ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 366.4— 2019

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 4

Верификация полноты аппаратных средств автоматизированной системы безопасности

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2019 г. № 40-пнст

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

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

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

© Стандартинформ, оформление, 2019

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Сокращения и обозначения 2
4 Термины и определения 2
5 Конструкция приборной системы безопасности 2
6 Работоспособность конструкции, требования к отказоустойчивости аппаратных средств 3
7 Вероятность возникновения отказа по запросу устройства обеспечения безопасности 5
7.1 Допущения. Основные положения 5
7.2 Общая процедура определения вероятности PFD 6
7.3 Приближенная формула определения вероятности наступления отказа в гомогенных системах 7
8 Определение характеристик надежности устройств 8
8.1 Данные изготовителя 8
8.2 Базы данных, составленные по результатам полевых испытаний 9
9 Типовые конструкции приборной системы безопасности 9
10 Полнота безопасности аппаратных средств опытного образца конструкции 10
10.1 Верификация конструкции, содержащей группу датчиков типа 2oo3 и группу пусковых устройств типа 1oo2, с помощью полевых устройств с качеством «проверено-на-практике» 10
10.2 Верификация конструкции, содержащей группу датчиков типа 1oo3 и две группы пусковых устройств типа 1oo2, с помощью полевых устройств с качеством «проверено-на-практике» 11
10.3 Верификация конструкции, содержащей группу датчиков типа 1oo2 и группу пусковых устройств типа 1oo2, с помощью полевых устройств с качеством «проверено-на-практике», сертифицированных на уровень обеспечения безопасности SIL 13

Введение

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

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

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

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 4

Верификация полноты аппаратных средств автоматизированной системы безопасности

Industrial automation systems and integration. Safety arrangements of industrial plants by means of process control engineering. Part 4. Verification of the hardware of safety instrumented system

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

1 Область применения

Настоящий стандарт устанавливает метод верификации требуемого уровня полноты безопасности (SIL) аппаратных средств приборной системы безопасности (SIS) и применяется совместно с другими стандартами настоящего комплекса стандартов.

Процедура верификации в соответствии с настоящим стандартом должна состоять из двух этапов. На первом этапе осуществляется оценка работоспособности конструкции приборной системы безопасности. На втором этапе рассматриваемой приборной системе безопасности назначается уровень полноты безопасности. Данный уровень зависит от вероятности возникновения отказа устройств (PFD), связанных с обеспечением безопасности. Необходимо учитывать влияние нижеследующих факторов:

- выбор оборудования и его надежность;
- конструкция устройства;
- интервалы между контрольными проверками приборной системы безопасности.

Примечание — Существуют два класса технологических процессов: 1) с качеством «проверено-на-практике» (на основе опыта предшествующего применения), 2) с проверенным типом. Они должны исключать наступление систематических сбоев соответствующих устройств. Устройства с качеством «проверено-на-практике» и устройства с проверенным типом должны рассматриваться одинаково в части устранения 1) систематических сбоев и 2) мнимых сбоев.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р МЭК 61508-6—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения

Издание официальное

(принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Сокращения и обозначения

В настоящем стандарте использованы следующие сокращения и обозначения:

FMEDA — методика анализа отказов, их последствий и диагностики (failure mode effect and diagnostics analysis);

HFT — отказоустойчивость аппаратных средств (hardware fault tolerance);

HPC — контроллер с жестко зашитой программой (hard-wired programmed controller);

MDT — среднее время простоя (mean downtime);

MooN (M-out-of-N) — комбинация M элементов из N. Комбинация справедлива при $M \leq N$;

MTBF — среднее время наработки на отказ (mean time between failures);

MTTD — среднее время обнаружения отказа (mean time to detection);

MTTF — среднее время наработки до отказа (mean time to failure);

MTTR — среднее время до восстановления (системы после отказа) (mean time to restoration);

PFD — вероятность отказа при наличии запроса (probability of failure on demand);

PFD_{FE} — вероятность PFD отказа конечного элемента подсистемы (PFD of subsystem final element);

PFD_{L} — PFD of subsystem logic solver (вероятность PFD отказа логического решателя подсистемы);

PFD_{MooN} — вероятность PFD наступления отказа комбинации M элементов из N (MooN) в подсистеме приборной системы безопасности (PFD of MooN group in a subsystem of an SIS);

PFD_{S} — вероятность PFD наступления отказа датчика подсистемы (PFD of subsystem sensor);

PFD_{Total} — вероятность PFD наступления неисправности приборной системы безопасности SIS в целом (PFD of complete SIS);

SFF — доля безопасных отказов (safe failure fraction);

SIF — функция безопасности приборной системы безопасности (safety instrumented function);

SIL — уровень полноты безопасности (safety integrity level);

SPLC — программируемый логический контроллер устройства обеспечения безопасности (safety related programmable logic controller);

T_1 — интервал между контрольными проверками;

β — доля не выявленных пассивных сбоев с общей причиной;

λ — интенсивность наступления всех (как активных, так и пассивных) сбоев;

λ_D — интенсивность наступления опасных пассивных сбоев;

λ_{DD} — интенсивность наступления опасных выявленных пассивных сбоев;

λ_{DU} — интенсивность наступления опасных не выявленных пассивных сбоев;

λ_S — интенсивность наступления безопасных активных сбоев.

Примечание — Также достаточно часто используются аббревиатуры PCE (устройства автоматического управления производственными процессами), MC (управление и контроль), EMC (электрические, управляющие и контрольные устройства).

4 Термины и определения

В настоящем стандарте применен следующий термин с соответствующим определением:

4.1

отказоустойчивость (fault tolerance): Способность функционального элемента продолжать выполнять требуемую функцию при наличии сбоев или ошибок.

[ГОСТ Р МЭК 61511-1, статья 3.2.21]

5 Конструкция приборной системы безопасности

Приборная система безопасности должна состоять из трех основных подсистем (см. рисунок 1):

- подсистема датчиков;
- программируемый логический контроллер;

- подсистема пусковых устройств приводных механизмов (исполнительные элементы).

Подсистемы датчиков и подсистемы пусковых устройств могут, в свою очередь, включать несколько групп датчиков и несколько групп пусковых устройств.

Для обеспечения работы функции безопасности необходима каждая из указанных групп. Группа M элементов из N включает N каналов, из которых требуется выбрать M элементов.

Примечание — Обычно датчики (определенных типов) отдельно и пусковые устройства (определенных типов) отдельно как части приборной системы безопасности образуют одну отдельную группу для каждого типа.

