

ЗАДАЧИ, ТЕСТЫ И УПРАЖНЕНИЯ ПО ПРОЕКТИРОВАНИЮ ПРИБОРНЫХ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ

Методические указания
Для студентов, обучающихся по направлению
150304/150404 «Автоматизация технологических процессов и производств»

Составитель Громаков Е.И.

УДК 658.512.2.011.56.681.3(075.8)

ББК 32.965я73

П79

Методические указания. Задачи, тесты и упражнения по проектированию приборных систем противоаварийной защиты : учебное пособие / сост. Е. И. Громаков. – Томск : Томский политехнический университет. – 2025. – 426 с.

В учебном пособии рассмотрены особенности управления жизненным циклом систем противоаварийной защиты непрерывных нефтехимических производств в виде упражнений (кейсов с ответами, тестов с ответами и без ответов), охватывающие основные понятия, структуры, классификации и методологии разработки противоаварийной защиты на основе стандартов ГОСТ Р МЭК 61508/61511.

Предназначено для студентов, обучающихся по направлению 150304 и 150404 «Автоматизация технологических процессов и производств».

Методические указания рассмотрены и рекомендованы
к использованию в учебном процессе
«05» 11 2025 года, протокол № 42

Руководитель
отделения ОАР ИШИТР



Филипас А.А.

ОГЛАВЛЕНИЕ

ПРИНЯТЫЕ СОКРАЩЕНИЯ	6
ВВЕДЕНИЕ	8
1. ФЕДЕРАЛЬНЫЕ И МЕЖДУНАРОДНЫЕ НОРМЫ И ПРАВИЛА В ОБЛАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ.....	9
1.1. Ключевые принципы норм и правил в области промышленной безопасности.	9
1.2. Практикум по применению стандартов при проектировании СПАЗ.	10
1.3. Тесты с решениями и объяснениями.	14
1.4. Тесты для самопроверки.	47
2. HAZOP/ HAZID АНАЛИЗ.	53
2.1. Ключевые принципы анализа опасностей.	53
2.1. Практикум по анализу HAZOP и HAZID.	56
2.3. Тесты с решениями и объяснениями.	61
2.4. Тесты для самопроверки.	66
3. ДЕРЕВЬЯ ОТКАЗОВ/СОБЫТИЙ И АНАЛИЗ СЛОЕВ ЗАЩИТЫ.	69
3.1. Ключевые принципы анализа защиты опасного производственного объекта.....	69
3.2. Практикум по анализу деревьев отказов/событий (и слоев защиты).	72
3.3. Тесты с решениями и объяснениями.	79
3.4. Тесты для самопроверки.	85
4. НАДЕЖНОСТЬ СИСТЕМ БЕЗОПАСНОСТИ.	92
4.1. Ключевые принципы оценки надежности систем безопасности.	92
4.2. Практикум по расчету надежности СПАЗ.	93
4.3. Тесты с решениями и объяснениями.	104
4.4 Тесты для самопроверки.	109
5. АНАЛИЗ РИСКОВ	113
5.1. Ключевые принципы анализа рисков.	113
5.2. Практикум по применению анализа рисков в СПАЗ.	116
5.3. Тесты с решениями и объяснениями.	124
5.4. Тесты для самопроверки.	129
6. ПОЛНОТА БЕЗОПАСНОСТИ, ОБЕСПЕЧИВАЕМАЯ СИСТЕМОЙ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ.	135
6.1. Ключевые принципы полноты безопасности (SIL).....	135
6.2. Практикум по оценке полноты безопасности.	136
6.3. Тесты с решениями и объяснениями.	141
6.4. Тесты для самопроверки.	147
7. СПЕЦИФИКАЦИЯ СИСТЕМЫ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ.	150
7.1 Назначение и роль SRS в жизненном цикле безопасности.	150
7.2. Практикум по разработке спецификации СПАЗ.....	154
7.3. Тесты с решениями и объяснениями.	163

7.4. Тесты для самопроверки.....	175
8. РЕЗЕРВИРОВАНИЕ.....	181
8.1. Ключевые принципы резервирования.....	181
8.2. Практикум по применению резервирования при проектировании СПАЗ.....	188
8.3. Тесты с решениями и объяснениями.....	197
8.4. Тесты для самопроверки.....	206
9. ЛОГИЧЕСКОЕ УСТРОЙСТВО. ПЛК.....	210
9.1. Ключевые принципы разработки логического устройства (ПЛК) СПАЗ.....	210
9.2. Практикум применению логического устройства в СПАЗ.....	211
9.3. Тесты с решениями и объяснениями выбору логического устройства СПАЗ.....	216
9.4. Тесты для самопроверки.....	227
10. ДИАГНОСТИКА СПАЗ.....	232
10.1. Ключевые принципы диагностики СПАЗ.....	232
10.2. Практикум по диагностированию СПАЗ ОПО.....	238
10.3. Тесты с решениями и объяснениями.....	254
10.4. Тесты для самопроверки.....	263
11. ПРОЕКТИРОВАНИЕ, СТРУКТУРА, КОМПОНЕНТЫ СПАЗ.....	266
11.1. Ключевые принципы проектирования СПАЗ от HAZID до верификации.....	266
11.2. Практикум проектирования СПАЗ.....	269
11.3. Тесты с решениями и объяснениями.....	277
11.4. Тесты для самопроверки.....	317
12. ДОКУМЕНТАЦИЯ СПАЗ.....	323
12.1. Ключевые принципы документирования СПАЗ.....	323
12.2. Практикум по документированию СПАЗ.....	327
12.3. Тесты с решениями и объяснениями.....	330
12.4. Тесты для самопроверки.....	348
ОТВЕТЫ.....	351
Раздел 1.....	351
Раздел 2.....	361
Раздел 3.....	365
Раздел 4.....	373
Раздел 5.....	380
Раздел 6.....	383
Раздел 7.....	388
Раздел 8.....	397
Раздел 9.....	401
Раздел 10.....	405
Раздел 11.....	409

Раздел 12.....	417
ЗАКЛЮЧЕНИЕ.....	420
СПИСОК ЛИТЕРАТУРЫ	423

ПРИНЯТЫЕ СОКРАЩЕНИЯ

λ_D	Общая интенсивность опасных отказов
λ_S	Общая интенсивность безопасных отказов
λ_{DD}	Интенсивность опасных обнаруженных отказов
λ_{DU}	Интенсивность опасных необнаруженных отказов
λ_{SD}	Интенсивность безопасных обнаруженных отказов
λ_{SU}	Интенсивность безопасных необнаруженных отказов
β	Процент общих отказов
T_i	Интервал периодического профилактического обслуживания и полной проверки системы
T_{Proof}	Период тестирования
F_t	Допустимый уровень риска, целевой показатель безопасности, отправная точка для расчетов
F_{np}	Частота при незащищенном риске
F_p	Частота при защищенном риске
CCF	Отказы по общей причине, общего происхождения
SFF	Доля безопасных отказов
SIF	Функция безопасности, контур аварийной защиты по параметру контроля
FMEA	Анализ видов и последствий отказов
FMEDA	Анализ режимов, эффектов и диагностики отказов
HAZOP	Исследование опасности и работоспособности
HAZID	Идентификация отказов
FTA	Анализ дерева отказов
SRS	Спецификация требований к безопасности, ТЗ
MTTF	Среднее время работы до отказа
MTTFS	Среднее время работы до первого ложного отказа
MTBF	Среднее время между отказами
MTTR	Среднее время восстановления работоспособности
CPT	Коэффициент покрытия диагностики. Количественная оценка Диагностический охват
ALARP	Настолько низкий показатель, уровень требований, насколько это оправдано практикой
АСДУ	Автоматизированная система диспетчерского (операторного) управления
Credit	Зачёт соответствия СПАЗ/SIS ожиданиям (критериям) при проектировании, потенциал эффективности проектного решения
DC	Диагностический охват
DTI	Интервал между неавтономными проверками, предназначенными для обнаружения отказов в системах, связанных с безопасностью, с заданным охватом диагностикой
DI	Средний интервал срабатывания СПАЗ
EMC	Устойчивость к электромагнитным помехам (EMI)
Ex ia	Искробезопасная электрическая цепь
ESD	Система аварийных блокировок параметров технологических установок
FIT	1.0×10^9 отказов в час
FMEDA	Анализ видов, последствий и диагностического покрытия отказов) в системах противоаварийной защиты
FAT	приемочные испытания, проводимые на заводе производителя

FSCP	Соединением полевых устройств FSoE (ГОСТ МЭК 61158)
FMEA	Систематический метод для выявления потенциальных отказов (проблем) СПАЗ/SIS
HFT	Допустимое число отказов оборудования. Аппаратная отказоустойчивость, устойчивость к опасным аппаратным сбоям
HART	Комбинированный цифро-аналоговый протокол передачи данных
MT	Время, на которое рассчитана система (часто принимается равным 10 годам)
MRT	Среднее время восстановления после обнаруженного отказа
PST	Испытание при неполном ходе, используемое для обнаружения состояний отказа в контроллере, приводе и арматуре в сборе
PSF	Вероятность систематического сбоя
PLL	Потенциальные потери жизни
PFH	Вероятность (интенсивность, частота) опасных отказов в час
PFD	Средняя вероятность отказа выполнения требуемой функции (отказа на запрос)
PDC	Степень диагностического контроля, отношение частоты проведения диагностических тестов и частоты запросов на функцию безопасности
PTC	Доля необнаруженных отказов, которую мы можем найти и устранить во время плановой ручной проверки
PTH	Ростехнадзор
ROUTE 1H	Упрощенный метод достижения заданного уровня полноты безопасности СПАЗ/SIS без резервирования и диагностики элементов типа А
ROUTE 2H	Набор строгих требований и условий для достижения заданного уровня полноты безопасности (SIL) интеллектуальных (сложных) программно-аппаратных средств типа В
RRF	Фактор снижения риска
SIL	Уровень полноты безопасности
SC	Уровень устойчивости СПАЗ/SIS к систематическим отказам
STR	Интенсивность ложных отказов
MOC	Структурированная процедура управления любыми изменениями в СПАЗ
SAT	Приемочные испытания на площадке заказчика
TR	Приемлемый риск
Валидация	Подтверждение соответствия путем испытаний и представления объективных свидетельств, выполнения конкретных требований к предусмотренному конкретному использованию
Аудит функциональной безопасности	Систематическое и независимое исследование, приводящееся с тем, чтобы определить, насколько эффективно реализованы процедуры, предназначенные для согласования требований к функциональной безопасности с запланированными мероприятиями, и определения, насколько они пригодны для достижения поставленных целей

ВВЕДЕНИЕ

Данное учебное пособие предназначено для студентов технологических университетов и посвящено проектированию приборных систем безопасности (СПАЗ/SIS – Safety Instrumented Systems). В отличие от традиционных учебников, оно построено на интерактивной основе изложения и включает тесты, практические упражнения и ситуационные задачи, направленные на закрепление теоретических знаний и формирование навыков проектирования систем противоаварийной защиты.

Изучение дисциплины «Проектирование автоматических систем технологической безопасности» необходимо для подготовки высококвалифицированных специалистов, способных решать задачи обеспечения безопасности на сложных промышленных объектах, особенно в нефтегазовой отрасли. Современные производственные требования предполагают не только глубокое понимание принципов проектирования и эксплуатации СПАЗ/SIS, но и умение применять международные и национальные стандарты на практике.

Пособие последовательно раскрывает ключевые аспекты проектирования в запуске СПАЗ/SIS: от основ технологической безопасности и практического выбора средств автоматизации до верификации и валидации системы противоаварийной защиты. В основу терминологии в задачах и упражнениях пособия положены сокращения, используемые в ИЕС 61508/61511. Целостная структура пособия позволяет студентам поэтапно осваивать материал, проверяя знания с помощью тестов и получая навыки на реальных кейсах.

Успешное выполнение практических заданий позволит будущим инженерам эффективно работать в области промышленной безопасности, в том числе на предприятиях нефтегазового комплекса и других отраслей.

Разработанное при технической поддержке ИИ DeepSeek-V3R1 интерактивное пособие поможет студентам не только освоить теоретические основы, но и подготовиться к решению производственных задач.

1. ФЕДЕРАЛЬНЫЕ И МЕЖДУНАРОДНЫЕ НОРМЫ И ПРАВИЛА В ОБЛАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ.

Задание 1.1. Уяснить ключевые принципы применения федеральных и международных норм и правил в области промышленной безопасности (систем приборной безопасности).

1.1. КЛЮЧЕВЫЕ ПРИНЦИПЫ НОРМ И ПРАВИЛ В ОБЛАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ.

Законы правительства и приказы Ростехнадзора (РТН) по системам противоаварийной защиты (СПАЗ/SIS, СПАЗ) написаны кровью. Их игнорирование при проектировании СПАЗ/SIS потенциальное преступление. Знание по приборным системам защиты – это не просто «сдать экзамен» по дисциплине, это ответственность за жизни людей.

Стандарты СПАЗ/SIS – это не набор разрозненных правил, а логичная «дорожная карта» для создания и эксплуатации доказательно безопасной системы. Каждый этап правил опирается на предыдущий. Пропуск этапа – это дыра в безопасности. Знание стандарта – это понимание всей картины минимизации потерь из-за аварий.

Вот список ключевых, основополагающих принципов, вытекающих из международных стандартов СПАЗ/SIS.

1. Принцип ALARP - это подход к оценке рисков, призванный найти баланс между затратами и усилиями, необходимыми для снижения рисков, и выгодами от такого снижения.

2. Принцип Независимости. СПАЗ/SIS должна быть независима от базовой системы управления процессом (автоматизированной системы диспетчерского управления, АСДУ) и других слоев защиты.

3. Принцип Избыточности и Диверсификации. Для достижения высокого уровня безопасности SIL (2,3,4) требуется резервирование и/или использование разных технологий реализации контуров защиты.

4. Принцип Верификации и Валидации. Безопасность нужно доказывать расчетами (PFDavg, SFF) и демонстрировать испытаниями.

5. Принцип Жизненного Цикла. Безопасность закладывается на этапе проектирования и поддерживается на всем протяжении эксплуатации.

6. Принцип Компетентности. Работы должны выполняться квалифицированным персоналом.

7. Принцип Документирования. Каждое решение и действие должно быть обосновано, верифицировано и задокументировано (требование Ростехнадзора, РТН).

Обучаемые по направлению промышленной безопасности будущие Инженеры Безопасности. Это не просто должность. Это гарантия. Гарантия того, что система противоаварийной защиты сработает именно тогда, когда это жизненно необходимо. Подпись специалиста на проекте – это его ответственность.

«Стандарты – это Щит Инженера». Знание и применение стандартов – это не бюрократия. Это его главная защита. Если случится инцидент (не дай бог), первым вопросом будет. «Вы следовали Приказу 533 и МЭК 61508/61511?». Если инженер может доказать, что да – это его профессиональная и юридическая защита. Если нет – последствия могут быть крайне тяжелыми.

«Язык Профессии». МЭК 61508/61511 – это международный язык специалистов по функциональной безопасности. Без его знания нельзя ни прочитать документацию ведущих вендоров, ни участвовать в серьезных международных проектах, ни понять отчеты по аудиту безопасности. Это ключ к карьере.

И, наконец, это Интересно! (По-настоящему). Проектирование СПАЗ/SIS – это самый сложный пазл инженерного искусства, где нужно совместить технологию, надежность, безопасность и экономику производства.

Стандарты – это правила инженерных решений. Понимать их – значит видеть их красоту и логику в области безопасности.

1.2. ПРАКТИКУМ ПО ПРИМЕНЕНИЮ СТАНДАРТОВ ПРИ ПРОЕКТИРОВАНИИ СПАЗ.

Задание 1.2. С поддержкой AI (типа GPT) подготовить свои решения кейсов и объяснения для одного или 2-х кейсов. Сделать вывод о правильности и качестве предложенных ответов и объяснений в кейсах.

Кейс 1.1. Выбор нормативной базы для проектирования СПАЗ. Ситуация.

На нефтеперерабатывающем заводе требуется модернизировать систему противоаварийной защиты (СПАЗ/SIS). Заказчик настаивает на использовании только ГОСТов, без учета МЭК 61508/61511.

Вопрос.

Какой документ является основным для проектирования СПАЗ/SIS на опасных производственных объектах в РФ?

Варианты.

А) ГОСТ Р 53325-2012.

В) Приказ Ростехнадзора №533.

С) Федеральный закон №116-ФЗ.

Д) МЭК 61508/61511 (как рекомендуемый технический стандарт)

Ответ. В и С (Приказ №533 и ФЗ №116-ФЗ – обязательные, МЭК 61508/61511 – рекомендуемые, технические стандарты жизненного цикла СПАЗ).

Объяснения .

ФЗ №116-ФЗ– базовый закон, регулирующий промышленную безопасность [12].

- Приказ №533 [13]. конкретизирует требования к СПАЗ/SIS, включая ссылки на МЭК 61508/61511.

- Игнорирование МЭК 61508/61511 может привести к ошибкам в расчетах уровня полноты безопасности (SIL) и проекте приборно-программных средств СПАЗ в целом.

Кейс 1.2. Ошибка в документации.

Ситуация.

Аудитор обнаружил, что в проекте СПАЗ/SIS не указаны:

- Режим работы (низкая/высокая интенсивность запросов).
- Методы верификации SIL.

Вопрос. Какое требование ГОСТ Р МЭК 61508-2 [2]. нарушено?

Ответ.

Нарушены:

1. П. 7.4.2 (документирование режима работы).
2. П. 7.6 (требования к верификации SIL).

Последствия.

Без этого невозможна оценка соответствия системы приборной защиты стандарту.

Кейс 1.3. Систематические отказы.

Ситуация.

Проектировщик предложил использовать для SIL 3 контура защиты на основе одного датчик давления без диагностики, но сертифицированного на SIL 3 и Route 2H, реле включения соленоидного клапана.

Вопрос. Почему это нарушает требования приказа №533 и ГОСТ Р МЭК 61508-2?

Ответ.

Для SIL 3 требуется архитектура с высокой отказоустойчивостью, которое достигается за счет резервирования.

Одиночный датчик не обеспечит стойкость к систематическим отказам (п. 7.4.5 стандарта).

Систематический отказ в любом компоненте контура аварийной защиты может привести к тотальному отказу всей системы защиты, если архитектура не отказоустойчива. В данном случае одиночный датчик – это единая точка систематического отказа.

Что такое систематический отказ и почему он опасен?
Чтобы понять ошибку проектировщика, сначала нужно четко усвоить, что такое **систематический отказ**.

Суть систематического отказа. Это не случайная поломка из-за износа. Это ошибка, «зашитая» в самом проекте, конструкции, программном обеспечении, производственном процессе или инструкциях по эксплуатации. Такой отказ предопределен и при определенных условиях обязательно проявится у всех одинаковых устройств или систем.

Пример. Если в программном коде резервированного ПЛК есть ошибка, приводящая к его зависанию при одновременном поступлении двух сигналов, это произойдет с каждым идентичным ПЛК в одинаковых условиях. Такой отказ нельзя предотвратить заменой устройства на аналогичное – в требуется **изменение проекта или программного кода**.

Главная опасность. Систематический отказ может привести к **тотальному (общему) отказу** всей системы защиты. Если все резервные каналы построены на одинаковых компонентах с одной и той же системной ошибкой, они откажут одновременно при возникновении условия, вызывающего эту ошибку.

Критический разбор предложенного проекта.

Предложение проектировщика использовать один датчик и компоненты без диагностики нарушает базовые принципы стандартов безопасности. В таблице ниже наглядно показаны проблемы.

Компонент / Решение	Проблема с точки зрения систематических отказов	Требования стандартов
Один датчик (SIL2, Route 2H)	Является единой точкой отказа . Любой систематический дефект, присущий этой модели датчика (например, ошибка в измерительном алгоритме), приведет к полной потере функции защиты. Архитектура не обладает отказоустойчивостью .	Для уровня SIL 2, 3 требуется архитектура с высокой отказоустойчивостью, исключая единые точки отказа. Стандарты 61508/61511 требуют резервирование .
ПЛК и клапан	Невозможно обнаружить скрытый отказ. Например, кла-	п. 7.4.5 ГОСТ Р МЭК 61508-2 (и другие разделы, посвященные диагностике) требует

Компонент / Решение	Проблема с точки зрения систематических отказов	Требования стандартов
без диагностики	пан может быть неработоспособен из-за системного дефекта, но система не узнает об этом, пока не потребуются аварийное срабатывание. Без диагностики отказ становится скрытым и может быть выявлен только при плановом ТО или в момент аварии.	применения средств контроля для обнаружения отказов. Приложение В стандарта прямо указывает на необходимость методов для предотвращения систематических отказов на всех этапах жизненного цикла.
Игнорирование Приказа №533	Приказ №533 обязывает проводить анализ опасностей технологического процесса на этапе проектирования. Решение с единственным датчиком не является обоснованным результатом такого анализа для высокого уровня риска (SIL 3).	Проектная документация должна содержать технические решения, обеспечивающие взрывобезопасность, исходя из категории взрывоопасности технологического блока.

Как избежать тотального отказа?

Чтобы система защиты была устойчива к систематическим отказам, необходимо реализовать два ключевых принципа.

1. **Резервирование (избыточность).** Использование двух или трех датчиков вместо одного. При этом важно применять **разнородное (диверсифицированное) резервирование**.

Пример. Использование датчиков давления *разных принципов действия* (например, пьезоэлектрический и емкостной) или от *разных производителей*. Это гарантирует, что систематическая ошибка, присущая одному типу датчиков, не затронет резервный канал.

2. **Диагностика и контроль.** Внедрение в систему средств постоянного самодиагностирования с использованием ПЛК.

Пример. Для клапана рекомендуется использование соленоида с обратной связью, который подтверждает свое срабатывание. Для ПЛК рекомендуется применение встроенных тестов, проверяющих целостность памяти и логики.

Кейс 1.4. Режимы работы СПАЗ/SIS.

Ситуация.

СПАЗ/SIS в режиме высокой интенсивности запросов (срабатывает несколько раз в неделю). Вероятность опасного отказа – 10^{-8} в час.

Вопрос. Соответствует ли это требованиям Приказа №533 и ГОСТ Р МЭК 61508-2?

Ответ.

Для высокоинтенсивного режима допустимая вероятность – не выше 10^{-9} в час (п. 7.4.3) поэтому вероятность опасного отказа 10^{-8} не соответствует требованиям.

Решение. Необходимо увеличить надежность (например, добавить резервирование).

Итоговые выводы.

1. Нормативная база СПАЗ.

- Обязательными требованиями являются ФЗ №116-ФЗ + Приказ №533.

- Рекомендуемыми МЭК 61511/61508.

2. Ключевые ошибки при проектировании СПАЗ.

- Неверный расчет SIL.

- Игнорирование особенностей режима работы СПАЗ/SIS.

- Недостаточная диагностика и отказоустойчивость компонентов СПАЗ.

3. Рекомендуемый подход.

Анализ рисков объекта повышенной опасности (ОПО) → спецификация (SRS) → SIL → анализ рисков СПАЗ/SIS (FMEA) → отказоустойчивая архитектура/структура SIF → диагностика/верификация.

1.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 1.3. Уяснить ответы и объяснения всех тестов. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 1.1. Федеральные нормы и правила в области промышленной безопасности.

Вопрос 1. Какие из следующих разделов относятся в первую очередь к проблеме «Общие правила взрывобезопасности»?

А) Проектирование зданий и сооружений.

В) Организация труда и обучение работников.

С) Оценка экологического воздействия.

Д) Все вышеперечисленное

Ответ В. Организация труда и обучение работников.

Объяснение.

Общие правила взрывобезопасности в первую очередь сосредоточены на организации безопасных условий труда, обучении работников и обеспечении мер по предотвращению взрывов и пожаров на опасных производственных объектах.

Вопрос 2. Какой из следующих документов является основным для соблюдения норм взрывобезопасности на нефтехимических и нефтеперерабатывающих производствах?

- А) ГОСТ Р 53325-2012.
- В) Приказ Ростехнадзора от 15.12.2020 N 533.
- С) Федеральный закон от 21.07.1997 № 116-ФЗ.
- Д) Правила охраны труда.

Ответ В. Приказ Ростехнадзора от 15.12.2020 N 533.

Объяснение.

Этот приказ устанавливает общие правила взрывобезопасности, которые обязательны для выполнения на химических, нефтехимических и нефтеперерабатывающих производствах, обеспечивая защиту от взрывов и пожаров.

Вопрос 3. Какой из следующих документов является основным нормативным актом, регулирующим вопросы промышленной безопасности на опасных производственных объектах?

- А) Приказ Ростехнадзора от 15.12.2020 N 533.
- В) Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».
- С) Правила проектирования систем автоматической пожарной сигнализации.
- Д) ГОСТ Р 53325-2012 «Системы противопожарной защиты. Пожарная сигнализация».

Ответ В. Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».

Объяснение. Этот закон является основополагающим документом, который устанавливает общие требования к безопасности на опасных производственных объектах, включая нефтехимические и нефтегазодобывающие производства. Он определяет права и обязанности организаций и работников, а также меры по предотвращению аварий.

Вопрос 4. Какое из следующих мероприятий не относится к мерам по предотвращению взрывов на опасных производственных объектах?

- А) Регулярное обучение персонала.
- В) Установка систем автоматического контроля.
- С) Менеджмент качества (ИСО 9001).
- Д) Проведение регулярных проверок оборудования.

Ответ С. Менеджмент качества (ИСО 9001).

Объяснение. Менеджмент качества (ИСО 9001) не относится к мерам по предотвращению взрывов на опасных производственных объектах, поскольку это общеуправленческая система, которая не предназначена для предотвращения взрывов и не является прямой мерой защиты. В то же время, обучение персонала (А), установка систем

контроля (В) и регулярные проверки (D) – это прямые и целенаправленные мероприятия, предписанные нормами промышленной безопасности. Важно понимать, что эффективная СМК (ISO 9001) способствует общей безопасности, но не подменяет собой специальные технические и организационные меры.

Тест 1.2. Какими законами и правилами следует руководствоваться при разработке СПАЗ?

Вопрос 1. Какой из следующих документов является основополагающим документом, регулирующим промышленную безопасность опасных производственных объектов?

- А) Приказ Ростехнадзора от 15.12.2020 N 533 [13].
- В) Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов» [12].
- С) Правила промышленной безопасности, утвержденные приказом Ростехнадзора от 25.03.2014 № 116.
- Д) Общие правила взрывобезопасности для взрывоопасных химических производств.

Ответ В. Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».

Объяснение. Этот закон является основополагающим документом в области промышленной безопасности и устанавливает общие требования к безопасности на опасных производственных объектах. Он определяет права и обязанности организаций и работников, а также меры по предотвращению аварий и обеспечению безопасности. В РФ принята иерархия нормативных документов по промышленной безопасности: ФЗ → приказ и руководства РТН → технические стандарты (МЭК 61508/61511) → отраслевые нормы и нормативные руководства предприятий.

Вопрос 2. Какой из следующих документов регулирует использование оборудования, работающего под избыточным давлением?

- А) Приказ Ростехнадзора от 15.12.2020 N 533.
- В) Федеральный закон от 21.07.1997 № 116-ФЗ.
- С) Правила промышленной безопасности, утвержденные приказом Ростехнадзора от 25.03.2014 № 116.
- Д) Общие правила охраны труда.

Ответ А.

Объяснение. Приказ Ростехнадзора от 15.12.2020 N 533.

Ранее таким документом были Правила, утвержденные Приказом №116 от 25.03.2014. Однако с 2021 года они были заменены на новые «Общие правила взрывобезопасности», утвержденные Приказом Ростехнадзора №533 от 15.12.2020. На сегодняшний день именно этот документ устанавливает требования к оборудованию, работающему под избыточным давлением, для соответствующих производств.

Тест 1.3 «Основные особенности применения закона от 21.07.1997 № 116-ФЗ.

Вопрос 1. Какова основная цель закона от 21.07.1997 № 116-ФЗ?

А) Установление штрафных санкций за нарушение норм безопасности.

В) Обеспечение промышленной безопасности на опасных производственных объектах.

С) Регулирование трудовых отношений на предприятиях.

Д) Определение стандартов качества продукции.

Ответ В. Обеспечение промышленной безопасности на опасных производственных объектах.

Объяснение. Закон от 21.07.1997 № 116-ФЗ с редакцией от 08.08.2024 (с изм. и доп., вступ. в силу с 01.09.2024) направлен на обеспечение безопасности на опасных производственных объектах, устанавливая общие требования и принципы, которые должны соблюдаться для предотвращения аварий и защиты жизни и здоровья работников.

Вопрос 2. Как закон от 21.07.1997 № 116-ФЗ влияет на проектирование новых производственных объектов?

А) Устанавливает финансовые требования.

В) Определяет требования к проектированию систем безопасности.

С) Не имеет отношения к проектированию.

Д) Упрощает процесс получения разрешений.

Ответ В. Определяет требования к проектированию систем безопасности.

Объяснение. Закон содержит нормы, касающиеся проектирования систем безопасности, включая требования к оценке рисков, выбору оборудования и организации безопасных условий труда, что критически важно для новых производственных объектов.

Вопрос 3. Какие объекты подпадают под действие закона от 21.07.1997 № 116-ФЗ?

А) Только государственные предприятия.

В) Все предприятия, независимо от формы собственности, которые ведут опасные производства.

С) Только предприятия, производящие химические вещества.

Д) Только малые и средние предприятия.

Ответ В. Все предприятия, независимо от формы собственности, у которых опасные производства.

Объяснение. Закон охватывает все опасные производственные объекты, независимо от их организационно-правовой формы, что обеспечивает единый подход к обеспечению безопасности на всех уровнях.

Вопрос 4. Какое значение имеет закон от 21.07.1997 № 116-ФЗ для работников опасных производств?

А) Он устанавливает правила назначения пенсий для работников ОАО.

В) Обеспечивает защиту прав работников и их безопасность.

С) Устанавливает только штрафы для работников.

Д) Определяет правила трудового распорядка.

Ответ В. Обеспечивает защиту прав работников и их безопасность.

Объяснение. Закон направлен на защиту работников, устанавливая требования к обеспечению безопасных условий труда и предотвращению аварий, что напрямую влияет на их здоровье и безопасность.

Вопрос 5. Какой документ служит основой для разработки более детализированных нормативных актов в области промышленной безопасности?

А) Приказ Ростехнадзора.

В) Закон от 21.07.1997 № 116-ФЗ.

С) Постановление правительства.

Д) Инструкции по охране труда.

Ответ В. Закон от 21.07.1997 № 116-ФЗ.

Объяснение. Закон от 21.07.1997 № 116-ФЗ с редакцией от 08.08.2024 (с изм. и доп., вступил в силу с 01.09.2024) является основным нормативным актом, на основе которого разрабатываются более детализированные документы и правила, регулирующие различные аспекты промышленной безопасности.

Тест 1.4. Основные особенности применения приказа Ростехнадзора от 15.12.2020 N 533.

Вопрос 1. Какова основная цель приказа Ростехнадзора от 15.12.2020 N 533?

А) Установление новых штрафов за нарушения.

В) Определение требований к промышленной безопасности на опасных производственных объектах.

С) Регулирование трудовых отношений.

Д) Упрощение процедурами лицензирования.

Ответ В. Определение требований к промышленной безопасности на опасных производственных объектах

Объяснение. Приказ направлен на установление четких требований к обеспечению безопасности на опасных производственных объектах, что включает в себя оценку рисков и контроль за соблюдением норм (I. Общие положения, пункт 2). Он не касается штрафов (А), трудовых отношений (С) или лицензирования (D).

Вопрос 2. Как приказ Ростехнадзора от 15.12.2020 N 533 влияет на проектирование систем безопасности?

А) Упрощает проектирование без дополнительных требований.

В) Устанавливает обязательные требования к проектированию систем безопасности.

С) Не имеет отношения к проектированию.

Д) Позволяет игнорировать существующие нормы безопасности.

Ответ В. Устанавливает обязательные требования к проектированию систем безопасности

Объяснение. Приказ устанавливает обязательные требования по обеспечению безопасности (Главы 3-11), вводит конкретные требования к проектированию систем безопасности, включая методы оценки рисков и выбор оборудования, что критично для обеспечения безопасности на ОПО. Варианты А и Д противоречат сути документа, а С неверен, так как приказ напрямую влияет на проектирование

Вопрос 3. Какой документ служит основой для разработки мероприятий по обеспечению безопасности на опасных производственных объектах согласно приказу Ростехнадзора от 15.12.2020 N 533?

А) Инструкции по охране труда.

В) Отчеты по оценке рисков.

С) Приказ Ростехнадзора от 15.12.2020 N 533.

Д) Постановления правительства.

Ответ С. Приказ Ростехнадзора от 15.12.2020 N 533.

Объяснение. Этот приказ является основным нормативным документом, на основе которого разрабатываются конкретные мероприятия и планы по обеспечению безопасности на опасных производственных объектах. Основным документом для разработки мер безопасности является сам приказ № 533. Инструкции по охране труда (А) и отчеты по оценке рисков (В) – это производные, внутренние документы организации, которые разрабатываются на основании требований, содержащихся в таких нормативных актах, как Приказ № 533. Постановления Правительства (Д) задают более общие рамки, но не заменяют собой детализированных правил, содержащихся в приказе надзорного органа

Вопрос 4. Каковы требования к проведению оценки риска на опасных производственных объектах согласно приказу Ростехнадзора?

А) Оценка риска выполняется Ростехнадзором.

В) Оценка риска выполняется согласно требованиям ГОСТ Р ИСО 9001.

С) Оценка риска должна проводиться систематически уполномоченными на предприятии и документироваться в виде отчетного документа установленной формы.

Д) Оценка риска проводится при возникновении аварий.

Ответ С. Оценка риска должна проводиться систематически уполномоченными на предприятии и документироваться в виде отчетной документации установленной формы.

Этот вариант точно отражает ключевые принципы, заложенные в требованиях Ростехнадзора по управлению промышленной безопасностью.

Почему вариант С правильный?

Требования приказа Ростехнадзора обязывают организацию, эксплуатирующую опасный производственный объект, самостоятельно и проактивно управлять рисками. Это означает.

Систематичность. Оценка риска – это не разовое мероприятие, а непрерывный процесс. Она проводится регулярно (например, по плану-графику), а также при изменении технологии, оборудования или нормативной базы.

Компетентность. Работу по оценке риска должны выполнять специально подготовленные и уполномоченные работники предприятия или привлеченные эксперты, обладающие необходимыми знаниями.

Документирование. Результаты оценки должны оформляться в виде отчетов или заключений. Это необходимо для предоставления в контролирующие органы (например, Ростехнадзор), анализа эффективности мероприятий и передачи информации.

Почему другие варианты неверные.

А) Оценка риска выполняется Ростехнадзором.

– Неверно. Ростехнадзор является надзорным органом. Его задача проверять, как предприятие выполняет требования законодательства, в том числе как оно само проводит оценку рисков и управляет ими. Непосредственное проведение оценки рисков для каждого объекта – это обязанность эксплуатирующей организации.

В) Оценка риска выполняется согласно требованиям ГОСТ Р ИСО 9001.

– Неверно. Хотя система менеджмента качества (ISO 9001) может быть интегрирована с системой управления промышленной безопасностью, она не подменяет собой специальные отраслевые правила. Оценка риска на ОПО регулируется в первую очередь федеральными нормами и правилами Ростехнадзора, а не стандартом по менеджменту качества.

Д) Оценка риска проводится только при возникновении аварий.
– Неверно. Этот подход является реактивным (после факта), в то время как современная концепция безопасности основана на проактивности (предупреждение). Оценка риска как раз и направлена на то, чтобы выявить потенциальные опасности и принять меры до того, как произойдет авария..

Вопрос 5. Какой из следующих аспектов не охватывается приказом Ростехнадзора от 15.12.2020 N 533?

А) Требования к проектированию систем безопасности.

В) Обязанности работников по соблюдению норм безопасности.

С) Установление штрафов за нарушения.

Д) Методология оценки рисков.

Ответ С. Установление штрафов за нарушения.

Объяснение. Приказ № 533 регулирует требования к безопасности (А), обязанности работников (В) и методологию оценки рисков (D), но не устанавливает штрафы – это компетенция КоАП РФ. Приказ сосредоточен на требованиях и методах обеспечения безопасности на опасных производственных объектах, оставляя вопросы ответственности и санкций для других нормативных актов.

Тест 1. 5. Проектирование СПАЗ/SIS в соответствии с ГОСТ Р МЭК 61508-1-2012 [1].

Вопрос 1. Какие стадии жизненного цикла системы безопасности рассматриваются в ГОСТ Р МЭК 61508-1-2012?

1. Проектирование и реализация.
2. Эксплуатация и техническое обслуживание.
3. Снятие с эксплуатации.
4. Маркетинг и продажи.
5. Первоначальная концепция.

Ответ. 1, 2, 3, 5.

Объяснение. ГОСТ Р МЭК 61508-1-2012 охватывает все стадии жизненного цикла системы безопасности, начиная с первоначальной концепции, проектирования, реализации, эксплуатации, технического обслуживания и заканчивая снятием с эксплуатации.

Маркетинг и продажи не относятся к стадиям жизненного цикла системы безопасности, рассматриваемым в стандарте.

Вопрос 2. Какой подход используется в ГОСТ Р МЭК 61508-1-2012 для определения требований к уровням полноты безопасности (SIL)?

1. Подход, основанный на оценке рисков.
2. Подход, основанный на стоимости системы.
3. Подход, основанный на аналитике экспертов.
4. Подход, основанный на анализе рынка.

Ответ. 1.

Объяснение. Стандарт использует подход, основанный на оценке рисков, для определения требований к уровням полноты безопасности (SIL). Это позволяет установить необходимый уровень безопасности, исходя из анализа потенциальных рисков и их последствий.

Вопрос 3. Какие требования устанавливает ГОСТ Р МЭК 61508-1-2012 для предотвращения систематических отказов?

1. Использование опыта и практических заключений.
2. Количественная оценка вероятности систематических отказов.
3. Внедрение мер по управлению систематическими отказами.
4. Игнорирование систематических отказов, так как их вероятность нельзя определить.

Ответ. 1, 3.

Объяснение. Стандарт устанавливает требования по предотвращению и управлению систематическими отказами, основанные на опыте и практических заключениях. При этом вероятность систематических отказов в общем случае не может быть определена количественно, поэтому стандарт фокусируется на мерах управления и предотвращения отказов СПАЗ.

Вопрос 4. Что означает понятие «стойкость к систематическим отказам» в контексте ГОСТ Р МЭК 61508-1-2012?

1. Уверенность в том, что элемент системы не будет подвержен систематическим отказам.
2. Уверенность в том, что полнота безопасности элемента соответствует заданным уровням SC и SIL.
3. Способность элемента системы работать без технического обслуживания.
4. Уверенность в том, что элемент системы будет дешевле в производстве.

Ответ. 2.

Объяснение. Стойкость к систематическим отказам характеризует уверенность в том, что полнота безопасности элемента системы, касающаяся систематических отказов, удовлетворяет требованиям заданного уровня полноты безопасности (SIL). Системная категория (SC) — это архитектурный, качественный показатель, определенный ГОСТ Р МЭК 61511, который задает требования к структуре и отказоустойчивости системы управления безопасностью. Она является ключевым инструментом для обеспечения того, что система обладает необходимой надежностью для предотвращения аварийных ситуаций в промышленности.

Вопрос 5. Какие из перечисленных действий необходимы для достижения заданной функциональной безопасности в соответствии с ГОСТ Р МЭК 61508-1-2012?

1. Разработка спецификации требований к системе безопасности.
2. Проведение оценки рисков.
3. Учет только случайных отказов.
4. Выполнение всех требований стандарта.

Ответ. 1, 2, 4.

Объяснение. Для достижения заданной функциональной безопасности необходимо разработать спецификацию требований к системе безопасности, провести оценку рисков и выполнить все требования стандарта. Учет только случайных отказов недостаточен, так как стандарт также требует управления систематическими отказами.

Вопрос 6. Какие из перечисленных утверждений верны относительно систематических отказов?

1. Вероятность систематических отказов можно точно определить количественно.

2. Систематические отказы могут быть предотвращены за счет качественного проектирования и управления.

3. Систематические отказы не влияют на функциональную безопасность.

4. ГОСТ Р МЭК 61508-1-2012 фокусируется на предотвращении систематических отказов.

Ответ. 2, 4.

Объяснение. Вероятность систематических отказов в общем случае не может быть определена количественно, но их можно предотвратить за счет качественного проектирования и управления. Стандарт фокусируется на предотвращении таких отказов, так как они напрямую влияют на функциональную безопасность.

Тест 1.6. Требования ГОСТ Р МЭК 61508-2-2012 [2]. Проектирование СПАЗ/SIS.

Вопрос 1. Какие из следующих утверждений соответствуют требованиям ГОСТ Р МЭК 61508-2-2012 к проектированию СПАЗ/SIS? (Выберите все Ответ.)

1. Уровни полноты безопасности (SIL) определяются на основе оценки рисков.

2. Для систем, работающих в режиме низкой интенсивности запросов, нижняя граница вероятности опасного отказа по запросу составляет 10^{-5} .

3. Для систем, работающих в режиме высокой интенсивности запросов, нижняя граница вероятности опасного отказа составляет 10^{-7} в час.

4. Целевые меры отказов для функций безопасности должны быть связаны с уровнями полноты безопасности (SIL).

5. ГОСТ Р МЭК 61508-2-2012 не устанавливает требований к вероятности опасных отказов.

Ответ: 1, 2, 4.

Объяснение.

1. Верно. Уровни полноты безопасности (SIL) определяются на основе оценки рисков. Это один из ключевых принципов стандарта, который требует анализа рисков для определения необходимого уровня безопасности.

2. Верно. Для систем, работающих в режиме низкой интенсивности запросов, стандарт устанавливает нижнюю границу вероятности опасного отказа по запросу на уровне 10^{-5} .

3. Неверно. Для систем, работающих в режиме высокой интенсивности запросов или в непрерывном режиме, нижняя граница вероятности опасного отказа составляет 10^{-9} в час, а не 10^{-7} .

4. Верно. Целевые меры отказов для функций безопасности должны быть связаны с уровнями полноты безопасности (SIL). Это

означает, что для каждого уровня SIL устанавливаются соответствующие требования к надежности системы.

5. Неверно. Стандарт явно устанавливает требования к вероятности опасных отказов в зависимости от режима работы системы.

Вопрос 2. Какие из следующих утверждений о режимах работы СПАЗ/SIS соответствуют требованиям ГОСТ Р МЭК 61508-2-2012? (Выберите все Ответ).

1. В режиме низкой интенсивности запросов вероятность опасного отказа по запросу должна быть не выше 10^{-5} .

2. В режиме высокой интенсивности запросов вероятность опасного отказа должна быть не выше 10^{-9} в час.

3. В непрерывном режиме работы вероятность опасного отказа должна быть не выше 10^{-7} в час.

4. Режим работы системы не влияет на требования к вероятности опасных отказов.

Ответ. 1, 2.

Объяснение.

1. Верно. Для режима низкой интенсивности запросов стандарт устанавливает вероятность опасного отказа по запросу на уровне не выше 10^{-5} .

2. Верно. Для режима высокой интенсивности запросов или непрерывного режима стандарт устанавливает вероятность опасного отказа на уровне не выше 10^{-9} в час.

3. Неверно. В непрерывном режиме работы вероятность опасного отказа должна быть не выше 10^{-9} в час, а не 10^{-7} .

4. Неверно. Режим работы системы напрямую влияет на требования к вероятности опасных отказов, так как для разных режимов установлены разные границы.

Вопрос 3. Какие из следующих шагов являются обязательными при проектировании СПАЗ/SIS в соответствии с ГОСТ Р МЭК 61508-2-2012? (Выберите все Ответ.)

1. Проведение анализа рисков для определения уровня полноты безопасности (SIL).

2. Разработка спецификации требований к безопасности.

3. Установление целевых мер отказов для функций безопасности.

4. Игнорирование режима работы системы при определении вероятности опасных отказов.

Ответ: 1, 2, 3.

Объяснение.

1. Верно. Анализ рисков является обязательным шагом для определения уровня полноты безопасности (SIL).

2. Верно. Разработка спецификации требований к безопасности необходима для обеспечения соответствия системы установленным стандартам.

3. Верно. Установление целевых мер отказов для функций безопасности является обязательным требованием стандарта.

4. Неверно. Режим работы системы должен учитываться при определении вероятности опасных отказов, так как для разных режимов установлены разные требования.

Вопрос 4. Какие из следующих утверждений о уровнях полноты безопасности (SIL) верны? (Выберите все Ответ.)

1. SIL 1 соответствует наименьшему уровню требований к безопасности.

2. SIL 4 соответствует наивысшему уровню требований к безопасности.

3. Уровень SIL определяется исключительно на основе стоимости системы.

4. Уровень SIL зависит от вероятности опасных отказов и режима работы системы.

Ответ: 1, 2, 4.

Объяснение.

1. Верно. SIL 1 соответствует наименьшему уровню требований к безопасности.

2. Верно. SIL 4 соответствует наивысшему уровню требований к безопасности.

3. Неверно. Уровень SIL определяется на основе анализа рисков, а не стоимости системы.

4. Верно. Уровень SIL зависит от вероятности опасных отказов и режима работы системы.

МЭК 61508-2 был разработан, чтобы формализовать требования к обеспечению полноты безопасности аппаратных, электронных и программных средств систем, связанных с безопасностью, включая датчики и исполнительные элементы. В нем приведены методы и средства, направленные против как случайных, так и систематических отказов аппаратных средств. Они, включают в себя соответствующую комбинацию средств по предотвращению неисправностей и управлению отказами. Если для обеспечения функциональной безопасности необходимы действия оператора, то приводятся требования к интерфейсу оператора.

Для обнаружения случайных отказов аппаратных средств в стандарте определяются методы и средства диагностического тестирования, реализуемые на уровне программного обеспечения и аппаратных средств, устанавливаются.

- метод разработки спецификации требований к безопасности, необходимых для достижения заданной функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью.

- целевые меры отказов для функций безопасности, связанные с уровнями полноты безопасности;

- нижняя граница для целевых мер отказов для функции безопасности, реализуемой одиночной Э/Э/ПЭ системой, связанной с безопасностью

- требования к предотвращению и управлению систематическими отказами, основанные на опыте и заключениях из практического опыта. Учитывая, что вероятность возникновения систематических отказов в общем случае не может быть определена количественно, настоящий стандарт позволяет утверждать для специфицируемой функции безопасности, что целевая мера отказов, связанных с этой функцией, может считаться достигнутой, если все требования стандарта были выполнены.

Основные моменты, на которые следует обратить внимание.

- Определение уровней полноты безопасности (SIL) на основе анализа рисков.

- Учет режима работы системы при установлении требований к вероятности опасных отказов.

- Связь целевых мер отказов с уровнями SIL.

Эти знания необходимы для понимания принципов функциональной безопасности и их применения в проектировании систем, связанных с безопасностью.

Тест 1.7. ГОСТ Р МЭК 61508-3-2018 [3]. Проектирование СПАЗ/SIS.

Вопрос 1. Какое программное обеспечение регулируется ГОСТ Р МЭК 61508-3-2018?

1. Любое прикладное программное обеспечение.
2. Программное обеспечение, связанное с безопасностью (включая ОС, системное ПО, программы в коммуникационных сетях).
3. Программное обеспечение АСУ ТП.
4. Инструменты для разработки не связанных с безопасностью систем.

Ответ 2.

Объяснение. Стандарт применяется к программному обеспечению, являющемуся частью системы безопасности или используемому для её разработки. Это включает ОС, системное ПО, программы в сетях, интерфейсы пользователей, встроенные программно-аппаратные средства и прикладные программы (пункт 1).

Вопрос 2. Какие требования устанавливает ГОСТ Р МЭК 61508-3-2018 к инструментальным средствам поддержки?

1. Они должны быть бесплатными.
2. Они должны соответствовать требованиям МЭК 61508-1 и МЭК 61508-2.
3. Их можно использовать без проверки.
4. Они должны быть разработаны только одной организацией.

Ответ. 2.

Объяснение. Стандарт задает конкретные требования к инструментальным средствам поддержки, используемым для разработки и конфигурации систем безопасности, в соответствии с МЭК 61508-1 и МЭК 61508-2 (пункт с).

Вопрос 3. Что включает модель жизненного цикла программного обеспечения по ГОСТ Р МЭК 61508-3-2018?

1. Применение методов для предотвращения ошибок, ранжированных по уровням стойкости к систематическим отказам.

2. Игнорирование этапа тестирования.

3. Требования только к этапу разработки.

4. Учет мнения пользователей на всех этапах.

Ответ 1.

Объяснение. Согласно ГОСТ Р МЭК 61508-3-2018 п.7, модель жизненного цикла программного обеспечения (ПО) – это не единая жесткая последовательность, а структурированный набор процессов и видов деятельности, которые должны быть адаптированы под конкретный проект.

Ключевые составляющие модели, описанные в стандарте, включают.

1. **Фундаментальные фазы жизненного цикла.**

- **Анализ требований к функциональной безопасности.** Определение целей безопасности и уровней полноты безопасности (Safety Integrity Level, SIL) для программных функций.

- **Проектирование.** Создание архитектуры ПО, детальное проектирование и выбор методов верификации для каждого уровня.

- **Кодирование и реализация.** Создание исходного кода с применением регламентированных языков и методов программирования.

- **Тестирование.** Планирование и проведение тестов (модульных, интеграционных, системных) для верификации и валидации ПО.

- **Интеграция.** Поэтапное объединение программных компонентов и интеграция ПО с аппаратными средствами.

- **Ввод в эксплуатацию, эксплуатация, техническое обслуживание и вывод из эксплуатации.**

2. **Концепция «V-модели» (или «V-диаграммы»).** Стандарт явно рекомендует использовать V-образную модель как иллюстрацию жизненного цикла. Ее суть в том, что каждой фазе разработки (спуск по левой стороне «V») соответствует строго определенная фаза тестирования (подъем по правой стороне «V»). Это обеспечивает прослеживаемость и планирование верификационных мероприятий на ранних этапах.

3. **Сквозные процессы и деятельность.** Модель включает не только этапы создания ПО, но и процессы, действующие на протяжении всего цикла.

- **Верификация и валидация.** Постоянная проверка на соответствие требованиям и правильность функционирования.
- **Управление конфигурацией.** Контроль версий и изменений всех артефактов (требования, код, тесты и т.д.).
- **Управление качеством и функциональной безопасностью.**
- **Оценка полноты безопасности.**

Стандарт не навязывает единую последовательность этапов (каскадную, интерактивную и т.д.). Он требует, чтобы организация *определила и документально зафиксировала* свою модель жизненного цикла ПО, которая должна охватывать все указанные в стандарте процессы и виды деятельности, обеспечивая необходимый уровень уверенности в функциональной безопасности.

Таким образом, модель по ГОСТ Р МЭК 61508-3-2018 – это индивидуально определяемая для проекта структура, основанная на принципах V-модели и включающая все обязательные процессы для достижения и подтверждения требуемого уровня безопасности ПО.

Вопрос 4. Какие аспекты программного обеспечения должны быть подтверждены перед интеграцией в Э/Э/ПЭ систему?

1. Соответствие требованиям безопасности, включая документацию и процедуры.
2. Стоимость разработки.
3. Популярность ПО на рынке.
4. Скорость выполнения кода.

Ответ 1.

Объяснение. Стандарт требует документированной информации, подтверждающей соответствие ПО требованиям безопасности, организации, выполняющей интеграцию (пункт f).

Вопрос 5. Какие требования предъявляются к пользователям для эксплуатации и обслуживания Э/Э/ПЭ систем?

1. Подготовка информации и процедур по работе с ПО.
2. Использование ПО без документации.
3. Проведение маркетингового анализа.
4. Отсутствие обучения персонала.

Ответ 1.

Объяснение. Стандарт требует подготовки информации и процедур, необходимых пользователям для эксплуатации и техобслуживания системы (ГОСТ Р МЭК 61508-3 пункт g).

Вопрос 6. Какие организации должны соблюдать требования ГОСТ Р МЭК 61508-3-2012 при модификации ПО?

1. Только разработчики.

2. Все организации, выполняющие модификацию ПО, связанного с безопасностью.

3. Только тестировщики.

4. Организации, не связанные с безопасностью.

Ответ 2.

Объяснение. Требования стандарта распространяются на любые организации, выполняющие модификацию ПО, связанного с безопасностью (Область применения пункт h).

Вопрос 7. Что включает понятие «стойкость к систематическим отказам» в контексте ПО?

1. Уверенность в том, что ПО не содержит ошибок проектирования.

2. Способность ПО сохранять функциональную безопасность при наличии систематических ошибок.

3. Использование только устаревших технологий.

4. Отказ от обновлений ПО.

Ответ 2.

Объяснение. Стойкость к систематическим отказам означает, что ПО сохраняет заданный уровень безопасности даже при наличии ошибок (Область применения пункт d).

Вопрос 8. Какие действия требуются на этапе проектирования ПО согласно стандарту?

1. Применение методов верификации и валидации.

2. Игнорирование анализа рисков.

3. Использование непроверенных инструментов.

4. Отказ от документирования процессов.

Ответ 1.

Объяснение. Стандарт требует применения мероприятий и методов (например, верификации, валидации) для предотвращения ошибок на всех этапах жизненного цикла (Область применения пункт e).

Вопрос 9. Какие из перечисленных требований относятся к жизненному циклу ПО?

1. Ранжирование методов по уровням SIL.

2. Учет только случайных отказов.

3. Использование устаревших стандартов.

4. Отсутствие этапа тестирования.

Ответ 1.

Объяснение. Методы и мероприятия ранжируются по уровням полноты безопасности (SIL) в зависимости от требуемой стойкости к отказам ((Область применения пункт e). Эти требования включают в себя применение мероприятий и методов, ранжированных по уровням требуемой стойкости к систематическим отказам и предназначенных для предотвращения и управления ошибками и отказами в программном обеспечении.

Вопрос 10. Для чего предназначена часть 3 ГОСТ Р МЭК 61508-3-2012?

1. Для регулирования механических компонентов.
2. Для управления рисками, связанными с программным обеспечением в системах безопасности.
3. Для разработки игровых приложений.
4. Для оценки стоимости проектов.

Ответ 2.

Объяснение. Часть 3 фокусируется на требованиях к программному обеспечению в системах безопасности, включая предотвращение систематических ошибок и управление жизненным циклом.

МЭК 61508-3 был разработан, чтобы формализовать требования обеспечения полноты безопасности для программного обеспечения как встроенного (включая диагностические средства обнаружения неисправностей), так и прикладного.

Стандарт требует использовать комбинированный подход, включающий исключение ошибок (обеспечение качества) и устойчивость к ошибкам (за счет архитектуры программного обеспечения), так как не существует известного способа проверить отсутствие отказов в достаточно сложном программном обеспечении, связанном с безопасностью, и особенно избежать ошибок в технических условиях и в проекте.

МЭК 61508-3 устанавливает принципы разработки программного обеспечения, включающие проектирование сверху вниз, модульность, проверка на каждой стадии жизненного цикла разработки, проверка программных модулей и библиотек программных модулей, а также четкое документирование для облегчения проверки и подтверждения соответствия. Для различных уровней программного обеспечения требуются различные уровни гарантии того, что эти и связанные с ними принципы были правильно реализованы. Ключевыми рекомендациями ГОСТ Р МЭК 61508-3-2012 являются.

- Применение к ПО, связанному с безопасностью.
- Требования к инструментам, жизненному циклу, стойкости к отказам.
- Документация и процедуры для пользователей.
- Обязанности организаций при модификации ПО.

Тест 1.8. ГОСТ Р МЭК 61508-4-2012 [4]. Проектирование СПАЗ/SIS.

Вопрос 1. Как описывается основная терминология СПАЗ в стандартах 61508 ?

1. Используется схема онтологии IDEF.
2. Приводится таблица в виде принятых определений и сокращений.

3. Термины и определения располагаются в алфавитном порядке английского языка.

4. Термины и определения располагаются в алфавитном порядке русского языка.

Ответ 3.

Национальный технический стандарт это официальный документ, предназначенный для использования в Российской Федерации. Для того чтобы специалисты могли быстро найти нужное определение, оно должно быть упорядочено по алфавиту языка, на котором написан сам стандарт и на котором он будет использоваться.

В целом основная терминология и определения СПАЗ объединены в 8 групп (п.3.1-3.8)

Представьте, что вы ищете термин «Система противоаварийной автоматической защиты». Если бы он был в английском порядке, вам пришлось бы сначала вспомнить английский аналог (Safety Instrumented System, СПАЗ/SIS) и искать по букве «S», что крайне неудобно. Поэтому логично и практически необходимо, чтобы порядок был по русскому алфавиту.

Вопрос 2. Какие технологии учитываются в стандарте для достижения безопасности?

1. Механические, гидравлические, пневматические.
2. Электрические, электронные, программируемые электронные.
3. Биологические и химические.
4. Только программируемая электроника.

Ответ. 1, 2.

Объяснение. Стандарт рассматривает комбинацию различных технологий. механических, гидравлических, пневматических, электрических, электронных и программируемых электронных систем (СПАЗ/SIS). Биологические и химические технологии не упоминаются. В стандарте ГОСТ Р 59790-2021/IEC TR 61511-0.2018 перечень технологий расширен и включает также химические (п. 4.1 стандарта ГОСТ Р 59790-2021).

Вопрос 3. Какие атрибуты входят в понятие «полнота безопасности»?

1. Безотказность.
2. Ремонтопригодность.
3. Готовность.
4. Информационная безопасность.

Ответ. 1, 2, 3, 4.

Объяснение. Полнота безопасности – это вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного интервала времени (п.3.5.4). Она включает

не только безотказность, но и ремонтпригодность, готовность, долговечность и информационную безопасность. Это расширяет классическое понятие надежности.

Вопрос 4. Что означает «стратегия безопасности» по ГОСТ Р МЭК 61508-4-2012?

1. Использование только одной технологии для упрощения системы.
2. Учет всех элементов системы (датчики, управляющие устройства, исполнительные механизмы).
3. Игнорирование человеческого фактора.
4. Фокус только на программное обеспечение.

Ответ 2.

Объяснение. Стратегия безопасности должна учитывать все элементы системы, включая датчики, управляющие устройства и исполнительные механизмы, а также комбинацию различных технологий.

Вопрос 5. Как полнота безопасности (SIL) соотносится с классической надежностью?

1. Это синонимы.
2. Полнота безопасности – часть надежности, включающая дополнительные атрибуты.
3. Надежность не связана с безопасностью.
4. Полнота безопасности учитывает только случайные отказы.

Ответ 2.

Объяснение. Полнота безопасности является частью надежности, но включает дополнительные аспекты. ремонтпригодность, готовность, долговечность и информационную безопасность.

Вопрос 6. Какие виды опасных событий рассматриваются в разделе 3.6 стандарта?

1. Сбои, отказы, ошибки.
2. Только аппаратные отказы.
3. Умышленные кибератаки.
4. Экономические риски.

Ответ 1.

Объяснение. Раздел 3.6 стандарта классифицирует опасные события на сбои, отказы и ошибки, что важно для анализа рисков.

Вопрос 7. Почему стандарт рекомендует использовать разнообразные технологии в СПАЗ/SIS?

1. Для снижения стоимости системы.
2. Чтобы минимизировать общие систематические ошибки за счет разнообразия.
3. Для упрощения интеграции.
4. Чтобы увеличить зависимость от одной технологии.

Ответ 2.

Объяснение. Использование разных технологий (например, механической и электронной) снижает вероятность одновременных систематических отказов, повышая общую надежность.

Вопрос 8. Какие требования предъявляются к проектированию СПАЗ/SIS для обеспечения информационной безопасности?

1. Шифрование всех данных.
2. Учет информационной безопасности как атрибута полноты безопасности.
3. Игнорирование кибератак.
4. Использование только аналоговых систем.

Ответ 2.

Объяснение. Информационная безопасность включена в атрибуты полноты безопасности, что требует её учета при проектировании СПАЗ/SIS (например, защита от несанкционированного доступа).

Вопрос 9. Какие этапы жизненного цикла системы должны учитывать полноту безопасности?

1. Только проектирование.
2. Только эксплуатация.
3. Все этапы (проектирование, разработка, эксплуатация, вывод из эксплуатации).
4. Только тестирование.

Ответ 3.

Объяснение. Полнота безопасности должна учитываться на всех этапах жизненного цикла системы, включая проектирование, эксплуатацию и вывод из эксплуатации.

Вопрос 10. Что подразумевает «готовность» как атрибут полноты безопасности?

1. Способность системы выполнять функцию безопасности в любой момент времени.
2. Работа без профилактического обслуживания.
3. Использование устаревших компонентов.
4. Фокус только на стоимость системы.

Ответ. 1.

Объяснение. Готовность означает, что система способна выполнить функцию безопасности в требуемый момент, что зависит от её надежности и ремонтпригодности.

Вопрос 11. Какие меры помогают управлять систематическими отказами в СПАЗ/SIS?

1. Применение разнообразных технологий.
2. Строгая верификация и валидация на всех этапах.
3. Игнорирование человеческого фактора.
4. Использование только случайных проверок.

Ответ 1, 2.

Объяснение. Систематические отказы предотвращаются за счет комбинации технологий и строгих процессов верификации/валидации на всех этапах жизненного цикла.

Тест охватывает ключевые аспекты ГОСТ Р МЭК 61508-4-2012.

- Многообразие технологий для снижения рисков.
- Полнота безопасности как комплексный атрибут (безотказность, ремонтпригодность, готовность, информационная безопасность).
- Учет всех элементов системы (датчики, управляющие устройства, исполнительные механизмы).
- Управление систематическими отказами через верификацию и разнообразие технологий.

Тест 1.9. ГОСТ Р МЭК 61508-5-2012 [5]. Проектирование СПАЗ/SIS.

Вопрос 1. Название стандарта «Рекомендации по применению методов определения уровней полноты безопасности». Что означает «полнота безопасности в режиме с различной частотой запросов»?

1. Уровень SIL одинаков для всех режимов работы системы.
2. SIL зависит от частоты (интенсивности) запросов на выполнение функции безопасности (низкая/высокая частота).
3. Требования к безопасности применяются только к системам с постоянной нагрузкой.
4. Частота запросов не влияет на проектирование СПАЗ/SIS.

Ответ 2.

Объяснение. В стандарте различают режимы с низкой (например, аварийное отключение) и высокой (например, непрерывный контроль) частотой запросов. Требуемый уровень SIL зависит от этого параметра, так как вероятность отказа функции безопасности должна быть ниже в режимах с высокой частотой запросов (раздел А.5)

Вопрос 2. Какие методы используются для минимизации отказов по общей причине (CCF)?

1. Применение идентичных компонентов во всех слоях защиты.
2. Использование разнообразных технологий и независимых каналов.
3. Увеличение количества резервных систем без проверки.
4. Отказ от анализа зависимых отказов.

Ответ 2.

Объяснение. Общая причина отказа (CCF) – это событие, при котором несколько компонентов системы выходят из строя одновременно из-за одной общей причины. Это особенно опасно в системах с резервированием, где несколько устройств должны обеспечить надежность. Если у них есть общая уязвимость, вся система может отказывать.

Примеры общих причин отказов.

Производственные/конструктивные дефекты Партия датчиков давления имеет один и тот же скрытый дефект из-за ошибки на заводе. Все датчики в системе выходят из строя одинаково при определенной температуре.

Ошибки установки и обслуживания При техническом обслуживании все три резервных насоса неправильно откалиброваны одним специалистом с использованием неверной методики.

Внешние воздействия и окружающая среда Наводнение в машинном зале выводит из строя все резервные источники питания, расположенные на одном этаже.

Программные ошибки. Во всех контроллерах системы управления используется одинаковая версия программного обеспечения. Обнаруженная ошибка в коде одновременно нарушает работу всех устройств.

Ошибки проектирования и процедур Недостаток в общей конструкции системы охлаждения (например, малый диаметр трубы) приводит к перегреву всех резервированных оборудования.

ССФ возникают, когда один дефект приводит к отказу нескольких компонентов. Для их предотвращения стандарт рекомендует использовать разнообразные технологии (например, механические + электронные) и независимые каналы, чтобы исключить общие точки отказа.

Вопрос 3. Как распределяются требования к SIL при наличии нескольких компонентов (устройств) к контуре (SIF) защиты?

1. Все компоненты должны иметь одинаковый SIL.
2. SIL распределяется так, чтобы общая безопасность соответствовала целевому уровню риска.
3. Требования к SIL применяются только к основному компоненту.
4. Компоненты защиты не влияют на SIL.

Ответ 2.

Объяснение. При наличии нескольких компонентов защиты (например, датчики + логический контроллер + исполнительный механизм) требования к SIL распределяются между ними. Это фундаментальный принцип стандартов МЭК 61508/61511. Цель – не сделать все слои одинаково «сильными», а обеспечить требуемое снижение риска в целом, часто наиболее экономичным способом.

Комбинация нескольких слабых элементов не дает простой суммы. Более того, стандарты накладывают ограничения на то, как можно комбинировать элементы для достижения целевого уровня.

Почему другие варианты неверны?

1) Все компоненты должны иметь одинаковый SIL. – Негибко и экономически неэффективно. Требуемая цель безопасности может быть достигнута разными путями.

3) Требования к SIL применяются только к основному компоненту. Не понятно какой компонент следует считать основным. Это игнорирует вклад других компонентов.

4) Компоненты защиты не влияют на SIL. – Абсолютно неверно. Основная задача анализа – как раз определить, какой вклад в снижение риска вносят все существующие компоненты защиты, чтобы понять, какие дополнительные меры (и с каким SIL) требуются.

Вопрос 4. Что такое метод ALARP?

1. Полное устранение всех рисков независимо от затрат.
2. Снижение рисков до уровня, который считается приемлемым с учетом экономических и технических факторов.
3. Игнорирование рисков, если их устранение дорого.
4. Использование только качественных компонентов.

Ответ 2.

Объяснение. Метод ALARP требует снижения рисков до минимально достижимого уровня, который технически и экономически оправдан. Риски должны быть «настолько низкими, насколько это разумно возможно» (Раздел В.2).

Вопрос 5. Какие этапы включает анализ слоя защиты (АСЗ)?

1. Идентификация опасностей, оценка эффективности существующих слоев защиты, определение необходимости дополнительных мер.
2. Проверка стоимости системы.
3. Анализ только программного обеспечения.
4. Игнорирование человеческого фактора.

Ответ 1.

Объяснение. АСЗ включает.

- Определение потенциальных опасностей.
- Оценку существующих слоев защиты (например, предохранительные клапаны, аварийное отключение).
- Расчет остаточного риска и необходимости дополнительных мер (например, внедрение СПАЗ/SIS). См. раздел F.6 стандарта.

Вопрос 6. Для чего используется метод графа рисков?

1. Для визуализации зависимостей между событиями, приводящими к аварии.
2. Для расчета стоимости проекта.
3. Для тестирования программного обеспечения.
4. Для оценки эргономики интерфейса.

Ответ 1.

Объяснение. Граф рисков (Risk Graph) – это качественный метод, который помогает определить требуемый SIL на основе оценки.

- Серьезности последствий (S).
- Частоты нахождения в опасной зоне (F).
- Вероятности отказа защитных мер (P).
- Вероятности аварии (W).

См. п Е.1-Е.6 стандарта

Вопрос 7. Что такое «ослабляющие системы»?

1. Системы, снижающие последствия аварии (например, аварийная вентиляция).

2. Резервные каналы СПАЗ/SIS.

3. Компоненты, увеличивающие риск.

4. Инструменты для калибровки датчиков.

Ответ 1.

Объяснение. Ослабляющие системы уменьшают последствия аварии, если предотвратить её не удалось. Примеры. системы пожаротушения, аварийные клапаны сброса давления.

См. А.9 стандарта.

Тест 1.10. ГОСТ Р МЭК 61508-7-2012 [7]. Проектирование СПАЗ/SIS.

Вопрос 1. Какие методы используются для управления случайными отказами в Э/Э/ПЭ системах?

1. Резервирование компонентов.

2. Регулярная калибровка оборудования.

3. Применение методов верификации кода.

4. Анализ дерева отказов (FTA).

Ответ: 1, 2, 4.

Объяснение.

Случайные отказы связаны с износом, внешними воздействиями или производственными дефектами.

- Резервирование снижает вероятность отказа системы (например, 1oo2 архитектура).

- Калибровка поддерживает точность оборудования.

- FTA помогает оценить вероятность случайных отказов.

Верификация кода относится к предотвращению систематических отказов.

См. приложение А стандарта

Вопрос 2. Что определяет систематическую способность. Этот показатель является мерой.

а) Частоты опасных отказов.

б) Количество остаточных ошибок проектирования СПАЗ/SIS.

с) Удобства использования на системном уровне.

д) Общей частоты отказов.

е) Точности продукта.

Ответ б.

Объяснение. Систематическая способность — это показатель, присваиваемый процессу проектирования и тестирования на основе соответствия этого процесса всем необходимым требованиям заданного уровня SIL в соответствии с МЭК 61508. Требования указаны в

таблицах частей 2 и 3 стандарта. Оценка SIL 3 присваивается только в том случае, если выполнены все требования SIL 3.

Вопрос 3. Что включает предотвращение систематических отказов программного обеспечения?

1. Тестирование на всех этапах жизненного цикла.
2. Использование стандартизированных протоколов связи.
3. Формальная верификация алгоритмов.
4. Применение разнообразных технологий в резервировании.

Ответ: 1, 3.

Объяснение.

- Систематические отказы вызваны ошибками проектирования, кодирования или документации.
- Тестирование (модульное, интеграционное, системное) выявляет ошибки на ранних этапах.
- Формальная верификация (например, математическая проверка кода) гарантирует соответствие требованиям.
- Пункты 2 и 4 относятся к аппаратным решениям.

Вопрос 4. Какие этапы жизненного цикла программного обеспечения регламентирует ГОСТ Р МЭК 61508-7-2012?

1. Сбор требований и спецификация.
2. Кодирование и тестирование.
3. Эксплуатация и вывод из эксплуатации.
4. Маркетинг и продажи.

Ответ: 1, 2, 3.

Объяснение.

Стандарт охватывает все этапы жизненного цикла ПО.

- Сбор требований (анализ рисков, спецификация функций безопасности).
- Разработка (кодирование, модульное тестирование).
- Внедрение (интеграция с аппаратурой).
- Эксплуатация (обновления, мониторинг).
- Вывод из эксплуатации (архивация данных, утилизация).

Маркетинг не относится к техническим этапам.

Вопрос 5. Что такое вероятностный подход к полноте безопасности предварительно разработанных программных средств?

1. Оценка вероятности опасного отказа на основе статистики использования.
2. Полный отказ от использования стороннего ПО.
3. Использование только открытого исходного кода.
4. Анализ соответствия SIL требованиям через тестовые сценарии.

Ответ 1.

Объяснение.

Предварительно разработанное ПО (например, библиотеки, ОС) должно иметь подтвержденную вероятность опасных отказов

(PFDavg/PFH), соответствующую требуемому SIL. Это достигается через анализ статистики отказов, верификацию и сертификацию.

Вопрос 6. Какие методы рекомендует стандарт для проектирования СПАЗ (систем противоаварийной защиты)?

1. Применение многослойной защиты (аппаратной и программной).

2. Использование только механических систем.

3. Интеграция с системами управления предприятием.

4. Игнорирование человеческого фактора.

Ответ 1.

Объяснение.

- СПАЗ должны комбинировать аппаратные и программные слои защиты для снижения систематических и случайных отказов.

- Пример. резервированные датчики (аппаратура) + логика аварийного отключения (ПО).

Вопрос 7. Что подразумевает объектно-ориентированное программирование (ООП) в контексте функциональной безопасности?

1. Инкапсуляция и наследование для упрощения тестирования.

2. Использование глобальных переменных для ускорения работы.

3. Отказ от документации для гибкости.

4. Применение только низкоуровневых языков.

Ответ 1.

Объяснение.

- ООП позволяет структурировать код, упрощая верификацию и тестирование.

- Инкапсуляция скрывает детали реализации, снижая риск ошибок.

- Наследование и полиморфизм должны использоваться осторожно, чтобы не усложнить анализ безопасности.

Вопрос 8. Как стандарт регулирует соответствие международных и российских нормативов?

1. Требуется полного перевода международных стандартов.

2. Устанавливает эквивалентность ссылочных стандартов (например, IEC 61508 → ГОСТ Р МЭК 61508).

3. Запрещает использование зарубежных аналогов.

4. Игнорирует различия в требованиях.

Ответ 2.

Объяснение. ГОСТ Р МЭК 61508-7-2012 является локализованной версией IEC 61508-7. Это означает, что международные стандарты по функциональной безопасности соответствуют российским аналогам. А это в свою очередь упрощает сертификацию систем безопасности зарубежными компаниями.

Вопрос 9. Какие меры применяются для достижения полноты безопасности ПО.

1. Статический анализ кода.
2. Динамическое тестирование в реальных условиях.
3. Использование типовых, но устаревших библиотек.
4. Ручной ввод данных без проверки.

Ответ 1, 2.

Объяснение.

- Статический анализ выявляет синтаксические и логические ошибки на этапе разработки.
- Динамическое тестирование проверяет работу системы в условиях, приближенных к реальным.
- Пункты 3 и 4 повышают риск систематических отказов.

Вопрос 10. Что такое стойкость к систематическим отказам для ПО?

1. Способность функционировать корректно при наличии ошибок в требованиях.
2. Гарантия отсутствия ошибок в коде.
3. Использование только аппаратных решений.
4. Игнорирование этапа тестирования.

Ответ 1.

Объяснение.

Стойкость к систематическим отказам означает, что ПО может сохранять безопасность даже при некорректных входных данных или частичных сбоях. Она достигается через защитное программирование, избыточные проверки и ограничение воздействия ошибок.

Вопрос 11. Какие методы анализа рисков применяются для СПАЗ?

1. HAZOP (Анализ опасностей и рабочих характеристик).
2. FMEA (Анализ видов и последствий отказов).
3. SWOT-анализ.
4. Маркетинговые исследования.

Ответ: 1, 2.

Объяснение.

- HAZOP [18] и FMEA [21] – ключевые методы для идентификации опасностей и оценки их влияния на систему.
- SWOT-анализ и маркетинг не связаны с технической безопасностью.

В стандарте дается.

- Анализ методов и средств для Э/Э/ПЭ систем, связанных с безопасностью. Управление случайными отказами технических средств.
- Анализ методов и средств для Э/Э/ПЭ систем, связанных с безопасностью. Предотвращение систематических отказов.
- Анализ методов и средств достижения полноты безопасности программного обеспечения.

- Вероятностный подход определения полноты безопасности предварительно разработанных программных средств обзор методов и мер для проектирования СПАЗ.

- Определение свойств стадий жизненного цикла программного обеспечения.

- Руководство по разработке связанного с безопасностью объектно ориентированного программного обеспечения

- Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации.

Тест охватывает ключевые аспекты ГОСТ Р МЭК 61508-7:

- Управление отказами. разделение на случайные и систематические, методы их предотвращения.

- Жизненный цикл ПО. от требований до вывода из эксплуатации.

- Верификация и Тестирование. статический/динамический анализ, формальные методы.

- Проектирование многослойных программных систем, структурирование кода.

- Гармонизация российских и международных требований по СПАЗ.

Тест 1.11. Назначение ГОСТ Р МЭК 61511-1-2018 [8]. Проектирование СПАЗ/SIS (СПАЗ).

Вопрос 1. Какая основная цель ГОСТ Р МЭК 61511-1-2018?

1. Установить требования к функциональной безопасности систем управления производством.

2. Определить жизненный цикл СПАЗ/SIS (СПАЗ) для снижения рисков в промышленных процессах.

3. Регулировать энергоэффективность оборудования.

4. Стандартизировать интерфейсы операторов.

Ответ 2.

Объяснение. ГОСТ Р МЭК 61511-1-2018 фокусируется на обеспечении функциональной безопасности СПАЗ/SIS на всех этапах жизненного цикла – от анализа рисков до вывода из эксплуатации. Его цель – минимизация рисков аварий в промышленных процессах (Раздел 1, Область применения).

Вопрос 2. Какие методы анализа рисков рекомендует стандарт?

1. HAZOP (Анализ опасностей и рабочих характеристик).

2. LOPA (Анализ слоев защиты).

3. SWOT-анализ.

4. FMEA (Анализ видов и последствий отказов).

Ответ:1, 2, 4.

Объяснение.

- HAZOP используется для идентификации потенциальных опасностей.

- LOPA определяет необходимые уровни защиты (SIL) для снижения риска до приемлемого.

- FMEA оценивает влияние отказов компонентов на систему.

(Раздел 8, Анализ рисков).

SWOT-анализ не относится к технической безопасности

Вопрос 3. Что такое SIL (Уровень полноты безопасности)?

1. Показатель надежности механических компонентов.

2. Количественная мера снижения риска, обеспечиваемая функцией безопасности.

3. Метод оценки стоимости системы.

4. Требование к скорости реакции оператора.

Ответ 2.

Объяснение. SIL определяет, насколько функция безопасности должна снижать риск (например, SIL 2 соответствует снижению риска в 100–1000 раз). Значение SIL устанавливается через LOPA (Раздел 9, Определение требований к безопасности).

Вопрос 4. Какие требования предъявляются к архитектуре СПАЗ/SIS?

1. Резервирование каналов для достижения высоких уровней SIL.

2. Использование только одного датчика для упрощения системы.

3. Игнорирование диагностики оборудования.

4. Зависимость от человеческого фактора.

Ответ 1.

Объяснение. Для SIL 3 и выше требуется резервирование (например, архитектура 1oo2 или 2oo3) и диагностика для выявления отказов (Раздел 11, Проектирование аппаратных средств).

Вопрос 5. Какие этапы включает жизненный цикл СПАЗ/SIS по стандарту?

1. Анализ рисков, проектирование, эксплуатация, вывод из эксплуатации.

2. Только монтаж и настройка.

3. Маркетинг и продажи.

4. Разработка ПО без тестирования.

Ответ 1.

Объяснение. Жизненный цикл охватывает.

- Планирование и анализ рисков.

- Проектирование и верификацию.

- Эксплуатацию, техническое обслуживание.

- Вывод из эксплуатации (Раздел 5, Общие требования).

Вопрос 6. Что такое верификация в контексте СПАЗ/SIS?

1. Проверка соответствия системы требованиям спецификации.

2. Оценка экономической эффективности.

3. Тестирование только аппаратных компонентов.

4. Разрешение на приобретение отказобезопасных компонентов СПАЗ.

Ответ 1.

Объяснение. Верификация подтверждает, что СПАЗ/SIS спроектирована в соответствии с требованиями безопасности (например, проверка расчетов PFDavg). Включает анализ документации и тестирование (Раздел 12, Верификация).

Вопрос 7. Какие требования к программному обеспечению СПАЗ/SIS?

1. Соответствие стандартам кодирования (например, MISRA).
2. Регулярное обновление без Тестирования.
3. Использование несертифицированных библиотек.
4. Отказ от резервирования логики.

Ответ 1.

Объяснение. Программное обеспечение должно разрабатываться по стандартам, минимизирующим систематические ошибки (например, MISRA для C). Требуется тестирование и верификация (Раздел 12, Программное обеспечение).

Вопрос 8. Что такое функция безопасности?

1. Любая функция системы управления.
2. Функция, предназначенная для снижения риска до приемлемого уровня.
3. Функция повышения производительности.
4. Автоматизация отчетности.

Ответ 2.

Объяснение. Функция безопасности (например, аварийное отключение) активируется при превышении заданных параметров риска. Её SIL определяется через LOPA (Раздел 3, Термины и определения).

Вопрос 9. Какие действия требуются при модификации СПАЗ/SIS?

1. Пересмотр анализа рисков и документации.
2. Игнорирование изменений, если система работает.
3. Обновление только аппаратной части.
4. Снижение уровня SIL без обоснования.

Ответ 1.

Объяснение. Любые изменения должны сопровождаться пересмотром анализа рисков, верификацией и обновлением документации (Раздел 16, Управление изменениями).

Вопрос 10. Какие документы необходимы для соответствия стандарту?

1. Отчет HAZOP/LOPA.
2. Спецификация требований безопасности (SRS).
3. Инструкция по эксплуатации для операторов.
4. Маркетинговый план.

Ответ: 1, 2, 3.

Объяснение.

- HAZOP/LOPA – основа для определения SIL.
- SRS – документирует требования к функциям безопасности.
- Инструкции обеспечивают корректную эксплуатацию (Раздел 5, Документация).

В большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. Но при необходимости процесс может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск. Системы защиты могут быть основаны на применении различных технологий. химических, механических. гидравлических, пневматических, электрических, электронных, программируемых электронных.

Для облегчения применения такого подхода настоящий стандарт.

- устанавливает требование выполнения анализа опасностей и рисков для определения общих требований к безопасности;
- устанавливает требования к безопасности в (по)приборной(ым) системе(ам) безопасности;
- реализует подход, который применим ко всем приборным мерам обеспечения функциональной безопасности;
- подробно рассматривает применение определенных действий по управлению безопасностью, которые могут быть применены ко всем методам обеспечения функциональной безопасности.

Ключевыми аспектами ГОСТ Р МЭК 61511-1-2018 являются.

- Анализ рисков. HAZOP, LOPA, FMEA.
- Уровни SIL. определение через LOPA, требования к архитектуре.
- Жизненный цикл СПАЗ/SIS. проектирование, верификация, эксплуатация.
- Документация. SRS, отчеты, инструкции.
- Управление изменениями. пересмотр рисков и документации.

В развитие стандартов ГОСТ Р МЭК 61511 новый стандарт ГОСТ Р 59504-2021/IEC TR 61511-4: 2020 [11] описывает обоснование основных разделов МЭК 61511-1, уточняет некоторые распространенные ошибочные представления об их применении и дает краткое объяснение типовых подходов для применения каждого основного раздела в секторе промышленных процессов. Этот стандарт профессионально и кратко представляет, как выполнить требования основных разделов ГОСТ Р МЭК 61511

Тест 1.12. ГОСТ Р МЭК 61511-2-2018 [9]. Проектирование СПАЗ (СПАЗ/SIS)

Вопрос 1. Что включает раздел А5 «Управление функциональной безопасностью»?

1. Разработку политики безопасности и распределение ответственности.

2. Требования к цвету интерфейса оператора.

3. Процедуры для анализа рисков и управления изменениями.

4. Маркетинговую стратегию системы.

Ответ: 1, 3.

Объяснение. Раздел А5 регламентирует создание политики безопасности, распределение ролей (например, ответственный за функциональную безопасность), а также процедуры для анализа рисков, аудитов и управления изменениями. Маркетинг и дизайн интерфейса не относятся к функциональной безопасности.

Вопрос 2. Какие этапы жизненного цикла системы безопасности рассматриваются в разделе А6?

1. Проектирование, эксплуатация, снятие с эксплуатации.

2. Только монтаж оборудования.

3. Анализ рисков, верификация, техническое обслуживание.

4. Продажа системы клиентам.

Ответ: 1, 3.

Объяснение. Жизненный цикл СПАЗ включает все этапы: анализ рисков (А8), проектирование (А11), эксплуатацию (А16), вывод из эксплуатации (А18). Продажи не являются частью технического жизненного цикла.

Вопрос 3. Что такое верификация (А7 стандарта) в контексте СПАЗ?

1. Проверка соответствия системы требованиям спецификации.

2. Оценка стоимости разработки.

3. Тестирование ПО в реальных условиях.

4. Анализ рыночной конкуренции.

Ответ: 1.

Объяснение. Верификация подтверждает, что система соответствует техническим требованиям и стандартам (например, проверка расчетов SIL, тестирование логики). Тестирование в реальных условиях относится к валидации.

Вопрос 4. Какие методы используются в разделе А8 «Анализ опасностей и рисков процесса»?

1. HAZOP и LOPA.

2. FMEA и FTA.

3. SWOT-анализ.

4. Маркетинговые исследования.

Ответ: 1, 2.

Объяснение. HAZOP (анализ опасностей), LOPA (оценка уровня защиты), FMEA (анализ видов отказов) и FTA (дерево отказов) – ключевые методы анализа рисков. SWOT и маркетинг не связаны с безопасностью.

Вопрос 5. Для чего выполняется распределение функций безопасности по слоям защиты (A9)?

1. Чтобы определить, какие слои защиты должны достигать целевого уровня SIL.
2. Для снижения затрат на разработку.
3. Чтобы исключить использование резервирования.
4. Для упрощения интерфейса оператора.

Ответ 1.

Объяснение. Распределение функций по слоям (например, механические клапаны, электронные датчики) позволяет определить, какой уровень полноты безопасности (SIL) требуется каждому слою для снижения риска до приемлемого.

Вопрос 6. Что должно быть включено в спецификацию требований к безопасности (A10)?

1. Требуемый SIL, условия срабатывания функции безопасности.
2. Стоимость компонентов.
3. Правильное оформление человеко-машинной панели управления.
4. Инструкции для маркетинговой команды.

Ответ 1.

Объяснение. Спецификация требований к безопасности (SRS) включает целевой SIL, условия активации функции безопасности, время реакции системы, требования к диагностике. Дизайн и маркетинг не регламентируются.

Вопрос 7. Какие требования предъявляются к проектированию аппаратных средств СПАЗ (A11)?

1. Резервирование каналов для высоких уровней SIL.
2. Использование только одного датчика.
3. Игнорирование температурных условий эксплуатации.
4. Отказ от диагностики.

Ответ 1.

Объяснение. Для SIL 2-3 требуется резервирование (например, архитектура 1oo2) и диагностика для выявления отказов. Условия эксплуатации (температура, влажность) также учитываются.

Вопрос 8. Что включает разработка прикладной программы СПАЗ (A12)?

1. Тестирование ПО на соответствие требованиям SIL.
2. Использование несертифицированных библиотек.
3. Программирование без документации.
4. Игнорирование модульного тестирования.

Ответ 1.

Объяснение. Программное обеспечение должно разрабатываться по стандартам (например, MISRA C), проходить модульное и интеграционное тестирование. Несертифицированные компоненты запрещены.

Вопрос 9. Какие действия выполняются на этапе ЗПИ заводских приемочных испытаний (А13)?

1. Проверка работоспособности системы в контролируемых условиях.

2. Установка системы на объекте.

3. Обучение операторов.

4. Анализ рыночного спроса.

Ответ 1.

Объяснение. ЗПИ включают Тестирование системы в условиях, имитирующих реальные, для проверки соответствия спецификациям. Установка на объекте относится к разделу А14.

Вопрос 10. Что требуется при модификации СПАЗ (А17)?

1. Пересмотр документации и анализ рисков.

2. Игнорирование изменений, если система работает.

3. Обновление только аппаратной части.

4. Снижение уровня SIL без обоснования.

Ответ 1.

Объяснение. Любые изменения (аппаратные, программные) требуют пересмотра анализа рисков, верификации и обновления документации для сохранения соответствия SIL.

Ключевые требования в ГОСТ Р МЭК 61511-2-2018 формируются в виде разделов

А5. Управление функциональной безопасностью. А6. Требования к жизненному циклу системы безопасности.

А7. Верификация.

А.8 Анализ опасностей и рисков процесса.

А.9 Распределение функций безопасности по слоям защиты.

А.10 Спецификация требований к безопасности СПАЗ/SIS.

А.11 Проектирование и разработка СПАЗ/SIS.

А.12 Разработка прикладной программы СПАЗ/SIS.

А.13 Заводские приемочные испытания (ЗПИ).

А.14 Установка и ввод в действие СПАЗ/SIS.

А.15 Подтверждение соответствия безопасности СПАЗ/SIS.

А.16 Эксплуатация и обслуживание СПАЗ/SIS.

А.17 Модификация СПАЗ/SIS.

А.18 Снятие с эксплуатации СПАЗ/SIS

А.19 Требования к информации и документации.

1.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 1.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 1».

Тест 1.13. Руководящие документы для проектирования СПАЗ.

Вопрос 1. В каком порядке следует применять закон от 21.07.1997 № 116-ФЗ и Приказ Ростехнадзора от 15.12.2020 N 533?

- А) Сначала Приказ Ростехнадзора, затем закон.
- В) Сначала закон, затем Приказ Ростехнадзора.
- С) Одновременно.
- Д) Закон не имеет значения.

Вопрос 2. Какое значение имеет закон № 116-ФЗ для проектирования систем безопасности?

- А) Он не имеет значения.
- В) Устанавливает общие принципы и требования.
- С) Является лишь рекомендацией.
- Д) Определяет только штрафные санкции.

Вопрос 3. Какую роль играет Приказ № 533 в контексте закона № 116-ФЗ?

- А) Является более важным, чем закон.
- В) Является дополнением и конкретизацией требований закона.
- С) Не имеет отношения к закону.
- Д) Противоречит закону.

Вопрос 4. Почему важно соблюдать последовательность применения закона и приказа?

- А) Это не имеет значения.
- В) Чтобы избежать конфликтов в интерпретации норм.
- С) Чтобы сократить время проектирования.
- Д) Чтобы сэкономить средства.

Тест 1.14. Стандарты МЭК 61508 и 61511.

Вопрос 1. Какие основные цели преследуют стандарты МЭК 61508 и 61511?

Варианты ответов.

- А) Обеспечение функциональной безопасности систем защиты (СПАЗ/SIS) на всех этапах жизненного цикла.
- В) Упрощение процедур сертификации оборудования.
- С) Системный подход к управлению рисками и предотвращению системных ошибок.
- Д) Снижение стоимости разработки СПАЗ/SIS за счет унификации компонентов.

Вопрос 2. Чем отличается МЭК 61511 от МЭК 61508?

Варианты ответов.

- А) МЭК 61511 заменяет МЭК 61508 для процессных отраслей.
- В) МЭК 61508 – общий стандарт, а МЭК 61511 – его специализация для СПАЗ/SIS в процессах.
- С) МЭК 61511 исключает требования к аппаратному обеспечению.
- Д) МЭК 61511 добавляет требования к эксплуатации и обслуживанию СПАЗ/SIS.

Вопрос 3. Как принцип системности реализуется в стандартах?

Варианты ответов.

- А) Учет взаимосвязей между объектами ОПО и их проблемами.
- В) Упрощение документации за счет шаблонов.
- С) Унификация требований к СПАЗ/SIS для исключения дублирования в нормативных документах.

Д) Фокус только на этапе проектирования СПАЗ/SIS.

Вопрос 4. Какие уровни системообразования выделяются в стандартах?

Варианты ответов.

- А) Расчет показателей надежности (SIL).
- В) Физическая защита оборудования от внешних воздействий.
- С) Диагностика и тестирование в процессе верификации.
- Д) Аудит функциональной безопасности.

Вопрос 5. Какие требования к жизненному циклу СПАЗ/SIS устанавливают стандарты?

Варианты ответов.

- А) Проектирование, эксплуатация, вывод из эксплуатации.
- В) Верификация и валидация на каждом этапе.
- С) Обязательное использование конкретных производителей оборудования.
- Д) Учет только технических факторов (исключая человеческий фактор).

Вопрос 6. Почему диагностика и тестирование критичны для СПАЗ/SIS?

Варианты Ответов.

- А) Позволяют обнаружить скрытые отказы.
- В) Снижают затраты на разработку.
- С) Обеспечивают соответствие требованиям SIL.
- Д) Заменяют аудит функциональной безопасности.

Вопрос 7. Что проверяет аудит функциональной безопасности?

Варианты ответов.

- А) Соответствие процессов требованиям МЭК 61508/61511.
- В) Экономическую эффективность СПАЗ/SIS.
- С) Наличие отклонений в документации и практике внедрения.
- Д) Компетенцию персонала, участвующего в жизненном цикле СПАЗ/SIS.

Вопрос 8. Какое преимущество дает системный подход стандартов?

Варианты ответов.

- А) Снижение дублирования требований в нормативных документах.
- В) Ускорение разработки СПАЗ/SIS без этапа валидации.
- С) Согласование взаимосвязанных требований к СПАЗ/SIS.
- Д) Повышение гибкости в выборе методов расчета надежности.

Тест 1.15. ГОСТ Р МЭК 61508-6-2012 [6]. Проектирование СПАЗ/SIS.

Вопрос 1. Какие методы вероятностных расчетов используются в ГОСТ Р МЭК 61508-6-2012?

1. Модель Маркова.
2. Анализ дерева отказов (FTA).
3. Экспертные оценки без математической основы.
4. Метод Монте-Карло.

Вопрос 2. Какие параметры безопасности используются для режимов с низкой и высокой частотой запросов?

1. PFDavg (Average Probability of Failure on Demand) – для низкой частоты.
2. PFH (Probability of Failure per Hour) – для высокой частоты.
3. MTBF (Mean Time Between Failures) – для всех режимов.
4. SIL – только для механических систем.

Вопрос 3. Что такое «подтверждение соответствия безопасности»?

1. Проверка, что система соответствует требованиям SIL через тестирование и расчеты.
2. Документальное оформление без проверки.
3. Устранение только случайных отказов.
4. Оценка стоимости системы.

Вопрос 4. Какие требования предъявляются к модели расчета безотказности?

1. Учет как случайных, так и систематических отказов.
2. Использование только качественных методов.
3. Игнорирование человеческого фактора.
4. Применение исключительно экспертных оценок.

Вопрос 5. Какие факторы влияют на выбор архитектуры резервирования?

1. Требуемый уровень SIL.
2. Экономическая целесообразность.
3. Сложность обслуживания.
4. Цвет интерфейса оператора.

Вопрос 6. Для чего используется анализ дерева отказов (FTA)?

1. Для определения корневых причин аварий.
2. Для расчета вероятности отказа системы.
3. Для оценки эргономики интерфейса.
4. Для маркетингового анализа.

Тест 1.16. ГОСТ Р МЭК 61511-3-2018 [10]. Проектирование СПАЗ (СПАЗ/SIS).

Вопрос 1. Какие методы анализа рисков описаны в Приложении В и D?

1. Качественный граф риска (Приложение E).

2. Полуколичественный анализ дерева событий (Приложение В).

3. Калиброванный граф риска (Приложение D).

4. Матрица слоев безопасности (Приложение C).

Вопрос 2. Для чего используется матрица слоев безопасности (Приложение C)?

1. Для визуализации связи между рисками и слоями защиты.

2. Для расчета стоимости системы.

3. Для определения цветовой схемы интерфейса.

4. Для оценки уровня SIL без учета рисков.

Вопрос 3. Что такое «калиброванный граф риска» (Приложение D)?

1. Метод, сочетающий качественные и количественные данные для оценки SIL.

2. Инструмент для тестирования ПО.

3. Способ визуализации маркетинговых данных.

4. Метод расчета механической прочности.

Вопрос 4. Какие методы относятся к качественным (Приложение E и H)?

1. Граф риска (Приложение E).

2. Анализ дерева отказов (FTA).

3. Качественный подход для назначения SIL (Приложение H).

4. Метод Монте-Карло.

Вопрос 5. Что такое «анализ слоев защиты» (Приложение F и G)?

1. Оценка эффективности каждого слоя защиты в снижении риска.

2. Расчет стоимости резервных компонентов.

3. Тестирование пользовательского интерфейса.

4. Анализ рыночной конкуренции.

Вопрос 6. Для чего предназначено Приложение I?

1. Создание и калибровка графа риска.

2. Разработка ПО для СПАЗ.

3. Расчет механических нагрузок.

4. Оценка экономической эффективности.

Вопрос 7. Какой метод позволяет назначить SIL (SIL) без точных расчетов?

1. Качественный граф риска (Приложение E).

2. Матрица слоев безопасности (Приложение C).

3. Калиброванный граф риска (Приложение D).

4. Анализ дерева событий (Приложение В).

Вопрос 8. Какие параметры учитываются в калиброванном графе риска (Приложение D)?

1. Тяжесть последствий, вероятность события, возможность предотвращения аварии.

2. Стоимость компонентов, цвет интерфейса, размер системы.
3. Скорость реакции оператора, температура среды, влажность.
4. Количество сотрудников, маркетинговый бюджет.

Вопрос 9. Какой метод сочетает качественные и количественные данные?

1. Калиброванный граф риска (Приложение D).
2. Качественный граф риска (Приложение E).
3. Матрица слоев безопасности (Приложение C).
4. SWOT-анализ.

2. HAZOP/ HAZID АНАЛИЗ.

Задание 2.1. Уяснить ключевые принципы HAZOP/ HAZID анализа опасностей на различных этапах проектирования систем приборной безопасности.

2.1. КЛЮЧЕВЫЕ ПРИНЦИПЫ АНАЛИЗА ОПАСНОСТЕЙ.

HAZID и HAZOP – это не просто инженерные инструменты, а *способы мышления*, раскрывающие границы между порядком и хаосом.

HAZID и HAZOP это два взгляда на реальность опасности.

HAZID – это взгляд с высоты, попытка охватить все возможные угрозы объекта повышенной опасности.

HAZOP – это анализ того, почему наша защита может не сработать. Это взгляд эксперта скептика, сомневающегося в надежности системы безопасности СПАЗ/SIS.

Другими словами. HAZID – это «Онтология опасности» это первичное осознание угроз, которые могут возникнуть на ОПО, попытка описать все возможные ситуации, в которых объект повышенной опасности может перейти в опасное состояние для окружающего мира. Основой такого осознания опасностей являются управляющие слова.

Управляющие слова – это не просто инструменты, а способы мышления. Они заставляют нас выйти за рамки привычного и увидеть систему такой, какой она может быть, а не только такой, какой мы её ожидаем увидеть.

Философской основой HAZID является ответ на вопросы.

- «**Что, если...?**», Вопрос, который лежит в основе философского познания опасных ситуаций на ОПО.

- «**Где?**», «**Когда?**», «**Почему?**» заставляют задуматься о пространственно-временной природе опасности.

Пример.

«*Что, если давление в реакторе превысит допустимое?*» → Это не просто инженерный вопрос, а философское исследование устойчивости бытия системы, метафизическое допущение о пределах устойчивости системы (ОПО).

Если HAZID – это «карта рисков, опасностей на ОПО», то HAZOP [18] – «критика чистого разума» инженерных решений по СПАЗ HAZOP, в свою очередь, это «Гносеология отказов СПАЗ», глубокий анализ причинно-следственных связей опасностей ОПО с отказами СПАЗ. Каждое управляющее слово в таком исследовании – это реконструкция нормального состояния СПАЗ.

- «**Нет**» (отсутствие сигнала) → Что, если реальность искажена? «*А существует ли сигнал на самом деле?*»

- «**Больше**»/«**Меньше**» → Вопрос о пределах. «*Где граница между нормой и катастрофой?*»

- **«Иначе»** → Допущение альтернативной реальности, где система ведёт себя не так, как ожидалось.

И очень важно понимать два лика HAZOP – Проектный и Верификационный.

Представьте, что вы строите дом.

Проектный HAZOP (на этапе создания спецификации) – это как совещание с архитектором и инженерами, когда у вас только чертежи.

Вопросы. «А что, если мы поставим котельную здесь? Достаточно ли будет вентиляции? Что, если труба прорвется? А если электричество отключится, насос остановится?» Нужна защита? КАК? ЧЕМ?

Цель. внести в спецификацию необходимые требования к программно-аппаратным средствам СПАЗ до начала закупки материалов и строительства. Это проактивное действие.

Верификационный HAZOP (на этапе завершения проекта) – это как осмотр готового дома перед сдачей, но с инженерной проверкой.

Вопросы. «Мы спроектировали котельную по всем правилам. Но что, если строители не смогли найти трубу нужного диаметра и поставили чуть уже? Что, если монтажники установили предохранительный клапан не туда? Что, если выяснилось, что ремонт насоса будет занимать не день, а неделю из-за логистики?»

Цель. Убедиться, что готовый объект (или его документация) соответствует тем требованиям безопасности, которые были заложены в проекте. И если нет – выявить новые риски, возникшие на этапе реализации, и принять компенсирующие меры. Это и верификация, и реактивное действие по отношению к ошибкам монтажа/поставок.

Как увязать это в единую систему?

Правильнее говорить о разных целях и временных точках проведения одного и того же метода HAZOP в жизненном цикле проекта.

Вот жизненный цикл и точки применения HAZOP.

Стадия проектирования (Создание спецификации).

HAZOP1 (Базовый/Проектный). Проводится на финальной версии P&ID до закупки оборудования. Его цель – убедиться, что проектные решения в целом обеспечивают безопасность. Результат. Список действий необходимых для обеспечения безопасности ОПО (например, «добавить датчик температуры», «указать в спецификации требуемый DC=99%»). В целом на этом этапе определяются основные требования к программно-аппаратным средствам ОПО,

Стадия закупки и монтажа.

Происходит закупка, монтаж, программирование СПАЗ.

Стадия верификации (Завершение проекта).

HAZOP2 (Верификационный/Детальный). Проводится после того, как определено точное поставляемое оборудование, его характеристики (например, реальный DC=90% вместо 99%), готовы программы ПЛК и известны реальные сроки поставки запчастей.

Его посыл – именно «**What If?**» (А что, если?).

«Что если реальная глубина диагностики (DC) составила не 99%, а 90%? Как это повлияет на PFD? Нужно ли нам пересматривать SIL?»

«Что если MTTR для этого клапана составляет не 8 часов, а 2 недели? Достаточно ли у нас резервных элементов? Нужно ли вводить новую процедуру?»

Результат HAZOP на этапе верификации.

- Обоснование пересчета и принятия риска (если он остался в допустимых границах).
- Оценка возможной корректировки процедур эксплуатации и технического обслуживания СПАЗ.
- Разработка плана закупки дополнительных запчастей.
- Четкое понимание остаточных рисков для передачи эксплуатационному персоналу.

Таким образом первый HAZOP (после HAZID) – это про то «Что мы проектируем?». Он задает спецификацию требований к СПАЗ.

Второй HAZOP (на этапе верификации) – это про то «Что мы в итоге построили и можем ли мы этим безопасно управлять?». Он проверяет соответствие и выявляет новые операционные риски.

Оба этапа критически важны. Пропуск второго HAZOP – это слепая вера в то, что проект реализован идеально, что в реальности тяжелые последствия никогда не случатся.

Анализ опасностей для СПАЗ/SIS – это «игра в зеркала», где система должна защищать не только объект, но и саму себя от внутренних опасностей. Документация, климат и человеческий фактор становятся «мета-угрозами», которые нельзя обнаружить прямыми методами вроде расчета SIL.

Здесь важно понимать, что СПАЗ/SIS – это живой организм, где неполадки в «информационных клетках» (документация) или «нервной системе» (персонал) могут убить его быстрее, чем внешние угрозы.

Сравнительная философия HAZID и HAZOP

Аспект	HAZID (Опасности объекта)	HAZOP (Отказы СПАЗ/SIS)
Подход	Макроуровень (общие угрозы)	Микроуровень (конкретные отказы аппаратно-программных и организационных средств СПАЗ)
Философия	Онтология (что может быть?)	Гносеология (почему ошибается СПАЗ?)

Аспект	HAZID (Опасности объекта)	HAZOP (Отказы СПАЗ/SIS)
Управляющие слова	«Что, если?», «Где?», «Когда?»	«Нет», «Больше», «Иначе»
Метафора	Карта неизведанных земель	Исследование слепых пятен на этих землях

2.1. ПРАКТИКУМ ПО АНАЛИЗУ HAZOP И HAZID.

Задание 2.2. С поддержкой AI (типа GPT) подготовить свои решения кейсов и объяснения для одного или 2-х кейсов. Сделать вывод о правильности и качестве предложенных ответов и объяснений в кейсах.

Кейс 2.1. Выбор последовательности методов анализа рисков для модернизации химического реактора.

Ситуация.

На химическом предприятии планируется модернизация реактора с высокоэкзотермической реакцией. Процесс включает использование токсичного сырья и повышенных давлений. Техническое задание на модернизацию готово, но детальное проектирование АСУТП и СПАЗ/SIS еще не началось. Команде проекта необходимо обеспечить безопасность установки и соответствие требованиям ГОСТ Р МЭК 61511 / МЭК 61511.

Вопрос. Какую последовательность методов анализа рисков следует применить для комплексного выявления и оценки опасностей?

Варианты решений.

А) Сразу провести HAZOP-анализ.

В) Сначала провести HAZID-анализ, а затем, на основе его результатов, запланировать более детальные методы (HAZOP, LOPA).

С) Провести анализ дерева неисправностей (FTA) для существующей системы.

Д) Сразу перейти к уровневому анализу защит (LOPA) для определения требований к СПАЗ/SIS.

Ответ В. Сначала провести HAZID-анализ, а затем, на основе его результатов, запланировать более детальные методы (HAZOP, LOPA).

Развернутое объяснение с примерами отчетов.

Правильный выбор метода и его *последовательности* критически важен для эффективного управления рисками. Эти методы не взаимозаменяемы, а дополняют друг друга, формируя «воронку» анализа.

1. Почему HAZID – правильный первый шаг?

HAZID (Hazard Identification) – это методика **высокоуровневого скрининга**. Ее цель – быстро, на ранней стадии проекта, составить общую карту всех потенциальных опасностей, не углубляясь в детальные причины и последствия.

Когда применяется? На стадии концептуального проектирования или FEED (Front End Engineering Design).

Результат. Список всех основных опасных сценариев для дальнейших принятий проектных решений.

Практический пример отчета HAZID.

ID	Опасность	Возможное следствие	Область воздействия	Рекомендуемые дальнейшие действия
HZ-1	Разрыв реактора из-за превышения давления	Выброс токсичной реакционной массы, пожар, взрыв	Цех, персонал, окружающая среда	Детально проанализировать HAZOP. Рассмотреть сценарий на LOPA для определения SIL.
HZ-2	Ошибка оператора при загрузке сырья (не компонент)	Неконтролируемая экзотермическая реакция, рост давления	Реактор, цех	Включить в HAZOP (направляющее слово «НЕ ТОТ»). Рассмотреть процедурные средства защиты.
HZ-3	Отказ системы охлаждения реактора	Перегрев, рост давления, разгерметизация	Реактор	Включить в HAZOP (направляющее слово «НЕТ»). Провести LOPA для функции аварийного охлаждения.
HZ-4	Утечка токсичного сырья из трубопровода	Отравление персонала, загрязнение среды	Помещение склада сырья	Рассмотреть системы обнаружения утечек и вентиляции. <i>Возможно, не требует HAZOP, достаточно проверки проектных решений.</i>

Вывод по HAZID. Этот анализ помогает понять, *какие* из опасностей наиболее значимы для нашего проекта СПАЗ. Он отвечает на вопрос. «На чем нам сфокусировать наши усилия и ресурсы?»»

2. Почему НЕЛЬЗЯ начинать сразу с HAZOP?

HAZOP (Hazard and Operability Study) – это **детальный, систематический и трудоемкий** анализ проектных решений СПАЗ. Его проводят, когда есть готовый набор проектной документации (P&ID, функциональные схемы АСУ ТП).

Когда применяется. На стадии детального проектирования СПАЗ тогда, когда схемы КИПиА СПАЗ почти готовы.

Проблема начала проекта с HAZOP. Если начать HAZOP без HAZID, можно потратить огромное количество времени (а значит, денег) на анализ узлов и сценариев, которые не являются критичными. HAZID же помогает составить **фокус-лист** для HAZOP, сделав его эффективным.

Практический пример отчета HAZOP (для сценария, выявленного в HAZID).

Узел. Реактор R-101. Назначение. Проведение экзотермической реакции при давлении 5 бар и температуре 120°C.

Параметр. Расход. Направляющее слово. НЕТ (NO). Отклонение. Нет расхода хладагента в рубашке.

Причина	Следствие	Существующие средства защиты	Рекомендации
Отказ насоса охлаждения	Рост температуры и давления, разрыв реактора	Необходима аварийная сигнализация по высокой температуре (операторское действие)	Проанализировать на LOPA. Требуется ли автоматическая СПАЗ/SIS для остановки реакции и аварийного сброса давления? Определить целевой SIL.
Засорение линии охлаждения	Рост температуры и давления, разрыв реактора	Необходим контроль расхода охлаждающей жидкости	Проанализировать ФТА засорения линии охлаждения. Требуется предохранительный клапан на реакторе?
Ошибка оператора (закрыл задвижку)	Рост температуры и давления, разрыв реактора	Необходимо исключить ручные операции	Необходимо предусмотреть контур автоматической SIF аварийного управления задвижкой

Вывод по HAZOP. HAZOP отвечает на вопросы. «Почему это может произойти?» и «Какие защитные слои уже есть?». Он гене-

рирует сценарии для количественной оценки возможных несоответствий СПАЗ. Правильный подход – это последовательный, итеративный процесс, где каждый метод решает свою задачу:

HAZID → Широкий охват: Первичное выявление опасностей.

HAZOP → Глубина и причины: Систематический анализ отклонений и их последствий. Создает основу для всех последующих количественных оценок.

LOPA → Количественная оценка и SIL: Определение целевых показателей надёжности для функций безопасности.

FMEA/FMEDA → Компонентная надёжность: Количественное подтверждение, что аппаратная часть системы соответствует целевому SIL.

FTA → Детальный анализ конкретных отказов: Углублённый расчет для критических функций СПАЗ/SIS.

Таким образом, HAZOP отражает системный и экономически эффективный подход, выступая стратегической картой, которая направляет и обеспечивает входными данными все последующие, более затратные и детальные исследования. Последовательность (HAZID → HAZOP → LOPA) является методически верным фундаментом, на который уже надстраиваются FMEA и FMEDA для верификации аппаратной части.

Кейс 2.2. Анализ сценария утечки на нефтепроводе.

Ситуация. На магистральном нефтепроводе возможна утечка из-за коррозии. Требуется определить, какие элементы СПАЗ/SIS (датчики, клапаны) могут отказать при переводе нефтепровода в безопасное состояние.

Вопрос. Какой метод выявит конкретные отказы системы защиты?

- A) HAZID.
- B) IDEF 0.
- C) HAZOP.
- D) What-If.

Ответ C. HAZOP.

Объяснение.

Вопрос: «Какой метод выявит конкретные отказы системы защиты?»

HAZOP (Анализ опасностей и работоспособности) – это блестящий метод для анализа технологического процесса. Он отвечает на вопросы: «Что будет, если контур защиты по давлению или по расходу не сработает?». Он выявляет опасные сценарии на уровне технологии.

Однако, для детального анализа отказов конкретных компонентов системы защиты (СПАЗ/SIS) существуют более специализированные методы.

