ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59504— 2021/ IEC TR 61511-4:2020

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 4

Пояснение и обоснование изменений, внесенных в МЭК 61511-1 из издания 1 в издание 2

(IEC TR 61511-4:2020, IDT)

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» совместно с Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 395-ст

4 Настоящий стандарт идентичен международному документу IEC TR 61511-4:2020 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 4. Пояснение и обоснование изменений, внесенных в МЭК 61511-1 из издания 1 в издание 2» (IEC TR 61511-4:2020 «Functional safety — Safety instrumented systems for the process industry sector — Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные 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 (*gost.e-ecolog.ru

© IEC, 2020 — Все права сохраняются
© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
3.1 Термины и определения 2
3.2 Сокращения 2
4 Предварительная информация 3
5 Управление функциональной безопасностью (изд. 2, раздел 5) 3
5.1 Почему этот раздел важен? 3
5.2 Распространенные ошибки 4
5.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 4
5.4 Кратко о том, что изменилось 5
6 Жизненный цикл системы безопасности (изд. 2, раздел 6) 6
6.1 Почему этот раздел важен? 6
6.2 Распространенные ошибки 6
6.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 6
6.4 Кратко о том, что изменилось 6
7 Верификация (изд. 2, раздел 7) 6
7.1 Почему этот раздел важен? 6
7.2 Распространенные ошибки 6
7.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 7
7.4 Кратко о том, что изменилось 7
8 Анализ опасностей и рисков (изд. 2, раздел 8) 7
8.1 Почему этот раздел важен? 7
8.2 Распространенные ошибки 7
8.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 8
8.4 Кратко о том, что изменилось 8
9 Распределение функций безопасности по слоям защиты (изд. 2, раздел 9) 8
9.1 Почему этот раздел важен? 8
9.2 Распространенные ошибки 9
9.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 9
9.4 Кратко о том, что изменилось 10
10 Спецификация требований безопасности SIS (изд. 1, раздел 10) 10
10.1 Почему этот раздел важен? 10
10.2 Распространенные ошибки 11
10.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 11
10.4 Кратко о том, что изменилось 11
11 Проектирование и разработка (изд. 2, раздел 11) 12
11.1 Почему этот раздел важен? 12
11.2 Распространенные ошибки 12
11.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 13
11.4 Кратко о том, что изменилось 14
12 Разработка прикладной программы (изд. 2, раздел 12) 15
12.1 Почему этот раздел важен? 15
12.2 Распространенные ошибки 15
12.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 15
12.4 Кратко о том, что изменилось 16
13 Заводские приемочные испытания (изд. 2, раздел 13) 16
13.1 Почему этот раздел важен? 16
13.2 Распространенные ошибки 16
13.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 16
13.4 Кратко о том, что изменилось 17
14 Установка (изд. 2, раздел 14) 17
14.1 Почему этот раздел важен? 17
14.2 Распространенные ошибки 17

14.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 17
14.4 Кратко о том, что изменилось 17
15 Валидация (изд. 2, раздел 15) 18
15.1 Почему этот раздел важен? 18
15.2 Распространенные ошибки 18
15.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 18
15.4 Кратко о том, что изменилось 18
16 Эксплуатация и техническое обслуживание (изд. 2, раздел 16) 19
16.1 Почему этот раздел важен? 19
16.2 Распространенные ошибки 19
16.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 19
16.4 Кратко о том, что изменилось 20
17 Модификация (изд. 2, раздел 17) 20
17.1 Почему этот раздел важен? 20
17.2 Распространенные ошибки 20
17.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 21
17.4 Кратко о том, что изменилось 21
18 Снятие с эксплуатации (изд. 2, раздел 18) 21
18.1 Почему этот раздел важен? 21
18.2 Распространенные ошибки 21
18.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 22
18.4 Кратко о том, что изменилось 22
19 Документация (изд. 2, раздел 19) 22
19.1 Почему этот раздел важен? 22
19.2 Распространенные ошибки 22
19.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 22
19.4 Кратко о том, что изменилось 22
20 Определения (изд. 2, раздел 3) 23
20.1 Почему этот раздел важен? 23
20.2 Распространенные ошибки 23
20.3 Что изменилось во 2-м издании по сравнению с 1-м и почему? 23
20.4 Кратко о том, что изменилось 32
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 33
Библиография 34

Введение

В МЭК 61511 (все части) рассматриваются приборные системы безопасности (SIS) для сектора промышленных процессов. В настоящем стандарте предлагается использовать известную в данном секторе терминологию и определять практические требования к реализации на основе независимых от сектора положений, представленных в базовом стандарте по безопасности МЭК 61508. МЭК 61511-1 во многих странах признается эффективной инженерной практикой и во все большем числе стран является обязательным требованием.

Тем не менее стандарты развиваются с учетом опыта их применения в рассматриваемом секторе. Второе издание МЭК 61511-1 отредактировано на основе десятилетнего международного опыта применения в секторе промышленных процессов требований, представленных в первом издании МЭК 61511-1:2003. Изменения издания 1, внесенные в издание 2, инициированы замечаниями специалистов национальных комитетов, представляющих широкий спектр пользователей стандарта во всем мире.

Требования первого издания 2003 г. (изд. 1)[1)], относящиеся к предотвращению и управлению систематическими ошибками, которые возникают при проектировании, разработке, эксплуатации, обслуживании и модификации, были предназначены прежде всего для независимых функций безопасности, имеющих целевой уровень полноты безопасности вплоть до значения SIL 3. В отличие от этого, во втором издании 2016 г. (изд. 2) необходимо было учитывать устоявшуюся тенденцию разделяемого использования систем автоматики сразу несколькими функциями безопасности.

В изд. 2 также потребовалось устранить основные некорректные интерпретации требований изд. 1, которые за прошедшие годы стали очевидными для разработчиков МЭК 61511 (МТ 61511). Например, в изд. 2 вместо узкой концентрации на расчетах основное внимание уделено менеджменту функциональной безопасности при проектировании и обеспечению фактических характеристик SIS в течение ее жизненного цикла.

Настоящий стандарт был создан для краткого ознакомления широкой аудитории с вышеупомянутыми вопросами, при этом более подробное содержание осталось в основных частях комплекса стандартов МЭК 61511. Настоящий стандарт описывает обоснование основных разделов МЭК 61511-1, уточняет некоторые распространенные ошибочные представления об их применении, приводит перечень основных различий между первым и вторым изданиями МЭК 61511-1 и дает краткое объяснение типовых подходов для применения каждого основного раздела в секторе промышленных процессов.

[1)] Для удобства чтения в настоящем стандарте будут использоваться «изд. 1» и «изд. 2» вместо МЭК 61511-1:2003 и МЭК 61511-1:2016, соответственно.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 4

Пояснение и обоснование изменений, внесенных в МЭК 61511-1 из издания 1 в издание 2

Functional safety. Safety instrumented systems for the process industry sector.
Part 4. Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт:

- предоставляет обоснование всех разделов МЭК 61511 и взаимосвязь между ними;
- информирует о наиболее распространенных ошибках и неправильном толковании конкретных разделов стандарта и об изменениях в них;
- объясняет различия между изд. 1 и изд. 2 МЭК 61511-1 и причины этих изменений;
- профессионально и кратко представляет, как выполнить требования его разделов;
- объясняет различия в терминологии между МЭК 61508 и изд. 2 МЭК 61511.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения к нему).

IEC 60050-192, International Electrotechnical Vocabulary (IEV) — Part 192: Dependability (доступно по адресу gost.e-ecolog.ru) (Международный электротехнический словарь. Часть 192. Надежность)

IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 4. Термины и определения)

IEC 61511-1:2016, Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements (Безопасность функциональная. Приборные системы безопасности, для промышленных процессов. Часть 1. Термины, определения и технические требования)

IEC 61511-1:2016/AMD 1:2017

ISO/IEC Guide 51:2014, Safety aspects — Guidelines for their inclusion in standards (Аспекты безопасности. Руководящие указания по включению их в стандарты)

Издание официальное

3 Термины, определения и сокращения

3.1 Термины и определения

Для целей настоящего стандарта применяются термины и определения, приведенные в Руководстве ИСО/МЭК 51, МЭК 60050-192, МЭК 61508-4 и МЭК 61511-1.

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

- IEC Electropedia: доступна по адресу http://www.electropedia.org/
- ИСО онлайн платформа: доступна по адресу gost.e-ecolog.ru

3.2 Сокращения

В таблице 1 приведены сокращенные термины, используемые в настоящем стандарте. Также включены некоторые общие сокращенные термины, относящиеся к функциональной безопасности сектора промышленных процессов.

Таблица 1 — Сокращения терминов, используемых в настоящем стандарте

Сокращение	Полное название
AIChE	Американский институт инженеров-химиков (American Institute of Chemical Engineers)
ANSI	Американский национальный институт стандартов (American National Standards Institute)
BPCS	Базовая система управления процессом (Basic process control system)
CCPS	Центр безопасности химических процессов [Centre for Chemical Process Safety (AIChE)]
Ed.	Издание (edition)
FAT	Заводские приемочные испытания (Factory acceptance test)
FMEA	Анализ видов и последствий отказов (Failure mode and effects analysis)
FMEDA	Анализ видов, последствий и диагностики отказов (Failure modes, effects, and diagnostic analysis)
FPL	Фиксированный язык программирования (Fixed program language)
FSA	Оценка функциональной безопасности (Functional safety assessment)
FVL	Язык программирования с полной изменчивостью (Full variability language)
HFT	Отказоустойчивость аппаратных средств (Hardware fault tolerance)
H&RA	Оценка опасностей и рисков (Hazard and Risk Assessment)
HAZOP	Исследование опасности и работоспособности (Hazard and Operability Study)
HMI	Человеко-машинный интерфес (Human machine interface)
IEC	Международная электротехническая комиссия (International Electrotechnical Commission)
IPL	Независимый защитный слой (Independent protection layer)
ISA	Международная ассоциация автоматизации (International Society of Automation)
ISO	Международная организация по стандартизации (International Organization for Standardization)
LOPA	Анализ уровней надежности средств защиты (Layers of protection analysis)
LVL	Язык программирования с ограниченной изменчивостью (Limited variability language)
MOC	Управление изменениями (Management of change)
MooN*	Канальная архитектура M из N ("M" out of "N" channel architecture)
MPRT	Максимально допустимая продолжительность ремонта (Maximum permitted repair time)
MRT	Средняя продолжительность ремонта (Mean repair time)

Окончание таблицы 1

Сокращение	Полное название
MTTR	Среднее время восстановления (Mean time to restoration)
NP	Непрограммируемый (Non-programmable)
PE	Программируемая электроника (Programmable electronics)
PES	Программируемая электронная система (Programmable electronic system)
PFDavg	Средняя вероятность опасного отказа по запросу (Average probability of dangerous failure on demand)
RRF	Коэффициент снижения риска (Risk reduction factor)
SAT	Приемочные испытания на месте (Site acceptance test)
SIF	Функция безопасности приборной системы безопасности (Safety instrumented function)
SIL	Уровень полноты безопасности (Safety integrity level)
SIS	Приборная система безопасности (Safety instrumented system)
SRS	Спецификация требований безопасности (Safety requirement specification)

4 Предварительная информация

В выбранную вначале коллективом разработчиков структуру МЭК 61511 не была включена более подробная информация, поясняющая цели или раскрывающая обоснования разработки или изменения в его разделах. Поэтому существует необходимость разъяснить изменения, предоставить обоснование каждого раздела стандарта, а также начальные сведения по функциональной безопасности в области промышленных процессов.

Настоящий стандарт помогает улучшить выполнение требований, содержащихся в изд. 2 в области промышленных процессов, предоставляя краткие ответы на вопросы «что», «почему» и «как» для каждого его раздела. Используя настоящий краткий обзор, начинающие специалисты в области функциональной безопасности смогут понять основные идеи, лежащие в основе положений изд. 2.

5 Управление функциональной безопасностью (изд. 2, раздел 5)

5.1 Почему этот раздел важен?

Управление функциональной безопасностью позволяет вести борьбу с систематическими отказами, которые в основном вызваны действиями людей и не поддаются количественной оценке, как в математических моделях. Эти действия, охватывающие весь жизненный цикл системы безопасности, выполняются в рамках процессов и процедур.

Функциональная безопасность не может быть реализована без участия людей, таких как персонал, участвующий в деятельности по обеспечению безопасности эксплуатирующей компании, инженерной компании, поставщика или любого лица, взаимодействующего с системой безопасности. В этом многопрофильном окружении все мероприятия необходимо четко определить и возложить их исполнение на конкретных лиц. Это повышает вероятность того, что никакая задача не будет пропущена, и обеспечит наличие ответственного лица для каждой задачи.

Для успешного выполнения каждой задачи МЭК 61511-1 требует компетентности всех сотрудников, назначенных для выполнения обязанностей по обеспечению безопасности на протяжении жизненного цикла SIS. В число таких сотрудников входят как руководители, так и подчиненные им ответственные исполнители. Ответственным исполнителем является лицо, которое в конечном счете несет ответственность за выполняемое действие или принимаемое решение. Для выполнения действия может быть назначен только один ответственный исполнитель. Руководителем является лицо(а), выполняющее определенную задачу.

