ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62682— 2019

СИСТЕМЫ АВАРИЙНОЙ СИГНАЛИЗАЦИИ ДЛЯ ОБРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

(IEC 62682:2014, IDT)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» совместно с ФГУП «СТАНДАРТИНФОРМ» на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 9 августа 2019 г. № 491-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62682:2014 «Системы аварийной сигнализации для обрабатывающей промышленности» (IEC 62682:2014 «Management of alarms systems for the process industries», IDT)

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.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
1.1 Основные области применения 1
1.2 Область применения и исключения из нее 2
2 Нормативные ссылки 3
3 Термины, определения и сокращения 3
3.1 Термины и определения 3
3.2 Сокращения 8
4 Соответствие настоящему стандарту 9
4.1 Правило обеспечения соответствия 9
4.2 Существующие системы 9
4.3 Ответственность 9
5 Модели систем аварийной сигнализации 9
5.1 Системы аварийной сигнализации 9
5.2 Менеджмент жизненного цикла аварийной сигнализации 9
5.3 Состояния аварийной сигнализации 15
5.4 Временная диаграмма аварийной сигнализации 18
5.5 Модель взаимодействия «оператор — производственный процесс» с обратной связью 19
6 Концепция аварийной сигнализации 20
6.1 Цель 20
6.2 Содержание концепции аварийной сигнализации 20
6.3 Разработка и поддержка концепции аварийной сигнализации 25
7 Спецификация требований к системам аварийной сигнализации 26
7.1 Цель 26
7.2 Рекомендации 26
7.3 Разработка 26
7.4 Оценка систем 27
7.5 Настройка 27
7.6 Требования к испытанию системы аварийной сигнализации 27
8 Идентификация 27
8.1 Цель 27
8.2 Методы идентификации аварийных сигнализаций 27
8.3 Обучение идентификации 28
9 Рационализация 28
9.1 Цель 28
9.2 Документация на этапе рационализации 28
9.3 Обоснование аварийной сигнализации 29
9.4 Определение уставки срабатывания сигнализации 29
9.5 Установление приоритетов 29
9.6 Удаление 30
9.7 Классификация 30
9.8 Анализ 30
9.9 Использование документации 30

10 Детальное проектирование. Технический проект системы аварийной сигнализации 31
10.1 Цель 31
10.2 Использование состояний аварийной сигнализации 31
10.3 Типы аварийных сигнализаций 31
10.4 Атрибуты аварийной сигнализации 32
10.5 Программные изменения атрибутов аварийной сигнализации 33
10.6 Анализ технического проекта системы аварийной сигнализации 33
11 Детальное проектирование. Проектирование человеко-машинного интерфейса для систем аварийной сигнализации 34
11.1 Цель 34
11.2 Функции человеко-машинного интерфейса 34
11.3 Индикации состояний аварийной сигнализации 35
11.4 Индикация приоритетов аварийной сигнализации 36
11.5 Индикация сообщений аварийной сигнализации 37
11.6 Отображение аварийных сигнализаций 37
11.7 Задержка аварийной сигнализации 40
11.8 Выведенные из обслуживания аварийные сигнализации 41
11.9 Запрещенные проектом аварийные сигнализации 41
11.10 Интеграция аварийных оповещательных устройств 42
11.11 Человеко-машинный интерфейс аварийной сигнализации безопасности 42
12 Детальное проектирование. Методы повышения эффективности и усовершенствования аварийной сигнализации 43
12.1 Цель 43
12.2 Основы повышения эффективности и усовершенствования аварийной сигнализации 43
12.3 Информационные связи 43
12.4 Аварийная сигнализация, основанная на логике 44
12.5 Аварийная сигнализация, управляемая моделями 44
12.6 Дополнительные аспекты аварийной сигнализации 44
12.7 Обучение, выполнение испытаний и аудирование систем 45
12.8 Соблюдение установленных атрибутов аварийной сигнализации 46
13 Внедрение 46
13.1 Цель 46
13.2 Планирование внедрения 46
13.3 Подготовка к внедрению 46
13.4 Испытание и подтверждение соответствия при внедрении 47
13.5 Документация по внедрению 48
14 Эксплуатация 48
14.1 Цель 48
14.2 Процедуры ответа аварийной сигнализации 48
14.3 Задержка аварийной сигнализации 49
14.4 Переподготовка операторов 49
15 Техническое обслуживание 50
15.1 Цель 50
15.2 Периодические испытания аварийной сигнализации 50
15.3 Вывод аварийных сигнализаций из обслуживания 51

15.4 Ремонт оборудования . . . 51
15.5 Замена оборудования . . . 51
15.6 Переподготовка персонала для технического обслуживания . . . 52
16 Контроль и оценка . . . 52
16.1 Цель . . . 52
16.2 Требования . . . 52
16.3 Контроль, оценка, аудит и оценка параметров . . . 52
16.4 Контроль системы аварийной сигнализации . . . 53
16.5 Метрики производительности системы аварийной сигнализации . . . 53
16.6 Запрещение несанкционированных аварийных сигналов . . . 56
16.7 Контроль атрибутов аварийных сигнализаций . . . 56
16.8 Предоставление аналитических отчетов по системе аварийной сигнализации . . . 56
16.9 Общая сводка метрик производительности системы аварийной сигнализации . . . 56
17 Управление изменениями . . . 58
17.1 Цель . . . 58
17.2 Процедура управления изменениями . . . 58
17.3 Требования к изменению документации . . . 58
17.4 Рекомендации к изменению документации . . . 58
17.5 Рекомендации по удалению аварийных сигнализаций . . . 59
18 Аудит . . . 59
18.1 Цель . . . 59
18.2 Оценка параметров . . . 59
18.3 Опросы для аудита . . . 59
18.4 Рекомендации по аудиту . . . 60
18.5 Планы действий . . . 60
Библиография . . . 61

Введение

Цель

В настоящем стандарте рассматриваются вопросы разработки, проектирования, установки и менеджмента системам аварийной сигнализации в обрабатывающей промышленности. Менеджмент аварийной сигнализацией включает в себя множество рабочих процессов на протяжении всего жизненного цикла системы аварийной сигнализации. В настоящем стандарте определены термины и модели, необходимые для разработки системы аварийной сигнализации, а также определены рабочие процессы, рекомендуемые для эффективной поддержки систем аварийной сигнализации на всем их жизненном цикле.

Настоящий стандарт основан на стандарте Международной ассоциации автоматизации (ISA) ANSI/ISA-18.2-2009, «Management of Alarm Systems for the Process Industries», а также учитывает требования других руководящих документов, которые были разработаны в разных отраслях промышленности. На неэффективность систем аварийной сигнализации часто ссылаются в отчетах о расследовании последствий серьезных инцидентов процесса в качестве факторов, способствующих таким инцидентам. В настоящем стандарте представлена методология, которая должна обеспечить повышение уровня безопасности в обрабатывающей промышленности.

Настоящий стандарт не является первым документом, в котором представлены термины и методы, предназначенные для создания эффективных систем сигнализации. В 1999 г. Ассоциация потребителей инженерного оборудования и материалов (EEMUA) выпустила документ Publication 191, «Alarm Systems: A Guide to Design, Management and Procurement». В 2003 г. Германская ассоциация стандартизации для технологий измерения и управления в химической промышленности (НАМЮР) выпустила рабочий документ NA 102, «Alarm Management».

Во время разработки настоящего стандарта были предприняты все усилия, чтобы терминология и методы были сохранены и согласованы с предшествующей работой этих уважаемых организаций.

В настоящем стандарте представлены требования к менеджменту аварийной сигнализацией и к системам аварийной сигнализации. Настоящий стандарт предназначен для тех специалистов и организаций, которые:

a) изготавливают или выпускают встроенные системы аварийной сигнализации;

b) изготавливают или выпускают независимое программное обеспечение для систем аварийной сигнализации;

c) проектируют или устанавливают системы аварийной сигнализации;

d) эксплуатируют и/или технически поддерживают системы аварийной сигнализации и

e) выполняют аудит или оценивают производительность системы аварийной сигнализации.

Организация

Настоящий стандарт состоит из двух частей. Первая часть — вводная (разделы 1—5). Далее следует основная часть стандарта (разделы 6—18).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ АВАРИЙНОЙ СИГНАЛИЗАЦИИ ДЛЯ ОБРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

Management of alarms systems for the process industries

Дата введения — 2020—07—01

1 Область применения

1.1 Основные области применения

Настоящий стандарт определяет общие принципы и процессы для менеджмента жизненного цикла систем аварийной сигнализации, реализуемые на электронных программируемых контроллерах и компьютерных технологиях человеко-машинного интерфейса (ЧМИ), для применений в обрабатывающей промышленности. Настоящий стандарт охватывает все аварийные сигналы, с которыми сталкивается оператор, включая аварийные сигналы от основных систем управления процессом, панелей индикации, приборных систем безопасности, систем пожарной и газовой сигнализации и аварийных систем.

Представленные в настоящем стандарте методы применимы к непрерывным, групповым и дискретным процессам обработки. Различия в реализации этих методов зависят от конкретных требований типа процесса.

В юрисдикциях, где руководящие органы (например, национальные, федеральные, областные, городские), в дополнение к требованиям настоящего стандарта, установили требования к проектированию производственной безопасности, менеджменту производственной безопасностью или другие требования, эти требования должны быть учтены.

Основная функция системы аварийной сигнализации — уведомить операторов об отклонениях от нормы технологических параметров или о сбоях оборудования и содействовать ответному действию. Системы аварийной сигнализации могут быть включены как в основную систему управления технологическим процессом (ОСУТП), так и в приборную систему безопасности (ПСБ), каждая из которых выполняет измерения технологических параметров и логические операции для формирования аварийных сигналов. Рисунок 1 иллюстрирует концепцию аварийной сигнализации и связанного с ответным действием потока информации в системе аварийной сигнализации. Система аварийной сигнализации также включает механизм для передачи оператору информации об аварийном сигнале через ЧМИ, как правило, на монитор или панель индикации. Дополнительными функциями системы аварийной сигнализации являются ведение журнала регистрации аварийных сигналов и событий, поддержка сервера архива аварийных событий и генерация метрик производительности для конкретной системы аварийной сигнализации. Существуют внешние системы, которые могут использовать данные из системы аварийной сигнализации.

Издание официальное

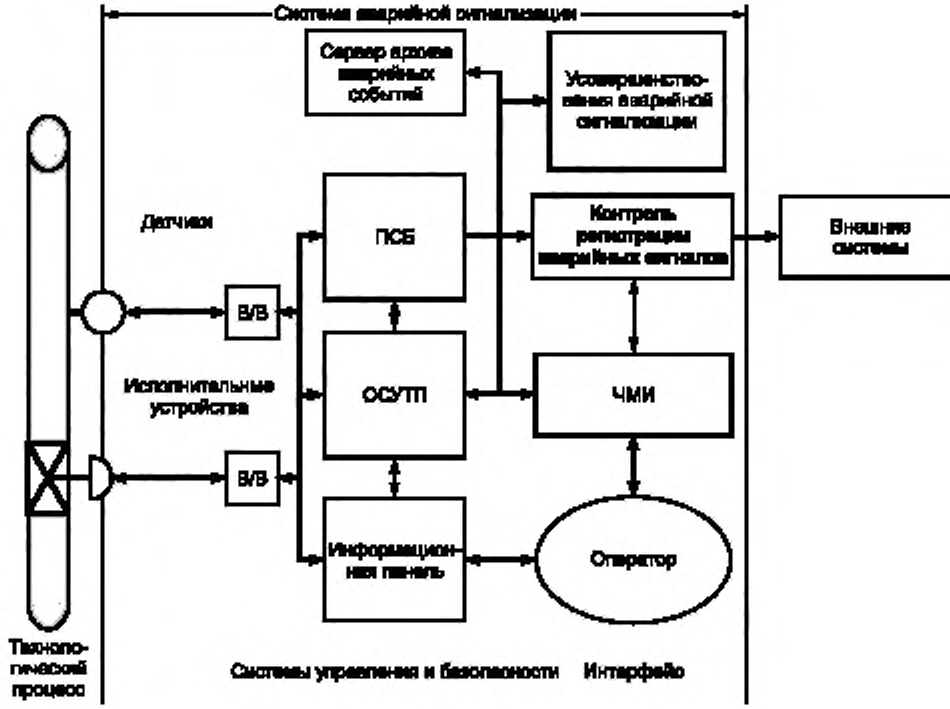

Рисунок 1 — Потоки данных в системе аварийной сигнализации

1.2 Область применения и исключения из нее

1.2.1 Операторы

В область применения настоящего стандарта входят функции оператора, получающего и отвечающего на аварийную сигнализацию. Контроль над действиями операторов не входит в область применения настоящего стандарта.

1.2.2 Датчики и исполнительные элементы технологического процесса

В область применения настоящего стандарта входит аварийная сигнализация от датчиков и исполнительных элементов. Датчики и исполнительные элементы технологического процесса, показанные на рисунке 1, указывают на то, что они могут быть источником аварийной сигнализации. Проектирование и менеджмент датчиками и исполнительными элементами технологического процесса не входит в область применения настоящего стандарта.

1.2.3 Приборные системы безопасности

Аварийная сигнализация от приборных систем безопасности включена в область применения настоящего стандарта. Приборные системы безопасности (ПСБ), показанные на рисунке 1, указывают на то, что они могут быть источником аварийной сигнализации. Проектирование и менеджмент приборных систем безопасности не входят в область применения настоящего стандарта, эти требования определены в МЭК 61511.

Аварийная сигнализация и сигналы диагностики от систем пожарной сигнализации и огнезащиты или от охранных систем, которые представлены оператору системой управления, включены в область применения настоящего стандарта. В область применения настоящего стандарта не входят системы пожарной сигнализации и огнезащиты и охранные системы.

1.2.4 Информация о событиях

Индикация и обработка аналоговой, дискретной информации и информации о событиях, в отличие от индикации аварийной сигнализации, не входят в область применения настоящего стандарта. Методы анализа, обрабатывающие как информацию аварийной сигнализации, так и информацию о событиях не входят в область применения настоящего стандарта.

1.2.5 Методы идентификации аварийной сигнализации

В настоящем стандарте не определены необходимые методы идентификации аварийной сигнализации, а перечислены только примеры методов идентификации аварийной сигнализации.

1.2.6 Управление изменениями

Конкретные процедуры управления изменениями в настоящем стандарте не рассматриваются. Включены некоторые требования и рекомендации для процедуры управления изменениями.

2 Нормативные ссылки

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

Нормативные ссылки отсутствуют.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **абсолютная аварийная сигнализация** (absolute alarm): Аварийная сигнализация, в которой аварийный сигнал формируется в случае превышения уставки срабатывания сигнализации.

3.1.2 **подтверждение** (acknowledge): Действие оператора, которое подтверждает признание аварийной сигнализации.

3.1.3 **активное** (active): Состояние аварийной сигнализации, в котором условие возникновения аварийного сигнала выполнено.

3.1.4 **адаптивная аварийная сигнализация** (adaptive alarm): Аварийная сигнализация, в которой уставка изменяется в соответствии с алгоритмом (например, в зависимости от значения интенсивности параметра).

3.1.5 **регулируемая аварийная сигнализация, устанавливаемая оператором аварийная сигнализация** (adjustable alarm, operator-set alarm): Аварийная сигнализация, в которой условие возникновения аварийного сигнала может быть изменено оператором вручную.

3.1.6 **усовершенствованная система аварийной сигнализации** (advanced alarming): Система, разработанная на основе применения комплекса методов, которые могут помочь управлять оповещениями во время конкретных ситуаций.

Пример — Система аварийной сигнализации на основе состояний.

3.1.7 **аварийный сигнал** (alarm): Воспринимаемый оператором на слух и/или зрительно сигнал средств индикации о сбое оборудования, отклонении технологического процесса или неправильном условии, требующий своевременной реакции.

3.1.8 **оповещение, оповещение аварийной сигнализацией** (annunciation, alarm annunciation): Функция системы аварийной сигнализации, позволяющая привлечь внимание оператора к сигналу об аварии.

3.1.9 **атрибут аварийной сигнализации** (alarm attribute): Параметр срабатывания аварийной сигнализации в системе управления технологическим процессом.

Пример — Уставка аварийной сигнализации.

3.1.10 **класс аварийных сигнализаций** (alarm class): Группа аварийных сигнализаций с единым набором требований к управлению аварийной сигнализацией (например, требования к испытанию, обучению, контролю и аудиту).

Пример — Класс аварийных сигнализаций, связанных с безопасностью.

3.1.11 **мертвая зона аварийной сигнализации** (alarm deadband): Отклонение сигнала от значения уставки аварийной сигнализации, обеспечивающее возвращение системы аварийной сигнализации в исходное состояние.

3.1.12 **фильтрация (аварийного сигнала)** [(alarm) filtering]: Функция, которая выбирает записи аварийного сигнала для их отображения в соответствии с заданным элементом записи аварийного сигнала.

3.1.13 **поток аварийных сигналов** (alarm flood): Условие, при котором количество поступающих аварийных сигналов больше того количества, с которым оператор может эффективно справиться (например, более 10 аварийных сигналов в течение 10 мин).

3.1.14 **группа аварийных сигналов** (alarm group): Набор связанных между собой аварийных сигналов (например, от производственной установки, производственного участка, комплекта оборудования или обслуживания).

3.1.15 **сервер архива аварийных событий** (alarm historian): Долгосрочное хранилище для записей аварийных сигналов.

3.1.16 **журнал регистрации аварийных сигналов** (alarm log): Краткосрочное хранилище для записей аварийных сигналов.

3.1.17 **менеджмент аварийной сигнализацией, менеджмент системы аварийной сигнализации** (alarm management, alarm system management): Набор процессов и методов для определения, документирования, проектирования, контроля, и эксплуатационной поддержки систем аварийной сигнализации.

3.1.18 **сообщение об аварийной ситуации** (alarm message): Текстовая строка, отображаемая с индикацией аварийного сигнала, которая предоставляет дополнительную информацию оператору (например, о действиях оператора).

3.1.19 **задержка отключения аварийной сигнализации, устранение ложных повторных нажатий клавиши** (alarm off-delay, debounce): Время, в течение которого показания технологического замера остаются в исходном состоянии до того момента, когда аварийная сигнализация перестает быть активной.

3.1.20 **задержка включения аварийной сигнализации** (alarm on-delay): Время, в течение которого показания технологического замера остаются в состоянии, вызывающем аварийный сигнал, до момента оповещения об аварии.

3.1.21 **концепция аварийной сигнализации** (alarm philosophy): Документ, который устанавливает основные определения, принципы и процессы для проектирования, внедрения и поддержки системы аварийной сигнализации.

3.1.22 **приоритет аварийной сигнализации** (alarm priority): Относительная значимость, назначенная аварийной сигнализации в системе аварийной сигнализации, для указания на важность отклика (например, серьезность последствий и допустимое время отклика).

3.1.23 **интенсивность аварийных сигналов** (alarm rate): Количество оповещающих аварийных сигналов на одного оператора за конкретный период времени.

3.1.24 **запись (аварийного сигнала)** [(alarm) record]: Набор информации, описывающий изменение состояния аварийной сигнализации.

3.1.25 **уставка срабатывания аварийной сигнализации, предел аварийной сигнализации, точка срабатывания аварийной сигнализации** (alarm setpoint, alarm limit, alarm trip point): Пороговое значение параметра, описывающего непрерывное или дискретное состояние технологического процесса, которое инициирует индикацию аварийной сигнализации.

3.1.26 **сортировка (аварийных сигналов)** [(alarm) sorting]: Функция, которая упорядочивает записи аварийных сигналов для их отображения в соответствии с заданным элементом записи аварийного сигнала.

3.1.27 **сводка аварийных сигналов, список аварийных сигналов** (alarm summary, alarm list): Отображение, которое перечисляет оповещающие аварийные сигнализации с отобранной информацией (например, датой, временем, приоритетом и типом аварийной сигнализации).

Примечание — Возвращение к исходным индикациям также может появиться в сводке аварийных сигналов.

3.1.28 **система аварийной сигнализации** (alarm system): Система поддержки оператора для формирования и обработки аварийных сигналов для управления аварийными ситуациями.

Примечание — Оператор включен в систему аварийной сигнализации (см. рисунок 1).

3.1.29 **спецификация требований к системе аварийной сигнализации** (alarm system requirements specification): Документ, который подробно определяет проект системы аварийной сигнализации.

3.1.30 **тип аварийной сигнализации** (alarm type): Атрибут аварийной сигнализации, разные значения которого связаны с разными аварийными ситуациями.

Пример — Аварийная сигнализация по низкому значению технологического параметра, аварийная сигнализация по высокому значению технологического параметра или аварийная сигнализация по расхождению.

3.1.31 **предупреждение об опасности** (alert): Воспринимаемые оператором световые и звуковые сигналы средств индикации, которые указывают на возможную необходимость оценки оборудования или условия технологического процесса, когда позволит время.

3.1.32 **допустимое значение времени реакции** (allowable response time): Максимальное значение времени между оповещением системы сигнализации и выполнением оператором корректирующих мер для предотвращения последствия.

3.1.33 **индикаторная панель** (annunciator): Устройство или группа устройств, которые привлекают внимание к изменениям условий технологического процесса.

3.1.34 **оценка** (assessment): Сравнение результатов контроля и дополнительных качественных (субъективных) измерений с установленными целями и заданными метриками производительности.

3.1.35 **аудит** (audit): Комплексная оценка, включающая оценку производительности системы аварийной сигнализации и эффективность методов работы, используемых для администрирования системы аварийной сигнализации.

3.1.36 **аварийная сигнализация при измерении дефекта** (bad-measurement alarm): Аварийная сигнализация, в которой аварийный сигнал формируется в тех случаях, если значение сигнала при измерениях технологического процесса оказывается вне ожидаемого диапазона (например, измеренное значение сигнала равно 3,8 мА для диапазона от 4 до 20 мА).

3.1.37 **оценка параметров** (benchmark): Начальный аудит системы аварийной сигнализации, специально разработанный для определения проблемных областей в целях формирования планов по улучшению.

3.1.38 **аварийная сигнализация, управляемая битовым шаблоном** (bit-pattern alarm): Аварийная сигнализация, в которой аварийный сигнал формируется в том случае, если значение цифрового сигнала соответствует предопределенному битовому шаблону.

3.1.39 **аварийная сигнализация, управляемая расчетом** (calculated alarm): Аварийная сигнализация, в которой аварийный сигнал формируется в результате расчета, а не прямого измерения в технологическом процессе.

3.1.40 **аварийная сигнализация, использующая другие средства сообщений** (call-out alarm): Аварийная сигнализация, в которой аварийный сигнал уведомляет оператора и поступает к нему с помощью средств отличных от (или в дополнение к) дисплея пульта оператора (например, с помощью пейджера или телефона).

3.1.41 **дребезг аварийной сигнализации** (chattering alarm): Аварийная сигнализация, в которой аварийный сигнал повторно появляется при каждом переходе между состоянием аварии и исходным состоянием в течение короткого периода времени.

3.1.42 **классификация** (classification): Процесс разделения аварийных сигнализаций на классы аварийных сигнализаций, основанных на общих требованиях (например, требований к испытанию, обучению, контролю и аудиту).

3.1.43 **система управления** (control system): Система, которая отвечает на входные сигналы от управляемого оборудования и/или от оператора и формирует выходные сигналы, которые обеспечивают работу управляемого оборудования необходимым образом.

Примечание — Система управления может включать как основные системы управления технологическим процессом (ОСУТП), так и приборные системы безопасности (ПСБ).

3.1.44 **аварийная сигнализация, использующая выход контроллера** (controller-output alarm): Аварийная сигнализация, в которой аварийный сигнал формируется из выходного сигнала (алгоритма управления) контроллера (например, ПИД-регулятора), а не от непосредственного измерения в технологическом процессе.

3.1.45 **вывод из эксплуатации** (decommission): Процесс удаления аварийной сигнализации из системы аварийной сигнализации.

3.1.46 **аварийная сигнализация по отклонению** (deviation alarm): Аварийная сигнализация, в которой аварийный сигнал формируется, когда различие между двумя значениями превышает некоторое предельное значение (например, отклонение между основными и резервными средствами измерений или отклонение между переменным значением параметра технологического процесса и уставкой).

3.1.47 **аварийная сигнализация по расхождению, аварийная сигнализация по несоответствию** (discrepancy alarm, mismatch alarm): Аварийная сигнализация, в которой аварийный сигнал формируется в результате различия между ожидаемым состоянием объекта или устройства и его реальным состоянием (например, когда двигатель не запускается после того, как подана команда на его запуск).

3.1.48 **отображение** (display): Визуальное представление информации, используемой оператором для контроля и управления.

3.1.49 **динамическая аварийная сигнализация** (dynamic alarming): Аварийная сигнализация, в которой выполняется автоматическое изменение атрибутов аварийной сигнализации в зависимости от состояния или условий технологического процесса.