Более корректными методами для этой задачи являются:

FMEA (AnalyСПАЗ/SIS of Failure Mode and Effect AnalyСПАЗ/SIS / Анализ видов и последствий отказов): Этот метод целенаправленно анализирует каждый компонент системы, перебирая все возможные виды его отказов (например, «датчик давления: заниженные показания», «клапан: заклинило в открытом положении») и оценивает последствия каждого отказа для системы в целом.

FTA (Fault Tree AnalyСПАЗ/SIS / Анализ деревьев неисправностей): Этот метод используется для анализа отказов всей системы в целом, выводя возможные комбинации отказов компонентов, которые могут привести к главному нежелательному событию (например, «несрабатывание системы защиты при утечке»).

Но следует исходить, что HAZOP-анализ является первоосновой. Действительно, в рамках HAZOP-анализа для выявленного опасного сценария (например, «утечка») рассматриваются существующие средства защиты и анализируются их возможные недостатки. То есть, можно задать направляющее слово к функции защиты: «Защита НЕ СРАБАТЫВАЕТ».

Пример в стиле HAZOP для функции СПАЗ/SIS:

Отклонение: ЗАЩИТА НЕТ.

Причина: Отказ датчика утечки; заклинивание отсечного клапана; ошибка в логике ПЛК.

Последствие: Утечка не останавливается, приводя к пожару и экологическому ущербу.

Меры: Требуется обеспечить отказобезопасность СПАЗ/SIS, предусмотреть резервирование и диагностику.

Объяснение. Хотя для детального анализа аппаратных отказов чаще применяются методы FMEA и FTA, HAZOP-анализ является ключевым методом на этапе доработки функциональных требований к системе защиты. В рамках HAZOP для опасного сценария, например, «утечка» анализируется эффективность средств защиты. Путем применения направляющих слов к функциям безопасности (например, «ЗАЩИТА НЕТ») выявляются и документируются конкретные причины отказа СПАЗ/SIS, такие как «неисправность датчика давления» или «заклинивание отсечного клапана». Это позволяет сформулировать требования к отказоустойчивости и архитектуре СПАЗ/SIS.

Варианты:

A (HAZID) – это идентификация опасностей на ранней стадии,

B (IDEF0) – метод функционального моделирования,

D (What-If) – более простой метод, менее структурированный, чем HAZOP.

Эти методы не используются для анализа отказов СПАЗ.

Кейс 2.3. Определение опасных зон на нефтехранилище.

Ситуация. На нефтебазе необходимо составить карту рисков с указанием зон возможных возгораний и утечек.

Вопрос. Какой метод подойдет для этой задачи?

- A) FTA.
- B) HAZID.
- C) LOPA.
- D) FMEA.

Ответ В. HAZID.

Объяснение.

HAZID фиксирует опасные узлы ОПО.

- Резервуары с легко воспламеняющейся жидкостью (ЛВЖ).
- Насосные станции.
- Места соединения трубопроводов.

Кейс 2.4. Анализ мета-рисков для СПАЗ/SIS (HAZOP).

Задача. Для системы аварийного останова реактора (SIL 2) выявить «мета-проблемы».

- Ошибки документации (неактуальные схемы подключения).
- Климатические воздействия (работа в условиях высокой влажности).
- Человеческий фактор (неправильная интерпретация диагностики).

Вопросы. Какие ключевые слова HAZOP применить для анализа СПАЗ/SIS? (*Пример. «Нет сигнала», «Ложное срабатывание»*).

1. Как влажность влияет на PFDavg, если датчики сертифицированы для 60% влажности, а реальная – 85%?
2. Предложить меры для минимизации рисков документации.

Решение.

- HAZOP. Анализ сценариев «датчик залип» (ложное безопасное состояние) и «потеря связи с ПЛК».
- Влажность. Коррозия контактов → рост λ_{DU} на 20%. Необходим дополнительный кожух.
- Документация. Внедрение цифрового двойника с автоматической проверкой актуальности схем.

2.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 2.3. Уяснить ответы и объяснения всех тестов. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 2.1. Анализ опасностей ОПО и СПАЗ/SIS (SIF) с использованием HAZID и HAZOP.

Вопрос 1. Какова основная цель HAZID при проектировании СПАЗ?

Варианты.

- A) Определить вероятности отказов датчиков и клапанов.

В) Выявить все потенциально опасные узлы ОПО (аппараты, трубопроводы, зоны).

С) Рассчитать SIL для каждого контура SIF.

Д) Проверить работоспособность логического контроллера.

Ответ В. Выявить все потенциально опасные узлы ОПО.

Пояснение.

HAZID – это первичный анализ, который идентифицирует опасные зоны объекта (например, места возможных утечек, взрывов, разрушений), но не углубляется в отказы конкретных элементов (датчиков, исполнительных устройств, ПО...) СПАЗ/SIS.

Вопрос 2. Какой метод используется для определения концептуальных требований к контурам аварийной защиты (SIF)?

Варианты.

А) HAZID.

В) HAZOP.

С) FTA .

Д) LOPA.

Ответ В. HAZOP.

Пояснение.

HAZOP анализирует причины и последствия отказов и на основе этого формирует требования к SIF, например. *«При превышении давления в реакторе более 10 бар должен сработать отсечной клапан с SIL 2»*).

Вопрос 3. В каком отчете по анализу опасностей появятся формулировки типа: «При отказе датчика давления возможен разрыв аппарата»?

Варианты.

А) Отчет HAZID.

В) Отчет HAZOP.

С) Отчет FMEA.

Д) Отчет Bow-Tie.

Ответ В. Отчет HAZOP.

Пояснение.

HAZOP фокусируется на причинно-следственных связях в СПАЗ/SIS (отказ датчика → разрыв аппарата), тогда как HAZID лишь отмечает, что *«аппарат (ОПО) может разрушиться, например, при избыточном давлении»*.

Вопрос 4. На нефтехимическом заводе проводится анализ опасностей.

В каком отчете появится запись. «Резервуар с аммиаком – потенциальный источник токсичного выброса»?

Варианты.

А) HAZOP.

В) HAZID.

С) LOPA.

D) FTA.

Ответ В. HAZID.

Пояснение.

Это идентификация опасного узла, а не анализ отказов системы защиты.

Вопрос 5. В каком отчете будет указано. «При заклинивании отсечного клапана в открытом положении возможен перелив ёмкости, требуется SIF с SIL 1»?

Варианты.

A) HAZID.

B) HAZOP.

C) Что-если анализ.

D) FMEA.

Ответ В. HAZOP.

Пояснение.

HAZOP определяет требования к SIF на основе сценариев отказов.

Вопрос 6. Сопоставьте этапы анализа с их результатами показанными в таблице.

Метод	Результат
1. HAZID	A) Требования к SIL для SIF
2. HAZOP	B) Список опасных зон объекта

Правильное сопоставление.

1) **В** (HAZID выявляет опасные узлы ОПО).

2) **А** (HAZOP формирует требования к SIF).

Выводы.

• **HAZID** → «Где опасность?» (Выявление опасных узлов. аппараты, трубопроводы, зоны возможных аварий).

• **HAZOP** → «Как защититься?» (Определение SIF. какие датчики, логика и исполнительные механизмы нужны для предотвращения аварии).

Философская аналогия.

• **HAZID** – это «карта рисков», показывающая, где «водятся тигры».

• **HAZOP** – это «инструкция для охотников на тигров», объясняющая, какое оружие (SIF) и с какой надежностью (SIL) нужно, чтобы их победить.

Тест 2.2. «Два крыла» анализа опасностей в проектировании СПАЗ/SIS.

Вопрос 1. Какие методы образуют «два крыла» анализа опасностей объекта?

Варианты.

- A) HAZOP и LOPA.
- B) HAZID и FTA.
- C) FMEA и Bow-Tie.
- D) What-If и Checklist.

Ответ В. HAZID и FTA.

Объяснение.

- **HAZID** – выявляет опасные узлы объекта (аппараты, зоны, процессы).
- **FTA (Fault Tree Analysis/СПАЗ/SIS)** – анализирует причины и комбинации отказов, ведущих к аварии.

Это «крылья» анализа. одно ищет угрозы, другое раскладывает их на составляющие.

Вопрос 2. Какие методы образуют «два крыла» для установления уровня полноты безопасности (SIL)?

Варианты.

- A) HAZID и FTA.
- B) HAZOP и LOPA.
- C) FMEA и What-If.
- D) Bow-Tie и Markov Chains.

Ответ В. HAZOP и LOPA.

Объяснение.

HAZOP – определяет требования к SIF (например, «нужен клапан с SIL 2»).

LOPA (Layer of Protection Analysis/СПАЗ/SIS) – количественно обосновывает SIL, учитывая вероятности отказов и последствия. Это «крылья» SIL. Одно ставит задачу, другое даёт расчётное решение.

Вопрос 3. Где будет использоваться FTA при проектировании СПАЗ/SIS?

Варианты.

- A) Для первичного выявления зон возможных утечек на объекте.
- B) Для анализа, какие комбинации отказов приведут к взрыву реактора.
- C) Для расчёта вероятности ложных срабатываний клапана.
- D) Для определения требований к SIL.

Ответ В. Для анализа комбинаций отказов.

Объяснение.

FTA раскладывает аварию на «ветви» отказов, например, «Отказ датчика + заклинивание клапана = разрыв аппарата»).

Вопрос 4. Какой метод применим для обоснования, что SIF должен иметь SIL 3, а не SIL 2?

Варианты.

- A) HAZID.
- B) FTA.
- C) LOPA.
- D) What-If.

Ответ С. LOPA.

Объяснение.

LOPA считает риски и показывает, что для снижения вероятности аварии до допустимого уровня нужен именно SIL 3.

Вопрос 5. Сопоставьте методы приведенные в таблице с их ролью в проектировании СПАЗ/SIS.

Метод	Роль
1. HAZID	А) Количественное Объяснение SIL
2. FTA	В) Выявление опасных зон объекта
3. HAZOP	С) Определение требований к SIF
4. LOPA	Д) Анализ комбинаций отказов

Ответ

- 1 – В.
- 2 – D.
- 3 – С.
- 4 – А.

Почему это «крылья»?

1. **HAZID + FTA = «Крылья анализа опасностей».**

- HAZID. «Где драконы?» (поиск угроз).
- FTA. «Как драконы рождаются?» (разбор причин).

2. **HAZOP + LOPA = «Крылья SIL».**

- HAZOP. «Каким мечом рубить дракона?» (концепция защиты).
- LOPA. «Какой крепости должен быть меч?» (расчёт надёжности).

Поэтому

- Без HAZID/FTA вы не узнаете, от чего защищаться.
- Без HAZOP/LOPA вы не поймёте, как защищаться *безопасно*.

Крылья мудрости в проектировании СПАЗ/SIS.

Анализ опасностей это не сухие методики, а живая система мышления инженера– как у философа, который сначала ищет опасности бытия (HAZID), затем вглядывается в их корни (FTA), после решает, как защититься (HAZOP), и наконец – вычисляет «крепость защиты» (LOPA).

Тест 2.3. Квалификация инженера СПАЗ.

Вопрос 1. Почему инженер, проектирующий СПАЗ/SIS, похож на философа?

Варианты.

А) Потому что оба любят сложные термины.

В) Потому что ищут ответ на вопросы «Что есть риск?» и «Как с ним жить?».

С) Потому что проводят всё время в размышлениях.

Д) Потому что носят очки.

Ответ В.

Объяснение.

Настоящий инженер СПАЗ – это **философ безопасности**, который:

1. **Сомневается** (HAZID. «А точно ли это безопасно?»).
2. **Анализирует** (FTA. «Что, если всё пойдёт наперекосяк?»).
3. **Придумывает защиту** (HAZOP. «Как перехитрить риск?»).
4. **Доказывает** (LOPA. «Почему мой щит достаточно крепок?»).

P.S. HAZOP – это широкий взгляд на систему, как художник, который видит все оттенки риска. FTA – точечный хирург, вскрывающий цепочку причин для конкретного отказа. HAZOP задает вопросы. «А что, если...?». FTA отвечает. «Это произошло, потому что...». Их сила в сочетании. HAZOP находит угрозы, FTA оценивает их критичность.

2.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 2.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 2»..

Тест 2.4.

Перед выполнением анализа опасностей HAZOP, участникам исследования потребуется вся следующая информация по безопасности, за исключением:

- а) Блок-схемы или P&ID.
- б) Подробных схем внутренней коммутации между модулями СПАЗ/SIS. (например, соединения внутри шкафа безопасности).
- в) Классификации взрывоопасных зон и требований к искробезопасным цепям.
- г) Норм проектирования (например, API, МЭК 60079).
- е) Безопасных пределов параметров процесса.

Тест 2.5. Применение HAZOP и FTA для анализа безопасности.

Вопрос 1. Что является основной целью HAZOP в контексте СПАЗ/SIS?

Варианты ответов.

- А) построить дерево отказов для расчета вероятности аварии.
- В) выявить отклонения в работе системы и их причины через ключевые слова (например, «нет сигнала», «ложное срабатывание»).
- С) определить минимальные пути восстановления СПАЗ/SIS после отказа.

D) оценить надежность компонентов СПАЗ/SIS на основе статистики отказов.

Вопрос 2. Какой метод позволяет рассчитать вероятность отказа СПАЗ/SIS из-за комбинации событий. «отказ датчика + ошибка логического контроллера»?

Варианты ответов.

A) HAZOP.

B) FTA.

C) Оба метода.

D) Ни один из методов.

Вопрос 3. Что из перечисленного характерно только для FTA?

Варианты ответов.

A) Использование ключевых слов «больше», «меньше», «не».

B) Применение логических вентилей (И, ИЛИ) для моделирования причинно-следственных связей.

C) Анализ последствий отклонений для объекта повышенной опасности.

D) Составление рекомендаций по модификации технологического процесса.

Вопрос 4. Какой метод лучше подходит для анализа, почему СПАЗ/SIS не выдала сигнал аварийного останова?

Варианты ответов.

A) HAZOP – чтобы найти все возможные отклонения в работе системы.

B) FTA – чтобы определить комбинацию событий, приведшую к отказу.

C) Оба метода одинаково эффективны.

D) Ни один – это задача FMEA.

Вопрос 5. Что является результатом HAZOP для СПАЗ/SIS?

A) Дерево отказов с вероятностями событий.

B) Таблица с выявленными отклонениями, их причинами и рекомендациями.

C) График зависимости надежности СПАЗ/SIS от времени.

D) Отчет о соответствии системы требованиям SIL.

Вопрос 6. Почему HAZOP не используют для расчета SIL?

Варианты ответов.

A) HAZOP не учитывает человеческий фактор.

B) HAZOP не предоставляет количественных данных о вероятностях отказов.

C) HAZOP фокусируется только на программных ошибках.

D) HAZOP не применяется к СПАЗ/SIS.

Вопрос 7. Какое утверждение верно для FTA?

Варианты ответов.

A) позволяет определить, какие компоненты СПАЗ/SIS критичны для безопасности.

В) требует проведения мозгового штурма с участием всех специалистов.

С) используется для оптимизации бизнес-процессов.

Д) не работает с событиями, имеющими низкую вероятность.

Вопрос 8. В чем главное философское отличие HAZOP от FTA?

Варианты ответов.

А) HAZOP ищет «что может пойти не так», FTA – «почему это произошло».

В) HAZOP – для проектировщиков, FTA – для аудиторов.

С) HAZOP – профилактика, FTA – ретроспектива.

Д) HAZOP – для аппаратуры, FTA – для ПО.

3. ДЕРЕВЬЯ ОТКАЗОВ/СОБЫТИЙ И АНАЛИЗ СЛОЕВ ЗАЩИТЫ.

Задание 3.1. Уяснить ключевые принципы анализа защиты опасного производственного объекта.

3.1. КЛЮЧЕВЫЕ ПРИНЦИПЫ АНАЛИЗА ЗАЩИТЫ ОПАСНОГО ПРОИЗВОДСТВЕННОГО ОБЪЕКТА.

Деревья отказов/событий (ФТА/ЕТА) и метод LOPA – это способы анализа опасности на ОПО.

Эти инструменты позволяют на начальном этапе проектирования в значительной мере уяснить пути решения задачи защиты ОПО.

Дерево отказов (ФТА) [20]– это инструмент, который используется для анализа возможных отказов и для оценки их вероятностей. Он помогает визуализировать пути, ведущие к опасному событию, и позволяет лучше понимать, какие элементы системы защиты наиболее критичны.

Построение дерева начинается с главного опасного события (аварии– корень дерева), затем добавляются узлы-причины. Используя вероятности или интенсивности базовых событий и логические операции (И, ИЛИ), можно рассчитать вероятность аварии.

При построении дерева отказов важно выделять отдельными кусты отказов ОПО и кусты отказов СПАЗ по собственным аппаратно-программным причинам.

Дерево событий (ЕТА) [19]– это инструмент для ответа на вопрос «ЧТО ЕСЛИ?». Это качественный и описательный анализ развития опасности. Для этого берется одно опасное событие (например, разрыв трубы) и рисуются все возможные сценарии его развития, как в жизни– «найди худшие последствия».

Цель этого метода установить полный перечень опасных сценариев, понять цепочки причинно-следственных связей, оценить возможный ущерб.

В результате построения дерева показывается весь спектр угроз, что позволяет на этапе проектирования понять пути защиты опасного производственного объекта, отвечая на вопросы.

- «Что произойдет, если этот клапан не закроется?».
- «Куда пойдет облако газа при разных направлениях ветра?».
- «Какие последовательности событий приведут к пожару, а какие – к взрыву?».

Другой инструмент LOPA – лежат в одном ящике с ЕТА. Они похожи друг на друга, но используются для решения принципиально разных задач. Путать их – все равно что использовать молоток вместо отвертки. вроде бы можно, но результат будет плохим.

LOPA (Анализ слоев защиты) – это инструмент для ответа на вопрос «**СКОЛЬКО нужно слоев защиты?**» (**ХВАТАЕТ ЛИ ИХ?**). Он берет уже готовый, конкретный сценарий из ЕТА, HAZOP или другого анализа и подсчитывает риск опасности.

Цель этого инструмента количественно оценить риск одного сценария и проверить, достаточно ли существующих слоев защиты (предупредительные таблички, оператор, АСУ ТП, САЗ, физические барьеры), чтобы снизить риск до допустимого уровня.

Анализ слоев защиты основан на концепции многоуровневой защиты. Каждый слой снижает риск, а вместе они обеспечивают комплексную безопасность. Пример.

- Слой 1. Полевая сигнализация (снижение риска в 10 раз).
- Слой 2. Оператор в SCADA (снижение в 10 раз).
- Слой 3. СПАЗ/SIS (снижение в 10 раз).

Итого. общее снижение риска в 1000 раз.

Вероятность того, что все слои откажут одновременно, равна произведению их вероятностей отказа. Поэтому даже слои с умеренной надежностью, будучи независимыми, создают высоконадежную систему.

Слои защиты функционируют в этом случае как оборонительные рубежи.

• 1-й слой. Полевая сигнализация → «Часовые на стене» (Пример. PFD=0.1).

• 2-й слой. Оператор SCADA → «Командный центр» (Пример. PFD=0.5).

• 3-й слой. СПАЗ/SIS → «Неприступная крепость» (Пример. PFD=0.01).

Математика безопасности.

Общая вероятность опасного события это вероятность без защиты PFD_{доп}, умноженная на $\prod(PFD \text{ отказов слоёв})$.

Пример. $(10^{-2}/\text{год} \times 0.5 \times 0.01) \times PFD_{\text{доп}} = 5 \times 10^{-5} \times PFD_{\text{доп}}$ в год.

Таблица 3.1. Применение FTA\ LOPA.

Метод	Роль	Философская аналогия
FTA	Диагностика причин	Аристотелевский анализ
LOPA	Проектирование щита защиты	Платоновская иерархия идей

Сводные сравнения применения методов анализа отказобезопасности приведены в таблице 3.2.

Таблица 3.2.

Крите-рий	Дерево событий (ЕТА)	Анализ слоев защиты (LORA)
Основ-ной во-прос	Что если? (Какие сце-нарии возможны?)	Сколько? (Какова частота? Хватает ли защиты?)
Суть	Генерация сцена-риев, качественный анализ	Оценка риска, полуколичественный анализ
Тип ана-лиза	Широкий, творческий, исследовательский	Узкий, стандартизированный, аудитор-ский
Ре-зультат	Полный перечень цепочек развития аварий	Расчетная частота нежелательного события и рекомендация по необходимости САЗ (СПАЗ/SIS)
Место в про-цессе	Этап 1. Идентификация опасностей	Этап 2. Оценка достаточности слоев защиты для конкретного сценария из Этапа 1
Стан-дарты	ГОСТ Р МЭК 31010 (как метод анализа рисков)	МЭК 61511-3 (как ключевой метод для обоснования требований к СПАЗ/SIS)

Как они работают вместе на практике?

Проводим HAZOP/FTA. Команда на мозговом штурме выявляет опасность. *«При остановке насоса возможен обратный поток и разрыв трубопровода».* Эта опасность возникает по ряду возможных событий. Дерево FTA устанавливает вероятность опасности.

1. Выбираем сценарий слоев защиты для углубленного анализа. Мы понимаем, что этот сценарий очень опасен. Это ЕТА. Теперь нам нужно не просто его описать, а посчитать его риск.

2. Запускаем LORA. Берем этот конкретный сценарий.

Пусть опасное событие (вероятность рассчитана и показана в вершине FTA дерева) – это остановка насоса (частота. 2 раза в год).

Слои защиты.

Предупредительная сигнализация и оператор (PFD = 0.1) должен заметить и закрыть задвижку вручную.

Обратный клапан (PFD = 0.01) должен автоматически предотвратить поток.

Считаем риск. $2/\text{год} \times 0.1 \times 0.01 = 0.002$ события в год (раз в 500 лет).

1. Принимаем решение. Пусть нормативами, исходя из практики применения, установлено, что допустимая частота такой аварии не чаще чем один раз в 10 000 лет. А наша вероятность остановки (один раз в 500 лет) **недопустимо высокая!**

2. LOPA дает рекомендацию. Необходим дополнительный, более надежный слой защиты. Используем SIF с клапаном отсекателем и логическим решающим устройством, так что PFD этого контура защиты не хуже 0.001.

Пересчитываем.

$2/\text{год} \times 0.1 \times 0.01 \times 0.001 = 2 \times 10^{-6}/\text{год}$ (раз в 500 000 лет).

Теперь риск допустим!

3. Финал. На основе вывода LOPA мы обосновываем проектировщикам и финансистам, почему нам жизненно необходима эта дорогая система безопасности.

FTA диагностирует причины опасности. ETA рисует карту событий, а LOPA помогает решить, где именно и для какой прочности защиты нужно поставить ограждение, чтобы через него никто не провалился.

В современной международной практике (МЭК 61511) LOPA является ключевым мостом между качественным анализом опасностей и строгим количественным обоснованием для проектирования систем безопасности.

3.2. ПРАКТИКУМ ПО АНАЛИЗУ ДЕРЕВЬЕВ ОТКАЗОВ/СОБЫТИЙ (И СЛОЕВ ЗАЩИТЫ).

Задание 3.2. С поддержкой AI (типа GPT) подготовить свои решения кейсов и объяснения для одного или 2-х кейсов. Сделать вывод о правильности и качестве предложенных ответов и объяснений в кейсах.

Деревья как инструмент предотвращения аварий. FTA и ETA – это инструменты, которые стоят на страже человеческих жизней и окружающей среды. Ошибка в их построении или игнорирование их важности может иметь фатальные последствия. Речь идет об анализе причин и последствий аварий. С их помощью рисуются логические элементы и проектируется система безопасности, от которой зависят судьбы людей.

Кейс 3.1. «Цепная реакция беды» (Дерево отказов - FTA).

Ситуация.

Представьте многотонную стальную емкость, раскаленную до сотен градусов, под колоссальным давлением. Внутри – токсичные, взрывоопасные химикаты. Это реактор. Теперь представьте, что эта

стальная машина разрывается как бумажный пакет. Это не просто авария. Это катастрофа местного масштаба. ударная волна, разлет осколков, пожар, химическое заражение территории, неминуемые жертвы среди персонала.

Ваша задача, как инженера по безопасности. не допустить этого. Но чтобы предотвратить, нужно понять все возможные пути, ведущие к катастрофе. Именно для этого строится дерево отказов. В результате ищется не одна причина, а все комбинации сбоев, которые могут сложиться в роковую цепь событий.

Верхнее событие (то, чего мы всеми силами стараемся избежать). разрыв корпуса химического реактора из-за критического превышения давления.

Задание.

Постройте ФТА, чтобы выявить уязвимые места системы (табл. 3.3). Разделите все причины на две принципиальные группы.

- Технологические сбои (Отказы объекта). То, что может пойти не так в основном процессе.
- Отказы системы противоаварийной защиты (СПАЗ/SIS). Последняя линия обороны, которая должна сработать, когда основной процесс вышел из-под контроля. Ее отказ – это приговор.

Таблица 3.3. Уровни событий отказов.

Уровень анализа	Причины / События	Комментарий для «приукрашивания»
Верхнее событие	Разрыв реактора (катастрофа)	Цель. не допустить этого любой ценой.
Промежуточное событие	Критическое превышение давления в реакторе	Давление так высоко, что прочность металла на пределе.
Отказы объекта (Технологические сбои)	Выход из строя теплообменника → неконтролируемая экзотермическая реакция → перегрев → рост давления. • Ошибка оператора. Неправильная загрузка реагентов (слишком много активного компонента).	Это «спусковой крючок». Процесс пошел не так. Теперь все зависит от системы защиты.
Отказы СПАЗ/SIS (Отказы последней линии защиты)	• Датчик давления зависил показания (PFD = 0.01). «Мозг» системы не видит проблемы. • Логический контроллер завис/не обработал сигнал	СПАЗ/SIS – это «ангел-хранитель» реактора. Но и у ангелов бывают сбои. Мы количественно оцениваем их ненадежность (PFD).

Уровень анализа	Причины / События	Комментарий для «приукрашивания»
	(PFD = 0.001). «Мозг» системы не среагировал. • Аварийный предохранительный клапан не открылся (PFD = 0.05). «Рука» системы не выполнила команду – это самый слабый элемент.	

Ключевой вывод. Катастрофа наступает не из-за одной ошибки, а из-за рокового стечения обстоятельств. В данном случае. технологический сбой (отказ теплообменника) **И** одновременный отказ системы защиты (например, датчика). Дерево отказов наглядно показывает эту смертельную комбинацию **И**. Понимая это, мы можем добавить резервирование датчиков, улучшить ТО клапанов – точно усилить систему именно в самых слабых точках. Такое дерево – это карта рисков, которые вы обезвреживаете.

Кейс 3.2. «Сценарий кошмара» (Дерево событий - ЕТА).

Аммиак. Хладагент, который спасает продукты, но убивает людей. При утечке он образует ядовитое облако, вызывающее удушье и химические ожоги. Ваша задача – спрогнозировать развитие аварии и рассчитать риск гибели людей. Без этого расчета вся безопасность – это просто слова. Дерево событий (ЕТА) – это наш инструмент для написания сценариев развития аварии и оценки их вероятности.

Иницилирующее событие.

Разрыв трубопровода с жидким аммиаком высокого давления из-за коррозии. Частота этого события. 1 раз в 1000 лет (10^{-3} /год). Кажется, что это редко? На одном предприятии таких трубопроводов могут быть километры.

Задание.

Построить ЕТА, чтобы смоделировать два возможных сценария после разрыва. Оцените риск самого страшного из них.

Дерево событий.

1. Иницилирующее событие. Произошел разрыв трубопровода (Коррозия, 10^{-3} /год).

Развивается первый сценарий.

Сработала система аварийной остановки (СПАЗ/SIS). Автоматика засекла падение давления/утечку и за миллисекунды перекрыла клапаны.

Вероятность успеха СПАЗ/SIS: $(1 - \text{PFD}) = 0.98$.

Результат. Утечка локализована, небольшой выброс, обошлось без жертв.

Развивается второй сценарий (кошмарный).

Произошел отказ СПАЗ/SIS. Датчик не сработал ИЛИ клапан не закрылся. Вероятность отказа СПАЗ/SIS (PFD) = 0.02.

Результат. Массивный неконтролируемый выброс аммиака.

Облако аммиака достигает зоны нахождения персонала.

Конечный результат. Тяжелое поражение персонала, возможные летальные исходы.

Расчёт риска.

«Инженеры оперируют не страхами, а цифрами. Мы должны количественно оценить угрозу».

Частота сценария с жертвами = Частота инициирующего события × Вероятность отказа СПАЗ/SIS

Вероятность такого сценария равна $(10^{-3}/\text{год}) \times (0.02) = 0.00002$ (или 2×10^{-5}) случаев в год.

Что значит эта цифра? Это значит, что в среднем такая катастрофа будет происходить один раз в 50 000 лет. Звучит успокаивающе? Но если таких трубопроводов на вашем заводе 100 единиц, общий риск возрастает до 1 раза в 500 лет. А если заводов по стране 100? Риск становится уже вполне осязаемым.

Вся работа по построению ЕТА и расчету риска – это не абстракция. Это обоснование для инвестора, почему нужно выделить \$500 000 на замену всех устаревших клапанов и датчиков. Вы не рисуете дерево, вы принимаете решение, которое спасает жизни»

Кейс 3.3. Анализ слоев защиты (LORA) для сценария утечки аммиака.

Исходные данные.

Вы – инженер по безопасности. На основе построенного вами в Кейсе 3.2 «Дерева событий» (ЕТА) для сценария «Разрыв трубопровода с аммиаком» Вам поручено провести более детальный анализ LORA для количественной оценки риска и проверки, является ли существующая система защиты достаточной.

Сценарий для LORA. Массивная утечка аммиака с последующим поражением персонала (конечное катастрофическое событие из ЕТА).

Данные из ЕТА.

- **Иницилирующее событие ОПО (ИС):** Разрыв трубопровода.

- **Частота по ЕТА ($f_{\text{ИС}}$):** 10^{-3} событий/год (1 раз в 1000 лет).

Вероятность отказа СПАЗ.

$PFD_{\text{СПАЗ}} = 0.02$ (Вероятность отказа на требование). Это наш единственный независимый слой защиты (IPL) в предыдущем анализе.

Расчет из ЕТА.

Частота реализации сценария (F_{nr}) = $f_{ис} \times PFD_{СПАЗ} = 10^{-3}/\text{год} \times 0.02 = 2 \times 10^{-5}/\text{год}$.

Задание 1. Оценка приемлемости риска.

1. Руководство предприятия установило **целевой показатель риска** для сценариев с потенциально летальным исходом (F_{target}) на уровне **$10^{-6}/\text{год}$** (1 случай на 1 000 000 лет на одно оборудование).

2. Сравните расчетную частоту сценария ($F_{nr} = 2 \times 10^{-5}/\text{год}$) с целевым показателем ($F_{target} = 10^{-6}/\text{год}$).

Вопрос. Является ли риск приемлемым? Во сколько раз расчетный риск превышает целевой?

Задание 2. Идентификация дополнительных слоев защиты (LORA)

Ваша задача – найти и учесть в расчетах независимые слои защиты (IPL), которые могут предотвратить развитие аварии даже после отказа базовой ПАЗ. Проанализируйте предлагаемые меры и определите, какие из них могут считаться независимыми слоями защиты (IPL).

IPL 1. Полевая аварийная вентиляция и орошение (Детектор аммиака + система водяных завес). При обнаружении аммиака в воздухе система автоматически включает мощную вытяжную вентиляцию и водяные завесы для осаждения облака. PFD данной системы = 0.1.

IPL 2. Операторское вмешательство. Дежурный оператор в диспетчерской видит сигнал «УТЕЧКА АММИАКА» на мнемосхеме и вручную запускает систему орошения и включает сирену тревоги.

PFD для успешного и своевременного действия оператора = 0.5 (учтена вероятность ошибки, паники, отсутствия на месте).

IPL 3. Организационно-административный барьер. «Наличие противопогаза на рабочем месте». Является ли этот барьер *независимым слоем защиты* (IPL) в данном сценарии? Обоснуйте свой ответ, исходя из критериев IPL (независимость, специфичность, надежность, проверяемость).

Задание 3. Пересчет риска с учетом новых данных.

1. Проведите новый расчет частоты реализации сценария, учтя только те IPL, которые вы признали действительными в Задании 2.

2. Формула для LORA. $F_{nr} = f_{ис} \times PFD_{IPL1} \times PFD_{IPL2} \times \dots$

3. Сравните новый результат с целевым показателем риска ($10^{-6}/\text{год}$). Достаточно ли этих мер?

Задание 4. Принятие инженерного решения.

Расчеты показали, что риск все еще превышает целевой. Инвестор готов выделить средства на дополнительное оборудование, но запрашивает обоснование.

Вариант А. Установить вторую, резервную систему ПАЗ (СПАЗ/SIS) с таким же $PFD=0.02$, работающую полностью независимо от первой (другие датчики, другой логический контроллер, другие исполнительные механизмы).

Вариант Б. Модернизировать существующую систему аварийной вентиляции и орошения, снизив ее PFD с 0.1 до 0.01.

Вопрос. Какой вариант эффективнее снизит общий риск? Рассчитайте частоту сценария для каждого варианта, добавив их в свою модель LOPA. Какой вариант вы порекомендуете инвестору и почему?

Ответы.

Задание 1.

Риск неприемлем. Расчетный риск (2×10^{-5}) превышает целевой (1×10^{-6}) в **20 раз**.

Задание 2.

- IPL 1. Да, это технический, независимый и проверяемый слой. $PFD=0.1$.

- IPL 2. Да, при определенных условиях (обучение, процедуры, тревога) действие оператора может считаться IPL. $PFD=0.5$.

- IPL 3. Нет. Этот барьер не является *независимым* от инициирующего события. Разрыв трубы может произойти внезапно, у персонала может не быть времени надеть противогазы. Кроме того, надежность этого барьера низка и плохо поддается проверке.

Задание 3.

$F_{np} = f_{ис} \times PFD_{СПАЗ} \times PFD_{IPL1} \times PFD_{IPL2} = 10^{-3} \times 0.02 \times 0.1 \times 0.5 = 1 \times 10^{-6}/\text{год}$. Риск достиг целевого уровня.

Задание 4.

Вариант А. Добавляется новый IPL с $PFD=0.02$. $F_{np} = 10^{-3} \times 0.02 \times 0.1 \times 0.5 \times 0.02 = 2 \times 10^{-8}/\text{год}$. (Снижение в 50 раз от предыдущего результата).

Вариант Б. PFD_{IPL1} улучшается с 0.1 до 0.01. $F_{np} = 10^{-3} \times 0.02 \times 0.01 \times 0.5 = 1 \times 10^{-7}/\text{год}$. (Снижение в 10 раз от предыдущего результата).

Вывод. Вариант А эффективнее (снижает риск в 50 раз против 10). Однако вариант Б также перевыполняет целевой показатель и может быть дешевле. Решение требует технико-экономического обоснования.

Кейс 3.4. Пожар на нефтебазе.

Ситуация. Возможен пожар из-за статического разряда при наливке цистерны.

Задание.

Проведите FTA-анализ, учитывая:

- Отсутствие заземления (объект).
- Отказ системы искрозащиты (СПАЗ/SIS).

Решение.

Верхнее событие. Пожар.

1. Отказы объекта:

- Неисправность заземляющего контура.
- Нарушение технологии налива.

2. Отказы СПАЗ/SIS:

- Датчик статического заряда не сработал (PFD = 0.05).
- Система подавления искр отключена.

Рекомендации.

- Установить резервное заземление.
- Снизить PFD СПАЗ/SIS до 0.01 (SIL 2).

Кейс 3.5. Взрыв на газовом месторождении.

Ситуация. Причина взрыва – одновременный отказ предохранительного клапана ESD и СПАЗ/SIS.

Задание.

Рассчитайте вероятность аварии, если.

- Частота превышения давления. $10^{-2}/\text{год}$.
- PFD клапана = 0.1.
- PFD СПАЗ/SIS = 0.01.

Решение.

Риск = $10^{-2} \times (0.1 \times 0.01) = 10^{-5}/\text{год}$.

Вывод.

Риск приемлем (менее $10^{-4}/\text{год}$), но требуется мониторинг клапана.

Кейс 3.6. Отказ аварийного останова насоса.

Ситуация. Насос не отключился при перегреве, что привело к поломке.

Задание.

Определите слабые места СПАЗ/SIS, если.

- Датчик температуры. PFD = 0.02.
- Контроллер. PFD = 0.005.
- Реле отключения. PFD = 0.1.

Решение.

Общий PFD = $0.02 + 0.005 + 0.1 = 0.125$ (SIL 1).

Проблема. Реле – «слабое звено». Замена на PFD = 0.01 (SIL 2) снизит PFD до 0.035.

Кейс 3.7. LOPA-анализ для компрессора.

Ситуация. Иницирующее событие – «Разрыв мембраны компрессора» (частота. $5 \times 10^{-3}/\text{год}$).

Задание.

Определите требуемый SIL СПАЗ/SIS, если.

- Целевой риск. $<10^{-5}/\text{год}$.
- Существующие слои защиты:

- Механический клапан ($PFD = 0.1$).
- Аварийная вентиляция ($PFD = 0.01$).

Решение.

1. Риск после клапана. $5 \times 10^{-3} \times 0.1 = 5 \times 10^{-4}$.
2. Риск после вентиляции. $5 \times 10^{-4} \times 0.01 = 5 \times 10^{-6}$.
3. Требуемый PFD СПАЗ/SIS = $10^{-5} / 5 \times 10^{-6} = 0.2$ (SIL 1).

Выводы.

1. FTA анализирует причины отказов (объект + СПАЗ/SIS).
2. ЕТА моделирует последствия (развитие аварии).
3. LOPA связывает частоту событий с PFD для определения SIL.
4. Критичные ошибки при анализе опасностей ОПО:
 - Игнорирование зависимых отказов (например, общее питание).
 - Неучёт «слабых звеньев» (клапаны, реле).

Пример для самостоятельной работы.

- Постройте FTA для сценария «Утечка хлора на водочистке».
- Рассчитайте риск, если PFD СПАЗ/SIS = 0.05, а частота утечки = 10^{-3} /год.

3.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 3.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 3.1.

Задание. Решите дерево отказов, приведенное на рисунке 3.1.

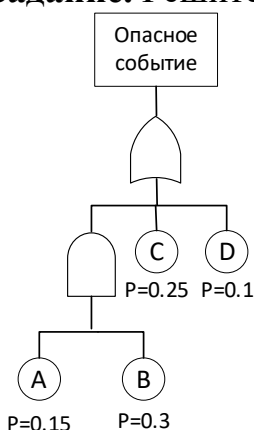


Рис.3.1. Дерево отказов

События, показанные на рис. 3.1, не являются взаимоисключающими [27]. Вероятность наступления верхнего события ближе всего к какой величине?

- а) 0.01.

- b) 0.355.
- c) 0.025.
- d) 0.395.
- e) 0.755.

Ответ b.

Расчет: $P(\text{Опасное событие}) = P(A) \times P(B) + P(C) + P(D) - (P(A) \times P(B) \times P(C)) - (P(A) \times P(B) \times P(D)) - (P(C) \times P(D)) + (P(A) \times P(B) \times P(C) \times P(D))$

Для получения дополнительной информации см. [24]/

Вопрос 1. Как «дерево отказов» для СПАЗ/SIS может включать человеческий фактор?

Варианты ответов.

A) как базовое событие в сценарии «отказ исполнительного механизма».

B) как независимый риск, не связанный с аппаратной частью.

C) как корневую причину ошибок конфигурации ПО.

D) как внешнее воздействие, не требующее анализа.

Ответ: A и C. Как базовое событие в сценарии «отказ исполнительного механизма». Как корневую причину ошибок конфигурации ПО.

Объяснение.

В FTA человеческий фактор – это базовое событие (A). например, неправильное техническое обслуживание клапана, что приводит к его отказу.

Корневая причина (C) при разработке СПАЗ это ошибка программирования СПАЗ/SIS (МЭК 61511, п. 12.2).

Вариант B – человеческий фактор анализируется в связке с системой.

Вариант D игнорирует требования стандартов.

Вопрос 2. Какие факторы включают в «Дерево отказов документации СПАЗ»?

Варианты ответов.

A) Несоответствие схем подключения реальной конфигурации.

B) Устаревшие версии руководств по эксплуатации.

C) Отсутствие сертификатов SIL у компонентов.

D) Некорректные расчеты PFavg (Probability of Failure on Demand).

Ответ:

A) Несоответствие схем подключения реальной конфигурации.

B) Устаревшие версии руководств по эксплуатации.

D) Некорректные расчеты PFDavg.

Объяснение.

Дерево отказов документации анализирует ошибки в документах, влияющие на безопасность.

Неверные схемы (A) → неправильный монтаж.

Устаревшие руководства (B) → ошибки эксплуатации.

Ошибки в расчетах PFDavg (D) → неверный SIL (МЭК 61511, п. 5.2.6).

Вариант C (отсутствие сертификатов) – это проблема аппаратного обеспечения, а не документации.

Вопрос 3. Какие отказы СПАЗ/SIS чаще всего связаны с «дерево отсутствия компетенций»?

Варианты ответов.

A) Неправильная интерпретация диагностических сообщений.

B) Механический износ клапанов из-за вибрации.

C) Использование неквалифицированным персоналом неподходящих инструментов для калибровки.

D) Перегрев процессора из-за плохой вентиляции.

Правильный Ответ

A) Неправильная интерпретация диагностических сообщений.

C) Использование неквалифицированным персоналом неподходящих инструментов для калибровки.

Объяснение.

Человеческий фактор в СПАЗ/SIS (МЭК 61511, п. 16).

Ошибки диагностики (A) → пропуск критических отказов.

Неправильная калибровка (C) → снижение точности измерений.

Варианты B и D – аппаратные отказы, не связанные с компетенциями.

Для получения дополнительной информации см. [27].

Тест 3.2. Оценка слоев защиты в системе управления.

Система имеет в своем составе датчик расхода охлаждающей воды в конденсатор. Этот датчик подключен к разным входам АСДУ аварийной сигнализации и контроллера регулирования температуры. При малом потоке охлаждающей воды в конденсатор срабатывает аварийная сигнализация, требующая от оператора вмешаться в ход процесса и перекрыть подачу пара.

Аварийная сигнализация в этом случае является автоматической. Она размещается в другом по отношению к контуру регулирования температуры контроллере АСДУ. Не зависит от человека. И потому может считаться слоем защиты.

Группа экспертов (АСЗ) принимает решение, что в этом случае среднюю вероятность отказа при запросе можно принять равной 0,1, так как оператор всегда находится в операторском помещении. Поэтому в колонку «Сигнализация» графы LOPA заносят значение 0,1.

Во время работы установки доступ в рабочую зону ограничен. Обслуживание производят только в те периоды, когда оборудование остановлено и отключено.

План безопасного ведения процесса требует, чтобы все лица, не относящиеся к оперативному персоналу, отмечались при входе в рабочее помещение и предупреждали о своем приходе оператора.

Вопрос 1. Какова основная функция датчика расхода охлаждающей воды в конденсаторе?

- A) Измерение температуры в конденсаторе.
- B) Контроль уровня жидкости в конденсаторе.
- C) Измерение потока охлаждающей воды и сигнализация о малом потоке.
- D) Увеличение подачи пара в конденсатор.

Вопрос 2. Почему аварийная сигнализация может считаться слоем защиты?

- A) Она всегда срабатывает при любом изменении.
- B) Она размещается в другом контуре по сравнению с контроллером регулирования температуры.
- C) Она не требует вмешательства оператора.
- D) Она уменьшает температуру в конденсаторе.

Вопрос 3. Какова вероятность отказа аварийной сигнализации, согласно данным группы АСЗ?

- A) 0,05.
- B) 0,1.
- C) 0,2.
- D) 0,15.

Вопрос 4. Какое должно быть внесено в графу «Дополнительное ослабление, ограничение доступа»?

- A) 0,05.
- B) 0,1.
- C) 0,2.
- D) 0,3.

Вопрос 5. Какой коэффициент присутствия используется для расчета вероятности травмы оператора?

- A) 0,02.
- B) 0,03.
- C) 0,04.
- D) 0,05.

Ответ и объяснения.

Вопрос 1.

Ответ С. Измерение потока охлаждающей воды и сигнализация о малом потоке.

Датчик предназначен для контроля потока охлаждающей воды и срабатывает, если поток становится слишком мал, что может привести к аварийной ситуации.

Вопрос 2.

Ответ В. АСДУ размещается в другом контуре по сравнению с контроллером регулирования температуры.

Хотя аварийная сигнализация не является надежным независимым слоем защиты в некоторых случаях разработчики считают ее слоем защиты, так как она функционирует независимо от основного контура управления температурой, и это увеличивает общую безопасность системы.

Вопрос 3.

Ответ В. 0,1.

Группа АСЗ установила вероятность отказа аварийной сигнализации на уровне 0,1, что указывает на ее надежность при наличии запроса.

Вопрос 4.

Ответ В. 0,1.

В графу «Дополнительное ослабление, ограничение доступа» было внесено значение 0,1, что указывает на снижение риска для оперативного персонала благодаря ограниченному доступу.

Вопрос 5.

Ответ С. 0,04.

Коэффициент присутствия был рассчитан как $0,5 \text{ ч} / 12 \text{ ч} = 0,04$, и он используется для корректировки вероятности травмы оператора в случае возникновения аварийной ситуации.

Объяснение.

Хотя аварийная сигнализация не может считаться надежным слоем защиты, она может ограничивать доступ на ОПО, что играет важную роль в снижении рисков, и правильное ее применение помогает предотвратить аварийные ситуации.

Группа анализа слоев защиты полагает ее независимым слоем защиты так, что наличие усиленных ограничений доступа приводит к снижению риска для оперативного персонала на порядок. Поэтому в графу «Дополнительное ослабление, ограничение доступа» было введено значение 0,1.

Если возгорание в результате протечки уплотнения насоса возникает во время обхода территории оператором, оператор может получить травму при условии нахождения рядом с насосом.

Оператор может находиться вблизи насоса в течение 30 минут за смену. В этом случае коэффициент присутствия равен $0,5 \text{ ч} / 12 \text{ ч} = 0,04$, а вероятность события должна умножаться на рассчитанный таким образом коэффициент присутствия для получения откорректированного значения частотности.

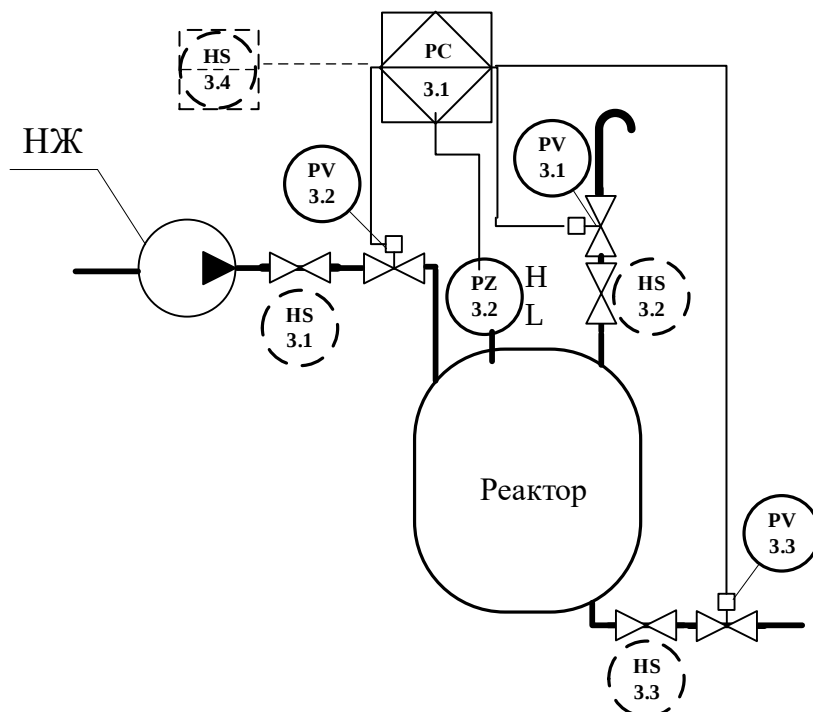
Тест 3.3. Функция безопасности для защиты реактора.

Для защиты реактора от избыточного давления (или от возможных событий, приводящих к избыточному давлению) требуется функция безопасности. Функция разделена на три подфункции, каждая из которых реагирует на одно из трех возможных событий.

Подфункция 1. Потеря подачи жидкости в реактор.

Подфункция 2. Высокое или низкое давление в реакторе.

Подфункция 3. Ручной останов или потеря управляемости. Подфункции 1 и 2 могут быть также инициированы путем нажатия кнопки аварийного останова HS01. В случае потери питания приборов должны немедленно сработать отключающие клапаны PV3.2 и PV3.1 и остановлен насос НЖ.



.Рис. 3.2. Схема управления реактором

Вопрос 1. Где на схеме должен быть показан ручной останов (HS 3.4)?

- А) В области управления насосом НЖ.
- В) В области управления предохранительным клапаном PV3.4.
- С) В области управления клапаном PV3.3.
- Д) В области управления всеми функциями безопасности.

Вопрос 2. Является ли кнопка аварийного останова (HS 3.4) дополнительным слоем защиты?

- А) Да, она обеспечивает дополнительную защиту в случае автоматических систем.
- В) Нет, она просто дублирует функции автоматических систем.
- С) Да, но только в случае потери питания.
- Д) Нет, она не влияет на безопасность системы.

Вопрос 3. Какова последовательность действий при обнаружении потери подачи ?

- А) Открыть предохранительный вентиль HS 3.2, закрыть вентили HS 3.1 и HS 3.3 затем остановить насос НЖ.
- В) Закрыть вентили HS 3.1 и HS 3.3, затем остановить насос через 30 секунд.
- С) Остановить насос сразу после закрытия клапана HS 3.1.
- Д) Ничего не делать, пока не будет нажата кнопка HS 3.4.

Вопрос 4. Что происходит при обнаружении высокого давления в реакторе?

- А) Сначала останавливается насос.
- В) Закрывается клапан PV3.2, затем открывается предохранительный клапан PV3.1.
- С) Немедленно срабатывает предохранительный клапан PV3.1, затем отключается питание.
- Д) Ничего не происходит, пока не будет нажата кнопка HS 3.4.

Ответ.

Вопрос 1: Д. В области управления всеми функциями безопасности.

Ручной останов (HS 3.4) должен быть показан на схеме в области управления всеми функциями безопасности на ПЛК, так как он может инициировать все необходимые действия для защиты реактора от избыточного давления в случае потери управляемости.

Вопрос 2: А. Да, она обеспечивает дополнительную защиту в случае автоматических систем. Кнопка аварийного останова (HS 3.4) является дополнительным слоем защиты, так как позволяет оператору вручную прервать процесс и активировать защитные меры, если автоматические системы не срабатывают.

Вопрос 3: В. Закрывать вентили HS 3.1 и HS 3.3, затем остановить насос через 30 секунд.

При обнаружении потери энергии необходимо сначала закрыть вентили HS 3.1 и HS 3.3 для прекращения подачи энергии в реактор, а затем остановить насос через 30 секунд.

Вопрос 4: Ответ С. Немедленно срабатывает предохранительный клапан PV3.1, затем отключается питание. При обнаружении высокого давления в реакторе предохранительный клапан PV3.1 срабатывает немедленно, а затем отключается питание для обеспечения безопасности.

Объяснение.

Правильное понимание функций безопасности и их последовательности критически важно для предотвращения аварийных ситуаций в реакторах. Приказ РТН N 533 устанавливает и требует наличия как автоматических систем защиты, так и средств ручного управления и останова, работающих как различные, часто независимые слои защиты, которые вместе обеспечивают требуемый уровень безопасности. Автоматическая защита – это первый и наиболее надежный барьер против многих типов аварий, а ручной останов – это важный аварийный резерв, управляемый человеком. Ручной останов и автоматические системы защиты работают в тандеме, обеспечивая дополнительный уровень безопасности.

Для получения дополнительной информации см. [27].

3.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 3.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ» «Раздел 3».

Тест 3.6. Построить дерево отказов.

Критический случай опасности 0,21 раз/год возникает при формировании взрывчатой смеси (1,05 раз/год) и вероятности воспламенения 0,2. Взрывчатая смесь возникает если впрыск ее осуществляется до стадии вакуумирования или появления воздуха в подаче газа (0,1 раз в год) или проникновения воздуха после вакуумирования (0,55 раз/год).

Впрыск газа до стадии вакуумирования возникает из за отказа клапана 0,05 раз в год или незапланированного открытия клапана (0,35 раз в год) или присутствия воздуха после вакуумирования (0,55 раз в год) которое возможно из за ошибочного теста (диагностики) на вакуум (0,3 раза в год) или из за утечки после измерения на вакуум (0,25 раз/год).

Ошибочный тест на вакуум возможен из-за ошибки программы проверки (0,2 раз/год) или ошибки технических средств контроля (0,1 раз в год). Незапланированное открытие клапана возникает из ошибки оператора или ремонтника (0,2 раз/год) или из-за отказа оборудования управления клапаном (0,1 раз/год) или отказа программы ПЛК (0,05 раз в год). Построить дерево отказов с указанием интенсивностей отказов в узлах.

Вопрос 1. Рассчитайте частоту незапланированного открытия клапана.

Варианты.

- a) 0,1 раз/год.
- b) 0,2 раз/год.
- c) 0,35 раз/год.
- d) 0,4 раз/год.

Вопрос 2. Какова частота ошибочного теста на вакуум?

Варианты.

- a) 0,1 раз/год.
- b) 0,2 раз/год.
- c) 0,3 раз/год.
- d) 0,55 раз/год.

Вопрос 3. Рассчитайте ожидаемую частоту впрыска до вакуумирования.

Варианты.

- a) 0,05 раз/год.
- b) 0,35 раз/год.
- c) 0,55 раз/год.
- d) 0,1 раз/год.

Вопрос 4. Почему данные задачи противоречивы?

Варианты.

- a) Неверно указана вероятность воспламенения.
- b) Сумма частот для формирования взрывчатой смеси не сходится.
- c) Ошибочно рассчитана частота критического случая.
- d) Все варианты верны.
- e) 1,05 раз/год.

.Вопрос 5. Если проигнорировать противоречия, чему равна частота критического случая?

Варианты.

- a) 0,21 раз/год.
- b) 1,05 раз/год.
- c) 0,55 раз/год.
- d) 0,13 раз/год.

Тест 3.7. Дерево событий.

В процессе эксплуатации вагона возможно опрокидывание и разрушения железнодорожной цистерны. Дерево событий показано на рисунке 3.3. Для реализации системы безопасности (SIF) используется архитектура (1001) без резервирования. В СПАЗ выполняется автоматическая диагностика каждую секунду (интервал диагностики, $DTI = 1$ секунда). Контур безопасности (SIF) запрограммирована на перевод процесса в безопасное состояние при обнаружении отказа оборудования SIF. Время отклика на отключение составляет 10 миллисекунд. Опасное состояние возникает в среднем каждую минуту (интервал опасного состояния, $DI = 1$ минута). Какой режим (непрерывного, высокого или низкого запроса) СПАЗ используется, и можно ли учесть автоматическую диагностику при расчете вероятности отказа?

$DI = 1$ минута, $DTI = 1$ секунда. Интервал DI (1 минута) в 60 раз больше, чем DTI , и SIF автоматически отключает процесс при обнаружении внутреннего отказа оборудования. Этот режим работы SIF классифицируется как режим высокого запроса. Поскольку DI меньше, чем в 100 раз DTI , то только частичный вклад автоматической диагностики при вероятностном анализе можно учесть. И это не означает, что режим работы SIF должен быть классифицирован как режим непрерывного спроса. Таким образом, работа SIF с использованием автоматической диагностики обеспечивает защиту ОУ при условии высокого (но не непрерывного) запроса СПАЗ.

Вопрос. Учитывая приведенное дерево событий, частоту опрокидывания и разрушения железнодорожной цистерны, частота мгновенного возгорания, наиболее близка к

- a) 4.0×10^{-5} /год.
- b) 2.0×10^{-7} /год.
- c) 1.2×10^{-5} /год.
- d) 3.8×10^{-6} /год.

е) не один ответ не корректен.

Падение вагона и разрушение Утечка	Разлив Материала Тип	Легко воспламеняющийся	Источник воспламенения Соприкоснулся?	исход
			P=0.05	Вспышка (взрыв)
		P=0.25	Yes	
		Yes	P=0.95	Без последствий
	P=0.2		No	
	Летучая жидкость	P=0.75		Экологические проблемы
		No		
F = 8.0 x 10 ⁻⁵ /year	P=0.4			Экологические проблемы
	Не летучая жидкость			
	P=0.4			Environmental
	Порошок			

Рис. 3.3. Дерево событий

Информацию о деревьях событий см. в книге Practical SIL Target Selection. Risk AnalyСПАЗ/SIS per the МЭК61511 Safety Lifecycle авторства E.W. Scharpf, H.W Thomas и T.R. Stauffer, глава 7.

Для получения дополнительной информации см. [27].

Тест 3.8. Анализируется LOPA защиты ОПО.

Вопрос 1. Может ли сигнал тревоги оператора быть слоем защиты? Какие пункты должны быть верны, чтобы принять такой слой защиты?

а) Сигналы тревоги на пульте оператора должны быть рационализированы.

б) Индикатор оператора должен быть жестко подключен к СПАЗ.

с) Никакой кредит^х (англ. яз. термин) для сигнала тревоги оператора не может быть принят, если оборудование не сертифицировано SIL.

^хКредиты – это «зачёты» (критерии соответствия проектным требованиям) при проектировании СПАЗ.

д) Качественный LOPA не использует сигнал тревоги оператора в качестве слоя защиты.

Для получения дополнительной информации см. [24].

Тест 3.9. Как влияют ручные проверочные испытания на PFDavg для структуры SIF 1001 с учетом их периодичности.

Использовать упрощенную формулу PFDavg. Считать $\lambda = 0.01$ и $T_i = 20$ вычислить значение PFDavg.

Вопрос 1. Определение PFDavg.

Как определяется показатель PFDavg для одноканальной системы с ручными проверочными испытаниями?

- A) $PFD_{avg} = \lambda d \times T_i$.
- B) $PFD_{avg} = \lambda d \times T_i / 2$.
- C) $PFD_{avg} = \lambda d \times t$.
- D) $PFD_{avg} = 1 - e^{\lambda d \times t}$.

Вопрос 2. Влияние интервала T_i . Какое влияние оказывает увеличение интервала T_i на значение PFDavg?

- A) Увеличение PFDavg.
- B) Уменьшение PFDavg.
- C) Не влияет на PFDavg.
- D) Увеличивает вероятность отказа.

Вопрос 3. Условия применения формулы. При каких условиях можно использовать упрощенную формулу $PFD_{avg} = \lambda d \times T_i / 2$?

- A) Когда $\lambda d \times t$ значительно больше единицы.
- B) Когда $\lambda d \times t$ значительно меньше единицы.
- C) Когда $\lambda d \times t$ равно единице.
- D) Когда система многоканальная.

Вопрос 4. Интерпретация результатов. Если $\lambda = 0.01$ и $T_i = 0,5$, каково значение PFDavg?

- A) 0..
- B) 0.2.
- C) 0.01.
- D) 0.05.

Тест 3.10. Совместное использование АСДУ и СПАЗ.

Система имеет в своем составе датчик расхода охлаждающей воды в конденсатор. Этот датчик подключен ко входам контроллера регулирования температуры автоматизированной системы диспетчерского управления (АСДУ) и PLC SIF системы СПАЗ/SIS (рис. 3.4) [28].

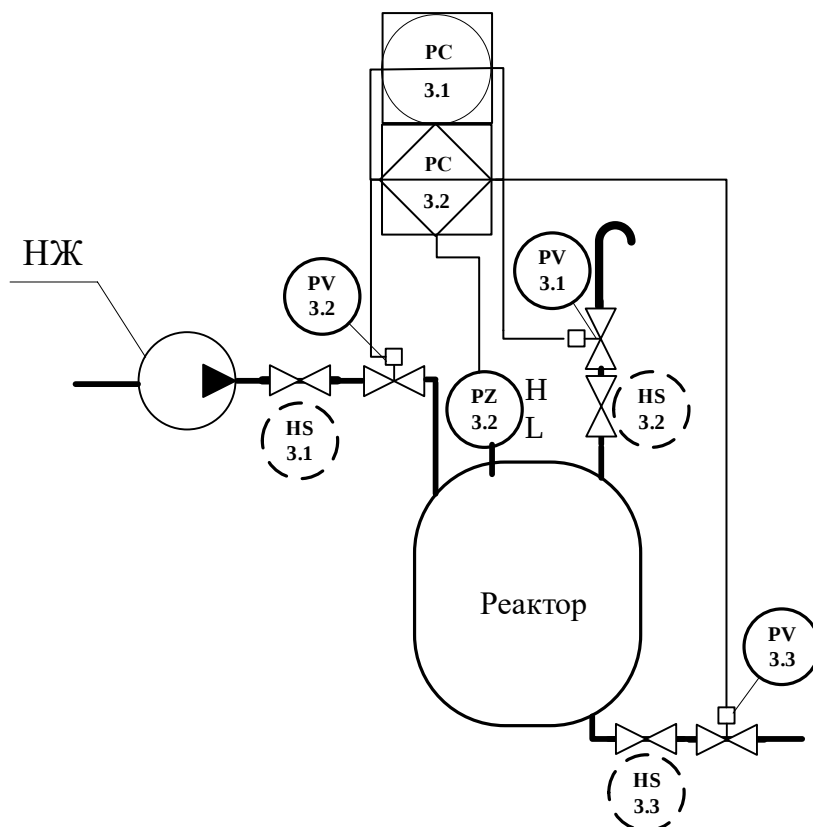


Рис. 3.4. Совместное включение датчика в АСДУ и СПАЗ

Вопрос 1. В реакторе срабатывает аварийная сигнализация при малом потоке. Может ли считаться слоем защиты аварийная сигнализация на экране компьютера АСДУ?

- А) Не может считаться.
- В) Может считаться, если оператор имеет соответствующую квалификацию.
- С) Может считаться, так как контур сигнализации АСДУ является независимым слоем защиты.
- Д) Не может считаться, так как аварийная сигнализация зависит от вмешательства оператора.

Вопрос 2. Каковы ключевые требования стандарта МЭК 61508 в контексте слоев защиты?

- А) Слои защиты должны быть независимыми друг от друга.
- В) Каждый слой защиты должен снижать риск непреднамеренных событий.
- С) Эффективность слоев защиты должна быть проверена.
- Д) Все вышеперечисленное.

Вопрос 3. Почему аварийная сигнализация, требующая вмешательства оператора, не может считаться надежным слоем защиты?

- А) Она не может предотвратить аварийные ситуации.
- В) Она зависит от квалификации оператора.
- С) Она не является автоматической системой.
- Д) Все вышеперечисленное.

Вопрос 4. Каковы основные акценты стандарта МЭК 61511 в отношении систем безопасности процессов?

- А) Системы должны быть полностью автоматизированы.
 - В) Каждый слой защиты должен быть независимым.
 - С) Оператор не должен вмешиваться в процессы.
 - Д) Стандарты не имеют значения для проектирования.
- Для получения дополнительной информации см. [27].

Тест 3.11. Оценка независимости слоев защиты в системе управления.

Вопрос 1. Какова основная функция АСДУ в контексте управления температурой в реакторе?

- А) Изменение давления в реакторе.
- В) Прекращение подачи пара в рубашку реактора при превышении температуры.
- С) Увеличение подачи пара в рубашку реактора.
- Д) Контроль уровня жидкости в реакторе.

Вопрос 2. Является ли АСДУ независимым слоем защиты в данной системе управления?

- А) Да, всегда.
- В) Нет, никогда.
- С) Да, если она надежна.
- Д) Нет, если вероятность отказа высока.

Вопрос 3. Почему прекращение подачи пара в рубашку реактора можно считать слоем защиты?

- А) Оно снижает риск возникновения аварийной ситуации.
- В) Оно увеличивает давление в реакторе.
- С) Оно не влияет на безопасность.
- Д) Оно увеличивает температуру в реакторе.

Тест 3.12. СПАЗ для системы защиты утечки метана (частота 2×10^{-2} /год) реализована на основе:

- 1. Датчик газа (PFD=0.01).
- 2. Отсечной клапан (PFD=0.05).
- 3. Целевой риск. $<10^{-4}$ /год.

Вопрос 1. Какой требуется SIL для СПАЗ/SIS?

Вопрос 2. Достаточна ли конфигурация для обеспечения целевого риска?

4. НАДЕЖНОСТЬ СИСТЕМ БЕЗОПАСНОСТИ.

4.1. КЛЮЧЕВЫЕ ПРИНЦИПЫ ОЦЕНКИ НАДЕЖНОСТИ СИСТЕМ БЕЗОПАСНОСТИ.

Задание 4.1. Уяснить ключевые принципы оценки надежности систем безопасности.

Надежность систем промышленной безопасности – это не просто технический показатель, а средство защиты жизни. Каждый расчет, каждый компонент СПАЗ/SIS представляет собой этическое обязательство перед людьми, которые доверяют свою безопасность этим системам. Как инженеры, Вы проектируете не просто цепи реле и логические контроллеры. Вы создаете последний рубеж защиты между технологическим процессом и катастрофой.

В этом контексте надежность СПАЗ/SIS приобретает глубокий социальный смысл, выражаемый через ключевые параметры.

- **Отказоустойчивость (Fault Tolerance)** – это способность продолжать защищать даже при частичных отказах, подобно тому, как хорошая система охраны продолжает работать при выходе из строя отдельных датчиков.

- **Отказобезопасность (Fail-Safe)** – это принцип, по которому любой сбой должен приводить систему в максимально безопасное состояние, аналогично тому, как сломанный светофор переключается в режим мигающего красного сигнала.

- **Вероятность отказа по требованию (PFDavg)** – это математическое выражение нашего профессионального стремления к идеалу. Система должна срабатывать всегда, когда действительно нужна, как надежный страж, который никогда не засыпает на посту.

- **Частота ложных срабатываний (STR)** – это напоминание о том, что избыточная осторожность тоже имеет свою цену, поскольку каждое ложное срабатывание – это остановка производства, финансовые потери и риск «привыкания» персонала к тревогам.

Эти показатели не просто цифры в отчете по верификации. Они представляют собой квинтэссенцию инженерной этики, определяющей пути создания надежной системы, чтобы предотвратить катастрофу, и при этом не настолько консервативной, чтобы парализовать производство. Этот баланс – высшее проявление профессионального мастерства в области промышленной безопасности.

Отказоустойчивость и отказобезопасность обеспечиваются правильным выбором сертифицированных компонентов СПАЗ/SIS с использованием механизмов резервирования и регулярного диагностирования (рис. 4.1).

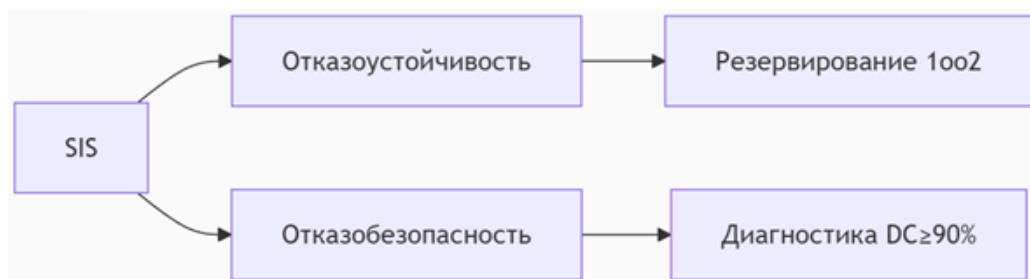


Рис 4.1. Механизмы отказоустойчивости и отказобезопасности

4.2. ПРАКТИКУМ ПО РАСЧЕТУ НАДЕЖНОСТИ СПАЗ.

Задание 4.2. С поддержкой AI (типа GPT) подготовить свои решения кейсов и объяснения для одного или 2-х кейсов. Сделать вывод о правильности и качестве предложенных ответов и объяснений в кейсах.

Кейс 4.1. Дилемма выбора надежности СПАЗ инженером по безопасности.

Сценарий.

Вы – ведущий инженер на установке фторирования питьевой воды. Для дозирования опасного фтороводорода используется одна насосная система с контуром безопасности. Отказ этого насоса или его несвоевременная остановка может привести к массовому отравлению в жилом районе. Но и частые ложные остановки – это не просто неудобство, это экстренные выезды бригад, расследования, миллионы рублей убытков и пикеты недовольных жителей.

Ваша задача – проанализировать текущую систему и предложить решения, которые спасают жизни, но не разоряют компанию.

Текущая система (СПАЗ/SIS).

У вас установлена простейшая система аварийного останова конфигурации 1oo1:

- Один датчик давления на выходе насоса.
- Один отсечной клапан.

Проведем анализ, разбив систему на элементы. датчик (S) и исполнительный элемент (клапан, LV).

Анализ текущей системы (СПАЗ/SIS 1oo1).

Для расчета показателей надежности SIF, состоящей из нескольких элементов, используются следующие подходы.

• $PFD_{avg\_system} \approx PFD_{avg\_S} + PFD_{avg\_LV}$ (для конфигурации 1oo1 без ПЛК)

• $STR_{system} \approx STR_S + STR_{LV}$ (для конфигурации 1oo1)

Пусть типовые интенсивности отказов для элементов:

- Датчик давления (S).

– $\lambda_{du\_S} = 0.006$ (1/год). Интенсивность опасного недетектируемого отказа датчика составляет ~60% от общего λ_{du} SIF.

– $\lambda_{sd\_S} = 0.04$ (1/год). Это ~80% от общего λ_{sd} .

• **Отсечной клапан (LV).**

– $\lambda_{du\_LV} = 0.004$ (1/год) // ~40% от общего λ_{du} .

– $\lambda_{sd\_LV} = 0.01$ (1/год) // ~20% от общего λ_{sd} .

Выполним расчеты интенсивностей опасных и безопасных отказов.

$$\lambda_{du\_S} + \lambda_{du\_LV} = 0.01; \lambda_{sd\_S} + \lambda_{sd\_LV} = 0.05.$$

1. Расчет PFDavg и SIL для текущей системы (1oo1)

• $PFD_{avg\_S} = \lambda_{du\_S} \times T_1 / 2 = 0.006 \times 1 / 2 = 0.003.$

• $PFD_{avg\_LV} = \lambda_{du\_LV} \times T_1 / 2 = 0.004 \times 1 / 2 = 0.002.$

• **$PFD_{avg\_system} = 0.003 + 0.002 = 0.005$** (что соответствует SIL 2).

2. Расчет STR для текущей системы (1oo1).

• $STR\_S = \lambda_{sd\_S} = 0.04$ / год.

• $STR\_LV = \lambda_{sd\_LV} = 0.01$ / год.

• **$STR_{system} \approx 0.04 + 0.01 = 0.05$ / год** (ложное срабатывание в среднем раз в 20 лет)

• **Годовые убытки. $0.05 \times 500\,000\text{ Р} = 25\,000\text{ Р/год}$**

3. Анализ вариантов модернизации с учетом архитектуры СПАЗ/SIS элементов (функциональная безопасность).

Вариант А. Переход на архитектуру 1oo2 только для датчиков.

Это наиболее распространенный и экономичный подход, так как резервирование клапана обычно значительно дороже.

Архитектура. Два датчика (1oo2) + один клапан (1oo1).

Расчет PFDavg:

– Для датчиков (1oo2). $PFD_{avg\_1oo2\_S} = (\lambda_{du\_S} \times T_1)^2 / 3 = (0.006 \times 1)^2 / 3 = 0.000012.$

– Для клапана (1oo1). $PFD_{avg\_LV} = 0.002$ (как и было).

$PFD_{avg\_system} \approx 0.000012 + 0.002 = 0.002012$ (что соответствует **верхней границе SIL 2**, ближе к SIL 3). Резервирование датчиков само по себе дает значительное улучшение компонента измерения, но «бутылочным горлышком» теперь становится нерезервированный клапан.

• **Расчет STR.**

– Для датчиков (1oo2). $STR_{1oo2\_S} \approx 2 \times \lambda_{sd\_S} = 2 \times 0.04 = 0.08$ / год.

– Для клапана (1oo1). $STR_{LV} = 0.01$ / год.

$STR_{system} \approx 0.08 + 0.01 = 0.09$ / год (ложное срабатывание в среднем раз в ~11 лет).

Годовые убытки из за ложных остановок ТП: **$0.09 \times 500\,000\text{ Р} = 45\,000\text{ Р/год}.$**

Вывод по варианту А. Резервирование только датчиков существенно повышает безопасность, но почти вдвое увеличивает частоту ложных срабатываний и убытки. Это классический компромисс.

Вариант Б. Установка более современных датчиков с самодиагностикой (без резервирования).

• **Предположим,** новые датчики имеют улучшенные параметры благодаря диагностике.

- $\lambda_{du\_S\_new} = 0.003$ (снизилось в 2 раза).
- $\lambda_{sd\_S\_new} = 0.03$ (может незначительно вырасти из-за диагностических ложных тревог).

• **Архитектура.** Один улучшенный датчик (1oo1) + один старый клапан (1oo1).

• **Расчет PFDavg:**

- $PFDavg\_S\_new = \lambda_{du\_S\_new} \times T1 / 2 = 0.003 \times 1 / 2 = 0.0015$.
- $PFDavg\_LV = 0.002$.

PFDavg_system = 0.0015 + 0.002 = 0.0035 (остается в SIL 2, но показатель улучшился на 30%).

• **Расчет STR:**

- $STR\_S\_new = \lambda_{sd\_S\_new} = 0.03$ / год.
- $STR\_LV = 0.01$ / год.

STR_system $\approx 0.03 + 0.01 = 0.04$ / год.

Годовые убытки: $0.04 \times 500\,000\text{ Р} = 20\,000\text{ Р/год}$.

Вывод по Варианту Б. Мы получаем умеренное улучшение по безопасности и небольшое улучшение по экономике (меньше ложных остановок). Это эволюционный путь.

4. Итоговое предложение и аргументация.

Рекомендуемое решение. Гибридный вариант – Резервирование датчиков 1oo2 + модернизация клапана.

Анализ показал, что после резервирования датчиков основным источником риска становится клапан. Поэтому идеальное решение включает три шага.

1. Немедленно. Перейти на архитектуру 1oo2 для датчиков. Это даст немедленный и значительный выигрыш в безопасности ($PFDavg \sim 0.002$), даже с существующим оборудованием. Мы осознанно идем на увеличение операционных расходов на 20 000 руб./год (с 25к до 45к) ради жизни людей.

2. В среднесрочной перспективе. Установить новые датчики с диагностикой в конфигурации 1oo2. Это позволит улучшить и безопасность, и экономику.

- $PFDavg_{1oo2}$ станет еще ниже (например, $(0.003 \times 1)^2 / 3 = 0.000003$).
- STR_{1oo2} снизится ($2 \times 0.03 = 0.06$ /год вместо 0.08).

3. В долгосрочной перспективе. Модернизировать клапан. Заменить его на более надежную модель с лучшими показателями λ_{du} и λ_{sd} . Это окончательно снизит «слабое звено» системы и может позволить выйти на уровень SIL 3.

Аргументация для Совета директоров.

«Наш анализ выявил, что ключевой риск опасного отказа сосредоточен не только в датчиках, но и в клапане. Простое резервирование датчиков решает лишь часть проблемы.

Поэтому мы предлагаем поэтапный план модернизации, который оптимизирует инвестиции и риски.

1. Сначала мы резервируем датчики. Это немедленно и кардинально снизит вероятность аварии, купирова самый серьезный риск. Мы готовы нести возросшие, но прогнозируемые операционные расходы на ложные срабатывания.

2. Затем мы улучшаем датчики. Новое оборудование с диагностикой не только в будущем повысит безопасность, но и компенсирует возросшую частоту ложных остановок, снизив её почти до исходного уровня.

3. Наконец, мы модернизируем клапан. Это окончательно закрепит высокий уровень безопасности и надежности всей системы.

Этот план распределяет затраты во времени и целенаправленно атакует самые критические точки системы, обеспечивая максимальную отдачу от вложенных средств как в аспекте спасения жизней, так и в аспекте операционной эффективности».

Кейс 4.2. Формулы расчета надежности для архитектуры 1oo2 и их объяснение.

Вот как выглядят формулы расчета отказоустойчивости для архитектуры 1oo2 на разных этапах эволюции проекта СПАЗ.

Упрощённая формула (ISA TR84.00.02).

$$PFD_{avg} \approx ((\lambda_{DU} * TI)^2) / 3 + \beta * \lambda_{DU} * TI / 2$$

Эта формула основана на ключевом упрощении в приближении редких событий. Она состоит из двух основных частей:

- $((\lambda_{DU} * TI)^2) / 3$ – Эта часть учитывает вероятность одновременного отказа двух каналов из-за независимых случайных причин. Она доминирует в системах с хорошо организованной защитой от общих причин.
- $\beta * \lambda_{DU} * TI / 2$ – Эта часть учитывает отказы из-за общих причин (Common Cause Failures), которые могут вывести из строя оба канала одновременно. β -фактор – это доля отказов, которые являются общими.

Когда применяется: Для предварительных расчётов, эскизного проектирования, когда нет полных данных о диагностике и времени восстановления.

Расширенная формула (на основе МЭК 61508):

$$PFD_{avg} = [PTC^2 * (\lambda_{DU} * (1-\beta))^2 * TI^2] / 3 + [(1-PTC)^2 * (\lambda_{DU} * (1-\beta))^2 * SL^2] / 3 + 2 * (\lambda_{DD} * (1-\beta))^2 * (MTTR + T_D/2)^2 + (\beta * \lambda_{DU} * TI) / 2 + \beta * \lambda_{DD} * (MTTR + T_D/2).$$

Объяснение.

Эта формула раскладывает вероятность отказа СПАЗ/SIS по частям:

Первые два слагаемых – учитывают необнаружимые опасные отказы (λ_{DU}).

$[PTC^2 * (\lambda_{DU} * (1-\beta))^2 * TI^2] / 3$ – Отказы, обнаруживаемые при периодическом плановом тестировании (Proof Test Coverage, PTC).

$[(1-PTC)^2 * (\lambda_{DU} * (1-\beta))^2 * SL^2] / 3$ – Отказы, которые НЕ обнаруживаются даже плановым тестированием. SL – это срок службы системы, и эта часть показывает, как со временем накапливаются скрытые дефекты.

Третье слагаемое – $2 * (\lambda_{DD} * (1-\beta))^2 * (MTTR + T_D/2)^2$ – учитывает обнаруживаемые опасные отказы (λ_{DD}). Система диагностики обнаруживает их практически сразу, и здесь ключевую роль играет не интервал тестирования, а среднее время восстановления (MTTR) и время диагностики.

Четвёртое и пятое слагаемые – учитывают отказы по общим причинам (β) как для обнаруживаемых, так и для необнаруживаемых отказов.

Когда применяется эта формула: Для финальной верификации, подготовки отчётов для сертификации, когда известны все параметры из FMEDA-отчётов и определены политики эксплуатации.

Задача А: «Рассчитать PFD_{avg} на этапе концептуального проектирования, если известны только λ_{DU} , TI. Правильный ответ: Упрощённая формула А.

Задача В: «Рассчитать PFD_{avg} на этапе концептуального проектирования, если известны только λ_{DU} , TI. Правильный ответ: Упрощённая формула В

Задача С: «Верифицировать SIL 3 для существующего проекта, имеются FMEDA-отчёты с данными по λ_{DU} и λ_{DD} , известна полнота тестов PTC».

Ответ: Расширенная формула С

Объясните ограничения: Упрощённая формула может занижать PFD_{avg} , так как не учитывает, что некоторые отказы не обнаруживаются при тестировании (1-PTC) и что система часть времени находится в деградированном состоянии из-за обнаруживаемых отказов (влияние MTTR).

Кейс 4.3. Простая система без резервирования (ROUTE 1H).

Ситуация. На складе с негорючими материалами установлен один датчик задымления (1oo1). Ложное срабатывание приводит

лишь к включению вентиляции.

Задача. Рассчитать PFD_{avg} для SIL 1.

Решение.

1. **Метод.** ROUTE 1H (упрощенный, т.к. нет резервирования и диагностики).

2. **Данные.**

- $\lambda_{du} = 0.1$ (опасные необнаруженные отказы/год),
- $T1 = 1$ год (период тестирования).

3. **Формула.**

$$PFD_{avg} = \lambda_{du} \times T1 / 2 = 0.1 \times 0.5 = 0.05.$$

4. **Вывод.** Значение соответствует SIL 1 ($PFD_{avg} > 0.01$).

Аналогия. SIL 1 это как бы оценка здоровья по общему самочувствию без анализов.

Кейс 4.4. Расчет STR для системы с резервированием 2oo3.

Условие.

Три датчика температуры в конфигурации 2oo3.

- $\lambda_{sd} = 0.005$ (безопасные отказы/год).
- Логика. $\lambda_{sd} = 0.001$.
- Клапан. $\lambda_{sd} = 0.01$.

Вопрос. Какова частота ложных срабатываний (STR)?

Решение.

1. **Упрощенная формула STR для 2oo3.**

$$STR = 3 \cdot (\lambda_{sd, sensor})^2 \cdot MTTR + \lambda_{sd, logic} + \lambda_{sd, valve}.$$

(MTTR = время восстановления, пусть 8 часов ≈ 0.001 года).

2. **Расчет для датчиков.**

$$STR_{sensors} = 3 \cdot (0.005)^2 \cdot 0.001 = 7.5 \cdot 10^{-8}.$$

3. **Логика и клапан.**

$$STR_{total} = 7.5 \cdot 10^{-8} + 0.001 + 0.01 \approx 0.011 \text{ /год.}$$

Вывод. Основной вклад в ложные срабатывания вносит клапан.

Кейс 4.5 Влияние диагностического покрытия (DC).

Оценить влияние диагностики датчиков на надежность контрольно-измерительного прибора.

Ситуация. Рассматривается датчик системы противоаварийной защиты. Его надежность характеризуется интенсивностью отказов. Отказы бывают двух типов:

Обнаруживаемые (λ_{dd}) выявляет встроенная система диагностики.

Скрытые (λ_{du}) отказы остаются незамеченными до момента срабатывания системы.

Интенсивность отказов датчика: $\lambda_{du} = 0.001$ и $\lambda_{dd} = 0.009$. Нужно оценить влияние DC на PFD_{avg} .

Решение.

Цель диагностики превратить скрытые отказы в обнаруживаемые. Чем лучше диагностика, тем больше скрытых отказов она «видит».

Метрика эффективности диагностического покрытия (DC). Этот показатель отвечает на вопрос: «Какая доля всех опасных отказов будет своевременно обнаружена?» Исходная эффективность:

$$DC = \lambda_{dd} / (\lambda_{dd} + \lambda_{du}) = 0.009 / (0.009 + 0.001) = 90\%.$$

Без диагностики ($DC \approx 0\%$) все опасные отказы являются скрытыми. Если $DC = 0\%$, датчик согласно требованиям стандартов МЭК 61508/61511 может быть применен только в структурах СПАЗ ROUTE 1Н, которые реализуют низкий уровень полноты безопасности.

Для обеспечения высокой надежности блока измерения СПАЗ (например, SIL 2 или 3) применяют структурное резервирование (Route 2Н), которое предусматривает регулярную диагностику компонентов с последующей заменой.

С диагностикой ($DC > 90\%$) большинство отказов обнаруживается в реальном масштабе времени. Поэтому диагностику в СПАЗ можно считать «виртуальным резервированием», которая преобразует скрытые отказы в обнаруживаемые с заменой отказавшего компонента. Это обеспечивает датчику большую надежность, так как период его «необнаруженной неработоспособности» резко сокращается. Высокое DC является основанием для применения датчика в высоконадежных структурах СПАЗ Route 2Н.

Кейс 4.6.

Ситуация. На химическом заводе в СПАЗ датчики давления включены по схеме 1oo2 с диагностикой.

Выполнить верификацию блока измерения СПАЗ.

Исходные данные.

- Выбранная архитектура – 1oo2.
- Интенсивность отказов каждого датчика (λ): $\lambda_{total} = 0.0011$ в час (или ~ 0.009636 в год).

Из них.

- Обнаруживаемые опасные отказы (λ_{dd}) – 0.001 в час.
- Необнаруживаемые опасные отказы (λ_{du}) – 0.0001 в час.
- Степень диагностирования (Diagnostic Coverage, DC). Предположим, что $DC = 99\%$ (типичное значение для хорошей диагностики). *Это ключевое дополнение.*
 - Время восстановления (MTTR) – 8 часов (~ 0.000913 года).
 - Интервал тестирования (T_1) – 1 год.
 - Время проверки диагностики (T_{cycle}). Для простоты примем, что диагностика работает непрерывно, поэтому T_{cycle} стремится к 0, и время на обнаружение отказа равно MTTR. Бета- фактор β (общие отказы) не учитывается.

Резервирование с диагностикой обеспечивает эффективное применение ROUTE 2Н.

Метод ROUTE 2Н устанавливает требование использовать архитектуру HFT=1 (в частности, 1oo2) для достижения SIL 3. Особую роль в такой структуре играет диагностика.

Оценка надежности схемы блока измерения.

1. Расчет интенсивностей отказов с учетом DC.

Глубина диагностики определяет, какая часть необнаруженных отказов становится обнаружимой благодаря диагностике.

Реальные обнаруживаемые отказы.

$$\lambda_{dd\_eff} = \lambda_{dd} + (DC \times \lambda_{du}).$$

Реальные не обнаруживаемые отказы.

$$\lambda_{du\_eff} = (1 - DC) \times \lambda_{du}.$$

Подставляем значения ($DC = 99\% = 0.99$).

- $\lambda_{dd\_eff} = 0.001 + (0.99 \times 0.0001) = 0.001099$ в час.

- $\lambda_{du\_eff} = (1 - 0.99) \times 0.0001 = 0.000001$ в час (10^{-6}).

2. Расчет PFDavg для архитектуры 1oo2.

Формула расчета PFDavg архитектуры 1oo2 учитывает вклад как обнаружимых, так и необнаружимых отказов.

$$PFDavg \approx (\lambda_{du\_eff})^2 \times (T1)^2 / 3 + (\lambda_{du\_eff} \times \lambda_{dd\_eff} \times T1 \times MTTR) + (\lambda_{dd\_eff} \times T1 / 2).$$

Первый член – это вероятность необнаруженного опасного отказа СПАЗ/SIS.

Второй член – вероятность возникновения второго необнаруженного отказа во время ремонта обнаруженного отказа.

Третий член – вероятность систематического отказа.

Однако для простоты и учитывая, что

$\lambda_{dd\_eff} \times MTTR$ очень мала, часто используют упрощенную формулу.

$$PFDavg \approx (\lambda_{du\_eff} \times T1)^2 / 3 + (\lambda_{dd\_eff} \times MTTR).$$

Первое слагаемое (вклад необнаружимых отказов):

$$(0.000001 \times 8760)^2 / 3 \text{ (переводим часы в год. 1 год = 8760 часов)} \\ = (0.00876)^2 / 3 = 0.0000767 / 3 \approx 0.00002557.$$

Второе слагаемое (вклад обнаружимых во время ремонта отказов):

$$0.001099 \times 8 \approx 0.008792.$$

Суммарная вероятность отказа СПАЗ

$$PFDavg \approx 0.00002557 + 0.008792 = 0.0088176.$$

Это значение ($\sim 8.8E-03$) не соответствует SIL 3 (требуется $PFDavg < 10^{-3}$), а соответствует только SIL 2 ($10^{-2} > PFDavg \geq 10^{-3}$).

Однако выполненный расчет вызывает сомнения.

В представленном решении использовалась гибридная и некорректная формула.

$$PFDavg \approx (\lambda_{du\_eff} \times T1)^2 / 3 + (\lambda_{dd\_eff} \times MTTR).$$

Почему это ошибка?

Первое слагаемое $(\lambda_{du\_eff} \times T1)^2 / 3$ – **это верно**. Оно описывает вероятность того, что *оба* датчика одновременно потерпят необнаруживаемый опасный отказ в течение интервала тестирования.

Второе слагаемое $(\lambda_{dd\_eff} \times MTTR)$ – **неверно**. Оно пытается описать вклад *обнаружимых отказов*, но делает это неправильно.

Другая логика для обнаружимых отказов (λ_{dd}) в архитектуре 1oo2.

Система 1oo2 откажет (не сработает по требованию) только если оба датчика откажут одновременно. Однако, если один датчик имеет обнаруживаемый опасный отказ (λ_{dd}), его почти сразу же обнаружит диагностика (в среднем за время MTTR), и его заменят или починят.

Второе слагаемое расчетной формулы PFDavg может быть уточнено.

Оно должно учитывать вероятность совпадения двух событий.

1. Отказ первого датчика (обнаруживаемый).
2. Отказ второго датчика в течение времени восстановления первого.

Тогда формула принимает вид:

$$(\lambda_{dd\_1} \times MTTR) \times (\lambda_{du\_2} \times \lambda_{dd\_2}) \times MTTR.$$

Так как датчики идентичны, её упрощают.

Упрощённая формула для PFDavg системы 1oo2 (для идентичных каналов).

$$PFDavg \approx (\lambda_{du} \times T1)^2 / 3 + (\lambda_{dd} \times MTTR)^2 + (\lambda_{du} \times \lambda_{dd} \times T1 \times MTTR).$$

Но из-за того что MTTR очень мала, а λ_{dd} велика, то используют более практичную и правильную формулу из стандартов (МЭК 61508-6).

$$PFDavg \approx (\lambda_{du} \times T1)^2 / 3 + (\lambda_{dd} \times MTTR) \times (\lambda \times MTTR),$$

где $\lambda = \lambda_{du} + \lambda_{dd}$ (общая интенсивность отказов канала). Эта формула лучше отражает физический смысл.

Вот объяснение роли диагностики в схеме 1oo2 на примере. Представьте, что это не датчики, а два охранника с рациями (диагностика) на вышке (1oo2). Они должны заметить опасность и нажать кнопку тревоги.

- λ_{du} – это вероятность, что охранник уснёт и его рация отключится (никто не узнает, что он спит).

- λ_{dd} – это вероятность, что у охранника сломается рация (он сразу крикнет об этом напарнику).

- **MTTR** – время, за которое заменят охранника со сломанной рацией.

- **T1** – время одной смены.

Система не сработает (опасный отказ), если:

1. **Сценарий 1 (Тихий час?).** Оба охранника засыпают одновременно $(\lambda_{du} \times T1)^2 / 3$. Это маловероятно.

2. Сценарий 2 (Неустранённая поломка). У одного охранника ломается рация (λ_{dd}). Пока бегут на замену (MTTR), его *напарник тоже выходит из строя* ($\lambda \times \text{MTTR}$). Вот именно вероятность этого события ($\lambda_{dd} \times \text{MTTR}$) $\times$ ($\lambda \times \text{MTTR}$) и была упущена в первоначальном решении. Это и есть ключ уточнения расчета.

Уточненный расчет надежности схемы.

1. **Дано:**

– $\lambda_{du} = 0.0001$ /час.

– $\lambda_{dd} = 0.001$ /час.

– Если $DC = 0.99$, то $\lambda_{du\_eff} = (1 - DC) \times \lambda_{du} = 0.000001$ /час и $\lambda_{dd\_eff} = \lambda_{dd} + (DC \times \lambda_{du}) = 0.001 + 0.000099 = 0.001099$ /час

– $\text{MTTR} = 8$ час

– $T1 = 8760$ час (1 год)

$\lambda_{eff} = \lambda_{du\_eff} + \lambda_{dd\_eff} \approx 0.0011$ /час (пренебрегаем малой λ_{du_eff})

2. **Расчёт PFDavg по откорректированной формуле.**
 $\text{PFDavg}_{1002} \approx (\lambda_{du\_eff} \times T1)^2 / 3 + (\lambda_{dd\_eff} \times \text{MTTR}) \times (\lambda_{eff} \times \text{MTTR})$.

Слагаемое 1. (Необнаружимые отказы). $(0.000001 \times 8760)^2 / 3 = (0.00876)^2 / 3 \approx 2.56\text{e-}05$

Слагаемое 2. (Обнаружимые отказы). $(0.001099 \times 8) \times (0.0011 \times 8) = (0.008792) \times (0.0088) \approx 7.74\text{e-}05$.

Итого. $\text{PFDavg} \approx 2.56\text{e-}05 + 7.74\text{e-}05 = 0.000103 \approx 1.03\text{e-}04$

3. **Вывод.**

PFDavg = 1.03e-04 что меньше **1e-03** (граница SIL 3). Значит, система **соответствует SIL 3** по надёжности.

Изначальная ошибка в формуле привела к сильному завышению оценки PFDavg (получили 0.0088 вместо реальных 0.000103). Из-за этого делался неверный вывод, что система не соответствует SIL 3. Правильный расчёт показывает, что система с диагностикой и архитектурой 1002 – мощный инструмент для достижения высоких уровней SIL без избыточного усложнения.

Кейс 4.7. Выбор метода расчета надежности СПАЗ между ROUTE 1Н и ROUTE 2Н.

Ситуация. Инженер проектирует СПАЗ/SIS для насосной станции. Он не уверен, какой метод расчета надежности применить.

Задача. Выбрать метод расчета.

Критерии выбора.

1. **ROUTE 1Н**, если.

- Нет резервирования (архитектура 1001),
- Нет данных по диагностике (DC неизвестно).

2. **ROUTE 2Н**, если.

- Есть резервирование (напр., 1002),

- Если В СПАЗ используются программируемые компоненты.

- Известны λ_{dd} и MTTR.

Пример.

- Для одиночного клапана без диагностики → ROUTE 1Н.
- Для двух датчиков температуры с HART-диагностикой → ROUTE 2Н.

Кейс 4.8. Учет общих причин отказов (CCF).

Будет ли резервированная система соответствовать по надежности с учетом общих причин отказов?

Исходные данные.

- Архитектура. 1oo2.
- Интенсивность отказов каждого датчика.
 - $\lambda_{total} = 0.0011$ в час.
 - $\lambda_{dd} = 0.001$ в час (обнаруживаемые опасные отказы).
 - $\lambda_{du} = 0.0001$ в час (необнаруживаемые опасные отказы).
- Степень диагностирования (DC) = 99% = 0.99.
- Время восстановления (MTTR) = 8 часов.
- Интервал тестирования (T1) = 1 год = 8760 часов.
- β -фактор для общих причин отказов = 5% = 0.05.

Расчет эффективных интенсивностей отказов после диагностики.

- $\lambda_{du\_eff} = (1 - DC) \times \lambda_{du} = (1 - 0.99) \times 0.0001 = 0.000001$ в час.
- $\lambda_{dd\_eff} = \lambda_{dd} + (DC \times \lambda_{du}) = 0.001 + (0.99 \times 0.0001) = 0.001099$ в час.

Формула для PFDavg с учетом CCF.

$$PFD_{avg} \approx (1-\beta)^2 \times (\lambda_{du\_eff} \times T1)^2 / 3 + \beta \times \lambda_{du\_eff} \times T1 / 2 + (1-\beta)^2 \times (\lambda_{dd\_eff} \times MTTR)^2 + \beta \times \lambda_{dd\_eff} \times MTTR.$$

Расчет каждого слагаемого.

1. Независимые необнаруживаемые отказы.

$$A = (1-0.05)^2 \times (0.000001 \times 8760)^2 / 3 = (0.95)^2 \times (0.00876)^2 / 3 = 0.9025 \times 0.0000767376 / 3 \approx 0.000023087.$$

2. Общие необнаруживаемые отказы.

$$B = 0.05 \times 0.000001 \times 8760 / 2 = 0.05 \times 0.00876 / 2 \approx 0.000219.$$

3. Независимые обнаруживаемые отказы.

$$C = (1-0.05)^2 \times (0.001099 \times 8)^2 = (0.95)^2 \times (0.008792)^2 = 0.9025 \times 0.000077299264 \approx 0.00006974.$$

4. Общие обнаруживаемые отказы.

$$D = 0.05 \times 0.001099 \times 8 \approx 0.0004396.$$

Суммарный PFDavg.

$$PFD_{avg} = A + B + C + D \approx 0.000023087 + 0.000219 + 0.00006974 + 0.0004396 \approx 0.000751427.$$

Вывод.

$PFD_{avg} \approx 7.51 \times 10^{-4}$, что меньше требуемого значения для SIL 3 (10^{-3}). Таким образом, система соответствует уровню SIL 3 по надежности, даже с учетом общих причин отказов.

Дополнительные замечания.

Частота ложных срабатываний (STR) для системы 1002 с диагностикой рассчитывается как $STR = 2 \lambda_{sd}$ (упрощенная формула ISA TR84). В данном случае λ_{sd} не учитывается, но обычно она есть в данных о отказах. Если предположить, что $\lambda_{sd} = 0$ (все отказы опасные), то $STR = 0$. Однако, на практике кроме безопасных отказов могут присутствовать детектируемые опасные отказы, и их нужно учитывать.

Для частоты ложных срабатываний полное уравнение для 1002 выглядит следующим образом:

$$STR = [2(\lambda^s + \lambda^{DD})] + [\beta(\lambda^s + \lambda^{DD})] + \lambda_r^s$$

Первый член содержит отказы, связанные с обнаружением устройством опасного отказа, приводящего к переходу логики в состояние отключения, или безопасного отказа. Из-за опасений ложных срабатываний многие пользователи предпочитают отключать обнаруженный отказ устройства из панели управления. Это переводит логику в режим «1001» для оставшегося устройства до начала ремонта. При использовании такого типа логики вклад опасного обнаруженного отказа в частоту ложных отказов можно считать равным нулю.

Второй член – это член общей причины, а третий – систематическая интенсивность отказов. Эффективное проектирование и продуманные инженерные методы должны минимизировать оба этих члена.

Меры для повышения отказоустойчивости без снижения отказобезопасности включают использование датчиков с более высокой диагностикой (увеличение DC), уменьшение MTTR за счет улучшения процедур обслуживания, или применение архитектуры 2003, которая может снизить PFD_{avg} без значительного увеличения STR.

Чтобы снизить β -фактор, необходимо разнести датчики физически (установить в разные места, на разные импульсные линии), использовать датчики разного принципа действия (например, мембранный, пьезоэлектрический и резонансный) или от разных производителей. Это снижает вероятность того, что одна и та же причина (вибрация, загрязнение, влажность, ошибка КИПиА выведет их всех из строя одновременно.

4.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 4.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 4. 1. Определение уровня SIL для нерезервированной системы (1oo1).

Ситуация.

Оборудование.

1 датчик (архитектура **1oo1**), сертифицирован для **SIL 3**.

Выполняется проверка. один раз в 5 лет, но диагностический охват тестов – 90%.

Нет автоматического отключения при отказе, но есть сигнализация.

Исходные данные.

- $\lambda_{DD} = 950 \text{ FIT}$ (обнаруживаемые отказы).
- $\lambda_{DU} = 450 \text{ FIT}$ (необнаруживаемые отказы).

Вопрос 1. Какая архитектура используется в системе?

- A) 1oo2.
- B) 1oo1.
- C) 2oo2.
- D) 2oo1.

Ответ В. Система нерезервированная, только 1 датчик.

Вопрос 2. Чему равна λ_{DD} ?

- A) 450 FIT
- B) 950 FIT
- C) $4,5 \times 10^{-7}$.
- D) $9,5 \times 10^{-7}$.

Ответ В.

Вопрос 3. Чему равна λ_{DU} ?

- 950 FIT.
- 450 FIT (Правильно $450 \text{ FIT} = 4,5 \times 10^{-7} \text{ отказов/час}$).
- $4,5 \times 10^{-7}$.
- $9,5 \times 10^{-7}$.

Ответ В.

Вопрос 4. Какова вероятность отказа по требованию (PIF)?

- A) 0,1.
- B) 0.
- C) 0,9.
- D) 1.

Ответ В.

Вопрос 5. Какой уровень SIL у системы?

- A) SIL 1
- B) SIL 2.
- C) SIL 3.
- D) SIL 4.

Ответ А. $PFD_{avg} \approx 0,0129 \cdot 10^{-2}$

Объяснение.

PFD_{avg} рассчитывается по формуле.

$$PFD_{avg} = \lambda_{DD} \cdot MRT_{DD} + CPT \cdot \lambda_{DU} \cdot TI/2 + (1 - CPT) \cdot \lambda_{DU} \cdot MT/2.$$

Подставляем значения.

- $\lambda_{DD}=950 \times 10^{-9}$, $MRT_{DD}=96$ часов,
- $CPT=0.9$, $TI=5$ лет, (Mission Time) $MT=20$ лет.

Итог. $PFD_{avg} \approx 0,0129 \rightarrow SIL\ 1$ (по таблице МЭК 61508).

Вывод. Даже при сертификации датчика SIL 3, из-за отсутствия резервирования (1oo1) и редких проверок система соответствует только SIL 1.

Тест 4. 2. Расчет надежности для SIF с резервированием.

Условие. Дана система СПАЗ/SIS с двумя датчиками давления (1oo2), логическим реле и клапаном.

- Датчики. $\lambda_{du} = 0.001$ (опасные необнаруженные отказы/год), $\lambda_{sd} = 0.01$ (безопасные обнаруженные/год).
- Логика. $\lambda_{du} = 0.0005$, $\lambda_{sd} = 0.005$.
- Клапан. $\lambda_{du} = 0.002$, $\lambda_{sd} = 0.02$.
- Период тестирования ($T1$). 1 год.

Вопрос 1. Рассчитайте PFD_{avg} для этой конфигурации.

Решение.

Упрощенная формула PFD_{avg} для резервирования датчиков 1oo2.

$$PFD_{avg} \approx (\lambda_{du} \cdot TI)^2 / 3 + \lambda_{du,logic} \cdot TI / 2 + \lambda_{du,valve} \cdot TI / 2.$$

Расчет для датчиков.

$$PFD_{sensors} = (0.001 \cdot 1)^2 / 3 = 3.33 \cdot 10^{-7}.$$

Логика и клапан (без резервирования).

$$PFD_{logic} = 0.0005 \cdot 1 / 2 = 2.5 \cdot 10^{-4}.$$

$$PFD_{valve} = 0.002 \cdot 1 / 2 = 0.001.$$

Суммарный PFD_{avg} .

$$PFD_{total} = 3.33 \cdot 10^{-7} + 2.5 \cdot 10^{-4} + 0.001 \approx 0.00125 \text{ (SIL1)}.$$

Вывод. Система соответствует SIL 1. Основной вклад в низкий уровень отказобезопасности вносит клапан.

Вопрос 2. Расчет STR для системы с резервированием 2oo3.

Условие.

Три датчика температуры в конфигурации 2oo3.

- $\lambda_{sd} = 0.005$ (безопасные отказы/год).
- Логика. $\lambda_{sd} = 0.001$.
- Клапан. $\lambda_{sd} = 0.01$.

Какова частота ложных срабатываний (STR)?

Решение.

Упрощенная формула STR для 2oo3.

$$STR = 3 \cdot (\lambda_{sd\_sensor})^2 \cdot MTTR + \lambda_{sd\_logic} + \lambda_{sd\_valve}.$$

($MTTR$ = время восстановления, пусть 8 часов ≈ 0.001 года).

Расчет для датчиков.

$$STR_{sensors} = 3 \cdot (0.005)^2 \cdot 0.001 = 7.5 \cdot 10^{-8}.$$

Логика и клапан.

$$STR_{total} = 7.5 \cdot 10^{-8} + 0.001 + 0.01 \approx 0.011 \text{ /год.}$$

Расчеты показывают, что использование 2oo3 для датчиков создает в сравнении со структурой 1oo2 еще более низкую вероятность ложного срабатывания, так как требуется, чтобы как минимум два из трех датчиков дали ложный сигнал одновременно.

Однако основной вклад в ложные срабатывания (отказоустойчивость) по-прежнему вносит клапан. В результате, не смотря на резервирование датчиков, полнота безопасности СПАЗ находится в пределах SIL1.

Тест 4. 3. Анализ отказоустойчивости и отказобезопасности.

Условие.

- СПАЗ/SIS с конфигурацией 1oo1 (один датчик, один клапан).
- $\lambda_{du} = 0.01$, $\lambda_{sd} = 0.05$.

Вопрос 1. Какова вероятность опасного отказа (PFD_{avg})?

Ответ $PFD_{avg} = \lambda_{du} \cdot T / 2 = 0.01 \cdot 0.5 = 0.005$ (SIL2).

Вопрос 2. Какова частота ложных срабатываний (STR)?

$STR = \lambda_{sd} = 0.05$ /год.

Вопрос 3. Какие меры повысят надежность СПАЗ?

Меры:

- Переход на 1oo2 для датчиков снизит PFD, но примерно вдвое увеличится STR.
- Использование датчиков с диагностикой уменьшит λ_{du} .

Тест 4.4. Расчет общей частоты отказов ПЛК (λ_{SF}).

Ситуация. ПЛК имеет:

- 3 аналоговых модулей ввода,
- 1 аналоговый модуль вывода,
- 1 процессор,
- 2 дискретных модулей вывода.

Оценить надежность ПЛК в составе процессорного модуля, дискретного ввода и модулей ввода/вывода. Для расчетов использовать обозначения, приведённые в таблице 4.1 и показатели надежности модулей в FIT.

- Модуль аналогового ввода: $\lambda_{DU} = 38$ FIT.
- Модуль аналогового вывода: $\lambda_{DU} = 250$ FIT.
- Модуль дискретного вывода: $\lambda_{DU} = 75$ FIT.
- Модуль дискретного ввода: $\lambda_{DU} = 125$ FIT.
- Процессор. $\lambda_{DU} = 1,500$ FIT.

Таблица 4.1 Обозначения формулы расчета общей интенсивности отказов ПЛК λ_{SF} .

Обозначение в формуле	Что это на простом языке?	Пояснение
λAI	Частота отказов одного модуля аналогового ввода	Это интенсивность отказов аналогового модуля, которая берется из паспорта или справочника на конкретный модуль. Показывает, как часто он в среднем выходит из строя (опасным образом).
λAO	Частота отказов одного модуля аналогового вывода	
λDI	Частота отказов одного модуля дискретного ввода	Это интенсивность отказов дискретного модуля, которая берется из паспорта или справочника на конкретный модуль. Показывает, как часто он в среднем выходит из строя (опасным образом).
λDO	Частота отказов одного модуля дискретного вывода	
λMP	Частота отказов процессора (CPU)	Это отказ процессорного модуля ПЛК. В формуле он один, так как обычно есть один основной процессор (даже в резервированных системах часто считается как единый логический элемент).
n, m, l, k	Число модулей аналогового ввода/вывода, дискретного ввода/вывода.	

Вопрос 1. Как рассчитать λSF по формуле?

- A) $\lambda SF = n \cdot \lambda AI + k \cdot \lambda MP + l \cdot \lambda DO$.
- B) $\lambda SF = n \cdot \lambda AI + m \cdot \lambda AO + \lambda MP + l \cdot \lambda DI + k \cdot \lambda DI$.
- C) $\lambda SF = \lambda MP + n + m + mOC$.
- D) $\lambda SF = n \cdot \lambda AO + l \cdot \lambda IP + m \cdot \lambda DI + \lambda MP$.

Ответ В. Правильная формула.

Вопрос 2. Что означает $n \cdot \lambda AI$?

- A) Количество выходных каналов.
- B) Количество входных каналов.
- C) Количество модулей аналогового ввода.
- D) Количество модулей аналогового вывода.

Ответ D. 1 аналоговый выход.

Вопрос 3. Какую роль играет λMP ?

- A) Интенсивность отказов модулей ввода.
- B) Интенсивность отказов процессора.
- C) Интенсивность отказов выходных каналов.

Д) Общая интенсивность отказов.

Ответ В. Интенсивность отказов процессора $\lambda_{MP} = 1,500 \text{ FIT}$.

Вопрос 4. Как рассчитать λ_{SF} для данной системы?

А) Неопределенно.

В) 0.

С) сложить все отказы

Д) 1.

Ответ С. Нужно сложить все отказы.

Вывод.

Расчетная интенсивность отказов ПЛК .

$$\lambda_{СПАЗ/SIS} = 3 \cdot 38 + 1 \cdot 250 + 1 \cdot 1,500 + 1 \cdot 125 + 2 \cdot 75 = 18,705 \text{ FIT}$$
$$3 \cdot 38 + 1 \cdot 250 + 1 \cdot 1,500 + 1 \cdot 125 + 2 \cdot 75 = 18,705 \text{ FIT}$$

Итог. Общая частота отказов ПЛК = 18,705 FIT

Для повышения надежности можно добавить **резервирование** или улучшить диагностику.

Тест 4.5. Влияние диагностического покрытия (DC) на PFD_{avg} .

Ситуация. Датчик с $\lambda_{DU} = 0,001$, $\lambda_{DD} = 0,009$.

Вопрос 1. Как рассчитать DC?

А) $DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$.

В) $DC = \lambda_{DU} / (\lambda_{DD} + \lambda_{DU})$.

С) $DC = \lambda_{DD} / \lambda_{DU}$.

Д) $DC = 1 - \lambda_{DU}$.

Ответ А. $DC = 0,009 / (0,009 + 0,001) = 90\%$.

Вопрос 2. Что дает высокий диагностический охват DC?

А) Уменьшает PFD_{avg} .

В) Увеличивает λ_{DU} .

С) Не влияет на надежность.

Д) Требуется резервирования.

Ответ А. Чем выше DC, тем меньше необнаруженных отказов.

Вывод. DC = 90% означает, что система включения датчика в СПАЗ/SIS надежная, но для SIL 3 нужно резервирование.

1. PFD_{avg} зависит от следующего:

- Архитектуры (1oo1 1oo2),
- Диагностики (DC),
- Периода проверок (TI).

2. λ_{SF} – интенсивность отказов ПЛК.

3. SIL системы может быть ниже, чем SIL компонентов, из-за плохой архитектуры.

4.4 ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 4.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 4».

Тест 4.5.

Для верификации SIF требуется входная переменная «Время миссии» (Mission Time). Также важно проверить срок службы (Useful Life) всех компонентов, чтобы установить план замены/восстановления. В чем разница между «Временем миссии» и «Сроком службы»?

Вопрос 1. Что означает термин «Время миссии» (Mission Time)?

А) Время, в течение которого система должна функционировать без сбоев.

В) Время, необходимое для установки системы.

С) Общее время, в течение которого система была в эксплуатации.