Существует различие между оценкой функциональной безопасности (FSA) и аудитом функциональной безопасности. FSA представляет собой подробный обзор всех аспектов конкретной стадии жизненного цикла системы безопасности. Сроки проведения 1-го, 2-го и 3-го аудита функциональной безопасности связаны с основными стадиями реализации проекта с учетом того, где с точки зрения затрат эта работа будет выполнена наиболее эффективно, в отличие от одной оценки функциональной безопасности, выполняемой в конце проекта. С другой стороны, в процессе аудита функциональной безопасности выполняется анализ информации, документов и записей для определения того, что система менеджмента функциональной безопасности соответствует требованиям.

5.2 Распространенные ошибки

Существует ошибочное мнение, что система менеджмента МЭК 61511-1 и строгость требования к проекту для SIL 1 менее важны, чем для SIL 3. Системы менеджмента функциональной безопасности более высокого уровня (такие как квалификация, управление изменениями, оценка и аудит) в МЭК 61511-1 одинаково важны и направлены на предотвращение систематических ошибок или управление ими. Хотя реализация связанных и несвязанных с безопасностью функций в одной и той же системе не рекомендуется, но некоторые процедуры менеджмента функциональной безопасности, реализуемые для SIS, могут успешно использоваться для критических небезопасных систем, таких как системы защиты активов.

Проектные команды, стремящиеся к легко реализуемым решениям, иногда используют «мышление чек-листа» (формирование списка проверяемых результатов проекта, не обеспечивая их эффективным содержанием). Системы менеджмента являются «живыми» системами, которые нуждаются в постоянной поддержке для сохранения их эффективности. Информация, содержащаяся в этих системах, со временем используется для обеспечения корректной эксплуатации, технического обслуживания, управления изменениями и аудита систем безопасности.

Часто возникает желание отложить рассмотрение вопросов мониторинга функционирования и непрерывного менеджмента функциональной безопасности на время после запуска проекта. Хотя эти обязанности полностью ложатся на владельца/оператора, но возможности, необходимые для обеспечения этой деятельности, наилучшим образом реализуются при разработке проекта на основе междисциплинарного подхода, позволяющего проводить успешные предварительные проверки и избегать дорогостоящих доработок впоследствии.

Представленный в стандарте упрощенный пример жизненного цикла недостаточно детализирован для его реализации непосредственно на предприятии. Компания, внедряющая рабочую модель жизненного цикла, должна учитывать свою уникальную организационную структуру. План обеспечения безопасности оборудования этого предприятия должен включать дополнительные детали, такие как конкретные роли и обязанности, необходимые для его обоснованной установки в этой организации.

5.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

5.3.1 Существующие системы

Новое требование менеджмента функциональной безопасности в изд. 2, указывающее на приемлемость существующих систем, реализованных в соответствии с изд. 1 (или с предшествующими стандартами), признано необходимым и соответствующим области применения изд. 2. Это понятие иногда называют «освобождение от соблюдения новых норм». Обычно, это понимают неверно и считают, что для управления этими системами никакие действия не нужны. Поэтому в новом пункте 5.2.5.4 изд. 2 использован термин «существующие системы». С целью обеспечения достижения функциональной безопасности проводится оценка существующих систем и практик. Это требует, по крайней мере, выполнения оценки рисков, а затем анализ каждого независимого слоя защиты (IPL) для предотвращения и снижения оцениваемых рисков. Этот новый пункт также привел к пересмотру раздела 17, связанного с модификацией таких существующих систем.

В изд. 2 изменен пункт: 17.2.3.

В изд. 2 по отношению к изд. 1 включен новый пункт: 5.2.5.4.

5.3.2 Управление изменениями

Поскольку существующие системы, как правило, изменяются частично, необходимо было внести дополнительную ясность в вопрос о том, как выполнять такие изменения, используя системы менеджмента функциональной безопасности, включая анализ влияния изменений и анализ функциональной

безопасности, в рамках управления изменениями. Аналогично выполняются изменения требований к существующим SIS.

В изд. 2 по отношению к изд. 1 включены новые пункты: 5.2.6.1.9, 5.2.6.2.5 (см. также раздел 17).

5.3.3 Показатели производительности и обеспечение качества

Общей проблемой при проектировании SIS является использование чрезмерно оптимистичных данных, которые не применимы к условиям эксплуатации, в которой будет использоваться SIS. Однако даже если при первоначальном проектировании SIS используются данные и допущения, подходящие для данных условий эксплуатации, то изменения характеристик процесса, параметров эксплуатации, технического обслуживания и систем управления автоматикой со временем могут привести к снижению производительности системы и неприемлемому повышению риска. Основным подходом, указанным в МЭК 61511-1, для определения реально достигаемого снижения риска и его восстановления, является постоянный сбор данных о рабочих характеристиках, периодическая оценка их соответствия результатам анализа опасностей и рисков (H&RA) и требованиям SRS (то есть периодическое выполнение стадии 4 FSA) и, при необходимости, устранение отклонений. Ожидаемые результаты, связанные с контролем функционирования и обеспечением качества, соответствуют основным правилам менеджмента безопасности производственных процессов, таким как USA CFR 1910.119(j) США, контроль опасности возникновения крупномасштабных аварий на производстве (COMAH) Великобритании, правила, касающиеся опасных веществ и взрывоопасных сред (DSEAR) и приложение III к Директиве Совета 2012/18/EU Европейского сообщества, а также международным отраслевым стандартам (например, ИСО 14224).

В изд. 2 изменены пункты: 3.2.51, 5.2.5.3, 16.2.2.

В изд. 2 по отношению к изд. 1 включены новые пункты: 5.2.6.1.10, 11.4.9, 11.9.4, 16.2.9.

5.3.4 Компетентность

SIS, как правило, изменяются и влияют друг на друга реже, чем BPCS. Без переподготовки и постоянного практического опыта первоначальная компетентность специалистов со временем может снизиться. Наиболее распространенными областями, где это вызывает озабоченность, являются квалификация поставщиков услуг по проектированию SIS и при выполнении работ по H&RA и разработке SRS, персонал которых не имеет профессиональной подготовки и не демонстрирует компетентность как в области предотвращения ущерба, так и при реализации требований МЭК 61511-1. Поэтому необходима система управления компетентностью персонала.

В изд. 2 изменены пункты: отсутствуют.

В изд. 2 по отношению к изд. 1 включен новый пункт: 5.2.2.3.

5.3.5 Дополнительные требования к поставщикам изделий и услуг в области функциональной безопасности

Для обеспечения того, чтобы поставщики изделий и услуг в области функциональной безопасности были способны обеспечить достижение требуемых значений SIL и стойкости к систематическим отказам, эти поставщики помимо системы менеджмента качества теперь должны иметь систему менеджмента функциональной безопасности.

В изд. 2 изменены пункты: отсутствуют.

В изд. 2 по отношению к изд. 1 переработан пункт 5.2.5.2.

5.4 Кратко о том, что изменилось

Каждый проект SIS должен имеет четкие роли и обязанности. Все участвующие стороны должны быть осведомлены о своих обязанностях и компетентны выполнять соответствующие мероприятия, необходимые для обеспечения функциональной безопасности. Профессиональные качества должны обновляться. Все необходимые операции в проекте должны описываться в плане обеспечения безопасности, который может быть специальным для проекта или общим документом компании. Для всех соответствующих видов деятельности должен выполняться анализ функциональной безопасности (FSA), чтобы продемонстрировать, что функция безопасности SIS удовлетворяет всем требованиям и соответствует согласованным стандартам. Управление эффективностью функционирования в ходе эксплуатации должно осуществляться путем сбора полевых данных для обеспечения безотказности SIS и информации о запросах к SIS. Аудиты функциональной безопасности должны проводиться через равные промежутки времени, чтобы продемонстрировать, что участвующие организации по-прежнему способны выполнять заданные требования функциональной безопасности. Деятельность по оценке и аудиту должна осуществляться отдельными лицами, независимыми от группы проектировщиков. По

результатам оценки и аудита должна быть сформирована содержательная документация, а рекомендации должны сопровождаться с целью их эффективного выполнения.

6 Жизненный цикл системы безопасности (изд. 2, раздел 6)

6.1 Почему этот раздел важен?

Для обеспечения функциональной безопасности необходимо выполнить ряд действий (в основном выполняются различными заинтересованными сторонами, например конечным пользователем, проектной организацией, поставщиками). Все эти действия связаны друг с другом подобно цепи, и прочность этой цепи будет равна прочности самого слабого звена. Крайне важно рассматривать функциональную безопасность как жизненный цикл, который начинается с идентификации опасности и заканчивается выводом из эксплуатации SIS, а не как самостоятельные и отдельные действия. Все действия на жизненном цикле системы безопасности зависят от действий на восходящих и нисходящих ветвях.

6.2 Распространенные ошибки

Помимо необходимости включить в план обеспечения безопасности детальную информацию, связанную с конкретной организацией, проектные команды, не имеющие опыта реализации жизненного цикла системы безопасности, часто не понимают и не планируют итеративный характер выполнения H&RA, разработки SRS и проектирования SIS. Это может привести к неожиданным исправлениям проекта и увеличению затрат. Если персонал проекта прошел достаточно узкоспециализированную подготовку, то необходимые (в процессе проектирования) взаимодействия могут быть не замечены.

6.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

Раздел 6 был обновлен с целью охвата всех видов деятельности, в частности прикладного программирования. Материалы, касающиеся прикладного программирования, из раздела 12 были включены в раздел 6. Дополнительные сведения о перемещении информации, связанной с прикладным программированием, см. также в 12.3.

6.4 Кратко о том, что изменилось

На стадии планирования должна определяться общая последовательность работ на жизненном цикле SIS. На следующем шаге должен быть создан подробный список действий, включающий разработку прикладного программного обеспечения, и другие рабочие процессы. Описание жизненного цикла должно включать в себя входную и выходную информацию, процедуры и процессы, обеспечивающие выполнение каждой его стадии, и, наконец, данные об организациях/лицах, ответственных за ее выполнение.

7 Верификация (изд. 2, раздел 7)

7.1 Почему этот раздел важен?

Последовательное выполнение исследования, анализа и/или тестирования для каждой стадии сокращает количество систематических ошибок и позволяет найти возможные проблемы и ошибки с целью повышения эффективности затрат. Данный раздел определяет некоторые вопросы планирования верификации. В частности, верификация, использующая тестирование, включает в себя несколько подробно описанных задач, позволяющих убедиться, что тест выявит любые ошибки.

7.2 Распространенные ошибки

Люди часто полагают, что верификация и валидация — это одно и то же, что приводит к тому, что одна из этих процедур не выполняется. Кроме этого, существует непонимание того, что верификация выполняется только в рамках заводских испытаний (FAT) или предпускового анализа безопасности, а не систематически на протяжении всего жизненного цикла.

7.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

Были добавлены требования к верификации, которые включают тестирование, обеспечивающее отсутствие влияния функций, не связанных с безопасностью, на выполнение функций, связанных с безопасностью, и применение оценок влияния изменений, выявленных в ходе верификации. В случае обновлений также необходимо, чтобы модификации, выполняемые во время тестирования, были повторно верифицированы.

В изд. 2 изменены пункты: 7.2.1, 7.2.6 (был 7.1.1.2).

В изд. 2 по отношению к изд. 1 включены новые пункты: 7.2.2, 7.2.3 и 7.2.5.

7.4 Кратко о том, что изменилось

Должен быть создан план тестирования и анализа для каждого действия, включая разработку прикладной программы и жизненного цикла системы безопасности. Этот план должен включать способы выполнения тестирования или анализа и критерии успешности для выполнения требований каждой задачи.

8 Анализ опасностей и рисков (изд. 2, раздел 8)

8.1 Почему этот раздел важен?

Процесс H&RA оценивает технологическую схему для определения опасных событий, ограничений проектирования, возможных причин этих событий и защиты от них. H&RA разрабатывает основу функциональной безопасности процесса. Анализ опасностей имеет важное значение для выявления конкретных опасностей процесса и определения уровня защиты, необходимой для конкретных событий. В раздел 8 включен анализ защищенности для решения проблем кибер- и физической безопасности.

Частота отказов, связанных с отказами, возникающими в BPCS, а также некоторое снижение риска, распределенное по уровням защиты BPCS (см. 9.3.1, где рассматриваются уровни защиты BPCS), непосредственно влияют на целевое значение уровня снижения риска и режим работы, соответствующей функции безопасности SIS. Поэтому изд. 2 ограничивает (на основе устоявшегося консенсуса в области промышленных процессов) значение интенсивности отказов, которое может быть заявлено для BPCS.

8.2 Распространенные ошибки

Персонал, выполняющий H&RA технологического процесса с помощью методов анализа рисков (HAZOP, FMEA, что если?), часто не понимает требования к определению режима работы функции безопасности SIS и необходимому значению SIL для нее. Кроме того, разработчикам часто не хватает навыков для надлежащего выполнения этих задач из-за того, что они не знакомы с методологиями назначения величины интенсивности отказов для BPCS, SIS и SIL (такими как LOPA, граф рисков, Матрица рисков, описанные в МЭК 61511-3), что часто приводит к неудовлетворительному выполнению процессов H&RA и распределению приборных уровней защиты.