3.1.50 **соблюдение** (enforcement): Метод повышения эффективности аварийной сигнализации, обеспечивающий проверку и восстановление атрибутов аварийной сигнализации в системе управления до определенных значений из общей базы данных аварийных сигналов.

3.1.51 **событие** (event): Представление предусмотренного или непредусмотренного факта, указывающее на изменение текущего состояния предприятия.

Примечание — Например, изменения режима, изменения состояния устройства.

[МЭК 62264-2:2004, п. 3.1.2, изменен, добавлено примечание.]

3.1.52 **кратковременная аварийная сигнализация** (fleeting alarm): Аварийная сигнализация, в которой аварийный сигнал появляется при выполнении переходов между состоянием с активной аварийной сигнализацией и состоянием с неактивной аварийной сигнализацией в течение короткого периода времени.

3.1.53 **аварийный сигнал, обрабатываемый в порядке поступления, первый обрабатываемый аварийный сигнал** (first-out alarm, first-up alarm): Аварийный сигнал, претендующий (в логике обратного магазинного типа) быть первым в сценарии обработки среди множества аварийных сигналов.

3.1.54 **наиболее важная аварийная сигнализация** (highly managed alarm): Аварийная сигнализация, аварийный сигнал которой принадлежит к классу аварийных сигналов с дополнительными, помимо общих, требованиями.

Пример — Аварийная сигнализация системы безопасности.

3.1.55 **человеко-машинный интерфейс**; ЧМИ (human machine interface, HMI): Совокупность аппаратного и программного обеспечения, используемого оператором, для контроля и взаимодействия с системой управления и с технологическим процессом через систему управления.

3.1.56 **внедрение** (implementation): Промежуточная стадия между проектированием и эксплуатацией, во время которой система аварийной сигнализации вводится в эксплуатацию.

Примечание — Внедрение включает в себя такие действия, как приемка в эксплуатацию и обучение.

3.1.57 **аварийная сигнализация диагностики прибора** (instrument diagnostic alarm): Аварийная сигнализация, в которой аварийный сигнал формируется периферийным устройством и указывает на сбой в этом устройстве (например, отказ датчика).

3.1.58 **временная аварийная сигнализация** (interim alarm): Аварийная сигнализация, в которой аварийный сигнал используется на временной основе, чтобы заменить вышедшую из строя систему аварийной сигнализации.

3.1.59 **аварийная сигнализация с фиксацией аварийного сигнала** (latching alarm): Аварийная сигнализация, в которой аварийный сигнал продолжает указывать на аварию после того, как условия технологического процесса возвратились к исходному состоянию, и до тех пор, пока оператор не предпримет действия по ее отключению.

3.1.60 **общая база данных аварийных сигналов** (master alarm database): Согласованный список рационализированных аварийных сигнализаций и их атрибутов.

3.1.61 **контроль** (monitoring): Измерение и подготовка отчета о количественных (объективных) аспектах производительности системы аварийной сигнализации.

3.1.62 **ложный аварийный сигнал** (nuisance alarm): Аварийный сигнал, который выдается избыточно, без необходимости, либо не возвращается в исходное состояние после выполнения необходимых действий оператора.

Пример — В случаях дребезжащей аварийной сигнализации, кратковременной аварийной сигнализации или просроченной аварийной сигнализации.

3.1.63 **оператор, диспетчер** (operator, controller): Лицо, которое контролирует и вносит изменения в технологический процесс.

3.1.64 **пульт (оператора)** ((operator) console): Интерфейс оператора для контроля и/или управления технологическим процессом, который может включать несколько дисплеев или устройств оповещения и определяет границы зоны ответственности оператора.

3.1.65 **рабочая станция оператора** (operator station): Человеко-машинный интерфейс с пультом оператора.

Примечание — Рабочая станция оператора может включать много экранов.

3.1.66 **выведена из эксплуатации** (out-of-service): Состояние системы аварийной сигнализации, во время которого индикация аварийной сигнализации отключена вручную (например, во время технического обслуживания).

3.1.67 **состояние предприятия, режим предприятия** (plant state, plant mode): Определенный набор условий эксплуатации для производственного предприятия.

Пример — Приостановка работы, нормальное функционирование.

3.1.68 **установление приоритетов** (prioritization): Процесс назначения уровня важности аварийной сигнализации для процесса эксплуатации.

3.1.69 **производственный участок** (process area): Физическая, территориальная или логически объединенная группа объектов, определяемая в рамках производственной площадки.

[МЭК 62264-1:2003, п. 3.1]

3.1.70 **аварийная сигнализация о скорости изменения** (rate-of-change alarm): Аварийная сигнализация, в которой аварийный сигнал формируется, если изменение значения переменной технологического процесса в единицу времени (dPV/dt) превышает определенное значение уставки.

3.1.71 **рационализация** (rationalization): Процесс анализа возможных для применения аварийных сигнализаций, использующий основные положения концепции аварийной сигнализации, производимой с целью проектирования и документального оформления обоснованности выбора аварийной сигнализации.

3.1.72 **аварийная сигнализация с повторяющимся аварийным сигналом, аварийная сигнализация с повторно запускаемым аварийным сигналом** (re-alarming alarm, re-triggering alarm): Аварийная сигнализация, в которой аварийный сигнал при определенных условиях автоматически повторно оповещает оператора об аварии.

3.1.73 **аварийная сигнализация, управляемая набором правил** (recipe-driven alarm): Аварийная сигнализация с уставками, зависящими от набора правил, выполняемых в текущий момент.

3.1.74 **удаленная аварийная сигнализация** (remote alarm): Аварийная сигнализация, в которой аварийный сигнал поступает от удаленно эксплуатируемого средства или направлен к удаленному интерфейсу.

3.1.75 **сброс** (reset): Действие оператора, которое отключает зафиксированную в активном состоянии аварийную сигнализацию.

3.1.76 **возврат к исходному состоянию, установка в исходное состояние** (return to normal, clear): Переход аварийной сигнализации от активного состояния оповещения об аварийном сигнале к неактивному состоянию оповещения об аварийном сигнале.

3.1.77 **приборная система безопасности** (safety instrumented system): Приборная система, реализующая одну или несколько приборных функций безопасности. ПСБ состоит из некоторой комбинации датчика(ов), логического(их) решающего(их) устройства(в) и исполнительного(ых) элемента(ов).

Примечание — ПСБ может включать либо приборные функции безопасности системы управления, либо приборные функции безопасности системы защиты, либо обе из них.

[МЭК 61511-1:2003, п. 3.2.72]

3.1.78 **связанная с безопасностью аварийная сигнализация, аварийная сигнализация безопасности** (safety related alarm, safety alarm): Система аварийной сигнализации, которая классифицируется как критическая для безопасности технологического процесса и обеспечивает защиту жизни человека или окружающей среды.

Пример — Система аварийной сигнализации, снижающая риск более, чем в 10 раз.

3.1.79 **откладывание аварийной сигнализации** (shelve): Временное запрещение аварийной сигнализации по инициативе оператора с использованием технических средств управления для ее разрешения.

3.1.80 **отсутствие звука** (silence): Результат действия оператора, которое завершает звуковую индикацию аварийной сигнализации.

3.1.81 **просроченная аварийная сигнализация** (stale alarm): Аварийная сигнализация, в которой аварийный сигнал остается оповещающим в течение длительного периода времени (например, 24 ч).

3.1.82 **аварийная сигнализация, управляемая состоянием, аварийные сигнализации, управляемые режимами работы** (state-based alarm, mode-based alarms): Аварийная сигнализация, имеющая атрибуты, которые изменяются или запрещаются в зависимости от эксплуатационных состояний или условий технологического процесса.

3.1.83 **аварийная сигнализация, основанная на статистике** (statistical alarm): Аварийная сигнализация, в которой аварийный сигнал сформирован на основе статистической обработки значений переменной или переменных технологического процесса.

3.1.84 **запрещение аварийной сигнализации** (suppress): Предотвращение оповещения аварийной сигнализации оператору, когда она активна.

Пример — Отложить, запретить в соответствии с проектом, вывести из эксплуатации.

3.1.85 **запрещенная в соответствии с проектом** (suppressed by design): Оповещение аварийной сигнализации оператору предотвращается в зависимости от состояния производственного объекта или других условий.

3.1.86 **аварийная сигнализация системы диагностики** (system diagnostic alarm): Аварийная сигнализация, в которой аварийный сигнал сформирован системой управления, чтобы указать на сбой в аппаратных средствах, программном обеспечении или компонентах.

Пример — Ошибка обмена данных.

3.1.87 **признак, пункт** (tag, point): Уникальный идентификатор, присвоенный измерению в технологическом процессе, вычислению или устройству в системе управления.

3.1.88 **неподтвержденный** (unacknowledged): Состояние аварийной сигнализации, при котором оператор еще пока не подтвердил признание индикации аварийной сигнализации.

3.2 Сокращения

ACKED — подтвержденный;

ASRS — спецификация требований к системе аварийной сигнализации;

BPCS — основная система управления технологическим процессом (ОСУТП);

cGMP — современная надлежащая производственная практика;

DSUPR — запрещение в соответствии с проектом;

EEMUA — ассоциация потребителей инженерного оборудования и материалов;

ERP — планирование ресурсов предприятий;

FMEA — анализ вида и последствий отказов;

HAZOP — исследование опасности и работоспособности;

HMA — наиболее важная аварийная сигнализация;

HMI — человеко-машинный интерфейс;

I/O — ввод/вывод;

LOPA — анализ слоев защиты;

MES — система управления производством;

MOC — управление изменениями;

NORM — норма;

OOSRV — выведена из эксплуатации;

P&ID — схема трубопроводов (или технологического процесса) и контрольно-измерительных приборов;

PHA — анализ опасностей технологического процесса;

RTNUN — возврат к исходному неподтвержденному состоянию;

SHLVD — отложенный;

SIS — приборная система безопасности;

SOP — типовая рабочая процедура;

UNACK — неподтвержденный.

4 Соответствие настоящему стандарту

4.1 Правило обеспечения соответствия

Для соответствия настоящему стандарту необходимо показать, что каждое из требований в нормативных разделах было удовлетворено. За это несет ответственность владелец/оператор.

4.2 Существующие системы

Для существующих систем аварийной сигнализации, которые были разработаны и построены в соответствии с нормами и правилами, стандартами и/или методами до выпуска настоящего стандарта, владелец/оператор должен установить, что оборудование разрабатывается, поддерживается, проверяется, испытывается и управляется безопасным способом. Методы и процедуры, представленные в настоящем стандарте, должны быть применены к существующим системам в разумный срок, который определяет владелец/оператор.

4.3 Ответственность

За соответствие настоящему стандарту ответственность несет владелец/оператор.

5 Модели систем аварийной сигнализации

5.1 Системы аварийной сигнализации

Системы аварийной сигнализации предназначены для передачи операторам, контролирующему и выполняющему производственный процесс персоналу информации о некорректных условиях технологического процесса или о неисправностях в работе оборудования, а также для поддержки ответа. Эффективные системы аварийной сигнализации должны быть хорошо спроектированы, качественно внедрены, на высоком уровне — эксплуатироваться и технически обслуживаться. Менеджмент аварийной сигнализацией — это набор методов и процессов, который гарантирует эффективную работу системы аварийной сигнализации.

Основополагающей частью менеджмента аварийной сигнализацией является определение аварийного сигнала, звукового или видимого (по средствам индикации) сообщающего оператору о сбое оборудования, отклонении технологического процесса или некорректном условии и требующего отклика. Важным элементом этого определения является отклик на аварийную сигнализацию. Данное определение раскрыто и поддержано описанными в настоящем стандарте процессами менеджмента аварийной сигнализацией.

5.2 Менеджмент жизненного цикла аварийной сигнализации

5.2.1 Модель менеджмента жизненного цикла аварийной сигнализации

На рисунке 2 показаны связи между всеми стадиями менеджмента жизненного цикла аварийной сигнализации, описанного в настоящем стандарте. Менеджмент жизненного цикла аварийной сигнализации охватывает спецификацию системы аварийной сигнализации, ее проектирование, реализацию, функционирование, контроль, техническое обслуживание и действия по ее изменению: от начальной концепции до утилизации.

Модель жизненного цикла полезна для идентификации требований и обязанностей при реализации системы менеджмента аварийной сигнализации. Жизненный цикл допускается применять для установки новых систем аварийной сигнализации или для управления существующей системой.

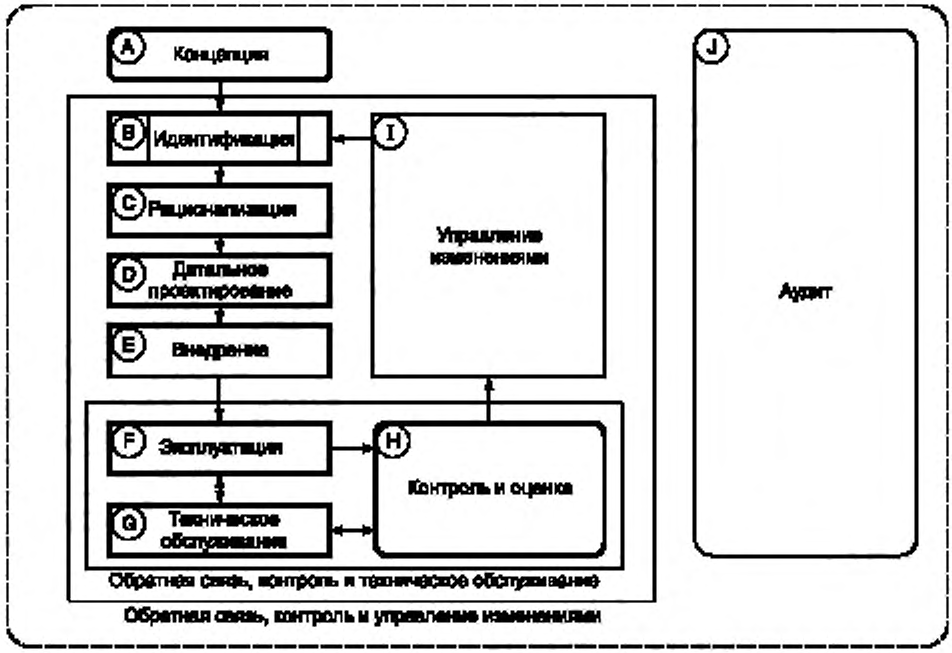

Рисунок 2 — Менеджмент жизненного цикла аварийной сигнализации

Примечания

1 Стадия B, выделенная как блок, представляет процесс, который не определен согласно 5.2.2.3.

2 Независимая стадия J представляет процесс, который связан со всеми другими стадиями и описан в 5.2.2.11.

3 Стадии A, H, и J, выделенные закругленными рамками представляют точки входа в жизненный цикл и описаны в 5.2.3.

4 Пунктирные линии указывают на обратные связи в жизненном цикле, которые описаны в 5.2.5.

5.2.2 Стадии менеджмента жизненного цикла аварийной сигнализации

5.2.2.1 Общие положения

Стадии менеджмента жизненного цикла аварийной сигнализации, показанные на рисунке 2, кратко описаны в следующих подпунктах. Символьный знак является идентификатором и используется далее по тексту. Требования и рекомендации для каждой стадии приведены в разделах 6—18.

5.2.2.2 Концепция аварийной сигнализации (A)

Перед проектированием новой системы аварийной сигнализации или модификацией существующей системы необходимо выполнить основное планирование. Обычно первым шагом является разработка концепции аварийной сигнализации, в документах которой должны быть представлены описания целей системы аварийной сигнализации, а также процессов, обеспечивающих достижение этих целей. Для новых систем концепция аварийной сигнализации служит основой для документа, который называют спецификацией требований к системе аварийной сигнализации (ASRS).

Концепция начинается с основных определений, расширяет и доводит их до рабочих определений. Критерии установления приоритетов для аварийных сигнализаций и определения классов аварийных сигнализаций, метрик производительности, предельных технических характеристик и требований к отчетности должны быть основаны на целях и принципах систем аварийной сигнализации. Схемы представления индикаций аварий в ЧМИ, включая использование приоритетов, также устанавливают в концепции аварийной сигнализации, которая должна быть согласована с проектом всего ЧМИ. Эта концепция определяет процессы, используемые для каждой из стадий менеджмента жизненного цикла аварийной сигнализации, такие, как начало процесса управления изменениями и конкретные требо-

вания к изменениям. Эта концепция поддерживается, чтобы гарантировать последовательный менеджмент аварийной сигнализации на всем жизненном цикле системы аварийной сигнализации.

Разработка ASRS должна быть включена в стадию концепции жизненного цикла. Такая спецификация может быть конкретной для каждого предприятия и представлять подробную информацию об ограничениях или вариантах, а также может быть основанием для выбора новых или изменения существующих систем управления. Спецификация аварийной сигнализации является более подробной, чем концепция, и может быть конкретным руководством для проектирования системы.

5.2.2.3 Идентификация (B)

На стадии идентификации собирают все возможные аварийные сигнализации, определенные любым из используемых методов, в тех случаях, когда аварийная сигнализация может потребоваться. Определение этих методов не входит в область применения настоящего стандарта, поэтому стадия идентификации представлена в жизненном цикле как заранее определенный процесс. Методы могут быть формальными, такие как анализ опасностей процесса, спецификация требований к безопасности, анализ рекомендаций, сформированных по расследованиям причин аварий, обзор надлежащей производственной практики, оценка природоохранных разрешений, анализ разработки P&ID или технологического процесса. Изменения технологического процесса и эксплуатационные испытания также могут привести к необходимости использования аварийных сигнализаций или их модификаций. Некоторые изменения аварийной сигнализации будут определены в результате обычного контроля производительности системы аварийной сигнализации. На данной стадии должна быть определена потребность в новой системе аварийной сигнализации или в модификациях существующей, то есть она должна быть готова к рационализации.

5.2.2.4 Рационализация (C)

На стадии рационализации выполняют согласование выявленной потребности в системе аварийной сигнализации или в изменении существующей с принципами концепции аварийной сигнализации. Эти действия могут быть выполнены в рамках одного процесса или последовательности процессов. В результате рационализации формируется документация на систему аварийной сигнализации, которая включает любые методы усовершенствования аварийной сигнализации, которые могут использоваться при проектировании.

Рационализация — это процесс применения требований к системе аварийной сигнализации и формирования сопроводительной документации, являющейся основой для определения уставки срабатывания аварийной сигнализации, последствий и корректирующих действий, которые могут быть предприняты оператором.

Рационализация включает установление приоритетов для аварийных сигнализаций на основе метода, определенного в концепции аварийной сигнализации. Часто определение приоритета связано с последствиями конкретной аварийной ситуации и значением допустимого времени отклика.

Рационализация также включает действия по классификации, в результате которых аварийная сигнализация включается в один или несколько классов для установления требований (например, требований к проектированию, испытанию, обучению или отчетности). Тип последствий рационализированной аварийной сигнализации или другие критерии могут использоваться для разделения аварийных сигналов на классы, как определено в концепции аварийной сигнализации.

Результаты рационализации документально оформляются, как правило, в общей базе данных аварийных сигналов (т. е. принятый документ или файл), которую поддерживают на всем сроке службы системы аварийной сигнализации.

5.2.2.5 Детальное проектирование (D)

На стадии проектирования атрибуты аварийной сигнализации должны быть определены и разработаны на основе требований, определенных на стадии рационализации. На данной стадии проектирование выполняется по трем направлениям: техническое проектирование системы аварийной сигнализации, проектирование ЧМИ и проектирование методов усовершенствования системы аварийной сигнализации.

Технический проект для каждой аварийной сигнализации выполняют в соответствии с руководящими указаниями, тесно связанными с типом аварийной сигнализации и конкретной системой управления.

Проект ЧМИ включает описание средств отображения и оповещения аварийных сигналов, включая индикацию приоритетов аварийной сигнализации.

Методы усовершенствования систем аварийной сигнализации — это дополнительные функции, которые повышают эффективность системы аварийной сигнализации помимо основного проекта си-

стемы аварийной сигнализации и ЧМИ. Эти методы включают аварийную сигнализацию, управляемую состояниями.

5.2.2.6 Внедрение (E)

На стадии внедрения выполняют действия, необходимые для установки аварийной сигнализации или системы аварийной сигнализации и сдачи ее в эксплуатацию. Внедрение новой аварийной сигнализации или новой системы аварийной сигнализации должно включать работы по физической и логической установке и функциональную проверку системы.

Так как операторы являются неотъемлемой частью системы аварийной сигнализации, то обучение оператора — важная деятельность во время внедрения. Испытание новых аварийных сигналов часто является требованием стадии внедрения. Документация для обучения, испытания и ввода в действие может меняться в зависимости от классификации, как определено в концепции аварийной сигнализации.

5.2.2.7 Эксплуатация (F)

На стадии эксплуатации аварийная сигнализация или система аварийной сигнализации находятся в процессе обслуживания и выполняют свою предназначенную функцию. На данной стадии также выполняется переподготовка как в области концепции аварийной сигнализации, так и в области анализа цели каждой аварийной сигнализации.

5.2.2.8 Техническое обслуживание (G)

На стадии технического обслуживания аварийная сигнализация или система аварийной сигнализации считаются еще не готовыми к эксплуатации, так как их испытывают и ремонтируют. Периодическое техническое обслуживание (например, испытание приборов) необходимо, чтобы гарантировать выполнение функций системы аварийной сигнализации в соответствии с проектом.

5.2.2.9 Контроль и оценка (H)

На стадии контроля и оценки непрерывно проверяют соответствие общих показателей работы системы аварийной сигнализации и отдельных аварийных сигнализаций целевым характеристикам, указанным в концепции аварийной сигнализации. Контроль и оценка данных, полученных на стадии эксплуатации, может инициировать работы по техническому обслуживанию или указывать на необходимость внесения изменений в систему аварийной сигнализации или в рабочие процедуры. Контроль и оценка данных, полученных на стадии технического обслуживания, позволяет определять эффективность технического обслуживания. Общие показатели работы системы аварийной сигнализации также контролируются и оцениваются в соответствии с целями, определенными в концепции аварийной сигнализации. Без постоянного контроля работа системы аварийной сигнализации может ухудшиться.

5.2.2.10 Управление изменениями (I)

На стадии управления изменениями предлагают и одобряют модификации системы аварийной сигнализации. Процесс изменения должен следовать за каждой из стадий менеджмента жизненного цикла аварийной сигнализации: от идентификации до внедрения.

5.2.2.11 Аудит (J)

На стадии аудита проводят периодические обзоры, чтобы поддержать целостность системы аварийной сигнализации и процессов менеджмента аварийной сигнализации. Аудиты производительности системы позволяют обнаружить недостатки, которые не очевидны при обычном контроле. Кроме того, выполняют аудит на соответствие концепции аварийной сигнализации, чтобы определить улучшения системы, такие как модификации концепции аварийной сигнализации. Аудиты могут также определить необходимость в повышении дисциплины организации, чтобы соответствовать концепции аварийной сигнализации.

5.2.3 Точки входа в жизненный цикл аварийной сигнализации

5.2.3.1 Общие положения

В зависимости от выбранного подхода существует три точки входа в менеджмент жизненного цикла аварийной сигнализации.

a) концепция аварийной сигнализации;

b) контроль и оценка;

c) аудит.

Эти точки входа выделены закругленными рамками на рисунке 2. Эти стадии жизненного цикла являются только начальными шагами в управлении системой аварийной сигнализации как отправные точки. Для реализации менеджмента системой аварийной сигнализации в полном объеме необходимы все стадии жизненного цикла.

5.2.3.2 Начало — концепция аварийной сигнализации (A)

Первой возможной отправной точкой является разработка концепции аварийной сигнализации, которая устанавливает цели системы аварийной сигнализации и используется в качестве основания для спецификации требований системы аварийной сигнализации. Это — входная точка в жизненный цикл для новых установок.

5.2.3.3 Начало — контроль и оценка (H)

Второй возможной входной точкой является контроль существующей системы аварийной сигнализации и оценка ее работы. Сначала выявляются проблемы аварийной сигнализации, и затем их устраняют методами технического обслуживания или управления изменениями. При этом допускается использовать данные контроля для сравнительной оценки параметров с данными, полученными до разработки концепции аварийной сигнализации.

5.2.3.4 Начало — аудит (J)

Третьей возможной входной точкой является первоначальный аудит или оценка параметров всех аспектов менеджмента аварийной сигнализации, которые предоставлены документально оформленными методами, перечисленными в настоящем стандарте или им подобными. Результаты начального аудита могут использоваться для развития концепции.

5.2.4 Одновременно выполняемые и охватывающие стадии

На диаграмме жизненного цикла (см. рисунок 2) представлена последовательность всех стадий. Ряд из них могут выполняться одновременно, а некоторые стадии могут охватывать действия других стадий.

