ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 366.2— 2019

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 2

Системы менеджмента

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН ООО «НИИ экономики связи и информатики «Интерэкомс» (ООО «НИИ «Интерэкомс») совместно с ООО «Корпоративные электронные системы» (ООО «КЭЛС-центр»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 100 «Стратегический и инновационный менеджмент» и ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2019 г. № 38-пнст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 дня до истечения срока его действия разработчику настоящего стандарта по адресу: gost.e-ecolog.ru *и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 109074 Москва, Китайгородский проезд, д. 7, стр. 1.*

*В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2019

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 Менеджмент функциональной безопасности 1
2.1 Общие положения 1
2.2 Организация и ресурсы 2
2.3 Планирование мероприятий по обеспечению безопасности 2
2.4 Практическая реализация и мониторинг 4
2.5 Оценка, аудиторские проверки, модификация 4
3 Верификация 10
4 Валидация 10

Введение

Комплекс предварительных национальных стандартов по тематике «обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами» состоит из следующих частей:

- Часть 1. Основные положения, принципы и понятия;
- Часть 2. Системы менеджмента (настоящий стандарт);
- Часть 3. Подготовка, запуск и эксплуатация устройств безопасности;
- Часть 4. Верификация полноты аппаратных средств автоматизированной системы безопасности;
- Часть 5. Руководство по практическому применению;
- Часть 6. Приложения для обеспечения безопасности промышленных предприятий с повышенным уровнем опасности.

Настоящий стандарт не предназначен для целей сертификации и носит исключительно рекомендательный характер. Использование настоящего стандарта предполагает, что при организации производства, при практической реализации (наладке и вводе в эксплуатацию) и функционировании производственного оборудования в обязательном порядке соблюдаются все законодательные нормы, необходимые и достаточные меры технической безопасности, меры по предотвращению опасных инцидентов, а также прочие требования, установленные в национальных стандартах и других нормативных и технических документах.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 2

Системы менеджмента

Industrial automation systems and integration. Safety and security arrangements of industrial process plants by means of process control engineering. Part 2. Management systems

Срок действия — с 2020—01—01
до 2022—01—01

1 Область применения

В настоящем стандарте определены положения, касающиеся обеспечения безопасности производственных установок при помощи устройств автоматического управления производственными процессами (PCE), а также организационные меры и порядок действий, гарантирующие, что рассматриваемые производственные установки не накладывают дополнительные риски на людей и экологию на протяжении всего их жизненного цикла.

Примечание — Вопросы практической реализации устройств автоматического управления производственными процессами соответствуют общей концепции безопасности, установленной в ПНСТ-1—2019 «Системы промышленной автоматизации и интеграция. Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами. Часть 1. Основные положения, принципы и понятия».

2 Менеджмент функциональной безопасности

2.1 Общие положения

Любая организация, вне зависимости от ее типа и размера, должна обеспечивать функциональную безопасность и работать в соответствии со стандартами, устанавливающими требования к функциональной безопасности. Ссылки на соответствующие стандарты должны содержаться во внутренних документах предприятия (в т. ч. в корпоративных стандартах) и определять методы проведения работ и процедуры обеспечения безопасности.

Настоящий стандарт способствует достижению корпоративной цели обеспечения безопасности предприятия. Он позволяет оценить действенность мероприятий по обеспечению безопасности.

Системы менеджмента безопасности должны гарантировать, что при необходимости рассматриваемая технологическая установка переводится в безопасное состояние или удерживается в нем.

Также допускается вариант, при котором в существующие интегрированные системы менеджмента предприятия инкорпорируются системы менеджмента безопасности.

Издание официальное

2.2 Организация и ресурсы

Конкретные физические лица, подразделения предприятия, организации или другие производственные единицы, чьи функции включают обеспечение требуемых производственных показателей и мониторинга производства, в целях обеспечения безопасности рассматриваемого жизненного цикла должны быть названы поименно и проинформированы о налагаемой на них ответственности. То же самое относится и к органам, обеспечивающим контрольные и надзорные функции.

Данное требование обеспечивается путем введения соответствующих определений в корпоративные стандарты (стандарты организаций) и в структуру организации (описание должностных обязанностей менеджеров и инженеров-технологов предприятия, назначение ответственных и т. п.).

