

В отдельных случаях не понятно, с помощью какого параметра описывается тот или иной элемент сценария аварии. Например, присутствие сотрудника может быть учтено в условии инициирующего события I_R или в параметре F_r (см. 5.7). Аналогичным образом действия операторов по снижению риска могут быть выражены в I_R (когда оператор не является лицом, подвергающимся риску) или в A_v (когда оператор является лицом, подвергающимся воздействию). Конкретные методологии и средства также могут различаться в этом отношении.

6.2 Режим работы с высокой частотой запросов или непрерывный режим работы

Для функции безопасности в режиме работы с высокой частотой запросов или в непрерывном режиме вышеизложенные принципы выражаются нижеприведенным образом.

Уровень опасности H_R можно представить следующей формулой:

$$H_R = \text{PFH} \cdot P_r \cdot F_r \cdot (1 - A_v). \quad (6)$$

В приведенной формуле (6) соотношение H_R = PFH может быть получено из уравнения Хенли—Кумамото $H_R = \text{PFH} \cdot (1 - e^{-D_R \cdot T_I/2})$. Это следует из предположения, что интенсивность запросов безопасности D_R × интервал контрольных проверок T_I значительно более 1.

Соответственно, функция безопасности с PFH должна удовлетворять следующему условию:

$$\text{PFH} \cdot P_r \cdot F_r \cdot (1 - A_v) \le L_{(S)}. \quad (7)$$

Интенсивность инициирующих событий I_R, рассмотренная в 5.9.3, не применена в формуле (6). Причина в том, что для опасного события непременно необходимы два условия:

- наличие инициирующей причины, которая не устраняется мерой защиты или слоем защиты, а только функцией безопасности. Интенсивность связанных событий — I_R;
- отказ функции безопасности. Интенсивность связанных событий — PFH.

В режиме работы с высокой частотой запросов или в непрерывном режиме в общей интенсивности событий, связанных с совпадением обеих вышеперечисленных причин, полностью преобладает вторая, отказ функции безопасности с интенсивностью PFH. Уровень опасности H_R ограничен интенсивностью опасных отказов функции безопасности.

Предположим, что функция безопасности отказала, и этот отказ не был обнаружен явным нарушением процесса (параметр P_r) или наблюдением внимательного оператора или стороннего наблюдателя — параметр $1 - A_v$. В этом случае отказ функции безопасности будет оставаться скрытым до тех пор, пока следующая инициирующая причина не приведет к опасному событию. В зависимости от приложения следующее опасное событие может произойти через несколько секунд или через несколько недель, что является внушительным разбросом в интенсивности инициирующих событий I_R. Однако типичное время между отказами функции безопасности не имеет отношения к типичному времени до следующего инициирующего события. В режиме работы с высокой частотой запросов интенсивность аварий можно определить по интенсивности отказов функций безопасности по формуле (6). Это также относится к режиму с непрерывными запросами.

6.3 Режим работы с низкой частотой запросов

Для функции безопасности в режиме работы с низкой частотой запросов вышеуказанные принципы могут быть выражены следующим образом:

$$H_R = \text{PFD}_{avg} \cdot D_R = \text{PFD}_{avg} \cdot I_R \cdot P_r \cdot F_r \cdot (1 - A_v) \quad (8)$$

и

$$\text{PFD}_{avg} = 1/2 \cdot \text{PFH} \cdot T_I = \text{PFH} / (2 \cdot T_R). \quad (9)$$

Формула (7) может быть приведена для функции единичного канала с одним интервалом контрольных проверок. Для общей функции эта и производные формулы могут быть соответственно обобщены. В данном контексте данный конкретный случай вполне подтверждает все выводы.

Соотношение $H_R = D_R \cdot 1/2 \cdot \text{PFH} \cdot T_I$ можно получить из уравнения Хенли—Кумамото $H_R = \text{PFH} \cdot (1 - e^{-D_R \cdot T_I/2})$. Это следует из предположения, что интенсивность запросов безопасности D_R × интервал контрольных проверок T_I значительно менее 1.

Функция безопасности с PFD_{avg} должна удовлетворять следующему условию:

$$\text{PFD}_{avg} \cdot I_R \cdot P_r \cdot F_r \cdot (1 - A_v) \le L_{(S)}. \quad (10)$$

7 Назначение режима запросов

7.1 Режим запросов. Общие положения

То, что функция управления безопасностью рассматривается как функция, работающая в режиме с низкой частотой запросов, по существу означает, что общая количественная оценка риска учитывает контрольные проверки. Если контрольные проверки проводят достаточно часто по сравнению с интенсивностью запросов, то это позволяет обнаруживать отказы функции безопасности до того, как возникнет запрос. Учет контрольных проверок по существу отличает режим работы с низкой частотой запросов, с одной стороны, от режима работы с высокой частотой запросов или непрерывного режима работы, с другой стороны. Согласно базовой логике обоснования функцию безопасности можно рассматривать как функцию:

- с низкой частотой запросов, если интервал периодических контрольных проверок достаточно мал по сравнению со средним периодом между запросами;
- высокой частотой запросов или с непрерывными запросами, если это не так.

Для единичного канала с одним интервалом контрольных проверок пороговое соотношение интенсивности событий может быть получено путем подстановки, определяющей значение PFD_{avg} по формуле (9), в формулу (8) расчета уровня опасности. В результате получают:

$$H_R = PFH \cdot [I_R/(2T_R)] \cdot P_r \cdot F_r \cdot (1 - A_v). \quad (11)$$

Формула (11) применима непосредственно к режиму работы с низкой частотой запросов. Она идентична аналогичной формуле (6) для режима работы с высокой частотой запросов или с непрерывными запросами, за исключением одного дополнительного параметра в правой части — $I_R/(2T_R)$.

Этот параметр можно назвать фактором контрольных проверок PTF:

$$PTF_{lin} = I_R/(2T_R). \quad (12)$$

Фактор контрольных проверок может быть использован для описания снижения риска за счет выполнения контрольных проверок. Контрольные проверки становятся эффективными, если частота контрольных проверок одного порядка с интенсивностью инициирующего события. Чем больше контрольные проверки снижают риск отказов функций безопасности, тем чаще она корректно реагирует на инициирующие события. Фактор контрольных проверок достигает значения 1 или более, если интенсивность инициирующих событий слишком высока по сравнению с частотой контрольных проверок или если контрольные проверки не проводят. Точка перехода между приведенными выше формулами (6) и (8) может быть определена следующим образом:

$$I_R/(2T_R) = 1 \text{ или } I_R = (2T_R). \quad (13)$$

Если интенсивность инициирующих событий превышает удвоенную частоту контрольных проверок, то фактор контрольных проверок больше не используют. Это эквивалентно его применению со значением 1.

Формулы, приведенные в разделе 6, являются приближенными, описывающими те случаи, когда частота запросов либо предельно высокая или запросы непрерывные, либо частота запросов низкая. Актуальные статистические данные не дают скачкообразного перехода от одного вида статистики к другому. Следовательно, существует другое обобщенное выражение для формул (6) и (9), описывающее плавный переход. Этот переход часто описывается в литературе уравнением Хенли—Кумамото. В соответствии с текущими обозначениями это определено следующим образом:

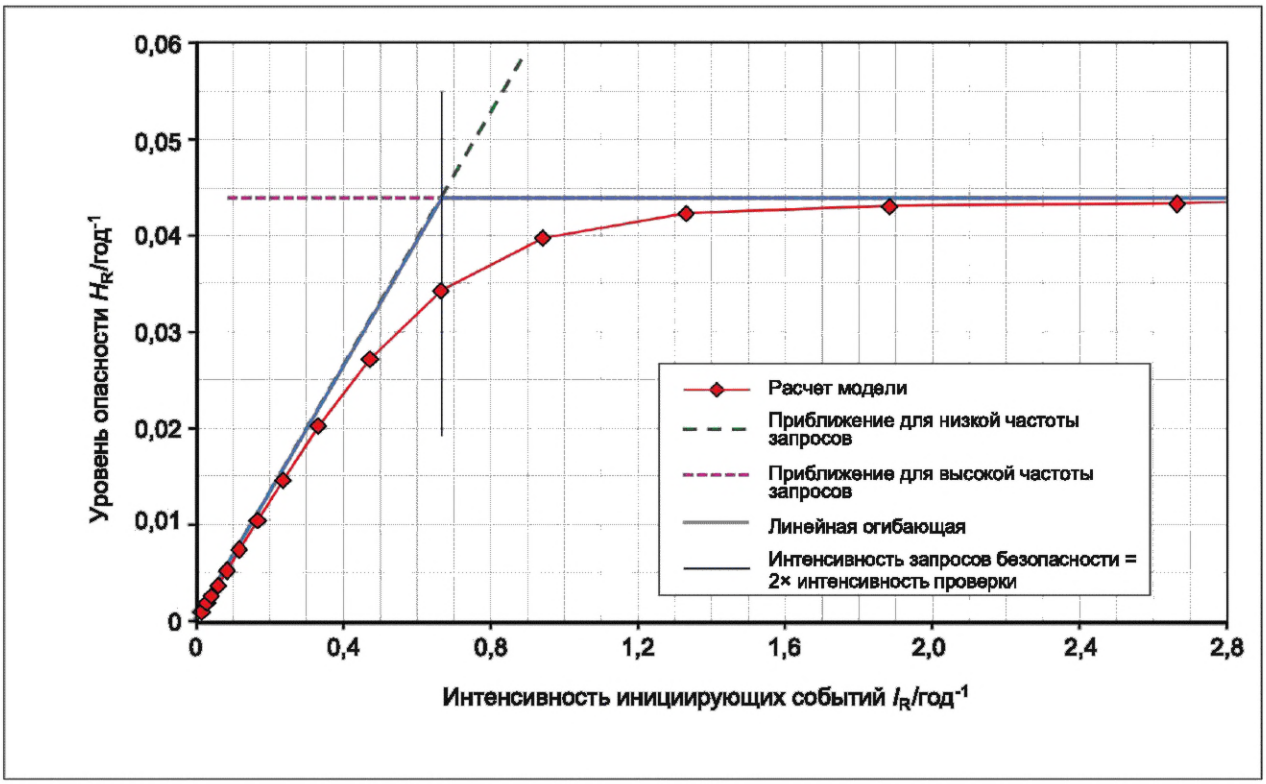
$$PTF_{H\&K} = 1 - e^{-D_R \cdot T_I/2}. \quad (14)$$