Стадия контроля и оценки (H) выполняется одновременно со стадиями эксплуатации и технического обслуживания.

На стадии управления изменениями (I) запускается процесс изменения, на котором все соответствующие стадии жизненного цикла должны выполняться санкционированно.

Стадия аудита (J) является всеохватывающей, действия которой могут выполняться на любом этапе жизненного цикла, и включает анализ действий на других стадиях.

5.2.5 Обратные связи менеджмента жизненного цикла аварийной сигнализации

5.2.5.1 Общие положения

Кроме стадий менеджмента жизненного цикла аварийной сигнализации также существуют три вида обратных связей. Каждая обратная связь выполняет определенную функцию во время своего цикла.

5.2.5.2 Обратная связь «контроль и техническое обслуживание»

Обратная связь «эксплуатация—контроль и оценка—техническое обслуживание» реализует текущий мониторинг, который определяет проблемные аварийные сигнализации, для которых требуется техническое обслуживание. Восстановленные системы аварийной сигнализации должны быть возвращены в эксплуатацию.

5.2.5.3 Обратная связь «контроль и управление изменениями»

Обратная связь «эксплуатация—контроль и оценка—управление изменениями» реализуется, когда текущий контроль указывает, что проект аварийной сигнализации не может быть совместим с концепцией аварийной сигнализации. Возможно, проект должен быть изменен или должен быть применен метод усовершенствования аварийной сигнализации. Система аварийной сигнализации может эксплуатироваться, но при этом запускается процесс управления изменениями и стадии жизненного цикла выполняются повторно.

5.2.5.4 Обратная связь «аудит и концепция аварийной сигнализации»

Обратная связь «аудит и концепция аварийной сигнализации» представляет собой сам жизненный цикл и реализует процесс непрерывного улучшения системы аварийной сигнализации. Аудит определяет процессы в жизненном цикле для их подтверждения.

5.2.6 Входы и выходы стадий менеджмента жизненного цикла аварийной сигнализации

Стадии менеджмента жизненного цикла аварийной сигнализации связаны между собой, поскольку выходные данные одной стадии часто являются входными данными другой стадии. На диаграмме жизненного цикла (см. рисунок 2) эти связи представлены не полностью. Таблица 1 предоставляет больше информации об отношениях между входами и выходами стадий жизненного цикла.

Таблица 1 — Входы и выходы стадий менеджмента жизненного цикла аварийной сигнализации

Стадия менеджмента жизненного цикла аварийной сигнализации		Действия	Номер раздела	Входы	Выходы
Стадия	Название				
A	Концепция	Документирование целей, рекомендаций и рабочих процессов для менеджмента аварийной сигнализацией и ASRS	6, 7	Цели и стандарты	Концепция аварийной сигнализации и ASRS
B	Идентификация	Определение возможных аварийных сигналов	8	Отчет PHA, SRS, P&ID, рабочие процедуры и др.	Список возможных аварийных сигналов
C	Рационализация	Рационализация, классификация, определение приоритетов и документирование	9	Концепция аварийной сигнализации и Список возможных аварийных сигналов	Общая база данных аварийных сигналов и требования к проекту аварийной сигнализации
D	Детальное проектирование	Проектирование основной системы аварийной сигнализации, ЧМИ и методов усовершенствования аварийной сигнализации	10, 11, 12	Общая база данных аварийных сигналов и требования к проекту аварийной сигнализации	Полный проект аварийной сигнализации
E	Внедрение	Установка аварийной сигнализации, испытание и обучение	13	Полный проект аварийной сигнализации и общая база данных аварийных сигналов	Готовая к эксплуатации аварийная сигнализация и процедуры отклика аварийной сигнализации
F	Эксплуатация	Реакция оператора на аварийные сигналы и переподготовка	14	Готовая к эксплуатации аварийная сигнализация и процедуры отклика аварийной сигнализации	Данные аварийной сигнализации
G	Техническая поддержка	Обслуживание, ремонт и замена; периодическое испытание	15	Отчеты контроля аварийных сигналов и концепция аварийной сигнализации	Данные аварийной сигнализации
H	Контроль и оценка	Контроль данных аварийной сигнализации и отчет о работе	16	Данные аварийной сигнализации и концепция аварийной сигнализации	Отчеты о контроле аварийной сигнализации и предложенные изменения
I	Управление изменениями	Процесс одобрения дополнения, модификации и удаления аварийных сигнализаций	17	Концепция аварийной сигнализации и предложенные изменения	Санкционированные изменения аварийной сигнализации
J	Аудит	Периодический аудит процессов менеджмента аварийной сигнализации	18	Стандарты, концепция аварийной сигнализации и протокол аудита	Рекомендации для усовершенствования

5.3 Состояния аварийной сигнализации

5.3.1 Диаграмма переходов состояний аварийной сигнализации

Диаграмма переходов состояний аварийной сигнализации, показанная на рисунке 3, представляет состояния и переходы для типичной аварийной сигнализации. Хотя и существуют исключения, но данная диаграмма описывает большинство систем аварийной сигнализации и служит полезным примером для разработки принципов систем аварийной сигнализации и функций ЧМИ.

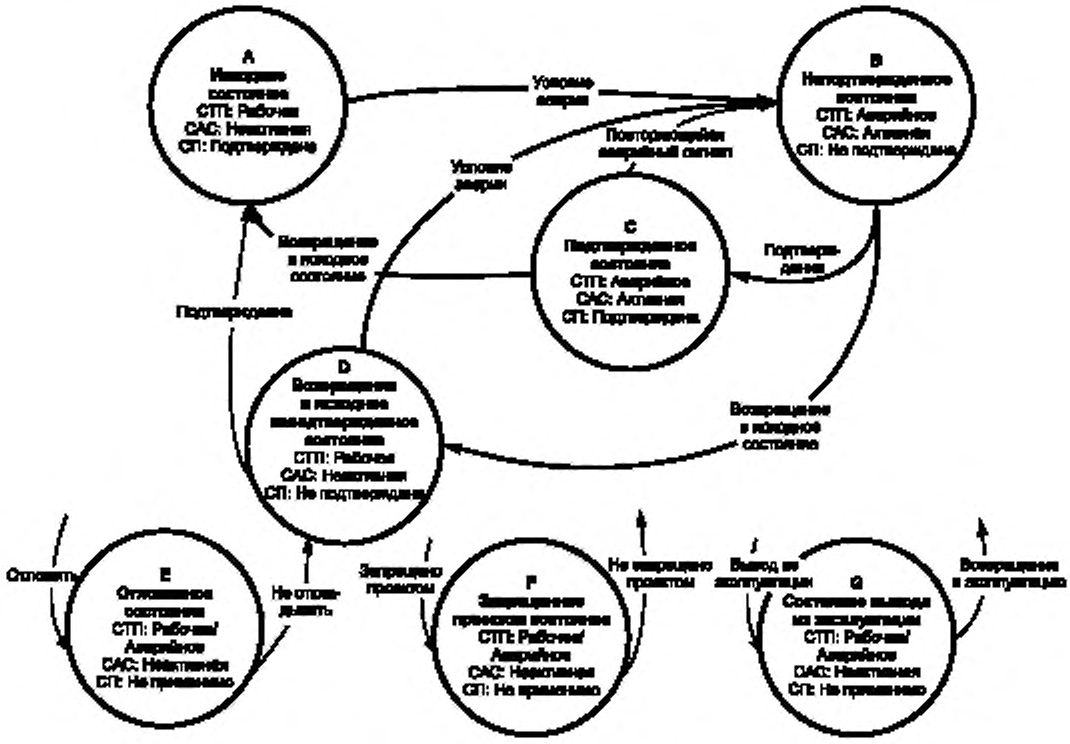

Рисунок 3 — Диаграмма переходов состояний аварийной сигнализации

Примечания

1 Состояния E, F и G могут быть соединены с любым состоянием аварийной сигнализации, указанным на диаграмме.

2 Пунктир означает редко осуществляемый переход.

5.3.2 Состояния аварийной сигнализации

5.3.2.1 Общие положения

Круги на рисунке 3 представляют состояния аварийной сигнализации. Буквенные обозначения — их идентификаторы. На второй строке — имя состояния, которое часто сокращается. На третьей строке описаны условия технологического процесса, а на четвертой и пятой строках представлены статус аварийной сигнализации и его статус подтверждения, соответственно. Возможные состояния запрещения аварийной сигнализации показаны в нижней части диаграммы.

5.3.2.2 Исходное состояние (A)

Исходное состояние аварийной сигнализации (NORM) определено как состояние, в котором производственный процесс выполняется при номинальных значениях технических требований, аварийная сигнализация не активна, а прошлые аварийные сигналы были подтверждены.

5.3.2.3 Неподтвержденное состояние (B)

Неподтвержденное состояние аварийной сигнализации (UNACK) — начальное состояние аварийной сигнализации, которое активизируется в результате нарушения нормальных условий эксплуатации. В этом состоянии аварийный сигнал не подтвержден. Аварийная сигнализация может быть спроектирована так, что подтвержденные ранее аварийные сигналы повторяются, вызывая возвращение в это неподтвержденное состояние.

5.3.2.4 Подтвержденное состояние (C)

Подтвержденным состоянием аварийной сигнализации (ACKED) является состояние, в котором аварийная сигнализация активна, а оператор подтвердил аварийный сигнал.

5.3.2.5 Возвращение в исходное неподтвержденное состояние (D)

Исходное неподтвержденное состояние аварийной сигнализации (RTNUN) — состояние, показывающее, что производственный процесс находится в пределах нормы, а аварийная сигнализация неактивна до тех пор, пока оператор не подтвердит условие аварийного сигнала.

5.3.2.6 Отложенное состояние (E)

В состоянии отложенной аварийной сигнализации (SHLVD) управляемый метод временно запрещает аварийную сигнализацию и оповещение о ней не запускается. Аварийная сигнализация в отложенном состоянии находится под управлением оператора. Функция, реализующая состояние отложенной аварийной сигнализации, может это состояние автоматически отменить.

5.3.2.7 Запрещенное проектом состояние (F)

В запрещенном проектом состоянии аварийной сигнализации (DSUPR) аварийная сигнализация запрещается в определенных условиях эксплуатации или при определенных состояниях объекта и оповещение о ней не запускается. Аварийная сигнализация в запрещенном проектом состоянии управляется логикой, которая и определяет ее соответствие указанным условиям или состояниям.

5.3.2.8 Состояние вывода из эксплуатации (G)

В состоянии вывода аварийной сигнализации из эксплуатации (OOSRV) аварийная сигнализация запрещается вручную (например, функции системы управления выводят аварийную сигнализацию из эксплуатации), когда она выводится из эксплуатации обычно для технического обслуживания, и оповещение о ней не запускается. Аварийная сигнализация в состоянии вывода из эксплуатации находится под управлением системы технического обслуживания.

5.3.2.9 Статусы аварийных сигнализаций в различных состояниях

Статусы аварийных сигнализаций в различных состояниях этих сигнализаций представлены в таблице 2.

Таблица 2 — Состояния аварийных сигнализаций

Идентификатор	Сокращенное имя	Имя состояния	Условие процесса	Статус аварийной сигнализации	Статус оповещения	Статус подтверждения
A	NORM	Исходное состояние	Исходное	Неактивный	Нет оповещения	Подтвержденное
B	UNACK	Неподтвержденное состояние	Исходное или нерабочее	Активный	Есть оповещение	Не подтвержденное
C	ACKED	Подтвержденное состояние	Исходное или нерабочее	Активный	Есть оповещение	Подтвержденное
D	RTNUN	Возвращение в исходное неподтвержденное состояние	Исходное	Неактивный	Есть оповещение	Не подтвержденное
E	SHLVD	Отложенное состояние	Исходное или нерабочее	Активный или неактивный	Запрещено	Не применимо
F	DSUPR	Запрещенное проектом состояние	Исходное или нерабочее	Активный или неактивный	Запрещено	Не применимо
G	OOSRV	Состояние вывода из эксплуатации	Исходное или нерабочее	Активный или неактивный	Запрещено	Не применимо

5.3.3 Переходы между состояниями аварийной сигнализации

5.3.3.1 Общие положения

Стрелки на рисунке 3 представляют переходы между состояниями. Для простоты понимания на диаграмме не показано влияние мертвой зоны, а также задержки включения или задержки выключения аварийной сигнализации.

5.3.3.2 Переход из исходного в неподтвержденное состояние (A → B)

Данный переход происходит, когда исходный режим технологического процесса оказывается вне диапазона, определенного уставками срабатывания сигнализации, и остается в этом состоянии достаточно долго, что вызывает срабатывание аварийной сигнализации.

5.3.3.3 Переход из неподтвержденного в подтвержденное состояние (B → C)

Этот переход происходит, когда оператор подтверждает срабатывание аварийной сигнализации, которая остается активной до возврата технологического процесса в исходное состояние.

5.3.3.4 Переход из подтвержденного в неподтвержденное состояние (C → B)

Этот нечасто используемый переход периодически формирует повторяющиеся аварийные сигналы для отдельной аварийной сигнализации, в то время как она остается в состоянии срабатывания аварийной сигнализации.

5.3.3.5 Переход из подтвержденного в исходное состояние (C → A)

Данный переход является частью обычной последовательности состояний аварийной сигнализации. Аварийная сигнализация переходит из подтвержденного состояния в исходное состояние.

5.3.3.6 Переход из неподтвержденного в состояние возвращения в исходное неподтвержденное состояние (B → D)

Переход в это состояние происходит, когда производственный процесс возвращается в исходное состояние, и длится оно до тех пор, пока оператор не подтвердит аварийную сигнализацию.

5.3.3.7 Переход из состояния возвращения в исходное неподтвержденное состояние в исходное состояние (D → A)

Этот переход происходит, когда аварийная сигнализация возвратилась в исходное состояние и становится неактивной и оператор может подтвердить ее срабатывание либо оно может быть подтверждено автоматически.

5.3.3.8 Переход в отложенное состояние (любое состояние → E)

Такой переход происходит, когда оператор откладывает срабатывание аварийной сигнализации, чтобы избежать помех при отображении на экране дисплея активных аварийных сигналов. Задержка выполняется оператором вручную.

5.3.3.9 Переход из отложенного состояния в исходное или неподтвержденное состояние (E → A или B)

Данный переход происходит, когда срабатывание аварийной сигнализации не отложено и выполняется вручную оператором или автоматически. Если аварийная сигнализация не активна, то должен быть выполнен ее переход в исходное состояние. Если аварийная сигнализация активна, то должен произойти ее переход в неподтвержденное состояние.

5.3.3.10 Переход в запрещенное проектом состояние (любое состояние → F)

Этот переход выполняется, если условия или состояния технологического процесса используются для запрещения аварийных сигнализаций при проектировании. Такое запрещение, как правило, выполняется автоматически.

5.3.3.11 Переходы из запрещенного проектом состояния в исходное или неподтвержденное состояние (F → A или B)

Такой переход происходит, если условия или состояния технологического процесса используются для того, чтобы в надлежащих случаях не запрещать аварийные сигналы. Такое не запрещение, как правило, выполняется в автоматическом режиме. Если аварийная сигнализация не активна, то должен быть выполнен ее переход в исходное состояние. Если аварийная сигнализация активна, то должен произойти ее переход в неподтвержденное состояние.

5.3.3.12 Переход в состояние вывода из эксплуатации (любое состояние → G)

Аварийная сигнализация может быть выведена из эксплуатации для технического обслуживания или по другим причинам. Вывод из эксплуатации, как правило, выполняется оператором вручную.

5.3.3.13 Переход из состояния вывода из эксплуатации в исходное или неподтвержденное состояние (G → A или B)

Аварийная сигнализация может быть возвращена в эксплуатацию, когда она готова к применению. Возвращение в эксплуатацию, как правило, выполняется оператором вручную. Если аварийная

сигнализация не активна, то должен быть выполнен ее переход в исходное состояние. Если аварийная сигнализация активна, то должен быть выполнен ее переход в неподтвержденное состояние.

5.4 Временная диаграмма аварийной сигнализации

5.4.1 Общие положения

На рисунке 4 представлено измерение некоторого параметра технологического процесса, значение которого увеличивается от значений в исходном режиме до значений аварийного режима, а также два возможных сценария, связанных с тем, принимает ли оператор меры по ликвидации последствий или нет. Разумно отобразить некоторые состояния аварийной сигнализации, представленные на рисунке 3, на временной диаграмме, показанной на рисунке 4 для того, чтобы разъяснить определения терминов, связанных со временем.

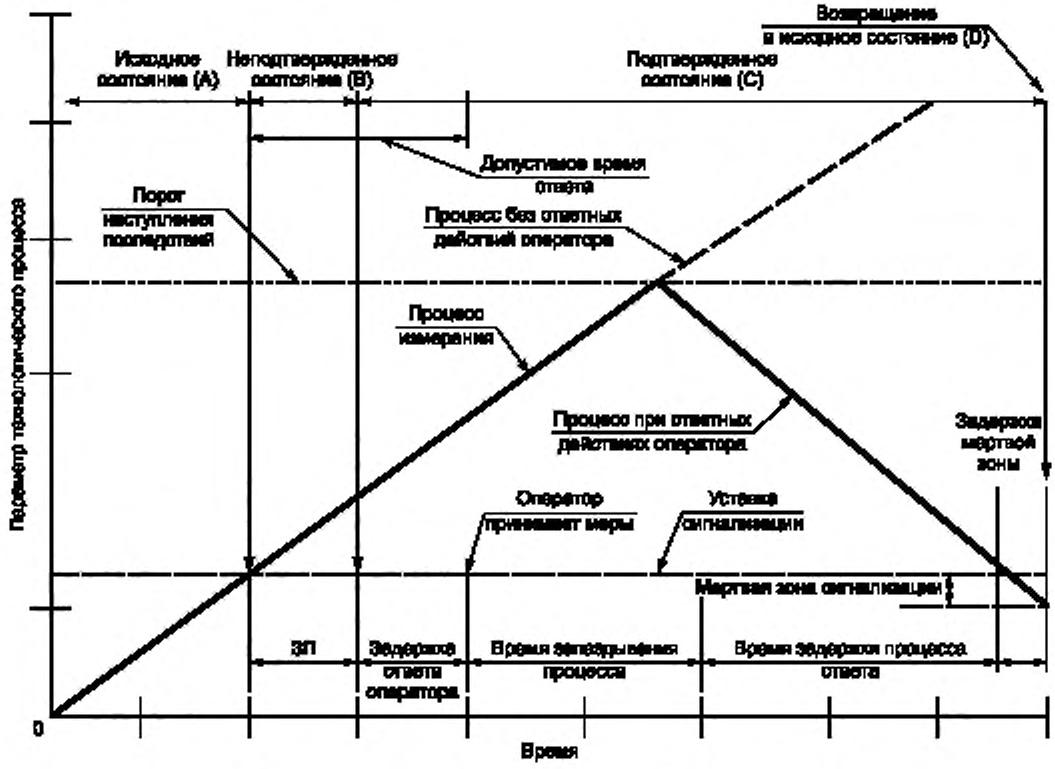

Рисунок 4 — Временная диаграмма аварийной сигнализации

5.4.2 Исходное состояние (A)

Исходное состояние аварийной сигнализации определено как состояние, в котором производственный процесс выполняется в рабочем диапазоне технических требований, аварийная сигнализация не активна, а все прошлые аварийные сигналы были подтверждены.

5.4.3 Неподтвержденное состояние (B)

Неподтвержденное состояние аварийной сигнализации заканчивается, когда измеряемое значение пересекает значение уставки срабатывания сигнализации. Существует несколько факторов, которые влияют на оповещение аварийной сигнализации, такие как:

a) точность измерения;

b) интервал выборки;

c) задержка включения аварийной сигнализации.

Не всегда аварийная сигнализация сразу подтверждается оператором.

5.4.4 Подтвержденное состояние (C) и ответ

Подтвержденное состояние аварийной сигнализации достигнуто, если оператор подтверждает условие срабатывания аварийной сигнализации после задержки подтверждения. В этом состоянии аварийная сигнализация активна. Существует несколько факторов, которые влияют на время ответа оператора, такие как:

a) скорость обработки данных в системе;

b) проект ЧМИ и его ясность;

c) знания и профессиональная подготовка оператора;

d) рабочая нагрузка оператора;

e) сложность определения конкретного действия оператора;

f) сложность выполнения конкретного действия оператора.

Фактическое время ответа на срабатывание аварийной сигнализации начинается в момент времени, когда происходит оповещение аварийной сигнализации, и заканчивается, когда оператор принимает меры по ликвидации последствий. Оно включает обнаружение аварийного сигнала, диагностирование ситуации, определение ответных действий оператора и выполнение этих действий. Верхним пределом времени ответа является допустимое время ответа, при превышении которого наступят последствия, даже если будут приняты меры по их ликвидации.

5.4.5 Возвращение в исходное неподтвержденное состояние (D)

Возвращение аварийной сигнализации в исходное неподтвержденное состояние должно происходить в результате правильных действий оператора в течение допустимого времени ответа. Существует несколько факторов, которые влияют на время возвращения аварийной сигнализации в исходное состояние, такие как:

a) задержка ответа оператора;

b) уровень принятых мер по ликвидации последствий;

c) время задержки технологического процесса, связанного с запуском ответного корректирующего действия;

d) время выполнения ответного корректирующего действия производственным процессом;

e) точность измерения в производственном процессе;

f) мертвая зона значения уставки срабатывания сигнализации;

g) скорость срабатывания системы аварийной сигнализации.

5.4.6 Порог наступления последствий

Последствия наступают, если оператор не принимает никаких мер, принятые меры некорректны или недостаточны, или действие оператора не завершено в течение допустимого времени ответа. Последствия начинают происходить при достижении порога наступления последствий.

5.5 Модель взаимодействия «оператор — производственный процесс» с обратной связью

5.5.1 Общие положения

Модель взаимодействия «оператор — производственный процесс» показана на рисунке 5. В результате помех или сбоя производственный процесс или система претерпевает некоторое изменение. Если это изменение приводит к значительному отклонению от опорной величины или от технического требования для технологического процесса, то оператор предпринимает действия, чтобы возвратить производственный процесс к опорной величине, и продолжает контролировать измерение на протяжении всего процесса возврата. Выполнение этих действий можно разделить на три этапа:

a) обнаружение отклонения от желаемого функционирования;

b) диагностика ситуации и определение корректирующих действий;

c) выполнение корректирующих действий для устранения причины отклонения.

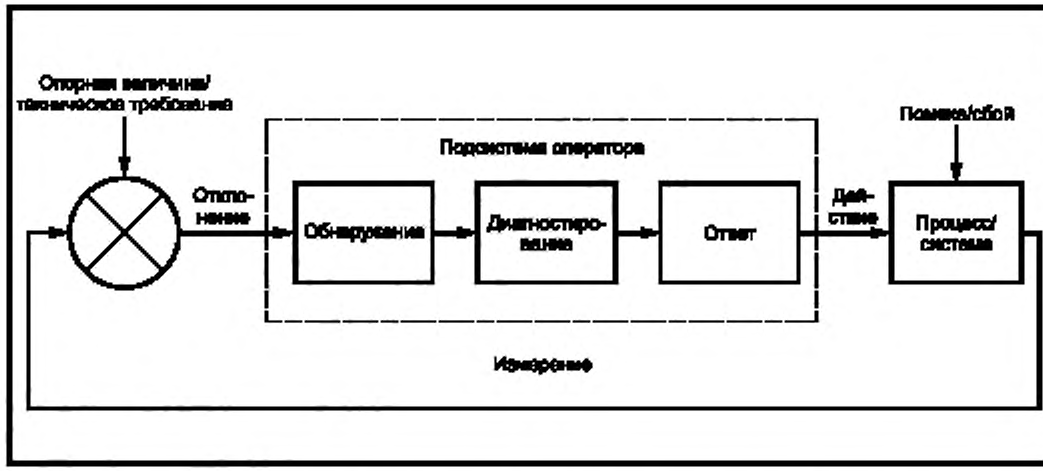

Рисунок 5 — Модель взаимодействия «оператор — производственный процесс» с обратной связью

5.5.2 Обнаружение

Аварийная сигнализация информирует оператора об отклонении от желаемого условия. Проект системы аварийной сигнализации и интерфейса оператора облегчает обнаружение отклонения.

5.5.3 Диагностирование

Оператор использует знание и навыки, чтобы интерпретировать информацию, диагностировать ситуацию и определить корректирующее действие для устранения отклонения.

5.5.4 Ответ

Оператор предпринимает меры по устранению отклонения.

5.5.5 Определяющие факторы эффективности

Способность оператора выполнить функции подсистемы зависит от множества факторов, включая рабочую нагрузку, ограничение краткосрочной или рабочей памяти, усталость, обучение и мотивацию.