Физические лица, подразделения предприятия и организации, принимающие конкретные меры по обеспечению безопасности производства в течение всего жизненного цикла, должны иметь необходимые компетенции для выполнения действий, за результаты которых они несут ответственность.

Соответствующие компетенции приобретаются:

1) путем обучения на внутренних и внешних семинарах по безопасности предприятия;

2) путем накопления профессионального производственного опыта.

При оценке указанных компетенций необходимо учитывать:

- технические знания, повышение квалификации и производственный опыт, непосредственно относящиеся к областям применения производственного процесса;
- технические знания, повышение квалификации и производственный опыт, непосредственно относящиеся к используемой технологии (например, к электротехнике, электронике, к технологиям, связанным с программируемыми электронными устройствами, и т. п.);
- технические знания, повышение квалификации и производственный опыт, непосредственно относящиеся к измерительным устройствам и приводным механизмам;
- знания, связанные с обеспечением безопасности (например, с оценкой безопасности);
- знание законодательных и нормативных требований;
- наличие навыков управления и лидерских качеств для выполнения особых заданий при обеспечении безопасности жизненного цикла производства;
- понимание возможных последствий нежелательных событий;
- уровень полноты безопасности, обеспечиваемый приборной функцией безопасности;
- новизну и сложность рассматриваемого приложения (технологии).

2.3 Планирование мероприятий по обеспечению безопасности

Мероприятия по обеспечению безопасности планируются с участием физических лиц, подразделений предприятий, организаций и других структурных подразделений, несущих ответственность за практическую реализацию мероприятий по обеспечению безопасности, а также с учетом действующих национальных, межгосударственных и корпоративных стандартов. Пример сопоставления положений документов, устанавливающих требования к системам менеджмента безопасности (СМБ), удовлетворяющим требованиям мер по предотвращению опасных инцидентов, и системам менеджмента качества приведен в таблице 1.

Планирование мероприятий по обеспечению безопасности должно включать в себя определение жизненного цикла системы безопасности в форме «плана мероприятий по обеспечению безопасности» (см. рисунок 1 и таблицу 2).

Планирование мероприятий по обеспечению безопасности осуществляется на уровне всего предприятия в целом. План мероприятий должен включать ответственных за оценку безопасности, перечень текущих мероприятий, порядок технического обслуживания, модификацию оборудования и т. п. Планирование осуществляется в соответствии с имеющимися внутренними и внешними корпоративными стандартами предприятия.

К целям жизненного цикла системы безопасности относятся:

- определение рабочих фаз и установление ассоциированных требований;
- организация технических действий в рамках рассматриваемого жизненного цикла;
- предоставление гарантий, что разработанный план функционирования имеющейся приборной системы безопасности (SIS-системы) удовлетворяет установленным требованиям безопасности.

Каждая стадия жизненного цикла системы безопасности описывается с указанием необходимых обязательных условий производства, ожидаемых результатов работы, процедуры верификации выполненных действий (см. таблица 2).

Таблица 1 — Сравнение системы менеджмента безопасности (СМБ), удовлетворяющей требованиям установленных мер по предотвращению опасных инцидентов, и системы менеджмента качества

Общие требования к СМБ, установленные в директивных документах	Требования к сотрудникам, установленные в директивных документах	Соответствующие разделы ГОСТ ISO 9001*	Возможные корпоративные процессы
1 Концепция предотвращения опасных инцидентов: - общие цели; - общие принципы процедуры ограничения уровня опасности опасных инцидентов; - письменная копия	Общие обязанности оператора. Требования по предотвращению опасных инцидентов. Требования по ограничению последствий опасных инцидентов. Дополнительные требования. Уведомления	4.1 Общие требования 5.1 Обязательства руководства 5.3 Политика в области качества 5.4.1 Цели в области качества 5.4.2 Планирование создания, поддержания и улучшения системы менеджмента качества 5.5.1 Ответственность и полномочия 8.5.2 Корректирующие действия	Корпоративная политика: - основные принципы; - цели
	Политика по предотвращению опасных инцидентов с учетом основных принципов	8.5.3 Предупреждающие действия	
2 Системы менеджмента безопасности, общие требования	Практическая реализация концепции предотвращения опасных инцидентов	4.1 Общие требования 4.2 Требования к документации	Система менеджмента, общее описание