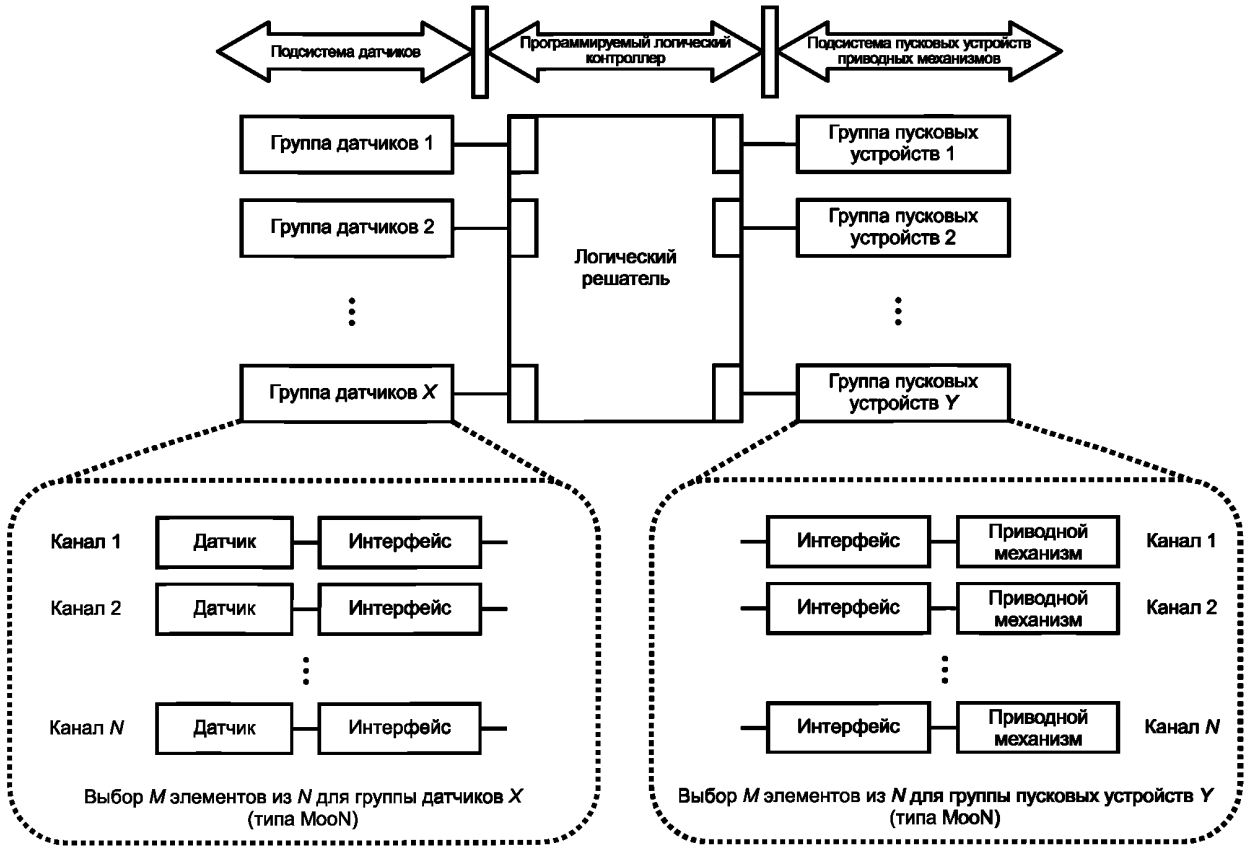


Рисунок 1 — Структура приборной системы безопасности

6 Работоспособность конструкции, требования к отказоустойчивости аппаратных средств

Обеспечение работоспособности конструкции приборной системы безопасности невозможно без обеспечения отказоустойчивости HFT ее аппаратных средств (см. раздел 4).

И наоборот, обеспечение отказоустойчивости HFT аппаратных средств — необходимое условие надлежащего функционирования приборной системы безопасности.

Подсистемы датчиков, логические устройства и подсистемы пусковых устройств приборной системы безопасности должны иметь минимальную отказоустойчивость HFT в соответствии с ГОСТ Р МЭК 61511-1.

Примечание 1 — Отказоустойчивость HFT — это способность устройства (подсистемы) выполнять требуемые функции, связанные с обеспечением безопасности даже при наличии одного или нескольких опасных сбоев аппаратных средств. Аббревиатура HFT 1 означает, что имеется, например, два устройства и опасный сбой одного устройства не препятствует принятию мер обеспечения безопасности.

Примечание 2 — Отказоустойчивость HFT компенсирует возможные отказы, возникающие при задействовании приборной функции безопасности (SIF). Отказоустойчивость — базовое свойство конструкции.

Она должна обеспечиваться в условиях неизвестной заранее интенсивности наступления отказов устройств (подсистем) в различных приложениях производственного процесса.

Примечание 3 — Важно, чтобы выполнение требований обеспечения отказоустойчивости HFT не сводилось к бесконечному запараллеливанию устройств (подсистем). Тем не менее для подтверждения назначенного уровня SIL (функции безопасности SIF) может оказаться необходимым запараллелить рассматриваемое устройство (в зависимости от вида приложения, интенсивности наступления отказов и интервала между контрольными проверками и т. п.).

Для логических подсистем целесообразно использовать сертифицированные логические контроллеры устройств обеспечения безопасности SPLC, для которых изготовителем уже приняты соответствующие меры обеспечения отказоустойчивости HFT. Использование сертифицированных контроллеров HPC с «жестко зашитой» программой в настоящем стандарте не рассматривается.

Если большинство сбоев полевых устройств (подсистем датчиков, подсистем пусковых устройств и т. п.) сравнительно безопасны (в зависимости от приложения, а также для устройств, работающих по принципу «обесточить для аварийного отключения») или легко выявляются (например, путем соответствующей диагностики), то можно использовать архитектуру, указанную в таблице 1. Необходимо принять во внимание:

- место полевого устройства в технологическом процессе;
- значимость диагностической информации о полевом устройстве для валидации его рабочих сигналов;
- возможность использования доступных свойств отказоустойчивости полевого устройства (например, реализацию принципа «обесточить для аварийного отключения» и т. п.).

Таблица 1 — Минимально допустимое значение отказоустойчивости HFT и примеры архитектуры полевых устройств с назначенным уровнем полноты безопасности SIL для заданной приборной функции безопасности SIF.

SIL	HFT	Примеры архитектуры полевых устройств
1	0	1oo1, 2oo2
2	1	1oo2, 2oo3
3	2	1oo3
4	Не рекомендуется	

Если указанные условия не выполняются, то отказоустойчивость HFT приобретает значение HFT 1, увеличенное на 1 (см. примечание 1 выше). Отказоустойчивость уровня HFT 1 может оказаться необходимой для достижения уровня полноты безопасности SIL 1.