6 Концепция аварийной сигнализации

6.1 Цель

Концепция аварийной сигнализации — это отдельная стадия менеджмента жизненного цикла аварийной сигнализации. Концепция аварийной сигнализации представляет собой общую схему, в рамках которой формируются критерии, определения, принципы и сферы ответственности по всем стадиям менеджмента жизненного цикла аварийной сигнализации. Это обеспечивается представленными ниже элементами, которые включают методы идентификации аварийной сигнализации, ее рационализацию, контроль, управление изменениями и аудит. Документально оформленная концепция аварийной сигнализации упрощает достижение:

a) согласованности во всей системе аварийной сигнализации;

b) согласованности с целями и задачами управления рисками;

c) соответствия передовому техническому опыту;

d) такого проекта и менеджмента системы аварийной сигнализации, который поддерживает эффективный ответ оператора.

6.2 Содержание концепции аварийной сигнализации

6.2.1 Общие положения

В подразделе 6.2 представлено минимальное и рекомендуемое содержание, концепции аварийной сигнализации. Из-за большого разнообразия оборудования, используемого в обрабатывающей

промышленности, конкретное содержание концепции аварийной сигнализации может меняться в зависимости от отрасли промышленности и от места расположения. Необходимое и рекомендуемое содержание концепции аварийной сигнализации перечислено в таблице 3.

Таблица 3 — Необходимое и рекомендуемое содержание концепции аварийной сигнализации

Содержание концепции аварийной сигнализации	Требуемое/ рекомендуемое	Пункт
Цель системы аварийной сигнализации	Требуемое	6.2.2
Определения	Требуемое	6.2.3
Ссылки	Требуемое	6.2.4
Функции и сферы ответственности при менеджменте аварийной сигнализацией	Требуемое	6.2.5
Принципы проектирования аварийной сигнализации	Требуемое	6.2.6
Рационализация	Требуемое	6.2.7
Определение класса аварийных сигналов	Требуемое	6.2.8
Наиболее важная аварийная сигнализация	Рекомендуемое	6.2.9
Принципы разработки ЧМИ	Требуемое	6.2.10
Метод установления приоритетов	Требуемое	6.2.11
Определение уставки срабатывания аварийной сигнализации	Рекомендуемое	6.2.12
Контроль производительности системы аварийной сигнализации	Требуемое	6.2.13
Техническое обслуживание системы аварийной сигнализации	Требуемое	6.2.14
Испытание системы аварийной сигнализации	Требуемое	6.2.15
Одобренные методы повышения эффективности и усовершенствования систем аварийной сигнализации	Рекомендуемое	6.2.16
Документация на аварийную сигнализацию	Требуемое	6.2.17
Руководство по внедрению	Требуемое	6.2.18
Управление изменениями	Требуемое	6.2.19
Обучение	Требуемое	6.2.20
Хранение истории аварийных сигналов	Требуемое	6.2.21
Процедуры, связанные с производственным объектом	Рекомендуемое	6.2.22
Конкретные варианты аварийной сигнализации	Рекомендуемое	6.2.23
Аудит систем аварийной сигнализации	Требуемое	6.2.24

Для систем аварийной сигнализации, разработанных для новых предприятий, концепция аварийной сигнализации должна войти в состав документов по планированию проекта и разработке и должна быть полностью сформирована и принята перед этапом рационализации аварийной сигнализации.

Для существующих систем аварийной сигнализации, в которых устраняют недостатки, и для которых не существует концепции аварийной сигнализации, стадия концепции аварийной сигнализации должна быть одной из первых стадий с мероприятиями по ликвидации недостатков.

Необходимое содержание концепции аварийной сигнализации может существовать в других процедурах объекта, на которые необходимо сослаться в этой концепции.

6.2.2 Цель системы аварийной сигнализации

Должны быть определены цель и задачи системы аварийной сигнализации обрабатывающего предприятия. Наличие четких целей и задач определяет направления действий участников при

проектировании и усовершенствовании систем. Такое определение может упростить реализацию и техническое обслуживание эффективной системы аварийной сигнализации.

6.2.3 Определения

Для гарантии взаимопонимания между всеми участниками должны быть определены термины, которые будут использовать в процессе проектирования и усовершенствования системы аварийной сигнализации.

6.2.4 Ссылки

Должен быть включен список соответствующих ссылок по менеджменту аварийной сигнализацией. Ссылки могут быть на внутренние документы компании (например, управление изменениями) или на материалы, изданные вне компании.

6.2.5 Роли и сферы ответственности в менеджменте аварийной сигнализацией

В концепции аварийной сигнализации должна быть установлена ответственность за действия при осуществлении менеджмента жизненного цикла аварийной сигнализации. Определенные вопросы, которые должны быть решены, включают:

a) кто является владельцем системы аварийной сигнализации, концепции и соответствующих документов;

b) кто несет ответственность за менеджмент и регулярное техническое обслуживание системы аварийной сигнализации;

c) кто несет ответственность за оказание технической поддержки, для решения проблем с системой аварийной сигнализации;

d) кто несет ответственность за гарантию выполнения требований, описанные в общих чертах в концепции аварийной сигнализации.

6.2.6 Принципы проектирования аварийной сигнализации

Определение аварийной сигнализации, с примерами, которые удовлетворяют и не удовлетворяют этому определению, должно быть документально оформлено в концепции аварийной сигнализации. Критерии выбора и принципы проектирования систем аварийной сигнализации должны быть согласованы с определением аварийной сигнализации.

Критерии и принципы должны определять:

a) роль системы аварийной сигнализации в идентификации подходов к опасному или неоптимальному функционированию, в предупреждении сбоев и в указании оператору на необходимые конструктивные изменения в производственном процессе;

b) методы, которые будут использоваться для идентификации аварийных сигнализаций;

c) состояние аварийной сигнализации (например, исходное, подтвержденное, отложенное и т. д.), которое будет использовать средства обработки.

6.2.7 Рационализация

Для максимального увеличения функциональности системы аварийной сигнализации очень важно, чтобы оператор получил только те аварийные сигналы, которые требуют от него ответа. Обеспечение гарантии того, что аварийная сигнализация указывает на необходимость ответа, реализовано с помощью рационализации аварийной сигнализации. В данном разделе должны быть перечислены критерии для оценки аварийной сигнализации и информация, которая будет использована во время рационализации.

Этот раздел должен дать представление о знаниях и опыте выполняющей рационализацию команды, которая должна включать специалистов в областях:

a) эксплуатации;

b) производственных процессов;

c) систем управления;

d) концепции аварийной сигнализации.

6.2.8 Определение класса аварийных сигналов

Классы аварийных сигнализаций используются для установления общих требований для управления аварийными сигнализациями. Аварийная сигнализация может принадлежать более, чем одному классу. Данный раздел должен включать определение классов аварийных сигнализаций. Он должен также включать следующие требования к классу:

a) документацию на аварийную сигнализацию;

b) обучение оператора и учебную документацию;

c) рабочие процедуры, связанные с этими аварийными сигнализациями;

d) техническое обслуживание аварийной сигнализации;

e) испытание аварийных сигналов;

f) контроль и оценка аварийной сигнализации;

g) управление изменениями аварийной сигнализации;

h) хранение истории аварийной сигнализации;

i) аудит аварийной сигнализации;

j) установление приоритетов аварийной сигнализации;

k) проект ЧМИ.

6.2.9 Наиболее важная аварийная сигнализация

Классами наиболее важных аварийных сигналов (НМА) являются классы аварийных сигналов, которые требуют большей координации и документирования, чем другие. Так как критерии могут меняться в зависимости от технологического процесса, отрасли промышленности или места нахождения, то концепция аварийной сигнализации должна определить критерии включения аварийных сигналов в классы НМА, если классы НМА будут использоваться. Обозначение классов аварийных сигнализаций, как наиболее важных, должно быть основано на одном или нескольких из следующих положений:

a) аварийные сигнализации, критические для безопасности технологического процесса при защите человеческой жизни (например, аварийные сигнализации системы безопасности);

b) аварийные сигнализации по безопасности или защите персонала;

c) аварийные сигнализации, связанные с охраной окружающей среды;

d) аварийные сигнализации в текущей надлежащей производственной практике;

e) аварийные сигнализации в области коммерческих потерь;

f) аварийные сигнализации, связанные с обеспечением качества изделия;

g) аварийные сигнализации, связанные с требованиями компании лицензиара технологического процесса;

h) аварийные сигнализации, связанные с политикой компании.

Если используются классы НМА, то в данном разделе концепции аварийной сигнализации должны быть документально оформлены требования для этих классов аварийных сигнализаций.

6.2.10 Принципы разработки ЧМИ

Документально оформляя метод, формат и кодирование (например, цвет, символы и алфавитно-цифровое кодирование) для представления аварийных сигналов оператору, устанавливают принципы для их отображения и оповещения так, чтобы они были единообразными по всему предприятию.

Конкретные элементы, которые должны быть охвачены данным разделом, включают:

a) механизм, используемый (например, информационное табло, экраны пульта управления ОСУТП и т. д.) для сообщения оператору об аварийных сигналах;

b) рекомендации по индикации состояний аварийных сигнализаций на ЧМИ (например, исходное, подтвержденное, отложенное и т. д.), которые будут использоваться на предприятии;

c) типы используемых отображений на экране (например, общая сводка аварийных сигнализаций, в порядке поступления и т. д.);

d) функции, которые будут доступны в ЧМИ, включая откладывание и запрещение.

6.2.11 Метод установления приоритетов

Последовательные приоритеты помогают оператору определить порядок ответа в период высокой интенсивности аварийных сигналов. Конкретные элементы, которые должны быть охвачены данным разделом, включают:

a) основание для установления приоритетов аварийных сигнализаций (например, серьезность последствия, время ответа и т. д.);

b) метрики для конфигурации аварийных сигнализаций (например, распределение количества и приоритета аварийных сигналов);

c) влияние классификации на установление приоритетов.

6.2.12 Определение уставки срабатывания аварийной сигнализации

Данный раздел должен содержать указания по методам, используемым для определения уставок срабатывания аварийной сигнализации.

6.2.13 Контроль производительности системы аварийной сигнализации

Для контроля производительности системы аварийной сигнализации на соответствие целевым уровням качества используются метрики. Настоящий раздел является основным для оценки производительности, чтобы решить, требуются ли усовершенствования.

Конкретные элементы, которые должны быть охвачены настоящим разделом, включают:

a) цель контроля и оценки;

b) метрики контроля и целевые значения;

c) руководящие указания по выбору частоты выполнения анализа производительности системы аварийной сигнализации;

d) руководящие указания по выбору подхода для повышения производительности согласно определенным метрикам.

6.2.14 Техническое обслуживание системы аварийной сигнализации

Данный раздел определяет действия, необходимые для технического обслуживания системы аварийной сигнализации. Конкретные элементы, которые должны быть охвачены данным разделом, включают:

a) ведение учета технического обслуживания системы аварийной сигнализации;

b) требования к аварийным сигнализациям для их вывода из эксплуатации;

c) политика использования временных аварийных сигнализаций.

6.2.15 Испытание системы аварийной сигнализации

Данный раздел определяет процедуры, обеспечивающие последовательное и соответствующее испытание системы аварийной сигнализации на всем ее жизненном цикле. Используемые при испытаниях возможности применения, критерии, методы и частота должны быть полностью документально оформлены для классов аварийных сигналов.

6.2.16 Одобренные методы повышения эффективности и усовершенствования систем аварийной сигнализации

Должны быть определены одобренные для применения методы повышения эффективности и усовершенствования систем аварийной сигнализации и условия или критерии их использования. Персонал должен пройти обучение по применению этих методов.

Методы повышения эффективности и усовершенствования систем аварийной сигнализации (см. раздел 12) будут использоваться не везде. Но если такие методы используются, то в концепции аварийной сигнализации данный раздел должен присутствовать, чтобы определить эти методы и связанные с ними выполняемые функции и рабочие процессы.

6.2.17 Документация на аварийную сигнализацию

В концепции аварийной сигнализации должна быть представлена соответствующая документация, которая может включать:

a) информацию о рационализации (например, общая база данных аварийных сигналов);

b) периодические отчеты о работе аварийной сигнализации;

c) технические требования к усовершенствованным методам управления аварийной сигнализацией;

d) технические требования к процедуре запрещения в соответствии с проектом.

Необходимость в другой документации может быть определена требованиями различных классов аварийных сигнализаций.

Соответствующая документация гарантирует, что усовершенствованные методы выполняются единообразно, обеспечивая ожидаемые схемы поведения для оператора во всех режимах работы.

6.2.18 Руководство по внедрению

Определение основного подхода для начальной подготовки персонала, ввода в действие и отладки системы аварийной сигнализации упрощает согласованность по всему предприятию или компании. Это гарантирует эффективное внедрение системы аварийной сигнализации.

6.2.19 Управление изменениями

В данном разделе определяются типы изменений и применимые для них процедуры. Управление процедурой изменения должно быть документально оформлено. Типы изменений могут включать:

a) временные изменения аварийных сигнализаций (например, вывод их из обслуживания);

b) постоянные изменения в общей базе данных аварийных сигналов, атрибутов аварийных сигналов или методов повышения эффективности и усовершенствования систем аварийной сигнализации.

Постоянные изменения выполняются под управлением процедуры изменения, чтобы гарантировать, что изменения, внесенные во время проектирования, внедрения, эксплуатации или технического обслуживания, были соответственно оценены и одобрены уполномоченными подразделениями и документально оформлены. Как правило, эти документы включают информацию о результатах оценки каждого изменения и отчеты о модификациях системы, и разрешение на выполнение изменения.

6.2.20 Обучение

Данный раздел определяет чему должен быть обучен персонал предприятия, чтобы он мог использовать, управлять и проектировать системы аварийной сигнализации. В данном разделе также определены требования к учебной документации.

Конкретные вопросы обучения, которые должны быть рассмотрены в концепции аварийной сигнализации или в другой эквивалентной документации для каждого из класса аварийных сигнализаций, включают:

a) должностные роли или персонал, требующий обучения по системам аварийной сигнализации;

b) краткий обзор содержания учебного материала;

c) когда требуется обучение.

6.2.21 Хранение истории аварийных сигналов

Данный раздел определяет какая информация из «истории» аварийной сигнализации (например, статус оповещения, статус подтверждения, возвращение в исходное состояние и действия оператора) должна быть сохранена, а также срок ее хранения (например, период инцидента, время нарушения безопасных эксплуатационных ограничений). В некоторых отраслях промышленности и регионах органы власти или местные законы могут потребовать сохранения этой информации.

6.2.22 Процедуры, связанные с производственным объектом

Чтобы избежать несоответствий между концепцией аварийной сигнализации и другими процедурами производственного объекта, концепция аварийной сигнализации должна содержать соответствующие процедуры производственного объекта. Следующие документы могут быть связаны с концепцией аварийной сигнализации:

a) стандартные рабочие процедуры;

b) политика и руководства по обучению оператора;

c) процедуры безопасности, охраны здоровья и экологии;

d) правила технического обслуживания;

e) политика, нормы и правила обработки аварийной сигнализации;

f) рекомендации по прикладному программированию,

g) ввод в действие или квалификационные процессы и процедуры;

h) процедура управления изменениями;

i) другие процедуры производственного объекта, связанные с концепцией аварийной сигнализации и зависящие от конкретного производственного объекта.

6.2.23 Конкретные варианты аварийной сигнализации

Документ с концепцией аварийной сигнализации должен определять правила и методы для проектирования аварийной сигнализации, охватывающей конкретные ситуации, где очень важна согласованность (например, аварийных сигналов байпаса от аварийных сигналов от резервных датчиков). Классы аварийных сигналов могут быть источником таких конкретных вариантов.

6.2.24 Аудит систем аварийной сигнализации

Документ с концепцией аварийной сигнализации должен определить требования к управлению периодическими аудитами аварийной сигнализации. Эти требования могут включать.

a) частоту аудита, которая может быть определена на основе класса аварийной сигнализации;

b) тематику аудита;

c) технологию опросов оператора.

6.3 Разработка и поддержка концепции аварийной сигнализации

Персонал, применяющий концепцию аварийной сигнализации, должен быть вовлечен в ее развитие. Вовлеченная команда должна располагать детальным знанием и пониманием проектирования, эксплуатации и технического обслуживания технологического процесса, связанного с производственным объектом. Конкретные области экспертных знаний включают:

a) технологические операции;

b) приборное обеспечение процесса;

c) системы управления;

d) производственные технологии;

e) технология машиностроения/обеспечения надежности;

f) безопасность, охрана здоровья и экологии;

g) безопасность производства;

h) человеческий фактор;
i) управление аварийной сигнализацией;
j) процесс управления изменениями.

7 Спецификация требований к системам аварийной сигнализации

7.1 Цель

Спецификация требований к системам аварийной сигнализации (ASRS), которую можно также назвать спецификацией функциональных требований к аварийной сигнализации, является частью стадии концепции жизненного цикла аварийной сигнализации. Данный раздел дает представление о развитии и использовании спецификации требований системы аварийной сигнализации. В ASRS документально оформлена функциональность аварийной сигнализации, выполнение которой планируется системой управления. ASRS часто является подмножеством полной спецификации системных требований системы управления.

Спецификация требований к системам аварийной сигнализации, как правило, зависит от конкретного производственного объекта, отдельной системы управления или группы подобных систем управления. Хотя ASRS согласуется с концепцией аварийной сигнализации, но она содержит более подробные функциональные требования системы аварийной сигнализации, по сравнению с концепцией, так как включает подробные требования пользователей и рассматривает соответствующие требования инфраструктуры производственного объекта. Эти требования используются, чтобы помочь оценить системы, вести детальное проектирование систем и служат первичной основой для испытания функций систем аварийной сигнализации во время их внедрения. Важно отличить ASRS от действий отдельной аварийной сигнализации, которые происходят на последующих стадиях жизненного цикла системы. ASRS определяет какая функциональность системы аварийной сигнализации должна быть обеспечена в процессе ее рационализации, проектирования, внедрения, визуализации и записи отдельных аварийных сигналов, а также при анализе их записей.

ASRS, как правило, формируются на ранней стадии при планировании новой системы управления. Они обновляются на стадии внедрения, чтобы гарантировать согласованность с целевыми возможностями выбранной системы, и поэтому важны для улучшения проектирования системы, испытаний системы и мероприятий по подготовке персонала. ASRS обычно не обновляются после внедрения системы. Изменения функциональности системы аварийной сигнализации могут происходить в течение всего жизненного цикла системы. Этими изменениями можно управлять и их можно документально оформлять средствами управления изменениями.

7.2 Рекомендации

Планирование новых систем управления и основных версий функциональности аварийной сигнализации для существующих систем управления должно включать ASRS, содержащую все или некоторые из перечисленных технических требований:

a) атрибуты аварийной сигнализации;
b) ЧМИ аварийной сигнализации;
c) протокол связи аварийной сигнализации;
d) ведение журнала записей срабатывания аварийной сигнализации;
e) анализ записей срабатывания аварийной сигнализации;
f) другие меры, которые облегчают действия в течение жизненного цикла аварийной сигнализации.

Может возникнуть новый проект системы управления, в котором определено, что в ASRS нет необходимости (например, копируя существующие системы). Решение не использовать ASRS и объяснение такого решения должно быть документально оформлено.

7.3 Разработка

Система аварийной сигнализации является только одной из функциональных систем в системе управления, и производительность всей системы может потребовать компромисса для требований системы аварийной сигнализации. Концепции аварийной сигнализации содержат руководство, которое может использоваться для формирования части спецификации требований, относящейся к системе аварийной сигнализации. Такие ASRS должны включать:

a) доступные приоритеты аварийных сигналов;
b) функциональность видимого оповещения, такая как цвета и символы;
c) функциональность звукового оповещения срабатывания аварийной сигнализации;
d) функциональность демонстрации отчета по срабатыванию аварийных сигнализаций;
e) функциональность откладывания срабатывания аварийной сигнализации;
f) функциональность запрещения срабатывания аварийной сигнализации;
g) функциональность конфигурации аварийной сигнализации (например, формирующая мертвую зону, задержку включения и задержку выключения);
h) журнал регистрации функциональных возможностей аварийной сигнализации;
i) функциональность контроля и оценки аварийной сигнализации;
j) функциональность аудита системы аварийной сигнализации;
k) функциональность усовершенствования систем аварийной сигнализации.

Примечание — Некоторые требования к аварийной сигнализации могут существовать в других документах, в таких как спецификация требований к безопасности для применения ПСБ, которая определена в МЭК 61511.

7.4 Оценка систем

Функциональность системы аварийной сигнализации должна быть оценена на соответствие требованиям во время выбора системы управления. Функциональность системы аварийной сигнализации систем управления варьируется от очень ограниченной до очень развитой. Спецификация требований к системе аварийной сигнализации предоставляет список определенных критериев, которые могут способствовать сравнительной оценке различных систем.

7.5 Настройка

Если стандартные коммерческие изделия не удовлетворяют важным требованиям к системе из-за ее спецификации, то возникает необходимость в разработке настраиваемых решений или в пересмотре спецификации. Спецификация требований к системе аварийной сигнализации позволяет на более ранней стадии признать необходимость в индивидуальных решениях и может инициировать для них функционально-стоимостный анализ.

7.6 Требования к испытанию системы аварийной сигнализации

Каждое требование к системе аварийной сигнализации должно быть подвергнуто испытаниям до стадии ее эксплуатации.

8 Идентификация

8.1 Цель

Идентификация является отдельным этапом жизненного цикла системы аварийной сигнализации. Идентификация — это общий термин для различных методов, которые могут использоваться, чтобы определить возможную востребованность в системе аварийной сигнализации или в изменении системы аварийной сигнализации. Стадия идентификации является начальной стадией жизненного цикла систем аварийной сигнализации, на которой рекомендуются модели аварийных сигнализаций или изменения к существующим аварийным сигнализациям. Информация об идентифицированных аварийных сигнализациях является входной для стадии рационализации.

8.2 Методы идентификации аварийных сигнализаций

Настоящий стандарт не определяет и не требует применения какого-либо конкретного метода для идентификации аварийной сигнализации. Аварийные сигналы могут быть идентифицированы за счет ряда передовых технических методов или требований стандартов. Для определения возможных аварийных сигналов должна использоваться некоторая комбинация методов идентификации. Идентификация аварийной сигнализации может быть выполнена во время рационализации аварийной сигнализации, где это необходимо.

Некоторые общие методы идентификации аварийной сигнализации:

a) распределение слоев безопасности;

b) анализ опасностей технологического процесса (PHA);
c) исследование опасности и работоспособности (HAZOP);
d) анализ слоев защиты (LOPA);
e) расследования происшествий;
f) природоохранные разрешения;
g) анализ видов и последствий отказов (FMEA);
h) современная надлежащая производственная практика (cGMP);
i) проверки качества;
j) экспертизы P&ID;
k) проверки рабочих процедур;
l) рекомендации производителя для блоков оборудования.

8.3 Обучение идентификации

Персонал, использующий любой метод для идентификации аварийной сигнализации, должен пройти обучение по концепции аварийной сигнализации и по критериям оценки аварийных сигналов.

9 Рационализация

9.1 Цель

Рационализация является отдельным этапом жизненного цикла системы аварийной сигнализации. Во время рационализации существующие или возможные аварийные сигналы систематически сравниваются с критериями аварийных сигналов, сформулированными в концепции аварийной сигнализации. Если рассматриваемая аварийная сигнализация соответствует критериям, то уставки срабатывания сигнализации, ее последствия и действие оператора оформляются документально, а для аварийной сигнализации определяется приоритет и она классифицируется согласно концепции аварийной сигнализации.

На стадии рационализации формируется подробная информация о проекте, необходимая на стадии проектирования жизненного цикла системы аварийной сигнализации.

На стадии рационализации должно быть определено и документально оформлено для каждой аварийной сигнализации, рационализированной в соответствии с концепцией аварийной сигнализации и для каждого предприятия, отвечающего данному применению состояния, как минимум следующее:

a) тип аварийной сигнализации;
b) приоритет;
c) класс;
d) уставка срабатывания сигнализации или логическое условие (например, в случае аварии);
e) действие оператора;
f) последствие бездействия или неправильного действия;
g) вероятная причина;
h) необходимость в методах усовершенствования систем аварийной сигнализации при необходимости.

9.2 Документация на этапе рационализации

9.2.1 Требования к документации на этапе рационализации

Документация на этапе рационализации для каждой аварийной сигнализации должна содержать следующее:

a) тип аварийной сигнализации;
b) приоритет;
c) класс,
d) уставка срабатывания аварийной сигнализации или логическое условие (например, в случае аварии);
e) действие оператора;
f) последствие бездействия или неправильного действия.

9.2.2 Документально оформленные рекомендации на этапе рационализации

Документация на этапе рационализации для каждой аварийной сигнализации должна содержать следующее:

a) максимальное допустимое время ответа;

b) возможная причина;

c) метод идентификации;

d) необходимость в методах усовершенствования систем аварийной сигнализации при необходимости.

9.3 Обоснование аварийной сигнализации

9.3.1 Процесс обоснования аварийной сигнализации

Каждая аварийная сигнализация, требующая рационализации, для ее подтверждения сравнивается с критериями, представленными в концепции аварийной сигнализации.

Критерии, соответствующие определению аварийной сигнализации, включают:

a) аварийная сигнализация предназначена оператору;

b) аварийная сигнализация указывает на отклонение в технологическом процессе, аномальное условие или сбой оборудования;

c) аварийная сигнализация требует своевременной реакции.

9.3.2 Подход к обоснованию

Процесс обоснования аварийной сигнализации должен:

a) использовать командный подход;

b) полагаться в большой степени на вмешательство оператора;

c) сосредоточить внимание на действии оператора, которое будет предложено.

9.3.3 Обоснование отдельной аварийной сигнализации

В процессе рационализации все аварийные сигнализации систематически анализируются. Обычно это делается с использованием конструкторской документации, баз данных или выводов данных на экран ЧМИ. Информация, которая будет связана с каждой рационализированной аварийной сигнализацией, должна быть определена в концепции аварийные сигнализации и, как правило, включать:

a) проверку того, что рассматриваемая аварийная сигнализация соответствует критериям аварийной сигнализации, представленным в концепции аварийной сигнализации;

b) ответное действие (действия), которое оператор может выполнить;

c) последствие, которое произойдет, если действие не будет выполнено или его выполнение окажется неудачным;

d) время между оповещением срабатывания аварийной сигнализации и возникновением соответствующего последствия.

Должны быть рассмотрены те аварийные сигналы, для которых ответ оператора заключается только в простой передаче информации соответствующему лицу или группе лиц для выполнения ими действия (например, при аварийной сигнализации — диагностики прибора) для того, чтобы определить, существует ли дополнительный метод передачи информации, не загружающий оператора или систему сигнализации.

9.3.4 Влияние на систему аварийной сигнализации

Обоснование аварийной сигнализации должно гарантировать, что:

a) срабатывание конкретной аварийной сигнализации не является ложным;

b) аварийная сигнализация не дублирует другую аварийную сигнализацию, на которую оператор реагирует тем же действием.

Чтобы предотвратить негативное воздействие на систему аварийной сигнализации могут быть определены методы усовершенствования систем аварийной сигнализации (например, аварийная сигнализация, основанная на состояниях, или аварийные сигнализации, основанные на логике).

9.4 Определение уставки срабатывания сигнализации

Для определения уставок срабатывания сигнализации, определенных в концепции аварийной сигнализации, применяется руководство. Эффективные методы учитывают допустимое время ответа (см. рисунок 5), сложность действия оператора, знания о технологическом процессе и хронологию, а также другие факторы.

9.5 Установление приоритетов

Для распределения приоритетов рационализированным аварийным сигнализациям используется метод назначения приоритетов, определенный в концепции аварийной сигнализации. Эффективное

установление приоритетов, как правило, приводит к тому, что аварийные сигнализации с более высоким приоритетом, выбираются менее часто, чем аварийные сигнализации с более низким приоритетом. Большинству аварийных сигнализаций должен быть назначен достаточно низкий приоритет (менее важные аварийные сигнализации), а меньшему количеству аварийных сигнализаций — более высокий приоритет (наиболее важные аварийные сигнализации) с возможным обоснованным переходом между ними. Получаемый аварийными сигнализациями приоритет должен соответствовать определенным последствиям и допустимому времени ответа так, что аварийная сигнализация с самым низким приоритетом должна быть связана с наименее серьезным последствием и иметь наиболее длительное допустимое время ответа, а аварийная сигнализация с самым высоким приоритетом должна быть связана с самым серьезным последствием (например, аварийные сигналы о пожарной и газовой опасности) и иметь самое короткое допустимое время ответа. Метрики распределения приоритета рассмотрены в разделе 16.

Установление приоритетов может включать рассмотрение классов аварийных сигнализаций (например, классов наиболее важных аварийных сигнализаций) или методов идентификации (например, LOPA) при установлении приоритета аварийной сигнализации.

9.6 Удаление

Существующие аварийные сигнализации, которые не соответствуют критериям аварийной сигнализации, представленным в концепции аварийной сигнализации, должны быть документально оформлены вместе с обоснованием (т. е. с указанием критерия, которому они не соответствуют) их удаления. С такими аварийными сигнализациями далее должна работать процедура управления изменениями, чтобы удалить их из системы.

9.7 Классификация

Классификация является деятельностью, выполняемой полностью на стадии рационализации жизненного цикла системы аварийной сигнализации. Аварийные сигнализации должны быть отнесены к одному или нескольким классам, как определено в концепции аварийной сигнализации.

Для аварийных сигнализаций, относящихся к одному и тому же классу, не требуется, чтобы они имели одинаковый приоритет. Классификация может происходить до, во время, или после выполнения обоснования аварийной сигнализации и установления ее приоритета.

9.8 Анализ

При завершении начального обоснования, установления приоритетов и классификации всех необходимых аварийных сигнализаций эти результаты должны быть проанализированы, чтобы гарантировать согласованное применение критериев на всем производственном процессе. Результаты необходимо сравнить с любыми целями и приоритетом аварийных сигнализаций, которые могли бы быть установлены в концепции аварийной сигнализации.

9.9 Использование документации

Результаты рационализации должны быть документально оформлены, они являются основанием для обеспечения целостности системы аварийной сигнализации. Документация (например, общая база данных аварийных сигналов) описывает связь между каждой аварийной сигнализацией и концепцией аварийной сигнализации и может использоваться для ряда целей, включая:

a) вход в стадию детального проектирования жизненного цикла системы аварийной сигнализации;

b) использование системы в составе управления изменениями;

c) обучение и обзор операторов;

d) периодический аудит и согласование параметров настройки аварийной сигнализации системы управления;

e) оценка контроля аварийной сигнализации и данных об эффективности.

10 Детальное проектирование. Технический проект системы аварийной сигнализации

10.1 Цель

Технический проект системы аварийной сигнализации является частью стадии детального проектирования жизненного цикла системы аварийной сигнализации. В данном разделе представлены специальные требования к реализации аварийных сигнализаций, определенных в процессе рационализации для конкретной системы управления. В данном разделе рассматриваются вопросы разработки, связанные со срабатыванием аварийных сигнализаций. Все вопросы разработки, связанные с представлением аварийных сигнализаций, содержатся в разделе 11.

10.2 Использование состояний аварийной сигнализации

10.2.1 Состояние срабатывания аварийной сигнализации

Источник для каждой аварийной сигнализации в системе должен быть документально оформлен. Изменения состояния аварийной сигнализации могут быть запущены из различных источников в системе управления, как показано в рисунке 1, включая:

a) полевое устройство (например, датчики и исполнительные элементы);
b) систему управления и безопасности;
c) ЧМИ.

10.2.2 Состояния аварийной сигнализации и другие логические функции

Для использования информации о состоянии аварийной сигнализации для других логических функций (например, для блокирующих действий) должно быть обеспечено ясное руководство по проектированию. Если уставки срабатывания сигнализации будут использоваться в дополнение к оповещению оператора (например, как уставка блокирования), то это может повлиять на документацию, обучение и управление изменениями. Кроме того, влияние изменения атрибутов аварийных сигнализаций, а также использование спроектированного запрещения должно быть ясно определено, документально оформлено и по возможности ограничено (например, требованием дополнительного подтверждения или более высокого уровня доступа). Эта информация должна быть специально документально оформлена в концепции аварийной сигнализации в виде принципов разработки аварийной сигнализации.

10.2.3 Запрещение аварийной сигнализации и другие логические функции

Функциональность запрещения аварийной сигнализации не должна обходить другие логические функции (например, блокирующие действия).

10.3 Типы аварийных сигнализаций

Тип аварийной сигнализации должен быть назначен для каждой аварийной сигнализации, определенной во время рационализации. Тип аварийной сигнализации определяется, чтобы дать возможность оператору визуально различать аварийные сигналы. К общим типам аварийных сигнализаций можно отнести:

a) абсолютные аварийные сигнализации;
b) аварийные сигнализации по отклонению;
c) аварийные сигнализации о скорости изменения;
d) аварийные сигнализации по расхождению;
e) аварийные сигнализации, управляемые расчетом;
f) аварийные сигнализации, управляемые набором правил;
g) аварийные сигнализации, управляемые битовым шаблоном;
h) аварийные сигнализации, использующие выход контроллера;
i) аварийные сигнализации от системы диагностики;
j) аварийные сигнализации диагностики прибора;
k) регулируемые аварийные сигнализации;
l) адаптивные аварийные сигнализации;
m) аварийные сигнализации с повторяющимся аварийным сигналом;
n) аварийные сигнализации, основанные на статистике;
o) аварийные сигнализации, обрабатываемые в порядке поступления;
p) аварийные сигнализации о дефектных измерениях.

В систему управления включают различные типы аварийных сигнализаций. Может возникнуть необходимость в создании специального типа аварийной сигнализации, который будет частью работ по проектированию системы управления.

Типы аварийных сигнализаций должны быть тщательно отобраны на основе технического обоснования. При нарушении нормальных условий эксплуатации, если аварийные сигнализации несоответственно применены, некоторые типы, такие как аварийные сигнализации о скорости изменения, об отклонении, о дефектных измерениях и аварийные сигнализации, использующие выход контроллера, являются общими источниками ложных аварийных сигналов.

10.4 Атрибуты аварийной сигнализации

10.4.1 Общие положения

В процессе выполнения технического проекта атрибуты аварийной сигнализации должны формироваться по умолчанию для каждой аварийной сигнализации, которая была определена на стадии рационализации и установлена на основе технического обоснования. Атрибуты, такие как уставка срабатывания и мертвая зона, могут отличаться в зависимости от конкретного типа реализуемой аварийной сигнализации. Определение соответствующих атрибутов аварийной сигнализации может помочь минимизировать количество ложных аварийных сигналов, которые возникают в процессе эксплуатации. Рекомендации для проектирования конкретных атрибутов аварийной сигнализации предоставлены в следующих пунктах. Атрибутами аварийной сигнализации являются:

a) уставка срабатывания аварийной сигнализации или логические условия;
b) тип аварийной сигнализации;
c) приоритет аварийной сигнализации;
d) группа аварийных сигналов;
e) задержка включения или задержка выключения;
f) мертвая зона;
g) сообщение об аварийной ситуации.

10.4.2 Описание аварийной сигнализации

Все аварийные сигнализации должны иметь информативный текст в виде описания маркировки атрибута, или описания аварийной сигнализации, или оба описания. При этом рекомендуется использовать структурированное представление и согласованные формулировки.

10.4.3 Уставки срабатывания аварийной сигнализации

Уставки срабатывания аварийной сигнализации должны формироваться на основе документально оформленной информации в общей базе данных аварийных сигналов.

10.4.4 Приоритет аварийной сигнализации

Приоритет аварийной сигнализации должен быть назначен на основе документально оформленной информации в общей базе данных аварийных сигналов.

10.4.5 Мертвые зоны аварийной сигнализации

10.4.5.1 Общие положения

Мертвая зона аварийной сигнализации является ее атрибутом в системе управления, которая требует, чтобы значение параметра технологического процесса пересекало значение уставки срабатывания сигнализации в рабочем диапазоне эксплуатации с некоторым определенным шагом или процентным значением от этого диапазона. Мертвые зоны, как правило, устанавливаются на основе рабочего диапазона эксплуатации параметра технологического процесса, ошибки измерения и типа параметра технологического процесса. Применение мертвых зон может быть очень эффективным при устранении ложных аварийных сигналов.

10.4.5.2 Требования к мертвой зоне аварийной сигнализации

Система управления должна обеспечить способность реализации функциональных возможностей мертвой зоны.

10.4.5.3 Рекомендации для мертвой зоны аварийной сигнализации

Конструкторско-технологическое обоснование для установления мертвой зоны должно быть документально оформлено в концепции аварийной сигнализации. При установлении мертвой зоны необходимо использовать техническую оценку, чтобы минимизировать ложные аварийные сигналы, поддерживая при этом контроль технологического процесса и безопасность предприятия/персонала. Чрезмерно большая мертвая зона, т. е. такая, при которой вычисления могут быть выполнены приборами с большим диапазоном (например, от 0 до 100), может действовать как замок, создавая про-

сроченное срабатывание аварийной сигнализации. Параметры настройки должны быть документально оформлены и затем проверены во время ввода в действие и после длительной эксплуатации.

10.4.6 Задержка включения и задержка выключения аварийной сигнализации

10.4.6.1 Общие положения

Атрибуты задержки включения и задержки выключения (т. е. устраняющий дребезг таймер), могут использоваться для устранения ложных аварийных сигналов. Задержка включения используется, чтобы избежать ненужных аварийных сигналов, когда значение сигнала временно выходит за установленные пределы значений своей заданной уставки, таким образом препятствуя вызову аварийной сигнализации, пока сигнал не оказывается в постоянном состоянии аварийной сигнализации в течение заданного отрезка времени. Задержка выключения используется, чтобы сократить дребезжащие аварийные сигналы, блокируя индикацию аварийной сигнализации на некоторый определенный период времени после того, как условие технологического процесса возвратится в исходное состояние.

10.4.6.2 Требования к задержке включения и задержке выключения аварийной сигнализации

Система управления должна обеспечить способность реализации функциональных возможностей задержки включения и задержки выключения.

10.4.6.3 Рекомендации для задержки включения и задержки выключения аварийной сигнализации

При установлении задержки включения и задержки выключения необходимо выполнить техническую оценку, чтобы минимизировать ложные аварийные сигналы, поддерживая при этом контроль технологического процесса и безопасность предприятия/персонала.

Времена рассматриваемых задержек должны учитывать время реакции технологического процесса для всех режимов эксплуатации, а также учитывать применяется ли фильтрация для уменьшения шума сигнала. Времена задержек включения должны применяться только после тщательной оценки возможных влияний системы управления в процессе эксплуатации. Параметры настройки должны быть проверены во время ввода в действие и после длительной эксплуатации.

10.5 Программные изменения атрибутов аварийной сигнализации

Для некоторых производственных объектов приходится изменять атрибуты аварийной сигнализации, если учитывать условия, такие как пакетный режим, тип изделия или марка. Далее перечислены возможные, обычно используемые источники изменения атрибутов аварийной сигнализации:

a) интерфейс оператора (например, ручные изменения во время эксплуатации);

b) инженерный интерфейс (например, изменения в проекте, выполняемые под управлением изменениями);

c) логика управления (например, последовательности, стадии);

d) методы усовершенствования систем аварийной сигнализации;

e) внешний источник по отношению к системе управления [например, система управления производством (MES), система планирования ресурсов предприятия (ERP)].

Концепция аварийной сигнализации должна детализировать использование и ограничения этой функциональности. Для каждой аварийной сигнализации пользователь должен определить и документально оформить перечень программ системы, имеющих доступ для изменения атрибутов аварийной сигнализации во время эксплуатации и перечень изменений выполненных процедурами управления изменениями. Методы усовершенствования систем аварийной сигнализации, применяемые для изменения атрибутов аварийной сигнализации, рассмотрены в разделе 12.

10.6 Анализ технического проекта системы аварийной сигнализации

Типичная система управления предоставляет пользователю возможность реализовать большее количество различных типов аварийных сигнализаций для одной переменной технологического процесса. Чтобы минимизировать нагрузку аварийных сигналов на оператора, результаты технического проекта системы аварийной сигнализации необходимо сравнить с общей базой данных аварийных сигналов, чтобы гарантировать существование только необходимых аварийных сигналов.

11 Детальное проектирование. Проектирование человеко-машинного интерфейса для систем аварийной сигнализации

11.1 Цель

Проектирование ЧМИ для систем аварийной сигнализации является частью стадии детального проектирования жизненного цикла систем аварийной сигнализации. В данном разделе описана функциональность, обеспечивающая индикацию аварийных сигнализаций и связанных с ними функций оператору и другим пользователям ЧМИ. Индикация и отображение аварийных сигнализаций является только одним из компонентов в проекте ЧМИ, но способствуют эффективному взаимодействию оператора с производственным процессом (см. рисунок 5). Руководящие указания по проектированию полного ЧМИ для систем управления не входят в область применения настоящего стандарта.

11.2 Функции человеко-машинного интерфейса

11.2.1 Общие положения

Проект ЧМИ для систем аварийной сигнализации должен быть согласован с концепцией аварийной сигнализации и общим подходом к проектированию ЧМИ. При проектировании ЧМИ должны быть рассмотрены возможности системы управления.

11.2.2 Требования к информации ЧМИ

ЧМИ должен ясно указывать на:

a) активные аварийные сигнализации;

b) состояния аварийных сигнализаций;

c) приоритеты аварийных сигнализаций;

d) типы аварийных сигнализаций.

11.2.3 Функциональные требования к ЧМИ

ЧМИ должен обладать способностью обеспечить оператору:

a) заглушенные звуковые индикации аварийной сигнализации (т. е. аварийную сигнализацию без подтверждения);

b) подтвержденные аварийные сигнализации;

c) вывод аварийных сигнализаций из обслуживания с помощью методов с управляемым доступом в соответствии с концепцией аварийной сигнализации;

d) изменение атрибутов аварийных сигнализаций только с помощью методов с управляемым доступом;

e) запуск функции, реализующей состояние отложенной аварийной сигнализации;

f) демонстрацию сообщений аварийных сигнализаций,

g) назначение аварийных сигнализаций рабочим станциям оператора.

11.2.4 Требования к отображению ЧМИ

ЧМИ должен обеспечить возможность для следующих или эквивалентных отображений:

a) общей сводки аварийных сигнализаций;

b) индикации аварийных сигнализаций на технологическом процессе;

c) индикации аварийных сигнализаций на подробном отображении тега;

d) общей сводки отложенных аварийных сигнализаций;

e) общей сводки выведенных из обслуживания аварийных сигнализаций.

11.2.5 Требования к записям об аварийной сигнализации

Записью об аварийной сигнализации является набор информации, который документально фиксирует изменение состояния аварийной сигнализации.

Запись об аварийной сигнализации должна иметь следующие атрибуты:

a) имя тега аварийной сигнализации;

b) описание тега аварийной сигнализации или описание аварийной сигнализации;

c) состояние аварийной сигнализации;

d) приоритет аварийной сигнализации;

e) тип аварийной сигнализации;

f) время и дата возникновения изменения состояния аварийной сигнализации.

11.2.6 Рекомендации к записям об аварийной сигнализации

Запись об аварийной сигнализации должна иметь следующие элементы:

a) значение технологического параметра в то время, когда выполняется запись аварийной сигнализации;

b) уставка аварийной сигнализации;
c) производственная зона;
d) группа аварийной сигнализации;
e) сообщение аварийной сигнализации.

11.3 Индикации состояний аварийной сигнализации

11.3.1 Общие положения

Состояния аварийных сигнализаций определяет диаграмма переходов состояний аварийной сигнализации (см. рисунок 3).

11.3.2 Необходимые индикации состояний аварийной сигнализации

Комбинация визуальных индикаторов, звуковых индикаторов или тех и других должна использоваться, чтобы однозначно различать следующие состояния аварийной сигнализации:

a) исходное;
b) неподтвержденная аварийная сигнализация;
c) подтвержденная аварийная сигнализация;
d) возвращенная в исходное неподтвержденное состояние аварийная сигнализация;
e) отложенная аварийная сигнализация;
f) запрещенное проектом состояние аварийной сигнализации;
g) выведенная из обслуживания аварийная сигнализация.

11.3.3 Рекомендуемые индикации состояний аварийной сигнализации

11.3.3.1 Общие положения

Следующие рекомендуемые индикации состояний аварийной сигнализации являются общей промышленной практикой.

11.3.3.2 Индикация исходного состояния

Исходное состояние не должно использовать звуковую индикацию. Визуальная индикация исходного состояния должна совпасть с индикациями без аварийных сигнализаций.

11.3.3.3 Индикация состояния неподтвержденной аварийной сигнализации

Состояние неподтвержденной аварийной сигнализации должно использовать как звуковую индикацию, так и визуальную индикацию. Звуковая индикация должна быть прекращена после действия оператора по отключению звука или по подтверждению аварийной сигнализации. А визуальная индикация должна явно отличаться от индикации исходного состояния, используя цвета и символы (например, фигуры или текст). Визуальная индикация неподтвержденной аварийной сигнализации должна включать мерцающий элемент. Существуют некоторые внешние условия, в которых звуковая индикация не является эффективным индикатором неподтвержденной аварийной сигнализации.

11.3.3.4 Индикация состояния подтвержденной аварийной сигнализации

Состояние подтвержденной аварийной сигнализации не должно использовать звуковую индикацию. Визуальная индикация состояния подтвержденной аварийной сигнализации должна явно отличаться от индикации исходного состояния, используя символы (например, фигура или текст), и должна быть идентична по цвету с индикацией неподтвержденного состояния. Для визуальной индикации подтвержденной аварийной сигнализации не должен использоваться мерцающий элемент.

11.3.3.5 Индикация аварийной сигнализации, возвращенной в исходное неподтвержденное состояние

Возвращенная в исходное неподтвержденное состояние аварийная сигнализация не должна использовать звуковую индикацию. Визуальная индикация возвращения в исходное неподтвержденное состояние аварийной сигнализации может совпадать с индикацией исходного состояния либо она может указывать на неподтвержденный статус с мерцающим элементом.

11.3.3.6 Индикация состояния отложенной аварийной сигнализации

Визуальная индикация состояния отложенной аварийной сигнализации должна быть представлена в ЧМИ. Визуальная индикация для отложенной аварийной сигнализации не должна включать мерцающий элемент. Индикация состояния отложенной аварийной сигнализации должна быть четко выраженной. Никакая звуковая индикация не должна использоваться для идентификации отложенных аварийных сигнализаций.

11.3.3.7 Индикация запрещенного проектом состояния аварийной сигнализации

Визуальная индикация запрещенного проектом состояния аварийной сигнализации должна быть представлена в ЧМИ. Визуальная индикация для запрещенного проектом состояния аварийной сигнализации не должна включать мерцающий элемент. Индикация запрещенного проектом состояния

аварийной сигнализации должна отличаться от индикации неподтвержденного и подтвержденного состояний. Никакая звуковая индикация не должна использоваться для идентификации запрещенных проектом аварийных сигнализаций.

11.3.3.8 Индикация состояния выведенной из обслуживания аварийной сигнализации

Визуальная индикация состояния выведенной из обслуживания аварийной сигнализации должна быть представлена в ЧМИ. Визуальная индикация для выведенной из обслуживания аварийной сигнализации не должна включать мерцающий элемент. Индикация состояния выведенной из обслуживания аварийной сигнализации должна отличаться от индикаций подтвержденного и неподтвержденного состояний. Никакая звуковая индикация не должна использоваться для идентификации выведенных из обслуживания аварийных сигнализаций.

11.3.3.9 Резюме по индикации состояний аварийной сигнализации

Рекомендуемые звуковые и визуальные индикации состояний для типовых аварийных сигнализаций представлены в таблице 4.

Таблица 4 — Рекомендуемые индикации состояний аварийной сигнализации

Состояние аварийной сигнализации	Звуковая индикация	Визуальная индикация		
		Цвет	Символ	Мерцание
Исходное	Нет	Нет	Нет	Нет
Неподтвержденная аварийная сигнализация	Да	Да	Да	Да
Подтвержденная аварийная сигнализация	Нет	Да	Да	Нет
Аварийная сигнализация, возвращенная в исходное неподтвержденное состояние	Нет	Сочетание		Необязательная
Отложенная аварийная сигнализация	Нет	Сочетание		Нет
Запрещенная проектом аварийная сигнализация	Нет	Сочетание		Нет
Выведенная из обслуживания аварийная сигнализация	Нет	Сочетание		Нет
«Да» означает, что данный тип индикации должен использоваться для описания состояния аварийной сигнализации. «Нет» означает, что данный тип индикации не должен использоваться для описания состояния аварийной сигнализации.				

11.3.4 Звуковая индикация состояния аварийной сигнализации

Звуковая индикация аварийной сигнализации для неподтвержденных аварийных сигнализаций может использоваться также для указания на приоритет, производственную зону или группу аварийной сигнализации в зависимости от концепции аварийной сигнализации.

В окружающей среде, где звуковая индикация неподтвержденной аварийной сигнализации не эффективна (например, внешняя среда с высоким уровнем окружающих шумов), должна использоваться явная визуальная индикация неподтвержденной аварийной сигнализации, которая всегда находится в поле зрения оператора (например, светосигнал или серия светосигналов).