Планирование мероприятий по обеспечению безопасности, связанное с определением рабочих критериев, методов работы, принимаемых мер и рабочих процедур на каждой фазе цикла обеспечения безопасности требует:

- подтверждения того, что установленные требования безопасности SIS-системы выполняются для каждого конкретного режима функционирования производственного процесса. Это касается как функциональных требований, так и требований полноты безопасности. На основании информации, предоставленной собственником или изготовителем используемого оборудования, обязательно подтверждается пригодность конечного оборудования в части соответствия установленным эксплуатационным требованиям;
- гарантированной установки и ввода в эксплуатацию приборной системы безопасности;
- гарантированной полноты обеспечения безопасности самих приборных функций безопасности после их установки;
- поддержания полноты безопасности на производстве (повторные проверки, проверочный контроль, оперативный анализ неисправности и т. п.);
- контроля возможных угроз, возникающих на производстве в ходе технического обслуживания приборных систем безопасности.

Используемая методика планирования должна обновляться по мере необходимости в течение всего жизненного цикла рассматриваемой системы безопасности.

Разработанный план мероприятий по обеспечению безопасности можно рассматривать как:

- составную часть Руководства по обеспечению качества продукции с заголовком «План мероприятий по обеспечению безопасности»;
- независимый документ с заголовком «План мероприятий по обеспечению безопасности»;
- совокупность документов, включающих корпоративные нормативные документы и рабочие инструкции предприятия.

* ГОСТ ISO 9001 «Системы менеджмента качества. Требования».

2.4 Практическая реализация и мониторинг

Рассматриваемые процедуры должны гарантировать разработку и практическую реализацию положений (рекомендаций) с учетом:

- результатов анализа рисков и угроз;
- результатов оценки предпринимаемых действий и результатов аудиторских проверок;
- верификации предпринимаемых действий;
- валидации действий;
- действий, предпринимаемых после инцидентов и происшествий.

Каждый производитель, предоставляющий продукты и услуги в организацию и несущий общую ответственность за обеспечение безопасности одной или нескольких фаз жизненного цикла, должен иметь рабочую систему менеджмента качества. Свои продукты и услуги производитель предоставляет в соответствии с требованиями указанной организации. Производственные процедуры должны гарантировать пригодность используемой системы менеджмента качества.

Примечание — Данное требование не означает, что организация, принимающая продукцию, оценивает их качество в соответствии с ГОСТ ISO 9001. Данным стандартом должен руководствоваться производитель при построении системы менеджмента качества своей продукции.

Необходимо задействовать специальные процедуры (например, сбор данных об отказах, анализ собранных данных и т. п.) оценки производственных показателей приборных систем безопасности с учетом требований безопасности. Данные процедуры требуют:

1) выявления и предотвращения систематических отказов, оказывающих влияние на безопасность системы;

2) выяснения, соответствует ли фактическое значение вероятности опасных отказов приборной системы безопасности исходному проектному допущению;

3) определения частоты, с которой приборные функции безопасности задействуются в ходе реального функционирования, чтобы верифицировать допущения, сделанные в ходе оценки риска при определении требований уровня полноты безопасности (SIL- уровня).

При оценке работы установки в режиме запроса предполагается, что число запросов функций безопасности за год равно максимальному значению. Третье вышеуказанное требование удовлетворяется, если принимаются контрмеры и если число запросов превышает максимальное значение (в целях обеспечения эксплуатационной готовности).

2.5 Оценка, аудиторские проверки, модификация

2.5.1 Оценка функциональной безопасности

Частота выполнения текущих оценок системы безопасности в ходе ее жизненного цикла определяется как элемент планирования мероприятий по обеспечению безопасности. Данная оценка выполняется особой группой специалистов, обладающих необходимыми техническими знаниями и производственным опытом.