Одно из распространенных заблуждений состоит в том, что МЭК 61511-1 не включает требования к H&RA или приборным уровням защиты с уровнем снижения риска (RRF) менее или равным 10. Из-за непосредственного и неизбежного влияния отказов BPCS и других приборных уровней защиты на спецификацию и проектирование функции безопасности SIS эти требования были признаны необходимыми и были включены в разделы, рассматривающие H&RA.

Другое ошибочное мнение состоит в том, что предельное значение частоты отказов BPCS в качестве исходного источника предназначено специально для аппаратных средств BPCS (или даже только для самого контроллера). BPCS, как определено в изд. 2, включает в себя все устройства, необходимые для обеспечения того, чтобы технологический процесс выполнялся заданным способом, за конкретным исключением устройств, выполняющих функции безопасности SIS (то есть SIS). Задавая планируемую частоту отказов (примерно один отказ в десять лет), важно понимать, что в характеристике интенсивности отказов BPCS обычно доминирует частота ошибок человека (например, контроллеры были оставлены в ручном режиме, неуправляемые изменения в настройках программы или эксплуатация при значениях параметров, выходящих за ограничения, предусмотренные в первоначальном проекте технологического процесса).

Команды H&RA, которые не привлекают специалиста, компетентного в обеспечении функциональной безопасности технологического процесса, как правило, недооценивают долгосрочные затраты и сложность выполняемых действий на стадиях жизненного цикла SIS. Это приводит к тому, что не рассматриваются другие методы снижения риска, что приводит к дополнительным функциям безопасности SIS или аварийным сигналам вместо того, чтобы создать изначально более безопасный проект, используя предохранительные клапаны давления или пассивные средства обеспечения безопасности, которые будут иметь более низкую стоимость владения на протяжении длительного времени. Также зачастую недооценивается последствие несвоевременного выполнения работы по H&RA.

H&RA — это, как правило, итеративная работа, которая часто не понимается или не отражается в графике проекта и штатном расписании. Например проекты, в которых используются поставляемые комплекты, обычно предоставляют информацию по функциональной безопасности позже, чем это необходимо для конкретной проектной деятельности, или не могут использовать подходы H&RA, которые соответствуют основным принципам безопасности предприятия. Это может привести к дополнительной верификации и оценкам (см. раздел 5).

Одно из ошибочных мнений, связанное с H&RA, состоит в том, чтобы сосредоточиться только на предписанном режиме работы технологического процесса, забывая о других режимах работы, таких как запуск, останов, техническое обслуживание, сбой процесса и аварийный останов. Опыт показывает, что большинство инцидентов возникают в не предписанных режимах работы.

8.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

В связи с увеличением числа инцидентов кибербезопасности в системах управления и безопасности промышленной автоматики во всем индустриальном мире и более частым применением SIS с возможностью цифровой связи с другими устройствами, в изд. 2 были добавлены повышенные требования к защите информации. В область применения и цели изд. 1 не предполагалось включать дополнительные подробные требования к информационной безопасности в модель жизненного цикла SIS. Изд. 1 указывает, что функциональная безопасность может быть достигнута только с учетом угроз кибербезопасности путем тесной координации между соответствующими дисциплинами в рамках общего управления технологическим процессом. Изд. 2 уточняет, какие минимальные действия по защите информации должны быть выполнены для ее обеспечения в SIS без дублирования необходимых средств или целей обеспечения такой защиты, поскольку это входит в область применения специальных документов, таких как МЭК 62443 (все части). Новые разделы указывают, что должна быть выполнена оценка рисков, связанных с возможными нарушениями защиты информации, включая SIS, и чтобы SIS была разработана с учетом обеспечения необходимой устойчивости к рискам защиты информации и постоянного управления ими (см. также раздел 10).

В изд. 2 по отношению к изд. 1 включен новый пункт: 8.2.4.

8.4 Кратко о том, что изменилось

H&RA технологического процесса должен быть выполнен во время начальной стадии проектирования и повторно выполняется после рабочего проектирования. В разделах 8 и 9 определяются требуемое снижение риска и слои защиты для обеспечения снижение риска с любым значением коэффициента снижения риска от значения риска, присущего технологическому процессу, до допустимого значения риска, установленного уполномоченным органом. Примеры того, как это может быть выполнено, приведены в МЭК 61511-3:2016. Анализ системы защиты информации BPCS, включающей в себя SIS, выполняется, как определено в 8.2.4 изд. 2. В примечаниях к 8.2.4 изд. 2 приведены примеры выполнения такого анализа. Несоответствия, выявленные в ходе этого анализа, оформляются документально и устраняются перед запуском нового или измененного технологического процесса.

9 Распределение функций безопасности по слоям защиты (изд. 2, раздел 9)

9.1 Почему этот раздел важен?

Не все меры безопасности в соответствии с требованием могут обеспечить снижение риска, необходимое для того или иного опасного события. Отсутствие независимости между слоями защиты может привести к недостаточному снижению риска по отношению к требуемому значению. В настоящем разделе определяются некоторые требования к функциям безопасности и способы их распределения

по слоям защиты, включая оценку общих причин, ограничений на слои защиты BPCS, а также рассматривается влияние разнообразия, разделения и независимости.

9.2 Распространенные ошибки

Зависимость между слоями защиты и инициирующим источником опасного события часто считают незначительной. Как правило, это связано с несоответствующей документацией по функциональной безопасности или неполным H&RA технологического процесса. Аналогичным образом при назначении целей снижения риска средствам обеспечения безопасности часто не учитываются ограничения существующего оборудования, например устройства могут находиться в труднодоступном месте или иметь известные проблемы с производительностью. Наконец, команды часто игнорируют возможную зависимость слоя защиты BPCS и завышают оценку снижения риска для BPCS.

Другое ошибочное мнение состоит в том, что слой защиты BPCS и BPCS являются терминами, которые могут использоваться как взаимозаменяемые. BPCS — это интегрированная система устройств (таких как полевые приборы, контроллеры, вспомогательные системы и HMI), которые используются для безопасной эксплуатации производственной системы, за исключением SIS. Слой защиты BPCS является конкретным независимым механизмом в BPCS (устройством BPCS или набором устройств BPCS), реализующим функции безопасности. С достаточным уровнем независимости между слоями защиты BPCS в BPCS могут поддерживаться до двух таких слоев защиты BPCS.

Часто считают, что МЭК 61511-1 применяется только к превентивным мерам обеспечения безопасности. Требования жизненного цикла в МЭК 61511-1 применяются также к слоям защиты, которые смягчают последствия опасного события и основаны на приборных функциях с требуемым значением SIL, равным 1 или более, определенным в результате анализа опасности технологического процесса. Например, системы обнаружения пожарной и газовой опасности и запуска водяной завесы. Верификация снижения риска для этих систем включает в себя анализ охвата устройства обнаружения и эффективности ослабления не только датчика, логического решателя, исполнительного устройства, но и аппаратных средств системы вспомогательных устройств, вносящими вклад в интенсивность отказов. Реализация мер по смягчению последствий, осуществляющих снижение риска более, чем в 10 раз, является достаточно трудной задачей.

9.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

9.3.1 Ограничения на слои защиты BPCS

Частота отказов, заявленная для инициирующих источников, связанных с отказом контура управления BPCS, и снижение риска, распределенное слоям защиты BPCS, таким как типовые аварийные сигнализации, непосредственно влияют на достижение цели снижения риска и режим работы для соответствующей функции безопасности SIS. Опыт применения изд. 1 показал, что в его пунктах 9.4.2 и 9.4.3 недостаточно четко были выражены следующие ограничения, предусмотренные ТК МЭК 65А:

- максимальное снижение риска, которое может быть назначено для слоя защиты BPCS;
- максимальное количество независимых слоев защиты, которые могут быть реализованы в BPCS для данного опасного события;
- требования к независимости для слоев защиты, реализуемых в BPCS.

Эти ограничения отражают общее влияние на эффективность, связанное с менее строгими методами проектирования, реализации и менеджмента, обычно применяемыми для BPCS (по сравнению с методами, используемыми для SIS). Важность каждого из этих ограничений, представленных в изд. 1, соответствуют постоянно развивающейся практике, которая в последнее время была продемонстрирована в публикации в области обрабатывающей промышленности, такой как CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, опубликованной в 2014 году.

Следует помнить о следующих ключевых моментах:

a) если для слоя защиты BPCS было назначено RRF > 10, то к подсистеме, реализующей этот слой защиты, применяются все соответствующие требования изд.1 (т. е. ее функция безопасности реализуется как для функции безопасности SIS);

b) если конкретное опасное событие затрагивает две функции BPCS (являющиеся инициирующим источником опасного события или слоем (слоями) защиты), то системы, выполняющие эти функции, либо должны быть независимыми, либо эти совместно используемые подсистемы должны соответствовать требованиям изд.1 к совместному снижению частоты последствий (т. е. совместно используемая подсистема фактически является подсистемой SIS).

В изд. 2 изменены пункты: 3.2.3, 8.2.2, 9.3.2, 9.3.3.

В изд. 2 по отношению к изд. 1 включены новые пункты: 9.3.4, 9.3.5.

9.3.2 Требование общего снижения риска более, чем в 10000 раз, для мер снижения риска

Основная причина изменения заключается в том, что, в то время как изд. 1 предусматривало требования для одиночной функции с SIL 4, в изд. 2 было принято решение о том, что вопрос об общем снижении риска в 10000 раз следует рассматривать независимо от того, относится ли оно к одной или нескольким функциям на различных слоях защиты. Если определено, что SIS или SIS совместно с BPCS должны обеспечить высокий уровень снижения риска (RRF > 10000), то группе H&RA следует пересмотреть изначально более безопасный проект или другие слои защиты (например, предохранительную арматуру, пассивные барьеры, административные средства управления доступом) для снижения риска. В то время как функция с SIL 4 или значение RRF, равное 10000, могут быть достигнуты математически, опыт сектора промышленных процессов показывает, что вопросы, связанные с систематическими отказами, при реализации таких высоких уровней снижения риска чрезвычайно затрудняют (и существенно повышают стоимость) не только их достижение, но и вызывают гораздо больше проблем при их технической поддержке. Даже когда снижение риска распределяется по нескольким слоям защиты с независимыми устройствами исходной системы безопасности (датчиками, логическими решателями, исполнительными устройствами), то для программирования, эксплуатации и обслуживания приборных средств обеспечения безопасности часто используется общий персонал. Если после анализа изначально более безопасного варианта реализации приборных функций защиты все еще подтверждается необходимость для RRF > 10000, то требуется более глубокий анализ случайных и систематических ошибок.

В изд. 2 изменен пункт: 9.2.5.

В изд. 2 по отношению к изд. 1 включены новые пункты: 9.2.6, 9.2.7.

9.4 Кратко о том, что изменилось

Анализ риска опасных событий (см. примеры в МЭК 61511-3) должен проводиться в соответствии с допустимыми требованиями к риску, установленными соответствующим уполномоченным органом или нормативно-правовой базой.

Одним из результатов этого анализа является выбор функций безопасности и их распределение по слоям защиты для снижения риска до допустимого уровня. Анализ функций безопасности и уровней защиты, используемый для проверки общего снижения риска, должен быть обоснованным и заслуживающим доверия подходом. Этот анализ должен учитывать множество факторов, таких как независимость, разнообразие, общая причина, обеспечение полноты, аудитопригодность, тестируемость и разделение между слоями. Если общее снижение риска, распределяемое приборным средствам обеспечения безопасности, превышает 10000, то следует тщательно проанализировать допущения, касающиеся эффективности и независимости слоев защиты (для каждого и инициирующего события). Если зависимость будет выявлена, то анализ ее последствий должен быть включен в общий количественный анализ. Этот анализ должен быть выполнен в процессе H&RA, а также в конце рабочего проектирования функций.

10 Спецификация требований безопасности SIS (изд. 1, раздел 10)

10.1 Почему этот раздел важен?

Каждой функции безопасности SIS необходима четко определенная и прослеживаемая спецификация требований в качестве основы для разработки SIS. Элементы требований к функционированию, которые документально оформлены в SRS, включая философию блокировок, основные принципы тестирования, утвержденные критерии устройства и время отклика функции безопасности SIS, обеспечивают важные входные данные для эффективной разработки SIS. SRS описывает требуемые функциональные возможности и безотказность, а также требования к прикладной программе.

Цель SRS состоит в том, чтобы служить базовой документацией при разработке SIS и определять функциональные требования и требования к полноте безопасности для всех функций безопасности SIS, которые должны быть частью SIS. SRS используется для формирования требований к проектированию аппаратных средств SIS и разработке прикладных программ. Она также используется для валидации SIS и может упростить подготовку процедур эксплуатации, технического обслуживания SIS,

контрольной проверки и ответа оператора на отказ функции безопасности SIS. SRS — это постоянно актуальная документация, которая подлежит обновлению в случае внесения каких-либо изменений в SIS. Для дальнейшей поддержки управления изменениями и для других действий по менеджменту функциональной безопасности также требуются определенная цель и подход, необходимые для получения более подробной информации из SRS.