11.4 Индикация приоритетов аварийной сигнализации

11.4.1 Общие положения

Концепция аварийной сигнализации вводит ряд приоритетов для аварийной сигнализации, которые используются в ЧМИ, чтобы помочь оператору в выборе правильной последовательности аварийных сигнализаций для ответных действий.

11.4.2 Требования к индикации приоритетов аварийной сигнализации

Чтобы отличать приоритеты аварийной сигнализации конкретной системы аварийной сигнализации для нее должна использоваться уникальная комбинация визуальных индикаций, звуковых индикаций или тех и других.

11.4.3 Требования к цветовой индикации приоритетов аварийной сигнализации

Для каждого приоритета аварийной сигнализации, кроме производственной среды, где это не целесообразно, должен использоваться отдельный цветной индикатор. Цвета приоритетов аварийной сигнализации должны быть зарезервированы и не должны использоваться для других элементов ЧМИ.

11.4.4 Рекомендуемая индикация приоритетов аварийной сигнализации

11.4.4.1 Общие положения

Следующие рекомендуемые индикаторы приоритетов аварийных сигнализаций являются общей промышленной практикой.

11.4.4.2 Символьная индикация приоритетов аварийной сигнализации

Для указания на каждый приоритет аварийной сигнализации должен использоваться усиленный цветной маркировкой уникальный символ (например, фигура или текст).

11.4.4.3 Звуковая индикация приоритетов аварийной сигнализации

Для каждого приоритета аварийной сигнализации должен использоваться звуковой индикатор. В окружающей среде, где звуковая индикация не используется в качестве индикации приоритетов, должна использоваться визуальная индикация приоритетов.

11.5 Индикация сообщений аварийной сигнализации

11.5.1 Общие положения

Сообщение аварийной сигнализации предоставляет дополнительную информацию об аварийной сигнализации помимо имени тега, индикации состояния и приоритета. Оно может также включать часть действий оператора или ссылку на процедуру реагирования на эту аварийную сигнализацию.

11.5.2 Рекомендуемая индикация сообщений аварийной сигнализации

11.5.2.1 Общие положения

Следующие рекомендуемые индикаторы сообщений аварийной сигнализации являются общей промышленной практикой:

a) визуальная индикация сообщений аварийной сигнализации;

b) озвученная индикация сообщений аварийной сигнализации.

11.5.2.2 Визуальная индикация сообщений аварийной сигнализации

Визуальное сообщение аварийной сигнализации должно быть сформировано для каждой аварийной сигнализации и отображено в общей сводке аварийных сигналов. Визуальное сообщение аварийной сигнализации обычно не отображается на дисплеях технологического процесса.

11.5.2.3 Озвученная индикация сообщений аварийной сигнализации

Озвученная индикация сообщений аварийной сигнализации может быть реализована с помощью голосового синтезатора. Озвученная индикация сообщений должна быть структурирована и лаконична. Озвученная индикация сообщений должна быть прекращена после отключения звука оператором или подтверждения аварийной сигнализации. Вместе с озвученной индикацией сообщений аварийной сигнализации должна использоваться визуальная индикация.

11.6 Отображение аварийных сигнализаций

11.6.1 Общие положения

В ЧМИ существует несколько типов отображений, которые являются эффективными в рамках системы аварийных сигнализаций, и включают следующие:

a) отображение общей сводки аварийных сигнализаций;

b) отображение общей сводки статусов аварийных сигнализаций;

c) отображение архива аварийных сигнализаций;

d) отображение технологического процесса;

e) подробное отображение тега;

f) отображение аварийных сигнализаций системы диагностики;

g) отображение отложенных аварийных сигнализаций;

h) отображение выведенных из обслуживания аварийных сигнализаций;

i) отображение запрещенных проектом аварийных сигнализаций.

11.6.2 Отображение общей сводки аварийных сигнализаций

11.6.2.1 Требования к демонстрации общей сводки аварийных сигнализаций

По крайней мере, требуется одно отображение общей сводки аварийных сигнализаций. Отображение общей сводки аварийных сигнализаций предоставляет список активных аварийных сигнализаций в системе аварийных сигнализаций. Для отображений общей сводки аварийных сигнализаций существует несколько необходимых и рекомендуемых функций.

11.6.2.2 Информационные требования

В отображении общей сводки аварийных сигнализаций должна быть перечислена информация только об аварийных сигнализациях. Такое отображение должно предоставлять следующую информацию для каждой аварийной сигнализации:

a) имя тега для аварийной сигнализации;
b) описание тега или описание аварийного сигнала для аварийной сигнализации;
c) состояние аварийной сигнализации (включая статус подтверждения);
d) приоритет аварийной сигнализации;
e) время/дата, когда аварийная сигнализация стала активной;
f) тип аварийной сигнализации.

11.6.2.3 Информационные рекомендации

В демонстрации общей сводки аварийных сигнализаций для каждой аварийной сигнализации должно быть предоставлено следующее:

a) значение технологического параметра;
b) уставка аварийной сигнализации;
c) производственная зона;
d) группа аварийной сигнализации,
e) сообщение аварийной сигнализации.

11.6.2.4 Рекомендации по дополнительной информации

Кроме того, общая сводка аварийных сигнализаций должна отображать:

a) количество аварийных сигнализаций в сводном списке;
b) количество неподтвержденных аварийных сигнализаций в сводном списке.

11.6.2.5 Функциональные требования

Отображение общей сводки аварийных сигнализаций должно быть обеспечено следующими функциями:

a) сортировка аварийных сигнализаций в хронологическом порядке;
b) сортировка аварийных сигнализаций по приоритетам;
c) индивидуальное подтверждение для каждой аварийной сигнализации;
d) подтверждение визуальных аварийных сигнализаций.

11.6.2.6 Функциональные рекомендации

Отображение общей сводки аварийных сигнализаций должно быть обеспечено следующими функциями:

a) навигационная связь с отображением соответствующего технологического процесса;
b) фильтрация аварийных сигнализаций по времени срабатывания аварийной сигнализации;
c) фильтрация аварийных сигнализаций по приоритету;
d) фильтрация аварийных сигнализаций по типу аварийной сигнализации;
e) фильтрация аварийных сигнализаций по группе аварийной сигнализации;
f) фильтрация аварийных сигнализаций по производственной зоне;
g) фильтрация аварийных сигнализаций по имени тега;
h) ограничения по времени для средств фильтрации;
i) сортировка аварийных сигнализаций по имени тега.

Если в отображениях общих сводок аварийных сигнализаций используются фильтры, то отображение должно ясно указать, какой фильтр используется. Ограничение по времени — это функция, которая устраняет фильтр, когда истекает определенный период времени.

11.6.3 Общая сводка статусов аварийных сигнализаций

11.6.3.1 Общие положения

Рекомендуется отображение общей сводки статусов аварийных сигнализаций. Отображение общей сводки статусов аварийных сигнализаций обеспечивает индикацию определенного количества активных аварийных сигнализаций по приоритету для каждой производственной зоны.

11.6.3.2 Информационные рекомендации

Отображение общей сводки статусов аварийных сигнализаций для каждой производственной зоны или другой группировки должно предоставлять следующее:

a) количество аварийных сигнализаций в каждой группе аварийных сигнализаций с одинаковым приоритетом;

b) количество неподтвержденных аварийных сигнализаций в каждой группе с одинаковым приоритетом;

c) индикацию, если все аварийные сигнализации в группе с одинаковым приоритетом подтверждены.

11.6.3.3 Функциональные рекомендации

Отображение общей сводки статусов аварийных сигнализаций должно обеспечить навигационную связь с отображением соответствующего технологического процесса.

11.6.4 Отображения архива аварийных сигнализаций

11.6.4.1 Общие положения

Должно быть реализовано отображение архива аварийных сигнализаций. Отображение архива аварийных сигнализаций обеспечивает доступ к архиву аварийных сигнализаций, который содержит записи об изменении состояния каждой аварийной сигнализации (например, подтверждение, возвращение в исходное состояние и т. д.).

11.6.4.2 Информационные рекомендации

Отображение архива аварийных сигнализаций должно предоставлять из записей об аварийной сигнализации следующую информацию:

a) имя тега для аварийной сигнализации;

b) описание тега или описание аварийной сигнализации для аварийной сигнализации;

c) состояние аварийной сигнализации (включая статус подтверждения);

d) приоритет аварийной сигнализации;

e) дату и время срабатывания аварийной сигнализации;

f) дату и время подтверждения;

g) дату и время возвращения в исходное состояние;

h) тип аварийной сигнализации.

11.6.4.3 Функциональные рекомендации

Отображение архива аварийных сигнализаций должно быть обеспечено следующими функциями:

a) фильтрация аварийных сигнализаций по имени тега;

b) фильтрация аварийных сигнализаций по времени срабатывания аварийной сигнализации;

c) фильтрация аварийных сигнализаций по приоритету;

d) фильтрация аварийных сигнализаций по типу аварийной сигнализации;

e) фильтрация аварийных сигнализаций по группе аварийной сигнализации;

f) фильтрация аварийных сигнализаций по производственной зоне.

11.6.5 Отображения технологического процесса

Отображения технологического процесса обеспечивают контекст технологического процесса для аварийных сигнализаций. Отображения технологического процесса должны предоставлять следующее:

a) имя тега (с помощью текста или других методов доступа);

b) состояние аварийной сигнализации, включая статус подтверждения;

c) приоритет аварийной сигнализации;

d) статус запрещения аварийной сигнализации;

e) тип аварийной сигнализации.

11.6.6 Подробные отображения тега

Подробные отображения тега обеспечивают подробную информацию о теге аварийной сигнализации. Подробное отображение должно предоставлять следующую информацию:

a) состояние аварийной сигнализации (включая статус подтверждения);

b) приоритет аварийной сигнализации;

c) группу аварийной сигнализации;

d) тип аварийной сигнализации,

e) уставку аварийной сигнализации;

f) статус запрещения аварийной сигнализации;

g) текущее значение параметра технологического процесса или состояния.

11.6.7 Другие элементы отображения

Допускается использовать другие элементы отображения для указания на состояния аварийной сигнализации.

11.7 Задержка аварийной сигнализации

11.7.1 Общие положения

Задержка по времени аварийной сигнализации оператором является функцией, которая используется для устранения влияния ложных аварийных сигналов на эффективность системы сигнализации. Задержка включает функцию, гарантирующую целостность системы аварийной сигнализации.

11.7.2 Требования к функциям откладывания аварийной сигнализации

Функция откладывания аварийной сигнализации должна обеспечить следующее:

a) способность отложить аварийную сигнализацию;

b) отображения отложенных аварийных сигнализаций или эквивалентного списка средств, чтобы указать на все отложенные аварийные сигнализации;

c) предельное время откладывания;

d) управление доступом для откладывания аварийных сигнализаций;

e) способность не откладывать аварийные сигнализации;

f) запись каждой отложенной аварийной сигнализации.

Предельное время — это время через которое специальная функция завершает откладывание аварийной сигнализации.

11.7.3 Функциональные рекомендации откладывания аварийной сигнализации

Для предотвращения потока аварийных сигналов, когда активные аварийные сигнализации автоматически не откладываются, должна быть разработана функция откладывания аварийной сигнализации, которая:

a) должна вручную неотложенную аварийную сигнализацию перевести в состояние подтвержденной аварийной сигнализации;

b) должна автоматически неотложенную аварийную сигнализацию перевести в состояния неподтвержденной аварийной сигнализации.

11.7.4 Отображения отложенных аварийных сигнализаций

11.7.4.1 Общие положения

Отображения отложенных аварийных сигнализаций или эквивалентного списка средств для системы аварийной сигнализации с функционалом откладывания имеют несколько необходимых и рекомендуемых функций.

11.7.4.2 Информационные требования

Отображения отложенных аварийных сигнализаций должны предоставлять следующую информацию:

a) имя тега аварийной сигнализации;

b) описание тега или описание аварийной сигнализации для аварийного сигнала;

c) тип аварийной сигнализации,

d) статус аварийной сигнализации (т. е. активная или неактивная);

e) приоритет аварийной сигнализации,

f) оставшееся время до завершения откладывания или время и дату, когда аварийная сигнализация была отложена.

11.7.4.3 Функциональные требования

Отображения отложенных аварийных сигнализаций должны поддерживаться следующими функциями:

a) сортировка аварийных сигнализаций в хронологическом порядке по времени начала откладывания или по оставшемуся времени до завершения откладывания;

b) сортировка аварийных сигнализаций по приоритету;

c) сортировка аварийных сигнализаций по тегу;

d) отключение откладывания для отдельных аварийных сигнализаций.

11.7.4.4 Функциональные рекомендации

Отображения отложенных аварийных сигнализаций будут поддерживаться следующими функциями:

a) фильтрация аварийных сигнализаций по приоритету;

b) фильтрация аварийных сигнализаций по состоянию;

c) фильтрация аварийных сигнализаций по производственной зоне;

d) ввод данных оператором о причине откладывания аварийной сигнализации;

e) отключение откладывания для группы аварийных сигнализаций;

f) навигационная связь с отображением технологического процесса;

g) навигационная связь с подробным отображением тега.

11.8 Выведенные из обслуживания аварийные сигнализации

11.8.1 Общие положения

Запрещение аварийных сигнализаций их выводом из обслуживания является обычной практикой исключения аварийных сигнализаций из функционирования, чтобы обеспечить техническое обслуживание. Существует несколько необходимых и рекомендуемых функций ЧМИ, связанных с выводом из обслуживания аварийных сигнализаций.

11.8.2 Необходимые функции вывода из обслуживания аварийной сигнализации

Вывод из обслуживания аварийной сигнализации должен поддерживаться следующими функциями.

a) методом индивидуального исключения каждой аварийной сигнализации из функционирования;

b) методом индивидуального возврата каждой аварийной сигнализации в исходное состояние;

c) отображением задержанных аварийных сигнализаций или эквивалентного списка средств, чтобы указать на все задержанные аварийные сигнализации;

d) управлением доступом для вывода из обслуживания аварийной сигнализации, если это позволено;

e) записью о каждой аварийной сигнализации, выведенной из обслуживания.

11.8.3 Отображения вывода из обслуживания аварийных сигнализаций

11.8.3.1 Требования к отображению вывода из обслуживания аварийных сигнализаций

Для каждой системы аварийной сигнализации должно быть обеспечено отображение ее вывода из обслуживания либо эквивалентного набора средств для этого. Отображения вывода из обслуживания аварийных сигнализаций имеют несколько необходимых и рекомендуемых функций.

11.8.3.2 Информационные требования

Отображения вывода из обслуживания аварийных сигнализаций должны предоставлять следующую информацию:

a) имя тега аварийной сигнализации;

b) описание тега или описание аварийной сигнализации для аварийной сигнализации;

c) тип аварийной сигнализации;

d) статус незапрещенной аварийной сигнализации (т. е. активная или неактивная);

e) приоритет аварийной сигнализации;

f) время и дату вывода аварийной сигнализации из обслуживания.

11.8.3.3 Функциональные требования

Отображения вывода из обслуживания аварийных сигнализаций должны поддерживаться следующими функциями:

a) сортировка аварийных сигнализаций в хронологическом порядке запрещения;

b) сортировка аварийных сигнализаций по приоритету;

c) сортировка аварийных сигнализаций по статусу (т. е. активная или неактивная);

d) сортировка аварийных сигнализаций по производственной зоне;

e) независимое возвращение в эксплуатацию аварийных сигнализаций.

11.8.3.4 Функциональные рекомендации

Отображения вывода из обслуживания аварийной сигнализации должен поддерживать оператор, используя функцию ввода данных о причине запрещения аварийной сигнализации.

11.9 Запрещенные проектом аварийные сигнализации

11.9.1 Общие положения

Специально спроектированное запрещение аварийных сигнализаций, в которых нет необходимости из-за планируемых или фактических условий работы, является обычной практикой.

11.9.2 Необходимые функции проектируемого запрещения

Функция проектируемого запрещения должна обеспечить следующее:

a) отображения запрещенных проектом аварийных сигнализаций или эквивалентного списка средств для индикации всех запрещенных проектом аварийных сигнализаций;

b) запись о каждой запрещенной проектом аварийной сигнализации.

11.9.3 Функциональные рекомендации проектируемого запрещения

Для предотвращения потока аварийных сигналов, когда активные аварийные сигнализации автоматически не запрещаются, должна быть разработана функция проектируемого запрещения.

Автоматически незапрещенная аварийная сигнализация должна перейти в состояние неподтвержденной аварийной сигнализации.

11.9.4 Отображения запрещенных проектом аварийных сигнализаций

11.9.4.1 Общие положения

Отображения запрещенных проектом аварийных сигнализаций или эквивалентного списка средств должны быть сформированы для системы аварийной сигнализации. Отображения запрещенных проектом аварийных сигнализаций должны поддерживаться рядом необходимых и рекомендуемых функций.

11.9.4.2 Информационные требования

Отображения запрещенных проектом аварийных сигнализаций должны предоставлять следующую информацию:

a) имя тега аварийной сигнализации;
b) описание тега или описание аварийной сигнализации для аварийного сигнала;
c) тип аварийной сигнализации;
d) статус незапрещенной аварийной сигнализации (т. е. активная или неактивная);
e) приоритет аварийной сигнализации;
f) время и дату, когда аварийная сигнализация была запрещена.

11.9.4.3 Информационные рекомендации

Отображения запрещенных проектом аварийных сигнализаций будут обеспечивать индикацию метода запрещения (например, проектируемое запрещение).

11.9.4.4 Функциональные требования

Отображения запрещенных проектом аварийных сигнализаций должны поддерживаться следующими функциями:

a) сортировка аварийных сигнализаций в хронологическом порядке запрещения;
b) сортировка аварийных сигнализаций по приоритету;
c) сортировка аварийных сигнализаций по статусу;
d) сортировка аварийных сигнализаций по производственной зоне.

11.10 Интеграция аварийных оповещательных устройств

11.10.1 Общие положения

Системы аварийной сигнализации могут включать отдельные устройства аварийного оповещения. Данный подраздел описывает рекомендации по интеграции независимых устройств оповещения в системе аварийной сигнализации.

11.10.2 Рекомендации по интеграции аварийных оповещательных устройств

Аварийные оповещательные устройства должны быть интегрированы для поддержки следующих функций:

a) связь информации о состоянии аварийной сигнализации с архивом аварийных сигнализаций;
b) предотвращение избыточных аварийных сигнализаций в системе управления;
c) предотвращение необходимости в избыточном подтверждении в системе управления.

11.10.3 Рекомендации по отображению интеграции аварийных оповещательных устройств

Аварийные оповещательные устройства должны быть интегрированы так, чтобы расположение аварийной сигнализации на аварийном оповещательном устройстве соответствовало согласованной методике.

11.11 Человеко-машинный интерфейс аварийной сигнализации безопасности

11.11.1 Общие положения

Для некоторых аварийных сигнализаций безопасности в соответствии с правилами или стандартами может требоваться независимый ЧМИ. Методы идентификации аварийных сигнализаций безопасности не входят в область применения настоящего стандарта.

11.11.2 Независимый ЧМИ аварийной сигнализации безопасности

ЧМИ, независимый от ОСУТП, может потребоваться для следующих аварийных сигнализаций безопасности:

a) связанных с безопасностью аварийных сигнализаций в зависимости от проблемы (например, от уровня снижения риска);

b) аварийных сигнализаций системы диагностики ПСБ, которые указывают на опасные сбои в зависимости от проблемы (например, от ответа оператора, от коммуникационного сбоя).

Примечание — Дальнейшие указания см. в МЭК 61511.

12 Детальное проектирование. Методы повышения эффективности и усовершенствования аварийной сигнализации

12.1 Цель

Повышение эффективности и усовершенствование аварийной сигнализации является частью стадии детального проектирования жизненного цикла аварийной сигнализации. Настоящий раздел рассматривает дополнительные методы управления аварийной сигнализацией кроме тех, которые обычно используются в системах управления. Эти методы обычно обеспечивают дополнительную функциональность к техническому проекту системы аварийной сигнализации и особенно полезны для управления действиями оператора при нарушении нормальных условий эксплуатации технологического процесса.

Применение методов повышения эффективности и усовершенствование аварийной сигнализации ведет к дополнительным уровням логики, программирования или моделирования, используемым для изменения атрибутов аварийной сигнализации. Эти методы включают динамическую аварийную сигнализацию, аварийную сигнализацию, управляемую состояниями (т. е аварийную сигнализацию, управляемую условиями) и адаптивную аварийную сигнализацию. Большинство разработанных методов запрещения аварийных сигнализаций являются методами усовершенствования аварийной сигнализации.

Обеспечить оператору более точную информацию об аварийной сигнализации, помимо методов усовершенствования аварийной сигнализации, также могут методы повышения эффективности. Более точную информацию обычно считают необходимой, чтобы или избежать, или смягчить эксплуатационные проблемы, которые могут привести к инцидентам.

Для снижения потоков аварийных сигналов или ослабления их последствий может оказаться недостаточно методов технического проектирования системы аварийной сигнализации, поэтому необходимы методы повышения эффективности и усовершенствования. Описанные методы могут снизить или устранить поток аварийных сигналов.

12.2 Основы повышения эффективности и усовершенствования аварийной сигнализации

12.2.1 Общие положения

Методы повышения эффективности и усовершенствования аварийной сигнализации часто используются, если технический проект системы аварийной сигнализации не достигает целевых характеристик, указанных в концепции аварийной сигнализации. Концепция аварийной сигнализации или спецификация требований к системе аварийной сигнализации должны включать список приемлемых методов повышения эффективности и усовершенствования аварийной сигнализации.

12.2.2 Трудоемкость, требования к персоналу и сложность

В связи с дополнительными сложностями применения методов повышения эффективности и усовершенствования аварийной сигнализации возникает необходимость в дополнительных ресурсах для их проектирования, внедрения и технического обслуживания. Процесс управления изменениями должен включать анализ влияния изменений на методы повышения эффективности и усовершенствования аварийной сигнализации.

Стоимость дополнительной сложности системы аварийной сигнализации должна быть сравнима с дополнительными преимуществами от улучшения производительности системы аварийной сигнализации.

Перед подтверждением применения и во время проектирования методов повышения эффективности и усовершенствования аварийной сигнализации для них необходимо выполнить анализ рисков сценариев отказов.

12.3 Информационные связи

Эффективность системы аварийной сигнализации может быть повышена, если есть связь с информацией из общей базы данных аварийных сигналов (например, о действии оператора или последствии). Информация может также быть взята из других источников, включая рабочие процедуры,

журналы регистрации действий оператора, данные о техническом обслуживании или проектную документацию. Эти связи должны быть легко управляемыми и поддерживаемыми.

12.4 Аварийная сигнализация, основанная на логике

12.4.1 Общие положения

Аварийная сигнализация, основанная на логике, реализуется с использованием булевой логики или древовидных схем решений для определения модификаций, которые будут выполнены с системами аварийной сигнализации.

12.4.2 Модификация атрибутов аварийной сигнализации

Для некоторых методов повышения эффективности и усовершенствования аварийной сигнализации существует необходимость в применении функциональных возможностей для изменения некоторых атрибутов аварийной сигнализации (например, уставки или приоритеты аварийной сигнализации).

12.4.3 Внешние системы

Внешние системы получают аварийный сигнал и обрабатывают данные из системы управления, а также используют информацию для определения условий работы предприятия и соответствующей модификации атрибутов аварийной сигнализации.

12.4.4 Логическое запрещение аварийных сигналов и модификация их атрибутов

Логические методы запрещения аварийной сигнализации используют условия состояния аварийной сигнализации из некоторых аварийных сигнализаций, чтобы изменить атрибуты других аварийных сигнализаций (например, для аварийных сигнализаций, обрабатываемых в порядке поступления).

12.4.5 Аварийная сигнализация, управляемая состояниями

Аварийная сигнализация, управляемая состояниями, является методом усовершенствования аварийной сигнализации, который изменяет уставку, приоритет или статус запрещения аварийной сигнализации на основе определенных рабочих состояний оборудования или технологических процессов. Состояния часто определяются:

a) статусом логической переменной;

b) определенным параметром технологического процесса, который достигает заданного предела;

c) логикой, которая «просматривает» много переменных и индикаторов;

d) выбором оператора.

Определение состояния и модификация аварийной сигнализации могут быть выполнены неавтоматизированными, полуавтоматическими (например, некоторой комбинацией неавтоматизированного и автоматизированного методов) или полностью автоматизированным методами. Отработанное состояние должно быть понятно оператору.

12.5 Аварийная сигнализация, управляемая моделями

Аварийная сигнализация, управляемая моделями, может использоваться в областях, где требуется более сложная система оповещения аварийной сигнализации, в которой параметры сложного технологического процесса могут сформировать результат на основе множества данных точек измерения, или в которой оценка состояния предприятия может быть получена на основе модели.

Основанные на модели системы аварийной сигнализации не должны заменять технический проект системы аварийной сигнализации без тщательного анализа.

12.6 Дополнительные аспекты аварийной сигнализации

12.6.1 Общие положения

Некоторые дополнительные усовершенствования повышают эффективность системы сигнализации. Эти усовершенствования обычно выполняются для основной системы аварийной сигнализации.

12.6.2 Аварийная сигнализация, не связанная с данным пультом управления

Предполагается, что операторы должны отвечать на аварийные сигналы, но если информация о выполнении задач не поступает на их пульт управления, то можно использовать отображение и подтверждение удаленной аварийной сигнализации. Может возникнуть необходимость в процедурах, направляющих аварийные сигналы резервному оператору. Если используются удаленные системы аварийной сигнализации, то в концепцию аварийной сигнализации должны быть включены такие системы.

Используемые подходы оповещения от удаленной аварийной сигнализации должны включать периодические контрольные сообщения для повышения надежности. Следует рассмотреть процедуру, гарантирующую ответ на аварийный сигнал.

12.6.3 Удаленные системы аварийной сигнализации

Могут существовать ситуации, в которых лицо, которое наиболее заинтересовано в информации об аварийной ситуации и принимает решение о ней, не является оператором пульта управления. В таких ситуациях можно воспользоваться наличием удаленной системы аварийной сигнализации (например, используя пейджер, электронную почту и т. д.).

Безотказность доставки сообщений является важной задачей для удаленных систем аварийной сигнализации и эту задачу следует рассмотреть. Может быть необходимо также обеспечить удаленное подтверждение аварийной сигнализации.

12.6.4 Дополнительные системы аварийной сигнализации

Дополнительные системы аварийной сигнализации (например, экспертная система для ответа на аварийную сигнализацию) могут заменить систему оповещения аварийной сигнализации в системе управления или использовать существующую графическую среду для формирования общего интерфейса. Кроме того, такие системы могут использоваться в дополнение к существующей системе аварийной сигнализации, чтобы предоставить дополнительную или альтернативную информацию об аварийной сигнализации.

Необходимо соблюдать особую осторожность, чтобы быть уверенным, что дополнительная информация важна. Дополнительная система аварийной сигнализации должна быть разработана так, чтобы гарантировать приемлемые доступность и безотказность аварийной сигнализации.

Если используется дополнительная система аварийной сигнализации, то она должна удовлетворять всем требованиям настоящего стандарта.

12.6.5 Групповой процесс производства

12.6.5.1 Общие положения

Условия, состояния и стадии технологического процесса могут привести к изменению аварийной сигнализации в групповых процессах производства. Часто она реализуется, как аварийная сигнализация, управляемая состояниями.

12.6.5.2 Плавно регулируемые пороги срабатывания аварийной сигнализации

Аварийные сигнализации в групповых процессах производства часто применяются только к конкретным этапам технологического процесса или связаны с изменением уставок контура управления, или с изменяющимися во времени данными технологического процесса. Если не соблюдать особую осторожность, то групповые процессы производства могут быть подвержены появлению ложных аварийных сигналов. Методы усовершенствования аварийной сигнализации могут помочь в создании устройства для решения этих проблем, связанных с аварийной сигнализацией в групповых процессах производства.

12.6.5.3 Относительное время и абсолютное время

Временные метки данных и записей аварийных сигналов обычно формируются в компьютерных системах, используя при этом календарное время. Для получения информации о групповом процессе производства более удобно использовать относительное время (т. е. время от начала группового процесса или этапа технологического процесса). Особенностью усовершенствованной аварийной сигнализации является ее способность использовать календарные временные метки и для электронных записей, указывающих, когда начались групповой процесс или стадия, и для выполнения вычисления и отображения аварийных сигнализаций использовать относительное время.

12.6.5.4 Включение номера группы и других идентифицирующих меток

Для некоторых производственных объектов можно определить функциональность, связывающую идентификационные номера с аварийными сигнализациями. Способность сортировать записи выбранной идентификацией также полезна при создании официальной документации на производственный цикл партии изделий и при сравнении такой документации для других производственных циклов. Методы формирования и применения таких идентифицирующих меток должны быть доказаны и безотказны в работе.

12.7 Обучение, выполнение испытаний и аудирование систем

В концепции аварийной сигнализации должны быть определены шаги, гарантирующие дальнейшее применение методов для усовершенствования аварийной сигнализации, выполнения обучения, испытания и аудита. Процедуры обучения, испытания и аудита должны включать методы повышения эффективности и усовершенствования аварийной сигнализации.

12.8 Соблюдение установленных атрибутов аварийной сигнализации

Чтобы поддержать спроектированные значения атрибутов настройки аварийной сигнализации (например, уставки аварийной сигнализации и приоритета аварийной сигнализации) на согласованных уровнях, необходимо регулярное сравнение их рационализированных значений с реальными значениями параметров настройки системы управления. Контроль за соблюдением установки, автоматическая проверка и восстановление атрибутов аварийной сигнализации, является методом повышения эффективности, который выполняется за счет функций, связанных с контролем, оценкой и аудитом. Контроль за соблюдением установки может быть инициирован на планируемой основе или по запросу и должен различать изменения, которые обусловлены применением методологии реализации аварийной сигнализации, управляемой состояниями, от изменений, которые обусловленны применением методологии откладывания аварийной сигнализации.

13 Внедрение

13.1 Цель

Внедрение — это отдельная стадия жизненного цикла системы аварийной сигнализации, которая является переходом от проектирования к эксплуатации. Настоящий раздел охватывает общие требования к внедрению или изменению аварийной сигнализации или системы аварийной сигнализации.

13.2 Планирование внедрения

Область применения проекта или изменения определяют объем необходимой работы. Планирование внедрения должно учитывать следующее:

a) прерывание технологического процесса;

b) доступность компетентных ресурсов;

c) функциональное испытание или подтверждение соответствия;

d) проверку документации;

e) обучение операторов.

13.3 Подготовка к внедрению

13.3.1 Общие положения

Требования к подготовке по внедрению новых систем аварийной сигнализации и модификации существующих определены на основе классификации аварийных сигнализаций и требований к каждому их классу, что подробно представлено в концепции аварийной сигнализации.

13.3.2 Обучение внедрению

Операторы должны быть обучены тому, как отвечать на аварийные сигнализации всех новых (внедренных) или модифицированных систем аварийной сигнализации до того, как операторы принимают на себя ответственность за работу с новыми или модифицированными системами аварийной сигнализации.

13.3.3 Требования к подготовке внедрения

Подготовка должна включать:

a) информацию о рационализации аварийной сигнализации (например, последствие, причины возникновения аварийных сигналов, корректирующие действия и т. д.);

b) звуковую и визуальную индикацию аварийной сигнализации.

13.3.4 Требования к документации о подготовке по наиболее важным аварийным сигнализациям

Документация о подготовке по новым или модифицированным наиболее важным аварийным сигнализациям должна включать следующее:

a) обученный персонал;

b) метод обучения;

c) дата обучения.

13.3.5 Рекомендуемая документация о подготовке

Документация о подготовке должна включать следующее:

a) обученный персонал;

b) метод обучения;

c) дата обучения.

13.3.6 Требования к подготовке к внедрению новых или модифицированных систем аварийной сигнализации

Операторы должны быть подготовлены к работе со всеми новыми или модифицированными системами сигнализации.

13.3.7 Рекомендации по подготовке к внедрению новых или модифицированных систем аварийной сигнализации

Рекомендации к подготовке к работе с модифицированными системами аварийной сигнализации должны соответствовать характеру модификации. Рекомендации к подготовке к работе с новой системой аварийной сигнализации должны включать следующее:

a) звуковую и визуальную индикацию аварийной сигнализации;

b) отличительные признаки приоритетов аварийной сигнализации;

c) использование характеристик ЧМИ аварийной сигнализации (например, общая сводка сортировки и фильтрации аварийной сигнализации);

d) методы откладывания и запрещения;

e) методы вывода из эксплуатации аварийной сигнализации.

13.4 Испытание и подтверждение соответствия при внедрении

13.4.1 Общие положения

Требования при внедрении к испытаниям новых систем аварийной сигнализации и модификаций существующих систем аварийной сигнализации определены на основе классификации аварийной сигнализации и требований к каждому их классу, что подробно представлено в концепции аварийной сигнализации.

13.4.2 Требования к испытаниям при внедрении наиболее важных аварийных сигнализаций

В концепции аварийной сигнализации должны быть определены требования к испытаниям для наиболее важных аварийных сигнализаций перед их вводом в эксплуатацию. Испытание должно быть документально оформлено и включать следующие сведения:

a) уставка или логические условия аварийной сигнализации;

b) приоритет аварийной сигнализации;

c) звуковая и визуальная индикация аварийной сигнализации;

d) любое другое заданное функциональное требование к аварийной сигнализации;

e) персонал, выполняющий испытание;

f) метод испытания и критерии годности;

g) результат испытания и решение вопросов по любым отказам или несоответствиям;

h) дата испытания;

i) дата ввод в эксплуатацию аварийной сигнализации.

13.4.3 Рекомендации по испытаниям при внедрении новых или модифицированных систем аварийной сигнализации

Аварийные сигналы должны быть испытаны во время внедрения. Испытание должно включать проверку:

a) уставки или логических условий аварийной сигнализации;

b) приоритета аварийной сигнализации;

c) звуковой и визуальной индикации аварийной сигнализации;

d) любого другого заданного функционального требования к аварийной сигнализации.

13.4.4 Требования к испытаниям при внедрении новых или модифицированных систем аварийной сигнализации

Системы аварийной сигнализации должны быть испытаны во время внедрения, чтобы гарантировать, что они удовлетворяют соответствующим разделам концепции аварийной сигнализации и ASRS. Испытание модифицированной системы аварийной сигнализации должно соответствовать характеру модификации, как определено процедурой управления изменениями производственного объекта. Испытание новых систем аварийной сигнализации должно включать проверки:

a) звуковой и визуальной индикации для каждого приоритета аварийной сигнализации;

b) характеристик ЧМИ, таких как отправка сообщений об аварийной сигнализации в общую сводку аварийной сигнализации или в эквивалентную структуру;

c) методов вывода аварийной сигнализации из эксплуатации и ее ввода в эксплуатацию;

d) методов задержки;

e) методов запрещения аварийной сигнализации;

f) любых дополнительных функций методов повышения эффективности и усовершенствования аварийной сигнализации;

g) методов фильтрации, сортировки, сборки аварийных сигнализаций для отображения технологического процесса.

13.5 Документация по внедрению

13.5.1 Общие положения

Существует несколько требований и рекомендаций к документации для внедрения систем аварийной сигнализации.

13.5.2 Требования к документации

Должна быть предоставлена следующая документация:

a) с информацией о рационализации;

b) с достаточной информацией для выполнения испытания аварийных сигнализаций;

c) на процедуры ответа аварийных сигнализаций;

d) на любую разработку запрещения или повышения эффективности аварийной сигнализации.

После завершения внедрения системы аварийной сигнализации должна быть обновлена информация о рационализации в соответствии с процедурой управления изменениями производственного объекта.

13.5.3 Рекомендации к документации при внедрении

Метод создания отчетов, формат и структура документации должны соответствовать процедурам проектной документации и требованиям документации владельца.

Методология и документация испытания должны соответствовать характеру изменения, как определено процедурами управления изменениями производственного объекта или концепцией аварийной сигнализации.

Информация, используемая при испытании новых и модифицированных систем аварийной сигнализации, может включать:

a) имя тега аварийной сигнализации;

b) описание тега или описание аварийной сигнализации для аварийного сигнала;

c) тип аварийной сигнализации;

d) приоритет;

e) значение уставки или логическое условие аварийной сигнализации;

f) действие оператора;

g) последствие бездействия;

h) дату испытания и изменения;

i) метод испытания и критерии годности;

j) результаты испытания и решение вопросов по любым отказам или несоответствиям.

14 Эксплуатация

14.1 Цель

Эксплуатация — это отдельная стадия жизненного цикла менеджмента системы аварийной сигнализации. Настоящий раздел охватывает требования, обеспечивающие для аварийной сигнализации возвращение или нахождение в состоянии эксплуатации. Состояние эксплуатации — это состояние, в котором аварийная сигнализация способна указать оператору на ненормальное условие эксплуатации. Также описаны инструментальные средства для обработки аварийной сигнализации в состоянии эксплуатации. Эксплуатация — это стадия жизненного цикла, которая следует за стадией внедрения и в которую происходит возврат из стадии технического обслуживания.

14.2 Процедуры ответа аварийной сигнализации

14.2.1 Требования к процедурам ответа аварийной сигнализации

Процедуры ответа аварийных сигналов должны быть легкодоступными для оператора.

14.2.2 Рекомендации к процедуре ответа аварийной сигнализации

Должна использоваться наиболее доступная для обслуживающего персонала форма документации на аварийную сигнализацию. Вся информация об аварийных сигнализациях, записанная во время их рационализации, должна также быть легкодоступной.

Если иначе не определено в концепции аварийной сигнализации, то процедуры ответа аварийной сигнализации должны включать:

a) имя тега аварийной сигнализации;
b) описание тега или описание аварийной сигнализации для аварийного сигнала;
c) тип аварийной сигнализации;
d) значение уставки аварийной сигнализации;
e) возможные причины;
f) последствие бездействия;
g) действие оператора;
h) допустимое время ответа;
i) класс аварийной сигнализации.

14.3 Задержка аварийной сигнализации

14.3.1 Требования к задержке аварийной сигнализации

Задержка аварийной сигнализации должна быть разрешена в соответствии с документацией на класс аварийной сигнализации, как описано в концепции аварийной сигнализации.

14.3.2 Задержка аварийной сигнализации для наиболее важных аварийных сигнализаций

Если используется класс наиболее важных аварийных сигнализаций, то их задержка должна соответствовать требованиям по подтверждению полномочий и повторному подтверждению полномочий, как это описано в концепции аварийной сигнализации.

Необходимо наличие документации, включающей одобрение, временные аварийные сигнализации и процедуры, а также детали повторного подтверждения полномочий.

14.3.3 Рекомендации к откладыванию аварийной сигнализации

Должны быть рассмотрены аварийные сигнализации, отложенные более, чем на одну рабочую смену. Требования к рассмотрению отложенных аварийных сигнализаций должны быть представлены документально в концепции аварийной сигнализации.

14.3.4 Требования к записи отложенного аварийного сигнала

Следующая информация должна быть записана для каждого аварийного сигнала, отложенного более, чем на одну рабочую смену:

a) имя тега аварийного сигнала;
b) описание тега или описание аварийной сигнализации для аварийного сигнала;
c) причина откладывания.

14.4 Переподготовка операторов

14.4.1 Требования к переподготовке операторов

Требования к подготовке в области аварийной сигнализации должны быть определены в соответствии с классификацией аварийной сигнализации и требованиями к конкретному классу, как представлено в концепции аварийной сигнализации.

14.4.2 Документация о переподготовке по наиболее важным аварийным сигнализациям

Если используется класс наиболее важных аварийных сигнализаций, то должна быть документально оформлена следующая информация о подготовке:

a) обученный персонал;
b) метод подготовки;
c) дата подготовки;
d) хронология подготовки.

Частота подготовки должна быть определена в концепции аварийной сигнализации. Документация о подготовке должна храниться в течение периода, определенного в концепции аварийной сигнализации или установленного в соответствии с политикой компании.

14.4.3 Содержание переподготовки по наиболее важным аварийным сигнализациям

Если используется класс наиболее важных аварийных сигнализаций, то операторы должны периодически проходить подготовку, работая с характеристиками каждой наиболее важной аварийной сигнализации. Содержание переподготовки должно включать:

a) информацию о рационализации аварийной сигнализации;
b) звуковую и визуальную индикацию аварийной сигнализации.

14.4.4 Рекомендации к переподготовке по аварийной сигнализации

Операторы должны проходить переподготовку, включающую рассмотрение процедур ответа аварийных сигнализаций. Подготовка должна охватывать широкий набор сценариев технологического процесса. Подготовка должна включать:

a) информацию о рационализации аварийной сигнализации;

b) звуковую и визуальную индикацию аварийной сигнализации.

Необходимо вести учет переподготовки, указывая, кто получил подготовку и время ее получения.

15 Техническое обслуживание

15.1 Цель

Техническое обслуживание — это отдельная стадия жизненного цикла менеджмента системы аварийной сигнализации. Настоящий раздел охватывает требования, обеспечивающие испытание системы аварийной сигнализации, равнозначную замену и ремонт. В настоящем разделе описан переход аварийных сигнализаций в состояние вывода из эксплуатации, и затем их возвращение в рабочее состояние. Техническое обслуживание также требует переподготовку персонала, обслуживающего систему аварийной сигнализации.

15.2 Периодические испытания аварийной сигнализации

15.2.1 Общие положения

Требования к периодическим испытаниям аварийной сигнализации должны быть определены требованиями к классу аварийной сигнализации, как представлено в концепции аварийной сигнализации. Цель периодических испытаний состоит в том, чтобы гарантировать, что аварийная сигнализация продолжает выполнять свои функции в соответствии с проектом.

15.2.2 Требования к периодическим испытаниям аварийной сигнализации

В течение периода, определенного в концепции аварийной сигнализации, необходимо вести учет, когда были выполнены испытания. Отчеты об испытаниях должны содержать следующую информацию:

a) дата (даты) испытания;

b) имя (имена) лица (лиц), который выполнил испытание или контроль;

c) уникальный идентификатор оборудования (например, номер шлейфа, технологический номер и номер оборудования);

d) результаты испытаний (например, состояние непосредственно перед началом поверки и состояние непосредственно после окончания поверки);

e) ссылка на процедуру испытаний и используемые методы;

f) причина отказов испытаний.

Если в концепции аварийной сигнализации указано о необходимости периодически выполнять испытания для некоторых аварийных сигнализаций, то в ней также должны быть представлены рекомендации о частоте и методе такого испытания.

15.2.3 Периодические испытания аварийной сигнализации с наиболее важными аварийными сигналами

Если применяются классы наиболее важных аварийных сигнализаций, то для них должны периодически выполняться испытания для гарантии их работоспособности.

Любые неполадки, найденные во время периодического испытания наиболее важных аварийных сигнализаций, должны быть устранены, в противном случае, в установленные сроки должны быть задействованы временные аварийные сигнализации или процедуры.

15.2.4 Требования к процедурам периодического испытания аварийной сигнализации

Аварийные сигнализации, для которых требуется выполнить испытание, должны быть подвергнуты испытательным процедурам.

15.2.5 Рекомендации к процедурам периодического испытания аварийной сигнализации

Процедуры должны содержать:

a) шаги, обеспечивающие вывод аварийной сигнализации из обслуживания, выполнение испытаний и перевод аварийной сигнализации в исходное состояние после испытания;

b) соответствующие предупреждения относительно контуров управления или исполнительных элементов, которые могли бы быть затронуты при испытании;

c) действия, связанные с использованием методов усовершенствования аварийной сигнализации, если это возможно.

15.2.6 Рекомендации к периодическим испытаниям аварийной сигнализации

Протоколы испытаний должны содержать следующее:

a) метод испытания;

b) запланированный интервал перед следующим испытанием.

Любые неполадки, найденные во время периодического испытания аварийной сигнализации, должны быть устранены в установленные сроки.

15.3 Вывод аварийных сигнализаций из обслуживания

15.3.1 Общие положения

Требования к процедуре вывода из обслуживания должны быть определены в требованиях к классу аварийных сигнализаций, как представлено в концепции аварийной сигнализации.

15.3.2 Требования к процессу вывода из обслуживания

Аварийные сигнализации, которые выведены из обслуживания в течение длительных периодов (например, дни, недели или месяцы) должны быть исследованы для определения необходимости временной аварийной сигнализации или процедуры.

Чтобы вывести аварийную сиг нализацию из обслуживания необходимо использовать процесс получения разрешения и процедуру документирования.

Для каждой выведенной из эксплуатации аварийной сигнализации должна быть учтена следующая информация:

a) имя тега аварийной сигнализации;

b) тип аварийной сигнализации;

c) детали разрешения для аварийной сигнализации;

d) детали, связанные с временной аварийной сигнализацией или процедурой, при необходимости;

e) причина вывода аварийной сигнализации из обслуживания.

15.3.3 Вывод из обслуживания наиболее важных аварийных сигнализаций

Если наиболее важная аварийная сигнализация выводится из обслуживания, то должны быть определены соответствующие временные аварийные сигнализации или процедуры, учитывая требования снижения риска и состояние предприятия.

15.3.4 Рекомендации к процессу вывода из обслуживания

Условия одобрения вывода аварийной сигнализации из обслуживания должны быть определены в концепции аварийной сигнализации. Продолжительность хранения документации должна быть определена в концепции аварийной сигнализации.

15.3.5 Требования к возвращению аварийных сигнализаций в эксплуатацию

Перед возвращением выведенных из обслуживания аварийных сигнализаций в состояние эксплуатации операторы должны быть уведомлены об этом, чтобы гарантировать, что они знают о возвращении аварийной сигнализации в эксплуатацию и об удалении временных методов.

Временные аварийные сигнализации и процедуры удаляются по возможности при возвращении в эксплуатацию первоначальных аварийных сигнализаций.

15.4 Ремонт оборудования

Информация, связанная с неправильными действиями аварийной сигнализации, должна быть доступна оператору. Аварийные сигнализации, связанные с нефункционирующим оборудованием (например, с оборудованием, которое снято с эксплуатации для ремонта или профилактического обслуживания), должны быть выведены из обслуживания, если эта проблема не будет решена в течение соответствующего времени, как определено в концепции аварийной сигнализации.

15.5 Замена оборудования

Процедуры управления изменениями производственного объекта реализуют обращение к оборудованию для замены (например, к устройствам измерения, клапанам, технологическому оборудованию), поэтому изменяются атрибуты аварийной сигнализации. Если замена выполнена, то в зависимости от класса аварийной сигнализации, определенной в концепции аварийной сигнализации, может требоваться подтверждение соответствия аварийной сигнализации.

15.6 Переподготовка персонала для технического обслуживания

15.6.1 Общие требования

Требования к переподготовке персонала для технического обслуживания аварийной сигнализации должны быть определены в требованиях к их классу, как представлено в концепции аварийной сигнализации.

15.6.2 Требования к переподготовке персонала по наиболее важным аварийным сигнализациям

Если используется класс наиболее важных аварийных сигнализаций, то персонал должен периодически проходить подготовку, осваивая конкретные требованиях к техническому обслуживанию всех наиболее важных аварийных сигнализаций. Периодичность обучения должна быть определена в концепции аварийной сигнализации. Документация, связанная с обучением, должна сохраниться в течение периода, определенного в концепции аварийной сигнализации или установленного в соответствии с политикой компании.

15.6.3 Рекомендации по переподготовке персонала в области аварийной сигнализации

Персонал по техническому обслуживанию должен получить переподготовку в области обеспечения требований к техническому обслуживанию аварийной сигнализации. Необходимо вести учет переподготовки, указывая, кто прошел обучение и дату прохождения. Необходимо провести оценку, чтобы гарантировать, что процедуры технического обслуживания производственного объекта без сомнения усвоены.

16 Контроль и оценка

16.1 Цель

Контроль и оценка — это отдельная стадия жизненного цикла. Эта стадия проверяет, что проектирование, внедрение, рационализация, эксплуатация и техническое обслуживание удовлетворяют соответствующим требованиям. В данном разделе представлены руководящие указания по использованию анализа системы аварийной сигнализации как для постоянного мониторинга, так и для периодической оценки ее рабочих характеристик. Эти действия используют во многом одни и те же типы мер. Несколько критериев качества работы рекомендуется включить в концепцию аварийной сигнализации.

Проблемы, выявленные с помощью контроля системы аварийной сигнализации, могут быть решены на нескольких различных стадиях жизненного цикла (например, проектирование, техническое обслуживание или управление изменениями) в зависимости от сути проблемы.

16.2 Требования

Производительность системы аварийной сигнализации должна находиться под контролем. Контроль и оценка производительности системы аварийной сигнализации должны выполняться на соответствие целевым уровням качества, которые представлены в концепции аварийной сигнализации.

16.3 Контроль, оценка, аудит и оценка параметров

Термины контроль, оценка, аудит и оценка параметров используются в следующем контексте:

- контроль — измерение и сообщение о количественных (объективных) аспектах производительности системы аварийной сигнализации;
- оценка — сравнение результатов контроля и дополнительных качественных (субъективных) измерений с установленными целями и заданными метриками производительности;
- аудит — комплексная оценка, включающая оценку эффективности методов работы, используемых для управления системой аварийной сигнализации;
- оценка параметров — начальный аудит системы аварийной сигнализации, разработанный, чтобы специально определить проблемные области в целях формирования планов по усовершенствованию.

Контроль, как правило, должен проводиться чаще оценки. Контроль некоторых аспектов производительности системы аварийной сигнализации основан на непрерывном измерении. Назначение контроля состоит в том, чтобы определить проблемы и выполнить корректирующие действия для их устранения.