Оценка функциональной безопасности должна выполняться на нижеследующих стадиях работ (см. рисунок 1):

стадия 1: после наступления нежелательного события, после анализа риска, после определения уровня защиты и разработки проекта спецификации безопасности;

стадия 2: после разработки приборной системы безопасности.Это дополнительный раздел экспертизы безопасности (для более сложных установок). В большинстве реальных ситуаций стадия 2 объединяется со стадией 3;

стадия 3: после установки, ввода в эксплуатацию, заключительных проверок приборной системы безопасности, завершения подготовки Руководства по эксплуатации, техническому обслуживанию и ремонту данной системы. Проверка также проводится перед вводом в эксплуатацию;

стадия 4: после накопления достаточного производственного опыта эксплуатации, технического обслуживания и ремонта системы, по заданию высшего руководства предприятия, в ходе выполнения производственных обязанностей инженера (в комбинации с методом анализа «слабых мест» и т. п.);

стадия 5: после модификации приборной системы безопасности, перед выводом ее из эксплуатации, в ходе т. н. «мини-экспертизы безопасности».

В случае появления новых угроз (в результате модификации оборудования) на предприятии следует проводить дополнительную оценку функциональной безопасности.

Количество, область применения и границы мероприятий по оценке функциональной безопасности следует скорректировать в соответствии с фактической ситуацией. Определяющими факторами являются:

- масштаб проекта;
- уровень сложности;
- уровень полноты безопасности;
- последствия возникновения неисправности;
- уровень стандартизации проектных характеристик;
- требования законодательства;
- имеющийся производственный опыт работы с аналогичной системой.

Группа, дающая оценку системе безопасности, должна иметь, по крайней мере, одного опытного компетентного человека, не задействованного в разработке проекта.

На крупных предприятиях данное требование выполняется центральной службой охраны труда и техники безопасности. Сотрудники подразделения-заказчика (производственного отдела) обычно на эту роль не подходят, так как являются заинтересованной стороной.

Если группа, проводящая оценку системы безопасности, большая, то для выполнения работы может потребоваться уже не один, а несколько опытных компетентных людей, не задействованных в разработке проекта.

При планировании мероприятий по оценке функциональной безопасности необходимо принять во внимание:

- область применения оценки функциональной безопасности;
- состав группы исполнителей;
- умения членов группы оценки и их ответственность;
- документацию, выпускаемую по результатам оценки функциональной безопасности;
- другие группы экспертов безопасности, принимающие участие в работе;
- ресурсы, необходимые для выполнения оценки в полном объеме;
- степень независимости группы в принятии решений;
- возможность повторной валидации оборудования, модифицированного по результатам оценки.