10.2 Распространенные ошибки

Хотя основные положения SRS получены из документации по H&RA и распределению рисков, было бы неправильным считать, что все содержание SRS основано на документации по H&RA. Например, в 9.2.9 изд. 2 устанавливается, что в SRS должны быть также определены и документально оформлены функциональные потребности производственного процесса. Эта спецификация требований к производственному процессу затем используется в качестве входных данных для подготовки SRS.

SRS обеспечивает функциональные требования и требования к полноте безопасности для всех функций безопасности SIS. В соответствии с минимальными требованиями к содержанию SRS представляет собой документ, содержащий технические требования, а не документ для рабочего проектирования, для которого потребуется дополнительная документация, чтобы создать необходимый проект. Например, при проектировании отсутствие документации о требованиях к программированию дополнительных приложений может привести к тому, что программа не будет отвечать определенным функциональным требованиям SRS, таким как функционирование, необходимое в условиях отказа устройства. Дополнительные требования к проектированию аппаратных средств и разработке прикладных программ SIS могут быть представлены в руководствах по безопасности, руководствах по эксплуатации логических решателей и устройств SIS, методиках проектирования SIS, руководстве по установке контрольно-измерительных приборов, нормативных требованиях и в соответствующих общих отраслевых стандартах. Следует отметить, что проектная документация SIS включает также требования к функциям, не связанным с безопасностью, которые являются частью требований к SIS (в SRS не рассматриваются).

Часто возникают недоразумения относительно того, кто должен разрабатывать SRS (ошибочно считается, что оно формируется в результате отдельного направления деятельности) и когда, что приводит к отсутствию фактической информации или документации в SRS о том, как была создана SIS (что, в свою очередь, приводит к изменению задуманного порядка разработки и проекта).

Неверное представление о том, что SIS будет функционировать всегда, может привести к неудовлетворительному планированию действий в разделах SRS, касающихся ручной остановки, сохранения работоспособности в случае серьезного события или компенсирующих мер.

10.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

Опыт использования изд. 1 показал, что SRS и обоснование выбора устройств иногда излагаются на технически сложном языке, который может не поддерживаться, не поддаваться проверке или быть трудным для понимания при эксплуатации и техническом обслуживании, но который считается соответствующим изд.1. Например не всегда можно определить, что информация, используемая при выборе устройства и проектировании системы, связана с условиями эксплуатации данной установки. Поскольку ясность и применимость этой информации имеют существенно важное значение для достижения и поддержания ожидаемой эффективности функции безопасности, были представлены дополнительные рекомендации и требования. Например, были добавлены требования, касающиеся проведения контрольных проверок и их охвата, диапазона и точности измерений технологических показателей, выполняемых SIS, скорости утечки для арматуры трубопроводов, письменно оформленных процедур управления байпасами и требований к безопасности прикладных программ.

В изд. 2 изменены пункты: 7.2.1, 10.2, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6.

В изд. 2 по отношению к изд. 1 переработаны/включены новые пункты: 11.5.2.2, 11.9.2, 11.9.3, 16.2.13.

10.4 Кратко о том, что изменилось

Определение требований функций безопасности SIS является одним из важнейших направлений деятельности. Только полные и поддающиеся количественной оценке SRS гарантируют надлежащее проектирование, реализацию и испытание функции безопасности SIS. Полный набор SRS должен охватывать все вопросы функционирования, безопасности и безотказности, а также требования диагно-

стики и тестирования. Это можно выполнить в разных форматах, но на практике себя зарекомендовала форма, основанная на формате контрольного листа. Основной вклад в SRS должны вносить результаты, полученные из технологического/производственного отдела и предприятий и являющиеся в основном результатом стадии H&RA.

11 Проектирование и разработка (изд. 2, раздел 11)

11.1 Почему этот раздел важен?

Проектирование SIS включает в себя управление последствиями случайных отказов аппаратных средств и предотвращение или управление систематическими отказами. Эту деятельность в основном можно разделить на следующие четыре части.

a) выбор устройств надлежащим образом (на основе предыдущего использования или в соответствии с МЭК 61508-2);

b) обеспечение минимального резервирования, определяя HFT, либо в соответствии с подходом, используемым в секторе промышленных процессов и определенным в МЭК 61511-1, либо в соответствии с МЭК 61508-2;

c) проектирование архитектуры и прикладной программы в соответствии с требованиями SRS и проверка выполнения заданных технических требований по обеспечению полноты, безотказности и управлению систематическими ошибками (включая такие вопросы, как способности человека, управление байпасом, диагностический охват, отказы по общей причине, интервал контрольных проверок, MTTR);

d) обеспечение надлежащего разделения между SIS и BPCS как для аппаратных средств, так и для прикладных программ с тем, чтобы обеспечить выполнение общего снижения рисков.

Раздел 11 содержит проектные и технические требования к аппаратным средствам SIS, в то время как раздел 12 содержит соответствующие требования к прикладной программе.

11.2 Распространенные ошибки

При проектировании SIS необходимо выполнить несколько требований. Группы разработчиков, как правило, ориентируются на расчет SIL и уделяют недостаточное внимание прогнозируемой безотказности системы и систематическим требованиям проектирования, таким как важность использования полевых устройств с успешным предшествующим применением в аналогичных условиях эксплуатации и соответствие указанной требованиями HFT. При выполнении верификации SIL отсутствие понимания того, как будет использоваться диагностика устройства, может привести к оптимистическим результатам расчета.

Кроме того, команды могут неправильно использовать данные параметров безотказности из руководств по безопасности, не учитывая влияние приложения на способ использования этих данных. Некоторые расхождения, которые могут повлиять на правильное использование информации руководства по безопасности, включают в себя применение нормально-закрытых или нормально-открытых устройств, использование диагностик в архитектуре и влияние производственного процесса или внешней среды на производительность. Аналогично, существует недопонимание того, что использование устройства, удовлетворяющего требованиям МЭК 61508, не устраняет требование к устройству для оценки его пригодности в конкретных условиях эксплуатации. По этой причине в новых/измененных пунктах сформировано требование о сборе данных по надежности от потребителей, эксплуатирующих изделия в аналогичных условиях эксплуатации.

Команды часто неправильно сопоставляют значение SIL отдельных устройств, таких как логический решатель, с достигнутым значением SIL. Требования SIL применяются ко всей функции, а не к отдельным устройствам. Хотя все устройства, используемые в SIS, выбраны как подходящие для использования в применении с этим SIL (либо называются «соответствующие целевому назначению»), достигаемое значение SIL функции будет зависеть от многих факторов, таких как отказоустойчивость, безотказность и необходимый интервал контрольных проверок.

Например, для SIS, удовлетворяющей требованию SIL 2, которое было распределено ее функции безопасности в соответствии со значением снижения риска, полученным в результате его анализа, оцениваются две альтернативы значений характеристик устройств этой SIS. В обоих вариантах вклад

*PFD*avg каждой подсистемы находится в пределах SIL 2 или выше. Однако в варианте 1 общее значение превышает верхний предел, что приводит к общему значению SIL, равному 1.



Вариант 1 4E-3 + 5E-4 + 8E-3 = 12.5E-3 (> 1E-2)
Вариант 2 2E-3 + 5E-4 + 4E-3 = 6.5E-3 (< 1E-2)

Проектировщикам также следует учитывать, что для устройств, выбираемых в соответствии с требованиями МЭК 61508, для достижения необходимого значения SIL соответствующее руководство по безопасности может содержать требования о дополнительном их резервировании сверх минимального.

11.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

11.3.1 Отказоустойчивость аппаратных средств

Предписывающие ограничения HFT в изд. 1 были созданы, чтобы смягчить некоторые из наиболее распространенных систематических отказов проектирования и реализации:

- использование слишком оптимистичных допущений для параметров безотказности;
- ошибка технического обслуживания, например осталась закрыта коренная задвижка или перепускная перемычка осталась открытой.

В изд. 1 полевые устройства и логические решатели имели различные требования к HFT, поскольку полевые устройства были устройствами низкой сложности, а логические решатели были устройствами высокой сложности. Однако опыт применения HFT согласно требованиям изд. 1 выявил некоторые проблемы (например, снижение HFT на основе «доли безопасных отказов»).

В изд. 2 представлены три различных метода, позволяющие определить HFT:

- использование таблицы 6 в изд. 2, в сочетании с требованиями 11.4.5—11.4.9 в изд. 2;
- использование способа 1_H МЭК 61508-2 на основе анализа FMEDA и обеспечение соответствия с требованиями соответствующих пунктов МЭК 61508-2;
- использование способа 2_H МЭК 61508-2, основанного на возврате производителю информации об эксплуатации изделия, и обеспечение соответствия с требованиями соответствующих пунктов МЭК 61508-2.

Требования, представленные в изд. 2, таблица 6 и 11.4.5—11.4.9, были сформированы из описания способа 2_H, предложенного в МЭК 61508-2, и представляют собой упрощенные требования к HFT, основанные на SIL и режиме работы функции безопасности SIS. Например, в 11.4.9 определяется верхнее максимальное значение статистического доверительного интервала не менее 70 % вместо 90 %, которое требуется для способа 2_H, на том основании, что интенсивность отказов обоснована достаточными доказательствами, полученными от предыдущего использования в аналогичной среде, а также существующей системой технического обслуживания, ремонта и процедур восстановления.

Таблица 6 в изд. 2 была разработана для определения минимального значения HFT независимо от процесса, реализуемого для принятия решения об использовании устройств (см. 11.5). Важно отметить, что данная таблица применяется только в том случае, если выполнены требования 11.5—11.9 изд. 2 (такие как 11.5.2.2, где требуется, чтобы устройство соответствовало условиям эксплуатации). Например, для устройств, использующих программное обеспечение на языке программирования с полной изменчивостью (FVL) или на языке программирования с ограниченной изменчивостью (LVL), был установлен минимальный диагностический охват. С учетом соответствия требованиям остальных пунктов необходимость в отдельной таблице для программируемых устройств (например, логических решателей) не возникла. В изд. 2 аналогичным образом рассматриваются проекты для применений с SIL 4, но они имеют конкретные дополнительные требования, предусмотренные в разделах 9 и 12.

Кроме того, были добавлены пункты, указывающие, в каких случаях некоторые сбои могут быть исключены из анализа HFT. Если элемент системы имеет очень низкую вероятность случайных отказов из-за свойств, внутренне присущих его проекту и конструкции, то, возможно, отсутствует необходимость ограничивать полноту безопасности функции исходя из резервирования этого элемента. Например, при наличии резервированной входной платы логического решателя и резервированного процессора одноканальное подключение терминала не может существенно повлиять на интенсивность опасных отка-

зов. Другим примером может быть шкаф, совместно используемый платами резервированного канала ввода-вывода или процессорами логического решателя.

В изд. 2 изменены пункты: 11.4.3, 11.9.3—11.9.5.

В изд. 2 по отношению к изд. 1 переработаны/включены новые пункты: 11.4.1, 11.4.2, 11.4.4 в 11.4.9, 11.9.2.

11.3.2 Требования к риску, связанному с защитой информации

С ростом проблем защиты информации среды, окружающей SIS, был добавлен пункт об оценке рисков защиты информации с соответствующим требованием к проекту об обеспечении необходимого уровня устойчивости к идентифицированным рискам в области защиты информации (см. также раздел 7).

В изд. 2 по отношению к изд. 1 включен новый пункт: 11.2.12.

11.3.3 Руководство по безопасности

В изд. 1 необходимость разработки руководства по безопасности была определена сложным образом на основе значения SIL приложения, типа устройств (с/без прикладной программой) и типа языка программирования [фиксированный язык программирования (FPL), язык программирования с ограниченной изменчивостью (LVL) или язык программирования с полной изменчивостью (FVL)]. Для всех систем требовалось содержание операций адресации, технического обслуживания, обнаружения сбоев и ограничений реализации. Это требование в изд. 2 было упрощено, что неизбежно привело к независимому от технологий или значений SIL набору требований к формированию руководства по безопасности для SIS.

В изд. 2 по отношению к изд. 1 включен новый пункт, заменяющий несколько предыдущих: 11.2.13.

11.3.4 Требования к функционированию системы при обнаружении сбоя

Изд. 1 содержало три пункта, в каждом из которых описывались конкретные случаи, связанные с наличием отказоустойчивостью, отсутствием отказоустойчивости и непрерывными запросами, причем все они достигали общую цель. Эти три случая не охватывали все возможные случаи, поэтому в изд. 2 эти требования были упрощены и представлены двумя пунктами, где определены конкретные цели, которые будут применяться к любой реализации функции безопасности SIS.

В изд. 2 по отношению к изд. 1 переработаны пункты: 11.3.1 и 11.3.2.

В изд. 2 исключен пункт: 11.3.3 (перешел в 11.3.1 и 11.3.2, изд. 2).