Предметом процесса оценки является применение технической оценки и анализа, чтобы определить, хорошо ли работает система. Оценка рабочих процессов, связанных с системой аварийной сигнализации, представлена в разделе 18.

16.4 Контроль системы аварийной сигнализации

Контроль работы лежит в основе управления и усовершенствования. Система аварийной сигнализации со временем будет, вероятно, испытывать ухудшение работы, так как меняются длительность эксплуатации датчиков и условия технологического процесса, либо если политика управления изменениями аварийной сигнализации не действует. Продолжающееся измерение эксплуатационных характеристик может определить, когда необходимы корректирующие действия.

Когда аварийные сигнализации рационализированы и разработаны, а ложные аварийные сигналы (например, дребезжащие аварийные сигнализации) устранены, то результирующая интенсивность аварийных сигналов отражает способность системы управления поддерживать производственный процесс в известных пределах, не требуя вмешательства оператора. Решения для более высоких интенсивностей аварийных сигналов могут включать усовершенствования системы управления или технологического процесса, а не адаптации системы аварийной сигнализации. Могут быть необходимы методы повышения эффективности и усовершенствования аварийной сигнализации.

16.5 Метрики производительности системы аварийной сигнализации

16.5.1 Общие положения

Существуют различные виды анализа системы аварийной сигнализации, ключевые показатели производительности и методы. И начальная оценка системы аварийной сигнализации, и постоянный контроль должны включать меры, подобные представленным в таблице 7. Весь список выбранных видов анализа должен отражать решения, принятые в концепции аварийной сигнализации.

Типовая система аварийной сигнализации описывается двумя категориями данных: записями об аварийных сигналах (т. е. динамическими или данными реального времени) и атрибутами аварийной сигнализации (т. е. уставками аварийной сигнализации или данными о конфигурации). Обе категории важны при измерении производительности системы аварийной сигнализации и анализируются они различным методами:

a) записи об аварийных сигналах содержат связанную с аварийной сигнализацией информацию и создаются системой, когда аварийная сигнализация появляется;

b) атрибуты аварийной сигнализации формируют основополагающую структуру, которая необходима для создания записей об аварийных сигналах, включая типы аварийных сигнализаций, уставки аварийных сигнализаций, приоритеты, мертвые зоны и подобные элементы.

Обычно для вычисления метрик желательно иметь данные, по крайней мере, за тридцатидневный период. Для групповых операций более применимы данные, соответствующие нескольким аналогичным партиям.

Целевые метрики, описанные ниже, приблизительны и зависят от многих факторов (например, тип технологического процесса, опыт оператора, ЧМИ, степень автоматизации, операционная среда, типы и значимость формируемых аварийных сигналов). Максимальные приемлемые числа аварийных сигналов могли быть значительно ниже или, возможно, немного выше в зависимости от этих факторов. Одна только интенсивность аварийных сигналов не является индикатором приемлемости.

16.5.2 Средняя интенсивность аварийных сигналов для пульта оператора

Анализ интенсивности аварийных сигналов (т. е. интенсивность оповещающих о себе аварийных сигнализаций) является хорошим индикатором общего состояния системы аварийной сигнализации. Рекомендуемые цели для средней интенсивности аварийных сигналов для пульта оператора (т. е. норма контроля и ответственность за аварийный сигнал отдельного оператора), основанные на данных для одного месяца, показаны в таблице 5. Эти интенсивности основаны на способности оператора и времени, необходимом для обнаружения аварийного сигнала, диагностики ситуации, ответа с корректирующим действием (действиями) и контроля условия, обеспечивающего проверку того, что неправильное условие было исправлено.

Таблица 5 — Средние интенсивности аварийных сигналов

Приемлемое количество	Максимально управляемое количество
Примерно 144 аварийных сигналов в день	Примерно 288 аварийных сигналов в день
Примерно 6 аварийных сигналов в час (в среднем)	Примерно 12 аварийных сигналов в час (в среднем)
Примерно 1 аварийный сигнал за 10 минут (в среднем)	Примерно 2 аварийных сигнала за 10 минут (в среднем)

Длительная эксплуатация количества аварийных сигналов выше рекомендуемого максимально управляемого значения указывает на то, что система аварийной сигнализации оповещает о большем числе аварийных сигналов, чем оператор может обработать, и об увеличении вероятности потери аварийных сигналов.

Отрезок времени, за который возникает больше аварийных сигналов, чем оператор может обработать, увеличивает вероятность пропущенных аварийных сигналов, даже если среднее число для всего интервала приемлемо.

16.5.3 Пиковая интенсивность аварийных сигналов для пульта оператора

Интенсивности аварийных сигналов, равные десяти или более за десятиминутный период времени могут превысить способность оператора эффективно отвечать на аварийные сигналы или привести к их пропуску. Интенсивности, приближающиеся к десяти аварийным сигналам за 10 мин, не могут стабильно обрабатываться оператором в течение длительного периода времени.

Для анализа пиковой интенсивности аварийных сигналов подсчитываются оповещающие аварийные сигнализации регулярно за каждые 10 мин (например, с 13:00 до 13:09). Рекомендуемая цель, соответствующая данным за один месяц, состоит в том, чтобы примерно меньше 1 % десятиминутных интервалов содержали больше 10 аварийных сигналов.

И пиковые и средние интенсивности аварийных сигналов должны быть учтены одновременно, так как любое отдельное измерение может вводить в заблуждение. О количестве интервалов, превышающих 10 аварийных сигналов, и о величине наибольших ликов необходимо сообщать.

16.5.4 Переполнение аварийных сигналов

Переполнение аварийных сигналов происходит в периоды времени переменной длительности, во время которых аварийные сигналы появляются с интенсивностью оповещения, возможно, превышающей способность оператора ответить на них. Во время переполнения аварийных сигналов система аварийной сигнализации, вероятно, не является эффективным помощником оператора.

Расчеты для определения переполнения аварийных сигналов включают определение смежных периодов времени, где интенсивность аварийных сигналов высокая, формируя, таким образом, полное событие переполнения.

Начало переполнения аварийных сигналов указывается первым регулярным десятиминутным интервалом с интенсивностью аварийных сигналов, превышающей 10 аварийных сигналов за 10 мин. Окончание переполнения аварийных сигналов определяется первым регулярным десятиминутным интервалом с интенсивностью аварийных сигналов, не превышающей пяти аварийных сигналов за 10 мин. Переполнения аварийных сигналов должны быть кратковременными и с небольшим общим количеством аварийных сигналов. Как рекомендуемая цель, система аварийной сигнализации должна находиться в состоянии переполнения примерно меньше 1 % времени.

Необходимость усовершенствования системы аварийной сигнализации и технологического процесса может быть определена в результате анализа переполнения аварийных сигналов. Цели для этих метрик не определены. Анализ переполнения аварийных сигналов должен включать:

a) количество переполнений аварийных сигналов;

b) продолжительность каждого переполнения аварийных сигналов;

c) количество аварийных сигналов в каждом переполнении аварийных сигналов;

d) пиковая интенсивность переполнения аварийных сигналов для каждого переполнения аварийных сигналов.

Методы усовершенствования аварийной сигнализации могут ослабить переполнения аварийных сигналов, поэтому может возникнуть необходимость их привлечения. Эти методы описаны в разделе 12.

16.5.5 Частота появления аварийных сигналов

Относительно немного отдельных аварийных сигналов (например, 10—20 аварийных сигналов) часто составляют наибольший процент от общей нагрузки на систему аварийной сигнализации (на-

пример, от 20 % до 80 %). Наиболее частые аварийные сигналы должны рассматриваться регулярно (например, ежедневно, еженедельно или ежемесячно). Решая проблемы с наиболее часто появляющимися аварийными сигналами, можно существенно повысить производительность системы.

Методология анализа должна использовать, по крайней мере, данные за несколько недель и записи обо всех аварийных сигналах от наиболее до наименее часто появляющихся. Наиболее частые аварийные сигналы, вероятно, говорят о неправильном функционировании или о некорректной разработке. Наиболее часто появляющиеся аварийные сигналы обычно больше всего искажают другие показатели эффективности.

Десять наиболее часто появляющихся аварийных сигналов должны составлять небольшой процент общей нагрузки на систему (например, от 1 % до 5 %). Действия, выполняемые в результате этого анализа, включают анализ правильного функционирования и корректности проекта.

16.5.6 Дребезжащие и кратковременные аварийные сигнализации

Дребезжащий аварийный сигнал повторно появляется при каждом переходе между состоянием аварии и исходным состоянием в течение короткого периода времени. Кратковременные аварийные сигналы являются подобными аварийными сигналами короткой продолжительности, но которые не повторяются немедленно. В обоих случаях переход происходит не в результате действия оператора.

Для дребезжащей аварийной сигнализации, которая повторяется три раза или более за одну минуту, часто используют этот порог в качестве идентификации наихудших динамических аварийных сигналов первого уровня. Могут использоваться и другие значения.

Для дребезжащей аварийной сигнализации за несколько часов может быть сгенерировано сотни или тысячи записей. Это значительно отвлекает операторов. Динамических аварийных сигналов часто бывает больше всего в списке наиболее часто появляющихся аварийных сигналов. Дребезжащие и кратковременные аварийные сигналы должны быть устранены. Не существует никакого установившегося приемлемого количества дребезжащих и кратковременных аварийных сигналов.

16.5.7 Просроченные аварийные сигнализации

Аварийные сигнализации, которые остаются постоянно активными более 24 ч, можно считать просроченными аварийными сигнализациями. Для устранения таких аварийных сигналов могут использоваться методы усовершенствования аварийной сигнализации.

Просроченных аварийных сигналов должно быть меньше пяти.

16.5.8 Распределение приоритета оповещающих аварийных сигнализаций

Эффективное использование приоритета аварийных сигнализаций может увеличить способность оператора управлять аварийными сигнализациями и предоставлять ответ. Эффективность приоритета аварийных сигнализаций связана с распределением их приоритетов: более высокие приоритеты должны использоваться менее часто.

Таблица 6 — Распределение приоритета оповещающих аварийных сигнализаций

Обозначение приоритетов	Процентное распределение
3 приоритета: низкий, средний, высокий	Низкий — примерно 80 %; средний — примерно 15 %; высокий — примерно 5 %
4 приоритета: низкий, средний, высокий, очень высокий	Низкий — примерно 80 %; средний — примерно 15 %; высокий — примерно 5 %; очень высокий — примерно < 1 %

Некоторые системы аварийной сигнализации используют дополнительный высший приоритет для нескольких аварийных сигналов с серьезными последствиями.

Могут быть полезны дополнительные приоритеты, такие как очень низкий приоритет для аварийного сигнала аварийной сигнализация диагностики прибора с очень ограниченным действием оператора. Не существует рекомендуемой частоты или процентного распределения для диагностических аварийных сигнализаций, так как нет никакой рекомендуемой частоты отказов прибора. Низкие значения — лучшее решение.

Для специальных случаев иногда используются различные приоритеты при ограничении оповещения (например, для незвуковой индикации аварийных сигнализаций). Не существует рекомендуемого распределения приоритетов при ограничении оповещения.

Распределения с большим разбросом этих процентных значений могут снизить ценность установления приоритетов и они обычно указывают на устанавливаемые приоритеты аварийных сигнали-

заций, которые не следуют из согласованной методологии рационализации аварийных сигнализаций. Нормальным решением является эффективная рационализация.

16.5.9 Распределение приоритетов аварийных сигнализаций

Усилие по эффективной рационализации аварийных сигнализаций сформирует распределение приоритетов оповещающих аварийных сигнализаций, подобно представленному в таблице 6. Распределение приоритетов оповещающих аварийных сигнализаций не будет соответствовать распределениям приоритетов рационализированных аварийных сигнализаций, так как все аварийные сигналы не появляются равновероятно. Для систем аварийной сигнализации, которые не позволяют установление приоритетов для аварийных сигнализаций приборов или диагностических систем, такие аварийные сигнализации могут быть исключены из вычислений распределения с учетом приоритета, чтобы предотвратить ассиметричное распределение.

16.6 Запрещение несанкционированных аварийных сигналов

Все состояния аварийной сигнализации отложенной, запрещенной в соответствии с проектом и выведенной из обслуживания рассматриваются как управляемые методологии. Аварийные сигнализации могут быть запрещены без этих методологий. Несанкционированное запрещение аварийных сигнализаций необходимо выявлять и отражать в отчетности. Высока вероятность ошибок и результирующего риска.

В отчетности должны быть отражены переходы аварийных сигнализаций в запрещенные состояния и из запрещенных состояний. Должны использоваться методы анализа для обнаружения и отражения в отчетности любых аварийных сигналов, запрещенных без перечисленных выше методологий. Не должно быть никаких аварийных сигналов, которые запрещены без разрешения.

16.7 Контроль атрибутов аварийных сигнализаций

Несанкционированные изменения атрибутов аварийных сигнализаций следует выявлять и принимать по ним решения, используя сравнения фактических атрибутов аварийных сигнализаций с информацией о рационализации. Также следует определить несоответствия и быстро принять по ним решения. Целевое значение для несанкционированных изменений аварийных сигнализаций равно нулю.

16.8 Предоставление аналитических отчетов по системе аварийной сигнализации

Аналитические отчеты по системе аварийной сигнализации необходимо предоставлять персоналу (например, операторам, сотрудникам и аппарату управления), связанному с системой аварийной сигнализацией с соответствующей частотой.

На различных стадиях внедрения усилий по дальнейшему развитию должны выполняться аналитические отчеты за различные отчетные периоды (например, предоставление еженедельных отчетов в начале внедрения усилий и ежемесячных отчетов в дальнейшем). Еженедельные аналитические отчеты также могут охватывать данные предшествующих тридцати дней, чтобы сформировать существующие тенденции. Концепция аварийной сигнализации должна определить формы аналитических отчетов и периодичности их предоставления.

По проблемам, определенным в аналитических отчетах о системе аварийной сигнализации, должны быть приняты меры. Ход выполнения и результаты действий необходимо регулярно отражать в отчетности.

16.9 Общая сводка метрик производительности системы аварийной сигнализации

Метрики производительности аварийной сигнализации и типовые целевые значения, ранее описанные, с теми же классификациями, представлены в таблице 7.

Таблица 7 — Рекомендуемая общая сводка метрик производительности аварийной сигнализации

Метрики производительности аварийной сигнализации, основанные, по крайней мере, на данных за 30 дней		
Метрика	Целевое значение	
Оповещающие аварийные сигналы	Целевое значение: весьма вероятно, было приемлемо	Целевое значение: максимально управляемое количество
Оповещающие аварийные сигналы в день для пульта оператора	Примерно 144 аварийных сигналов	Примерно 288 аварийных сигналов в день
Оповещающие аварийные сигналы в час для пульта оператора	Примерно 6 (в среднем)	Примерно 12 (в среднем)
Оповещающие аварийные сигналы за 10 м для пульта оператора	Примерно 1 (в среднем)	Примерно 2 (в среднем)
Метрика	Целевое значение	
Процент часов, содержащих более 30 аварийных сигналов	Примерно < 1 %	
Процент десятиминутных периодов, содержащих более 10 аварийных сигналов	Примерно < 1 %	
Максимальное число аварийных сигналов в десятиминутном периоде	≤ 10	
Процент времени, в котором система аварийной сигнализации находится в условиях переполнения	Примерно < 1 %	
Процентный вклад десяти аварийных сигналов с наибольшей частотой в общем объеме аварийных сигналов	Примерно от <1 % до 5 % максимально, с планами действий по устранению неполадок	
Количество дребезжащих и кратковременных аварийных сигналов	Ноль, планы действий по корректировке любых из этих аварийных сигналов	
Просроченные аварийные сигнализации	Менее 5 в любой день, с планами действий по их устранению	
Распределение приоритета оповещающих аварийных сигналов	3 приоритета: низкий — примерно 80 %; средний — примерно 15 %; высокий — примерно 5 % или 4 приоритета: низкий — примерно 80 %; средний — примерно 15 %; высокий — примерно 5 %; очень высокий — примерно < 1 %. Другие специализированные приоритеты (например, для аварийных сигнализаций системы диагностики) не включены в вычисление	
Запрещение несанкционированных аварийных сигнализаций	Ноль аварийных сигналов, запрещенных неуправляемыми или неразрешенными методологиями	
Несанкционированные изменения атрибутов аварийных сигнализаций	Ноль изменений атрибутов аварийных сигналов неразрешенными методологиями или не средствами управления изменениями	

17 Управление изменениями

17.1 Цель

Управление изменениями является отдельной стадией жизненного цикла. Настоящий раздел охватывает требования к изменениям системы аварийной сигнализации, связанные с добавлением новых аварийных сигнализаций, удалением существующих аварийных сигнализаций, модификацией атрибутов аварийных сигнализаций, получением разрешения и документальным оформлением. Цель управления изменениями состоит в том, чтобы гарантировать, что изменения разрешены и удовлетворяют критериям оценки, описанным в концепции аварийной сигнализации. Управление процессом изменений гарантирует, что действия, выполняемые на жизненном цикле, применены к изменениям системы аварийной сигнализации.

17.2 Процедура управления изменениями

Для выполнения добавления или удаления аварийных сигнализаций, а также модификации указанных атрибутов необходимо получение разрешения, формируемого процедурой управления изменениями. Постоянные изменения, которые приводят к расхождению с разрешенными значениями уставки, класса, приоритета, последствия, обоснования, логики запрещения или времени ответа аварийной сигнализации, требуют оценки, которая выполняется процедурой управления изменениями.

Процедура управления изменениями должна гарантировать рассмотрение следующих вопросов:

a) техническое обоснование для предложенного изменения;

b) влияние изменения на здоровье, безопасность и окружающую среду;

c) выполнение модификаций в соответствии с концепцией аварийной сигнализации;

d) выполнение модификаций для рабочих процедур;

e) обоснование периода времени выполнения каждого изменения;

f) требования к разрешению для предложенного изменения;

g) сохранение уровня безопасности, если аварийный сигнал связан с обеспечением безопасности;

h) привлечение к выполнению анализа соответствующих специалистов;

i) изменения системы аварийной сигнализации следуют за всеми соответствующими последовательными действиями по управлению ее жизненным циклом;

j) внедрение всех изменений выполняется в соответствии с процедурами, определенными в концепции аварийной сигнализации.

17.3 Требования к изменению документации

Требования к изменению документации должны быть определены на основе классификации аварийных сигнализаций и требований к классу, как подробно описано в концепции аварийной сигнализации.

Для одобренных изменений должно быть отражено в отчетности следующее:

a) причина изменения;

b) дата выполнения изменения;

c) имя лица, осуществляющего изменение;

d) имя лица, разрешающего изменение;

e) суть изменения (т. е. до и после);

f) требования к подготовке персонала;

g) требования к испытаниям.

17.4 Рекомендации к изменению документации

В результате изменений системы аварийной сигнализации, требуются изменения связанных с ней компонентов и документации, которые должны быть отражены в отчетности как часть отчета об изменениях. Эти отчеты должны:

a) быть защищены от несанкционированной модификации, разрушения или потери;

b) пересматриваться, исправляться, рассматриваться и одобряться в соответствии с процедурой управления документацией;

c) храниться в период времени, определенный политикой хранения документации производственного объекта;

d) администрироваться в соответствии с требованиями к классу, представленными в концепции аварийной сигнализации.

17.5 Рекомендации по удалению аварийных сигнализаций

Если в аварийной сигнализации больше нет необходимости, то она должна быть удалена из системы аварийной сигнализации. Отображения и связанная с удалением документация должны быть изменены в течение соответствующего времени.

17.6 Рекомендации по модификации атрибутов аварийных сигнализаций

Следует формировать и поддерживать список ссылок на необходимые материалы (например, графику, логику управления, P&ID, рабочие процессы и HAZOP). Этот справочный список следует рассмотреть до внесения изменений в аварийные сигнализации. Это предотвращает введение неправильной информации в документацию и помогает предотвратить ошибки временной логики автоматизации и графики.

18 Аудит

18.1 Цель

Аудит является отдельной стадией жизненного цикла, которая выполняется периодически для поддержания целостности системы аварийной сигнализации и процессов менеджмента аварийной сигнализации. Аудит производительности системы позволяют обнаружить недостатки, не очевидные при обычном контроле. Кроме того, выполняется аудит на соответствие концепции аварийной сигнализации, чтобы определить любые требования для улучшений системы, таких как модификации концепции аварийной сигнализации или определенных там рабочих процессов.

Аудит рассматривает методы управления и работы, связанные с системой аварийной сигнализации. Он определяет, достаточно ли этих методов, чтобы адекватно управлять системой, рассматривая соответствие методов процедурам, а процедур политике или требованиям. Аудит также включает сравнение методов менеджмента аварийной сигнализации с отраслевыми руководствами.

Аудит выполняется с меньшей частотой по сравнению с контролем и оценкой.

18.2 Оценка параметров

18.2.1 Общие положения

Перед действиями по дальнейшему развитию для всех аспектов менеджмента аварийной сигнализации следует выполнить аудит. Первичный аудит или оценка параметров должны быть выполнены с помощью документально оформленных методов (например, методов, перечисленных в настоящем стандарте). Оценка параметров включает начальную итерацию аудита технологического процесса, чтобы охватить все, что связано с рабочим процессом. Результаты первичного аудита могут использоваться для развития концепции.

18.2.2 Требования к первичному аудиту или оценке параметров

Частота аудита и конкретные требования аудита, указанные в концепции аварийной сигнализации, должны быть определены для всех аварийных сигнализаций, как это требуется для класса аварийных сигнализаций.

Аудит должен удовлетворять всем применимым требованиям настоящего стандарта.

18.3 Опросы для аудита

Опросы персонала или анкетирования должны выполняться, как часть аудита, чтобы определить проблемы производительности и эксплуатации. Темы опросов могут включать:

a) аварийные сигналы происходят только при условиях, требующих действия оператора;

b) приоритет аварийных сигнализаций применяется единообразно и имеет важное значение;

c) аварийные сигналы появляются до выполнения эффективных действий, которые могут быть привлечены;

d) определение функции и сферы ответственности пользователей системы аварийной сигнализации и вспомогательного персонала;

e) эффективность обучения, связанного с использованием и функционированием системы аварийной сигнализации.

18.4 Рекомендации по аудиту

Для концепции аварийной сигнализации должен быть выполнен аудит на соответствие отраслевым руководствам, а также требованиям и рекомендациям настоящего стандарта. Для обеспечения эффективности для рабочих процессов и процедур, которые гарантируют соответствие с концепцией аварийной сигнализации, должна периодически выполняться оценка. Аудит должен рассмотреть всю соответствующую документацию, которая может включать:

a) проверку того, что аварийные сигнализации требуют действий от оператора, предотвращающих определенные последствия;

b) документацию на атрибуты и рационализацию аварийных сигнализаций;

c) документацию по управлению изменениями для модификаций атрибутов аварийных сигнализаций в общей базе данных аварийных сигналов;

d) отчеты контроля работы аварийной сигнализации;

e) документацию на ремонтные работы, неправильно сработавших аварийных сигнализаций;

f) документацию на выведенные из обслуживания аварийные сигнализации.

18.5 Планы действий

Планы действий должны быть разработаны для проблем, выявленных во время выполнения аудита. При определении плана действий для каждого его пункта должны быть назначены сроки, виды отчетности и согласование полученных результатов.

Библиография

[1] IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector

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

[3] IEC 62241, Nuclear power plants — Main control room — Alarm functions and presentation

[4] IEC 62541-9, OPC unified architecture — Part 9: Alarms and conditions

[5] Alarm Management, NAMUR-Worksheet NA 102, 3rd Edition, NAMUR-Geschäftsstelle, Leverkusen, Germany (2008)

[6] ANSI/ISA-18.02-2009, Management of Alarm Systems for the Process Industries

[7] Engineering Equipment Materials Users' Association, Alarm Systems — A Guide to Design, Management and Procurement, EEMUA Publication No. 191, 2nd Edition, EEMUA, London, UK (2007).

[8] Engineering Equipment Materials Users' Association, Alarm Systems. — A Guide to Design, Management and Procurement. EEMUA Publication No. 191, 2nd edition. London: EEMUA, 2007

УДК 621.396/.397.001.4:006.354 ОКС 13.110

Ключевые слова: аварийный сигнал, аварийная сигнализация, система аварийной сигнализации, менеджмент жизненного цикла аварийной сигнализации, человеко-машинный интерфейс, основная система управления процессом, оператор

БЗ 9—2019/53

Редактор *Е.А. Моисеева*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 12.08.2019. Подписано в печать 16.08.2019. Формат 60×84¼. Гарнитура Ариал
Усл. печ. л. 7,91. Уч.-изд. л. 7,15.

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.
www.gostinfo.ru info@gostinfo.ru