При определенных обстоятельствах значение отказоустойчивости HFT, определенное таблицей 1, можно уменьшить на 1 (см. таблицу 2). Обязательными условиями этого являются:

- использование только устройств на основе опыта предшествующего применения («проверено-на-практике»), см. раздел 11.5.3 ГОСТ Р МЭК 61511-1—2018;
- устройствам можно задавать настройки, только относящиеся к технологическому процессу (например, диапазон управления, направление прохождения сигнала в случае отказа и т. п.);
- задание настроек параметров технологического процесса должно быть защищено от несанкционированного доступа (например, перемычкой, паролем и т. п.).

Таблица 2 — Минимальное значение отказоустойчивости HFT и примеры архитектур специально квалифицированных полевых устройств на основе опыта предшествующего применения (с качеством «проверено-на-практике») для назначенного уровня полноты безопасности SIL приборной системы безопасности SIF.

SIL	HFT	Примеры архитектур специально квалифицированных полевых устройств (с качеством «проверено-на-практике»)
1	0	1oo1, 2oo2
2	0	1oo1, 2oo2
3	1	1oo2, 2oo3
4	Не рекомендуется	

7 Вероятность возникновения отказа по запросу устройства обеспечения безопасности

Приборные системы безопасности обычно вмешиваются в производственный процесс только в случае крайней необходимости. Соответственно, вероятность PFD возникновения отказа самого устройства обеспечения безопасности — это мера его простоя. Перед вычислением значения вероятности PFD упрощенным методом, описанным далее, необходимо принять некоторые допущения, обычно справедливые для производственного процесса.

7.1 Допущения. Основные положения

а) Интенсивность наступления отказов аппаратных средств устройств не изменяется с течением времени (является константой).

б) Значения интенсивности наступления отказов аппаратных средств (исходные данные) задаются только для одного канала (подсистемы). Они основаны на стандартизованных данных изготовителя и/или на коммерческих статистических оценках.

в) Интервал диагностики должен быть на порядок меньше интервала между испытаниями. Интенсивность наступления выявленных (дополнительной диагностикой) опасных пассивных сбоев λ_{DD} пренебрежимо мала по сравнению с интенсивностью наступления не выявленных (указанной диагностикой) опасных пассивных сбоев λ_{DU}, обнаруживаемых только испытаниями рабочих функций (с учетом заданного интервала между испытаниями).

г) Время между двумя запросами должно быть на порядок больше среднего времени восстановления.

д) Только пассивные сбои создают угрозу безопасности;

е) Интервал между испытаниями достаточно мал по сравнению со средним временем наработки на отказ, то есть $T_1 << MTBF$.

ж) Среднее время до восстановления (системы после отказа) достаточно мало по сравнению с интервалом между испытаниями, то есть $MTTR << T_1$.

и) В соответствии с допущениями (е) и (ж) среднее время простоя достаточно мало по сравнению со средним временем наработки до отказа, то есть $MDT << MTTF$.

к) Все сбои, возникающие во время испытаний, обнаруживаются во время данных испытаний. После ремонта номинальный статус безотказной работы установки восстанавливается.

л) Результат умножения интенсивности наступления выявленных пассивных сбоев на интервал между испытаниями всегда много меньше единицы, то есть $\lambda_{DU} \cdot T_1 << 1$.

Указанные допущения сохраняют силу во всех нижеследующих разделах настоящего стандарта.

Рабочие данные ниже объясняются в контексте значений надежности приборной системы безопасности SIS.

Среднее время простоя MDT — это сумма среднего времени обнаружения отказа MTTD и среднего времени до восстановления (системы после отказа) установки MTTR:

$$MDT = MTTD + MTTR. \quad (1)$$

Сумма среднего времени наработки до отказа MTTF и среднего времени простоя MDT — это среднее время наработки на отказ MTBF:

$$MTBF = MTTF + MDT. \quad (2)$$

В соответствии с допущением (h) можно считать, что:

$$MTBF \approx MTTF. \quad (3)$$

Среднее время штатной работы технологической линии до наступления очередного отказа MTTF — величина обратная общей интенсивности наступления отказов λ:

$$MTTF = \frac{1}{\lambda}. \quad (4)$$

Порядок сопряжения рассматриваемых интервалов времени приведен на рисунке 2.

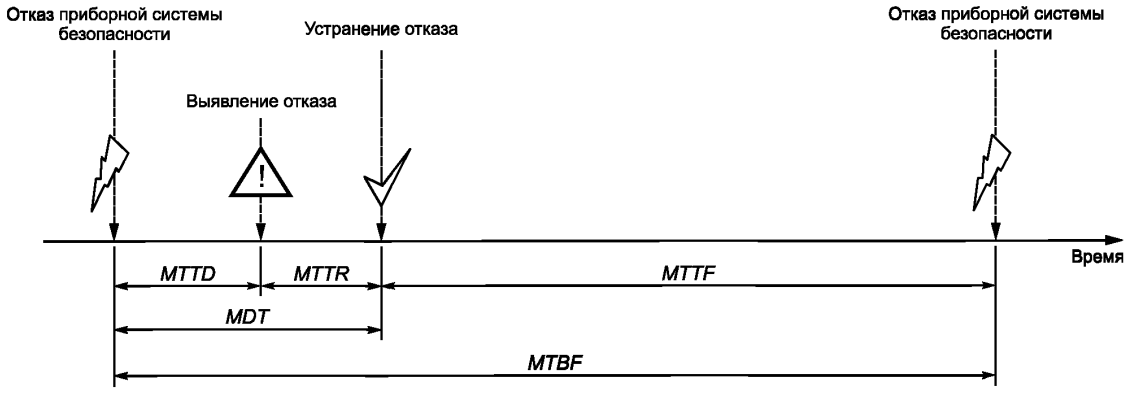


Рисунок 2 — Порядок сопряжения интервалов времени

Рассматриваемые интервалы ограничены наступлением очередного не выявленного пассивного сбоя (см. перечисление в)). Вероятность наступления неисправности приборной системы безопасности SIS в целом PFD_{Total} может быть вычислена по формуле (5):

$$PDF_{Total} = \frac{MTTD_{DU} + MTTR}{MTTF_{DU} + MTTD_{DU} + MTTR} = \frac{MDT_{DU}}{MTBF_{DU}}. \quad (5)$$

7.2 Общая процедура определения вероятности PFD

Пассивный сбой может как заблокировать аварийный сигнал, так и вызвать отключение технологической установки (от источника напряжения) при превышении предельного значения параметра. В соответствии с допущениями, указанными в подразделе 7.1, только пассивные, не выявленные сбои влияют на безопасность производственного процесса.

Примечание — Ниже приведены приближенные формулы определения вероятности PFD, справедливые для большинства случаев и приложений.