11.3.5 Ограничения на проект формирования соединения полевых устройств

Пункт изд. 1, требующий выделенных линий связи для полевых устройств, был исключен вследствие прогресса в области измерительных и коммуникационных технологий (таких как разработка безопасных полевых шин) и во избежание предъявления требований, привязанных к определенным технологиям.

В изд. 1 исключен пункт: 11.6.3.

11.4 Кратко о том, что изменилось

Процесс проектирования предназначен для того, чтобы функция безопасности SIS выполнялась в соответствии с требованиями, определенными в SRS. Этот процесс также должен обеспечить: соответствие со всеми требованиями руководства по безопасности устройств, требованиями независимости и требованиями к тестируемости функции безопасности SIS.

Такие проектные решения, как выбор устройства/технологии, информация о взаимосвязях подсистем, способ обнаружения сбоев, соответствие архитектуры требованиям HFT, метод тестирования функции безопасности SIS, метод устранения систематических ошибок, а также случаи соответствия или превышения проектом целевых требований к полноте безопасности должны быть подробно документально оформлены. Например, должны быть подробно документально оформлены конкретные сведения о том, как следует информировать об обнаруженных сбоях, как на них следует реагировать (например, будет ли ответная реакция реализована автоматически или в ручном режиме) и какие системы используются для выполнения этого ответа. Эта документация должна использоваться при верификации проекта до его реализации, при верификации и валидации реализации проекта до возникновения опасности, а также при периодической оценке работы в процессе эксплуатации. Одним из основных документов, полученным в результате выполнения процесса проектирования, должно быть руководство по безопасности, в котором рассматриваются конкретные требования к эксплуатации и техническому обслуживанию для реализуемой SIS.

Без изменений по сравнению с изд. 1 осталось требование о том, что информация о предыдущем использовании (например, достаточный опыт, полученный при применении сложного логического решателя, а также учет других факторов, таких как среда эксплуатации устройства) может быть использована для принятия решения о применении сконфигурированных для выполнения функций безопасности логических решателей общего назначения вплоть до значений SIL, равного 2 (но не значения SIL, равного 3). Если требуется значение SIL, равное 3 (или выше), то анализ пригодности логического решателя требует применения более специализированных методов, представленных в МЭК 61508.

12 Разработка прикладной программы (изд. 2, раздел 12)

12.1 Почему этот раздел важен?

Подход МЭК 61511 в отличие от МЭК 61508 заключается в том, чтобы устанавливать требования к целям, которые должны быть достигнуты вместо того, чтобы требовать применения методов и методик для достижения тех же целей. В МЭК 61511-1 отсутствует градация целей разработки прикладной программы, так как этот стандарт разработан для последовательного создания соответствующей прикладной программы, реализующей функции со значениями SIL вплоть до равной 3 включительно.

Таким образом, МЭК 61511-1 разработан так, чтобы быть эффективным в пределах определенных ограничений, которые включают:

- использование языка программирования с ограниченной изменчивостью (LVL);
- использование простых приложений, для которых, как ожидается, технология LVL обеспечит разумную защиту от систематических ошибок, которые могут возникнуть при разработке прикладных программ.

Эти ограничения подробно описаны в приложениях E и G изд. 2.

Необходимо иметь процедуру последовательной разработки прикладной программы. В зависимости от сложности программного обеспечения, включая степень гибкости языка программирования и знакомство с этим языком групп прикладного программирования и эксплуатации, в такую процедуру разработки прикладной программы могут быть включены различные этапы. Минимальным набором таких этапов являются спецификация, реализация и верификация прикладной программы.

Изд. 2 включает требования к прикладному программированию со значением SIL, равным 4, но на подробную реализацию этих требований, чтобы избежать дублирования, делается ссылка на МЭК 61508.

12.2 Распространенные ошибки

Распространенное недопонимание состоит в том, что верификация SIS ограничивается проверкой аппаратных средств или проверкой функциональных свойств простыми тестами. Однако требуется верификация прикладной программы/конфигурации, которая может включать более сложные действия, такие как анализ динамического и статического функционирования и подтверждение отсутствия опасных комбинаций переменных.

12.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

В изд. 1 положения, касающиеся прикладного программирования SIS, представлены в разделе 12. Поскольку остальная часть этого стандарта структурирована в соответствии с порядком жизненного цикла системы безопасности, это привело к путанице относительно того, когда в процессе выполнения проекта должны были выполняться действия по программированию приложений. Кроме того, некоторые из этих действий будут влиять на разработку или реализацию как аппаратных средств, так и прикладных программ.

В изд. 2 раздел 12 был значительно пересмотрен по многим причинам, одной из которых было более эффективное выполнение требуемых задач по верификации и оценке функции безопасности. Некоторые положения были перенесены из раздела 12, чтобы дать более четкие указания относительно того, когда должны быть выполнены эти задачи. Например, требования безопасности прикладных программ включены в основные требования SRS, чтобы подчеркнуть необходимость тесной взаимосвязи между SRS SIS и требованиями безопасности прикладных программ.

Другие разделы включают в себя требования о том, чтобы прикладная программа была разработана таким образом, чтобы упростить прослеживаемость требований этого стандарта (включая SRS), что приводит к легко читаемой и понятной программе.

В изд. 2 изменены пункты: 6.2.1, 7.2.1, 10.3.2, 17.2.3.

В изд. 2 по отношению к изд. 1 перемещены пункты (с дополнительной модификацией или без нее): 5.2.7.2, 6.3.1—6.3.3, 7.2.2, 7.2.3, 7.2.5, 10.3.3—10.3.6.

12.4 Кратко о том, что изменилось

Как и в разделе 11, процесс разработки прикладной программы предназначен для обеспечения реализации функции безопасности SIS в соответствии с требованиями, определенными в SRS, всеми требованиями руководств по безопасности устройств, требованиями независимости как для систем, связанных с безопасностью, так и систем, несвязанных с безопасностью, а также любыми конкретными требованиями к прикладному программному обеспечению из SRS.

Проектные решения, такие как выбор языка, модульность прикладной программы, блок-схема прикладной программы, определения переменных, способ верификации прикладной программы, а также способ устранения систематических ошибок, должны быть документально оформлены, чтобы проект можно было верифицировать на соответствие SRS до реализации. Прикладная программа документально оформляется для обеспечения возможности ее обратной прослеживаемости с SRS и условий сопровождения на стадии эксплуатации жизненного цикла.

13 Заводские приемочные испытания (изд. 2, раздел 13)

13.1 Почему этот раздел важен?

В области промышленных процессов обычно заводские приемочные испытания (FAT) включаются в договор на капитальное строительство объектов. Поэтому, если FAT требуются в соответствии с обеспечением безопасности, то раздел 13 предусматривает требования по созданию согласованной структуры действий для выполнения FAT. FAT — это способ выполнения верификации и валидации для некоторых элементов (разделы 7 и 15) в более контролируемой заводской среде, где легче и экономически выгоднее корректировать причины отказов или ошибок, а не устранять их после поставки и установки системы у заказчика.

13.2 Распространенные ошибки

Не всегда понятно, что FAT требуются только в том случае, если они были определены как часть процессов тестирования при планировании мер обеспечения безопасности.

Недопонимая ограничение области применения FAT, некоторые команды разработчиков могут путать эти действия с валидацией и попытаться исключить их из плана работ. FAT могут быть частью валидации, но не могут соответствовать всем требованиям валидации.

Другое ошибочное мнение заключается в том, что в FAT отсутствует цель, направленная на изменение проектов. В некоторых случаях, когда к существующей SIS добавляются функции безопасности, выполнение FAT всей системы может оказаться невозможным. Однако перед валидацией можно провести испытания отдельных компонентов. Преимущество FAT для компонентов/подсистем системы в этом сценарии состоит в том, чтобы минимизировать время нахождения в неисправном состоянии и/или риск ложных аварийных отключений во время выполнения валидации перед вводом новой или измененной функции безопасности SIS в эксплуатацию.

FAT не всегда могут быть одноразовым действием. Многоэтапные FAT становятся все более распространенными в более крупных проектах. FAT могут быть выполнены отдельно от тестирования аппаратных средств. Аналогично, тестирование интеграции системы коммуникаций обычно выполняется отдельно.

13.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

В принципе, цели изд. 1 и изд. 2 для FAT не изменились. Тем не менее, в изд. 1 раздел 13 являлся информативным, так как при планировании вы могли принять решение о выполнении или невыполнении FAT. В изд. 2 было принято решение более конкретно указать, что содержание раздела 13 требует-

ся для выполнения FAT, если FAT выбираются при планировании. Поэтому во всех подразделах слова «следует» изменены на «должен».

В изд. 2 незначительно изменены пункты: 13.1, 13.2.1—13.2.7.

13.4 Кратко о том, что изменилось

Документально оформленная процедура FAT должна включать объем и содержание работ при выполнении FAT, включая инструментальные средства, необходимые для выполнения этой процедуры. Кроме того, план функциональной безопасности, разработанный в соответствии с разделом 5, должен документально определить место FAT и ресурсы, выделяемые на их выполнение. График проекта обычно документально оформляется при его выполнении. Окончательный утвержденный отчет должен содержать документы об исполнении FAT, включая выводы и документы, подтверждающие исправления.

14 Установка (изд. 2, раздел 14)

14.1 Почему этот раздел важен?

В данном разделе рассматривается работа с компонентами SIS от момента их прибытия на объект до установки и ввода в эксплуатацию для подтверждения готовности компонентов к валидации. Систематические ошибки во время установки могут привести к отказу функции безопасности SIS. Например, неправильное выполнение мер по подготовке к зимнему периоду может привести к закупориванию импульсных линий связи или труб. Компоненты SIS обычно устанавливаются в соответствии с проектными и монтажными чертежами. Однако иногда при установке на предприятии необходимо вносить изменения в SIS. Например, воздух системы управления, подаваемый к клапану, необходимо направить в другой коллектор воздуха системы управления. Эти изменения должны быть рассмотрены компетентным лицом, которое может оценить влияние изменений на функцию безопасности SIS и саму SIS.

Ввод в эксплуатацию интеллектуальных полевых устройств является важной процедурой, поскольку при этом проверяется правильность калибровки и конфигурации устройства. Параметры технологического процесса, например удельная плотность рабочей жидкости, являются критическими для регламентированного функционирования полевого устройства и предписанного выполнения функции безопасности SIS.

14.2 Распространенные ошибки

Условия ввода в эксплуатацию и завершения монтажных работ для SIS часто неправильно понимают и представляют в графике проекта. Например, проводятся ли проверки контуров до или после завершения монтажных работ? Требования данного раздела — это перечень типовых операций ввода в эксплуатацию.

14.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

В изд. 2 существенные изменения в данном разделе отсутствуют. Незначительные изменения только в пунктах 14.1, 14.2.2—14.2.5 изд. 2.

14.4 Кратко о том, что изменилось

Установка, как правило, производится подрядчиками. Следовательно, очень важно довести до них в полном объеме и доступном виде информацию о процедурах ввода в эксплуатацию SIS и процедурах управления изменениями для компонентов SIS. Необходимо устанавливать компоненты SIS на основе проектной и монтажной документации, так как значительное количество систематических отказов SIS происходит из-за неправильной установки компонентов SIS. Любые отклонения должны проверяться квалифицированным персоналом для подтверждения того, что изменения не влияют на выполнение требований функциональной безопасности, указанные в SRS.

Планы ввода в эксплуатацию должны разрабатываться совместно с другими направлениями проектных работ. Например, на компоненты SIS могут оказывать воздействие гидравлические испытания труб. Ввод в эксплуатацию интеллектуальных полевых устройств должен включать проверку параметров конфигурации, таких как плотность заполняющей жидкости для уровнемера по перепаду давления. Документы по планированию использования ресурсов должны предусмотреть привлечение квали-

фицированных специалистов в области взаимодействия с другими системами, поскольку интерфейсы с другими системами обычно во время ввода в эксплуатацию тестируются впервые.

15 Валидация (изд. 2, раздел 15)

15.1 Почему этот раздел важен?

Валидация — это последняя операция, выполняемая перед вводом SIS и связанных с ней функций безопасности в эксплуатацию на заводском оборудовании. Валидация функции безопасности SIS — это сквозное тестирование, которое проверяет, что все компоненты, включая прикладную программу, функционируют в соответствии с целями SRS. Валидация также является последней возможностью обнаружить какие-либо отказы перед вводом SIS в эксплуатацию.

15.2 Распространенные ошибки

В некоторой степени как часть валидации могут быть использованы результаты FAT, но валидация не может быть исключена из графика работ на том основании, что выполнены FAT. FAT обычно тестируют один или несколько компонентов SIS в заводской среде. Однако они не заменяют валидацию, которая подтверждает, что интегрированная система на месте эксплуатации функционирует удовлетворительно.

Другое недопонимание заключается в том, что действия на жизненном цикле системы безопасности завершаются валидацией [которая может называться приемочными испытаниями на объекте (SAT)] или пуском предприятия. Согласно рисунку 8 изд. 1 и рисунку 7 изд. 2 жизненный цикл на этом не останавливается, а переходит на стадию эксплуатации, технического обслуживания и вывода из эксплуатации.