Используя уравнение Хенли—Кумамото для значения фактора контрольных проверок, получают для уровня опасности H_R:

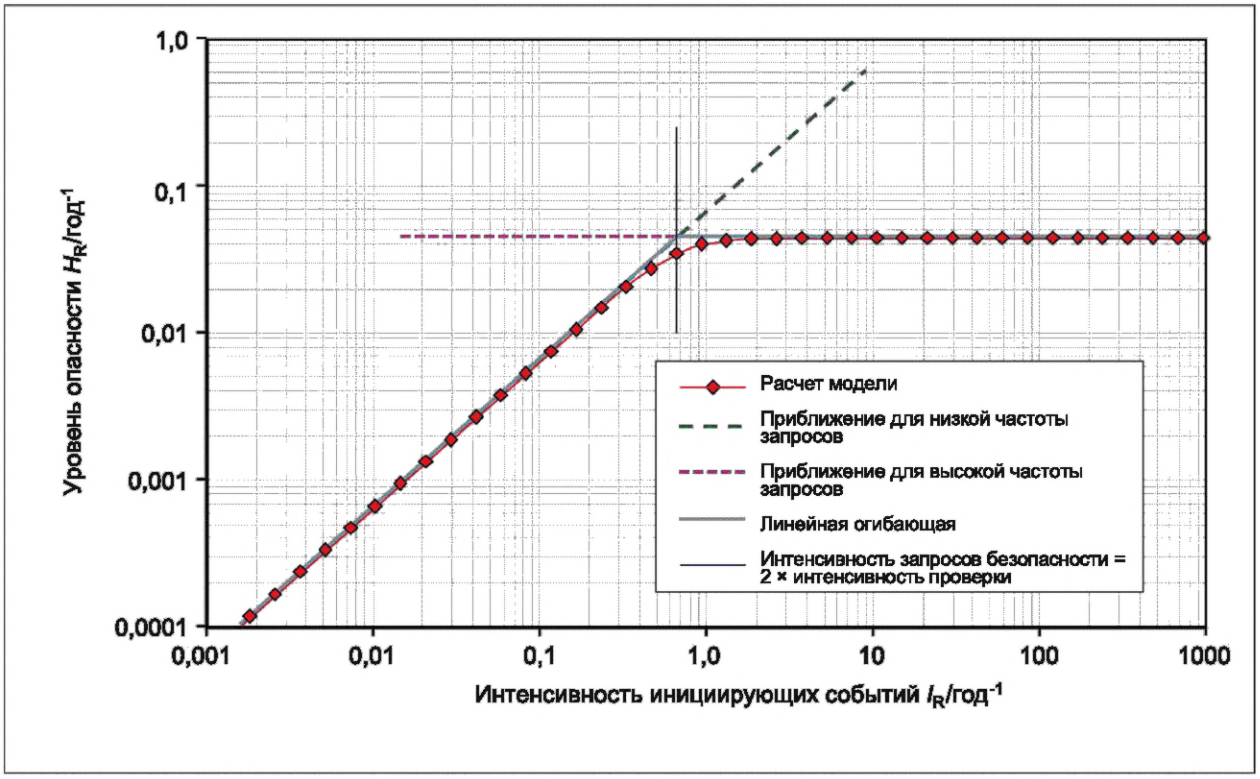
$$H_R = PFH \cdot (1 - e^{-D_R \cdot T_I/2}) \cdot P_r \cdot F_r \cdot (1 - A_v). \quad (15)$$

В формуле (15) аппроксимации для высокой частоты запросов или непрерывных запросов, а также для низкой частоты запросов обобщаются в одном выражении. Для практического применения достаточно использовать одно из двух приближений граничных случаев в соответствии с 6.3 (низкая частота запросов) или 6.2 (высокая частота запросов или непрерывные запросы), в зависимости от того, что больше подходит. Критерии приведены в 7.2.

На рисунке 3 показан пример расчета модели для одноканальной функции безопасности с интенсивностью опасных отказов PFH, равной $5 \cdot 10^{-6}$/ч (соответствует 0,044/год) и с интенсивностью контрольных проверок T_R, равной 1/3 года.



a) Линейные шкалы



b) Логарифмические шкалы

Рисунок 3 — Уровень опасности согласно уравнению Хенли—Кумамото

7.2 Критерии назначения

Функцию безопасности можно рассматривать как функцию, работающую в режиме с низкой частотой запросов, если выполняются оба следующих условия по перечислениям a) и b). Если одно из условий по перечислению a) или b) не применяют, то используют режим работы с высокой частотой запросов или с непрерывными запросами:

a) в условиях использования функции безопасности через регулярные промежутки времени предусмотрены и осуществимы контрольные проверки;

b) интервал контрольных проверок не превышает удвоенного среднего значения периода между инициирующими событиями: $D_R/2T_R < 1$, тогда $D_R < 2T_R$ или $T_I < 2\ D_I$.

МЭК 61508-4 и стандарты безопасности, основанные на этой базовой публикации по безопасности, определяют еще один критерий:

c) функцию безопасности можно рассматривать как функцию, работающую в режиме с низкой частотой запросов, если частота запросов менее одного раза в год (см., например, МЭК 61508-4:2010, 3.5.16).

Это не совсем понятно, так как если термин «частота запросов» не установлен в МЭК 61508-4, то может быть любое из трех определений, указанных в 5.10. Какое бы из этих определений ни использовалось в конечном итоге, предельное значение частоты запросов «один раз в год» для разделения режима с низкой частотой запросов и режима с высокой частотой запросов или с непрерывными запросами не может быть выведено из рассмотрения базового обоснования.

Существует разумный верхний предел интенсивности контрольных проверок, который может быть реализован в конкретном применении функции управления безопасностью. Предполагая, что частота запросов, предложенная в МЭК 61508-4, может быть в соответствии с 5.9.3 наиболее полно выражена интенсивностью инициирующих событий, тогда фактор контрольных проверок $I_R/(2T_R)$ будет связывать предельное значение 1 в год для частоты запросов с максимальной возможной интенсивностью контрольных проверок 1/2 в год, т. е. одна контрольная проверка каждые два года. Соответственно, контрольные проверки чаще, чем один раз в два года, не будут считаться эффективными для обнаружения отказов функций безопасности до того, как возникнет следующий запрос.

В современной технической литературе, как правило, не поддерживают требование о необходимости проведения контрольных проверок чаще, чем один раз в два года. Отсутствуют доказательства того, что консенсус по этому вопросу достигнут в стандартах безопасности. Ограничение в один запрос в год к функции безопасности может быть обосновано соображениями, выходящими за рамки настоящего стандарта. Это не поддерживается базовым обоснованием. Ограничение в один год можно использовать в качестве критерия для разделения режимов работы с высокой частотой запросов или с непрерывными запросами и низкой частотой запросов без логического противоречия с другим содержанием настоящего стандарта.

Еще один критерий может быть определен следующим образом. Применяют режим работы с высокой частотой запросов или с непрерывными запросами независимо от других критериев, если функция безопасности является единственным уровнем защиты, который предотвращает перерастание инициирующего события в аварию.

Этот критерий не основан на строго вероятностном обосновании и может отражать опасения против допустимости контрольных проверок как меры предотвращения несчастных случаев. Данный критерий также может отражать общественные или политические запросы. Применительно к катастрофическим авариям может оказаться недопустимым, чтобы рассматриваемая система безопасности находилась в нерабочем состоянии в течение любого промежутка времени. Однако это подразумевается уже тогда, когда вероятность отказа вообще определяется как свойство технической системы. Вопрос о том, действительно ли назначение режима работы с высокой частотой запросов или с непрерывными запросами приводит к более приемлемой ситуации, необходимо определять в каждом конкретном случае, так как это не является частью базового обоснования.