Д) Время, необходимое для обслуживания системы.

Вопрос 2. Каково значение термина «Срок службы» (Useful Life)?

А) Максимальное время, в течение которого компонент может функционировать эффективно.

В) Время, в течение которого система была в эксплуатации.

С) Время, необходимое для установки системы.

Д) Время, в течение которого система должна функционировать без сбоев.

Вопрос 3. Почему важно учитывать оба показателя при верификации SIF?

А) Для оценки стоимости системы.

В) Для определения надежности и планирования обслуживания.

С) Для оценки производительности системы.

Д) Для определения времени установки.

Вопросы для самопроверки.

а) Почему в расчете PFD_{avg} для резервированных компонентов используется квадрат λ_{du} ?

б) Как конфигурация 2oo3 влияет на PFD_{avg} и STR по сравнению с 1oo2?

с) Какие компоненты СПАЗ/SIS обычно вносят наибольший вклад в STR?

Тест 4.6. Бросаются три игральных кубика. Рассмотрите сумму чисел, выпавших на трех кубиках.

Определите вероятность того, что сумма составит 3 или 5.

Выбрать правильный ответ.

Вопрос 1.

Какова вероятность того, что сумма чисел на трех игральных кубиках составит 3?

А) 1/216.

В) 1/36.

С) 1/6.

Д) 1/108.

Вопрос 2.

Какова вероятность того, что сумма чисел на трех игральных кубиках составит 5?

- A) $3/216$.
- B) $1/36$.
- C) $5/216$.
- D) $10/216$.

Тест 4.7. При рассмотрении событий и их комбинаций для анализа их вероятностей события считаются зависимыми и независимыми, а группы событий – взаимоисключающими, не взаимоисключающими или дополнительными.

С точки зрения зависимости/независимости и взаимоисключаемости *опишите* допущения, сделанные относительно отказов компонентов СПАЗ/SIS при проведении анализа надежности. Выбрать правильные ответы.

Вопрос 1. Какое из следующих утверждений верно для независимых событий в контексте отказов компонентов СПАЗ/SIS?

- A) Отказ одного компонента влияет на вероятность отказа другого компонента.
- B) Отказ одного компонента не влияет на вероятность отказа другого компонента.
- C) Все компоненты СПАЗ/SIS всегда работают одновременно.
- D) Отказ одного компонента всегда приводит к отказу системы.

Вопрос 2. Какое из следующих утверждений верно для зависимых событий в контексте отказов компонентов СПАЗ/SIS?

- A) Все события происходят независимо друг от друга.
- B) Вероятность отказа одного компонента изменяется в зависимости от состояния другого компонента.
- C) Все компоненты имеют одинаковую вероятность отказа.
- D) Отказы компонентов не имеют влияния на систему в целом.

Вопрос 3. Что такое взаимоисключающие события в контексте отказов компонентов СПАЗ/SIS?

- A) События, которые могут произойти одновременно.
- B) События, которые не могут произойти одновременно.
- C) События, которые зависят друг от друга.
- D) События, которые имеют одинаковую вероятность.

Вопрос 4. Какое из следующих утверждений верно для дополнительных событий в контексте отказов компонентов СПАЗ/SIS?

Выбрать правильный ответ

- A) Они могут произойти одновременно.
- B) В случае одного события вероятность другого события равна нулю.
- C) Сумма вероятностей дополнительных событий равна 1.
- D) Они зависят друг от друга.

Тест 4.8. Датчик имеет постоянную интенсивность отказов 9×10^{-7} отказов в час в течение срока службы.

а) Рассчитайте среднее время наработки на отказ (MTTF) передатчика в годах в течение срока службы.

б) Рассчитайте вероятность того, что данный передатчик проработает три года без отказов.

Вопрос 1. Какое среднее время наработки на отказ (MTTF) передатчика в годах, если интенсивность отказов составляет 9×10^{-7} отказов в час?

Выбрать правильный ответ.

A) 1.14 года.

B) 5.68 года.

C) 10.34 года.

D) 2.52 года.

Тест 4.9. Рассчитайте надежность системы печи за пятилетний период.

Для работы печи необходима работа одного из двух вентиляторов с вероятностью надежной работы $R=0,95$ каждый, горелки с вероятностью надежной работы $R=0,97$ и системы управления с вероятностью надежной работы $R=0,8$.

Вопрос 1.

Какова общая надежность системы печи за пятилетний период, если для работы печи необходима работа одного из двух вентиляторов, горелки и системы управления? Вероятности надежной работы следующие:

- Вентиляторы. $R_1 = 0.95$ (каждый).

- Горелки. $R_2 = 0.97$.

- Система управления. $R_3 = 0.80$.

Выбрать правильный ответ:

A) 0.95.

B) 0.97.

C) 0.80.

D) 0.776.

5. АНАЛИЗ РИСКОВ

5.1. КЛЮЧЕВЫЕ ПРИНЦИПЫ АНАЛИЗА РИСКОВ.

Задание 5.1. Уяснить ключевые принципы рисков опасностей ОПО и СПАЗ и систем приборной безопасности.

Риск – это не физический параметр. Представьте, что вам дали задание. «*Измерить риск взрыва на химическом заводе в килограммах*». Абсурдно? Именно! Риск нельзя выразить в единицах массы, напряжения или других физических величин – но его можно системно оценить, сравнивая опасности между собой.

Почему анализ рисков – это сложно?

Субъективность оценки риска?

Да, тяжесть последствий зависит от контекста. Например, потеря пальца для пианиста критичнее, чем для программиста.

Динамичность факторов, ведущих к тяжелым последствиям риска.

Например, частота нахождения людей в опасной зоне (F) может меняться из-за смены графика работы или ремонта оборудования.

Базовые понятия.

Риск в СПАЗ/SIS – это сочетание двух факторов.

- **Вероятность** опасного события (например, разгерметизация реактора).

- **Серьезность последствий** (от финансовых потерь до катастрофы).

И на практике:

- Нет «абсолютных» единиц измерения риска (как кг или метры).
- Есть относительные критерии (стандарты, отраслевые нормы, корпоративные требования).

Пример.

Допустим, на производстве возможна утечка токсичного газа.

- **ОПО без СПАЗ/SIS.** Пусть риск неприемлем (вероятность 1 раз в 10 лет, но последствия – смертельные).

- **Пусть с использованием СПАЗ/SIS** приборная система безопасности снижает риск до допустимого (вероятность 1 раз в 10 000 лет).

Как оценивают риск и степень снижения риска?

Для оценки риска используется структурированный подход, который включает:

1. **Анализ опасностей (HAZOP, FMEA)** – выявляется, *что может пойти не так*.
2. **Оценку С/Е/Р (Consequence, Frequency, Probability of Avoidance).** Все без СПАЗ/SIS.
 - **С** – тяжесть последствий (по шкале стандарта).
 - **Е** – как часто люди/оборудование подвергаются опасности.

▪ **Р** – шанс избежать аварии (есть ли время на реакцию безопасности жизнедеятельности у работников?).

Алгоритм анализа рисков:

Шаг 1. Для объективной оценки используются эти три ключевые параметра:

• **С (Последствия)**, для оценки которых применяются стандартизированные шкалы (например, ГОСТ, смерть = 5 баллов, легкая травма = 2 балла»).

Пример. Ампутация руки – 4 балла, ожог 2-й степени – 3 балла.

• **F (Частота)**, для оценки которой используется периодичность нахождения в опасной зоне людей и оборудования. Эти сведения берутся обычно из таких источников опасных инцидентов, как журналы рабочего времени, данные хронометража доступа, статистика инцидентов.

Пример. Персонал находится в опасной зоне 3 раза в смену, что означает F = «высокая».

• **P (Вероятность избегания)**. Для оценки этого параметра риска, опираются на сведения о подготовленности персонала (ТБ) и исторические данные.

Пример. Только 60% работников успевают отключить оборудование за 1 минуту. Т.е. P = 0.6. Это низкая вероятность избежать опасность на ОПО без СПАЗ/SIS.

Шаг 2. Классифицируется риск.

Согласно части 3 статьи 2 ФЗ-116, опасные производственные объекты в зависимости от уровня потенциальной опасности аварий на них для жизненно важных интересов личности и общества подразделяются в соответствии с критериями, указанными в приложении 2 к настоящему Федеральному закону, на четыре класса опасности. Для оценки рисков ОПО используют матрицу рисков с цветовой кодировкой (например, **I – красный, IV – зеленый**).

Классы опасности опасных производственных объектов (табл.5.1).

Таблица 5.1

Класс опасности	Уровень опасности	Характеристика
I класс	Чрезвычайно высокая опасность	Объекты с максимальным уровнем потенциальной опасности аварий для жизни и общества
II класс	Высокая опасность	Объекты со значительным уровнем потенциальной опасности
III класс	Средняя опасность	Объекты с умеренным уровнем потенциальной опасности

Класс опасности	Уровень опасности	Характеристика
IV класс	Низкая опасность	Объекты с минимальным уровнем потенциальной опасности

Важно. Присвоение класса опасности (табл.5.2) опасному производственному объекту осуществляется при его регистрации в государственном реестре ОПО. Руководитель организации несет ответственность за полноту и достоверность предоставленных сведений.

Для ряда опасных производственных объектов класс опасности устанавливается не по опасности, а по специальным критериям, учитывающим специфику производственной деятельности.

Например, несмотря на отсутствие нормативного требования категоричности опасности для объектов нефтегазодобычи (ФНиП ОПВБ приказ №533), для установок бурения и добычи нефти, газа и газового конденсата класс опасности определяется содержанием сернистого водорода в продукции. И в этом случае в соответствии с (ФНиП ХОПО приказ №500) категория опасности ОПО нефтедобычи при содержании H_2S свыше 6% устанавливается II класс, от 1% до 6% - III класс, менее 1% - IV класс опасности.

Шаг 3. Установить требования промышленной безопасности по классам ОПО.

Таблица 5.2.

Требование	I класс	II класс	III класс	IV класс
Лицензия на эксплуатацию	Обязательна	Обязательна	Обязательна	Не требуется
Декларация промышленной безопасности	Обязательна	Обязательна	Не требуется	Не требуется
Система управления промышленной безопасностью	Обязательна	Обязательна	Не требуется	Не требуется
План мероприятий по локализации и ликвидации аварий (ПМЛА)	Обязателен	Обязателен	Обязателен	Обязателен
Положение о производственном контроле	Обязательно	Обязательно	Обязательно	Обязательно
Обязательное страхование	Обязательно	Обязательно	Обязательно	Обязательно
Аудит СПАЗ (с 01.09.2024)	Обязателен	Не требуется	Не требуется	Не требуется

Важно. С 1 сентября 2024 года введено обязательное требование проведения внешнего аудита системы управления промышленной безопасностью для организаций, эксплуатирующих ОПО I класса опасности. Это требование направлено на повышение эффективности СПАЗ на наиболее опасных объектах.

Шаг 4. Исходя из проверенной практикой вероятности потенциальной опасности ОПО, выполняется категоризация класса риска: «W3–неприемлемый риск», «W2–риск требует анализа» и «W1–риск приемлем». По результату анализа на диаграмме риска устанавливается потребность в уровне полноты безопасности SIL, которая должна быть реализована СПАЗ.

Шаг 5. Доказывается эффективность снижения риска за счет специальных слоев защиты СПАЗ.

Для этого применяют метод LOPA-анализ (оценка, как существующие меры снижают риск).

Пример последовательных слоев защиты: (слой 1) защита от дурака +(слой 2) немедленная остановка. В результате снижается риск на 90%.

С 1 сентября 2025 года вступила в силу новая редакция ФЗ-116 (в редакции от 08.08.2024), которая предусматривает дополнительные изменения в системе регулирования промышленной безопасности, включая новые подходы к профилактическим мероприятиям и консультированию.

Типичные ошибки в анализе.

1. Миф. «Сигнализация это уже СПАЗ».

Реальность. СПАЗ требует автоматического действия (например, отключение питания). Сигнализация без реакции – лишь «слой защиты».

2. Ловушка. Игнорирование человеческого фактора.

Пример. Если персонал не использует средства индивидуальной защиты, то вероятность травмы (Р) становится **1**, даже при идеальной технике.

5.2. ПРАКТИКУМ ПО ПРИМЕНЕНИЮ АНАЛИЗА РИСКОВ В СПАЗ.

Задание 5.2. С поддержкой AI (типа GPT) подготовить свои решения кейсов и объяснения для одного или 2-х кейсов. Сделать вывод о правильности и качестве предложенных ответов и объяснений в кейсах.

Кейс 5.1. Нужен ли СПАЗ/SIS для защиты от перегрева реактора?

На химическом заводе есть риск перегрева реактора.

Известно.

C = 4 – последствия. разрушение оборудования и травмы (высокая тяжесть).

F = 2 – частота воздействия. персонал проверяет реактор раз в смену (что означает регулярное присутствие людей в зоне риска).

P = 0.5 – вероятность того, что существующие меры защиты не сработают (исходно есть аварийная кнопка, но медленная реакция).

Задача. Определить, требуется ли система аварийной защиты СПАЗ/SIS для снижения риска до приемлемого уровня.

Решение.

Шаг 1. Оценка класса риска исходной ситуации.

В упрощенных методах анализа риска (например, с использованием матрицы рисков) класс риска определяется на основе комбинации C, F и P. Обычно:

- **Класс I.** Это неприемлемый риск – требуется немедленное внедрение дополнительных мер (например, СПАЗ/SIS).

- **Класс II.** Этот риск требует анализа – необходимо оценить существующие меры и возможно внедрить улучшения.

- **Класс III.** Этот риск приемлем – дополнительные меры не требуются.

Исходные значения. C=4, F=2, P=0.5.

- Опасные последствия (C=4) и средняя частота возникновения опасности (F=2) уже указывают на потенциально высокий риск.

- Вероятность не успеть выйти из опасной зоны (P=0.5) означает, что в 50% случаев авария приведет к тяжелым последствиям.

- Комбинация этих факторов дает класс риска II – риск требует анализа. Это означает, что текущая ситуация небезопасна, но не критична, и нужно изучить, можно ли снизить риск за счет других мер (не обязательно СПАЗ/SIS).

Шаг 2. Учет существующих мер защиты.

Предложены две меры.

1. **Обучение персонала** – улучшает реакцию персонала на аварийную ситуацию. Исходная вероятность неправильных действий работника P=0.5. После обучения эта вероятность снижается до 0.3. Это означает, что персонал лучше подготовлен, и шанс избежать опасности увеличивается (хотя P интерпретируется как вероятность неудачи, поэтому снижение P – это улучшение).

2. **Механический клапан** – устанавливается дополнительное физическое устройство с PFD = 0.1. Это означает, что клапан не сработает по требованию с вероятностью 10% (что соответствует уровню надежности SIL 1).

Как комбинируются меры?

Поскольку меры независимы, общая вероятность того, что защита не сработает (P_{total}), рассчитывается как произведение вероятностей неудачи каждой меры (каждого слоя защиты).

- После обучения. P_{learning} = 0.3.

- После установки клапана. P_{valve} = PFD = 0.1.

- **Итоговая P_{total} = P_{learning} × P_{valve} = 0.3 × 0.1 = 0.03.**

Таким образом, общая вероятность отказа защиты снижается до 0.03 (3%).

Шаг 3. Пересчет класса риска после выполненных мер снижения риска опасности. Новые параметры: $C=4$, $F=2$, $P=0.03$. В результате:

- C и F остаются неизменными, но P значительно снизилась.
- По матрице рисков. комбинация $C=4$, $F=2$, $P=0.03$ соответствует классу риска III, что означает «риск приемлем» и дополнительных мер защиты (таких как СПАЗ/SIS) не требуется.

Вывод. СПАЗ/SIS не нужна, при условии, что внедрены обучение персонала и механический клапан.

Ответ на вопрос: действия клапана определяются ESD или СПАЗ/SIS?

- **ESD (Emergency Shutdown System)** – это система аварийной остановки, которая может быть частью СПАЗ/SIS или самостоятельной системой защиты ESD.

- **СПАЗ/SIS** – это более широкое понятие, включающее датчики, логический решатель и исполнительные механизмы (например клапаны) для выполнения функций безопасности. СПАЗ/SIS имеет определенные уровни надежности (SIL).

В данном кейсе механический клапан с $PFD=0.1$, вероятно, является автономным устройством, например, предохранительным или термозапорным клапаном, который срабатывает непосредственно от температуры или давления (без электронного управления). Такой клапан не управляется ни **ESD**, ни **СПАЗ/SIS** – он работает по принципу прямой физической связи (например, плавкая вставка или пружинный механизм).

Это собственная мера защиты ОПО, которая не требует сложной электроники и соответствует уровню SIL 1, но она не является частью СПАЗ/SIS, так как СПАЗ/SIS подразумевает программно-аппаратную систему с диагностикой и резервированием.

Не все меры безопасности должны быть реализованы через СПАЗ/SIS. Существуют разные слои защиты (например, механические устройства, обучение персонала, процедуры).

В данном случае, автономный механический клапан – это простой и надежный способ снизить риск без затрат на СПАЗ/SIS.

Заключение.

- Упрощенные методы анализа риска (оценка класса риска) полезны для быстрой оценки, но они должны применяться с пониманием контекста. Всегда учитывайте, что параметры, подобные P в диаграмме риска, могут интерпретироваться как вероятность неудачи защиты.

- Решение не применять СПАЗ/SIS основано на том, что комбинация обучения и механического клапана снижает риск до приемлемого уровня. Однако необходимо обеспечить, чтобы эти меры были

реализованы и поддерживались (например, регулярной проверкой клапана, повторным обучением персонала).

- Если бы риск остался классом II или I, то потребовалась бы СПАЗ/SIS с соответствующим SIL (например, SIL 2 или выше).

Этот подход показывает, как инженеры балансируют между безопасностью и затратами, выбирая наиболее практичные решения.

Кейс 5.2. Отказы ОПО из-за человеческого фактора.

Задача. Ложные срабатывания клапана аварийного сброса происходят из-за:

- Неправильной калибровки (вероятность = 0.3).
- Игнорирования предупреждений (вероятность = 0.2).
- Использования неподходящего инструмента (вероятность = 0.1).

Вопросы.

1. Построить дерево отказов для сценария «Ложное срабатывание клапана».

2. Рассчитать общую вероятность опасного события.

3. Предложить меры для снижения вероятности.

Решение.

Вершина дерева (ТОР-событие) – это ложное срабатывание клапана аварийного сброса.

Тип логической связи событий: ИЛИ (достаточно одного события).

Базовые события:

V1: Неправильная калибровка ($P = 0.3$).

V2: Игнорирование предупреждений ($P = 0.2$).

V3: Использование неподходящего инструмента ($P = 0.1$).

Расчет общей вероятности.

Для независимых событий, связанных через логическое ИЛИ, общая вероятность рассчитывается по формуле:

$$P = P_1 + P_2 + P_3 - P_1 \times P_2 - P_1 \times P_3 - P_2 \times P_3 + P_1 \times P_2 \times P_3.$$

$$P = 0.3 + 0.2 + 0.1 - (0.3 \times 0.2) - (0.3 \times 0.1) - (0.2 \times 0.1) + (0.3 \times 0.2 \times 0.1).$$

$$P = 0.6 - 0.06 - 0.03 - 0.02 + 0.006.$$

$$P = 0.6 - 0.11 + 0.006 = 0.496.$$

Однако! Для событий с малыми вероятностями (обычно < 0.1) используется приближение:

$$P \approx P_1 + P_2 + P_3 = 0.3 + 0.2 + 0.1 = 0.6.$$

В данном случае вероятности достаточно велики, поэтому точный расчет дает $P = 0.496$, а приближенный - 0.6.

Для очень малых вероятностей (типичных для аппаратных отказов): $P \approx \sum P_i$.

Для вероятностей > 0.1 (типичных для человеческого фактора): нужно использовать точную формулу.

Корректировка мер для снижения вероятности ложного отказа, равной 0.496 (49.6%).

Предлагаемые меры:

- Автоматическая калибровка (снижение P1 с 0.3 до 0.05).
- Тренинги персонала (снижение P2 с 0.2 до 0.05).
- Стандартизация инструмента (снижение P3 с 0.1 до 0.02).

После внедрения мер:

$$P = 0.05 + 0.05 + 0.02 - (0.05 \times 0.05) - (0.05 \times 0.02) - (0.05 \times 0.02) + (0.05 \times 0.05 \times 0.02)$$

$P = 0.12 - 0.0025 - 0.001 - 0.001 + 0.00005 \approx 0.1155$ (11.55%) , что близко к упрощенному расчету 12%.

Кейс 5.4. Количественная оценка климатических рисков.

Задача. Температурный датчик (SIL 2) работает при -30°C (сертифицирован до -20°C).

- $\lambda_{DU} = 5 \times 10^{-6}/\text{час}$ (в норме).
- $TI = 1$ год.

Вопросы.

1. Пересчитать PFD_{avg} с учетом переохлаждения.
2. Соответствует ли система SIL 2?
3. Какой период TI сохранит SIL 2?

Расчеты и ответы.

Самая большая проблема – неизвестный характер зависимости λ_{DU} от температуры. Производитель редко предоставляет такие данные. Поэтому мы должны смоделировать эту зависимость, исходя из общих инженерных принципов. Могут использоваться 2 подхода:

Использование модельного коэффициента надежности Аррениуса для электронных компонентов.

Использование процентного подхода.

На практике более реалистичным является модель Аррениуса.

Пример расчета:

Снижение температуры: $\Delta T = T_{\text{реал}} - T_{\text{норм}} = -30^{\circ}\text{C} - (-20^{\circ}\text{C}) = -10^{\circ}\text{C}$.

Применяем правило: Ухудшение условий (в данном случае – экстремальное охлаждение) может приводить к росту интенсивности отказов. Примем, что при выходе за нижний эксплуатационный предел отказы растут с аналогичным темпом – в 2 раза на 10°C .

1. Тогда расчетное значение PFD_{avg} будет:

$\lambda_{DU\_новое} = 10 \times 10^{-6} PFD_{avg} = 10^{-5} \times 8760/2 = 4,38 \times 10^{-2}$, что превышает предел SIL 2.

2. Нет, только SIL 1.

3. Для SIL 2. $PFD_{avg} < 10^{-3} \rightarrow TI_{\text{max}} = 12/4,38 \approx 2,74$ месяца.

Для снижения риска.

(a) установить обогреваемый кожух,

(b) сократить TI до 3 месяцев,

(c) заменить датчик на морозостойкий (до -50°C).

Кейс 5.3. Оптимизация SIL через RRF.

Задача. Технологический процесс имеет:

- Риск взрыва без СПАЗ/SIS – 10^{-2} /год.
- Допустимый риск – 10^{-4} /год.
- Механические защиты снижают риск в 8 раз.

Вопросы.

1. Найти RRF для СПАЗ/SIS.
2. Определить PFDavg и SIL.
3. Что изменится, если механические защиты улучшатся до RRF=15?

Ответ:

1. $RRF_{\text{СПАЗ/SIS}} = (10^{-2} / 10^{-4}) / 8 = 12.5$.
2. $PFD_{\text{avg}} = 1/12.5 = 0.08 \rightarrow \text{SIL 1}$.
3. $RRF_{\text{СПАЗ/SIS}} = 6.67 \rightarrow PFD_{\text{avg}} = 0.15 \rightarrow \text{SIL 1}$ (но запас снижается).

Кейс 5.4. Утечка с возгоранием.

Дано: На нефтебазе возможна утечка с возгоранием ($C=4$, $F=3$, $P=0.5$). Существуют. инструктаж, ручные клапаны. Достаточно ли этого?

Решение.

1. Расчет дает класс риска II (по таблице).
2. Проверяем LOPA. Инструктаж снижает P до 0.3, защита от дурака – снижает P до 0.2. Итоговый риск $\rightarrow$ III (приемлемо). Вывод. СПАЗ не требуется?

Философия документации о выполненном анализе рисков.

Правило. «Не написал – не сделал». Аудит проверяет не ваши мысли, а записи.

Пример плохой записи. «Риск низкий, СПАЗ не нужен».

Пример хорошей записи.

«Риск класса III ($C=4$, $F=3$, $P=0.5$).

Существующие меры обеспечения приемлемой безопасности:

- 1) Инструктаж ($PFD=0.7$),
- 2) Защита от дурака ($PFD=0.5$).

В результате суммарный $PFD=0.35$ ведет к риску категории III. Основание. Протокол от 12.03.2024».

Ключевой анализ рисков – это не поиск «точного числа», а обоснованное принятие решений в условиях неопределенности. Чем прозрачнее логика, тем легче защитить свое решение перед аудитором.

Вот отредактированная версия тестов с улучшенной структурой и подачей материала.

Понимание рисков для СПАЗ/SIS.

(Ключевой принцип. «Риск – это не цифра, а аргументированное суждение»)

Классификация риска (I-IV) – определяем, насколько риск критичен.

Слэнг проектировщика СПАЗ.

«Этот сценарий аварии классифицируется опасностью класса II, но если добавить клапан СПАЗ/SIS, то риск уйдёт в III!». Или «PFD нашего ОПО= $1e-3$, а по LOPA нужно $1e-4$ – значит, нужна СПАЗ/SIS!».

Кейс 5.5. Анализ ложных срабатываний STR.

Задача. Система защиты выполнена на основе 2 датчиков давления ($\lambda S = 0.8 \times 10^{-6}/\text{час}$) и клапана ($\lambda S = 1 \times 10^{-6}/\text{час}$).

- Архитектура: 1oo2 датчиков + 1oo1 клапан.
- $\beta = 5\%$.

Вопросы.

1. Рассчитать MTTFs системы.
2. Соответствует ли требование MTTFs > 10 лет?

Интенсивность ложных срабатываний (Spurious Trip Rate, STR) – это частота, с которой система выдает ложное срабатывание. Измеряется, например, в 1/час.

Среднее время до ложного срабатывания (Mean Time To Spurious Trip, MTTFs) – это среднее время, которое система проработает до ложного срабатывания. Это ключевой показатель надёжности против ложных срабатываний.

Формула. $MTTFs = 1 / STR$.

Система защиты состоит из двух частей.

Подсистема датчиков (1oo2). Это означает «1 из 2». Ложное срабатывание этой подсистемы произойдет, если ЛЮБОЙ из двух датчиков ложно сработает ИЛИ если оба сработают одновременно из-за общей причины. Это типичная архитектура для снижения вероятности ложного останова.

Подсистема клапана (1oo1). Это означает «1 из 1». Ложное срабатывание произойдет, если клапан откажет таким образом, что самопроизвольно закроется (или откроется, в зависимости от логики). Это просто одиночный элемент.

Шаг 2. Расчет STR для подсистемы датчиков (1oo2).

Для архитектуры 1oo2 упрощенная формула для расчёта интенсивности ложных срабатываний с учётом общих причин (β -фактор) выглядит так.

$$STR_{1oo2} = (1 - \beta) \times \lambda S \times 2 + \beta \times \lambda S,$$

где.

$(1 - \beta) \times \lambda S \times 2$ – это учёт независимых отказов двух датчиков. Если один отказывает (ложное срабатывание), вся подсистема датчиков ложно срабатывает.

$\beta \times \lambda S$ – это учёт отказов по общей причине. Если оба датчика отказывают одновременно из-за общей причины (например, скачок напряжения), это также вызывает ложное срабатывание подсистемы.

Подставляем наши цифры.

$$STR_{\text{датчиков}} = (1 - 0.05) \times (0.8 \times 10^{-6}) \times 2 + 0.05 \times (0.8 \times 10^{-6}).$$

Вычисляем по частям.

$$(1 - 0.05) = 0.95.$$

$$0.95 \times (0.8 \times 10^{-6}) = 7.6 \times 10^{-7}.$$

$$7.6 \times 10^{-7} \times 2 = 1.52 \times 10^{-6} \text{ (вклад независимых отказов)}$$

$$0.05 \times (0.8 \times 10^{-6}) = 0.04 \times 10^{-6} = 4 \times 10^{-8} \text{ (вклад общих отказов)}$$

$$\text{Суммируем. } STR_{\text{датчиков}} = 1.52 \times 10^{-6} + 0.04 \times 10^{-6} = 1.56 \times 10^{-6} / \text{час.}$$

Шаг 3. Расчет STR для подсистемы клапана (1001).

Для архитектуры 1001 всё просто. Ложное срабатывание происходит, если отказывает сам клапан.

$$STR_{\text{клапана}} = \lambda S_{\text{клапана}} = 1 \times 10^{-6} / \text{час}$$

Шаг 4. Расчет общего STR системы

Вся система сработает ложно, если сработает ложно подсистема датчиков ИЛИ подсистема клапана. Так как отказы элементов предполагаются независимыми, общая интенсивность отказов системы равна сумме интенсивностей отказов её подсистем.

Формула.

$$STR_{\text{системы}} = STR_{\text{датчиков}} + STR_{\text{клапана}}.$$

Подставляем цифры.

$$STR_{\text{системы}} = (1.56 \times 10^{-6}) + (1 \times 10^{-6}) = 2.56 \times 10^{-6} / \text{час.}$$

Шаг 5. Расчет MTTFs системы.

Формула.

$$MTTFs = 1 / STR_{\text{системы}}.$$

Подставляем цифры.

$$MTTFs = 1 / (2.56 \times 10^{-6}) \text{ час.}$$

Чтобы перевести часы в годы, вспомним, что в одном году примерно 8760 часов (365 дней $\times$ 24 часа).

$$MTTFs = 1 / (2.56 \times 10^{-6} \times 8760) \text{ лет.}$$

Сначала посчитаем в часах, а потом их переведем в годы.

$$MTTFs = 1 / 2.56 \times 10^{-6} \approx 390\,625 \text{ часов.}$$

$$MTTFs \approx 390\,625 / 8760 \approx 44.6 \text{ лет.}$$

Ответ.

Вопрос 1. MTTFs системы составляет приблизительно 44.6 лет .

Вопрос 2. Соответствует ли требованию $MTTFs > 10$ лет?

Сравниваем. Рассчитанное нами MTTFs (~43 года) значительно больше требуемого значения (10 лет).

Ответ на вопрос 2. Да, рассчитанное MTTFs системы соответствует требованию > 10 лет.

Итоговый вывод.

Система имеет высокую надёжность в отношении ложных срабатываний благодаря резервированию 1oo2 для датчиков. Эта архитектура избыточна для повышения доступности (увеличения MTTFs), но при этом вносит дополнительную сложность и стоимость. Расчёт показывает, что выбранная архитектура с запасом удовлетворяет поставленному требованию.

Итоговые рекомендации.

1. Для SIL 2 и выше всегда резервируйте критические датчики (1oo2/2oo3).
2. Учитывайте отказ по общей причине более 1% в резервированных системах.
3. Климатические условия могут «сломать» даже сертифицированное оборудование – проводите полевые испытания. Переохлаждение датчика снижает SIL системы с 2 до 1.
4. Документируйте все изменения конфигурации – 90% отказов СПАЗ/SIS связаны с человеческим фактором.

Риск – это не гадание, а структурированная оценка.

СПАЗ/SIS – не панацея, а часть многослойной защиты.

Язык инженера СПАЗ – это ссылки на стандарты, расчеты и документирование.

Финал.

«Хороший проект СПАЗ/SIS – это не там, где всё перестраховано, а где каждый элемент обоснован нормативами и расчетами».

Стиль.

- Минимум воды, максимум практических связей (нормы → расчеты → решение).
- Слэнг и аббревиатуры (как в реальной работе).
- Акцент на доказательность (не «нам кажется», а «по п. 5.3 ГОСТ Р МЭК 61508»).

5.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 5.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 5.1. Понимание рисков для СПАЗ/SIS и мета-проблем СПАЗ.

Вопрос 1. Какая основная цель FMEA при анализе СПАЗ/SIS?

Варианты.

- А. Оценить влияние отказов СПАЗ/SIS на объект.
- В. Выявить скрытые отказы самой СПАЗ/SIS.
- С. Определить вероятность аварии из-за СПАЗ/SIS.

D. Проверить соответствие SIL без учета человеческого фактора.

Ответ А.

Объяснение. FMEA – это метод анализа отказов и их последствий.

Основная цель – выявить, как отказ компонента СПАЗ/SIS (например, датчика или логического контроллера) повлияет на безопасность объекта (МЭК 61508, ч. 2, п. 7.4.3).

Вариант В (скрытые отказы) – это задача диагностики, а не FMEA.

Вариант С – часть HAZOP, а не FMEA.

Вариант D не учитывает системный подход.

FMEA для СПАЗ/SIS сосредоточен на внутренних уязвимостях системы (отказы датчиков, логики, исполнительных механизмов), а не на внешних последствиях. Человеческий фактор также учитывается.

Вопрос 2. Адаптация HAZOP для СПАЗ/SIS.

Варианты.

- A. Анализ ключевых слов («нет сигнала»).
- B. Оценка влияния на технологию.
- C. Поиск ошибок только в ПО.
- D. Сценарии, где СПАЗ/SIS - источник риска.

Ответ А, D.

HAZOP для СПАЗ/SIS фокусируется на отклонениях в работе (МЭК 61882, п. 6.2).

«Нет сигнала» → отказ датчика.

«Ложное срабатывание» → нештатное отключение процесса

Объяснение. HAZOP для СПАЗ/SIS использует методику ключевых слов и рассматривает случаи, когда система сама создает опасность.

Вариант В – часть общего HAZOP, а не специфики СПАЗ/SIS.

Вариант С слишком узкий (анализируется только приборная часть САЗ).

Тест 5.2. Определение требуемого SIL для ОПО с низкой частотой возникновения опасности.

Вопрос 1. Величина Ft это?

Ответ. Допустимый уровень риска.

Объяснение. Ft - целевой показатель безопасности, отправная точка для расчетов.

Вопрос 2. Первый шаг определения SIL.

Ответ. Установить приемлемый уровень риска Ft.

Объяснение. Без четкого критерия приемлемого риска дальнейшие расчеты бессмысленны.

Вопрос 3. Расчет PFD_{avg} .

Ответ $PFD_{avg} = 1/RRF$.

Объяснение. PFD_{avg} вычисляют как обратную величину коэффициента снижения риска.

Вопрос 4. Какой параметр определяет SIL для системы, работающей в режиме низкой частоты запросов?

Варианты ответов.

- А) Средняя вероятность отказа по требованию (PFDavg).
- В) Частота опасных отказов в час (PFH).
- С) Коэффициент готовности системы.
- Д) Время восстановления после отказа (MTTR).

Ответ А. Средняя вероятность отказа по требованию (PFDavg).

Объяснение.

Для систем, работающих в режиме низкой частоты запросов, SIL определяется по PFDavg (средней вероятности отказа по требованию).

PFH (вариант В) используется для систем с высокочастотными запросами (непрерывный режим запросов).

Коэффициент готовности (вариант С) и MTTR (вариант Д) влияют на надежность, но не являются прямыми критериями SIL.

Вопрос 4. Какой SIL будет у системы, если $PFDavg = 5 \times 10^{-3}$, а $PFH = 3 \times 10^{-7}$ 1/час?

Варианты ответов.

- А) SIL 2, так как PFDavg соответствует SIL 2 (0.001–0.01).
- В) SIL 3, так как PFH соответствует SIL 3 (1×10^{-7} – 1×10^{-6}).
- С) SIL 2, если режим низких запросов.
- Д) SIL определяется по худшему показателю. SIL.

Ответ С. SIL 2, если режим низких запросов.

Объяснение.

Для режима низких запросов SIL определяется по $PFDavg = 5 \times 10^{-3}$ (SIL 2).

$PFH = 3 \times 10^{-7}$ (SIL 3) не учитывается, так как это параметр для высокочастотных систем.

Вариант Д некорректен. SIL определяется по режиму работы, а не «худшему» показателю.

Тест 5.3. Классификация рисков ОПО.

Вопрос 1. В чем заключается основная проблема оценки риска?

Ответ. Отсутствие универсальной шкалы.

Объяснение. Невозможно создать единый «измеритель» риска, который бы одинаково хорошо работал для кибербезопасности, медицины, строительства и финансов. Каждая отрасль имеет свои уникальные последствия (ущерб здоровью, финансовые потери, экологический вред) и вероятности наступления опасных событий, которые измеряются в разных шкалах.

Вот примеры из практики:

- В охране труда риск оценивается по классам условий труда (от оптимальных до опасных) и требует соответствующих средств индивидуальной защиты.

- В медицине для оценки риска смерти от сердечно-сосудистых заболеваний используется шкала SCORE, которая рассчитывает вероятность в процентах на основе возраста, давления и других факторов .
- В государственном надзоре категории риска (от низкого до чрезвычайно высокого) определяют периодичность плановых проверок предприятий (от 1 раза в год до их полного отсутствия).

Таким образом, основная сложность заключается в понимании и сопоставлении рисков из разных сфер деятельности для принятия управленческих решений на национальном или корпоративном уровне.

Вопрос 2. В случае опасности класса I необходимо снижение риска?

Ответ. Требуется обязательное снижение риска для ОПО.

Объяснение. Класс I (или «Чрезвычайно высокий риск») присваивается тем видам деятельности или производственным объектам, где потенциальные последствия аварии или инцидента наиболее тяжелы, а вероятность их возникновения высока. Такой уровень риска считается недопустимым для нормальной эксплуатации. Он характеризуется:

- Обязательностью мер. Поскольку риск неприемлем, его нельзя сохранять или игнорировать. Требования стандартов и законодательства в этом случае носят императивный характер, предписывая обязательную разработку и внедрение мер по снижению риска до приемлемого уровня . Это может быть усиление контроля, изменение технологического процесса, введение дополнительных средств защиты или даже остановка опасного производства.

- Правовыми последствиями. В контексте государственного надзора, например, присвоение опасности для ОПО класса I влечет за собой наиболее строгий режим проверок – раз в год, что подчеркивает его приоритетность для контролирующих органов .

Тест 5.4. Снижение риска в СПАЗ.

Вопрос 1. Что является конечной целью снижения риска с помощью СПАЗ?

- а) Полная ликвидация любого риска.
- б) Достижение приемлемого уровня риска.
- в) Снижение страховых взносов предприятия.

Ответ: б) Достижение приемлемого уровня риска.

Объяснение.

Безопасность не требует нулевого риска – это недостижимо и экономически нецелесообразно. Цель – снизить риск до приемлемого уровня, который определяется обществом и регулирующими органами. Этот принцип известен как **ALARP** – «настолько низко,

насколько это разумно достижимо». СПАЗ/SIS является одним из инструментов для достижения этого состояния.

Вопрос 2. Какие методы используются для определения необходимой степени снижения риска?

- а) Только качественные.
- б) Только количественные.
- с) Качественные и количественные, в зависимости от сложности и последствий.

Ответ: с) Качественные и количественные, в зависимости от сложности и последствий.

Объяснение.

Оба подхода дополняют друг друга:

- **Качественные методы** (например, **HAZOP**) основаны на опыте экспертов. Команда анализирует процесс и находит потенциальные опасности и отклонения, давая им описательную оценку (например, «высокий», «средний», «низкий» риск). Это быстрый и эффективный способ выявить проблемы.

- **Количественные методы** (например, **LOPA** – Анализ слоев защиты) используются, когда качественного анализа недостаточно. LOPA присваивает числовые значения вероятностям событий и эффективности защитных слоев, чтобы **рассчитать, насколько именно необходимо снизить риск**, и определить требуемый **Уровень полноты безопасности (SIL)** для СПАЗ.

Вопрос 3. Какой инструмент используется для количественного обоснования требований к СПАЗ (SIL) после качественного анализа HAZOP?

- а) FMEA (Анализ видов и последствий отказов).
- б) LOPA (Анализ слоев защиты).
- с) FTA (Анализ деревьев неисправностей).

Ответ: б) LOPA (Анализ слоев защиты).

Объяснение.

HAZOP → LOPA → Определение SIL – это классическая последовательность.

HAZOP отвечает на вопрос: «**Что** может произойти плохого и **почему?**»

LOPA отвечает на вопрос: «**Насколько сильно** нам нужно защититься?» Он рассматривает все независимые защитные слои (обучение операторов, предохранительные клапаны и т.д.) и вычисляет, какой «вклад» в снижение риска должна внести СПАЗ. Этот «вклад» и выражается в виде **целевого SIL**.

Вопрос 4. При каком условии функция безопасности (SIF) считается эффективной?

- а) Когда она имеет максимально возможный SIL.
- б) Когда ее вероятность отказа на требование (PFD) обеспечивает необходимое снижение риска до приемлемого уровня.

с) Когда она использует самое дорогое и современное оборудование.
Ответ: b) Когда ее вероятность отказа на требование (PFD) обеспечивает необходимое снижение риска до приемлемого уровня.

Объяснение.

Гонка за высоким SIL без необходимости – это неоправданные затраты. Ключевой параметр – вероятность **PFD**, что система не сработает, когда это потребуется. Расчетное значение PFD для каждой функции безопасности (SIF) должно подтверждать, что риск снижается до целевого, приемлемого уровня. Система с SIL 1, адекватно подобранная для конкретной опасности, будет гораздо эффективнее и безопаснее, чем неправильно спроектированная система с SIL 3. Снижение риска – это не абстрактная концепция, а **инженерный процесс** чтобы:

1. **Выявить опасности (HAZOP).**
2. **Оценить, насколько нужно снизить риск (LOPA -> Целевой SIL).**
3. **Спроектировать систему, которая гарантированно обеспечит это снижение (PFDavg, соответствующий целевому SIL).**
4. **Доказать, что риск стал приемлемым.**

5.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 5.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 5».

Тест 5.5.

Анализируется опасность с использованием диаграммы риска (рис.5.1) для выбора SIL контура защиты, который снижает риск [27]. Ожидается, что нежелательное событие приведет к серьезным травмам нескольких человек, но без смертельных исходов. Существует значительная задержка в возникновении события, что создает возможность спасения рабочих. Кроме того, продолжительность нахождения в опасной зоне высока и относительно высокая вероятность того, что нежелательное событие произойдет. На основании предоставленной информации, какой SIL следует выбрать?

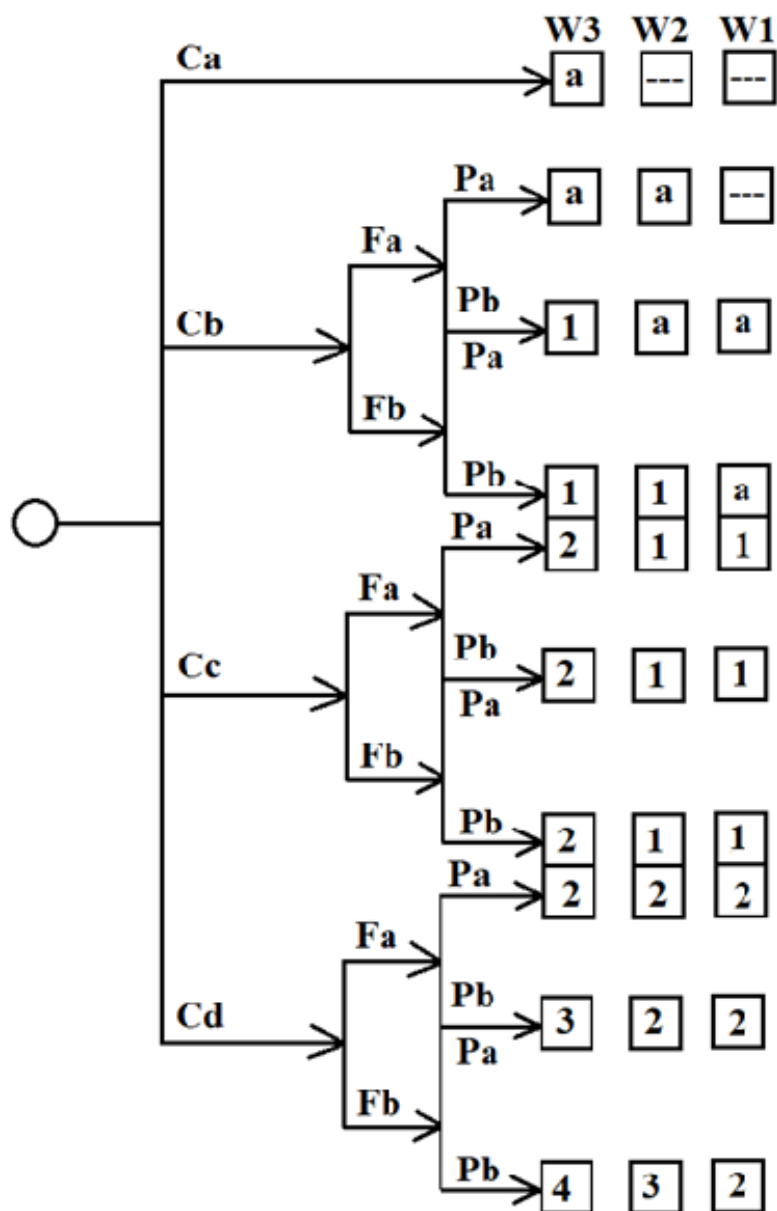


Рис 5.1. Диаграмма риска

Здесь параметры риска определяют следующим образом.

1. Классификации последствий.

Ca – Незначительная травма.

Cb – Серьезная травма одного или нескольких человек, смерть одного человека.

Cc – Смерть нескольких человек.

Cd – Очень много погибших Классификации вероятностей.

2. Продолжительность нахождения в опасной зоне.

Fa – от редкого до относительно частого.

Fb – частое или постоянное.

3. Предотвращение опасности.

Pa – возможно при определённых обстоятельствах.

Pb – невозможно.

4. Интенсивность запросов (число случаев за год, когда опасная ситуация возникает в отсутствие рассматриваемой функции безопасности СПАЗ/SIS).

W1 – Очень малая вероятность возникновения, и только несколько случаев вероятны.

W2 – Небольшая вероятность, несколько случаев вероятны.

W3 – Относительно высокая вероятность того, что нежелательное событие произойдет, и частые некоторые нежелательные случаи вероятны.

Вопрос. Какой SIL необходим для установленного риска на ОПО?

a) SIL=1.

b) SIL=2.

c) SIL=3.

d) SIL=4.

e) Невозможно выбрать SIL из этой информации.

Для получения дополнительной информации см. [27].

Тест 5.6.

При каких условиях коэффициент присутствия оператора возле объекта повышенной опасности будет соответствовать значению Fa? Выбрать правильный ответ.

Вопрос 1. Какое условие необходимо для того, чтобы коэффициент присутствия оператора возле объекта повышенной опасности соответствовал значению Fa (редкого до относительно частого) на диаграмме риска?

A) Операторы должны находиться в зоне риска постоянно.

B) Доступ в рабочую зону должен быть строго ограничен.

C) Операторы не должны проходить обучение.

D) Обслуживание оборудования должно проводиться в любое время.

Вопрос 2. Какое значение имеет обучение и подготовка персонала в контексте снижения коэффициента присутствия оператора?

A) Обучение не имеет значения.

B) Операторы должны проходить регулярное обучение по безопасным методам работы.

C) Обучение должно проводиться только один раз.

D) Операторы должны обучаться самостоятельно.

Вопрос 3. Почему планирование обслуживания оборудования важно для снижения коэффициента присутствия оператора?

A) Обслуживание можно проводить в любой момент.

B) Обслуживание должно проводиться только в заранее запланированные периоды.

C) Операторы должны всегда присутствовать во время обслуживания.

D) Планирование не влияет на безопасность.

Вопрос 4. Какую роль играют аварийные процедуры в снижении коэффициента присутствия оператора?

- А) Они не имеют значения.
- В) Четкие аварийные процедуры помогают минимизировать риски.
- С) Аварийные процедуры должны быть неизвестны операторам.
- Д) Аварийные процедуры должны быть сложными.

Вопрос 5. Как регулярные оценки рисков влияют на коэффициент присутствия оператора?

- А) Они не влияют на безопасность.
- В) Позволяют выявлять и устранять потенциальные угрозы.
- С) Увеличивают риск аварий.
- Д) Необходимы только один раз.

Тест 5.7.

При каких условиях коэффициент предотвращения опасности из за присутствия оператора возле объекта повышенной опасности будет соответствовать значению Р (возможно при определенных условиях).

Вопрос 1. Какое условие необходимо для того, чтобы коэффициент предотвращения опасности Р соответствовал значению Ра «возможно при определенных условиях»?

- А) Оператор должен находиться в зоне риска постоянно.
- В) Оператор должен быть обучен и готов к реагированию на опасности.
- С) Оператор не должен использовать средства индивидуальной защиты.
- Д) Доступ в рабочую зону должен быть неограниченным.

Вопрос 2. Какое значение имеет наличие четких процедур безопасности для коэффициента предотвращения опасности?

- А) Процедуры не влияют на безопасность.
- В) Четкие процедуры помогают оператору действовать быстро и эффективно в экстренных ситуациях.
- С) Процедуры усложняют работу оператора.
- Д) Наличие процедур не имеет значения, если оператор опытен.

Вопрос 3. Какую роль играют регулярные тренировки для операторов в контексте коэффициента предотвращения личной или групповой опасности на ОПО?

- А) Тренировки не нужны, если оператор имеет опыт.
- В) Регулярные тренировки помогают поддерживать навыки и уверенность оператора.
- С) Тренировки могут отвлекать оператора от основной работы.
- Д) Тренировки необходимы только в начале работы.

Вопрос 4. Как регулярные оценки рисков влияют на коэффициент предотвращения опасности?

- А) Они не влияют на безопасность.

- В) Позволяют выявлять и устранять потенциальные угрозы.
 - С) Увеличивают риск аварий.
 - Д) Необходимы только один раз.
- Выбрать правильные ответ.

Тест 5.8. Определение уровня SIL для системы управления горелками.

На предприятии имеется большая нагревательная печь, где в качестве топлива используется газ. В результате изучения опасностей было установлено, что в камере сгорания возможен взрыв, если в результате погасания пламени образуется смесь воздуха и несгоревшего газа. Эта ситуация может возникнуть, если после погасания пламени подача газа не будет немедленно остановлена.

Система управления горелками снабжена датчиком пламени, который при погасании пламени немедленно отключает основной и пилотный клапаны на линии подачи газа. Система защиты от погасания пламени явно должна классифицироваться как система функциональной безопасности.

Пусть частота погасания пламени составляет два раза в год и что вероятность взрыва возникает в одном событии из четырех.

Изучив архивные данные установлено что частота взрывов, не превышающая один раз в 5000 лет, и тем самым является приемлемой. Эта цифра дает нам значение $F_{пр}$ – целевое значение защищенной частоты риска, равное $1/5000 = 2 \times 10^{-4}$ в год.

Выбрать правильный ответ.

Вопрос 1. Какова частота погасания пламени в данной системе?

- А) 1 раз в год.
- В) 2 раза в год.
- С) 4 раза в год.
- Д) 0 раз в год.

Вопрос 2. Какова вероятность взрыва при погасании пламени?

- А) 0,1.
- В) 0,25.
- С) 0,5.
- Д) 1.

Вопрос 3. Как рассчитывается ожидаемое значение частоты взрывов ($F_{пр}$)?

- А) $F_{пр} = \text{частота погасания пламени} \times \text{вероятность взрыва}$.
- В) $F_{пр} = \text{частота погасания пламени} + \text{вероятность взрыва}$.
- С) $F_{пр} = \text{частота погасания пламени} / \text{вероятность взрыва}$.
- Д) $F_{пр} = \text{частота погасания пламени} - \text{вероятность взрыва}$.

Вопрос 4. Какова целевая частота риска (F_r) для данной системы?

- А) 1 раз в 1000 лет.
- В) 1 раз в 5000 лет.

C) 1 раз в 10000 лет.

D) 1 раз в 2000 лет.

Вопрос 5. Какова целевая частота риска в год (F_p) для значения 1 раз в 5000 лет?

A) 1×10^{-4} .

B) 2×10^{-4} .

C) 1×10^{-5} .

D) 2×10^{-5} .

Вопрос 6. Как рассчитывается коэффициент снижения риска (RRF)?

A) $RRF = F_{np} \times F_p$.

B) $RRF = F_{np} / F_p$.

C) $RRF = F_{np} - F_p$.

D) $RRF = F_{np} + F_p$.

Вопрос 7. Каково значение PFD_{avg} для данной системы?

A) $1 / RRF = 2 \times 10^{-4}$.

B) $PFD_{avg} = 1 / RRF = 4 \times 10^{-4}$.

C) $PFD_{avg} = RRF$.

D) $PFD_{avg} = 2 \times 10^{-4}$.

Вопрос 8. Какой уровень SIL соответствует рассчитанному значению PFD_{avg} ?

A) SIL 1.

B) SIL 2.

C) SIL 3.

D) SIL 4.

Для получения дополнительной информации см. [27].

6. ПОЛНОТА БЕЗОПАСНОСТИ, ОБЕСПЕЧИВАЕМАЯ СИСТЕМОЙ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ.

6.1. Ключевые принципы полноты безопасности (SIL).

Задание 6.1. Уяснить ключевые принципы полноты безопасности СПАЗ/SIS.

«SIL –это не просто цифра, а системный подход к управлению жизненным циклом безопасности».

1. Базовые концепции.

SIL (Safety Integrity Level) – это количественная мера надежности системы безопасности, показывающая (табл.6.1).

- Вероятность опасного отказа в год (для работающих систем с низкой частотой запроса на срабатывание).

- Вероятность опасного отказа в час (для постоянно работающих систем).

- Требования к резервированию.

Таблица 6.1 Четыре уровня SIL и их практическая интерпретация.

Уро- вень SIL	Вероятность отказа по за- просу (PFD)	Вероятность опасного от- каза в час (PFH)	Область приме- нения	Требования к архитектуре
SIL 4	$\geq 10^{-5}$ до $< 10^{-4}$	$\geq 10^{-9}$ до $< 10^{-8}$	Критические си- стемы защиты, атомная энерге- тика	Резервирование 2oo3, диагностика > 99%
SIL 3	$\geq 10^{-4}$ до $< 10^{-3}$	$\geq 10^{-8}$ до $< 10^{-7}$	Нефтегазовая промышленность, химические про- цессы	Резервирование 1oo2, диагностика > 90%
SIL 2	$\geq 10^{-3}$ до $< 10^{-2}$	$\geq 10^{-7}$ до $< 10^{-6}$	Производствен- ные процессы, ма- шиностроение	Одноканальная с диагностикой > 60%
SIL 1	$\geq 10^{-2}$ до $< 10^{-1}$	$\geq 10^{-6}$ до $< 10^{-5}$	Базовые системы защиты, неопас- ные процессы	Одноканальная, ограниченная ди- агностика

2. Жизненный цикл SIL-системы.

a) Анализ рисков.

– Методы. HAZOP, LOPA, FTA.

– Определение целевого коэффициента снижения риска (RRF).

b) Выбор SIL.

Расчет требуемого $PFD_{avg} = 1/RRF$.

Пример. Если $RRF = 1000 \rightarrow PFD_{avg} \leq 0.001 \rightarrow SIL\ 3$.

c) Проектирование.

- Избыточность (1oo2, 2oo3).

- Диверсификация.

- Самодиагностика.

d) Верификация.

- Расчет PFDavg.

- Доли безопасных отказов SFF (Safe Failure Fraction).

f) Валидация.

- Тестирование с введением неисправностей.

- Валидация SIF.

3 Отраслевые особенности.

Нефтегаз.

- Типовые SIL: 2-3.

- Примеры критических SIF.

- Аварийное отключение технического оборудования.

- Защита от переполнения резервуаров.

Химия.

- Особенность. Коррозионные среды → требования к аппаратной надежности.

- Пример. SIL 2 для систем вентиляции на хлорных производствах.

4. Типичные ошибки проектирования.

1. «SIL, обеспечивающий максимальную безопасность»:

- Попытка назначать максимальный SIL без обоснования.

- Последствие. Неоправданные затраты.

2. «Бумажный SIL».

Несоответствие документации при реальных проблемах:

- Нет данных по MTBF компонентов.

- Нет анализа DC.

- Отсутствие плана обслуживания.

3. Неучет «человеческого фактора»:

SIL не может быть обеспечен (например SIL3) в СПАЗ с ручным управлением в критическом контуре.

Расчет SIL – это не просто подстановка чисел в формулы, а понимание «души» системы. Например, диагностическое покрытие 99% не сделает систему надежной, если 1% необнаруженных отказов приходится на критичные компоненты.

Формулы – это карта, но компанию им должен составлять инженерный здравый смысл. SIL – это не цель, а инструмент для управления рисками отказов СПАЗ/SIS.

6.2. ПРАКТИКУМ ПО ОЦЕНКЕ ПОЛНОТЫ БЕЗОПАСНОСТИ.

Задание 6.2. С поддержкой AI (типа GPT) подготовить свои решения кейсов и объяснения для одного или 2-х кейсов. Сделать вывод о правильности и качестве предложенных ответов и объяснений в кейсах.

Кейс 6.1. Климатический парадокс.

Ситуация. На нефтехимическом заводе система аварийного отключения (СПАЗ/SIS) не сработала из-за датчиков, что привело к пожару. Выполнить анализ причин.

Исходные данные.

Блок датчиков аварийного отключения (СПАЗ/SIS), реализованный на основе архитектуры 1oo2 с расчетным обоснованием $PFD_{avg} = 0.0025$ (SIL 2), не сработал при -40°C , что привело к пожару.

Паспортные данные датчика: $\lambda DU = 1 \times 10^{-6} \text{1/час}$ (для $-20^{\circ}\text{C} \dots +60^{\circ}\text{C}$).

Расчетные данные для датчиков температуры.

- Период тестирования (T_{Proof}) = 1 год.
- Без учета общих отказов каналов SIF.

Почему был отказ? Может быть было недостаточное диагностическое покрытие? Почему Diagnostic Coverage (DC) важен?

Диагностика постоянно мониторит исправность канала и с определенной вероятностью (DC) и может обнаружить опасный отказ (DU), переводя его в разряд обнаруженных (DD).

Обнаруженный отказ, как правило, переводит канал измерения в безопасное состояние (например, переводит его в режим маскирования) и выполняется немедленное уведомление оператора о необходимости ремонта. Это сокращает время, в течение которого канал находится в неработоспособном состоянии.

Но без диагностики все отказы остаются скрытыми до следующего планового ТО.

С диагностикой часть этих отказов ($\lambda DU \times DC$) обнаруживается и устраняется практически в реальном масштабе времени (в расчетах принимается среднее время восстановления MTTR, порядка 8-24 часов). Правда, другая часть отказов ($\lambda DU \times (1-DC)$) остается скрытой.

Экспертная оценка установила, что глубина диагностического покрытия в СПАЗ соответствовала (DC) = 90%.

Формула для расчета PFD_{avg} одного канала резервирования.

$PFD_{avg\_1\text{канал}} \approx (\lambda DU \times (1 - DC) \times T_{Proof}) / 2 + (\lambda DU \times DC \times MTTR)$,

где

- $\lambda DU \times (1 - DC)$ – интенсивность *необнаруживаемых* опасных отказов (остаются скрытыми до теста).

- $\lambda DU \times DC$ – интенсивность *обнаруживаемых* опасных отказов.

- MTTR – среднее время восстановления (Mean Time To Repair).

Для оценок она часто принимается равной 8 часам (1 рабочая смена).

Рассчитаем PFD_{avg} для одного датчика с учетом исходных данных (для штатного режима $-20^{\circ}\text{C} \dots +60^{\circ}\text{C}$)

$\lambda DU = 1 \times 10^{-6} \text{1/час}$.

$DC = 90\%$ или 0.9.

$T_{Proof} = 1 \text{ год} = 8760 \text{ часов.}$

$MTTR = 8 \text{ часов (стандартное допущение).}$

1. Вероятность необнаруживаемых отказов $(1 \times 10^{-6} \times (1 - 0.9) \times 8760) / 2 = (0.0000001 \times 8760) / 2 = 0.000876 / 2 = 0.000438$

2. Вероятность обнаруживаемых отказов. $(1 \times 10^{-6} \times 0.9 \times 8) = 0.0000009 \times 8 = 0.0000072.$

Итого: $PFD_{avg\_1} \text{ канал} \approx 0.000438 + 0.0000072 = 0.0004452.$

Вывод. Отказоустойчивость одного канала измерения с диагностикой $PFD_{avg} \approx 4.4510^{-4}.$

Теперь выполним расчет вероятности отказа блока измерения для архитектуры 1oo2.

Для упрощения расчета резервированного по схеме 1oo2 блока измерения с учетом диагностики часто используют формулу, которая учитывает, что оба канала идентичны и отказы независимы:

$PFD_{avg\_1oo2} \approx 2 \times (PFD_{avg\_1 \text{ канал}})^2.$

Это упрощение, но оно дает хорошую оценку для высоконадежных систем.

Подставляем:

$PFD_{avg\_1oo2} \approx 2 \times (0.0004452)^2 = 2 \times (1.982e^{-7}) \approx 3.964 \times 10^{-7}.$

Вывод. Расчетное PFD_{avg} для резервированных 1oo2 датчиков с учетом диагностики составляет примерно 0.000000396. Это значительно лучше исходной цифры 0.0025 и соответствует высокому уровню **SIL 3**. Выполненная верификация СПАЗ/SIS с учетом DC показывает высокую расчетную надежность резервированного блока датчиков. И это прибавляет уверенность в безаварийной эксплуатации такой схемы датчиков.

Но не был выполнен учет погодных условий!

Выполним оценку надежности схемы при $-40^{\circ}\text{C}.$

Практика показывает что из за температурного феномена возможно увеличение λ_{DU} в 1000 раз.

$\lambda_{DU\_new} = 1 \times 10^{-6} \times 1000 = 1 \times 10^{-3} \text{ 1/час.}$

Рассчитаем PFD_{avg} для одного датчика при $-40^{\circ}\text{C}.$

Теперь:

1. Часть от не обнаруживаемых отказов. $(0.001 \times (1 - 0.9) \times 8760) / 2 = (0.0001 \times 8760) / 2 = 0.876 / 2 = 0.438.$

2. Часть от обнаруживаемых отказов. $(0.001 \times 0.9 \times 8) = 0.0009 \times 8 = 0.0072.$

$PFD_{avg\_1\_new} \approx 0.438 + 0.0072 = 0.4452.$

И вероятность отказа блока датчиков при запросе становится:
 $PFD_{avg\_1oo2\_new} \approx 2 \times (0.4452)^2 = 2 \times 0.1982 \approx 0.3964.$

Из таблицы SIL следует что полнота безопасности снизилась до уровня SIL1. Результаты верификации СПАЗ можно свести в таблицу 6.2.

Таблица 6.2 Сводная таблица и итоговый вывод

Параметр	Без DC (пред. расчет)	С DC=90% (корректный)	При -40°C (с DC)
PFDavg_1002	$\sim 1.92 \times 10^{-5}$ (SIL 3)	$\sim 3.96 \times 10^{-7}$ (SIL 3)	~ 0.396 (SIL 1)
Вероятность отказа	Ничтожна	Чрезвычайно ничтожна	Около 30%. Это стало причиной отказа блока датчиков

Ответы на вопросы.

1. **Почему не был учтен DC изначально?** Была ошибка. Был выполнен расчет с использованием упрощенной формулы, но это было некорректно. Для СПАЗ/SIS, обеспечивающих полноту безопасности SIL 2 и выше учет DC обязателен.

В штатных условиях диагностика улучшает показатели безопасности на порядки (сравните 1.92×10^{-5} и 3.96×10^{-7}). Она значительно снижает PFDavg.

2. **В аварийной ситуации** (при -40°C) диагностика тоже *немного помогает* (вероятность отказа была 19.2, а стала 0.396), но это все равно катастрофически плохой показатель. Вероятность отказа системы составляет почти 30%, что абсолютно недопустимо.

Итог.

Диагностическое покрытие – мощный инструмент для повышения безопасности, но оно бессильно против фундаментальной ошибки – неправильного выбора оборудования. Если компонент работает в нерасчетных условиях и его базовая интенсивность отказов (λ) взлетает до небес, никакая диагностика не спасет.

Кейс 6.2. Человеческий фактор и SIL

Ситуация. СПАЗ/SIS аварийной вентиляции (PFDavg= 0.00438, SIL 2) была отключена персоналом, принявшим срабатывание за ложную тревогу.

Расчеты.

- Вероятность ручного отключения. 0.1 (1 раз в 10 случаев)
- Реальный PFDavg.

$$PFDavg = 0.00438 + 0.1 = 0.10438.$$

Вопросы.

1. Почему человеческий фактор редко включают в PFDavg?
2. Какие технические меры предотвратят ошибочное отключение?

Решение.

- Блокировка ручного управления при аварии.
- Обязательная двухэтапная подтверждение действий.

Вывод.

СПАЗ/SIS бесполезна, если персонал может её отключить

«на глазок». Интегрируйте организационные меры в расчеты надежности.

Кейс 6.3. Электромагнитная ловушка.

Ситуация. На АЭС СПАЗ/SIS (архитектура 2004) с скопированным из стороннего проекта $PFD_{avg} = 5 \times 10^{-7}$ (SIL 3) отказала из-за EMI от высоковольтной линии.

Причина.

Новое расположение кабелей увеличило λ_{DU} датчиков с 1×10^{-8} до 1×10^{-5} 1/час.

Вопросы.

1. Почему EMI часто упускают из виду?
2. Как проверить устойчивость СПАЗ/SIS к помехам?

Методы защиты.

- Экранирование кабелей.
- Разнесение трасс (>1 м от силовых линий).

Вывод.

Копирование расчетов без анализа изменений в проекте – грубая ошибка. Всегда оценивайте электромагнитную совместимость.

Кейс 6.4. Определение SIL через коэффициент снижения риска (МЭК 61508).

Задача. Для насосной станции с риском утечки токсичного вещества.

- Текущая частота события (F_0) = 10^{-3} /год.
- Допустимый риск (F_T) = 10^{-5} /год.
- Другие меры защиты снижают риск в 5 раз.

Вопросы.

1. Рассчитать общий коэффициент снижения риска (RRF).
2. Определить требуемый PFD_{avg} для СПАЗ/SIS.
3. Выбрать уровень SIL из таблицы МЭК 61511-1.

Расчеты.

1. $RRF = F_0 / F_T = 10^{-3} / 10^{-5} = 100$.
2. RRF для СПАЗ/SIS = $100 / 5 = 20 \rightarrow PFD_{avg} = 1/RRF = 0.05$.
3. По таблице SIL. $PFD_{avg} \in [0.01, 0.1] \rightarrow SIL 1$.

Кейс 6.5. Практическое задание.

Дано:

- Техпроцесс с допустимой частотой аварии 10^{-5} событий/год.
- Частота без СПАЗ/SIS. 10^{-2} событий/год.

Задание.

1. Рассчитать требуемый RRF.
2. Определить минимальный SIL.
3. Предложить архитектуру системы.

Решение.

1. $RRF = 10^{-2} / 10^{-5} = 1000$.
2. $PFD_{avg} \leq 0.001 \rightarrow SIL\ 3$.
3. Варианты.
 - 2003 датчики.
 - Разнесенные логические контроллеры.
 - Двойные исполнительные механизмы.

КЛЮЧЕВЫЕ ВЫВОДЫ.

1. SIL – инструмент управления рисками, а не самоцель.
2. Требуется комплексного подхода на всех этапах жизненного цикла.
3. Эффективность определяется слабым звеном в цепочке безопасности.

Общие рекомендации по расчетам SIL.

1. Учитывайте реальные условия (климат, ЕМИ, вибрации).
2. Проверяйте границы применимости сертификационных данных.
3. Диагностируйте всё – от аппаратуры до ПО.
4. Моделируйте человеческий фактор – добавьте вероятность ошибок в PFD_{avg} .
5. Аудит изменений – даже незначительные правки проекта могут убить SIL.

Итог.

«SIL – это не математическая абстракция, а отражение реальной работоспособности системы. Если расчеты не учитывают эксплуатационные риски – они опасны.»

Расчет SIL – это не просто подстановка чисел в формулы, а понимание «души» системы. Например, диагностическое покрытие 99% не сделает систему надежной, если 1% необнаруженных отказов приходится на критичные компоненты. Формулы – это карта, но компанию им должен составлять инженерный здравый смысл. Помните. SIL – это не цель, а инструмент для управления рисками.

6.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 6.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 6.1.

Условие. Ожидается, что опасное событие вызовет взрыв с потенциальной потерей жизни (PLL) 22,8 [27]. Анализ показал частоту события. $5,7 \times 10^{-5}$ в год. Завод использует допустимый индивидуальный риск $1,0 \times 10^{-5}$ смертей/год.

Вопрос. Какой SIL требуется для СПАЗ/SIS, чтобы снизить риск до допустимого уровня?

Варианты.

- a) SIL=1.
- b) SIL=2.
- c) SIL=3.
- d) SIL=4.

Ответ С. SIL=3.

Решение.

1. Допустимая частота событий.

Частота=Допустимый риск $PLL=1,0 \times 10^{-5}/22,8=4,4 \times 10^{-7}$ событий.

2. Требуемая вероятность отказа (PFDavg).

PFDavg=Допустимая частота события.

$=4,4 \times 10^{-7}/5,7 \times 10^{-5}=7,7 \times 10^{-3}$.

3. Фактор снижения риска (RRF).

RRF=1, PFDavg=130 .

- SIL 1. RRF 10–100.
- SIL 2. RRF 100–1000.
- SIL 3. RRF 1000–10 000.

Для RRF ≥ 130 требуется SIL 2 (Однако SIL 2 может не покрыть минимальный RRF, поэтому нужен SIL 3).

Примечание. Предполагается, что.

- 1. SRS указывает только SIL, а не RRF.
- 2. Не используется фактор избегания для множественных смертей.

Тест 6.2.

Условие. FMEA -анализ выявил опасное состояние СПАЗ с резервированием (HFT = 1) с частотой 1 раз в 4 года. Автодиагностика выполняется ежедневно, интервал ручных проверок (TI) – 5 лет.

Вопрос 1. Классифицируется ли SIF как система низкого спроса?

Ответ. Да, так как частота запросов ($1/4$ года = $0,25/\text{год}$) $< 1/\text{год}$. TI (5 лет) $>$ DI (4 года), но $DI < 2 \times TI$ ($4 < 10$), что соответствует стандартам.

система классифицируется как система низкого спроса.

Обоснование:

Согласно стандартам МЭК 61508/61511, ключевой критерий для систем низкого спроса – частота запросов на выполнение защитной функции не превышает одного раза в год.

Анализ частоты запросов:

FMEA-анализ выявил, что опасное состояние возникает с частотой 1 раз в 4 года.

Это эквивалентно 0.25 запроса в год.

Вывод: $0.25/\text{год} < 1/\text{год}$, что явно соответствует определению системы низкого спроса.

Проверка корректности интервала проверок (TI):

Для систем низкого спроса критически важен период, в течение которого скрытые отказы могут оставаться необнаруженными. Стандарты требуют, чтобы интервал ручных проверок (TI) был достаточно коротким, чтобы вероятность множественных отказов была приемлемо низкой.

Эмпирическое правило (руководящий принцип): TI должен быть меньше или, в крайнем случае, не более чем в два раза превышать среднюю наработку на отказ по требованию ($1/\lambda$, которая в данном контексте аппроксимируется частотой запроса 1 раз в 4 года).

В нашем случае:

Частота запроса: 1 раз в 4 года $\rightarrow$ Условный «период» = 4 года.

TI = 5 лет.

Да, TI (5 лет) > периода запроса (4 года), что не является идеальным, но критическое соотношение $2 \times \text{TI} = 10 \text{ лет} > 4 \text{ лет}$ – выполняется. Это означает, что скрытые отказы в среднем будут обнаруживаться ручной проверкой до того, как с высокой вероятностью произойдет второе опасное событие. Таким образом, установленный TI = 5 лет является допустимым, хотя и близким к границе.

Вопрос 2. Какие требования выставляются по SIL 3 в системах низкого спроса?

Для обеспечения требований SIL 3 в системах низкого спроса стандарт предъявляет строгие требования к аппаратной отказоустойчивости (HFT).

Требование HFT = 1 означает, что архитектура системы должна оставаться работоспособной при возникновении одного опасного отказа. На практике это почти всегда означает архитектурное резервирование.

Обязательно требуется: резервирование каналов измерения (например, 2oo3, 1oo2) и резервирование логического вычислителя (ПЛК, 1oo2D или аналоги). Использование одиночного (симплексного) ПЛК для SIL 3, как правило, недопустимо.

Тест 6.3.

Условие. Используется SIF с HFT=0, временем срабатывания 50 мс и временем до инцидента 100 мс.

Исходные данные.

$\lambda_{DD} = 8,5 \times 10^{-6}/\text{час}$, $\lambda_{DU} = 0,5 \times 10^{-6}/\text{час}$.

Вопрос 1. К какому классу спроса относится SIF?

Ответ. Это система высокого (непрерывного) спроса.

Обоснование.

Так как время срабатывания системы ($T_1 = 50 \text{ мс}$) и время до развития необратимого инцидента ($T_2 = 100 \text{ мс}$) соотносятся как T_1 (50

мс) < T₂ (100 мс), то это означает, что система должна **непрерывно** отслеживать процесс и успеть среагировать на опасное отклонение *до того*, как оно приведет к аварии. Это классический признак системы высокого спроса.

Вопрос 2. Рассчитать PFH и определить SIL.

Ответ: PFH = 9×10^{-6} /час, что соответствует **SIL 1**.

Решение и обоснование.

Общая интенсивность опасных отказов (λ_D): Это сумма всех опасных отказов, независимо от того, обнаруживаются они диагностиками или нет.

$$\lambda_D = \lambda_{DD} + \lambda_{DU} = 8.5 \times 10^{-6} / \text{час} + 0.5 \times 10^{-6} / \text{час} = 9.0 \times 10^{-6} / \text{час}$$

Для симплексной системы (HFT=0) в режиме высокого спроса, стандарт МЭК 61508-6 (Приложение В) дает простую и консервативную формулу:

$$PFH = \lambda_D.$$

Почему так? В системе высокого спроса функция безопасности активна постоянно. Любой опасный отказ (как обнаруженный λ_{DD} , так и необнаруженный λ_{DU}) немедленно приводит к потере функции безопасности. В момент своего возникновения такой отказ делает систему неспособной выполнить свою защитную функцию.

Обнаруженный отказ (λ_{DD}): Да, система перейдет в безопасное состояние (например, остановится), но сам факт ее остановки означает, что в этот конкретный момент она не смогла выполнить свою функцию по непрерывному контролю и предотвращению инцидента. Она уже «провалилась». Поэтому λ_{DD} учитывается в полном объеме.

1. Сравнение с таблицей SIL для систем высокого спроса:

SIL 4: PFH $\geq 10^{-9}$ до $< 10^{-8}$.

SIL 3: PFH $\geq 10^{-8}$ до $< 10^{-7}$.

SIL 2: PFH $\geq 10^{-7}$ до $< 10^{-6}$.

SIL 1: PFH $\geq 10^{-6}$ до $< 10^{-5}$.

Наш результат PFH = 9.0×10^{-6} /час попадает в диапазон $\geq 10^{-6}$ до $< 10^{-5}$, что соответствует **SIL 1**.

Итоговый ответ:

- Класс системы: Высокого спроса.
- Рассчитанный PFH: 9.0×10^{-6} /час.
- Достигаемый SIL: SIL 1.

Архитектурное ограничение (HFT):

Для систем высокого спроса стандарт предъявляет жесткие требования к аппаратной отказоустойчивости (HFT):

Для **SIL 1** допускается HFT = 0.

Для **SIL 2** требуется HFT ≥ 1 .

Для **SIL 3** требуется HFT ≥ 2 .

В нашем случае:

- Рассчитанный PFD (9.0×10^{-6} /час) соответствует SIL 1.

• Архитектура системы (HFT=0) также соответствует требованиям для SIL 1.

Вывод. Система может быть классифицирована как **SIL 1** как по вероятности отказа, так и по архитектурным ограничениям.

Тест 6.4. Расчет SIL. Нюансы и подводные камни.

Условие. SIF с $PFD_{avg} = 2,5 \times 10^{-3}$ работает в системе, где допустимый риск -1×10^{-4} смертей/год. Частота опасного события – 0,1/год.

Вопрос 1. Достаточен ли данный SIL для соответствия требованиям?

Варианты.

- a) Да, т.к. $PFD_{avg} < 1 \times 10^{-2}$ (SIL 1).
- b) Нет, т.к. итоговый риск ($2,5 \times 10^{-4}$) превышает допустимый.
- c) Да, если увеличить диагностическое покрытие.
- d) Нет, требуется дополнительный SIF.

Ответ вам.

Объяснение.

Итоговый риск = $PFD_{avg} \times \text{Частота события} = 2,5 \times 10^{-3} \times 0,1 = 2,5 \times 10^{-4}$, что выше допустимого (1×10^{-4}).

Вопрос 2. Выбор оборудования.

Условие.

Для SIF с $PFH = 8 \times 10^{-7}$ отказов/час выбрано оборудование.

- Датчик (SFF=90%, HFT=1).
- Логика (SFF=99%, HFT=2).
- Клапан (SFF=60%, HFT=0).

Вопрос. Соответствует ли архитектура требованиям SIL 3?

Варианты.

- a) Да, т.к. PFH в пределах SIL 3.
- b) Нет, из-за клапана с HFT=0.
- c) Да, если добавить резервирование клапана.
- d) Нет, т.к. SFF клапана <90%.

Ответ b.

Объяснение.

Для SIL 3 клапан (тип А, SFF=60%) необходимо оказоустойчивое оборудование $HFT \geq 1$ (МЭК 61511-1, Таблица 6). Текущее $HFT=0$ недопустимо.

Вопрос 3. Какая PFD_{avg} получится при использовании формулы. $PFD_{avg} = \lambda DU \times TI / 2 \times (1 - DC)$.

Условие.

SIF имеет:

- $\lambda DU = 1 \times 10^{-6}$ /час, $TI = 1$ год.
- Диагностическое покрытие (DC) = 90%.

Варианты.

- a) 5×10^{-5} .
- b) $1,8 \times 10^{-6}$.

с) $4,5 \times 10^{-7}$.

д) Ошибка в формуле.

Ответ д.

Объяснение.

Правильная формула.

$$PFD_{avg} = \lambda DU \times TI / 2 \times (1 - DC) + \lambda DD \times MTTR$$

В условии не хватает данных по λDD и $MTTR$.

Вопрос 4. Какой будет реальная PFD_{avg} ?

Условие. Инженер рассчитал SIL для SIF с $PFD_{avg} = 3 \times 10^{-3}$, но забыл учесть.

- Время восстановления ($MTTR$) = 8 часов.
- $\lambda DD = 5 \times 10^{-7}$ /час.

Варианты.

а) $3,004 \times 10^{-3}$.

б) $3,5 \times 10^{-3}$.

с) $4,1 \times 10^{-3}$.

д) Не изменится.

Ответ а.

Объяснение.

Коррекция для обнаруженных отказов.

$$\Delta PFD = \lambda DD \times MTTR_{8760} = 5 \times 10^{-7} \times 8 \approx 4,0 \times 10^{-6}.$$

$$\text{Итоговая } PFD_{avg} \approx 3 \times 10^{-3} + 4,0 \times 10^{-6} \approx 3 \times 10^{-3}.$$

Вопрос 5. Какое дополнительное условие делает риск допустимым?

Условие.

SIF с SIL 2 ($PFD_{avg} = 1 \times 10^{-2}$) применяется для события с частотой 0,05/год.

Варианты.

а) $PLL = 1$.

б) $DC > 95\%$.

с) Время реакции < 1 секунды.

д) $HFT=2$.

Ответ А.

Объяснение.

$$\text{Риск} = PFD_{avg} \times \text{Частота} \times PLL.$$

При $PLL=1$. $1 \times 10^{-2} \times 0,05 \times 1 = 5 \times 10^{-4}$ (допустимо для многих стандартов).

Ключевые выводы по тестам.

1. PFD_{avg} . Риск. Даже соответствие SIL не гарантирует приемлемого риска – всегда проверяйте итоговые значения.

2. Архитектурные ограничения. HFT и SFF критичны. Например, SIL 3 требует $HFT \geq 1$ для компонентов с $SFF < 90\%$.

3. Ошибки в формулах. Упрощенные расчеты могут дать неверный результат.

4. Диагностика и MTTR. Обнаруженные отказы (λ_{DD}) часто незначительно влияют на PFD_{avg} .

5. Контекст. PLL, частота событий и дополнительные SIF могут изменить допустимость риска.

Рекомендация. Всегда проверяйте.

- Полноту формулы (учтены ли λ_{DD} , MTTR).
- Соответствие архитектуры таблицам МЭК 61508.
- Итоговый риск, а не только SIL.

6.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на пункты стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 6».

Тест 6.7. HFT исполнительного устройства [24].

Узел ИУ, состоящий из электромагнитного клапана, клапана быстрого выпуска, привода и дроссельной заслонки, используется в приложении с низким уровнем требований SIL 2. Сборка элементов имеет SFF 54%. Для ответа использовать таблицы 6.2-6.5.

Вопрос 1. Какое HFT требуется в соответствии с МЭК 61508 Route 1H?

Вопрос 2. Какой HFT требуется в соответствии с Route 2H МЭК 61508?

Вопрос 3. Какой HFT требуется согласно МЭК 61511.2016?

Для ответа использовать таблицы из стандартов 61508 и 61 511.

Таблица 6.2

SIL	Запрос	Min HFT
1	Любой	0
2	С низким запросом	0
2	С высоким или постоянным	1
3	Любой	1
4	Любой	2

Таблица 6.3

Доля безопасных отказов	Устойчивость к аппаратным отказам		
TYPE A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% < 90%	SIL 2	SIL 3	SIL 4
90% < 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Таблица 6.4 Route 2_H

SIL	Запрос	Min HFT
1	Любой	0
2	С низким запросом	0
2	С высоким или постоянным	1
3	Любой	1
4	Любой	2

Таблица 6.5 Type B Route 1_н

Доля без- опасных отказов	Устойчивость к аппаратным отказам		
	Не допуска- ется	SIL 1	SIL 2
< 60%	Не допуска- ется	SIL 1	SIL 2
60% < 90%	SIL 1	SIL 2	SIL 3
90% < 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Для получения дополнительной информации см. [24].

Тест 6.8. Для SIF используется комплект нерезервированного (1oo1, HFT = 0) оборудования безопасности. DTI составляет 100 миллисекунд.

Система запрограммирована на перевод процесса в безопасное состояние, когда диагностика указывает на внутреннюю отказ. Время реакции SIF для достижения безопасного состояния составляет 50 миллисекунд.

Время безопасности процесса составляет 500 миллисекунд. Средний интервал спроса равен 1 сек. Следующие данные о частоте отказов получены для оборудования SIF.

$\lambda_{DD} = 8,5 \cdot 10^{-6}$ отказов в час.

$\lambda_{DU} = 0,5 \cdot 10^{-6}$ отказов в час.

Какой уровень SIL достигается с помощью этой конструкции, исходя из требований PFH?

Для ответа использовать таблицы 6.2- 6.5, взятые из стандартов 61508 и 61 511.

Тест 6.9. Для реализации SIF используется нерезервированная архитектура (1oo1, HFT = 0) оборудования безопасности. DTI составляет 100 миллисекунд.

Система запрограммирована на перевод процесса в безопасное состояние, когда диагностика указывает на внутренний отказ. Время отклика SIF для достижения безопасного состояния составляет 50 миллисекунд.

Время безопасности процесса составляет 2 секунды. Средний интервал срабатывания составляет 1 минуту. Для оборудования получены следующие данные по интенсивности отказов путем суммирования интенсивностей отказов всех компонентов.

$\lambda_{DD} = 8,5 \cdot 10^{-6}$ отказов в час

$\lambda_{DU} = 0,5 \cdot 10^{-6}$ отказов в час

Какой уровень SIL достигается данной конструкцией на основе требований к PFH?

Вопрос 1. Какова архитектура оборудования безопасности в данной задаче?

А) 1oo2.

В) 1001.

С) 2002.

Д) 2001.

Вопрос 2. Каково время отклика SIF для достижения безопасного состояния?

А) 50 миллисекунд.

В) 100 миллисекунд.

С) 1 секунда.

Д) 2 секунды.

Вопрос 3. Какова общая интенсивность опасных отказов (λD) для системы SIF?

А) $8,5 \cdot 10^{-6}$ отказов в час.

В) $0,5 \cdot 10^{-6}$ отказов в час.

С) $9 \cdot 10^{-6}$ отказов в час.

Д) $1 \cdot 10^{-6}$ отказов в час.

Вопрос 4. Какое время безопасности процесса в данной системе?

А) 50 миллисекунд.

В) 1 секунда.

С) 2 секунды.

Д) 5 секунд.

7. СПЕЦИФИКАЦИЯ СИСТЕМЫ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ.

7.1 Назначение и роль SRS в жизненном цикле безопасности.

Задание 7.1. Уяснить назначение и роль спецификации SRS в жизненном цикле безопасности.

Спецификация требований к безопасности (Safety Requirements Specification, SRS) – это основной документ проекта СПАЗ, который формально определяет «ЧТО должна делать система», «ПОЧЕМУ она это должна делать» и «НАСКОЛЬКО ХОРОШО она должна это делать».

SRS создается на основе анализа опасностей и рисков (HAZOP, LOPA) и является исходным документом для проектирования, верификации, монтажа и эксплуатации системы.

Ключевой принцип. SRS должна содержать измеримые, однозначные и верифицируемые требования.

Структура и содержание SRS (на основе общих принципов проектирования).

1. Требования к функциональности (ЧТО делать?).

Оно представляется в виде описания каждой Функции Безопасности (SF). Для каждой функции должно быть четко указано:

Цель. Например, «Остановить насос П-101 при превышении давления в аппарате А-202 выше 15 бар».

Иницилирующее событие. «Аналоговый сигнал давления от РТ-202».

Логика. «Если РТ-202 > 15 бар, то выдать дискретный выходной сигнал на закрытие клапана ZV-101 и останов насоса П-101».

Действие. «Закрыть отсечной клапан ZV-101 и отключить питание насоса П-101».

Время отклика. «Весь контур защиты (датчик + логика + исполнительный механизм) должен выполнить функцию в течении 2 секунды с момента превышения уставки». Это прямое отражение принципа Детерминированности.

2. Требования к полноте безопасности (НАСКОЛЬКО ХОРОШО?).

Требуемый уровень полноты безопасности (SIL). Для каждой функции безопасности должен быть указан целевой SIL (например, SIL 2), полученный в результате анализа LOPA.

Целевые показатели надежности. Требуемая средневероятная вероятность опасного отказа (PFDavg, например, < 1.00E-03 для SIL 2) и частота опасных отказов (PFH для режима высоких требований).

3. Требования к аппаратному обеспечению (КАКИМ СПОСОБОМ?)

Архитектурные ограничения. Требования к аппаратному резервированию (HFT) и показателю безопасных отказов (SFF) для достижения целевого SIL.

Пример. «Архитектура подсистемы датчиков давления для функции SF-001 должна иметь $HFT \geq 1$ и использовать датчики с $SFF > 90\%$ ». Это формальное выражение принципов Отказоустойчивости и Избыточности.

Требования к отказобезопасности. Четкое определение безопасного состояния для каждого элемента.

Пример. «При потере питания или обрыве сигнального провода датчик РТ-202 должен инициировать аварийный сигнал, а логический решатель должен интерпретировать это как команду на выполнение функции безопасности». Это формальное требование Отказобезопасности и Отказоустойчивости.

Требования к отказоустойчивости. В стандартах серии МЭК 61511 в разделе «Спецификация требований к безопасности ПСБ» указано, что требования должны включать максимально допустимую интенсивность ложных срабатываний».

Пример. «При ложном отказе контроллера СПАЗ должен выдаваться автоматический сигнал watchdog timer «Зависание СПАЗ». Во время нормальной работы ПЛК регулярно сбрасывает счетчик сторожевого таймера, чтобы предотвратить его истечение. Если сброса не произошло, то происходит принудительная перезагрузка ПЛК.

Отказобезопасность гарантирует, что отказ любого компонента системы приведет объект в предсказуемое БЕЗОПАСНОЕ состояние.

Конструкция и логика СПАЗ должны быть таковы, что любая неисправность (потеря питания, обрыв провода, сбой процессора) интерпретируется как однозначный сигнал к активации защиты и перевода процесса в состояние с минимальным риском.

Отказоустойчивость гарантирует, что одиночный отказ одного или нескольких компонентов НЕ приведет к потере защитной функции и позволит системе продолжать работу в штатном режиме БЕЗ активации останова.

Система должна быть способна переносить отказы без потери своей функциональности. Это достигается за счет избыточности (дублирования) контуров одноточечной защиты, путем использования специальных архитектур, обеспечивающих отказоустойчивость.

Современная СПАЗ должна быть одновременно и отказоустойчивой (чтобы избегать ненужных остановок), и отказобезопасной (чтобы гарантировать безопасность при любых обстоятельствах).

4. Требования к программному обеспечению.

Требования к ПО. Запрет на использование несертифицированных инструментов и языков программирования, не предназначенных для задач безопасности.

Пример. «Логика должна быть реализована на сертифицированном ПЛК безопасности с использованием функциональных блочных диаграмм (FBD) в среде TIA Portal Safety. Запрещено использование универсальных языков высокого уровня (например, C++) без валидации». Это основа для Верификации и Валидации.

5. Требования к интерфейсам и управлению.

Требования к независимости АСДУ и СПАЗ. Должно быть четкое разграничение функций управления и безопасности..

Пример. «Сигналы от датчиков РТ-202 должны поступать в СПАЗ по независимым аппаратным каналам, физически отделенным от каналов АСУТП». Это прямое требование Функциональной независимости и Иерархичности защиты.

Человеко-машинный интерфейс (АСДУ).

Система должна быть спроектирована для работы в паре с человеком.

Должна быть обеспечена прозрачность и трассируемость последствий. Оператор должен не только видеть причину срабатывания, но и получать прогноз последствий предлагаемых системой действий (например, «Останов насоса А приведет к останову секции Б на 8 часов»).

При реализации 3-х уровней контроля должно быть четкое разделение зон ответственности: полный автоматизм (СПАЗ/SIS), дистанционное управление (АСДУ) и локальное ручное дублирование.

Пример. «При срабатывании функции SF-001 на графической мнемосхеме оператору должен быть явно указан инициирующий датчик (РТ-202), выполненные действия (закрытие ZV-101, останов П-101) и текущий статус системы (требуется перезапуск/сброс)».

Это позволяет принять взвешенное решение в условиях неопределенности.

6. Требования к многослойности защиты.

Иерархичность и эшелонирование защиты (Защита в глубину). Защита должна состоять из каскада независимых и разнородных рубежей.

- Уровень 1. Предупредительно-упреждающий (АСУ ТП). Основная система управления пытается мягко вернуть процесс в норму через регулирование и предупредительную сигнализацию оператору.

- Уровень 2. Безаварийный останов (СПАЗ, мягкий останов). При невозможности восстановления рабочего режима работа оборудования плавно прекращается без повреждения технологической линии.

- Уровень 3. Аварийный останов (СПАЗ, жесткий останов). Последний рубеж, обеспечивающий полную остановку процесса для предотвращения катастрофы.

Критерий. Каждый последующий уровень должен иметь более высокую надежность и независимость от предыдущих.

Функциональная независимость.

Чтобы избежать общих отказов, различные уровни защиты и их компоненты должны быть максимально независимыми. Датчики, контроллеры и исполнительные механизмы для разных уровней должны быть физически и программно разделены (диверсифицированы).

Избыточность и живучесть.

Критичные функции должны быть дублированы для обеспечения работоспособности системы даже при отказе одного или нескольких компонентов.

Архитектура. Применение отказоустойчивых архитектур (напр., 2oo3, 1oo2D) для логических решателей (ПЛК) и датчиков.

Диагностика. Реализация непрерывного самоконтроля для обнаружения и локализации отказов аппаратной части.

Детерминированность и предсказуемость.

Поведение системы в аварийной ситуации должно быть строго предопределено и понятно для персонала.

Простая и верифицируемая логика. Предпочтение простым алгоритмам («если температура > X, то закрыть клапан Y») перед сложными многофакторными моделями.

Время отклика (RT). Система должна быть рассчитана так, чтобы ее время срабатывания было на порядок меньше времени развития аварии.

7. Требования верификации и валидации на всем жизненном цикле [23 - 25].

Каждая функция безопасности должна иметь строгое документальное обоснование и должна быть проверена на соответствие ему.

Верификация («Мы сделали систему правильно?»). Проверка на соответствие проектной документации.

Валидация («Мы сделали правильную систему?»). Проверка того, что система в сборе действительно выполняет возложенные на нее функции безопасности.

С применением перечисленных принципов проектирования СПАЗ действует по принципу «градуированного ответа».

- Анализирует тяжесть отклонения.
- Пытается устранить его наименее затратным способом (мягкое регулирование).
- Эскалирует меры воздействия только в случае неудачи предыдущих шагов.
- Информировывает оператора о своих действиях и последствиях, оставляя за ним право на принятие решения в рамках отведенного времени.

Такой подход не только снижает количество ложных и избыточных остановок, но и повышает общее доверие к системе безопасности со стороны производственного персонала, что не менее важно.

8. Требования к эксплуатации и техобслуживанию.

Периодичность функциональных проверок. На основе расчетов PFDavg определяется максимальный интервал между проверками.

Пример. «Функция SF-001 должна проходить полную функциональную проверку с тестированием датчика, логики и исполнительного механизма не реже одного раза в 12 месяцев».

Процедуры деблокирования и перезапуска. Четкое описание, как привести систему в рабочее состояние после срабатывания, исключающее возможность сброса до устранения причины.

Принципы проектирования (Отказобезопасность, Отказоустойчивость и др.) являются философской основой. SRS – это тот документ, где эти принципы превращаются в конкретные, измеримые и проверяемые технические требования.

7.2. ПРАКТИКУМ ПО РАЗРАБОТКЕ СПЕЦИФИКАЦИИ СПАЗ.

Задание 7.2. В предположении наличия исходных требований ОПО к СПАЗ подготовить отчет по верификации и отчет по валидации решения в кейсе.

Кейс 7.1. Спецификация экономического обоснования внедрения СПАЗ [27].

Ситуация. На нефтеперерабатывающем заводе выявлена опасность с потенциальным ущербом \$2,5 млн и частотой события $7,0 \times 10^{-4}$ /год. Предлагается установить СПАЗ с PFD=0,01 и годовой стоимостью \$5,500. В спецификации нужно привести оценку целесообразности СПАЗ.

Задания.

1. Рассчитайте соотношение выгод к затратам.
2. Проанализируйте, при каком PFD система станет экономически нецелесообразной.
3. Предложите альтернативные меры, если соотношение выгод к затратам $< 0,3$.

Задание 1. Годовые потери без СПАЗ. Ущерб $\times$ Частоту = $\$2,500,000 \times 7,0 \times 10^{-4} = \$1,750$ в год.

Расчет годовых потерь при работе СПАЗ.

СПАЗ с PFD=0.01 означает, что она не сработает только в 1% случаев. Поэтому остаточный риск рассчитывается как.

(Потери без СПАЗ) $\times$ (Вероятность отказа СПАЗ) = $\$1,750 \times 0.01 = \$17.5$ в год.

Годовая выгода.

Потери без СПАЗ – выгода со СПАЗ = $\$1,750 - \$17.5 = \$1,732.5$ в год.

Соотношение выгод к затратам.

Выгода / Затраты = $\$1,732.5 / \$5,500 \approx 0.315$.

Ответ на задание 1. Соотношение выгод к затратам составляет ~ 0.315 .

Анализ целесообразности. Несмотря на то, что значение выше 0.3, оно очень близко к границе. На решение могут повлиять другие факторы, неучтенные в модели (стоимость простоя, репутационные риски, требования законодательства). Однако, чисто экономически, проект окупает лишь 31.5% своих ежегодных затрат, что делает его сомнительным или нецелесообразным для реализации только на основе экономии от избегания ущерба.

Задание 2. При каком PFD система станет экономически нецелесообразной?

Экономическая нецелесообразность наступает, когда Выгода << Затрат.

Формула для расчета. $\text{Выгода} = (\text{Ущерб} \times \text{Частота}) \times \text{PFD}$.

Находим точку безубыточности.

$(\text{Ущерб} \times \text{Частота}) \times \text{PFD} = \text{Годовые затраты на СПАЗ}$.

$\$1,750 \times \text{PFD} = \$5,500$.

Решаем уравнение относительно PFD.

$\text{PFD} = \$5,500 / \$1,750$.

$\text{PFD} \approx 3.14$.

Ответ на задание 2. Система станет экономически нецелесообразной (убыточной), если ее PFD будет хуже (больше) значения ~ 3.14 . Это абсурдное значение для системы безопасности (PFD. Оно не может быть >1), что означает следующее. «данная система с заявленными характеристиками (PFD=0.01) никогда не будет экономически целесообразна по чисто финансовым соображениям при таких исходных данных. Затраты на ее содержание всегда будут выше предотвращаемых ежегодных потерь.

Мы рассматриваем ее только, если того требуют нормативы или если нам критически важно снизить частоту события.

Задание 3. Альтернативные меры при соотношении <0.3 .

Соотношение 0.315 формально немного выше 0.3, но учитывая пограничное значение и исправленный расчет, предложения остаются актуальными.

Отказ от внедрения. Если риск признан допустимым (ALARP), руководство может принять решение о его принятии без установки дополнительных дорогостоящих систем.

Поиск более простых и дешевых технических решений. Именно об этом говорится в исходном решении – ESD-защита без использования дорогого программируемого логического контроллера (ПЛК). Это может быть.

- Релейная система на панели управления.
- Датчики с прямым подключением к отсекательному клапану (например, системы с «пилотным управлением»).
- Пневматические или механические системы (например, системы типа «тросовый выключатель»).

Такие системы часто имеют более низкие капитальные и операционные расходы, хотя их PFD может быть немного хуже (например, 0.1 вместо 0.01), но в данном случае это может улучшить соотношение затрат и выгод.

Снижение риска другими, не техническими средствами.

- Пересмотр процедур эксплуатации и ремонта.
- Усиление обучения персонала на отработку правильных действий при аварийных ситуациях.
- Установка дополнительных предупредительных знаков, ограждений.
- Внедрение более строгого планового профилактического обслуживания существующего оборудования для снижения базовой частоты события.
- Страхование риска. Передача финансовых последствий риска страховой компании может быть более экономически эффективным решением.

Пример. *Проект спецификации экономического обоснования.*

Спецификация № ЭО-7.1 на систему аварийной защиты (СПАЗ) для объекта [Наименование объекта, например, Резервуарный парк R-101].

1. Введение.

Настоящий документ содержит экономическое обоснование целесообразности внедрения системы аварийной защиты (СПАЗ) на объекте [Наименование объекта] в целях (снижения) выявленного риска.

2. Исходные данные.

- Потенциальный ущерб от реализовавшегося события 2,500,000 USD.
- Базовая частота события (без СПАЗ) 7.0×10^{-4} /год.
- Годовой риск (без СПАЗ) 1,750 USD/год $(2,500,000 \times 7.0 \times 10^{-4})$.
- Целевое PFD для СПАЗ 0.01.
- Расчетные капитальные затраты (CAPEX) [Указать, если есть].

- Расчетные годовые эксплуатационные затраты (OPEX) 5,500. USD/год Включая ТО, ремонт, диагностику.

3. Расчет экономической эффективности (Показатель. Расчет. Значение).

- Остаточный риск (со СПАЗ) $1,750 \text{ USD/год} \times 0.01$ 17.5 USD/год.
 - Годовая выгода (снижение потерь) 1,750 USD/год - 17.5 USD/год 1,732.5 USD/год.
 - Соотношение выгод к затратам $1,732.5 / 5,500$ ~0.315.
- #### 4. Выводы и рекомендации.

4.1. Расчетное соотношение выгод к затратам (0.315) находится на границе общепринятого корпоративного критерия целесообразности (0.3). Чисто экономически эффективность проекта является низкой.

4.2. Установка СПАЗ с заданными параметрами ($PFD=0.01$) и годовыми затратами в \$5,500 не может быть рекомендована исключительно на основе экономии от избегания ущерба.

5. Предлагаемое решение

На основании выводов п.4, а также требования снизить риск до уровня ALARP, предлагается рассмотреть альтернативные варианты реализации защиты.

Например, внедрение упрощенной ESD-системы на релейной логике. Ожидаемые параметры. $PFD \sim 0.1$, годовые затраты $\sim 2,000$ USD/год.

Расчет для этого варианта. Остаточный риск $= 1,750 \times 0.1 = 175$ USD/год. Выгода $= 1,750 - 175 = 1,575$ USD/год. Соотношение $= 1,575 / 2,000 = 0.787$ (что является приемлемым показателем).

6. Заключение

Установка СПАЗ в первоначально предложенной конфигурации экономически нецелесообразна. Рекомендуется к реализации «Вариант Б» (упрощенная ESD-система) как обеспечивающий адекватное снижение риска с приемлемым соотношением затрат и выгод.

[Должность].

[Подпись].

[ФИО].

[Дата].

Кейс 7.2. Классификация оборудования в SIF.

Ситуация. Для сепаратора проектируется контур защиты SIF, который реализуется на основе:

- Датчик уровня (LT-2025).
- Выходной клапан (LV-2003).
- Ручной переключатель (HS-2000).

Задания.

1. Определите, какое оборудование является основным и вспомогательным.

Ответ.

Основное оборудование: LV -2003 (непосредственно предотвращает «проскок»).

Вспомогательное. HS-2000 (нормативное требование), насос MC-1005 (не влияет на опасность).

Внести эти требования в SRS.

Кейс 7.3.

Указать в спецификации выбор режима срабатывания (Отключение при обесточивании и Срабатывание при подаче энергии) для каждого контура защиты.

Ситуация. Для клапана высокого давления необходимо выбрать функции:

- Отключение при обесточивании.
- Срабатывание при подаче энергии.

Задание. Выбрать, как клапан будет срабатывать в аварийной ситуации: самопроизвольно при пропадании питания или по сигналу при подаче энергии.

1. Сравнить риски каждого варианта.
2. Указать, какие дополнительные меры нужны для отключения при обесточивании.
3. Внести требования в SRS.

1. Сравнение рисков:

1.1. Отключение при обесточивании:

Принцип: Пока на клапан подается энергия, он открыт/закрыт (работает). Если питание пропало (отказ) – клапан *автоматически* переходит в безопасное состояние.

Риск: **НИЗКИЙ**. Система по умолчанию безопасна. Самый частый тип отказа (потеря питания) приводит к безопасной остановке процесса.

Аналогия: Предохранительный клапан в системе отопления, который срабатывает, если давление слишком высокое, без всякого электричества.

1.2. Срабатывание при подаче энергии:

Принцип: Чтобы перевести клапан в безопасное состояние, на него нужно *подать* энергию.

Риск: **ВЫСОКИЙ**. Если пропадет питание или оборвется кабель, система не сможет выполнить защитную функцию. Это *ненадежно по своей природе*.

Аналогия: Чтобы потушить пожар, нужно включить систему пожаротушения. А если электричество отключилось, система не работает.

2. Дополнительные меры для срабатывания при подаче энергии:

Поскольку этот режим опасен, его можно применять **только** при наличии дополнительных мер, компенсирующих риски:

- Независимый и резервированный источник питания (ИБП, аккумуляторы).
- Непрерывный мониторинг целостности цепи питания и управления до самого клапана. Любой обрыв или неисправность должны немедленно сигнализироваться как неисправность.
- Высокий уровень надежности всех компонентов цепи.

3. Требование в спецификации по безопасности (пример):

- **Функциональное требование:** Аварийный отсечной клапан высокого давления К-101 должен закрываться при активации СПАЗ/SIS.
- **Требование по отказоустойчивости:** Клапан К-101 должен быть выполнен в исполнении **»перевод в безопасное состояние при обесточивании»**.
- Потеря питания или управляющего сигнала должна приводить к его безопасному закрытию.
Внести эти требования в SRS

Кейс 7.4. Установление в спецификации времени отклика СПАЗ/SIS.

Ситуация. Время безопасности процесса – 5 сек.

Задание: убедиться, что система защиты сработает достаточно быстро, чтобы успеть остановить аварию.

1. Определить оптимальное время отклика СПАЗ/SIS.
2. Оценить последствия выбора времени 4 сек и 2,5 сек.
3. Предложить архитектуру СПАЗ/SIS для обеспечения заданного времени.

1. Определение оптимального времени отклика:

- **Время безопасности процесса (5 сек):** Это время, которое у вас есть с момента начала аварии до момента, когда она станет необратимой (взрыв, разрушение).
- **Правило «50%»:** Оптимальное время отклика СПАЗ/SIS должно быть **не более половины** времени безопасности процесса.
- **Расчет:** $5 \text{ сек} / 2 = 2.5 \text{ сек}$.
- **Логика:** Это дает **запас прочности**. У системы есть 2.5 сек на срабатывание, и еще 2.5 сек в запасе на непредвиденные задержки, неточности расчетов или развитие аварии быстрее, чем ожидалось.

2. Оценка последствий выбора времени.

Время отклика 4 сек:

Последствие: КРИТИЧЕСКИЙ РИСК.

Почему: СПАЗ/SIS будет срабатывать почти в самый последний момент. Любая небольшая дополнительная задержка (например, инерция клапана) приведет к тому, что система не успеет предотвратить аварию. Запас прочности практически отсутствует.

Время отклика 2.5 сек:

Последствие: БЕЗОПАСНЫЙ ВАРИАНТ.

Почему: Соответствует правилу 50%, обеспечивает достаточный запас прочности. Однако это **технически сложнее**, так как требуется применение высокоскоростных компонентов.

3. Предлагаемая в спецификации архитектура СПАЗ/SIS:

Чтобы гарантированно уложиться в 2.5 сек, нужна архитектура без использования «медленных» элементов:

- **Высокоскоростные датчики** (например, пьезоэлектрические, с малым временем отклика).
- **Быстродействующий ПЛК** или, что еще лучше, специализированные релейные схемы или твердотельные логические решатели (SSS), которые работают быстрее ПЛК.
- **Быстродействующий исполнительный механизм** (например, пневмоцилиндр с соленоидным клапаном прямого действия, а не медленный электрический мотор).

Кейс 7.5. Спецификация SIF для печи .

Ситуация.

На технологической печи существует риск подачи недостаточного количества топливного газа, что может привести к его незапланированному гашению. После гашения несгоревший газ может продолжить поступать в топку, создавая взрывоопасную концентрацию.

Система ПАЗ (СПАЗ/SIS) должна предотвратить это путем аварийного отключения подачи топлива по двум критическим параметрам.

- Низкий поток газа (FT-8421). Косвенный признак проблем на линии подачи.
- Низкое давление газа (PSL-8401/8402). Прямой и более быстрый признак разрыва линии или катастрофического падения давления.

Задания.

- Разработайте логику СПАЗ/SIS.
- Обоснуйте необходимость задержки для сигнала по низкому потоку.
- Проверьте соответствие архитектуры требованиям SIL 3.

Решение.

1. Разработка логики СПАЗ/SIS (с учетом лучших практик).

Для сигналов низкого давления (PSL-8401 и PSL-8402) – это сигналы «Немедленного действия».

Логика. **ЕСЛИ (PSL-8401 = LOW) ИЛИ (PSL-8402 = LOW) ТОГДА Немедленно инициировать команду на закрытие UV-8409 и UV-8411.**

Обоснование. Низкое давление, особенно на двух независимых датчиках, с высокой вероятностью указывает на серьезную аварию (разрыв трубопровода, отказ регулятора давления). Медлить здесь нельзя. Использование двух датчиков по схеме 1oo2 (один из двух) позволяет повысить доступность системы (снизить ложные срабатывания) без потери функциональной безопасности.

Сигнал низкого потока (FT-8421). Это сигнал «Действия с задержкой».

Логика. ЕСЛИ (FT-8421 < MIN) В ТЕЧЕНИЕ > 15 секунд ТО-ГДА Инициировать команду на закрытие UV-8409.

Обоснование. Поток – более инерционный и менее стабильный параметр. Кратковременные колебания – это норма. Для исключения ложных срабатываний вводится таймер задержки на срабатывание (Timer On Delay).

Итоговая архитектура SIF.

Давление. Два датчика PSL (1002 архитектура -> высокая доступность, соответствует SIL 3).

Поток. Один датчик FT (архитектура 1001, но с таймером для повышения доступности).

Исполнительный механизм. Два отсечных клапана (UV-8409, UV-8411), работающих от одного соленоида, или независимые соленоиды в зависимости от расчета надежности. Часто требуется архитектура с резервированием (например, 1002 для клапанов) для достижения SIL 3.

6. Обоснование задержки для низкого потока. Задержка в 15 секунд – это не произвольное число, а результат инженерной оценки процесса. Ее введение преследует две основные цели.

А. Подавление кратковременных колебаний. Расход топлива – динамический параметр. Кратковременные провалы расхода могут быть вызваны переключением насосов, работой регуляторов, небольшими изменениями в составе газа или просто турбулентностью потока. Эти колебания длятся секунды и не несут угрозы для процесса.

Без задержки система СПАЗ/SIS реагировала бы на каждое такое колебание, вызывая ложную остановку.

Частые ложные срабатывания останавливают производство, ведут к потере продукции, создают риски для оборудования при частых пусках/остановах и формируют у персонала привычку игнорировать аварийные сигналы или вручную их ингибировать, что полностью нивелирует пользу СПАЗ/SIS.

Б. Обеспечение времени для восстановления стабильного режима. В системе управления технологическим процессом (АСДУ) есть свои контуры регулирования (например, регулятор расхода FIC). При небольшом параметрическом возмущении АСДУ должна иметь возможность парировать его и вернуть поток в норму без вмешательства более высокого (аварийного) уровня – СПАЗ/SIS.

15 секунд – это расчетное или эмпирически установленное время, которого достаточно контуру регулирования АСУТП, чтобы скомпенсировать отклонение. СПАЗ/SIS вмешивается только в случае устойчивой, не компенсируемой неисправности.

Такая задержка не снижает безопасность, а повышает надежность системы в целом, предотвращая ложные срабатывания, при этом сохраняя ее функциональную безопасность для реальных аварийных ситуаций.

3. Проверка соответствия SIL 3.

Первоначальное решение не раскрывает этот критически важный аспект. Соответствие SIL 3 – это не только логика, но и аппаратное обеспечение.

А. Требования к аппаратной надежности (HFT).

Для достижения SIL 3 архитектура подсистем должна иметь HFT = 1 или выше. Это означает, что отказ одного компонента не должен приводить к потере защитной функции.