15.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

Новые пункты не добавлены. В 15.2.1 были добавлены дополнительные абзацы, касающиеся оборудования, необходимого для выполнения периодических испытаний, а в 15.2.2 о валидации документов на точность, согласованность и прослеживаемость.

В изд. 2 по отношению к изд. 1 для уточнения целей незначительно изменены пункты: 15.2.1, 15.2.2, 15.2.4—15.2.8.

15.4 Кратко о том, что изменилось

Валидация, как правило, приостанавливается, если другие направления проектных работ идут с отставанием от графика. Однако важно предоставить достаточно времени для валидации устанавливаемых и введенных в эксплуатацию SIS.

Результаты FAT можно использовать. Однако вопросы интеграции системы, которые не могут быть протестированы в процессе выполнения FAT, должны быть включены в план валидации. Например, общее время реакции функции, корректность подключения и конфигурацию отдельных устройств в производственной системе, а также подтверждение отсутствия взаимовлияний в установленной системе.

План валидации должен учитывать изменения, внесенные во время установки и ввода в эксплуатацию. Например, робастная процедура валидации должна выявлять систематические ошибки, такие как приведение в действие клапана SIS гидравлической системой, используемой для его срабатывания, при более низком давлении, что указано в технических условиях проекта. Любые изменения в SIS в ходе валидации должны проверяться квалифицированным персоналом для подтверждения того, что эти изменения не влияют на выполнение требований функциональной безопасности, указанные в SRS, а все изменения тестируются.

При проведении предпускового анализа безопасности (включающего стадию 3 оценки функциональной безопасности) должно быть проверено, что все функции безопасности SIS функционируют, включая подтверждение того, что байпасы/источники давления отключены, а измерительные отсечные клапаны или клапаны для отбора проб находятся в регламентированном положении.

16 Эксплуатация и техническое обслуживание (изд. 2, раздел 16)

16.1 Почему этот раздел важен?

В разделе 16 рассматриваются аспекты стадий эксплуатации и технического обслуживания жизненного цикла системы безопасности и их влияние на значение SIL в процессе эксплуатации и технического обслуживания для обеспечения требуемой полноты безопасности, поддерживаемой во время эксплуатации и соответствующим образом управляемой во время технического обслуживания.

16.2 Распространенные ошибки

Техническое обслуживание — это не только выполнение полного функционального тестирования. Выполнение полного функционального тестирования не является подтверждением того, что общая эффективность безопасности удовлетворительна. Для достижения ожидаемой эффективности от устройств SIS необходимы надзор и профилактическое техническое обслуживание. Для обеспечения достижения целей функциональной безопасности используется периодический контроль функционирования и устранение выявленных несоответствий.

План эксплуатации и технического обслуживания не может быть унифицирован и зависит от значения SIL и соответствующих особенностей технического обслуживания каждой функции безопасности SIS. План эксплуатации и технического обслуживания, процедуры и сбор данных о надежности включают в новый или измененный проект, что дает возможность выполнить эти задачи согласованно, без переработки и чрезмерных затрат.

Другая проблема, вызывающая путаницу в отношении технического обслуживания, связана с объектами, для которых требуется большой интервал между проверками. Устройства SIS не соответствуют целевым требованиям, если для них не могут быть выполнены контрольные проверки с определенной в проекте частотой из-за требований к эксплуатационной готовности. Существующая система, которая не может быть протестирована для достижения проектного значения SIL, нуждается в перепроектировании. Автоматизация диагностического тестирования и отчетности может быть полезна, но она не заменяет контрольную проверку и повторный ввод в эксплуатацию после проверки. Устройства, для которых невозможно избежать неполных контрольных проверок, заменяются или восстанавливаются на заводе-изготовителе с интервалом контрольных проверок, необходимым для достижения заданного значения SIL.

Другим распространенным заблуждением является то, что в процессе технического обслуживания при равнозначной замене не требуется выполнения процедур менеджмента функциональной безопасности или не требуется выполнения процедур управления изменениями при незначительных изменениях контрольно-измерительных приборов или при изменениях в процедурах эксплуатации и технического обслуживания SIS. И то, и другое необходимо для поддержания достигнутых результатов в течение продолжительного времени. Например, для случая использования байпаса при техническом обслуживании выполняется анализ снижения риска с применением компенсирующих мер для устранения возможного ухудшения характеристик.

Существует много ошибочных представлений, связанных с контрольными проверками устройств или подсистем после ремонта неисправного устройства, изменения установки или при проведении некоторого количества диагностических или частичных испытаний. Во всех этих случаях контрольные проверки по-прежнему являются необходимой частью обеспечения своевременного обнаружения и исправления как случайных, так и систематических опасных необнаруженных отказов.

16.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

16.3.1 Обнаружение сбоев, байпас и компенсирующие меры

Одним из распространенных базовых допущений при проектировании SIS является то, что устройство SIS будет выходить из рабочего режима при байпасе или при обнаружении отказа в течение ограниченного периода времени и что для устранения любого снижения риска в течение этого времени будут использоваться компенсирующие меры. Опыт, накопленный после публикации изд. 1, свидетельствует об отсутствии ясности в отношении этих основных ожиданий, связанных с управлением известными периодами неготовности SIS или с ухудшением характеристик. Для обеспечения оперативного реагирования на сбои и отказы, а также своевременного и удовлетворяющего требованиям использования байпасов эти действия необходимо учитывать при анализе опасностей, проектировании, планировании

эксплуатации и технического обслуживания, например, при формировании программы запасных частей. Аналогично, основные принципы механической целостности указывают, что необходимо собирать данные о параметрах надежности, чтобы можно было оценить рабочие характеристики. Анализ этих данных может выявить установки, которые нуждаются в корректировке, или возможное направление для снижения затрат на установку. Необходимы процедуры, выполняющие этих действия, для стадий эксплуатации и технического обслуживания.

В изд. 2 изменены пункты: 16.2.1, 16.2.3, 16.2.6, 16.2.9 и 16.2.10.

В изд. 2 по отношению к изд. 1 переработаны/включены новые пункты: 3.2.7, 11.3.1, 11.3.2, 11.8.4, 11.8.5, 16.2.4, 16.2.7, 16.2.12 и 16.2.13.

16.3.2 Контрольная проверка после ремонта и изменения

Во избежание указанных выше ошибок в интерпретации стандарта содержание пунктов было изменено, чтобы подчеркнуть необходимость контрольных проверок после ремонта и изменения устройства или прикладной программы, а также для ввода требования о наличии процедуры, определяющей действия в случае переноса сроков контрольных проверок.

В изд. 2 изменены пункты: 16.3.1.3, 16.3.1.4 и 16.3.1.6.

В изд. 2 по отношению к изд. 1 включен новый пункт: 16.3.1.7.

16.4 Кратко о том, что изменилось

Эксплуатация и техническое обслуживание SIS планируются на стадии проектирования до эксплуатации SIS. Для сохранения эффективности систем безопасности и управления рисками персонал по эксплуатации и техническому обслуживанию должен четко понимать опасности, существующие на объекте, и выполнять требуемые от них действия в соответствии с определенным планированием обеспечения безопасности, например готовность к выполнению действий, необходимых для осуществления компенсирующих мер, когда SIS обнаруживает отказ или находится в режиме байпаса. Операторы и обслуживающий персонал должен получать необходимую информацию в письменном виде и проходить обучение по обеспечению полноты безопасности всех функций на заданном уровне. Для них должны быть разработаны процедуры выполнения операций по эксплуатации и техническому обслуживанию в соответствии с планом обеспечения безопасности, включая компенсирующие меры, обеспечивающие безопасность в непрерывном режиме при отключении или ухудшении характеристик SIS из-за байпаса, ремонта или контрольной проверки.

17 Модификация (изд. 2, раздел 17)

17.1 Почему этот раздел важен?

Если модификация не планируется, не оценивается, не анализируется, не утверждается и документально не оформляется, то существует достаточно высокая вероятность ее негативного воздействия на функционирование SIS и на другие аспекты жизненного цикла системы безопасности.

17.2 Распространенные ошибки

Цели раздела 17 — разъяснить, что перед внесением изменений, влияющих на SIS, проводится анализ влияния этих изменений на функциональную безопасность, а для реализации изменений выполняется планирование обеспечения безопасности. Этот анализ влияния предназначен не только для инженеров SIS и/или оборудования, которые реализуют эти изменения, но и для задействованных членов группы H&RA, в которые могут включать дополнительные роли, такие как эксплуатационный персонал, технологи и инженеры по контрольно-измерительным приборам. Если влияние на функциональную безопасность было обнаружено, то далее выполняются процедуры оценки изменений и управления изменениями, которые определяют соответствующую(ие) стадию(и) жизненного цикла системы безопасности и действия, которые будут выполнены повторно, прежде чем изменение будет реализовано. Анализ влияния изменений также должен выполняться на стадиях проектирования и реализации проекта, если предлагаются изменения к утвержденным результатам предыдущих стадий проекта.

На некоторых предприятиях ошибочно считают, что документы H&RA и SRS необходимо обновлять только для аудита или другого анализа безопасности, а не в рамках текущего управления изменениями. Кроме того, могут не выполняться процедуры управления изменениями для изменений, внесенных в прикладную программу после успешной ее верификации, таких как изменение точек останова

или диагностических настроек. Аналогично, замена полевого устройства устройством, не полностью отвечающим требованиям SRS и, таким образом, не отвечающим критериям «равнозначной замены», может быть пропущена некоторыми программами управления изменениями. Анализ изменения может также ошибочно сконцентрироваться на изменении функции безопасности SIS и не оценивать влияние изменений на другие защитные или критические контуры управления.

17.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

Планирование и завершение изменения

Для устранения указанных выше ошибочных представлений были изменены и предложены пункты, обеспечивающие упреждающее планирование изменений, понимание влияния изменений на безопасность до внесения изменений и исчерпывающее обновление документации с внесением изменений (см. также раздел 4).

В изд. 2 изменены пункты: 17.2.3 и 17.2.6.

В изд. 2 по отношению к изд. 1 включены новые пункты: 17.2.4 и 17.2.5.

17.4 Кратко о том, что изменилось

Модификации должны выполняться в соответствии с процедурой получения разрешения и управления изменениями. Объем изменений должен готовиться вместе с соответствующим планом обеспечения безопасности, который содержит указания по оценке влияния предложенного изменения на функциональную безопасность, включая оценку риска, оценку влияния на другие функции и персонал, на полноту безопасности до и после модификации, на модификации SRS и документации. Этот план обеспечения безопасности должен быть документально оформлен, проанализирован и утвержден до получения разрешения. Модификацию должен выполнять квалифицированный персонал. Необходимая информация должна быть сохранена, и соответствующая документация обновлена. Чтобы избежать рисков, связанных с изменением, перечисленные выше действия должны выполняться и для простых изменений. Как правило, для простых изменений усилия на проведение оценки будут незначительными.

18 Снятие с эксплуатации (изд. 2, раздел 18)

18.1 Почему этот раздел важен?

Если снятие с эксплуатации не планируется, не оценивается, не анализируется, не утверждается и документально не оформляется, то существует достаточно высокая вероятность ее негативного влияния на функционирование SIS и на другие аспекты жизненного цикла системы безопасности.

18.2 Распространенные ошибки

В рамках текущего управления изменениями одним из распространенных заблуждений было не рассматривать изменения, связанные со снятием с эксплуатации, внесенные только в прикладную программу, например удаление программы для снятой с эксплуатации функции безопасности SIS, оставляя полевые устройства на месте для других целей. Анализ изменений также может быть ошибочно направлен на снятие с эксплуатации функции безопасности SIS без оценки влияния на проект SIS, вызванного снятием с эксплуатации других защитных средств или критических контуров управления. Например, снятие с эксплуатации функции управления сервисом или функции безопасности на одном оборудовании может оказать влияние на функциональную безопасность оборудования, совместно использующего этот сервис.

Другой распространенной ошибкой, связанной со снятием с эксплуатации, является то, что можно лишь частично выполнить работу по отключению SIS. Например, просто преобразовать подсистемы с остановом по включению питания и затем обесточить их, демонтируя сами устройства, но оставляя их в технической документации, или не учитывать функции и устройства при анализе опасности и исключить их из технической документации или документации по конфигурации, не демонтируя сами устройства, ЧМИ или шкаф управления этими устройствами. Такая частично выполненная работа может создать новые источники отказов и снизить эффективность усилий дальнейшего управления изменениями.

18.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

18.3.1 Планирование и завершение изменения

Для устранения указанных выше ошибочных представлений были изменены и сформированы пункты, обеспечивающие упреждающее планирование снятия с эксплуатации, понимание влияния изменений на безопасность до выполнения изменений и исчерпывающее обновление документации с внесением изменений (см. также раздел 4).

В изд. 2 изменены пункты: 18.2.1, 18.2.3, 18.2.4 и 18.2.5.