Вероятность PFD можно верифицировать с помощью соответствующего коммерческого программного обеспечения. Данные об отказах конкретных устройств (компонентов) следует хранить в рабочих базах данных. Уровень детализации данных может отличаться от продукта к продукту. Пользование указанными программами требует дополнительных затрат на повышение квалификации персонала.

В общем случае для оценки вероятности PFD рекомендуется нижеследующий подход.

Вероятность наступления неисправности всей приборной системы безопасности SIS в целом (PFD_{Total}) определяется путем независимого вычисления и суммирования значений PFD подсистемы датчиков, логического устройства и подсистем пусковых устройств.

В соответствии с допущением (j) величина PFD_{Total} может быть вычислена по формуле (6):

$$PFD_{Total} = PFD_S + PFD_L + PFD_{FE}. \quad (6)$$

Кроме того, для определения вероятности PFD_{Total} может быть использована нижеследующая пошаговая процедура:

Шаг 1

На рисунке 1 показаны приборная система безопасности SIS, структура ее подсистем и все соответствующие устройства. Подсистема датчиков и подсистема пусковых устройств могут быть разбиты на несколько групп датчиков и групп пусковых устройств. Каждая группа соответствует комбинации каналов, сгруппированных по правилу MooN.

Шаг 2

Для каждой *i-й* группы датчиков (i = 1, ..., X, см. рисунок 1) и каждой *j*-й группы пусковых устройств (j = 1, ..., Y, см. рисунок 1) вероятность PFD_{Gi} и вероятность PFD_{Gj} можно вычислить для соответствующей комбинации каналов MooN. Соответствующие упрощенные формулы приведены в подразделе 7.3. Принято допущение, что все каналы рассматриваемой группы идентичны, интенсивности наступления отказов λ_{DU} во всех каналах одинаковы. Интервалы между испытаниями T_1 также одинаковы.

Соответствующие интенсивности наступления отказов λ_{DU} в каналах определяются путем суммирования интенсивностей наступления отказов соответствующих устройств. Интервалы между испытаниями T_1 и количество неисправностей с общей причиной β обычно определяются самим пользователем.

Если параллельные группы датчиков и параллельные группы пусковых устройств являются диверсифицированными, то приближенные формулы подраздела 7.3 можно использовать только для консервативной оценки вероятности PFD. Для этого интенсивности наступления отказов соответствующих групп всех рассматриваемых каналов следует принять равными их наибольшему значению. Для упрощенной формулы подраздела 7.3 данный диверсифицированный случай можно рассматривать только путем редуцирования фактора не выявленных пассивных сбоев с общей причиной.

Чтобы получить совокупную вероятность PFD_S подсистемы датчиков, необходимо просуммировать парциальные вероятности PFD_{Gi} по i-м группам датчиков. Аналогично, чтобы получить совокупную вероятность PFD_{FE} подсистемы пусковых устройств, надо просуммировать парциальные вероятности PFD_{Gj} по j-м группам пусковых устройств:

$$PFD_S = \sum_i PFD_{Gi} \quad \text{и} \quad PFD_{FE} = \sum_j PFD_{Gj} . \tag{7}$$

Шаг 3

Значение вероятности PFD_L логической подсистемы, а также соответствующие интервалы между испытаниями T_1 должны определяться изготовителем.

Данное значение может учитывать работу входных и выходных модулей контроллера устройства обеспечения безопасности SPLC. Данное значение формально закрепляется за соответствующими каналами, содержащими рассматриваемые датчики и пусковые устройства. Отметим, что данное уточнение (предоставляется изготовителем) является несущественным, так как значения вероятности PFD_L обычно пренебрежимо малы по сравнению с суммарной вероятностью PFD приборной системы безопасности.

Шаг 4

Значение вероятности PFD_{Total} определяется формулой (6).

Рассмотренный метод применим для большинства случаев и приложений. Однако если нужны точные значения вероятности PFD для диверсифицированных параллельных систем, а также для систем повышенной сложности, то рекомендуется использовать и другие процедуры анализа надежности:

- анализ дерева отказов;
- модель Маркова;
- метод статистических испытаний Монте-Карло;
- блок-схемы надежности.

7.3 Приближенная формула определения вероятности наступления отказа в гомогенных системах

Формулы, приведенные в таблице 3, — это упрощенные формулы, приведенные в ГОСТ Р МЭК 61508-6. Они служат инструментом оценки вероятности PFD наступления неисправности различных гомогенных запараллеленных устройств.

Таблица 3 — Приближенные формулы определения вероятности PFD наступления отказа

Формулы, основанные на вычислении интенсивности наступления опасных, не выявленных пассивных сбоев λ_{DU}	Формулы, основанные на вычислении вероятности PFD_{1oo1} наступления отказов для комбинации 1oo1
$PFD_{1oo1} \approx \frac{1}{2}\lambda_{DU} \cdot T_1$ (8)	
$PFD_{1oo2} \approx \frac{\lambda_{DU}^2 * T_1^2}{3} + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$ (9)	$PFD_{1oo2} \approx \frac{4}{3} \cdot PFD_{1oo1}^2 + \beta \cdot PFD_{1oo1}$
$PFD_{1oo3} \approx \frac{\lambda_{DU}^3 * T_1^3}{4} + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$ (10)	$PFD_{1oo3} \approx 2 \cdot PFD_{1oo1}^3 + \beta \cdot PFD_{1oo1}$
$PFD_{2oo2} \approx \lambda_{DU} \cdot T_1$ (11)	$PFD_{2oo2} \approx 2 \cdot PFD_{1oo1}$
$PFD_{2oo3} \approx \lambda_{DU}^2 \cdot T_1^2 + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$ (12)	$PFD_{2oo3} \approx 4 \cdot PFD_{1oo1}^2 + \beta \cdot PFD_{1oo1}$

Общая формула оценки вероятности наступления отказов комбинации MooN имеет вид:

$$PFD_{MooN} = \frac{N!}{(M-1)!(N-M+2)!}\lambda_{DU}^{N-M+1} \cdot T_1^{N-M+1} + \beta \cdot \frac{1}{2} \cdot \lambda_{DU} \cdot T_1. \quad (13)$$

Из нее можно вывести упрощенные формулы для различных вариантов расчета. Например, если M = N, то второе слагаемое формулы (13), содержащее β, может быть опущено.

Фактор β определяет число не выявленных пассивных сбоев с общей причиной. Существует также фактор общей причины CCF. В запараллеленной приборной системе безопасности он оказывает влияние на все каналы одновременно. Метод оценки фактора β описан в приложение D ГОСТ Р МЭК 61508-6—2012. На практике значение β обычно лежит в диапазоне от 1 % до 5 %.