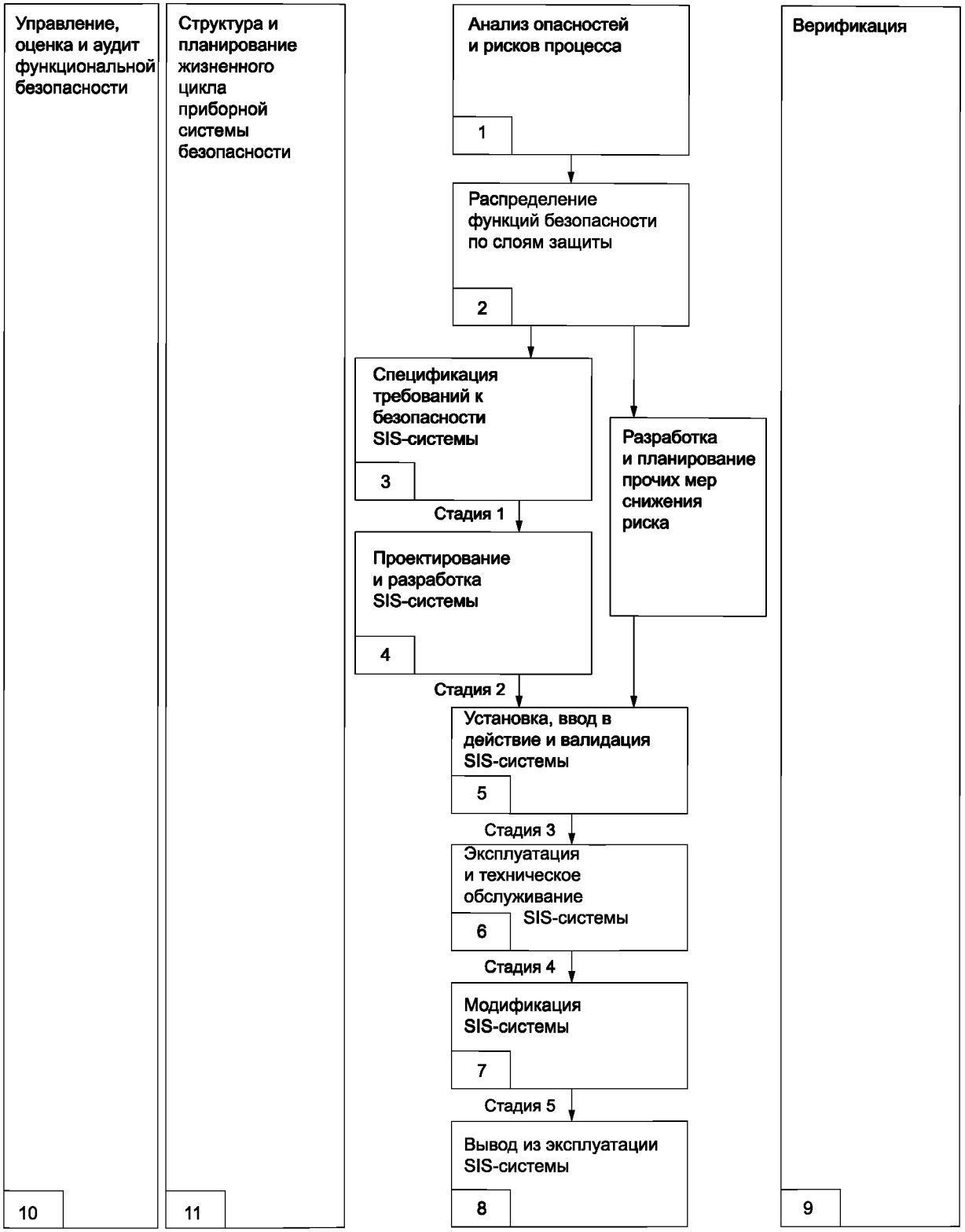

Рисунок 1 — Стадии жизненного цикла SIS-системы и стадии оценки функциональной безопасности

Таблица 2 — Общее описание жизненного цикла SIS-системы

Стадия жизненного цикла SIS-системы		Цели	Раздел ГОСТ Р МЭК 61511-1*	Руководящие положения и направления	Результаты
Блок на рисунке 1	Заголовок				
1	Анализ опасностей и рисков процесса	Определение: - угроз и опасных инцидентов, возникающих в производственном процессе или на ассоциированном оборудовании; - последствий событий, ведущих к опасным инцидентам и рискам производственного процесса, ассоциированным с данными событиями; - требуемого снижения риска; - приборных функций безопасности, необходимых для требуемого снижения риска	8	Технологическое проектирование, планировка оборудования, метрики персонала, цели обеспечения безопасности	Описание угроз, задействованных функций безопасности и соответствующее снижение риска
2	Распределение функций безопасности по слоям защиты	Назначение функций безопасности соответствующим слоям защиты; определение каждой функции безопасности SIS-системы соответствующего уровня полноты безопасности (SIL-уровня)	9	Описание задействованных приборных функций безопасности, включая требования полноты безопасности	Описание процедуры назначения требований безопасности
3	Спецификация требований к безопасности SIS-системы	Определение требований к каждой SIS-системе (в форме необходимой приборной функции безопасности и ассоциированного уровня полноты безопасности) для достижения требуемого уровня функциональной безопасности	10	Описание процедуры назначения требований безопасности	Требования к приборной системе безопасности, к безопасности программного и аппаратного обеспечения
4	Проектирование и разработка SIS-системы	Планирование работы SIS-системы, с учетом требований к приборной функции безопасности и к полноте безопасности	11 и 12.4	Требования безопасности SIS-системы и безопасности программного обеспечения	Проектирование SIS-системы в соответствии с требованиями безопасности; планирование комплексных испытаний SIS-системы
5	Установка, ввод в действие и валидация SIS-системы	Интеграция и тестирование SIS-системы, комплексная проверка SIS-системы, отдельных приборных функций безопасности и соответствующей полноты безопасности установленным требованиям безопасности	12.3, 14, 15	Проектирование SIS-системы; планирование комплексных испытаний SIS-системы;	Полностью функционирующая SIS-система в соответствии с планом;

* ГОСТ Р МЭК 61511-1 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования».

Окончание таблицы 2

Стадия жизненного цикла SIS-системы		Цели	Раздел ГОСТ Р МЭК 61511-1	Руководящие положения и направления	Результаты
Блок на рисунке 1	Заголовок				
				требования безопасности SIS-системы; планирование мероприятий по валидации SIS-системы	результаты комплексных испытаний SIS-системы; результаты установки, ввода в действие и мероприятий по валидации
6	Эксплуатация и техническое обслуживание SIS-системы	Обеспечение функциональной безопасности SIS-системы в ходе функционирования системы и ее технического обслуживания	16	Требования к SIS-системе; конструкция SIS-системы; планирование работы и технического обслуживания SIS-системы	Результаты мероприятий, проведенных в рамках функционирования и технического обслуживания SIS-системы
7	Модификация SIS-системы	Внесение исправлений, улучшений и доработок SIS-системы для обеспечения требуемого уровня полноты безопасности	17	Пересмотренные требования безопасности SIS-системы	Результаты модификации SIS-системы
8	Вывод из эксплуатации SIS-системы	Гарантирование (путем надлежащего тестирования и структурирования оборудования), что незадействованные функции безопасности остаются работоспособными	18	Требования безопасности и документация установки (в заводском исполнении)	Неработающие приборные функции безопасности
9	Верификация SIS-системы	Тестирование и оценка результатов фазы работ (в части корректности и совместимости) в соответствии со спецификациями и стандартами, применимыми к данной фазе работ	7, 12.7	Спецификации планирования мероприятий по верификации конкретных фаз работы SIS-системы	Результаты верификации SIS-системы по каждой фазе работ
10	Подтверждение функциональной безопасности SIS-системы	Исследование и оценка функциональной безопасности SIS-системы	5	План оценки функциональной безопасности SIS-системы; требования безопасности SIS-системы	Результаты оценки функциональной безопасности SIS-системы

Группа оценки безопасности должна подтвердить (как самое позднее перед вводом приборной системы безопасности в эксплуатацию), что:

- анализ угроз и рисков выполнен;
- рекомендации, основанные на результатах анализа угроз и рисков приборной системы безопасности, реализованы на практике (приняты к рассмотрению);
- процедуры планирования модификации задействованы (приняты к рассмотрению);
- рекомендации, следующие из предварительной оценки функциональной безопасности, приняты к рассмотрению;
- конструкция, практическая реализация и установка приборной системы безопасности соответствуют спецификации безопасности; имеющиеся несоответствия идентифицированы и задокументированы;
- руководство по безопасности, руководство пользователя, руководство по техническому обслуживанию и план действий в аварийной ситуации, относящиеся к рассматриваемой приборной системе безопасности, задействованы;
- правила валидации приборной системы безопасности задействованы, валидация успешно выполнена;
- обучение персонала завершено, персонал технического обслуживания и рабочий персонал ознакомлены с самой приборной системой безопасности и с ее документацией;
- планы (процедуры) дополнительной оценки функциональной безопасности задействованы.

Если в ходе жизненного цикла системы безопасности используются какие-либо дополнительные разработки (технологическая оснастка), то их функциональную безопасность также необходимо оценить.

Примечания:

1 Примеры дополнительных разработок и технологической оснастки: инструменты моделирования (модели), измерительные приборы, испытательное оборудование, оборудование технического обслуживания, инструменты конфигурирования.

2 Оценка функциональной безопасности инструмента может включать результаты отслеживания выполнения требований стандарта калибровки, историю применения инструмента, журнал регистрации отказов.

3 Глубина оценки безопасности инструмента определяется его важностью для обеспечения безопасности установки в целом.

Все документы по функциональной безопасности должны быть доступны для членов группы оценки по первому требованию.

Результаты последней оценки функциональной безопасности, а также все рекомендации, основанные на данной оценке, должны быть доступны для всех заинтересованных лиц.

2.5.2 Аудиторские проверки

Аудит предполагает проведение систематических и независимых проверок. Они устанавливают степень соответствия рабочих процедур (требований функциональной безопасности) запланированным мероприятиям. В ходе аудиторской проверки производится оценка эффективности установленных процедур, целесообразности их использования для достижения поставленных целей.

Внеплановые внутренние аудиторские проверки проводятся инженерами различных вспомогательных структурных подразделений предприятия. Основной инструмент проверки — стандартизованный опросник.

Основные аспекты рабочих процедур аудиторских проверок:

- частота аудиторских проверок;
- степень независимости аудиторов от конкретных физических лиц, подразделений предприятия, организаций и прочих структурных подразделений;
- регистрация и обработка результатов аудиторской проверки.

2.5.3 Модификация

Процедура модификации производства должна быть официально утверждена. Использование запчастей к модификации не относится. При модификации устанавливается особый порядок инициирования модификации, оформления документации, выполнения экспертиз, практической реализации и приемки модификации приборной системы безопасности.

Отслеживание производственных показателей модификации рассматриваемой установки включается в жизненный цикл системы безопасности.

3 Верификация

В контексте настоящего стандарта, верификация (управление процедурой верификации) означает, что для каждой стадии жизненного цикла, связанной с обеспечением безопасности, путем специального анализа (тестирования) должно быть показано, что отклики системы на заданные воздействия по всем аспектам соответствуют поставленным целям и требованиям, определенным для данной фазы.

Все мероприятия конкретной стадии (см. рисунок 1) жизненного цикла приборной системы безопасности должны предусматриваться планом верификации. План верификации включает:

- перечень мероприятий верификации;
- процедуры, меры и методики, задействованные в ходе верификации, устранение недостатков, выявленных в ходе верификации;
- сроки верификации;
- физические лица, подразделения предприятия и организации, ответственные за выполнение работ, степень их самостоятельности в принятии решений;
- скорректированный список установок;
- перечень документов, в соответствии с которыми производится верификация;
- порядок устранения несоответствий;
- инструменты, оборудование, обеспечивающие испытания и проверки.

Верификация выполняется в соответствии с требованиями плана верификации.

Результаты верификации должны быть задокументированы.

Выбор процедур и мер процесса верификации, а также степень самостоятельности в принятии решений зависят от ряда факторов, включающих уровень сложности, новизну конструкции (технологии), требуемый уровень полноты безопасности и т. п.

Верификация может включать экспертизу проекта, проверку действенности используемых методов организации работ, проверку эффективности технологий, верификацию программного обеспечения и средств компьютерной поддержки производства.

4 Валидация

Валидация предполагает подтверждение (путем тестирования, оценки значимых свойств и т. п.) того, что использование рассматриваемых средств производства соответствует требованиям их целевого назначения. Валидация также предполагает, что проверенная система безопасности полностью удовлетворяет установленным требованиям безопасности. Валидация программного обеспечения, например, подтверждает, что данное программное обеспечение удовлетворяет требованиям спецификации, связанным с обеспечением безопасности производства.

Все мероприятия валидации определяются планом валидации.

План валидации включает:

- перечень мероприятий валидации, в том числе валидацию приборной системы безопасности с учетом требований спецификаций безопасности, а также инкорпорацию и практическую реализацию рекомендаций, сформулированных в ходе жизненного цикла системы безопасности;
- валидацию всех рабочих режимов производственного процесса и ассоциированных установок, включающих:
  - подготовку к работе, задание установок и настроек;
  - запуск оборудования, автоматическое, полуавтоматическое и ручное управление, стационарный режим работы;
  - перезагрузку, отключение и техническое обслуживание;
  - реакцию на прогнозируемые сбои, например сбои, идентифицированные в результате анализа риска;
- руководящие материалы, меры и процедуры валидации;
- сроки проведения разработанных мероприятий;
- сотрудников, подразделения предприятия и организации, несущие ответственность за проведение указанных мероприятий, степень их независимости в принятии решений по процедуре валидации.

Примером валидации является ответ на вопрос: «Используются ли заказанные производственные компоненты и модули по целевому назначению?».

План дополнительной валидации составляется с учетом нижеследующих пунктов. Он касается также компьютерных программ обеспечения безопасности приложений:

- проверка достоверности сертификатов на все инструменты и средства;
- проверка пригодности компьютерных программ.

Если проверка точности измерений — это необходимое мероприятие валидации производственного процесса, то все используемые измерительные приборы должны быть откалиброваны в соответствии с их спецификациями. Точность измерений должна соответствовать требованиям приложения и рекомендациям соответствующих стандартов. Если требуемая калибровка невозможна, то задействуется альтернативный метод. Использование альтернативного метода обосновывается и документируется в установленном порядке.

Валидация приборной системы безопасности и ассоциированных приборных функций безопасности производится в соответствии с планом валидации SIS-системы. Валидация должна отвечать на следующие вопросы:

- Если приборная система безопасности реагирует определенным образом на задаваемые воздействия в ходе штатных и специальных режимов работы (например, пуск системы, отключение системы и т. п.), то соответствуют ли данные реакции требованиям спецификации безопасности?
- Имеется ли паразитное влияние основных систем управления процессами (BPCS-систем) и других смежных систем на рассматриваемую приборную систему безопасности?
- Соответствует ли работа датчиков, логических устройств и приводных механизмов (дублирующих каналов в том числе) требованиям спецификации безопасности?
- Соответствует ли рабочее состояние приборной системы безопасности требованиям сопроводительной документации?
- Подтверждается ли, что автоматическая функция безопасности срабатывает необходимым образом в случае нештатных измерений (например, при выходе за пределы установленного измерительного диапазона и т. п.)?
- Правильно ли срабатывает система в режиме отключения?
- Правильно ли срабатывает приборная система безопасности в режиме выдачи аварийного сигнала, в режиме визуализации рабочих режимов?
- Правильно ли выполнены проектные расчеты приборной системы безопасности?
- Соответствует ли работа приборной системы безопасности в режиме перезагрузки требованиям спецификации безопасности?
- Уменьшается ли безопасность системы в режиме запуска (в режиме перехода на параллельный канал)?
- Содержит ли инструкция по проверкам календарный план проверок?
- Удовлетворяют ли сообщения функций диагностики оборудования установленным требованиям?
- Можно ли утверждать, что приборная система безопасности правильно реагирует на прекращение поступления рабочих ресурсов (например, электроэнергии, воздуха, гидравлической жидкости и т. п.)? Возвращается ли рассматриваемая приборная система безопасности в требуемое состояние при возобновлении поступления рабочих ресурсов?

Результаты валидации утверждаются и документируются в установленном порядке. Результаты валидации конкретизируют:

- версию плана валидации SIS-системы;
- проверенную (испытанную) приборную функцию безопасности со ссылкой на требование плана валидации SIS-системы;
- используемые инструменты и оборудование, данные калибровки;
- результаты каждого испытания;
- версию используемой инструкции по валидационным испытаниям;
- версию протестированного аппаратного (программного) обеспечения;
- все зарегистрированные несоответствия установленным требованиям;
- при наличии несоответствий, конкретизируется решение о продолжении испытаний (о направлении запроса на внесение изменений, о возврате на предшествующую фазу жизненного цикла системы безопасности и т. п.).

Если ожидаемые результаты и полученные результаты испытаний не совпадают, то результатами валидации являются:

1) полученные результаты испытаний;

2) решение продолжить валидацию (направить запрос на внесение изменений, вернуться на предшествующую фазу жизненного цикла системы безопасности и т. п.).

УДК 658.52.011.56:006.354 ОКС 25.040.40

Ключевые слова: системы автоматического управления производственными процессами; производственные процессы; приборные системы безопасности; планирование функциональной безопасности; уровень полноты безопасности; системы менеджмента безопасности

БЗ 10—2019/141

Редактор *П.К. Одинцов*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 24.09.2019. Подписано в печать 10.10.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,70.
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