8 Взаимосвязь с ИСО 12100

Определения в настоящем стандарте могут быть связаны с определениями, приведенными в ИСО 12100 : 2010 (см. также рисунок 3 в ИСО 12100 : 2010). Риск и существенность вреда определены идентично в ИСО 12100 : 2010 и в настоящем стандарте.

Под вероятностью нанесения ущерба на рисунке 4 будет подразумеваться частота запросов, а не вероятность в терминологии настоящего стандарта.

Вероятность нанесения ущерба согласно ИСО 12100 : 2010 состоит из трех элементов.

1) Элемент риска «подверженность человека (лиц) опасности» в ИСО 12100:2010 выражен параметром воздействия согласно 5.7.

2) Элемент риска «возможность избежать или ограничить ущерб» выражен вероятностью предотвращения или ограничения ущерба согласно 5.8.

3) Элемент «возникновение опасного события», представленный на рисунке 3 ИСО 12100, можно определить с помощью:

- ($I_R \cdot P_r$), если функция безопасности отсутствует;
- (PFH $\cdot P_r$) — для функции безопасности в режиме высокой частоты запросов или постоянных запросов;
- ($PFD_{avg} \cdot I_R \cdot P_r$) — для функции безопасности в режиме работы с низкой частотой запросов.

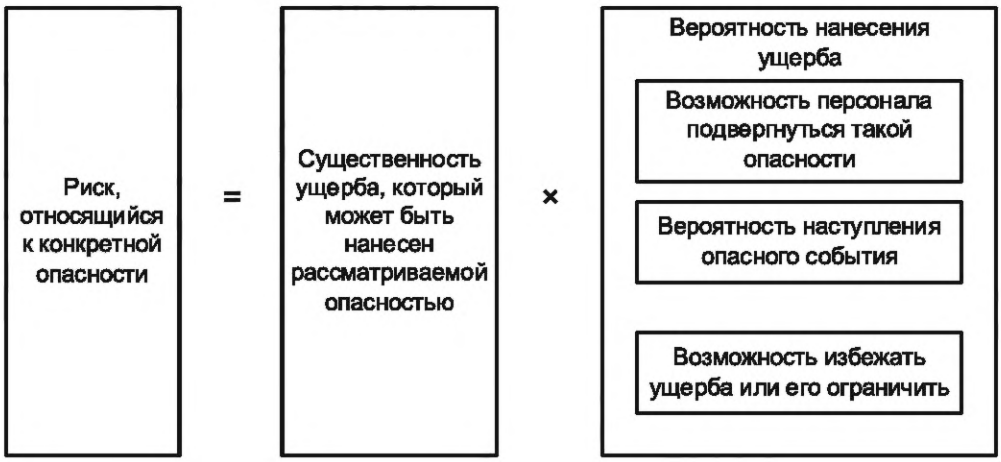


Рисунок основан на ИСО 12100 : 2010, рисунок 3 (изменен)

Рисунок 4 — Элементы риска согласно ИСО 12100

9 Методы и средства для обеспечения функциональной безопасности

9.1 Общие положения

Методы и средства для определения значений SIL или PL, графы рисков, матрицы рисков, методы подсчета баллов и т. п. по существу являются представлениями формул (7) или (10) с использованием графических средств или таблиц. Эти представления могут быть получены из данных формул согласно следующей последовательности:

- выбор используемых параметров;
- логарифмирование параметров;
- дискретизация логарифмических параметров;
- определение значений баллов настройкам отдельных дискретных параметров;
- кодирование взаимосвязей между баллами и требуемой полнотой безопасности в графическом дереве решений (графе рисков) или в таблице (таблица рисков, матрица рисков);
- настройка и адаптация, такие как ограничение предлагаемого пути (комбинации параметров) в концевых вершинах графа, настройка параметров и т. п.

Данный подход применим только к режиму с высокой частотой запросов, или постоянными запросами, или с низкой частотой запросов во всех типичных случаях. Выбор между этими режимами работы делают до того, как будут использованы методы, основанные на графах, таблицах или методах подсчета баллов для определения значения SIL.

В настоящем стандарте не отдается предпочтение ни одному из описанных методов для определения значения SIL, а также использованию таких методов или работе только с математическими формулами. Числовая точность не является главной задачей при определении значения SIL. Данное определение основано на небольшом количестве входных параметров, которые в большинстве случаев могут быть оценены количественно с ограниченной точностью. Таким образом, для метода определения можно допустить конкретную степень числовой неточности, если это облегчает задачу пользова-

телю или требуется компромисс для других граничных условий. Однако не следует нарушать основную логику, которая представлена выбором и внутренним содержанием параметров, их размерностями (т. е. в основном — время$^{-1}$ или безразмерными) и их отношениями.

Примеры применения методов для обеспечения функциональной безопасности приведены в приложении А.

9.2 Выбор независимых параметров

Метод назначения не обязательно использует каждый из параметров в формулах (7) или (10) как независимый. Логически это эквивалентно использованию определенных вероятностей только со значением, равным 1.

Например, если в конкретной области технических приложений все соответствующие отказы функций безопасности считаются скрытыми отказами, то отсутствует необходимость использовать параметры P_r, F_r и $(1 - A_v)$ в методе определения значения SIL для данного конкретного приложения. Подобные параметры неизменно будут принимать значение 1 в данном контексте.

В качестве более распространенного примера общепринятые графы риска для определения SIL функциям в режиме с низкой частотой запросов используют параметр W («W» — «Wahrscheinlichkeit», т. е. вероятность). Параметр W можно представить как произведение $I_R \cdot P_r$ в формуле (10). Эти графы рисков не учитывают частоту инициирующих событий I_R и P_r по отдельности (см. МЭК 61511-3, приложения D и E).

9.3 Логарифмирование параметров

Применение умножения в базовых формулах (7) и (10) для определения SIL может быть реализовано в графических средствах или методах путем логарифмирования параметров. Таким образом, умножения могут быть выполнены как сложения. Это позволяет, например, строить номограммы.

9.4 Дискретизация параметров

Более типичными, чем номограммы, являются методы с графом дерева решений или с табличной структурой, где пользователь может выбирать только дискретные значения для используемых параметров. В этих методах параметры дискретизированы, чаще всего с равноотстоящим шагом в логарифмическом масштабе.

Дискретизация означает, что непрерывный числовой диапазон представлен набором дискретных чисел. Это можно проиллюстрировать на шкале PFH, которая часто представляется только как набор дискретных уровней SIL, таких как SIL0, SIL1, SIL2 и т. д. В последовательности значений SIL каждый дискретный уровень заменяет и представляет целую декаду на непрерывной шкале PFH в единицах h^{-1} или PFD_{avg} (см. рисунок 5). Принцип дискретизации непрерывного числового параметра показан с помощью шкалы PFH в единицах [ч$^{-1}$], которая представлена дискретно набором значений SIL.

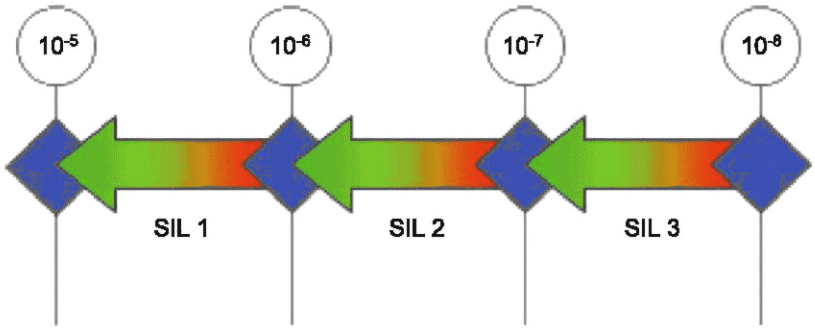


Рисунок 5 — Дискретизация параметров

9.5 Оценка параметров в баллах

Если входные параметры для определения SIL используют в логарифмически дискретизированном формате, то они могут быть представлены небольшими натуральными числами или баллами. Табличный метод определения или метод определения на основе графов дает требуемое значение SIL в результате общей суммы баллов. Добавление баллов может быть выполнено на графе дерева реше-

ний. Это принцип работы графа рисков. Таблицы рисков или матрицы рисков связывают сумму баллов по одной оси и параметр существенности по другой оси со значением требуемой полноты безопасности.

Система подсчета баллов во всех случаях будет соответствовать следующим принципам, которые проанализированы в приложении А:

- для параметров P_r, F_r, $1 - A_v$ и I_R значение баллов возрастает с увеличением значения параметра;
- для параметра S значение баллов возрастает с увеличением уровня существенности. Соответственно, значение баллов увеличивается с уменьшением допустимого предела риска $L_{(S)}$;
- аналогичным образом для показателя полноты безопасности значение баллов возрастает с увеличением требований к полноте, т. е. увеличивается с уменьшением значения подразумеваемой целевой меры отказа, т. е. PFH или PFD_{avg}.

При условии соблюдения изложенных выше принципов соотношения в формулах (7) и (10) можно преобразовать к следующему виду, пригодному для табличного представления или в виде графов:

- для режима работы с высокой частотой запросов или с непрерывными запросами по формуле (7):

$$SIL \geq A \cdot SC(S) + B \cdot [SC(P_r) + SC(F_r) + SC(1 - A_v)] + C; \quad (16)$$

- для режима работы с низкой частотой запросов по формуле (10):

$$SIL \geq A \cdot SC(S) + B \cdot [SC(P_r) + SC(F_r) + SC(1 - A_v) + SC(I_R)] + C, \quad (17)$$

где $SC(S)$ — значение в баллах для уровня существенности таких параметров, как S, P_r, A_v;

$SC(P_r)$ — значение в баллах параметра P_r;

$SC(F_r)$ — значение в баллах параметра F_r;

$SC(1 - A_v)$ — значение в баллах параметра $1 - A_v$;

$SC(I_R)$ — значение в баллах параметра I_R. Коэффициенты A и B в формулах (16) и (17) необходимы, если для дискретизации различных параметров использовались разные логарифмические шкалы;

параметр C — параметр, который требуется для корректировки произвольно выбранной нулевой точки оценочной шкалы в соответствии с предполагаемым допустимым риском.

В приложении А на примерах показано, как параметры в формулах (16) или (17) могут быть получены из конкретных графов рисков или матриц рисков. Насколько это возможно, указанные графы рисков или таблица рисков соответствуют формуле (7) для режима работы с высокой частотой запросов или с непрерывными запросами или соотношению по формуле (10) для режима работы с низкой частотой запросов.

9.6 Более жесткие методы подсчета баллов

Термин «метод подсчета баллов» иногда используют в более узком значении для тех методов, которые количественно определяют данный параметр как сумму баллов, связанных с качественными аспектами приложения. Эти аспекты фиксируют в вопросах с предопределенным набором возможных ответов, каждый из которых связан с оценкой. Общая оценка параметра может быть определена как результирующая сумма всех вопросов, связанных с параметром. Например, параметр $1 - A_v$ можно количественно определить с помощью следующих вопросов:

- как быстро развивается авария от первых признаков нарушения до полного воздействия опасности:
  - менее чем за 30 с — 10 баллов,
  - от 30 с до 2 мин — 7 баллов,
  - в период от 2 до 15 мин — 3 балла,
  - более 15 мин — 0 баллов;
- насколько потенциально подвергающийся воздействию персонал знаком с рассматриваемым оборудованием/процессом:
  - мало — 10 баллов,
  - удовлетворительно — 5 баллов,
  - очень хорошо — 0 баллов;

и так далее.

В задачи настоящего стандарта не входит обсуждение адекватности конкретных вопросов, возможных ответов и соответствующей оценки. Как правило, это предлагаемый способ получить количественные оценки из качественных описаний с четкой воспроизводимостью, если вопросы для оценки адекватны и ясны, а оценки установлены надлежащим образом.

В настоящем стандарте приведены примеры параметров и внутренне присущие им значения, которые могут быть целью вопросов для оценки. В 6.1 в качестве примеров рассмотрены основные принципы, которые также могут быть применены к целевым аспектам следующих оценивающих вопросов:

- каждый аспект, на который нацелен оценочный вопрос, должен быть эффективным средством снижения риска. Например, скорость развития опасного события является частичной мерой связанного с ним риска только в том случае, если потенциально подверженные риску лица имеют средства для предотвращения воздействия в течение заданного времени, как правило, с машинами или промышленными процессами;
- корреляция должна быть слабой между разными аспектами, т. е. между ответами на разные вопросы по одному параметру. Это означает, что ответ на один вопрос не должен отдавать явного предпочтения ответам, которые будут даны на другие вопросы.

В настоящем стандарте также описывается пример метода извлечения неявной количественной основы из заданной системы оценки. Все утверждения в 9.5 могут быть применены и к методам оценки в более узком значении.

Приложение А
(справочное)

Примеры методов анализа при назначении SIL

А.1 Общие положения

В настоящем приложении для нескольких типичных примеров описывается, как с помощью подхода, основанного на графе рисков или таблице, в соответствии с базовыми соотношениями по формуле (7) и формуле (10) может быть получена последовательность вычислений для определения SIL. Это подтверждает то, что широко распространенные методы действительно можно рассматривать как отдельные выражения базовых отношений.

Выбор входных параметров является первым критерием — критерием согласованности. Для функции безопасности приложения с высокой частотой запросов или с непрерывными запросами обычно используют следующие параметры:

- существенность события;
- вероятность возникновения опасного события P_r;
- воздействие F_r;
- вероятность предотвращения или ограничения вреда A_v.

Параметр «существенность события» требуется неизменно, так как он определяет значение допустимого предела риска. Другие параметры могут быть опущены, т. е. значение параметра равно 1, если он не имеет отношения к данной области применения. Единственный параметр, который можно разделить на конкретные аспекты в соответствии с тем примером, который приведен в 5.9, — это вероятность предотвращения или ограничения вреда путем разделения этого параметра на предотвратимость в более узком значении и уязвимость.

Если средство или метод предназначены для режима применения с низкой частотой запросов, то требуется дополнительный входной параметр, который включает частоту инициирующих событий l_R. Этот параметр будет иметь размерность время$^{-1}$, обычно в единицах «в год» или год$^{-1}$.

Соответственно:

- если не зависимый от времени, то метод позволяет определить значение полноты безопасности для режима работы с высокой частотой запросов или с непрерывными запросами, которое может быть связано с PFH в качестве целевой меры отказа;
- если с размерностью время$^{-1}$, то метод определяет значение полноты безопасности для режима работы с низкой частотой запросов, которое может быть связано с PFD_{avg} в качестве целевой меры отказа.

Все методы назначения, проанализированные в А.4, А.5 и А.6, должны пройти эту базовую проверку согласованности.

А.2 Назначение значений баллов вводимым параметрам

В табличных или основанных на графах методах установленное параметру числовое значение баллов часто рассматривают как элемент вводимых данных. Если, например, для параметра воздействия F_r можно выбрать F1 или F2, то SC(F_r) в формулах (А.1) и (А.2) естественно примет значения 1 или 2. Такой же принцип применяют, например, к параметрам существенности S1, S2 и т. д. Если числовое значение баллов параметра не очевидно непосредственно в качестве элемента возможных вводимых данных, то его можно вычислить, связав с последовательностью натуральных чисел или заменив числами символьную последовательность. Например, последовательность уровней эффективности защиты от PLa до PLe может быть связана с последовательностью чисел от 1 до 5 (см. таблицу А.1 в А.5).

А.3 Определение пределов допустимого риска

Предел допустимого риска можно получить с помощью методов назначения SIL, выбрав уровень существенности и далее для вводимых данных для P_r, F_r и $1 - A_v$, используя максимальные значения баллов. Это соответствует устанавливаемым значениям параметров, которые подразумевают, что другой способ снижения риска отсутствует, кроме применения функции безопасности.

Использование метода для режима с высокой частотой запросов или с непрерывными запросами приводит к значению полноты безопасности, которое в терминах PFH представляет максимальную интенсивность событий, допустимую для данного уровня существенности [см. рисунок А.1 a)].

При использовании метода для режима с низкой частотой запросов необходимо сделать дополнительный выбор в этом процессе. Это значение полноты безопасности, равное 1, которое представляет PFD_{avg}. В подходах на основе SIL такое значение («другие меры») определено как SIL0, или OM, или A, или подстрочное a для значения «надлежащая инженерная практика». Данные значения для PFD_{avg} соответствуют следующему числовому диапазону: $1 \le PFD_{avg} < 10$. Следовательно, SIL0 или эквивалентные обозначения включают значение 1 для PFD_{avg} как наиболее консервативное предположение. В результате это приводит к зависимому от времени входному параметру, который представляет в терминах l_R максимальную интенсивность событий, допустимую для данного уровня существенности [см. рисунок А.1 b)].