Примечание — Если внутренняя структура производственного модуля неизвестна, то указанная формула не дает возможности определить интенсивность λ_{DU} по заданному значению вероятности PFD.

Если рассматриваются сбои с общей причиной, то их количество нужно вычесть из количества сбоев с произвольной (независимой) причиной. Полученная величина, равная (1 – β), в вышеуказанные формулы не входит. Она достаточно мала, и ею можно пренебречь.

При увеличении интервалов между испытаниями и неизменном уровне полноты безопасности можно добиться:

- уменьшения интенсивности наступления не выявленных пассивных сбоев λ_{DU} путем дополнительной диагностики. Некоторые типы сбоев, учитываемые интенсивностью λ_{DU}, могут, при необходимости, диагностироваться и выявляться автоматически. Такие сбои переводятся в разряд выявленных пассивных сбоев λ_{DD}. В соответствии с вышеуказанным допущением (в) вероятность PFD их наступления пренебрежимо мала. Существуют типы сбоев, которые можно протестировать, не останавливая производственный процесс. Например, тестирование достоверности измеренных значений, мониторинг невязок значений величин, измеренных в параллельных структурах и т. п.;
- повышения отказоустойчивости путем надлежащего запараллеливания.

На практике часто выбирают стандартные интервалы между испытаниями. Как правило, это относится к подсистемам датчиков и подсистемам пусковых устройств приборной системы безопасности. Также возможно тестировать группы подсистем с различными интервалами между испытаниями.

Необходимо отметить, что при увеличении интервалов между испытаниями в приложениях уточнения расчетов можно добиться, привлекая разумные инженерные гипотезы и соображения. Рассмотренные выше приемы вычислений вероятности PFD наступления отказов приборной системы безопасности — не единственный критерий принятия решения.

8 Определение характеристик надежности устройств

Необходимые для расчета характеристики надежности устройств приборной системы безопасности можно получить из различных источников. Указанные источники разнятся по методам вычислений и условиям эксплуатации установок. Далее рассмотрены две категории источников.

8.1 Данные изготовителя

В большинстве случаев требуемые характеристики надежности устройств предоставляются изготовителем. Базовая характеристика — интенсивность наступления сбоев устройства. Значения указанных интенсивностей определяются следующим образом:

Метод №1

Интенсивность наступления сбоев устройства оценивается по методике анализа устройств FMEDA. В соответствии с данной методикой изготовитель сначала рассматривает компоненты своего устройства на предмет возможных сбоев, оценивает влияние данных сбоев на поведение устройства. Каждому конкретному сбою компонента изготовителем назначается значение интенсивности наступления данного сбоя, взятое из стандартизованной базы данных рассматриваемого компонента. Если устройство электронное, то значение интенсивности наступления его сбоев зависит, как правило, от таких факторов, как средняя температура окружающей среды, относительная влажность. Оператор установки должен прежде всего уделить внимание факторам и параметрам, определяющим интенсивность наступления сбоев электронных устройств. Соответствующие рекомендации даются изготовителем в руководстве пользователя.

Характеристики надежности устройства, получаемые методом №1, относятся к конкретным условиям эксплуатации установки. Данные условия указываются изготовителем в руководстве пользователя. Условия эксплуатации установки на практике могут существенно отличаться. В ряде случаев необходима адаптация установки к реальным условиям. Это необходимо учитывать на этапе планирования производства.

Метод №2

Изготовитель предоставляет данные, взятые не из стандартизованной базы данных, а из коммерческой базы данных, составленной по результатам полевых испытаний конкретного устройства. Важным условием является условие сравнимости данных, полученных в различных тестовых условиях эксплуатации устройства.

8.2 Базы данных, составленные по результатам полевых испытаний

Данные, взятые из стандартизованной базы данных полевых испытаний изготовителя, можно дополнить данными, взятыми из базы данных полевых испытаний, выполненных другой коммерческой организацией. При коммерческом подходе уровень детализации данных растет, он может доходить до отдельных устройств (шаровых клапанов, датчиков давления и т. п.). В некоторых случаях данные определяются конкретным типом приложения (например, устройство аварийного отключения установки и т. п.).

При использовании различных баз данных необходимо удостовериться в их сравнимости (например, сравнимости условий окружающей среды, сравнимости рабочих условий эксплуатации со стандартными условиями эксплуатации и т. п.).

Для производственного процесса пример базовых значений характеристик надежности полевых устройств с качеством «проверено-на-практике» приведен в таблице 4.

Таблица 4 — Базовые значения для характеристик надежности подсистем датчиков и подсистем пусковых устройств на основе предшествующего опыта («проверено-на-практике»)

Тип канала	Интенсивность λ_{DU} наступления не выявленных пассивных сбоев в канале	Рекомендуемый интервал T_1 между испытаниями	Доля β не выявленных пассивных сбоев с общей причиной
Подсистема датчиков, измеряемый параметр P	$1 \cdot 10^{-6} \cdot (MTBF_{DU} = 114a)$	8760 час = 1 год	5 %
Подсистема датчиков, измеряемый параметр T	$5 \cdot 10^{-7} \cdot h^{-1}(MTBF_{DU} = 228a)$		
Подсистема датчиков, измеряемый параметр L	$4 \cdot 10^{-7} \cdot h^{-1}(MTBF_{DU} = 285a)$		
Подсистема датчиков, измеряемый параметр F	$1 \cdot 10^{-6} \cdot h^{-1}(MTBF_{DU} = 114a)$		
Подсистема пусковых устройств	$4 \cdot 10^{-7} \cdot h^{-1}(MTBF_{DU} = 285a)$		

9 Типовые конструкции приборной системы безопасности

Приборная система безопасности обычно содержит группу датчиков и группу пусковых устройств, соединенных программируемым логическим контроллером устройства обеспечения безопасности SPLC. Группа датчиков образует структуру, включающую не более трех каналов. Группа пусковых устройств образует структуру, включающую не более двух каналов (см. рисунок 3).

Типы конструкций, рассмотренные на рисунке 3, относятся к большинству приложений. Это могут быть изолированные варианты конструкций, где подсистемы датчиков (подсистемы пусковых устройств) включают несколько групп. Указанные взаимосвязи, например, необходимы для выполнения аварийных отключений.

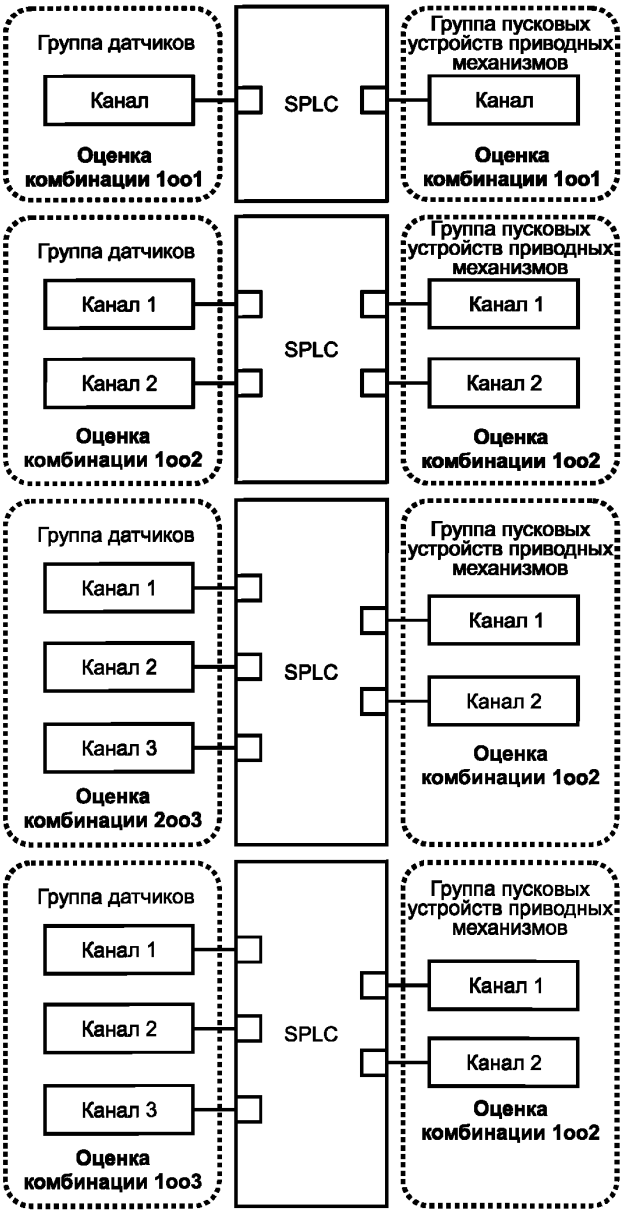


Рисунок 3 — Обзор типов конструкций

10 Полнота безопасности аппаратных средств опытного образца конструкции

10.1 Верификация конструкции, содержащей группу датчиков типа 2oo3 и группу пусковых устройств типа 1oo2, с помощью полевых устройств с качеством «проверено-на-практике»

Если давление установки больше допуска, то приборная система безопасности (см. рисунок 4) закрывает два шаровых клапана, установленных последовательно в трубе. Достаточная герметичность обеспечивается уже одним закрытым шаровым клапаном. Для подсистемы датчиков и подсистемы пусковых устройств принято, что конструкция является гомогенной.

Программируемый логический контроллер SPLC (включая его входные и выходные модули) сертифицирован изготовителем на уровень полноты безопасности SIL 3. Интервал между испытаниями составляет в среднем десять лет.

Подсистема датчиков и подсистема пусковых устройств включают устройства с качеством «проверено-на-практике». По данной причине значения, рекомендуемые в таблице 4, могут использоваться в комбинации с формулами (12) и (9).

С учетом результатов оценки отказоустойчивости HFT и вероятности PFD (см. таблицу 5) рассматриваемой конструкции может быть назначен уровень полноты безопасности SIL 3.

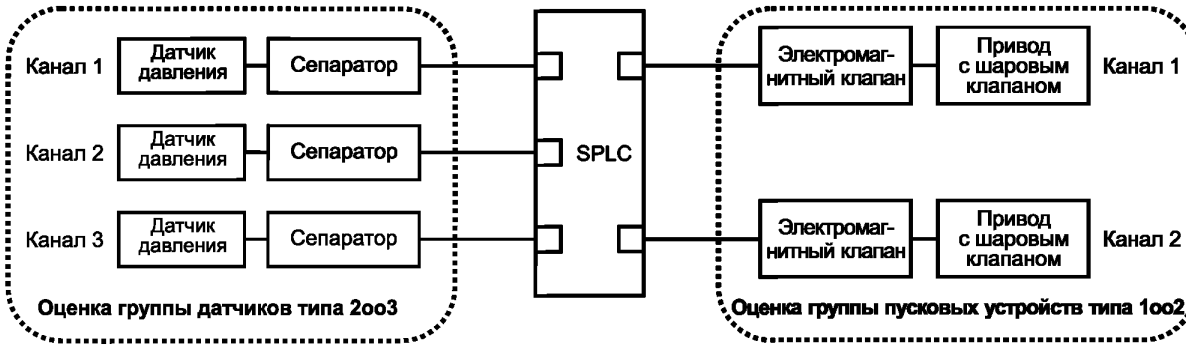


Рисунок 4 — Блок-схема конструкции, содержащей группу датчиков типа 2oo3 и группу пусковых устройств типа 1oo2

10.2 Верификация конструкции, содержащей группу датчиков типа 1oo3 и две группы пусковых устройств типа 1oo2, с помощью полевых устройств с качеством «проверено-на-практике»

Рассматриваемая приборная система безопасности (см. блок-схему на рисунке 5) обслуживает две линии, идущие к реактору. Линии отключаются, если уровень заполнения реактора превышает установленный допуск. В каждой линии последовательно установлены два шаровых клапана. Достаточная герметичность обеспечивается уже одним закрытым шаровым клапаном. Для подсистемы датчиков и подсистемы пусковых устройств принято, что конструкция является гомогенной.

Программируемый логический контроллер SPLC (включая его входные модули и выходные модули) сертифицирован изготовителем на уровень полноты безопасности SIL 3. Интервал между испытаниями составляет десять лет.

В соответствии с 10.1 подсистема датчиков и подсистема пусковых устройств включают устройства с качеством «проверено-на-практике». Значения, рекомендуемые в таблице 4, могут комбинироваться с устройствами типа MooN. Вероятность PFD наступления отказа данной подсистемы датчиков соответствует вероятности PFD наступления отказа подсистемы датчиков, рассмотренной в разделе 10.1. Вероятность PFD всей подсистемы пусковых устройств получается путем суммирования парциальных вероятностей PFD отдельных групп пусковых устройств.

Таблица 5 — Требуемый уровень полноты безопасности аппаратных средств конструкции

Общая информация о рассматриваемой приборной системе безопасности				
Подсистема датчиков		Логическая подсистема	Подсистема пусковых устройств	
Датчик P	Сепаратор	SPLC, включая входной и выходной модули	Электромагнитный клапан	Привод с шаровым клапаном
С качеством «проверено-на-практике»	С качеством «проверено-на-практике»	Изготовитель	С качеством «проверено-на-практике»	С качеством «проверено-на-практике»
2oo3		—	1oo2	

Требования к отказоустойчивости HFT аппаратных средств		
HFT 1	—	HFT 1
Требуемый уровень SIL 3 (таблица 2)	Требуемый уровень SIL 3	Требуемый уровень SIL 3 (таблица 2)
Требуемый уровень SIL 3		

Вероятность PFD возникновения отказа по запросу		
$\lambda_{DU} = 1{,}0 \cdot 10^{-6} \cdot ч^{-1}$	—	$\lambda_{DU} = 4{,}0 \cdot 10^{-7} \cdot ч^{-1}$
T_1 = 8760 ч = 1 год	T_1 = 87600 ч = 10 лет	T_1 = 8760 ч = 1 год
β = 5 %	—	β = 5 %
$PFD_S = 3{,}0 \cdot 10^{-4}$	$PFD_L = 1{,}0 \cdot 10^{-5}$	$PFD_{FE} = 9{,}2 \cdot 10^{-5}$
$PFD_{Total} = 4{,}0 \cdot 10^{-4}$ → требуемый уровень SIL 3		

С учетом результатов оценки отказоустойчивости HFT и вероятности PFD (см. таблицу 6) рассматриваемой конструкции может быть назначен уровень полноты безопасности SIL 3.

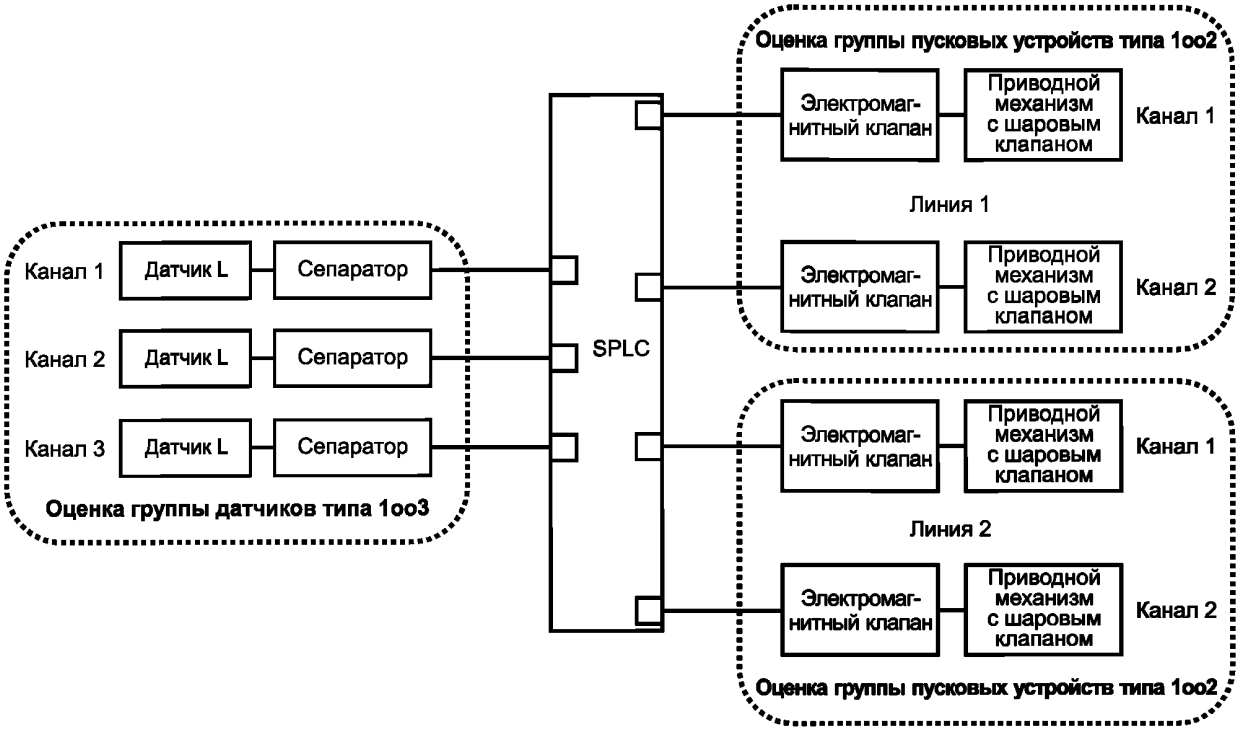


Рисунок 5 — Блок-схема конструкции, содержащей группу датчиков типа 1oo3 и две группы пусковых устройств типа 1oo2

Таблица 6 — Требуемый уровень полноты безопасности аппаратных средств конструкции

Общая информация о рассматриваемой приборной системе безопасности				
Подсистема датчиков		Логическая подсистема	Подсистема пусковых устройств	
Датчик L	Сепаратор	SPLC, включая входные и выходные модули	Электромагнитный клапан	Привод с шаровым клапаном
С качеством «проверено-на-практике»	С качеством «проверено-на-практике»	Изготовитель	С качеством «проверено-на-практике»	С качеством «проверено-на-практике»
1oo3		—	1oo2 для каждой линии	

Требования к отказоустойчивости HFT аппаратных средств		
HFT 2	—	HFT 1 для каждой линии
Требуемый уровень SIL 3 (таблица 2)	Требуемый уровень SIL 3	Требуемый уровень SIL 3 (таблица 2)
Требуемый уровень SIL 3		

Вероятность PFD возникновения отказа по запросу		
$\lambda_{DU} = 4{,}0 \cdot 10^{-7} \cdot ч^{-1}$	—	$\lambda_{DU} = 4{,}0 \cdot 10^{-7} \cdot ч^{-1}$
T_1 = 8760 ч = 1 год	T_1 = 87600 ч = 10 лет	T_1 = 8760 ч = 1 год
β = 5 %	—	β = 5 %
$PFD_S = 9{,}2 \cdot 10^{-5}$	$PFD_L = 1{,}0 \cdot 10^{-5}$	$PFD_{FE} = 2 \cdot 9{,}2 \cdot 10^{-5}$
$PFD_{Total} = 2{,}8 \cdot 10^{-4}$ → требуемый уровень SIL 3		

10.3 Верификация конструкции, содержащей группу датчиков типа 1oo2 и группу пусковых устройств типа 1oo2, с помощью полевых устройств с качеством «проверено-на-практике», сертифицированных на уровень обеспечения безопасности SIL

Блок-схема рассматриваемой приборной системы безопасности приведена на рисунке 6. Если температура превышает допуск, то парозаборник закрывается. Достаточная герметичность обеспечивается уже одним закрытым шаровым клапаном. Для подсистемы датчиков и подсистемы пусковых устройств принято, что конструкция является гомогенной.

Программируемый логический контроллер SPLC (включая его входные и выходные модули) сертифицирован изготовителем на уровень полноты безопасности SIL 3. Интервал между испытаниями составляет десять лет.

Подсистема датчиков и электромагнитные клапаны подсистемы пусковых устройств имеют декларации (сертификаты) изготовителя. Качество «проверено-на-практике» обеспечено. Если устройство имеет декларацию (сертификат) изготовителя, то его отказоустойчивость HFT соответствует требованиям комплекса стандартов ГОСТ Р МЭК 61508. Данная процедура сертификации отличается от процедуры, установленной в разделе 6. В дальнейшем также предполагается, что отказоустойчивость HFT устройств соответствует требованиям комплекса стандартов ГОСТ Р МЭК 61508. В данном конкретном примере изготовитель считает, что даже для повышенной отказоустойчивости HFT датчика T (датчика температуры) данному устройству может быть назначен только уровень полноты безопасности SIL 2 (см. таблицу 7).

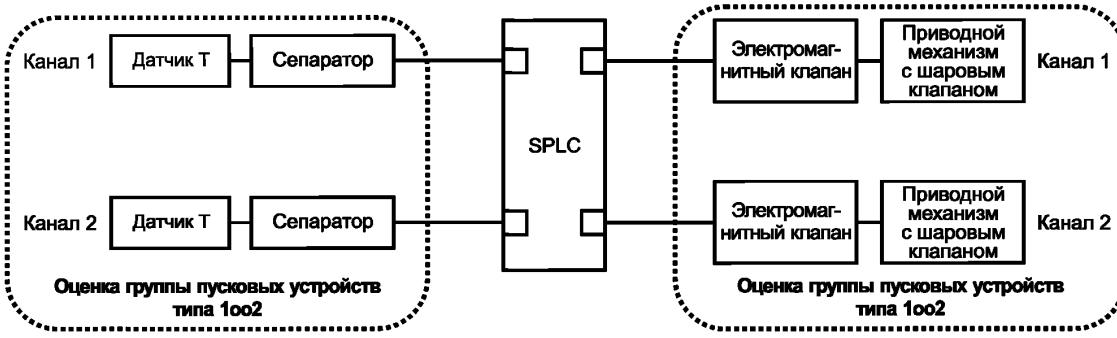


Рисунок 6 — Блок-схема конструкции, содержащей группу датчиков типа 1oo2 и группу пусковых устройств приводного механизма типа 1oo2

Таблица 7 — Оценка полноты безопасности аппаратных средств конструкции

Общая информация о рассматриваемой приборной системе безопасности				
Подсистема датчиков		Логическая подсистема	Подсистема пусковых устройств	
Датчик Т	Сепаратор	SPLC, включая входной и выходной модули	Электромагнитный клапан	Привод с шаровым клапаном
Требуемый уровень SIL 2, отказоустойчивость HFT 0 в соответствии со стандартом изготовителя	Требуемый уровень SIL 2, отказоустойчивость HFT 0 в соответствии со стандартом изготовителя	Изготовитель	Требуемый уровень SIL 2, отказоустойчивость HFT 0 в соответствии со стандартом изготовителя	С качеством «проверено-на-практике»
1oo2		—	1oo2	
Требования к отказоустойчивости HFT аппаратных средств				
HFT 1		—	HFT 1	
Максимально допустимый уровень SIL 2 в соответствии со стандартом изготовителя	Требуемый уровень SIL 3 в соответствии со стандартом изготовителя	Требуемый уровень SIL 3	Требуемый уровень SIL 3 в соответствии со стандартом изготовителя	Требуемый уровень SIL 3 (таблица 2)
Требуемый уровень SIL 2				

Вероятность PFD возникновения отказа по запросу		
$\lambda_{DU} = 1{,}5 \cdot 10^{-7} \cdot ч^{-1} + 1{,}0 \cdot 10^{-7} \cdot ч^{-1}$	—	$\lambda_{DU} = 1{,}0 \cdot 10^{-7} \cdot h^{-1} + 4{,}0 \cdot 10^{-7} \cdot h^{-1}$
T_1 = 8760 ч = 1 год	T_1 = 87600 ч = 10 лет	T_1 = 8760 ч = 1 год
β = 5 %	—	β = 5 %
$PFD_S = 5{,}6 \cdot 10^{-5}$	$PFD_L = 1{,}0 \cdot 10^{-5}$	$PFD_{FE} = 1{,}2 \cdot 10^{-4}$
$PFD_{Total} = 1{,}9 \cdot 10^{-4}$ →Требуемый уровень SIL 3		

Приводной механизм и шаровой клапан подсистемы пускового устройства имеют качество «проверено-на-практике». В таблице 4 приведены рекомендуемые значения используемых величин. Рекомендуемые значения вероятности PFD наступления отказа подсистемы датчиков (подсистемы пусковых устройств) соответствуют значениям вероятности PFD наступления отказа подсистемы датчиков (подсистемы пусковых устройств), установленным в 10.1.

При вычислении вероятности PFD_S (изготовителем) принято следующее допущение. В рассматриваемом канале значение интенсивности λ_{DU} наступления отказов датчика Т (датчика температуры) и значение интенсивности λ_{DU} наступления отказов сепаратора равны соответственно $1{,}5 \cdot 10^{-7} \cdot ч^{-1}$ и $1{,}0 \cdot 10^{-7} \cdot ч^{-1}$.

Приводной механизм и шаровой клапан имеют качество «проверено-на-практике». Поэтому при вычислении вероятности PFD_{FE} (изготовителем) принято следующее допущение. В рассматриваемом канале рекомендуемое значение интенсивности λ_{DU} наступления отказов приводного механизма и шарового клапана равно $4{,}0 \cdot 10^{-7} \cdot ч^{-1}$ (см. таблицу 4). В отличие от них значение интенсивности наступления отказов λ_{DU} электромагнитного клапана принято равным $1{,}0 \cdot 10^{-7} \cdot ч^{-1}$.

Значения указанных величин, принятые изготовителем, представляются реалистичными.

В заключение отметим, что в рассматриваемом примере для заданной отказоустойчивости HFT максимально допустимый уровень полноты безопасности равен SIL 2 (в соответствии со стандартом изготовителя). И это несмотря на то, что формально расчетному значению вероятности PFD наступления отказа по запросу соответствует уровень полноты безопасности SIL 3.

УДК 658.52.011.56:006.354 ОКС 25.040.40, 35.240.50

Ключевые слова: системы автоматического управления производственными процессами; производственные процессы; приборные системы безопасности; уровень полноты безопасности, верификация полноты аппаратных средств автоматизированной системы безопасности

БЗ 10—2019/8

Редактор *П.К. Одинцов*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 24.09.2019. Подписано в печать 15.10.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

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

gost.e-ecolog.ru