Давление (датчики). Архитектура 1oo2 (один из двух) для PSL-8401 и PSL-8402 является оптимальной. Она имеет HFT=1 (отказ одного датчика не препятствует срабатыванию по второму) и высокую диагностику отказов (диагностируемые отказы выявляются сравнением двух сигналов). Эта архитектура стандартно используется для SIL 2/SIL 3.

Поток (датчик). Архитектура 1oo1 (один из одного) для FT-8421 имеет HFT=0. Для использования в SIL 3 петле она недостаточна. Требуется, либо резервирование датчика (например, конфигурация 1oo2 или 2oo2), либо использование датчика с очень высоким показателем SFF > 99% и встроенной диагностикой, что на практике встречается редко и дорого.

Логический решатель (PLC/СПАЗ/SIS). Должен быть сертифицирован под SIL 3 и иметь резервированную архитектуру (например, двойное или тройное резервирование).

Исполнительные элементы (Клапаны). Обычно являются самым слабым звеном. Одиночный клапан (архитектура 1oo1) почти никогда не удовлетворяет требованиям SIL 3 по PFDavg. Необходимо резервирование, например, два клапана, установленных последовательно, с конфигурацией 1oo2 (оба должны закрыться для выполнения функции). Это увеличивает HFT до 1.

Б. Количественная проверка (Расчет PFDavg). Для окончательного подтверждения SIL 3 необходимо выполнить расчет вероятности отказа по требованию (PFDavg) для всей петли. Датчики -> Логика -> Исполнительный механизм.

Этот расчет выполняется с использованием данных о интенсивностях отказов (λ) каждого компонента, взятых из сертификатов и баз данных (например, по стандарту МЭК 61508/61511).

Расчет покажет попадает ли суммарная PFDavg петли в диапазон $[10^{-4}, 10^{-3}]$, требуемый для SIL 3. Без резервирования датчика потока и исполнительных клапанов это маловероятно.

Заключение по SIL 3. Предложенная в исходном решении архитектура в целом верна по логике, но, скорее всего, не соответствует SIL 3 по аппаратной реализации. Для соответствия требуется.

Резервировать датчик потока (FT-8421) по схеме 1oo2.

Убедиться, что логический решатель сертифицирован для SIL 3.

Установить необходимое для SIL3 степень диагностического покрытия.

Резервировать исполнительные элементы (установить два отсечных клапана последовательно с конфигурацией 1oo2), либо использовать ИУ с самодиагностикой.

Выполнить количественный расчет PFD_{avg} для подтверждения этих рекомендаций.

7.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 7.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 7.1. Спецификация. Требования к управлению деблокирующими ключами с использованием программно-аппаратных средств СПАЗ.

Вопрос 1. Что такое ключ деблокирования?

А) Средство, используемое для отключения блокировки выполнения функций АСУ ТП.

В) Средство маскирования канала измерения.

С) Средство включения канала измерения

Д) Тумблер на щите оператора.

Вопрос 2. Какова основная функция АРМ СПАЗ в контексте управления деблокирующими ключами?

А) Обеспечение физической защиты ключей.

В) Регистрация информации о первопричине и последовательности срабатывания.

С) Установка новых ключей.

Д) Обучение персонала по работе с ключами.

Вопрос 3. Какой протокол используется для управления КИП в АРМ СПАЗ?

А) Modbus.

В) HART-протокол.

С) Profibus.

Д) CAN-шина.

Вопрос 4. Почему необходим отдельный АРМ СПАЗ в проектировании автоматизированных систем (АС)?

А) Для повышения производительности системы.

В) Для управления деблокирующими ключами и регистрации информации.

С) Для уменьшения затрат на оборудование.

Д) Для обеспечения совместимости с другими системами.

Вопрос 5. Какую информацию регистрирует АРМ СПАЗ при срабатывании деблокирующих ключей?

- А) Только время срабатывания.
- В) Первопричину и последовательность срабатывания.
- С) Имя оператора, осуществляющего срабатывание.
- Д) Местоположение ключа.

Ответы.

А) Средство, используемое для отключения блокировки выполнения функций АСУ ТП.

В) Регистрация информации о первопричине и последовательности срабатывания СПАЗ.

В) HART-протокол.

В) Для управления деблокирующими ключами и регистрации информации.

В) Первопричину и последовательность срабатывания.

Объяснения Управление процессом деблокирования ключей обычно включает в себя несколько основных аспектов.

Блокировки необходимы для обслуживания, проведения работ или других специальных операций.

Деблокирование – это процесс отключения блокировок. восстановления защитных показателей.

Процедуры деблокирования должны быть строго регламентированы и выполняться только уполномоченным персоналом. Деблокирование может производиться с помощью специальных ключей или программных инструментов.

После деблокирования необходимо проверить восстановление целостности системы и убедиться, что все необходимые меры безопасности соблюдены

В целом, управление процессом деблокирования ключей в СПАЗ или аналогичных сложных требует **тщательного планирования, строгого контроля и точного документирования** для обеспечения безопасности, и безопасности систем. Для решения этих задач могут использовать специальный АРМ СПАЗ. Необходимость отдельного АРМ СПАЗ определяется в ТЗ на проектирование СПАЗ. Эти требования следует указать в спецификации.

Тест 7.2. Классификация оборудования в системе безопасности (SIF) уровня SIL 3.

Контекст. Пусть в техническом задании (SRS) определена система безопасности (SIF) уровня SIL 3. При обнаружении низкого уровня жидкости (LT-2025) в сепараторе необходимо.

1. Закрыть выходной клапан сепаратора (VI-2003) для защиты от «проскока» давления.

2. Закрыть входной клапан сепаратора (VI-2002), остановить насос (МС-1005) и перекрыть клапан другого блока (VI-3001) для минимизации технологических нарушений.

3. Выбрать логический решатель – ПЛК уровня SIL 3.

4. Добавить ручной переключатель (HS-2000) для соответствия нормам.

Вопрос 1. Какое оборудование классифицируется как основное в данной SIF?

- A) Входной клапан (VI-3001).
- B) Ручной переключатель (HS-2000).
- C) Выходной клапан сепаратора (VI-2003).
- D) Насос (MC-1005).

Ответ С. Выходной клапан сепаратора (VI-2003). Объяснение. Основные элементы SIF напрямую предотвращают опасность. VI-2003 исключает «проскок» давления – ключевой риск в данном сценарии.

Вопрос 2. Какое оборудование является вспомогательным?

- A) Выходной клапан сепаратора (VI-2003).
- B) Входной клапан сепаратора (VI-2002).
- C) Ручной переключатель (HS-2000).
- D) Все перечисленные.

Ответ D. Все перечисленные.

Объяснение.

- VI-2002 и MC-1005 защищают оборудование, но не являются критичными для предотвращения «проскока».
- HS-2000 не участвует в автоматической защите (требование нормативов).

Вопрос 3. Роль ручного переключателя (HS-2000).

- A) Основной элемент защиты.
- B) Компонент автоматизации.
- C) Элемент для соответствия нормам.
- D) Средство предотвращения «проскока».

Ответ С. Элемент для соответствия нормативным требованиям. Для получения дополнительной информации см. [28].

Тест 7.3.

Указать в SRS выбор режима срабатывания СПАЗ/SIS.

Задание: В спецификации требований безопасности (SRS) для системы противоаварийной защиты (СПАЗ/SIS) необходимо выбрать режим срабатывания исполнительных устройств.

Выберите правильные утверждения:

1. Оба режима – «Отключение при обесточивании» и «Срабатывание при подаче энергии» – являются допустимыми вариантами в проектной практике.
2. Режим «Отключение при обесточивании» является единственным безопасным методом, а режим «Срабатывание при подаче энергии» запрещен нормами промышленной безопасности.

3. Системы с режимом «Срабатывание при подаче энергии» допустимы, но требуют применения дополнительных мер повышенной надежности (например, резервированного источника питания и непрерывного мониторинга цепей).

Ответ: Верны пункты 1 и 3.

Объяснение.

Ключевой принцип: Выбор режима срабатывания определяется принципом отказобезопасности. Система при любом отказе должна переходить в заранее определенное безопасное состояние. Поэтому:

Пункт 1: ВЕРНО.

«Отключение при обесточивании»: В этом случае клапан закрывается при пропадании питания. Это наиболее предпочтительный и надежный вариант, так как самые частые отказы (потеря питания, обрыв кабеля) автоматически приводят систему в безопасное состояние.

«Срабатывание при подаче энергии»: В этом случае клапан закрывается при подаче управляющего сигнала. Этот режим допустим, но его применение требует строгого обоснования и компенсирующих мер, так как он по своей природе менее надежен.

Пункт 2: НЕВЕРНО.

Утверждение о том, что режим «Срабатывание при подаче энергии» запрещен, является ошибочным. Он не запрещен, но его использование регламентируется строгими требованиями стандартов (например, МЭК 61511). Его применение возможно, когда переход в безопасное состояние требует затрат энергии (например, останов турбины по сложному алгоритму).

Пункт 3: ВЕРНО.

Это корректная формулировка требований для режима «Срабатывание при подаче энергии». Поскольку этот режим не является отказобезопасным по умолчанию, его надежность должна быть обеспечена на системном уровне.

К обязательным мерам также относятся:

Резервированный источник бесперебойного питания (ИБП).

Непрерывный мониторинг целостности всей цепи управления (от логического решателя до исполнительного механизма).

Высокий уровень диагностического покрытия (DC) для немедленного обнаружения неисправности.

Вывод для включения в SRS:

«Для исполнительных механизмов СПАЗ должен быть выбран режим «Отключение при обесточивании». Использование режима «Срабатывание при подаче энергии» допускается только при технической невозможности реализации первого варианта и должно быть сопровождено в SRS перечнем компенсирующих мер, обеспечивающих эквивалентный уровень безопасности.»

Тест 7.4. Определение времени отклика СПАЗ/SIS.

Вопрос 1. Время безопасности процесса – это:

- А) Время завершения операций.
- В) Интервал между обнаружением опасности и аварией.
- С) Время настройки СПАЗ/SIS.
- Д) Период обслуживания.

Ответ В.

Вопрос 2. Эмпирическое правило для времени отклика СПАЗ/SIS.

- А) $>$ Времени безопасности.
- В) $< 50\%$ времени безопасности.
- С) Не имеет значения.
- Д) $=$ Времени безопасности.

Ответ В.

Пример. Если время безопасности – 5 сек, оптимальный отклик СПАЗ/SIS – 2.5 сек.

Тест 7.5. Требования к SIF для защиты от высокого давления.

Вопрос 1. Критичное требование к конструкции SIF.

- А) Постоянное питание блока.
- В) Отключение питания при аварии.
- С) Резервное питание.
- Д) Дополнительные датчики.

Ответ В. Отключение питания при аварии.

Почему это критичное требование?

1. Принцип «Безопасное состояние при отказе».

Для защиты от высокого давления безопасным состоянием является **сброс давления** (например, открытие предохранительного клапана или закрытие питающего клапана).

Если клапан настроен на **«отключение при обесточивании»**, то при любой неисправности (потеря питания, обрыв провода, отказ контроллера) он **автоматически перейдет в это безопасное состояние**.

Аналогия: Это как предохранительный клапан в скороварке, который механически открывается при превышении давления – ему не нужно электричество, чтобы сработать.

2. Сравнение с опасной альтернативой:

Если бы клапан требовал подачи энергии для срабатывания, то при обрыве кабеля или разряде батареи система была бы неспособна защитить оборудование. Это неприемлемо для критичных систем безопасности.

3. Прямое отношение к физике процесса.

Высокое давление – это быстропротекающая опасность. Система защиты должна быть максимально простой и надежной. Отказ от питания как способ активации – это самый простой и безотказный механизм.

Почему другие варианты НЕ являются критичными требованиями?

Ответ А. Постоянное питание блока.

Это важная **вспомогательная мера**, но не критичное требование к конструкции SIF. Резервирование питания улучшает доступность, но сама функция безопасности должна работать даже при его отсутствии.

Ответ С. Резервное питание.

Аналогично пункту А. Это средство повышения надежности, но не определяющий принцип. Критичный принцип – это то, *что происходит* при отказе этого питания.

Ответ D. Дополнительные датчики.

Это вопрос **архитектуры резервирования** (например, 1oo2, 2oo3). Она влияет на уровень SIL (целостности безопасности), но не является фундаментальным принципом того, как система переходит в безопасное состояние. Можно иметь систему с одним датчиком, но она все равно должна быть спроектирована по принципу Fail-Safe.

Критичное требование определяет **поведение системы при отказах**. Для опасных процессов, таких как высокое давление, поведение по умолчанию должно быть безопасным, что и обеспечивается принципом «Отключение питания при аварии».

Как это требование оформляется в SRS (Спецификации требований безопасности)?

Пример формулировки этого требования для SRS.

1. Функциональное требование (Что должна делать система?):

SIF-001: При обнаружении давления в сосудах V-101 выше значения PSH-001 (15 бар) система СПАЗ/SIS должна инициировать закрытие запорного клапана ZV-101 и открытие предохранительного клапана PV-101.

2. Требование по отказоустойчивости (Как система ведет себя при отказах?)

SIF-001-FT1. Все исполнительные элементы (клапаны ZV-101 и PV-101), входящие в SIF-001, должны быть выполнены в исполнении **»Отключение при обесточивании» (Fail-Safe)**.

SIF-001-FT2. Потеря питания или управляющего сигнала на любой из клапанов (ZV-101, PV-101) должна приводить к их переходу в безопасное состояние (закрытие для ZV-101, открытие для PV-101).

3. Требование к времени отклика (Как быстро?).

SIF-001-PT1. Полное время отклика функции SIF-001, от момента превышения давления до полного закрытия клапана ZV-101, не должно превышать 2 секунд.

Таким образом, в SRS мы переходим от общей философии безопасности к точным, измеримым и проверяемым требованиям для

каждого компонента системы. Это и есть профессиональный подход к проектированию безопасности.

Тест 7.6. Требования спецификации для SIF нагревательной печи.

Функциональные требования:

- При низком потоке газа (FT-8421). закрыть UV-8409 и UV-8411 (задержка 15 сек).
- При низком давлении газа (PSL-8401/8402). закрыть соответствующие клапаны.
- Ручной выключатель (US-8431). аварийное отключение.

Чтобы система была не просто функциональной, но и **безопасной и надежной**, в спецификацию необходимо добавить следующие типы требований:

1. Требования по Отказоустойчивости.

Эти требования определяют, как система должна вести себя при отказе любого компонента (датчика, провода, питания, ПЛК).

Для датчиков давления (PSL-8401/8402):

«В случае обрыва или короткого замыкания в цепи датчиков PSL-8401 и PSL-8402, а также при потере питания, логический решатель СПАЗ/SIS должен интерпретировать этот сигнал как сигнал **Низкое давление** и инициировать соответствующее отключение.»

Для клапанов (UV-8409, UV-8411):

«Все аварийные отсечные клапаны (UV-8409, UV-8411) должны быть исполнения **»Закрытие при обесточивании«**. Потеря управляющего сигнала или питания должна приводить к их безопасному закрытию.»

2. Требования к диагностике.

Эти требования описывают, как система должна самостоятельно обнаруживать внутренние неисправности, чтобы не допустить скрытых отказов.

Диагностика целостности шлейфа:

«СПАЗ/SIS должна непрерывно контролировать целостность шлейфов всех входных устройств (датчики FT-8421, PSL-8401, PSL-8402, ручной выключатель US-8431) и выходных устройств (клапаны UV-8409, UV-8411). Обнаружение обрыва или короткого замыкания должно приводить к активации звуковой и световой сигнализации на операторской панели».

Диагностика логического решателя (ПЛК):

«Логический решатель СПАЗ/SIS должен выполнять встроенный диагностический тест (Watchdog Test) с заданным интервалом. Сбой теста должен приводить к переходу системы в predetermined безопасное состояние (отключение всех клапанов)».

Диагностика исполнительных механизмов (частичное тестирование):

«Система должна поддерживать функцию частичного тестирования (Partial Stroke Test) отсечных клапанов UV-8409 и UV-8411 без полного останова технологического процесса. Тест должен выполняться с заданным интервалом, не превышающим [например, 3 месяца]».

3. Требования к Времени Отклика (Response Time).

Общее время отклика SIF:

«Полное время отклика для функции 'Защита от низкого давления' (от момента срабатывания PSL-8401/8402 до полного закрытия соответствующих клапанов) не должно превышать **2 секунд**.»
«Полное время отклика для функции 'Защита от низкого потока' (от момента срабатывания FT-8421 до полного закрытия клапанов UV-8409 и UV-8411), **включая задержку в 15 секунд**, не должно превышать **17 секунд**.»

Спецификация требований безопасности (SRS) – это не просто список функций. Это комплексный документ, который должен отвечать на три ключевых вопроса:

1. **ЧТО** делает система? → *Функциональные требования.*
2. **КАК** она ведет себя при неисправностях? → *Требования по отказоустойчивости.*
3. **КАК** система сообщает о своих неисправностях? → *Требования к диагностике.*

Только такой подход гарантирует, что спроектированная система будет по-настоящему безопасной и надежной

Тест 7.7. Простой и сложный останов процесса.

Выбрать правильный ответ.

Вопрос . Отличие сложного процесса.

- A) Отсутствие контроля уровня.
- B) Наличие турбин, горелок и утилизации полуфабрикатов.
- C) Более высокая безопасность.

Ответ: B) Наличие турбин, горелок и утилизации полуфабрикатов.

Этот ответ является прямым примером, иллюстрирующим суть сложного процесса. Давайте разберем саму концепцию.

В чем суть?

Любой аварийный останов (Shutdown) можно разделить на два типа:

1. Простой останов (Simple / Basic Shutdown).

Что это? Останов одного аппарата или простой технологической линии.

Как работает? Срабатывает 1-2 защитных механизма по 1-2 причинам.

Пример: Насос отключается при низком давлении на входе. Или смеситель останавливается при превышении температуры.

2. Сложный/каскадный останов (Complex / Cascade Shutdown).

Что это? Согласованное и последовательное отключение целого комплекса взаимосвязанного оборудования.

Как работает? Одно аварийное событие запускает целую цепочку заранее запрограммированных действий для безопасного вывода всего узла из работы.

Цель: Не просто «выключить ток», а безопасно остановить сложные физико-химические процессы, предотвратив повреждение дорогостоящего оборудования, выбросы продукции и обеспечив безопасность.

Почему ответ В правильный?

Оборудование из варианта В – **турбины, горелки, системы утилизации** – является ядром сложного процесса.

- **Турбину** нельзя просто «выключить как лампочку». Её нужно останавливать по специальному графику, чтобы избежать повреждения лопаток и ротора.

- **Горелки** нужно гасить в определенной последовательности, чтобы избежать хлопка и взрыва в топке.

- **Системы утилизации полуфабрикатов** означают, что различные потоки (газы, жидкости) связаны между собой. Останов одной установки требует перенаправления или безопасного сброса потоков с других установок.

Вывод: Наличие такого оборудования автоматически означает, что процесс является **сложным и взаимосвязанным**. Его аварийный останов будет **сложным (каскадным)**, а не простым.

Почему другие варианты неверны?

А) Отсутствие контроля уровня: Это не характеристика сложности процесса, а недостаток в системе контроля и безопасности. Простой процесс тоже может быть плохо оборудован приборами.

С) Более высокая безопасность: Это цель, а не отличительный признак. Сложные процессы часто таят в себе больше рисков, поэтому и требования к системе их защиты (СПАЗ/SIS) и процедурам останова – гораздо выше.

Ключевой признак сложного процесса – взаимосвязь оборудования и технологических потоков. Останов такого процесса – это не просто «выключить», а провести безопасную и последовательную операцию по его демонтажу в аварийном режиме. Ответ В как раз и перечисляет примеры такого сложного, взаимосвязанного оборудования

Формулирований требований по останову ОПО в спецификации (SRS)

Для каждого типа останова требования будут различаться по степени детализации, сложности логики и приоритету.

1. Простой останов (например, отключение насоса) (табл.7.1).

Характер: Локальный, быстрый, обычно основан на одном параметре.

Таблица 7.1.

Категория	Требования в спецификации
Функциональность	• Условие: - Давление на входе PSL-5101 < 2 бар. • Действие: - Немедленное отключение насоса P-501. • Время: - Полное время отклика ≤ 1 сек.
Надежность	• Архитектура: HFT=0 (допустимо для SIL1). • Критичный отказ: Отказ датчика PSL-5101 не должен препятствовать отключению насоса.
Безопасность	• Принцип: »Отключение при обесточивании». • Безопасное состояние: Насос остановлен. • Блокировки: Требуется ручной сброс аварии перед повторным пуском.
Диагностика	• Мониторинг: Контроль целостности шлейфа датчика PSL-5101. • Сигнализация: Аварийная сигнализация «Низкое давление PSL-5101» и «Обрыв цепи датчика PSL-5101».
Техническое обслуживание	• Тестирование: Возможность проверки срабатывания датчика PSL-5101 вручную (кнопка «Test») без остановки процесса. • Периодичность: Визуальная проверка - 1 раз в месяц.

2. Сложный (каскадный) останов (например, останов печи с горелками и турбиной) (табл. 7.2)

Характер: Последовательный, требует координации множества систем.

Таблица 7.2.

Категория	Требования в спецификации
Функциональность	• Условия (логика «ИЛИ»): - Пламя горелки В-101 не обнаружено. - Температура дымовых газов TSH-102 > 600°C. - Нажатие аварийной кнопки US-8431. • Последовательность действий: 1. T=0 сек: Подать сигнал «Прекращение подачи топлива» на клапаны UV-8409, UV-8411. 2. T+2 сек: Убедиться в закрытии клапанов (по сигналу ZSC-8409/8411). 3. T+5 сек: Отключить главный вентилятор горения FAN-

Категория	Требования в спецификации
	801. 4. T+10 сек: Перевести турбину Т-901 в режим «Холостого хода». • Время: Каждый шаг должен выполняться в заданный временной интервал.
Надежность	• Архитектура: HFT=1 для всех критичных контуров (резервирование датчиков пламени, температуры, ПЛК). • Отказоустойчивость: Отказ одного канала не должен останавливать всю последовательность, но должен активировать сигнализацию.
Безопасность	• Приоритет: Безопасность людей и оборудования выше, чем сохранение продукта. • Безопасное состояние: Все топливные клапаны закрыты, вращающееся оборудование остановлено. • Ведение журнала: Обязательная запись всех шагов останова и параметров для последующего расследования.
Диагностика	• Мониторинг в реальном времени: - Состояние всех клапанов (открыт/закрыт). - Исправность датчиков и цепей. - Корректность выполнения шагов последовательности. • Сигнализация: - «Аварийный останов активирован». - «Отказ шага [N] последовательности останова». - «Система в деградированном режиме» (если часть каналов неисправна).
Техническое обслуживание	• Тестирование: - Возможность пошаговой проверки последовательности в режиме «Эмуляции» (без реального воздействия на процесс). - Функция частичного тестирования (PST) клапанов UV-8409/8411. • Периодичность: - Полное функциональное тестирование всей последовательности - 1 раз в 12 месяцев. - Проверка времени отклика ключевых элементов - 1 раз в 3 месяца.

Ключевые различия в подходах по остановке ОПО для спецификации.

• **Детализация логики:**

Простой: Одно условие → одно действие.

Сложный: Множество условий → последовательность взаимосвязанных действий с контролем их выполнения.

• **Приоритеты:**

Простой: Скорость и надежность одиночного действия.

Сложный: Координация и предотвращение вторичных аварий (например, обеспечение продувки перед остановкой горелки).

• **Диагностика и мониторинг:**

Простой: Контроль состояния основных компонентов.

Сложный: Контроль корректности выполнения процесса останова, а не только состояния компонентов.

При составлении SRS для сложного останова вы проектируете сценарий поведения системы в аварии. Это требует не просто перечисления устройств, а описания временной логики, приоритетов и механизмов контроля каждого шага. Для простого останова сценарий тривиален, а акцент делается на безотказности единичного действия.

Тест 7.8. Управление деблокирующими ключами.

Вопрос 1. Какова основная функция АРМ СПАЗ в контексте управления деблокирующими ключами?

- А) Обеспечение физической защиты ключей.
- В) Регистрация информации о первопричине и последовательности срабатывания.
- С) Установка новых ключей.
- Д) Обучение персонала по работе с ключами.

Вопрос 2. Какой протокол используется для реализации менеджера КИП в АРМ СПАЗ?

- А) Modbus.
- В) HART-протокол.
- С) Profibus.
- Д) CAN-шина.

Вопрос 3. Почему необходим отдельный АРМ СПАЗ при проектировании автоматизированных систем (АС)?

- А) Для повышения производительности системы.
- В) Для управления деблокирующими ключами и регистрации информации.
- С) Для уменьшения затрат на оборудование.
- Д) Для обеспечения совместимости с другими системами.

Вопрос 4. Какую информацию регистрирует АРМ СПАЗ при срабатывании деблокирующих ключей?

- А) Только время срабатывания.
- В) Первопричину и последовательность срабатывания.
- С) Имя оператора, осуществляющего срабатывание.
- Д) Местоположение ключа.

Вопрос 5. Ключ деблокирования – это.

- А) Средство отключения блокировки функций АСУ ТП.
- В) Маскирование канала измерения.

Ответы.

Вопрос 1 В. Регистрация информации о первопричине и последовательности срабатывания СПАЗ 2.

Вопрос 2 В. HART-протокол.

Вопрос 3 В. Для управления деблокирующими ключами и регистрации информации.

Вопрос 4 В. Первопричину и последовательность срабатывания.

Вопрос 5 А. Средство отключения блокировки функций АСУ ТП.

Процедуры деблокирования должны быть строго регламентированы и выполняться только уполномоченным персоналом.

Деблокирование может производиться с помощью специальных ключей или программных инструментов.

Контроль имеет значение. После деблокирования необходимо проверить целостность системы и убедиться, что все необходимые меры безопасности соблюдены.

В целом, управление процессом деблокирования ключей в СПАЗ или аналогичных сложных требует тщательного планирования, строгого контроля и точного документирования для обеспечения безопасности СПАЗ. Для решения этих задач могут использовать специальный АРМ СПАЗ. Необходимость отдельного АРМ СПАЗ определяется в ТЗ на проектирование СПАЗ.

7.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 7.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 7».

Тест 7.9. Спецификация. Установка точки срабатывания системы защиты от перегрева [27].

Задача. Реактор спроектирован для выдерживания температур, превышающих обычные температуры окружающей среды. В паспорте реактора указано, что максимальная допустимая рабочая температура составляет 500 °С. Нормальная рабочая температура находится в диапазоне от 150 до 350 °С. Точка срабатывания системы защиты от перегрева высокой целостности в данном случае должна быть ближе всего к.

- a) 345 °С.
- b) 450 °С.
- c) 355 °С.
- d) 125 °С.
- e) Ни одна из указанных выше точек срабатывания не подходит.

Тест 7.10. Что означает принцип «проверено практикой» «Proven-in-use»?

Вопрос 1. Что означает принцип «проверено практикой» в контексте ГОСТ Р МЭК 61511-1?

А) Устройство должно быть сертифицировано международной организацией.

В) Устройство может применяться в системах безопасности, если есть документированная оценка его предыдущего использования.

С) Устройство должно быть протестировано в лабораторных условиях.

Д) Концепция, при которой продукт демонстрирует приемлемую безопасность и надежность в конкретном применении, а его производительность подтверждается точными записями конкретной компании.

Вопрос 2. Какое из следующих утверждений верно для применения устройств в системах, связанных с безопасностью?

А) Достаточно только теоретических исследований.

В) Необходимо наличие документированной оценки на основе предыдущего опыта использования.

С) Устройства могут использоваться без каких-либо предварительных проверок.

Д) Устройства должны быть новыми и не использоваться ранее.

Вопрос 3. Какой документ является ключевым для подтверждения пригодности устройства для применения в СПАЗ?

А) Сертификат соответствия.

В) Документированная оценка на основе опыта предыдущего использования.

С) Техническое описание устройства.

Д) Протокол испытаний.

Тест 7.11

При разработке спецификации выбрать ответ с объяснением.

Вопрос 1. Какое из следующих утверждений наилучшим образом описывает влияние ложных срабатываний на технологическую установку?

А) Ложные срабатывания не влияют на безопасность.

В) Ложные срабатывания могут привести к значительным финансовым потерям и создать новые опасные условия.

С) Ложные срабатывания только увеличивают доступность установки.

Д) Ложные срабатывания не требуют учета при проектировании SIF.

Вопрос 2. Каковы основные требования к ложным срабатываниям, установленные стандартами для систем инструментальной безопасности (SIF)?

А) Не учитывать частоту ложных срабатываний.

В) Ограничить частоту ложных срабатываний до приемлемого уровня, чтобы минимизировать риск и потери.

С) Увеличить частоту ложных срабатываний для повышения безопасности.

Д) Игнорировать затраты, связанные с ложными срабатываниями.

Вопрос 3 Почему ложные срабатывания являются серьезным фактором, который необходимо учитывать при разработке спецификации SIF?

А) Они не влияют на производительность установки.

В) Они могут привести к значительным затратам и новым опасностям.

С) Они всегда улучшают безопасность.

Д) Они не имеют отношения к проектированию SIF.

Вопрос 4. Какое второстепенное соображение должно быть учтено при указании частоты ложных срабатываний в техническом задании на безопасность?

А) Увеличение частоты ложных срабатываний.

В) Ограничение затрат, связанных с потерей производства.

С) Игнорирование затрат.

Д) Уменьшение безопасности системы.

Вопрос 5. Как ложные срабатывания могут создать новые опасные условия?

А) Они не влияют на безопасность.

В) Ложные срабатывания могут привести к ненадлежащему реагированию на реальные угрозы.

С) Ложные срабатывания всегда безопасны.

Д) Они увеличивают доступность системы.

Тест 7.12. В спецификации обосновать требования.

Вопрос 1. Какие опасные скрытые отказы СПАЗ/SIS могут возникнуть, и как они влияют на систему?

Вопрос 2. Как опасные явные отказы СПАЗ/SIS влияют на производственный процесс?

Вопрос 3. Какие преимущества и недостатки имеют резервированные системы?

Вопрос 4. Как ложные срабатывания СПАЗ/SIS влияют на затраты и производственный процесс?

Тест 7.13 Какие сигналы о несоответствии могут приводить к остановке процесса.

А. Частота опасных необнаруженных отказов.

В. Частота опасных обнаруженных отказов.

С. Интервал проверки.

Д. Коэффициент покрытия проверки (эффективность проверки).

Е. Время обхода проверки (длительность проверки).

Ф. Среднее время восстановления.

Г. Вероятность начального отказа.

Н. Индекс безопасности на объекте (операционная культура безопасности).

I. Избыточная архитектура.

Тест 7.14.

Когда выполняется проверка с обходом SIF при работающем процессе и наличии опасностей, каково мгновенное значение PFD во время обхода?

- а) Ноль.
- б) Оно должно быть рассчитано с использованием частоты опасных отказов и длительности проверки.
- в) Единица.
- г) Оно рассчитывается с использованием длительности проверки и интервала проверки.
- д) Ни одно из вышеуказанных утверждений не верно.

Тест 7.15 Как взаимодействуют между собой сигнализации АСДУ и СПАЗ.

Системы сигнализации АСУ ТП очень тесно связаны с системами аварийного останова, с безопасностью, однако их функции отличаются от функций приборных систем безопасности. По существу, цель сигнализации – привлечь внимание оператора к тому, что условия вышли за пределы, соответствующие режиму нормального функционирования (ГОСТ Р МЭК 62682). Это обстоятельство требует принятия решения – вмешиваться или не вмешиваться в процесс. В тех случаях, когда такое вмешательство влияет на безопасность, необходимо учитывать ограниченные возможности человека-оператора.

Вопрос 1. Какова основная цель систем сигнализации в производственном процессе?

- А) Обеспечить автоматическое управление процессом.
- В) Привлечь внимание оператора к отклонениям от нормальных условий.
- С) Устранить все возможные неисправности оборудования.
- Д) Снизить затраты на обслуживание.

Вопрос 2. Какое из следующих утверждений о сигнализации, связанной с безопасностью, является верным?

- А) Она предназначена для управления производственными процессами.
- В) Она сигнализирует о необходимости вмешательства оператора в процесс.
- С) Она используется только в аварийных ситуациях.
- Д) Ее функции полностью совпадают с функциями систем аварийного останова.

Вопрос 3. Какое значение имеют сигнализации, связанные с машинами и оборудованием?

- А) Они не влияют на безопасность.
- В) Они помогают предотвратить повреждение оборудования и обеспечивают его правильную работу.
- С) Они полностью заменяют необходимость в регулярном обслуживании.
- Д) Они служат только для информирования о завершении работы.

Вопрос 4. Как взаимодействуют сигнализации аварийного останова с другими системами сигнализации?

- А) Они полностью независимы и не влияют друг на друга.
- В) Они активируются только в случае полного отказа системы.
- С) Они могут работать совместно, чтобы обеспечить безопасность и предотвратить аварийные ситуации.
- Д) Они служат только для информирования о завершении работы системы.

Вопрос 5. Почему важно учитывать ограниченные возможности человека-оператора при проектировании систем сигнализации?

- А) Оператор всегда может справиться с любой ситуацией.
- В) Оператор может быть перегружен информацией, что приводит к ошибкам в принятии решений.
- С) Оператор не имеет никакого влияния на процесс.
- Д) Ограниченные возможности оператора не имеют значения для безопасности.

Тест 7.16.

Как выполнять объединение СПАЗ и АСДУ в контексте решения задач безопасности и управления в распределенных системах управления и программируемых логических контроллерах (ПЛК)?

Вопрос 1. Что подразумевается под «объединением» функций безопасности и управления в контексте распределенных систем?

- А) Полное физическое объединение оборудования для управления и безопасности.
- В) Логическое объединение, при котором функции могут взаимодействовать, но остаются на отдельных устройствах.
- С) Упрощение системы за счет удаления функций безопасности.
- Д) Создание единой программы, которая управляет как безопасностью, так и процессами.

Вопрос 2. Каковы основные риски объединения функций безопасности и управления на одном оборудовании?

- А) Увеличение стоимости системы.
- В) Упрощение обслуживания.
- С) Потенциальные уязвимости в системе безопасности.
- Д) Повышение производительности системы.

Вопрос 3. При каких условиях может быть приемлемо объединение функций безопасности и управления?

- A) Когда система имеет низкий уровень риска.
- B) Когда функции безопасности могут быть полностью игнорированы.
- C) Когда оборудование сертифицировано для выполнения обеих функций.
- D) Когда нет других доступных решений.

Вопрос 4. Какое из следующих утверждений является правильным в отношении функций безопасности и управления?

- A) Функции управления всегда важнее функций безопасности.
- B) Объединение функций может привести к конфликтам в управлении рисками.
- C) Безопасность может быть полностью обеспечена программным обеспечением.
- D) Все системы управления должны иметь функции безопасности по умолчанию.

Вопрос 5. Какова основная цель разделения функций безопасности и управления в системах?

- A) Упрощение проектирования системы.
- B) Обеспечение более высокого уровня безопасности и надежности.
- C) Снижение затрат на оборудование.
- D) Увеличение скорости обработки данных.

8. РЕЗЕРВИРОВАНИЕ.

8.1. Ключевые принципы резервирования.

Задание 8.1. Уяснить ключевые принципы резервирования в области промышленной безопасности (систем приборной безопасности).

Резервирование в SIS – это использование нескольких идентичных или функционально эквивалентных компонентов SIF (датчиков, контроллеров, исполнительных механизмов) для выполнения одной и той же функции безопасности. Цель резервирования:

1. Повышение безопасности. Обеспечение того, что система срабатывает, когда это необходимо, даже при отказе одного из компонентов (снижение числа опасных отказов «по требованию».

2. Повышение доступности – это минимизация ложных срабатываний или остановок процесса по безопасным отказам, что позволяет процессу продолжать работу, пока неисправный компонент ремонтируется.

Резервирование в системах противоаварийной защиты – это не просто дублирование компонентов, а сложный инженерный компромисс между.

- требованиями безопасности;
- экономической целесообразностью;
- нормативными ограничениями.

На практике даже при высокой надежности нерезервированной СПАЗ/SIS существует фундаментальная необходимость в резервировании, обусловленная следующими факторами.

Расчеты вероятности отказа (PFD) и уровня SIL – это важная, но теоретическая основа. На практике резервирование является часто не просто способом достичь более высокого SIL, а стратегической необходимостью для обеспечения реальной, а не «бумажной» безопасности. Почему это так?

1. Ограничения теории вероятностей и «реального мира».

Систематические ошибки. Модели PFD учитывают только случайные аппаратные отказы. Они бессильны против ошибок, заложенных на этапах проектирования, программирования или монтажа.

Пример: Ошибка в программном коде ПЛК, неправильная настройка датчика, обрыв кабеля в неверно рассчитанном кабельном канале.

Роль резервирования. Резервирование с использованием разнородных технологий (например, релейная система + ПЛК) или разных поставщиков позволяет устранить систематические ошибки. Ошибка в одном канале вряд ли повторится в абсолютно другом.

Неидеальность эксплуатации. Вероятностные модели предполагают «нормальные» условия. В реальности система подвергается непредусмотренным воздействиям.

Пример. Вибрация, перепады температур, попадание влаги, коррозия, случайные механические повреждения при ремонте соседнего оборудования.

Роль резервирования. Физическое и географическое разделение резервных каналов (разные кабельные трассы, разные шкафы) защищает систему от локальных внешних воздействий. Повреждение одного канала не затронет другой.

2. Феномен «скрытых отказов» и старение.

Неидеальность диагностики. Никакая диагностика не может иметь 100% диагностическое покрытие. Всегда остаются отказы, которые система не может обнаружить самостоятельно.

Пример: Датчик давления может выдавать корректный сигнал в пределах шкалы, но иметь нелинейную характеристику, из-за чего он не сработает в нужный момент. Диагностика ПЛК может не обнаружить ошибку в определенной комбинации входных сигналов.

Роль резервирования/ Наличие резервированного, независимого канала кардинально снижает вероятность того, что оба канала одновременно будут иметь разные необнаруживаемые отказы, приводящие к отказу функции.

Кумулятивный эффект старения: Все компоненты деградируют. Период между плановыми техобслуживаниями – это компромисс между экономикой и безопасностью.

Пример: Партия конденсаторов в ПЛК может начать массово выходить из строя ближе к концу своего срока службы.

Роль резервирования. Резервирование позволяет реализовать сдвиг по фазе в графиках технического обслуживания каналов. Это предотвращает ситуацию, когда оба канала находятся в наиболее изношенном состоянии перед очередной проверкой.

3. Человеческий фактор.

Ошибки при обслуживании. Человек самый непредсказуемый элемент системы.

Пример: Техник при проверке датчика случайно повреждает его мембрану. Программист вносит некорректное изменение в логику во время ремонтных работ.

Роль резервирования. Если при обслуживании одного канала он выводится из работы или повреждается, второй канал остается в строю и продолжает обеспечивать защиту. Это превращает потенциально опасную ситуацию (ошибка при ТО) в управляемую.

Непреднамеренные вмешательства. Персонал, не связанный с обслуживанием СПАЗ/SIS, может повлиять на ее работу.

Пример: Строительные работы повреждают кабельный лоток с сигнальными проводами.

Роль резервирования. Раздельное прокладывание кабелей резервных каналов гарантирует, что подобный инцидент не выведет из строя всю систему безопасности.

4. Обеспечение доступности и возможность «Горячего» обслуживания.

Это ключевой экономический и операционный аргумент.

Проблема. Останов технологического процесса для планового обслуживания СПАЗ/SIS крайне дорог. В результате руководство может стремиться увеличить интервалы ТО, что снижает безопасность.

Решение. Резервированная архитектура (например, 1oo2, 2oo3) позволяет выводить на обслуживание один канал без остановки технологического процесса.

Роль резервирования. Система продолжает выполнять защитную функцию (хотя и с пониженным уровнем целостности безопасности, например, с SIL 2 вместо SIL 3), пока один из каналов обслуживается. Это делает процедуры поддержания безопасности практически выполнимыми без прямого конфликта с производственными планами.

Балансирование проектировщика между хорошим решением и наилучшим.

При принятии решения о резервировании необходимо балансировать между.

- Требованиями безопасности.
- Уменьшение PFDavg.
- Повышение отказоустойчивости.
- Экономическими ограничениями, связанными с капитальными затратами на дополнительное оборудование, операционными расходами на обслуживание.
- Техническими компромиссами, связанными с усложнением архитектуры системы, увеличением вероятности ложных срабатываний.

Для SIF стандарты **МЭК 61508/61511** вводят важные ограничения:

- Для устройств с SFF 60-90% максимальный достижимый SIL ограничен структурными требованиями по резервированию.
- Интеллектуальные датчики требуют особого подхода к резервированию.

Пример. Одиночное устройство с показателем резервирования HFT=0 не может обеспечить SIL3 (табл.8.1).

Таблица 8.1. Архитектурные ограничения.

Тип подсистемы	HFT	Макс. SIL (SFF 60%) <	Макс. SIL (SFF 60-90%)	Макс. SIL (SFF ≥ 90%)
A	0	SIL1	SIL2	SIL3
A	1	SIL2	SIL3	SIL4
B	0	Нет	SIL1	SIL2

Тип подсистемы	HFT	Макс. SIL (SFF 60%) <	Макс. SIL (SFF 60-90%)	Макс. SIL (SFF 90%) ≥
В	1	SIL1	SIL2	SIL3

Практические рекомендации по резервированию компонентов SIF.

1. Для полевых устройств:
 - Использовать разнородное резервирование для интеллектуальных датчиков.
 - Применять 1oo2D/H/L архитектур для критических применений.
2. Для логических решателей:
 - Предпочитать 2oo3 вместо 1oo2 для SIL3.
 - Учитывать в разных каналах отказ по общей причине в расчетах.
3. Для исполнительных механизмов:
 - Комбинировать резервирование с механической защитой
 - Использовать частичное резервирование (например, только критичных компонентов)

Современные стандарты (МЭК 61508/61511) задают лишь минимальные требования, оставляя пространство для инженерного творчества. Ключ к успеху - глубокое понимание как теории надежности, так и практических ограничений конкретного применения резервирования.

Архитектура резервирования XooY означает, что из Y компонентов, X должны быть в рабочем состоянии для выполнения функции.

Наиболее распространенными архитектурами резервирования в СПАЗ являются схемы **1ooYN: 1oo2, 1oo2D 1oo2H, 1oo2L**

«D» в обозначении 1ooD означает, что в схеме применяется логика обнаружения диагностикой отказа резервированного канала и переключение в этом случае на выполнение функций обеспечения безопасности одним исправным каналом.

«H» (High / Высокая доступность). Система сконфигурирована так, чтобы максимизировать вероятность ее работоспособности. Ключевой элемент «H». Это не просто 1oo2, это 1oo2 с очень развитой и высокоинтегрированной диагностикой. Если один компонент отказывает безопасно (например, датчик начинает показывать неверное значение), система обнаруживает это через диагностику (например, сравнение показаний двух датчиков, внутренние проверки контроллера) и выдает аварийный сигнал, но не останавливает процесс. Это позволяет операторам запланировать ремонт или замену неисправного компонента в режиме онлайн, без остановки.

Если один компонент отказывает опасно (например, датчик завис в нормальном положении, но давление на самом деле высокое), развитая диагностика должна обнаружить этот отказ (например, через периодическое он-лайн тестирование, сравнение с математической моделью или показаниями других, косвенных датчиков). При обнаружении опасного отказа система переходит в режим 1oo1 (защита осуществляется только одним оставшимся компонентом) и выдает сигнал тревоги, требуя немедленного вмешательства, но без немедленной остановки процесса.

«L» (Low / Высокая безопасность). Система сконфигурирована так, чтобы максимизировать вероятность безопасного перехода в защитное состояние при отказе. Отказ одного канала приводит к безопасному отключению системы.

Высокая доступность SIF – это, если один канал выходит из строя, то система ПРОДОЛЖАЕТ РАБОТАТЬ на основе исправного канала. Это и есть суть «высокой доступности», т.е. система избегает ложных остановов.

В отличие от простой 1oo2, в архитектуре 1oo2N используется переключатель (Switch), который постоянно контролирует исправность обоих каналов и, при отказе одного, автоматически переводит систему на работу по одному исправному каналу.

Преимущества:

- Максимальная доступность. Очень низкая вероятность ложного срабатывания и останова технологического процесса.

- Высокая надежность. Сохраняет функцию защиты даже при отказе одного канала.

Недостатки / Риски:

- Снижение безопасности. Главный риск! Если происходит опасный отказ (например, канал «залипает» в неактивном состоянии), система может не выполнить защитную функцию по требованию, так как второй, исправный канал, также может отказаться.

- Сложность диагностики и более высокая стоимость из-за дополнительного оборудования (переключателя).

Влияние на показатели:

- Улучшает показатель доступности.

- Ухудшает показатель PFD по сравнению с 1oo2, так как отказ одного канала «маскируется» и не приводит к безопасному состоянию.

1oo2 (без «Н»): Классическая структура «1 из 2». При отказе одного канала система, как правило, переходит в безопасное состояние (ложное срабатывание). Это более безопасный, но менее доступный вариант.

1oo2N: Для выполнения функции безопасности достаточно, чтобы хотя бы один из двух компонентов был исправен. Система продолжит работать, даже если один компонент выйдет из строя. Буква

«Н» означает, что система специально спроектирована для обеспечения высокой готовности за счет минимизации ложных срабатываний, при этом ею поддерживается высокий уровень безопасности, благодаря развитой диагностики

1oo2L (Low): Явное указание, что система оптимизирована на безопасность. Отказ СПАЗ/SIS ОПО категорически переводится в безопасное состояние. Безопасный останов!

Практический пример.

Объект: Насосная станция, где насосы должны быть остановлены при высоком давлении в системе.

Архитектура 1oo2Н. Установлены два датчика давления и два логических контроллера.

Нормальная работа. Оба канала исправны, система работает.

Отказ датчика №1. Переключатель (Switch) обнаруживает отказ и изолирует (маскирует) неисправный канал №1. Система продолжает работать в режиме «1oo1» на основе канала №2. Техпроцесс не остановлен.

Ситуация высокого давления. Если теперь возникнет авария, то для остановки насоса будет использоваться только один исправный канал №2.

Риск. Если в момент аварии канал №2 также окажется неисправен (например, из-за скрытого отказа), защита не сработает.

Вывод (табл.8.2).

Особенность 1oo2Н – это компромисс в пользу непрерывности технологического процесса (доступности) в ущерб максимальной безопасности. Эта архитектура применяется там, где ложная остановка производства крайне нежелательна и дорого стоит, но при этом инженеры должны проводить тщательный анализ рисков, чтобы убедиться, что остаточный уровень безопасности является приемлемым.

Таблица 8.2 Сравнительная таблица: 1oo2Н, 1oo2L, 1oo2D.

Параметр	1oo2Н	1oo2L	1oo2D
Основная цель	Максимизация работы процесса	Максимизация безопасности	Баланс безопасности и доступности
Реакция на отказ 1 канала	Продолжает работу на 1 канале	Безопасный останов	Продолжает работу на 1 канале
Влияние на PFD	Ухудшает (риск маскировки отказа)	Значительно улучшает	Улучшает (отказный канал исключается)

Параметр	1oo2N	1oo2L	1oo2D
Влияние на Доступность	Высокая доступность, минимальные простои	Низкая (частые остановки)	Улучшенная диагностика и переключение
Сложность	Средняя (нужен переключатель)	Низкая	Высокая (нужна диагностика и «умный» решатель)
Типичное применение	Критичные процессы, где останов крайне дорог (нефтехимия)	Объекты с высоким риском для персонала (химия, ТЭЦ)	Системы, где важны и непрерывность, и безопасность (газотурбинные установки, компрессорные станции)

Таким образом, **1oo2N** – это эволюция резервированных архитектур, которая за счет интеллектуальной диагностики и динамического переконфигурирования пытается «снять сливки» как с D-, H-, так и с L-подходов, жертвуя для этого стоимостью и сложностью.

Для схем типа 1oo2N используют следующие формулы PFDavg:

1. Архитектура 1oo2.

Логика: Система срабатывает если хотя бы один канал требует срабатывания. Опасный отказ, если оба канала имеют необнаруженные опасные отказы

$$PFD_{avg\_1oo2} \approx (1-\beta)^2 \times (\lambda_{DU} \times T_I)^2 / 3 + \beta \times \lambda_{DU} \times T_I / 2$$

2. Архитектура 1oo2D.

Логика: Диагностика обнаруживает отказы и переключает на исправный канал.

$$PFD_{avg\_1oo2D} \approx (1-\beta)^2 \times (\lambda_{DU} \times T_I)^2 / 3 + \beta \times \lambda_{DU} \times T_I / 2 + (1-DC) \times \lambda_{DD} \times MRT.$$

3. Архитектура 1oo2H.

Логика: Система продолжает работать при отказе одного канала.

$$PFD_{avg\_1oo2H} \approx (1-\beta)^2 \times (\lambda_{DU} \times T_I)^2 / 3 + \beta \times \lambda_{DU} \times T_I / 2.$$

Ключевые метрики:

$$\text{Доступность} = MTBF / (MTBF + MTTR)$$

$$STR_{1oo2H} \approx 2 \times \lambda_{spurious} \times MTTR,$$

где $\lambda_{spurious}$ - интенсивность отказов, приводящих к ложным срабатываниям.

4. Архитектура 1oo2L.

Логика: Система переходит в безопасное состояние при любом отказе, обеспечивая высокую безопасность.

$$PFD_{avg\_1oo2L} \approx (1-\beta)^2 \times (\lambda_{DU} \times T_I)^2 / 3 + \beta \times \lambda_{DU} \times T_I / 2.$$

Ключевые метрики:

$$\text{Доступность} = MTBF / (MTBF + MTTR)$$

$$STR_{1oo2L} \approx 2 \times \lambda_{spurious} \times T_I$$

где $\lambda_{\text{spurious}}$ - интенсивность отказов, приводящих к ложным срабатываниям.

Формальный алгоритм выбора

Рассчитать PFD_{avg} для требуемого SIL

Оценить STR и стоимость простоев

Оценить риск аварии = $PFD_{avg} \times \text{Частота запросов} \times \text{Ущерб}$

Сравнить:

Если стоимость простоев > риска аварии $\rightarrow 1002H$

Если риск аварии > стоимости простоев $\rightarrow 1002L$

Если соизмеримы $\rightarrow 1002$ или $1002D$

Таким образом:

Для систем с высокой доступностью выбирайте $1002H$.

Для систем с высокой безопасностью выбирайте $1002L$.

Для оптимального баланса с диагностикой выбирайте $1002D$.

Всегда учитывайте фактор общих причин (β) в расчетах.

8.2. ПРАКТИКУМ ПО ПРИМЕНЕНИЮ РЕЗЕРВИРОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ СПАЗ.

Задание 8.2. В предположении наличия исходных требований ОПО к СПАЗ подготовить отчет по верификации и отчет по валидации решения в кейсе.

Кейс 8.1. Резервирование системы безопасности (СПАЗ/SIS) для защиты реактора на нефтеперерабатывающем заводе.

Ситуация.

На действующем нефтеперерабатывающем заводе требуется модернизировать систему защиты критически важного реактора. Базовый анализ рисков показал, что для функции безопасности (IPL) «Останов реактора при превышении давления» требуется уровень полноты безопасности **SIL 3** (по шкале МЭК 61511/МЭК 61508).

• Исходные данные.

- Текущая средневероятная вероятность опасного отказа функции (**PFD_{avg}**) составляет $5.00E-03$ (что соответствует SIL 2).
- Для достижения **SIL 3** требуется **$PFD_{avg} < 1.00E-03$** .
- В рамках проекта доступны современные интеллектуальные датчики давления с показателем **SFF = 85%**.

Последствия отказа. Взрыв реактора, катастрофические последствия для персонала, оборудования и окружающей среды. Требуется максимально снизить вероятность *общего отказа* системы.

Режим работы. Система работает в режиме низкой частоты запросов (Low Demand Mode).

Требования к техническому обслуживанию. Плановая остановка завода для полного технического обслуживания (ТО) проводится раз в 2 года. Система безопасности должна сохранять целостность на протяжении всего этого периода. Любые работы по ТО

должны быть максимально оптимизированы для сокращения времени простоя.

Задача.

Спроектировать архитектуру подсистемы датчиков (Sensor Subsystem), которая удовлетворяет требованиям SIL 3, минимизирует риски и учитывает эксплуатационные ограничения.

Решение.

Шаг 1. Анализ конфигурации без резервирования (1oo1).

Расчет. Один канал с $PFD_{avg} = 5.00E-03$ и $SFF=85\%$.

Основные требования по МЭК 61508/61511.

– **Требование по HFT (Hardware Fault Tolerance).** Для элемента с SFF от 60% до 90% требуется $HFT = 1$ для достижения SIL 3. Одиночный элемент (1oo1) имеет $HFT = 0$.

– **Требование по PFD_{avg} .** Текущее значение не соответствует целеому (SIL 3 требует $PFD_{avg} < 1E-03$).

Вывод. Конфигурация 1oo1 неприемлема ни по одному из критериев. Требуется резервирование.

Шаг 2. Выбор и сравнение архитектур резервирования

Сравниваются две основные резервированные архитектуры. **1oo2** и **2oo3** (табл.8.3).

Таблица 8.3.

Параметр	Архитектура 1oo2 (Два датчика, отключение по любому)	Архитектура 2oo3 (Три датчика, отключение по двум)	Комментарий
Безопасность	Выше. Меньшая вероятность безопасного отказа (ложного срабатывания).	Ниже. Более высокая вероятность безопасного отказа.	Для реактора ложные срабатывания дороги (остановка, потеря продукции). 1oo2 предпочтительнее.
Глубина диагностики	Требуется очень высокая диагностика для подавления ложных срабатываний.	Высокая диагностика позволяет идентифицировать и изолировать отказавший датчик, сохраняя систему	2oo3 более устойчива к единичным отказам.

Параметр	Архитектура 1oo2 (Два датчика, отключение по любому)	Архитектура 2oo3 (Три датчика, отключение по двум)	Комментарий
		работоспособной.	
Отказоустойчивость	Ниже (ложные срабатывания останавливают процесс).	Выше. Система остается работоспособной при отказе одного датчика.	Ключевое эксплуатационное преимущество 2oo3.
PFDavg (Отказобезопасность)	Значительно ниже. Легко достижимо SIL 3.	Ниже, но требует более строгого контроля CCF для достижения SIL 3.	Обе архитектуры подходят.
Уязвимость к CCF	Выше. Общий отказ двух датчиков приводит к отказу системы.	Ниже. Для отказа системы требуется общий отказ двух из трех датчиков.	2oo3 более устойчива к CCF, что критично для SIL 3.
Стоимость	Ниже (2 датчика).	Выше (3 датчика, более сложная логика).	

Обоснование выбора 2oo3.

Хотя 1oo2 обеспечивает лучшую защиту от ложных срабатываний, ее уязвимость к **общему отказу (CCF)** является критическим недостатком для функции уровня SIL 3 с катастрофическими последствиями. Архитектура **2oo3** была выбрана, потому что она.

1. **Обеспечивает требуемый HFT = 1** для элементов с SFF=85%.
2. **Значительно снижает риск общего отказа (CCF)** за счет принципа «два из трех».

3. **Повышает готовность системы.** Техническое обслуживание или отказ одного датчика не приводят к останову установки, что соответствует требованию к длительному межсервисному интервалу (2 года).

4. Позволяет реализовать продвинутую диагностику. ПЛК может легко идентифицировать и изолировать «зависший» или отключающийся датчик, поддерживая систему в рабочем состоянии и формируя предупредительное сообщение для планового ТО.

Шаг 3. Проектирование архитектуры логического решателя (PLC / Logic Solver).

Задача. Обеспечить бесперебойное выполнение логики безопасности с высочайшей доступностью и требуемой глубиной диагностики.

Анализ. Одиночный ПЛК не обеспечивает необходимого уровня отказоустойчивости ($HFT=0$) для SIL 3. Его отказ приведет к полной потере функции безопасности.

Выбор конфигурации. Для достижения $HFT = 1$ требуется резервированная архитектура.

Предлагаемое решение. Резервированный ПЛК безопасности по конфигурации 1oo2D.

Обоснование выбора 1oo2D.

Принцип работы. Два центральных процессорных модуля (ЦП) работают в «горячем» резерве, синхронизируясь друг с другом. Они выполняют одну и ту же программу и непрерывно сравнивают свои результаты.

Глубокая диагностика. Встроенная диагностика (D - Diagnostics) постоянно проверяет целостность процессоров, памяти, модулей ввода/вывода и внутренних шин. При обнаружении несоответствия или отказа в одном из ЦП, управление мгновенно (бесперебойно) переходит на исправный процессор. Это предотвращает ложное срабатывание и сохраняет систему в рабочем состоянии.

Соответствие стандарту. Данная конфигурация обеспечивает $HFT = 1$ для логического решателя, что является обязательным требованием для SIL 3.

Эксплуатационное преимущество. Позволяет проводить «горячую» замену отказавшего модуля без остановки технологического процесса, что критично для длительного межсервисного интервала.

Шаг 4. Проектирование архитектуры исполнительных устройств (Final Elements)

Задача. Обеспечить выполнение защитного действия (закрытие отсечного клапана) с высочайшей надежностью. Это часто самое слабое звено в цепи СПАЗ/SIS.

Анализ. Одиночный отсечной клапан с одним исполнительным механизмом имеет $HFT=0$. Его отказ (например, залипание клапана, отказ пневматики) приведет к общему отказу всей системы безопасности.

Выбор конфигурации. Требуется резервирование. Однако просто поставить два клапана последовательно (1oo2) – дорого и может ухудшить гидравлику системы.

Предлагаемое решение. Использование частичного резервирования и продвинутой диагностики.

Обоснование и варианты решений.

Использование исполнительного устройства из АСУТП.

Суть. Рассмотреть возможность использования в качестве первого уровня защиты уже установленного на линии отсечного клапана, управляемого АСУТП.

Плюсы. Значительное снижение капитальных затрат.

Минусы и риски. Требуется крайне тщательного анализа! Такой клапан становится общим элементом (Shared Element), и его отказ повлияет и на АСУТП, и на СПАЗ/SIS. Стандарт МЭК 61511 накладывает строгие ограничения. Необходимо доказать, что его надежность (PFDavg) и режим технического обслуживания полностью удовлетворяют требованиям SIL 3 для функции СПАЗ/SIS. На практике это очень сложно. Чаще это допустимо для функций более низкого SIL. Однако это решение может быть подкреплено использованием исполнительного устройства с контролем неполного хода.

Выделенное исполнительное устройство с контролем неполного хода (PST) – это фактически непрерывный контроль (диагностика) готовности ИУ выполнять отсечные действия.

Как это работает. Система PST периодически (например, раз в неделю автоматически) дает команду на закрытие клапана на 10-15% от хода, не нарушая технологический процесс. Это позволяет проверить способность привода и клапана выполнять движение, выявить потенциальные проблемы (залипание, засорение) на ранней стадии.

Результат. PST резко снижает вероятность опасного отказа (PFDavg) клапана, так как такой контроль сокращает интервал эффективной проверки его работоспособности. Это позволяет одному клапану (HFT=0) с системой PST по своей надежности приблизиться к требованиям SIL 3, но для его гарантированного достижения используется резервирование клапаном в базовой системе диспетчерского управления АСУ ТП.

Итоговый результат всей цепи СПАЗ/SIS (Sensors + Logic + Final Elements).

Разработана резервированная архитектура системы безопасности.

- Датчики. 2003 (высокая готовность, устойчивость к CCF).
- Логический решатель. Резервированный ПЛК 1002D (глубокая диагностика, бесперебойность).
- Исполнительные устройства. Отсечной клапан с системой PST + Использование исполнительного устройства из АСУТП.

Результат.

Разработанная архитектура подсистемы датчиков 2003.

1. Соответствует целевым показателям SIL 3 по PFDavg.
2. Соответствует требованиям стандарта по HFT и SFF.

3. **Минимизирует риск общего отказа (CCF)** за счет разнородности и физического разделения.

4. **Обеспечивает высокую готовность** и позволяет проводить ТО без остановки процесса.

5. **Учитывает требование к межсервисному интервалу** в 2 года за счет комбинации резервирования и встроенной диагностики.

Данное решение является инженерным компромиссом резервирования в СПАЗ. В реальном проекте этот выбор должен быть задокументирован в отчете по анализу безопасности, а все допущения и расчеты – верифицированы с помощью специализированного инструментария (например, Exida SILCalc™).

Кейс 8.2. Нефтеперерабатывающий завод. защита реактора крекинга.

Проблема.

- Схема соединения датчика давления (SIL2) не обеспечивает требуемый SIL3.

- $PFD=0.005$ не соответствует целевому значению 0.001.

Решение.

- Внедрена схема 2oo3 с тремя датчиками разных производителей.

- Реализована независимая кабельная разводка.

- Добавлен диагностический модуль с периодичностью Тестов 1 раз в 8 часов.

Результат.

Суть: Три датчика вместо одного.

PFD снижен до 0.0008 (соответствует SIL3).

Отказоустойчивость. система продолжает работать при отказе 1 датчика. 2 из 3 датчиков гарантируют безопасное отключение.

Главное преимущество: Оптимальный баланс. Система достигает высочайшей безопасности (SIL 3) и при этом остается работоспособной при отказе любого датчика.

Проще говоря: Система не кричит от каждого «чиха»(устойчива к помехам), но гарантированно поднимет тревогу при реальной угрозе, даже если один «сторож» уснул.

Кейс 8.3. Химическое производство. система аварийного сброса.

Проблема.

- Клапан сброса давления (SIL1) имеет высокую вероятность опасного отказа ($PFD=0.1$).

- Частые ложные срабатывания приводят к потерям продукции.

Решение.

- Внедрена архитектура 1oo2 с двумя клапанами.

- Используются клапаны с разными принципами действия (пневматический + электрический).

- Реализована схема «голосования» с независимыми каналами управления.

Результат. Два клапана вместо одного

- **PFD снижен до 0.01** (соответствует SIL2).
- **Отказоустойчивость.** при отказе одного клапана второй обеспечивает безопасность.
- **Отказобезопасность.** Исключены ложные срабатывания из-за дублирования.
- **Главное преимущество: Ликвидация «одиночных точек отказа».** Резервирование не только повысило безопасность до SIL 2, но и резко сократило ложные срабатывания, что экономически выгодно.
- **Проще говоря:** «Теперь для ложного срабатывания должны ошибиться оба клапана одновременно, а для опасного отказа — не сработать оба сразу. Вероятность и того, и другого — ничтожна».

Кейс 8.4. Атомная электростанция. система аварийной остановки реактора.

Проблема.

- Одиночный канал управления (SIL2) не соответствует требованиям SIL4.
- Высокий риск опасного отказа (отказ в срабатывании).

Решение.

- Применена 3-канальная схема 2oo3 с полным аппаратным резервированием.
- Выполнено разнесение каналов по разным шкафам для исключения общей причины отказа.
- Использование разнородных технологий (релейная + микро-процессорная логика).

Результат.

Тройное резервирование с разнородными технологиями.

- **PFD снижен до 0.0001** (соответствует SIL4).
- **Отказоустойчивость.** Система работает даже при отказе 1-2 каналов.
- **Отказобезопасность.** Гарантированное срабатывание при любом отказе.

- **Главное преимущество: Максимальная устойчивость.** Система защищена от любых единичных и даже множественных отказов, а также от систематических ошибок (благодаря разным технологиям).

Проще говоря: «Это 'непотопляемый' корабль безопасности. Он останется на плаву и выполнит свою миссию даже при серьезных повреждениях».

Кейс 8.5. Газопровод. система обнаружения утечек.

Проблема.

- Ложные срабатывания из-за помех в одиночном датчике.
- Опасный отказ (не обнаружение утечки) с PFD=0.05.

Решение.

- Внедрена 2oo2D (схема с диагностикой).
- Используются инфракрасные и ультразвуковые датчики для разнообразия.
- Автоматический тест каждые 4 часа.

Результат.

Два «умных» разнотипных датчика с взаимной диагностикой.

- **PFD снижен до 0.002** (соответствует SIL3).
- **Отказоустойчивость.** система продолжает работать при отказе одного датчика.
- **Отказобезопасность.** Диагностика предотвращает опасные отказы.

• **Главное преимущество: Интеллектуальный контроль.** Система не просто дублирует каналы, а заставляет их следить друг за другом. Это позволяет отличать реальную утечку от помехи или отказа датчика.

Проще говоря: »Два детектива с разными методами работы следят за объектом. Они не только ловят преступника, но и постоянно проверяют друг у друга алиби, исключая ложные версии.

Кейс 8.6. Нефтехимический комплекс. защита от перегрева колонны.

Проблема.

- Одиночный термопарный датчик (SIL1) не обеспечивает надежность.
- Высокий риск ложного отключения из-за дрейфа сигнала.

Решение.

- Применена схема 1oo1D с диагностикой и резервным датчиком RTD.
- Регулярная калибровка и автоматический мониторинг.

Результат.

- **PFD снижен до 0.003** (соответствует SIL2).
- **Отказоустойчивость.** Исключены ложные срабатывания.
- **Отказобезопасность.** Возможность переключения на резервный датчик, который постоянно сравнивает свои показания с основным.

Что значит 1oo1D на практике?

Это архитектура, где есть **один основной рабочий канал** (в данном случае – термопара), но к нему добавлена система диагностики, которая сама может быть резервным каналом.

В кейсе диагностика реализована в виде **второго, резервного датчика (RTD)**, который постоянно сравнивает свои показания с основным.

Так это 1oo1D или 1oo2?

• Если система работает **только на основном датчике**, а резервный (RTD) только проверяет его исправность и при отказе переключается на себя – это **1oo1D**. Основной канал один, диагностика – с резервированием.

• Если оба датчика (и термопара, и RTD) **равноправны** и для срабатывания достаточно сигнала от любого из них – это уже **1oo2**.

Судя по формулировке «система переключается на резервный датчик», в кейсе описана именно архитектура **1oo1D**.

Таблица 8.4. Сводная таблица преимуществ архитектур резервирования

Кейс	Архитектура	Ключевое преимущество	Результат
8.2 Реактор	2oo3	Баланс безопасности и доступности	SIL 3 + Отказоустойчивость
8.3 Сброс	1oo2	Борьба с ложными срабатываниями и опасными отказами	SIL 2 + сохранение продукта
8.4 АЭС	2oo3 (разнород.)	Абсолютная отказоустойчивость и защита от системных ошибок	SIL 4 + устойчивость к множественным отказам
8.5 Утечки	2oo2D	Интеллектуальная диагностика и разнородность	SIL 3 + Минимум ложных тревог
8.6 Перегрев	1oo1D	Повышение надежности: Диагностика и автоматическое переключение на резервный датчик без потери функции.	SIL 2 + Непрерывность работы

Резервирование – это не просто «больше датчиков». Это стратегический инструмент, который позволяет:

1. Повысить уровень безопасности (SIL).
2. **Увеличить доступность** (снизить ложные срабатывания).
3. **Обеспечить работу системы при отказах.**
4. **Защититься от скрытых и систематических ошибок.**

Как выбрать архитектуру (табл. 8.4)?

1. Нужно резко повысить безопасность (SIL)?

Используйте 2oo3 (лучший баланс) или 1oo2D (с интеллектуальной диагностикой).

2. Нужно бороться с ложными срабатываниями и повысить безопасность?

Используйте 1002H. Для ложного срабатывания нужно, чтобы оба канала сработали ошибочно.

3. Нужна максимальная надежность для экстремальных рисков (АЭС)?

Используйте 2003 с разнородными технологиями.

4. Нужно повысить надежность одиночного канала без перехода на полное дублирование?

Используйте 1001D. Это экономит ресурсы, но дает значительный выигрыш в безопасности и диагностике.

8.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 8.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 8.1. Резервирование полевого устройства [28].

В процессе проектирования систем безопасности (СПАЗ) важно принимать обоснованные решения о резервировании полевых устройств. Это решение часто оказывается непростым из-за противоречий между требованиями безопасности, надежности, стоимости и обязательными нормативными документами (рис.8.1).

Задание.

Ответьте на следующие вопросы, выбрав один из предложенных вариантов. Обоснуйте свой выбор, указав, какие проблемы могут возникнуть при выборе того или иного подхода к резервированию.

Вопрос 1. Какое из следующих утверждений о резервировании полевых устройств является верным?

а) Резервирование всегда увеличивает стоимость системы, но не влияет на надежность.

б) Резервирование увеличивает отказоустойчивость системы, но может не всегда быть оправдано с точки зрения стоимости.

в) Резервирование не требуется для устройств типа А, так как они всегда имеют высокую отказоустойчивость.

г) Резервирование не влияет на требования к доле безопасных отказов.

Ответ б.

Объяснение. Резервирование действительно повышает отказоустойчивость системы, что особенно важно для обеспечения безопасности. Однако, как правило, это также приводит к увеличению стоимости системы, что может быть критическим фактором при проектировании. Следовательно, необходимо тщательно взвешивать преимущества и недостатки резервирования в контексте конкретного проекта.

Вопрос 2. Какое минимальное значение отказоустойчивости должно быть у системы, если доля безопасных отказов составляет от 60 до 90%?

- a) 10%.
- b) 20%.
- c) 30%.
- d) 40%.

Ответ b.

Объяснение: Минимальное значение отказоустойчивости системы напрямую зависит от доли безопасных отказов (SFF) оборудования, как это регламентировано стандартами МЭК 61508 и МЭК 61511. Для устройств с SFF в диапазоне 60–90% минимальная аппаратная отказоустойчивость (HFT, hardware fault tolerance) должна быть равна 1, что соответствует примерно 20% отказоустойчивости.

Это означает, что система способна выдержать один отказ оборудования без потери функции безопасности, обеспечивая требуемый уровень SIL. Такой подход позволяет балансировать между безопасностью и стоимостью системы: достаточно минимального резервирования для поддержания надежности, но без излишнего дублирования, которое повышало бы расходы и сложность эксплуатации.

Вопрос 3. Какое влияние имеет использование программируемой электроники (ПЭС) на надежность устройства?

- a) Увеличивает надежность устройства, так как ПЭС более точны.
- b) Уменьшает надежность устройства, так как ПЭС более подвержены отказам но при использовании алгоритмов диагностики может увеличивать надежность.
- c) Не имеет никакого влияния на надежность устройства.
- d) Увеличивает стоимость, но не влияет на надежность.

Ответ b.

Объяснение. Устройства, использующие программируемую электронику, действительно более подвержены различным видам отказов, что делает их менее надежными по сравнению с простыми устройствами. Это подчеркивает важность резервирования, тщательного выбора архитектуры системы и глубокой их непрерывной диагностики.

Вопрос 4. Какое из следующих условий позволяет уменьшить уровень отказоустойчивости на единицу?

- a) Доля безопасных отказов превышает 90% и используется диагностика.
- b) Устройство имеет высокую степень конфигурируемости.
- c) Устройство не имеет пароля.
- d) Уровень SIL превышает 4.

Ответ a.

Объяснение. Если доля безопасных отказов превышает 90% и используется диагностика, это позволяет уменьшить уровень отказоустойчивости на единицу. Это условие обеспечивает достаточный уровень защиты, несмотря на снижение отказоустойчивости.

Вопрос 5. Какое из следующих утверждений о конфигурациях резервирования является верным?

- a) Конфигурация 1oo2 всегда предпочтительнее 2oo3.
- b) Конфигурация 2oo3 более устойчива к систематическим ошибкам.
- c) Конфигурация 1oo2 не требует диагностики.
- d) Конфигурация 2oo3 не может быть использована в системах с высокой интенсивностью ложных срабатываний.

Ответ b.

Объяснение. Конфигурация 2oo3 (две из трех) обеспечивает большую устойчивость к систематическим ошибкам, поскольку для достижения отказа системы требуется, чтобы два устройства вышли из строя одновременно. Это делает систему более надежной в условиях возможных систематических ошибок.

Конфигурация схемы датчиков или исполнительных устройств (рис. 8.1).

При выборе резервирования используйте таблицы 8.5, 8.6.

Используйте выбор 1oo1, если задания по PFD и ложные срабатывания удовлетворяются.

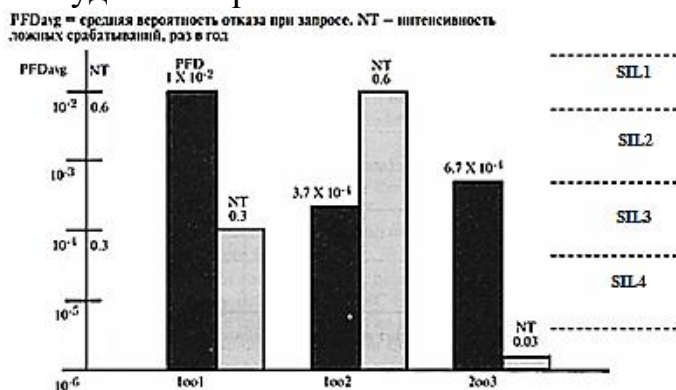


Рис 8.1. Сравнение вариантов резервирования

Используйте выбор 1oo2. Значение PFD «улучшается». Интенсивность ложных срабатываний удваивается.

Используйте выбор 2oo3. Значение PFD уменьшается по сравнению с архитектурой 1oo1. Интенсивность ложных срабатываний значительно уменьшается.

Таблица 8.5 Наиболее часто встречающиеся варианты резервирования

Конфигурация схемы датчиков или ИУ	Выбор
1oo1	Используйте если требования спецификации по опасным и безопасным отказам удовлетворяются

1oo2	Значение PFD «улучшается». Интенсивность ложных отказов удваивается.
2oo3	Значение PFD уменьшается по сравнению с архитектурой 1oo2. Интенсивность ложных срабатываний значительно снижается.

Таблица 8.6 Варианты минимизации резервирования полевых устройств с помощью диагностики

Конфигурация схемы датчиков и ИУ	Выбор
1oo1D	Внутренняя и внешняя диагностики используются для увеличения доли безопасных отказов. Альтернатива архитектуре 1oo2 для SIL2
1oo2D	То же что и в случае 1oo1D, но может допускать один отказ и переходит в режим 1oo1D при ремонтах. Удовлетворяет требованиям С, если доля безопасных отказов превышает 90%. И не соответствует требованиям SIL3 (отказам по общей причине). Снижает интенсивность ложных отказов. Хорошая альтернатива архитектуре 2oo3.

Для получения дополнительной информации см. [28].

Тест 8.2. Резервирование.

Вопрос 1. Какое из следующих утверждений верно в отношении простых и сложных устройств?

- а) Простые устройства менее подвержены отказам, чем сложные.
- б) Сложные устройства всегда требуют резервирования.
- с) Простые устройства имеют более высокую степень конфигурируемости.
- д) Сложные устройства имеют более высокую надежность по сравнению с простыми устройствами.

Ответ а.

Объяснение. Простые устройства, не использующие программируемую электронику, как правило, имеют более низкую вероятность отказа, поскольку они основаны на менее сложных технологиях. Сложные устройства, использующие программируемую электронику, подвержены большему количеству потенциальных отказов, что делает их менее надежными.

Вопрос 2. Какое условие позволяет уменьшить уровень отказоустойчивости на единицу?

- а) Устройство имеет высокую степень конфигурируемости.
- б) Доля безопасных отказов превышает 90%, и используется диагностика.
- с) Устройство защищено паролем.
- д) Устройство имеет SIL меньше 4.

Ответ в.

Объяснение. Если устройство имеет долю безопасных отказов более 90% и применяется диагностика, это позволяет уменьшить уровень отказоустойчивости на единицу. Это условие обеспечивает достаточный уровень защиты, даже если уровень отказоустойчивости снижен.

Вопрос 3. Какое из следующих условий увеличивает уровень отказоустойчивости на единицу?

- a) Устройство имеет высокую степень конфигурируемости.
- b) Доля безопасных отказов составляет меньше 60%.
- c) Устройство проверено практикой применения и защищено паролем.
- d) Устройство имеет SIL больше 4.

Ответ в.

Объяснение. Если доля безопасных отказов составляет менее 60%, это обычно указывает на низкую надежность устройства, что требует увеличения уровня отказоустойчивости для обеспечения необходимой защиты. Использование таких устройств следует избегать, так как они могут привести к серьезным последствиям.

Вопрос 4. Какое влияние имеет использование резервированной архитектуры 1oo2 или 1oo3 на систему?

- a) Увеличивает вероятность отказа системы.
- b) Уменьшает вероятность систематических ошибок.
- c) Позволяет достичь заданного уровня ПФД при высоком значении показателя PFD устройства.
- d) Не влияет на надежность системы.

Ответ с.

Объяснение. Использование резервированной архитектуры, такой как 1oo2 или 1oo3, позволяет достичь необходимого уровня надежности (ПФД) даже при высоком значении показателя PFD устройства. Это важно для обеспечения безопасности системы.

Вопрос 5. Какое из следующих утверждений о конфигурации 2oo3 является верным?

- a) Конфигурация 2oo3 не может быть использована в системах с высокой интенсивностью ложных срабатываний.
- b) Конфигурация 2oo3 всегда предпочтительнее 1oo2.
- c) Конфигурация 2oo3 более устойчива к систематическим ошибкам, чем 1oo2.
- d) Конфигурация 2oo3 требует меньше затрат на реализацию, чем 1oo2.

Ответ с.

Объяснение.

Ответ а. Неверный ответ «Конфигурация 2oo3 не может быть использована в системах с высокой интенсивностью ложных срабатыва-

ний». Наоборот, одной из главных причин использования конфигурации 2oo3 (два из трех) является снижение ложных (или ложных) срабатываний.

В системе 1oo2 (один из двух) любое ложное показание от одного датчика приведет к срабатыванию системы.

В системе 2oo3 требуется, чтобы два из трех датчиков одновременно показали аномальное состояние для срабатывания. Это означает, что одиночный ложный сигнал от одного датчика будет проигнорирован (поскольку два других датчика будут показывать нормальное состояние), что значительно повышает устойчивость системы к ложным срабатываниям и, следовательно, улучшает эксплуатационную готовность.

Ответ б. Неверно утверждение. *Конфигурация 2oo3 всегда предпочтительнее 1oo2.*

В инженерии безопасности нет концепции «всегда предпочтительнее». Выбор конфигурации зависит от множества факторов, включая:

- Требуемый уровень полноты безопасности (SIL). Для более высоких SIL часто нужны более сложные конфигурации, но это не всегда 2oo3.

- Стоимость. 2oo3 значительно дороже из-за необходимости приобретения и установки большего количества оборудования (3 датчика, 3 линии связи, 3 входных канала логического решателя).

- Сложность. 2oo3 более сложна в проектировании, установке, обслуживании и тестировании.

- Баланс между безопасностью и доступностью. 2oo3 обеспечивает отличный баланс. она безопасна (терпима к отказу одного датчика, который должен был сработать) и имеет высокую эксплуатационную готовность (терпима к отказу одного датчика, который дал ложный сигнал). Однако, для некоторых приложений, 1oo2 может быть достаточно и экономически целесообразно.

Ответ с. Верно. Конфигурация 2oo3 более устойчива к систематическим ошибкам, чем 1oo2.

Систематические ошибки – это ошибки, которые возникают из-за недостатков в проектировании, производстве, установке, обслуживании или программном обеспечении, а не из-за случайных отказов компонентов.

Примеры систематических отказов:

1. Ошибки проектирования СПАЗ/SIS.
2. Ошибки аппаратной реализации.
3. Ошибки программного обеспечения.
4. Ошибки человеческого взаимодействия.
5. Ошибки проектирования оборудования.
6. Ошибки модификации.

Если такая ошибка существует, она, скорее всего, проявится в нескольких одинаковых компонентах.

Хотя никакая конфигурация не может полностью устранить риск систематических ошибок (особенно если все три компонента идентичны и имеют общий систематический дефект), 2003 обеспечивает лучшую возможность обнаружения и локализации таких ошибок, чем 1002.

Как это работает. В 2003 системе, если один из трех датчиков начинает выдавать некорректные показания (из-за систематической ошибки в его калибровке, дрейфа или другого внутреннего дефекта), два других датчика будут показывать правильные значения. Это позволяет системе управления идентифицировать «отклонившийся» датчик, подать диагностический сигнал об ошибке и вывести этот датчик из работы для обслуживания, при этом функция безопасности продолжает выполняться корректно (система остаётся в режиме 2002 или 1002, пока неисправный датчик не будет заменен).

В 1002 системе, если один датчик имеет систематическую ошибку, он либо вызовет ложное срабатывание, либо система станет менее безопасной, поскольку ее резервирование снизится до 1001 без возможности обнаружения отказа второго датчика. 2003 дает «третью точку зрения» для диагностики.

Ответ d. Неверно утверждение *«Конфигурация 2003 требует меньше затрат на реализацию, чем 1002»*.

2003 требует большего количества оборудования, большего объема монтажных работ, более сложной логики и, как следствие, значительно больших затрат на реализацию по сравнению с 1002.

Конфигурация 2003 – это мощный инструмент для систем безопасности, который обеспечивает высокий уровень эксплуатационной готовности и безопасности, а также значительно улучшенную диагностику и устойчивость к некоторым видам систематических ошибок, особенно к тем, которые проявляются на уровне одного компонента.

Тест 8.3.

Для реализации SIF используется нерезервированная архитектура (1001, HFT = 0) оборудования безопасности. DTI составляет 100 миллисекунд.

Система запрограммирована на перевод процесса в безопасное состояние, когда диагностика указывает на внутренний отказ. Время отклика SIF для достижения безопасного состояния составляет 50 миллисекунд. Время безопасности процесса составляет 2 секунды. Средний интервал срабатывания составляет 1 минуту. Для оборудования получены следующие данные по интенсивности отказов путем суммирования интенсивностей отказов всех компонентов.

$$\lambda_{DD} = 8,5 \cdot 10^{-6} \text{ отказов в час.}$$

$$\lambda_{DU} = 0,5 \cdot 10^{-6} \text{ отказов в час.}$$

Вопрос 1. Какова архитектура оборудования безопасности в данной задаче?

- A) 1002.
- B) 1001.
- C) 2002.
- D) 2001.

Вопрос 2. Каково время отклика SIF для достижения безопасного состояния?

- A) 50 миллисекунд.
- B) 100 миллисекунд.
- C) 1 секунда.
- D) 2 секунды.

Вопрос 3. Какова общая интенсивность опасных отказов (λ_D) для системы SIF?

- A) $8,5 \cdot 10^{-6}$ отказов в час.
- B) $0,5 \cdot 10^{-6}$ отказов в час.
- C) $9 \cdot 10^{-6}$ отказов в час.
- D) $1 \cdot 10^{-6}$ отказов в час.

Вопрос 4. Какое время безопасности процесса в данной системе?

- A) 50 миллисекунд.
- B) 1 секунда.
- C) 2 секунды.
- D) 5 секунд.

Ответы.

Вопрос 1. Ответ B.

Архитектура системы безопасности в данной задаче – нерезервированная (1001), что означает, что имеется одно устройство, выполняющее функцию безопасности без резервирования.

Вопрос 2. Ответ A.

Время отклика SIF для достижения безопасного состояния составляет 50 миллисекунд, как указано в задаче.

Вопрос 3. Ответ C. $9 \cdot 10^{-6}$ отказов в час.

Общая интенсивность опасных отказов (λ_D) определяется как сумма λ_{DD} и λ_{DU} . $\lambda_D = \lambda_{DD} + \lambda_{DU} = 8,5 \cdot 10^{-6} + 0,5 \cdot 10^{-6} = 9 \cdot 10^{-6}$ отказов в час.

Вопрос 4. Ответ C.

Время безопасности процесса в данной системе составляет 2 секунды, как указано в задаче.

Объяснение решения.

Для определения уровня SIL необходимо учитывать, что время диагностики (DTI) составляет 100 миллисекунд, а время отклика SIF для достижения безопасного состояния – 50 миллисекунд. Суммарное время отклика (DTI + время отклика SIF) составляет 150 миллисекунд, что значительно меньше времени безопасности процесса, равного 2 секундам.

Так как система запрограммирована на перевод процесса в безопасное состояние при обнаружении внутреннего отказа, и учитывая, что предусматривается высокий охват диагностикой SIF, то это позволяет обеспечить установленную общую безопасность системы. Согласно таблице требований к частоте отказов в час (PFH), полученное значение $PFH = 9 \cdot 10^{-6}$ соответствует требованиям для уровня SIL 1. Таким образом, данная конструкция достигает уровня SIL 1.

Решение. Средний интервал срабатывания СПАЗ $DI = 1$ минута и Время диагностики $DTI = 100$ миллисекунд. Следовательно, $DI = 600 \times DTI$.

Сумма отклика DTI плюс время отклика SIF равно 150 миллисекунд, что значительно меньше времени безопасности процесса (2 секунды).

Эта SIF обеспечивает защиту высокого спроса и может получить соответствие необходимым проектным требованиям по скорости срабатывания в случае высокого диагностического покрытия. Такое соответствие предполагает, что система будет проводить диагностику с учетом оценки своей надежности и способности предотвращать опасные ситуации. Это позволит улучшить общую систему безопасности, так как диагностика с высоким покрытием помогает выявить и предотвратить потенциальные неисправности до того, как они привели к аварийным ситуациям.

Тест 8.4.

Интеллектуальный КИП имеет долю безопасных отказов (SFF) 86,2% в соответствии с МЭК 61508, Route 1H. В архитектуре 1oo1, к какому уровню SIL соответствует данная конструкция по МЭК 61508?

- a) 0.
- b) 1.
- c) 2.
- d) 3.
- e) 4.

Ответ с.

Так как интеллектуальный КИП классифицируется как устройство типа В, то показатель SFF, равный 86,2%, позволяет использовать продукт в приложении SIL даже с использованием архитектуры 1oo1. Это указано в МЭК 61508, часть 2, таблица 3, пункт 7.4.4.2.2.

Учесть то, что МЭК 61511 также устанавливает архитектурные ограничения, основанные на SFF, за исключением того, что доказательства «практического применения» могут использоваться для квалификации конкретной конструкции на один уровень SIL выше. См. МЭК 61511, часть 1, пункт 11.4.4.

Вопрос 2. Какова вероятность того, что данный датчик проработает три года без отказов?

- A) 0.9997.

- В) 0.9990.
- С) 0.9980.
- Д) 0.9975.

Ответ А.

Объяснение. Вероятность безотказной работы (Р) может быть рассчитана с использованием формулы для экспоненциального распределения.

$$P(t) = e^{-\lambda t}.$$

где

- $\lambda = 9 \times 10^{-7}$ (интенсивность отказов в час),
- $t = 3 \text{ года} = 3 \times 365 \times 24 \text{ часов} = 26280 \text{ часов}$.

Теперь подставим значения.

$$P(3 \text{ года}) = e^{-(9 \times 10^{-7}) \times 26280}.$$

$$P(3 \text{ года}) = e^{-0.0000236} \approx 0.9767.$$

Таким образом, вероятность того, что КИП проработает три года без отказов, составляет примерно 0.9997 при высоком спросе.

Датчик имеет постоянную частоту отказов 9×10^{-7} отказов/час.

а) $\lambda = 9 \times 10^{-7}$ отказов/час = 9×10^{-7} отказов/час $\times 8760$ часов/год
 $\lambda = 0,00788$ отказов/год при низком спросе.

MTTF (среднее время наработки на отказ) = $1/\lambda = 1/0,00788$ года
= 126,8 года.

б) Надежность $R = e^{-\lambda t}$.

$$R(3 \text{ года}) = e^{-\lambda t} = e^{-0.00788 \times 3} = 0,9766.$$

Все эти расчеты предполагают отсутствие тестирования и ремонта передатчика. Дополнительная информация о расчетах надежности приведена в книге. Гоубл, У.М. «Оценка безопасности и надежности систем управления», 3-е издание, глава 4.

8.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 8.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 8».

Тест 8.5.

Расположите следующие схемы избыточности в порядке от наименьшей вероятности отказа по требованию (PFD) до наибольшей.

Наименьшая – Наибольшая.

- а) 1oo2 – 2oo2 – 2oo3.
- б) 2oo2 – 1oo2 – 2oo3.
- с) 2oo3 – 2oo2 – 1oo2.
- д) 2oo2 – 2oo3 – 1oo2.
- е) 1oo2 – 2oo3 – 2oo2.

Тест 8.6.

Какая архитектура систем безопасности (СПАЗ) лучше. 2oo3 или 1oo2D?

Вопрос 1. Какую вероятность отказов имеет система с архитектурой 2oo3 по сравнению с системой 1oo2D?

- A) Меньшую вероятность отказов.
- B) Большую вероятность отказов.
- C) Одинаковую вероятность отказов.
- D) Вероятность отказов невозможно определить.

Вопрос 2. Каковы возможные недостатки архитектуры 1oo2D в условиях низкого диагностического покрытия?

- A) Высокая вероятность ложных срабатываний и безопасных отказов.
- B) Низкая вероятность ложных срабатываний.
- C) Высокая надежность и безопасность.
- D) Необходимость в дополнительных устройствах.

Вопрос 3. Какую архитектуру целесообразно выбирать при использовании неинтеллектуальных устройств, таких как терморелы и реле?

- A) 1oo2D.
- B) 2oo3.
- C) 1oo1.
- D) 3oo3.

Вопрос 4. Какую основную выгоду предоставляет архитектура 2oo3 в контексте безопасных отказов и ложных срабатываний?

- A) Увеличивает вероятность ложных срабатываний.
- B) Обеспечивает удовлетворительные показатели для отказов обоих видов (безопасных и опасных).
- C) Уменьшает диагностическое покрытие.
- D) Увеличивает сложность системы.

Тест 8.7.

Сколько уровней устойчивости к опасным отказам (в соответствии с МЭК 61508) существует в архитектуре 1oo2?

- a) 0.
- b) 1.
- c) 2.
- d) 4.
- e) 3.

Тест 8.8.

Как резервирование влияет на надежность этих систем?

Вопрос 1. Какое из следующих утверждений верно в отношении простых и сложных устройств?

- a) Простые устройства менее подвержены отказам, чем сложные.
- b) Сложные устройства всегда требуют резервирования.

с) Простые устройства имеют более высокую степень конфигурируемости.

д) Сложные устройства имеют более высокую надежность по сравнению с простыми устройствами.

Вопрос 2. Какое условие позволяет уменьшить уровень отказоустойчивости на единицу?

а) Устройство имеет высокую степень конфигурируемости.

б) Доля безопасных отказов превышает 90%, и используется диагностика.

с) Устройство защищено паролем.

д) Устройство имеет SIL меньше 4.

Вопрос 3. Какое из следующих условий увеличивает уровень отказоустойчивости на единицу?

а) Устройство имеет высокую степень конфигурируемости.

б) Доля безопасных отказов составляет меньше 60%.

с) Устройство проверено практикой применения и защищено паролем.

д) Устройство имеет SIL больше 4.

Вопрос 4. Какое влияние имеет использование резервированной архитектуры 1oo2 или 1oo3 на систему?

а) Увеличивает вероятность отказа системы.

б) Уменьшает вероятность систематических ошибок.

с) Позволяет достичь заданного уровня PFD при высоком значении показателя PFD устройства.

д) Не влияет на надежность системы.

Вопрос 5. Какое из следующих утверждений о конфигурации 2oo3 является верным?

а) Конфигурация 2oo3 не может быть использована в системах с высокой интенсивностью ложных срабатываний.

б) Конфигурация 2oo3 всегда предпочтительнее 1oo2.

с) Конфигурация 2oo3 более устойчива к систематическим ошибкам, чем 1oo2.

д) Конфигурация 2oo3 требует меньше затрат на реализацию, чем 1oo2.

Тест 8.9.

Использование при резервировании общих датчиков в СПАЗ и АСДУ.

Вопрос. Почему не следует использовать общие датчики для систем безопасности (СПАЗ) и автоматизированных систем диспетчерского управления (АСДУ)?

а) Нарушает принципы независимости СПАЗ/SIS от базовой системы управления процессом.

б) Создает возможность появления отказов по общим причинам.

с) Не создает отдельного защитного уровня.

d) Процедуры обслуживания, проверки и защиты устройства могут оказаться неадекватными.

9. ЛОГИЧЕСКОЕ УСТРОЙСТВО. ПЛК.

9.1. Ключевые принципы разработки логического устройства (ПЛК) СПАЗ.

Задание 9.1. Уяснить ключевые принципы разработки логического устройства СПАЗ.

При проектировании систем безопасности (СПАЗ/SIS) традиционно основное внимание уделяется аппаратному резервированию ПЛК (например, 2oo3, 1oo2D), что соответствует рекомендациям ROUTE 2H и стандартам МЭК 61508 / МЭК 61511. Однако программное обеспечение (ПО) играет не менее важную роль в обеспечении надежности и отказоустойчивости системы [17]fnx].

Почему оно критично?

- Аппаратные отказы можно смягчить резервированием, но ошибки ПО (логики, конфигурации, обработки данных) могут привести к системному отказу, который не устраняется дублированием.
- Некорректная логика защиты способна вызвать ложные срабатывания или, что хуже, невыполнение защитных функций.
- Совместимость между ПЛК и ПО влияет на стабильность работы и простоту сопровождения системы.

При разработке ПО для систем безопасности следует придерживаться следующих принципов.

1. Детерминированность и простота.
 - Минимизация сложности – чем проще алгоритм, тем ниже вероятность ошибки.
 - Запрет динамического изменения кода – программа должна быть статичной после загрузки в ПЛК.
 - Предсказуемость выполнения – отсутствие неконтролируемых задержек (например, из-за сборки мусора в некоторых средах).

2. Верификация и валидация.

Для этого применяется:

- Статический анализ кода (MISRA-C, LDRA) для выявления потенциальных уязвимостей.
- Моделирование и тестирование (включая аварийные сценарии) для подтверждения корректности логики.
- Документирование требований (в соответствии с МЭК 61511) и трассируемость изменений.

3. Отказоустойчивость на уровне ПО это:

- Контроль целостности (CRC, watchdog-таймеры).
- Корректная обработка сбоев (например, безопасное состояние при потере связи с датчиками).
- Защита от «зависаний» (например, через контроль времени выполнения циклов).
- Согласованный выбор ПЛК и ПО.

4. Критерии выбора ПЛК.

- Сертификация по SIL (например, SIL2/SIL3).
- Поддержка необходимых схем резервирования (2oo3, 1oo2D).
- Встроенные механизмы диагностики (например, самодиагностика CPU, модулей ввода-вывода).

5. Критерии выбора ПО.

- Сертифицированные среды разработки (например, TIA Portal с SIL3-сертификацией для SIMATIC S7-1500).
- Поддержка стандартов функциональной безопасности (МЭК 61508, МЭК 61131-3 с дополнениями для СПАЗ/SIS).
- Инструменты для верификации (например, анализ в CODESYS Safety).

Интеграция ПЛК и ПО.

- Использование готовых библиотек безопасности (например, F-Libs для SIMATIC).
- Ограничение использования небезопасных функций (например, динамическое выделение памяти).
- Строгий контроль версий (чтобы исключить несовместимость ПО и информационное обеспечение ПЛК).

Типичные ошибки и рекомендации при выборе ПЛК и ПО.

Ошибка 1. Выбор ПЛК с избыточным резервированием, но с ненадежным ПО.

Правило. Оценивать не только аппаратную среду, но и среду разработки в соответствии с SIL.

Ошибка 2. Использование сложной логики с множеством условий, что затрудняет верификацию.

Решение. Применять модульный подход с простыми, проверяемыми блоками.

Ошибка 3. Отсутствие тестирования на «нештатные» сценарии (например, задержки в сети).

Рекомендуемое решение. Включать в тесты инъекцию ошибок.

Надежность СПАЗ/SIS определяется не только резервированием «железа» ПЛК, но и качеством ПО.

Согласованный выбор ПЛК и программного обеспечения позволяет:

- снизить вероятность системных отказов,
- упростить верификацию и сопровождение,
- обеспечить предсказуемость работы системы в аварийных условиях.

9.2. Практикум применению логического устройства в СПАЗ.

Задание 9.2. В предположении наличия исходных требований ОПО к СПАЗ подготовить отчет по верификации и отчет по валидации решения в кейсе.

Кейс 9.1. Нефтеперерабатывающий завод. Системный анализ отказа функциональной безопасности.

Ситуация.

На нефтеперерабатывающем заводе была внедрена система противоаварийной защиты (СПАЗ/СПАЗ/SIS) для аварийного отключения и предотвращения разгерметизации технологического трубопровода с опасным средой. При проектировании системы были приняты следующие решения.

Логический решатель (ПЛК).

Выбран стандартный, более дешевый универсальный ПЛК, не имеющий сертификации по стандартам функциональной безопасности (МЭК 61508/61511).

Программное обеспечение.

Для программирования логики безопасности использовалось универсальное ПО, не предназначенное и не валидированное для критических применений.

Процесс проектирования. После монтажа системы не был выполнен заключительный анализ опасностей и работоспособности (HAZOP) на спроектированную конфигурацию.

Инцидент. При возникновении аварийной ситуации (превышение давления) система безопасности не инициировала закрытие аварийных клапанов. Произошла разгерметизация трубопровода с выбросом опасных веществ. К счастью, обошлось без жертв.

Объяснения (Почему система не сработала?).

Ошибка заключалась не в одном неправильном компоненте, а в системном провале на всех этапах жизненного цикла безопасности, регламентированного стандартом МЭК 61511.

Этап жизненного цикла по МЭК 61511. Допущенные ошибки.

Последствия и разъяснение.

1. Анализ опасностей и рисков (HAZOP). Отсутствие заключительного HAZOP.

HAZOP – это не единовременное действие, а итеративный процесс. Финальный HAZOP необходим для проверки того, что спроектированная система адекватно отвечает на все выявленные ранее сценарии рисков. Без этого финальная верификация ПЛК отсутствует и это означает несоответствие требованиям стандартов.

2. Спецификация требований к безопасности (SRS). Требования к аппаратному и программному обеспечению ПЛК, вероятно, не были формализованы в SRS или были проигнорированы. SRS – это главный документ, «библия» проекта СПАЗ/SIS. В нем должны быть четко указаны все требования, включая требуемый SIL для каждой функции, требования к аппаратному обеспечению (HFT, SFF) и программному обеспечению (методология разработки, стандарт кодирования).

3. Проектирование и выбор оборудования. Выбор несертифицированного ПЛК и неподходящего ПО. Это ключевая ошибка. Стандартный ПЛК и ПО не обеспечивают:

- Аппаратную отказоустойчивость (HFT). В обычном ПЛК нет резервированных процессоров, модулей ввода/вывода с диагностикой.

- Контроль целостности памяти. Нет защиты от сбоев в памяти программы или данных.

- Диагностику. Вероятное несоответствие низкая степень самодиагностики (менее 90%), которая неспособна обнаружить опасный отказ в течение требуемого времени.

- Верификацию ПО. Универсальное ПО не следует строгим стандартам кодирования (например, MISRA C), не имеет защиты от изменения кода, не поддерживает тестирование функциональной безопасности. Такой ПЛК не может быть верифицирован на соответствие SIL.

4. Внедрение и верификация Использование неподходящего ПО привело к невозможности корректной верификации логики. Для сертифицированных ПЛК безопасности (например, Siemens S7-1500F, Rockwell GuardLogix) используется специализированное ПО (TIA Portal Safety, Studio 5000 Logix Designer). Такое ПО:

- Имеет встроенные блоки безопасности (FBD/LD), прошедшие валидацию.

- Автоматически проверяет логику на соответствие стандартам (перекрестные ссылки, типы данных, запрещенные операции).

- Ведет журнал изменений и обеспечивает парольную защиту.

Универсальное ПО всего этого лишено.

5. Эксплуатация и техобслуживание. Не было оснований для планирования ТО, так как параметры надежности системы были неизвестны. Для сертифицированной системы обязательны показатели надежности (PFDavg, MTBF), на основе которых рассчитывается периодичность функциональных проверок. Для несертифицированной системы этот период взят «с потолка», что могло привести к накоплению необнаруженных отказов.

Решение и выводы.

Логический решатель должен быть заменен на ПЛК, сертифицированный под SIL 3 (напр., Siemens S7-1500F/Termium 4titude, Rockwell GuardLogix, HIMA HiQuad), запрограммированный с использованием специализированного ПО для функциональной безопасности.

Системный вывод. Проблема была не просто в «неправильном ПЛК». Проблема была в игнорировании жизненного цикла функциональной безопасности, описанного в стандартах МЭК 61508 (для производителей оборудования) и МЭК 61511 (для проектировщиков и эксплуатантов).

Стандарты – это не просто «бумажка» – для сертификации. Это пошаговая инструкция, позволяющая избежать системных ошибок.

Требования носят системный характер. Каждый элемент – от менеджмента проекта и компетенций персонала до методики программирования и аппаратной диагностики – важен. Нельзя соблюдать стандарт выборочно.

Сертификация оборудования – это гарантия того, что разработчик проекта выполнил свою часть работы, провел расчеты надежности, анализ отказов (FMEDA), валидировал аппаратуру и программные инструменты. Проектировщик, выбирая сертифицированное оборудование, опирался на доказательства, а не изобретает велосипед.

Методическая рекомендация. Для любых критических применений обязательным является не только выбор сертифицированных компонентов, но и строгое следование всем этапам жизненного цикла СПАЗ/SIS, описанным в МЭК 61511, включая финальный анализ и аудит.

Кейс 9.2. Химическое производство. Ошибка в ПО для СПАЗ/SIS.

Ситуация: Инженеры сэкономили, выбрав универсальное ПО для программирования системы безопасности.

Проблема:

- **Следствие.** Ложные срабатывания и простои производства.
- **Причина.** Универсальное ПО не имеет защит от ошибок программиста. Оно позволяет писать любой код, который может быть логически неверным или не соответствовать стандартам МЭК 61508 для СПАЗ/SIS.

Решение. Переход на специализированное ПО для СПАЗ/SIS (например, EcoStruxure Safety Expert, Safety Manager).

- **Встроенные шаблоны (FBD/LD).** Программист не пишет код с нуля, а использует готовые, сертифицированные блоки (AND, OR, Timer, Vote). Это исключает синтаксические и логические ошибки.

- **Автоматическая верификация:** ПО автоматически проверяет всю логику на соответствие стандартам (например, отсутствие тупиковых веток, проверка временных циклов).

Вывод:

ПО для СПАЗ/SIS – это не просто инструмент для написания кода, а «защищенная среда», которая не позволяет инженеру допустить ошибку. Его главная задача – **исключить человеческий фактор** на этапе программирования. Экономия на таком ПО – это прямой риск безопасности и бесперебойности работы.

Кейс 9.3. Энергетика. Отказ из-за отсутствия резервирования ПЛК

Ситуация. Для критически важной турбины выбрали симплексный (одиночный) ПЛК с целью экономии.

Проблема: Отказ СПАЗ.

- **Следствие:** Аварийный останов и повреждение дорогостоящего оборудования.

- **Причина:** «Одиночная точка отказа». Любой сбой в процессоре, памяти или питании ПЛК приводил к полной потере контрольной функции.

Решение: Внедрение дублированной системы с горячим резервированием (например, ProSafe-RS, AC 800M HI).

- **Принцип «1 из 2» (1oo2).** Два ПЛК работают синхронно. Если один выходит из строя, второй мгновенно берет управление на себя без прерывания процесса. Это обеспечивает высокую доступность.

- **Принцип «2 из 3» (2oo3).** Три ПЛК работают параллельно. Система продолжает работать даже при отказе одного (а в некоторых случаях и двух) ПЛК. Это обеспечивает максимальную отказоустойчивость.

Вывод.

Для критических процессов в энергетике и в нефтегазовой отрасли резервирование ПЛК – не опция, а обязательное требование. Архитектуры 1oo2D или 2oo3 позволяют системе продолжать работу при отказе аппаратной части, превращая потенциальную аварию в управляемое событие, которое можно устранить «на ходу».

Кейс 9.4. Фармацевтика. Проблемы интеграции разнородных систем.

Ситуация. ПЛК АСУ ТП (Siemens) и система СПАЗ/SIS (Honeywell) были от разных производителей.

Проблема: отказ ПЛК.

Следствие. Нарушение контроля критических параметров процесса (температура, давление).

Причина. Сложная и медленная связь между системами через шлюзы (OPC) или нестандартные протоколы. Данные от СПАЗ/SIS к АСУ ТП (и наоборот) приходили с задержкой, из-за чего управление было несинхронным.

Решение. Выбор единой интегрированной экосистемы (например, Emerson DeltaV СПАЗ/SIS + DeltaV PLC).

- **Единая среда** – это если аппаратура и ПО для АСУ ТП и СПАЗ/SIS разработаны одним производителем для совместной работы.

- **Беспроблемная связь** – это когда обмен данными происходит по внутренней высокоскоростной шине без задержек и потерь.

Вывод.

Таблица 9.1. Безопасность – это не только отдельная СПАЗ/SIS, но и ее эффективное взаимодействие с системой базового управления. Интегрированные платформы устраняют «трение» на стыке систем, обеспечивая быстрый и надежный обмен данными. Это снижает сложность проектирования, монтажа и сопровождения, повышая общую надежность комплекса.

Таблица 9.1. Сводная таблица уроков применения ПЛК в СПАЗ

Кейс	Ошибочный подход	Правильное решение	Ключевой принцип
9.2. Химия	Универсальное ПО	Специализированное ПО СПАЗ/SIS	Защита от ошибок: Среда программирования должна исключать человеческий фактор.
9.3. Энергетика	Симплексный ПЛК	Резервированные архитектуры (1oo2, 2oo3)	Отказоустойчивость: Для критичных процессов отсутствие резервирования – недопустимо.
9.4. Фармацевтика	Разнородные системы	Единая интегрированная платформа	Интеграция: Совместимость и бесшовная связь между АСУ ТП и СПАЗ/SIS так же важны, как и надежность их отдельных компонентов.

Кейс 9.5. Водоочистные сооружения. Экономия на ПО для диагностики.

Ситуация. Заказчик отказался от лицензионного ПО с функцией мониторинга в пользу бесплатного аналога.

Проблема. Не выявленный заранее износ датчиков привел к загрязнению воды.

Решение. Внедрение ПО с предиктивной аналитикой (напр., Siemens SIMATIC PCS 7, Rockwell PlantPAx).

Вывод. Современное ПО должно включать диагностику и прогнозирование отказов.

Общие рекомендации.

1. **Стандарты.** Всегда проверяйте соответствие ПО стандартам МЭК 61508 (функциональная безопасность) и МЭК 61511 (для процессов).

2. **Резервирование.** Для критичных систем – только SIL-3 с аппаратным резервированием.

3. **ПО.** Выбирайте специализированные среды (например, CODESYS Safety, Siemens STEP 7 Safety).

4. **Производитель.** Лучше использовать СПАЗ/SIS программно-аппаратные решения одного вендора для упрощения интеграции.

9.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ ВЫБОРУ ЛОГИЧЕСКОГО УСТРОЙСТВА СПАЗ.

Задание 9.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 9.1. Выбор типа логического устройства для проектирования СПАЗ в соответствии с МЭК 61508.

Вопрос 1. Какое логическое устройство является предпочтительным для реализации функций безопасности (SIF) в СПАЗ согласно МЭК 61508?

1. Релейные схемы.
2. Пневматические системы.
3. Программируемые логические контроллеры (ПЛК).
4. Микропроцессорные системы с элементами ИИ.

Ответ 3. Программируемые логические контроллеры (ПЛК).

Объяснение. Стандарт МЭК 61508 рекомендует использовать ПЛК для реализации функций безопасности, так как они обеспечивают.

- Гибкость программирования.
- Возможность диагностики и тестирования.
- Соответствие требуемому уровню SIL (при наличии сертификации).

Хотя релейные и пневматические системы применяются в некоторых отраслях (например, на морских платформах или в релейной логике останова), ПЛК являются наиболее универсальным и современным решением.

Вопрос 2. Если в СПАЗ большинство SIF имеют уровень SIL1 или SIL2, но хотя бы один SIF требует SIL3, каким требованиям должен соответствовать ПЛК?

1. Достаточно SIL2.
2. ПЛК должен соответствовать SIL3.
3. Можно использовать два ПЛК с SIL2 в резервированной схеме.
4. Достаточно SIL1 с дополнительными мерами безопасности.

Ответ 2. ПЛК должен соответствовать SIL3.

Объяснение. Согласно МЭК 61508, если в системе есть хотя бы одна функция безопасности с SIL3, то весь логический решатель (ПЛК) должен быть сертифицирован на этот уровень. Это связано с тем, что.

- Ошибки в логике выполнения могут повлиять на все SIF.
- SIL3 требует более жестких требований к надежности и диагностике.

Резервирование ПЛК с SIL2 (вариант 3) может быть рассмотрено, но только если это явно разрешено стандартом и подтверждено расчетами.

Вопрос 3. Какие ПЛК используются в нефтехимической промышленности для реализации SIL3? (Выберите несколько вариантов).

1. Siemens S7-1500 (SIL3).
2. Rockwell ControlLogix (до SIL2).
3. Honeywell Safety Manager (SIL3).
4. Emerson DeltaV СПАЗ/SIS (SIL3).

Ответ 1, 3, 4.

Объяснение.

- **Siemens S7-1500** (с соответствующими модулями безопасности) сертифицирован до SIL3.

- **Honeywell Safety Manager** и **Emerson DeltaV СПАЗ/SIS** – специализированные системы для SIL3 в нефтехимии.

- **Rockwell ControlLogix** обычно сертифицирован до SIL2, для SIL3 требуется дополнительное резервирование.

Вопрос 4. Почему для СПАЗ не всегда подходят ПЛК с упрощенной логикой или элементами ИИ?

1. Они дешевле.
2. Они не всегда имеют сертификацию SIL.
3. ИИ может принимать непредсказуемые решения.
4. Они требуют меньше диагностики.

Ответ 2, 3.

Объяснение.

- Упрощенные ПЛК могут не соответствовать требованиям SIL по надежности и диагностике.

- Системы с ИИ могут быть непредсказуемы в критических ситуациях, что недопустимо для детерминированных систем безопасности.

Вопрос 5. Какой документ подтверждает, что ПЛК пригоден для использования в СПАЗ?

1. Руководство по эксплуатации.
2. Сертификат SIL.
3. Декларация соответствия ГОСТ.
4. Заключение оператора.

Ответ 2. Сертификат SIL.

Объяснение.

Только сертификат SIL (например, SIL3 по МЭК 61508) подтверждает, что ПЛК прошел необходимые испытания и соответствует требованиям безопасности.

Вывод.

При проектировании СПАЗ важно.

1. Выбирать ПЛК с сертификацией SIL, соответствующей максимальному уровню SIF в системе.
2. Использовать проверенные решения (Siemens, Honeywell, Emerson).

3. Избегать непредсказуемых решений (ИИ) и упрощенных логических устройств без сертификации.

Тест 9.2. Выбор компонентов ПЛК для СПАЗ/SIS с учетом SIL.

Часть 1. Базовые принципы архитектуры ПЛК для СПАЗ/SIS.

Вопрос 1. Почему в СПАЗ/SIS критически важна самодиагностика модулей ПЛК?

1. Чтобы снизить стоимость системы.
2. Для своевременного обнаружения отказов и выполнения требований SIL.
3. Чтобы уменьшить энергопотребление.
4. Для упрощения программирования.

Ответ 2. Для своевременного обнаружения отказов и выполнения требований SIL.

Объяснение.

- Самодиагностика (например, проверка целостности данных, Тестирование каналов ввода-вывода) позволяет выявлять скрытые отказы, которые могут привести к нарушению работы СПАЗ/SIS.
- Согласно МЭК 61508, для достижения SIL2/SIL3 необходимо, чтобы коэффициент безопасных отказов (SFF) был $\geq 90\%$ (для аппаратной части). Без диагностики это невозможно.
- Пример. Диагностический коммуникационный модуль проверяет исправность связи между компонентами.

Вопрос 2. Зачем в ПЛК для СПАЗ/SIS используется сторожевой таймер?

1. Для экономии памяти.
2. Для контроля «зависания» программы и перезапуска процессора в аварийном режиме.
3. Для ускорения вычислений.
4. Для автоматического обновления ПО.

Ответ 2. Для контроля «зависания» программы и перезапуска процессора в аварийном режиме.

Объяснение.

- Сторожевой таймер – это аппаратный таймер, который перезагружает процессор, если программа не отправляет ему сигнал в заданный интервал времени.
- Без него зависание ПО могло бы привести к отказу СПАЗ/SIS (например, не сработал бы аварийный останов).
- Он в обязательном порядке требуется для SIL2/SIL3, так как снижает вероятность опасного отказа ПЛК.

Часть 2. Выбор модулей ввода-вывода (I/O) с учетом SIL.

Вопрос 3. Почему в СПАЗ/SIS применяется линейный мониторинг входных сигналов?

1. Чтобы уменьшить количество проводов.
2. Для обнаружения обрыва линии или короткого замыкания.

3. Для ускорения обработки сигналов.
4. Чтобы снизить нагрузку на процессор.

Ответ 2. Для обнаружения обрыва линии или короткого замыкания.

Объяснение.

Линейный мониторинг (например, 4-20 мА сигналов с супервизорным контролем) позволяет:

- Обнаружить обрыв цепи (ток падает ниже 3,6 мА).
- Выявить КЗ (ток превышает 21 мА).

Без этого датчик мог бы «молчать» при аварии, и СПАЗ/SIS не сработала бы.

Мониторинг требуется для SIL2/SIL3, так как снижает вероятность ложного пропуска опасного события.

Вопрос 4.

Зачем в выходных модулях СПАЗ/SIS мониторится состояние плавких предохранителей?

1. Чтобы уменьшить, нагрев модуля.
2. Для контроля перегрузки по току и сигнализации об отказе защиты по току.
3. Для ускорения переключения реле.
4. Чтобы снизить стоимость модуля.

Ответ 2. Для защиты от перегрузки по току и сигнализации об отказе.

Объяснение.

- Если предохранитель перегорел, выходной модуль не сможет выполнить аварийное отключение.
- Светодиодная индикация (красный LED) сразу показывает неисправность предохранителя.

Часть 3. Телекоммуникация и резервирование.

Вопрос 5. Почему в СПАЗ/SIS часто используют избыточные (резервированные) коммуникационные шины?

1. Чтобы увеличить скорость передачи данных.
2. Для обеспечения отказоустойчивости при обрыве связи.
3. Чтобы упростить настройку сети.
4. Для снижения электропотребления.

Ответ 2. Для обеспечения отказоустойчивости при обрыве связи.

Объяснение.

- Если основная шина (например, PROFIBUS PA) откажет, резервная (Ethernet) обеспечит передачу аварийных сигналов.
- Требуется для SIL3, так как одиночный отказ не должен приводить к потере функции безопасности.

Часть 4. Практический пример выбора ПЛК для СПАЗ/SIS.

Вопрос 6. Какой из перечисленных ПЛК подходит для SIL3 в нефтехимии?

1. Siemens S7-1200 (SIL2).
2. Honeywell Safety Manager (SIL3).
3. Allen-Bradley Micro800 (SIL1).
4. Omron CP1E (не сертифицирован для СПАЗ/SIS).

Ответ 2. Honeywell Safety Manager (SIL3).

Объяснение.

- S7-1200 – только SIL2, недостаточно для критичных SIF.
- Safety Manager специально разработан для нефтехимии и имеет сертификацию SIL3.
- Micro800 и CP1E не подходят для СПАЗ/SIS.

Выводы.

1. Самодиагностика и Watchdog Timer – обязательны для SIL2/SIL3.
2. Мониторинг I/O (входы/выходы) предотвращает скрытые отказы.
3. Резервирование (коммуникации, питание) необходимо для SIL3.
4. Сертификация SIL – ключевой критерий выбора ПЛК.
Для получения дополнительной информации см. [28].

Тест 9.3. Разбор реальных проблем выбора ПЛК для СПАЗ (СПАЗ/SIS) с учетом SIL.

Часть 1. Реальные аварии из-за ошибок в проектировании СПАЗ/SIS.

Ситуация. Взрыв на нефтеперерабатывающем заводе в Техасе (2019). Датчик уровня в сепараторе не обнаружил переполнение из-за отсутствия линейного мониторинга. ПЛК не получил сигнал и СПАЗ/SIS не сработала.

Вопрос 1. Какое решение предотвратило бы аварию?

1. Использование аналогового датчика 4-20 мА с супервизорным контролем обрыва/КЗ.
2. Установка механического клапана с пневматическим приводом.
3. Отказ от ПЛК в пользу релейной логики.

Ответ 1. Аналоговый датчик с супервизорным контролем.

Объяснение.

Мониторинг тока 4-20 мА выявляет обрыв (<3.6 мА) и КЗ (>21 мА).

Ситуация. Отказ системы останова на химическом заводе в Германии (2016).

Причина. Сторожевой таймер ПЛК был отключен для «ускорения работы». При зависании программы аварийный останов не активировался.

Вопрос 2. Какой принцип СПАЗ/SIS был нарушен?

1. Отказобезопасность.
2. Избыточность.
3. Масштабируемость.

Ответ 1. Отказобезопасность.

Объяснение.

Сторожевой таймер обязателен для SIL2/SIL3. Его отключение → нарушение МЭК 61508-2.

Часть 2. Расчеты и выбор компонентов.

Ситуация. Выбор ПЛК для установки SIL3 (компрессорный цех)

Дано:

Требуется $PFH < 1e^{-8}$ (для SIL3).

Доступны:

- Siemens S7-1500F ($PFH = 5e^{-9}$).
- Allen-Bradley GuardLogix ($PFH = 2e^{-8}$).

Вопрос 3. Какой ПЛК подходит?

1. Только Siemens.
2. Только GuardLogix.
3. Оба, но GuardLogix требует резервирования.

Ответ 1. Только Siemens.

Объяснение.

- GuardLogix не вписывается в PFH для SIL3 ($2e^{-8} > 1e^{-8}$).
- Для него потребовалось бы 2003 голосование, что удорожает систему.

Ситуация. Отказ резервированного модуля ввода (нефтепровод, 2020)

Из-за коррозии отказали оба аналоговых входа (не было диагностики влажности).

Вопрос 4. Какое решение исключит такой сценарий?

1. Модули с IP67 и мониторингом состояния контактов.
2. Переход на дискретные датчики.
3. Установка ПЛК без резервирования.

Ответ 1. Модули с IP67 и диагностикой.

Объяснение.

- IP67 защищает от влаги.
- Диагностика контактного сопротивления выявляет коррозию до отказа.

Часть 3. Практическое задание.

Спроектируйте архитектуру СПАЗ/SIS для реактора высокого давления (SIL3).

- Датчики: 3х давление (2003), 2х температура (1002).
- Исполнительные устройства: 2х отсечных клапана (1002).

- Требования. $PFH < 1e^{-8}$, отказоустойчивая связь.

Вопрос 5. Какие компоненты вы выберете?

1. ПЛК. Honeywell SM (SIL3), модули ввода 6ES7134-6GF00-0AA1 (SIL3).
2. ПЛК. Siemens S7-1200 (SIL2), модули 6ES7131-6BH01-0BA0 (SIL2).
3. Пневматическая система с реле.

Ответ 1. Honeywell SM + SIL3-модули

Объяснение.

- S7-1200 не подходит по SIL.
- Пневматика не обеспечит $PFH < 1e^{-8}$.

Выводы.

1. Реальные аварии происходят из-за игнорирования диагностики и SIL.
2. Расчет PFH – ключевой этап выбора ПЛК.
3. Резервирование $\neq$ надежность – важно учитывать общие причины отказов (коррозия, ЕМИ).

Тест 9.4. Разбор реального сертификата SIL (на примере Exida) и FMEA для ПЛК.

Часть 1. Анализ сертификата SIL (Exida для ПЛК Siemens S7-1500F).

Пример сертификата Exida (ключевые разделы).

1. Общие данные.

- Устройство. Siemens SIMATIC S7-1500F (логический решатель).
- Стандарт. МЭК 61508.2010, Part 1/2.
- Уровень SIL. SIL3 (для аппаратной части).
- PFH . 5.3×10^{-9} (для конфигурации 1oo1D).

2. Критические параметры.

- $SFF \geq 90\%$ (требование SIL3).
- HFT 1 (возможность работы с одним отказом).
- Температурный диапазон. $0...+60^{\circ}\text{C}$ (выход за пределы $\rightarrow$ потеря сертификации).

3. Ограничения.

Запрещено:

- Использование несертифицированных модулей ввода-вывода.
- Изменение алгоритмического без верификации Exida.

Требуется.

Ежегодный тест диагностики (например, проверка Watchdog Timer).

Вопрос 1. Можно ли его использовать для SIL3?

Дано: Сертификат ПЛК с $SFF = 85\%$ и $HFT = 0$.

Ответ. Нет! Для SIL3 нужно $SFF \geq 90\%$ и $HFT \geq 1$.

Часть 2. FMEA СПАЗ/SIS) для ПЛК.

Цель FMEA. Выявить потенциальные отказы компонентов ПЛК и их влияние на СПАЗ/SIS.

Пример FMEA для модуля ввода ПЛК (табл. 9.1).

Таблица 9.1. FMEA для модуля ввода ПЛК.

Компонент	Вид отказа	Причина	Эффект	Меры
Аналоговый вход	Обрыв цепи	Коррозия контактов	Ложный «нормальный» сигнал	Мониторинг тока 4-20 мА
CPU	Зависание	Сбой ПО	Отказ СПАЗ/SIS	Watchdog Timer + резервирование
Выходной релейный модуль	Залипание контактов	Перегрев	Невозможность аварийного останова	Диагностика состояния контактов

Дано:

В FMEA для ПЛК не учтен отказ коммуникационного модуля.

Вопрос 1. Чем это грозит?

Ответ. Риск потери связи с датчиками/исполнительными механизмами → отказ СПАЗ/SIS.

Решение. Резервирование шины (например, PROFIBUS + Ethernet).

Ситуация. После модернизации СПАЗ/SIS с ПЛК Rockwell GuardLogix (SIL2) произошел отказ аварийного останова. Аудит выявил:

- Использованы несертифицированные модули ввода (SFF < 60%).

- Сторожевой таймер был отключен для «оптимизации».

Последствия. Простой завода + штраф \$500K.

Вопрос 2. Какие нарушения МЭК 61511 здесь допущены?

1. Использование SIL2-ПЛК для SIL3-функций.
2. Несоответствие SFF и отключение диагностики.
3. Отказ от резервирования.

Ответ 2. Несоответствие SFF и отключение диагностики

Итоговые вопросы.

Вопрос 3. Где в сертификате EXIDA искать данные о PFH?

1. В разделе «Environmental Conditions».
2. В таблице «Safety Parameters».
3. В приложении «Warranty».

Ответ 3. В таблице «Safety Parameters».

Вопрос 4. Какое значение SFF допустимо для SIL2?

1. 60-90%.

2. <50%.

3. 99%.

Ответ 4. 60-90%.

Вопрос 5. Зачем выполняют FMEA для ПЛК?

1. Оцениваются последствия отказов компонентов.

2. Измеряется температура корпуса.

3. Оптимизируется код программы.

Ответ 5. Оцениваются последствия отказов компонентов.

Ключевые выводы.

1. Сертификат SIL – это «паспорт безопасности», где критичны PFH, SFF, HFT.

2. FMEA помогает предупредить отказы на этапе проектирования.

3. Нарушение условий сертификации (например, температурный режим) аннулирует SIL!

Тест 9.5.

Спецификация требований безопасности описывает логику, которую должен выполнять логический решатель, с использованием следующего текстового описания.

Реактор периодического действия имеет два режима работы. «смешивание» (режим 1) и «стерилизация на месте» (SIP, режим 2). Режим SIP (ГОСТ Р ИСО 13408-5-2011) включает введение дезинфицирующего химического вещества в смесительный сосуд при высокой температуре и давлении. В режиме SIP пределы температуры и давления установлены на 100 кПа (изб.) и 230°C. В другом режиме пределы установлены на 200 кПа (изб.) и 300 °C. Режим определяется двумя дискретными сигналами, которые равны логической 1, когда режим активен.

ЗАДАНИЕ. Нарисуйте блок схему для программируемой электронной системы (PES), который будет выполнять задачи, требуемые спецификацией требований безопасности. Для каждой технологической переменной предполагается, что код для сканирования входов и выходов, а также преобразования сигналов передатчиков в реальные значения в инженерных единицах уже написан.

Вопрос 1. Какие два режима работы описаны в спецификации?

Ответ В. Смешивание и стерилизация на месте (SIP).

Объяснение. Это базовый вопрос на понимание теста. Спецификация явно называет два режима: «смешивание» (режим 1) и «стерилизация на месте, SIP» (режим 2).

Вопрос 2. Каковы пределы температуры и давления для режима стерилизации на месте (SIP)?

Ответ А. 100 кПа и 230°C.

Объяснение. В тексте прямо указано: «*В режиме SIP пределы температуры и давления установлены на 100 кПа (изб.)*»

и 230°C». Важно запомнить, что для каждого режима есть свои критические параметры, которые система безопасности должна контролировать.

Вопрос 3. Как определяется режим работы реактора?

Ответ С. По двум дискретным сигналам.

Объяснение. Режим определяется не технологическими параметрами (температурой, давлением), а отдельными дискретными сигналами (вкл/выкл), которые явно указывают системе, какой режим активен. Это стандартная практика для четкого разграничения состояний.

Вопрос 4. Какой логический оператор следует использовать для определения состояния режима SIP, если оба сигнала равны 1?

Ответ А. «И» (AND).

Объяснение (ключевое): В спецификации сказано [27]: *«Режим определяется двумя дискретными сигналами, которые равны логической 1, когда режим активен»*. Это означает, что для активации режима SIP необходимы одновременно оба сигнала. Логическая операция, которая дает истину (1) только тогда, когда **все** ее входы истинны (1), – это оператор **»И» (AND)**.

Объяснение.

Для решения задачи по спецификации требований безопасности необходимо разработать логическую схему, которая будет управлять режимами работы реактора.

Определение режимов. У нас есть два режима работы. «смешивание» и «стерилизация на месте». Каждый из этих режимов имеет свои пределы для температуры и давления. Нам нужно, чтобы система выбирала уставки в зависимости от режима. Если активен режим SIP (сигнал_SIP = 1), мы используем одни уставки, если активен режим смешивания (сигнал_Mix = 1) – другие.

Логика управления. Для управления режимами необходимо использовать два дискретных сигнала. Если оба сигнала равны 1, это означает, что активен режим SIP. Логическая схема должна обрабатывать входные данные и включать соответствующие системы управления ((рис.9.1).

В блок схеме для программируемой электронной системы следует реализовать логику, которая будет проверять значения этих сигналов и, в зависимости от их состояния, управлять соответствующими выходами (например, запускать насосы, открывать клапаны и т.д.).

Нужно не только выбрать уставки, но и проверить, что сигналы режимов не конфликтуют (оба не активны одновременно или оба не выключены)

Безопасность. Учитывая, что в режиме SIP технологические установки работают при высоких температурах и давлениях, важно преду-

смотреть дополнительные меры безопасности, такие как автоматические отключения и сигнализации при превышении установленных пределов.

Логика (табл.9.2) может быть реализована различными способами. Один из вариантов представлен в виде логической блок-схемы, включающей проверку недопустимых режимов. При обнаружении неверных входных сигналов режима активируются нижние пределы давления и температуры.

Таблица 9.2. Логическая таблица истинности

Режим1	Режим2	Ошибка режима	Выбор режима
0	0	0	Низкий предел
0	1	1	Низкий предел
1	0	1	Высокий предел
1	1	0	Низкий предел

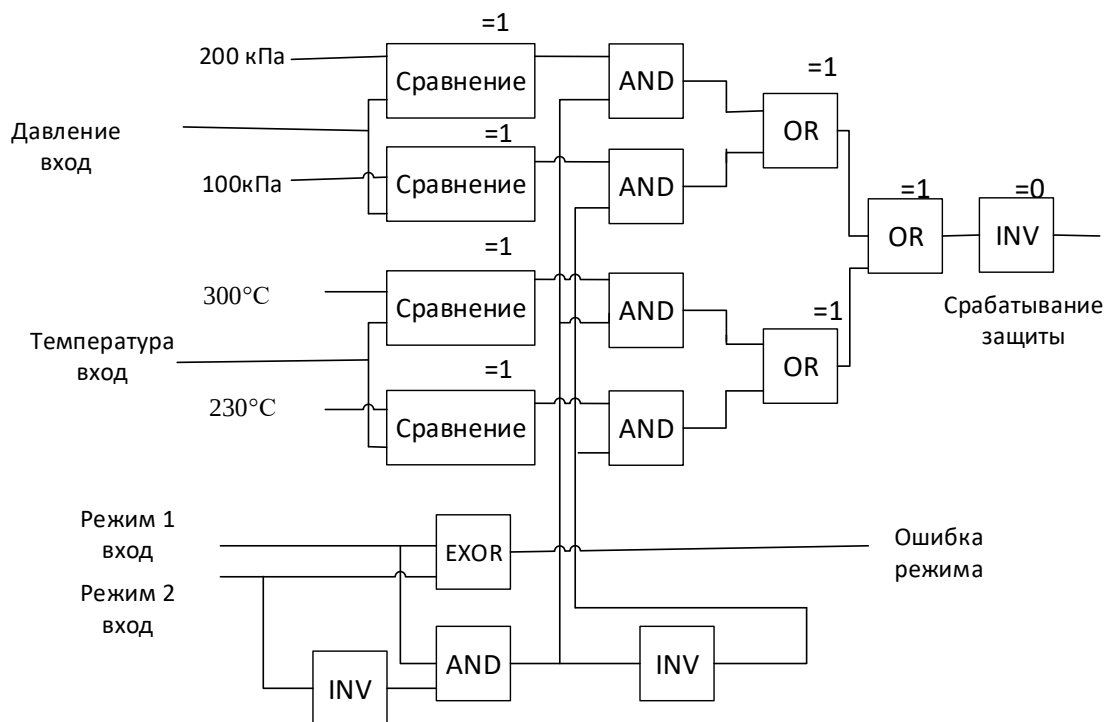


Рис.9.1. Блок схема для программируемой электронной системы

Приведенная выше диаграмма представляет собой упрощенное толкование требований, изложенных в вопросе. Она не включает другие функции, которые потребовались бы в реальной системе, такие как фиксация (чтобы при срабатывании функции).

Для получения дополнительной информации см. [27].

9.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 9.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 9».

Тест 9.6. Дана диаграмма причин и следствий, приведенная ниже (табл.9.3).

Таблица 9.3. Диаграмма причин и следствий [27].

Tag	Описание	SIL	Диапазон прибора
TSH-25	Высокая температура верха реактора	2	Дискрет.
TSH-26	Высокая температура низа реактора	2	Дискрет.

Предполагая, что система работает по принципу «отключение при обесточивании» и когда входной сигнал активен, он логически истинен в логическом решателе. Какой функциональный блок следует использовать для соединения двух входов температурных реле с выходным клапаном?

- И (AND).
- ИЛИ (OR).
- НЕ-ИЛИ (NOR).
- НЕ-И (NAND).
- Ни один из вышеуказанных ответов не верен.

Тест 9.7. Какое утверждение на языке релейной логики (рис9.2). наиболее точно соответствует следующему текстовому утверждению? [27]

Если вход А истинен, а вход В не истинен, то выход С должен быть истинен.

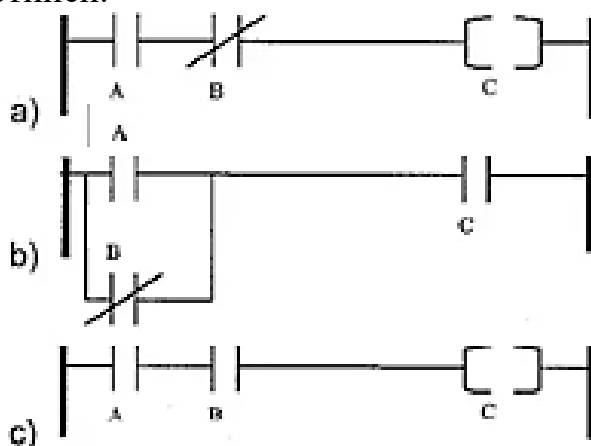


Рис. 9.2. Логика защиты на языке релейной схемы

Для получения дополнительной информации см. [27].

Тест 9.8 А, В и С – дискретные входы в безопасный ПЛК, а D – выход (рис.9.3). Какое утверждение на языке релейной логики наиболее точно представляет голосование 2oo3 для этих входов [27]?

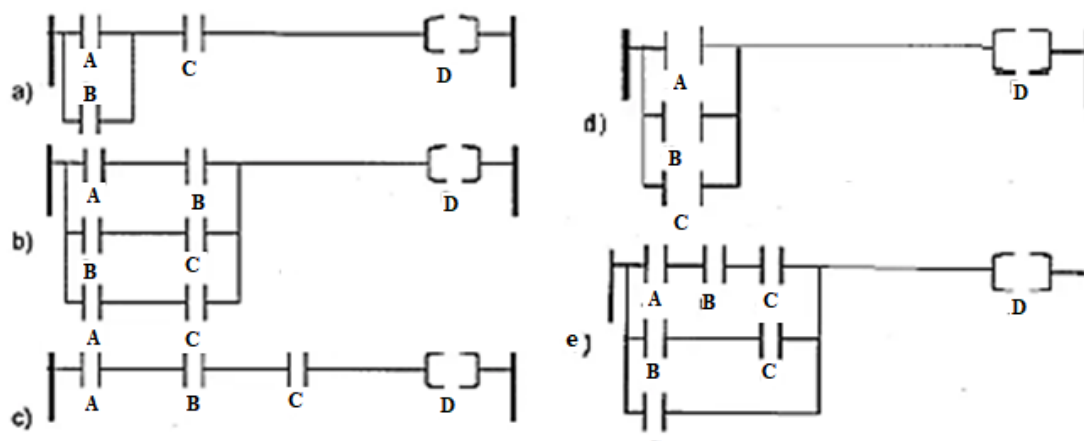


Рис. 9.3. Логика защиты на языке релейной схемы к тесту 9.8
Для получения дополнительной информации см. [27].

Тест 9.9. Система безопасности (СПАЗ/SIS) инициирует остановку с помощью клапанов для остановки с голосованием 1oo2. Система имеет ручной обходной путь, который позволяет проводить тестирование [27].

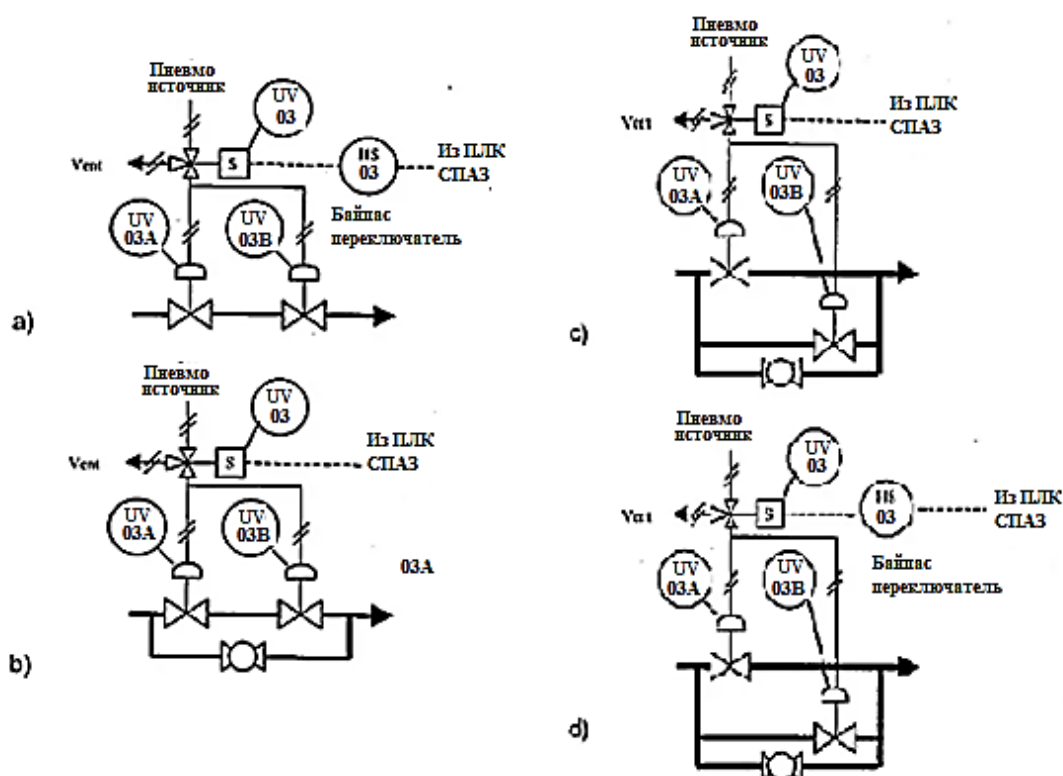


Рис. 9.4. Функциональные схемы для выбора в тесте

Выбор a, b, c, d (рис.9.4), e – ни одно из представлений выше не является правильным.

Какое из следующих изображений лучше всего представляет эту ситуацию на схеме трубопроводов и приборов (P&ID), показывая как переключатель обхода, так и клапан обхода?

Для получения дополнительной информации см. [27].

Тест 9.10.

Датчик с выходным сигналом 4–20 мА подключен к аналоговому входу безопасного ПЛК. Сигнал преобразуется в цифровой с помощью 12-битного преобразователя и представляется числом от 0 до 4095. Датчик откалиброван на диапазон процесса 100 (689.47 кПа)–250 (1723.68 кПа). Точка срабатывания функции безопасности должна быть установлена на 1378 кПа.

Уставка в блоке сравнения должна быть наиболее близка к.

- a) 3277.
- b) 2730.
- c) 3000.
- d) 2750.
- e) 4210.

Тест 9.11.

Детальное проектирование включает выбор технологии. Возможные технологии включают электромеханические реле, твердотельную логику и программируемые электронные системы (PES).

Сравните PES и электромеханические реле, указав преимущества и недостатки каждого. Также объясните, в каких ситуациях каждая технология будет более предпочтительной.

Могут быть упомянуты значительное количество аргументов в Ответе на вопрос:

Объясните, как аналоговый датчик с выходным сигналом 4–20 мА может использоваться в СПАЗ/SIS, где логическая часть состоит из электромеханических реле.

Тест 9.12. Сравнение технологий для систем безопасности (СПАЗ/SIS).

Вопрос 1. Каковы основные преимущества программируемых электронных систем (PES) по сравнению с электромеханическими реле?

- A) Низкая стоимость.
- B) Гибкость настройки логики.
- C) Устойчивость к помехам.
- D) Простота установки.

Вопрос 2. В каких ситуациях более предпочтительно использовать электромеханические реле?

- A) Для сложных логических задач.
- B) Для простых логических задач.
- C) Когда требуется высокая гибкость.
- D) Для систем с необходимостью встроенной диагностики.

Вопрос 3. Какие недостатки имеют PES по сравнению с реле?

- А) Высокий уровень ложных срабатываний.
- В) Необходимость сертификации по SIL.
- С) Более сложная установка.
- Д) Все вышеперечисленное.

Вопрос 4. Как аналоговый передатчик с выходным сигналом 4–20 мА может использоваться в СПАЗ/SIS с электромеханическими реле?

- А) Для передачи данных в облако.
- В) Для измерения температуры.
- С) Для сравнения аналогового сигнала с заданной точкой срабатывания.
- Д) Для управления насосами.

Тест 9.13. Итоговые вопросы для самопроверки.

1. Почему в формуле расчета PFD_{avg} для резервированных компонентов используется квадрат λ_{du} ?
2. Как конфигурация 2oo3 влияет на PFD_{avg} и STR по сравнению с 1oo2?
3. Какие компоненты СПАЗ/SIS обычно вносят наибольший вклад в STR?

10. ДИАГНОСТИКА СПАЗ.

10.1. Ключевые принципы диагностики СПАЗ.

Задание 10.1. Уяснить ключевые принципы применения систем приборной безопасности.

Современные программно-аппаратные средства контроля и интеллектуальные технологии значительно повысили эффективность диагностики компонентов систем противоаварийной защиты (СПАЗ).

Хотя современная система противоаварийной защиты (СПАЗ) оснащена интеллектуальными датчиками, продвинутыми алгоритмами самодиагностики и мощными контроллерами и кажется, что все риски под контролем, но... почему аварии всё ещё происходят?

Оказывается, даже самые совершенные системы уязвимы перед динамикой технологического процесса – внезапные изменения давления, температуры или нагрузки могут маскировать опасные отказы.

Представьте, что мы оцениваем здоровье человека (нашу систему безопасности).

Опасные отказы (λ_D) – это все возможные болезни.

Обнаруживаемые опасные отказы (λ_{DD}) – это болезни, которые можно выявить на ежегодном медосмотре (например, повышенное давление).

Необнаруживаемые опасные отказы (λ_{DU}) – это скрытые болезни, которые протекают бессимптомно и могут внезапно проявиться (например, ранняя стадия онкологии без симптомов).

Теперь применим эту аналогию к используемым формулам расчета диагностики.

DC (Diagnostic Coverage) – Диагностический контроль.

Что это? Это **эффективность** встроенной, автоматической диагностики, которая работает в режиме реального времени (например, самодиагностика ПЛК, контроль обрыва петли, проверка целостности памяти). Время обнаружения несоответствия секунды/минуты.

Как работает? Постоянно, без остановки процесса.

Что обнаруживает? Отказы, которые можно выявить «изнутри» системы.

Что показывает? Насколько хорошо она находит отказы, когда они происходят.

Формула для расчета:

$$DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU}) = \lambda_{DD} / \lambda_D.$$

Пример:

Если датчик имеет общую интенсивность опасных отказов (λ_D) 1000 FIT (10^{-6} /час), и диагностика обнаруживает 900 из них ($\lambda_{DD} = 900$ FIT), то:

$$DC = 900 / 1000 = 0.9 \text{ или } \mathbf{90\%}.$$

Вывод: DC – это показатель качества диагностики одного компонента СПАЗ или канала.

Диагностический контроль (DC) – это способность системы выявлять собственные внутренние неисправности. Он разделяется на и **PTC** (ручную периодическую проверку), которая проводится в плановом порядке и обычно требует частичной остановки СПАЗ и **PDC** (автоматическую периодическую диагностику), которая работает постоянно.

1. **PTC (Proof Test Coverage)** – это коэффициент, доля опасных отказов, которые обнаруживаются в результате периодических, плановых, ручных (или полуавтоматических) испытаний, проводимых на всей СПАЗ или ее части.

Такие тесты часто требуют остановки или частичного вывода из эксплуатации для проверки фактической способности SIS выполнять свою защитную функцию.

Примеры:

Тестирование срабатывания датчика: Подача на датчик реального или имитированного сигнала, чтобы убедиться, что он корректно реагирует.

Полное тестирование цикла SIS: Инициирование срабатывания всей цепи безопасности (от датчика до исполнительного элемента), чтобы убедиться, что она работает как единое целое. Например, проверка закрытия аварийного клапана.

Калибровка датчиков: Проверка и корректировка точности измерений.

Период проверки: месяцы/годы (интервал TI).

Как работает?

Требуется планирования и часто человеческого вмешательства.

Обнаруживает скрытые отказы, которые не были выявлены автоматической диагностикой.

PTC является ключевым инструментом для снижения PFD_{avg} , поскольку он "сбрасывает" накопленную вероятность скрытых опасных отказов до каждого теста

Что обнаруживает? Скрытые отказы, которые не ловит автоматическая диагностика.

Формула расчета:

$$PTC = (\lambda_{DD} + \lambda_{DT}) / \lambda_D,$$

где λ_{DT} – интенсивность отказов, обнаруживаемых ручной проверкой.

2. **PDC (Periodic Diagnostic Coverage)** – это коэффициент, доля опасных отказов, которые обнаруживаются автоматическими, встроенными диагностическими функциями в процессе нормальной работы системы, без остановки процесса и без вмешательства оператора.

Эти диагностики обычно выполняются с определенной периодичностью (например, каждые несколько миллисекунд или секунд). Это понятие относится к аппаратно-программным средствам контроля и является более точной, вероятностной мерой эффективности диагностики.

Это расчетный показатель диагностики, который оценивает, насколько эффективно автоматическая диагностика, работающая циклически (например, самотестирование ПЛК раз в минуту), успеет обнаружить отказ до того, как произойдет опасное событие.

Примеры:

Сравнение показаний двух идентичных датчиков. Если их показания сильно расходятся, это указывает на отказ одного из них.

Контроль целостности цепи. Например, обрыв кабеля датчика.

Контроль функции ПЛК. Проверка внутренней логики и памяти.

Контроль сигналов. Постоянная отправка и прием коротких сигналов для подтверждения работоспособности.

PDC обнаруживает отказы, но не предотвращает их. Он лишь выявляет уже произошедшие опасные отказы.

Что оценивает? Риск того, что отказ произойдет в интервале между диагностическими тестами.

$$PDC \approx (\lambda_{\text{Diag}}/\lambda_{\text{Demand}}) (1 - \exp [-\lambda_{\text{Demand}}/\lambda_{\text{Diag}}]).$$

Здесь.

λ_{Diag} (Частота диагностических тестов) – это частота, с которой система проводит свои внутренние или внешние диагностические тесты. Например, если диагностический тест выполняется каждые 100 часов, то $\lambda_{\text{Diag}} = 1/100 \text{ час}^{-1}$.

λ_{Demand} – это интенсивность, с которой на функцию безопасности поступает запрос на срабатывание (т.е., как часто возникает опасная ситуация, требующая активации СПАЗ/SIS).

Формула показывает, что потенциал эффективного диагностического покрытия, которое мы можем приписать SIF или СПАЗ/SIS, так называемый кредит, зависит от соотношения частоты диагностических проверок и частоты возникновения опасных ситуаций.

Если диагностические тесты проводятся значительно чаще, чем возникают опасные запросы ($\lambda_{\text{Diag}} \gg \lambda_{\text{Demand}}$), то вероятность обнаружения отказа до запроса $P = \exp(-\lambda_{\text{Demand}} / \lambda_{\text{Diag}})$ будет высокой.

P – это вероятность того, что за время между двумя диагностическими проверками отказ **НЕ** произойдет.

Прямо в международных стандартах на основе МЭК 61508 эта **конкретная** формула не прописана. Она является развитием и детализацией общих принципов, заложенных в этих стандартах. Введение этой количественной меры одна из ключевых методик, продвигаемых организацией **Exida** для более точного и обоснованного расчёта показателей безопасности (как PFDavg).

Это часть ее фирменного метода расчёта, который часто называют «**Методом Exida**» или упоминают в их руководствах и стандартах. Такой подход развивает принципы, заложенные в международном стандарте МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью», и предназначен для более точного расчёта вклада автоматической диагностики в показатели безопасности системы.

Таблица зависимости PDC от соотношения частот

$\lambda_{\text{Diag}} / \lambda_{\text{Demand}}$	PDC	Объяснение
2	~78%	Диагностика запускается всего в 2 раза чаще, чем возможна авария. Высокий риск, что отказ произойдет <i>до</i> того, как диагностика его обнаружит.
10	~95%	Диагностика работает в 10 раз чаще. Риск значительно снижается. Это часто целевое значение для SIL 2/3.
100	~99%	Диагностика практически непрерывна относительно частоты аварий. Очень высокая эффективность (соответствует SIL 3/4).

Почему это важно? Классический коэффициент DC говорит: «Наша диагностика умеет обнаружить 99% отказов». Коэффициент PDC уточняет: «Но так как она запускается только раз в минуту, а авария может случиться в любой момент, ее реальная эффективность (PDC) составляет, например, 95%».

PTC и PDC влияют на PFDavg по-разному:

PDC постоянно «отсекает» часть накапливающихся опасных отказов, переводя их в обнаруженные и ремонтпригодные. Это сглаживает кривую PFDavg, снижая её общий уровень. Он уменьшает «склон» пины.

PTC же «сбрасывает» накопленные скрытые отказы до каждого проверочного теста. Он уменьшает «высоту» пины и определяет интервал между «зубьями».

3. SFF (Safe Failure Fraction) – это доля безопасных отказов.

Что это? Суммарный показатель, учитывающий ВСЕ механизмы обнаружения: и автоматические, и ручные.

Суть: Какова вероятность, что при отказе система перейдет в БЕЗОПАСНОЕ состояние? Учитываются ВСЕ отказы: и безопасные (λ_S), и опасные, но обнаруженные (λ_{DD}).

Формула:

$$SFF = (\Sigma \lambda_S + \Sigma \lambda_{DD} + \Sigma \lambda_{DT}) / (\Sigma \lambda_S + \Sigma \lambda_D).$$

Что показывает:

Склонность системы к безопасному поведению при отказах. Это ключевой параметр для определения минимального уровня аппаратной отказоустойчивости (HFT) согласно стандарту МЭК 61508.

Пример:

Пусть у нашего датчика:

$\lambda_S = 500$ FIT (безопасные отказы, например, обрыв провода)

$\lambda_{DD} = 900$ FIT (обнаруженные опасные отказы)

$\lambda_{DU} = 100$ FIT (необнаруженные опасные отказы)

$\lambda_D = \lambda_{DD} + \lambda_{DU} = 1000$ FIT

$SFF = (500 + 900) / (500 + 1000) = 1400 / 1500 \approx 0.933$ или **93.3%**

Это значение SFF позволяет, например, использовать архитектуру с HFT=0 (один канал) для SIL 2.

Вывод: SFF – это «архитектурный» показатель, определяющий, КАК мы можем строить систему (сколько нужно резервирования).

Сводная таблица расчетов диагностики показана (табл.10.2).

Таблица 10.2. Расчетные формулы диагностики SIF.

Параметр	Тип диагностики	Периодичность	Обнаруживает	Формула
DC	Автоматическая	Постоянно	λ_{DD}	$DC = \lambda_{DD} / \lambda_D$
PTC	Ручная проверка	Периодически (TI)	$\lambda_{DD} + \lambda_{DT}$	$PTC = (\lambda_{DD} + \lambda_{DT}) / \lambda_D$
SFF	Суммарный показатель	-	Все обнаруженные отказы	$SFF = (\lambda_S + \lambda_{DD} + \lambda_{DT}) / (\lambda_S + \lambda_D)$

Ключевые выводы:

1. **DC и PTC – дополняют друг друга, а не заменяют.**
2. **Чем выше DC – тем меньше необходимость в PTC.**
3. **SFF зависит от обоих видов диагностики.**
4. **PTC всегда $\geq$ DC** (поскольку ручная проверка обычно обнаруживает больше).

Именно эта связка **DC + PTC $\rightarrow$ SFF** определяет, какую архитектуру (HFT) мы можем использовать для достижения целевого SIL.

Необходимый уровень диагностического покрытия определяется в зависимости от сложности компонентов СПАЗ и выбранного метода проектирования из вариантов **ROUTE 1H** и **ROUTE 2H** (ГОСТ Р МЭК 61508/61511).

Реализация сложной диагностики осуществляется с использованием программно-аппаратных средств на основе метода ROUTE 2H, в

то время как ROUTE 1H предполагает менее строгие требования к ней.

Если ROUTE 1H – это «базовая страховка», то ROUTE 2H – это полный аудит безопасности в течение жизненного цикла СПАЗ. В чём их разница.

ROUTE 2H требует:

- Использовать программно-аппаратные компоненты СПАЗ/SIS типа В.
- Детектировать 99% опасных отказов ($DC \geq 99\%$ для SIL 3) – почти как в авиации!
- Анализировать каждый возможный сценарий отказа – никаких «авось пронесёт».
- Жёстко привязывать DC к уровню SIL. Ошибки в расчётах могут стоить большим потерям.

Для компонентов СПАЗ/SIS стандарт МЭК 61508 требует подтверждения того, что элемент и система разработаны в соответствии со строгим жизненным циклом безопасности, минимизирующим систематические ошибки проектирования.

Это достигается путем:

- «Proven in Use» (подтвержденным опытом эксплуатации), доказательством того, что компонент успешно и безопасно использовался в аналогичных приложениях в течение достаточного времени.
- Доказательством применения строгих методов и процедур жизненного цикла (верификация, валидация, анализ рисков и т.д.).
- Доказательством того, что устойчивость к случайным аппаратным сбоям достигается за счет:
 - Аппаратной отказоустойчивости (HFT) с использованием резервирования компонентов (например, 1oo2, 2oo3 и т.д.).
 - Глубокого диагностического покрытия (Diagnostic Coverage - DC), способности системы обнаруживать опасные сбои.

ROUTE 1H допускает:

- Упрощённые допущения, что позволяет работать по типовым данным, а не под конкретный риск.
- Меньшие требования к DC. В результате некоторые отказы могут остаться «в слепой зоне».
- Акцент на предотвращение, а не на диагностику (как если бы врач лечил, не ставя точный диагноз).

Выбор между ROUTE 1H и ROUTE 2H – это компромисс между стоимостью и безопасностью. Если ОПО – это нефтеперерабатывающий завод, где ошибка означает взрыв, то ROUTE 2H не обсуж-

дается. За счет глубокой диагностики СПАЗ в этом методе проектирования достигается низкая вероятность опасного отказа в течение всего жизненного цикла.

Чем выше DC, тем выше SIL – но и тем сложнее (и дороже) система. Однако классический коэффициент DC не учитывает частоту выполнения самой диагностики. Диагностика, которая выполняется раз в год, менее эффективна, чем та же самая диагностика, выполняемая раз в секунду.

Поэтому применяемый ведущими компаниями по сертификации коэффициент диагностического покрытия PDC – это более точный, **расчётный** показатель, который учитывает не только способность диагностики обнаружить отказ, но и то, как часто она это делает.

10.2. ПРАКТИКУМ ПО ДИАГНОСТИРОВАНИЮ СПАЗ ОПО.

Задание 10.2. В предположении наличия исходных требований ОПО к СПАЗ подготовить отчет по верификации и отчет по валидации решения в кейсе.

Кейс 10.1. Разбор инцидента «Ложное срабатывание аварийного отключения (ESD)».

.Событие.

На установке переработки газа произошло необоснованное аварийное отключение (Emergency Shutdown). Технологические параметры (давление, уровень, расход) находились в норме, но система безопасности инициировала полную остановку, приведя к значительным финансовым потерям.

Задача. Вы – инженер по функциональной безопасности. Вам поручено провести расследование и найти причину ложного срабатывания.

План расследования и решения (Пошаговый алгоритм)

Чтобы найти «иголку в стоге сена», необходимо действовать системно – от самого простого и вероятного к сложному.

ШАГ 1: Анализ «цифровых уликов» – Журналы событий SIS.

Действие: Первым делом запросите и изучите журнал событий ПЛК безопасности (например, Siemens S7-400H) и журналы АСУ ТП.

Что ищем:

Какой именно датчик инициировал отключение? (например, датчик давления PSL-2105).

Какое значение он передавал в момент срабатывания? (Было ли это скачкообразное изменение или плавный дрейф?).

Были ли предупреждения о неисправности? (Сигналы «Обрыв цепи», «Неисправность датчика»).

Вывод: Этот шаг сужает круг «подозреваемых» до конкретного оборудования или сигнала.

ШАГ 2: Визуальный и аппаратный осмотр «подозреваемого».

Действие: Осмотрите датчик (например, Rosemount 3051) и его подводящую линию.

Что ищем:

Физические повреждения: Трещины, следы коррозии, попадание влаги в клеммную коробку.

Загрязнение. Отложение продуктов процесса на мембране датчика.

Состояние импульсных линий. Засорение, обледенение.

ШАГ 3: Проверка «нервной системы» – Сигнальные линии.

Действие. Проведите электротехнические измерения сигнального кабеля (4-20 мА).

Что ищем.

Обрыв или короткое замыкание: Проверка мультиметром.

Электромагнитные помехи. Осциллографом можно обнаружить наводки от силовых кабелей, проложенных рядом.

Качество заземления: Плохое заземление – частая причина помех.

ШАГ 4: Проверка «логики и настроек» – Программа и конфигурация.

Действие: Проверьте конфигурацию в логическом решателе.

Что ищем:

Корректность уставок. Например, уставка срабатывания PSL-2105 установлена на 50 бар, а не на 5.0 бар? (Ошибка при вводе).

Логiku обработки сигнала. Используется ли фильтрация сигнала для подавления кратковременных скачков? Возможно, она отключена или настроена неверно.

Калибровку. Проведите поверку датчика калибратором. Соответствует ли выходной сигнал (мА) реальному давлению?

Диагностика (памятка). Основные причины ложных срабатываний.

1. Отказы датчиков (~60% случаев).
2. Дрейф. Постепенное изменение метрологических характеристик.
3. Внезапный отказ. Выход из строя чувствительного элемента.
4. «Залипание» мембраны из-за полимеризации продукта.
5. Проблемы с сигнальными линиями (~25% случаев).
6. Электромагнитные помехи (ЭМП). Наводки от силового оборудования.
7. Обрыв. Короткое замыкание: Механические повреждения кабеля.
8. Плохие контакты: Окисление в клеммных колодках.
9. Ошибки в проектировании и настройке (~15% случаев).
10. Неправильные уставки. Ошибка при вводе в систему.
11. Отсутствие фильтров. Система реагирует на кратковременные технологические «выбросы».

12. Ошибки в логике ПЛК. Например, неверная временная задержка.

Ложное срабатывание – это не просто досадная неприятность, а симптом потенциальной слабости в системе безопасности.

Эффективное расследование строится на последовательном исключении возможных причин:

Начните с данных (журналы событий).

Перейдите к «железу» (датчик, кабель).

Завершите проверкой «логики» (программа, настройки).

Такой системный подход позволяет не только устранить последствия, но и предотвратить повторение инцидента в будущем.

Кейс 10.2. Миф о 99% диагностике.

Ситуация. СПАЗ/SIS для газовой турбины (архитектура 2oo3) с заявленным $PFD_{avg} = 7.6 \times 10^{-4}$ (SIL 3), отказала как это потом было установлено, из-за необнаруженной ошибки ПО.

Исходные данные.

Логический контроллер.

– $\lambda DU = 1 \times 10^{-7}$ 1/час (аппаратная часть).

– DC = 99% (только для аппаратуры!).

Была спроектирована высоконадежная система защиты (СПАЗ/SIS) для газовой турбины с архитектурой 2oo3 (два из трех). Это означает, что для срабатывания защиты должны отказать как минимум два из трех каналов. Такая архитектура очень надежна и должна обеспечивать высокий уровень полноты безопасности (SIL 3).

Был выполнен расчет. Инженеры рассчитали $PFD_{avg} = 7.6 \times 10^{-4}$, что соответствует SIL 3. В расчетах они использовали очень хорошие показатели для аппаратной части контроллеров. низкую интенсивность необнаруженных опасных отказов ($\lambda DU = 1 \times 10^{-7}$) и очень высокий коэффициент диагностического покрытия (DC = 99%). Это означало, что по их расчетам, система вовремя обнаруживает и парирует 99% всех аппаратных сбоев.

Но вот проблема («Подвох»). Расчеты учитывали только аппаратные отказы. В реальности система управляется программным обеспечением (ПО). В ПО была ошибка (например, логическая ошибка или зацикливание), которую внутренняя диагностика контроллера не могла обнаружить. Таким образом, реальная интенсивность необнаруженных опасных отказов всей системы (аппаратура + ПО) была намного выше. $\lambda DU_{real} = 5 \times 10^{-1}$.

Катастрофический результат. Произошел отказ системы защиты именно по этой необнаруженной программной причине. Пересчет PFD_{avg} с учетом реальной λDU ПО дал значение 0.19, что соответствует SIL 0 (т.е. система фактически не обеспечивает никакой защиты). Формально была система SIL 3, а на деле – SIL 0!

Такой «подвох» может быть и из-за неучета условий эксплуатации.

Ответы на вопросы кейса.

Вопрос 1. Почему DC никогда не бывает 100%?

Диагностическое покрытие (DC) – это вероятность того, что опасный отказ будет обнаружен средствами встроенной диагностики до того, как он приведет к аварийной ситуации.

Утверждение, что DC никогда не бывает 100%, является фундаментальным принципом проектирования систем безопасности. Вот основные причины, почему это невозможно.

Природа отказов. Некоторые отказы по своей природе не могут быть обнаружены простыми средствами диагностики.

Пример 1. Ошибка в алгоритме программы (как в нашем кейсе). Диагностика, предназначенная для проверки целостности памяти процессора или обрыва провода, не может обнаружить логическую ошибку в бизнес-логике приложения.

Пример 2. Систематические ошибки (ошибки проектирования, требования). Если система спроектирована неправильно, она будет неправильно работать всегда, и диагностика этого не увидит.

Отказы самой диагностики. Средства диагностики сами являются частью системы и также могут отказаться. Нельзя создать абсолютно надежный механизм диагностики внутри ненадежной системы.

Латентный период (время обнаружения). Даже если отказ в конечном итоге будет обнаружен, может существовать промежуток времени между моментом возникновения отказа и моментом его обнаружения. В течение этого периода отказ считается необнаруженным (DU). 100% покрытие подразумевало бы нулевой латентный период для всех без исключения отказов, что невозможно.

Конечная полнота тестов. Встроенная диагностика – это, по сути, набор тестов. Тестирование не может доказать отсутствие ошибок (теорема Дейкстры). Можно найти множество ошибок, но нельзя найти все. Всегда существует вероятность существования еще не обнаруженного сценария отказа.

Вывод. Заявление о DC=100% – это красный флаг, признак некомпетентности или недобросовестности. Всегда следует скептически относиться к столь высоким показателям и задавать вопрос. «А что именно диагностируется, а что может остаться незамеченным?»

Вопрос 2. Как разделять диагностику аппаратной и программной частей?

Это ключевой вопрос современного проектирования СПАЗ/SIS. Аппаратная и программная части требуют принципиально разных подходов к диагностике.

А. Диагностика аппаратной части.

Цель. Обнаружение физических дефектов и случайных аппаратных сбоев (обрыв цепи, короткое замыкание, отказ микросхемы памяти, отказ процессора).

Методы.

1. **Избыточность и сравнение.** В архитектурах 2002 или 2003 два канала выполняют одни и те же вычисления, и их результаты сравниваются. Расхождение означает отказ в одном из каналов.

2. **Тестирование по известным образцам.** Периодически на вход алгоритма подается заведомо известный тестовый сигнал, и результат вычислений сравнивается с эталонным ответом. Несовпадение указывает на сбой в аппаратуре или в базовых алгоритмах.

3. **Контроль целостности памяти (CRC, Checksums).** Проверка, что программный код и критичные данные в памяти не были физически повреждены.

4. **Контроль временных циклов (Watchdog Timer).** Специальная схема следит, что процессор регулярно «отчитывается» о своей работе. Если отчет не поступает (процессор «завис»), watchdog перезагружает систему.

5. **Аналоговый мониторинг.** Проверка сигналов на обрыв и короткое замыкание (например, путем подачи слабого тестового тока и измерения падения напряжения).

Б. Диагностика программной части (Software) и системных ошибок.

Цель. Обнаружение логических ошибок, ошибок в требованиях, ошибок в коде и некорректного поведения системы в целом.

Методы (гораздо более сложные).

Функциональное тестирование. Проверка сложных сценариев и граничных условий. Это делается в основном на этапе разработки и валидации системы, а не в ходе ее эксплуатации.

Диверсификация (снижение рисков) за счет резервирования. Два канала выполняют одну и ту же функцию, но используют для этого разное аппаратное обеспечение, разные процессоры, разные операционные системы и, что важно, программное обеспечение, написанное разными командами разработчиков по разным методикам. Это помогает избежать общих ошибок (как в нашем кейсе), когда одна и та же ошибка в ПО проявляется одновременно во всех каналах. Архитектура 2003 с диверсифицированным ПО – золотой стандарт для достижения SIL 3.

Мониторинг контроля потока. Специальная программа или аппаратные средства следят за тем, чтобы выполнение кода шло по предопределенным, корректным путям, а не «уходило в сторону» из-за ошибки.

Мониторинг состояния процесса. Система безопасности не должна слепо доверять логике основного контроллера. Она может использовать дополнительные, независимые датчики и простую логику

(например, «если скорость турбины $> X$, а температура выхлопа $> Y$, и при этом нет команды на останов от основного контроллера – это авария») для выявления неадекватного поведения основной системы управления.

Миф о 99% диагностике развенчивается тем, что эти 99% обычно относятся только к случайным аппаратным отказам. Они бессильны против систематических ошибок, особенно в программном обеспечении.

DC $\approx$ 99% возможно для аппаратуры.

DC $\approx$ 0% часто бывает для сложного ПО, если не применять специальные методы.

Поэтому при анализе надёжности системы критически важно спрашивать.

К какой части системы применяется этот высокий DC?

Какие методы используются для диагностики программных и систематических ошибок?

Используется ли диверсификация (снижение рисков) для защиты от общих ошибок в ПО?

Этот кейс наглядно показывает, что формальный расчет PFD_{avg} на основе красивых цифр из документации – это лишь вершина айсберга. Реальная безопасность обеспечивается глубоким пониманием ограничений диагностики и применением целого комплекса организационных и технических мер на всех этапах жизненного цикла системы.

Кейс 10.3. Отказ клапана сброса давления (PSV). Диагностика.

Проблема: Сигнал от SIS есть, но клапан не открылся.

Диагностический подход: «От сигнала к механике».

Проверка получения команды (Цифровой след).

Действие. Анализ журналов SIS. Был ли команда на открытие отправлена на конкретный выходной модуль (DO)?

Цель. Подтвердить, что ошибка не в логике ПЛК, а в физическом исполнении.

Проверка электромеханической части (Силы, чтобы сдвинуть).

Действие. Проверить срабатывание соленоидного клапана (SOV). Подается ли на него напряжение с выхода SIS? Слышен ли щелчок срабатывающего?

Цель. Убедиться, что электрическая команда преобразуется в перемещение.

Проверка пневматической части (Силы, чтобы управлять):

Действие. Проверить давление воздуха на входе и выходе SOV. Есть ли утечки в пневмолинии после соленоида? Доходит ли воздух до пневмопривода клапана?

Цель. Убедиться, что пневмоэнергия доходит до конечного исполнительного механизма.

Проверка механики (Последний рубеж):

Действие. Провести механическую проверку штока клапана на заклинивание (возможно, частичный ход при отключенном воздухе).

Цель. Исключить физическое заедание, коррозию или загрязнение, блокирующее движение.

Это классический пример диагностики последовательной цепи. Отказ произошел на одном из этапов преобразования сигнала: Логика (SIS) -> Электрика (SOV) -> Пневматика (Воздух) -> Механика (Клапан). Решалась задача – пройти по этой цепочке и найти разрыв.

Кейс 10.4. Потеря связи по HART-протоколу.

Проблема. Датчики рабочие, но данные не доходят в систему.

Диагностический подход: «Снизу вверх по сетевому стеку».

Физический уровень (Основа связи).

Действие. Проверить напряжение и ток в петле 4-20 мА. Обрыв или КЗ? Проверить целостность терминаторов.

Цель. Убедиться, что физическая среда для передачи данных исправна. HART – это цифровой сигнал, наложенный на аналоговый ток 4-20 мА. Если петля тока разорвана, то не будет ни того, ни другого.

Уровень конфигурации сети (Правила общения):

Действие. Проверить настройки HART-мультиплексора или интерфейсного модуля. Совпадают ли адреса устройств? Корректно ли настроен опрос?

Цель. Убедиться, что все устройства в сети «говорят на одном языке» и корректно адресованы.

Уровень устройств (Источник проблемы).

Действие. Подключиться к датчику напрямую с помощью HART-коммуникатора. Читаются ли его параметры?

Цель. Локализовать проблему: неисправен конкретный датчик или вся сеть?

HART-сеть – это цепочка. Диагностика всегда начинается с самого простого: есть ли «питание» связи (ток 4-20 мА)? Затем проверяются «правила дорожного движения» (конфигурация сети), и только потом проверяется «исправность машин» (отдельные датчики).

Кейс 10.5. Ложные срабатывания пожарной системы (F&G). Диагностика.

Проблема. Датчики пламени срабатывают без причины.

Диагностический подход: «Разделение сигнала и помехи».

Уровень сигнала и внешние помехи (Окружающая среда).

Действие. Проанализировать обстановку в момент срабатывания: пыль, пар, сварка, блики от солнца или фар.

Цель: Идентифицировать внешний источник, который датчик мог ошибочно принять за пламя.

Состояние датчика (готовность выполнять функции).

Действие. Проверить оптику на загрязнение. Провести калибровку и выполнить функциональный тест с эталонным источником пламени.

Цель. Убедиться, что датчик физически исправен и правильно реагирует на реальное пламя.

Логика системы (Порог чувствительности):

Действие. Проверить в конфигурации SIS порог срабатывания и временные задержки. Слишком низкий порог или отсутствие задержки на подтверждение сигнала?

Цель. Убедиться, что система не настроена излишне чувствительно.

Задача F&G-системы отличать пожар (сигнал) от не-пожара (помеха). Диагностика заключается в том, чтобы понять: система реагирует на реальную, но безобидную помеху (пыль), или она неисправна и «видит» то, чего нет (глюк датчика), или же она настроена так, что любая мелочь вызывает тревогу (ошибка конфигурации).

Кейс 10.6. Диагностика логического устройства (ПЛК SIS).

Объяснение (схематично).

Представьте, что ПЛК SIS – это «командный центр безопасности». Его диагностика – это постоянная самопроверка всех отделов этого центра.

Компонент ПЛК. Что проверяет диагностика?

Центральный процессор (ЦП). Главный командир (мозг). Не «завис» ли он? Правильно ли выполняет логические инструкции? Исправна ли его память?

Модули ввода (DI/AI) Разведчики (глаза и уши). Приносят данные с поля (значения датчиков). Не оборвался ли «телефонный провод» (обрыв шлейфа)? «Не врет ли разведчик» (выход за пределы сигнала)? Не «залип» ли его переключатель?

Модули вывода (DO/AO) – это исполнители ПЛК, его «руки и ноги». Они передают команды исполнительным механизмам. Могут ли они подать нужную команду? Не «коротнули» ли они на месте? Исправна ли их силовая часть?

Коммуникационный модуль – это связист. Обеспечивает связь с другими центрами (АСУ ТП, SCADA). Не разорвана ли связь? Не искажаются ли донесения (ошибки в пакетах данных)?

Диагностический модуль – это внутренняя безопасность. Он непрерывно «обходит все подразделения» центра, сверяет их работу и немедленно докладывает о любых неисправностях, выводя систему в безопасное состояние.

Ключевой вывод.

Диагностика в SIS – это не периодическая проверка, а непрерывный процесс самоконтроля. Каждый модуль постоянно отвечает на во-

прос: «Я еще исправен?» Это единственный способ обнаружить скрытый отказ – неисправность, которая никак не проявляет себя до момента аварии.

Кейс 10.7. Диагностика аварийного повышения давления.

Ситуация.

На химическом предприятии система ПАЗ не сработала при аварийном повышении давления в реакторе. Расследование показало, что.

- Датчик давления (AI-модуль) выдавал некорректное значение.
- Сигнал не был распознан как ошибочный.
- Клапан аварийного сброса (DO-модуль) не открылся.

Задание.

1. Какие методы диагностики должны были выявить неисправность?
2. Как настроить систему, чтобы подобная ошибка обнаруживалась автоматически?
3. Какие дополнительные меры повысят надежность?

Решение (разбор кейса).

1. Методы диагностики, которые должны были сработать (табл.10.3).

Таблица 10.3. Методы диагностики «физики» датчика.

Метод	Что проверяют?	Почему не сработал?
Проверка диапазона сигнала (4–20 мА)	Выход за пределы 3.8–20.5 мА	Датчик выдавал значение в пределах, но неверное
Сравнение с резервным датчиком	Расхождение между двумя датчиками	Резервирование не использовалось
Контроль скорости изменения (dP/dt)	Резкий скачок/падение давления	Не был настроен алгоритм динамической проверки
Диагностика модуля AI (CRC, обрыв цепи)	Целостность сигнальной линии. Ошибки передачи	Ошибка была в самом датчике, а не в линии

Вывод. Нужна комбинация методов, так как один способ может не выявить ошибку.

2. Настройка системы для автоматического обнаружения:

- Ввести резервирование. 2 датчика + голосование (2oo3).
- Добавить динамическую проверку. Если давление не меняется слишком долго или меняется скачком – аварийный сигнал.

- Использовать интеллектуальные датчики с самодиагностикой (например, HART-протокол).

- Настроить периодический тест AI-модулей (например, подача тестового сигнала 10 мА и проверка ответа).

3. Дополнительные меры для повышения надежности:

- Регулярные функциональные тесты (раз в 3–6 месяцев).
- Мониторинг импульсных линий (засорение, обледенение).
- Логирование событий с анализом трендов (если датчик «залипает»).
- Внедрение SIL-2/SIL-3 (стандарты безопасности для датчиков и логики).

4. Вопросы для закрепления.

Вопрос 1. Какой метод диагностики НЕ обнаруживает «залипание» датчика?

- а) Проверка диапазона 4–20 мА.
- б) Контроль скорости изменения сигнала.
- в) CRC-проверка модуля AI.
- г) Резервирование и голосование 2oo3.

Ответ в. (CRC проверяет целостность данных, но не физическое состояние датчика)

Вопрос 2. Почему резервирование датчиков повышает надежность?

- а) Позволяет сравнивать показания и исключать ошибки.
- б) Увеличивает частоту опроса.
- в) Заменяет необходимость функциональных тестов.
- г) Устраняет все виды отказов.

Ответ а.

Вопрос 3. Какая ошибка НЕ будет обнаружена встроенной диагностикой ПЛК?

- а) Обрыв сигнального провода.
- б) Засорение импульсной линии.
- в) Выход сигнала за диапазон 4–20 мА.
- г) Короткое замыкание в модуле AI.

Ответ б. (требуется дополнительный мониторинг).

Данный кейс помогает понять:

- Важность многоуровневой диагностики (аппаратная + логическая).
- Необходимость резервирования и динамических проверок.
- Ограничения встроенной диагностики и важность ручных тестов.

Такой подход соответствует современным стандартам (МЭК 61508, МЭК 61511) и учит проектировать надежные системы ПАЗ.

Заключение.

Диагностика может применяться в виде самотестирования в дополнение к функциональным или контрольным проверкам, которые проводятся периодически как часть общего обслуживания СПАЗ/SIS.

До появления микропроцессоров не удавалось нормально выполнить диагностирование датчиков и исполнительных устройств. Программируемые системы позволили создать более совершенные методы самодиагностики. Вот некоторые новые возможности:

- сравнение значения сигнала срабатывания со связанными переменными;
- использование интеллектуальных датчиков с диагностической сигнализацией;
- использование резервированных компонентов для сравнения значений.

Интеллектуальные датчики и датчики с сертификатами безопасности осуществляют диагностический мониторинг своей электроники и могут обнаружить ошибку или выход сигнала за допустимые пределы.

Кейс 10.8. Диагностика датчика SIF.

На предприятии используют как автоматическую (PDC), так и ручную диагностику (PTC) датчиков. Оценить преимущества применения этих диагностик.

Что такое PTC в контексте PFD?

PTC (Proof Test Coverage) – это доля необнаруженных опасных отказов (λ_{DU}), которую мы можем найти и устранить во время плановой ручной проверки.

- Если **PTC = 100%**, то проверка идеальна: мы находим и исправляем ВСЕ скрытые отказы, накопившиеся за период T_I .
- Если **PTC = 90%**, то мы находим 90% отказов, а 10% остаются в системе и продолжают вносить вклад в риск.

Таким образом, PTC позволяет нам рассчитать эффективную интенсивность необнаруженных отказов (λ_{DU_eff}), которая и используется в формулах PFD.

Классическая формула PFD (без учета PTC)

Для одиночного элемента (1oo1) с постоянной интенсивностью отказов:

$$PFD_{avg} \approx (\lambda_{DU} * T_I) / 2$$

Где:

- λ_{DU} – полная интенсивность необнаруженных опасных отказов.
- T_I – интервал между проверками.

Проблема: Эта формула неявно предполагает, что ручная проверка (**Proof Test**) имеет **100% покрытие (PTC=1)**. То есть, в момент проверки система возвращается в состояние «как новая», так как все скрытые отказы устранены.

Уточненная формула PFDavg с учетом PTC

Когда мы учитываем, что проверка неидеальна ($PTC < 1$), формула усложняется. Полная модель для среднего значения PFD выглядит так:

$$PFD_{avg} \approx [(1 - PTC) * \lambda_{DU} * T_I] / 2 + [PTC * \lambda_{DU} * (T_D/2 + T_R)],$$

где:

- λ_{DU} – полная интенсивность необнаруженных опасных отказов.
- PTC – коэффициент покрытия проверкой (от 0 до 1).
- T_I – интервал между периодическими проверками.
- T_R – среднее время восстановления (время до ремонта после обнаружения отказа).

Разберем формулу на составляющие:

1. $[(1 - PTC) * \lambda_{DU} * T_I] / 2$ – вклад в PFD от тех отказов, которые НЕ обнаруживаются при плановой проверке. Эти отказы могут сохраняться в системе неограниченно долго (множество периодов T_I).

2. $[PTC * \lambda_{DU} * (T_D/2 + T_R)]$ – вклад в PFD от тех отказов, которые обнаруживаются при плановой проверке. Система находится в неработоспособном состоянии только в течение среднего времени восстановления T_R .

Практический пример.

Данные:

- Датчик: $\lambda_{DU} = 0.001$ (1/год)
- Интервал проверок: $T_I = 1$ год
- Время восстановления: $T_R = 8$ часов
- Время диагностики $T_D = 2$ часа
- Покрытие проверкой: $PTC = 0.9$ (90%)

Расчет по классической формуле ($PTC=100\%$):

$$PFD_{avg} \approx (0.001) / 2 = 0.0005, \text{ что соответствует SIL 1}$$

Расчет по уточненной формуле ($PTC=90\%$):

$$PFD_{avg} \approx [(1 - 0.9) * 0.001 / 2 + [0.9 * 0.001 * (2/24 + 8/24)]]$$

$$PFD_{avg} \approx [0.0001] / 2$$

$$PFD_{avg} \approx 0.00005 + 10^{-7} = 0.00005, \text{ что соответствует SIL 2}$$

Вывод из примера: ручная проверка улучшает отказоустойчивость.

Когда использование PTC становится КРИТИЧЕСКИ важным?

1. **Низкое покрытие проверкой ($PTC \ll 1$).** Например, сложность или стоимость проверки позволяет проверить только 60% возможных отказов.

2. **Длинные интервалы T_I .** Если проверки проводятся раз в 2-5 лет, то необнаруженные отказы $(1-PTC)$ накапливаются и значительно увеличивают PFD.

3. **Высокие требования к SIL.** Для SIL 3 и особенно SIL 4 необходим учет всех факторов, влияющих на точность расчета PFD.

Итог.

- **РТС** – это не отдельная формула, а коэффициент уточнения внутри стандартных (МЭК 61508/61511) моделей надежности.

- Стандарты МЭК 61508/61511 используют упрощенные модели, предполагая **РТС ≈ 1**.

- В реальных проектах **учет РТС < 1** позволяет проводить более точные и консервативные расчеты PFD.

- Игнорирование РТС может привести к неконсервативной оценке

(завышению надежности системы), особенно при низком качестве проведения Proof Test.

Уточненная формула PFDavg с учетом PDC.

Для системы с периодической диагностикой (например, самотестирование с интервалом TD) формула средней вероятности отказа по требованию выглядит так:

$$PFD_{avg} \approx [(1 - PDC) \cdot \lambda_{DU} \cdot T_I / 2] + [PDC \cdot DU \cdot (TD / 2 + MR)],$$

где:

- λ_{DU} – интенсивность необнаруженных опасных отказов;
- PDC – коэффициент покрытия периодической диагностикой;
- T_I – интервал между полными плановыми проверками (Proof Test);

- T_D – интервал между циклами периодической диагностики ($TD < T_{ITD} < TI$);

- MR – среднее время восстановления после обнаружения отказа диагностикой.

Разбор формулы на составляющие.

Первый компонент: Отказы, не обнаруживаемые диагностикой $(1 - PDC) \cdot \lambda_{DU} \cdot T_I / 2$.

- $(1 - PDC) \cdot \lambda_{DU}$ – часть необнаруженных отказов, которые диагностика **не может найти**.

Эти отказы остаются в системе до следующей плановой проверки (T_I).

- Множитель $T_I / 2$ – стандартное усреднение за период плановой проверки.

Второй компонент: Отказы, обнаруживаемые диагностикой. $PDC \cdot \lambda_{DU} \cdot (T_D / 2 + MR)$,

где

$PDC \cdot \lambda_{DU}$ – часть необнаруженных отказов, которые диагностика **может обнаружить**;

$T_D / 2$ – среднее время существования отказа до его обнаружения (предполагается равномерное распределение);

MR – среднее время восстановления после обнаружения отказа.

Практический пример.

Данные системы:

- Логический решатель: $\lambda_{DU} = 0.00001$ 1/час.
- Интервал плановых проверок: $T_I = 8760$ часов (1 год).

- Интервал самодиагностики: $T_D = 8$ часов.
- Время восстановления: $MR = 2$ часа.
- Покрытие диагностикой: $PDC = 0.95$ (95%).

Расчет PFD_{avg} :

1. Отказы, не обнаруживаемые диагностикой:

$$(1 - 0.95) \cdot 0.00001 \cdot 8760 / 2 = 0.05 \cdot 0.00001 \cdot 4380 = 0.00219.$$

2. Отказы, обнаруживаемые диагностикой:

$$0.95 \cdot 0.00001 \cdot (8/2 + 2) = 0.95 \cdot 0.00001 \cdot 6 = 0.000057.$$

3. Суммарный PFD_{avg} :

$$0.00219 + 0.000057 = 0.002247.$$

Результат: $PFD \approx 2.25 \times 10^{-3}$, что соответствует **SIL 2**.

Сравнение с подходом без учета PDC.

Если бы мы использовали классическую формулу без диагностики:
 $PFD_{avg} \approx \lambda_{DU} \cdot T_I / 2 = 0.00001 \cdot 4380 = 0.0438 \rightarrow$ соответствует **SIL 1**.

Вывод: Эффективная периодическая диагностика с высоким PDC позволила повысить уровень безопасности с SIL 1 до SIL 2.

Когда особенно важно использовать эту формулу?

1. Для систем с автоматической самодиагностикой.
2. При проектировании архитектур с высокими требованиями к SIL.
3. Когда необходимо оптимизировать интервалы технического обслуживания
4. Для точного расчета вклада диагностических подсистем

Эта методика позволяет более точно оценивать реальные показатели безопасности и обосновывать технические решения при проектировании СПАЗ/SIS

Кейс 10.9. Диагностика клапана/задвижки в системе ПАЗ.

Ситуация. На нефтеперерабатывающем заводе аварийный отсечной клапан (ESD.-клапан) не сработал при утечке. Расследование показало:

- Клапан не двигался из-за заклинивания штока.
- Обратная связь (концевой выключатель) показывала «открыто», хотя команда на закрытие была подана.
- Последняя проверка (год назад) не выявила проблем.

Вопрос. Какие методы диагностики могли бы предотвратить аварию (табл. 10.4)?

Таблица 10.4 Методы диагностики клапанов (сравнение).

Метод	Решение	Преимущества	Недостатки	Когда применять
Контрольная проверка (полное сравнение)	Ручное/автоматическое открытие/закрытие	Проверяет работоспособность	Останавливает процесс, требует байпаса	Плановые ТО (раз в 1–2 года)

Сигнализация несоответствия	Сравнение команды и обратной связи (концевик)	Быстрое обнаружение отказа	Не выявляет частичные заклинивания	Постоянный мониторинг
Проверка с обратной связью по положению	Запись графика движения (время, скорость)	Выявляет износ, засоры	Требуется датчик положения	Автоматические тесты (раз в месяц)
Частичное закрытие (25%)	Автоматическое прикрытие на 25% без остановки процесса	Минимальное влияние на процесс	Менее точная проверка	Частые тесты (раз в неделю/месяц)
Интеллектуальный позиционер	Автоматическая диагностика (трение, время срабатывания)	Самодиагностика, прогноз износа	Высокая стоимость	Современные системы ПАЗ

1. Разбор кейса.

Что пошло не так?

- Контрольная проверка раз в год → недостаточно для критичного клапана.

- Нет датчика положения → только концевик, который не видит частичные заклинивания.

- Нет автоматических тестов → износ не обнаружен вовремя.

Как исправить?

1. Внедрить частичное закрытие (25%)

- Логика ПЛК подает импульс на закрытие, затем отменяет команду.

- Датчик положения фиксирует.

- Время срабатывания (замедление = износ).

- Достиг ли клапан 25% (если нет – заклинивание).

2. Установить интеллектуальный позиционер, который:

- Автоматически строит графики «давление-положение-время».

- Сравнивает с эталоном и сигнализирует об отклонениях.

3. Увеличить частоту проверок. Выполнять:

- Полный тест с байпасом – раз в год.

- Частичный тест – раз в месяц.

- Мониторинг трения в позиционере – онлайн.

Рекомендации.

1. Анализируйте логику СПАЗ/SIS – это ключевой источник информации.

2. Проверяйте полевое оборудование (датчики, клапаны, кабели).

3. Учитывайте среду эксплуатации (температура, влажность, вибрации).

4. Тестируйте систему после изменений (моделирование аварийных ситуаций).

Пример расчёта PDC.

Условие.

• Компонент имеет интенсивность отказов $\lambda_{\text{Demand}} = 500 \text{ FIT} = 500 \times 10^{-9} \text{ 1/час}$.

• Встроенная диагностика проверяет его состояние каждые 200 мс.

Рассчитать PDC.

Решение.

1. **Находим λ_{Diag} .**

- Период диагностики. $T_{\text{Diag}} = 200 \text{ мс} = 0.2 \text{ с}$.
- Переведём в часы. $T_{\text{Diag}} = 0.2 \text{ с} / 3600 \text{ с/час} \approx 5.556 \times 10^{-5} \text{ часа}$.
- Частота диагностики. $\lambda_{\text{Diag}} = 1 / T_{\text{Diag}} = 1 / (5.556 \times 10^{-5}) \approx 18 \text{ 000 1/час}$.

2. **Подставляем в формулу.**

$$\text{PDC} = (\lambda_{\text{Diag}} / \lambda_{\text{Demand}}) \times (1 - \exp(-\lambda_{\text{Demand}} / \lambda_{\text{Diag}})).$$

Здесь.

• $\lambda_{\text{Diag}} / \lambda_{\text{Demand}} = 18 \text{ 000} / (500 \times 10^{-9}) = 3.6 \times 10^{13}$ (Это огромное число – «идеальный кредит» очень высок).

• $\lambda_{\text{Demand}} / \lambda_{\text{Diag}} = (500 \times 10^{-9}) / 18 \text{ 000} \approx 2.778 \times 10^{-14}$ (Это очень маленькое число).

• $\exp(-\lambda_{\text{Demand}} / \lambda_{\text{Diag}}) \approx \exp(-2.778 \times 10^{-14}) \approx 1$ (Т.к. e в степени, близкой к нулю, равна почти 1).

• $(1 - \exp(...)) \approx (1 - 1) = 0$.

Получаем результат.

$$\text{PDC} \approx (3.6 \times 10^{13}) \times 0 = 0.$$

Вывод и объяснение.

Расчёт показывает $\text{PDC} \approx 0$. Это не значит, что диагностика плохая. Это значит, что она бесполезна для этого конкретного компонента.

Почему?

Потому что компонент чрезвычайно надёжен (маленькая λ_{Demand}). Он ломается в среднем раз в 228 лет $1 / (500 \times 10^{-9}) \approx 228$ лет). Диагностика, которая проверяет его каждые 200 мс, просто не успевает ничего обнаружить, потому что обнаруживать нечего. Она срабатывает вхолостую миллионы раз за время жизни системы.

PDC помогает оценить, насколько целесообразна сложная и частая диагностика для данного компонента. Она не всегда нужна и полезна. Эту меру важно использовать для оптимизации архитектуры системы безопасности.

10.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 10.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 10.1. Общие вопросы по диагностике СПАЗ.

Вопрос 1. Какой метод НЕ является диагностическим?

- а) Контрольная проверка (полное срабатывание).
- б) Сигнализация несоответствия по концевику.
- в) Частичное закрытие с датчиком положения.
- г) Запись графика скорости срабатывания.

Ответ а. Это контрольная проверка, а не диагностика.

Вопрос 2. Почему интеллектуальный позиционер лучше концевого выключателя?

- а) Показывает только «открыто/закрыто».
- б) Фиксирует положение, время, трение и сравнивает с нормой.
- в) Не требует подключения к ПЛК.
- г) Дешевле.

Ответ б.

Вопрос 3. Как частичное закрытие улучшает PFD (Probability of Failure on Demand)?

- а) Увеличивает интервалы между проверками.
- б) Позволяет чаще выявлять деградацию клапана.
- в) Полностью заменяет полные проверки.
- г) Требуется остановки процесса.

Ответ б. Чем чаще тесты, тем ниже PFD.

Диагностика это не контрольная проверка. Нужны оба метода, но с разной частотой.

Минимум для клапана ПАЗ.

- Концевой выключатель (сигнализация несоответствия).
- Датчик положения (график срабатывания).
- Регулярные частичные тесты (25%).

Идеальный вариант. интеллектуальный позиционер плюс интеграция с ПЛК.

Объяснения.

Контрольная проверка системы безопасности с инструментальным обеспечением – это процесс, направленный на оценку корректности работы компонентов SIS (датчиков, логических решателей, конечных элементов). Цель – убедиться, что система выполняет инструментальную функцию безопасности (SIF) – предотвращает небезопасные технологические операции при возникновении опасных условий.

С помощью диагностики пытаются доказать или убедиться, что клапан работает нормально. Это не просто вопрос констатации, что

клапан двигается, поскольку признаки опасности могут появиться и при движущемся клапане. Необходимо проверить свободу перемещения, правильность сброса соленоида, нормальность времени реакции и отсутствие каких-либо тенденций к застреванию или «подвисанию».

Однако если можно полностью открыть (или закрыть) клапан, не останавливая процесс, например, путем использования параллельных каналов или байпасов, то проверки можно будет проводить через регулярные интервалы, улучшая, тем самым, показатель PFD клапана. Вот основные методы диагностики клапанов.

1. Сигнализация несоответствия. Используется сигнал обратной связи от конечного выключателя; логическое решающее устройство генерирует сигнал, если положение клапана не соответствует поданной команде.

2. Проверка срабатывания с обратной связью по положению. Сигнал по положению клапана позволит испытателю визуально оценить скорость реакции на тест и, таким образом, правильность перемещения. Если используется логическое устройство, то можно проверить и даже записать профиль (график) реакции и найти отклонения от стандартной версии.

3. Проверка путем частичного закрытия. то же, что и проверка срабатывания. Отличие состоит лишь в том, что срабатывание клапана инициируется автоматически логическим решающим устройством. Затем, когда перекрытие клапана составит примерно 25%, сигнал срабатывания снимается. Устройство обратной связи по положению может быть таким же простым, что и концевой выключатель, но датчик положения является предпочтительным. Возмущение на процесс при этом минимально

4. Применение для проверок интеллектуального позиционера клапана. Интеллектуальное устройство позволяет проводить проверки путем частичного закрытия автоматически от соленоидного позиционера системы управления, независимо от решающего устройства. Это позволяет также зафиксировать связь между давлением соленоида и временем реакции и проверять различия за время между проверками.

Тест 10.2.

Датчик давления использует внутреннюю автоматическую диагностику, которая обнаруживает большинство внутренних сбоев.

Этот датчик имеет режимы отказа и частота его отказов приведена в таблице 10.5. Он используется в нерезервированной схеме (1oo1) в SIF и предназначен для остановки процесса, когда давление превышает 80 % от давления в шкале (16 мА).

Этот датчик подключен к ПЛК безопасности, который запрограммирован на обнаружение выхода текущего сигнала за пределы

диапазона ($< 3,6$ мА) и выхода за пределы диапазона (> 21 мА), сигнал об этом отправляется в ремонтный центр.

«Дрейф» – это уход показаний прибора от истинного значения со временем. «Вверх» и «вниз» – уточняют направление дрейфа. Если это «не обнаружено», то возможны печальные последствия.

«Отказ диагностики» означает, что сама функция диагностики прибора или модуля, отвечающего за диагностику, вышла из строя.

Таблица 10.5. Данные по функциональным отказам датчика давления

Вид отказа датчика давления	Интенсивность отказов	Единицы измерения
Отказ. выходной сигнал превышен (> 21 мА)	0.000745	Отказов в год
Отказ. выходной сигнал занижен (< 3.6 мА)	0.002540	Отказов в год
Отказ. выходной сигнал завис, не обнаружен	0.000464	Отказов в год
Отказ. дрейф выходного сигнала вверх, не обнаружен	0.000096	Отказов в год
Отказ. дрейф выходного сигнала вниз, не обнаружен	0.000096	Отказов в год
Отказ, обнаруженный диагностикой	0.004380	Отказов в год
Отказ диагностики	0.000342	Отказов в год

Приведенные в таблице 10.6 данные означают, как различные функциональные отказы датчика (из предыдущей таблицы) классифицируются с точки зрения их влияния на функцию безопасности SIF.

То есть, ведет ли отказ датчика к безопасному или опасному состоянию контура защиты, и обнаруживается ли он диагностикой. Это не просто вид отказа прибора, а каким образом этот отказ влияет на способность SIF выполнять свою функцию.

Таблица 10.6 Данные о режимах отказов датчика давления для анализа SIF

Вид отказа датчика давления (для SIF)	Интенсивность отказов Отказов в год	Интенсивность отказов Отказов в час	FITS
Безопасный отказ, обнаруженный	0.000000	0.000000000	0
Безопасный отказ, не обнаруженный	0.000096	0.000000011	11
Опасный отказ, обнаруженный	0.000561	0.000000064	64
Опасный отказ, не обнаруженный	0.007665	0.000000875	875

Отказ сигнализации, не обнаруженный	0.000342	0.000000039	39

Отказ сигнализации, не обнаруженный – это специфический вид отказа, когда система оповещения (например, сигнализация или индикация) не срабатывает или дает ложную информацию, и это не обнаруживается. В зависимости от контекста и дизайна SIF такой отказ может быть классифицирован как безопасный или опасный, но в таблице он выделен отдельно, так как относится к функции информирования оператора.

В программируемом логическом контроллере (ПЛК) предусмотрена задержка срабатывания на аналоговом входе, чтобы предотвратить ложные срабатывания при переходе тока от рабочего значения к состоянию отказа.

Датчик давления запрограммирован на подачу низкого выходного сигнала при обнаружении отказа, чтобы избежать ложного (паразитного) срабатывания процесса.

Используя приведенные выше определения режимов отказа, как можно определить интенсивности отказов?

Анализ отказов датчика давления.

Вопрос 1. Какой максимальный выходной сигнал у датчика давления считается опасным?

- A) <3.6 мА.
- B) 16 мА.
- C) > 21 мА.
- D) 80% от шкалы.

Ответ C. > 21 мА.

Сигнал выше 21 мА считается опасным, так как это состояние может указывать на сбой датчика, что требует остановки процесса для предотвращения аварийной ситуации. Однако режим «< 3.6 мА» имеет наибольшую частоту отказов (0.002540) среди перечисленных, что делает его наиболее критичным для системы.

Вопрос 2. Какой режим отказа датчика давления считается «опасным, но обнаруженным»?

- A) Safe Undetected.
- B) Dangerous Detected.
- C) Dangerous Undetected.
- D) Safe Detected.

Ответ A. Dangerous Undetected.

Отказ «Dangerous Undetected» имеет наибольшую частоту (0.007665) среди всех перечисленных режимов, что делает его наиболее критичным для системы.

Вопрос 3. Какова частота отказов для режима «Dangerous Undetected»?

- A) 0.000096 отказов в год.

- В) 0.007665 отказов в год.
- С) 0.000561 отказов в год.
- Д) 0.000000 отказов в год.
- В) 0.000561 отказов в год.

Ответ В. Частота отказов для режима «Dangerous Undetected» составляет 0.007665 отказов в год, что указывает на риск, если сбой не будет обнаружен.

Вопрос 4. Какую роль играет задержка срабатывания в программируемом логическом контроллере (ПЛК)?

- А) Увеличивает скорость реакции системы.
- В) Предотвращает ложные срабатывания при переходе тока.
- С) Увеличивает частоту отказов.
- Д) Уменьшает время диагностики.

Ответ В. Предотвращает ложные срабатывания при переходе тока

Задержка срабатывания в ПЛК предназначена для предотвращения ложных срабатываний при переходе сигнала от нормального состояния к состоянию отказа, что важно для обеспечения надежности системы.

Ответ Режим «Dangerous Detected» означает, что сбой был обнаружен, и система может реагировать на него, что делает его «опасным, но обнаруженным».

Вопрос 5. Какова общая интенсивность отказов SIF, если ПЛК не распознает выход тока с завышением допустимого диапазона как указание неисправности?

- А) 0.000841 отказов в год.
- В) 0.000745 отказов в год.
- С) 0.000000 отказов в год.
- Д) 0.000096 отказов в год.

Ответ В. 0.00745 отказов в год.

Частота отказов для режима «Dangerous Undetected» в приложении без обнаружения отказов ПЛК составляет 0.00745 отказов в год. Это важно, так как этот режим представляет собой серьезный риск для системы

Вопрос 6. Какова роль автоматической диагностики в датчике давления?

- А) Увеличивает частоту отказов.
- В) Обнаруживает большинство внутренних сбоев.
- С) Уменьшает время ремонта.
- Д) Увеличивает скорость реакции системы.

Ответ В. Обнаруживает большинство внутренних сбоев.

Автоматическая диагностика в датчике давления предназначена для обнаружения большинства внутренних сбоев, что помогает улучшить надежность системы и предотвращает потенциальные аварии.

Объяснение.

В этом тесте анализируются частоты отказов различных режимов и необходимо понимать, как они влияют на безопасность системы.

Определение режимов отказа. Необходимо уметь различать безопасные и опасные режимы, а также понимать, какие из них могут быть обнаружены системой.

Частота отказов. Знание частоты отказов помогает оценить надежность системы и необходимость в дополнительных мерах безопасности.

Понимание функций автоматической диагностики критично для создания безопасных систем, так как она позволяет обнаруживать сбои до того, как они приведут к аварии.

Если в архитектуре 1oo1 датчик в приложении с высоким уровнем срабатывания выходит из строя с выходным сигналом, превышающим допустимый диапазон (> 21 мА), то произойдет ложное срабатывание системы функциональной безопасности (СПАЗ), поскольку выходной сигнал датчика пройдет через точку срабатывания, а ПЛК не запрограммирован интерпретировать это как отказ датчика. В этой ситуации режим отказа классифицируется как SU (безопасный необнаруженный отказ).

Некоторые обучаемые могут подумать. «Почему необнаруженный?» Если датчик вызывает срабатывание процесса, он обнаруживается! Объясняется это тем, что определение «необнаруженный» относится только к автоматической диагностике в рамках СПАЗ, а не к распознаванию операционным персоналом. Это делается для того, чтобы правильно использовать частоты отказов в модели любой избыточной архитектуры, включая те, в которых безопасный отказ одного датчика не вызывает остановки установки.

Если датчик выходит из строя с выходным сигналом, находящимся за пределами нижнего допустимого диапазона ($< 3,6$ мА), выходной сигнал датчика будет отклоняться от точки срабатывания. Впоследствии датчик не способен реагировать на запрос до тех пор, пока не будет выполнен ремонт. Этот режим отказа классифицируется как DU (опасный необнаруженный отказ).

Если датчик выходит из строя с замороженным выходным сигналом, то датчик не способен реагировать на запрос. Ток, вероятно, будет в рабочем диапазоне, но режим отказа классифицируется как DU.

Если датчик выходит из строя с дрейфом выходного сигнала вверх, он неточно сигнализирует об измеряемом значении процесса, но ток, вероятно, находится в активном диапазоне 4–20 мА. Поскольку ток дрейфует к точке срабатывания, этот отказ может вызвать ложное срабатывание. Этот режим отказа классифицируется как SU.

При отказе датчика с дрейфом выходного сигнала вниз он неточно передает измеренное значение процесса, отклоняясь от точки срабатывания. Ток, вероятно, находится в рабочем диапазоне 4–20

мА. Этот режим отказа классифицируется как DU (опасный необнаруженный отказ).

Внутренние отказы, обнаруживаемые автоматической диагностикой внутри датчика, устанавливают уровень тока на predetermined значение, указанное в конфигурации датчика. В данном случае, согласно условию задачи, уровень тока станет низким ($< 3,6$ мА). Датчик не способен реагировать на запрос до тех пор, пока не будет выполнен ремонт; таким образом, отказ должен быть классифицирован как DU.

При отказе датчика с дрейфом выходного сигнала вверх он не точно сигнализирует об измеряемом значении процесса, однако ток, вероятно, находится в активном диапазоне 4–20 мА. Поскольку ток дрейфует к точке срабатывания, этот отказ может вызвать ложное срабатывание. Если эта ситуация не обнаружена никакой внутренней автоматической диагностикой датчика, то она классифицируется как SU (безопасный необнаруженный отказ).

При отказе датчика с дрейфом выходного сигнала вниз он не точно сигнализирует об измеряемом значении процесса, и он отклоняется от точки срабатывания. Ток, вероятно, находится в активном диапазоне 4–20 мА. Если эта ситуация не обнаружена никакой внутренней автоматической диагностикой датчика, она классифицируется как DU (опасный необнаруженный отказ).

Внутренние отказы, которые обнаруживаются автоматической диагностикой в датчике, приведут к установке уровня тока на predetermined значение, указанное в датчике. В этом случае условие задачи указывает, что уровень тока будет низким ($< 3,6$ мА). Пока уровень тока выходит за пределы диапазона, фактический уровень не имеет значения, поскольку ПЛК безопасности обнаружит высокое или низкое значение и отправит сообщение об отказе ремонтной бригаде. Однако, поскольку датчик не способен реагировать на запрос в течение этого времени, отказ должен быть классифицирован как DD (опасный обнаруженный отказ).

Поскольку отказы в датчике, которые приводят к потере диагностики, не влияют на функциональную безопасность, эти отказы не могут быть классифицированы как безопасные или опасные. Хотя влияние этих отказов на целостность безопасности, вероятно, невелико, эти отказы могут быть смоделированы для повышения точности. Эти отказы будут идентифицированы как необнаруженные сигналы.

Интенсивность отказов для этого приложения определяется путем сложения интенсивности отказов для каждого режима в Таблице 10-1 и относятся к соответствующей категории. Например, DD категория включает в себя.

- Высокий выходной сигнал ошибки -0,000745 отказов в год.
- Низкий выходной сигнал ошибки -0,002540 отказов в год.
- Обнаружен сбой -0,004360 отказов в год.

Всего- 0,007665 отказов в год.

Тест 10.3. Методы диагностики клапанов в системах предотвращения аварий (СПАЗ).

Вопрос 1. Какие методы диагностики клапанов применяются в системах предотвращения аварий (СПАЗ)? Укажите все верные утверждения.

а) Проверка срабатывания клапана в рабочем состоянии проводится путем полного открытия или закрытия клапана, если это возможно без остановки процесса, используя параллельные каналы или байпасы.

б) Сигнализация несоответствия использует сигнал обратной связи от конечного выключателя для генерации сигнала, если положение клапана не соответствует поданной команде.

с) Проверка срабатывания с обратной связью по положению позволяет визуализировать скорость реакции клапана на тест и оценить правильность его перемещения.

д) Проверка путем частичного закрытия аналогична проверке срабатывания, но отличается тем, что срабатывание клапана инициируется автоматически логическим решающим устройством.

е) Интеллектуальные позиционеры клапанов позволяют проводить автоматические проверки, фиксировать связь между давлением соленоида и временем реакции, а также проверять изменения параметров между проверками.

ф) Диагностика клапанов заключается только в оценке движения клапана, без учета свободы перемещения, правильности сброса соленоида и отсутствия тенденций к застреванию.

г) Все перечисленные методы применимы ко всем типам клапанов и систем предотвращения аварий без исключений.

Ответ. Правильно:

а) Проверка срабатывания клапана в рабочем состоянии действительно возможна, если клапан можно полностью открыть или закрыть без остановки процесса, например, с использованием параллельных каналов или байпасов. Это позволяет проводить проверки через регулярные интервалы, улучшая показатель частоты ложных отказов (PFD) клапана.

б) Сигнализация несоответствия действительно использует сигнал обратной связи от конечного выключателя для генерации сигнала тревоги, если положение клапана не совпадает с поданной командой. Этот метод помогает оперативно выявлять расхождения между фактическим положением клапана и требуемым состоянием.

с) При проверке срабатывания с обратной связью по положению оператор получает информацию о скорости реакции клапана на ко-

манду, что позволяет визуально оценить корректность его перемещения. Логическое устройство ПЭС может дополнительно регистрировать график реакции клапана, помогая находить отклонения от нормы.

d) Проверка путем частичного закрытия действительно схожа с обычной проверкой срабатывания, но в данном случае срабатывание клапана инициируется автоматически логическим решающим устройством. После достижения определенного уровня перекрытия (обычно около 25%) команда на закрытие снимается, позволяя минимизировать возмущение процесса.

e) Интеллектуальные позиционеры клапанов действительно позволяют проводить автоматические проверки, отслеживать взаимосвязь между давлением соленоида и временем реакции, а также контролировать изменения параметров между проверками. Это значительно облегчает процесс диагностики и повышает её точность.

Неверно:

f) Диагностика клапанов не ограничивается только оценкой движения клапана. Она должна включать проверку свободы перемещения, правильности сброса соленоида, времени реакции и наличия тенденций к застреванию или «подвисанию». Это необходимо для полной уверенности в исправности клапана.

g) Перечисленные методы диагностики не универсальны и не применимы ко всем типам клапанов и систем предотвращения аварий без исключений. Выбор метода зависит от конкретных особенностей системы и требований безопасности.

Подробное объяснение каждого пункта.

Ответ а. Полное открытие или закрытие клапана в процессе эксплуатации, если это возможно без остановки производства, позволяет провести диагностику в реальных условиях работы. Использование параллельных каналов или байпасов помогает избежать нарушений технологического процесса и улучшить показатели надёжности клапана.

Ответ б. Сигнализация несоответствия основана на использовании сигналов обратной связи от конечных выключателей. Если реальное положение клапана не соответствует командам управления, система генерирует предупреждающий сигнал. Это помогает быстро обнаружить любые расхождения и предотвратить возможные аварии.

Ответ с. Обратная связь по положению клапана даёт возможность визуально оценивать скорость его реакции на команды и определять, правильно ли происходит движение. Если используется логическое устройство ПЭС, можно зарегистрировать профиль реакции клапана и сравнить его с эталонным, что поможет выявить отклонения.

Ответ d. Частичное закрытие клапана имитирует реальную ситуацию срабатывания, но с меньшим воздействием на технологический процесс. После достижения определённого уровня перекрытия (около

25%) команда на закрытие снимается, что сводит к минимуму возмущение процесса. Это удобный метод для автоматической диагностики.

Ответ е. Интеллектуальные позиционеры клапанов позволяют автоматизировать процесс диагностики, отслеживая давление соленоида, время реакции и изменения параметров между проверками. Это повышает точность диагностики и снижает нагрузку на операторов.

Ответ f. Диагностика клапанов включает не только оценку движения клапана, но и проверку множества других факторов, таких как свобода перемещения, правильность сброса соленоида, время реакции и наличие тенденций к застреванию. Игнорирование этих аспектов может привести к недооценке потенциальных угроз.

Ответ г. Универсального подхода к диагностике клапанов нет. Выбор метода зависит от типа клапана, специфики системы предотвращения аварий и требований безопасности. Нельзя утверждать, что все перечисленные методы подходят для любых ситуаций.

10.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 10».

Тест 10.4. Диагностика в системах предотвращения аварий (СПАЗ).

Вопрос. Что включает в себя диагностика в системах предотвращения аварий (СПАЗ)? Укажите все верные утверждения.

а) Диагностика предполагает проведение регулярных проверок состояния устройств, таких как программируемые электронные системы (ПЭС) и датчики.

б) Высокий уровень охвата диагностикой преобразует потенциально опасные условия отказа в безопасные благодаря своевременному аварийному сигналу или останову.

с) Диагностику датчиков и клапанов можно проводить в форме самотестирования, которое дополняет функциональные или контрольные проверки, выполняемые в рамках регулярного технического обслуживания.

д) До внедрения микропроцессорных технологий было невозможно эффективно осуществлять диагностику датчиков и исполнительных устройств.

е) Современные программные системы позволяют реализовать усовершенствованные методы самодиагностики.

ф) Контрольные проверки считаются частью диагностики, потому что они регулярно проводятся в рамках планового технического обслуживания.

g) Новые подходы включают сравнение значения сигнала срабатывания с другими связанными переменными, хотя этот метод используется редко.

h) Рекомендуются использовать датчики с сертификатом безопасности и интеллектуальные датчики с функцией диагностической сигнализации.

i) Резервированные датчики полезны для сравнения показаний и выявления отклонений.

j) Контрольные проверки не являются диагностическими, так как их проводят редко.

Тест 10.5. Определение SFF и SIL для одноканальной конструкции.

Химическая компания требует, чтобы использовался МЭК 61508 Route 1Н для определения архитектурных ограничений ИУ в сборке.

Каков SFF, учитывая частоту отказов в примере 12-3? Что представляет собой SIL для одноканальной (1oo1) конструкции?

Вопрос 1. Какова интенсивность безопасных отказов (λ_S) для системы, если известны следующие данные. $\lambda_S = 450$ FITS, $\lambda_D = 240$ FITS, и данные о частоте безопасных отказов для трехходового прямодействующего тарельчатого электромагнитного клапана отсутствуют?

- A) 240 FITS.
- B) 450 FITS.
- C) 1250 FITS.
- D) Неопределенно.

Вопрос 2. Какова общая интенсивность безопасных отказов ($\lambda_{S_{total}}$) для системы, если известны интенсивности безопасных отказов для всех элементов. 450 FITS, 800 FITS и 0 FITS?

- A) 800 FITS.
- B) 1250 FITS.
- C) 450 FITS.
- D) 1590 FITS.

Вопрос 3. Какова интенсивность опасных необнаруженных отказов (λ_{DU}) для системы, если известны интенсивности опасных необнаруженных отказов для всех элементов. 240 FITS, 650 FITS и 700 FITS?

- A) 240 FITS.
- B) 650 FITS.
- C) 1590 FITS.
- D) 700 FITS.

Вопрос 4. Как вычисляется SFF (Safe Failure Fraction)?

- A) $\lambda_S / (\lambda_S + \lambda_D)$.
- B) $\lambda_S / (\lambda_S + \lambda_{DU})$.
- C) $\lambda_{S_{total}} / (\lambda_{S_{total}} + \lambda_{DU_{всего}})$.
- D) $\lambda_D / (\lambda_D + \lambda_{DU})$.

Вопрос 5. Какой уровень безопасности (SIL) соответствует конструкции с HFT = 0?

- A) SIL 1.
- B) SIL 2.
- C) SIL 3.
- D) SIL 4.

Тест 10.6. Расчет диагностического покрытия (DC) по методу Route 2H (МЭК 61508).

Вопрос 1. Какой компонент СПАЗ обычно имеет наивысший DC?

- а) Датчик.
- б) ПЛК.
- в) Исполнительное устройство.

Вопрос 2. Что из перечисленного НЕ учитывается при расчете DC по Route 2H?

- а) Безопасные отказы.
- б) Опасные отказы.
- в) Время восстановления.

Вопрос 3. Если для клапана DC = 75%, а общая вероятность опасного отказа (λD) = 0.001 1/час, какова вероятность необнаруженного опасного отказа?

- а) 0.00025 1/час.
- б) 0.00075 1/час.
- в) 0.001 1/час.

10.7. Практическое задание.

Задача. Рассчитайте DC для резервированного датчика температуры (2oo3), если.

- Опасные отказы. завышение показаний, занижение показаний, обрыв цепи.
- Диагностика. контроль диапазона (4–20 мА), сравнение показаний трех датчиков.

Формула для запоминания.

$$DC = 100\% \lambda_{DD} / \lambda_D.$$

где

- λ_{DD} – интенсивность обнаруженных опасных отказов,
- λ_D – общая интенсивность опасных отказов.

11. ПРОЕКТИРОВАНИЕ, СТРУКТУРА, КОМПОНЕНТЫ СПАЗ.

11.1. КЛЮЧЕВЫЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СПАЗ ОТ HAZID ДО ВЕРИФИКАЦИИ.

Задание 11.1. Уяснить ключевые принципы проектирования СПАЗ от HAZID до верификации систем приборной безопасности.

СПАЗ – это «последний рубеж» безопасности на опасных производственных объектах. Её задача – предотвратить катастрофу, когда другие системы контроля уже не справляются [14-16, 26].

Проектирование СПАЗ – это не просто подбор оборудования, а строгий инженерный процесс, основанный на анализе рисков и верификации решений.

1. HAZID. Понимание опасностей.

HAZID – это первый шаг разработки проекта: оценка опасностей ОПО. Что может пойти не так на объекте? Как это работает? Для этого устанавливается:

- Список всех возможных аварийных сценариев ОПО.
- Первичные требования к СПАЗ (например, нужен аварийный клапан + датчик давления).
- Первичный потребный для защиты ОПО уровень SIL (например, назначаемый нормативным документом).

2. Спецификация – это не просто документ, а концептуальная основа, которая определяет, сможет ли система стать надежным защитником или останется лишь формальным артефактом.

Спецификация требований к системе безопасности – это не свод догм, а инструкция по созданию реальной защиты. Ее сила – не в объеме или формальном соответствии стандартам, а в способности трансформироваться в инженерные решения, которые предупреждают, выдерживают и нейтрализуют угрозы.

Как превратить требования в живую, работающую систему?

При разработке спецификации СПАЗ используют различную последовательность этапов проектирования HAZID- HAZOP/ FAT/ LOPA/FMEA- SIL.

2.1 На основе HAZID формируется структура и функции безопасности (SIF), потребные для ОПО. Например. **«При давлении выше 50 бар – закрыть клапан за 2 секунды.»**, **«При температуре 100° С в реакторе включить клапан охлаждения»**.

Процесс, ОПО разбирается по компонентам (узлы, трубопроводы, реакторы).

Ищутся отклонения (например, «высокое давление», «обратный поток»).

Оцениваются последствия и риски.

В случае взрывоопасности в соответствии с ФНиП «Общие правила взрывобезопасности для взрывопожароопасных химических,

нефтехимических и нефтеперерабатывающих производств» утв. приказом Ростехнадзора от 15.12.2020 г. № 533, п. 233, 248 выполняется:

- Идентификация опасного события. Определяется сценарий (разгерметизация, переполнение емкости), массу выброса вещества (масса_вещества), тип взрыва (в облаке/в объеме).
- Расчет тротилового эквивалента (M_{TNT}).
- Оценка последствий. Например, рассчитывается избыточное давление в контрольных точках (места нахождения персонала, критическое оборудование) и оцениваются потенциальные разрушения.

2.2. HAZOP/FMEA. На этом этапе выполняется детальный анализ отказов СПАЗ/SIS. HAZOP/FMEA помогают устранить слабые места СПАЗ/SIS до внедрения системы.

Проверяется *«А точно ли концептуально спроектированная СПАЗ справится?»*

Выполняется анализ дерева отказов СПАЗ/SIS и дерева событий. Устанавливаются необходимые слои защиты (полевая сигнализация, ESD, аварийная сигнализация АСДУ, активные и пассивные слои противоаварийной защиты).

2.3. Определяется по стандарту МЭК 61508/61511 требуемый уровень полноты безопасности (SIL).

Анализируются риски на основе отдельных слоев защиты (LOPA). На основе частоты инициирующего события и тяжести последствий определяется, насколько необходимо снизить риск.

Устанавливаются структурные требования к оборудованию:

- Датчики (например, резервированные для SIL2).
- Логический контроллер (например, SIL3 сертифицированный ПЛК).
- Исполнительные устройства (отсечные клапаны с пневмоприводом или электроприводом).

Ошибка новичков.

Выбор дешёвого оборудования без SIL-сертификации в результате система может не сработать в критический момент.

Выполняется FMEA (ГОСТ Р 51901.12-2007) СПАЗ/SIS:

- Анализируется каждый компонент СПАЗ (датчик, ПЛК, клапан).

- Определяется:

- Как он может сломаться? (например, «залипание контактов»).
- Как это повлияет на систему? Выполняется анализ СПАЗ/SIS.

Пример. *«Если датчик давления занижает показания, то СПАЗ не сработает вовремя, то возможен взрыв».*

- Устанавливается как снизить риск? (например, резервирование).

- Оценивается PFDavg (отказобезопасность) и STR (отказоустойчивость).

Техническое задание, спецификация – это ДНК системы безопасности. Если оно четко прописано, система будет работать правильно. Если же она противоречива или неполна – даже самая продвинутая технология даст сбой. **Хорошие требования не описывают идеал – они делают его достижимым!**

3. Верификация. Проверка, что СПАЗ работает.

Это самая важная часть проекта! Даже идеальная на бумаге система может дать сбой в реальности.

Что проверяется?

А. Правильность логики (например, тестовыми сценариями).

«Если давление 55 бар → клапан закрывается за 2 сек?»

В. Надёжность аппаратуры (расчёт вероятности опасного и без-опасного отказа). соответствует ли SIL?

С. Стресс-тесты (например, имитация, сбоя питания).

Почему верификация критична?

Без неё СПАЗ может:

- Не сработать (катастрофа).
- Ложно срабатывать (остановки производства → убытки).

Пример аварии из-за отсутствия верификации. **На химическом заводе не проверили задержку сигнала → клапан сработал слишком поздно → произошел выброс токсичных веществ.**

Методы верификации:

- Расчетные с построением графиков зависимостей (такие графики очень важная часть верификации).
- Моделирование (например, в Exida SILver).
- Аппаратные испытания (тестовые аварийные ситуации).
- Аудит независимыми экспертами.

Как определить, что система действительно безопасна? Где граница между достаточным и избыточным? Эти вопросы требуют не только глубокого понимания нормативных документов, но и философского осмысления самой природы риска. Ведь безопасность – это не отсутствие угроз, а способность системы сохранять функциональность вопреки им.

Но как избежать разрыва между «должно быть» и «есть»? Как превратить сухие формулировки в работающие механизмы? Ключ – в трех этапах.

1. От абстракции к конкретике.

Требование вроде **«Система должна обеспечивать отказоустойчивость»** бесполезно без четких критериев, что считается отказом, какие режимы работы допустимы, как измеряется устойчивость? Хорошая спецификация заменяет общие слова на параметры, допуски и сценарии.

2. От предписания к воплощению.

Даже идеально прописанные требования мертвы без обратной связи от проектировщиков. Если нормы вступают в конфликт с физическими законами или логикой системы – значит, либо требования ошибочны, либо нужен нестандартный подход. Спецификация должна эволюционировать в диалоге с теми, кто ее реализует.

3. От документа к поведению.

Настоящая проверка проекта – не аудит, а моделирование аварий. Если при тестах система ведет себя иначе, чем задумано, проблема не в железе или ПО, а в изначальных требованиях. Живая спецификация учится на выявлении производственных опасностей и предотвращения несчастных случаев на предприятии) и уточняет себя.

Когда проект будет работать?

– Когда инженер, глядя на СПАЗ, видит систему, а не просто пункты для галочки.

– Когда при аварийном сценарии реакция СПАЗ/SIS предсказуема по тому, что требования учитывали именно этот случай.

– Когда аудитор и проектировщик говорят на одном языке – языке конкретных рисков, а не на языке расплывчатых формулировок.

11.2. ПРАКТИКУМ ПРОЕКТИРОВАНИЯ СПАЗ.

Задание 11.2. В предположении наличия исходных требований ОПО к СПАЗ подготовить отчет по верификации и отчет по валидации решения в кейсе.

Кейс 11.1. Взрыв на нефтеперерабатывающем заводе (Техас, 2005)

Ошибки проектирования. Причины:

1. Недостаточный HAZOP. Не выявлен риск переполнения резервуара из-за отказа единственного уровнемера.

2. Низкий уровень SIL. Система имела архитектуру SIL1 (один датчик) вместо необходимого SIL2 (отсутствовало резервирование).

3. Отсутствие анализа общих отказов компонентов СПАЗ. Датчик и его дубликат могли отказать одновременно из-за коррозии.

Последствия.

Переполнение резервуара → облако паров → взрыв → 15 погибших, разрушение 80% завода.

Решения.

Для критичных процессов обязательно резервирование (например, 2oo3 архитектура).

HAZOP должен учитывать маловероятные, но катастрофические сценарии.

ПРИМЕР.

ОТЧЕТ ПО ВЕРИФИКАЦИИ КЕЙСА 11.1.

(Соответствует ли проект стандартам?)

Объект верификации: Проектные решения по предотвращению аварии, аналогичной Техасской (2005).

1. Верификация архитектурных решений.

Требование: Для функций безопасности с целевым SIL 2 необходимо обеспечить $HFT \geq 1$ (МЭК 61511-1, таблица 6).

Проверка варианта решения "2oo3 архитектура":

$HFT = 1$ (система работоспособна при отказе 1 из 3 датчиков).

Вывод: Соответствует.

$PFD_{avg} 2oo3 \approx 3 \times (\lambda DU \times TI)^2 \rightarrow \sim 10^{-3}$ (SIL 2).

Вывод: Соответствует.

Одновременный отказ нескольких датчиков: предусмотрено использование датчиков разных поставщиков.

Верифицирующий вывод: Архитектура 2oo3 удовлетворяет требованиям SIL 2 по аппаратной отказоустойчивости.

2. Верификация методов анализа рисков.

Требование: Новый HAZOP должен идентифицировать все значительные опасности отказа СПАЗ (МЭК 61511-1, раздел 8.2).

Проверка: Рассмотрены дополнительные сценарии:

SIL1: Отказ единственного датчика уровня.

Одновременный отказ нескольких одинаковых компонентов СПАЗ.

Потеря питания группы приборов.

Верифицирующий вывод: Выполненный новый анализ HAZOP соответствует требованиям полноты идентификации опасностей.

ОТЧЕТ ПО ВАЛИДАЦИИ.

(Будет ли проектное решение работать в реальных условиях? Подготовка разрешения на применение СПАЗ).

Объект валидации: Эффективность предложенных решений в реальной эксплуатации.

1. Валидация резервированной архитектуры.

Анализ в реальных условиях:

Коррозия: 3 датчика в 2oo3 архитектуре размещены в разных точках резервуара → снижение вероятности одновременного отказа.

Обслуживание: Поэтапная проверка резервированных HARD датчиков возможна без остановки процесса.

Диагностика: Предусмотрен встроенный мониторинг различий в показаниях датчиков.

Валидирующий вывод: Архитектура 2oo3 обеспечивает отказоустойчивость в реальных условиях эксплуатации.

2. Валидация HAZOP

Проверка практической реализации:

При реинжиниринге проектных решений включены дополнительные сценарии с вероятностью $< 10^{-5}$ /год, но с катастрофическими последствиями

Учтены каскадные отказы (потеря питания + отказ АСУ ТП)

Проанализированы человеческие ошибки при обслуживании

Валидирующий вывод: Выполненный новый HAZOP эффективно выявляет "неочевидные" сценарии с высоким риском.

3. Валидация защиты от общих отказов.

Предложенные меры:

Раздельные кабельные трассы для резервированных датчиков

Независимые источники питания

Датчики разных производителей (для критичных SIF)

Валидирующий вывод: Меры адекватно снижают β -фактор до 2-5%, что приемлемо для SIL 2.

ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ

Дополнительные меры для верификации:

Расчет PFDavg для всей SIF (датчики $\rightarrow$ логика $\rightarrow$ исполнительные механизмы)

Анализ временных характеристик - время отклика SIF $<$ времени развития аварии

Проверка независимости СПАЗ от базовой системы управления

Дополнительные меры для валидации:

Тестирование в реальных условиях:

Проверка срабатывания при имитации отказа датчика

Испытания при максимальной нагрузке процесса

Подготовка персонала:

Тренинги по реагированию на сигналы СПАЗ

Процедуры управления в деградированном режиме (при отказе 1 датчика в 2003)

Критерии успешного проекта:

Этап: Критерий верификации/Критерий валидации

Этап	Критерий верификации	Критерий валидации
HAZOP	Соответствие МЭК 61511	Выявление реальных сценариев на объекте
Архитектура	$HFT \geq 1$ для SIL 2	Устойчивость к коррозии, помехам
SIL	$PFD_{avg} < 0.01$	Система срабатывает в реальной аварии

Финальный вывод:

Предложенные решения проходят верификацию на соответствие стандартам и валидацию на практическую применимость. Выдается разрешение на применение нового проекта СПАЗ.

Однако следует дополнительно проработать вопросы кибербезопасности и долгосрочного поддержания SIL в течение жизненного цикла установки.

Этот отчет демонстрирует системный подход к анализу проектных решений и служит образцом для выполнения кейс практики по 11 разделу УМП.

Кейс 11.2. Ложные срабатывания на химическом заводе. Уроки проектирования.

Событие. На химическом заводе в Германии в 2012 году система аварийной защиты (SIS) ежемесячно по 12 раз без причины останавливала производство. Каждый останов приносил огромные убытки, а общие потери составили около 2 миллионов евро.

Расследование показало, что проблема была заложена на этапе проектирования.

Критические ошибки проектирования:

1. Ошибка №1. Неполный анализ рисков (HAZOP SIS только для нормального режима).

Что сделали не так. Провели анализ HAZOP только для стабильной работы установки, полностью проигнорировав переходные режимы (пуск, останов, вывод на мощность).

Почему это ошибка. Именно в нестабильных режимах параметры (давление, температура, расход) наиболее нестабильны и склонны к колебаниям. Система, настроенная только на «идеальные» условия, воспринимала эти естественные колебания как аварию.

Вывод: HAZOP SIS должен охватывать ВСЕ режимы работы процесса, особенно самые нестабильные.

2. Ошибка №2. Игнорирование помех в системе (Отсутствие фильтрации сигналов).

Что сделали не так. Спроектировали систему, которая принимала показания датчиков температуры «как есть», без какой-либо программной или аппаратной фильтрации.

Почему это ошибка. В промышленной среде всегда присутствуют электромагнитные помехи, скачки напряжения и кратковременные «выбросы» сигналов. Без фильтрации любой такой выброс система воспринимала как реальное превышение температуры.

Вывод: Сигналы от полевых устройств никогда не бывают идеально чистыми. Фильтрация – это не опция, а обязательный элемент проектирования надежной SIS.

3. Ошибка №3. Отсутствие анализа отказов на компонентном уровне (FMEA).

Что сделали не так. Не провели анализ видов и последствий отказов (FMEA) для оценки того, как отказы отдельных компонентов (датчиков, кабелей) или внешние воздействия (ЭМП) повлияют на работу всей системы.

Почему это ошибка. Проектировщики не учли, что датчики и кабели могут быть источником ложных сигналов не из-за своей неисправности, а из-за воздействия внешней среды. FMEA помог бы выявить эту уязвимость на бумаге, до монтажа.

Вывод. FMEA помогает выявить и устранить «слабые места» системы, вызванные не только внутренними отказами, но и внешними воздействиями.

Принятые решения (Как исправили):

1. Внедрение двухступенчатой фильтрации.

Аппаратная фильтрация: Установка специальных фильтров в цепях подключения датчиков для подавления высокочастотных помех.

Программная фильтрация: Настройка в логике ПЛК SIS алгоритмов усреднения сигнала и временных задержек (например, «тревога должна длиться не менее 3 секунд»), чтобы отсекал кратковременные скачки.

2. Выполнен углубленный анализ FMEA для переходных режимов работы ОПО.

Был проведен тщательный анализ всех датчиков и кабельных трасс на предмет уязвимости от внешних воздействий, что позволило выявить и защитить самые критичные точки.

В результате выполнены:

- **Всеобъемлющий HAZOP** (все режимы работы).
- **Защита от помех** (фильтрация сигналов).
- **Детальный FMEA** (предвидение отказов и внешних воздействий).

Пренебрежение любым из этих элементов на этапе проектирования неминуемо приводит к финансовым потерям и подрывает доверие к системе безопасности.

Надежность SIS определяется не только ее способностью среагировать на реальную аварию, но и ее устойчивостью к ложным срабатываниям.

Кейс 11.3. Катастрофа на установке крекинга. Почему SIL оказался «бумажным барьером».

Событие. В 2017 году на нефтеперерабатывающем заводе в Саудовской Аравии произошла авария. Когда технологические параметры вышли за критические пределы, система аварийного останова (SIS) не сработала. Последовали пожар, разрушение двух реакторов и колоссальные убытки в \$50 млн.

Расследование показало, что хотя расчетные показатели системы формально соответствовали высокому SIL, но на практике система была ненадежной. Ошибки были заложены на этапе SIL-анализа и верификации.

Критические ошибки SIL-анализа.

1. Нереалистичный расчет PFDavg. «Слепая вера в каталоги».

Суть ошибки. Для расчета средней вероятности отказа на требование (PFDavg) использовались интенсивности отказов (λ) из каталогов производителей, полученные в идеальных лабораторных условиях.

Почему это фатально. В реальности установка работала в условиях сильной запыленности, вибрации и экстремальных температур. Эти факторы ускоряют износ и многократно увеличивают интенсивность отказов.

Вывод. Реальный PFD всегда хуже лабораторного расчета. При математических расчетах должны применяться коэффициенты утяжеления лабораторных интенсивностей отказов с учетом условий эксплуатации (песок, вибрация, влажность). Это не формальность, а необходимость.

2. Игнорирование общих причин отказа. «Все яйца были в одной корзине».

Суть ошибки: Все критичные компоненты SIS (датчики, логический решатель) были запитаны от одной электрической подстанции.

Почему это фатально: Резервирование каналов (например, 1oo2) становится бесполезным, если существует общая точка отказа. Отказ подстанции привел к одновременному отказу всех «резервных» каналов системы безопасности.

Вывод. Резервирование должно быть истинно независимым. Требуется разделение не только каналов, но и их инфраструктуры. Должны быть разные источники питания, разные кабельные трассы, разные корпуса.

3. Неадекватная верификация. «Проверка в тепличных условиях».

Суть ошибки. Финальное тестирование (верификация) SIS проводилось на «холодном» стенде при комнатной температуре, без имитации реальных нагрузок и внешних воздействий.

Почему это фатально: Тест не выявил, как система поведет себя в реальных условиях: перегрев электроники при +50°C в пустыне, конденсат влаги, влияние электромагнитных помех от мощного соседнего оборудования.

Вывод. Верификация должна моделировать реальные рабочие и аварийные условия. Только так можно обнаружить скрытые дефекты, которые никогда не проявятся в «стерильной» лаборатории.

Уроки:

Этот кейс – суровое напоминание о том, что SIL – это не просто цифра в отчете, а культура проектирования.

Доверяй, но проверяй (данные): Лабораторные λ – это отправная точка. Всегда применяй коэффициенты на условия эксплуатации.

Думай о системных рисках Резервирование бессмысленно без анализа и исключения общих точек отказа (питание, окружающая среда, человеческий фактор).

Испытывай жестко верифицируй СПАЗ. Стендовые тесты должны быть максимально приближены к суровой реальности эксплуатации.

Система безопасности, спроектированная без учета этих принципов – это «замок с картонной дверью». Она может иметь все сертификаты, но в момент истины она подведет, что приведет не к убыткам, а к катастрофе.

Кейс 11.4. Утечка токсичного газа (Индия, 2018).

Конкретика ошибок проектирования и как НЕЛЬЗЯ проектировать.

А. Неверный выбор датчиков.

Нельзя брать первый попавшийся или самый дешёвый датчик из каталога, не анализируя химический состав среды, в которой он будет работать. В данном случае электрохимические сенсоры подвергались воздействию высокой влажности. Вода конденсировалась на сенсоре, растворяла электролит и либо выводила его из строя (ложный отказ), либо меняла его электрохимические характеристики (сенсорная часть датчика не смогла измерить наличие газа).

Конкретная ошибка 1.

Проектировщики не выполнили анализ технологической среды для точки отбора проб. Они не учли, что в момент запуска оборудования, после промывки или при изменении погоды возможен конденсат.

Б. Задержка срабатывания.

Нельзя игнорировать требования к функциональной безопасности (МЭК 61511) и выбирать оборудование, которое физически не может сработать достаточно быстро для данного типа опасности. Фосген – это быстродействующий отравляющий газ. Даже задержка в 3 секунды может быть критической.

Конкретная ошибка 2.

Время отклика датчика было (T_{90}) + время обработки сигнала в контроллере + время срабатывания исполнительного механизма (например, клапана), что в сумме превысило допустимое время для эффективного предотвращения последствий. Система была формально рабочей, но фактически бесполезной против утечки фосгена.

Как НУЖНО проектировать.

Выбор датчика. Для агрессивных сред, сред с высокой влажностью или возможностью конденсации применяют оптические (инфракрасные) датчики (NDIR). Принцип их действия основан на поглощении ИК-излучения газом. В них нет чувствительных электродов или жидкостей, которые могут быть повреждены влагой. Они гораздо более устойчивы к таким условиям.

Верификация времени выброса. На этапе тестирования СПАЗ необходимо не просто проверить, что датчик показывает «0» и «100», а смоделировать реальный выброс химически опасного продукта.

Для этого следует с помощью калибровочной газовой смеси подать газ в датчик и засечь время от момента подачи до момента прихода команды на исполнительный механизм на клеммах шкафа управления.

Это время должно быть задокументировано и соответствовать расчетам, сделанным на этапе проектирования.

Кейс 11.5. Отказ системы аварийного останова (Саудовская Аравия, 2017). Конкретика ошибок SIL-анализа.

Расчет PFDavg.

Нельзя слепо использовать данные о интенсивности отказов из каталога производителя. Эти данные обычно получены в идеальных «лабораторных» условиях (например, по стандарту MIL-HDBK-217).

Конкретная ошибка. Проектировщики не применили поправочные коэффициенты для тяжёлых условий эксплуатации.

Пыль забивает механические части клапанов, заслоняет оптические датчики.

Вибрация ослабляет соединения, приводит к усталостным разрушениям, вызывает ложные срабатывания вибрационных датчиков.

Это в разы увеличивает реальную интенсивность отказов. В результате расчетный PFDavg был красивым (SIL 2), а реальный – на уровне SIL 0.

Общие причины отказа.

Нельзя:

прокладывать кабели питания и сигнальные кабели всех каналов безопасности в одном лотке;

запитывать всю систему безопасности (датчики, контроллер, клапаны) от одной электрической подстанции или даже от одной секции шин.

Конкретная ошибка. Отказ подстанции (короткое замыкание, срабатывание вводного автомата, перерыв в электроснабжении) привёл к одновременному отказу ВСЕХ элементов системы. и датчиков, и «мозга» (логического решателя), и исполнительных механизмов.

Система была реализована с архитектурой 1oo3 (три датчика). Однако из-за электрического останова она мгновенно превратилась в систему 1oo0.

Верификация.

Нельзя тестировать систему только при комнатной температуре (+20°C) на чистом стенде в офисе.

Конкретная ошибка. Полупроводниковые компоненты (микропроцессоры в контроллерах) имеют совершенно разные характеристики при высокой температуре. При +50°C могут возникать сбои в работе памяти, процессор может уходить в сброс или «зависать». Тестирование в «холодных» условиях этого не выявило. Система, признанная работоспособной на стенде, отказала в реальных пустынных условиях.

Как НУЖНО делать.

Расчет PFDavg. Необходимо использовать стандарты, учитывающие условия эксплуатации, например, EXIDA или OREDA. Выбирать оборудование с сертификацией SIL именно для того типа применения, которое у вас есть (например, для высоко вибрационных зон). Умножать «каталожные» λ на коэффициенты окружающей среды, коэффициенты применения и т.д.

Архитектура и инфраструктура. Раздельное питание. Датчики канала измерения запитывать от источника бесперебойного питания (ИБП) №1. Контроллер и датчики второго канала – от ИБП №2. Исполнительные механизмы – от отдельной подстанции с дизель-генератором.

Физическое разделение. Кабели резервных каналов должны прокладываться по разным маршрутам (например, по разным эстакадам), чтобы пожар или механическое повреждение не вывело из строя все каналы сразу.

Верификация опасностей отказов должна включать тепловые испытания. Шкафы управления должны помещаться в термокамеру и работать при максимальной заявленной температуре окружающей среды (+50°C, +60°C). Под нагрузкой (эмулируется работа всех входов/выходов) проверяется стабильность работы контроллера, время реакции и отсутствие сбоев. Аналогично должны тестироваться датчики и исполнительные механизмы.

Проектирование систем безопасности – это не протоколы и бюрократия. Это глубокая инженерная дисциплина, требующая:

- Понимания физики и химии процесса, который вы защищаете.
- Понимания реальных, а не кабинетных условий эксплуатации (пыль, влага, вибрация, температура).
- Понимания принципов избыточности и независимости для исключения общих точек отказа.
- Жесткого и реалистичного тестирования, которое доказывает, что система работает не только в идеальных условиях, но и в условиях, максимально приближенных к аварийным.

11.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 11.3. Уяснить ответы и объяснения всех тестов раздела. С поддержкой AI (типа GPT) подготовить свои ответы и объяснения для 2-х или 3-х тестов этого раздела, задаваемых преподавателем, со ссылками на соответствующие разделы норм и стандартов.

Тест 11.1. Формирование требований к проектированию систем безопасности (СПАЗ/SIS).

Вопрос 1. Какие из следующих утверждений верны относительно требований к приборной системе безопасности (СПАЗ/SIS)?

а) СПАЗ/SIS должна соответствовать установленному уровню безопасности (SIL).

б) СПАЗ/SIS должна выполнять только одну функцию безопасности.

с) СПАЗ/SIS должна иметь документацию, подлежащую формализованному пересмотру.

д) СПАЗ/SIS может выполнять функции логических последовательностей.

Ответ. Согласно международному стандарту ГОСТ Р МЭК 61511-1-2018, который устанавливает ключевые требования к приборным системам безопасности (ПСБ/SIS), правильными являются варианты а), с) и д).

Объяснение.

а) Соответствие SIL. Уровень полноты безопасности (SIL) – это ключевой параметр. Соответствие гарантирует, что система обеспечит необходимый уровень снижения риска. Это требование стандарта.

с) Документация и формализованный пересмотр. Стандарты 61508/61511 требуют наличия документированных процедур и их строгого анализа на всех этапах жизненного цикла SIS для исключения ошибок.

д) Выполнение логических последовательностей. SIS может выполнять не только единичные действия, но и сложные последовательности операций для перевода процесса в целом в безопасное состояние. Это соответствует требованию стандарта.

б) Только одна функция. Это ошибочное утверждение. Одна система SIS может быть спроектирована для реализации нескольких функций безопасности (SIF), каждая со своим SIL. Это противоречит стандарту.

Практические рекомендации по проектированию.

При формировании требований к SIS следует ориентироваться на ее жизненный цикл, определенный в стандарте.

Требования в спецификации СПАЗ должны охватывать все этапы – от HAZID и проектирования до монтажа, эксплуатации и вывода из эксплуатации.

Четкое разделение ответственности. Стандарт требует, чтобы все обязанности были четко распределены между различными сторонами (проектировщиками, поставщиками, эксплуатантами), даже если он не предписывает, кому именно какая роль достается.

Вопрос 2. Какие функции может выполнять СПАЗ/SIS?

- a) Только функции, связанные с безопасностью.
- b) Функции логических последовательностей и другие функции безопасности.
- c) Не классифицированные блокировки, если они не влияют на безопасность.
- d) Любые функции, не требующие сертификации.

Ответ: b), c).

Объяснение.

b) СПАЗ/SIS может выполнять функции логических последовательностей, а также другие функции безопасности, что позволяет адаптировать систему к различным требованиям.

c) Не классифицированные блокировки могут быть введены в СПАЗ/SIS, при условии, что они не прерывают или не ухудшают выполнение функций безопасности.

Вопрос 3. Почему важно, чтобы документация и оборудование СПАЗ/SIS подвергались формализованному пересмотру и контролю за выпуском?

- a) Это помогает избежать ошибок и несоответствий.
- b) Это не имеет значения для безопасности системы.
- c) Это увеличивает время разработки системы.
- d) Это позволяет поддерживать актуальность и надежность системы.

Ответ: a), d).

Объяснение.

a) Формализованный пересмотр и контроль за выпуском необходимы для предотвращения ошибок и обеспечения соответствия стандартам.

d) Важно, чтобы документация и оборудование СПАЗ/SIS подвергались формализованному пересмотру и контролю за выпуском. Это помогает поддерживать актуальность и надежность системы, что критически важно для безопасности.

Вопрос 4. Каковы требования к безопасным срабатываниям системы?

- a) Безопасные срабатывания должны быть четко определены для каждого компонента.
- b) Безопасные срабатывания могут быть отменены в любой момент.
- c) Безопасные срабатывания должны оставаться активными до перенастройки.

d) Безопасные состояния не имеют значения для функционирования системы.

Ответ: а), с).

Объяснение.

а) Безопасные срабатывания каждого компонента должны быть четко определены, чтобы система могла эффективно реагировать на аварийные ситуации.

с) Способность срабатывания СПАЗ должна оставаться активной до перенастройки (деблокировки), чтобы гарантировать, что система остается в безопасном состоянии.

Вопрос 5. Какие меры предосторожности следует учитывать при изменениях в техническом и программном обеспечении СПАЗ/SIS?

а) Изменения могут создать новые риски и уязвимости.

б) Изменения не влияют на безопасность системы.

с) Необходимо проводить оценку воздействия изменений на безопасность.

д) Все изменения должны быть верифицированы и валидированы.

Ответ: а), с), d).

Объяснение.

а) Изменения в техническом и программном обеспечении могут создать новые риски и уязвимости, что требует осторожности.

с) Необходимо проводить оценку воздействия изменений на безопасность, чтобы выявить потенциальные угрозы.

д) Все изменения в СПАЗ должны быть верифицированы и валидированы, чтобы гарантировать соответствие установленным требованиям по безопасности.

Вопрос 6. Какие общие требования технических стандартов должны быть учтены при проектировании СПАЗ/SIS?

а) Любая одиночная неисправность, приводящая к отказу СПАЗ/SIS, должна приводить к защитным действиям.

б) Цепи питания входов/выходов СПАЗ/SIS должны быть отделены от всех других цепей.

с) Необходимо применять только стандартные требования, не учитывающие окружающую среду.

д) Проектирование должно учитывать условия окружающей среды (температуру, влажность, вибрацию, взрывоопасность) в соответствии с применимыми стандартами (например, серией МЭК 60079.

Ответ: а, b, d.

Объяснение.

а) Это требование гарантирует, что в случае отказа системы будут предприняты соответствующие защитные действия, минимизирующие риски.

б) Отделение цепей питания входов/выходов от других цепей предотвращает влияние неисправностей на работу системы безопасности.

д) Применение подходящих нормативов и стандартов позволяет учитывать все возможные риски, связанные с окружающей средой и классификацией опасностей.

Вопрос 7. Каковы основные принципы, которые следует учитывать при проектировании системы безопасности автоматизации?

а) Все компоненты системы должны быть сертифицированы по стандартам безопасности.

б) Проектирование должно учитывать возможные одиночные неисправности и их последствия.

с) Все изменения в системе должны быть одобрены только одним специалистом.

д) Необходимо проводить регулярные проверки и тестирования системы.

Ответ: а, б, д.

Почему эти принципы важны:

а) Сертификация компонентов. Использование аппаратных и программных средств, сертифицированных для целевого уровня полноты безопасности (SIL), является базовым требованием стандарта. Это гарантирует, что каждый компонент обладает необходимыми характеристиками надежности и соответствует строгим стандартам, таким как МЭК 61508 и МЭК 61511.

б) Учет одиночных неисправностей. Проектирование должно быть отказоустойчивым. Стандарт требует анализа и предотвращения отказов по общей причине, а также зависимых отказов. На практике это реализуется через резервирование каналов, диагностику для выявления скрытых отказов и архитектурные решения (например, 1oo2, 2oo3), которые гарантируют переход в безопасное состояние при любой единичной неисправности.

д) Регулярные проверки и тестирования. Функциональная безопасность обеспечивается на протяжении всего жизненного цикла системы. Стандарт устанавливает требования не только к проектированию, но и к эксплуатации и техническому обслуживанию. Регулярные проверки, контрольные испытания и техническое обслуживание необходимы для своевременного обнаружения и устранения скрытых отказов, которые могут накапливаться со временем.

Почему вариант «с» ошибочен?

Требование о том, чтобы все изменения в системе были одобрены только одним специалистом, является неверным и потенциально опасным.

Такой подход создает «единую точку отказа» и увеличивает риск человеческой ошибки. Без коллективной проверки и всестороннего

анализа одно упущение или неверное решение единственного специалиста может привести к внесению в систему опасной ошибки.

Процедуры управления изменениями (модификацией) системы безопасности требуют строгого документирования, анализа влияния на безопасность и утверждения компетентными лицами. Это коллективный и документированный процесс, а не единоличное решение.

См. ГОСТ Р МЭК 61 511-1 -2018 Раздел 11.

Тест 11.2. Раздельные АСДУ и СПАЗ и совместное использование КИПиА.

Вопрос1. Какие исключения из правил раздельного использования датчиков допускаются согласно стандартам ISA и МЭК 61511?

- а) Совместное использование датчиков допускается только в системах с уровнем полноты безопасности SIL 1.
- б) Датчик может использоваться в АСДУ для функций управления, не связанных с СПАЗ/SIS.
- с) Необходима дополнительная диагностика для обеспечения требований по надежности.
- д) Все вышеперечисленные пункты являются корректными.

Ответ D. Все вышеперечисленные пункты являются корректными.

Вопрос 2. Какие условия должны быть выполнены для совместного использования датчиков АСДУ/СПАЗ в системах с уровнем полноты безопасности SIL 1?

- а) Датчики должны использоваться только для функций, связанных с СПАЗ/SIS.
- б) Датчики могут использоваться в АСДУ для функций управления, не связанных со СПАЗ/SIS.
- с) Необходима полная изоляция датчиков от других систем.
- д) Датчики должны быть сертифицированы для совместного использования.

Ответ В. Датчики могут использоваться в АСДУ для функций управления, не связанных со СПАЗ/SIS.

Объяснение.

Совместное использование датчиков в системах с уровнем полноты безопасности SIL 1 допускается только в том случае, если они используются в автоматизированной системе диспетчерского управления (АСДУ) для функций, не связанных с задачами систем безопасности (СПАЗ/SIS). Это позволяет избежать увеличения опасных запросов на СПАЗ/SIS в случае отказа датчика.

Вопрос 3. Какое значение имеет дополнительная диагностика при совместном использовании датчиков?

- а) Она не имеет значения, так как датчики всегда надежны.
- б) Она служит для повышения производительности системы.

с) Она необходима для обеспечения требований по надежности при совместном использовании.

д) Она используется только для датчиков, которые находятся под высоким давлением.

Ответ С. Она необходима для обеспечения требований по надежности при совместном использовании.

Объяснение.

Дополнительная диагностика необходима для обеспечения требований по надежности, когда датчики используются совместно. Это позволяет гарантировать, что даже при отказе одного из датчиков система остается надежной и безопасной. Без дополнительной диагностики невозможно эффективно управлять рисками, связанными с возможными отказами.

Вопрос 4. Как следует рассматривать датчик, который используется для записи данных в системе?

а) Как часть системы СПАЗ/SIS с необходимыми функциями защиты и тестирования.

б) Как отдельный компонент, не влияющий на безопасность.

с) Как ненадежный элемент, который следует игнорировать.

д) Как временный датчик, который не требует тестирования.

Ответ а.

Объяснение.

Если датчик используется для записи данных, его следует рассматривать как часть системы СПАЗ/SIS с необходимыми функциями защиты и тестирования. Это означает, что он должен соответствовать всем требованиям безопасности, иначе его отказ может привести к опасным ситуациям.

Вопрос 5. Каковы требования к разделению датчиков СПАЗ/SIS и датчиков АСДУ?

а) Датчики СПАЗ/SIS и АСДУ должны быть полностью изолированы друг от друга.

б) Резервированные датчики могут использоваться совместно с датчиками АСДУ.

с) Совместное использование датчиков не допускается в любых условиях.

д) Резервированная защита может быть совместно использована.

Ответ. а), б), д).

Объяснение.

а) Полная изоляция датчиков СПАЗ/SIS и АСДУ необходима для предотвращения влияния одной системы на другую и обеспечения надежности работы.

б) Резервированные датчики могут быть исключением, так как они предназначены для обеспечения дополнительной надежности.

d) Резервированная защита может быть использована совместно, так как она служит для повышения безопасности и надежности системы.

Вопрос 6. Какие исключения из правил раздельного использования датчиков допускаются согласно стандартам ISA и МЭК 61511? Выберите ответ.

a) Раздельное использование датчиков и исполнительных устройств может быть исключено в системах с уровнем полноты безопасности SIL2, если удастся доказать выполнение требований полноты безопасности.

b) Раздельное использование датчиков и исполнительных устройств может быть исключено в системах с уровнем полноты безопасности SIL3, если датчики используются исключительно для записи данных.

c) Раздельное использование датчиков и исполнительных устройств может быть исключено в системах с уровнем полноты безопасности SIL 4, если датчики применяются только для мониторинга процессов.

d) Раздельное использование датчиков и исполнительных устройств может быть исключено в системах с уровнем полноты безопасности SIL1, если удастся доказать выполнение требований полноты безопасности и датчик используется в системе автоматического управления (АСДУ), но не связан с задачами системы предотвращения аварий (СПАЗ/SIS).

e) Раздельное использование датчиков и исполнительных устройств всегда обязательно во всех случаях независимо от уровня полноты безопасности.

Ответ d. Раздельное использование датчиков и исполнительных устройств может быть исключено в системах с уровнем полноты безопасности SIL1, если удастся доказать выполнение требований полноты безопасности и датчик используется в системе автоматического управления (АСДУ), но не связан с задачами системы предотвращения аварий (СПАЗ/SIS).

Объяснение ответа d. Согласно стандартам МЭК 61511, исключение из правила раздельного использования датчиков и исполнительных устройств действительно возможно в системах с низким уровнем полноты безопасности SIL1, если соблюдаются определенные условия.

Не верно.

a) Не соответствует действительности, так как стандарты требуют раздельного использования датчиков и исполнительных устройств в системах с более высокими уровнями полноты безопасности (SIL 2 и выше).

б) Использование датчиков исключительно для записи данных само по себе не является основанием для исключения из правила раздельного использования. Датчики должны соответствовать требованиям стандартов и выполнять свои задачи без увеличения риска аварии.

с) Мониторинг процессов сам по себе не исключает необходимости соблюдения принципа раздельного использования датчиков и исполнительных устройств.

е) Всегда обязательное раздельное использование датчиков и исполнительных устройств не указано в стандартах; есть конкретные случаи, когда можно сделать исключение, например, при низком уровне полноты безопасности (SIL 1) и соблюдении определенных условий.

Исключения из правил раздельного использования датчиков допускаются в системах с уровнем полноты безопасности SIL 1 только при соблюдении определенных условий.

Важно, чтобы датчики использовались только для функций, не связанных со СПАЗ/SIS, и чтобы была обеспечена дополнительная диагностика для поддержания надежности системы. Вот что гарантирует, что совместное использование не приведет к увеличению рисков и обеспечит безопасность процессов.

Стандарты МЭК 61511 допускают совместное использование датчиков в системах с уровнем полноты безопасности SIL 1 при условии, что будут выполнены требования по полноте безопасности. Это означает, что в таких системах необходимо тщательно оценить риски и гарантировать, что использование общих датчиков не приведет к увеличению опасных запросов на системы безопасности (СПАЗ/SIS).

Датчик может быть использован в автоматизированной системе диспетчерского управления (АСДУ) для выполнения функций, не связанных с задачами систем безопасности. Это важно, так как если датчик используется только для управления, не влияя на безопасность, его отказ не должен привести к опасным ситуациям. Однако, если датчик используется для записи данных, его следует рассматривать как часть СПАЗ/SIS.

Для выполнения требований по надежности, когда датчики используются совместно, может потребоваться дополнительная диагностика. Это необходимо для того, чтобы убедиться, что даже при совместном использовании датчиков, система остается надежной и безопасной, и что все возможные отказы могут быть обнаружены и устранены.

Анализ совместного и раздельного использования датчиков показан на рисунке 11.1. Раздельно используемый датчик снижает вероятность опасного отказа СПАЗ [28].

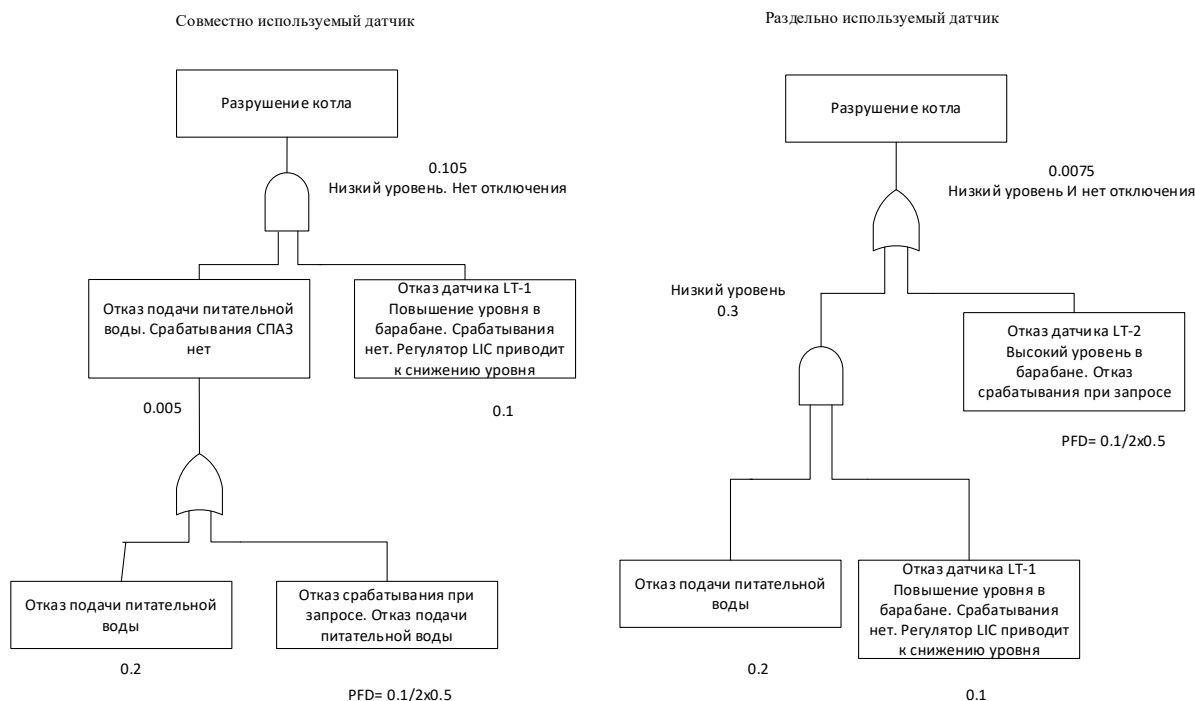


Рис. 11.1. Анализ дерева ошибок, показывающий как отдельные датчики снижают частоту опасных событий

Тест 11.3. Выбор компонентов СПАЗ/SIS (датчиков, логики, исполнительных устройств).

Ключевая идея. Надежность СПАЗ/SIS зависит от трех ключевых компонентов.

1. Датчики (давления, температуры, расхода) — это «глаза и уши» системы.

2. Логический решатель (ПЛК, реле) — это «мозг», принимающий решение.

3. Исполнительные устройства (клапаны, приводы) — это «руки», выполняющие действие.

Каждый компонент влияет на PFD_{avg} (отказобезопасность) и STR (отказоустойчивость).

Вопрос 1. Датчики СПАЗ. Как выбрать?

Ответ. Критерии выбора.

1. Тип отказа и диагностическое покрытие (DC).

Высокое $DC \geq 90\%$. Это датчики с самодиагностикой (например, аналоговые 4–20 мА + HART с диагностикой обрыва, короткого замыкания, дрейфа).

Низкая опасная необнаруженная интенсивность отказов (λ_{du}). Это датчики с высокой надежностью (например, вибрационные вместо механических концевых выключателей).

2. Сертификация.

Датчик должен иметь сертификат полноты безопасности **SIL** и применения **ROUTE** (МЭК 61508 / МЭК 61511), и соответствовать заявленному уровню безопасности.

Проверка. Смотри FMEDA-отчет, данные по λ_{du} , λ_{su} , SFF.

3. Резервирование (архитектура голосования).

1oo2 (два датчика, срабатывание по любому):

- Снижает PFDavg (вероятность опасного отказа).
- Увеличивает STR (частота ложных срабатываний).

2oo3 (три датчика, срабатывание по двум).

- Оптимальный баланс между PFDavg и STR. Обеспечивает:
- Выше стоимость и сложность.

4. Условия эксплуатации.

- Температура, вибрация, коррозия, взрывоопасная зона (Ех-защита).
- Влияние на λ_{du} (например, пыль может ухудшить диагностику).

Примеры выбора приведены в таблице 11.1.

Таблица 11.1.

Требуемый SIL	Архитектура	Тип датчика	Пример
SIL 2	1oo2	$\lambda_{du} < 0.001$, DC $\geq 90\%$	Rosemount 3051S (HART + диагностика)
SIL 3	2oo3	$\lambda_{du} < 0.0001$, DC $\geq 99\%$	Pepperl+Fuchs R2000 (SIL 3)

Типичные ошибки.

- Выбор датчика без диагностики ведет к высокому λ_{du} , что неприемлемо для SIL 2/3.
- Игнорирование резервирования для SIL 3 – это недостаточная безопасность.
- Несертифицированные датчики означает, что нет подтвержденных данных по λ_{du} и SFF.
- Пренебрежение условиями эксплуатации – это ускоренный износ, рост отказов.
- Неправильная классификация датчика с HART протоколом как тип А, полагая, что 4-20 мА канал является «простым» аналоговым сигналом.

Классификация датчика как Type В для определения SIL требует дополнительных расчетов с учетом того, что:

- а) его коэффициент безопасных отказов (SFF) должен рассчитываться на основе подробного анализа режимов отказа (FMEDA), с учетом безопасных обнаруженных, безопасных необнаруженных, опасных обнаруженных и опасных необнаруженных отказов;

б) при расчете высоких уровней SIL (в частности, SIL 2, SIL 3) должны устанавливаться более строгие требования к архитектурной избыточности (HFT) по сравнению с элементами Type A. Это связано с учетом возможности систематических отказов;

с) для Type B элементов необходимо уделять больше внимания предотвращению и контролю систематических отказов (вызванных, например, ошибками в проектировании или ПО), в дополнение к случайным аппаратным отказам.

Дополнительные рекомендации:

- Проводить верификацию λ_{du} по FMEDA.
- Учитывать время восстановления (MTTR) для расчета PFD_{avg} .
- Анализировать общую архитектуру СПАЗ/SIS (датчики + логика + исполнительные элементы).

Вопрос 2. Исполнительные устройства для СПАЗ как выбрать?

Критерии выбора.

1. Тип отказа и диагностика.

- **Высокое λ_{du}** соответствует устройствам с самодиагностикой (например, интеллектуальные позиционеры клапанов с мониторингом трения, износа, времени срабатывания).
- **Низкое λ_{du}** соответствует отказобезопасной конструкции (пружинный возврат, дублированные катушки для электромагнитных клапанов).

2. Сертификация.

- Сертификат **SIL и ROUTE** (например, МЭК 61508 для клапанов, МЭК 61511 для архитектуры).
- Данные из FMEDA (λ_{du} , SFF, время срабатывания для расчета PFD_{avg}).

3. Резервирование.

- **Схема 1oo2** (два клапана, срабатывание любого) снижает PFD_{avg} , но повышает STR.
- **2oo2** (два клапана, срабатывание обоих) уменьшает STR, но увеличивает PFD_{avg} .
- **2oo3** (три клапана, срабатывание двух) – это компромисс для SIL 3.

4. Условия эксплуатации.

- Давление, температура, агрессивная среда (например, нержавеющая сталь для химических производств).
- Влияние на надежность (например, заклинивание клапана из-за коррозии).

Примеры выбора ИУ приведены в таблице 11.2.

Таблица 11. 2 Примеры выбора ИУ.

Требуемый SIL	Архитектура	Тип устройства	Пример
SIL 2	1oo2	Клапан с пружинным возвратом + интеллектуальный позиционер	Samson 3724 (SIL 2)
SIL 3	2oo3	Дутированный шаровый клапан с резервированными катушками	Metso ND9000 (SIL 3)

Возможные ошибки выбора:

- Отсутствие диагностики (например, клапан без мониторинга позиции).
- Игнорирование времени срабатывания (не вписывается в общее время отклика СПАЗ/SIS).
- Выбор клапана без испытания на частичный ход PST для SIL 3.
- Игнорирование λ_{du} при выборе.
- Несоответствие среды (например, эпоксидное покрытие для кислот вместо тефлона).

Вопрос 3. Выбор ПЛК для СПАЗ.

Ответ. Критерии выбора.

1.Сертификация.

- **Сертификат SIL** (МЭК 61508, МЭК 61131 для ПО).
- Подтвержденные данные. **PFDavg**, SFF, архитектура (1oo1, 1oo2D и т.д.).

1. Диагностика.

- Встроенные тесты. контроль ОЗУ, ЦП, входов/выходов.
- Watchdog-таймеры для обнаружения «зависаний».
- $DC \geq 99\%$ для SIL 3.

2. Резервирование.

- **1oo1D** (1 канал + диагностика) – для SIL 2.
- **2oo3** – для SIL 3
- **1oo2D** (два процессора с взаимным контролем для SIL 3).
- Параллельное резервирование снижает MTTR.

3. Интеграция.

- Поддержка протоколов (HART, Profibus SAFE, FSoE).
- Совместимость с датчиками/исполнительными устройствами.

3.2. Примеры выбора ПЛК приведены в таблице 11.3.

Таблица 11.3.

Требуемый SIL	Архитектура ПЛК	Пример
SIL 2	1oo1	Siemens S7-1500F (с диагностикой)
SIL 3	1oo2D	Honeywell Safety Manager SC450

Возможные ошибки выбора:

- **Использование обычного ПЛК.**
- **Не было учета времени восстановления (MTTR) для диагностики.**
- **Слабая диагностика** (например, нет контроля перегрева).
- **Неправильный расчет PFD_{avg}** (не учтены задержки передачи сигнала).

Практическое правило. «Золотая тройка».

Чтобы СПАЗ/SIS соответствовала требуемому SIL, все три компонента должны быть согласованы по надежности:

1. **Датчики.** Резервирование + диагностика.
2. **Логика.** Отказоустойчивая архитектура.
3. **Клапаны.** Fail-safe конструкция + PST.

Пример для SIL 2. Выбор:

- Датчики. 1oo2 ($\lambda_{du}=0.0005$).
- Логика. 1oo1D (ПЛК с DC > 90%).
- Клапан. Один с PST ($\lambda_{du}=0.001$).

Датчики. Чем выше SIL, тем важнее резервирование и диагностика.

Логика. Safety-ПЛК + архитектура (1oo2, 2oo3).

Клапаны. Отказоустойчивость + PST.

Главный секрет. Нельзя сделать систему надежной, если один компонент слабее других (например, датчики с SIL 3, а клапан с SIL 1). Все должно быть сбалансировано!

Тест 11.4. Правила раздельного использования оконечных элементов в СПАЗ.

Вопрос 1. Каковы основные правила раздельного использования оконечных элементов (ИУ) [28] в системах предотвращения аварий (СПАЗ)?

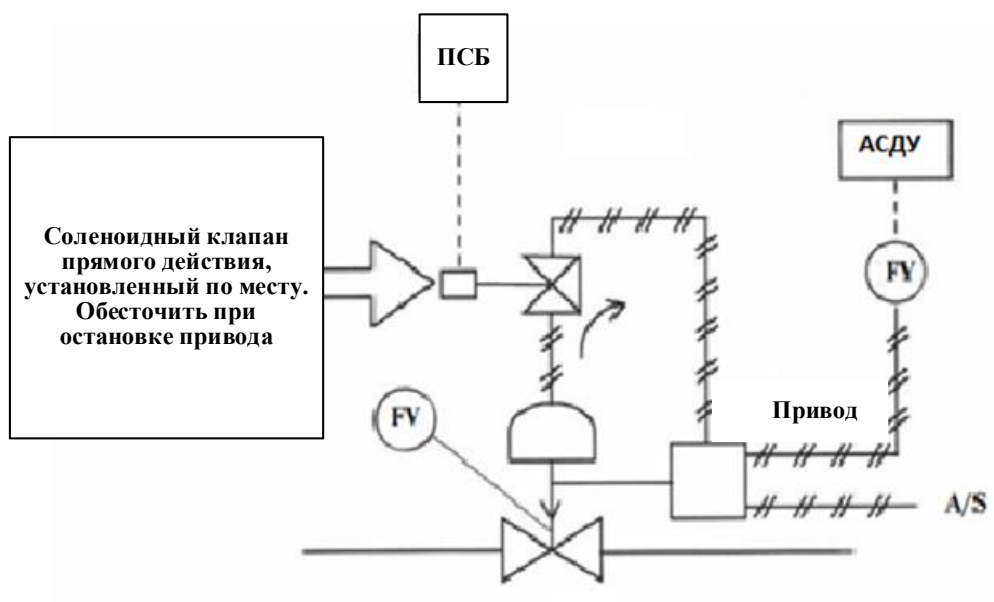


Рис 11.2 Совместное использование ИУ АСДУ и СПАЗ (SIL 1)

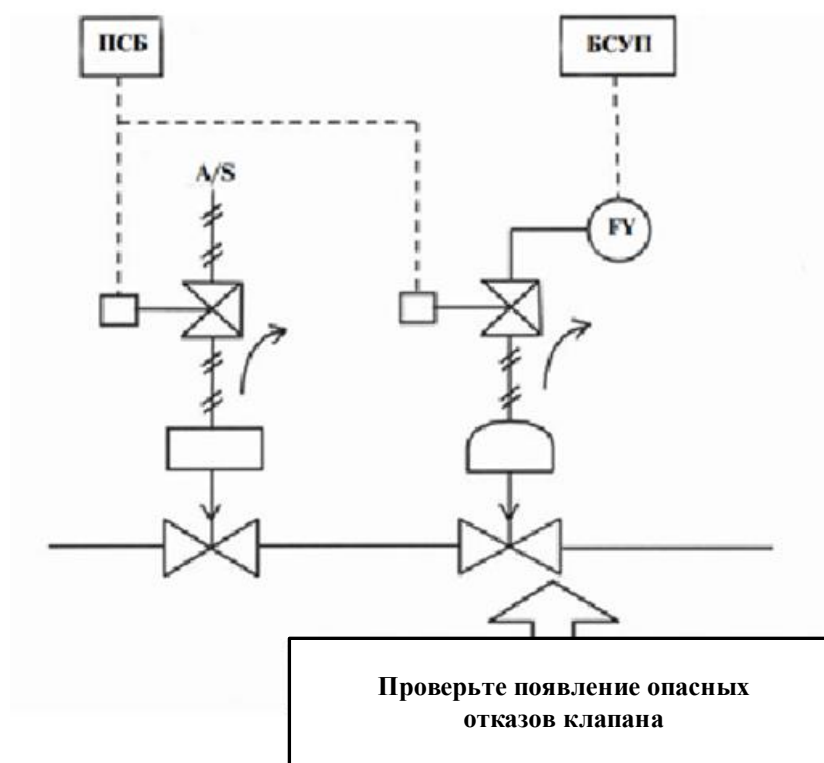


Рис. 11.3. Совместное использование ИУ АСДУ и СПАЗ (SIL 2, SIL 3)

Примеры функциональных схем совместного использования ИУ приведены на рисунках 11.2 и 11.3.

Укажите все верные утверждения.

а) В системах с уровнем полноты безопасности (SIL) 1 и SIL 2 рекомендуется снимать напряжение с главного управляющего контактора для отключения электроприводов.

b) В системах с SIL 3 требуется использование второго контактора для обеспечения резервирования.

c) Один и тот же клапан может использоваться одновременно в базовой системе управления процессом и в системе предотвращения аварий (СПАЗ/SIS), если отказ этого клапана не вызывает запрос на срабатывание СПАЗ/SIS и диагностическое покрытие достаточно для выполнения требований полноты безопасности.

d) В системах с SIL 1 использование клапана, существующего в системе управления процессом, для отключения процесса считается приемлемым, если анализ опасности показывает, что ошибки в этом клапане вряд ли вызовут запрос в СПАЗ/SIS.

e) Стандарт МЭК 61511 требует включения соленоидов срабатывания по специальной схеме для гарантии того, что дефекты позиционера не помешают выполнению срабатывания.

f) В системах с SIL 2 предпочтительным методом является установка отдельного клапана останова для выполнения задач отсечения или сброса.

g) Во всех системах с любым уровнем полноты безопасности всегда требуется строгое разделение окончных элементов между системами управления процессами и системами предотвращения аварий.

Ответ.

a) В системах с уровнем полноты безопасности (SIL) 1 и SIL 2 снятие напряжения с главного управляющего контактора для отключения электроприводов действительно считается нормальной практикой.

b) В системах с SIL 3 действительно требуется использование второго контактора для обеспечения резервирования, чтобы повысить надежность системы.

c) Один и тот же клапан может использоваться одновременно в базовой системе управления процессом и в системе предотвращения аварий (СПАЗ/SIS), если соблюдены два важных условия. отказ клапана не приводит к запросу на срабатывание СПАЗ/SIS, и диагностические возможности достаточные для выполнения требований полноты безопасности.

d) В системах с SIL 1 использование клапана, уже имеющегося в системе управления процессом, для отключения процесса допустимо, если анализ опасности подтверждает низкую вероятность появления запроса в СПАЗ/SIS вследствие ошибок в работе этого клапана.

e) Согласно стандарту МЭК 61511, действительно требуется специальная схема подключения соленоидов срабатывания, которая предотвращает влияние дефектов позиционера на выполнение срабатывания.

f) В системах с SIL 2 действительно предпочтительно устанавливать отдельный клапан останова для выполнения задач отсечения или

сброса, чтобы обеспечить высокую степень надежности и безопасности.

Неправильный ответ.

g) Утверждение о строгом разделении оконечных элементов во всех системах с любым уровнем полноты безопасности неверно. Стандарты допускают некоторые исключения, особенно для систем с низким уровнем полноты безопасности (например, SIL 1), где могут применяться общие элементы, если они соответствуют определенным условиям.

Объяснение.

Пункт а). В системах с уровнем полноты безопасности (SIL) 1 и SIL 2, как правило, применяется практика снятия напряжения с главного управляющего контактора для отключения электроприводов. Это связано с тем, что такие системы имеют относительно низкий уровень критичности, и такой подход обеспечивает достаточное быстрое действие и надежность для выполнения защитных функций.

Пункт б). Системы с уровнем полноты безопасности (SIL) 3 относятся к категории более высоких уровней критичности. Поэтому здесь требуется резервирование компонентов, включая контакторы, для повышения общей надежности системы и снижения вероятности отказа оборудования.

Пункт с). Использование одного и того же клапана в обеих системах – управлении процессом и предотвращении аварий – допускается, если отказ этого клапана не приведет к возникновению запроса на срабатывание системы предотвращения аварий. Кроме того, важно убедиться, что система обладает достаточной диагностической способностью для своевременного обнаружения возможных проблем и выполнения требований полноты безопасности.

Вот нужная памятка.

Чтобы проверить, можно ли использовать общий клапан, нужно задать себе контрольный вопрос:

«Если этот клапан сломается в любом положении (откроется, заклинит или останется на месте), потребует ли эта поломка срабатывания SIS, чтобы предотвратить аварию?»

Если ДА, то использование общего клапана ЗАПРЕЩЕНО. Нужен отдельный клапан для SIS.

Если НЕТ, то использование общего клапана МОЖЕТ БЫТЬ РАЗРЕШЕНО (при условии, что он соответствует другим требованиям по SIL).

Этот принцип гарантирует, что система безопасности остается независимой и эффективной даже при отказах в системе базового управления.

Пункт d). В системах с уровнем полноты безопасности (SIL) 1 иногда разрешается использовать существующие клапаны системы

управления процессом для отключения процесса. Однако это допустимо лишь тогда, когда анализ опасности показывает, что возможные неисправности данного клапана вряд ли приведут к появлению запроса на срабатывание системы предотвращения аварий.

Пункт е). Стандарт МЭК 61511 предписывает подключение соленоидов срабатывания таким образом, чтобы исключить возможность влияния неисправностей позиционеров на выполнение защитного срабатывания. Это повышает общую безопасность системы, минимизируя риски, связанные с дефектами отдельных компонентов.

Пункт f). В системах с уровнем полноты безопасности (SIL) 2 рекомендуется применять отдельные клапаны останова для выполнения задач отсечения или сброса. Это позволяет повысить надежность системы и снизить вероятность возникновения аварийных ситуаций.

Пункт g). Неверное утверждение. Хотя в большинстве случаев рекомендуется разделять оконечные элементы между системами управления процессами и системами предотвращения аварий, существуют исключения, особенно для систем с низким уровнем полноты безопасности (например, SIL 1), где могут использоваться общие компоненты при выполнении определенных условий.

Для получения дополнительной информации см. [28].

Тест 11.5. Применение позиционеров в системах безопасности.

Вопрос 1. Какова основная функция позиционера в системах безопасности?

- a) Управление скоростью потока жидкости.
- b) Автоматическая проверка значений обратной связи и тестирование клапанов.
- c) Обеспечение визуального контроля за состоянием системы.
- d) Изменение температуры в системе.

Ответ b. Автоматическая проверка значений обратной связи и тестирование клапанов.

Объяснение. Основная функция позиционера в системах безопасности заключается в автоматической проверке значений обратной связи, а также в проведении тестов, таких как тест частичного закрытия, чтобы убедиться, что клапан работает правильно и соответствует заданным параметрам. Это критически важно для надежности систем безопасности.

Вопрос 2. Как позиционеры помогают улучшить коэффициент охвата диагностикой для опасных отказов?

- a) Уменьшают количество необходимых проверок.
- b) Путем проведения регулярных диагностических тестов.
- c) Увеличивают время реакции системы.
- d) Игнорируют данные обратной связи.

Ответ b. Путем проведения регулярных диагностических тестов

Объяснение. Регулярные диагностические тесты внутри позиционера позволяют выявлять потенциальные проблемы и обеспечивают улучшение коэффициента охвата для опасных отказов. Это позволяет системе более эффективно реагировать на возможные неисправности, что повышает общую безопасность.

Вопрос 3. Какое значение имеет тест частичного закрытия для отсечного клапана?

- a) Увеличение давления в системе.
- b) Проверка правильности срабатывания клапана.
- c) Снижение температуры в системе.
- d) Изменение типа используемого клапана.

Ответ b. Проверка правильности срабатывания клапана.

Объяснение. Тест частичного закрытия позволяет проверить, правильно ли срабатывает отсечной клапан и соответствует ли его движение заданным параметрам. Это важный аспект для обеспечения надежности и безопасности системы.

Вопрос 4. Какую информацию можно получить от данных обратной связи, поступающих в АСДУ?

- a) Только текущее состояние клапана.
- b) Сравнение состояния клапана с требуемым состоянием.
- c) Информацию о погодных условиях.
- d) Данные о расходах на обслуживание.

Ответ b. Сравнение состояния клапана с требуемым состоянием.

Объяснение. Данные обратной связи, поступающие в автоматизированную систему диспетчерского управления (АСДУ), позволяют сравнивать текущее состояние клапана с требуемым состоянием. Это критически важно для мониторинга работы системы и принятия решений о необходимости обслуживания или корректировки.

Вопрос 5. Как позиционеры могут прогнозировать необходимость обслуживания?

- a) Путем анализа данных о температуре в системе.
- b) Измеряя нагрузку в виде трения на исполнительное устройство.
- c) Управляя скоростью потока жидкости.
- d) Увеличивая время работы клапана.

Ответ b. Измеряя нагрузку в виде трения на исполнительное устройство.

Объяснение. Позиционеры могут измерять нагрузку в виде трения на исполнительное устройство, что позволяет прогнозировать необходимость обслуживания. Это помогает предотвратить потенциальные сбои и обеспечивает более надежную работу системы.

Вопрос 6. Какое влияние оказывают частые проверки на показатели PFDavg для установленных клапанов?

- a) Увеличивают PFDavg.
- b) Не оказывают никакого влияния.

- с) Обеспечивают существенное улучшение PFDavg.
- д) Уменьшают необходимость в обслуживании.

Ответ с. Обеспечивают существенное улучшение PFDavg.

Объяснение. Частые проверки при типичных значениях доли возможных опасных отказов комбинации привода и клапана (60-70%) обеспечивают существенное улучшение показателя PFDavg для установленных клапанов. Это критически важно для повышения надежности и безопасности системы.

Вопрос 7. Какое из перечисленных является ключевым преимуществом использования позиционеров для клапанов в системах безопасности с точки зрения эксплуатации и обслуживания?

- а) Повышение вероятности аварийных ситуаций.
- б) Снижение трудозатрат на калибровку и диагностику.
- с) Устранение проблем с забиванием клапана технологической средой.

Ответ б. Снижение трудозатрат на калибровку и диагностику.

Чтобы понять такой ответ, нужно разобраться, что такое позиционер и какую проблему он решает.

Проблема: Обычный клапан с пневмоприводом получает сигнал «открыться на 50%». Но из-за трения в сальнике, износа или изменения давления воздуха он может открыться только на 40% или на 60%. Мы не можем быть уверены в его реальном положении.

Поэтому позиционер – это «умный» контроллер, который устанавливается на клапан и постоянно сравнивает заданный сигнал (скажем, 50%) с реальным положением штока. Если есть расхождение, он немедленно его корректирует, подавая или стравливая воздух.

Без позиционера, чтобы убедиться, что клапан работает точно, его нужно регулярно выводить в цех и вручную, с помощью эталонных приборов, проверять и калибровать. Это долго, требует остановки процесса и трудозатратно.

С позиционером легко выполняется автоматическая калибровка. Кроме того, многие современные позиционеры умеют проводить самодиагностику. Например, позиционер по цифровому протоколу (HART, Foundation Fieldbus) может передавать на верхний уровень различную информацию: «Я получил сигнал 50%, но мне пришлось подать больше воздуха, чтобы преодолеть трение», «Сальник начал подтекать», «Время срабатывания увеличилось».

В результате реализуется простота обслуживания. Инженер видит эти данные на экране в операторной и понимает, какой клапан требует внимания, не выходя на объект.

Таким образом, позиционер превращает клапан из «немного» исполнительного механизма в «интеллектуальное» устройство, которое само сообщает о своем состоянии. Это снижает потребность в частом и сложном обучении персонала методам ручной диагностики и высвобождает время для решения более важных задач.

Почему другие варианты неверны.

а) Увеличение количества аварий? Это абсурд. Позиционер, наоборот, повышает точность и надежность работы, что является прямым вкладом в безопасность. Он помогает предотвратить аварии, вызванные некорректным положением клапана.

с) Устранение проблем с забиванием? Позиционер не борется с причиной забивания (например, смолами или кристаллизацией). Он лишь точно позиционирует клапан. Более того, если проходное сечение забито, он бессилён. Для борьбы с забиванием применяют другие решения: специальные конструкции клапанов (шаровые, мембранные), промывку, обогрев. Позиционер же может лишь зафиксировать факт возросшего усилия на закрытие/открытие, которое может быть симптомом забивания, и сообщить об этом.

Ключевое преимущество позиционера – это не просто «двигать клапан», а обеспечивать точность его работы и предоставлять ценнейшие данные для прогнозного обслуживания, что значительно облегчает жизнь и работу обслуживающего персонала.

Схемы контроля и диагностики позиционеров показаны на рис. 11.4 и 11.5 [28].

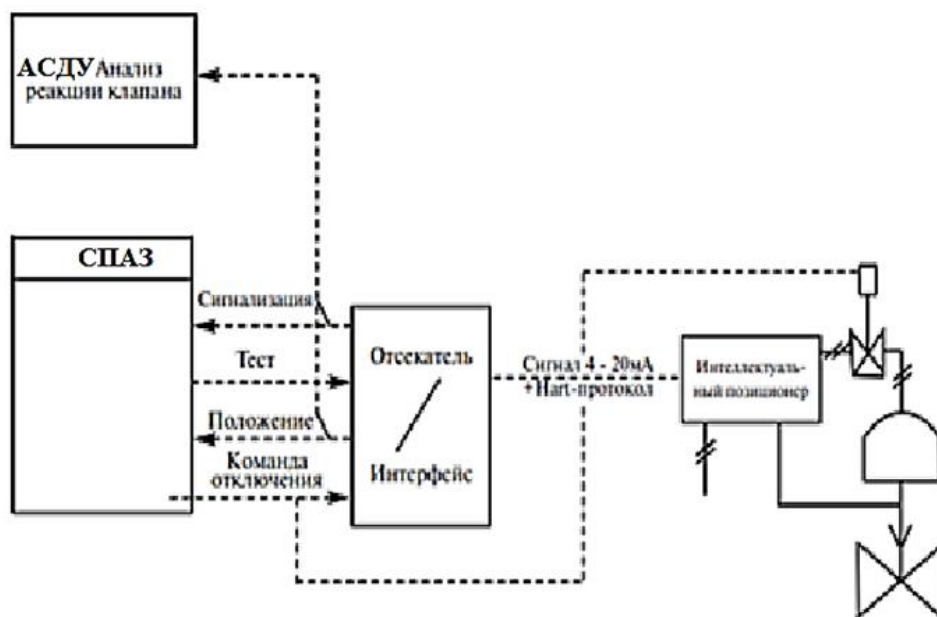


Рис 11.4. Управляющий клапан с интеллектуальным позиционером

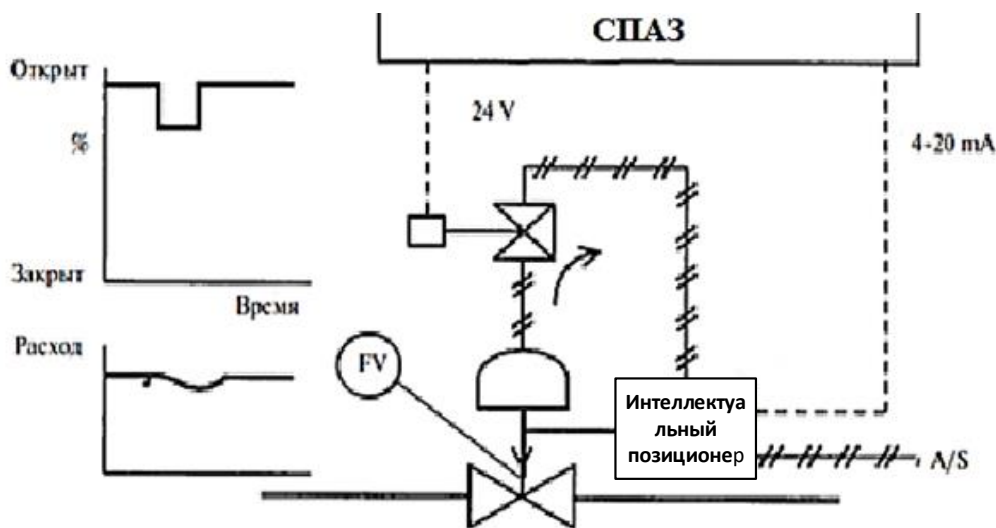


Рис. 11.5. Автоматическая проверка способом частичного закрытия ИУ с сертифицированным интеллектуальным позиционером или регулятором положения

Для получения дополнительной информации см. [28].

Тест 11.6. Ручное управление СПАЗ/SIS.

Вопрос 1. Каковы основные требования к средствам ручного воздействия на исполнительные элементы системы в соответствии со стандартом 61511-2 [28]?

- а) Средства ручного воздействия должны быть независимыми от логической части СПАЗ/SIS.
- б) Средства ручного воздействия могут быть интегрированы в логическую часть системы.
- в) Средства ручного воздействия должны быть предусмотрены, если это не противоречит спецификациям требований безопасности.
- г) Средства ручного воздействия не требуются при наличии автоматических систем управления.

Ответ: а и в.

Объяснение.

а) Средства ручного воздействия должны быть независимыми от логической части СПАЗ/SIS для обеспечения возможности ручного вмешательства в случае сбоя автоматической системы.

в) Эти средства должны быть предусмотрены, если это не противоречит спецификациям требований безопасности, что позволяет учитывать уникальные потребности системы.

Вопрос 2. Каковы потенциальные проблемы, связанные с ручными средствами срабатывания выходов в системе?

- а) Логическая часть СПАЗ/SIS должна отслеживать ручные срабатывания.
- б) Ручные срабатывания могут не фиксироваться в системе.
- в) Ручные средства могут вводить дополнительные риски при неправильном использовании.

d) Ручные средства срабатывания не требуют никакого контроля.

Ответ: a, b, c.

Объяснение.

a) Логическая часть СПАЗ/SIS должна отслеживать, что произошло срабатывание, инициированное вручную, чтобы обеспечить безопасность и контроль.

b) Если ручные срабатывания не фиксируются, это может привести к несоответствиям в документации и затруднениям в расследовании инцидентов.

c) Ручные средства могут вводить дополнительные риски, если они не будут правильно использованы, что требует дополнительного обучения и контроля.

Вопрос 3. Какие общие требования из стандарта 61511-2 должны быть учтены при проектировании СПАЗ/SIS?

a) Любая одиночная неисправность, приводящая к отказу СПАЗ/SIS, должна приводить к защитным действиям.

b) Цепи питания входов/выходов СПАЗ/SIS должны быть отделены от всех других цепей.

c) Необходимо применять только стандартные коды, не учитывающие окружающую среду.

d) В проекте должны быть применены подходящие коды или стандарты окружающей среды и классификации опасностей.

Ответ: a, b, d.

Объяснение.

a). Это требование гарантирует, что в случае отказа системы будут предприняты соответствующие защитные действия, минимизирующие риски.

b). Отделение цепей питания входов/выходов от других цепей предотвращает влияние неисправностей на работу системы безопасности.

d). Применение подходящих кодов и стандартов позволяет учитывать все возможные риски, связанные с окружающей средой и классификацией опасностей.

Вопрос 4. Почему важно применять полевую шину с одобрения пользователя в проекте СПАЗ/SIS?

a) Это позволяет снизить затраты на проектирование.

b) Это обеспечивает совместимость с другими системами информационного обеспечения.

c) Это гарантирует безопасность и надежность передачи сигналов.

d) Это не имеет значения для безопасности системы.

Ответ: b, c.

Объяснение.

b) Применение полевой шины с одобрения пользователя обеспечивает совместимость с другими системами и компонентами, что важно для интеграции СПАЗ в АСУ предприятия.

c) Это также гарантирует безопасность и надежность передачи сигналов, что критично для функционирования системы безопасности.

Тест 11.7. Логическая часть СПАЗ.

Вопрос 1. Какие данные должен предоставить поставщик при проектировании логической части СПАЗ?

- a) Перечень видов отказов.
- b) Интенсивность скрытых отказов.
- c) Методики или источники получения данных о отказах.
- d) Список всех используемых компонентов системы.

Ответ: a, b, c.

Объяснение.

a) Поставщик должен предоставить перечень видов отказов для анализа рисков и разработки защитных мер.

b) Интенсивность скрытых отказов важна для понимания надежности системы и планирования диагностики.

c) Методики или источники получения данных о отказах позволяют обеспечить прозрачность и возможность анализа состояния системы.

Вопрос 2. Каковы основные требования к средствам диагностики в производственной электронной системе?

a) Средства диагностики должны быть встроены или основаны на прикладных программах.

b) Диагностика должна проводиться только вручную.

c) Средства диагностики должны обеспечивать автоматическое выявление всех видов отказов.

d) Диагностика должна быть доступна для пользователей без специальной подготовки.

Ответ: a, c.

Объяснение.

a) Встроенные или прикладные средства диагностики позволяют оперативно выявлять и устранять неисправности системы.

c) Автоматическое выявление отказов существенно повышает надежность системы и снижает время простоя.

Вопрос 3. Какое требование касается перезапуска процессов после потери питания?

a) Процесс должен перезапускаться автоматически после восстановления питания.

b) Не следует допускать перезапуска процесса после потери питания, если это не требуется.

c) Перезапуск должен осуществляться только вручную.

d) Перезапуск процессов не имеет значения для безопасности системы.

Ответ: b, c.

Объяснение.

b) Это требование предотвращает возможные аварийные ситуации, которые могут возникнуть при неконтролируемом перезапуске.

c) Ручной перезапуск позволяет оператору убедиться в безопасности условий перед возобновлением работы.

Вопрос 4. Каковы основные функции панели аварийного останова в системе?

a) Сигнализация на дистанционной панели при закрытии клапана.

b) Срабатывание дистанционной панели при активации местной панели.

c) Индикатор состояния местной панели «Сработала/Норма».

d) Обеспечение управления всеми процессами в системе.

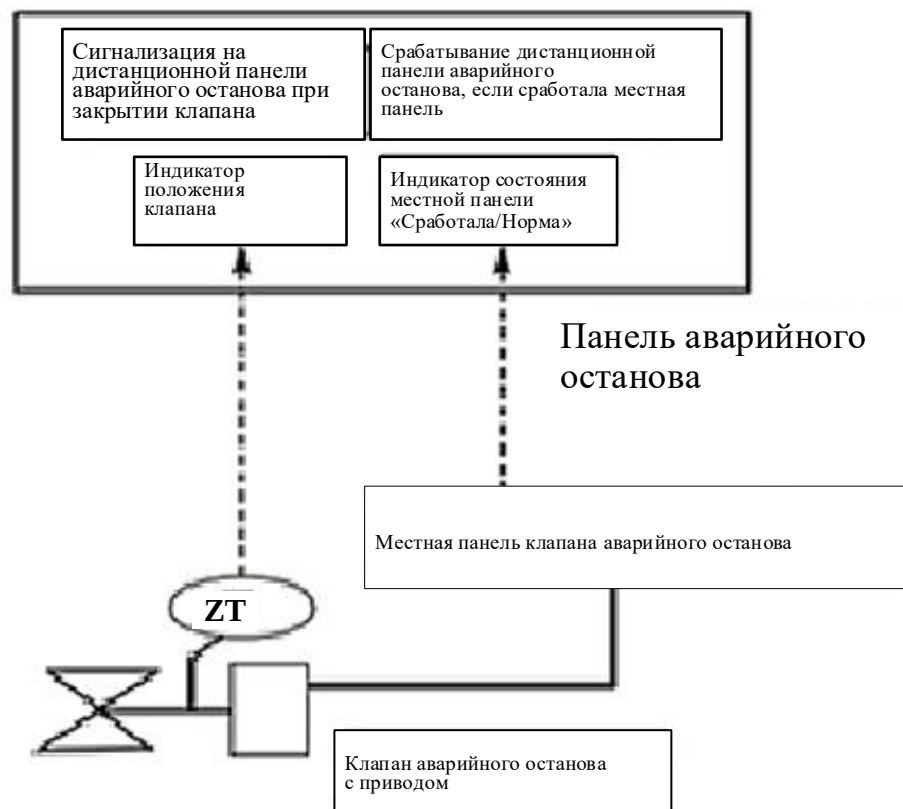
Ответ: a, b, c.

Объяснение.

a) Сигнализация (рис.11.6) позволяет немедленно информировать операторов о критических состояниях [28].

b) Срабатывание дистанционной панели при активации местной панели обеспечивает дублирование сигналов и повышает безопасность.

c) Индикатор состояния помогает операторам быстро оценить текущее состояние системы и принимать решения.



Вопрос 5. Каковы требования к разделению АСДУ (базовая система управления процессами) и логической части СПАЗ/SIS?

а) АСДУ и логическая часть СПАЗ/SIS должны быть разделены для повышения безопасности.

б) Исключения допускаются только для комбинированных систем, отвечающих требованиям по SIL.

с) Разделение не имеет значения, если системы работают корректно.

д) Все системы должны быть интегрированы для повышения эффективности.

Ответ: а, б.

Объяснение.

а) Разделение АСДУ и логической части СПАЗ/SIS минимизирует риски, связанные с возможными сбоями.

б) Исключения для комбинированных систем, таких как управление горелкой, должны быть обоснованы и соответствовать строгим требованиям безопасности.

В стандарте указывается, что.

- интеллектуальные датчики должны быть «защищены от записи»;

- системы с магистралью не следует использовать, если не получено «одобрение пользователя».

- датчики СПАЗ/SIS должны быть отделены от датчиков АСДУ. Исключения.

- резервированные датчики и резервированная защита;

- диагностика датчика должна соответствовать заданному SIL..

- отдельный клапан останова в системах с SIL 3;

Основной принцип СПАЗ/SIS— это «последний рубеж обороны», который должен сработать, когда основная система управления (АСДУ) не справилась. Представьте, что АСДУ – это водитель, а СПАЗ/SIS – это подушка безопасности и ремни. Они должны быть независимы, чтобы сработать, даже если водитель растерялся.

Почему это требование такое строгое:

Чтобы избежать общей точки отказа: Если АСДУ и СПАЗ/SIS используют общий процессор или источник питания, сбой в этом общем элементе может вывести из строя обе системы одновременно. Это лишит производство последней защиты .

Для предотвращения человеческой ошибки: Программист, внося изменения в программу АСДУ, по ошибке может затронуть и записи в логику безопасности. Разделение систем позволяет защитить логику

СПАЗ/SIS от несанкционированных изменений –это и значит «защищены от записи».

На практике это реализуется с помощью паролей, ключей-переключателей и строгих процедур управления доступом, чтобы никто не мог случайно или намеренно «отключить» защиту.

«Одобрение пользователя» – это не просто чья-то подпись. Это целый официальный процесс, в котором ответственные инженеры и специалисты по безопасности анализируют риски и документально подтверждают, что они понимают все последствия использования общей сети (магистральной) для АСДУ и СПАЗ/SIS и принимают на себя эту ответственность.

Когда можно совмещать системы

Вариант ответа b как раз про эти строго регламентированные исключения. Совмещение АСДУ и СПАЗ/SIS в одном устройстве (так называемые «комбинированные системы») возможно, но только при одновременном выполнении жестких условий:

Устройство должно иметь сертификат SIL, подтверждающий, что оно по своей надежности подходит для функций безопасности.

Должна быть проведена тщательная оценка рисков, доказывающая, что общие причины отказов (например, общий блок питания) учтены и сведены к приемлемому минимуму.

Должны быть реализованы усиленные меры защиты от изменений и независимые каналы диагностики.

Таким образом, требование разделения – это не прихоть, а проверенный мировой практикой способ обеспечить независимый и надежный последний уровень защиты. Все исключения из этого правила строго регламентированы и требуют глубокого технического обоснования.

Для получения дополнительной информации см. [28].

Тест 11.8. Полевые устройства.

Вопрос 1. В каких случаях применяется включение СПАЗ при срабатывании полевых устройств?

- a) В системах противопожарной защиты.
- b) В системах управления освещением.
- c) В системах газовой защиты.
- d) В системах управления машинами.

Ответ: a, c, d.

Объяснение.

a) В системах противопожарной защиты срабатывание полевых устройств должно обеспечивать немедленное действие для предотвращения распространения огня.

c) В системах газовой защиты включение полевых устройств позволяет быстро реагировать на утечки газа и активировать защитные меры.

d) В системах управления машинами мощные электроприводы или переключатели мощности могут быть активированы для управления работой оборудования.

Вопрос 2. Какой метод обеспечивает цельность системы в проектировании СПАЗ/SIS (систем безопасности)?

- a) Использование контуров управления, чувствительных по току.
- b) Применение стандартных проводных линий для всех устройств.
- c) Обеспечение дублирования всех полевых устройств.
- d) Использование метода обеспечения цельности системы, рекомендованного ISA.

Ответ: a, d.

Объяснение.

a) Контуров управления, чувствительные по току, позволяют контролировать состояние системы и обеспечивать надежность работы полевых устройств.

d) Метод обеспечения цельности системы, рекомендованный ISA, включает в себя различные подходы и практики, направленные на повышение надежности и безопасности системы.

Вопрос 3. Каковы требования к удаленным системам ввода/вывода в логической подсистеме?

- a) Они должны быть интегрированы в общую систему управления.
- b) Необходимо использовать специальные проводные линии для каждого полевого устройства.
- c) Удаленные системы не требуют защиты от помех.
- d) Удаленные системы должны быть доступны для диагностики и обслуживания.

Ответ: a, b, d.

Объяснение.

a) Интеграция удаленных систем ввода/вывода в общую систему управления позволяет обеспечить согласованность данных и управление процессами.

b) Использование специальных проводных линий для каждого полевого устройства обеспечивает надежную передачу сигналов и предотвращает помехи.

d) Доступность удаленных систем для диагностики и обслуживания критична для поддержания надежности и быстрого реагирования на неисправности.

Отдельные традиционные аналоговые и дискретные каналы связи, безусловно, проверены временем. Но у них есть внутренние ограничения, которые становятся все более заметными по мере усложнения технологических процессов:

Ограниченность диагностики: Аналоговый сигнал 4-20 мА может сообщить о самом параметре (например, давлении), но ему сложно передать информацию о состоянии самого датчика. Цифровой же протокол может передавать не только измеренное значение, но и данные о его достоверности, диагностике неисправностей, текущей конфигурации и т.д.

Стоимость и сложность инфраструктуры: Каждый аналоговый датчик требует отдельной пары проводов, что приводит к огромным затратам на кабель, монтаж и проектирование. Цифровые полевые шины (например, Profibus PA, Foundation Fieldbus H1) позволяют по одной паре проводов соединять множество устройств, что естественно снижает стоимость коммуникационной среда.

Современное предприятие – это единое информационное пространство. Цифровая полевая среда, построенная на стандартах вроде MQTT или с использованием специализированных IoT-платформ, позволяет СПАЗ не быть «островком», а стать частью общей системы прогнозного обслуживания и анализа данных.

Для наглядности рассмотрим ключевые различия двух подходов в контексте требований к СПАЗ (табл. 11.3).

Таблица 11.3. Сравнительная таблица. Аналоговый и цифровой подход

Критерий	Классический аналоговый/дискретный подход	Цифровая полевая среда
Диагностика	Основной фокус на контроль целостности шлейфа (обрыв, КЗ). Сложно обнаружить дрейф характеристик датчика.	Расширенная диагностика самого устройства : «залипание» значения, предупреждение о загрязнении, самодиагностика электроники.
Надежность	Высокая, проверенная. Резервирование реализуется дублированием каналов на аналоговом уровне,	Высокая, но требует защиты от киберугроз . Позволяет реализовать логическое и аппаратное резервирование на новой основе.
Стоимость	Высокие капитальные затраты на кабельную инфраструктуру. Низкие операционные затраты.	Низкие капитальные затраты на кабель и монтаж. Возможность снижения операционных затрат за счет предиктивного анализа .

Крите- рий	Классический аналого- вый/дискретный подход	Цифровая полевая среда
Инфор- матив- ность	Передача одного основного параметра.	Передача значения параметра, его статуса (достоверно/недостоверно) и диагностической информации.

Все компоненты цифровой системы (датчики, актуаторы, контроллеры) должны иметь сертификаты соответствия стандартам функциональной безопасности, таким как МЭК 61508 и МЭК 61511, для требуемого уровня полноты безопасности (SIL).

Приоритет безопасности: Архитектура системы должна гарантировать, что команды управления, сформированные алгоритмами защиты, имеют безусловный приоритет над любыми другими командами, включая команды оперативного персонала.

Защита от киберугроз: Цифровая система должна быть изолирована от непроверенных сетей, иметь средства защиты от несанкционированного доступа и построена с учетом требований кибербезопасности для АСУ ТП.

Вопрос 4. Каковы преимущества применения специальных проводных линий для полевых устройств?

- a) Упрощение монтажа системы.
- b) Повышение надежности передачи сигналов.
- c) Снижение затрат на проектирование.
- d) Защита от электромагнитных помех.

Ответ: b, d.

Объяснение.

b) Специальные проводные линии обеспечивают более надежную передачу сигналов, что критично для работы полевых устройств в системах безопасности.

d) Использование специализированных проводов помогает защитить систему от электромагнитных помех, что важно для обеспечения стабильной работы.

Вопрос 5. В каких случаях использование систем с магистралью не рекомендуется без получения одобрения пользователя?

- a) При наличии интеллектуальных датчиков.
- b) При использовании резервированных датчиков.
- c) В системах, где требуется высокая степень надежности.
- d) В системах с магистралью, которые могут подвергаться внешним воздействиям.

Ответ: a, c, d.

Объяснение.

a) Интеллектуальные датчики требуют особых условий эксплуатации и защиты от записи, что делает их использование в системах с магистралью рискованным без одобрения.

с) В системах, где требуется высокая степень надежности, важно тщательно оценить риски и обеспечить соответствие требованиям, прежде чем использовать магистральные системы.

д) Магистральные системы могут быть подвержены внешним воздействиям, поэтому их применение должно быть тщательно обосновано и одобрено пользователем.

Вопрос 8. Каковы требования к диагностике в СПАЗ?

а) Диагностика должна соответствовать заданному SIL.

б) Для SIL 3 требуется отдельный клапан останова.

с) SIL 1 и SIL 2 не требуют пересмотра.

д) Совместное использование регулирующего клапана АСДУ не поощряется.

Ответ: а, b, d.

Объяснение.

а) Соответствие диагностики заданному SIL обеспечивает необходимый уровень контроля и надежности системы.

б) Наличие отдельного клапана останова в системах с SIL 3 критично для обеспечения безопасности и быстрого реагирования на аварийные ситуации.

д) Совместное использование регулирующего клапана АСДУ не рекомендуется, так как это может привести к снижению надежности и безопасности системы.

Устройства должны быть разработаны в соответствии с ГОСТ Р МЭК 61508-2.2012 (требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью) и ГОСТ Р МЭК 61508-3.2010 (требования к ПО) ГОСТ Р МЭК 61511-2.2018.

Тест 11.9. Человеко-машинные интерфейсы.

Вопрос 1. Какое требование должно быть соблюдено для обеспечения надежности систем безопасности при нарушении интерфейса?

а) Нарушение интерфейса не должно влиять на готовность СПАЗ/SIS.

б) Человек должен иметь возможность вручную управлять системой в случае сбоя интерфейса.

с) Все операции должны быть зафиксированы в журнале.

д) Необходимо обеспечить средства резервирования работы.

Ответ: а, d.

Объяснение.

а) Нарушение интерфейса не должно влиять на готовность СПАЗ/SIS, чтобы система могла продолжать функционировать даже в условиях сбоя.

д) Обеспечение средств резервирования работы критически важно для поддержания функционирования системы в случае возникновения проблем с интерфейсом.

Вопрос 2. Какие меры необходимо предпринять для обеспечения надежности интерфейсов в системах безопасности?

- a) Регулярное обновление программного обеспечения.
- b) Обучение обслуживающего персонала.
- c) Ограничение доступа к интерфейсам.
- d) Проведение регулярных тестов и проверок системы.
- e) Установка дополнительных устройств для мониторинга.

Ответ: a, b, c, d, e.

Объяснение.

a) Регулярные обновления программного обеспечения помогают устранить уязвимости и повысить безопасность.

b) Обучение персонала критически важно для правильного использования интерфейсов и предотвращения ошибок.

c) Ограничение доступа к интерфейсам защищает систему от несанкционированного вмешательства.

d) Проведение регулярных тестов и проверок системы позволяет выявить и устранить потенциальные проблемы.

e) Установка дополнительных устройств для мониторинга помогает контролировать состояние системы и оперативно реагировать на сбои.

Вопрос 3. Какую информацию должен предоставлять человеко-машинный интерфейс для операторов?

- a) Полную информацию о состоянии СПАЗ/SIS.
- b) Доступ к изменению прикладного программного обеспечения.
- c) Информацию о текущих процессах и их состоянии.
- d) Возможность выбора логической функции для периодических процессов.

Ответ: a, c, d.

Объяснение.

a) Операторы должны иметь доступ к полной информации о состоянии СПАЗ/SIS для принятия обоснованных решений.

c) Информация о текущих процессах и их состоянии помогает операторам в мониторинге и управлении системой.

d) Возможность выбора логической функции для периодических процессов позволяет операторам адаптировать систему под текущие нужды, однако это должно быть сделано с соблюдением всех мер безопасности.

Вопрос 4. Каковы ограничения на изменение прикладного программного обеспечения СПАЗ/SIS?

a) Оператор может изменять программное обеспечение через операторский интерфейс.

b) Изменения должны осуществляться только через интерфейс обслуживающего или технического персонала.

c) Необходимо фиксировать все изменения в журнале.

d) Оператор может временно отключить защитные функции для внесения изменений.

Ответ: b, c.

Объяснение.

b) Изменения в прикладном программном обеспечении должны осуществляться только через интерфейс обслуживающего или технического персонала, чтобы предотвратить несанкционированные изменения и обеспечить безопасность системы.

c) Фиксация всех изменений в журнале необходима для обеспечения прозрачности и возможности аудита.

Вопрос 5. Какие функции должны быть предусмотрены для операторов и АСДУ в случае периодических процессов?

a) Возможность выбора подходящей логической функции.

b) Доступ к изменению всех параметров системы.

c) Функции выборочной записи.

d) Автоматическое управление без участия оператора.

Ответ: a, c.

Объяснение.

a) Операторы и АСДУ должны иметь возможность выбирать подходящую логическую функцию для адаптации системы к текущим условиям.

c) Функции выборочной записи необходимы для обеспечения контроля и возможности анализа данных, что важно для поддержания безопасности и надежности системы.

Вопрос 6. Какие элементы должны быть включены в границы интерфейса обслуживающего персонала?

a) Инструкции и средства программного обеспечения.

b) Устройства для автоматического управления.

c) Терминалы программирования.

d) Средства диагностирования.

e) Устройства калибровки.

Ответ: a, c, d, e.

Объяснение.

a) Инструкции и средства программного обеспечения необходимы для корректного выполнения задач обслуживающим персоналом.

c) Терминалы программирования позволяют оператору взаимодействовать с системой и вносить необходимые изменения.

d) Средства диагностирования помогают в выявлении и устранении неисправностей, что критично для поддержания работоспособности системы.

e) Устройства калибровки необходимы для обеспечения точности измерений и корректной работы системы.

Вопрос 7. Что должно быть учтено при обеспечении безопасности доступа к интерфейсу обслуживания?

- а) Режимы эксплуатации СПАЗ/SIS.
- б) Наличие физического доступа к оборудованию.
- с) Диагностика СПАЗ/SIS и обслуживание неисправностей.
- д) Добавление, удаление или внесение изменений в программное обеспечение.

е) Данные, необходимые для выявления неисправностей.

Ответ: а, с, д, е.

Объяснение.

а) Режимы эксплуатации СПАЗ/SIS должны быть четко определены для предотвращения несанкционированного доступа.

с) Диагностика и обслуживание неисправностей требуют безопасного доступа к системам для их эффективного функционирования.

д) Изменения в программном обеспечении должны контролироваться, чтобы избежать потенциальных угроз безопасности.

е) Данные для выявления неисправностей необходимы для быстрого реагирования на проблемы, что также требует безопасного доступа.

Вопрос 8. Какой из следующих факторов не должен влиять на отказобезопасное функционирование СПАЗ/SIS?

- а) Отказ интерфейса.
- б) Защитные сообщения от других источников энергии.
- с) Неправильные действия обслуживающего персонала.
- д) Неполадки в программном обеспечении.

Ответ: а, б.

Объяснение.

а) Отказ интерфейса не должен влиять на отказобезопасное функционирование системы, поскольку это критично для обеспечения безопасности.

б) Защитные сообщения от других источников энергии могут помочь системе оставаться в рабочем состоянии, даже если интерфейс выходит из строя.

с) и д) Неправильные действия обслуживающего персонала и неполадки в программном обеспечении могут повлиять на функционирование системы, но не должны влиять на ее отказобезопасность, если система правильно спроектирована.

См. ГОСТ Р МЭК 62 682, ГОСТ Р МЭК 61511-2 2018 п. А.11.7.

Тест 11.10. Источники питания и распределение питания устройств ввода/вывода.

Вопрос 1. Какие требования должны соблюдаться при проектировании источников питания для СПАЗ?

а) Источники питания должны соответствовать требованиям надежности и полноты безопасности.

b) Резервирование источников питания всегда должно быть обязательным.

c) Переход на резервные источники питания должен быть безударным.

d) Диагностика должна предотвращать использование системы при отказе питания.

e) Источники питания могут быть любых типов, без учета их характеристик.

Ответ: a, c, d.

Объяснение.

a) Источники питания должны соответствовать требованиям надежности и полноты безопасности, чтобы обеспечить стабильную работу системы и защиту от сбоев.

c) Переход на резервные источники питания должен быть безударным, чтобы избежать резких колебаний напряжения, которые могут повредить оборудование.

d) Диагностика должна предотвращать использование системы при отказе питания, что позволяет избежать потенциальных аварий и небезопасных ситуаций.

Вопрос 2. Какие меры могут быть предприняты для обеспечения надежности источников питания в СПАЗ?

a) Использование резервирования модулей питания.

b) Применение совместно используемых проводов для упрощения схемы.

c) Фильтрация и защита питания от резких скачков.

d) Защита электроники от радиочастотных и электромагнитных излучений.

e) Игнорирование состояния прерывателя цепи.

Ответ: a, c, d.

Объяснение.

a) Резервирование модулей питания позволяет обеспечить бесперебойную работу системы в случае отказа основного источника.

c) Фильтрация и защита питания от резких скачков защищает систему от повреждений, вызванных перегрузками.

d) Защита электроники от радиочастотных и электромагнитных излучений важна для предотвращения помех и сбоев в работе системы.

Вопрос 3. Каковы основные принципы распределения питания для устройств ввода/вывода?

a) Использование совместно используемых проводов для упрощения установки.

b) Положительная ветвь цепи защиты от превышения по току и напряжению.

c) Плавающее или заземленное в одной точке питание входов/выходов.

- d) Устранение ложных путей заземления.
- e) Применение любых схем подключения, не учитывающих требования безопасности.

Ответ: b, c, d.

Объяснение.

b) Положительная ветвь цепи защиты от превышения по току и напряжению необходима для защиты оборудования от повреждений.

c) Плавающее или заземленное в одной точке питание входов/выходов помогает избежать проблем с заземлением и ложными срабатываниями.

d) Устранение ложных путей заземления критично для предотвращения возможных коротких замыканий и других аварийных ситуаций в системе.

Вопрос 4. Какой подход следует использовать для обеспечения надежности и безопасности системы при проектировании источников питания?

a) Применение только одного источника питания без резервирования.

b) Использование принципа «включения питания для срабатывания» в тяжелых случаях.

c) Игнорирование диагностики состояния источника питания.

d) Регулярное тестирование и проверка системы питания.

e) Обеспечение физической защиты источников питания от внешних воздействий.

Ответ: b, d, e.

Объяснение.

b) Использование принципа «включения питания для срабатывания» в тяжелых случаях позволяет гарантировать, что система будет работать даже в условиях отказа основного источника.

d) Регулярное тестирование и проверка системы питания необходимы для выявления потенциальных проблем до того, как они станут критическими.

e) Обеспечение физической защиты источников питания помогает предотвратить отказ ИП.

Типичную цепь входа следует построить так, чтобы обеспечить, что случайное заземление заставит входной сигнал перейти в состояние «ноль», как показано на следующем рисунке 11.7 [28]/

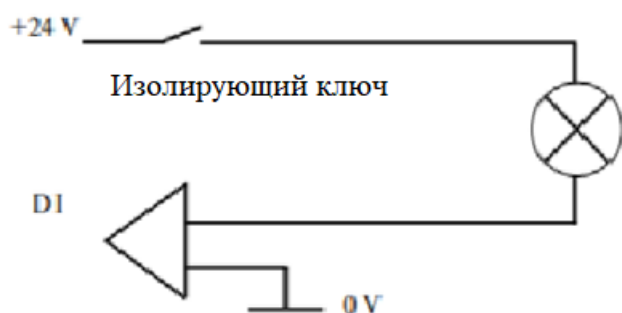


Рис.11.7. Конфигурация цепи ввода обеспечивающая безопасный отказ при случайном заземлении

Для получения дополнительной информации см. [28].

Тест 11.11. Влияние окружающей среды.

Каждый вопрос имеет несколько правильных ответов, и к каждому из них прилагается подробное объяснение.

Вопрос 1. Какие факторы окружающей среды могут негативно повлиять на работу СПАЗ?

- а) Высокая температура.
- б) Низкая влажность.
- с) Вибрации.
- д) Радиочастотные и электромагнитные излучения.
- е) Протекающие крыши и дренажные потоки.

Ответ: а, с, д, е.

Объяснение.

а) Высокая температура может привести к перегреву компонентов системы, что может вызвать сбои в работе или даже повреждение оборудования.

с) Вибрации могут негативно сказаться на механических частях системы, вызывая их износ или повреждение.

д) Радиочастотные и электромагнитные излучения могут вызывать помехи в работе электроники, что может привести к неправильной работе системы.

е) Протекающие крыши и дренажные потоки создают риск затопления оборудования, что может привести к коротким замыканиям и отказам.

Вопрос 2. Какие меры следует предпринять для защиты СПАЗ от неблагоприятных условий окружающей среды?

а) Установить кондиционеры и фильтры для улучшения условий.

б) Разместить оборудование в залах управления, где есть риск затопления.

с) Применять вентиляцию и охлаждение панелей.

д) Игнорировать спецификации требований к окружающей среде для компонентов.

е) Проверять спецификации требований к окружающей среде для всех компонентов системы.

Ответ: а, с, е.

Объяснение.

а) Установка кондиционеров и фильтров помогает поддерживать оптимальные условия работы для оборудования, что снижает риск повреждений.

с) Применение вентиляции и охлаждения панелей позволяет эффективно удалять избыточное тепло и поддерживать стабильную температуру.

е) Проверка спецификаций требований к окружающей среде для компонентов системы позволяет убедиться, что они соответствуют условиям эксплуатации и обеспечивают надежную работу.

Вопрос 3. Каковы основные требования к проектированию СПАЗ в отношении защиты от окружающей среды?

а) Использование компонентов, устойчивых к высоким температурам.

б) Размещение оборудования в местах с высоким уровнем влажности без защиты.

с) Защита от электромагнитных помех.

д) Игнорирование требований к вибрациям при проектировании.

е) Установка оборудования вдали от потенциальных источников затопления.

Ответ: а, с, е.

Объяснение.

а) Использование компонентов, устойчивых к высоким температурам, помогает предотвратить перегрев и сбои в работе системы.

с) Защита от электромагнитных помех важна для обеспечения надежной работы электроники в условиях воздействия внешних излучений.

е) Установка оборудования вдали от потенциальных источников затопления минимизирует риски, связанные с повреждением от воды.

Вопрос 4. Каковы последствия игнорирования влияния окружающей среды на проектирование СПАЗ?

а) Повышение надежности системы.

б) Увеличение вероятности отказов оборудования.

с) Увеличение затрат на обслуживание и ремонт.

д) Улучшение условий эксплуатации системы.

е) Увеличение времени простоя системы.

Ответ: б, с, е.

Объяснение.

б) Игнорирование влияния окружающей среды может привести к увеличению вероятности отказов оборудования из-за неблагоприятных условий.

с) Увеличение затрат на обслуживание и ремонт связано с частыми поломками и необходимостью замены компонентов, поврежденных из-за воздействия окружающей среды.

е) Увеличение времени простоя системы происходит из-за частых сбоев и необходимости в ремонте, что негативно сказывается на общей эффективности работы.

Тест 11.12. Прикладная логика.

Вопросы имеют несколько правильных ответов, и к каждому из них прилагается подробное объяснение.

Вопрос 1. Какие из следующих требований должны быть соблюдены при проектировании прикладного программного обеспечения логической части СПАЗ/SIS?

а) Использование только той логики, которая определяется пользователем под управлением программы формальной проверки и допуска.

б) Разрешение пользователю модифицировать встроенные программы и утилиты.

с) Предоставление ясной и сжатой документации на систему.

д) Все программы СПАЗ/SIS должны управляться программой формальной проверки и допуска.

е) Ответственность за формальную проверку и управление допуском встроенного программного обеспечения лежит на пользователе.

Ответ: а, с, d.

Объяснение.

а) Использование логики, определяемой пользователем под управлением программы формальной проверки, обеспечивает соответствие требованиям безопасности и минимизирует риски ошибок.

с) Ясная и сжатая документация необходима для понимания системы и ее функционирования, что упрощает обучение и эксплуатацию.

д) Управление всеми программами СПАЗ/SIS программой формальной проверки и допуска гарантирует, что они соответствуют необходимым стандартам безопасности и функциональности.

Вопрос 2. Кто несет ответственность за формальную проверку и управление допуском встроенного программного обеспечения?

а) Пользователь.

б) Изготовитель.

с) Технический специалист.

д) Внешний аудитор.

е) Команда разработки.

Ответ б.

Объяснение.

б). Ответственность за формальную проверку и управление выпуском встроенного программного обеспечения лежит на изготовителе, который должен обеспечить соответствие программного обеспечения установленным стандартам и требованиям безопасности.

Вопрос 3. Какое требование касается модификации встроенных программ и утилит пользователем?

а) Пользователь может модифицировать встроенные программы при необходимости.

б) Пользователь не имеет права модифицировать встроенные программы и утилиты.

с) Пользователь может изменять только документацию.

д) Модификация разрешена только в рамках тестирования.

е) Модификация встроенных программ допускается, если это не нарушает безопасность системы.

Ответ б.

Объяснение.

б) Пользователь не имеет права модифицировать встроенные программы и утилиты, чтобы избежать потенциальных рисков безопасности и обеспечить стабильность работы системы.

Вопрос 4. Какую документацию должен получить пользователь по прикладной логике?

а) Документацию, составленную в ясной и сжатой форме.

б) Полную техническую документацию без упрощений.

с) Документацию, составленную только на английском языке.

д) Документацию, содержащую все возможные изменения и модификации.

е) Документацию, соответствующую требованиям формальной проверки.

Ответ: а, е.

Объяснение.

а) Документация должна быть ясной и сжатой, чтобы пользователи могли легко понять логику системы и её функционирование.

е) Документация, соответствующая требованиям формальной проверки, необходима для обеспечения соответствия стандартам безопасности и функциональности.

Вопрос 5. Каким образом программа управления формальной проверкой и выпуском прикладного программного обеспечения должна обслуживаться?

а) Программой, разработанной пользователем.

б) Программой, обслуживаемой изготовителем.

с) Программой, которая может быть изменена пользователем.

д) Программой, которая должна быть поддерживаемой только техническими специалистами.

е) Программой, которая должна обслуживаться пользователем.

Ответ б.

Объяснение.

б) Программа управления формальной проверкой и выпуском прикладного программного обеспечения должна обслуживаться изготовителем, чтобы гарантировать соблюдение всех стандартов и требований.

См. ГОСТ Р МЭК 61511-2 -2018 А12, ГОСТ Р МЭК 61508-3-2013.

11.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 11.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов. Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 11».

Тест 11.13. Проводка полевого устройства к системе ввода/вывода.

Каждое полевое устройство должно иметь собственную выделенную проводку к системе ввода/вывода. Но есть исключения из этого правила:

1. Несколько дискретных датчиков подключены последовательно к одному входу, и все датчики контролируют одно и то же состояние процесса (например, перегрузки двигателя).
2. Несколько конечных элементов подключены к одному выходу.
3. Используется полевая шина на основе стандарта МЭК 1158 для объединения нескольких полевых приборов в сеть.

Вопрос 1. Какие варианты ответов правильные?

- a) Все утверждения верны, специальных требований нет.
- b) Утверждение 3 верно, утверждения 1 и 2 неверны.
- c) Утверждение 2 верно, утверждения 1 и 3 неверны.
- d) Утверждения 1 и 2 верны, утверждение 3 неверно.
- e) Ни одно из вышеуказанных утверждений не верно, исключений из правила нет.

Тест 11.14. Сертификат соленоидного клапана.

Сторонняя организация выдала сертификат функциональной безопасности для соленоидного клапана. В сертификате указано, что клапан может использоваться без резервирования в приложениях уровня SIL 3 и даже соответствует требованиям SIL 4 при использовании с аппаратной устойчивостью к отказам уровня 1.

Объясните, почему пользователь этого соленоидного клапана в процессной промышленности не может просто принять этот сертификат без дополнительной информации.

Вопрос 1. Почему пользователь соленоидного клапана не может просто принять сертификат функциональной безопасности, выданный сторонней организацией, без дополнительной информации?

- А) Сертификат не учитывает условия эксплуатации клапана.
- В) Сертификат выдан только для одного типа применения.
- С) Сертификат не содержит информации о Тестировании клапана.
- Д) Все вышеперечисленное.

Вопрос 2.

Что еще должен сделать пользователь, чтобы убедиться в соответствии соленоидного клапана требованиям безопасности?

- А) Провести независимую оценку клапана.
- В) Изучить документацию производителя.
- С) Проверить наличие сертификатов на другие компоненты системы.
- Д) Все вышеперечисленное.

Тест 11.15. Расчет суммарной интенсивности опасных отказов исполнительного механизма.

Система функциональной безопасности (СПАЗ) [24] использует один пневматический исполнительный механизм, состоящий из трехходового прямодействующего золотникового соленоидного клапана 3/2, пружинного возвратно-шестерёнчатого привода и трехэксцентрикового дискового затвора. Ситуация находится в режиме близком к срабатыванию. Какова суммарная интенсивность опасных отказов исполнительного механизма?

Вопрос 1. Какова интенсивность опасных отказов трехходового прямодействующего золотникового соленоидного клапана 3/2 согласно стандартным справочным данным?

- А) 240 FIT.
- В) 750 FIT.
- С) 900 FIT.
- Д) 1000 FIT.

Вопрос 2. Какова интенсивность опасных отказов пружинного возвратно-шестерёнчатого привода согласно стандартным справочным данным?

- А) 240 FIT.
- В) 900 FIT.
- С) 750 FIT.
- Д) 500 FIT.

Вопрос 3. Какова интенсивность опасных отказов трехэксцентрикового дискового затвора в режиме близком к срабатыванию согласно стандартным справочным данным?

- А) 240 FIT.
- В) 900 FIT.
- С) 750 FIT.
- Д) 100 FIT.

Вопрос 4. Как рассчитывается суммарная интенсивность опасных отказов исполнительного механизма?

- A) Сумма всех интенсивностей отказов.
- B) Умножение всех интенсивностей отказов.
- C) Разность максимальной и минимальной интенсивностей отказов.
- D) Среднее арифметическое интенсивностей отказов.

Вопрос 5. Какова суммарная интенсивность опасных отказов исполнительного механизма, если известны интенсивности. клапан - 240 FIT, привод - 900 FIT, затвор - 750 FIT?

- A) 1880 FIT.
- B) 240 FIT.
- C) 750 FIT.
- D) 900 FIT.

Тест 11.16. Расчет вероятности опасного отказа пневматического ИУ.

В SIF используется один узел пневматического исполнительного элемента, состоящий из золотникового электромагнитного клапана 3/2 с пилотным управлением [24], кулисного механизма с пружинным возвратом, привода и поплавкового шарового клапана с возможностью срабатывания.

Ситуация близка к срабатыванию.

Все устройства прошли аттестацию для применения. Все устройства сертифицированы по стандарту МЭК 61508, систематическая возможность SC 3. MRT на неисправности, обнаруженные в ходе контрольных испытаний составляет 24 часа. После установки сборку можно полностью протестировать.

Контрольное тестирование – планируется каждые 2 года во время остановки технологического процесса.

Доказательное испытание – выполняется вскоре после остановки процесса при сборке конечного элемента близкой к рабочей температуре; таким образом, предполагается, что СРТ составит 93%.

Применение продлится 10 лет до полного капитального ремонта. Определить PFDavg окончательной сборки ИУ? Выполнить расчет PFDavg для пневматического исполнительного элемента

Вопрос 1. Какова частота отказов золотникового электромагнитного клапана 3/2 с пилотным управлением?

- A) 720 FITS.
- B) 1250 FITS.
- C) 900 FITS.
- D) 2870 FITS.

Вопрос 2. Какова частота отказов привода с кулисным механизмом с пружинным возвратом?

- A) 720 FITS.
- B) 1250 FITS.
- C) 900 FITS.
- D) 2870 FITS.

Вопрос 3. Какова частота отказов поплавкового шарового клапана в режиме близком к срабатыванию?

- A) 720 FITS.
- B) 1250 FITS.
- C) 900 FITS.
- D) 2870 FITS.

Вопрос 4. Какова формула для расчета PFD_{avg} в данной системе?

- A) $PFD_{avg} = \lambda_{DU} \cdot MRTDU$.
- B) $PFD_{avg} \approx \lambda_{DD} \cdot MRTDD + CPT \cdot \lambda_{DU} \cdot (TI/2 + MRTDU) + (1 - CPT) \cdot \lambda_{DU} \cdot MT/2$.
- C) $PFD_{avg} = \lambda_{DU} + CPT$.
- D) $PFD_{avg} = \lambda_{DU} \cdot TI + MRTDU$.

Вопрос 5. Какова средняя вероятность отказа (PFD_{avg}) окончательной сборки ИУ?

- A) 0,0201.
- B) 0,0322.
- C) 0,0450.
- D) 0,0500.

Тест 11.17 Отказы по общей причине [28] .

Вопрос 1. Что такое отказы по общей причине?

- a) Отказы, вызванные случайными факторами.
- b) Отказы, возникающие из-за одинаковых дефектов в нескольких компонентах системы (рис.11.7).
- c) Отказы, которые происходят только в сложных устройствах.
- d) Отказы, возникающие из-за неправильной эксплуатации системы.

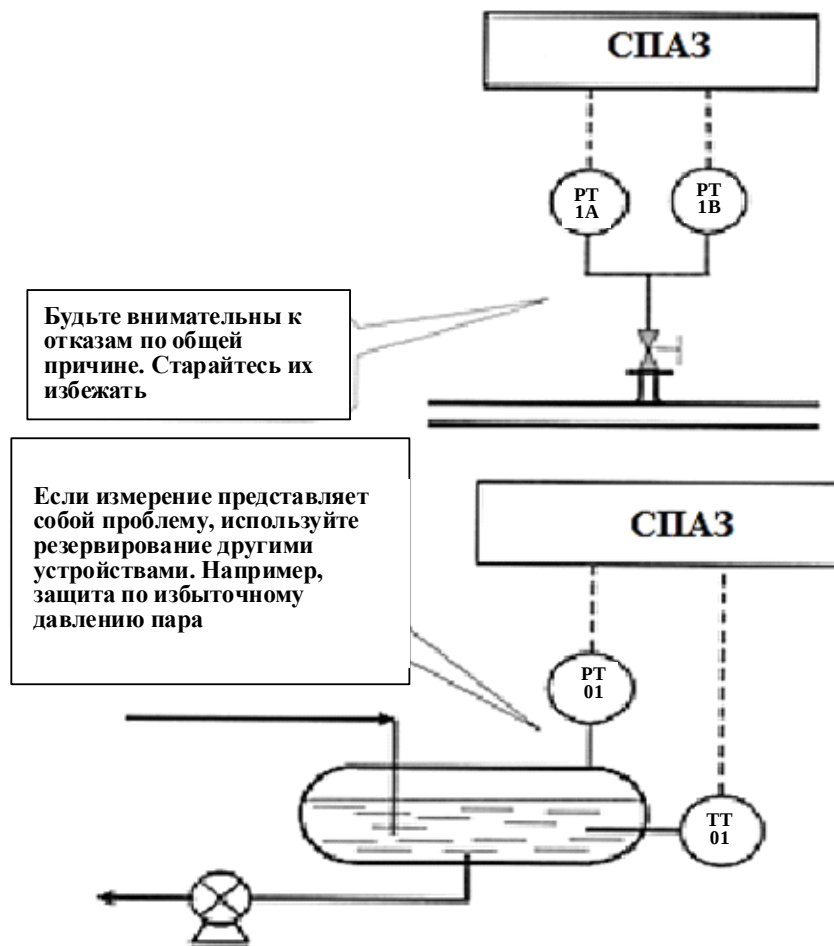


Рис.11.7. Отказы по общей причине и пример решения проблемы

Вопрос 2. Какой из следующих видов дефектов документации не следует игнорировать при проектировании СПАЗ?

- а) Неправильная спецификация.
- б) Случайные отказы.
- в) Устаревшие технологии.
- г) Неправильная эксплуатация.

Вопрос 3. Какое воздействие со стороны окружающей среды может привести к отказам по общей причине?

- а) Изменение температуры.
- б) Повышенная влажность.
- в) Электромагнитные помехи.
- г) Все вышеперечисленное.

Вопрос 4. Как неправильные процедуры обслуживания могут привести к отказам по общей причине?

- а) Они не влияют на надежность системы.
- б) Они могут привести к неправильной калибровке и увеличению вероятности отказа.
- в) Они всегда улучшают работу системы.
- г) Они только увеличивают затраты на обслуживание.

Вопрос 5. Как можно минимизировать риски отказов по общей причине в проектировании СПАЗ?

- a) Использование одинаковых компонентов во всех системах.
- b) Проведение регулярного обслуживания и калибровки.
- c) Игнорирование воздействия окружающей среды.
- d) Упрощение проектирования системы.

Для получения дополнительной информации см. [28].

Тест 11.18. Концепция «доказано практикой».

Вопрос 1. Что означает термин «доказано практикой» в контексте систем безопасности?

- a) Это означает, что компонент был протестирован в лабораторных условиях.
- b) Это обозначает, что компонент был использован в реальных условиях и показал свою надежность.
- c) Это относится к компонентам, которые имеют сертификаты от независимых организаций.
- d) Это термин, который используется только для новых технологий.

Вопрос 2. Какое из следующих требований должно быть выполнено для того, чтобы компонент считался «доказанным практикой»?

- a) Компонент должен быть дешевым.
- b) Необходима оценка, подтверждающая его пригодность.
- c) Компонент должен быть новым на рынке.
- d) Компонент должен быть произведен известной компанией.

Вопрос 3. Что должно быть учтено при проведении оценки компонента для признания его «доказанным практикой»?

- a) Только стоимость компонента.
- b) Система оценки качества производителя.
- c) Личное мнение инженера.
- d) Только технические характеристики компонента.

Вопрос 4. Какую дополнительную оценку необходимо провести для интеллектуальных устройств (ПЭС)?

- a) Никакую, если устройство прошло стандартные тесты.
- b) Оценку, основанную на предыдущем опыте использования аналогичных устройств.
- c) Оценку только по стоимости устройства.
- d) Оценку только по его техническим характеристикам.

Вопрос 5. Какое исключение существует для конфигураций, ограниченных защитой в виде пароля?

- a) Они не требуют никакой оценки.
- b) Они могут использоваться без дополнительной проверки.
- c) Они требуют только базовой оценки.
- d) Они требуют дополнительной оценки, если позволяют изменять настройки параметров процесса.

12. ДОКУМЕНТАЦИЯ СПАЗ.

12.1. Ключевые принципы документирования СПАЗ.

Задание 12.1. Уяснить ключевые принципы документирования СПАЗ в области промышленной безопасности (систем приборной безопасности).

Документирование в СПАЗ/SIS – это не бюрократия, а «кровеносная система» жизненного цикла безопасности и главный инструмент доказательства соответствия требованиям Ростехнадзора (и международным стандартам).

Почему это так важно:

1. «Без бумажки ты... виноват!» (Юридическая защита).

Реальность. При аварии или аудите РТН (Разрешение Ростехнадзора) первое, что спросят. «Где документы, подтверждающие, что вы все сделали правильно?».

Философия. Документ – это юридическое доказательство вашей компетентности и соблюдения требований (116-ФЗ, Приказ 533, МЭК 61511). Нет документа значит нет доказательства, значит ваша профессиональная ответственность под вопросом.

Пример. «Представьте, что через 5 лет на вашем объекте происходит инцидент. Расследование. Вы уверены, что спроектировали все идеально. Но журналов калибровки датчиков СПАЗ/SIS нет. Ваше слово против факта отсутствия документов. Чем вы докажете свою невиновность?»

Документ СПАЗ – это «Машина времени инженера» (Трассируемость и история).

СПАЗ/SIS эксплуатируются десятилетиями. Люди уходят, меняются подрядчики. Как понять почему было принято решение 10 лет назад?

Документация – это исторический журнал и карта проекта. Она обеспечивает трассируемость решений от анализа рисков до конкретного клапана. Без нее модификации становятся опасной игрой в «испорченный телефон».

Пример. «Новый инженер видит резервный датчик температуры в СПАЗ/SIS. Зачем он? Старая документация показывает, это было требование LOPA для достижения SIL 2. Без этой записи датчик могут посчитать лишним и демонтировать – ослабив защиту!»

Документ – это «Общий язык безопасности» (Коммуникация и однозначность).

Над СПАЗ/SIS работают проектировщики, программисты, монтажники, эксплуатационники, аудиторы.

Стандартизированная документация (по МЭК 61511 и Приказу 533) – это единый язык, исключая разночтения. Например, спецификация безопасности (SRS) – это «конституция» СПАЗ/SIS, которую понимают все.

Пример. «Техник в цеху видит в SRS, что клапан AV-101 должен закрыться за МАКСИМУМ 5 секунд при срабатывании SIF-120. Таким образом, он точно знает норму (и было выполнено тестирование, которое показало приемлемое время срабатывания). Без SRS – он бы догадывался каким-то образом или делал бы так, как привык».

Аудит документации – это не проверка «галочки», а проверка безопасности (подтверждение соответствия). Он на 80% состоит из проверки документов и записей. В среде этих записей аудитор ищет доказательства выполнения требований на каждом этапе, ищет доказательства безопасности. Нет записей о валидации? Значит, нет доказательства, что система работает. Нет анализа изменений? Значит, есть риск, что модификация нарушила безопасность.

Пример. Аудитор спрашивает: «Как Вы подтверждаете, что расчет PFDavg для этого контура защиты соответствует SIL 2?». Только правильно оформленный отчет по верификации с подписями будет доказательством.

Ваши слова «мы считали по формулами» не пройдут!

Основная документация СПАЗ/SIS показана на рисунке 12.1. Она включает в себя:

1. SRS- спецификация требований безопасности.

Это «Библия СПАЗ/SIS», главный документ! Формализует ВСЕ требования к системе на этапе разработки ТЗ. Это этап HAZOP/LOPA проекта СПАЗ/SIS.

Это Синописис-Карта жизненного цикла СПАЗ/SIS (Краткое описание «Кровеносной Системы» Безопасности). Ее цель показать ЧТО, КОГДА и ЗАЧЕМ документируется на каждом шагу проектирования, и как документы связаны между собой.

SRS –это точное описание функций безопасности (SIF), условия срабатывания, целевой SIL, время отклика, требования к диагностике, режимы работы (постоянный/запросный), требования к оборудованию, условия эксплуатации, интервалы тестирования.

Это основа для проектирования, валидации, аудита. Без SRS проект СПАЗ/SIS просто «слепой».

Основные требования к SRS изложены в МЭК 61511-1 (Пункт 10), Приказ 533 (требования к проектной документации).

2. Верификационные отчеты (PFDavg, SFF, HFT).

Это «Математика безопасности». Документальное доказательство, что проектное решение (архитектура) соответствует целевому SIL.

«Что внутри»? Это детальные расчеты вероятности опасного отказа (PFDavg), безопасных отказов (SFF), анализ резервирования (HFT).

Без расчетов утверждение «SIL 2 достигнут» голословно. Аудит РТН требует отчет.

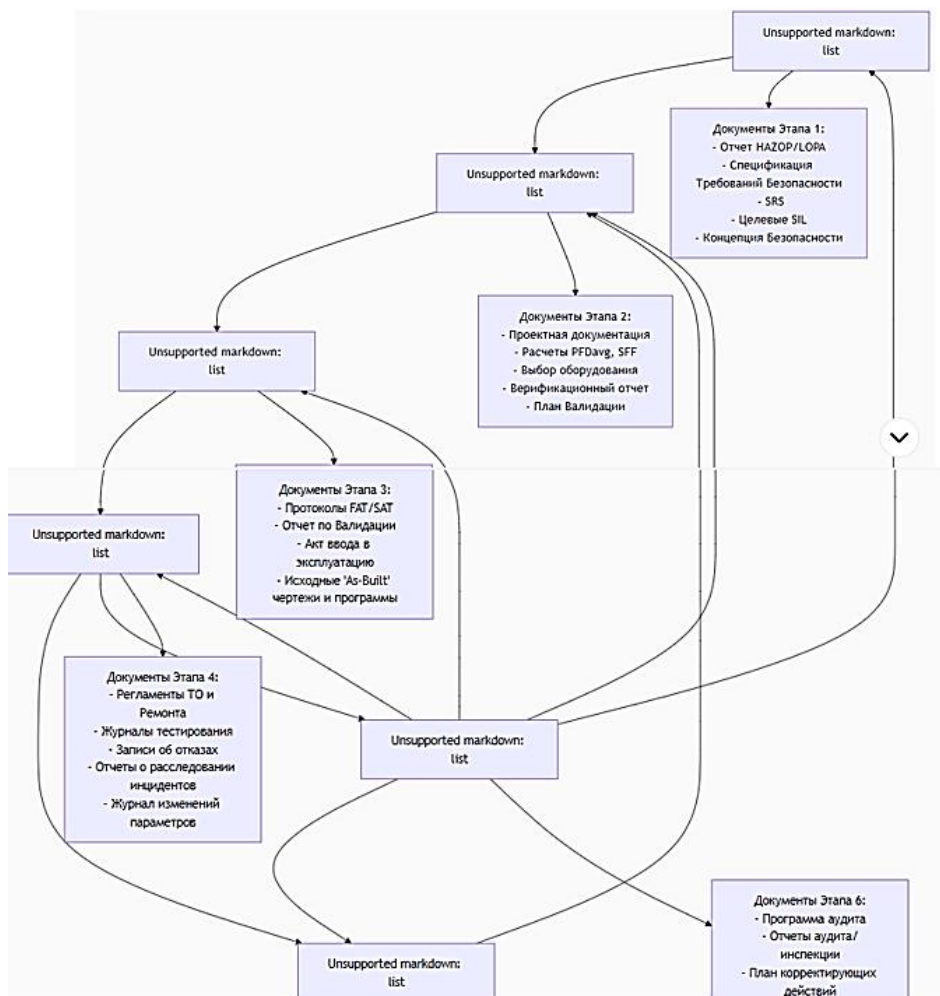


Рис. 12.1. Основные документы СПАЗ

Требования к документации установлены в МЭК 61511-1 (Пункт 11) и в Приказе 533 (Объяснение решений).

3. Валидационные протоколы (FAT, SAT, Site Validation).

Валидационные протоколы FAT, SAT и Site Validation представляют собой этапы подтверждения соответствия оборудования или системы установленным требованиям и спецификациям.

FAT – это приемочные испытания, проводимые производителем (поставщиком).

SAT – приемочные испытания на площадке заказчика.

Site Validation – это общая процедура подтверждения работоспособности и соответствия всей системы в целом.

«Испытание HIL» – это доказательство, что реальная, смонтированная система работает ТОЧНО так, как описано в SRS и проекте.

«Что внутри»? Это результаты (отчеты) комплексных испытаний «в железе» (HIL), у поставщика (FAT), у заказчика (SAT), проверка всех сценариев срабатывания, временных параметров СПАЗ.

Зачем нужны эти документы? Технический проект на бумаге – это еще не работающая система. Только после валидации проекта

начинается эксплуатационный период СПАЗ/SIS. Валидация – это финальная проверка перед доверием жизни системе. Без нее ввод запрещен!

См. требования МЭК 61511-1 (Пункт 12), Приказ 533 (требования к вводу в эксплуатацию).

4. Журналы Технического Обслуживания и Тестирования.

Это «Пульс безопасности», доказательство, что заявленная надежность (SIL) поддерживается в течение ВСЕГО срока службы.

Что внутри? Это подробные записи о каждом плановом и внеплановом ТО, результатах функциональных тестов (с указанием даты, исполнителя, параметров теста, обнаруженных неисправностей, замененных компонентов).

Зачем они нужны? Интервалы тестирования и процедуры – это часть расчетов PFDavg. Невыполнение тестов – это необоснованная вера в надежность. Эти журналы первое, что проверяет аудит РТН при инспекции!

См. требования. МЭК 61511-1 (Пункт 16, 17), Приказ 533 (требования к эксплуатации), 116-ФЗ (обязанности эксплуатирующей организации).

5. Управление Изменениями (МОС).

Это «Страховка от непреднамеренного вреда». Гарантия, что любая модификация не разрушит изначально заложенную безопасность.

Что внутри? Это формальная заявка на изменение, оценка влияния на безопасность (пересмотр HAZOP), пересчет SIL, обновление SRS), план повторной валидации, утверждение, обновление ВСЕЙ затронутой документации.

Зачем все это? Более 50% аварий происходят из-за плохо управляемых изменений! Документы МОС – доказательство, что безопасность не была нарушена после изменений.

См. Требования МЭК 61511-1 (Пункт 15), Приказ 533 (требования к модернизации).

6. Отчеты по Расследованию Инцидентов и Отказов.

«Учимся на ошибках»: фиксация и анализ любого отказа или ложного срабатывания СПАЗ/SIS для улучшения системы и процедур.

Что внутри? Это описание инцидента, анализ первопричины, принятые корректирующие действия, обновление документации (если нужно).

Зачем? Чтобы одна и та же ошибка не повторилась. Доказательство РТН, что организация учится и улучшает систему безопасности.

Требование. МЭК 61511-1 (Пункт 16), Приказ 533 (требования к мониторингу).

СПАЗ/SIS – это последний рубеж, когда:

- Риск ОПО изначально неприемлем (класс I).
- Другие меры (обучение, механическая защита) не снижают риск до ALARP.

Пример. На нефтеперекачивающей станции установлены датчики утечки, выполняется обучение персонала.

Проблема. При быстрой разгерметизации персонал не успеет среагировать (на диаграмме риска $P \approx 0$).

Решение. Необходим СПАЗ/SIS с автоматическим отсекателем ($PFD = 1e-3$).

Важно. СПАЗ/SIS не заменяет другие меры обеспечения безопасности, а дополняет их!

«Не записал – не сделал» – золотое правило функциональной безопасности.

Обязательным при документировании является:

- Четкое объяснение класса риска (ссылки на HAZOP, статистику).
- Расчеты PFD/SFF (например, через FTA).
- Сравнение с ALARP («риск снижен настолько, насколько это разумно»).

12.2. ПРАКТИКУМ ПО ДОКУМЕНТИРОВАНИЮ СПАЗ.

Задание 12.2. В предположении внешнего аудита СПАЗ подготовить отчет по верификации и отчет по валидации решения в кейсе. Для этого использовать типовой шаблон аудита

Кейс 12.1. SRS. Неполные требования к SIF.

На нефтеперерабатывающем заводе СПАЗ/SIS должен аварийно отключаться насос при высоком давлении. В SRS указано только условие срабатывания (>50 бар), но нет.

- Времени отклика (1 секунда? 10 секунд?).
- Требований к диагностике (например, проверка исправности датчиков раз в месяц).
- Режима работы (запросный/постоянный).

Последствия.

- Проектировщики выбрали клапан с временем срабатывания 30 сек, но это слишком медленно для процесса прокачки нефти.
- При аудите РТН выявлено несоответствие МЭК 61511-1 (п. 10.3.2).

Решение.

Дополнить SRS.

- SIF-001– Аварийное отключение насоса Р-101 при давлении >50 бар.
- Целевой SIL – SIL 2.
- Время отклика ≤ 2 сек (включая задержку датчика, логического реле и исполнительного механизма).
- Диагностика – Автоматический тест датчиков давления раз в 24 часа.

- Режим – Запросный (Low Demand).
- Интервал тестирования – Полный функциональный тест 1 раз в 12 месяцев.

Нормативные требования. МЭК 61511-1 (Пункт 10), Приказ 533 (п. 15).

Кейс 12.2. Верификационный отчет. Некорректный расчет PFDavg.

Для SIF с SIL 2 проектная организация предоставила отчет, где PFDavg = 0.02, но:

- Не учтена задержка передачи сигнала по полевой шине (она добавляет 0.005 сек).
- Использованы данные о надежности клапана из общего каталога, а не от производителя.

Последствия. Фактический PFDavg = 0.028 (превышает допустимый 0.01 для SIL 2). При аудите система признана не соответствующей SIL.

Решение.

Пересчитать PFDavg с:

- Реальными данными MTBF от вендора.
- Учетом всех компонентов (датчик + шина + логический реле + клапан).
- Приложением сертификатов оборудования.

Нормативные требования. МЭК 61511-1 (Пункт 11.4), Приказ 533 (п. 18).

Кейс 12.3. Валидационный протокол FAT. Отсутствие теста граничных условий.

На заводе-изготовителе проведен FAT для логического реле СПАЗ/SIS, но проверены только штатные сценарии (например, срабатывание при 50 бар). Не тестированы.

- Крайние значения (50.1 бар и 49.9 бар).
- Одновременный отказ датчика и резервного канала.

Последствия. В эксплуатации система не сработала при 49.8 бар (погрешность датчика не учтена).

Решение.

Дополнить протокол FAT.

Тест x1. Проверка срабатывания при 49.9 бар (нижняя граница). Результат: СПАЗ/SIS активирована за 1.8 сек (соответствует SRS).

Тест x2. Эмуляция отказа основного датчика. Результат: Резервный канал активирован за 2.1 сек.»

Нормативные требования. МЭК 61511-1 (Пункт 12.2), Приказ 533 (п. 22).

Кейс 12.4. Журнал тестирования – Отсутствие записи о замене датчика.

На химическом заводе датчик давления СПАЗ/SIS был заменен во время планового ТО, но в журнале не указано.

- Модель нового датчика (отличается от исходной).
- Калибровочные данные.

Последствия. При расчете PFDavg для аудита использованы старые данные. Фактическая надежность системы неизвестна.

Решение.

Должна быть запись в журнале, например: «15.05.2024. Замена датчика РТ-10 на новый датчик Rosemount 3051S:

- SIL 3 сертифицирован.
- Калибровка 0-100 бар, погрешность $\pm 0.1\%$.
- Исполнитель. Иванов А.П. (подпись)».

Нормативные требования. МЭК 61511-1 (Пункт 16.3), 116-ФЗ (ст. 9).

Кейс 12.5. Изменение логики без пересмотра SRS.

Инженеры изменили условие срабатывания SIF с «>50 бар» на «>55 бар» для оптимизации процесса, но.

- Не провели HAZOP для нового значения.
- Не обновили SRS.

Последствия. При 52 бар произошел разрыв трубопровода – система не сработала. Расследование выявило несанкционированное изменение.

Решение.

Форма логики должна включать:

1. Оценка рисков. Пересмотр HAZOP (новое значение 55 бар увеличивает частоту опасных событий с $1e-5$ до $1e-4$ /год).

2. Пересчет SIL. Требуется SIL 3 вместо SIL 2.

3. Обновленные документы. SRS, верификационные отчеты.»

Нормативные требования. МЭК 61511-1 (Пункт 15), Приказ 533 (п. 25).

Кейс 12.6. Отчет об инциденте. Ложное срабатывание СПАЗ/SIS. СПАЗ/SIS отключила компрессор без причины. Отчет содержит только запись. «Отказ датчика».

Проблемы.

- Нет анализа первопричины (влажность в шкафу?).
- Нет корректирующих действий.

Решение.

Отчет должен включать:

1. Первопричина. Коррозия контактов из-за конденсата (проверка по МЭК 60079-14).

2. Действия. Установка обогревателя в JB, замена датчика на

взрывозащищенный.

3. Обновление SRS. Добавлено требование к шкафу СПАЗ.

Нормативные требования. МЭК 61511-1 (Пункт 16.4), Приказ 533 (п. 30).

Документация СПАЗ/SIS – это не бумажки для Ростехнадзора.

Это материальное воплощение Вашей профессиональной ответственности за безопасность. Каждая подпись в журнале тестирования, каждая строка в SRS – это ваша личная гарантия, что система работает, когда это будет жизненно необходимо. Без документов безопасность недоказуема, а ваша репутация не защитима.

12.3. ТЕСТЫ С РЕШЕНИЯМИ И ОБЪЯСНЕНИЯМИ.

Задание 12.2. В предположении наличия исходных требований ОПО к СПАЗ и документации СПАЗ подготовить отчет по верификации и отчет по валидации документации промбезопасности.

Тест 12.1. Какие документы являются входными данными для спецификации требований к СПАЗ.

Вопрос 1. Какой из следующих документов обычно используется в качестве входных данных для составления Технического задания на безопасность?

- А) Отчет о финансовом анализе.
- В) Отчет об анализе опасности технологического процесса (например, отчет HAZOP).
- С) Инструкция по эксплуатации оборудования.
- Д) План маркетинга.

Ответ В. Отчет об анализе опасности технологического процесса (например, отчет HAZID).

Объяснение. Отчет HAZID является важным документом, который помогает выявить потенциальные опасности и определить требования к безопасности для систем функциональной безопасности (СПАЗ).

Вопрос 2. Какой документ содержит список выявленных функций безопасности с указанием входных и выходных данных для каждой из них?

- А) Принципиальные технологические схемы.
- В) Список функций безопасности.
- С) Отчет об анализе риска.
- Д) Описание технологических процессов.

Ответ В. Список функций безопасности.

Объяснение. Список функций безопасности является ключевым документом, который детализирует функции, необходимые для обеспечения безопасности, а также их входные и выходные данные.

Вопрос 3. Какой документ указывает на требуемый уровень целостности безопасности (SIL) и коэффициент снижения риска для каждой системы функциональной безопасности?

- А) Принципиальные технологические схемы.
- В) Отчет об анализе риска (диаграмма риска).
- С) Описание технологических процессов.
- Д) Техническое задание на безопасность.

Ответ В. Отчет об анализе риска.

Объяснение. Отчет об анализе риска содержит информацию о требуемом уровне SIL и коэффициенте снижения риска, что является критически важным для определения мер безопасности.

Вопрос 4. Какой из следующих документов предоставляет графическое представление технологических процессов?

- А) Описание технологических процессов.
- В) Принципиальные технологические схемы.
- С) Отчет HAZOP.
- Д) Список функций безопасности.

Ответ В. Принципиальные технологические схемы.

Объяснение. Принципиальные технологические схемы представляют собой графическое изображение технологических процессов, что помогает в понимании структуры и взаимосвязей в системе.

Вопрос 5 Рассмотрим следующие документы. Какой из этих документов, скорее всего, является обязательным входным документом для спецификации требований безопасности?

- 1. Отчет об анализе опасностей и рисков.
- 2. Процедуры установки и ввода в эксплуатацию.
- 3. Технологические схемы.

Выбрать для ответа:

- а) «1 и 2 необходимы, 3 – нет».
- б) «2 и 3 необходимы, 1 – нет».
- с) «1 и 3 необходимы, 2 – нет».
- д) «2 необходим, 1 и 3 – нет».
- е) «3 и 2, и 1 необходимы».

Ответ е. «3 и 2 и 1 необходимы».

Объяснение стандарт МЭК 61511 требует, чтобы спецификация требований безопасности содержала функциональную взаимосвязь между входами и выходами СПАЗ/SIS (системы инструментальной безопасности), включая логику, математические функции и любые необходимые разрешения. (См. МЭК 61511, часть 1, пункт 10.3.1, пункт 11).

Диаграммы причинно-следственных связей являются одним из самых популярных инструментов для представления логики благодаря их простоте использования и компактному представлению ин-

формации. В случаях, когда требуется больше информации, чем может быть представлено на простой диаграмме, эффективны диаграммы двоичной логики, такие как описанные в стандарте ISA 5.2.

Помимо формализованных методов представления логики, таких как описанные выше, обычный текст также является допустимым способом представления действий СПАЗ/SIS. Обычный текст по-прежнему остается одним из наиболее часто используемых методов представления логики, особенно среди специалистов, не занимающихся управлением процессами, поскольку не требует знаний о формальных системах представления.

Согласно стандарту, МЭК 61511 отчет об анализе опасностей и рисков (пункт 1) является критически важным для понимания потенциальных угроз и рисков, связанных с системой. Процедуры установки и ввода в эксплуатацию (пункт 2) также необходимы для обеспечения правильной работы системы. Технологические схемы (пункт 3), хотя и полезны, не являются обязательными для спецификации требований безопасности, так как они не содержат информации о рисках и процедурах, необходимых для обеспечения безопасности.

Вопрос 6. Какой документ содержит детальное описание процессов, используемых в технологической установке?

- A) Принципиальные технологические схемы.
- B) Описание технологических процессов.
- C) Отчет об анализе риска.
- D) Список функций безопасности.

Ответ В. Описание технологических процессов.

Объяснение. Описание технологических процессов предоставляет подробную информацию о каждом процессе, что важно для понимания и анализа безопасности.

Техническое задание на безопасность (ТЗ) обычно составляется в два этапа. Во-первых, по завершении анализа рисков составляется спецификация для отображения основных требований к снижению риска для каждой SIF системы функциональной безопасности. Некоторые из обычно используемых на этом этапе входных документов включают в себя.

Отчет об анализе опасности технологического процесса (например, отчет HAZOP).

Список выявленных функций безопасности с указанием входных и выходных данных для каждой из них.

Отчеты об анализе риска для каждой SIF, показывающие требуемый уровень целостности безопасности (SIL) и коэффициент снижения риска.

Принципиальные технологические схемы.

Технологические схемы.

Описания технологических процессов.

В целом, перечисленные выше документы описывают контролируемый технологический процесс, связанные с ним опасности и способ достижения требуемого снижения риска с помощью СПАЗ/SIS.

Во-вторых, после завершения детального проектирования СПАЗ/SIS ТЗ обновляется, чтобы включить все остальные требования, перечисленные в стандарте (см. МЭК 61508 часть 1, пункт 7, и МЭК 61511 часть 1, пункт 10). Для этого, вероятно, потребуются такие входные документы, как:

- Детальный проект СПАЗ/SIS, включая время отклика, поведение при отказах, процедуры запуска и останова, обходы, сбросы, переопределения, требования к техническому обслуживанию (включая необходимое время).
- Стратегия и процедуры технического обслуживания.
- Спецификация устойчивости к электромагнитным помехам.
- Детальные монтажные чертежи, по которым можно определить рабочую среду СПАЗ/SIS.
- Спецификация цикла работы и срока службы предприятия.
- Детальная спецификация технологического процесса, приводящая к определению уставок срабатывания СПАЗ/SIS.
- Проектирование человеко-машинного интерфейса (HMI).
- Проектирование прикладного программного обеспечения.

Тест 12.2. Аудит документации СПАЗ/SIS – это искусство видеть невидимое.

Вопрос 1. Какие документы чаще всего содержат «подводные камни» при аудите СПАЗ/SIS?

Варианты ответов.

- A) Спецификация требований безопасности (SRS).
- B) P&ID-схемы с пометкой «Как построено».
- C) Резюме сотрудников, обслуживающих СПАЗ/SIS.
- D) Протоколы функционального тестирования.

Ответ: A, B, D.

Объяснение.

Ответ А. SRS, если требования не соответствуют SIL или неполны (например, отсутствуют условия срабатывания), это критично.

Ответ В. P&ID «Как построено» могут не отражать реальную конфигурацию (например, забыли добавить датчик, установленный во время монтажа).

Ответ D. Протоколы тестирования часто содержат подписи без детальных данных (например, «Тест пройден», но без значений срабатывания).

Ответ С. Резюме сотрудников не относятся к документации СПАЗ/SIS, если только не проверяется компетенция через запись об опыте.

Вопрос 2. Как на аудите обнаружить, что расчеты PFDavg были скопированы из другого проекта?

Варианты ответов.

А) Проверить, совпадают ли значения λ (интенсивность отказов) компонентов с их сертификатами.

В) Найти упоминание неиспользуемых в проекте компонентов в формулах.

С) Убедиться, что в расчетах учтены реальные периоды тестирования (T_{Proof}).

Д) Сравнить подпись Ответственного инженера с другими документами.

Ответ В.

С.

Объяснение.

- Если в расчетах фигурируют компоненты, отсутствующие в спецификациях (Ответ В) – явный признак копирования.

- Нереалистичные T_{Proof} (Ответ С) – например, период тестирования 2 года, хотя на практике проверки проводятся каждые 6 месяцев. Сертификаты (Ответ А) и подписи (Ответ Д) не помогут выявить копирование.

Вопрос 3. Что указывает на устаревшую версию документации СПАЗ/SIS?

Варианты ответов.

А) Отсутствие ревизионных пометок и дат изменений.

В) Использование устаревшего логотипа компании.

С) Несоответствие между P&ID и списком компонентов в SRS.

Д) Упоминание стандарта МЭК 61508.1998 вместо МЭК 61508.2010.

Ответ: А, С, Д.

Объяснение.

- **Нет ревизий (Ответ А)** – документ мог не обновляться годами.

- **Расхождение P&ID и SRS (Ответ С)** – например, в SRS указан клапан от производителя X, а на схеме – от Y.

- **Устаревший стандарт (Ответ Д)** – Например, МЭК 61508.1998 был заменен на версию 2010 года.

Логотип (Ответ В) – косвенный признак, но не критичный для безопасности.

Вопрос 4. Где чаще всего скрывается ошибка в спецификации требований безопасности (SRS)?

Варианты ответов.

А) Некорректное указание условий окружающей среды (например, температура).

В) Отсутствие ссылок на стандарты МЭК 61511.

С) Несоответствие между SIL-уровнем и требованиями к диагностическому покрытию (DC).

Д) Использование аббревиатур без расшифровки.

Ответ А.

С.

Объяснение.

• **Условия среды (Ответ А)** – если СПАЗ/SIS рассчитана на -20°C , но в спецификации указано 0°C , компоненты могут отказать.

• **Несоответствие SIL и DC (Ответ С)** – например, SIL 2 требует $\text{DC} \geq 90\%$, но в проекте $\text{DC} = 60\%$.

Ссылки на стандарты (Ответ В) и аббревиатуры (Ответ Д) – формальные ошибки, но не влияют на функциональность.

Вопрос 5. Как проверить, что протоколы тестирования СПАЗ/SIS не фальсифицированы?

Варианты ответов.

А) Сравнить даты тестирования с графиком ТО.

В) Найти упоминание тестового оборудования, которого нет на складе.

С) Проверить логи контроллера на соответствие датам в протоколе.

Д) Убедиться, что все подписи выполнены одной ручкой.

Ответ: А, В, С.

Объяснение.

• **Расхождение дат (Ответ А)** – если тест проведен в выходной день.

• **Несуществующее оборудование (Ответ В)** – в протоколе указан генератор сигналов модели X, но его нет в компании.

• **Лог контроллера (Ответ С)** – если в них нет записей о тестах в указанные даты.

• **Одна ручка (Ответ Д)** – ненадежный признак.

Вопрос 6. Что НЕ является «подводным камнем» в документации СПАЗ/SIS?

Варианты ответов.

А) Отсутствие трассируемости между требованиями SRS и тестами.

В) Опечатки в фамилиях ответственных лиц.

С) Использование устаревшей версии ПО для логического контроллера.

Д) Отсутствие сертификатов SIL для датчиков.

Ответ В.

Объяснение..

• **Отсутствие трассируемости (Ответ А)** – нельзя доказать, что требования проверены.

• **Опечатки в фамилиях (Ответ В)** – формальная ошибка, но не влияет на безопасность. Остальные варианты критические

• **Устаревшее ПО (Ответ С)** – может содержать не устранённые уязвимости.

• **Нет сертификатов (Ответ D)** – компоненты не соответствуют SIL.

Вопрос 7. Как выявить, что изменения в СПАЗ/SIS не были задокументированы?

Варианты ответов.

A) Сравнить дату последней ревизии SRS с датой модификации ПО контроллера.

B) Найти несоответствие между SRS и руководством по эксплуатации.

C) Проверить, есть ли подпись руководителя проекта на всех документах.

D) Убедиться, что в журнале изменений указана причина модификации.

Ответ: A, B, D.

Объяснение.

• **Разные даты (Ответ A)** – если ПО обновляли после последней ревизии SRS, изменения могли не быть утверждены.

• **Несоответствие SRS и руководства (Ответ B)** – например, в SRS указана частота тестирования 1 раз в год, а в руководстве – 2 раза.

• **Причина изменений (Ответ D)** – если графа «Причина» пустая, модификация не обоснована.

Подписи (**Ответ C**) – не гарантируют, что изменения учтены.

Вопрос 8. Что указывает на некомпетентность аудитора?

Варианты ответов.

A) Он проверяет только наличие документов, а не их содержание.

B) Он требует предоставить сертификаты SIL для отверток.

C) Он использует чек-лист, соответствующий МЭК 61511.

D) Он задает вопросы о соответствии расчетов PFDavg архитектуре СПАЗ/SIS.

Ответ: A, B.

Объяснение.

• **Поверхностная проверка (Ответ A)** – аудитор не ищет «подводные камни».

• **Сертификаты для отверток (Ответ B)** – инструменты не относятся к СПАЗ/SIS.

Варианты C и D – признаки компетентности.

Вопрос 9. МЭК 61511 требует проведения аудита соответствия требованиям безопасности, перечисленным для СПАЗ/SIS, через какой интервал?

a) Два раза в год.

b) Один раз в год.

c) Один раз в три года.

d) Один раз в пять лет.

е) МЭК 61511 не указывает требуемый временной интервал для аудитов соответствия.

Ответ е. МЭК 61511 не указывает требуемый временной интервал для аудитов соответствия.

Объяснение.

Стандарты требуют планирования частоты аудитов, но не указывают требуемый временной интервал. Каждая отдельная эксплуатирующая компания должна выбрать необходимый интервал после тщательного анализа связанного риска. При этом выборе следует учитывать законы и правила, действующие в компании технологической установки.

Например, правила управления безопасностью процессов и управления рисками в Северной Америке требуют аудита соответствия плану управления безопасностью процессов владельца процесса каждые три года. Аудиты функциональной безопасности SIF должны быть частью этого процесса.

Вопрос 10. Для какой из следующих задач, влияющих на функциональную безопасность СПАЗ/SIS, не требуется разработка процедуры для управления её реализацией.

1. Модификация существующей СПАЗ/SIS.

2. Аудит соответствия требованиям СПАЗ/SIS.

3. Отслеживание конфигураций СПАЗ/SIS

a) 1 и 2 требуются, 3 – нет.

b) 1 и 3 требуются, 2 – нет.

c) 2 и 3 требуются, 1 – нет.

d) 1, 2 и 3 требуются.

e) Ни одна из вышеперечисленных задач не требует процедур.

Ответ d.

Объяснение.

Процедуры требуются для ряда задач жизненного цикла безопасности. Модификации SIF должны выполняться в соответствии с процедурой управления изменениями. Стандарты требуют процедур аудита соответствия SIF требованиям безопасности. Отслеживание изменений конфигурации SIF является модификацией SIF, которая должна выполняться в соответствии с теми же процедурами, которые применялись бы при физическом изменении оборудования. Процедуры управления изменениями также применяются к программному обеспечению.

См. МЭК 61511 часть 1, раздел 5.2, особенно пункты 5.2.6.2 и 5.2.7.

Заключительный комментарий.

Аудит документации СПАЗ/SIS – это искусство видеть невидимое. Например, идеальные подписи в протоколах могут скрывать то, что тесты никогда не проводились, а красивые графики PFDavg – быть копией из прошлого проекта. Главный секрет. документы – это

«следы», оставленные разработчиками. Если следы ведут в никуда (нет трассируемости) или внезапно обрываются (несоответствие версий), за этим стоит большая проблема. Помните. СПАЗ/SIS надежна ровно настолько, насколько честна её документация.

Тест 12.3. Документация о производительности СПАЗ. Процедуры для оценки фактической производительности СПАЗ/SIS.

Вопрос 1. Какие два атрибута спецификации требований СПАЗ/SIS должны быть переоценены для обеспечения выполнения целей допустимого риска?

- А) Фактическая частота отказов компонентов СПАЗ.
- В) Документация по проектированию и план управления проектом.
- С) Уровень SIL и архитектура системы.
- Д) Обучение персонала и процедуры обслуживания.

Ответ А. Фактическая частота отказов компонентов СПАЗ.

Объяснение. Фактическая частота отказов компонентов СПАЗ (как реальные, так и ложные срабатывания) и фактические частоты отказов компонентов являются критически важными атрибутами, которые необходимо переоценивать для обеспечения того, чтобы система соответствовала установленным целям допустимого риска. Эти данные помогают понять, насколько эффективно система выполняет свои функции безопасности в реальных условиях эксплуатации.

Вопрос 2. Почему важно проверять фактические частоты отказов компонентов СПАЗ/SIS в сравнении с предположениями, сделанными на этапе проектирования?

- А) Чтобы уменьшить затраты на проект.
- В) Чтобы убедиться, что система соответствует требованиям SIL.
- С) Чтобы определить, необходимо ли обновление оборудования.
- Д) Чтобы обеспечить соответствие фактической производительности и предположений, что может повлиять на уровень SIL и архитектуру СПАЗ/SIS.

Ответ Д. Чтобы обеспечить соответствие фактической производительности и предположений, что может повлиять на уровень SIL и архитектуру СПАЗ/SIS.

Объяснение. Проверка фактических частот отказов помогает выявить расхождения между проектными предположениями и реальной работой системы. Если фактические данные показывают, что предположения были неверными, это может потребовать изменения требований безопасности для СПАЗ/SIS, что, в свою очередь, может повлиять на уровень SIL и архитектуру системы.

Вопрос 3. Какова основная цель внедрения процедур для оценки фактической производительности СПАЗ/SIS?

- А) Увеличение бюджета проекта.
- В) Обеспечение соответствия законодательным требованиям.

С) Оптимизация процессов обслуживания.

Д) Обеспечение соответствия фактической производительности спецификации требований и целей допустимого риска.

Ответ Д. Обеспечение соответствия фактической производительности спецификации требований и целей допустимого риска.

Объяснение. Основная цель внедрения процедур оценки фактической производительности СПАЗ/SIS заключается в том, чтобы гарантировать, что система продолжает соответствовать установленным требованиям и целям допустимого риска, что критически важно для обеспечения безопасности процессов.

Вопрос 4. Что может произойти, если фактическая производительность СПАЗ/SIS не соответствует предположениям, сделанным на этапе проектирования?

А) Система будет работать более эффективно.

В) Увеличится вероятность аварийных ситуаций.

С) Не потребуются никаких изменений в системе.

Д) Система будет соответствовать требованиям SIL без изменений.

Ответ В. Увеличится вероятность аварийных ситуаций.

Объяснение. Если фактическая функциональность СПАЗ/SIS не соответствует требованиям, то это может привести к недостаточной эффективности системы безопасности, что, в свою очередь, увеличивает вероятность аварийных ситуаций и может угрожать безопасности процессов.

Два атрибута спецификации требований СПАЗ/SIS, которые следует проверить на соответствие фактической производительности.

- Требования к частоте отказов СПАЗ (как реальные срабатывания, так и ложные срабатывания).
- Фактические частоты отказов компонентов СПАЗ/SIS.

При проектировании системы безопасности (СПАЗ/SIS) делаются определенные предположения на основе исторических данных из этой и других аналогичных установок. Эти предположения могут повлиять на выбранный уровень SIL и необходимую архитектуру или выбор компонентов установленной СПАЗ/SIS. Если фактический опыт показывает, что предположения, использованные на этапе проектирования, неверны, то требования безопасности для СПАЗ/SIS должны быть изменены для отражения фактических условий эксплуатации. Стандарты содержат требования для проверки фактической производительности в сравнении с предположениями, сделанными на этапе проектирования.

См. требование к мониторингу производительности СПАЗ/SIS изложенное в части 1 стандарта МЭК 61511, пункт 5.2.5.3.

Тест 12.4.

Документация о компетентности лиц, выполняющих мероприятия по жизненному циклу безопасности. Перечислите как минимум 4 атрибута, которые следует учитывать при определении компетентности лиц для выполнения задач жизненного цикла безопасности.

Вопрос 1. Какой из следующих атрибутов является ключевым для определения компетентности лиц, выполняющих мероприятия по жизненному циклу безопасности?

- A) Умение работать в команде.
- B) Инженерные знания, обучение и опыт, соответствующие приложению процесса.
- C) Знание иностранных языков.
- D) Умение проводить презентации.

Ответ В. Инженерные знания, обучение и опыт, соответствующие приложению процесса.

Объяснение. Этот атрибут критически важен, поскольку понимание частоты и последствий опасных событий напрямую влияет на способность профессионала принимать обоснованные решения в области безопасности.

Вопрос 2. Какой атрибут относится к пониманию технологий, используемых в системах безопасности?

- A) Знание методов вероятностного анализа.
- B) Умение работать с документами.
- C) Инженерные знания, обучение и/или опыт, соответствующие используемой технологии.
- D) Навыки управления проектами.

Ответ С. Инженерные знания, обучение и/или опыт, соответствующие используемой технологии.

Объяснение. Понимание специфических технологий (например, электрических или программируемых) необходимо для эффективного управления системами безопасности и их рисками.

Вопрос 3. Какой из следующих атрибутов связан с анализом безопасности и оценкой рисков?

- A) Знание правовых и нормативных требований безопасности.
- B) Достаточные навыки управления и руководства.
- C) Знание методов вероятностного и надежного инженерного анализа безопасности.
- D) Умение работать с клиентами.

Ответ С. Знание методов вероятностного и надежного инженерного анализа безопасности.

Объяснение. Этот атрибут позволяет специалистам оценивать риски и вероятность опасных событий, что является основой для принятия решений в области безопасности.

Вопрос 4. Какой атрибут важен для соблюдения законов и стандартов в области безопасности?

- А) Инженерные знания, обучение и опыт, соответствующие датчикам и конечным элементам.
- В) Знание правовых и нормативных требований безопасности и применимых стандартов.
- С) Умение проводить тренинги.
- Д) Навыки работы с программным обеспечением.

Ответ В. Знание правовых и нормативных требований безопасности и применимых стандартов.

Объяснение. Понимание правовых норм и стандартов является обязательным для обеспечения соответствия и защиты как работников, так и окружающей среды.

Вопрос 5. Какое из следующих утверждений о необходимой компетентности лиц, выполняющих задачи жизненного цикла безопасности, является верным?

1. Должен иметь инженерное образование в аккредитованном университете.
 2. Должен быть сертифицирован независимой сторонней организацией.
 3. Руководитель проекта должен убедиться, что человек компетентен на всех этапах жизненного цикла безопасности.
- a) 1 и 2 верны, 3 – неверно.
 - b) 1 и 3 верны, 2 – неверно.
 - c) 2 и 3 верны, 1 – неверно.
 - d) 1, 2 и 3 верны.
 - e) Ни одно из вышеперечисленных утверждений неверно.

Ответ е.

Объяснение.

Необходимо иметь диплом инженера аккредитованного университета». Стандарты и правила, регулирующие использование SIF, не требуют какого-либо конкретного образования, а лишь требуют компетентности человека в задачах жизненного цикла безопасности, которые ему поручены.

Необходимо иметь сертификат независимой третьей стороны. Ни один из стандартов SIF не требует сертификации третьей стороной для ЛЮБОГО положения, включая компетентность персонала.

Руководитель проекта должен убедиться, что человек компетентен во всех фазах жизненного цикла безопасности». Его охват требований слишком широк. Лица, выполняющие задачи жизненного цикла безопасности, должны быть компетентны только в тех задачах, которые им поручены, а не во всех задачах жизненного цикла безопасности. Это важное различие. Например, инженеры-технологи, являющиеся экспертами в области анализа риска, не обязаны также быть экспертами в программировании PES для выполнения этапов оценки опасности и риска в жизненном цикле безопасности.

См. требования к компетентности описаны в МЭК 61508.2010 часть 1, пункты 6.2.13–6.2.15.

Вопрос 6. Какой атрибут относится к управлению и руководству в области безопасности?

- А) Умение работать в команде.
- В) Достаточные навыки управления и руководства, соответствующие их роли.
- С) Знание технологий.
- Д) Инженерные знания по проектированию.

Ответ В. Достаточные навыки управления и руководства, соответствующие их роли.

Объяснение. Эти навыки необходимы для эффективного руководства и координации мероприятий по жизненному циклу безопасности, что способствует созданию безопасной рабочей среды.

При определении компетентности лица, выполняющего действия жизненного цикла безопасности, следует учитывать следующие качества.

- Инженерные знания, обучение и опыт, соответствующие приложению процесса, включая понимание частоты и последствий опасных событий.

- Инженерные знания, обучение и/или опыт, соответствующие используемой технологии (например, электрической, электронной или программируемой электронной).

- Инженерные знания, обучение и опыт, соответствующие датчикам и конечным элементам.

- Знание методов вероятностного и надежного/инженерного анализа безопасности.

- Знание правовых и нормативно-правовых требований безопасности и применимых стандартов.

- Достаточные навыки управления и руководства, соответствующие их роли в деятельности по жизненному циклу безопасности.

См. Требования к компетентности описаны в МЭК 61508 часть 1, пункты 6.2.13–6.2.15.

Тест 12.5. Контроль версий документов. Перечислите атрибуты успешной системы контроля версий документов. Например, какой атрибут необходим для обеспечения того, чтобы используемый документ не был старой версией?

Вопрос 1. Какой атрибут необходим для обеспечения того, чтобы используемый документ не был старой версией?

- А) Наличие уникального идентификатора документа.
- В) Четкое указание текущего номера ревизии и даты завершения ревизии.

- С) Наличие списка всех предыдущих версий документа.
- Д) Указание авторов документа.

Ответ В.

Объяснение. Четкое указание текущего номера ревизии и даты завершения ревизии позволяет пользователям легко идентифицировать актуальную версию документа и предотвращает использование устаревших версий.

Вопрос 2. Какова роль проверки документа в системе контроля версий?

- А) Убедиться, что документ написан правильно.
- В) Подтвердить, что документ соответствует требованиям и стандартам.
- С) Определить, кто автор документа.
- Д) Убедиться, что документ доступен для всех.

Ответ В.

Объяснение. Проверка документа компетентным лицом необходима для подтверждения его соответствия требованиям и стандартам, что является важным этапом в процессе контроля версий.

Вопрос 3. Кто должен утверждать документ в системе контроля версий?

- А) Любой сотрудник компании.
- В) Лицо, уполномоченное на выполнение задач жизненного цикла безопасности.
- С) Автор документа.
- Д) Любой менеджер.

Ответ В.

Объяснение. Утверждение документа должно происходить только лицом, уполномоченным на выполнение задач жизненного цикла безопасности, чтобы гарантировать, что документ соответствует необходимым стандартам и требованиям.

Вопрос 4. Какова основная цель схемы контроля документации?

- А) Обеспечить доступность документов для всех сотрудников.
- В) Обеспечить выполнение всех задач, связанных с пересмотром, проверкой и утверждением документов.
- С) Упростить процесс создания документов.
- Д) Убедиться, что все документы имеют одинаковый формат.

Ответ В.

Объяснение. Основная цель схемы контроля документации – обеспечить выполнение всех задач, связанных с пересмотром, проверкой и утверждением документов, что критически важно для поддержания актуальности и качества документации.

Вопрос 5. Где подробно изложены требования к контролю документов?

- А) В ISO 9001.
- В) В МЭК 61508 часть 1, раздел 5.

- С) В документации компании.
- Д) В руководстве по безопасности.

Ответ В.

Объяснение. Требования к контролю документов подробно изложены в МЭК 61508 часть 1, раздел 5, особенно в пункте 5.2.11, что делает этот стандарт ключевым для понимания системы контроля версий документов.

Вопрос 6. Какие из следующих утверждений о документации, необходимой для планирования безопасности, являются верными?

1. Документация по планированию безопасности должна быть включена в качестве раздела в плане качества под названием «план безопасности».

2. Планирование безопасности должно быть задокументировано в отдельном документе под названием «план безопасности».

3. Планирование безопасности должно быть задокументировано в серии документов, которые могут включать другие процедуры или рабочие практики компании, такие как корпоративные стандарты.

а) 1 и 2 верны, 3 – неверно.

б) 1 и 3 верны, 2 – неверно.

с) 2 верно, 1 и 3 – неверно.

д) 1, 2 и 3 верны.

е) Ни одно из вышеперечисленных утверждений неверно.

Ответ б.

Объяснение. Стандарты не требуют, чтобы это планирование хранилось в отдельном документе под названием «план безопасности», хотя это часто бывает на практике.

Стандарты предоставляют эксплуатирующим компаниям значительную свободу в выборе места и типа документации, используемой для демонстрации планирования безопасности. Рекомендации по месту хранения документации, приведенные в стандартах, включают отдельный раздел в плане качества, как указано в утверждении 1.

Стандарты также допускают, чтобы план безопасности содержался в ряде отдельных документов, таких как стандарты компании и рабочие процедуры, как указано в утверждении 3.

См. МЭК 61511 часть 1, пункт 5.2.4 для четкого изложения требований к документации по планированию.

Рассмотрим документацию, которая должна быть создана в соответствии с жизненным циклом безопасности.

Хорошая схема контроля документации требует, чтобы документы были.

- Пересмотрены. Каждый документ должен четко указывать текущий номер ревизии и дату завершения ревизии.

- Проверены. Каждый документ должен быть проверен компетентным лицом. В документе должно быть четко указано лицо, проверившее документ.

• Утверждены. Каждый документ должен быть утвержден лицом, уполномоченным на выполнение задач жизненного цикла безопасности. В документах должно быть четко указано лицо, утвердившее документ.

Должна существовать схема контроля документации, которая обеспечивает выполнение всех вышеперечисленных задач.

См. Требования к контролю документов в МЭК 61508 часть 1, раздел 5, особенно пункт 5.2.11. Для полезных рекомендаций по практической реализации см. Functional Safety - an МЭК 61508 Compliant Development Process, авторы M.D. Medoff и R. I Faller, глава 3.

Тест 12.6. Документация жизненного цикла СПАЗ.

Вопрос 1. Какая из следующих позиций информации НЕ должна поддерживаться на протяжении всего жизненного цикла СПАЗ/SIS_?

1. Результаты анализа опасностей и рисков и связанные с ними предположения.

2. Информация об элементах оборудования, используемых для функций безопасности, а также требования безопасности к функциям.

3. Процедуры, необходимые для поддержания функциональной безопасности.

а) 1 и 2 необходимы, 3 – нет.

б) 1 и 3 необходимы, 2 – нет.

с) 2 и 3 необходимы, 1 – нет.

д) 1, 2 и 3 необходимы.

е) Ни одна из перечисленных выше позиций информации не требуется.

Ответ d.

Объяснение.

Правильное применение жизненного цикла безопасности требует обширной документации. Цель документации – обеспечить основу для проектных решений, принимаемых на последующих этапах жизненного цикла безопасности, и инструкции по правильному использованию системы по завершении. Они также важны для целей аудита и проверки. Эти документы будут необходимы на протяжении всего жизненного цикла.

Результаты анализа опасностей и рисков и связанные с ними предположения являются основой для последующих этапов жизненного цикла безопасности, таких как выбор уровня целостности безопасности и распределение снижения риска.

Эта документация определяет функции безопасности, необходимые для процесса, и неснижаемый уровень риска.

Информация о применяемых элементах оборудования для функций безопасности, а также требования безопасности необходимы для дальнейшего технического обслуживания и эксплуатации СПАЗ.

Процедуры, необходимые для поддержания функциональной безопасности, также будут необходимы на протяжении всего жизненного цикла безопасности.

Вопрос 2. Рассмотрим следующие этапы жизненного цикла безопасности.

Этап 1 – После проведения анализа опасностей и рисков, выявления необходимых уровней защиты и разработки спецификации требований безопасности.

Этап 2 – После проектирования системы безопасности (СПАЗ/SIS).

Этап 3 – После завершения установки, предварительного ввода в эксплуатацию и окончательной валидации системы безопасности (СПАЗ/SIS) и разработки процедур эксплуатации и технического обслуживания.

Этап 4 – После получения опыта эксплуатации и технического обслуживания.

Этап 5 – После модификации и перед выводом из эксплуатации системы безопасности (СПАЗ/SIS).

Вопрос 3. После каких этапов необходимо проводить мероприятия по оценке функциональной безопасности?

- a) После всех этапов.
- b) После этапов 1, 2, 3 и 5.
- c) Только после этапа 5.
- d) Только после этапа 3.
- e) Ни одно из вышеперечисленных утверждений неверно.

Ответ d.

Объяснение. Количество и глубина необходимых оценок функциональной безопасности будут варьироваться в зависимости от типа проекта.

Некоторые из параметров, которые следует учитывать при планировании оценок функциональной безопасности, – это размер проекта, степень сложности, уровень целостности безопасности, продолжительность проекта, последствия в случае отказа и степень стандартизации конструктивных особенностей. Этапы, требующие оценок функциональной безопасности, должны быть определены на этапе планирования безопасности.

Хотя количество и глубина оценок варьируются от проекта к проекту, оценка функциональной безопасности всегда требуется после третьего этапа. Эта оценка, также называемая предварительным пусковым обзором безопасности или предварительным пусковым приемочным испытанием в терминологии как технических документов ГОСТ Р 61511 так и Федеральные норм и правил в области промышленной безопасности.

Во время этой оценки завершенная SIF, как установленная, а также сопутствующие процедуры эксплуатации и технического обслуживания проверяются на соответствие назначению и соответствие спецификации требований безопасности. Эта оценка должна быть проведена до ввода SIF в эксплуатацию.

См. МЭК 61511 часть 1, раздел 5.2.6.1.

Тест 12.7. Ответственность поставщика (разработчика) СПАЗ.

Поставщик, поставляющий продукцию или услуги организации, может нести общую ответственность за один или несколько этапов жизненного цикла безопасности при условии, чтобы.

а) Продукция и/или услуги поставщика сертифицированы независимой третьей стороной как соответствующие МЭК 61508.

б) Продукция и/или услуги поставляются в соответствии со спецификациями, предоставленными покупателем, и у поставщика есть соответствующая система управления качеством.

с) Продукция и/или услуги поставщика сертифицированы как соответствующие МЭК 61508, а их рабочие процессы сертифицированы как соответствующее ISO 9001, каждая независимой третьей стороной.

д) Продукция поставщика является самой дешевой в конкурентной ситуации тендерных торгов.

е) Ни один из вышеперечисленных вариантов не подходит, поставщики не могут нести ответственность за выполнение мероприятий жизненного цикла безопасности, это может быть выполнено только владельцем/эксплантатом процесса

Ответ б. Продукция и/или услуги поставляются в соответствии со спецификациями, предоставленными покупателем, и у поставщика есть соответствующая система управления качеством

Объяснение. Цель требований к сторонним поставщикам оборудования в стандартах – обеспечить поставку оборудования, соответствующего требованиям безопасности, и разрешить выполнение этой работы организациями, отличными от конечного пользователя.

Зачастую, опыт в специализированных задачах жизненного цикла, таких как руководство анализом технологических опасностей или анализ надежности SIF, не является основной компетенцией конечного пользователя. По этой причине стандарты допускают выполнение этой задачи поставщиками при определенных условиях. Таким образом, утверждение «е» неверно.

Хотя сертификация рекомендуется в большинстве случаев, нигде в стандартах нет требования, чтобы какие-либо задачи жизненного цикла безопасности были сертифицированы сторонней организацией. Во многих случаях проверка и авторизация задач жизненного цикла безопасности требуются от независимого лица или группы, но эта группа никогда не обязана быть другой компанией.

Внутренний персонал компании способен и имеет право выполнять различные задачи проверки и валидации, при условии, что они достаточно независимы от группы, которая выполняла проектирование.

Хотя конкурентный тендер является эффективным инструментом для обеспечения того, чтобы продукты и услуги, используемые владельцем/эксплантатом процесса, имели хорошую стоимость, стандарты, определяющие жизненный цикл безопасности, не предъявляют требований к деловой практике, используемой для проектирования СПАЗ. Стандарты определяют только требования к функциональной безопасности, а не к минимальной стоимости жизненного цикла.

12.4. ТЕСТЫ ДЛЯ САМОПРОВЕРКИ.

Задание 12.4. Выбрать правильный ответ. Дать развернутое объяснение выбранному ответу со ссылкой на разделы стандартов.

Ответ и объяснения смотрите в разделе «ОТВЕТ», «Раздел 12»

Тест 12. 8. Обслуживание СПАЗ.

Вопрос 1. Какие из следующих утверждений о проектировании системы безопасности автоматизации (СПАЗ/SIS) являются верными?

А) СПАЗ/SIS должна быть спроектирована так, чтобы обеспечить возможность обслуживания без отключения системы.

В) В проекте СПАЗ/SIS допускается использование перемычек для проверки работоспособности датчиков.

С) Все элементы системы должны быть доступны для обслуживания без риска ложных срабатываний.

Д) При проектировании СПАЗ/SIS необходимо учитывать возможность проведения испытаний на действующем процессе.

Вопрос 2. Каковы основные технические и процедурные требования к испытанию СПАЗ/SIS?

А) Испытания должны проводиться только в условиях, когда система полностью отключена.

В) Необходимо наличие четких инструкций по проведению испытаний для каждого элемента системы.

С) Все испытания должны документироваться для обеспечения отслеживаемости и анализа.

Д) Испытания могут проводиться без участия обслуживающего персонала.

Вопрос 3. Как следует организовать обслуживание датчиков и исполнительных элементов в рамках действующего процесса?

А) Обслуживающий персонал должен иметь доступ к элементам системы в любое время без предварительного уведомления.

В) Необходимо разработать процедуры, которые минимизируют риск ложных срабатываний при обслуживании.

С) Обслуживание должно проводиться в часы пик производственного процесса для повышения эффективности.

Д) Датчики и исполнительные элементы должны быть защищены от случайного вмешательства во время обслуживания.

Тест 12.9. Группа оценки функциональной безопасности.

Вопрос 1 Какие из следующих утверждений о назначаемой группе оценки функциональной безопасности верны?

1. Группа должна включать технических специалистов, специалистов по применению и эксплуатации, необходимых для конкретного применения.

2. Группа должна включать как минимум одного опытного компетентного человека, не участвующего в работе проектной группы.

3. Группа должна включать как минимум одного опытного компетентного человека из независимой сторонней организации.

a) 1 и 2 верны, 3 – неверно.

b) 1 и 3 верны, 2 – неверно.

c) 2 и 3 верны, 1 – неверно.

d) 1, 2 и 3 верны.

e) Ни одно из вышеперечисленных утверждений неверно.

Тест 12.10.

Какое из следующих утверждений наиболее точно описывает разницу между верификацией и валидацией, как определено в МЭК 61508 и МЭК 61511?

a) Различий нет. Верификация и валидация имеют одинаковое значение.

b) Верификация описывает задачи проверки, выполняемые независимыми оценочными группами. Валидация описывает задачи проверки, выполняемые проектной группой.

c) Валидация – это деятельность по демонстрации того, что СПАЗ/SIS соответствует спецификациям требований безопасности. Верификация – это деятельность по демонстрации того, что для каждой фазы жизненного цикла безопасности выполнены требования модели жизненного цикла безопасности.

d) Валидация – это процесс создания «V»-диаграммы задач, необходимых для завершения жизненного цикла безопасности. Верификация – это процесс обеспечения того, что компетентные лица выполнили эти задачи.

e) Ни один из вышеперечисленных ответов неверен.

Тест 12.11.

Какие из следующих утверждений верны для требований к документированию задач жизненного цикла безопасности в соответствии с МЭК 61511?

1. Информация должна быть трассируемой до требований стандарта.

2. Бумажные копии информации должны храниться у инженеров, ответственных за выполнение отдельных задач жизненного цикла безопасности, и у руководителя, ответственного за общее выполнение проекта СПАЗ/SIS.

3. Информация должна быть структурирована таким образом, чтобы можно было осуществлять поиск необходимой информации.

- a) 1 и 2 верны, 3 – неверно.
- b) 1 и 3 верны, 2 – неверно.
- c) 2 и 3 верны, 1 – неверно.
- d) 1, 2 и 3 верны.
- e) Ни одно из утверждений неверно.

Тест 12.12.

Если пользователь компонента СПАЗ, спроектированного в соответствии со стандартом МЭК 61508, должен периодически проводить ручные испытания для достижения уровня SIL, указанного в сертификате продукта, *то информация о необходимости испытания и частоте его проведения должна быть предоставлена в документ.*

- a) Руководстве по безопасности продукта.
- b) Технических характеристиках продукта.
- c) Маркетинговых материалах.
- d) Руководствах по установке оборудования.
- e) Ни один из вышеперечисленных вариантов не подходит, поставщик не обязан предоставлять эту информацию клиенту.

ОТВЕТЫ.

РАЗДЕЛ 1.

Тест 1.13. Руководящие документы для проектирования СПАЗ.

Вопрос 1. В каком порядке следует применять закон от 21.07.1997 № 116-ФЗ и Приказ Ростехнадзора от 15.12.2020 N 533?

Ответ В. Сначала закон, затем Приказ Ростехнадзора.

Объяснение.

Закон № 116-ФЗ – это основополагающий документ, устанавливающий общие принципы промышленной безопасности (ст. 1, ст. 3).

Приказ № 533 – это подзаконный акт, конкретизирующий требования закона для взрывобезопасности (п. 1 Приказа).

Иерархия норм. Закон имеет высшую силу. Приказ не может ему противоречить, а лишь детализирует его положения.

Вопрос 2. Какое значение имеет закон № 116-ФЗ для проектирования систем безопасности?

Ответ В. Устанавливает общие принципы и требования.

Объяснение.

Закон определяет:

- Понятие опасного производственного объекта (ОПО) (ст. 2).
- Обязанности организаций по обеспечению безопасности (ст. 9).
- Требования к проектной документации (ст. 8).
- Порядок расследования аварий (ст. 12).

Он создает правовую основу, на которую опираются все отраслевые правила (включая Приказ 533).

Вопрос 3. Какую роль играет Приказ № 533 в контексте закона № 116-ФЗ?

Ответ В. Является дополнением и конкретизацией требований закона.

Объяснение.

Приказ № 533 развивает положения закона применительно к химическим, нефтехимическим и нефтеперерабатывающим производствам.

Он устанавливает конкретные технические и организационные меры по предотвращению взрывов (разделы II-VI Приказа), которые проектировщик СПАЗ обязан учитывать.

Приказ №533 утверждает федеральные нормы и правила (ФНП) «Общие правила взрывобезопасности...», прямо указывая, что эти Правила разработаны в соответствии с ФЗ №116-ФЗ и содержат конкретные обязательные требования (схемы расчёта категорий, критерии выбора ПАЗ и т.п.).

Иными словами, Приказ реализует и конкретизирует нормы закона технически и процедурно, не заменяя и не превосходя по юридической силе сам закон.

Вопрос 4. Почему важно соблюдать последовательность применения закона и приказа?

Ответ В. Чтобы избежать конфликтов в интерпретации норм.

Объяснение.

Соблюдение иерархии норм исключает применение подзаконных актов в противоречии с законом; это предотвращает юридические коллизии и обеспечивает единообразное толкование и применение требований к проектированию и эксплуатации ОПО.

Конституция и ФЗ прямо закрепляют приоритет законов и порядок правового регулирования, а ФНП должны соответствовать и конкретизировать положения закона.

Тест 1.14. Стандарты МЭК 61508 и 61511/

Вопрос 1. Какие основные цели преследуют стандарты?

Ответ.

А) Обеспечение функциональной безопасности СПАЗ/SIS.

С) Системный подход к управлению рисками.

Объяснение.

А) Главная цель СПАЗ обеспечить, чтобы СПАЗ/SIS выполняла свои функции безопасности с требуемой надежностью (SIL) на всем жизненном цикле (от концепции до вывода из эксплуатации).

С) Стандарты реализуют системную методологию, где безопасность достигается не только техническими решениями, но и строгими процессами (управление ЖЦ, верификация, компетентность персонала).

МЭК 61508-1, разд. 1.2: цель стандарта — установить требования для обеспечения функциональной безопасности систем, связанных с безопасностью (E/E/PE safety-related systems), на протяжении всего жизненного цикла.

МЭК 61511-1, разд. 1.1: определяет требования для систем безопасности (SIS) в процессных отраслях и фиксирует системный подход к управлению рисками, включая предотвращение системных ошибок.

Таким образом, оба стандарта: обеспечивают безопасность в течение всего жизненного цикла SIS; вводят системный подход к управлению рисками и предотвращению систематических отказов.

Вопрос 2. Чем отличается МЭК 61511 от МЭК 61508?

Ответ. В. МЭК 61508 – общий стандарт, а МЭК 61511 – это скорее руководство по применению МЭК 61508 для СПАЗ/SIS в процессных отраслях производств.

Объяснение (рис.1.1):

• МЭК 61508 – «базовый» стандарт по функциональной безопасности для любых Э/Э/ПЭ систем (автомобили, медтехника, АЭС, процессы). (1 Область применения 1.1. Настоящий стандарт охватывает вопросы, которые должны учитываться при использовании электрических, электронных, программируемых электронных (Э/Э/ПЭ) систем для выполнения функций безопасности).

• МЭК 61511 – технический стандарт, разработанный на основе МЭК 61508, но специализированный для СПАЗ/SIS исключительно в процессных отраслях (химия, нефтегаз, ТЭК). Он определяет требования к спецификации, проектированию, монтажу, эксплуатации и техническому обслуживанию приборной системы безопасности (СПАЗ/SIS) так, чтобы она могла надежно переводить и удерживать процесс в безопасном состоянии. См. ГОСТ Р МЭК 61511-1.



Рис. 13.1. Стандарты по приборной безопасности

Вопрос 3. Как принцип системности реализуется в стандартах?

Ответ А. Учет взаимосвязей между объектами ОПО и С) Унификация требований.

Объяснение.

А) Стандарты требуют анализа взаимодействия СПАЗ/SIS с другими системами (АСДУ, другие слои защиты) и технологическим процессом.

С) Они создают единую терминологию и методологию (SIL, ЖЦ, верификация), устраняя дублирование и противоречия в отраслевых нормах.

МЭК 61508-1, разд. 7.4 устанавливает, что безопасность рассматривается с учётом взаимосвязей между элементами, влиянием организационных и человеческих факторов.

МЭК 61511-1, разд. 3.2.63 указывает, что системный подход — это учёт взаимодействия между процессом, SIS, персоналом, эксплуатацией и организационными мерами.

То есть стандарты требуют рассматривать безопасность не изолированно по отдельным элементам, а во взаимосвязи всех компонентов и процессов. Варианты В, С и D не отражают системный подход (например, унификация не исключает дублирования).

Вопрос 4. Какие уровни системообразования выделяются?

Ответ: А) Расчет показателей надежности (SIL) и С) Диагностика и тестирование.

Объяснение.

А) Ключевой системообразующий элемент – количественная оценка безопасности через SIL (PFDavg/PFH).

С) Диагностика и тестирование – системные механизмы для контроля состояния СПАЗ/SIS и обнаружения отказов.

МЭК 61508 (часть 2, п. 7.4) определяет уровень полноты безопасности СПАЗ/SIS (SIL ()) как ключевой параметр надежности.

МЭК 61511 (п. 11.2) требует верификации уровня полноты безопасности (SIL) для СПАЗ/SIS.

Варианты В, С и D – вторичные требования, но не уровни системообразования.

Вопрос 5. Какие основные требования к жизненному циклу СПАЗ/SIS устанавливают стандарты?

Ответ А и В Проектирование, эксплуатация, вывод и Верификация и валидация на каждом этапе.

Объяснение.

А) Стандарты четко структурируют ЖЦ на фазы. анализ рисков, проектирование, эксплуатация, модификация, вывод.

В) Верификация (проверка соответствия требованиям) и валидация (проверка правильности работы в реальных условиях) обязательны на всех ключевых этапах ЖЦ.

МЭК 61508 (часть 1, п. 7.1. и 4.8 Требования к верификации, которые должны быть выполнены для каждой стадии жизненного цикла всей системы безопасности, определены в 7.18.)

МЭК 61511 (п. 12, п. 15) п. 12.5 Требования к верификации прикладной программы (проверка и тестирование). п.15 Подтверждение соответствия (валидация) безопасности приборной системы безопасности.

Вариант А неполный (не хватает верификации), С и D противоречат стандартам.

Вопрос 6. Почему диагностика и тестирование критичны?

Ответ: А) Позволяют обнаружить скрытые отказы и **С)** Обеспечивают соответствие требованиям SIL.

Объяснение.

А) Скрытые (необнаруженные) отказы – главная опасность для СПАЗ/SIS. Диагностика и тестирование снижают их вероятность, повышая готовность системы.

С) Заданный уровень SIL напрямую зависит от эффективности диагностики (SFF) и регулярности тестирования (интервалы влияют на PFDavg).

МЭК 61508 (часть 2, п. 7.4.) требует периодического тестирования для выявления скрытых отказов.

МЭК 61511 (п. 16.3) связывает диагностику с поддержанием SIL. Варианты В и D не являются основными причинами.

Вопрос 7. Что проверяет аудит функциональной безопасности?

Ответы: **А)** Соответствие процессов требованиям, **С)** Наличие отклонений и **Д)** Подтверждающие документы о компетенции персонала.

Объяснение.

МЭК 61508 (часть 1, п. 8) требует аудита для проверки соблюдения стандартов. МЭК 61508-1, разд. 8.2: аудит функциональной безопасности предназначен для проверки соответствия процессов установленным требованиям стандарта.

МЭК 61511-1, разд. 5.2.6: аудит используется для подтверждения того, что SIS соответствует как требованиям стандарта, так и спецификации требований безопасности (SRS).

Аудит проверяет фактическое соблюдение требований стандартов (МЭК 61508/61511) в процессах компании (управление ЖЦ, верификация, компетенции) и выявляет несоответствия между документацией и практикой.

Варианты В и D не являются основными задачами аудита.

Вопрос 8. Какое преимущество дает системный подход?

Ответ С. Согласование взаимосвязанных требований.

Объяснение.

С) Согласование взаимосвязанных требований к СПАЗ/SIS.

Системный подход в контексте стандартов (например, МЭК 61508, МЭК 61511 для систем безопасности) означает рассмотрение всего процесса, объекта или системы как единого целого, учитывая все его компоненты, их взаимосвязи, взаимодействия и весь жизненный цикл.

Это основное и ключевое преимущество системного подхода. Системы инструментальной безопасности (СПАЗ/SIS) – это сложные, междисциплинарные системы, включающие аппаратное обеспечение (датчики, логические решатели, исполнительные механизмы), программное обеспечение, человеческий фактор, процедуры эксплуатации и обслуживания.

Системный подход гарантирует, что все эти разрозненные, но взаимозависимые требования (например, к проектированию, установке, тестированию, эксплуатации, техническому обслуживанию, модификациям и выводу из эксплуатации) согласованы между собой. Это предотвращает.

Противоречия. Когда одно требование входит в конфликт с другим.

Пробелы. Когда какая-то важная область безопасности остается неучтенной.

Неэффективность. Когда отдельные части системы работают неоптимально из-за отсутствия единого видения.

В результате согласования достигается комплексная безопасность на протяжении всего жизненного цикла СПАЗ/SIS.

Другие варианты ответов.

А) Снижение дублирования требований в нормативных документах.

Частично верно, но это не основное преимущество. Системный подход может косвенно привести к уменьшению дублирования требований за счет лучшей структуризации и иерархии документов. Однако его основная цель не в «экономии текста», а в обеспечении полноты и непротиворечивости требований. Если бы целью было только снижение дублирования, можно было бы просто удалить повторяющиеся абзацы, но это не гарантировало бы согласованности или полноты.

В) Ускорение разработки СПАЗ/SIS без этапа валидации.

Категорически неверно. Этап валидации (проверка того, что система соответствует исходным требованиям безопасности и выполняет свою функцию) является критически важным и обязательным этапом в жизненном цикле любой системы безопасности (СПАЗ/SIS). Системный подход стандартов (например, МЭК 61511) как раз подчеркивает важность и необходимость валидации, включая ее в комплекс требований. Никакое ускорение разработки не может быть достигнуто за счет исключения ключевых этапов обеспечения безопасности. Наоборот, системный подход помогает обеспечить, что все необходимые этапы, включая валидацию, будут выполнены надлежащим образом.

Д) Повышение гибкости в выборе методов расчета надежности.

Неверно. Стандарты, основанные на системном подходе (особенно в области безопасности), наоборот, стремятся обеспечить строгость, предсказуемость и сравнимость методов расчета надежности. Они обычно ограничивают или четко регламентируют допустимые методы расчета, а не «повышают гибкость» в их выборе. Цель стандартов – не дать полную свободу, а обеспечить, чтобы расчеты были выполнены правильно, единообразно и приводили к достижению заданных уровней полноты безопасности (SIL). Гибкость в данном случае могла бы привести к неконтролируемым и потенциально небезопасным результатам. МЭК 61508 (часть 1, п. 5.1) подчеркивает интеграцию всех этапов жизненного цикла.

Тест 1.15. ГОСТ Р МЭК 61508-6-2012 и проектирование СПАЗ/SIS.

Вопрос 1. Какие методы вероятностных расчетов используются?

Ответ. 1) Модель Маркова; **2)** Анализ дерева отказов (FTA); **4)** Метод Монте-Карло.

Объяснение.

- Модель Маркова. Анализирует состояния системы и переходы между ними (особенно для систем с ремонтом/восстановлением).
- FTA. Выявляет комбинации событий (отказов), ведущих к опасному состоянию системы («вершина» дерева).
- Метод Монте-Карло. Статистическое моделирование для оценки надежности сложных систем.

Вопрос 2. Какие параметры безопасности используются для режимов с низкой и высокой частотой запросов?

Ответы: 1. PFDavg (для низкой частоты); **2)** PFH (для высокой частоты).

Объяснение.

• PFDavg (Average Probability of Failure on Demand). Средняя вероятность опасного отказа по требованию (Low Demand Mode, SIL 1-3).

• PFH (Probability of Dangerous Failure per Hour). Вероятность опасного отказа в час (High Demand / Continuous Mode, SIL 1-4).

Вопрос 3. Что такое «подтверждение соответствия безопасности»?

Ответ 1. Проверка, что система соответствует требованиям SIL через тестирование и расчеты.

Объяснение.

ГОСТ Р МЭК 61508-6-2012 (п. 7.18) устанавливает, что подтверждение безопасности (safety validation) включает анализ, тестирование и расчёты для демонстрации соответствия требованиям SIL.

Это формальный процесс, включающий анализ, расчеты (PFDavg/PFH), Тестирование и экспертизу, доказывающий, что спроектированная СПАЗ/SIS достигает требуемого уровня SIL. Результат оформляется отчетом.

Вопрос 4. Какие требования к модели расчета?

Ответ 1. Учет как случайных, так и систематических отказов.

Объяснение.

Модель должна оценивать вклад случайных отказов (аппаратные сбои) и систематических отказов (ошибки проектирования, ПО, производства). Хотя вероятность систематических отказов сложно количественно оценить, модель должна показывать, что меры по их предотвращению соответствуют требуемому SIL.

Вопрос 5. Какие факторы влияют на выбор архитектуры?

Ответ: 1) Требуемый уровень SIL; **2)** Экономическая целесообразность; **3)** Сложность обслуживания.

Объяснение.

• SIL. Главный фактор. Высокий SIL требует резервирования (2Н, 2oo3Н).

- Экономика. Резервирование дорожке (оборудование, обслуживание).
- Обслуживание. Сложные системы требуют более квалифицированного персонала и времени.

Вопрос 6. Для чего используется FTA?

Ответ 1. Для определения корневых причин аварий и **2)** Для расчета вероятности отказа системы (п. В.2 ГОСТ Р МЭК 61508-6-2012).

Объяснение.

FTA выявляет комбинации базовых событий (отказы компонентов, ошибки), приводящих к аварийному событию (опасный отказ системы).

Тест 1.16. ГОСТ Р МЭК 61511-3-2018 и проектирование СПАЗ (СПАЗ/SIS).

Вопрос 1. Какие методы анализа рисков описаны в стандарте?

Ответ: 1) Качественный граф риска (Приложение Е), **2)** Полуколичественный анализ дерева событий (Приложение В) и **3)** Калиброванный граф риска (Приложение D).

Объяснение.

Приложение Е (Качественный граф риска).

Этот метод основан на экспертных суждениях и качественной оценке факторов риска, таких как тяжесть последствий, частота воздействия (потенциальная частота возникновения опасного события), возможность предотвращения (наличие независимых защитных слоев) и степень снижения риска, необходимая для достижения приемлемого уровня безопасности. Он используется для назначения SIL на основе субъективной, но обоснованной оценки ситуации.

Приложение В (Анализ дерева событий).

Это полуколичественный метод, который систематически оценивает последствия исходного нежелательного события. Он анализирует последовательность событий и реакций систем (слоев) защиты (функциональных событий защиты) для определения вероятности различных исходов, включая аварийные сценарии. Он позволяет оценить эффективность существующих слоев защиты и рассчитать общую вероятность нежелательного события с учетом их работы.

Приложение D (Калиброванный граф риска).

Этот метод представляет собой комбинацию качественного и количественного подходов. Он использует качественные параметры, аналогичные тем, что применяются в качественном графе риска, но с добавлением количественной калибровки для каждого шага или параметра. Это позволяет получить более точную и объективную оценку риска и назначить соответствующий SIL. Он обеспечивает мост между чисто качественными оценками и требовательными количественными анализами, предлагая баланс между простотой и точностью.

Все эти методы служат одной основной цели. определить требуемый уровень полноты безопасности (SIL) для каждой функции безопасности (SIF) в СПАЗ, исходя из анализа риска, связанного с процессом, и с учетом существующих независимых слоев защиты.

На практике, помимо методов, описанных в приложениях, очень часто применяется метод анализа слоев защиты (LOPA). LOPA является развитием полуколичественного подхода и широко используется для определения SIL, так как он систематически учитывает частоту исходного события и вероятность отказа каждого независимого слоя защиты. Хотя LOPA не представлен как отдельное приложение в этом стандарте, он является широко признанным и соответствующим требованиям стандарта методом.

Выбор конкретного метода зависит от различных факторов, включая сложность процесса, объем доступных данных, требуемую точность анализа, внутренние процедуры компании и законодательные требования.

Вопрос 2. Для чего используется матрица слоев безопасности (Приложение С)?

Ответ 1. Для визуализации связи между рисками и слоями защиты.

Объяснение.

Матрица наглядно отображает, как различные слои защиты (базовый контроль, предупредительная сигнализация, СПАЗ/SIS, физическая защита) влияют на снижение риска для конкретной опасности. Помогает понять достаточность существующих слоев.

Вопрос 3. Что такое «калиброванный граф риска» (Приложение D)?

Ответ 1. Метод, сочетающий качественные и количественные данные для оценки SIL.

Объяснение.

Этот метод использует структуру качественного графа риска (Прил. Е), но «калибрует» его с использованием количественных данных (например, частоты исходных событий, вероятности отказа слоев защиты). Это повышает объективность назначения SIL.

Вопрос 4. Какие методы относятся к качественным?

Ответ: 1) Граф риска (Приложение Е) и **3)** Качественный подход для назначения SIL (Приложение Н).

Объяснение.

Приложение Е и Н – чисто качественные методы. Назначение SIL основано на суждениях и опыте специалистов, оценивающих параметры риска (тяжесть, вероятность, предотвращение) без численных расчетов.

Вопрос 5. Что такое «анализ слоев защиты» (LORA)?

Ответ 1. Оценка эффективности каждого слоя защиты в снижении риска.

Объяснение.

LORA (прил. F и G) – полуколичественный метод. Он определяет, насколько каждый независимый слой защиты снижает частоту нежелательного события. Суммарное снижение риска должно достигать целевого уровня. Если нет, требуется СПАЗ/SIS с определенным SIL.

Вопрос 6. Для чего Приложение I в ГОСТ Р МЭК 61511-3-2018?

Ответ 1. Создание и калибровка графа риска.

Объяснение.

Приложение I содержит практические рекомендации по разработке и калибровке параметров графа риска (как качественного из Прил. E, так и калиброванного из Прил. D).

Вопрос 7. Какой метод позволяет назначить SIL без точных расчетов?

Ответ 1. Качественный граф риска (Приложение E).

Объяснение.

Приложение E описывает риск-граф, где SIL назначается по качественным параметрам (тяжесть последствий, частота, возможность предотвращения).

Это метод «без точных расчетов», в отличие от LORA и калиброванных графов. Он позволяет присвоить SIL на основе экспертной оценки риска и эффективности существующих слоев защиты без выполнения сложных количественных расчетов (PFD_{avg}/PFH).

Вопрос 8. Какие параметры учитывает калиброванный граф риска (Приложение D)?

Ответ 1. Тяжесть последствий, вероятность события, возможность предотвращения аварии.

Объяснение.

Как и качественный граф, калиброванный граф использует параметры:

C (Последствия). Тяжесть ущерба.

F (Частота и время нахождения в опасной зоне). Вероятность возникновения опасной ситуации и нахождения в ней людей/объектов.

P (Возможность предотвращения). Шанс избежать последствий после инициирующего события.

W (Вероятность нежелательного события). Частота исходного события.

Ключевое отличие. Эти параметры калибруются количественными данными (например, W берется из статистики/расчетов, P оценивается численно).

Вопрос 9. Какой метод сочетает качественные и количественные данные?

Ответ 1. Калиброванный граф риска (Приложение D).

Объяснение.

Чисто качественные — Прил. E, H; количественные — ETA (B), LOPA (C, F, G).

Калиброванный граф риска отталкивается от качественной логики графа риска, но калибруется количественными данными (частоты, вероятности).

Приложение D специально разработано как гибридный метод. Он берет структуру и логику качественного графа (Прил. E), но использует количественно определенные или оцененные входные параметры (W, C, F, P), что делает назначение SIL более обоснованным и воспроизводимым.

РАЗДЕЛ 2.

Тест 2.4. Базовый перечень технической документации для выполнения HAZOP.

Ответ b.

Все остальные документы требуются всем участникам РНА и перечислены в качестве обязательной информации о безопасности процесса, например, US OSHA и US EPA для выполнения эффективного анализа опасностей процесса.

Объяснение. Внутренние схемы электропроводки СПАЗ/SIS не помогают в оценке риска и поэтому не требуются на этапе анализа риска. на самом деле, они могут даже быть недоступны, если проект предназначен для нового участка. Если требуется такая специализированная информация, она может быть предоставлена и интерпретирована специалистом на специальной основе. в контексте HAZOP (или других методов РНА, таких как What-If, FMEA) основная цель — анализ технологических опасностей, а не детальное проектирование СПАЗ/SIS. Участники HAZOP фокусируются на.

- Параметрах процесса (давление, температура, уровень и т. д.),
- Отклонениях от нормального режима,
- Причинах и последствиях этих отклонений,
- Рекомендациях по мерам защиты (включая общие требования к СПАЗ/SIS, но не их детализацию).

Внутренняя проводка СПАЗ/SIS (например, соединения между логическим solver и модулями ввода/вывода) — это деталь реализации, которая обычно не требуется для HAZOP.

HAZOP не занимается проверкой соответствия стандартам SIL или МЭК 61508/61511 — этим занимается анализ СПАЗ/SIS (например, LOPA или детальное проектирование SRS).

Если участникам HAZOP понадобится информация о зонах взрывоопасности или искробезопасности, они могут запросить общие данные о классификации зон (Ответ «с»), но не схемы внутренней разводки СПАЗ/SIS.

Тест 2.5. Применение HAZOP и FTA для анализа безопасности.

Вопрос 1.

Объяснение.

Ответ В. Что такое HAZOP?

HAZOP (Hazard and Operability Study) – это систематический и структурированный метод качественного анализа, используемый для выявления потенциальных опасностей (hazards) и проблем работоспособности (operability problems), которые могут возникнуть из-за отклонений в проектировании или эксплуатации системы.

В контексте СПАЗ/SIS HAZOP применяется для тщательного изучения функций СПАЗ/SIS, ее взаимодействия с технологическим процессом и потенциальных сбоев, которые могут привести к опасным ситуациям. Метод позволяет выявить отклонения в работе системы и их причины через ключевые слова (например, «нет сигнала», «ложное срабатывание»).

Типичные направляющие слова. «Нет», «Больше», «Меньше», «Часть от», «Наоборот», «Другое, чем», «Помимо».

Примеры для СПАЗ/SIS.

«Нет» + «Сигнал». «Нет сигнала от датчика».

«Больше» + «Давление». «Давление выше уставки, но клапан не сработал» (Failure to trip).

«Другое, чем» + «Срабатывание». «Ложное срабатывание» (Spurious trip).

«Меньше» + «Расход». «Расход ниже критического уровня, но сигнализация не работала».

«В контексте СПАЗ/SIS» HAZOP помогает идентифицировать, когда СПАЗ/SIS может не сработать, сработать некорректно или вообще не выполнить свою защитную функцию, что критически важно для анализа безопасности.

Другие варианты.

Ответ А. Почему это неверно?

FTA – это дедуктивный, «сверху-вниз» метод, который начинается с нежелательного «топового события» (например, аварии) и графически отображает комбинации базовых событий (отказов компонентов, человеческих ошибок), которые могут привести к этому топовому событию.

FTA часто используется для количественной оценки вероятности аварии, в то время как HAZOP – это качественный метод идентификации опасностей. Результаты HAZOP могут быть исходными дан-

ными для построения дерева отказов (т.к. HAZOP выявляет потенциальные сбои), но сам HAZOP не занимается построением дерева отказов.

Ответ С. Почему это неверно? Этот ответ связан с планированием реагирования на чрезвычайные ситуации, процедурами восстановления или анализом ремонтпригодности, а не с основной целью HAZOP.

HAZOP выявляет потенциальные сбои и их последствия. На основе этих выводов могут быть разработаны процедуры восстановления или рекомендации по повышению восстанавливаемости.

Однако первичная цель HAZOP – это идентификация опасностей и проблем, а не разработка планов восстановления после того, как отказ уже произошел. HAZOP скорее сосредоточен на предотвращении или минимизации вероятности сбоя СПАЗ/SIS.

Ответ D. Почему это неверно?

Это относится к анализу надежности или количественной оценке SIL. Методы оценки надежности, такие как FMEA (Анализ Видов и Последствий Отказов) или специализированные расчеты SIL, используют статистические данные об отказах (например, вероятности отказа по требованию, интенсивности опасных отказов) для количественной оценки надежности компонентов или всей СПАЗ/SIS.

Основная цель HAZOP, особенно в контексте СПАЗ/SIS, – это систематическое выявление всех возможных отклонений СПАЗ от проектных условий или проектного поведения системы, а также их потенциальных причин и последствий, используя структурированный подход с ключевыми словами. Это позволяет превентивно выявить уязвимости безопасности, которые могут привести к авариям, и предложить меры по их устранению или смягчению.

Вопрос 2. Ответ В.

Объяснение.

FTA анализирует логические комбинации отказов (И/ИЛИ) через дерево событий. А HAZOP не рассчитывает вероятности, а выявляет потенциальные отклонения. Ответ С неверен, так как HAZOP не работает с комбинациями событий количественно.

Вопрос 3. Ответ В.

Объяснение.

Логические вентили – основа FTA (В).

Ключевые слова (Ответ А) – инструмент HAZOP.

Ответы С и D могут относиться к обоим методам, но не являются их уникальными чертами.

Вопрос 4. Ответ В.

Объяснение.

Для анализа, почему СПАЗ/SIS не выдала сигнал аварийного останова в конкретном случае отказа, наиболее подходящим методом является ответ В. FTA (Анализ дерева отказов) – это дедуктивный,

«сверху вниз» метод анализа. Он начинается с конкретного нежелательного «верхнего события» (в данном случае, «СПАЗ/SIS не выдала сигнал аварийного останова») и логически разбивает его на все возможные комбинации базовых событий, которые могли привести к этому отказу. Цель ФТА – определить конкретные причины и их комбинации, которые привели к наблюдаемому отказу. Это идеально подходит для диагностики уже произошедшего отказа.

HAZOP– это индуктивный, «снизу вверх» метод. Он используется для систематического выявления потенциальных опасностей и проблем с работоспособностью в системе, как правило, на стадии проектирования или для плановой оценки рисков. HAZOP исследует, что может пойти не так (потенциальные отклонения от проектных параметров) и каковы их причины и последствия. Хотя HAZOP может выявить сценарии, при которых СПАЗ/SIS может отказать, его основная задача – превентивное выявление рисков, а не диагностика конкретной причины уже произошедшего сбоя.

FMEA – это также индуктивный метод, «снизу вверх». Он систематически исследует каждый компонент системы, определяет все возможные «режимы отказа» этого компонента и их потенциальные «эффекты» на систему в целом. FMEA отлично подходит для выявления всех возможных способов отказа компонентов и их последствий, а также для оценки риска. Он помогает понять, как компоненты могут отказать, но не так эффективно, как ФТА, выявляет конкретную комбинацию событий, приведшую к определенному системному отказу.

Так как вопрос сформулирован. «почему СПАЗ/SIS не выдала сигнал...», то указывает на уже произошедший отказ, для которого нужно найти конкретные причины и их комбинации. Для такой задачи ФТА является самым прямым и эффективным инструментом, поскольку он разработан именно для ретроспективного анализа отказов, начиная с наблюдаемого нежелательного события.

Вопрос 5.

Ответ В.

Объяснение.

Результат HAZOP всегда документируется в таблицах: параметр - отклонение - причины - последствия - меры/рекомендации

ФТА дает дерево отказов (Ответ А), а

SIL (Ответ D) определяется через PFD_{avg}/PFH .

Вопрос 6. Ответ В.

Объяснение.

HAZOP – качественный метод, который выявляет риски, но не вычисляет вероятности (В).

Для SIL нужны количественные данные (PFD_{avg}), которые дает ФТА или FMEA.

Ответ D неверен. HAZOP применим к СПАЗ/SIS, но для других целей.

Вопрос 7.**Ответ А.****Объяснение.**

FTA выявляет критические компоненты через анализ их вклада в вероятность отказа (Ответ А).

Мозговой штурм (Ответ В) – особенность HAZOP.

FTA учитывает даже редкие события.

(Ответ D – ложно).

Вопрос 8. Ответ А и С.**Объяснение.**

HAZOP – проактивный метод. «Что если система получит некорректный сигнал?» (профилактика).

FTA – реактивный метод. «Почему СПАЗ/SIS не сработала?» (анализ причин).

Ответ В неверен – оба метода используются на этапе проектирования.

Ответ D ошибочен – FTA и HAZOP применимы к любым компонентам СПАЗ/SIS.

РАЗДЕЛ 3.**Тест 3.6. Построить Дерево отказов.**

Вопрос 1. Рассчитайте частоту незапланированного открытия клапана.

Ответ С. 0,35 раз/год.

Объяснение.

Незапланированное открытие клапана возникает из трех причин.

Ошибка оператора/ремонтника. 0,2 раз/год.

Отказ оборудования управления. 0,1 раз/год.

Отказ программы ПЛК. 0,05 раз/год.

При объединении независимых причин через логическое OR (любой из оснований вызывает незапланированное открытие) и при малых интенсивностях частоты обычно при расчетах складываются:

$$0,2 + 0,1 + 0,05 = 0,35 \text{ раз/год. } 0,2 + 0,1 + 0,05 = 0,35 \text{ раз/год.}$$

Вопрос 2. Какова частота ошибочного теста на вакуум?

Ответ С. 0,3 раз/год.

Объяснение.

Ошибочный тест на вакуум включает.

Ошибка программы проверки. 0,2 раз/год.

Ошибка техсредств контроля. 0,1 раз/год.

Суммарная частота.

$$0,2 + 0,1 = 0,3 \text{ раз/год.}$$

Вопрос 3. Рассчитайте ожидаемую частоту впрыска до вакуумирования.

Ответ С. 0,4 раз/год.

Объяснение.

Впрыск до вакуумирования происходит из-за:

Отказа клапана – 0,05 раз/год.

Незапланированного открытия клапана – 0,35 раз/год.

Суммарная частота:

$0,05 + 0,35 = 0,4$ раз/год.

Вопрос 4. Почему данные задачи противоречивы?

Ответ б. 1,05 раз/год.

Объяснение.

Обоснование: В тексте задано, что частота формирования взрывчатой смеси = 1,05 раз/год, а также отдельно указаны ветви, дающие 0,1 и 0,55 (их сумма 0,65), т.е. $0,65 \neq 1,05$.

Кроме того, в тексте та же «присутствие воздуха после вакуумирования 0,55» фигурирует как самостоятельная ветвь формирования смеси и одновременно как причина «впрыска до вакуумирования», что явно приводит к двойному учёту одной и той же причины.

Также суммирование причин для «впрыска до вакуумирования» ($0,05+0,35+0,55$) даёт 0,95, что не совпадает ни с ранее заявленным 0,1, ни с 0,55 и т. д.

Таким образом противоречие в основном в том, что суммы частот для формирования взрывчатой смеси не сходятся с указанной общей частотой 1,05, и что одни и те же элементы учтены в разных ветвях, что приводит к двойному их учёту.

Вопрос 5. Если проигнорировать противоречия, чему равна частота критического случая?

Ответ А. 0,21 раз/год.

Объяснение.

Если принять данную в самом начале агрегированную величину формирования взрывчатой смеси = 1,05 раз/год и вероятность воспламенения 0,2, то частота критического случая рассчитывается стандартно как: критический случай = формирование смеси × вероятность воспламенения, что = $1,05 \times 0,2 = 0,21$ раз/год.

Этого же числа (0,21) прямо указано в формулировке задания. Поэтому при игнорировании противоречий ответ (а) корректен.

Тест 3.7. Дерево событий.

Вопрос 1.

Ответ б. Учитывая приведенное дерево событий, частоту опрокидывания и разрушения железнодорожной цистерны, частота мгновенного возгорания, наиболее близка к **б**.

При решении дерева событий частота интересующего результата получается путем умножения частоты инициирующего события на все вероятности трека событий к результату. Инициирующее событие, опрокидывание и разрушение вагона, имеет частоту $8,0 \times 10^{-5}$ в год. Эта частота умножается на вероятности 0,2, 0,25 и 0,05, которые находятся на пути к интересующему результату (вспышка пожара).

Если существует более одного пути к интересующему результату, частоты отдельных путей следует суммировать, чтобы получить общую частоту событий.

В этом случае, например, какова будет частота экологического инцидента?

(Расчет. $1,2 \times 10^{-5} + 3,2 \times 10^{-5} + 3,2 \times 10^{-5} = 7,6 \times 10^{-5}/\text{год.}$).

Тест 3.8. Анализ LOPA защиты ОПО.

Вопрос 1.

Ответ а. Сигналы тревоги на пульте оператора должны быть рационализированы.

Объяснение.

Что означает рационализация сигналов тревоги (**ответ а**). Это ключевой аспект, который позволяет оператору эффективно реагировать на тревоги. Если на пульт оператора поступает слишком много сигналов тревоги, особенно ложных, это может привести к «усталости от тревог», когда оператор игнорирует важные предупреждения. Поэтому необходимо, чтобы сигналы тревоги были упорядочены и представлены в ясной и понятной форме, чтобы оператор мог быстро и правильно реагировать на реальные угрозы.

Жесткое подключение индикатора к СПАЗ (**ответ б**). Хотя это может быть полезным, жесткое подключение не является обязательным условием для того, чтобы сигнал тревоги считался слоем защиты. Важно, чтобы система была спроектирована так, чтобы оператор мог эффективно реагировать на сигналы тревоги, но жесткое подключение не является критерием.

Сертификация оборудования SIL (**ответ с**). Хотя сертификация SIL важна для обеспечения надежности систем безопасности, наличие сертификации не является необходимым условием для того, чтобы сигнал тревоги оператора был принят как слой защиты. Главное – это правильная организация и управление сигналами тревоги.

Качественный LOPA и сигналы тревоги (**ответ d**). Утверждение, что качественный LOPA не использует сигнал тревоги оператора в качестве слоя защиты, не является верным. Сигналы тревоги могут быть частью системы защиты, если они правильно организованы и интегрированы в процесс реагирования.

Заключение.

Сигналы тревоги оператора могут быть слоем защиты в рамках LOPA, но для этого необходимо, чтобы они были рационализированы. Это означает, что система сигнализации должна быть спроектирована так, чтобы минимизировать количество ложных тревог и обеспечить оператору четкие процедуры реагирования. Это критически важно для эффективного управления рисками и обеспечения безопасности на производстве.

Было бы неуместно заявлять PFD 0,1, если система сигнализации не рационализирована, если оператор подвергается потокам сигналов тревоги и ложным сигналам тревоги или если процедуры реагирования на сигналы тревоги не предоставляются автоматически и в контексте.

Тест 3.9. Влияние ручных проверочных испытаний на PFDavg для структуры SIF 1001 с учетом их периодичности.

Вопрос 1.

Ответ В. $PFD_{avg} = \lambda d \times T_i / 2$.

Объяснение.

PFDavg- это средняя вероятность отказа по требованию. Проще говоря, это вероятность того, что система безопасности откажет (не выполнит свою функцию), когда в ней возникнет необходимость, усредненная за определенный период времени. Чем ниже PFDavg, тем надежнее система.

SIF 1001- это конфигурация системы безопасности, где для выполнения функции требуется работа только одного элемента. Если этот элемент выходит из строя, функция безопасности также отказывает. Это самая простая и наименее избыточная конфигурация.

Ручные проверочные испытания. Это периодические испытания, которые проводятся для обнаружения скрытых опасных отказов в системе, которые не могут быть обнаружены автоматической диагностикой. После обнаружения, отказ устраняется, и система возвращается в работоспособное состояние.

λD (Интенсивность опасных отказов). Это частота, с которой компонент выходит из строя опасным и незамеченным образом.

T_i (Test Interval)- это интервал между последовательными проверочными испытаниями.

Влияние Ручных Проверочных Испытаний на PFDavg.

Ручные проверочные испытания играют ключевую роль в поддержании низкого значения PFDavg для структур SIF 1001, благодаря.

1. Обнаружению Скрытых Отказов. Основная цель этих тестов – найти опасные отказы, которые произошли с момента последнего испытания, но не были обнаружены автоматической диагностикой (если она есть). Без таких тестов, эти скрытые отказы накапливались бы, делая систему все более ненадежной, пока она не отказала бы при реальном запросе.

2. «Сбросу» Вероятности Отказа. Каждый раз, когда проводится успешное проверочное испытание, и любые обнаруженные отказы устраняются, выполняется «сбрасывание» накопленной вероятности отказа по требованию. Сразу после теста PFD стремится к нулю, а затем начинает линейно расти до следующего теста.

3. Периодичности (T_i). Чем чаще проводятся проверочные испытания (т.е. чем меньше T_i), тем меньше времени у скрытых отказов

для накопления. Это напрямую приводит к более низкому PFD_{avg} и, следовательно, к повышению уровня безопасности. И наоборот, увеличение интервала T_i приводит к повышению PFD_{avg} .

Для системы 1001 с периодическими проверочными испытаниями наиболее распространенная упрощенная формула PFD_{avg} выглядит так:

$$PFD_{avg} = \lambda D \times T_i / 2.$$

PFD_{avg} определяется как средняя частота отказов при наличии запроса, произошедших за время t . При ручных проверочных испытаниях с периодичностью T_i , когда $\lambda d \times t$ остается значительно меньше единицы, PFD_{avg} можно выразить как $PFD_{avg} = \lambda d \times T_i / 2$. Это означает, что с увеличением интервала между проверками T_i , PFD_{avg} может быть уменьшен.

Вопрос 2. Влияние интервала T_i . Какое влияние оказывает увеличение интервала T_i на значение PFD_{avg} ?

- A) Увеличение PFD_{avg} .
- B) Уменьшение PFD_{avg} .
- C) Не влияет на PFD_{avg} .
- D) Увеличивает вероятность отказа.

Вопрос 2. Ответ А. Увеличение PFD_{avg} .

Объяснение.

Физический смысл:

Чем дольше система работает без проверки (больше T_i), тем больше времени скрытые неисправности могут оставаться необнаруженными и, следовательно, вероятность того, что система окажется в неработоспособном состоянии в момент аварии, будет выше. Однако, выбор интервала T_i является компромиссом между требованиями безопасности и экономической эффективностью СПАЗ.

Вопрос 3. Ответ В. Когда $\lambda d \times t$ значительно меньше единицы.

Объяснение.

Упрощенная формула $PFD_{avg} = \lambda d \times T_i / 2$ применяется, когда это произведение значительно меньше единицы. Это позволяет использовать линейное приближение, что делает расчеты более простыми и понятными.

Вопрос 4. Ответ А. 0.0025.

Объяснение.

Подставим значения в формулу

$$PFD_{avg} = \lambda d \times T_i / 2. PFD_{avg} = (0.01)(20) / 2 = 0.1.$$

Это значение показывает, что вероятность отказа системы в данном интервале времени составляет 10%.

Одним из факторов улучшения показателя PFD_{avg} является применение ручных проверочных испытаний. Мы можем воздействовать на этот показатель, т.к. у нас есть возможность выбирать интервал между проверками так, чтобы улучшить значения PFD_{avg} для изделий соответствующей категории. Формула, связывающая величину

PFDavg с интенсивностью опасных отказов, для рассматриваемой одноканальной системы имеет следующий вид. Накопленная вероятность отказа одноканального устройства $p(t) = 1 - e^{-\lambda_d \times t}$.

Обычно значение произведения $\lambda_d \times t$ значительно меньше единицы, что позволяет считать, что $p(t) = \lambda_d \times t$, и принять, что зависимость между p и t имеет вид прямой линии с наклоном λ_d . Теперь показатель PFDavg определяется как средняя частота отказов при наличии запроса, произошедших за время t . При проведении ручных проверочных испытаний с периодичностью T_i , при условии, что значение $\lambda_d \times t$ остается значительно меньше единицы, величина PFDavg определяется соотношением $PFDavg = \lambda_d \times T_i / 2$. Смысл этого выражения состоит в том, что с помощью частых проверочных испытаний значение PFDavg может быть сделано меньше, чем λ_d .

Тест 3.10. Слои защиты.

Вопрос 1. В реакторе срабатывает аварийная сигнализация при малом потоке. Может ли считаться слоем защиты аварийная сигнализация на экране компьютера АСДУ?

Ответ А. Не может считаться.

Объяснение. Аварийная сигнализация на экране АСДУ не является независимым слоем защиты, так как она требует вмешательства оператора, и ее эффективность зависит от квалификации оператора и состояния системы управления. Это подтверждается стандартами МЭК 61508 и МЭК 61511, которые подчеркивают необходимость наличия независимых слоев защиты, которые не зависят от человеческого фактора.

Вопрос 2. Каковы ключевые требования стандарта МЭК 61508 в контексте слоев защиты?

Ответ D. Все вышеперечисленное.

Объяснение. Стандарт МЭК 61508 описывает функциональную безопасность и требует, чтобы слои защиты были независимыми, снижали риск непреднамеренных событий и их эффективность проверялась. Каждый слой защиты должен снижать риск непреднамеренных событий, и их эффективность должна быть проверена. Важно, чтобы слои защиты были независимыми друг от друга, чтобы избежать общей уязвимости. Если аварийная сигнализация зависит от работы оператора АСДУ, то она не может считаться независимым слоем защиты.

Вопрос 3. Почему аварийная сигнализация, требующая вмешательства оператора, не может считаться надежным слоем защиты?

Ответ D. Все вышеперечисленное

Объяснение. Аварийная сигнализация, требующая вмешательства оператора, не может считаться надежным слоем защиты, так как она не предотвращает аварийные ситуации автоматически и зависит от человеческого фактора и квалификации оператора.

Вопрос 4. Каковы основные акценты стандарта МЭК 61511 в отношении систем безопасности процессов?

Ответ В. Каждый слой защиты должен быть независимым.

Объяснение. Стандарт МЭК 61511 подчеркивает важность наличия независимых слоев защиты, которые способны предотвращать или смягчать последствия аварийных ситуаций без зависимости от других слоев.

Стандарт МЭК 61511, который касается систем безопасности процессов, также важность наличия независимых слоев защиты. Он акцентирует внимание на том, что каждый слой должен быть способен предотвратить или смягчить последствия аварийных ситуаций без зависимости от других слоев.

Аварийная сигнализация, которая требует вмешательства оператора, не является автоматическим слоем защиты. Она может быть частью системы управления, но не может считаться надежным слоем защиты, так как зависит от человеческого фактора.

Аварийная сигнализация на экране АСДУ не является независимым слоем защиты, так как она требует вмешательства оператора, и ее эффективность зависит от квалификации оператора и состояния системы управления. Это подтверждается требованиями стандартов МЭК 61508 и МЭК 61511.

Заключение

Использование общих датчиков в системах безопасности и управления недопустимо из-за нарушения принципов независимости, возможности отказов по общим причинам, отсутствия отдельного защитного уровня и потенциально неадекватных процедур обслуживания. Эти факторы могут существенно снизить уровень безопасности и повысить риск аварий на производстве.

В прежних руководящих материалах ISA и в новом стандарте МЭК 61511 содержатся допустимые исключения из правил раздельного использования датчиков и исполнительных устройств. Совместное использование допускается в системах с уровнем полноты безопасности SIL 1, если удастся доказать, что требования полноты безопасности при этом будут выполнены. Это возможно только в том случае, если датчик использовался в АСДУ для функции управления, не связанной с задачами СПАЗ/SIS. В таком случае отказ датчика не будет способствовать увеличению опасных запросов на СПАЗ/SIS. Практически это весьма маловероятно, если только датчик не используется как записывающее устройство.

Даже в этом примере датчик следовало бы с самого начала рассматривать как часть СПАЗ/SIS, со всеми ее функциями защиты и тестирования, а уж затем передать сигнал на вход в РСУ через устройство защиты цепи. Для выполнения заданных требований по надежности в этом случае также понадобится дополнительная диагностика.

Тест 3.11. Оценка независимости слоев защиты в системе управления

Вопрос 1. Какова основная функция ОСУП в контексте управления температурой в реакторе?

Ответ В. Прекращение подачи пара в рубашку реактора при превышении температуры.

Объяснение. АСДУ предназначена для автоматического управления подачей пара в рубашку реактора, что позволяет предотвратить превышение температуры и, как следствие, высокое давление.

Вопрос 2. Является ли АСДУ независимым слоем защиты в данной системе управления?

Ответ С.

Объяснение. АСДУ может считаться независимым слоем защиты, если она работает в автоматическом режиме и способна выполнять свою функцию без отказов. В данном случае, полагая, что АСДУ имеет высокую надежность, можно считать ее независимым слоем защиты.

Вопрос 3. Почему прекращение подачи пара в рубашку реактора можно считать слоем защиты?

Ответ А. Оно снижает риск возникновения аварийной ситуации. Прекращение подачи пара в рубашку реактора снижает риск возникновения высоких давлений, что делает его эффективным слоем защиты в системе управления.

Объяснение.

В данной задаче важно понимать, как различные слои защиты взаимодействуют друг с другом и как их надежность влияет на общую безопасность системы. СПАЗ и АСДУ работают в тандеме, чтобы предотвратить аварийные ситуации, и правильная оценка их надежности и независимости критична для обеспечения безопасной работы реактора.

Так как прекращение подачи пара способно предотвратить высокое давление, то АСДУ является слоем защиты. АСДУ является очень надежной цифровой системой управления, и оперативный персонал никогда не наблюдал отказа, в результате которого перестал бы работать контур управления температурой. Группа АСЗ принимает решение, что средняя вероятность отказа при наличии запроса составляет 0,1, и вносит значение 0,1 в колонку «АСДУ» графы 5 (0,1 - это минимально допустимое значение для АСДУ).

Давайте пошагово разберем задачу по расчету SIL для системы защиты от утечки метана.

Тест 3.12. СПАЗ для системы защиты утечки метана (частота 2×10^{-2} /год) реализована на основе датчика газа (PFD=0.01) и отсекающего клапана (PFD=0.05).

Целевой риск. $<10^{-4}$ /год.

Вопрос 1. Какой Требуемый SIL для СПАЗ/SIS?

Ответ:

1. Рассчитаем текущий риск без защиты.

Частота утечки метана.

$F_{\text{без СПАЗ/SIS}} = 2 \times 10^{-2} / \text{год}$.

2. Рассчитаем требуемое снижение риска (RRF).

Целевой риск. $10^{-4} / \text{год}$.

$RRF = 2 \times 10^{-2} / 10^{-4} = 200$.

3. Переведём RRF в PFD (Probability of Failure on Demand).

$PFD_{\text{треб}} = 1 / RRF = 1 / 200 = 0.005$

4. Определим требуемый SIL по таблице.

SIL	PFD диапазон	RRF диапазон
SIL 1	0.1 – 0.01	10 – 100
SIL 2	0.01 – 0.001	100 – 1000
SIL 3	0.001 – 0.0001	1000 – 10000

Наше $PFD_{\text{треб}} = 0.005$ попадает в диапазон SIL 2 (0.01 – 0.001).

Ответ на Вопрос 1.

Требуемый SIL для СПАЗ/SIS – SIL 2.

Вопрос 2. Достаточна ли конфигурация для обеспечения целевого риска?

1. Рассчитаем общее PFD системы.

СПАЗ/SIS состоит из датчика ($PFD_1 = 0.01$) и клапана ($PFD_2 = 0.05$).

Если они работают последовательно, то общее PFD системы.

$PFD_{\text{общее}} = PFD_1 + PFD_2 = 0.01 + 0.05 = 0.06$

2. Сравним с требуемым PFD.

- Требуемое $PFD_{\text{треб}} = 0.005$.

- Фактическое $PFD_{\text{общее}} = 0.06$

Вывод.

$0.06 > 0.005$.

Конфигурация НЕДОСТАТОЧНА, так как текущая система не обеспечивает нужного снижения риска.

Что можно сделать?

- Улучшить датчик (уменьшить PFD до 0.001).

- Улучшить клапан (уменьшить PFD до 0.004).

- Добавить резервирование (например, два датчика + голосование 1oo2).

Ответ на вопрос 2.

Нет, текущая конфигурация НЕДОСТАТОЧНА для достижения целевого риска.

РАЗДЕЛ 4.

Тест 4.5.

Вопрос 1. Что означает термин «Время миссии» (Mission Time)?

Ответ А.

Объяснение. Наиболее близкое к определению mission time — это проектно - заданный период (горизонт), в течение которого система обязана обеспечить выполнение своей функции безопасности. Формулировка «без сбоев» здесь отражает требование к надёжности в этот период (т.е. система должна оставаться работоспособной/способной выполнить функцию). Варианты В, С, D — либо о монтаже, либо ретроспективны (С — уже пройденное время), либо про обслуживание, и потому не соответствуют терминологии.

Вопрос 2. Каково значение термина «Срок службы» (Useful Life)?

Ответ В.

Объяснение. «Срок службы» — это время эксплуатации, а «Время миссии» — это время, в течение которого система может работать без обслуживания

Вопрос 3. Почему важно учитывать оба показателя при верификации SIF?

Ответ А.

Объяснение.

А) «Время миссии» относится к времени эксплуатации, а «Срок службы» — к времени, в течение которого система может оставаться работоспособной.

В) Для определения надёжности и планирования обслуживания.

Оба показателя важны для оценки надёжности системы и своевременного планирования ее обслуживания и замены компонентов.

«Время миссии» (Mission Time) и «Срок службы» (Useful Life) — это два ключевых временных показателя, которые играют важную роль в оценке надёжности и эффективности систем. Время миссии обозначает период, в течение которого система или компонент должны функционировать без сбоев, обеспечивая выполнение своих задач. Это критически важный параметр для систем, требующих высокой надёжности, таких как системы безопасности. Срок службы, с другой стороны, представляет собой максимальное время, в течение которого компонент может эффективно работать, прежде чем его производительность начнет снижаться или он выйдет из строя. Понимание различий между этими показателями помогает в планировании замены и обслуживания компонентов, что, в свою очередь, способствует повышению надёжности и безопасности систем.

Время работы — это расчетный период, часто выбираемый для представления временного интервала, в течение которого завод или технологическая установка эксплуатируются без ожидания полного капитального ремонта и перестройки.

Срок службы – это показатель того, когда конкретный компонент потребуется заменить или отремонтировать для поддержания заданной постоянной частоты отказов. Замену устройства всегда можно произвести в течение времени работы СФИ. Таким образом, эти понятия не тождественны.

Ответ на вопросы самопроверки.

Вопрос а. Почему в расчете PFD_{avg} для резервированных компонентов используется квадрат λ_{du} ?

В архитектуре с резервированием (например, 1oo2) опасный отказ наступает только если одновременно выйдут из строя оба канала. Для независимых каналов вероятность отказа примерно равна произведению вероятностей отказа каждого канала.

Если вероятность отказа одного канала за интервал проверки определяется как $\lambda_{DU} \cdot T/2$, то для двух независимых каналов вероятность совпадения $\approx (\lambda_{DU} \cdot T/2)^2$. Отсюда в формулах для PFD_{avg} часто появляется квадрат λ_{DU} (или других слагаемых), что отражает требование «одновременного отказа нескольких элементов».

Вопрос в. Как конфигурация 2oo3 влияет на PFD_{avg} и STR по сравнению с 1oo2?

Конфигурация 2oo3 по сравнению с 1oo2 даёт преимущество сразу в двух аспектах. Во-первых, вероятность отказа по требованию (PFD_{avg}) уменьшается, так как для отказа функции необходимо, чтобы два из трёх каналов оказались неисправны, а не один. Во-вторых, вероятность ложных срабатываний (STR) также снижается, поскольку в 1oo2 ложное срабатывание возможно при отказе одного канала, а в 2oo3 для этого требуется ошибка как минимум двух каналов. Таким образом, 2oo3 улучшает и надёжность выполнения функции безопасности, и доступность технологического процесса.

Вопрос с. Какие компоненты SIS обычно вносят наибольший вклад в STR?

Наибольший вклад в STR системы SIS обычно вносят датчики, так как они постоянно взаимодействуют с технологической средой, чаще подвержены отказам и способны инициировать сигнализацию или переход в безопасное состояние даже при частичных неисправностях. Логический модуль и исполнительные механизмы также влияют на общую статистику, но именно сенсоры чаще всего становятся источником ложных срабатываний.

Тест 4.6. Вероятность выпадения суммы чисел на 3-х игральных кубиках

Вопрос 1. Какова вероятность того, что сумма чисел на трех игральных кубиках составит 3?

Ответ А.

Объяснение. Сумма 3 может быть получена только одним способом.

(1, 1, 1). Поскольку общее количество возможных комбинаций при бросании трех кубиков составляет $6 \times 6 \times 6 = 216$, вероятность получения суммы 3 равна $1/216$.

Вопрос 2. Какова вероятность того, что сумма чисел на трех игральнх кубиках составит 5?

Ответ С. 5/216.

Объяснение. Сумма 5 может быть получена следующими комбинациями. (1, 1, 3), (1, 2, 2), (2, 1, 2), (3, 1, 1), (2, 2, 1). Всего 6 комбинаций, которые дают сумму 5. Поскольку общее количество комбинаций равно 216, вероятность составляет $6/216$, что сокращается до $1/36$.

Другой вариант объяснения. Количество возможных комбинаций для 3 объектов с шестью вариантами.

Возможности = $6^3 = 216$.

Число способов получить сумму 3 на трёх кубиках.
1+1+1.

Существует только одна комбинация, дающая сумму 3.

Число способов получить сумму 5 на трёх кубиках.
3+1+1.
1+3+1.
1+1+3.
2+2+1.
2+1+2.
1+2+2.

Всего существует 6 способов получить сумму 5.

Таким образом, суммарно есть 7 способов ($6 + 1$) получить либо 3, либо 5 на трёх кубиках, из общего числа 216 возможных комбинаций. Вероятность равна.

$P = 7/216 \approx 0,0324$.

Тест 4.7. Зависимые/независимые события.

Вопрос 1. Какое из следующих утверждений верно для независимых событий в контексте отказов компонентов СПАЗ/SIS?

Ответ В. Отказ одного компонента не влияет на вероятность отказа другого компонента.

Объяснение. Независимые события — это такие события, при которых факт наступления одного события не изменяет вероятность наступления другого. В случае независимых событий вероятность отказа одного компонента не влияет на вероятность отказа другого. Это важно для анализа надежности, так как позволяет рассматривать каждый компонент отдельно.

В контексте SIS это означает, что каждый компонент имеет свой собственный риск отказа, который не зависит от состояния других элементов. Например, два клапана в разных трубопроводах могут выйти из строя независимо друг от друга.

Вопрос 2. Какое из следующих утверждений верно для зависимых событий в контексте отказов компонентов СПАЗ/SIS?

Ответ В. Вероятность отказа одного компонента изменяется в зависимости от состояния другого компонента.

Объяснение. Зависимые события — это ситуации, когда отказ одного компонента влияет на вероятность отказа другого. В случае зависимых событий вероятность отказа одного компонента может быть изменена состоянием другого, что влияет на общий анализ надежности системы. В SIS это может происходить из-за общих причин отказов, механических связей или внешних условий (температура, вибрации, электропитание). Если зависимость не учитывать, расчёты надёжности будут неточными.

Вопрос 3.

Что такое взаимоисключающие события в контексте отказов компонентов СПАЗ/SIS?

Ответ В. События, которые не могут произойти одновременно.

Объяснение. Взаимоисключающие события – это такие события, которые не могут произойти одновременно. Например, если один компонент вышел из строя, это исключает возможность его нормальной работы в тот же момент. Для таких событий вероятность совместного наступления равна нулю: $P(A \cap B) = 0$, а вероятность наступления одного из событий равна сумме их вероятностей: $P(A \text{ или } B) = P(A) + P(B)$.

Вопрос 4.

Какое из следующих утверждений верно для дополнительных событий в контексте отказов компонентов СПАЗ/SIS?

Ответ С. Сумма вероятностей дополнительных событий равна 1.

Объяснение. Дополнительные события – это такие события, которые, если одно произошло, другое не может произойти. Сумма их вероятностей всегда равна 1, что отражает полное распределение вероятностей.

При анализе надёжности СПАЗ/SIS (используются следующие допущения.

- Отказы компонентов в разных подсистемах являются независимыми событиями. Например, отказ датчика не влияет на вероятность отказа запорного клапана.

- Отказы компонентов не являются взаимоисключающими. Это означает, что одновременно может существовать более одного отказа. При расчёте вероятностей отказов компонентов СПАЗ/SIS используется формула сложения для независимых событий.

- Состояния «отказ» и «работоспособность» компонентов СПАЗ/SIS взаимодополняющие. Компонент может находиться либо в состоянии отказа, либо в рабочем состоянии. Промежуточных состояний (ни отказа, ни работоспособности) не предполагается.

Тест 4.8.

Какое среднее время наработки на отказ (MTTF) передатчика в годах, если интенсивность отказов составляет 9×10^{-7} отказов в час?

Ответ А.

Объяснение. MTTF рассчитывается как обратная величина интенсивности отказов. Для этого нужно выполнить следующие шаги.

1. Интенсивность отказов. $\lambda = 9 \times 10^{-7}$ отказов в час.
2. MTTF (в часах) = $1 / \lambda = 1 / (9 \times 10^{-7}) \approx 1,111,111$ часов.
3. Переведем часы в годы. $1,111,111 \text{ часов} / (24 \text{ часов/день} \times 365 \text{ дней/год}) \approx 127.1$ года.

Таким образом, MTTF = 127 лет.

Тест 4.9. Рассчитайте надежность системы печи за пятилетний период (рис.13.2).

Вопрос 1. Какова общая надежность системы печи за пятилетний период, если для работы печи необходима работа одного из двух вентиляторов, горелки и системы управления? Вероятности надежной работы следующие.

- Вентиляторы. $R_1 = 0.95$ (каждый).
- Горелки. $R_2 = 0.97$.
- Система управления. $R_3 = 0.80$.

Ответ В. 0.99.

Объяснение.

1. Надежность вентиляторов. Поскольку у нас два вентилятора, система будет работать, если хотя бы один из них работает. Надежность системы вентиляторов можно рассчитать, как.

$$R_{\text{вент}} = 1 - (1 - R_1)^2 = 1 - (1 - 0.95)^2 = 1 - (0.05)^2 = 1 - 0.0025 = 0.9975.$$

Общая надежность системы. Теперь мы можем рассчитать общую надежность системы, учитывая надежность вентиляторов, горелок и системы управления. Поскольку все эти компоненты должны работать одновременно, общая надежность системы будет равна произведению надежностей всех компонентов.

$$R_{\text{системы}} = R_{\text{вент}} \times R_2 \times R_3 = 0.9975 \times 0.97 \times 0.80.$$

Подсчитаем.

$$R_{\text{системы}} = 0.9975 \times 0.97 \times 0.80 \approx 0.776.$$

Это значение не соответствует ни одному из предложенных вариантов.

2. Проверка расчетов.

$$R_{\text{системы}} = 0.9975 \times 0.97 \times 0.80 = 0.776.$$

Надежность системы печи за пятилетний период – это 0.776, что не соответствует предложенным вариантам. Возможно, нужно будет пересмотреть формулировку вопроса или варианты ответов.

Вопрос 2. Какова вероятность того, что система печи будет работать без сбоев в течение одного года?

Ответ D. 0.776.

Объяснение. Как мы рассчитали в предыдущем вопросе, надежность системы печи за пятилетний период составляет примерно 0.776. Это означает, что вероятность того, что система будет работать без сбоев в течение одного года, равна 0.776.

Для подсистемы вентиляторов используется логическое «ИЛИ». Для всей системы используется логическое «И» отдельных событий. Это можно изобразить с помощью диаграммы блоков надежности, как показано ниже. Надежность системы, или вероятность успеха за 5-летний период, вычисляется с помощью умножения вероятностей.

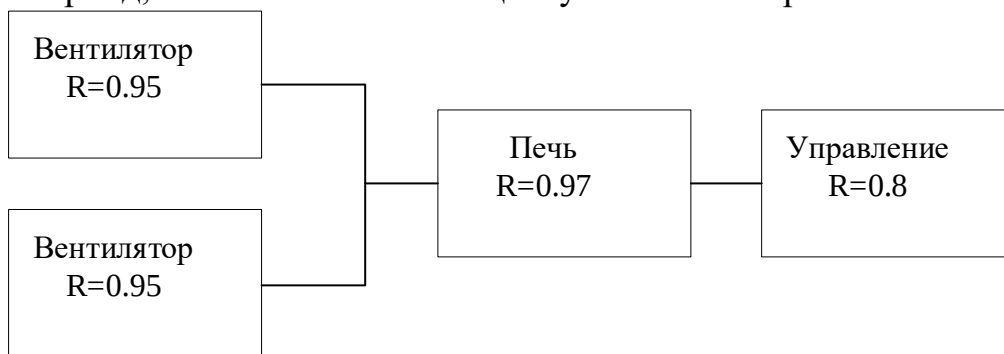


Рис.13.2. Надежность установки Вентилятор-Печь -Управление

Этот расчет упрощается тем фактом, что входные и выходные данные относятся к одному и тому же временному интервалу. 5 лет. Если временные интервалы различны, надежность компонентов необходимо пересчитать для требуемого выходного временного интервала. Это делается с помощью формулы $R = e^{-\lambda t}$ для вычисления λ для каждого компонента.

Fan Burner Controls:

$$R_{\text{Fan sub-system}} = R_{\text{Fan1}} + R_{\text{Fan2}} - (R_{\text{Fan1}} \times R_{\text{Fan2}}).$$

$$R_{\text{Fan sub-system}} = 0.95 + 0.95 - (0.95 \times 0.95) = 0.9975.$$

$$R_{\text{System}} = R_{\text{Fan sub-system}} \times R_{\text{Burner}} \times R_{\text{Controls}}.$$

$$R_{\text{System}} = 0.9975 \times 0.97 \times 0.8.$$

$$R_{\text{System}} = 0.774.$$

Дополнительная информация о диаграммах блоков надежности приведена в книге. Гоубл, У.М. «Оценка безопасности и надежности систем управления», 3-е издание, глава 7.

РАЗДЕЛ 5.

Тест 5.5.

Анализируется опасность с использованием графика риска (рис.13.3), показанного ниже, для выбора SIL для контура защиты который снижает риск.

Вопрос. Какой SIL необходим для установленного риска на ОПО

Ответ b.

Объяснение. Категория последствий, которая наиболее точно соответствует серьезным травмам нескольких человек, но без смертельных исходов – Cb.

Частота категории воздействия, которая наиболее точно соответствует области опасности, в которой в основном работают работники, – Fb.

Вероятность категории воздействия, которая наиболее точно соответствует возможности побега, Pa.

Вероятностная классификация, которая наиболее точно описывает более чем вероятное событие, – W3.

Следуя графику риска слева направо, используя выбранные категории, получаем значение SIL = 2.

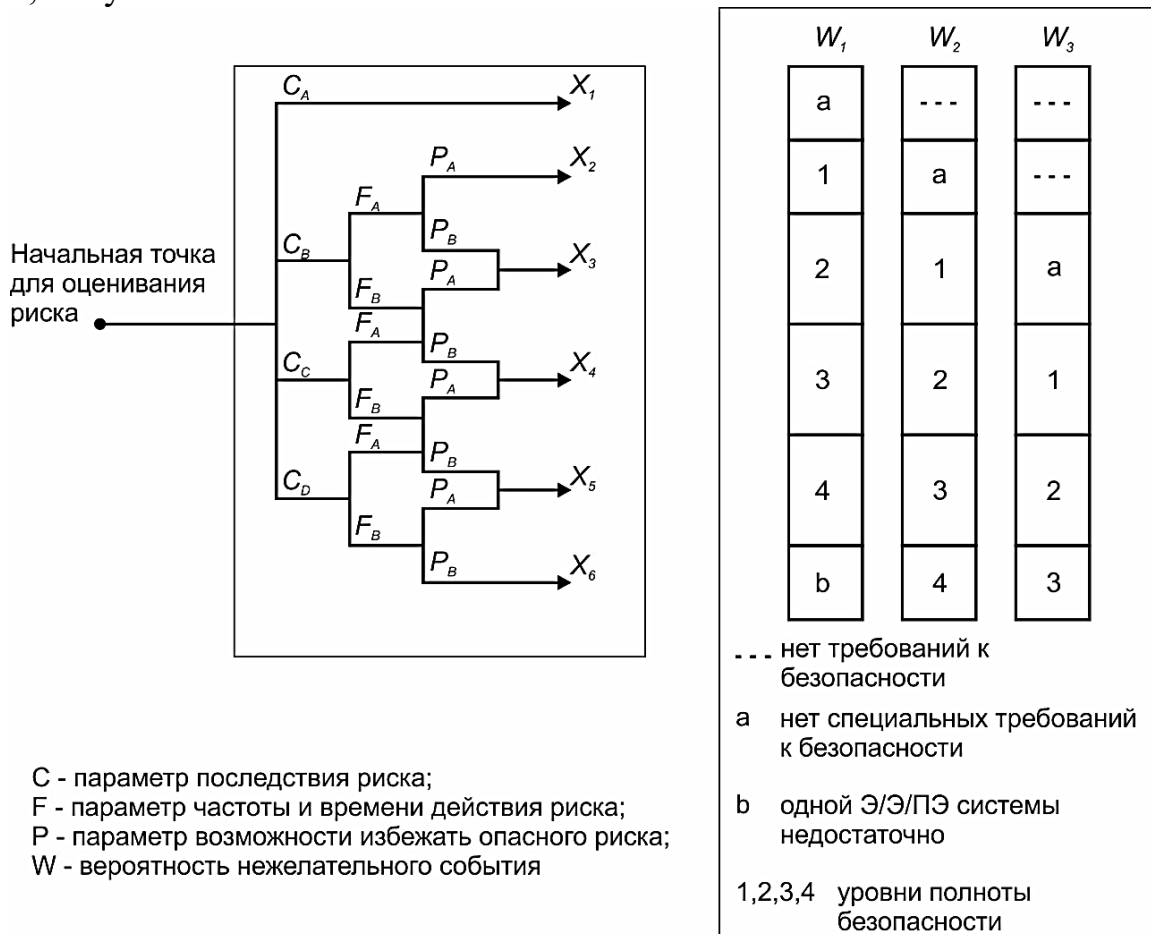


Рис. 13.3. Диаграмма рисков

Хотя описание события, приведенное в вопросе, не совсем соответствует графику риска (например, мы не знаем условий, при которых возможен выход из опасной зоны), у нас достаточно информации,

чтобы выбрать разумно правдоподобные параметры в графике риска. Учитывая, что график риска является качественным методом выбора SIL и включает существенную меру консерватизма, ответ «е» не обоснован.

Более подробную информацию об использовании графиков рисков для выбора SIL см. в МЭК 61511, часть 3, приложение D, и в книге [24].

Тест 5.6. Выбрать правильные ответы на вопросы.

Вопрос 1. Какое условие необходимо для того, чтобы коэффициент присутствия оператора возле объекта повышенной опасности соответствовал значению F_a (редкого до относительно частого) на диаграмме риска?

Ответ В.

Объяснение. Чтобы снизить коэффициент присутствия оператора, необходимо ограничить доступ в опасные зоны для всех, кроме оперативного персонала. Это помогает снизить риск аварийных ситуаций.

Вопрос 2. Какое значение имеет обучение и подготовка персонала в контексте снижения коэффициента присутствия оператора?

Ответ В.

Объяснение. Регулярное обучение помогает операторам быстро реагировать на возможные аварийные ситуации, что снижает риск травм и аварий.

Вопрос 3. Почему планирование обслуживания оборудования важно для снижения коэффициента присутствия оператора?

Ответ В.

Объяснение. Планирование обслуживания в безопасные периоды, когда оборудование остановлено, исключает возможность нахождения оператора в непосредственной близости от потенциально опасных объектов во время их работы.

Вопрос 4. Какую роль играют аварийные процедуры в снижении коэффициента присутствия оператора?

Ответ В.

Объяснение. Наличие заранее определенных аварийных процедур помогает операторам знать, как действовать в случае аварийной ситуации, что снижает риск травм.

Вопрос 5. Как регулярные оценки рисков влияют на коэффициент присутствия оператора?

Ответ В.

Объяснение. Периодическая оценка рисков помогает выявлять потенциальные угрозы и принимать меры для их устранения, что способствует снижению коэффициента присутствия оператора.

Тест 5.7. Условия предотвращения опасности (P_a).

Вопрос 1. Какое условие необходимо для того, чтобы коэффициент предотвращения опасности P_a соответствовал значению P_a – «возможно при определенных условиях»?

Ответ В.

Объяснение. Обучение и готовность оператора к действиям в экстренных ситуациях позволяют эффективно предотвращать опасные события, что соответствует значению P_a .

Вопрос 2. Какое значение имеет наличие четких процедур безопасности для коэффициента предотвращения опасности?

Ответ В.

Объяснение. Наличие заранее определенных процедур безопасности позволяет оператору быстро реагировать на изменения в ситуации, что снижает вероятность возникновения аварий и соответствует значению P_a .

Вопрос 3. Какую роль играют регулярные тренировки для операторов в контексте коэффициента предотвращения личной или групповой опасности на ОПО?

Ответ В.

Объяснение. Постоянное обучение и тренировки помогают оператору оставаться в форме и быть готовым к любым неожиданным ситуациям, что способствует соответствию коэффициента предотвращения опасности значению P_a .

Вопрос 4. Как регулярные оценки рисков влияют на коэффициент предотвращения опасности?

Ответ В.

Объяснение. Периодические оценки рисков помогают выявлять потенциальные угрозы и принимать меры для их устранения, что способствует снижению коэффициента предотвращения опасности и его соответствию значению P_a .

Коэффициент предотвращения опасности (или коэффициент безопасности) в контексте диаграммы риска по стандартам МЭК 61508 и 61511 представляет собой квалификацию, которая помогает оценить эффективность внутренней системы безопасности в предотвращении опасных событий. Это касается безопасности электрических, электронных и программируемых систем, обеспечивающих установленную функциональность объекта управления.

Он отражает вероятность того, что система безопасности (например, автоматизированные системы управления) предотвратит опасное событие. Чем выше этот коэффициент, тем более безопасна система в процессе эксплуатации.

Тест 5.8. Определение уровня SIL для системы управления горелками.

Вопрос 1. Какова частота погасания пламени в данной системе?

Ответ В.

Объяснение. В задаче указано, что частота погасания пламени составляет два раза в год.

Вопрос 2. Какова вероятность взрыва при погасании пламени?

Ответ В.

Объяснение. Вероятность взрыва в случае погасания пламени составляет 1 из 4, что эквивалентно 0,25.

Вопрос 3. Как рассчитывается ожидаемое значение частоты взрывов ($F_{пр}$)?

Ответ А.

Объяснение. Ожидаемое значение $F_{пр}$ рассчитывается как произведение частоты погасания пламени (2 раза в год) и вероятности взрыва (0,25).

Вопрос 4. Какова целевая частота риска (F_r) для данной системы?

Ответ В.

Объяснение. Изучив архивные данные, установлено, что частота взрывов, не превышающая один раз в 5000 лет, является приемлемой.

Вопрос 5. Какова целевая частота риска в год (F_r) для значения 1 раз в 5000 лет?

Ответ В.

Объяснение. Целевая частота риска 1 раз в 5000 лет равна $1/5000$, что дает значение 2×10^{-4} в год.

Вопрос 6. Как рассчитывается коэффициент снижения риска (RRF)?

Ответ А.

Объяснение. Коэффициент снижения риска рассчитывается как отношение ожидаемой частоты взрывов ($F_{пр} = 0,5$) к целевой частоте риска ($F_r = 2 \times 10^{-4}$).

Вопрос 7. Каково значение PFD_{avg} для данной системы?

Ответ В. $PFD_{avg} = 1 / RRF = 4 \times 10^{-4}$.

Объяснение. PFD_{avg} рассчитывается как $1 / RRF$, где $RRF = 2500$, что дает $PFD_{avg} = 4 \times 10^{-4}$.

Вопрос 8. Какой уровень SIL соответствует рассчитанному значению $PFD_{avg} = 4 \times 10^{-4}$?

Ответ С.

См. таблицу для SIL

РАЗДЕЛ 6.

Тест 6.7. HFT исполнительного устройства.

Вопрос 1. Какое значение HFT (частота опасных отказов) требуется для узла ИУ в соответствии с маршрутом 1Н МЭК 61508 для уровня SIL 2 ?

Ответ1.

Объяснение. Согласно таблице 8-3 МЭК 61508, для уровня SIL 2 требуется, чтобы HFT было равно 1. Это означает, что система может выдержать один опасный отказ без потери функциональности.

Вопрос 2. Какое значение HFT требуется для узла ИУ в соответствии с маршрутом 2Н МЭК 61508 для уровня SIL 2?

Ответ 1.

Объяснение. В соответствии с таблицей 8-5 МЭК 61508, маршрут 2Н для уровня SIL 2 (с низкой частотой запросов) устанавливает достаточность HFT равную 1. Но это означает, что система не должна иметь опасных отказов, чтобы функционировать безопасно.

Вопрос 3.

Какое значение HFT требуется согласно МЭК 61511.2016 для узла ИУ?

Ответ 1 или 2.

Объяснение. Рекомендация/требование по HFT (IEC 61511) — HFT = 1 (при использовании подхода, эквивалентного Route 2), но если применять строгий Route 1Н-подход (Type B) — HFT = 2. IEC 61511 переносит логику аппаратной устойчивости из IEC 61508 в прикладной контекст; при оценке компонентов SFF <60% обычно требует некоторого уровня резервирования для достижения SIL2. Практически, большинство прикладных интерпретаций 61511 (и практик промышленности) эквивалентны Route 2 с таблицами типа А: для SFF <60% и целевого SIL2 достаточно HFT=1. Тем не менее, если организация требует соблюдения Route 1Н / Type B (более жёсткий путь по 61508), тогда по таблице для <60% нужен HFT=2.

Иначе говоря: по 61511 (практическая реализация) — HFT=1 достаточен, но при применении строгих критериев Route1Н (как в 61508 Type B) — нужен HFT=2.

Тест 6.8. Потребный уровень SIL.

Ответ SIL 1.

Объяснение. Расчет SFF для подсистемы определяется как отношение безопасных и обнаруженных опасных отказов к общему количеству отказов.

$$SFF = \lambda_S + \lambda_D \lambda_S + \lambda_D + \lambda_{DU},$$

где.

- $\lambda_S = \lambda_{SU}$ (безопасные необнаруженные отказы),
- $\lambda_D = 0$ (обнаруженные опасные отказы отсутствуют, так как диагностики нет).

Для подсистемы (датчик + клапан).

- $\lambda_S = 2,4 \cdot 10^{-6} + 1,8 \cdot 10^{-6} = 4,2 \cdot 10^{-6}$.
- $\lambda_{DU} = 3,6 \cdot 10^{-6} + 1,2 \cdot 10^{-6} = 4,8 \cdot 10^{-6}$.
- $SFF = 4,2 \cdot 10^{-6} / (4,2 \cdot 10^{-6} + 4,8 \cdot 10^{-6}) = 4,29 \approx 46,67\%$.

Определение SIL по таблице МЭК 61508 д
Для устройств типа А с аппаратной устойчивостью к отказам (HFT) = 0 (без резервирования).

- Если $SFF < 60\%$, то SIL1.
- Если $60\% \leq SFF < 90\%$, то SIL2.
- Если $SFF \geq 90\%$, то SIL3.

В данном случае $SFF \approx 46,67\% < 60\%$, что соответствует SIL1.

Таким образом, конструкция SIF соответствует уровню безопасности SIL1 согласно ограничениям МЭК 61508.

Тест 6.9. Определение уровня SIL для системы SIF.

Вопрос 1.

Ответ В.

Архитектура системы безопасности в данной задаче – нерезервированная (1001), что означает, что имеется одно устройство, выполняющее функцию безопасности без резервирования.

Вопрос 2.

Ответ А.

Время отклика SIF для достижения безопасного состояния составляет 50 миллисекунд, как указано в задаче.

Вопрос 3. Ответ С. $9 \cdot 10^{-6}$ отказов в час.

Общая интенсивность опасных отказов (λD) определяется как сумма λDD и λDU . $\lambda D = \lambda DD + \lambda DU = 8,5 \cdot 10^{-6} + 0,5 \cdot 10^{-6} = 9 \cdot 10^{-6}$ отказов в час.

Вопрос 4.

Ответ В.

Время безопасности процесса в данной системе составляет 500 миллисекунд, как указано в задаче.

Объяснение.

Для определения уровня SIL необходимо учитывать, что время диагностики (DTI) составляет 100 миллисекунд, а время отклика SIF для достижения безопасного состояния – 50 миллисекунд. Суммарное время отклика (DTI + время отклика SIF) составляет 150 миллисекунд, что находится в пределах времени безопасности процесса, равного 500 миллисекундам.

Система работает в режиме высокого спроса ($DI = 1$ секунда), и учитывая, что DTI составляет 10 раз меньше DI, это позволяет системе иметь частичный диагностический кредит.

DTI плюс время отклика SIF составляет 150 миллисекунд, что находится в пределах.

Время безопасности процесса 500 миллисекунд. Следовательно, часть

опасных обнаруженных отказов, скорее всего, будут преобразованы в безопасные отказы. Соотношение частоты диагностики к частоте обращений равно 10 (таблица 6.6), Это требует кредит на диагностику равный.

$$PDC \approx (\lambda_{\text{Diag}}/\lambda_{\text{Demand}}) (1 - \exp [-\lambda_{\text{Demand}}/\lambda_{\text{Diag}}]) \\ = 10 \cdot (1 - \exp [-0,1]) = 0,9516 (95 \%).$$

Используя для расчета PFH.

$$PFH = (1 - 0,95) \cdot \lambda_{DD} + \lambda_{DU} \text{ получаем.}$$

$$PFH = (0,05 \cdot 8,5 \cdot 10^{-6}) + 0,5 \cdot 10^{-6} = 0,925 \cdot 10^{-6} \text{ отказов в час.}$$

Это соответствует требованиям SIL 2. Используется таблица 6.6.

Таблица 6.6. PDC Values for Select $\lambda_{\text{Diag}}/\lambda_{\text{Demand}}$ Ratios

$\lambda_{\text{Diag}}/\lambda_{\text{Demand}}$	PDC
2	78% Credit
10	95% Credit
100	99% Credit

Для оценки PDC можно применять таблицу E.1 — Примеры диагностического охвата (ГОСТ ISO 13849-1—2014)

Метод определения	DC
Входное устройство	
Испытания в режиме циклической нагрузки путем динамического изменения входного сигнала	90 %
Проверка правдоподобности, к примеру, применение нормально разомкнутых и нормально замкнутых механически соединенных контактов	99 %
Перекрестный контроль входов без применения динамических проверок	От 0 до 99%, зависит от того, насколько часто происходит изменение сигнала приложением
Перекрестный контроль входных сигналов с применением динамических проверок при отсутствии обнаружения короткого замыкания (для многих устройств ввода-вывода)	90 %
Перекрестный контроль входных сигналов и определение промежуточных результатов при помощи логической схемы и логически-временной программы наблюдения, а также с обнаружением статических сбоев и коротких замыканий (для многих устройств ввода-вывода)	99 %
Косвенное наблюдение (наблюдение при помощи переключателя давления, изучение электротехнических данных исполнительного устройства)	От 90 до 99 %, зависит от приложения
Прямое наблюдение (изучение электротехнических данных контрольных клапанов (вентилей), изучение электромеханических устройств с помощью механически соединенных контактов)	99 %
Обнаружение сбоев во время процесса	От 0 до 99 %, зависит от приложения; применение только одного этого метода недостаточно для требуемого уровня производительности
Исследование некоторых показателей датчика (время ответа, диапазон аналоговых сигналов, например, электрическое сопротивление, емкостное сопротивление)	60 %
Косвенное наблюдение (наблюдение при помощи переключателя давления, изучение электротехнических данных исполнительного устройства)	От 90 до 99 %, зависит от приложения
Прямое наблюдение (изучение электротехнических данных контрольных клапанов (вентилей), изучение электромеханических устройств с помощью механически соединенных контактов)	99 %
Обычный временной контроль логической схемы (например, таймер в качестве следящего устройства, где триггерные точки показаны в программе логической схемы)	60 %
Временной и логический контроль при помощи следящего устройства, в котором тестовое оборудование проверяет правдоподобие поведения логической схемы	90 %
Автоматические самопроверки на скрытые сбои в разных частях логической схемы (программы и банки данных, порты входа/выхода, интерфейсы)	90 % (зависит от метода проверки)

Проверка реакционной способности устройства наблюдения (устройства слежения) при помощи устройства ввода на главном канале (либо при запуске, либо когда требуется применение функции безопасности, либо по требованию внешнего сигнала)	90 %
Динамический принцип (все компоненты логической схемы должны изменить состояние ВКЛ-ВЫКЛ-ВКЛ, когда требуется применение функции безопасности), например, блокирующая схема, приводимая в действие при помощи реле	99 %
Неизменяемая память: подпись одинарным словом (8 бит)	90 %
Неизменяемая память: подпись двойным словом (16 бит)	99 %
Изменяемая память: проверка оперативной памяти с применением резервных данных (флагов, маркеров, постоянных, счетчиков) и перекрестное сравнение этих данных	60 %
Изменяемая память: проверка на возможность чтения и записи в использованных участках памяти	60 %
Изменяемая память: контроль оперативной памяти при помощи модифицированного кода Хэмминга или при помощи самопроверки оперативной памяти (например «galpat» или «Abraham»)	99 %
Программная самопроверка процессора	От 60 до 90 %
Кодированная обработка данных в процессоре	От 90 до 99 %
Обнаружение сбоев во время процесса	От 0 до 99 %, зависит от приложения; применение только одного этого метода недостаточно для требуемого уровня производительности
Выходное устройство	
Контроль выходов одним каналом без динамической проверки	От 0 до 99 %, зависит от того, насколько часто происходит изменение сигнала приложением
Перекрестный контроль выходов без применения динамических проверок	От 0 до 99 %, зависит от того, насколько часто происходит изменение сигнала приложением
Перекрестный контроль выходных сигналов с применением динамических проверок при отсутствии обнаружения короткого замыкания (для многих устройств ввода-вывода)	90 %
Перекрестный контроль выходных сигналов и определение промежуточных результатов при помощи логической схемы и логически-временной программы наблюдения, а также с обнаружением статических сбоев и коротких замыканий (для многих устройств ввода-вывода)	99 %
Резервированное отключение без наблюдения за исполнительным устройством	0 %
Резервированное отключение с наблюдением за одним из исполнительных устройств при помощи логической схемы или тестового оборудования	90 %
Косвенное наблюдение (наблюдение при помощи переключателя давления, изучение электротехнических данных исполнительного устройства)	От 90 до 99 %, зависит от приложения
Обнаружение сбоев во время процесса	От 0 до 99 %, зависит от приложения; применение только одного этого метода недостаточно для требуемого уровня производительности
Прямое наблюдение (изучение электротехнических данных контрольных клапанов (вентилей), изучение электромеханических устройств с помощью механически соединенных контактов)	99 %
П р и м е ч а н и е 1 — Для дополнительных методов определения см. IEC 61508-2, таблицы A.2 — A.15. П р и м е ч а н и е 2 — Если среднее или высокое значение DC достигнуто в логической схеме, то должен применяться хотя бы один метод изменяемой памяти, неизменяемой памяти и процессора со значением DC как минимум 60 %. Также могут применяться методы, не описанные в данной таблице.	

РАЗДЕЛ 7.

Тест 7.9. Установка точки срабатывания системы защиты от перегрева. Анализ нормального рабочего диапазона.

Вопрос Какая из перечисленных точек температуры ближе всего к точке срабатывания системы защиты от перегрева?

Ответ b. Наиболее подходящим вариантом будет b (450 °C), так как это значение находится в безопасной зоне между нормальным рабочим диапазоном и критической температурой.

Объяснение. Нормальная рабочая температура реактора находится в диапазоне от 150 до 350 °C. Это означает, что любые температуры в этом диапазоне считаются нормальными, и система управления должна быть настроена на поддержание температуры в этих пределах.

Критическая температура. Максимальная допустимая рабочая температура составляет 500 °C. Это значение указывает на критическую точку, выше которой реактор может выйти из строя или подвергнуться риску повреждения.

Установка точки срабатывания. Точка срабатывания системы защиты от перегрева должна быть установлена ниже критической температуры, но выше нормального рабочего диапазона.

Это необходимо для того, чтобы система могла реагировать на возможные отклонения и предотвратить перегрев. Стандарты, такие как ISO 13849 и МЭК 61508, подчеркивают важность выбора уставок, которые обеспечивают безопасность и предотвращают ложные срабатывания. Эти стандарты рекомендуют устанавливать точки срабатывания так, чтобы они находились в пределах безопасного диапазона, обеспечивая при этом защиту от потенциальных перегревов.

Варианты a (345 °C) и d (125 °C) находятся либо в пределах нормального рабочего диапазона, либо ниже его, что делает их неподходящими для установки точки срабатывания.

Варианты b (450 °C) и c (355 °C) находятся выше нормального рабочего диапазона, но ниже критической точки (500 °C). Однако, вариант c (355 °C) слишком близок к верхней границе нормального диапазона и может вызвать ложные срабатывания, если температура немного поднимется из-за нормальных колебаний.

ISO 13849 - Стандарт по безопасности машин.

МЭК 61508 - Стандарт по функциональной безопасности электрических/электронных/программируемых электронных систем.

Тест 7.10. Принцип «Проверено практикой».

Вопрос 1.

Ответ В и Д. Устройство может применяться в системах безопасности, если есть документированная оценка его предыдущего исполь-

зования. Концепция, при которой продукт демонстрирует приемлемую безопасность и надежность в конкретном применении, а его производительность подтверждается точными записями конкретной компании.

Вопрос 2.

Ответ В. Необходимо наличие документированной оценки на основе предыдущего опыта использования.

Вопрос 3.

Ответ В. Документированная оценка на основе опыта предыдущего использования.

Объяснения. В соответствии с ГОСТ Р МЭК 61511-1 принцип «проверено практикой» означает, что устройство данного типа может применяться в системах, связанных с безопасностью (включая СПАЗ), если существует документированная оценка, основанная на опыте предыдущего использования таких устройств и доказывающая, что эти устройства пригодны для применения в СПАЗ. Принцип «проверено практикой» (или «проверено опытом») применяется в проектировании систем противоаварийной защиты (СПАЗ) в тех случаях, когда.

Недостаточно теоретических расчетов или моделей для оценки рисков и последствий, и необходимо опираться на реальные примеры и опыт, накопленный в аналогичных системах.

В проектах, связанных с высокими рисками или сложными технологическими процессами, где факторы риска могут быть разнообразными и трудно предсказуемыми. В таких случаях опыт предыдущих проектов может помочь выявить потенциальные проблемы и решения.

При внедрении новых технологий или оборудования, когда отсутствует достаточная база данных для оценки их надежности и безопасности. В этом случае применяются данные из аналогичных проектов, чтобы определить, как эти технологии функционировали в реальных условиях.

При анализе произошедших инцидентов и аварий, чтобы понять, какие меры безопасности были эффективными, а какие – нет. Это помогает в дальнейшем проектировании более безопасных систем.

«Проверенный практикой» – это концепция, при которой устройство демонстрирует приемлемую безопасность и надежность в конкретном применении, а его характеристики подтверждаются документально зафиксированными данными.

См. Определение в МЭК 61511-1, раздел 3.2.60; Требования в МЭК 61508-2, раздел 7.4.10; Требования в МЭК 61511-1, раздел 11.5.3.

Применение этого принципа позволяет минимизировать неопределенности и повысить уровень доверия к проектируемым системам, основываясь на реальных данных и опыте.

Гост Р МЭК 61 511-2 -2018 п. А.11.5.3

См. Также обсуждение в работе »*Final Elements & the МЭК 61508 and МЭК 61511 Functional Safety Standards*» (С. O'Brien, L.D. Bredemeyer, стр. 40).

Тест 7.11. Выбрать ответ с объяснением для проблемы. Как ложные срабатывания СПАЗ/SIS влияют на ее работу и безопасность и на безопасность и технологичность ОПО.

Вопрос 1.

Ответ В.

Объяснение. Ложные срабатывания могут вызывать остановку производства, что приводит к убыткам, а также могут создавать новые опасные ситуации, что делает их критически важными для учета при проектировании систем безопасности.

Вопрос 2.

Ответ В.

Объяснение. Стандарты требуют, чтобы частота ложных срабатываний была сведена к минимуму, чтобы обеспечить безопасность и доступность установки, а также снизить финансовые потери.

Вопрос 3.

Ответ В.

Объяснение. Ложные срабатывания могут вызвать остановку производственных процессов, что приводит к финансовым потерям, а также могут создавать новые опасные условия, что делает их важным фактором при проектировании SIF.

Вопрос 4.

Ответ В.

Объяснение. Хотя основное внимание должно быть уделено ограничению количества ложных срабатываний, также важно учитывать затраты, связанные с потерей производства, что является второстепенным, но важным аспектом.

Вопрос 5.

Ответ В.

Объяснение. Этот вопрос требует «объяснения в спецификации».

Поскольку в МЭК 61511 (часть 1, пункт 10.3.1) лишь кратко упоминаются ложные срабатывания, а в МЭК 61508 они практически не упоминаются, необходимо дополнить Ответ кратким обсуждением важности учёта частоты ложных срабатываний.

Если система реагирует на ложные срабатывания, это может отвлекать внимание от реальных угроз, что увеличивает риск аварийных ситуаций и создает новые опасности.

Ложные срабатывания являются серьезным фактором, который необходимо учитывать при проектировании SIF (систем инструмен-

тальной безопасности). Существует две причины, по которым необходимо учитывать ложные срабатывания. Во-первых, они часто очень дорого обходятся из-за потери производства. Помимо финансовых соображений, ложные срабатывания могут также создавать опасные условия (новые опасности, которые ранее не были выявлены).

При указании частоты ложных срабатываний в техническом задании на безопасность основное внимание следует уделять ограничению количества ложных срабатываний до приемлемого уровня. Второстепенное соображение – ограничение затрат, связанных с потерей производства в результате ложных срабатываний.

Требование к определению времени отклика приведено в МЭК 61511, часть 1, пункт 10.3.1.

Тест 7.12. Объяснение преимущества внедрения СПАЗ/SIS.

Вопрос 1.

Ответ. Опасные скрытые (недетектируемые) отказы СПАЗ/SIS могут привести к тому, что система не сможет адекватно реагировать на аварийные ситуации, что увеличивает вероятность инцидентов. Установленный уровень SIL () должен быть основан на анализе опасностей, чтобы гарантировать, что PFDavg (Probability of Failure on Demand) остается в пределах допустимых значений. Надежность компонентов и интервалы проверок играют ключевую роль в снижении PFDavg.

Объяснение. ЛПП должны понимать, что надежность компонентов СПАЗ/SIS – это основа безопасности. Неправильная оценка рисков и скрытые отказы могут привести к серьезным последствиям, включая аварии и простои.

Вопрос 2.

Ответ. Опасные явные (детектируемые) отказы могут привести к остановкам в производственном процессе, что приводит к потерям доходов. Если проводить ремонты в режиме online, это увеличивает время, в течение которого процесс остается незащищенным, что повышает риск аварий.

Объяснение. ЛПП должны осознавать, что несмотря на возможность обнаружения отказов, их влияние на производственный процесс может быть значительным. Высокая интенсивность ложных срабатываний может служить основанием для улучшения предыдущих систем безопасности.

Вопрос 3.

Ответ. Резервированные системы обеспечивают высокий уровень защиты, но могут снизить защиту до уровня «один из двух» в случае отказа. Начальные затраты на установку могут быть выше, но стоимость жизненного цикла может оказаться ниже.

Объяснение. ЛПП должны анализировать затраты на жизненный цикл при выборе между резервированием и другими методами. Резервирование может быть более экономически эффективным в долгосрочной перспективе, несмотря на высокие начальные затраты.

Вопрос 4.

Ответ. Ложные срабатывания приводят к остановам, что означает потери для бизнеса. Аварийные остановки могут увеличить амортизационные затраты на основное оборудование и привести к дополнительным рискам при перезапуске.

Объяснение. ЛПП должны понимать, что меры по снижению частоты ложных срабатываний могут значительно снизить затраты на жизненный цикл и улучшить общую эффективность системы. Анализ затрат на жизненный цикл помогает обосновать инвестиции в компоненты повышенного качества.

Анализ затрат на жизненный цикл, а также понимание рисков, связанных с каждым типом отказа, являются ключевыми аспектами, которые ЛПП должны учитывать при принятии решений о разработке и оценке систем безопасности. Это знание не только улучшает качество производства, но и подготавливает его к реальным вызовам в области автоматизации и робототехники.

1 Опасные скрытые (недетектируемые) отказы СПАЗ/SIS SIL устанавливаются с помощью анализа опасностей. Надежность компонентов и интервалы проверок снижают PFD_{avg} до значения, соответствующего заданному. Низкая надежность компонентов повышает затраты на проверки риска потерь продукции. Отказы СПАЗ/SIS приводят к простоям или к неготовности СПАЗ/SIS. Возросшие риски для объекта и простоя Тяжелый случай для повышения избыточности. Надо анализировать затраты на жизненный цикл.

2 Опасные явные (детектируемые) отказы СПАЗ/SIS Отказы этого вида (безопасные или обнаруживаемые проверками) приводят к перерывам в процессе производства и, следовательно, к потерям доходов от бизнеса. Если пробовать проводить ремонты в режиме online, то возрастает время, в течение которого процесс остается незащищенным. Следовательно, при приобретении СПАЗ/SIS с низкими характеристиками эксплуатационные расходы могут возрасти. При отказах этого типа Объяснением для совершенствования прежней СПАЗ/SIS часто служит высокая интенсивность ложных срабатываний.

3. Постепенные отказы резервированной СПАЗ/SIS. Этот вид отказов свойственен резервированной системе, снижающей защиту до уровня одинарной или до вида «один из двух». Уровень защиты остается высоким, а частота остановов очень низкой. Начальные затраты на установку, вероятно, будут выше, но стоимость жизненного цикла может быть ниже. Для обоснования преимуществ резервирования надо анализировать затраты на жизненный цикл.

4. Отказы СПАЗ/SIS из-за ложных (досадных) срабатываний. Все формы остановов для бизнеса означают потери. Кроме того, если случаются аварийные остановки, потенциально существует возможность роста амортизационных затрат на основное оборудование объекта. Отказы влияют на производство и увеличивают амортизационные затраты. Опасности, связанные с перезапуском. Для выбора преимуществ резервирования и компонентов повышенного качества надо анализировать затраты на жизненный цикл. Поэтому, меры снижения частоты ложных или досадных срабатываний будут подобны тем, которые показывают преимущества по затратам на жизненный цикл.

Тест 7.13 Сигналы о несоответствии, которые могут приводить к остановке процесса.

Ответ: A, B, C, D, E, F, G, H и I.

Объяснение.

1. Частота опасных необнаруженных отказов (A). Это важный показатель, который указывает на количество отказов, которые могут произойти, но не были обнаружены. Высокая частота таких отказов может привести к серьезным последствиям, включая необходимость остановки процесса.

2. Частота опасных обнаруженных отказов (B). Эти отказы были обнаружены, что позволяет предпринять меры для их устранения. Если такие отказы не приводят к отключению системы функциональной безопасности (СФИ), это может угрожать безопасности и потребовать остановки процесса.

3. Интервал проверки (C). Частота, с которой проводятся проверки систем, критична для обеспечения их надежности. Если интервал слишком велик, это может привести к пропуску потенциальных проблем, что также может вызвать необходимость остановки процесса.

4. Коэффициент покрытия проверки (D). Эффективность проверок, то есть насколько хорошо они покрывают возможные отказы, имеет решающее значение. Низкий коэффициент покрытия может означать, что не все потенциальные проблемы будут выявлены, что может потребовать остановки процесса.

5. Время обхода проверки (E). Длительность проверки также важна. Если проверка занимает слишком много времени, это может повлиять на производственный процесс и вызвать остановку.

6. Среднее время восстановления (F). Это время, необходимое для восстановления системы после отказа. Длительное время восстановления может привести к необходимости остановки процесса, чтобы обеспечить безопасность.

7. Вероятность начального отказа (G). Эта переменная важна, так как высокая вероятность отказа может привести к необходимости остановки системы для устранения проблем.

8. Индекс безопасности на объекте (H). Операционная культура безопасности непосредственно влияет на управление рисками. Низкий индекс безопасности может привести к необходимости остановки процессов для улучшения условий безопасности.

9. Избыточная архитектура (I). Избыточные системы могут обеспечить дополнительный уровень безопасности. Если архитектура не избыточна, это может привести к необходимости остановки процесса в случае отказа.

Переменные A и C являются отправной точкой для любого расчета PFD_{AVG} (средняя вероятность отказа по требованию).

Избыточность безопасности I, также является известной переменной на протяжении многих лет.

Покрытие проверочных испытаний D, было признано критической переменной в 2005 году и является определяющим показателем СПАЗ.

Если опасные обнаруженные отказы не настроены на отключение контура защиты, то B и F могут быть значительными.

Когда проверочное испытание проводится при наличии технологических опасностей, продолжительность проверочного испытания, E, может быть значительной.

В ситуациях, когда изделия устанавливаются без полного тестирования, вероятность первоначального отказа, G, может быть значительной.

Многие переменные, характеризующие PFD_{AVG} зависят от процедур эксплуатации и технического обслуживания, поэтому индекс безопасности площадки (SSI), H, может быть значительным.

Таким образом Все перечисленные переменные играют важную роль в обеспечении безопасности и надежности процессов. Понимание их влияния и взаимосвязей помогает в управлении рисками и предотвращении аварийных ситуаций.

Для получения дополнительной информации см. [24].

Тест 7.14.

Вопрос 1.

Ответ с.

Объяснение. Если SIF находится в обходе, он не может реагировать на опасное состояние. Вероятность отказа по требованию в этой ситуации равна единице – он обязательно откажет по требованию.

Требование к определению времени отклика приведено в МЭК 61511, часть 1, пункт 10.3.1.

Тест 7.15.

Вопрос 1.**Ответ В.**

Объяснение. Различают:

- Сигнализация, связанная с процессом.
- Сигнализация, связанная с машинами и оборудованием.
- Сигнализация, связанная с безопасностью.
- Сигнализация аварийного останова.

Основная цель систем сигнализации заключается в привлечении внимания оператора к тому, что условия вышли за пределы, соответствующие режиму нормального функционирования. Это позволяет оператору принимать решения о необходимости вмешательства в процесс.

Вопрос 2.**Ответ В.**

Объяснение. Сигнализация, связанная с безопасностью, предназначена для информирования оператора о потенциальных угрозах, требующих вмешательства. Согласно ГОСТ Р МЭК 62682, сигнализация — это инструмент поддержки оператора, помогающий своевременно реагировать на ненормальные состояния процесса до того, как они перерастут в аварийные. Она помогает предотвратить аварийные ситуации, но не является системой аварийного останова.

Вопрос 3.**Ответ В.**

Объяснение. Сигнализации, связанные с машинами и оборудованием, помогают предотвратить повреждение оборудования и обеспечивают его правильную работу, информируя оператора о любых отклонениях, которые могут повлиять на функционирование машин.

Вопрос 4.**Ответ С.**

Объяснение. Системы СПАЗ и АСУ ТП обычно обмениваются данными через интерфейсы, чтобы:

- передавать оператору информацию о состоянии SIS,
- регистрировать события и последовательности срабатываний,
- исключать дублирование тревог,
- обеспечивать координацию между предупреждающими и аварийными сигналами.

Такое взаимодействие обеспечивает многоуровневую защиту (по принципу LOPA) и повышает общую эффективность реагирования на отклонения.

Вопрос 5.**Ответ В.**

Объяснение. Важно учитывать ограниченные возможности человека-оператора, поскольку перегрузка информацией может привести к ошибкам в принятии решений. Системы сигнализации должны

быть спроектированы так, чтобы минимизировать эту нагрузку и обеспечить оператору возможность быстро и эффективно реагировать на отклонения.

Тест 7.16. Как выполнять объединение СПАЗ и АСДУ в контексте объединения функций безопасности и управления в распределенных системах управления и программируемых логических контроллерах (ПЛК)?

Вопрос 1.

Ответ В.

Объяснение. Логическое объединение позволяет функциям безопасности и управления взаимодействовать, сохраняя при этом их независимость на уровне оборудования. Это важно для обеспечения надежности и безопасности, поскольку каждая функция может быть оптимизирована и протестирована отдельно.

Вопрос 2.

Ответ С.

Объяснение. Объединение функций на одном оборудовании может создать уязвимости, так как сбой или атака на одну функцию могут повлиять на другую. Это уменьшает уровень безопасности системы и может привести к серьезным последствиям.

Вопрос 3.

Ответ С.

Объяснение. Объединение функций может быть приемлемо, если оборудование сертифицировано для выполнения обеих функций. Это означает, что устройство прошло необходимые испытания и может безопасно выполнять обе задачи, минимизируя риски.

Например, допускается использование одного ПЛК для функций управления и безопасности, если это устройство имеет сертификат соответствия требованиям МЭК 61508/61511 и обеспечивает: аппаратную и программную изоляцию между функциями, независимую диагностику и тестирование, гарантированный уровень SIL для безопасности.

Вопрос 4.

Ответ В.

Объяснение. Объединение функций может действительно привести к конфликтам в управлении рисками, поскольку приоритеты и требования к безопасности могут противоречить требованиям управления. Это требует внимательного анализа и оценки.

Вопрос 5.

Ответ В.

Объяснение. Основная цель разделения функций безопасности и управления заключается в обеспечении более высокого уровня безопасности и надежности. Это позволяет минимизировать риски и гарантировать, что сбой в одной функции не повлияет на другую.

Управление процессом направлено на поддержание или направленное изменение условий хода процесса. Оно помогает обеспечить наилучшее протекание процесса и часто используется для того, чтобы вывести процесс на пределы, достижение которых не связано с нарушением безопасности. Поскольку эти системы действуют непрерывно, не предполагается, что они должны выполнять процедуры диагностики для поиска ошибок.

Обычно отказ в системе управления не является катастрофическим, хотя он может представлять опасность. Система управления безопасностью (СПАЗ) подобна полицейскому или сотруднику службы охраны. Она должна придерживаться фиксированного набора правил, и их доступ к внесению изменений в эти правила должен быть тщательно ограничен. Другими словами, они должны быть «непоколебимыми». При этом они должны быть высоконадежными и обладать мгновенной реакцией в случае тревоги. См. ГОСТ Р МЭК 61511-2 п. А.11.2.4

РАЗДЕЛ 8.

Тест 8.5. Расположите следующие схемы избыточности в порядке от наименьшей вероятности отказа по требованию (PFD) до наибольшей.

Ответ б.

Объяснение. Наибольшая частота опасных отказов в группе соответствует схеме голосования 2 из 2, а наименьшая – схеме голосования 2 из 3. Схема голосования 1 из 2 находится между этими двумя вариантами.

Тест 8.6. Какая архитектура систем безопасности (СПАЗ) лучше. 2oo3 или 1oo2D?

Вопрос 1. Какую вероятность отказов имеет система с архитектурой 2oo3 по сравнению с системой 1oo2D?

Ответ А.

Объяснение. Архитектура 2oo3 (двое из трёх) обеспечивает резервирование с голосованием, что уменьшает вероятность как опасных, так и ложных срабатываний.

1oo2D (один из двух с дублированием) менее устойчива к систематическим и случайным ошибкам, особенно при низком диагностическом покрытии

Вопрос 2. Каковы возможные недостатки архитектуры 1oo2D в условиях низкого диагностического покрытия?

Ответ А.

Объяснение. Низкое диагностическое покрытие (DC) означает, что опасные отказы могут оставаться необнаруженными, что увеличивает PFD.

1oo2D без эффективной диагностики не устраняет ложные срабатывания и может приводить к ненужным остановкам процесса.

Вопрос 3. Какую архитектуру целесообразно выбирать при использовании неинтеллектуальных устройств, таких как термопары и реле?

Ответ В.

Объяснение. Низкое диагностическое покрытие (DC) означает, что опасные отказы могут оставаться необнаруженными, что увеличивает PFD.

1oo2D без эффективной диагностики не устраняет ложные срабатывания и может приводить к ненужным остановкам процесса.

Вопрос 4. Какую основную выгоду предоставляет архитектура 2oo3 в контексте безопасных отказов и ложных срабатываний?

Ответ В. Она обеспечивает удовлетворительные показатели для отказов обоих видов (безопасных и опасных).

Объяснения. Система с архитектурой 2oo3 имеет большую вероятность отказов, чем система 1oo2D. Однако архитектура 1oo2D может быть неудовлетворительна с точки зрения безопасных отказов и ложных срабатываний (особенно в условиях низкого диагностического покрытия) в то время, как система с архитектурой 2oo3 обеспечивает удовлетворительные показатели для отказов обоих видов (безопасных и опасных).

Выбор архитектуры 2oo3 целесообразен при использовании неинтеллектуальных устройств, таких как термопары, термометры сопротивления, реле и другие подобные компоненты.

Тест 8.7. Сколько уровней устойчивости к опасным отказам (в соответствии с МЭК 61508) существует в архитектуре 1oo2?

Ответ б.

Объяснение. Архитектура 1oo2 обладает одним уровнем отказоустойчивости к опасным отказам. Иными словами, подсистема гарантированно будет работать даже при наличии одного опасного отказа. Это соответствует таблицам МЭК 61508 для архитектур с SFF < 90% и SIL 1–2.

Тест 8.8. Как резервирование влияет на надежность этих систем?

Вопрос 1. Какое из следующих утверждений верно в отношении простых и сложных устройств?

Ответ а.

Объяснение. Простые устройства, не использующие программируемую электронику, как правило, имеют более низкую вероятность отказа, поскольку они основаны на менее сложных технологиях. Сложные устройства, использующие программируемую электронику, подвержены большему количеству потенциальных отказов, что делает их менее надежными.

Вопрос 2. Какое условие позволяет уменьшить уровень отказоустойчивости на единицу?

Ответ в.

Объяснение. Если устройство имеет долю безопасных отказов более 90% и применяется диагностика, это позволяет уменьшить уровень отказоустойчивости на единицу. Это условие обеспечивает достаточный уровень защиты, даже если уровень отказоустойчивости снижен.

Вопрос 3. Какое из следующих условий увеличивает уровень отказоустойчивости на единицу?

Ответ с.

Объяснение. «Проверено практикой» повышает доверие к надежности устройства.

Защита паролем предотвращает неконтролируемую конфигурацию, снижая риск систематических ошибок.

Вместе эти факторы позволяют повысить уровень отказоустойчивости.

Остальные варианты не дают существенного повышения надежности

Вопрос 4. Какое влияние имеет использование резервированной архитектуры 1oo2 или 1oo3 на систему?

Ответ с. Позволяет достичь заданного уровня ПФД при высоком значении показателя PFD устройства.

Объяснение. Использование резервированной архитектуры, такой как 1oo2 или 1oo3, позволяет достичь необходимого уровня надежности (ПФД) даже при высоком значении показателя PFD устройства. Это важно для обеспечения безопасности системы.

Вопрос 5. Какое из следующих утверждений о конфигурации 2oo3 является верным?

Ответ с. Конфигурация 2oo3 более устойчива к систематическим ошибкам, чем 1oo2.

Объяснение. Конфигурация 2oo3 (две из трех) обеспечивает большую устойчивость к систематическим ошибкам, поскольку для достижения отказа системы требуется, чтобы два устройства вышли из строя одновременно. Это делает систему более надежной в условиях возможных систематических ошибок.

Однако отказы по общей причине способны ограничить выигрыш в надежности, достигаемый в результате резервирования, если не принять специальных мер по их сокращению. Всегда имеется опасность того, что все наши датчики или исполнительные устройства в одно и то же время окажутся жертвами одинаковых дефектов. Виды дефектов, которые не следует выпускать из поля зрения это.

- неправильная спецификация;
- ошибки в проектировании технических средств и в соединениях;

- воздействие со стороны окружающей среды;
- общие с процессом соединения;
- неправильные процедуры обслуживания;
- неправильная калибровка.

Тест 8.9. Использование при резервировании общих датчиков в СПАЗ и АСДУ.

Вопрос. Почему не следует использовать общие датчики для систем безопасности (СПАЗ) и автоматизированных систем диспетчерского управления (АСДУ)?

Ответ. Все перечисленные пункты (**a, b, c, d**) являются корректными причинами, почему не следует использовать общие датчики.

Объяснение. В современных промышленных системах безопасности и автоматизации важным аспектом является выбор правильной архитектуры и конфигурации систем. Одним из ключевых вопросов является использование общих датчиков для систем безопасности (СПАЗ) и автоматизированных систем диспетчерского управления (АСДУ).

Нарушение принципов независимости (вариант **a**). Системы безопасности должны быть независимыми от базовых систем управления процессом, чтобы избежать влияния возможных отказов в управлении на безопасность. Если датчики используются одновременно в обеих системах, это может привести к тому, что сбой в одной системе повлияет на другую, что недопустимо для обеспечения безопасности.

Системы безопасности должны функционировать независимо от основных систем управления, чтобы обеспечить надежную защиту в случае сбоя основной системы. Использование общих датчиков может привести к тому, что сбой в АСДУ повлияет на работу СПАЗ, что увеличивает риск несвоевременного реагирования на угрозы.

•Создание возможности появления отказов по общим причинам (вариант **b**). Общие датчики могут быть подвержены одинаковым воздействиям или неисправностям, что может привести к одновременному отказу как системы безопасности, так и диспетчерского управления. Это создает уязвимость, поскольку в критических ситуациях обе системы могут оказаться неработоспособными.

•Отсутствие отдельного защитного уровня (вариант **c**). Наличие отдельных датчиков для СПАЗ и АСДУ позволяет создать дополнительные уровни защиты. Общие датчики не обеспечивают необходимой изоляции, что может снизить общую эффективность системы безопасности.

•Неадекватные процедуры обслуживания, проверки и защиты устройства (вариант **d**). Обслуживание общих датчиков может быть затруднено, так как процедуры, предназначенные для одной системы, могут не подходить для другой. Это может привести к недостаточной

проверке и защите датчиков, что увеличивает риск их выхода из строя или неправильной работы.

- **Возможность отказов по общим причинам (вариант **b**).** Использование общих датчиков увеличивает риск отказов по общим причинам. Например, если датчик выходит из строя, это может повлиять как на систему управления, так и на систему безопасности, что увеличивает вероятность несчастного случая или аварии.

- **Отсутствие отдельного защитного уровня (вариант **c**).** Системы безопасности должны иметь свои собственные уровни защиты, чтобы обеспечить надежность и защиту от возможных угроз. Если используются общие датчики, то это может привести к недостаточной защите, так как один уровень может оказаться недостаточным для обеспечения безопасности.

- **Неадекватные процедуры обслуживания (вариант **d**).** Обслуживание и проверка общих датчиков могут быть неадекватными, так как они могут не соответствовать требованиям, необходимым для надежной работы системы безопасности. Это может привести к тому, что датчики не будут должным образом проверяться или обслуживаться, что увеличивает риск отказов.

Отметим, что разделение датчиков включает в себя и их отдельное подключение к процессу.

РАЗДЕЛ 9.

Тест 9.6. Дана диаграмма причин и следствий, приведенная ниже.

Какой функциональный блок следует использовать для соединения двух входов температурных реле с выходным клапаном?

Ответ а.

Объяснение. Из диаграммы причин и следствий видно, что если любой из двух датчиков сигнализирует о необходимости реакции процесса, клапан UV-01 должен закрыться. В нормальном режиме оба входа функционального блока имеют значение TRUE. Если один из входов меняется на FALSE, выход также должен стать FALSE. Этим свойством обладает блок AND.

Для справки. см. статью «Логический элемент» на www.wikipedia.org.

Тест 9.7. Какое утверждение на языке релейной логики (ladder logic) наиболее точно соответствует следующему текстовому утверждению?

Ответ а.

Объяснение. В лестничной диаграмме соединение должно быть выполнено между двумя линиями питания (слева направо). Соединение возникает только при условии, что вход A – TRUE, а вход B – NOT

TRUE. Следовательно, входы А и В должны быть соединены последовательно, а не параллельно. Варианты **b** и **c** неверны. Выход в лестничной диаграмме обозначается катушкой.

Для справки. см. статью «Лестничная логика» на www.wikipedia.org

Тест 9.8. А, В и С – дискретные входы в безопасный ПЛК, а D – выход. Какое утверждение на языке релейной логики наиболее точно представляет голосование 2oo3 для этих входов?

Ответ b.

Объяснение. Диаграмма **b** реализует логику 2oo3 для входов А, В и С. Диаграмма **a** соответствует логике $(A \text{ OR } B) \text{ AND } C$, **c** – $A \text{ AND } B \text{ AND } C$, **d** – $A \text{ OR } B \text{ OR } C$, а **e** зависит только от входа С (вне зависимости от А и В).

Тест 9.9. Система безопасности (СПАЗ/SIS) инициирует остановку с помощью клапанов для остановки с голосованием 1oo2. Система имеет ручной обходной путь, который позволяет проводить тестирование.

Ответ e. Ни один из вариантов не верен.

Объяснение. Варианты с и d показывают логику 2oo2 для клапанов, в то время как СПАЗ/SIS активирует остановку по логике 1oo2.

Вариант **a** не содержит байпасного клапана, а **b** – тестового переключателя.

Ближе всего к правильному вариант d, так как включает байпас и тестовый переключатель, но он всё равно не соответствует требованиям.

Тест 9.10. Датчик с выходным сигналом 4–20 мА подключен к аналоговому входу безопасного ПЛК. Уставка в блоке сравнения должна быть наиболее близка к какой величине?

Ответ b.

Объяснение. Калибровка передатчика рассчитана на диапазон 100–250 psi (изб.), что соответствует диапазону измерений (span) в 150 psi (изб.). Уставка задана на отметке 100 в пределах этого диапазона.

Таким образом, предельное значение для блока сравнения вычисляется по формуле.

$$(100 / 150) \times 4095 = 2730.$$

Тест 9.11. Сравните PES и электромеханические реле, указав преимущества и недостатки каждого. Также объясните, в каких ситуациях каждая технология будет более предпочтительной.

В качестве примера. приведен небольшой выбор преимуществ для каждой технологии.

Тест 9.12. Сравнение технологий для систем безопасности (СПАЗ/SIS).

Вопрос 1. Каковы основные преимущества программируемых электронных систем (PES) по сравнению с электромеханическими реле?

Ответ В. Гибкость настройки логики.

Объяснение. PES предлагают высокую гибкость в настройке логики, что позволяет адаптировать систему под конкретные потребности. В отличие от электромеханических реле, которые имеют фиксированную логику, PES могут выполнять сложные арифметические функции и поддерживать связь с ПК.

Вопрос 2. В каких ситуациях более предпочтительно использовать электромеханические реле?

Ответ В. Для простых логических задач.

Объяснение. Электромеханические реле лучше подходят для простых логических задач, особенно когда требуется высокая надежность и устойчивость к помехам. Они также могут быть более экономичными для простых приложений.

Вопрос 3. Какие недостатки имеют PES по сравнению с реле?

Ответ D. Все вышеперечисленное.

Объяснение. PES действительно имеют недостатки, такие как необходимость сертификации по SIL для обеспечения безопасности, более сложная установка и потенциально более высокий уровень ложных срабатываний по сравнению с реле.

Вопрос 4. Как аналоговый передатчик с выходным сигналом 4–20 мА может использоваться в СПАЗ/SIS с электромеханическими реле?

Ответ С. Для сравнения аналогового сигнала с заданной точкой срабатывания.

Объяснение. Аналоговый передатчик с выходным сигналом 4–20 мА может использоваться в СПАЗ/SIS с электромеханическими реле через реле срабатывания. Это устройство сравнивает аналоговый сигнал с установленной точкой срабатывания и генерирует цифровой выход для управления релейными системами. Такие реле должны иметь сертификат SIL для использования в системах безопасности.

При проектировании систем безопасности (СПАЗ/SIS) важно учитывать выбор технологии, так как от этого зависит надежность и безопасность системы. Сравнивая реле и PES, имеем:

PES

- + Самостоятельная документация.
- + Арифметические функции.
- + Гибкость настройки логики.
- + Поддержка связи с ПК.
- + Встроенная диагностика

Реле

- + Низкая стоимость.
- + Устойчивость к помехам.

Реле подходят для простых логических задач (при использовании специальных безопасных реле), но требуют частых проверок и могут иметь высокий уровень ложных срабатываний. Эти устройства просты в использовании и надежны при выполнении простых логических задач. Они устойчивы к внешним помехам и имеют низкую стоимость, что делает их идеальными для простых приложений. Однако они могут иметь высокий уровень ложных срабатываний и требуют частых проверок.

PES-системы гибки, но требуют сертификации по SIL для соответствия целям безопасности. Эти системы предлагают высокую гибкость, возможность выполнения сложных логических операций и встроенную диагностику. Они могут легко адаптироваться под изменяющиеся условия и требования системы. Однако их установка может быть более сложной, и они требуют сертификации по SIL для обеспечения безопасности.

Использование аналогового датчика с выходным сигналом 4–20 мА в системах с электромеханическими реле позволяет осуществлять мониторинг и контроль параметров. Реле срабатывания сравнивают аналоговые сигналы с заданными точками, что позволяет обеспечить безопасность и надежность системы. Эти устройства также должны иметь сертификаты SIL для обеспечения соответствия стандартам безопасности.

Таким образом, выбор между PES и электромеханическими реле зависит от конкретных требований системы, уровня сложности задач и бюджета.

Рекомендуют также использовать так называемые «Реле срабатывания» (trip relay). Это устройство сравнивает аналоговый сигнал с предварительно заданной точкой срабатывания и обычно имеет цифровой выход для подключения к релейным системам. Эти устройства должны иметь сертификат SIL для использования в системах безопасности.

Тест 9.13. Итоговые вопросы для самопроверки

1. Почему в расчете PFD_{avg} для резервированных компонентов используется квадрат λ_{du} ?

2. Как конфигурация 2oo3 влияет на PFD_{avg} и STR по сравнению с 1oo2?

3. Какие компоненты СПАЗ/SIS обычно вносят наибольший вклад в STR?

Ответ.

1. Потому что для отказа системы нужно, чтобы оба компонента отказали (Потому что для отказа системы, построенной на параллельном резервировании с голосованием 1oo2 (один из двух), нужно, чтобы оба компонента отказали небезопасным, обнаруженным об-

разом. Вероятность такого события является произведением вероятностей отказа каждого отдельного компонента (суммарная вероятность $\approx \lambda^2$). Квадрат λ (или более высокая степень) отражает значительное повышение надежности системы за счет резервирования. системе требуется гораздо более редкое событие (одновременный отказ нескольких элементов), чтобы ее функция безопасности была скомпрометирована.

2. Конфигурация 2oo3 обычно снижает PFDavg (повышая отказо-безопасность, но увеличивает STR (снижая отказоустойчивость). STR показывает, как часто система будет ложно срабатывать, переводя процесс в безопасное состояние без реальной необходимости. Чем ниже STR, тем выше отказоустойчивость (лучше непрерывность производства). Ложные срабатывания вызваны безопасными, необнаруженными отказами и опасными, обнаруженными отказами, которые диагностируются системой и приводят к ее срабатыванию.

3. Клапаны и исполнительные механизмы (высокий λ_{sd}). Клапаны и исполнительные механизмы, а также связанные с ними управляющие клапаны/регуляторы (например, соленоидные клапаны), обычно вносят наибольший вклад в STR. Исполнительные механизмы (например, отсечные клапаны) по своей природе имеют множество движущихся частей, подвержены износу, коррозии, загрязнению. Поэтому их часто настраивают на отказ в «безопасное» положение (например, клапан закрывается при потере питания. Соответственно, у них может быть относительно высокая частота безопасных отказов λ_s (сумма λ_{sd} и λ_{su}).

РАЗДЕЛ 10.

Тест 10.4.

Ответ: a, b, c, d, e, h, i, j.

Правильно:

a) Диагностика действительно подразумевает регулярные проверки состояния различных устройств, таких как программируемые электронные системы (ПЭС) и датчики, для оценки их работоспособности и выявления потенциальных проблем.

b) Высокий уровень охвата диагностикой действительно способствует снижению рисков, связанных с отказами оборудования, обеспечивая своевременную реакцию на возникающие проблемы.

c) Самотестирование является одним из методов диагностики, который дополняет другие виды проверок, проводимые в рамках технического обслуживания системы предотвращения аварий (СПАЗ/SIS).

d) До широкого распространения микропроцессорной техники действительно были ограниченные возможности для проведения эффективной диагностики датчиков и исполнительных устройств.

е) Современные программные системы действительно предоставляют расширенные возможности для реализации продвинутых методов самодиагностики.

h) Использование датчиков с сертификатом безопасности и интеллектуальных датчиков с функцией диагностической сигнализации является рекомендуемой практикой для повышения надежности и безопасности системы.

i) Применение резервированных датчиков полезно для сравнения показаний и выявления отклонений, что помогает улучшить точность и надежность работы системы.

j) Контрольные проверки действительно не рассматриваются как полноценная диагностика, так как они проводятся реже и направлены скорее на общее обслуживание системы, чем на оперативное выявление проблем.

Неправильно:

f) Контрольные проверки не входят в состав диагностики, так как они проводятся значительно реже и не обеспечивают непрерывного мониторинга состояния оборудования.

g) Метод сравнения значения сигнала срабатывания с другими связанными переменными действительно существует, но он не является новым и широко распространенным, поэтому данное утверждение некорректно.

Подробное объяснение каждого пункта.

Пункт а. Регулярные проверки состояния устройств, таких как программируемые электронные системы (ПЭС) и датчики, необходимы для поддержания высокой степени готовности системы предотвращения аварий. Эти проверки помогают выявить отклонения в работе оборудования до того, как они приведут к серьезным последствиям.

Пункт b. Высокий уровень охвата диагностикой играет ключевую роль в обеспечении безопасности, так как он позволяет вовремя обнаруживать потенциальные проблемы и принимать меры для их устранения. Это снижает вероятность развития аварийных ситуаций.

Пункт c. Самотестирование – это эффективный способ диагностики, который дополняет традиционные методы контроля, такие как функциональные и контрольные проверки. Оно позволяет выявлять неполадки в режиме реального времени, что делает систему более надежной.

Пункт d. До появления микропроцессоров возможности для диагностики датчиков и исполнительных устройств были ограниченными. Микропроцессорные технологии существенно улучшили качество и эффективность диагностики, предоставив инструменты для автоматизированного мониторинга и анализа данных.

Пункт е. Современные программные системы открывают новые горизонты в области самодиагностики. Они позволяют реализовывать сложные алгоритмы анализа данных, что улучшает точность и скорость выявления неисправностей.

Пункт h. Использование датчиков с сертификатом безопасности и интеллектуальных датчиков с функцией диагностической сигнализации помогает повысить надежность системы. Такие устройства способны самостоятельно отслеживать свою работу и сообщать об ошибках, что упрощает задачу операторам и инженерам.

Пункт i. Резервированные датчики играют важную роль в повышении точности измерений и обнаружении аномалий. Сравнивая показания нескольких датчиков, можно определить, какой из них работает неправильно, и принять соответствующие меры.

Пункт j. Контрольные проверки отличаются от диагностики тем, что они проводятся гораздо реже и служат больше для общего обслуживания системы, нежели для оперативного выявления проблем. Поэтому их нельзя считать полноценной заменой диагностики.

Тест 10.5. Определение SFF и SIL для одноканальной конструкции. Химическая компания требует, чтобы использовался МЭК 61508 Route 1Н для определения архитектурных ограничений ИУ в сборке.

Вопрос 1.

Ответ D.

Объяснение. Поскольку данные о частоте безопасных отказов для трехходового прямодействующего тарельчатого электромагнитного клапана не указаны, их невозможно точно определить. Однако, $\lambda_S = 450 \text{ FITS}$ и $\lambda_D = 240 \text{ FITS}$ известны.

Вопрос 2. Какова общая интенсивность безопасных отказов (λ_{Stotal}) для системы, если известны интенсивности безопасных отказов для всех элементов. 450 FITS, 800 FITS и 0 FITS?

Ответ B.

Объяснение. Общая интенсивность безопасных отказов (λ_{Stotal}) для системы рассчитывается как сумма всех интенсивностей безопасных отказов. $450 + 800 + 0 = 1250 \text{ FITS}$.

Вопрос 3.

Ответ C.

Объяснение. Интенсивность опасных необнаруженных отказов ($\lambda_{DUV\text{ всего}}$) рассчитывается как сумма всех интенсивностей. $240 + 650 + 700 = 1590 \text{ FITS}$.

Вопрос 4.

Ответ C.

Объяснение. SFF (Safe Failure Fraction) вычисляется как отношение общей интенсивности безопасных отказов к сумме общей интенсивности безопасных отказов и интенсивности опасных необнаруженных отказов. $SFF = \lambda_{Stotal} / (\lambda_{Stotal} + \lambda_{DUвсего})$.

Вопрос 5.

Ответ С.

Объяснение. Согласно МЭК 61508, конструкция с HFT = 0 соответствует требованиям уровня безопасности SIL 3, что указывает на высокую степень надежности системы

При анализе архитектурных ограничений и расчете SFF важно учитывать все данные о частоте отказов и правильно применять формулы для определения уровня безопасности (SIL). В данном случае, несмотря на отсутствие данных о безопасных отказах для одного из элементов, расчеты показывают, что система соответствует требованиям SIL 3, что критически важно для обеспечения надежной работы в технологической отрасли.

Решение. существует проблема с данными, предоставленными для 3/2 прямого действия.

Тарельчатый электромагнитный клапан, частота безопасных отказов не указана. Однако, поскольку данные об интенсивности опасных отказов сомнительны, общие данные об отказах получаются как $\lambda_S = 450$ FITS и $\lambda_D = 240$ FITS. SFF применяется к каждому «элементу» согласно МЭК 61508.

Интенсивность отказов ИУ суммируется для каждой категории следующим образом.

$$\lambda_{Stotal} = 450 + 800 + 0 = 1250 \text{ FITS.}$$

$$\lambda_{DUвсего} = 240 + 650 + 700 = 1590 \text{ FITS.}$$

$$SFF \text{ составляет } 1250 / (1250 + 1590) = 44\%.$$

Это элемент типа А. Ссылаясь на Таблицу 6 МЭК 61511-1, конструкция HFT = 0, что соответствует требованию уровня безопасности SIL 1.

Тест 10.6. Расчет диагностического покрытия (DC) по методу Route 2H (МЭК 61508).

Вопрос 1.

Ответ а.

Объяснение. Датчики с резервированием и самодиагностикой (например, HART) могут достигать $DC > 90\%$, тогда как исполнительные механизмы сложнее диагностировать.

Вопрос 2.

Ответ а.

Объяснение. DC рассчитывается только для опасных отказов.

Вопрос 3.

Ответ а.

Объяснение.

Необнаруженные отказы = $\lambda D \times (1 - DC) = 0.001 \times (1 - 0.75) = 0.00025$.

10.7. Практическое задание.

Задача. Рассчитайте DC для резервированного датчика температуры (2oo3), если имеют место быть опасные отказы (завышение показаний, занижение показаний, обрыв цепи) и выполняется контроль диапазона (4–20 мА), сравнение показаний трех датчиков.

Решение.

Всего опасных отказов. 3.

Для обнаружения обрыва цепи необходим контроль диапазона.

Для обнаружение завышение/занижение показаний используется голосование, например, 2oo3.

$DC = (3/3) \times 100 = 100\%$ (в идеальной модели).

DC зависит от типа компонента и применяемых методов диагностики.

Route 2H требует анализа всех опасных отказов.

Для достижения SIL 2/3 необходимо $DC > 60-90\%$.

Формула для запоминания.

$DC = 100\% \lambda_{DD} / \lambda_D$,

где:

- λ_{DD} – интенсивность обнаруженных опасных отказов,
- λ_D – общая интенсивность опасных отказов.

РАЗДЕЛ 11.

Тест 11.13. Проводка полевого устройства к системе ввода/вывода.

Ответ d.

Объяснение. Последовательное подключение нескольких дискретных датчиков к одному входу – метод, применяемый в некоторых системах безопасности (например, в системах пожарной сигнализации). Поскольку датчики контролируют одно и то же состояние процесса, такая схема допустима.

Подключение нескольких исполнительных устройств (отключаемых при срабатывании) к одному выходу не создает дополнительных рисков, если используется одинарная линия. Однако это может быть не рекомендовано в зависимости от токов нагрузки и требований производителя.

Использование полевой шины (fieldbus) увеличивает риск общих отказов для устройств, которые предполагаются независимыми. Стандарт ISA S84.01 явно запрещает применение fieldbus в системах безопасности.

Тест 11.14. Сертификат соленоидного клапана.

Вопрос 1. Почему пользователь соленоидного клапана не может просто принять сертификат функциональной безопасности, выданный сторонней организацией, без дополнительной информации?

Ответ D.

Объяснение.

1. Условия эксплуатации. Сертификат может указывать на уровень функциональной безопасности (SIL 3 или SIL 4), но не учитывает конкретные условия эксплуатации, такие как температура, давление, химическая среда и другие факторы, которые могут повлиять на надежность и безопасность клапана в реальных условиях.

2. Тип применения. Сертификат может быть выдан для определенного типа применения или сценария, но не обязательно подходит для всех возможных приложений в процессной промышленности. Пользователь должен убедиться, что клапан соответствует требованиям конкретного процесса.

3. Тестирование и верификация. Сертификат может не содержать достаточной информации о проведенных тестах и верификации. Пользователь должен знать, как проводились испытания, какие методы использовались и какие результаты были получены. Это важно для оценки надежности клапана в конкретной системе.

Таким образом, прежде чем принимать сертификат, пользователю необходимо провести дополнительный анализ и убедиться, что клапан соответствует всем требованиям их специфического применения.

Вопрос 2.

Ответ D.

Объяснение.

1. Независимая оценка. Пользователь может заказать независимую оценку клапана, чтобы получить объективное мнение о его надежности и соответствии требованиям безопасности.

2. Документация производителя. Изучение документации производителя поможет понять, как клапан должен использоваться, какие у него характеристики и какие ограничения могут быть.

3. Сертификаты других компонентов. Проверка сертификатов на другие компоненты системы важна для обеспечения совместимости и общей надежности всей системы.

Таким образом, для обеспечения безопасности и надежности системы необходимо учитывать все эти аспекты.

При проектировании функции безопасности всегда необходимо обосновывать использование конкретного оборудования. Это Объяснение относится к мерам защиты от систематических отказов, которые могут быть продемонстрированы с помощью сертификации по МЭК 61508 или документально подтвержденной информацией о практическом применении, а также к пригодности оборудования для использования.

В вопросе указано, что выдан сертификат. Однако не указано основание для выдачи сертификата; например, какой стандарт был принят во внимание. Оборудование, удовлетворяющее требованиям однократного использования для SIL 3, должно иметь высокий уровень диагностики, который может быть недоступен для соленоидов. Поэтому пользователь должен убедиться, что применение, используемое для демонстрации пригодности соленоида для применений SIL 3, соответствует его фактическим рабочим профилям. Оценивался ли соленоид на основе приложения для низконагрузочной технологической отрасли или циклового теста в лабораторных условиях? В последнем случае сертификат не будет пригоден для использования в типичном приложении технологической отрасли.

Тест 11.15. Интенсивность опасных отказов (λ_D) исполнительных устройств.

Значения интенсивностей отказов компонентов обычно берутся из баз данных стандартов или справочных каталогов производителей компонентов.

Вопрос 1. Для расчётов надёжности системы управления, какую типовую интенсивность опасных отказов (λ) следует принять для трёхходового прямодействующего золотникового соленоидного клапана 3/2 согласно стандартным справочным данным?

Ответ А.

Объяснение. Данное значение является стандартным справочным значением для данного типа клапанов. Учитывается вероятность залипания, износ соленоида. Это означает, что статистически ожидается 240 опасных отказов на миллиард часов непрерывной работы устройства.

Вопрос 2. Какова типовая интенсивность опасных отказов (λ) для пружинного возвратно-шестерёнчатого привода?

Ответ В.

Объяснение. Приводы, содержащие механические компоненты (шестерни, пружины), как правило, имеют более высокую интенсивность отказов по сравнению с чисто электромеханическими компонентами (как соленоид в предыдущем вопросе), что и отражает значение 900 FIT, которое взято из справочного каталога.

Вопрос 3. Какова типовая интенсивность опасных отказов (λ) трёхэксцентрикового дискового затвора, когда он находится в режиме, близком к срабатыванию (т.е., не постоянно открыт/закрыт, а циклически переключается)?

Ответ С.

Объяснение. Для арматуры (заслонок, клапанов) интенсивность отказов сильно зависит от режима работы. Циклическое переключение создает механический износ, что увеличивает вероятность отказа

по сравнению со статическим режимом. Согласно справочному каталогу значение 750 FIT является характерным для таких условий эксплуатации.

Вопрос 4. Как рассчитывается суммарная интенсивность опасных отказов (λ_{total}) всего исполнительного механизма, состоящего из нескольких устройств (например, клапан + привод)?

Ответ А.

Объяснение. Если отказ любого из компонентов приводит к отказу всей системы (последовательное соединение в смысле надёжности), то общая интенсивность отказов вычисляется как сумма интенсивностей отказов всех компонентов. $\lambda_{total} = \lambda_1 + \lambda_2 + \dots + \lambda_n$.

Вопрос 5. Чему равна суммарная интенсивность опасных отказов (λ_{total}) ИУ, состоящей из клапана (240 FIT), привода (900 FIT) и затвора (750 FIT)?

Ответ А.

Объяснение. Расчёт производится в соответствии с правилом из вопроса 4. $\lambda_{total} = \lambda_{\text{клапан}} + \lambda_{\text{привод}} + \lambda_{\text{затвор}} = 240 \text{ FIT} + 900 \text{ FIT} + 750 \text{ FIT} = 1890 \text{ FIT}$. Это значение является основой для дальнейшего расчёта вероятности отказа системы функциональной безопасности (PFD).

Тест 11.16. Расчёт вероятности опасного отказа (PFDavg).

Вопрос 1. Какова типовая интенсивность опасных отказов (λ) золотниковового электромагнитного клапана 3/2 с пилотным управлением?

Ответ А.

Объяснение. Клапаны с пилотным управлением сложнее прямодействующих, так как имеют дополнительную камеру источник и каналы для управления. Эта повышенная сложность согласно стандартным справочным данным приводит к увеличенной интенсивности опасных отказов (720 FIT).

Вопрос 2. Какова типовая интенсивность опасных отказов (λ) для привода с кулисным механизмом с пружинным возвратом?

Ответ В.

Объяснение. Кулисный механизм – это еще более сложная механическая система по сравнению с шестерёнчатым приводом. Дополнительные шарниры, оси и точки трения объясняют более высокое значение интенсивности отказов в 1250 FIT.

Вопрос 3. Какова типовая интенсивность отказов (λ) поплавкового шарового клапана в режиме, близком к срабатыванию?

Ответ С.

Объяснение. Шаровые клапаны в режиме, близком к срабатыванию, испытывают повышенные нагрузки. Интенсивность отказов $\approx 2.87 \times 10^{-6} / \text{час} = 2870 \text{ FIT}$ учитывает возможное залипание, износ уплотнений шарового клапана

Вопрос 4. Какая формула используется для расчёта PFDavg системы, если учитываются коэффициент эффективности автоматической диагностики CPT, время восстановления после обнаруженных отказов (MRT) и периодическое техническое обслуживание (с интервалом TI)?

Ответ В.

$PFD_{avg} \approx \lambda_{DD} \cdot MRT_{DD} + CPT \cdot \lambda_{DU} \cdot (TI/2 + MRT_{DU}) + (1 - CPT) \cdot \lambda_{DU} \cdot MT/2.$

Объяснение.

$\lambda_{DD} \cdot MRT_{DD}$ – это вклад *обнаруженных* опасных отказов. Система находится в нерабочем состоянии в среднее время их восстановления.

$CPT \cdot \lambda_{DU} \cdot (TI/2 + MRT_{DU})$. Вклад *необнаруженных* отказов, которые могла бы обнаружить диагностика (с коэффициентом покрытия CPT). Они выполняются с момента пуска до следующего ТО (в среднем $TI/2$), плюс время на их устранение.

$(1 - CPT) \cdot \lambda_{DU} \cdot MT/2$ – это вклад *необнаруженных* отказов, которые диагностика *обнаружить не может*. Считается, что такой отказ существует с момента пуска СПАЗ/SIS до конца срока службы системы (в среднем $MT/2$).

Вопрос 5. Рассчитайте PFDavg системы с общей интенсивностью *опасных необнаружимых* отказов $\lambda_{DU} = 2870 \text{ FIT}$ (т.е. $2870 \cdot 10^{-9} \text{ 1/час}$). Коэффициент эффективности автоматической диагностики $CPT = 93\%$, интервал ТО (TI) = 2 года, среднее время восстановления $MRT = 24$ часа. Срок службы (MT) принять равным 10 годам.

Ответ В.

Объяснение.

Шаг 1. Переводим всё в часы.

$TI = 2 \text{ года} \cdot 8760 \text{ час/год} = 17520 \text{ часов.}$

$MT = 10 \text{ лет} \cdot 8760 \text{ час/год} = 87600 \text{ часов.}$

$\lambda_{DU} = 2870 \cdot 10^{-9} \text{ 1/час.}$

Шаг 2. Анализируем формулу. В данной системе $\lambda_{DD} = 0$. В условии не дано, значит, все отказы считаются необнаруживаемыми до ТО? Поэтому формула упрощается до.

$PFD_{avg} \approx [CPT \cdot \lambda_{DU} \cdot (TI/2 + MRT)] + [(1 - CPT) \cdot \lambda_{DU} \cdot (MT/2)].$

Шаг 3. Подставляем значения.

Первое слагаемое. $0.93 \cdot (2870 \cdot 10^{-9}) \cdot (17520/2 + 24) = 0.93 \cdot 2870 \cdot 10^{-9} \cdot (8760 + 24) = 0.93 \cdot 2870 \cdot 10^{-9} \cdot 8784.$

Второе слагаемое. $(1 - 0.93) \cdot (2870 \cdot 10^{-9}) \cdot (87600/2) = 0.07 \cdot 2870 \cdot 10^{-9} \cdot 43800.$

Шаг 4. Производим вычисления.

Первое слагаемое $\approx 0.93 \cdot 2870 \cdot 8784 \cdot 10^{-9} \approx 0.0219.$

Второе слагаемое $\approx 0.07 \cdot 2870 \cdot 43800 \cdot 10^{-9} \approx 0.0103.$

$PFD_{avg} \approx 0.0219 + 0.0103 = 0.0322.$

Вывод. Средняя вероятность опасного отказа системы составляет **0.0322**, что соответствует уровню SIL 1 (PFDavg от 0.01 до 0.1).

Тест 11.17. Отказы по общей причине

Вопрос 1. Что такое отказы по общей причине?

Ответ b. Это отказы, возникающие из-за одинаковых дефектов в нескольких компонентах системы.

Объяснение. Отказы по общей причине происходят, когда несколько компоненты системы подвергаются одинаковым условиям или дефектам, что приводит к их одновременному выходу из строя. Это может значительно снизить надежность системы, особенно в условиях резервирования. Такие отказы могут устраняться различными путями. В частности использованием различных датчиков в схемах резервирования (рис. 11.1)

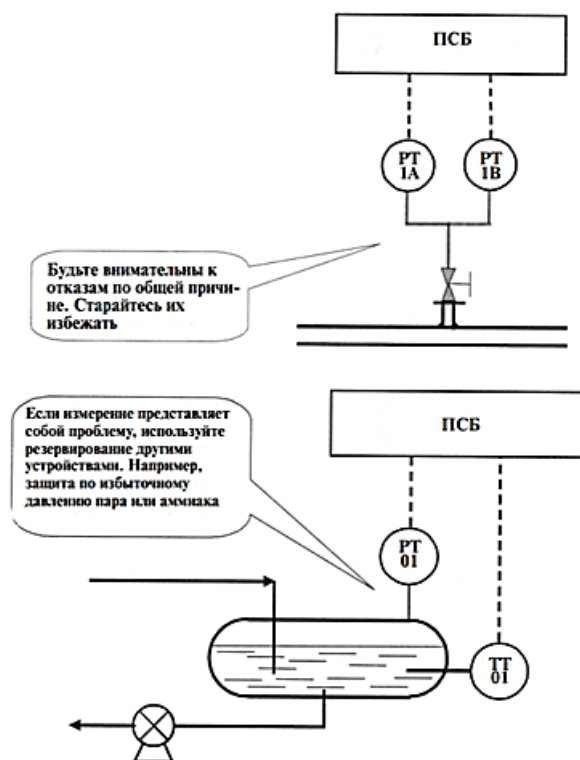


Рис 11.1. Отказы по общей причине и их устранение

Вопрос 2. Какой из следующих видов дефектов документации не следует игнорировать при проектировании СПАЗ?

Ответ а.

Объяснение. Неправильная спецификация может привести к тому, что компоненты системы не будут функционировать должным образом, что увеличивает риск отказов. Это важный аспект, который необходимо учитывать при проектировании систем безопасности.

Вопрос 3. Какое воздействие со стороны окружающей среды может привести к отказам по общей причине?

Ответ d.

Объяснение. Все перечисленные факторы могут негативно влиять на работу компонентов системы, вызывая отказы. Например, высокая температура или влажность могут привести к повреждению электроники, а электромагнитные помехи могут нарушить работу датчиков и исполнительных устройств.

Вопрос 4. Как неправильные процедуры обслуживания могут привести к отказам по общей причине?

Ответ b.

Объяснение. Неправильные процедуры обслуживания могут привести к тому, что компоненты системы будут неправильно настроены или откалиброваны, что в свою очередь увеличивает риск отказов и может привести к одновременному выходу из строя нескольких устройств.

Вопрос 5. Как можно минимизировать риски отказов по общей причине в проектировании СПАЗ?

Ответ b.

Объяснение. Регулярное обслуживание и калибровка помогают выявлять и устранять потенциальные проблемы, которые могут привести к отказам по общей причине. Это важная мера для повышения надежности системы и снижения рисков. Будьте внимательны к отказам по общей причине. Старайтесь их избежать

Для получения дополнительной информации см. [28].

Тест 11.18.

Вопрос 1. Что означает термин «доказано практикой» в контексте систем безопасности?

Ответ b. Это обозначает, что компонент был использован в реальных условиях и показал свою надежность.

Объяснение. Термин «доказано практикой» подразумевает, что компонент прошел документированную оценку на основе предыдущего использования и показал свою пригодность для применения в системах безопасности. Это важно для обеспечения надежности и безопасности системы.

Вопрос 2. Какое из следующих требований должно быть выполнено для того, чтобы компонент считался «доказанным практикой»?

Ответ b. Необходима оценка, подтверждающая его пригодность.

Объяснение. Для признания компонента «доказанным практикой» необходимо провести документированную оценку, которая подтверждает его пригодность для использования в системах безопасности. Это включает в себя анализ его работы в аналогичных условиях.

Вопрос 3. Что должно быть учтено при проведении оценки компонента для признания его «доказанным практикой»?

Ответ b. Система оценки качества производителя.

Объяснение. Оценка должна учитывать систему оценки качества производителя, чтобы убедиться в надежности и качестве компонента.

Это позволяет снизить риски, связанные с использованием ненадежных компонентов в системах безопасности.

Вопрос 4. Какую дополнительную оценку необходимо провести для интеллектуальных устройств (ПЭС)?

Ответ b. Оценка, основанную на предыдущем опыте использования аналогичных устройств.

Объяснение. Для интеллектуальных устройств требуется дополнительная оценка, чтобы убедиться в их надежности и пригодности для применения в системах безопасности. Это связано с тем, что такие устройства могут иметь сложные функции и потенциальные риски, которые необходимо учитывать.

Вопрос 5. Какое исключение существует для конфигураций, ограниченных защитой в виде пароля?

Ответ d. Они требуют дополнительной оценки, если позволяют изменять настройки параметров процесса.

Объяснение. Конфигурации, ограниченные защитой в виде пароля, требуют дополнительной оценки, если они позволяют изменять настройки параметров процесса. Это необходимо для обеспечения безопасности и надежности системы, поскольку изменения могут повлиять на работу системы.

Прибор должен соответствовать функциональным требованиям и требованиям полноты безопасности из СТБ. Должна иметься адекватная документация по интеграции, функционированию и обслуживанию.

Оценка должна базироваться на известном (исходя из практики) использовании прибора с уточнением совпадений с данным применением.

Покажите, что возможность появления систематических ошибок мала. Выделите неиспользуемые компоненты устройства и покажите, что они не повлияют на работу СПАЗ/SIS. Объем предыдущего опыта работы должен быть достаточен для обеспечения статистической достоверности. Время эксплуатации при предыдущем использовании компонента должно превышать один год.

Все сказанное выше направлено на то, чтобы убедиться, что пользователь применяет в системе безопасности не «просто какой то старый прибор». Фактически, больше проблем возникает с «каким либо новым устройством», поскольку в этом случае трудно установить, имеется ли необходимый предыдущий опыт работы. В частности, следует иметь в виду, что если мы хотим использовать в системе безопасности интеллектуальное устройство, то оно должно соответствовать приведенным выше требованиям, либо должно быть сертифицировано, что оно было построено и испытано в соответствии с требованиями стандартов МЭК 61508 и МЭК 61511.

Для получения дополнительной информации см. [28].

РАЗДЕЛ 12.

Тест 12. 8. Обслуживание СПАЗ.

Вопрос 1. Какие из следующих утверждений о проектировании системы безопасности автоматизации (СПАЗ/SIS) являются верными?

Ответ: А, С, D.

Объяснение.

Ответ А. Верно. Проектирование должно предусматривать возможность обслуживания системы без отключения, чтобы избежать простоя и поддерживать безопасность.

Ответ В. Неверно. Использование перемычек может угрожать целостности системы и привести к ложным срабатываниям, что недопустимо в СПАЗ/SIS.

Ответ С. Верно. Все элементы должны быть доступны для обслуживания с минимальными рисками для безопасности процесса.

Ответ D. Верно. Необходимо учитывать возможность испытаний на действующем процессе, чтобы гарантировать надежность и работоспособность системы.

Вопрос 2. Каковы основные технические и процедурные требования к испытанию СПАЗ/SIS?

Ответ: В, С.

Объяснение.

Ответ А. Неверно. Испытания не должны проводиться только в отключенном состоянии, так как это не отражает реальную работу системы.

Ответ В. Верно. Наличие четких инструкций позволяет избежать ошибок при проведении испытаний и обеспечивает их стандартизацию.

Ответ С. Верно. Документирование испытаний необходимо для анализа результатов и улучшения процессов обслуживания и испытаний.

Ответ D. Неверно. Обслуживающий персонал должен участвовать в испытаниях для обеспечения безопасности и правильного выполнения процедур.

Вопрос 3. Как следует организовать обслуживание датчиков и исполнительных элементов в рамках действующего процесса?

Ответ: В, D.

Объяснение.

Ответ А. Неверно. Доступ к элементам системы должен быть регламентирован, чтобы избежать случайного вмешательства.

Ответ В. Верно. Процедуры обслуживания должны минимизировать риск ложных срабатываний и обеспечивать безопасность процесса.

Ответ С. Неверно. Обслуживание не должно проводиться в часы пик, так как это увеличивает риски и может негативно сказаться на безопасности.

Ответ D. Верно. Защита датчиков и исполнительных элементов от случайного вмешательства важна для сохранения целостности системы.

Тест 12.9. Группа оценки функциональной безопасности.

Вопрос 1. Какие из следующих утверждений о назначаемой группе оценки функциональной безопасности верны?

Ответ а.

Объяснение. Группа, которая выполняет оценку функциональной безопасности, как и группа, которая выполняет анализ технологических опасностей, должна иметь разнообразный набор знаний, который максимизирует вероятность выявления любых существующих проблем. Эта группа должна включать членов из технического персонала, специалистов по приложениям и специалистов по эксплуатации.

Для обеспечения достаточного разделения между оценочной группой и проектной группой оценочная группа должна содержать как минимум одного старшего компетентного члена, который не участвует в проектировании. Это лицо должно обладать компетенцией для понимания приложения и жизненного цикла безопасности. Это лицо должно также иметь достаточный авторитет, чтобы проектная группа не могла игнорировать выводы группы по оценке функциональной безопасности. Как и в случае с другими задачами жизненного цикла безопасности, стандарты не требуют участия независимой третьей стороны в каких-либо задачах жизненного цикла безопасности.

См. МЭК 61511 часть 1, пункт 5.2.6.1.2, и тот же пункт в МЭК 61511 часть 2.

Тест 12.10. Какое из следующих утверждений наиболее точно описывает разницу между верификацией и валидацией, как определено в МЭК 61508 и МЭК 61511?

Ответ с.

Объяснение В соответствии с МЭК 61511 часть 1, раздел 3 (в котором перечислены все определения для стандарта), проверка и валидация имеют следующие определения.

Валидация – деятельность, демонстрирующая, что рассматриваемая система безопасности после установки во всех отношениях соответствует спецификации требований безопасности.

Проверка – деятельность, демонстрирующая для каждой фазы соответствующего жизненного цикла безопасности путем анализа и/или испытаний, что для конкретных входных данных результаты соответствуют во всех отношениях целям и требованиям, установленным для конкретной фазы.

Тест 12.11. Какие из следующих утверждений верны для требований к документированию задач жизненного цикла безопасности в соответствии с МЭК 61511?

Ответ б.

Объяснение. Стандарты, определяющие действия жизненного цикла безопасности, требуют создания документации для задач жизненного цикла безопасности, но не указывают, что документация должна быть на бумаге (хотя она должна быть доступна). Стандарты допускают, что документация может храниться в электронном формате, например, в файлах текстового процессора или на веб-страницах.

Информация, которая создается, должна быть легкодоступной и отслеживаемой в соответствии со стандартами. Поддержание документации в электронном формате, когда это уместно, будет способствовать выполнению этих требований.

Требования к документации кратко изложены в МЭК 61511 часть 1, раздел 19.

Тест 12.12.

Ответ а.

Объяснение. Многие компоненты системы безопасности требуют ручного тестирования, чтобы обеспечить поддержание уровня целостности безопасности, для которого они сертифицированы, во время работы. Информация о требованиях к тестированию и другая важная информация по установке и эксплуатации находится в руководстве по безопасности продукта. Это руководство по безопасности проверяется органом по сертификации и является неотъемлемой частью процесса утверждения.

Важно ознакомиться с Руководством по безопасности продукта компонента, поскольку оно может содержать важную информацию, которая может не быть включена в другую документацию, такую как спецификации и маркетинговая информация.

Требования, относящиеся к руководствам по безопасности, показаны в МЭК 61508.2010 часть 2, пункты 7.4.9.6 и 7.4.9.7, и Приложение D.

ЗАКЛЮЧЕНИЕ

Выполненные упражнения и тесты по проектированию и внедрению СПАЗ позволяют инженеру (внешнему аудитору) правильно оценивать исходные требования (полноту спецификации), проектные решения и эксплуатационные документы жизненного цикла СПАЗ. Для облегчения таких проверок рекомендуется использование готового шаблона.

Шаблон внутренней проверки (внешнего аудита) СПАЗ.

Проект: [Название проекта].

Дата аудита: [Дата].

Аудитор: [ФИО].

Цель аудита: Проверка документации, подтверждение и оценка соответствия расчетов и испытаний СПАЗ требованиям безопасности.

1. Проверка соответствия. Нормативная база.

Задача: Убедиться в соответствии нормативным документам.

Федеральный закон №116-ФЗ «О промышленной безопасности».

Приказ РТН №533 «Общие правила взрывобезопасности».

ГОСТ Р МЭК 61511 (Функциональная безопасность).

[Другие отраслевые стандарты и внутренние регламенты].

2. Подтверждение соответствия функции безопасности (SIF).

Задача: Верифицировать, что требования к каждой SIF детализованы, измеримы и подтверждены расчетами.

Для каждой SIF указан целевой SIL на основе отчетов HAZOP/LOPA, установлено правило проектирования ROUTE.

Однозначно определены условия срабатывания SIF и безопасное состояние ОПО.

Время отклика SIF рассчитано с запасом от времени развития аварии.

Архитектурные ограничения (HFT) соответствуют целевому SIL.

Подтверждающие документы: Отчеты HAZOP/LOPA, SRS, схемы логики.

3. Подтверждение соответствия. Аппаратные компоненты.

Задача: Убедиться, что спецификации компонентов обеспечат выполнение SIF (таблица 14.1).

Таблица 14.1. Критерии проверки спецификации

Компонент	Критерии проверки
Датчики	☐ Тип, диапазон (+20% запас) ☐ Время отклика < 50% от времени SIF ☐ Сертификаты SIL, взрывозащиты (Ex) ☐ Климатическое исполнение
Исполнительные механизмы	☐ Принцип (с пружинным возвратом?) ☐ Время срабатывания < 70% от критичного для SIF ☐ Диагностика (датчики положения, PST) ☐ Сертификация SIL

Компонент	Критерии проверки
Логический решатель	☐ Сертификация SIL ☐ Архитектура резервирования (процессор, питание) ☐ Поддержка протоколов диагностики

Варианты выбора компонентов можно найти в специальных руководствах поставщиков [22]

4. Оценка соответствия. Анализ надежности и системных рисков.

Задача: Дать экспертную оценку полноты анализа отказов и учета внешних факторов.

Систематические отказы. Имеется План обеспечения безопасности, ведется управление конфигурацией.

Случайные отказы. Проведен FMEDA, расчеты PFDavg/SFF подтверждают заявленный SIL.

Внешние воздействия. Климатическое исполнение и стойкость к вибрации подтверждены сертификатами/протоколами.

5. Проверка соответствия. Документация.

Задача: Проконтролировать наличие обязательных документов.

Спецификация требований безопасности (SRS).

Отчеты HAZID, HAZOP, LOPA.

Расчеты PFDavg/SFF (например, по методологии EXIDA).

Сертификаты SIL и взрывозащиты на оборудование.

Схемы логики срабатывания, Техническое задание (ТЗ).

Для экспертизы ПБ: Протоколы испытаний, Заключение независимой экспертизы.

6. Оценка соответствия. Эффективность СПАЗ.

Задача: Оценить, будет ли система работать в реальных условиях.

Реакция системы на неисправности приводит в безопасное состояние

Учтены все режимы работы процесса (пуск, останов, обслуживание)

Пример: »SIF-201 предназначена для защиты от превышения давления. Достаточен ли выбранный клапан и его пропускная способность для реального сценария?»

Чек-лист аудитора (10 ключевых пунктов).

Если «НЕТ» в любом из пунктов 1-7, то система не соответствует заявленному SIL.

1. Сертификаты SIL на все компоненты (датчики, ПЛК, исполнительные механизмы).

2. FMEDA-отчеты с подтвержденными параметрами (λ_{du} , SFF, DC).

3. Расчет PFDavg для каждой SIF (датчик → логика → исполнитель).

4. Резервирование архитектуры соответствует SIL (1oo2 для SIL 2, 2oo3 для SIL 3).

5. Диагностика (самоконтроль ПЛК, мониторинг клапанов PST, диагностика КИП).

6. Условия эксплуатации (температура, вибрация) соответствуют данным производителя.

7. Верификация ПО (соответствие МЭК 61511-3, отсутствие недокументированных функций).

Режимы работы: Пуск, реакция на неисправности, ручное отключение и все стадии процесса описаны.

Техническое обслуживание: Периодичность ТО соответствует расчетному MTTR.

Эксплуатация: Ведутся журналы отказов, данные анализируются

Итоговое заключение:

☐ Соответствует требованиям.

☐ Соответствует с замечаниями (указать).

☐ Не соответствует.

Замечания и рекомендации:

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р МЭК 61508-1–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования». – URL. <https://docs.cntd.ru/document/1200103191>.
2. ГОСТ Р МЭК 61508-2–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам». – URL. <https://docs.cntd.ru/document/1200100344>.
3. ГОСТ Р МЭК 61508-3–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению». – URL. <https://docs.cntd.ru/document/1200100350>.
4. ГОСТ Р МЭК 61508-4– 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения». – URL. <https://docs.cntd.ru/document/1200102418>.
5. ГОСТ Р МЭК 61508-5–2012. «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности». – URL. <https://docs.cntd.ru/document/1200103192>.
6. ГОСТ Р МЭК 61508-6-2012. «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению». – URL. <https://docs.cntd.ru/document/1200103253>.
7. ГОСТ Р МЭК 61508-7–2012. «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства». – URL. <https://meganorm.ru/Data2/1/4293776/4293776875.pdf>
8. ГОСТ Р МЭК 61511–1–2018. «Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования». – URL. <https://docs.cntd.ru/document/1200160087>.
9. ГОСТ Р МЭК 61511–2–2018. «Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1». – URL. <https://files.stroyinf.ru/Data/697/69748.pdf>
10. ГОСТ Р МЭК 61511–3–2018. «Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности». – URL. <https://docs.cntd.ru/document/1200160132>.
11. ГОСТ Р 59504-2021 / ГОСТ Р 59504-2021/IEC TR 61511-4:2020. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 4. Пояснение и Объяснение изменений, внесенных в МЭК 61511-1 из издания 1 в издание 2. – URL. <https://meganorm.ru/Index/75/75192.htm>.

12. Федеральный закон от 21.07.1997 N 116-ФЗ (ред. от 08.08.2024) «О промышленной безопасности опасных производственных объектов» (с изм. и доп., вступ. в силу с 01.09.2025). Российская Федерация. – URL. <https://legalacts.ru/doc/federalnyi-zakon-ot-21071997-n-116-fz-o>.

13. Приказ Ростехнадзора от 15.12.2020 № 533 «Об утверждении федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств»» (зарегистрировано в Минюсте России 25.12.2020 № 61808). – URL. <https://normativ.kontur.ru/document?moduleId=1&documentId=390702>.

14. Громаков Е. И., Зебзеев А. Г., Курганов В. В., Суходоев М. С. Проектирование системы противоаварийной защиты : учебное пособие / Е. И. Громаков, А. Г. Зебзеев, В. В. Курганов, М. С. Суходоев ; Национальный исследовательский Томский политехнический университет Томск : Изд-во ТПУ, 2025.

15. Федоров Ю.Н. Основы построения АСУ ТП взрывоопасных производств. В 2 томах. Том 1. Методология / Ю.Н. Федоров. – Москва . СИНТЕГ, 2006. – 720 с.

16. Федоров Ю.Н. Основы построения АСУ ТП взрывоопасных производств. В 2 томах. Том 2. Проектирование / Ю.Н. Федоров. – Москва . СИНТЕГ, 2006. – 620 с.

17. Якубов Н. Программируемые логические контроллеры серии Regul R500S для построения систем ПАЗ / Н. Якубов // Современные средства автоматизации. – 2021. – № 1. – С. 48–55.

18. ГОСТ Р 27.012–2019 (МЭК 61882.2016). Надежность в технике. Анализ опасности и работоспособности (HAZOP). – URL. <https://docs.cntd.ru/document/1200170007>.

19. ГОСТ Р МЭК 62502–2014. Менеджмент риска. Анализ дерева событий. – URL. <https://docs.cntd.ru/document/1200114221>.

20. ГОСТ Р 27.302–2009. Надежность в технике. Анализ дерева неисправностей. – URL. <https://docs.cntd.ru/document/1200081358>.

21. ГОСТ Р 27.303–2021 (МЭК 60812.2018). Надежность в технике. Анализ видов и последствий отказов. – URL. <https://docs.cntd.ru/document/1200180916>.

22. Руководство по безопасности датчиков серии ONE для систем безопасности. https://www.ueonline.com/techinfo/russian/im_onest_sm_ru.pdf, вход свободный.

23. 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 – <https://docs.cntd.ru/document/1200167830>, вход свободный.

24. Safety Instrumented System Design Techniques and Design Verification, By Iwan van Beurden, CFSE William M. Goble, CFSE – International Society of Automation, 2018 – 430 с.

25. Safety Instrumented Systems Verification: Practical Probabilistic Calculation by William M. Goble, Harry Cheddie Softcover, Isa, 2005 – 260 с.

26. Rausand M. Reliability of Safety-Critical Systems. Theory and Applications / M. Rausand. – Willey, 2014. – 448 с.

27. Certified Functional Safety Expert / Professional (CFSE / CFSP) Study Guide - 8th Edition – Exida.com, LLC, 2018 – 181 с. <https://www.exida.com/books/certified-functional-safety-expert-professional-cfse-cfsp-study-guide>.

28. Промышленная безопасность, оценивание риска и системы аварийного останова: практическое руководство / Дейв Макдональд; [пер. с англ. Хвилевецкого Л. О., Серебрянского А. Я.]. — Москва: Группа ИДТ, 2007 – 416 с.

На правах рукописи

ЗАДАЧИ, ТЕСТЫ И УПРАЖНЕНИЯ ПО ПРОЕКТИРОВАНИЮ ПРИБОРНЫХ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ

Методические указания

Для студентов, обучающихся по направлению

150304/150404 «Автоматизация технологических процессов и производств»

Составитель

ГРОМАКОВ Евгений Иванович