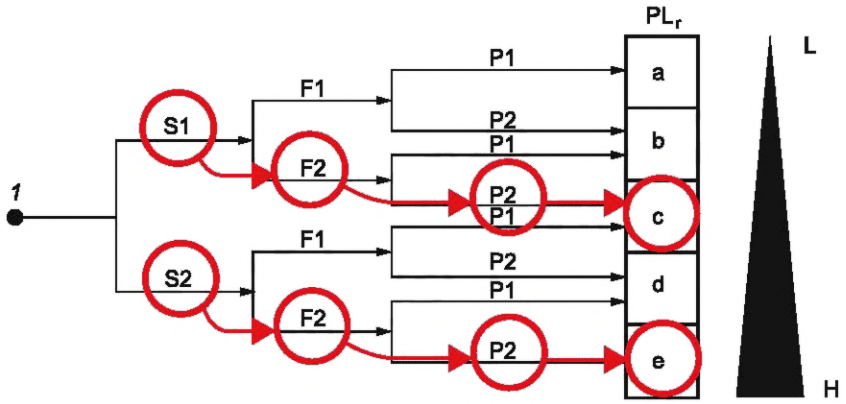
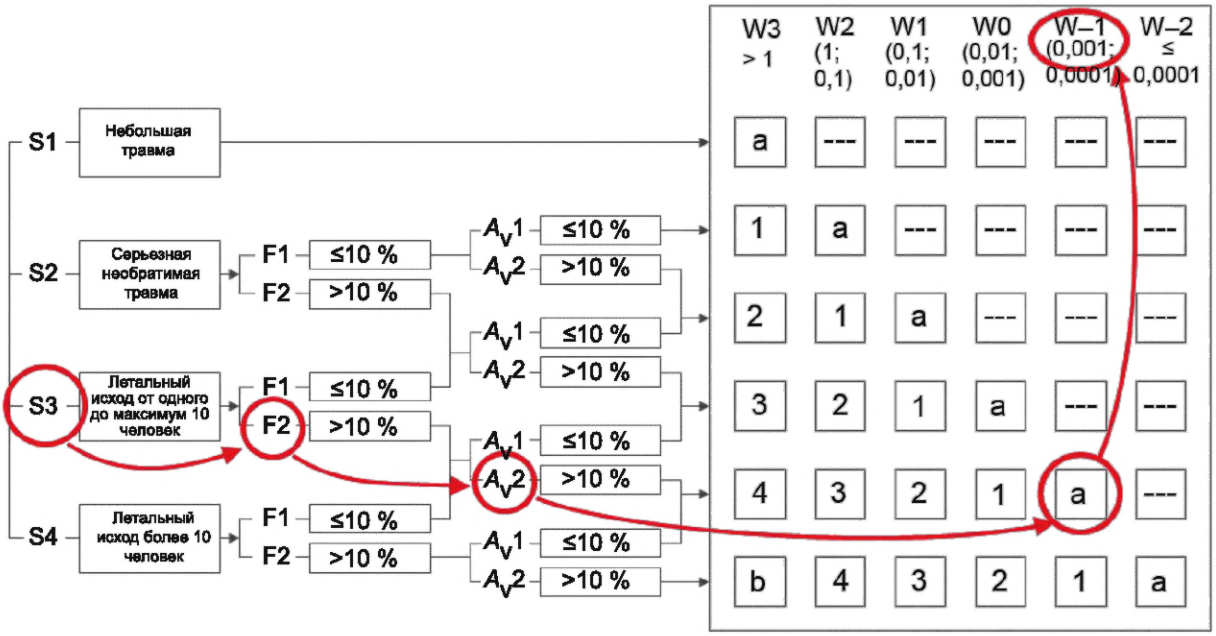


Рисунок основан на ИСО 13849-1:2015, рисунок А.1 (изменен)

a) Граф для определения требуемого параметра PL_r для функции безопасности



b) Рисунок 8 из VDMA 4315-1:2013-02. Турбомашины и генераторы[1)]

Рисунок А.1 — Определение пределов допустимого риска

В соответствии с описанным подходом графы рисков на рисунке А.1 представляют следующие допустимые пределы риска:

- приложение А ИСО 13849-1:2015, существенность S1 → PL c → PFH максимум $3 \cdot 10^{-6}$/ч → одно событие за 38 лет;
- приложение А ИСО 13849-1:2015, существенность S2 → PL e → PFH максимум $1 \cdot 10^{-7}$/ч → одно событие за 1142 года;
- VDMA 4315-1; существенность S3 → W^{-1} → максимум 0,001/год → одно событие на 1000 лет.

В первом перечислении результаты приблизительны и получены в описанном подходе. Не каждый граф рисков полностью соответствует числовой схеме без отклонений (см. пример в А.4). Если предел допустимого риска получен из одного графа рисков или матрицы рисков разными методами, то возможно, что результаты будут отличаться друг от друга на порядок величины, что зависит от соответствующего метода назначения.

[1)] Воспроизведено с разрешения VDMA.

А.4 Матрица рисков на основе МЭК 62061

На рисунке А.2 представлен пример матрицы рисков из ИСО 62061. Этот метод определения SIL предназначен для использования в машинах с функцией управления безопасностью в режиме работы с высокой частотой запросов или с непрерывными запросами. В качестве входных параметров использованы P_r, F_r и $1 - A_v$ в соответствии с формулой (7). Эти параметры представлены в виде суммы баллов, называемой в данном конкретном методе «класс» (заголовок столбца таблицы). Значения полноты безопасности приведены для обоих установленных понятий, как SIL, так и PL, в зависимости от уровней существенности.

Необходимо отметить, что A_v согласно матрице рисков, представленной на рисунке А.2 приложения А МЭК 62061:2021, соответствует $1 - A_v$ в настоящем стандарте, т. е. символ A_v используют в дополнительном значении. Кроме того, SIL 2 в классах 3 и 4 МЭК 62061:2021 снижен до SIL 1 из-за низкого балла для классов частоты, вероятности и предотвращения ущерба.

Следуя подходу, описанному в А.3, допустимые пределы риска могут быть получены как приблизительные значения из графы таблицы с максимальным значением баллов или графы «Класс». Максимальное количество баллов в этом методе — 15. Можно выделить следующие ограничения:

- существенность S1 → SIL1 → PFH максимум $1 \cdot 10^{-5}$/ч → один случай примерно за 10 лет
  или PL c → PFH максимум $3 \cdot 10^{-6}$/ч → одно событие примерно за 30 лет;
- существенность S2 → SIL2 → PFH максимум $1 \cdot 10^{-6}$/ч → одно событие примерно за 100 лет;
- существенность S3 → SIL3 → PFH максимум $1 \cdot 10^{-7}$/ч → одно событие примерно за 1000 лет;
- существенность S4 → SIL3 → PFH максимум $1 \cdot 10^{-7}$/ч → одно событие примерно за 1000 лет, т. е. такой же предел допустимого риска, как и для S3.

На рисунке А.3 приведена альтернатива представленному на рисунке А.2 с использованием только указанных значений SIL, отмеченных крестиком в каждых точках, которые отражают максимальное значение баллов, связанных с соответствующим значением SIL/PFH. Крестики для 16 баллов на правом краю графика установлены так, чтобы они наиболее соответствовали согласованной числовой схеме.

<table>
<tr><th rowspan="2">Последствия</th><th rowspan="2">Существенность Се</th><th colspan="15">Класс Cl = F_r + P_r + A_v</th></tr>
<tr><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th></tr>
<tr><td rowspan="2">Летальный исход, потеря глаза или руки</td><td rowspan="2">4</td><td colspan="2">SIL1</td><td colspan="3">SIL2</td><td colspan="3">SIL2</td><td colspan="3">SIL3</td><td colspan="2">SIL3</td></tr>
<tr><td>PL_r b</td><td>PL_r c</td><td colspan="3">PL_r d</td><td colspan="3">PL_r d</td><td colspan="3">PL_r e</td><td colspan="2">PL_r e</td></tr>
<tr><td rowspan="2">Постоянная травма, потеря пальцев</td><td rowspan="2">3</td><td colspan="2" rowspan="2">SIL (или PL) не требуется</td><td colspan="3">OM</td><td colspan="3">SIL1</td><td colspan="3">SIL2</td><td colspan="2">SIL3</td></tr>
<tr><td colspan="3">PL_r a</td><td>PL_r b</td><td colspan="2">PL_r c</td><td colspan="3">PL_r d</td><td colspan="2">PL_r e</td></tr>
<tr><td rowspan="2">Обратимая травма, медицинская помощь</td><td rowspan="2">2</td><td colspan="5" rowspan="2">SIL (или PL) не требуется</td><td colspan="3">OM</td><td colspan="3">SIL1</td><td colspan="2">SIL2</td></tr>
<tr><td colspan="3">PL_r a</td><td>PL_r b</td><td colspan="2">PL_r c</td><td colspan="2">PL_r d</td></tr>
<tr><td rowspan="2">Обратимая травма, первая помощь</td><td rowspan="2">1</td><td colspan="8" rowspan="2">SIL (или PL) не требуется</td><td colspan="3">OM</td><td colspan="2">SIL1</td></tr>
<tr><td colspan="3">PL_r a</td><td>PL_r b</td><td>PL_r c</td></tr>
</table>

OM — другие меры (например, основные принципы безопасности).

Примечание 1 – SIL2 для классов 3 и 4 в МЭК 62061:2021 снижен в данной таблице до SIL1 из-за низкого балла для классов частоты, вероятности и предотвращения ущерба.

Примечание 2 – SIL2 для классов 5, 6 и 7 не откалиброван в соответствии с остальной частью данной таблицы ввиду намерения учитывать средний балл для классов частоты, вероятности и предотвращения вреда в сочетании с возможностью смерти, как следствие.

Примечание 3 – Из-за характеристик рисков, присутствующих в оборудовании, SIL4 не рассмотрен. Для SIL4 см. МЭК 61508-1.

Примечание 4 – Соответствие между SIL и PL_r действительно только для требуемого уровня, а не для достигнутого уровня.

Рисунок А.2 — Матрица рисков на основе МЭК 62061

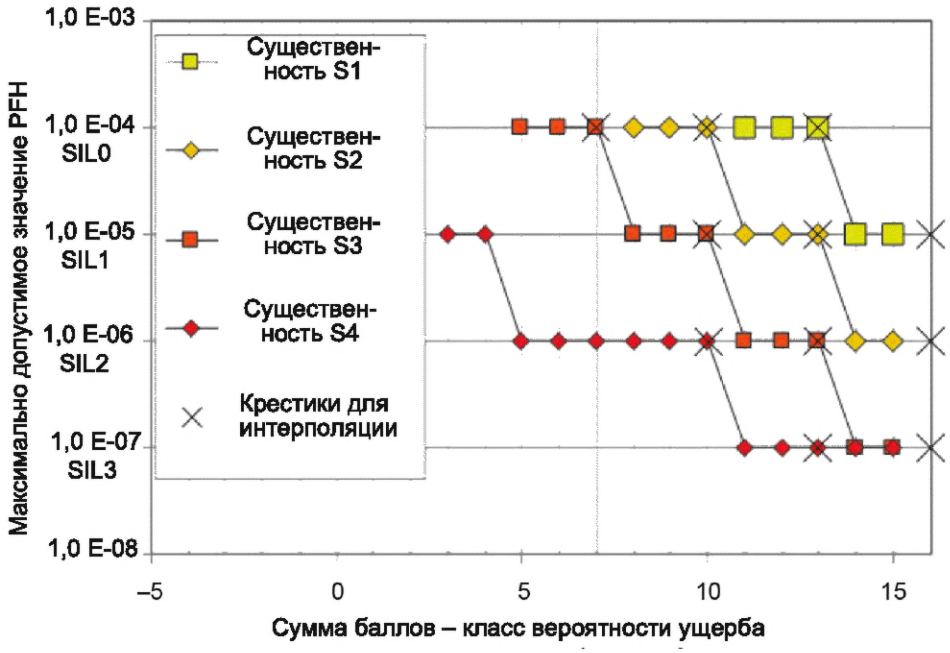


Рисунок А.3 — Максимально допустимое значение PFH как функция суммы баллов для различных уровней существенности

На рисунке А.3 для каждого уровня существенности представлены максимально допустимые значения PFH в зависимости от суммы баллов или класса. Графики выглядят как ступенчатые функции, а не как прямые линии, потому что вероятностные параметры P_r, F_r и $1 – A_v$ дискретизированы по шкале баллов в более мелких единицах, чем PFH по шкале SIL. Один шаг в SIL эквивалентен 3 баллам.

Для трех уровней существенности, от S1 до S3, матрица рисков для SIL может быть выражена в виде формулы (16). Для этого конкретного метода она принимает следующий вид:

$$SIL \geq SC(S) + 1/3 \cdot [SC(P_r) + SC(F_r) + SC(1 – A_v)] – 16/3. \quad (A.1)$$

Графическое представление формулы (А.1) показано на рисунке А.4. Для каждого уровня существенности формула (А.1) определяет верхнюю границу допустимого значения PFH. Точки графика для результатов вычислений такой матрицы не могут быть выше этой границы. Спускаясь от максимального значения по шкале баллов, результат вычислений может измениться на более высокий уровень по шкале PFH только тогда, когда граничная линия достигнет или пересечет этот уровень.

Формула (А.1) может быть преобразована в формат формулы (7), когда дискретизированные вводимые данные — SIL и количество баллов — заменяют их непрерывными числовыми значениями — PFH и $P_r \cdot F_r \cdot (1 – A_v)$. Анализ существенности S будет заменен пределами допустимого риска $L_{(S)}$:

- существенность S1 → $L_{(S)} = 2{,}15 \cdot 10^{-5}$/ч → одно событие примерно за 5,3 года;
- существенность S1 → $L_{(S)} = 2{,}15 \cdot 10^{-6}$/ч → одно событие примерно за 53 года;
- существенность S1 → $L_{(S)} = 2{,}15 \cdot 10^{-7}$ ч → одно событие примерно за 530 лет.

Приведенные выше пределы допустимого риска выше, чем в А.3 для такой же матрицы рисков, т. е. менее жесткие, в 101/3 = 2,15 раза. В данном конкретном случае разницу можно классифицировать как неточность дискретизации. Это объясняется тем, что матрица рисков использует только 2 балла для наивысшего значения SIL, в то время как в общем случае составляет 3 балла на шаг. При допущении, что матрица рисков в других случаях основана на последовательной схеме вычислений, пределы допустимого риска в А.3 представляют собой первое приближение, а указанные выше пределы являются точными в числовом отношении.

Для классов существенности 1—3, представленных на рисунке А.2, схема вычислений соответствует матрице риска, приведенной в МЭК 62061. Для класса существенности 4 допустимы отклонения. График на рисунках А.3 и А.4 соответствует схеме в диапазоне баллов от 8 до 13. Для баллов 14 и 15 матрица риска дает более низкое значение SIL, чем предлагается схемой вычисления, — SIL3 вместо SIL4. Для баллов 7 или ниже значение SIL, возвращаемое матрицей, на один уровень выше, чем предложено схемой. Отклонение рассмотрено в примечаниях 2 и 3 к рисунку А.2:

- SIL4 не применяют для машин. Поэтому вводимые данные в матрице рисков ограничены SIL3;
- нецелесообразно придерживаться риск-ориентированного подхода для высшего уровня существенности S4 в связи с возможным летальным исходом сотрудника.

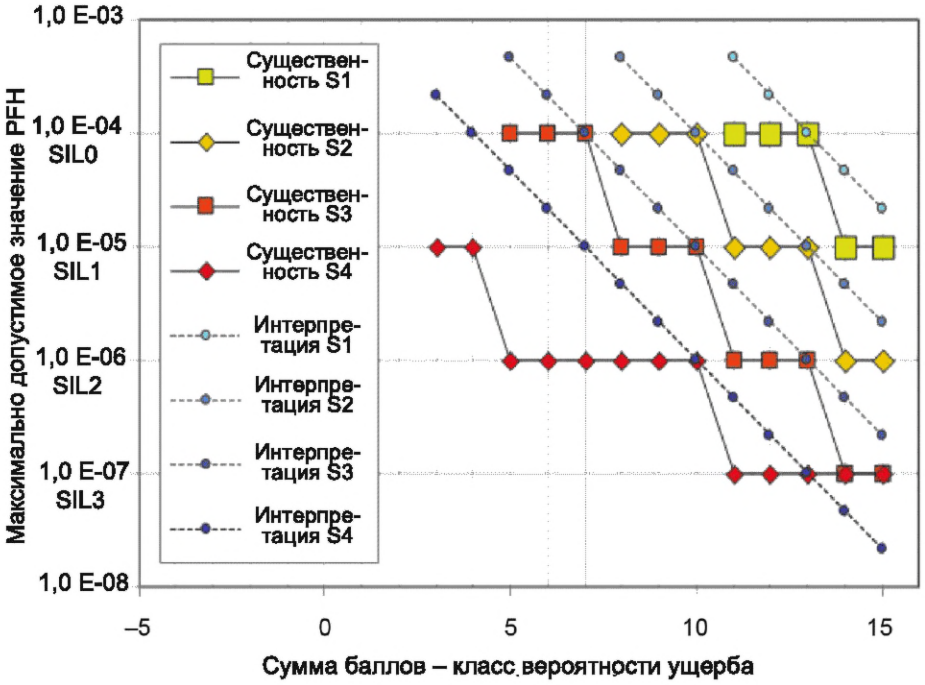


Рисунок А.4 — Представление непрерывной числовой интерполяцией

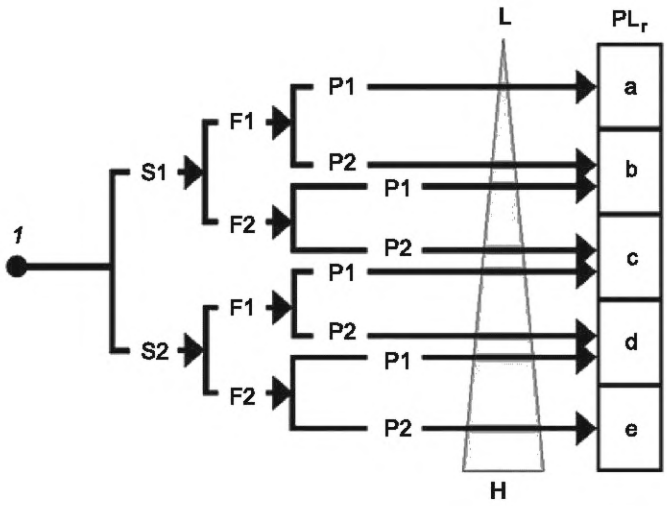
Оба утверждения не используются в контексте подхода, строго основанного на оценке риска, и это не делает их неверными. Однако проведение только количественной оценки риска не дает в этих случаях подтверждающего обоснования.

А.5 Граф риска по ИСО 13849

На рисунке А.5 представлен граф рисков, рассмотренный на рисунке А.1 в ИСО 13849-1:2015. Как и матрица рисков в приложении А МЭК 62061:2021, этот граф рисков предназначен для использования машин в рабочем режиме с функцией управления безопасностью в режиме работы с высокой частотой запросов или с непрерывными запросами.

В графе рисков на рисунке А.1 из ИСО 13849-1:2015 использованы параметры F_r, обозначенные как F на рисунке А.5, и $1 – A_v$, обозначенные как P на рисунке А.5. Параметр P_r для вероятности опасного события не включен в граф, однако он рассмотрен в соответствующем тексте: «Если вероятность возникновения опасного события может быть обоснована как низкая, то PL_r может быть уменьшен на один уровень» (см. ИСО 13849-1:2015, А.2.3). Таким образом, P_r можно определить как параметр с двумя уровнями подобно F и P. Входной параметр, зависящий от времени, отсутствует, и выходные данные заданы в терминах PFH в соответствии с А.1.

Выходные данные графа рисков на рисунке А.1 ИСО 13849-1:2015 приведены в уровнях эффективности защиты (PL). Дискретизация PFH $3 \cdot 10^{-6}$ в PL основана на десятичном логарифме, как и для SIL. Однако последовательность значений PL включает один промежуточный уровень — это PL_c с максимально допустимым значением PFH, равным $3 \cdot 10^{-6}$/ч, между уровнями SIL1 и SIL2 (см. таблицу А.1).



Данный рисунок основан на рисунке А.1 ИСО 13849-1:2015 (изменен)

1 — начальная точка для оценки вклада функции безопасности в снижение риска; L — низкий вклад в снижение риска; H — высокий вклад в снижение риска; PL_r — требуемый уровень эффективности защиты.

Параметры риска: *S* — существенность травмы; S1 — легкая (обычно обратимая травма); S2 — серьезные (обычно необратимое повреждение или летальный исход); *F* — частота и/или воздействие опасности; F1 — от редкого до менее частого воздействия и/или короткое время воздействия; F2 — от частого к постоянному воздействию и/или длительное время воздействия; *P* — возможность ограничить ущерб; P1 — избежать опасности возможно при определенных условиях; P2 — избежать опасности вряд ли возможно

Рисунок А.5 — Граф рисков по ИСО 13849-1

Таблица А.1 — Соотношение между PL и диапазонами в PFH

PL	Верхний предел PFH/ч$^{-1}$	Нижний предел PFH	Оценка PL в баллах
a	$1 \cdot 10^{-4}$	$1 \cdot 10^{-5}$	1
b	$1 \cdot 10^{-5}$	$3 \cdot 10^{-6}$	2
c	$3 \cdot 10^{-6}$	$1 \cdot 10^{-6}$	3
d	$1 \cdot 10^{-6}$	$1 \cdot 10^{-7}$	4
e	$1 \cdot 10^{-7}$	$1 \cdot 10^{-8}$	5

Таким образом, последовательность PL не является строго логарифмической в PFH, как ряд SIL. Это обстоятельство незначительно влияет на соответствие графа рисков схеме вычисления непрерывных значений по формуле (7).

На рисунке А.6 максимально допустимое значение PFH представлено для каждого уровня существенности в зависимости от суммы баллов входных параметров способом, аналогичным приведенному на рисунке А.4. Эти графики выглядят в основном как прямые линии. Различие по шкале PL дает лишь незначительное нарушение линейности логарифмического представления. На рисунке А.6 шаг между уровнями существенности S1 и S2 взвешенно эквивалентен 2 баллам для входных параметров F_r/F и $(1 - A_v)/P$. Соответственно, формула (16) принимает следующий вид для графа рисков на рисунке А.1 ИСО 13849-1:2015:

$$SC(PL) \approx 2 \cdot SC(S) + SC(F) + SC(P) - 3. \quad (A.2)$$

Взаимосвязь значений PL с их оценкой в баллах приведена в таблице А.1. График зависимости в формуле (А.2) также показан на рисунке А.6 и получен путем линейной аппроксимации логарифмических значений. В терминах вероятности или PFH 1 балл соответствует коэффициенту $10^{3/4}$, приблизительно равному 5,6. Распределение пяти PL по трем декадам аппроксимируется расстоянием в 0,75 декады от одного PL до другого. Пределы допустимого риска, которые можно получить по формуле (А.2) с шагом $10^{3/4}$, существенно не отличаются от пределов, определенных в соответствии с А.3:

- существенность S1 → предел риска: $3{,}16 \cdot 10^{-6}$/ч → одно событие за 36 лет;
- существенность S2 → предел риска: $1 \cdot 10^{-7}$/ч → одно событие за 1142 года.

Граф рисков на рисунке А.1 ИСО 13849-1:2015 можно понимать как представление формулы (7) без существенных отклонений.

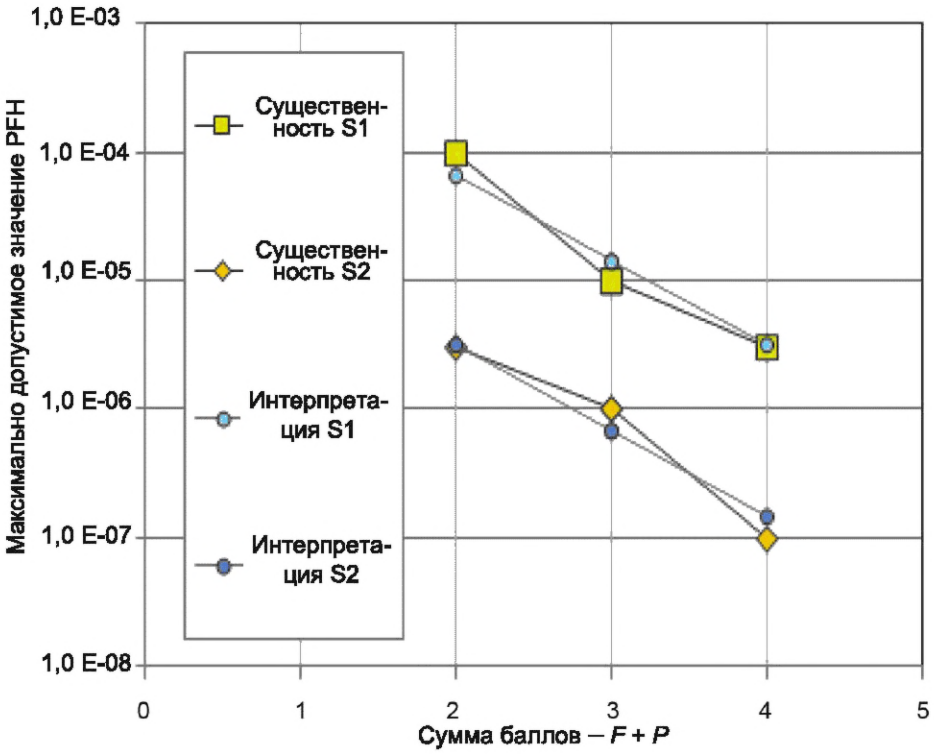


Рисунок А.6 — Интерполяция по уровням существенности

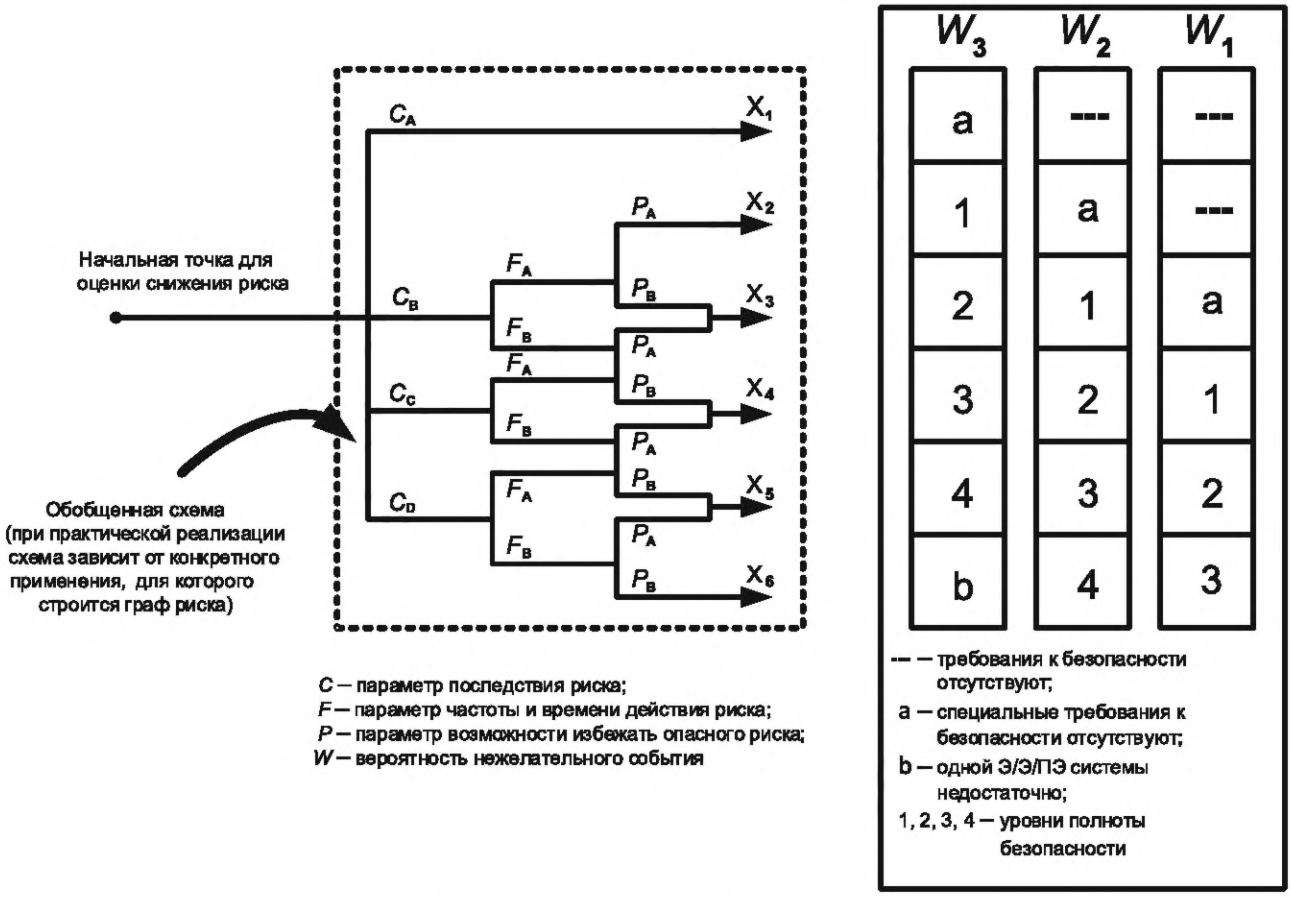
А.6 Графы рисков для режима работы с низкой частотой запросов

Графы рисков для функций безопасности в режиме работы с низкой частотой запросов в основном получены исходя из примера в МЭК 61058-5 (см. рисунок А.7).

Одна конкретная адаптация этого графа рисков осуществлена в VDMA 4315-1:2013 для применения с турбомашинами и генераторами (см. рисунок А.8).

Оба графа используют параметры F_r, обозначенные F на рисунках А.7 и А.8, и $1 – A_v$, обозначенные как A_v. Параметр P_r для вероятности опасного события не использован или применен неявно как элемент параметра W в верхней части табличной части графа, который выражает интенсивность возникновения опасных событий, связанных с опасностью и исследуемым оборудованием. Параметр W связан со временем, а выходные данные графа рисков представлены в терминах PFD_{avg} в соответствии с А.1.

В целом в версии VDMA калибровка параметра W становится обязательной при его включении в граф риска, в то время как в МЭК 61508-5 это предлагается только в отдельной таблице (МЭК 61508-5:2010, таблица Е.2). Кроме того, в версии VDMA диапазон параметра W расширен до предельно малых значений, так что этот метод можно использовать для сценариев аварий с предельно низкой интенсивностью событий. В остальном графы рисков на рисунках А.7 и А.8 структурно идентичны.



Источник: МЭК 61508-5:2010, рисунок Е.1

Рисунок А.7 — Граф риска для режима работы с низкой частотой запросов

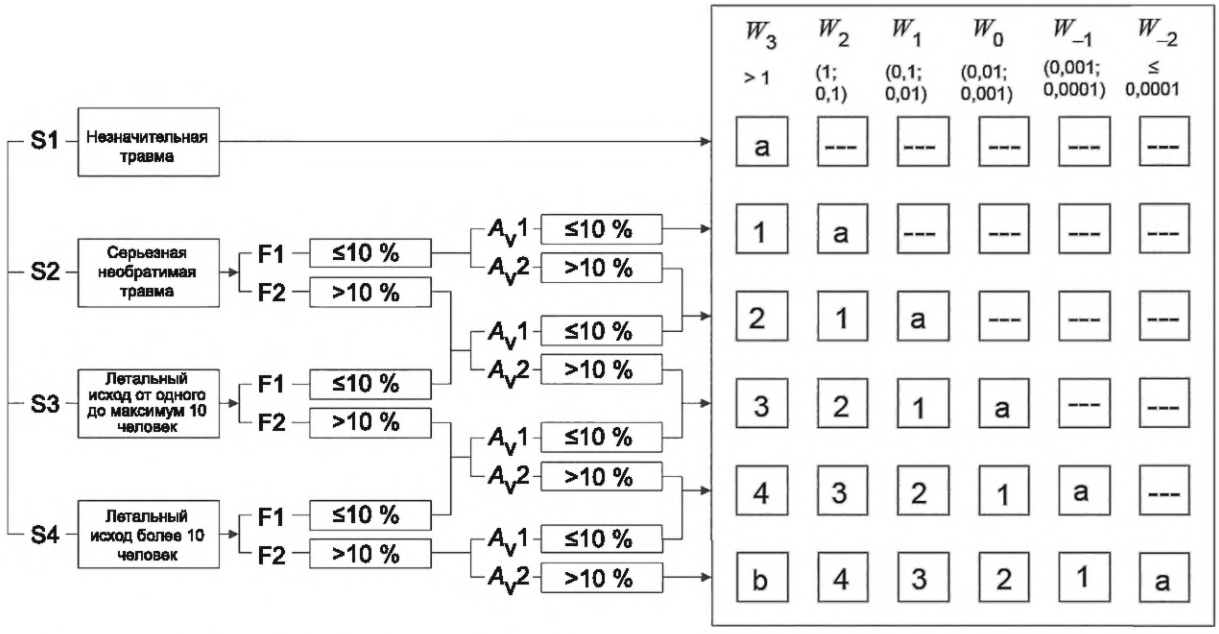


Рисунок А.8 — Граф рисков для режима работы с низкой частотой запросов (VDMA 4315-1, рисунок 7[1)])

[1)] Воспроизведено с разрешения VDMA.

На рисунке А.8 определен числовой подсчет баллов отдельных параметров. При таком подсчете баллов формула (17) в 9.5 принимает следующий вид:

$$SIL = SC(S) + SC(F) + SC(A_v) + SC(W) - 6. \quad (A.3)$$

Символ a в поле результата графа идентифицирован как отсутствие необходимости SIL, а символ b — как одной системы безопасности недостаточно. Числовое несоответствие с формулой (А.3) отсутствует, символ a соответствует оценке 0, а символ b — оценке 5. Таким образом, граф рисков можно рассматривать как дискретизированное представление формулы (10). Пределы допустимого риска в соответствии с описанным в А.3 методом получения четко обоснованы: $1 \cdot 10^{-3}$/год для существенности S3 с десятикратным повышением или понижением для других уровней существенности.

Следовательно, графы рисков для функций безопасности в режиме работы с низкой частотой запросов согласно примерам на рисунках А.7 и А.8 можно понимать как представление формулы (10). Для того чтобы установить взаимосвязь в числовом виде, в основном требуется, чтобы для графа вводимые данные для параметра *W* были количественно определены как интенсивности событий.

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 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 стандарта:

- IDT — идентичный стандарт.

Библиография

IEC 60050-103:2009, International Electrotechnical Vocabulary — Part 103: Mathematics — Functions

IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 4: Definitions and abbreviations

IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 5: Examples of methods for the determination of safety integrity levels

IEC 61511-1:2016, Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements

IEC 62061:2021, Safety of machinery — Functional safety of safety-related control systems

IEC TR 63039:2016, Probabilistic risk analysis of technological systems — Estimation of final event rate at a given initial state

ISO/IEC Guide 51:2014, Safety aspects — Guidelines for their inclusion in standards

ISO 13849 (all parts), Safety of machinery — Safety-related parts of control systems

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

ISO 31000:2018, Risk management — Guidelines

ISO 31010:2019, Risk management — Risk assessment techniques

E.J. Henley, H. Kumamoto, Reliability Engineering and Risk Assessment, New York, IEEE Press, 1992

VDMA 4315-1:2013, Turbomachinery and generators — Application of the principles of functional safety — Part 1: Methods for determination of the necessary risk reduction

УДК 62-783:614.8:331.454.004.056.5:006.354 ОКС 13.110, 29.020

Ключевые слова: функциональная безопасность, безопасность машин и механизмов, уровень полноты безопасности, уровень эффективности защиты, оценка рисков, требования безопасности, параметры безопасности

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 17.06.2024. Подписано в печать 25.06.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 3,72.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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