18.4 Кратко о том, что изменилось

Снятие с эксплуатации должно выполняться в соответствии с процедурой получения разрешения и управления изменениями. Объем работ по снятию с эксплуатации должен готовиться вместе с соответствующим планом обеспечения безопасности, который содержит указания по оценке влияния предложенного изменения на функциональную безопасность, включая оценку риска, оценку влияния на другие функции и персонал, на модификации SRS и документацию. Этот план обеспечения безопасности должен быть документально оформлен, проанализирован и утвержден до получения разрешения. Снятие с эксплуатации должен выполнять квалифицированный персонал. Необходимая информация должна быть сохранена, и соответствующая документация обновлена.

19 Документация (изд. 2, раздел 19)

19.1 Почему этот раздел важен?

На протяжении всего жизненного цикла системы безопасности имеется несколько заинтересованных сторон, ответственных за выполнение различных действий. Эти действия требуют определенную информацию, полученную в результате выполнения предыдущих действий. Для успешного выполнения каждого действия необходимо получать новую информацию и иметь актуальную документацию. По завершении действий необходимо сохранять информацию о результатах для дальнейшего доступа к ней и прослеживания.

19.2 Распространенные ошибки

Распространенное ошибочное представление о документации заключается в том, что информация о SIS должна находиться в одном документе, одной папке или в единой системе управления документами. Ключевым требованием является возможность прослеживания функциональных требований и требований полноты безопасности SIS.

19.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

Некоторые требования к документации стали нормативными (с использованием глагола «должен» вместо глагола «следует»). Кроме того, в перечень документов было добавлено руководство по безопасности.

В изд. 2 изменены пункты: 19.2.2, 19.2.9.

19.4 Кратко о том, что изменилось

«Связанная с SIS» информация должна разрабатываться на различных стадиях жизненного цикла SIS по нескольким направлениям и с участием нескольких отделов, поэтому информация может храниться в различных системах управления документами. Общий подход состоит в том, чтобы иметь документ, который описывает структуру информации, связанной с SIS, и предоставляет ссылку/указатель на местоположение, где хранится соответствующая информация. Например, SRS может находиться в папке SIS в системе управления документами производственной площадки, а записи контрольных проверок будут доступны в системе управления обслуживанием производственной площадки.

20 Определения (изд. 2, раздел 3)

20.1 Почему этот раздел важен?

Крайне важно, чтобы пользователи стандарта понимали используемую терминологию и почему определения в изд. 2 иногда отличаются от определений в других стандартах, таких как МЭК 61508 (все части).

20.2 Распространенные ошибки

Одно из распространенных заблуждений состоит в том, что определения в МЭК 61511 (все части) должны быть идентичны определениям в МЭК 61508 (все части). В целом определения в изд. 2 должны быть эквивалентны определениям в МЭК 61508-4:2012. Однако из-за значительного различия в контексте между МЭК 61511 (все части) и МЭК 61508 (все части) возникают ситуации, когда различие в определении или терминологии в определении считается необходимым для сектора промышленных процессов.

Определения в рамках МЭК 61508-4:2010 в некоторых случаях непременно формулируются на высоком концептуальном уровне или с использованием общей технической терминологии. Это необходимо для обеспечения того, чтобы содержание применялось ко всем секторам, попадающим в область применения этого базового стандарта безопасности. В результате в некоторых определениях МЭК 61508-4:2010 используется язык, недостаточно распространенный в секторе промышленных процессов. Это приводит к путанице для целевых пользователей сектора промышленных процессов МЭК 61511. Во избежание недоразумений в изд. 2 модифицированы или добавлены примечания к этим терминам.

Некоторые термины, используемые в изд. 2, не были определены в МЭК 61508-4:2010.

В тех случаях, когда отклонение от МЭК 61508-4:2010 было сочтено необходимым, комитет использовал действующие определения из материалов, указанных в Руководстве ИСО/МЭК 51:2014, МЭК 60050-192 (раздел надежности) или из аналогичных стандартов.

20.3 Что изменилось во 2-м издании по сравнению с 1-м и почему?

В таблице 2 перечислены все термины, определенные в изд. 2. В третьей графе таблицы 2 указывается на наличие одного или более изменений в профессиональной терминологии определения из изд. 1. В четвертой графе описывается основной подход к согласованию стандартов безопасности, применяемый для каждого термина, включая причины, по которым определение отличается от определения первоисточника, на который имеется ссылка. Если обоснование определений в изд. 2 приводится в контексте определений первоисточника, который с ними согласуется, то дополнительные пояснения в отношении изменений между изд. 1 и изд. 2 не приводятся.

Таблица 2 — Обоснование терминов и определений в изд. 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.1	Архитектура, конфигурация	Да	То же самое, что и в МЭК 61508-4:2010, но добавлено информативное примечание, уточняющее специфику сектора, см. обсуждение компонентов и элементов ниже
3.2.2	Защита имущества	Да	Уточнение, относящееся к обрабатывающей промышленности. В МЭК 61508-4:2010 не используется
3.2.3	Основная система управления процессом	Да	«Система управления EUC» определена в МЭК 61508-4:2010 слишком широко для использования в секторе обрабатывающей промышленности (также «EUC» обычно не используется в секторе промышленных процессов). Синонимом в изд. 2 является «основная система управления процессом»
3.2.4	Байпас	Новое	Уточнение, относящееся к обрабатывающей промышленности. МЭК 61508[1)] использует этот «запрещенный» термин, но не содержит его определение

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.5	Канал	Да	Эквивалентно определению в МЭК 61508-4:2010, см. обсуждение устройства и элемента. Применение изд. 2 не ограничивается функциями безопасности
3.2.6	Общая причина	Отдельное определение отсутствует	Отдельное определение отсутствует
3.2.6.1	Отказы по общей причине	Да	Определение из МЭК 61508-4 расширено и применяется в изд. 2 не только к каналам SIS. Оно уточняет, что отказы не являются следствиями друг друга, ограничивает общую причину отказов одним событием и не подразумевает, что в результате в системе происходит отказ
3.2.6.2	Отказы общего типа	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.7	Компенсирующие меры	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин не используется в МЭК 61508
3.2.8	Компонент	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.9	Управление конфигурацией	Да	Такое же, как в МЭК 61508-4:2010, за исключением примечания, касающегося требований к программному обеспечению
3.2.9.1	Консервативный подход	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.10	Система управления	Нет	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности. Термин «EUC» обычно не используется в обрабатывающей промышленности
3.2.11	Опасный отказ	Да	В техническом отношении аналогично определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.12	Зависимый отказ	Обновлены только примечания	Эквивалентно определению в МЭК 61508-4:2010. Для дальнейшего уточнения понятий были добавлены примечания
3.2.13	Обнаруженный, раскрытый, наблюдаемый	Да	Аналогично определению в МЭК 61508-4:2010, но определение в изд. 2 было расширено для включения программного обеспечения. Для дальнейшего уточнения понятий были добавлены примечания
3.2.14	Устройство	Да	Термин «элемент» из МЭК 61508-4 не используется в изд. 2. Этот термин создает путаницу в МЭК 61508-4:2010, поскольку определение «элемент» ссылается на «функцию безопасности элемента», определение которой, в свою очередь, ссылается на «элемент». Эта циклическая ссылка не может рассматриваться в качестве надлежащего определения ни одного из терминов. Термин используется только в изд. 2 как часть термина «исполнительный элемент»
3.2.14.1	Внешнее устройство	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин не используется в МЭК 61508
3.2.15	Диагностика	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.15.1	Охват диагностикой	Да	Определение изд. 2 аналогично определению в МЭК 61508-4:2010. Второе предложение в определении МЭК 61508-4 было заменено примечанием 2, поскольку оно не является ни определением, ни исключением. Для предотвращения неправильного употребления этого термина в определение изд. 2 было добавлено второе предложение для уточнения того, что не является диагностическим охватом. Это определение было расширено для применения к непостоянным интенсивностям отказов
3.2.16	Разнообразие	Да	Аналогично МЭК 61508-4:2010, с изменением примечаний для включения методов программирования
3.2.17	Ошибка	Нет	Соответствует 192-03-02 МЭК 60050-192:2015. Аналогично МЭК 61508-4
3.2.18	Отказ	Да	Соответствует 192-03-01 МЭК 60050-192:2015 с изменениями примечаний для уточнения, относящегося к обрабатывающей промышленности
3.2.18.1	Вид отказа	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен. Соответствует 192-03-17 МЭК 60050-192:2015
3.2.19	Сбой	Да	Соответствует 192-04-01 МЭК 60050-192:2015, модифицировано. Некоторые примечания изменены, другие удалены
3.2.20	Предотвращение сбоя	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует термин SIS для обрабатывающей промышленности
3.2.20.1	Исключение сбоев	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.21	Отказоустойчивость	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует «компонент» вместо «блок» по предложению рабочей группы
3.2.22	Исполнительный элемент	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.23	Функциональная безопасность	Удалено примечание	Эквивалентно определению в МЭК 61508-4:2010. Понятие «Система управления EUC», определенное в МЭК 61508-4:2010, является слишком широким для использования для обрабатывающей промышленности (термин «EUC» обычно не используется для обрабатывающей промышленности)
3.2.24	Оценка функциональной безопасности	Да	Эквивалентно определению в МЭК 61508-4:2010, но в изд. 2 используется терминология, соответствующая применению для обрабатывающей промышленности
3.2.25	Аудит функциональной безопасности	Нет	Аналогично МЭК 61508-4:2010
3.2.26	Полнота безопасности аппаратных средств	Да	Эквивалентно определению в МЭК 61508-4:2010, но в изд. 2 используется терминология, соответствующая применению для обрабатывающей промышленности
3.2.27	Вред	Да	Соответствует 3.1 Руководство ИСО/МЭК 51:2014. Эквивалентно определению в МЭК 61508-4:2010

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.27.1	Вредоносное событие	Новое	Эквивалентно определению в МЭК 61508-4:2010, но в изд. 2 предложено более краткое определение с использованием термина «опасное событие», к которому относятся «вредоносное событие» и «опасная ситуация» (см. примечание 1)
3.2.28	Опасность	Обновлены только примечания	Соответствует 3.2 Руководство ИСО/МЭК 51:2014. Модифицировано — добавлено примечание 1. Аналогично МЭК 61508-4:2010
3.2.28.1	Опасное событие	Новое	Соответствует 3.3 Руководство ИСО/МЭК 51:2014. Модифицировано — см. примечание 1. Эквивалентно определению в МЭК 61508-4:2010
3.2.28.2	Опасная ситуация	Новое	Соответствует 3.4 Руководство ИСО/МЭК 51:2014. Аналогично МЭК 61508-4:2010
3.2.29	Ошибка человека	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.30	Анализ влияния	Нет	Эквивалентно определению в МЭК 61508-4:2010. Удалено примечание из-за различий областей применения между МЭК 61508 и изд. 2
3.2.31	Независимая организация	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует термин SIS для обрабатывающей промышленности
3.2.32	Независимое лицо	Нет	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует термин SIS для обрабатывающей промышленности
3.2.33	Входная функция	Нет	Определение отраслевого термина добавлено, чтобы пояснить важность архитектуры, используемой в обрабатывающей промышленности. В МЭК 61508 термин не используется
3.2.34	Прибор	В определение термина 3.2.34.1 внесено примечание	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.34.1	Приборная система	Новое	Уточнение, относящееся к обрабатывающей промышленности. В МЭК 61508 термин не используется
3.2.35	Логическая функция	Нет (вторая фраза, которая не допустима в данном определении, была перенесена в примечание)	Добавлено специальное для сектора определение для уточнения важности архитектуры и логических преобразований ввода-вывода, используемых для обрабатывающей промышленности. Термин не используется в МЭК 61508
3.2.36	Логическое решающее устройство	Нет	Добавлено определение отраслевого термина для уточнения семейства контроллеров, используемых в обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.36.1	Конфигурируемое ПЭ логическое решающее устройство системы безопасности	Да	Добавлено определение отраслевого термина для уточнения важности двух типов логических решающих устройств, используемых в обрабатывающей промышленности для применения в системах безопасности. Термин не используется в МЭК 61508

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.37	Эксплуатационный/ инженерный интерфейс	Нет (вторая фраза, которая не допустима в данном определении, была перенесена в примечание)	Уточнение, относящееся к обрабатывающей промышленности. Эти термины не используются в МЭК 61508
3.2.37.1	Среднее время ремонта, MRT	Новое	Аналогично МЭК 61508-4:2010
3.2.37.2	Среднее время до восстановления, MTTR	Новое	Добавлено определение, совпадающее с МЭК 61508-4:2010, а также связанное с MPRT. Примечание — В МЭК 61508-4:2010 добавлено это определение, которое соответствует последним международным определениям (МЭК 61703), для строгого определения составных частей MTTR
3.2.37.3	Максимально допустимое время ремонта, MPRT	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин в МЭК 61508 не используется
3.2.38	Ослабление	Обновлены только примечания	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.39	Режим работы (функции безопасности SIS)	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.39.1	Режим работы функции безопасности SIS по запросу	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.39.2	Непрерывный режим работы функции безопасности SIS	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но отдельно не определен
3.2.40	Модуль	Да	Аналогично определению в МЭК 61508-4:2010, но с незначительными техническими изменениями, чтобы: i) повысить точность определения, поскольку модуль должен быть «автономным»; ii) признать, что изд. 2 сосредоточено только на программировании на LVL и FPL; iii) обновить даты для стандартов, указанных в примечаниях; iv) добавить примечание об одном возможном преимуществе использования модульного подхода
3.2.41	Moon	Нет	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.42	Необходимое снижение риска	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.43	Непрограммируемая система	Нет	Уточнение, относящееся к обрабатывающей промышленности. Термин не используется в МЭК 61508
3.2.44	Условия эксплуатации	Новое	Аналогично термину «окружение» в МЭК 61508-4:2010, но определение в изд. 2 более конкретно и рассматривает только условия эксплуатации технологического процесса
3.2.45	Режим работы, технологический процесс	Новое	Уточнение, относящееся к обрабатывающей промышленности
3.2.46	Интерфейс оператора	Да	Уточнение, относящееся к обрабатывающей промышленности
3.2.47	Выходная функция	Да	Добавлено специальное для сектора определение для уточнения важности архитектуры, используемой для обрабатывающей промышленности
3.2.48	Рабочая характеристика	Новое	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.49	Стадия	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.50	Предотвращение	Нет	Уточнение, относящееся к обрабатывающей промышленности. Термин не используется в МЭК 61508
3.2.51	Предшествующее применение	Да	Несмотря на ссылки на «проверено в эксплуатации», этот термин в МЭК 61511 не определен. В изд. 2 используется термин «предшествующее применение», семантика которого аналогична, но основан на установленных пользователем спецификациях в отличие от «проверено в эксплуатации», который основан на спецификациях производителя
3.2.52	Риск процесса	Нет	Уточнение, относящееся к обрабатывающей промышленности. Термин не используется в МЭК 61508
3.2.52.1	Время безопасности процесса	Новое	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.53	Программируемая электроника	Да	Аналогично МЭК 61508-4:2010, с незначительными техническими изменениями в примечаниях для демонстрации примеров, которые чаще всего встречаются в обрабатывающей промышленности
3.2.54	Программируемая электронная система, ПЭС	Да	Эквивалентно определению в МЭК 61508-4:2010, с изменениями для поддержания согласованности с терминологией для обрабатывающей промышленности, например, использование «устройство» вместо «элемент» (см. выше). Редакционные изменения: i) рисунок (для упрощения), ii) примечание (для упрощения объяснения). Не включены схемы конфигурирования ПЭС и заменены примечанием

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.55	Программирование	Обновлены только примечания	Добавлено специальное для сектора определение для уточнения значения прикладного программирования. Термин используется в МЭК 61508, но не определен
3.2.56	Контрольная проверка	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.57	Слой защиты	Обновлены только примечания	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.58	Качество	Нет	Уточнение, относящееся к обрабатывающей промышленности. Соответствует ИСО 9001
3.2.59	Случайный отказ аппаратных средств	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.60	Резервирование	Да	Аналогично МЭК 61508-4:2010, с изменением примечаний
3.2.61	Риск	Да	Соответствует 3.9 Руководство ИСО/МЭК 51:2014. Аналогично МЭК 61508-4:2010, с изменением примечаний
3.2.62	Безопасный отказ	Да	Определение в изд. 2 расширено относительно МЭК 61508-1:2010, так как от применения зависит, является ли отказ безопасным
3.2.63	Безопасное состояние	Обновлены только примечания	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.64	Безопасность	Да	Соответствует 3.14 Руководство ИСО/МЭК 51:2014, изменено с целью добавления примечания. Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.65	Функция безопасности	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.66	Функция безопасности приборной системы безопасности	Да	Уточнение относится к обрабатывающей промышленности и использует терминологию сектора промышленных процессов
3.2.67	Приборная система безопасности; SIS	Нет (вторая фраза, которая не допустима в данном определении, была перенесена в примечание)	Аналогично определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.68	Полнота безопасности	Да	Эквивалентно определению в МЭК 61508-4:2010, с изменениями для использования терминологии обрабатывающей промышленности. Кроме того, в примечания были внесены разъяснения вопросов, связанных с обрабатывающей промышленностью
3.2.69	Уровень полноты безопасности, SIL	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию для обрабатывающей промышленности

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.69.1	Требования к полноте безопасности	Новое	Изд. 2 обобщает это понятие от документа (согласно определению в МЭК 61508-4:2010) до соответствия целям этого документа, основываясь на использовании этого термина в контексте изд. 2
3.2.70	Жизненный цикл SIS	Да	Аналогично определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.71	Руководство по безопасности, руководство по функциональной безопасности	Да	Не эквивалентно определению в МЭК 61508-4:2010. Область применения руководства по безопасности в изд. 2 отличается от области применения руководства по безопасности в МЭК 61508-4:2010. Краткое объяснение приведено в примечании 4
3.2.72	Спецификация требований к безопасности SRS	Да	Аналогично определению в МЭК 61508-4:2010. Небольшое техническое отличие — МЭК 61508 разделяет требования к функции безопасности SIS и к SIS, а содержательно разделяет их по функциям и по значениям SIL. Изд. 2 соответствует подходу изд. 1, согласно с которым требования к функции безопасности SIS и SIS приведены в одной спецификации (которая также используется в МЭК 61508-2:2010). Изд. 2 также объединяет функциональные требования и требования к полноте в единую спецификацию
3.2.73	Датчик	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.74	Программное обеспечение, ПО	Да	Эквивалентно определению в МЭК 61508-4:2010, с незначительными редакторскими изменениями: i) исключен термин «продукт интеллектуальной деятельности», чтобы быть ближе к МЭК 60050-192:2015; ii) добавлено примечание для иллюстрации конкретных языков программного обеспечения, используемых в изд. 2
3.2.75	Языки прикладного программирования	Отдельное определение отсутствует	Отдельное определение отсутствует
3.2.75.1	Фиксированный язык программирования, FPL	Да	Добавлено специальное для сектора определение для уточнения различия между устройствами, содержащими программное обеспечение, которое может быть запрограммировано разработчиком приложения, и устройствами, которые ограничены выбором параметров. Термин не используется в МЭК 61508
3.2.75.2	Язык программирования с ограниченной изменчивостью, LVL	Да	Аналогично определению в МЭК 61508-4:2010, но имеет некоторые ключевые (существенные) отличия, чтобы сохранить цель изд. 2 в решении конкретных проблем, связанных с необходимыми ограничениями языка LVL при использовании для систем безопасности для обрабатывающей промышленности. МЭК 61508:2010, напротив, полностью принял терминологию МЭК 61131-3:2003, которая не требует каких-либо ограничений для применения в области безопасности. На самом деле в приложениях МЭК 61508-3:2010 указаны общие ограничения безопасности

Продолжение таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.75.3	Язык программирования с полной изменчивостью, FVL	Обновлены только примечания	Добавлено специальное для сектора определение для уточнения различия между общими языками программирования и LVL. Термин не используется в МЭК 61508
3.2.76	Типы ПО и программ	Отдельное определение отсутствует	Отдельное определение отсутствует
3.2.76.1	Прикладная программа	Да	МЭК 61508-4:2010 определяет термины «прикладное программное обеспечение», «данные приложения» и «данные конфигурации». Синонимом в изд. 2 является «прикладная программа»
3.2.76.2	Встроенное программное обеспечение	Нет (вторая фраза, которая не допустима в данном определении, была перенесена в примечание)	Аналогично определению «системное программное обеспечение» в МЭК 61508-4:2010, но определено конкретное ограничение в том, что системное программное обеспечение недоступно для конечного пользователя
3.2.76.3	Сервисное программное обеспечение	Нет (вторая фраза, которая не допустима в данном определении, была перенесена в примечание)	Аналогично определению «средства поддержки программного обеспечения в автономном режиме» в МЭК 61508-4:2010, но определено конкретное ограничение в том, что сервисное программное обеспечение не требуется для эксплуатации SIS конечным пользователем и поэтому класс Т3 исключается из 3.2.11 МЭК 61508-4:2010
3.2.77	Жизненный цикл прикладной программы	Да	Эквивалентно определению «жизненный цикл программного обеспечения» в МЭК 61508-4:2010, но изд. 2 ограничивается областью применения для обрабатывающей промышленности
3.2.78	Подсистема SIS	Да	Термин «подсистема» в изд. 2 используется по-разному. В изд. 2 см. синонимы: «подсистема SIS» и «система»
3.2.79	Система	Да	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
3.2.80	Стойкость к систематическим отказам	Новое	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.81	Систематический отказ	Да	Аналогично определению, содержащемуся в МЭК 61508-4:2010, но с незначительными изменениями в терминологии обрабатывающей промышленности, под «документом» понимаются все процедуры, такие как процедуры технического обслуживания, система управления документацией и эксплуатационные процедуры. Добавлено примечание 1
3.2.82	Систематическая полнота безопасности	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности
3.2.83	Целевая мера отказов	Да	Эквивалентно определению в МЭК 61508-4:2010, но изд. 2 использует терминологию обрабатывающей промышленности

Окончание таблицы 2

№ термина в изд. 2	Термин	Определения в изд. 1 и изд. 2 различаются?	Обоснование определения изд. 2
3.2.84	Приемлемый риск	Да	Соответствует 3.15 Руководство ИСО/МЭК 51:2014. Аналогично МЭК 61508-4:2010, с изменением примечания
3.2.85	Необнаруженный, нераскрытый, ненаблюдаемый	Да	Определения изд. 2 обнаруженный/раскрытый/наблюдаемый были расширены относительно МЭК 61508-4, чтобы включить программное обеспечение. Для дальнейшего уточнения этих концепций были добавлены примечания. Определения необнаруженный/нераскрытый/ненаблюдаемый были представлены простыми антонимами
3.2.86	Подтверждение соответствия	Да	Аналогично МЭК 61508-4:2010, но примечания были изменены для соответствия модели жизненного цикла изд. 2
3.2.87	Верификация	Да	Аналогично МЭК 61508-4:2010, но примечания были изменены для соответствия модели жизненного цикла изд. 2
3.2.88	Сторожевое устройство	Обновлены только примечания	Уточнение, относящееся к обрабатывающей промышленности. Термин используется в МЭК 61508, но не определен
[1] Если в настоящей таблице упоминается «МЭК 61508», то он относится ко «всем частям», если не упомянута конкретная часть.			

20.4 Кратко о том, что изменилось

Пользователи в секторе промышленных процессов иногда применяют принятую в компании терминологию, которая используется вместо терминов из отраслевых стандартов. Чтобы укреплять связь между партнерами из различных организаций и не вызывать путаницу, следует представлять ясную и согласованную документацию об этих различиях. Из-за большого объема изменений в документации и необходимого обучения процесс перехода от принятой в компании терминологии к более стандартной в отрасли терминологии, вероятно, будет развиваться поэтапно.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60050-192	—	*
IEC 61508-4:2010	IDT	ГОСТ Р МЭК 61508-4—2012 «Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 4. Термины и определения»
IEC 61511-1:2016	IDT	ГОСТ Р МЭК 61511-1—2018 «Безопасность функциональная. Приборные системы безопасности, для технологических процессов в промышленности. Часть 1. Термины, определения и технические требования»
ISO/IEC Guide 51:2014	IDT	ГОСТ Р 57149—2016/ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по включению их в стандарты»

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Официальный перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] CCPS/AIChE, Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Wiley-Interscience, New York (2014)

[2] Control of Major Accident Hazards Regulations 2015, Statutory Instrument 2015/483, Her Majesty's Stationery Office, London (2015)

[3] Dangerous Substances and Explosive Atmospheres Regulations 2002, Statutory Instrument 2002/2776, Her Majesty's Stationery Office, London (2002)

[4] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance

[5] IEC 60050 (all parts), International Electrotechnical Vocabulary (available at <gost.e-ecolog.ru)

[6] IEC 61131-3:2003[1)], Programmable controllers — Part 3: Programming languages

[7] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

[8] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

[9] IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/program-mable electronic safety-related systems

[10] IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements

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

[12] IEC 61508-6:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

[13] IEC 61508-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

[14] IEC 61511-1:2003[1)], Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements

[15] IEC 61511-2:2016, Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1:2016

[16] IEC 61511-3:2016, Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels

[17] IEC 61703:2016, Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[18] IEC 62443 (all parts), Security for industrial automation and control systems

[19] ISO 9001:2015, Quality management systems — Requirements

[20] ISO 14224:2016, Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment

[21] U.S. OSHA. 1992-2014. Occupational Safety and Health Standards: Process safety management of highly hazardous chemicals, 29 CFR 1910.119. Washington D.C.: OSHA

[1)] Отменен.

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

Ключевые слова: безопасность функциональная, жизненный цикл систем, электронные компоненты, системы, связанные с безопасностью, планирование функциональной безопасности, программное обеспечение, уровень полноты безопасности

Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 20.05.2021. Подписано в печать 28.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л.4,65. Уч.-изд. л. 4,21.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru