РУКОВОДСТВО ПО БЕЗОПАСНОСТИ ПРОЦЕССОВ 1

PlantPAx
Process Automation System

Функциональная безопасность в непрерывных производствах

Принципы, стандарты и реализация

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Содержание

Предисловие

Стандарт IEC 61508 определяет способы управления безопасностью электрических, электронных и программируемых электронных систем на всех этапах их жизненного цикла от замысла до вывода из эксплуатации. В нем оговорены принципы разработки и последующей эксплуатации систем.

Основным принципом является необходимость планирования безопасности и определение целей безопасности с последующим внедрением жестких механизмов управления и контроля с целью их достижения. Благодаря этому стандарт в большей степени ориентирован на достижение цели, а не является предписанием, поэтому соблюдение требований стандарта не освобождает пользователя от ответственности в случае проблем безопасности.

Стандарт является как основной более специфических стандартов, так и самостоятельным документом. Однако последнее предпочтительно. Использование данного стандарта в качестве самостоятельного требует адаптации стандарта к конкретным условиям, глубокого понимания его сути руководством и тщательного планирования выполнения и использования.

Для большинства данный стандарт сложен для восприятия. Тем не менее, он уже успел доказать свое влияние и важность. Стандарт является основой современных стандартов и законодательных актов в сфере безопасности, поэтому крайне важно обеспечить понимание стандарта всеми ответственными лицами на всех этапах жизненного цикла системы безопасности.

Данный документ является вводным и содержит описание функциональной безопасности и указания по применению стандарта IEC 61511, в частности – стандарта IEC 61508 в перерабатывающей промышленности. Будучи основанным на стандарте IEC 61511, стандарт США ANSI/ISA-84.00.01 идентичен ему и, следовательно, на него также распространяются изложенные здесь указания.

Цель данного документа заключается в предоставлении сведений и указаний для лучшего понимания стандартов и изложенных в них требований. Документ написан простым языком и содержит примеры из реальных проектов, иллюстрирующие основные принципы и требования, а также возможные методы выполнения этих требований.

Отказ от ответственности

Хотя представленные методы были успешно использованы для демонстрации соблюдения стандартов в реальных проектах, следует учесть, что за соблюдение стандарта, методы, использованные для демонстрации соблюдения стандарта, а также свидетельства соблюдения стандартов ответственность несут соответствующие лица.

В квадратных скобках [ ] приводятся ссылки на другие разделы данного документа.

1. Введение в IEC 61511

1.1. Что такое IEC 61508 и IEC 61511?

Стандарт IEC 61508 является международным стандартом, изданным Международной электротехнической комиссией (IEC), и его основной целью являются аспекты применения электрических, электронных и программируемых электронных систем обеспечения безопасности.

Стандарт IEC 61508 [19.1] – это групповой стандарт, применяющийся ко всем электрическим, электронным и программируемым электронным системам обеспечения безопасности, независимо от их назначения и характера использования. Название стандарта:

> **IEC 61508:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (Функциональная безопасность электрических, электронных и программируемых электронных систем обеспечения безопасности).**

Основной принцип, лежащий в основе стандарта, – это допущение существования процесса, создающего угрозу безопасности или окружающей среде, который может себя проявить в случае неблагоприятного стечения обстоятельств. Следовательно, стандарт ориентирован на нарушения в процессах и отказы системы (в отличие от угрозы здоровью и безопасности человека) и позволяет осуществлять системное и основанное на рисках управление безопасностью процессов.

Стандарт предполагает существование функций безопасности, снижающих уровень риска. Функции безопасности в совокупности образуют Инструментальную систему безопасности (SIS), устройство и принцип работы которой должны быть основаны на оценке и понимании возможных рисков.

Второстепенной целью стандарта IEC 61508 является создание условий для разработки электрических, электронных и программируемых электронных систем обеспечения безопасности для отраслей, в которых соответствующие стандарты отсутствуют. Такие указания второго уровня в непрерывных производствах рассматриваются в международном стандарте IEC 61511 [19.2]. Название стандарта:

> **IEC 61511:2004 Functional Safety – Safety Instrumented Systems for the Process Industry Sector (Функциональная безопасность – инструментальные системы безопасности для непрерывных производств).**

Стандарт IEC 61511 является не стандартом проектирования, а стандартом управления безопасностью на протяжении всего жизненного цикла системы от замысла до вывода из эксплуатации. Основой такого подхода является весь жизненный цикл системы

безопасности, который включает действия, касающиеся спецификации, разработки, эксплуатации и технического обслуживания SIS.

1.2. Что такое функциональная безопасность?

В стандарте IEC 61511-1, 3.2.25 приводится следующее определение:

«Функциональная безопасность является частью общей безопасности, касающейся системы обеспечения безопасности процесса и основной системы управления непрерывным процессом (BPCS), зависящей от корректной работы SIS и прочих уровней защиты».

Иными словами, функциональная безопасность – это снижение уровня риска путем внедрения функций обеспечения безопасного управления процессом.

1.3. Международная электротехническая комиссия (IEC)

Международная электротехническая комиссия была основана в 1906 году британским ученым лордом Кельвином, который и стал первым ее президентом. Штаб-квартира находится в Женеве, Швейцария. Комиссия разрабатывает и издает Международные стандарты в области электротехнических технологий (электротехника, электроника и прочие смежные технологии).

Комиссия обеспечивает безопасность и экологичность технологий, способствует эффективному энергопотреблению и использованию возобновляемых источников энергии, управляет оценкой оборудования, систем и компонентов на предмет соответствия международным стандартам.

Стандарт и прочие публикации IEC защищены и подчиняются некоторым условиям авторского права, но могут быть приобретены или загружены на веб-сайте IEC [http://www.iec.ch].

1.4. Структура стандарта

Стандарт состоит из трех частей, как показано на рис. 1.

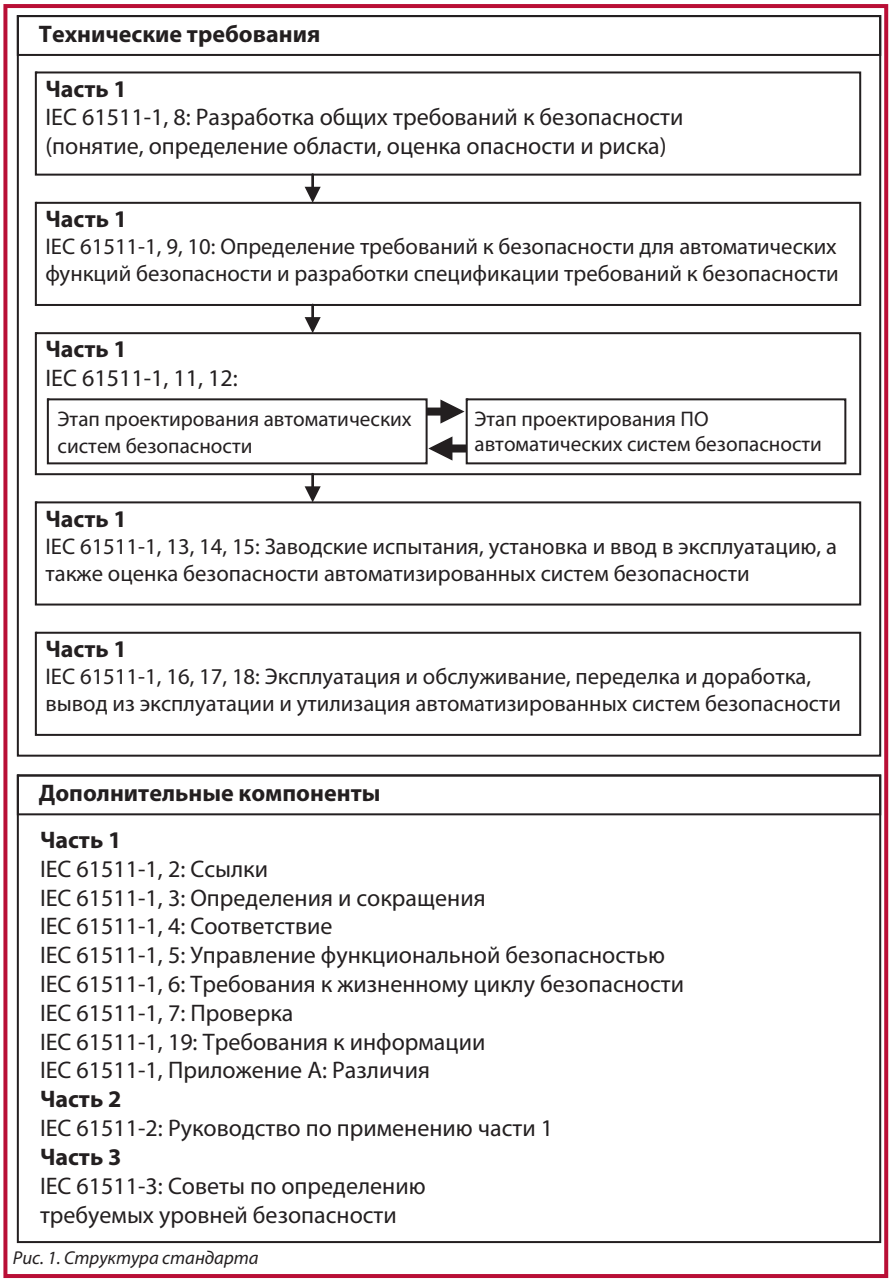


Рис. 1. Структура стандарта

В части 1 рассматриваются требования соответствия. Определяются принципы проектного планирования, управления, документации и требований компетентности, а также технические требования обеспечения безопасности на протяжении всего жизненного цикла системы безопасности.

В общем, часть 1 является «нормативной», поскольку определяет конкретные требования соответствия, представленные в виде согласованной структуры, позволяющей продемонстрировать соответствие по пунктам.

Часть 2 содержит указания по использованию части 1.

В части 3 представлены примеры оценки риска, приводящие к определению необходимых уровней полноты безопасности [4].

Части 2 и 3 – «информативные» и содержат указания и нормативные требования.

1.5. Соответствие требованиям стандарта IEC 61511

1.5.1. Требования Закона о гигиене и безопасности труда на рабочем месте 1974 года.

Закон о гигиене и безопасности труда на рабочем месте, 1974 г. (HASAW или HSW) – это основной закон Великобритании в области безопасности труда. Управление по вопросам охраны здоровья, техники безопасности и охраны труда (HSE) – орган, ответственный за обеспечение выполнения Закона и прочих нормативных актов и документов, относящихся к условиям труда.

Во многих странах мира действуют законодательство или директивы, аналогичные закону «Об охране здоровья и безопасности на рабочем месте» от 1974 года (Великобритания). Для удобства пользования в настоящем документе любая ссылка на закон «Об охране здоровья и безопасности на рабочем месте» включает в себя ссылку на соответствующие законы и директивы, действующие в Вашей стране.

Полный текст Закона можно получить в Управлении публичной информации (OPSI) или бесплатно загрузить с веб-сайта Управления. Пользователи правовой информации должны соблюдать предосторожность. Версии печатных или электронных документов могут быть устаревшими, поэтому пользователям рекомендуется обращаться к независимым консультантам или к службе интерактивных консультаций HSE Infoline [http://www.hse.gov.uk/contact/index.htm].

Если кратко, то в Законе о гигиене и безопасности труда на рабочем месте закреплено обязательство каждого работодателя обеспечить в разумных пределах каждого работника безопасным рабочим местом и создать все необходимые условия для работы. Это включает предоставление и поддержание в надлежащем состоянии (в

разумных пределах) предприятия и систем, в целях обеспечения безопасности работы без угрозы здоровью работников.

Кроме того, каждый работодатель обязан, прилагая разумные усилия, вести свои дела таким образом, чтобы лица, не нанятые им, не находились под угрозой здоровью и безопасности.

1.5.2. Требования соответствия

Стандарт IEC 61511 оговаривает, что для подтверждения соответствия необходимо продемонстрировать, что требования стандарта выполняются в должной степени по каждому пункту и подпункту и достигаются все поставленные цели.

На практике, как правило, сложно продемонстрировать полное соответствие всем пунктам и подпунктам стандарта, поэтому требуется разумно оценивать усилия, необходимые для выполнения некоторых требований стандарта. Обычно степень соответствия зависит от ряда факторов, таких как:

- природа опасности;
- тяжесть последствий;
- необходимое снижение уровня риска;
- применимый этап жизненного цикла;
- применяемая технология;
- новизна конструкции.

Иными словами, решения следует принимать на основании рисков. Если опыта недостаточно, в некоторых случаях достоверность может быть подтверждена путем привлечения внешних источников информации.

1.5.3. Последствия невыполнения требований

Однако стандарт не является законом, поэтому, соблюдая его или нет, вы должны осознавать последствия несоблюдения. Как работодатель, ответственное лицо или ответственный за риск, вы обязаны в соответствии с Законом о гигиене и безопасности труда на рабочем месте управлять риском на рабочем месте.

Стандарт предоставляет системный подход к управлению всеми действиями по обеспечению безопасности в рамках жизненного цикла систем, используемых для реализации функций безопасности, поэтому является хорошим источником информации и методик. В случае неблагоприятного стечения обстоятельств, приведшего к травме или болезни какого-либо лица, когда при управлении данным видом риска не использовалась вся разумно доступная информация, существует вероятность преследования по Закону о гигиене и безопасности труда на рабочем месте.

Собираемая информация и проводимые анализы при обеспечении выполнения требований стандарта IEC 61511 становятся эффективной защитой в суде в случае инцидента.

1.5.4. Требования соответствия для нового предприятия

Разумеется, что, если вы принимаете участие в каком-либо этапе жизненного цикла системы безопасности, разумно предполагать, что вы будете использовать всю доступную информацию для управления риском и удержания его на допустимом уровне. Можно оспорить утверждение, что вся доступная информация – это стандарт IEC 61511, и, таким образом, если что-то идет не так, невыполнение требований стандарта будет рассматриваться как халатность.

1.5.5. Требования соответствия для существующего предприятия

Многие предприятия проектировались и строились до того, как был разработан и официально опубликован стандарт IEC 61511. Однако в такой ситуации ваша ответственность не изменяется, и, если вы принимаете участие в каком-либо этапе жизненного цикла системы безопасности старого предприятия, например, в процессах эксплуатации, технического обслуживания и т. д., ваши обязательства по Закону о гигиене и безопасности труда на рабочем месте сохраняются, и возникший риск требует должного внимания. Таким образом, стандарт также распространяется и на старые предприятия.

Стандарт ANSI/ISA-84, в частности, касается старых систем, определяя, что для существующих автоматизированных систем безопасности, спроектированных и построенных в соответствии с нормами, стандартами и методами, применявшимися до издания стандарта, владелец/оператор должен определить, что оборудование спроектировано, обслуживается, осматривается, подвергается испытаниям и эксплуатируется безопасным образом. На самом деле, вы должны убедиться, что существующие системы безопасны и используют лучшие из доступных методов.

В реальности вы можете ощущать потребность в возврате к предыдущим этапам жизненного цикла системы безопасности существующего предприятия и повторном проведении анализа эксплуатационных характеристик и опасных факторов (HAZOP) с начального уровня. Выполнив процедуру до конца, вы можете выявить риски, не охваченные имеющейся системой функциональной безопасности, и ваша обязанность – обеспечить должное управление такими рисками.

По всей вероятности, нерентабельно создавать новые функции (SIF) для 20-летнего предприятия. Однако, если предприятие безопасно работало в течение достаточно длительного периода времени, выявленные факторы риска и их вероятность с учетом существующих мер безопасности могут быть уже достаточными.

Вашей обязанностью в таком случае будет тщательное документирование процесса: это делается для уверенности в том, что все опасности выявлены, факторы риска учтены, а эффективность существующих защитных функций и мер предосторожности оценена. В этой ситуации в отличие от нового производства у вас есть преимущество, которое заключается в том, что вы можете оглянуться и более точно количественно оценить периодичность угроз, используя исторические записи. Анализ позволит продемонстрировать, что выявленные факторы риска находятся на приемлемом уровне.

В худшем случае, если сложится ситуация, в которой имеет место непредусмотренная опасность или требуются дополнительные меры для снижения риска, об этом необходимо знать и предпринимать соответствующие действия.

1.5.6. Причины соблюдения требований стандарта IEC 61511

Наряду с подразумеваемыми обязательствами по Закону о гигиене и безопасности труда на рабочем месте могут быть и другие причины соблюдения требований стандарта:

- договорные обязательства;
- оптимизация архитектуры проекта;
- возможные рыночные преимущества.

Это позволяет утверждать, что первое обязательство бизнеса – это выживание, при этом главной целью является не получение максимальной прибыли, а избежание убытков. В связи с этим необходимо задать себе вопрос, что лучше: учиться на своих или на чужих ошибках.

1.6. Применение стандарта IEC 61511

Понятие «функциональная безопасность» применяется только к целостным функциям, включающим датчик, компьютер или программируемый логический контроллер и исполнительный механизм. Это понятие бессмысленно применять к изделиям: элементам оборудования, таким как датчики или компьютеры.

Таким образом, когда производитель утверждает, что изделие отвечает уровню защиты SIL2 или SIL3, то это означает, что такое изделие, будь то датчик давления или компьютер, пригодно для использования в системе, реализующей уровень защиты SIL2 или SIL3.

Производитель должен количественно оценить заявленный уровень, указав ограничения в применении, например, требования к отказоустойчивости [13.3.1] или проверочным испытаниям [12.8], чтобы гарантировать заявленный уровень SIL.

Заявления производителя могут быть подкреплены сертификатами SIL, выданными независимым экспертом, но это не предполагает, что стандартная функция безопасности будет соответствовать уровню SIL. Сертификат SIL не заменяет демонстрацию соблюдения требований стандарта, и ответственное лицо не может использовать свои заявления в отношении изделия в качестве аргумента при отказе от ответственности по Закону о гигиене и безопасности труда на рабочем месте.

1.7. Должен ли я выполнять требования стандарта?

1.7.1. Новое предприятие

Как было сказано выше, существуют подразумеваемые обязательства соблюдения требований стандарта. Это означает, что стандарт не является законом, а закон не требует от ответственного лица или ответственного за риск управлять риском с целью смягчения его до приемлемого уровня. Стандарт предоставляет системный подход к достижению этой цели, поэтому в случае неблагоприятного стечения обстоятельств, приведшего к травме, неиспользование всей разумно доступной информации может быть свидетельством халатности и подлежит преследованию по закону.

1.7.2. Существующее предприятие

Закон о гигиене и безопасности труда на рабочем месте также применим в отношении существующего предприятия, поэтому факторы риска равным образом подлежат идентификации и должному управлению [1.5.5]. Стандарт IEC 61511 также предоставляет соответствующую модель управления рисками для старых предприятий, спроектированных и построенных до разработки и публикации стандарта.

2. Обзор жизненного цикла системы безопасности

2.1. Жизненный цикл системы безопасности

Жизненный цикл системы безопасности включает все необходимые действия, включая описание технических характеристик, разработку, эксплуатацию и техническое обслуживание автоматизированной системы безопасности SIS. В зависимости от объема ваших полномочий вы можете участвовать только в некоторых этапах, например, в эксплуатации и техническом обслуживании; однако вы все равно должны иметь представление обо всем жизненном цикле.

Жизненный цикл системы безопасности схематично представлен на рис. 2.

Рис. 2. Жизненный цикл системы безопасности IEC 61511

2.2. Фазы жизненного цикла

На этапе 1 устанавливаются физические, социальные и политические рамки и оговариваются значимые для безопасности повреждения с точки зрения опасности и просчитывания риска. Это важно для понимания опасности и риска, свойственных процессу.

После определения необходимой степени снижения риска на этапе 2 определяются способы достижения поставленной цели и формулируются общие требования к безопасности (этап 3).

На этапе 4 на основании требований к безопасности разрабатываются функции обеспечения безопасности. На этом этапе выполняется оптимизация функций, разделение и прочие задачи проектирования, такие как определение принципов испытания. Планирование этих действий осуществляется на этапе 11.

Этапы с 5 по 10 показывают, что стандарт не ограничивается разработкой системы, а освещает также вопросы управления функциональной безопасностью на протяжении всего жизненного цикла системы.

Многие из требований стандарта по природе своей технические, но в подходе также не меньшее внимание уделяется важности управления, включающего планирование, документирование, эксплуатацию, обслуживание и модификацию, и эти действия должны быть включены в каждый этап. Документирование, менеджмент и оценка выполняются параллельно и также касаются всех этапов, представленных на рис. 2.

2.3. Требования соответствия

Поскольку стандарт не является предписывающим документом, его требования выполняются опосредованно. Ваши вложения в доказательство соблюдения требований – это вопросы личного выбора, но вы должны быть сами достаточно убеждены, что все выполнили правильно. Именно такой подход, заключающийся в выполнении требований по пунктам, рекомендуется для достижения уверенности в том, что выполнено всё, что необходимо. Иными словами, применяется прямолинейный подход.

Выполнение требований стандарта предполагает демонстрацию с помощью соответствующих свидетельств наличия внедренного системного подхода к управлению рисками и применения его на соответствующих этапах жизненного цикла изделия. Этот системный подход, который предлагается стандартом, основан на концепции жизненного цикла системы безопасности.

Соблюдение стандарта требует понимания концепции жизненного цикла и выработки и документирования соответствующего плана действий. Прослеживание жизненного

цикла – это не формальная бумажная работа, которая сводится к написанию отчетов и сдаче их в архив. Для соблюдения требований необходимо эффективно выполнять предусмотренные действия, получая информацию, которая необходима для реализации последующих этапов плана.

Как правило, деятельность осуществляется в широком контексте с учетом всех этапов жизненного цикла. Например, для оператора внесение изменений в этапы эксплуатации и технического обслуживания может потребовать также проведения оценки и принятия определенных решений на более ранних этапах, например, может потребоваться проведение HAZOP с последующей переоценкой рисков в жизненном цикле.

2.4. Фазы 1 и 2 жизненного цикла системы безопасности

Каждый этап жизненного цикла описывает действие, а каждое действие требует определенной информации на входе. Каждый этап включает действие, для которого должны быть предусмотрены документированные процедуры и которое производит данные для последующих этапов.

На рис. 3 представлены действия и требования к информации для этапа 1 (оценка опасности и риска) и этапа 2 (назначение требований к безопасности). На рисунке представлены необходимые входные данные (I/P) для действия и данные, производимые действием для последующих этапов.

Следует заметить, что, хотя стандарт и содержит описание этапов жизненного цикла и требований к информации для каждого этапа, на практике при необходимости могут быть совмещены некоторые этапы и связанные с ними документы. Важна ясность и простота, а выполнение действий и предоставление информации должны происходить как можно более эффективным способом.

Результат этапа 3 – это, как правило, HAZOP и анализ риска, в ходе которого определяются требования к функциям безопасности и цели снижения риска.

Этап 4 – назначение функций безопасности на основании требований к безопасности, определенных на предыдущем этапе. Назначение требований к безопасности – это процесс, предполагающий рассмотрение всех требований к безопасности и определение соответствующих автоматизированных функций безопасности. Это повторяющийся процесс, в котором учитываются меры по снижению уровня рисков, предусмотренные для удовлетворения требованиям в отношении полноты системы безопасности.

Важно, чтобы к началу этапа назначения функций безопасности были уже спланированы последующие этапы, такие как установка, пуск в эксплуатацию, проверка и техническое обслуживание (см. рис. 5).

Рис. 3. Фазы 1 и 2 жизненного цикла системы безопасности

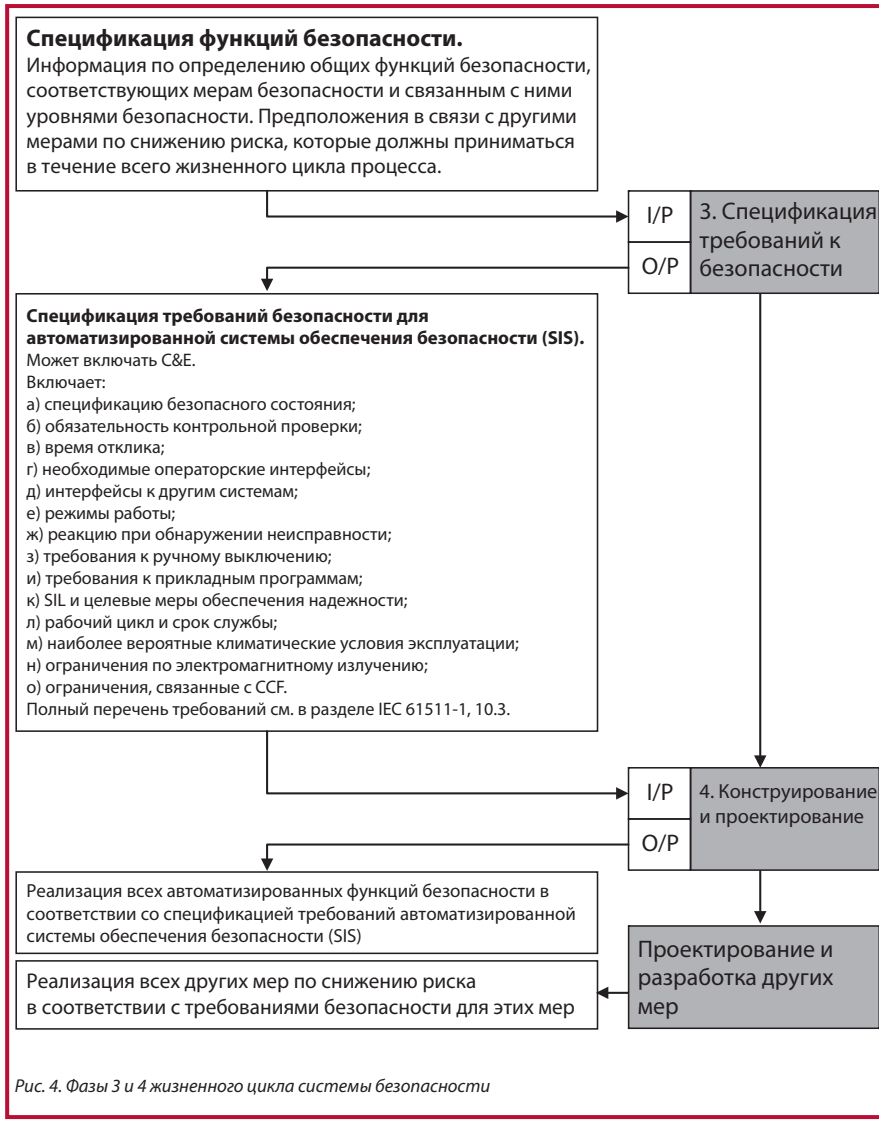


Рис. 4. Фазы 3 и 4 жизненного цикла системы безопасности

2.5. Фазы 3 и 4 жизненного цикла системы безопасности

Этап 3 заключается в разработке спецификации требований к безопасности (SRS), которая позволит приступить к проектированию и разработке системы безопасности на этапе 4 (см. рис. 4).

В организации может быть создан контрольный список элементов, которые необходимо включить в спецификацию проекта. Это позволит создать наиболее полную спецификацию и предотвратить отказы из-за ошибок в спецификации.

Этап 4 может быть в полной мере освещен в спецификации функционального проекта (FDS) или другом подобном документе, описывающем обстановку, процессы, окружающие условия, аспекты эксплуатации и объемы работ для последующих этапов.

2.6. Этапы 5 и 6 жизненного цикла системы безопасности

Этапы 5 и 6 заключаются в определении требований к автоматизированной системе безопасности, ее установке, пуску в эксплуатацию, проверке, эксплуатации и техническому обслуживанию (см. рис. 5).

2.7. Фазы 7 и 8 жизненного цикла системы безопасности

Входные данные, результаты и действия, связанные с этапом 7 (модификация), являются теми же, что и в этапе 8 (вывод из эксплуатации). По сути, вывод из эксплуатации – это модификация, происходящая в конце жизненного цикла и предполагающая те же инициирующие действия и способы управления (см. рис. 6).

План установки и ввода в эксплуатацию для автоматизированной системы обеспечения безопасности.
Обеспечивает планирование для установки и ввода в эксплуатацию используемых действий, процедур, методик и мер; а также для ответственного персонала и отделов.

План проверки общей безопасности автоматизированной системы обеспечения безопасности (SIS).
Обеспечивает планирование проверки безопасности автоматизированной системы обеспечения безопасности (SIS) по SRS и другой справочной информации, например по схемам причин и следствий. Проверка будет охватывать все соответствующие режимы работы (запуск, останов, обслуживание, нештатные условия и т. д.), применяемые процедуры, методики и меры, расписание, ответственный персонал и отделы. Кроме того, в нее войдет планирование проверки прикладного ПО безопасности.

Реализация всех автоматизированных функций безопасности в соответствии со спецификацией требований автоматизированной системы обеспечения безопасности

I/P
O/P
5. Установка, ввод в эксплуатацию и проверка

Полностью установленная и введенная в эксплуатацию автоматизированная система безопасности (SIS):
Установка документов; ссылки на отчеты о неполадках; устранение неполадок.

Подтверждение соответствия автоматизированной системы обеспечения безопасности общим требованиям к безопасности согласно требованиям к автоматизированным функциям безопасности и годности к эксплуатации, учитывая определение требований к безопасности. Требования к документации включают в себя: проверочные действия в хронологической последовательности; версию требований к безопасности, проверяемую функцию безопасности, инструмент и оборудование; результаты; проверяемый элемент, применяемую процедуру и условия проверки; неполадки; принятые в результате решения.

План эксплуатации и обслуживания автоматизированной системы обеспечения безопасности
Обеспечивает планирование действий при штатной и нештатной эксплуатации; проверочные испытания, действия по обслуживанию, применяемые процедуры, методики и меры, график, ответственный персонал и отделы, метод проверки по процедурам эксплуатации и обслуживания.

I/P
O/P
6. Эксплуатация, обслуживание и ремонт

Поддержание требуемого уровня функциональной безопасности для автоматизированной системы обеспечения безопасности. Необходимо выполнить следующие действия: План эксплуатации и обслуживания; процедуры эксплуатации, обслуживания и ремонта; реализация процедур; следование графику обслуживания; ведение документации; проведение регулярного аудита функциональной безопасности; изменения в документации; хронологическое документирование эксплуатации и обслуживания автоматизированной системы обеспечения безопасности.

Рис. 5. Фазы 5 и 6 жизненного цикла системы безопасности

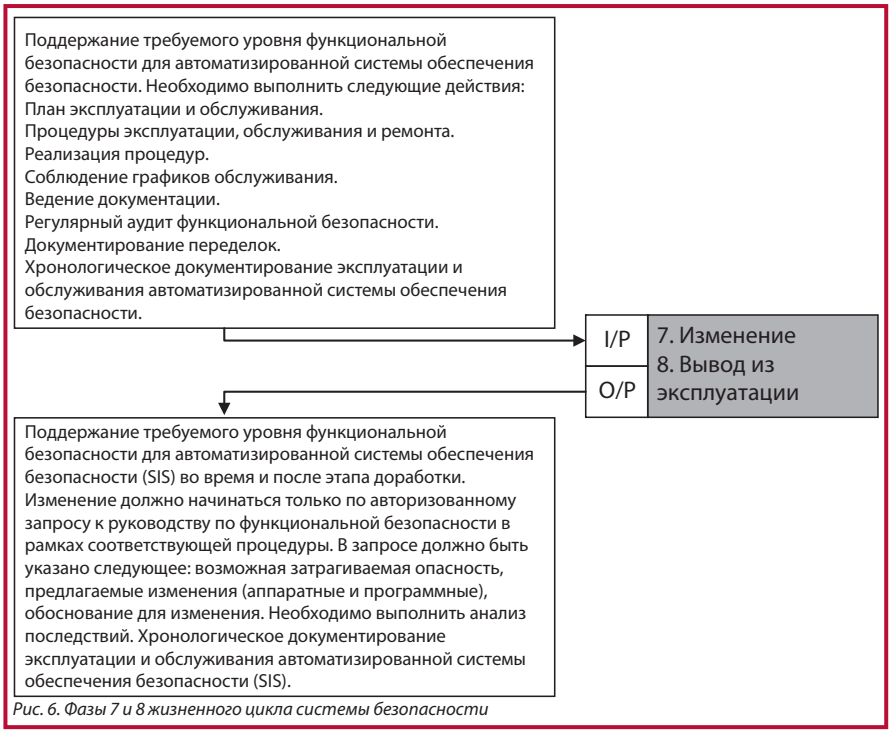


Рис. 6. Фазы 7 и 8 жизненного цикла системы безопасности

3. Опасности и идентификация опасностей

3.1. Фазы жизненного цикла

На рис. 7 представлен рассматриваемый этап жизненного цикла.

Рис. 7. Фаза жизненного цикла 1

Цель этого этапа, как указано в стандарте IEC 61511-1, 8.1, заключается в определении:

- опасностей и опасных событий в процессах и связанном с ними оборудовании, последовательностей событий, приводящих к возникновению опасности и связанных с процессом рисков [3.2 – 3.7];
- требований в отношении снижения уровня риска [5 и 6];
- функций безопасности, необходимых для снижения риска до требуемого уровня [7 и 8].

3.2. Факторы опасности

Понятие «опасность» может быть неоднозначным. Обычно в словарях отсутствует четкое толкование термина или приводится синоним «риск». Именно по этой причине многие путают эти два термина и используют их поочередно для обозначения одного и того же понятия.

В контексте функциональной безопасности опасностями считаются события, способные причинить ущерб, например, травму, вред окружающей среде или убыток в бизнесе.

Примерами опасности в доме являются:

- разбитое стекло как причина порезов;
- лужа воды как причина падения;
- чрезмерное количество вилок в розетках как причина пожара вследствие перегрузки сети.

Примерами опасности на рабочем месте являются:

- шум как причина ухудшения слуха;
- асбестовая пыль как причина рака.

Примерами опасности в непрерывных производствах являются:

- уровень жидкости в емкости: высокий уровень может привести к переливу и попаданию жидкости в газовые потоки, разливу опасных химических веществ или горючих жидкостей; низкий уровень опасен работой насосов всухую и попаданием газа в следующие по ходу технологического процесса емкости;
- давление жидкости в емкости: высокое давление может привести к разгерметизации, утечке и повреждению емкости.

Первым этапом оценки риска является выявление опасности. Существует множество способов определения опасности, но наибольшее распространение получил метод анализа эксплуатационных характеристик и опасных факторов (HAZOP).

3.3. Применение метода HAZOP в промышленности

Методы анализа опасностей и пригодности к эксплуатации были разработаны в Великобритании организацией ICI после катастрофы во Фликсборо в 1974 году, после чего получил широкое распространение в непрерывных производствах.

В субботу, 1 июня 1974 года, предприятие Nypro (Великобритания) близ Фликсборо получило серьезные повреждения в результате взрыва, при котором 28 человек погибли и еще 36 получили травмы. Было доказано, что число жертв могло бы быть

гораздо выше, если бы трагедия произошла в рабочий день, когда офисное знание полно людей. Сообщалось о том, что пострадали также 53 случайных человека за пределами территории, и был причинен ущерб собственности на прилегающих территориях.

18 человек в аппаратной погибли в результате разбития окон и обрушения кровли. Спастись не удалось никому. Предприятие горело несколько дней, что затруднило работу спасателей в последующие десять дней.

Появившись в химической промышленности и получив развитие в ходе обсуждения с персоналом, метод HAZOP был внедрен в нефтяной промышленности, где потенциальная вероятность катастроф находится примерно на том же уровне. Позднее метод стал использоваться в пищевой промышленности и водоснабжении и водоотведении, где потенциал опасности намного выше, но больше связан с загрязнением, а не со взрывом или выбросами химических веществ.

3.4. Смысл использования метода HAZOP

При том, что проект предприятия основан на нормативах и стандартах, процесс HAZOP дополняет стандарты и нормативы, позволяя выявить потенциальные отклонения вследствие, например, нарушения процессов, отказа оборудования или ошибок оператора.

Кроме того, жесткие графики реализации проектов могут приводить к ошибкам и недосмотру, а метод HAZOP позволяет вносить поправки до того, как цена ошибки станет слишком высокой. Благодаря простоте для понимания и возможности адаптации к условиям любого процесса и бизнеса метод HAZOP получил наибольшее распространение при определении факторов опасности.

3.5. Отклонение от проектного замысла

Все процессы, оборудование и промышленные объекты создаются по определенному замыслу. Замысел может предполагать определенную производительность, выраженную в годовом объеме производства конкретного химического вещества или в определенном количестве экземпляров продукции.

Однако второстепенным замыслом может быть безопасная и эффективная эксплуатация процессов, для чего требуется эффективное функционирование всего оборудования. Этот аспект можно рассматривать как проектный замысел конкретного компонента оборудования.

Например, в требования к производительности предприятия включена установка для охлаждения воды с контуром охлаждения, насосом и теплообменником, как показано на рис. 8.

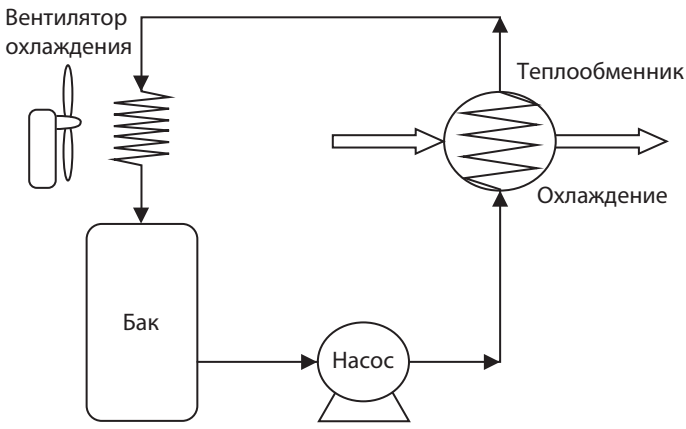


Рис. 8. Проектный замысел

Проектный замысел этого небольшого участка предприятия заключается в обеспечении непрерывной циркуляции охлаждающей воды с температурой x °C и расходом xxx литров в час. Анализ эксплуатационных характеристик и опасных факторов, как правило, ориентируется на проектный замысел низшего уровня. В таком контексте проще понять термин «отклонение». Отклонение или отход от замысла в применении к нашей установке охлаждения сводится к снижению расхода или увеличению температуры воды.

Обратите внимание на различие между отклонением и его причиной. В описанном случае отказ насоса будет причиной, но не отклонением.

Увеличение температуры воды является опасностью, так как влечет за собой ущерб, травмирование персонала и вред окружающей среде или убытки для бизнеса.

3.6. Методика HAZOP

Методы HAZOP применяются для обнаружения потенциальных опасностей и проблем работоспособности из-за отклонений от проектного замысла нового или старого предприятия и применяются периодически на протяжении всего жизненного цикла предприятия. Конечно, первоначальный анализ HAZOP следует проводить на ранних этапах проектирования. Процесс подлежит регулярному пересмотру по мере развития, в случае предложений внесения серьезных изменений, а также в конце разработки, чтобы убедиться в отсутствии остаточного риска до этапа постройки.

Анализ эксплуатационных характеристик и опасных факторов (HAZOP) выполняется совместно при участии представителей всех заинтересованных сторон, обладающих

знаниями и опытом эксплуатации и технического обслуживания. Совещание происходит в формате «мозгового штурма», в процессе которого формулируются и оцениваются все возможные опасности. Все предполагаемые опасности, их причины и последствия тщательно фиксируются в протоколе.

3.6.1. Рабочая группа HAZOP

Очень важно, чтобы в рабочую группу HAZOP входили лица, обладающие достаточными знаниями и опытом в рассматриваемых вопросах. Как правило, рабочая группа имеет следующий состав:

Название	**Роль**
Председатель	Объясняет процесс HAZOP, направляет обсуждение и продвигает HAZOP. Специалист, имеющий опыт в HAZOP, но непосредственно не вовлеченный в разработку, для обеспечения аккуратного следования методу.
Секретарь	Записывает обсуждение на совещании по HAZOP и составляет наглядный протокол дискуссии. Записывает рекомендации или действия.
Инженер-технолог	Как правило, инженер, ответственный за принципиальную схему технологических процессов и разработку схемы трубной обвязки и контрольно-измерительных приборов (Piping and Instrumentation Diagrams, P&IDs).
Пользователь/ оператор	Вносит рекомендации по использованию и работоспособности процесса, по воздействию отклонений.
Специалист по КИП	Специалист с соответствующими техническими знаниями по контрольно-измерительным приборам.
Специалист техобслуживания	Специалист, занятый в техническом обслуживании процесса.
Представитель проектной группы	Вносит рекомендации по подробностям проекта или дает необходимую информацию.

3.6.2. Информация, используемая в анализе HAZOP

Члены рабочей группы HAZOP должны изучить следующее:

- схемы трубопроводов и КИПиА предприятия;
- описания процессов и принципиальные схемы;
- существующие процедуры эксплуатации и технического обслуживания;
- причинно-следственные диаграммы;
- технологические схемы предприятия.

3.6.3. Процедура HAZOP

Процедура HAZOP включает полное описание процесса и систематическую оценку каждого этапа с целью определения, как отклонения от проектного замысла могут сказаться на безопасности и эффективности работы предприятия.

В процессе структурированного анализа члены группы дают волю фантазии, стремясь представить и оценить все возможные опасности.

На самом деле, многие опасности очевидны, например, рост температуры, однако, сила методики в том, что она позволяет обнаружить неочевидные опасности, какими бы маловероятными они ни казались при первом рассмотрении.

3.6.4. Управляющие слова

В процессе HAZOP для привлечения внимания к отклонениям от проектного замысла, возможным причинам и последствиям используются управляющие слова. Управляющие слова делятся на две подгруппы:

- главные управляющие слова, которые обращают внимание на конкретные аспекты проектного замысла или связанные с ним условия процесса, параметры, например, расход, температуру, давление, уровень и пр.;
- второстепенные управляющие слова, сочетаясь с главными, описывают возможные отклонения, такие как рост температуры, снижение уровня, отсутствие давления, обратный поток и пр.

Успех методики зависит от эффективного применения управляющих слов, поэтому их смысл должен быть понятен всем членам рабочей группы.

Следует отметить, что управляющие слова используются просто для стимулирования воображения при формулировании вариантов. Не все управляющие слова имеют смысл, и не все опасности вероятны. В таких случаях рекомендуется при выявлении бессмысленных и невероятных событий фиксировать и продолжать работу, не теряя времени.

3.6.5. Способы работы

Поскольку это анализ эксплуатационных характеристик и опасных факторов, важно рассматривать не только варианты нормальной работы, но и нештатные режимы, такие как пуск, останов, наполнение, опорожнение, перелив, контрольное испытание.

Для этого необходимо рассмотреть каждый режим работы, упомянутый в объеме исследований, в отдельности, соблюдая методику HAZOP. В качестве альтернативы,

применительно к относительно простым системам, возможно включение в таблицу дополнительного столбца для указания режима. Это позволит охватить одним анализом HAZOP сразу все режимы работы.

3.6.6. Запись анализа HAZOP

Существуют специальные программы для выполнения анализа HAZOP. Если их нет, то можно создать простую электронную таблицу для регистрации и оценки всех данных. Электронная таблица позволит быстро отсортировать данные, визуализировать их, проследить взаимосвязи между данными и другими анализами.

Рекомендуется регистрировать все события и все рассматриваемые сочетания управляющих слов. По возможности следует делать пометки: «Нет вероятной причины», «Без последствий», «Без опасности». Это считается «полной регистрацией», которая перерастает в отчет о результатах анализа HAZOP, который подтверждает полноту проведенного исследования. Этот отчет содержит бесценные материалы, необходимые для оценки безопасности и пригодности к эксплуатации при последующих изменениях.

Кроме описанных выше второстепенных управляющих слов, также используются слова «Все» и «Напоминание». Например, некоторые сочетания основных управляющих слов могут быть определены как имеющие вероятные причины: «расход/нет», «поток/обратный». Другие сочетания («расход/меньше», «расход/больше», «расход/другой»), где нельзя определить вероятные причины, возможно использование сочетания «расход/остаток».

3.6.7. Идентификация опасности – заголовки таблицы анализа HAZOP

В следующей таблице представлен пример листа HAZOP для декомпрессионной камеры. Обратите отметить, что пример исключительно иллюстративный и не отражает картину реальной системы.

Ссылки

Всегда имеет смысл включать в таблицу столбец для ссылок, чтобы связывать строки с другими данными и анализами для обеспечения прослеживаемости к последующим анализам, например, LOPA [8].

Управляющие слова

Должны использоваться главные и второстепенные управляющие слова. Списки управляющих слов для конкретных отраслей и видов бизнеса можно найти в Интернете.

Отклонение

Отклонение – это отход от проектного замысла, подсказанный сочетанием главных и вспомогательных управляющих слов и представляющий определенную опасность.

Причина

Потенциальные причины, которые могут привести к отклонению. Важно включить в таблицу конкретные сведения о причине. Например, если нас волнует увеличение концентрации кислорода, вызванное отказом датчика O_2, то мы должны учесть, что характеров отказа может быть множество, но лишь ложная регистрация снижения концентрации O_2 будет причиной увеличения концентрации.

Последствия

Последствия, возникающие в результате отклонения и действия причины. Следует всегда подробно описывать последствия. Не полагайтесь на то, что читатель со временем поймет суть опасности или характер последствий.

Фиксируя последствия, важно помнить о том, что результаты анализа HAZOP могут быть использованы при определении риска, поэтому крайне важно подробно описывать все опасности и их возможные последствия. Например, последствия можно описать так:

«Вероятность избыточного давления, способного привести к разрыву газоотводящего трубопровода с выбросом содержимого в окружающую среду. Большой объем выброшенного газа в зоне горячей выхлопной трубы может воспламениться или взорваться и привести к гибели двух человек из обслуживающего персонала. Повреждение компрессора стоимостью 2 млн фунтов стерлингов и остановка производства на срок до года».

При оценке последствий важно учитывать системы защиты и контрольно-измерительные приборы, имеющиеся в конструкции.

Меры безопасности

В этом столбце необходимо указать любые имеющиеся средства защиты, которые предотвращают причину либо предохраняют от последствий. При перечислении мер безопасности по возможности следует ограничиться оборудованием, приняв в расчет процедурные аспекты, такие как регулярный осмотр производственных мощностей (если вы уверены в том, что осмотр будет проводиться И это может предотвратить опасность).

3.7. Пример анализа HAZOP

3.7.1. Сосуд сепаратора

В следующем примере представлена упрощенная схема процесса сепарации. В сосуд поступает жидкость, нагретая газовой горелкой. Пары отделяются от жидкости и отводятся из сосуда. По завершении реакции оставшаяся концентрированная жидкость отсасывается из нижней части сосуда (см. рис. 9).

Сосуд оборудован распределенной системой управления, которая контролирует уровень жидкости в сосуде, давление газа и температуру.

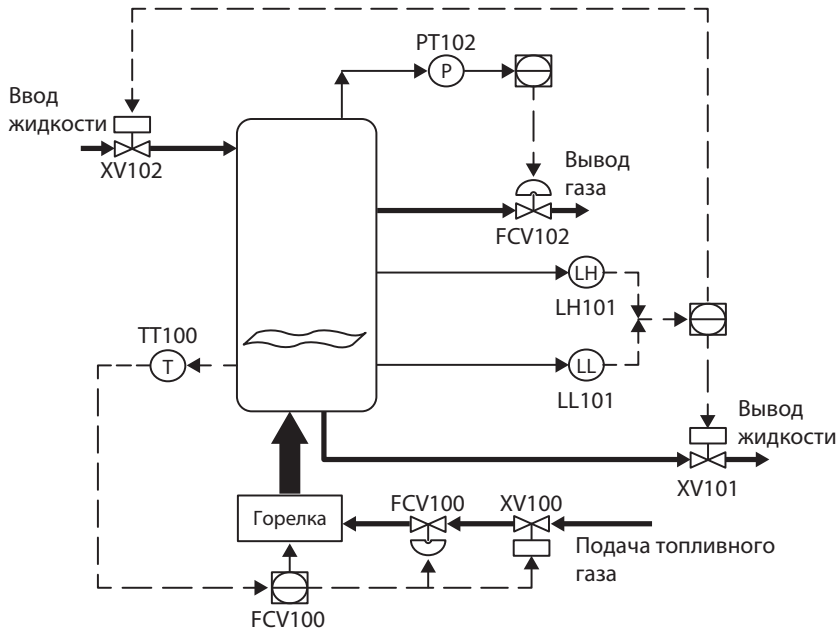


Рис. 9. Сосуд сепаратора

Пример анализа HAZOP системы сепаратора представлен на следующей диаграмме.

№	Основное справочное слово	Дополнительное справочное слово	Отклонение	Опасность	Последствия
01.01	Расход	Больше	Большой поток рабочей жидкости в резервуар.	Большой поток в резервуар может приводить к повышению уровня и попаданию жидкости в выпускаемый газ.	Повреждение оборудования ниже по потоку, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев.
01.02			Высокий уровень рабочей жидкости на выходе жидкости из резервуара.	Высокий уровень на выходе из резервуара может приводить к снижению уровня и попаданию газа в вывод жидкости.	Повреждение оборудования ниже по потоку, требующее чистки резервуара примерной стоимостью 2 млн фунтов стерлингов, и остановка производственного процесса на 6 недель.
01.03			Высокий расход газа на выходе газа из резервуара.	Нет вероятной опасности.	Нет.
01.04		Меньше	Недостаточный приток рабочей жидкости в резервуар.	Низкий уровень на входе в резервуар может приводить к снижению уровня и попаданию газа в вывод жидкости.	Повреждение оборудования ниже по потоку, требующее чистки резервуара примерной стоимостью 2 млн фунтов стерлингов, и остановка производственного процесса на 6 недель.
01.05			Низкий уровень рабочей жидкости на выходе жидкости из резервуара.	Низкий расход на выходе из резервуара может приводить к повышению уровня и попаданию жидкости в выпускаемый газ.	Повреждение оборудования ниже по потоку, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев.
01.06			Низкий расход газа на выходе газа из резервуара.	Нет вероятной опасности.	Нет.
01.07		Переворот	Нет вероятности.	Нет вероятной опасности.	Нет.
01.08		Кроме того	Нет вероятности.	Нет вероятной опасности.	Нет.
01.09		Другое	Нет вероятности.	Нет вероятной опасности.	Нет.
01.10	Давление	Больше	Высокое давление в резервуаре.	Прорыв резервуара и утечка газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух ремонтников. Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 1 год. Незначительный выброс в окружающую среду.
01.11		Меньше	Низкое давление в резервуаре.	Прорыв резервуара и утечка газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух ремонтников. Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 1 год. Незначительный выброс в окружающую среду.
01.12		Переворот	Нет вероятности.	Нет вероятной опасности.	Нет.
01.13		Кроме того	Нет вероятности.	Нет вероятной опасности.	Нет.
01.14		Другое	Нет вероятности.	Нет вероятной опасности.	Нет.
01.15	Температура	Больше	Высокая температура в резервуаре.	Высокая температура приводит к повышению давления, прорыву резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух ремонтников. Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 1 год. Незначительный выброс в окружающую среду.
01.16		Меньше	Низкая температура в резервуаре.	Возможно замерзание (загустение) жидкости, прорыв резервуара и нарушение герметичности.	Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев. Выброс в окружающую среду, требующий уведомления.
01.17		Переворот	Нет вероятности.	Нет вероятной опасности.	Нет.
01.18		Кроме того	Нет вероятности.	Нет вероятной опасности.	Нет.
01.19		Другое	Нет вероятности.	Нет вероятной опасности	Нет.
01.20	Уровень	Больше	Высокий уровень в резервуаре.	Высокий уровень в резервуаре может приводить к попаданию жидкости в выпускаемый газ.	Повреждение оборудования ниже по потоку, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев.
01.21		Меньше	Низкий уровень в резервуаре.	Низкий уровень в резервуаре может приводить к попаданию газа в выпускаемую жидкость.	Повреждение оборудования ниже по потоку, требующее чистки резервуара примерной стоимостью 2 млн фунтов стерлингов, и остановка производственного процесса на 6 недель.
01.22		Переворот	Нет вероятности.	Нет вероятной опасности.	Нет.
01.23		Кроме того	Нет вероятности.	Нет вероятной опасности.	Нет.
01.24		Другое	Нет вероятности.	Нет вероятной опасности.	Нет.

3.7.3. Результаты анализа HAZOP

Выявлены следующие опасности:

Опасность	**Последствия**
Высокий уровень в резервуаре может привести к уносу жидкости в вывод газа.	Повреждение оборудования по направлению потока, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процесса на 6 месяцев.
Высокое давление приводит к разрушению резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процессов на 1 год. Незначительный выброс в окружающую среду.
Высокая температура приводит к повышению давления, разрушению резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процессов на 1 год. Незначительный выброс в окружающую среду.
Низкий уровень в резервуаре может привести к прорыву газа в экспорт жидкости.	Повреждение оборудования по направлению потока, требующее чистки резервуара (примерно 2 млн фунтов стерлингов) и остановки процесса на 6 недель.
Низкое давление приводит к разрушению резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процессов на 1 год. Незначительный выброс в окружающую среду.
Низкая температура, возможное замерзание (затвердевание) жидкости, разрушение резервуара и утечка из реактора.	Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процесса на 6 месяцев. Выброс в окружающую среду, требующий уведомления.

Список выявленных опасностей и является «протоколом опасностей» для данной системы. Протокол опасностей должен быть постоянно обновляемым документом, подлежащим непрерывному пересмотру и дополнению на протяжении всего жизненного цикла системы.

Каждая из выявленных опасностей может иметь определенные возможные последствия для безопасности, окружающей среды и коммерческой сферы, но для выполнения обязательств по Закону о гигиене и безопасности труда на рабочем месте [1.5.1] необходимо определить уровень риска, присущий каждой опасности [4].

4. Риск и снижение степени риска

4.1. Понятие риска

Риск – это вероятность того, что опасность станет причиной измеримых неблагоприятных последствий.

Таким образом, это двоякое понятие, и для осмысления требуется обязательное присутствие двух факторов. Вероятность может выражаться различными способами, например, как пропорция («один на тысячу»), как периодичность («1000 случаев в год») или как качественная оценка («несущественно» или «существенно»).

Эффект также может быть описан различными способами. Например:

- серьезная травма или гибель одного работника;
- множественные травмы третьих сторон;
- поражение населения токсичными газами.

Среднегодовой риск несчастного случая со смертельным исходом на производстве [эффект] при контакте с подвижными механизмами [опасность] составляет менее одного случая на 100 000 [вероятность].

Таким образом, риск необходимо оценивать в двух измерениях. Должны быть определены как последствия опасности, так и их вероятность. Для простоты оцените каждый из параметров по шкале от 1 до 4, как показано на рис. 10, где большее значение указывает на большее воздействие и более высокую вероятность. В общем, определить приоритет и оценить риск можно с помощью матрицы рисков, подобной этой.

Рис. 10. Матрица рисков

Если вероятность высока, а тяжесть последствий мала, риск можно расценивать как средний. С другой стороны, если вероятность низкая, а тяжесть последствий высока, риск можно расценивать как высокий. Как правило, небольшая вероятность катастрофы должна привлекать больше внимания, чем незначительная помеха, которая часто имеет место.

Приведенные примеры риска касаются только безопасности персонала, но это не значит, что такой подход не может быть адаптирован к рискам для окружающей среды, бизнеса, активам, доходам, прибыльности, репутации предприятия или бесперебойности поставок, как в случае с энергетическими предприятиями.

4.2. Анализ опасности (HAZAN)

Первая оценка риска обычно выполняется в рамках HAZOP и известна как «оценка опасности» (HAZAN). Как показано на рис. 10, для любой опасности может быть определен уровень серьезности (как правило, от 1 до 4, где 4 – высшая степень) и вероятности (от 1 до 4, где 4 – высшая степень).

Как показано в примере, может быть выполнен анализ HAZOP [3.7.2] с последующим умножением показателей серьезности и вероятности опасности для получения предварительной оценки риска в виде «показателя приоритета уровня риска» (RPN), который используется для определения приоритета действий по снижению уровней риска [4.3].

4.3. Анализ HAZAN сепаратора

В столбце «Действие» можно указать рекомендованное действие, например, выполнение анализа с целью поиска возможности внедрения дополнительных средств защиты.

Возможны действия двух типов:

- действия, направленные на устранение причины;
- действия, направленные на смягчение последствий.

Предпочтительным действием является устранение причины опасности. Действия, направленные на смягчение последствий, допускаются только в случаях маловероятного риска.

4.3.1. Действия HAZOP

В таблицах HAZOP также определяются действия в рамках дальнейшего исследования. В данном примере определены следующие действия.

№	Отклонение	Опасность	Последствия	Кат. серьезности	Кат. частотности	RPN	Меры безопасности	Действие
01.01	Большой поток рабочей жидкости в резервуар.	Большой поток в резервуар может приводить к повышению уровня и попаданию жидкости в выпускаемый газ.	Повреждение оборудования ниже по потоку, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев.	3	2	6	Управление уровнем.	Рассмотрите вариант с установкой сигнализации высокого уровня.
01.02	Высокий уровень рабочей жидкости на выходе жидкости из резервуара.	Высокий уровень на выходе из резервуара может приводить к снижению уровня и попаданию газа в жидкость.	Повреждение оборудования ниже по потоку, требующее чистки резервуара примерной стоимостью 2 млн фунтов стерлингов, и остановка производственного процесса на 6 недель.	2	1	2	Управление уровнем.	Рассмотрите вариант с установкой сигнализации низкого уровня.
01.03	Высокий расход газа на выходе газа из резервуара.	Нет вероятной опасности.	Нет.				Нет.	
01.04	Недостаточный приток рабочей жидкости в резервуар.	Низкий уровень на входе в резервуар может приводить к снижению уровня и попаданию газа в жидкость.	Повреждение оборудования ниже по потоку, требующее чистки резервуара примерной стоимостью 2 млн фунтов стерлингов, и остановка производственного процесса на 6 недель.	2	2	4	Управление уровнем.	Рассмотрите вариант с установкой сигнализации низкого уровня.
01.05	Низкий уровень рабочей жидкости на выходе жидкости из резервуара.	Низкий расход на выходе из резервуара может приводить к повышению уровня и попаданию жидкости в выпускаемый газ.	Повреждение оборудования ниже по потоку, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев.	3	1	3	Управление уровнем.	Рассмотрите вариант с установкой сигнализации высокого уровня.
01.06	Низкий расход газа на выходе газа из резервуара.	Нет вероятной опасности.	Нет.				Нет.	
01.07	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.08	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.09	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.10	Высокое давление в резервуаре.	Прорыв резервуара и утечка газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух ремонтников. Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 1 год. Незначительный выброс в окружающую среду.	4	2	8	Контроль давления.	Рассмотрите вариант с установкой сигнализации высокого уровня.
01.11	Низкое давление в резервуаре.	Прорыв резервуара и утечка газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух ремонтников. Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 1 год. Незначительный выброс в окружающую среду.	4	1	4	Контроль давления.	Рассмотрите вариант с установкой сигнализации низкого уровня.
01.12	Нет вероятности.	Нет вероятной опасности	Нет.				Нет.	
01.13	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.14	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.15	Высокая температура в резервуаре.	Высокая температура приводит к повышению давления, прорыву резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух ремонтников. Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 1 год. Незначительный выброс в окружающую среду.	4	1	4	Контроль температуры.	Рассмотрите вариант с установкой сигнализации высокого уровня температуры.
01.16	Низкая температура в резервуаре.	Возможно замерзание (загустение) жидкости, прорыв резервуара и нарушение герметичности.	Повреждение оборудования, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев. Выброс в окружающую среду, требующий уведомления.	3	1	3	Контроль температуры.	Рассмотрите вариант с установкой сигнализации низкого уровня температуры.
01.17	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.18	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.19	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.20	Высокий уровень в резервуаре.	Высокий уровень в резервуаре может приводить к попаданию жидкости в выпускаемый газ.	Повреждение оборудования ниже по потоку, требующее замены резервуара примерной стоимостью 10 млн фунтов стерлингов, и остановка производственного процесса на 6 месяцев.	3	2	6	Управление уровнем.	Рассмотрите вариант с установкой сигнализации высокого уровня.
01.21	Низкий уровень в резервуаре.	Низкий уровень в резервуаре может приводить к попаданию газа в выпускаемую жидкость.	Повреждение оборудования ниже по потоку, требующее чистки резервуара примерной стоимостью 2 млн фунтов стерлингов, и остановка производственного процесса на 6 недель.	2	1	2	Управление уровнем.	Рассмотрите вариант с установкой сигнализации низкого уровня.
01.22	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.23	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	
01.24	Нет вероятности.	Нет вероятной опасности.	Нет.				Нет.	

№	Опасность	Последствия	Действие	Действие назначено	Дата завершения
01.01	Высокий расход на входе резервуара может привести к высокому уровню и уносу жидкости в вывод газа.	Повреждение оборудования по направлению потока.	Рассмотреть возможность установки аварийного сигнала для высокого уровня.	С. Смит Отдел КИП	14 апреля 2012 г.
01.02	Высокий расход на выходе резервуара может привести к низкому уровню и прорыву газа в вывод жидкости.	Повреждение оборудования по направлению потока.	Рассмотреть возможность установки аварийного сигнала для низкого уровня.	С. Смит Отдел КИП	14 апреля 2012 г.
01.04	Низкий расход на входе резервуара может привести к низкому уровню и прорыву газа в вывод жидкости.	Повреждение оборудования по направлению потока.	Рассмотреть возможность установки аварийного сигнала для низкого уровня.	С. Смит Отдел КИП	14 апреля 2012 г.
01.05	Низкий расход на выходе резервуара может привести к высокому уровню и уносу жидкости в вывод газа.	Повреждение оборудования по направлению потока.	Рассмотреть возможность установки аварийного сигнала для высокого уровня.	С. Смит Отдел КИП	14 апреля 2012 г.
01.10	Прорыв резервуара и утечка газа.	Возможна гибель людей из обслуживающего персонала. Повреждение оборудования. Выброс в окружающую среду.	Рассмотреть возможность установки аварийного сигнала для высокого давления.	Дж. Джонс Технолог. отдел	21 апреля 2012 г.
01.11	Прорыв резервуара и утечка газа.	Возможна гибель людей из обслуживающего персонала. Повреждение оборудования. Выброс в окружающую среду.	Рассмотреть возможность установки аварийного сигнала для низкого давления.	Дж. Джонс Технолог. отдел	21 апреля 2012 г.
01.15	Высокая температура приводит к повышению давления, разрушению резервуара и выбросу газа.	Возможна гибель людей из обслуживающего персонала. Повреждение оборудования. Выброс в окружающую среду.	Рассмотреть возможность установки аварийного сигнала для высокой температуры.	В Уайт Отдел КИП	21 апреля 2012 г.
01.16	Возможное замерзание жидкости, разрушение резервуара и утечка из реактора.	Повреждение оборудования. Выброс в окружающую среду.	Рассмотреть возможность установки аварийного сигнала для низкой температуры.	В Уайт Отдел КИП	21 апреля 2012 г.

№	Опасность	Последствия	Действие	Действие назначено	Дата завершения
01.20	Высокий уровень в резервуаре может привести к уносу жидкости в вывод газа	Повреждение оборудования по направлению потока.	Рассмотреть возможность установки аварийного сигнала для высокого уровня.	С. Смит Отдел КИП	14 апреля 2012 г.
01.21	Низкий уровень в резервуаре может привести к прорыву газа в вывод жидкости.	Повреждение оборудования по направлению потока.	Рассмотреть возможность установки аварийного сигнала для низкого уровня.	С. Смит Отдел КИП	14 апреля 2012 г.

4.4. Примеры классификации в таблице рисков

На рис. 11 представлена информация для использованной выше простой таблицы риска. Серьезность последствий определяется простым общим описанием, например, «побочные», «малой тяжести», «тяжелые», «катастрофические». Если был выполнен анализ HAZOP, то вероятные последствия выявленных опасностей, скорее всего, будут известны и уже распределены по категориям.

Дать количественную оценку вероятности труднее. На рис. 11 представлен подход, предполагающий описательную характеристику на основе периодичности, например, «возникает несколько раз в год», «возникает очень редко», «о случаях не сообщалось в отрасли» или «не сообщалось вообще». Такая количественная оценка вероятности позволяет присвоить каждой категории опасности ту или иную периодичность.

Полученная таблица позволяет распределить риски по уровням «очень низкий» (VL), «низкий» (L), «средний» (M), «высокий» (H) и «очень высокий» (VH) согласно серьезности последствий и периодичности.

Рис. 11. Матрица рисков

		Вероятность							
		Ничего не знаю о в какой-либо отрасли/сфере работ	Ничего не знаю о в отрасли/сфере работ	Знаю об отрасли/сфере работ	Встречалось в бизнесе	Несколько раз встречалось в бизнесе	Встречается на объекте	Встречается несколько раз на объектах	Встречается несколько раз в год на объектах
Серьезность		**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Катастрофически 10^{-6}/г	**6**	**VL**	**L**	**M**	**H**	**VH**	**VH**	**VH**	**VH**
Серьезно 10^{-5}/г	**5**		**VL**	**L**	**M**	**H**	**VH**	**VH**	**VH**
Крупно 10^{-4}/г	**4**			**VL**	**L**	**M**	**H**	**VH**	**VH**
Умеренно 10^{-3}/г	**3**				**VL**	**L**	**M**	**H**	**VH**
Незначительно 10^{-2}/г	**2**					**VL**	**L**	**M**	**H**
Случайно 10^{-1}/г	**1**						**VL**	**L**	**M**
		$<10^{-6}$/г	$10^{-6} - 10^{-5}$/г	$10^{-5} - 10^{-4}$/г	$10^{-4} - 10^{-3}$/г	$10^{-3} - 10^{-2}$/г	$10^{-2} - 10^{-1}$/г	$10^{-1} - 1$/г	>1/г

4.5. Количественная оценка риска

Приемлемость риска до сих пор оценивалась качественно. Количественная оценка приемлемости риска для личной безопасности зависит от восприятия риска и еще ряда факторов:

- личный опыт негативных последствий;
- социальный и культурный уровень и убеждения;
- уровень возможностей контроля риска;
- объем накопленной информации из различных источников.

Разумеется, риски высокого уровня неприемлемы (например, курение при беременности), а риски низкого уровня несущественны (кипящее молоко). Конечно, наиболее интересная сфера для обсуждения – это «серая» зона приемлемого риска, находящая между полюсами. Задача заключается в определении двух граничных условий:

- между неприемлемым и допустимым риском и
- между допустимым и приемлемым риском.

Руководство по технике безопасности и охране окружающей среды «Снижение риска и защита людей» (Reducing Risks, Protecting People – R2P2) [19.3] рекомендует **риск одного смертельного случая на миллион или в год как для работников, так и для гражданского населения** сопоставлять с очень низким уровнем риска, и использовать этот показатель как широко приемлемую (не принимаемую в расчет) границу риска.

Далее в документе R2P2 оговаривается, **что единичный случай смерти на тысячу в год** является граничным условием между тем, что является приемлемым для большинства категорий работников на протяжении большей части их жизни, и тем, что неприемлемо для большинства за исключением особых категорий. В Великобритании цели гигиены труда и безопасности на рабочем месте установлены на уровне привычной повседневной жизнедеятельности без негативных последствий.

Для представителей общественности, подверженных риску, этот предел устанавливается на один порядок ниже – **1 на 10 000 в год**.

Установленные в руководстве по технике безопасности и охране окружающей среды критерии можно проиллюстрировать приемлемостью риска (TOR), как показано на рис. 12. Отмечены максимально приемлемые и широко применяемые уровни риска.

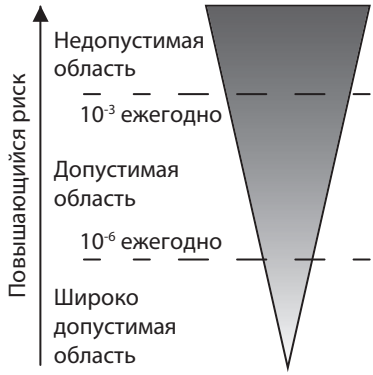


Рис. 12. Приемлемость риска

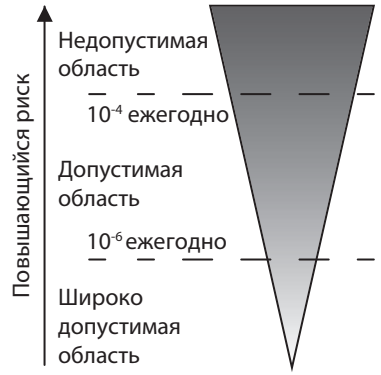


Рис. 13. Критерии индивидуального риска

4.6. Приемлемость и допустимость риска

При количественной оценке риска, обусловленного опасностью, определенной в ходе анализа HAZOP, необходимо установить количественные критерии и учесть прочие производственные риски, которым подвергается лицо в течение рабочего дня. Не лишен смысла метод построения предположений относительно того, что лицо будет подвержено 10 таким опасностям. Приемлемость критериев риска (рис. 12) может быть распределена между этими 10 опасностями с присвоением максимального значения отдельному риску смерти в 1 из 10 000 случаев в год (рис. 13).

Граница приемлемого риска для отдельного риска смерти как для работников, так и для широкой общественности остается на уровне одного случая на миллион в год, так как этот уровень уже признан несущественным. Приемлемость риска можно суммировать, как показано на рис. 14.

ИНДИВИДУАЛЬНЫЙ РИСК ежегодно

Последствия	Незначительные/Серьезные	Серьезные/Жертвы	Многочисленные жертвы
Сотрудники	10^{-3}	10^{-4}	10^{-5}
Население	10^{-4}	10^{-5}	10^{-6}

ШИРОКО ДОПУСТИМЫЙ РИСК (пренебрежимый)

Последствия	Незначительные/Серьезные	Серьезные/Жертвы	Многочисленные жертвы
Сотрудники	10^{-5}	10^{-6}	10^{-6}

Рис. 14. Приемлемость риска: резюме

На основании максимально приемлемого риска смерти на уровне 1 случая на 10 000 в год можно определить другие уровни риска с учетом серьезности и подверженности третьих лиц (см. рис. 15).

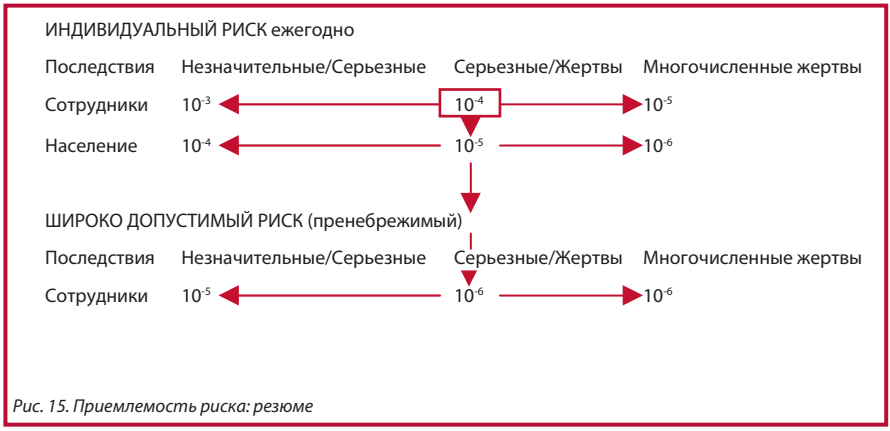


Рис. 15. Приемлемость риска: резюме

4.7. Приемлемость риска

Сводка приемлемости риска [рис. 15] представлена графически на рис. 16.

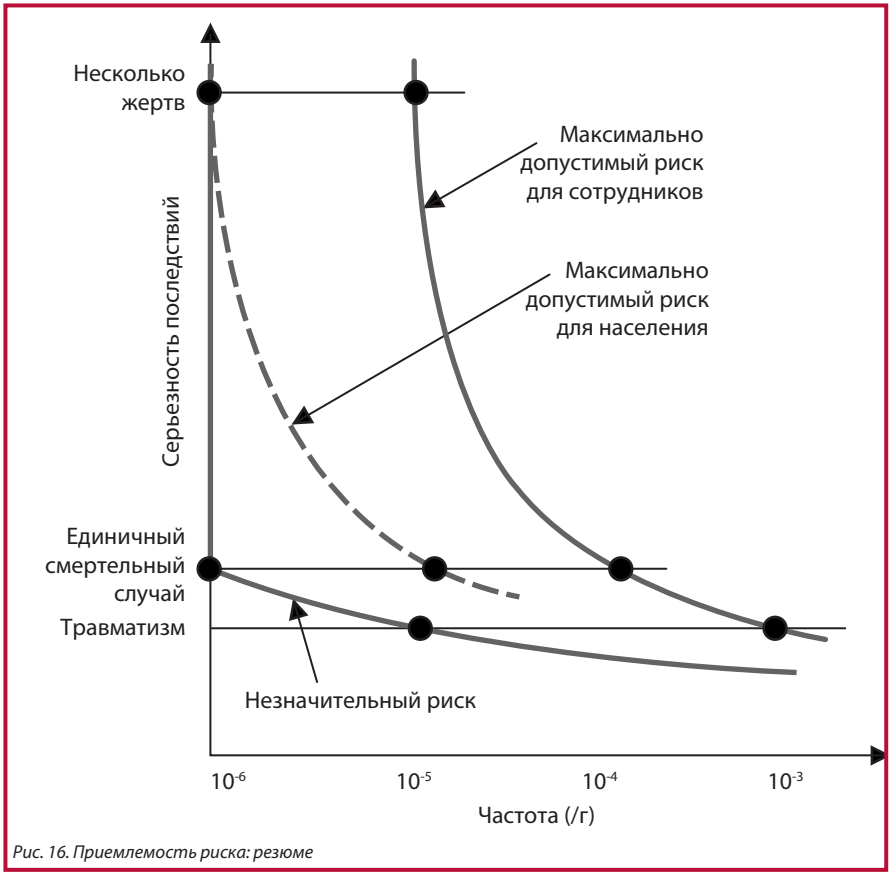


Рис. 16. Приемлемость риска: резюме

4.8. Требования соответствия

Требования в отношении уровней полноты безопасности формулируются на основании периодичности опасных событий. В зависимости от последствий опасности определяется максимально приемлемая периодичность, и все функции безопасности проектируются с целью приведения всех периодичностей к приемлемому уровню.

Степень снижения риска, требуемая от функции безопасности, – это первое требование соответствия стандарту: это выраженная в числовой форме надежность меры безопасности.

Выраженная в числовой форме надежность сопоставляется с определенным уровнем полноты безопасности (SIL). Существует четыре уровня полноты безопасности, основанных на требованиях к надежности мер безопасности. Уровень SIL4 – высший уровень полноты с наибольшим снижением рисков и самыми трудными задачами обеспечения надежности. Уровень SIL1 – низший уровень полноты с простейшими задачами обеспечения надежности.

4.9. Принцип минимального практически приемлемого уровня риска (ALARP)

Приведенный выше обзор анализа опасностей и рисков демонстрирует, как определяется риск и как обеспечивается его максимально приемлемый уровень. Однако в рамках HSAWA необходимо предпринять дополнительные действия для снижения уровня риска, пока не удастся доказать, что риск **находится на «минимальном практически приемлемом уровне»** (ALARP), то есть дальнейшее снижение риска нецелесообразно или нерентабельно [5].

5. Принцип минимального практически приемлемого уровня риска (ALARP)

5.1. Преимущества и недостатки

Использование «практически целесообразных» целей для ответственных лиц, а не предписаний. Гибкость – это огромное преимущество, поскольку ответственные лица получают возможность выбирать лучшие для себя методы, что обеспечивает поддержку инноваций. Однако есть и недостатки. Отнесение риска к «минимальному практически приемлемому уровню» – это непростая задача, требующая от ответственных лиц и оценщиков рассудительности.

Основные испытания, применяемые при работе с рисками на производстве, предполагают подтверждение того, что:

а) риск настолько велик, что его следует полностью отбросить;
б) риск настолько мал (изначально или в результате принятых мер), что им можно пренебречь;
в) риск находится между двумя описанными выше состояниями (а, б), но снижен до «минимального практически приемлемого уровня».

«Минимальному практически приемлемому уровню» трудно дать количественную оценку. Предполагается, что необходимо произвести вычисления, приняв во внимание достигаемое дополнительное снижение уровня риска и связанные с этим потери (денежных средств, времени, комфорта). Если обнаруживается существенная диспропорция, то полученные преимущества незначительны в сравнении с затратами, и риск оценивается как риск «минимального практически приемлемого уровня».

Так, для подтверждения того, что риски снижены до «минимального практически приемлемого уровня», требуется оценка:

- самого избегаемого риска;
- потерь (денег, времени, удобства) при принятии мер по снижению уровня риска;
- соотношения первого и второго.

Этот процесс может включать критерии различной степени строгости:

- природа опасности;
- масштаб риска;
- принимаемые меры по контролю.

При этом ответственные лица (и регулятивный орган) не должны создавать дополнительные трудности для себя, если надежность не гарантируется. Чем выше начальный уровень рассматриваемого риска, тем выше степень требуемой надежности.

5.2. Диспропорция

Принять решение о целесообразности дальнейшего снижения уровня риска ответственному лицу поможет «анализ эффективности затрат» (CBA). Дополнительные меры по снижению уровня риска могут считаться целесообразными до тех пор, пока затраты на их реализацию находятся в разумном соотношении с приносимой пользой. Попросту говоря, если соотношение «затраты/польза» превышают «коэффициент диспропорции» (DF), то такие меры считаются неоправданными для достигаемого снижения уровня риска.

Величина коэффициента диспропорции, которая считается чрезмерной, – это от 1 и выше – в зависимости от числа факторов воздействия, включающих тяжесть и периодичность последствий, т.е. чем выше риск, тем выше и коэффициент диспропорции.

5.3. Что такое чрезмерная диспропорция?

Управление по вопросам охраны здоровья, техники безопасности и охраны труда (HSE) не предоставляет готовый алгоритм расчета степени диспропорции, которая может считаться «чрезмерной». Не существует и каких-либо конкретных указаний судебных органов относительно того, что необходимо учитывать при оценке диспропорции затрат и выгоды. В связи с этим решение следует принимать с учетом условий каждого конкретного случая, опираясь на доступные данные об известных происшествиях.

Со времен исследований на объекте «Б» в Сайзуэлле 1987 года применяются следующие коэффициенты диспропорции:

- для рисков низкого уровня для общественности принят коэффициент 2;
- для рисков для работников принят коэффициент до 3 (т.е. затраты превышают отдачу в 3 раза);
- для рисков высокого уровня принят коэффициент 10.

5.4. Анализ эффективности затрат (CBA)

Во многих случаях принятия решений о «минимальном практически приемлемом уровне риска» (ALARP) Управление по вопросам охраны здоровья, техники безопасности и охраны труда (HSE) не требует от ответственных лиц проведения подробного анализа эффективности затрат (CBA). Достаточно простого сравнения затрат и выгоды.

Анализ эффективности затрат следует применять только при принятии решений ALARP. При этом этот анализ не должен быть единственным при принятии решения ALARP и не должен использоваться с целью изменения существующих стандартов и принятых методов. Результат CBA сам по себе не является основанием для принятия решения в отношении ALARP и не может использоваться для опровержения установленных правил, а также оправдания неприемлемого риска или очевидного некачественного проектирования.

Позволительные затраты, которые могут учитываться в анализе CBA, включают:

- установку;
- эксплуатацию;
- обучение;
- техническое обслуживание;
- коммерческие убытки, которые могут последовать в случае останова только с целью принятия мер по снижению уровня риска;
- процент на замедленную добычу, например, нефть или газ, оставшийся на месторождении во время проведения работ на платформе;
- все заявленные затраты, понесенные ответственным лицом (все затраты третьих сторон, т.е. общественности, исключаются);
- затраты, которые считаются необходимыми при принятии мер по снижению уровня риска (без роскоши и чрезмерных затрат).

Позволительные преимущества, которые могут быть заявлены в ходе анализа CBA, могут включать все преимущества от мер повышения безопасности в полном объеме, если они не недооценены. Преимущества должны включать все аспекты снижения уровня риска для населения, работников и общественности, включая:

- предотвращение гибели;
- предотвращение травм (легких и тяжелых);
- предотвращение ухудшения состояния здоровья;
- предотвращение ущерба окружающей среде, если применимо (например, контроль за основными факторами опасности на производстве, COMAH).

Заявленные преимущества, если необходимо, также могут включать предотвращение развертывания аварийных служб и принятия контрмер, таких как эвакуация и очистка после аварий. Однако для сравнения преимуществ мер повышения безопасности и соответствующих затрат должны использоваться общие основания. Простой метод грубого отбора мер позволяет сопоставить преимущества и затраты в простой форме «фунтов стерлингов в год» для всего жизненного цикла предприятия.

В таблице 1 представлены типичные денежные величины, которые можно использовать.

Гибель		1 336 800 фунтов стерлингов (x2 для рака)
Травма	Травма, приводящая к пожизненной инвалидности. Некоторые постоянные ограничения для отдыха и, возможно, определенной деятельности на работе.	207 200 фунтов стерлингов
	Серьезная. Некоторые ограничения в рабочей и/или досуговой деятельности в течение нескольких недель/месяцев.	20 500 фунтов стерлингов
	Легкие травмы, включая мелкие порезы и ушибы, с быстрым и полным выздоровлением.	300 фунтов стерлингов
Болезнь	Болезнь, приводящая к пожизненной инвалидности. То же, что для травмы.	193 100 фунтов стерлингов
	Другие случаи болезней. Более одной недели отсутствия. Без необратимых последствий для здоровья.	2300 фунтов стерлингов + 180 фунтов стерлингов за каждый день отсутствия
Незначительно	До одной недели отсутствия. Без необратимых последствий для здоровья.	530 фунтов стерлингов

Таблица 1: Типичное возмещение ущерба по суду (2003)

5.5. Пример

Вопрос: Рассмотреть химический завод с процессом, который в случае взрыва, приведет к:

- гибели 20 человек;
- инвалидности 40 человек;
- травмированию 100 человек (тяжелые травмы);
- легким травмам у 200 человек.

Вероятность взрыва оценивается в 10^{-5} в год, что эквивалентно 1 на 100 000 в год. Расчетный срок работы предприятия – 25 лет. Каковы разумные затраты организации на предотвращение риска взрыва?

Ответы: Если риск взрыва исключен, то преимущества можно оценить следующим образом:

Гибель:	20 x 1,336,800 фунтов стерлингов x 10^{-5} x 25 (лет)	= 6684 фунтов стерлингов
Инвалидность:	40 x 207,200 фунтов стерлингов x 10^{-5} x 25 (лет)	= 2072 фунтов стерлингов
Тяжелые травмы:	100 x 20,500 фунтов стерлингов x 10^{-5} x 25 (лет)	= 512 фунтов стерлингов
Легкие травмы:	200 x 300 фунтов стерлингов x 10^{-5} x 25 (лет)	= 15 фунтов стерлингов
Общие преимущества		= 9283 фунтов стерлингов

Величина 9283 фунтов стерлингов – это предполагаемая польза от предотвращения возможности взрыва на предприятии, основанная на сокращении возможного числа жертв. (Этот метод не учитывает амортизацию или инфляцию.)

Для мер, которые считаются неприемлемыми, затраты должны несоизмеримо превышать полученные преимущества. В этом случае коэффициент диспропорции укажет на то, что последствия такого взрыва имеют высокую цену. Коэффициент, превышающий 10, маловероятен, поэтому для предотвращения угрозы взрыва может оказаться «практически целесообразным» ограничить затраты суммой на уровне 93 000 фунтов стерлингов (9300 фунтов стерлингов x 10). Ответственное лицо должно обосновать применение низкого коэффициента.

Такой простой анализ позволит исключить или предусмотреть некоторые меры безопасности путем оценки альтернативных решений для снижения уровня риска.

Альтернативный поход

Вероятнее всего, меры повышения безопасности не исключат риск, а лишь немного снизят его вероятность, и это снижение уровня риска, как полученное преимущество, необходимо будет оценить, сопоставив с затратами.

Как правило, организации ориентируются на условную цифру «стоимости спасения одной жизни» (стоимость предотвращения гибели одного человека, VPF).

Стоимость предотвращения гибели за весь срок эксплуатации предприятия сопоставляется с целевой величиной VPF.

Усовершенствования в систему безопасности внедряются лишь в том случае, если затраты не являются несоизмеримо большими.

5.6. Пример

Вопрос: Применение ALARP

Целевая величина затрат, равная 2 миллионам фунтов стерлингов на одну спасенную жизнь, применяется в конкретной отрасли. Для определенной опасности установлен ориентировочный максимальный приемлемый риск на уровне 10^{-5} в год, что предполагает гибель 2 человек.

По оценке предложенной системы безопасности риск составляет 8,0 x 10^{-6}. Учитывая, что широко приемлемая (не принимаемая в расчет) граница риска составляет 10^{-6} в год, требуется проведение анализа ALARP.

В данном примере при затратах в размере 10 000 фунтов стерлингов дополнительные приборы и резервирование снизят риск до уровня 2,0 x 10^{-6} в год (чуть выше не принимаемого в расчет порога) на весь срок работы предприятия, равный 30 годам.

Следует ли принимать предложение?

Ответ: Число жизней, спасенных за весь срок работы предприятия, составляет:

N = (сокращение числа смертных случаев) x число смертных случаев на несчастный случай x срок работы предприятия
= (8,0 x 10^{-6} – 2,0 x 10^{-6}) x 2 x 30
= 3,6 x 10^{-4}

Следовательно, затраты на одну спасенную жизнь составляют:

VPF = 10 000/3,6 x 10^{-4}
= 27,8 млн фунтов стерлингов

Вычисленное значение VPF более чем в 10 раз превышает целевые затраты на одну спасенную жизнь (2 млн фунтов стерлингов), поэтому предложение должно быть отклонено.

6. Определение требуемого уровня полноты безопасности (SIL)

6.1. Функции безопасности управляемого режима и непрерывного режима

В зависимости от режима эксплуатации существует два способа оценки отказоустойчивости системы безопасности. Если система используется редко, например, реже одного раза в год, то такая система считается работающей в управляемом в режиме «по требованию». Примером такой системы безопасности может служить подушка безопасности в автомобиле.

А тормозная система автомобиля – это пример системы безопасности, работающей в непрерывном режиме: тормоза используются (практически) постоянно. Для систем безопасности, работающих в управляемом режиме, как правило, вычисляется «средняя вероятность отказа по требованию» (PFD), в то время как для систем с непрерывным режимом работы применяется показатель «вероятность опасного отказа в час» (PFH).

6.2. Режим управления – функция безопасности

Например, допустим, что на предприятии в среднем происходит 1 пожар в 2 года, и, если ничего не предпринимать, то пожар приведет к жертвам. Можно нарисовать график смертности от несчастных случаев (рис. 17). Уровень составит 0,5/год.

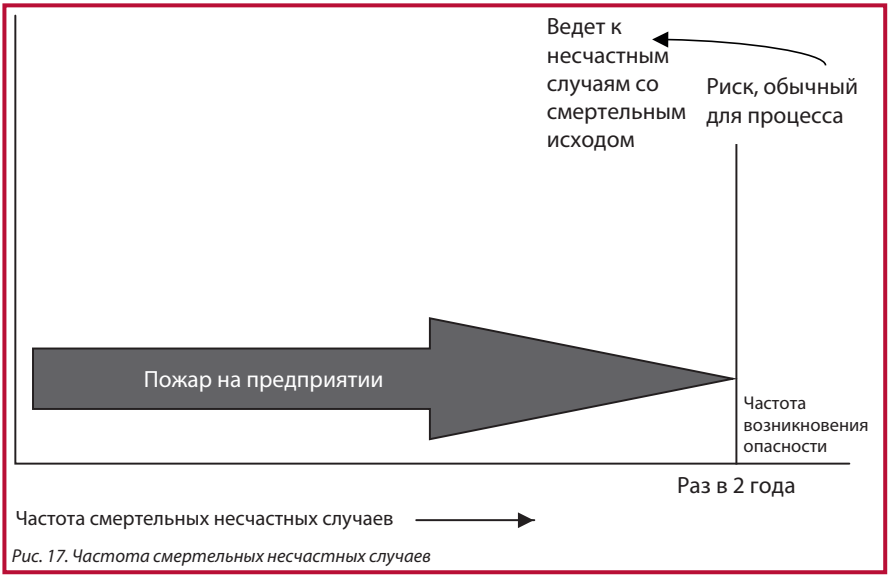


Рис. 17. Частота смертельных несчастных случаев

В этом случае важно, что при определении последствий пожара не принимаются во внимание средства защиты, которые могут уже быть в наличии. Внимание обращаем на худшие последствия.

Если установить систему сигнализации о появлении дыма, которая, допустим, будет срабатывать 9 раз из 10, несчастный случай произойдет в 1 случае из 10 пожаров, когда сигнализация даст сбой. В таком случае частота несчастных случаев со смертельным исходом снизится от 1 случая в 2 года до 1 случая в 20 лет.

Рис. 18. Сокращенная частота смертей

В этом примере, если сигнализация о появлении дыма срабатывает при 9 пожарах из 10, вероятность отказа по требованию (PFD) составляет 1/10 или 10%. В данном случае PFD = 0,1. Сигнализация о появлении дыма с показателем PFD, равным 0,1, снизит частоту несчастных случаев в 10 раз, дав коэффициент снижения риска (RRF) 10.

Итак, PFD = 1/RRF.

Важно помнить, что с точки зрения математики PFD – это вероятность, поэтому является безразмерной величиной между 0 и 1.

6.3. Пример требований к уровню полноты безопасности (SIL)

Подход, применяемый к определению УПБ, заключается в вычислении коэффициента снижения риска, необходимого для приведения вероятности последствий опасности до приемлемого уровня.

Рекомендованный подход к определению SIL предполагает оценку риска для каждой опасности на предприятии. Если провести анализ HAZOP и определить присущие процессам потенциальные опасности, которые причинят ущерб, если ничего не предпринимать, то необходимо оценить потенциальные последствия. Худшие последствия и определят максимальную приемлемую периодичность возникновения опасности.

Если опасность может привести к гибели работника, то в зависимости от приемлемости и допустимости критериев риска [4.6] можно установить максимальную приемлемую периодичность опасности. Иными словами, для определенной опасности можно установить максимальный приемлемый риск на уровне 10^{-4} случаев в год.

Проанализировав первопричины, можно оценить вероятность опасности в случае бездействия и сопоставить ее с установленной максимальной приемлемой периодичностью. Можно провести исследования и выяснить, что опасность, если ей не уделять внимания, может себя проявлять раз в год. Это и есть пробел в управлении риском – то, чему необходимо уделить внимание (рис. 19).

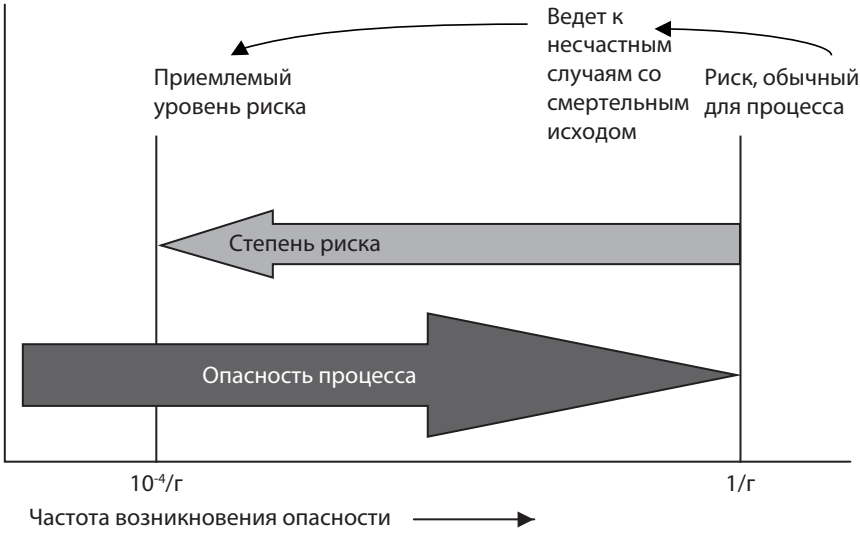


Рис. 19. Степень риска

Мы можем взять на себя ответственность за меры безопасности, которые уже могут быть предусмотрены для снижения периодичности риска, такие как система сигнализации (рис. 20). В таком случае сигнализация снизит периодичность последствий опасности на ее коэффициент PFD. Таким образом, пробел в управлении риском

сокращается, но общий остаточный риск, хоть и небольшой, по-прежнему превышает максимальный приемлемый риск.

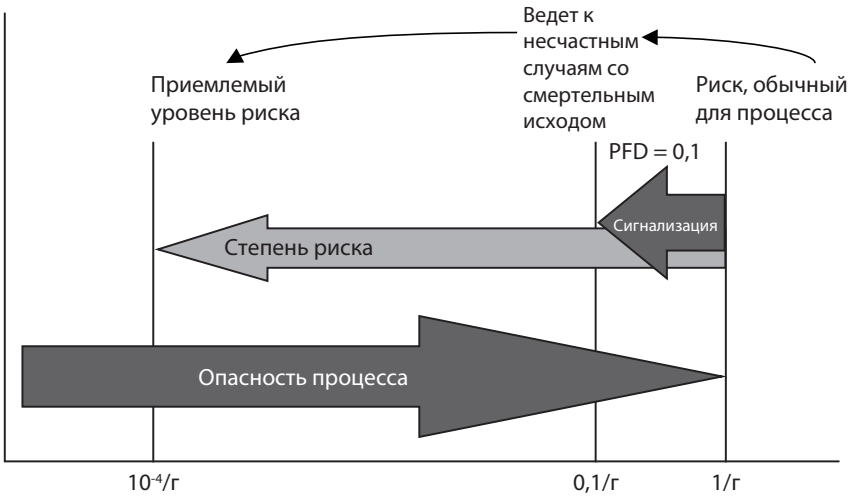


Рис. 20. Вклад устройств сигнализации

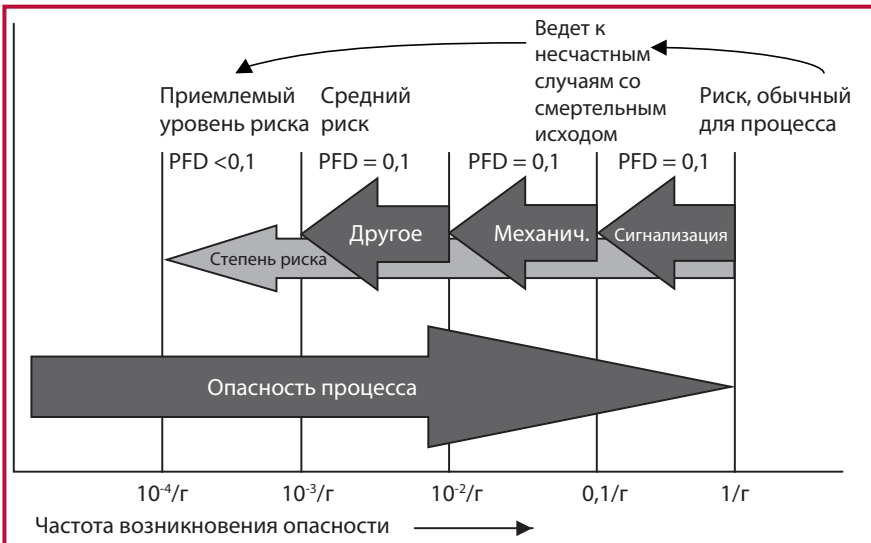


Рис. 21. Прочие уровни защиты

Принятие во внимание других уровней защиты позволит еще снизить остаточный риск. Могут быть предусмотрены механические устройства, такие как предохранительные клапаны, взрывозащитные стены или дамбы. Также меры снижения риска могут включать управление процессами, измерительные приборы и процедуры, при этом каждый их элементов внесет свой вклад в снижение уровня остаточного риска (рис. 21) на соответствующую ему величину PFD. В данном примере учтены все меры безопасности, имеющиеся на предприятии, но все равно остался пробел. Очевидно, что для снижения периодичности опасности до уровня ниже максимально приемлемого потребуется еще один уровень защиты с PFD менее 0,1. Это и есть задача обеспечения требуемого уровня SIS (рис. 22). Эти вычисления, хотя и выполненные в графической форме, дают нам целевое значение PFD для SIS и позволяют определить цели УПБ. Вот пример расчета функции безопасности с управляемым режимом работы.

Рис. 22. Цель PFD

6.4. Функции безопасности

Типовая компоновка SIS и процессов представлена на рис. 23.

Рис. 23. Автоматизированная система безопасности

Автоматизированная система безопасности отслеживает некоторые процессы и предпринимает действия для обеспечения их безопасности в случае выхода тех или иных параметров за установленные пределы. На рис. 24 представлен простой пример из перерабатывающей промышленности.

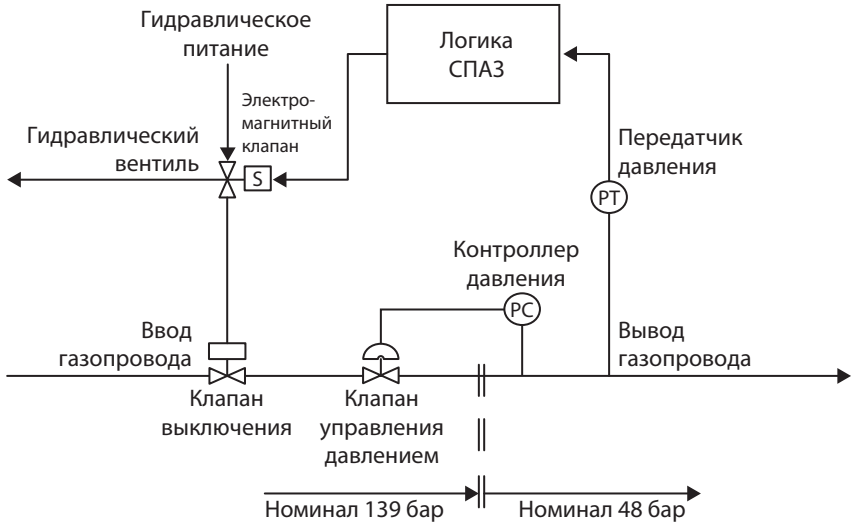


Рис. 24. Функция отказа в случае возникновения опасной ситуации

На рисунке показан газопровод, питающий электростанцию. Газ поступает слева направо в клапан регулировки давления (PCV) через отсекающий клапан. Клапан регулировки давления управляется контроллером давления (PC), который поддерживает давление газа на уровне ниже 48 бар, как предусмотрено техникой безопасности. Отказ функции контроля давления может привести к образованию избыточного давления в трубопроводе дальше по технологической цепочке, что угрожает разрывом, возгоранием и гибелью персонала, поэтому и была предусмотрена эта функция безопасности. Функция безопасности состоит из отдельного датчика давления (PT), системы аварийного отключения (СПАЗ) и отсекающего клапана (SDV), который приводится в действие гидравлическим клапаном с электромагнитным управлением (SOV) с целью прекращения подачи газа в случае превышения заданной установки давления ниже в технологической цепочке.

6.5. Пример функции безопасности с управляемым режимом работы

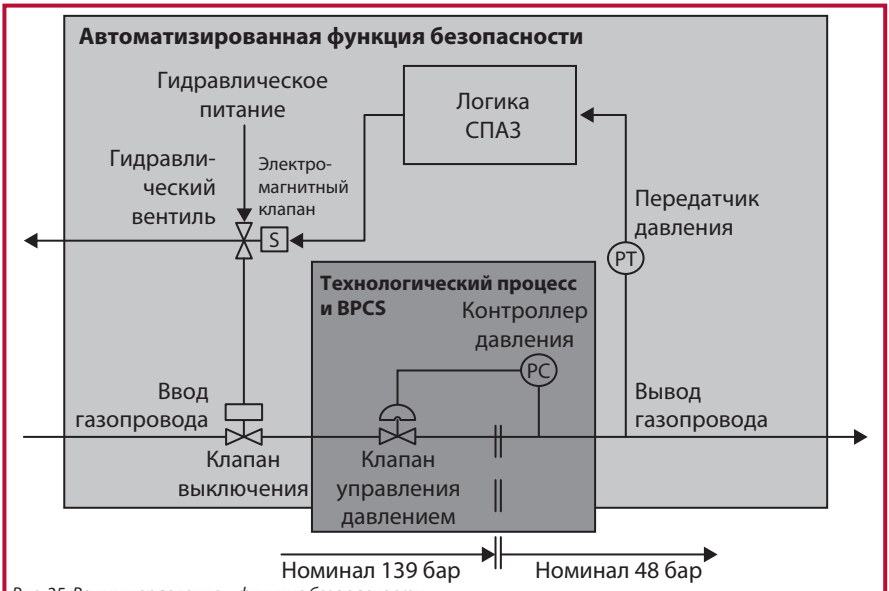


Рис. 25. Режим управления – функция безопасности

Вот пример расчета функции безопасности с управляемым режимом работы. Основные характеристики функции безопасности с управляемым режимом работы:

- автономность по отношению к процессу;
- отказ функции приводит к снижению безопасности, но не создает опасность;
- необходимая частота срабатывания низкая – менее 1 раза в год.

Функции безопасности с управляемым режимом работы включают системы останова технологического процесса (PSD), системы аварийного останова (СПАЗ) и отказоустойчивые системы защиты трубопроводов от повышенного давления (HIPPS).

Датчик давления (PT), как часть функции безопасности, обеспечивает непрерывный контроль давления, но это не мешает ему одновременно быть и компонентом функции безопасности с управляемым режимом работы. Термин «управляемый режим» отражает периодичность активации, т.е. периодичность скачков давления.

6.6. Пример функции безопасности с непрерывным режимом работы

На рис. 26 представлен пример функции безопасности с непрерывным режимом работы.

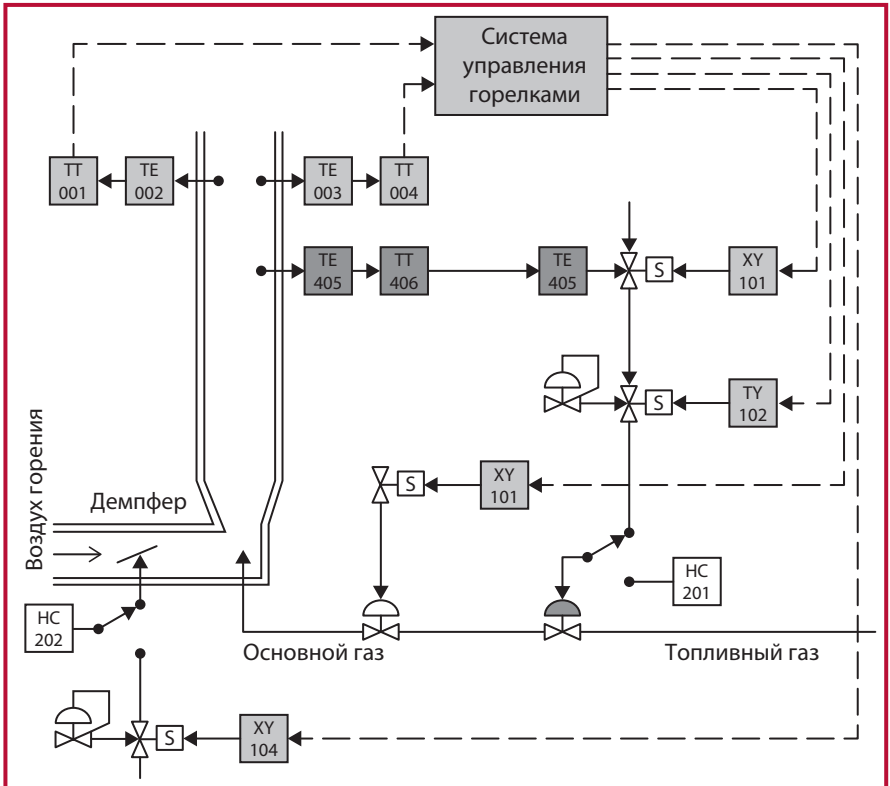


Рис. 26. Функция безопасности непрерывного режима

Это пример типичной системы управления работой котла. Система контролирует подачу топлива и воздуха в камеру сгорания и следит за пламенем, используя пламенные детекторы.

В случае исчезновения пламени система управления перекрывает подачу газа, чтобы предотвратить его скопление и возможность взрыва. Кроме того, перед розжигом камера сгорания также продувается с целью удаления газа, который мог в ней скопиться из-за утечки в клапанах или неисправности контрольно-измерительной аппаратуры.

Таким образом, система управления обеспечивает безопасный запуск, продувку, а также следит за работой в процессе горения. В данном примере система управления и связанные с ней датчики и клапаны образуют функцию безопасности с непрерывным режимом работы.

Основные характеристики функции безопасности с непрерывным режимом работы:

- реализация некоторых функций управления;
- отказ функции обычно приводит к созданию опасной ситуации;
- необходимая частота срабатывания высокая – более 1 раза в год или даже непрерывно.

Функции безопасности с непрерывным режимом работы, как правило, представлены системами управления работой котлов и турбин.

6.7. Требуемые уровни полноты безопасности (SIL) для функций с управляемым режимом работы

В стандарте IEC 61511-1 (9.2.4) целевые показатели PFD распределяются по группам или уровням полноты безопасности (SIL). В приведенном выше примере [6.3] для функции безопасности установлен целевой показатель PFD $<10^{-1}$, что приводит к требованиям уровня полноты безопасности SIL1, как показано в таблице 2.

Режим управления (Средняя вероятность отказа при выполнении проектной функции «по требованию»)	**Уровень полноты безопасности**
$\geq 10^{-5}$, но $<10^{-4}$	4
$\geq 10^{-4}$, но $<10^{-3}$	3
$\geq 10^{-3}$, но $<10^{-2}$	2
$\geq 10^{-2}$, но $<10^{-1}$	1

Таблица 2: Требуемые уровни отказоустойчивости (SIL) для функций с управляемым режимом работы

Примечание. Целевые величины PFD объединяются в уровни (SIL), так как стандарт требует обеспечения определенных уровней надежности техники и мер, применяемых при контроле и предотвращении систематических отказов. Эти требования подробнее рассматриваются в разделе [12.15].

6.8. Требуемые уровни полноты безопасности (SIL) для функций с непрерывным режимом работы

В стандарте IEC 61511-1 (9.2.4) также оговорены требуемые уровни полноты безопасности (SIL) для систем безопасности с непрерывным режимом работы (см. таб. 3).

Непрерывный режим (Вероятность опасного отказа на час, PFH)	**Уровень полноты безопасности**
$\geq 10^{-9}$, но $<10^{-8}$	4
$\geq 10^{-8}$, но $<10^{-7}$	3
$\geq 10^{-7}$, но $<10^{-6}$	2
$\geq 10^{-6}$, но $<10^{-5}$	1

Таблица 3: Требуемые уровни полноты безопасности (SIL) для функций с непрерывным режимом работы

Примечание. Единицей измерения и показателем отказоустойчивости для режима непрерывной работы является «интенсивность отказов» или «вероятность опасного отказа в час» (PFH).

Сноска.

На первый взгляд, целевые величины отказоустойчивости могут показаться более обременительными, чем для систем с управляемым режимом, например, SIL1 (управляемый режим) должен иметь PFD $<10^{-1}$, а SIL1 (непрерывный режим) имеет PFH $<10^{-5}$ отказов в час.

Таблицы сопоставимы, если преобразовать число отказов в час для непрерывного режима в число отказов в год. В году примерно 10^{-4} часов (если точно, то 8760), так что таблицу для непрерывного режима можно откорректировать следующим образом (таб. 4).

Непрерывный режим (Вероятность опасного отказа на год)	**Уровень полноты безопасности**
$\geq 10^{-5}$, но $<10^{-4}$	4
$\geq 10^{-4}$, но $<10^{-3}$	3
$\geq 10^{-3}$, но $<10^{-2}$	2
$\geq 10^{-2}$, но $<10^{-1}$	1

Таблица 4: Требуемые уровни полноты безопасности (SIL) для функций с непрерывным режимом работы

6.9. Режимы работы (управляемый и непрерывный)

Для определения способа работы SIS стандарт IEC 61511-1, 3.2.43 предлагает следующие определения.

Управляемый режим

- режим, в котором заданное действие выполняется в ответ на определенные условия процесса или команду. В случае опасного отказа функции автоматизированной защиты (SIF) потенциальная опасность возникнет только при отказе основной системы управления процессом (BPCS).

Непрерывный режим

- в случае опасного отказа функции автоматизированной защиты (SIF) потенциальная опасность возникнет без последующего отказа, если приняты меры по его предотвращению.

Практический способ определения, является ли функция безопасности полной или допускающей управляемый режим работы, – это определить значимую метрику или показатель надежности.

Например, подушки безопасности в автомобиле представляют собой ценную функцию безопасности и мне, как водителю, интересна вероятность отказа по требованию, которая бы подтвердила, что функция приемлема как функция с управляемым режимом работы. Учитывая изложенное в разделе [6.5], основные характеристики функции безопасности с управляемым режимом работы следующие:

- автономность по отношению к процессу;
- отказ функции приводит к снижению безопасности, но не создает опасность.

Таким образом, таблица 2 подтверждает, что целевой показатель функции с управляемым режимом работы – это вероятность отказа по требованию.

Для тормозной системы автомобиля, наоборот, значимой метрикой является интенсивность отказов или число отказов в час. Как водителю, мне интересно знать интенсивность отказов функции безопасности, поэтому это хороший признак, указывающий на функцию с непрерывным режимом работы.

Основные характеристики функции безопасности с непрерывным режимом работы:

- реализация некоторых функций управления (в данном случае – торможение);
- отказ функции обычно приводит к созданию опасной ситуации (в данном случае – потеря управления).

Таблица 3 подтверждает, что целевой показатель функции с непрерывным режимом работы – это число отказов в час.

6.10. Функции безопасности с управляемым режимом

6.10.1. Пример

Вопрос: В технологической зоне люди находятся в течение 2 часов в день. Избыток давления приводит к утечке газа и по оценкам 1 из 10 утечек газа приводит к взрыву, в результате которого гибнет оператор.

Анализ показывает, что случаи избыточного давления имеют место каждые 5 лет (т.е. 0,2 раза в год).

Допустим, максимальная приемлемая периодичность опасности (гибель оператора от взрыва) составляет 10^{-4} раз в год.

Каким будет требуемое значение PFD для SIS?

Ответ: Частота несчастных случаев со смертельным исходом:

= 0,2 (раза в год) x 2/24 x 1/10
= 1,67 x 10^{-3} раз в год.

Следовательно, система безопасности должна иметь вероятность отказа по требованию:

= 10^{-4} раз в год/1,67 x 10^{-3} раз в год
= 6,0 x 10^{-2}, что соответствует уровню SIL1.

Это пример автоматизированной системы безопасности с управляемым режимом работы, поскольку она активируется с периодичностью, определяемой интенсивностью отказов контролируемого оборудования.

Мы можем убедиться, что результат фактически является показателем PFD, так как это частное коэффициентов, представляющее собой безразмерную величину – вероятность.

6.11. Функции безопасности с непрерывным режимом

На рис. 27 представлен упрощенный пример функции безопасности с непрерывным режимом работы. Химическое вещество в котле нагревается электрическим элементом, работа которого контролируется датчиком температуры.

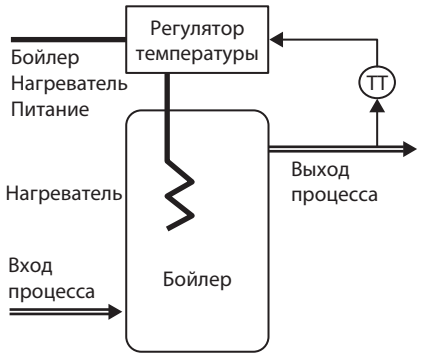


Рис. 27. Функция безопасности непрерывного режима

Допустим, что перегрев котла приводит к разрыву, утечке химического вещества и последующему возгоранию с вероятностью гибели персонала. Это явный риск, который следует предотвратить. В таком примере интенсивность отказов во всем технологическом процессе не должна превышать максимально приемлемый уровень риска для данной опасности.

6.11.1. Пример

Вопрос: Допустим, что отказ котла приводит к перегреву и пожару, а 1 из 400 отказов приводит к смерти. Допустим, максимальная приемлемая периодичность гибели составляет 10^{-5} раз в год (гибель третьих лиц).

Какой будет максимально приемлемая интенсивность отказов котла?

Ответ: Поскольку 1 из 400 отказов должен иметь вероятность, меньшую или равную максимально приемлемому уровню риска, можно сказать, что:

$$10^{-5} \text{ раз в год} \geq \lambda_B \times 1/400$$

где λ_B – интенсивность отказов котла.

Таким образом,

$$\lambda_B = 400 \times 10^{-5} \text{ раз в год}$$
$$= 4{,}0 \times 10^{-3} \text{ раз в год, что соответствует уровню SIL2.}$$

В данном примере системы безопасности с непрерывным режимом работы рассматривается система, которая постоянно находится в условиях риска, т.е. используется непрерывно. Котел может отказать в 400 раз чаще, чем максимальная приемлемая интенсивность отказов, так как лишь 1 из 400 отказов может привести к гибели.

В этом примере нам необходимо разработать и создать процесс, включающий котел, нагревательный элемент и датчик температуры, в соответствии с требованиями УПБ SIL2, при этом интенсивность отказов должна быть ниже $4{,}0 \times 10^{-3}$ раз в год. Это довольно сложная задача, но есть и другой способ.

6.11.2. Пример

Допустим, мы создали процесс с котлом и вычислили интенсивность отказов, равную $5{,}0 \times 10^{-2}$ раз в год, что превышает требуемую величину $4{,}0 \times 10^{-3}$ раза в год.

Если это так, и 1 из 400 отказов приводит к гибели, то частота несчастных случаев будет следующей:

$$= 5{,}0 \times 10^{-2} \text{ (раз в год),} 1/400$$
$$= 1{,}25 \times 10^{-4} \text{ раз}$$

что превышает максимальную приемлемую интенсивность в 10^{-5} раз в год (гибель третьих лиц).

Альтернативный подход может быть основан на допуске отказа котла при такой высокой интенсивности отказов и разработке функции защиты для снижения частоты смертных случаев до максимально приемлемого уровня (рис. 28).

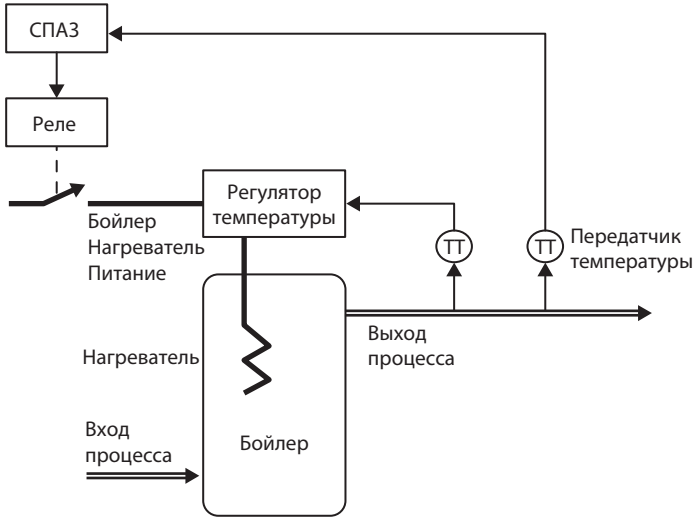


Рис. 28. Режим управления – функция безопасности

При такой конфигурации предусмотрен второй независимый датчик температуры для измерения температуры на выходе, используемый для выключения в случае отказа процесса питания нагревательного элемента посредством системы аварийного останова.

Можно сказать, что

$$10^{-5} \text{ раз в год} \geq \lambda_B \times PFD_T$$

где λ_B – интенсивность отказов котла, $1{,}25 \times 10^{-4}$ раз в год, а PFD_T – вероятность отказа по требованию для отдельного срабатывания.

Таким образом,

$$PFD_T \leq 10^{-5} \text{ раз в год} / 1{,}25 \times 10^{-4} \text{ раз в год}$$
$$PFD_T \leq 0{,}08$$

что соответствует УПБ SIL1 функции безопасности с управляемым режимом работы.

Примечание. Эти два примера позволяют спроектировать систему котла и оборудования в соответствии с УПБ SIL2 или же допустить отказ в работе системы котла при наличии функции защиты УПБ SIL1 с управляемым режимом работы. Оба варианта удовлетворяют требованиям в отношении максимально приемлемого риска, но разработка небольшой функции защиты УПБ SIL1 с управляемым режимом работы экономически выгоднее, чем разработка системы защиты УПБ SIL2.

7. Диаграммы риска

7.1. Введение

В разделах [6.10] и [6.11] представлены способы оценки требований в SIL методом расчета, однако в условиях множества опасностей удобнее выполнять анализ с использованием диаграммы риска. Метод построения диаграммы риска позволяет быстро произвести оценку сразу ряда опасностей.

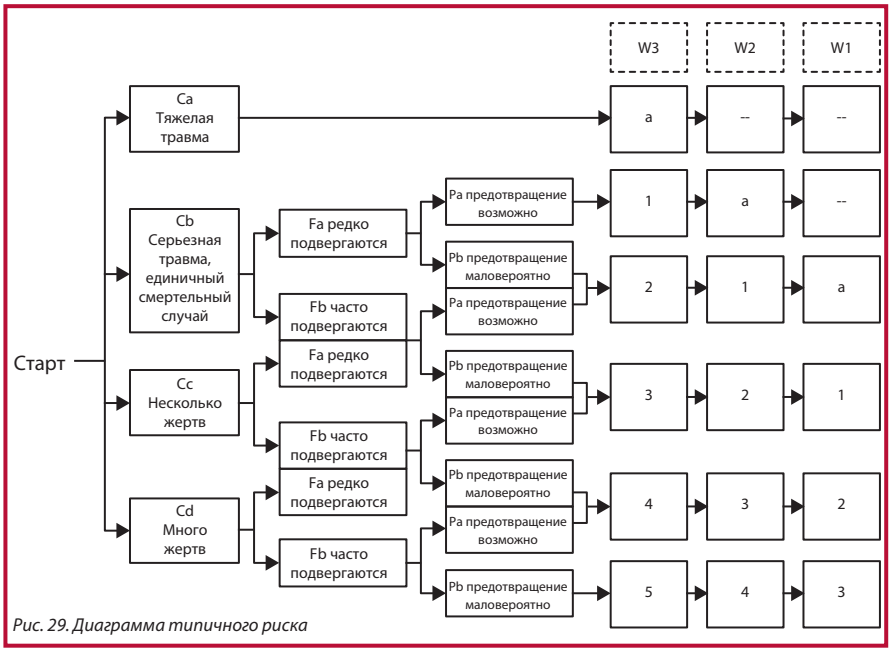


Рис. 29. Диаграмма типичного риска

Для начала определяются последствия опасности – Ca, Cb, Cc или Cd.

Затем определяется периодичность или концентрация риска для лица, наиболее подверженного опасности, а также делается различие между редкой подверженностью (Fa) и частой подверженность (Fb). Как правило, если вероятность того, что лицо, в наибольшей степени подверженное риску, попадет в эпицентр опасности, составляет 10% или меньше, то подверженность считается редкой. В противном случае подверженность считается высокой.

Если из диаграммы следует, что есть вероятность того, что лицо, подверженное риску, сможет избежать опасности, например, покинув опасное место, получив предварительное уведомление об опасности или воспользовавшись средствами

защиты, то можно утверждать, что опасности можно избежать, и такой вариант можно принять как рабочий. В противном случае следует допустить, что избежание опасности маловероятно, и принять позицию из области справа от диаграммы риска.

Наконец, необходимо принять вероятность опасности, выбрав соответствующий столбец – W3 (относительно высокая вероятность), W2 (незначительная вероятность) или W1 (низкая вероятность). В точке пересечения строки и столбца указан требуемый УПБ.

7.2. Пример

Для примера допустим, что емкость для хранения бензина может перелиться или выпустить пары содержимого, которые могут воспламениться и привести к катастрофе. Мы оценили периодичность заливки и приняли решение, что вероятность опасности находится на уровне W1 (низкая вероятность). У работников предприятия нет возможности избежать опасности, если она возникнет. Персонал находится на объекте редко, только когда проводится техническое обслуживание, как правило, менее 1 часа в сутки. На рис. 30 показано, как использовать диаграмму риска для достижения УПБ SIL1.

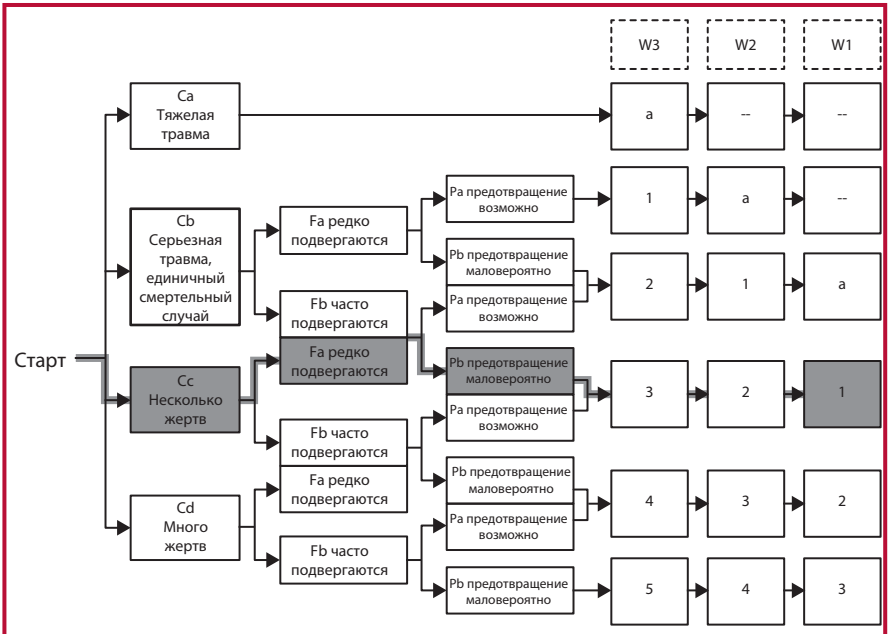


Рис. 30. Пример с использованием графа риска

В данном примере функция безопасности может быть представлена датчиком высокого уровня, по сигналу которого перекрывается впускной клапан. Это будет уровень полноты безопасности SIL1.

Однако общая диаграмма риска может быть субъективной и зависеть от вариаций в интерпретации параметров риска. Следовательно, возможны несогласованные результаты, которые могут привести к пессимистической оценке целей УПБ.

На данной диаграмме риска некоторые целевые уровни SIL отмечены буквами «a» и «b». Термины «SILa» и «SILb» иногда используются в промышленности, хоть и не фигурируют в стандарте. Термин SILa обычно предполагает, что требуется некоторое снижение уровня риска, но коэффициент снижения риска не должен быть таким большим, как для уровня SIL1. Иными словами, требуется PFD в пределах от 1 (без снижения уровня риска) до 0,1 (SIL1). Следует заметить, что некоторые организации используют SILa в значении SIL1.

Величина SILb показана немного выше, чем SIL4. В общем, если требуется уровень SIL4, рекомендуется пересмотреть процесс, так как он определенно слишком опасен. А уровень SILb еще опаснее.

7.3. Пример

На рис. 31 представлен пример диаграммы риска, подобной используемой в непрерывных производствах, на которой видны некоторые потенциальные проблемы, связанные с интерпретацией параметров риска.

Рис. 31. Диаграмма риска в перерабатывающей промышленности

Принцип использования тот же, что и у диаграммы риска, представленной на рис. 29, но в этом случае имеются некоторые указания по оценке рабочего цикла.

Если, например, опасность может стать причиной нескольких жертв при редкой подверженности и вероятности в 0,05/год, то это интенсивность срабатывания защиты в пределах от «низкой» до «средней», и требуется принятие решения о выборе правильного столбца. Применение консервативного подхода приведет к выбору УПБ SIL3 (рис. 32).

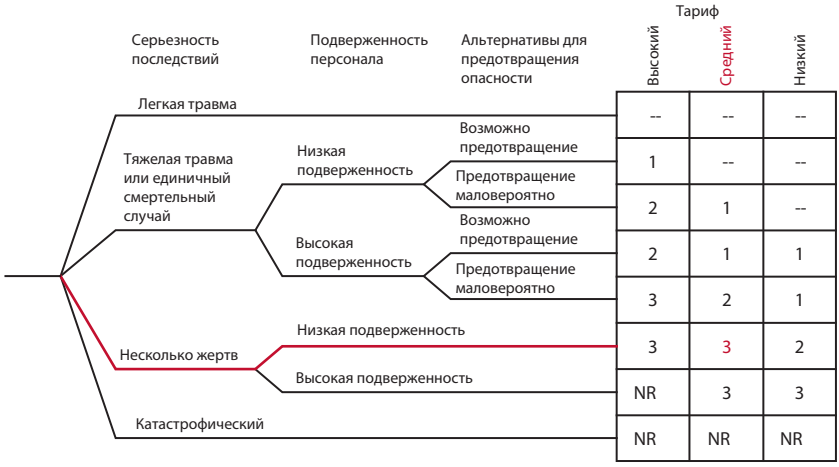


Рис. 32. Пример с использованием графа риска

Более смелая интерпретация приведет к выбору УПБ SIL2.

7.4. Пример

На рис. 33 представлен пример типичной таблицы рисков. В столбцах P, A, E и R приведены описания возможных последствий опасностей, периодичности и описания вероятности, а на пересечениях столбцов и строк указаны целевые УПБ.

P Персонал	A Ресурс	E Среда	R Репутация	<0,01/г A В отрасли неизвестно	<0,05/г B Бывало в отрасли	<0,25/г C Бывало в компании	>2/г D Бывает несколько раз в год в компании	>2/г E Бывает несколько раз в год на предприятии
Без травм	Без ущерба	Без эффекта	Без эффекта					(SIL1)
Легкая травма (<1/г)	Легкий ущерб (менее 10 тыс. долларов США)	Легкий эффект	Легкое воздействие				(SIL1)	SIL1
Легкая травма (<1E-01/г)	Незначительный ущерб (менее 100 тыс. долларов США)	Легкий эффект	Легкое воздействие			(SIL1)	SIL1	SIL2
Тяжелая травма (<1E-02/г)	Крупный ущерб (менее 500 тыс. долларов США)	Локализованный эффект	Значительное воздействие		(SIL1)	SIL1	SIL2	SIL3
Единичный смертельный случай (<1E-03/г)	Крупный ущерб (менее 10 млн долларов США)	Значительный эффект	Эффект национального масштаба	(SIL1)	SIL1	SIL2	SIL3	Нет данных
Несколько жертв (<1E-04/г)	Широкий ущерб (более 10 млн долларов США)	Массированный эффект	Международный эффект	SIL1	SIL2	SIL3	Нет данных	Нет данных

Рис. 33. Пример с использованием матрицы рисков

Это простой и удобный подход, но возможны проблемы, если не принять меры предосторожности.

А. Периодичности должны быть не только оценены количественно с учетом описаний, но и должны привести к выбору верных УПБ.

Б. Оценка «Неизвестно в отрасли» может быть дана по результатам рассмотрения, допустим, 5000 заводов, работающих в течение 20 лет, что даст периодичность около $<10^{-5}$/год, но не $<10^{-2}$/год, как показано. При максимально приемлемом риске $<10^{-4}$/год это приведет к отсутствию целевого SIL.

В. Максимально приемлемая периодичность риска должна быть соответствующей. Значение $<10^{-3}$/год для одного несчастного случая слишком высоко и приведет к слишком оптимистичной оценке целевого уровня SIL и неадекватному снижению риска.

Г. Целевые величины SIL увеличиваются от строки к строке и от столбца к столбцу, как показано на рис. 33, что соответствует увеличению значений периодичности от столбца к столбцу на порядок.

Д. Целевое значение УПБ (SIL1) означает, что требуется снижение риска, но побочных последствий нет. Если нет опасности, то защита не требуется.

Е. Наконец, для коммерческих категорий периодичность ущерба для имущества может быть реалистичной и согласованной с затратами на реализацию необходимого уровня SIF.

Таблица рисков, таким образом, нуждается в корректировке, как предлагается на рис. 34.

П Персонал	Р Ресурс	С Среда	РП Репутация	<1E-04/г	<1E-03/г	<1E-02/г	>0,1/г	>0,1/г
				A	B	C	D	E
				В отрасли неизвестно	Бывало в отрасли	Бывало в компании	Бывает несколько раз в год в компании	Бывает несколько раз в год на предприятии
Без травм	Без ущерба	Без эффекта	Без эффекта					
Легкая травма (<0,1/г)	Легкий ущерб (менее 10 тысяч долларов США)	Легкий эффект	Легкое воздействие				(SIL1)	SIL1
Легкая травма (<1E-02/г)	Незначительный ущерб (менее 100 тысяч долларов США)	Незначительный эффект	Незначительное воздействие			(SIL1)	SIL1	SIL2
Тяжелая травма (<1E-03/г)	Крупный ущерб (менее 500 тысяч долларов США)	Локализованный эффект	Значительное воздействие		(SIL1)	SIL1	SIL2	SIL3
Единичный смертельный случай (<1E-04/г)	Крупный ущерб (менее 10 млн долларов США)	Значительный эффект	Эффект национального масштаба	(SIL1)	SIL1	SIL2	SIL3	Нет данных
Несколько жертв (<1E-05/г)	Широкий ущерб (более 10 млн долларов США)	Массированный эффект	Международный эффект	SIL1	SIL2	SIL3	Нет данных	Нет данных

Рис. 34. Калибровка матрицы рисков

7.5. Обзор

Диаграммы и таблицы рисков могут быть очень полезны, особенно для первичной оценки ситуации и быстрого отбора высших уровней УПБ, т.е. уровня SIL2 и выше. Однако требуется точная корректировка таблицы для предотвращения ошибочных результатов из-за неочевидных трудностей.

8. Анализ уровня защиты (Layer of Protection Analysis, LOPA)

8.1. Введение

Анализ уровня защиты (LOPA) – это структурированный метод расчета целевых уровней снижения риска (и SIL). Анализ LOPA выполняется аналогично анализу HAZOP.

Потенциальные опасности обычно определяются с помощью процедуры HAZOP [3] и вносятся в таблицы LOPA, создавая прослеживаемую связь между двумя анализами – от идентификации опасности до требований в отношении снижения уровня риска и целевого уровня УПБ. Анализ LOPA может быть дополнением к HAZOP, расширяющим возможности оценки.

8.2. Рабочая группа LOPA

Очень важно, чтобы в рабочую группу LOPA входили лица, обладающие достаточными знаниями и опытом в рассматриваемых вопросах. Как правило, рабочая группа LOPA имеет следующий состав:

Название	**Роль**
Председатель	Объясняет процесс LOPA, направляет обсуждение и продвигает LOPA. Специалист, имеющий опыт в LOPA, но непосредственно не вовлеченный в разработку, для обеспечения аккуратного следования методу.
Секретарь	Записывает обсуждение на совещании LOPA и выполняет анализ целей SIL в реальном времени. Записывает рекомендации или действия.
Инженер-технолог	Как правило, инженер, ответственный за принципиальную схему технологических процессов и разработку схемы трубной обвязки и контрольно-измерительных приборов (Piping and Instrumentation Diagrams, P&IDs).
Пользователь/оператор	Вносит рекомендации по использованию и работоспособности процесса, по воздействию отклонений.
Специалист по КИП	Специалист с соответствующими техническими знаниями по контрольно-измерительным приборам.
Специалист техобслуживания	Специалист, занятый в техническом обслуживании процесса.
Представитель проектной группы	Вносит рекомендации по подробностям проекта или дает необходимую информацию.

8.3. Информация, используемая в анализе LOPA

Члены рабочей группы LOPA должны изучить следующее:

- схемы трубопроводов и КИПиА предприятия;
- описания процессов и принципиальные схемы;
- существующие процедуры эксплуатации и технического обслуживания;
- технологические схемы предприятия.

8.4. Определение требуемого уровня полноты безопасности (SIL)

Метод LOPA, как описано в документе «Анализ уровня безопасности» Центра безопасности химических процессов Американского института инженеров-химиков (2001 г.) [19.4], может использоваться для определения целевых уровней УПБ.

Анализ LOPA учитывает опасности, определенные другими способами, например, методом HAZOP, но анализ LOPA может выполняться в ходе совещания HAZOP для оценки каждой опасности по мере обнаружения.

Рабочая группа LOPA рассматривает каждую выявленную опасность и документирует первопричины и уровни безопасности, предотвращающие или смягчающие риск. Затем определяется общее снижение риска и потребность в дальнейшем его снижении. Если требуется дополнительная защита в виде SIS, методика позволяет определить соответствующий УПБ и PFD.

Процесс LOPA фиксируется в рабочих листах LOPA, которые позволяют количественно оценить первопричины и их периодичности, а также степень снижения рисков, обеспечиваемую каждым отдельным заявленным уровнем защиты. Заголовки рабочего листа рассматриваются в последующих разделах и в примере анализа LOPA [8.5].

8.5. Пример анализа LOPA

Если вернуться к примеру с емкостью под давлением [3.7], то можно импортировать в рабочий лист LOPA выявленные опасности и проанализировать риски.

8.6. Рабочие листы LOPA

8.6.1. Введение

В следующих разделах рассматриваются заголовки рабочих листов и квалификационные требования.

В этой главе приведен пример рабочего листа LOPA.

8.6.2. Ид. опасности/ссылка

Идентификатор для каждой опасности. В приведенном примере рассматривается опасность **1.10: Высокое давление в емкости.** Ссылка обеспечивает обратную прослеживаемость к более ранним исследованиям, в данном случае – HAZOP, а по мере развития проекта – к назначению SIF и проверке УПБ.

8.6.3. Описание события (опасности)

Описание выявленной потенциальной опасности.

8.6.4. Последствия

Описание последствий опасности. В примере анализа LOPA последствия опасности оцениваются с точки зрения безопасности персонала, а также риска для окружающей среды и имущества, т.е. коммерческого риска.

8.6.5. Категория серьезности (Sev Cat)

Серьезность документированных последствий определяется по таблице «Классификация рисков» (таб. 5).

8.6.6. Максимально приемлемый риск (MTR)

Максимально приемлемая периодичность возникновения последствий опасности для персонала, окружающей среды и репутации организации, а также коммерческий ущерб имуществу, бесперебойности поставок и упущенная прибыль. Максимально приемлемые периодичности должны соответствовать указаниям Управления по вопросам охраны здоровья, техники безопасности и охраны труда (HSE), например, R2P2 [19.3].

Однако максимально приемлемые периодичности последствий для окружающей среды, репутации и коммерческих рисков должны определяться компанией самостоятельно. Типовые значения, которые могут быть использованы в таблице 5.

Последствия	Серье з. Кат.	Частота цели по риску (в год)	Описание последствий	
			На производстве	**Вне производства**
Люди (безопасность)	P1	1,0E-01	Лечение сотрудника или травмы с ограничением трудоспособности	Лечение или травмы с ограничением трудоспособности (третьи лица)
	P2	1,0E-02	Происшествие с потерей рабочего времени сотрудника (LTA) без необратимых эффектов	LTA (третьи лица) без необратимых эффектов
	P3	1,0E-03	Необратимое воздействие на сотрудника	Без необратимого воздействия
	P4	1,0E-04	Гибель 1 сотрудника и/или несколько пожизненных инвалидностей	Необратимое воздействие (третье лицо)
	P5	1,0E-05	Гибель нескольких сотрудников (2–10)	Гибель одного третьего лица и/или много пожизненных инвалидностей
	P6	1,0E-06	Гибель многих сотрудников (более 10)	Гибель нескольких третьих лиц
Среда	E1	1,0E-01	Уведомлять власти не требуется, но необходима санитарная очистка	Уведомлять власти не требуется, но необходима небольшая санитарная очистка (например, разлив 1–100 л на развернутом оборудовании)
	E2	1,0E-02	Необходимо уведомить власти, но экологические последствия отсутствуют.	Необходимо уведомить власти, но экологические последствия отсутствуют. (например, разлив > 100 л на участке клиента с обваловкой/отсекателями)
	E3	1,0E-03	Умеренное загрязнение в пределах производства	Умеренное загрязнение, требующее работ по рекультивации (например, утечка шлейфа с площадки при сохранении ее функционально-сти)
	E4	1,0E-04	Значительное загрязнение в пределах производства. Эвакуация людей/временное закрытие ИЛИ значительное загрязнение вне производства. Эвакуация людей. (например, разлив вне площадки на заправочной станции)	Значительное загрязнение вне производства. Эвакуация людей. (например, разлив вне площадки на заправочной станции)
	E5	1,0E-05	см. последствия вне производства	Серьезное загрязнение с обратимыми экологическими последствиями вне производства. (например, крупная авария с ущербом для окружающей среды)
	E6	1,0E-06	см. последствия вне производства	Крупномасштабное и долговременное загрязнение вне производства и/или обширная гибель водной флоры и фауны (например, потеря груза судна)
Стоимость	C1	1,0E-01	Урон < 10 тыс. фунтов стерлингов	Нет данных
	C2	1,0E-02	Урон 10 тыс. < 100 тыс. фунтов стерлингов	Нет данных
	C3	1,0E-03	Урон 100 тыс. < 1 млн фунтов стерлингов	Нет данных
	C4	1,0E-04	Урон 1 млн < 10 млн фунтов стерлингов	Нет данных
	C5	1,0E-05	Урон 10 < 100 млн фунтов стерлингов	Нет данных
	C6	1,0E-06	Урон ≥ 100 млн фунтов стерлингов	Нет данных
Репутация	R1	1,0E-01	Без огласки. Местный масштаб.	Нет данных
	R2	1,0E-02	Местная пресса	Нет данных
	R3	1,0E-03	Национальная пресса	Нет данных
	R4	1,0E-04	Национальное телевидение	Нет данных
	R5	1,0E-05	Международная пресса	Нет данных
	R6	1,0E-06	Международное телевидение	Нет данных

Таблица 5: Критерии риска

Следует заметить, что в применении к безопасности персонала это отражает периодичность подверженности одного работника риску.

8.6.7. Первопричина

Список выявленных причин опасности. Эти причины определяются в ходе совещания LOPA на основании личного опыта участников. Для рассматриваемой в примере опасности – повышенного давления – первопричины, периодичности и последствия указаны в таблице 6. Анализ LOPA должен обеспечить видимость всех данных, представив все первопричины и периодичности со ссылками на источники данных.

Первопричина	**Вероятность возникновения (в год)**	**Источник данных**
DCS не удается проконтролировать давление.	1,65E-02	Exida 2007, эл-т x.x.x
Датчик жидкости LL101 отказывает и сообщает низкий уровень.	1,10E-02	Exida 2007, эл-т x.x.x
TT100 отказывает и сообщает низкую температуру.	2,68E-03	Exida 2007, эл-т x.x.x
PT102 отказывает и сообщает низкое давление.	8,58E-04	Exida 2007, эл-т x.x.x
FCV102 экспорта газа отказывает в закрытом положении.	1,01E-02	Oreda 2002, эл-т x.x.x
FCV100 топливного газа отказывает в открытом положении.	1,01E-02	Oreda 2002, эл-т x.x.x
XV102 экспорта жидкости отказывает в закрытом положении.	2,89E-03	Oreda 2002, эл-т x.x.x
XV102 импорта жидкости отказывает в открытом положении.	2,89E-03	Oreda 2002, эл-т x.x.x

Таблица 6: Первопричины и периодичности событий

8.6.8. Вероятность возникновения (/год), столбец [a]

Количественная оценка вероятности первопричин. Значение определяется на основании личного опыта и доступных исторических данных. Также возможно вычисление на основании данных об отказах из доступных источников [14.6].

Первопричины и их периодичность для использованного примера представлены в таблице 6.

Если вероятности первопричин зависят от человеческого фактора, например, ошибки оператора, оценка может быть затруднена. Один из методов заключается в оценке

периодичности возникновения возможностей ошибки оператора с последующим умножением на вероятность опасного исхода.

Например, допустим, что действия оператора (закрытие клапана) могут быть причиной повышения давления в трубопроводе. Обычно, перед тем как закрыть главный клапан, оператор открывает перепускной клапан. Делает он это ежемесячно. Базовая периодичность λ_B для данного действия составит 12 раз в год (один раз в месяц).

Можно допустить, что оператор хорошо обучен, задача привычная и оператор спокоен, поэтому можно оценить вероятность ошибки оператора, P_E, например, неоткрытия сначала перепускного клапана, как 1%. Периодичность первопричины, λ_{INIT}, можно оценить как:

$$\lambda_{INIT} = \lambda_B \times P_E$$
$$\lambda_{INIT} = 12 \times 1\%/\text{год}$$
$$\lambda_{INIT} = 0{,}12/\text{год}$$

Обычно можно проверить надежность данных, попросив участников анализа LOPA подтвердить известность рассматриваемого случая или разумность оценки периодичности. Периодичность в 0,12/год соответствует одной ошибке в 8 лет.

8.6.9. Условные модификаторы

Распределение утечек, столбец [b]

В данном примере установленные последствия опасности превышения давления могут иметь место, если повышенное давление приведет к разрыву емкости. Большинство случаев превышения давления не приведут к разливу содержимого или утечке во фланцевых соединениях. В данном примере рабочая группа LOPA оценила вероятность последствий первопричины в 10%.

Вероятность возгорания, столбец [c]

Для предполагаемых последствий для безопасности и коммерческой деятельности предприятия мы позволим газу воспламениться. В нашем примере мы ссылаемся на исследование пожаробезопасности, подтверждающее вероятность возгорания на 75% в описанных условиях повреждения емкости. Таким образом, мы можем использовать коэффициент 0,75 в качестве модификатора условий, снижающего периодичность возникновения первопричин.

Что касается последствий для окружающей среды, снижение риска не подтверждается, так как для последствий пожар не является обязательным условием.

Общий проект, столбец [d]

Пример общего проекта – это труба в обшивке, которая обеспечивает определенную защиту в случае разгерметизации. В рассматриваемом примере общий проект не заявляется, так как нет специальных проектных решений для снижения риска.

8.6.10. Независимые уровни защиты (IPL)

Каждый уровень защиты состоит из комплекта оборудования и/или административных мер в комплексе с другими уровнями защиты.

Уровень защиты, обеспеченный каждый IPL, оценивается по вероятности отказа при выполнении требуемой функции, т.е. PFD – безразмерная величина от 0 до 1. Чем меньше значение PFD, тем больше коэффициент снижения риска, примеряемый в качестве модифицирующего коэффициента при вычислении вероятности первопричины [8.6.8], поэтому, если IPL отсутствует, в ячейку LOPA вносится значение 1.

В данном примере заявленные уровни IPL, указанные в столбцах с [e] по [h], могут быть адаптированы к применению. Представлены типовые IPL.

Основная система управления процессом (BPCS), столбец [e].

Об ответственности можно заявлять, если управляющий контур BPCS (РСУ везде изменить) предотвращает опасность, возникшую из-за первопричины. В примере для некоторых из первопричин, например, отказ при открытии впускного клапана XV102, BPCS (DCS) может предпринять компенсирующее действие, например, открыть выпускной клапан, чтобы предотвратить повышение уровня. Заявлена величина PFD 0,1, которая означает, что DCS предотвратит последствия в 9 из 10 случаев.

PFD 0,1 – это наибольшее снижение риска, которое можно заявить для системы, не отвечающей требованиям УПБ. Из-за того, что РСУ можно регулировать вручную, нет четкого контроля установки точки срабатывания, а режим испытания не такой строгий, как для SIS.

Независимая сигнализация, столбец [f].

Доверять можно сигнализациям, которые независимы от BPCS, сообщают оператору о состоянии системы и используют действия оператора. Доверять следует только сигнализации, которая полностью независима от BPCS и SIF, и только в том случае, если оператор может отреагировать на сигнализацию и предпринять действия для предотвращения опасности процесса в течение безопасного периода.

Для независимой сигнализации можно заявить PFD величиной в 0,1. В данном примере это отсутствует.

8.6.11. Дополнительные способы смягчения риска

Занятость, столбец [g].

Доступ – уровни смягчения риска могут включать занятость, т.е. долю времени, когда оператор подвержен опасности и когда доступ в опасную зону ограничен. В данном примере занятость основана на 8-часовой смене.

Другие меры: столбец [h].

Дополнительные меры по смягчению могут включать:

- физические – уровни смягчения риска в виде физических препятствий развития опасности в случае возникновения первопричины (например, предохранительные клапаны и дамбы);
- действия оператора – доверять можно регулярной инспекции при условии, что оператор действует сообразно обстоятельствам.

В данном примере это отсутствует.

8.6.12. Вероятность события промежуточного уровня

Вероятность события промежуточного уровня определяется путем умножения вероятности первопричины на PFD уровней защиты. Единица измерения – количество событий в год. Общая вероятность события промежуточного уровня указывает на интенсивность запросов к предложенной SIF.

8.6.13. Требуемая величина PFD для SIS

Вычисляется путем сопоставления максимального приемлемого риска λMTR и вероятности события промежуточного уровня или периодичности опасности, λ_{HAZ}.

$$PFD = \lambda_{MTR}/\lambda_{HAZ}$$

8.6.14. Требуемая величина SIL для SIS

Получается из таблицы 7 в соответствии с требуемой величиной PFD для SIS.

УПБ	**Режим управления –** вероятность отказа по требованию	**Непрерывный режим** Количество отказов в час
SIL4	$\geq 10^{-5}$, но $<10^{-4}$	$\geq 10^{-9}$, но $<10^{-8}$
SIL3	$\geq 10^{-4}$, но $<10^{-3}$	$\geq 10^{-8}$, но $<10^{-7}$
SIL2	$\geq 10^{-3}$, но $<10^{-2}$	$\geq 10^{-7}$, но $<10^{-6}$
SIL1	$\geq 10^{-2}$, но $<10^{-1}$	$\geq 10^{-6}$, но $<10^{-5}$

Таблица 7: Требуемая величина PFD для УПБ и интенсивность отказа

Следует заметить, что PFD и интенсивность отказов для каждого УПБ зависит от режима эксплуатации, в котором предполагается использование SIS, и периодичности вызова обращения к SIS [8.6.12].

Ниже приведены рабочие листы LOPA.

№	Описание зоны	Описание события (опасности)	Последствия	Категория серьез-ности	Макс. допусти-мый риск (ежегодно)	Первопричина	Первона-чальная вероятно-сть (ежегодно)	Распреде-ление в зависи-мости от объема утечки	Вероятно-сть воспламе-нения	Проект общего назначен-ия (категория проекта)	Независимые уровни защиты				Вероятность событий промежуто-чного уровня (ежегодно)	Требуется SRS PFD	Требуется SRS SIL	Комментарии/Исходные предположения
											BPCS [DCS]	Независимая сигнализация	Дополнительные предупреждающие меры, например брандмауэры/ эксплуатационные процедуры/ предохранительные клапаны					
							[а]	[б]	[в]	[г]	[д]	[е]	[ж]	[з]				
1.10	Резервуар	Высокое давление приводит к разрыву резервуара и выбросу газа.	Безопасность: Выброс газа воспламеняется от горелки и горячих поверхностей. Возможна гибель двух ремонтников.	P5	1,00E-05	В DCS сбой управления давлением.	1,65E-02	0,10	0,75				0,33		4,13E-04	1,87E-02	SIL1	[а] См. данные по первоначальному событию. [б] Группа LOPA оценивает вероятность крупной утечки (прорыва) в 10%. [в] Исследование пожарной опасности показало вероятность возгорания 75%. [г] Кредитного заявления по деталям конструкции не поступало. [д] Система DCS инициирует основание, но рекламация в систему DCS не поступает. [е] Независимая сигнализация недоступна. Кредитного заявления не поступало. [ж] Область резервуара занята 8 часов в сутки. [з] Без предохранительных клапанов. Кредитного заявления не поступало.
						Отказ PT102, показывает низкое давление	8,58E-04	0,10	0,75				0,33		2,15E-05			См. выше.
						Вход жидкости XV102 нормально закрытый.	2,89E-03	0,10	0,75		0,10		0,33		7,23E-06			См. выше, кроме: [д] DCS может компенсировать отказы входных клапанов. Предположительный PFD = 0,1.
						Вывод газа FCV102 нормально открытый.	1,01E-02	0,10	0,75		0,10		0,33		2,52E-05			См. выше.
						Вывод жидкости XV102 нормально открытый.	2,89E-03	0,10	0,75		0,10		0,33		7,23E-06			См. выше.
						Отказ TT100 показывает низкую температуру	2,68E-03	0,10	0,75		0,10		0,33		6,70E-06			См. выше.
						Топливный газ FCV100 нормально закрытый.	1,01E-02	0,10	0,75		0,10		0,33		2,52E-05			См. выше.
						Отказ уровеня жидкости LL101 показывает низкий уровень.	1,10E-02	0,10	0,75		0,10		0,33		2,74E-05			См. выше.
															5,34E-04			

№	Описание зоны	Описание события (опасности)	Последствия	Категория серьезности	Макс. допустимый риск (ежегодно)	Первопричина	Первоначальная вероятность (ежегодно)	Распределение в зависимости от объема утечки	Вероятность воспламенения	Общего назначения Проект (оценка проекта)	Независимые уровни защиты				Вероятность событий промежуточного уровня (ежегодно)	Требуется SRS PFD	Требуется SRS SIL	Комментарии/Исходные предположения
											BPCS [DCS]	Независимая сигнализация	Дополнительные предупреждающие меры: Заполнение (уровни укомплектованности персоналом)	Дополнительные предупреждающие меры, например брандмауэры/ эксплуатационные процедуры/ предохранительные клапаны				
							[а]	[б]	[в]	[г]	[д]	[е]	[ж]	[з]				
1.10	Резервуар	Высокое давление приводит к разрыву резервуара и выбросу газа.	Экологические: Разрыв резервуара, утечка газа, без воспламенения. Выпуск на месте. Требуется очистка и отчет для властей, экологический ущерб отсутствует.	E2	1,00E-02	В DCS сбой управления давлением.	1,65E-02	0,10							1,65E-03	Нет	Нет	[а] См. данные по первоначальному событию. [б] Группа LOPA оценивает вероятность крупной утечки (прорыва) в 10%. [в] Воспламенение необязательно. Без заявки на снижение риска [г] Не поступало кредитного заявления по деталям конструкции. [д] Система DCS инициирует основание, но рекламация в систему DCS не поступает. [е] Независимая сигнализация недоступна. Кредитного заявления не поступало. [ж] Экологический риск 24 ч/сутки. Без заявки на снижение риска. 8 часов в сутки. [з] Без предохранительных клапанов. Кредитного заявления не поступало.
						Отказ PT102, показывает низкое давление	8,58E-04	0,10							8,58E-05			См. выше.
						Вход жидкости XV102 нормально закрытый.	2,89E-03	0,10			0,10				2,89E-05			См. выше, кроме: [д] DCS может компенсировать отказы входных клапанов. Предположительный PFD = 0,1.
						Вывод газа FCV102 нормально открытый.	1,01E-02	0,10			0,10				1,01E-04			См. выше.
						Вывод жидкости XV102 нормально открытый.	2,89E-03	0,10			0,10				2,89E-05			См. выше.
						Отказ TT100, показывает низкую температуру	2,68E-03	0,10			0,10				2,68E-05			См. выше.
						Топливный газ FCV100 нормально закрытый.	1,01E-02	0,10			0,10				1,01E-04			См. выше.
						Отказ уровеня жидкости LL101 показывает низкий уровень.	1,10E-02	0,10			0,10				1,10E-04			См. выше.
															2,14E-03			

Allen-Bradley

№	Описание зоны	Описание события (опасности)	Последствия	Категория серьезности	Макс. допустимый риск (ежегодно)	Первопричина	Первоначальная вероятность (ежегодно)	Распределение в зависимости от объема утечки	Вероятность воспламенения	Проект общего назначения (категория проекта)	Независимые уровни защиты				Вероятность событий промежуточного уровня (ежегодно)	Требуется SRS PFD	Требуется SRS SIL	Комментарии/Исходные предположения
											BPCS [DCS]	Независимая сигнализация	Дополнительные предупреждающие меры. Заполнение (уровни укомплектованности персоналом)	Дополнительные предупреждающие меры, например бранмауэры/ эксплуатационные процедуры/ предохранительные клапаны				
							[а]	[б]	[в]	[г]	[д]	[е]	[ж]	[з]				
1.10	Резервуар	Высокое давление приводит к разрыву резервуара и выбросу газа.	Коммерческие Прорыв резервуара, утечка газа, возгорание и повреждение ресурса. Повреждение оборудования, требующее замены резервуара приблизительной стоимостью 10 млн и прекращение производства на 1 год	C5	1,00E-05	В DCS сбой управления давлением.	1,65E-02	0,10	0,75						1,24E-03	6,24E-03	SIL2	[а] См. данные по первоначальному событию. [б] Группа LOPA оценивает вероятность крупной утечки (прорыва) в 10%. [в] Исследование пожарной опасности показало вероятность возгорания 75%. [г] Кредитного заявления по деталям конструкции не поступало. [д] Система DCS инициирует основание, но рекламация в систему DCS не поступает. [е] Независимая сигнализация недоступна. Кредитного заявления не поступало. [ж] Область резервуара занята 8 часов в сутки. [з] Без предохранительных клапанов. Кредитного заявления не поступало.
						Отказ PT102, показывает низкое давление	8,58E-04	0,10	0,75						6,44E-05			См. выше.
						Вход жидкости XV102 нормально закрытый.	2,89E-03	0,10	0,75		0,10				2,17E-05			См. выше, кроме: [д] DCS может компенсировать отказы входных клапанов. Предположительный PFD = 0,1.
						Вывод газа FCV102 нормально открытый.	1,01E-02	0,10	0,75		0,10				7,56E-05			См. выше.
						Вывод жидкости XV102 нормально открытый.	2,89E-03	0,10	0,75		0,10				2,17E-05			См. выше.
						Отказ TT100 показывает низкую температуру	2,68E-03	0,10	0,75		0,10				2,01E-05			См. выше.
						Топливный газ FCV100 нормально закрытый.	1,01E-02	0,10	0,75		0,10				7,56E-05			См. выше.
						Отказ уровеня жидкости LL101 показывает низкий уровень.	1,10E-02	0,10	0,75		0,10				8,21E-05			См. выше.
															1,60E-03			

8.6.15. Результаты анализа LOPA

Результаты, представленные в таблице 8, доказывают, что опасность превышения давления имеет последствия, которые можно предотвратить, внедрив систему безопасности УПБ SIL1 SIF с PFD ≤ 1,87E-02. Однако коммерческий риск преобладает и требует применения УПБ SIL2 SIF с PFD ≤ 8,24E-03.

Опасность	**Последствия**	**Цель SIL**	**Цель PFD**
Безопасность	Безопасность: Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала.	SIL1	1,87E-02
Экологические	Экологические: разрушение резервуара, утечка газа, без воспламенения. Утечка на территории производства. Необходимы санитарная очистка и уведомление властей, но экологические последствия отсутствуют.	Нет	Нет
Коммерческие	Коммерческие: разрушение резервуара, утечка газа, воспламенение и ущерб установке. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и потеря производства на 1 год.	SIL2	6,24E-03

Таблица 8: Результаты анализа LOPA

Очень часто доминирующими являются факторы, не связанные с производственной безопасностью. В данном примере опасности постоянно подвергается имущество, в то время как персонал подвергается опасности лишь периодически.

Автоматизированная функция защиты, предполагаемая для защиты от избыточного давления, должна удовлетворять коммерческим требованиям, и эта же функция, таким образом, обеспечит достаточную защиту персонала.

9. Распределение функций безопасности

9.1. Фазы жизненного цикла

На рис. 35 показана фаза применяемого жизненного цикла.

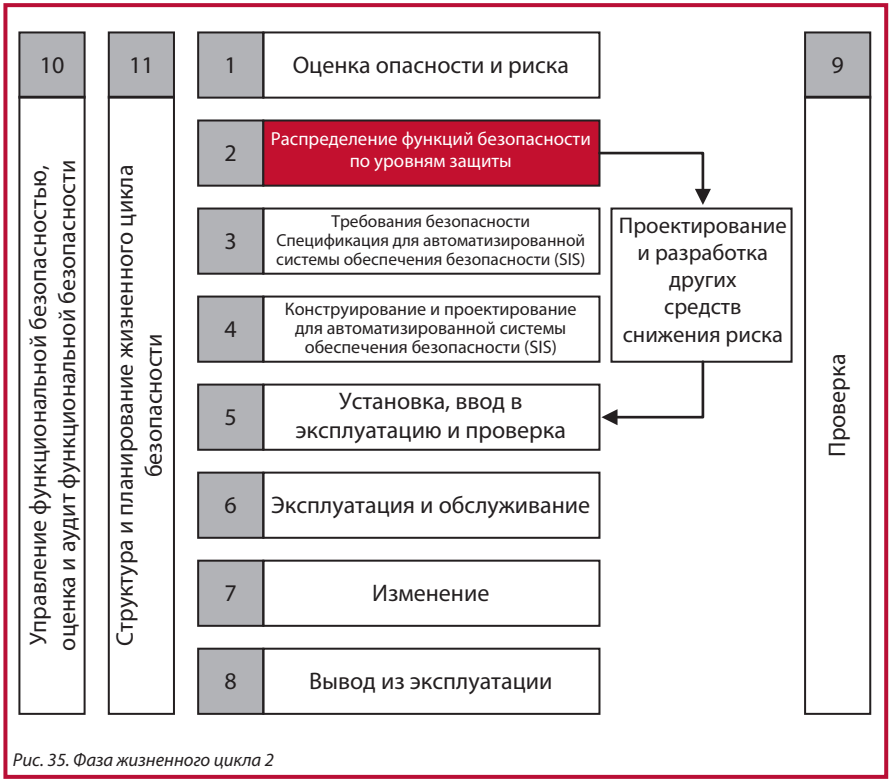


Рис. 35. Фаза жизненного цикла 2

Целью данной фазы, как определено в IEC 61511-1, 9.1, является распределение функций безопасности по уровням защиты.

В качестве входных данных фаза требует описания требований к функциям безопасности и требований к целостности функций безопасности.

В качестве выходных данных от фазы требуется предоставить информацию о распределении общих функций безопасности, заданных значениях частоты отказов и связанных с ними уровнях целостности функций безопасности. Также будут определены допущения, сделанные относительно прочих средств уменьшения риска, управление которыми требуется на всем протяжении жизни процесса/завода.

9.2. Распределение функций безопасности

На примере резервуара сепаратора (3.7.1) были определены следующие требования к функциям SIF и УПБ, таблица 9. Анализ справочного описания опасности 1.10 показан как часть примера анализа LOPA [8.5]. Анализ LOPA будет использоваться для определения целей уровня SIL и целей вероятности PFD для других найденных угроз.

Код HAZOP	Опасность	Последствия	УПБ	Цель PFD
1.01	Высокое давление приводит к разрушению резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процессов на 1 год. Незначительный выброс в окружающую среду.	SIL2	6,24E-03
1.11	Низкое давление приводит к разрушению резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процессов на 1 год. Незначительный выброс в окружающую среду.	Нет	Нет
1.15	Высокая температура приводит к повышению давления, разрушению резервуара и выбросу газа.	Выброс газа воспламеняется на горелках и горячих поверхностях. Возможна гибель двух человек из обслуживающего персонала. Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процессов на 1 год. Незначительный выброс в окружающую среду.	Нет	Нет
1.16	Низкая температура, возможное замерзание (затвердевание) жидкости, разрушение резервуара и утечка из реактора.	Повреждение оборудования, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процесса на 6 месяцев. Выброс в окружающую среду, требующий уведомления.	Нет	Нет
1.20	Высокий уровень в резервуаре может привести к уносу жидкости в вывод газа.	Повреждение оборудования по направлению потока, требующее замены резервуара (примерно 10 млн фунтов стерлингов) и остановки процесса на 6 месяцев.	SIL1	8,10E-02
1.21	Низкий уровень в резервуаре может привести к прорыву газа в вывод жидкости.	Повреждение оборудования по направлению потока, требующее чистки резервуара (примерно 2 млн фунтов стерлингов) и остановки процесса на 6 недель.	SIL1	6,22E-02

Таблица 9. Требования к функции SIF

Вероятность промежуточного события, найденная при помощи анализа LOPA, определила, что все предложенные функции SIF будут рассматриваться как режим управления. Цели SIL1 установлены для высокого и низкого уровней, вследствие чего были предложены следующие функции SIF. Для снижения уровня давления в качестве хорошего конструкторского приема был предусмотрен разгрузочный клапан давления, а также установлена функция SIF, как показано ниже.

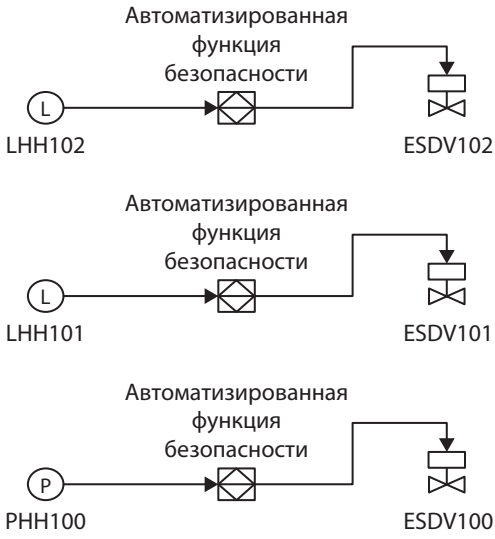


Рис. 35a. Фаза жизненного цикла 2

Отдельные функции SIF вместе формируют общую систему SIS.

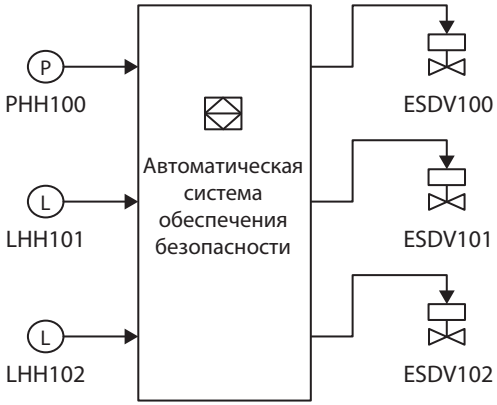


Рис. 35b. Фаза жизненного цикла 2

На следующей схеме представлены размещенные функции SIF.

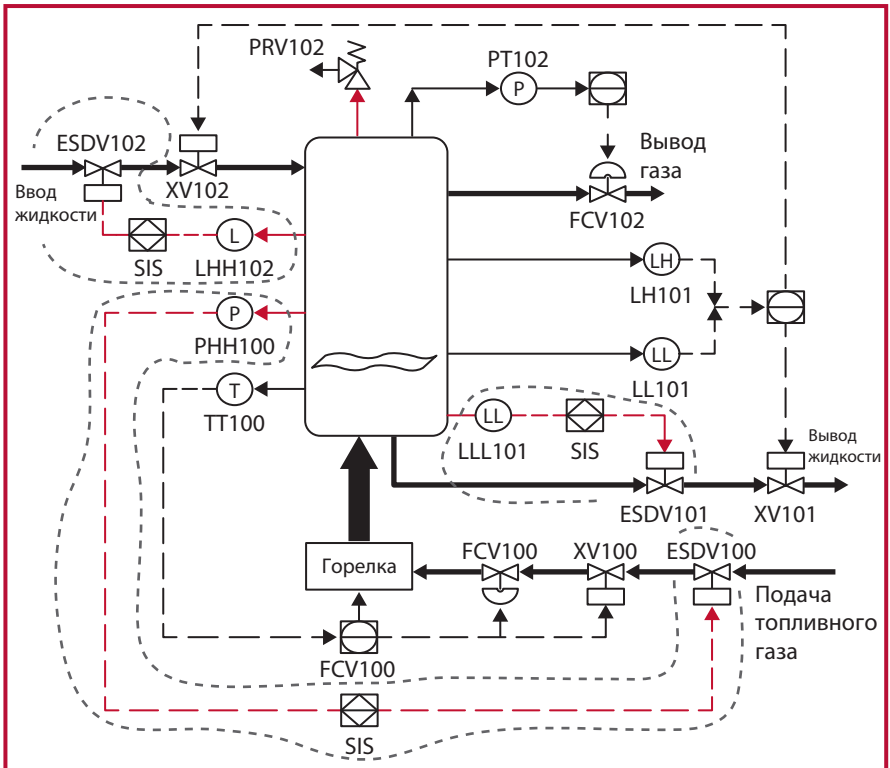


Рис. 35c. Фаза жизненного цикла 2

10. Спецификация требований к безопасности для системы SIS

10.1. Фазы жизненного цикла

На рис. 36 показана фаза применяемого жизненного цикла.

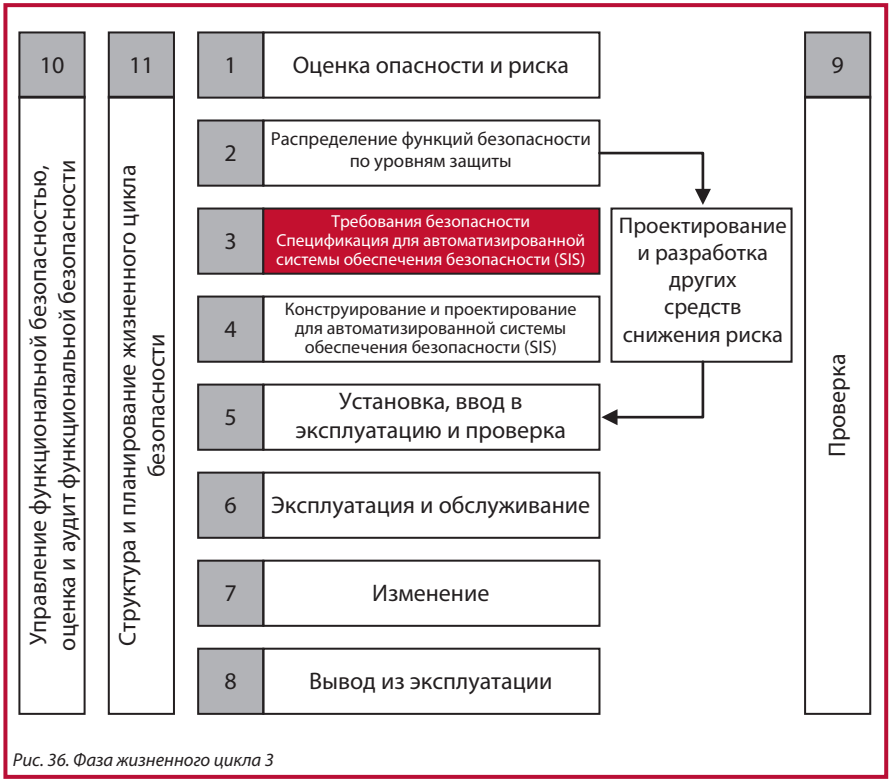


Рис. 36. Фаза жизненного цикла 3

Целью данной фазы, как определено в IEC 61511-1, 10.1, является определение требований для функции SIF.

10.2. Требования к полноте безопасности функции SIF

Уровень SIL каждой функции SIF выбирался в процессе определения SIL с использованием графика рисков, анализа LOPA или матрицы рисков.

Эту информацию необходимо передать команде разработчиков в виде спецификации требований к безопасности (SRS), чтобы гарантировать соответствие конструкции требованиям к полноте безопасности функции SIF в процессе реализации.

Спецификация SRS является основой оценки функции SIF.

10.3. Шаблон для спецификации SRS

Перед началом проектирования необходимо подготовить спецификацию SRS на основе указаний, содержащихся в IEC 61511-1/2, статья 10 и 12. Спецификация SRS включает требования к полноте и функциональным качествам каждой функции SIF и должна содержать достаточную информацию для проектирования и создания системы SIS. Она должна иметь ясный и четкий стиль изложения и структуру, допускать проверку, обслуживание и практическую реализацию и таким образом облегчать понимание со стороны лиц, использующих эту информацию на всех стадиях жизненного цикла.

Спецификация SRS должна содержать положения по следующим пунктам для каждой функции SIF:

- описание функции SIF;
- отказы по общей причине;
- определение безопасного состояния для функции SIF;
- размеры потребностей;
- интервалы контрольных проверок;
- время реакции для приведения процесса в безопасное состояние;
- уровень SIL и режим работы (по требованию или непрерывный);
- измерение технологических показателей и их предельные значения;
- выходные воздействия процесса и критерии успешной операции;
- функциональная связь между входами и выходами;
- требования к ручному выключению;
- подача питания или обесточивание до выключения;
- сброс после выключения;
- максимально допустимое кол-во ложных отключений;
- типы отказа и реакция SIS на отказы;
- запуск и перезапуск SIS;
- интерфейсы между SIS и любой другой системой;
- прикладное ПО;
- отмены/блокировки/обходы, как их снимать;
- действия, выполняемые при обнаружении SIS неисправности.

Система SIS может выполнять небезопасно реализованные функции для обеспечения планового отключения или более быстрого запуска.

11. Разработка и проектирование SIS

11.1. Фазы жизненного цикла

На рис. 37 показана фаза применяемого жизненного цикла.

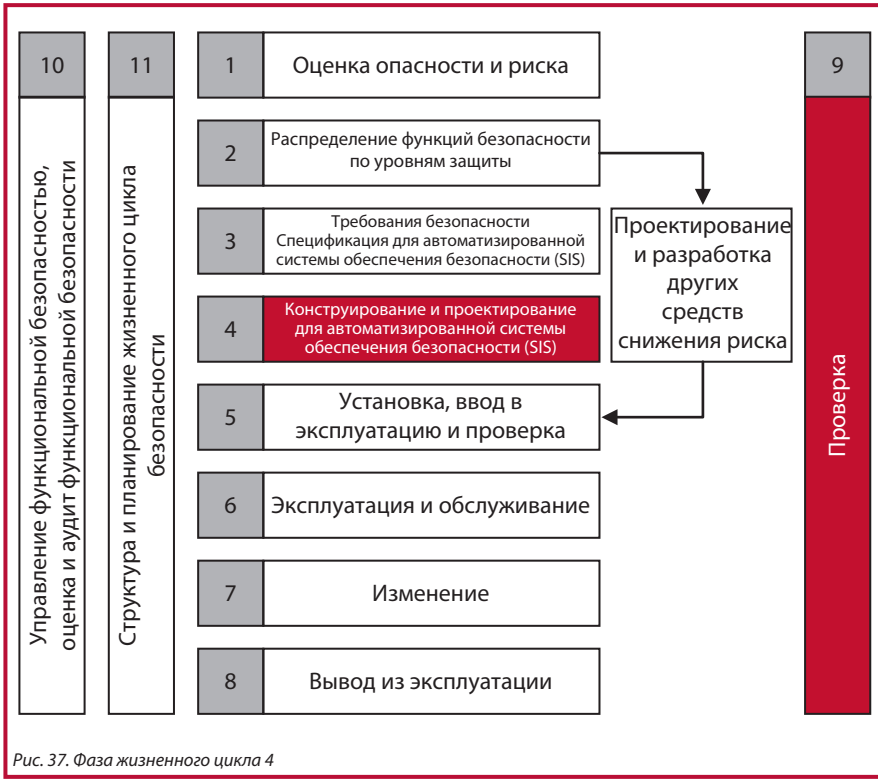


Рис. 37. Фаза жизненного цикла 4

Целью данной фазы, как определено в IEC 61511-1, 11.1, является:

- разработать SIS для предоставления необходимых функций SIF [11.2];
- убедиться, что конфигурация функции SIF соответствует указанному УПБ, определенному в процессе задания УПБ [13].

11.2. Проектирование функции SIF

Спецификация SRS формирует основу для проекта SIF и позволяет команде разработчиков преобразовать функциональность в проектную документацию, например в функциональную спецификацию проекта, FDS. Таким образом, FDS включает все требования к функциональности и целостности, необходимые для разработки и проектирования системы SIS.

Важно, чтобы проектная документация включала следующие требования:

- требования к поведению системы при обнаружении неисправности [13.2];
- аппаратная отказоустойчивость [13.3];
- выбор компонентов и подсистем [13.4];
- полевые устройства [13.5];
- оператор, персонал сопровождения и интерфейсы связи с SIS [13.6];
- требования к техническому обслуживанию и разработке тестирования [13.7];
- вероятность отказа функции SIF [13.8];
- прикладное ПО [13.9].

12. Методы обеспечения безопасности

12.1. Введение

В этом разделе дается краткое описание методов обеспечения надежности. Данный обзор методов обеспечения надежности ни в коей мере не является исчерпывающим, а также не претендует на новизну и оригинальность, поскольку описываемые здесь методы ежедневно используются инженерами по надежности.

12.2. Определения

Для удобства ниже приводится сокращенный перечень ключевых терминов и определений. Более полные определения терминов и понятий можно найти в стандартных текстах по этому вопросу.

Возможность – показатель способности элемента достигать цели задачи при данных условиях.

Восстанавливаемость – мера способности элемента быть сохраненным или восстановленным, если техническое обслуживание осуществляется персоналом, имеющим определенный уровень квалификации, с использованием предписанных процедур и ресурсов, на каждом предписанном уровне обслуживания и ремонта.

Доступность – показатель, до которого элемент находится в работоспособном и фиксируемом состоянии при запуске целевой задачи, если задача запрошена в неизвестном состоянии.

Кол-во отказов – общее количество отказов в пределах семейства элементов, поделенное на суммарное число жизненных элементов, потраченных этим семейством в течение определенного интервала измерения при определенных условиях.

Механизм отказа – физический, химический, электрический, термический или другой процесс, приводящий к отказу.

Надежность – (1) длительность или вероятность бесперебойного функционирования при заданных условиях; (2) вероятность того, что элемент сможет выполнять свое назначение в течение указанного интервала при заданных условиях. Для элементов без резервирования это эквивалентно определению (1). Для элементов с резервированием это является определением надежности выполнения задания.

Обслуживание, корректирующее – все действия, выполняемые в результате отказа с целью восстановления элемента до определенного состояния. Корректирующее обслуживание может включать любой из следующих шагов или их все: локализация,

изоляция, разборка, замена, повторная сборка, подгонка элементов и контрольная проверка.

Обслуживание, профилактическое – все действия, выполняемые в ходе попытки сохранить элемент в указанном состоянии путем проведения систематических осмотров, обнаружения и предотвращения начальных отказов.

Отказ – Прекращение возможности выполнять требуемую функцию

Отказ, зависимый – отказ, вызванный отказом смежных элементов. Не независимый.

Отказ, независимый – отказ, не вызванный отказом какого-либо другого элемента. Не зависимый.

Отказ, неопределенность – отказ, появление которого предсказуемо только в вероятностном или статистическом смысле. Это применимо ко всем распределениям.

Среднее время восстановления работоспособности после отказа (MTTR) – основная мера восстанавливаемости: сумма периодов корректирующего обслуживания на любом указанном уровне ремонта, деленное на общее число отказов в рамках элемента, ремонтируемого на этом уровне, в течение определенного интервала при заданных условиях.

Среднее время нормальной работы между двумя независимыми отказами (MTTF) – основная мера надежности для невосстанавливаемых элементов: среднее число элементов жизни, в течение которых все части элемента функционируют в указанных пределах в течение определенного интервала измерения при заданных условиях.

Среднее время между двумя независимыми отказами (MTBF) – основная мера надежности для восстанавливаемых элементов: среднее число элементов жизни, в течение которых все части элемента функционируют в указанных пределах в течение определенного интервала измерения при заданных условиях.

Тип отказа – результат действия механизма, вызывающего отказ, т. е. короткое замыкание, обрыв, слом, избыточный износ.

Функциональная надежность – показатель, до которого элемент находится в рабочем состоянии и способен выполнять требуемую от него функцию в любое (произвольное) время на протяжении указанной циклограммы выполняемого задания при условии доступности в момент запуска задания.

12.3. Основные математические понятия, используемые в технике обеспечения надежности

При создании техники обеспечения надежности используются многие математические понятия, особенно из области теории вероятности и статистики. Так, для различных целей можно использовать многие математические распределения, включая гауссово (нормальное) распределение, логнормальное распределение, распределение Рэлея, экспоненциальное распределение, распределение Вейбулла и множество других. В рамках этого краткого введения ограничимся рассмотрением экспоненциального распределения.

Интенсивность отказов и среднее время наработки на отказ (MTBF/MTTF).

Целью количественных методов оценки надежности является нахождение зависимости интенсивности отказов от времени и моделирование этой интенсивности отказов в виде математического распределения с целью понимания количественных аспектов отказа. Главным элементом расчета является интенсивность отказов, которая определяется следующим уравнением:

$$\lambda = F/T$$

где: λ = интенсивность отказов;

T = общее число часов работы устройства (время работы/циклы/мили/и т. д.) за период исследования для отказавших и неотказавших элементов;

F = общее число отказов, произошедших за исследуемый период.

Например, если пять электродвигателей работают в общей сложности 50 лет и за этой период произошло пять отказов, то интенсивность отказов равна 0,1 отказа в год.

Другим базовым понятием является средняя наработка на отказ (MTBF/MTTF). Единственное различие между MTBF и MTTF заключается в том, что MTBF используется, когда речь идет о тех элементах, которые подлежат ремонту в случае поломки. Для тех элементов, которые заменяются другими, используется MTTF. Расчеты остаются прежними. Для определения значений MTBF и MTTF нужно выполнить расчет, обратный по отношению к расчету функции интенсивности отказов. Оно вычисляется с использованием следующего уравнения:

$$\theta = T/F$$

где: θ = средняя наработка на отказ;

T = общее время работы/циклы/мили/и т. д. за период исследования для отказавших и неотказавших элементов;

F = общее число отказов, произошедших за исследуемый период.

MTBF для промышленного электродвигателя в нашем примере составляет 10 лет, что представляет собой величину, обратную частоте отказов. Заметим, что для электродвигателей, восстанавливаемых после отказа, найденное нами время означало бы MTBF. Для небольших двигателей, считающихся одноразовыми, это время означало бы MTTF.

Интенсивность отказов является базовым компонентом во многих сложных расчетах надежности. В зависимости от механической/электрической конструкции, рабочего контекста, окружающей среды и/или эффективности технического обслуживания интенсивность отказов машины как функция от времени может убывать, оставаться постоянной или возрастать линейно или в геометрической прогрессии. Однако в большинстве расчетов надежности интенсивность отказов считается постоянной.

12.4. U-образная кривая

По своему характеру U-образная кривая демонстрирует три основные характеристики частоты отказов машины: убывание, константное состояние или возрастание. На практике большинство машин остаются на ранней стадии эксплуатации или в области постоянной интенсивности отказов U-образной кривой. Зависимость механизмов отказа от времени наблюдается редко, поскольку промышленное оборудование регулярно обновляется или оснащается новыми деталями, прежде чем старые изнашиваются. Однако, несмотря на ограничения моделирования, U-образная кривая является полезным инструментом для объяснения основных понятий техники обеспечения надежности.

Человеческое тело – прекрасный пример системы, которая развивается по принципу U-образной кривой. У людей, как и у машин, интенсивность отказов (смертность) обычно бывает выше в первые годы жизни, и этот показатель снижается по мере того, как ребенок (продукт) становится старше. По достижении человеком двадцатилетнего возраста показатель смертности выходит на постоянный уровень и остается на нем, пока возрастные болезни (время) не начинают снова увеличивать частоту смертельных случаев (износ).

Считается, что U-образная кривая складывается из нескольких распределений отказов, рис. 38.

Снижающаяся интенсивность отказов на ранних этапах функционирования обусловлена системными причинами, такими как промышленные дефекты продукта. При производстве большой партии продуктов часть семейства неизбежно будет иметь

дефекты и откажет во время эксплуатации. По мере того как отказавшие элементы возвращаются назад после ремонта, доля слабых продуктов в семействе сокращается и интенсивность отказов соответственно убывает.

Увеличивающееся число отказов из-за износа может быть вызвано аналогичными системными причинами. Механизм отказа может быть обусловлен ослаблением, например в результате накаливания усталостных повреждений. В электронике механизмы отказа, обусловленные возрастом, обычно имеют механическую природу и включают усталостное разрушение паяных соединений.

Период константной частоты отказов составляет большую часть жизни продукта и является мерой качества конструкции, ее добротности. Именно в этой области константной частоты отказов выполняются элементарные расчеты надежности.

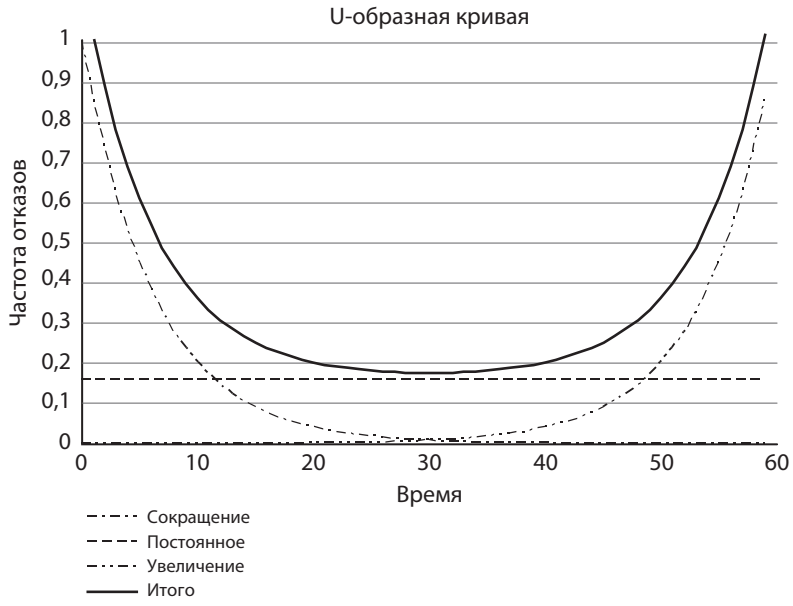


Рис. 38. U-образная кривая

12.5. Экспоненциальное распределение

Экспоненциальное распределение, самая основная и широко используемая формула для предсказания надежности, моделирует машины с константной интенсивностью отказов или рассматривает только плоский участок U-образной кривой. Большая часть промышленного оборудования работает большую часть своего срока службы с

постоянной интенсивностью отказов, поэтому эта формула имеет широкое применение.

Ниже приводится основное уравнение для оценки надежности машины по закону экспоненциального распределения, где интенсивность отказов как функция от времени является константой.

$$R(t) = \exp \{ -\lambda . t \}$$

где: R(t) = оценка надежности за период времени, количество циклов, миль и т. д. (t);

λ = интенсивность отказов (1/MTBF или 1/MTTF); t = опасный период.

В нашем примере с электродвигателем, если полагать интенсивность отказов величиной постоянной, вероятность того, что двигатель будет работать безотказно в течение шести лет, или проектируемая надежность, составляет 55%. Она подсчитывается следующим образом:

$$\begin{aligned} R(t) &= \exp \{ -0,1 \times 6 \} \\ &= \exp \{ -0,6 \} \\ &= 0,5488 \approx 55\% \end{aligned}$$

Другими словами, через шесть лет около 45% семейства идентичных двигателей, работающих в идентичных приложениях, по теории вероятности могут отказать. Здесь стоит напомнить, что эти расчеты определяют вероятность для семейства. Каждый отдельный элемент из этого семейства может отказать в первый же день работы, в то время как другой элемент будет работать 30 лет без перебоев. Такова природа вероятностного планирования надежности.

Характерной чертой экспоненциального распределения является то, что MTBF приходится на точку, в которой рассчитанная надежность равна 36,78%, или на момент, когда 63,22% машин уже вышли из строя. В нашем примере с двигателями через 10 лет можно ожидать, что из семейства идентичных двигателей, работающих в идентичных приложениях, 63,22% выйдут из строя. Иными словами, коэффициент выживаемости составляет 36,78% семейства.

12.6. Оценка надежности системы

После того как надежность компонентов или машин относительно рабочего контекста и требуемого времени выполнения задания была установлена, инженеры-технологи приступают к оценке надежности системы или процесса. Опять же из соображений простоты и краткости рассмотрим оценки надежности для систем последовательного включения, параллельных систем и систем с распределением нагрузок и резервированием (системы MooN).

12.6.1. Системы последовательного включения

Прежде чем перейти к рассмотрению систем последовательного включения, необходимо поговорить о блок-схемах расчета надежности (RBD). Блок-схемы RBD просто отображают процесс от начала до конца. В системах последовательного включения за подсистемой 1 следует подсистема 2 и т. д. В системах последовательного включения возможность задействовать подсистему 2 зависит от рабочего состояния подсистемы 1. Если подсистема 1 не работает, система не функционирует независимо от состояния подсистемы 2 [рис. 39].

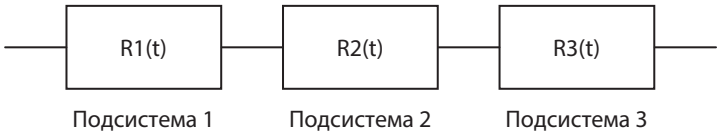


Рис. 39. Система последовательно включенных элементов

Чтобы подсчитать надежность системы для процесса с последовательным включением, необходимо умножить найденную надежность подсистемы 1 в момент времени (t) на найденную надежность подсистемы 2 в момент времени (t). Основное уравнение для вычисления надежности простой системы с последовательным включением имеет вид:

$$Rs(t) = R1(t) \cdot R2(t) \cdot R3(t)$$

где: Rs(t) – надежность системы в данный момент времени (t);

Rn(t) – надежность подсистемы или подфункции в данный момент времени (t).

Так, для простой системы с тремя подсистемами или подфункциями, у каждой из которых найденная надежность в момент времени (t) равна 0,90 (90%), надежность системы вычисляется как 0,90 X 0,90 X 0,90 = 0,729, или примерно 73%.

12.6.2. Параллельные системы

Часто инженеры-разработчики включают в критические станки избыток мощности. Специалисты по надежности называют такие системы параллельными. Такие системы могут быть спроектированы как активные параллельные системы или параллельные резервные системы. На рис. 40 показана блок-схема для простой двухкомпонентной параллельной системы.

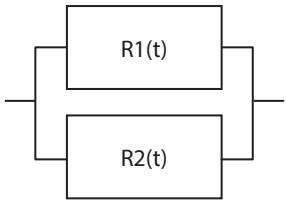


Рис. 40. Система параллельно включенных элементов

Чтобы подсчитать надежность активной параллельной системы, в которой обе машины работают, воспользуйтесь следующим простым уравнением:

$$Rs(t) = 1 - [\{1-R1(t)\} . \{1-R2(t)\}]$$

где: Rs(t) – надежность системы в данный момент времени (t);

Rn(t) – надежность подсистемы или подфункции в данный момент времени (t).

Наша простая параллельная система с двумя компонентами в параллели, надежность каждого из которых составляет 0,90, имеет суммарную надежность системы 1 – (0,1 X 0,1) = 0,99. Итак, надежность системы была существенно улучшена.

12.6.3. Системы M из N (MooN)

Для специалистов по надежности заводского оборудования очень важным является понятие системы MooN. Такие системы требуют, чтобы были доступны M элементов из общего семейства в N элементов. Хорошим примером из области промышленности является угольная мельница на электростанции. Инженеры часто проектируют эту функцию на заводе, используя метод MooN. Например, на элементе имеется четыре мельницы, и элемент требует, чтобы три из них работали с полной загрузкой [рис. 41].

12.7. Опасные и безопасные отказы

Чтобы расчеты надежности имели значение, нужно знать не только частоту отказов системы, но и то, как система может выйти из строя, т. е. тип отказа.

Типы отказов классифицируются как безопасные или опасные. На рис. 42 показан газовый трубопровод. Если по трубопроводу подается топливо на электростанцию и отсекающий клапан выйдет из строя и произведет ложное отключение, подача топлива будет прервана и это, возможно, приведет к финансовым потерям, но в данном случае тип отказа (поломка в закрытом состоянии) является безопасным.

Если тот же клапан сломается в открытом состоянии, подача топлива сохранится, но создастся ситуация повышенного давления. При этом невозможно изолировать

топливо и обезопасить трубопровод. Поэтому данный тип отказа (поломка в открытом состоянии) рассматривается как опасный.

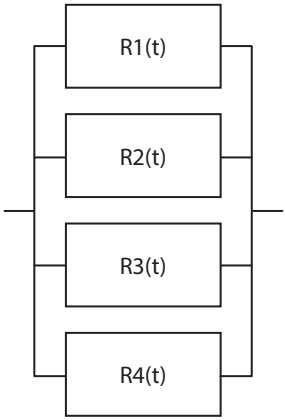


Рис. 41. Система 3oo4

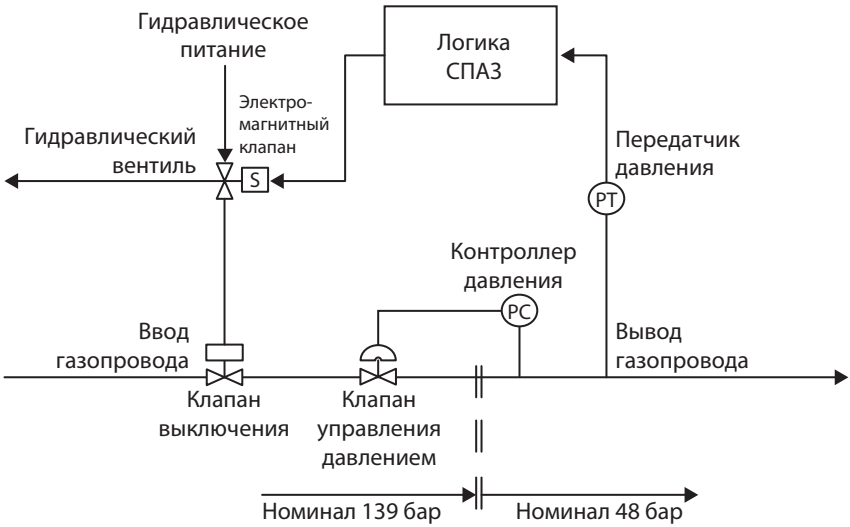


Рис. 42. Функция отказа в случае возникновения опасной ситуации

В этом примере опасный тип отказа (поломка в открытом состоянии) не будет обнаружен до тех пор, пока на него не поступит команда, т. е. пока клапан не получит команду закрыться. Это рассматривается как опасный необнаруженный отказ.

С другой стороны, если по трубопроводу на электростанцию подается теплоноситель и клапан SSV969A выйдет из строя и произведет ложное отключение, то подача теплоносителя прекратится и на электростанции может наступить перегрев. В этом приложении тот же самый клапан и тот же самый тип отказа (поломка в закрытом состоянии) являются опасным отказом. Если клапан выйдет из строя в открытом состоянии, поток теплоносителя сохраняется, поэтому тип отказа (поломка в открытом состоянии) будет рассматриваться как безопасный.

Опасный отказ компонента в приборной защитной функции мешает этой функции достичь безопасного состояния, когда это требуется. Частота опасных отказов обозначается символом: λ_D.

Безопасный отказ не способен привести автоматизированную систему безопасности в опасное или нерабочее состояние, однако такой отказ вызывает отключение системы или активацию приборной защитной функции при отсутствии угроз. Частота безопасных отказов обозначается символом: λ_S.

Существуют типы отказов, которые вообще не влияют на функцию безопасности. Они могут включать функции обслуживания, индикаторы, регистрацию данных и другие функции, не связанные с безопасностью (non-SR). Интенсивность отказов, не связанных с безопасностью, обозначается символом: $\lambda_{non\text{-}SR}$.

Общая интенсивность отказов элемента λ равна сумме интенсивности отказов, связанных с безопасностью и не связанных с безопасностью. Обычно в расчеты надежности включается только λ_D и λ_S.

$$\lambda = \lambda_D + \lambda_S + \lambda_{non\text{-}SR}$$

12.8. Выявленные и невыявленные отказы

PFD относится к опасным отказам, которые мешают SIS работать, когда это требуется. Эти типы отказов классифицируются либо как выявленные, т. е. они обнаружены системой диагностики, либо как невыявленные, т. е. те, которые обнаруживаются только в ходе ручных контрольных проверок, которые обычно выполняются раз в год. Рекомендуется, чтобы типы отказов, классифицированные FMECA как опасные выявленные отказы, обнаруживались в ходе диагностики и проверялись при оценке средств программного обеспечения. Кроме того, процедуры контрольной проверки должны гарантировать обнаружение опасных невыявленных типов, чтобы гарантировать эффективность контрольных проверок.

В соответствии с IEC 61508-6, приложение B.3.1, анализ может включать для каждой функции безопасности наличие полной контрольной проверки и ремонта, т. е. чтобы все невыявленные отказы обнаруживались в ходе контрольной проверки.

12.9. Периодичность контрольных проверок (T_p) и среднее время простоя (MDT)

Предполагается, что, если случается отказ, он в среднем приходится на середину интервала между проверками. Иными словами, отказ остается невыявленным на протяжении 50% испытательного периода.

Для выявленных и невыявленных отказов среднее время простоя (MDT) зависит от интервала между проверками, а также от продолжительности ремонта, или MTTR.

Следовательно, MDT вычисляется как:

$$MDT = \frac{\text{интервал между проверками}}{2} + MTTR$$

Поэтому MDT для выявленных отказов приближается к времени ремонта, поскольку интервал между проверками (автотестирование), как правило, несоизмеримо мал по сравнению с MTTR. Для невыявленных отказов продолжительность ремонта несоизмеримо мала по сравнению с интервалом между проверками (периодичность контрольных проверок Tp), поэтому MDT для невыявленных отказов приближается к Tp/2.

12.10. Моделирование частоты отказов системы (λsys)

Частоту отказов резервированной системы λsys можно вычислить, зная количество способов, какими система может выйти из строя. В системе 3oo4 для функционирования системы требуется, чтобы функционировали 3 из 4 каналов, поэтому любые два отказа могут привести к отказу системы.

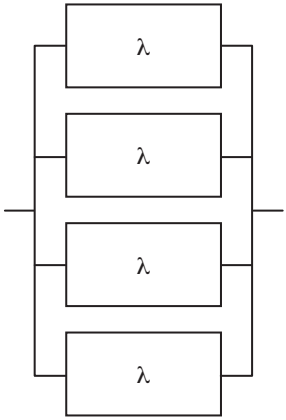


Рис. 43. Система 3oo4

Частота, с которой могут происходить сразу два отказа, λ_2 получается в результате умножения частоты отказов одного элемента λ на вероятность того, что второй отказ произойдет в период простоя первого элемента MDT λ.MDT.

Таким образом,

$$\lambda_2 = \lambda.(\lambda.MDT)$$

Однако существуют 12 возможных комбинаций (порядок важен) двух отказов в системе 3oo4: A.B, A.C, A.D, B.C, B.D, C.D, B.A, C.A, D.A, C.B, D.B и D.C. И необходимо учитывать их все. Поэтому интенсивность отказов системы приобретает вид:

$$\lambda_{SYS} = 12.\lambda^2.MDT$$

Чтобы быть точными, необходимо было включить все комбинации из 3 и 4 ных отказов, а также отказы, вызванные общими причинами, поскольку они также приводят к отказу системы, но в приближении первого порядка этими членами высшего порядка можно пренебречь. Интенсивность отказов системы 3oo4 и другие конфигурации представлены в таблице 10. Заметим, что эти значения являются приближенными и в них также опущены члены более высокого порядка.

Конфигурация	**λsys**
1oo1	λ
1oo2	$2.\lambda^2.MDT$
2oo2	2.λ
1oo3	$3.\lambda^3.MDT^2$
2oo3	$6.\lambda^2.MDT$
3oo3	3.λ
1oo4	$\lambda^4.MDT^3$
2oo4	$12.\lambda^3.MDT^2$
3oo4	$12.\lambda^2.MDT$
4oo4	4.λ

Таблица 10. Интенсивность отказов

Заметим, что вклад отказов, вызванных общими причинами, рассматривается далее [12.17].

12.11. Моделирование частоты опасных выявленных и невыявленных отказов (λ_{DD}) и (λ_{DU})

Подставляя λ_{DD} и λ_{DU} вместо λ в таблицу 10 и используя соответственно MDT или Tp/2, можно вывести частоту отказов системы в результате опасных выявленных или невыявленных отказов, таблица 11.

Конфигурация	**Обнаруженные**	**Необнаруженные**
	λsys	**λsys**
1oo1	λ_{DD}	λ_{DU}
1oo2	$2.\lambda_{DD}^2.MDT$	$\lambda_{DU}^2.T_P$
2oo2	$2.\lambda_{DD}$	$2.\lambda_{DU}$
1oo3	$3.\lambda_{DD}^3.MDT^2$	$\lambda_{DU}^3.T_P^2$
2oo3	$6.\lambda_{DD}^2.MDT$	$3.\lambda_{DU}^2.T_P$
3oo3	$3.\lambda_{DD}$	$3.\lambda_{DU}$
1oo4	$\lambda_{DD}^4.MDT^3$	$\lambda_{DU}^4.T_P^3$
2oo4	$12.\lambda_{DD}^3.MDT^2$	$4.\lambda_{DU}^3.T_P^2$
3oo4	$12.\lambda_{DD}^2.MDT$	$6.\lambda_{DU}^2.T_P$
4oo4	$4.\lambda_{DD}$	$4.\lambda_{DU}$

Таблица 11. Частота опасных отказов системы

12.12. Моделирование ложных отключений системы (λ_{STR})

Поскольку в большинстве случаев предполагается, что в схеме с резервированием интенсивность всех безопасных отказов выявлена, вышедшие из строя каналы подлежат ремонту при условии, что не произойдет аварийного отключения системы. Поэтому применяется метод, используемый по отношению к опасным выявленным сбоям, за исключением тех случаев, когда число отказов, требующееся для ложного отключения, отличается от соответствующего числа, требующегося для опасного отказа.

Обычно ложные отключения включают только значения частоты безопасных отказов, но в зависимости от поведения системного отказа после обнаружения дефекта могут быть включены и опасные выявленные отказы, и тогда интенсивность ложных отключений будет представлять собой сумму обеих величин.

В таблице 12 сведены значения интенсивности ложных отключений системы для безопасных отказов.

Конфигурация	**Ложное**
	λstr
1oo1	λ_S
1oo2	$2.\lambda_S$
2oo2	$2.\lambda_S^2.MDT$
1oo3	$3.\lambda_S$
2oo3	$6.\lambda_S^2.MDT$
3oo3	$3.\lambda_S^3.MDT^2$
1oo4	$4.\lambda_S$
2oo4	$12.\lambda_S^2.MDT$
3oo4	$12.\lambda_S^3.MDT^2$
4oo4	$\lambda_S^4.MDT^3$

Таблица 12. Частота ложных отключений системы

12.13. Моделирование доступности системы безопасности в режиме управления

Доступность системы безопасности в результате опасных выявленных отказов A_{DD} находится по формуле:

$$A_{DD} = 1/(1 + .\lambda_{DD(SYS)}.MDT)$$

где $\lambda_{DD(SYS)}$ – интенсивность отказов системы в результате опасного выявленного отказа [12.11].

Для опасных невыявленных отказов ADU вычисляется по формуле:

$$A_{DU} = 1/(1 + .\lambda_{DU(SYS)}.T_P/2)$$

где $\lambda_{DU(SYS)}$ – интенсивность отказов системы в результате опасного невыявленного отказа [12.11].

Для безопасных отказов A_S вычисляется по формуле:

$$A_S = 1/(1 + .\lambda_{S(SYS)}.MDT)$$

где $\lambda_{S(SYS)}$ – интенсивность отказов системы в результате ложных (безопасных) отказов [12.12].

Следовательно, доступность системы является произведением значений доступности вследствие выявленных, опасных, невыявленных и безопасных отказов:

$$A_{SYS} = A_{DD} \cdot A_{DU} \cdot A_S$$

Этот метод можно использовать для моделирования систем последовательного включения (simplex), а также резервированных систем.

12.14. Моделирование доступности системы безопасности в непрерывном режиме

Когда метод применяется к системам безопасности в непрерывном режиме, специалист, проводящий анализ, должен понимать природу команд, отдаваемых функции безопасности. Некоторые функции безопасности непрерывного режима работают по команде (как функции безопасности в режиме управления), но отнесены к классу функций непрерывного режима из-за частоты команд, которые поступают чаще 1 раза в год. В этом случае доступность можно вычислить так же, как для функции безопасности в режиме управления с той лишь разницей, что интервал между контрольными проверками T_P нужно заменить интервалом между командами T_D. Опасные невыявленные отказы остаются необнаруженными, пока функции безопасности не будет отдана команда.

Если функция безопасности в непрерывном режиме эффективно обеспечивает непрерывный контроль, доступность можно рассчитать как систему управления [12.15].

12.15. Моделирование доступности системы управления

При моделировании доступности систем управления и интересны отказы, влияющие на процесс, поэтому приходится решать, влияет ли отказ на процесс в такой степени, что система управления становится практически недоступна.

Обнаружение отказа производится либо системой диагностики и оповещения об ошибках, в этом случае требуется ремонт и система будет недоступна до устранения неисправности, либо по симптомам, в этом случае процесс под контролем продолжается за пределами указанных значений.

Невыявленные отказы не приводят к немедленному выводу системы управления из состояния доступности. Со временем невыявленные отказы могут приводить к выходу параметров процесса за указанные пределы, после чего отказ обнаруживается и система становится недоступна.

Поэтому доступность системы управления можно смоделировать, учитывая общую частоту отказов системы, A_{SYS} находим по формуле:

$$A_{SYS} = 1/(1 + \lambda_{SYS}.MDT)$$

где λ_{SYS} – общая интенсивность отказов системы в результате отказов всех типов [таблица 10].

12.16. Вероятность опасного отказа/час (PFH) и вероятность отказа при запросе (PFD)

Упрощенные формулы для вычисления PFH и PFD для обычных конфигураций представлены в таблице 13 для выявленных отказов и в таблице 14 для невыявленных отказов.

Конфигурация	**PFH**	**PFD**
1oo1	λ_{DD}	$\lambda_{DD}.MDT$
1oo2	$2.\lambda_{DD}^2.MDT$	$2.\lambda_{DD}^2.MDT^2$
2oo2	$2.\lambda_{DD}$	$2.\lambda_{DD}.MDT$
1oo3	$3.\lambda_{DD}^3.MDT^2$	$3.\lambda_{DD}^3.MDT^3$
2oo3	$6.\lambda_{DD}^2.MDT$	$3.\lambda_{DD}^2.MDT^2$
3oo3	$3.\lambda_{DD}$	$3.\lambda_{DD}.MDT$
1oo4	$4.\lambda_{DD}^4.MDT^3$	$\lambda_{DD}^4.MDT^4$
2oo4	$12.\lambda_{DD}^3.MDT^2$	$4.\lambda_{DD}^3.MDT^3$
3oo4	$12.\lambda_{DD}^2.MDT$	$6.\lambda_{DD}^2.MDT^2$
4oo4	$4.\lambda_{DD}$	$4.\lambda_{DD}.MDT$

Таблица 13. Подсчет PFH/PFD (выявленные отказы)

Конфигурация	PFH	PFD
1oo1	λ_{DU}	$\lambda_{DD}.T_P/2$
1oo2	$\lambda_{DU}^2.T_P$	$\lambda_{DD}^2.T_P^2/3$
2oo2	$2.\lambda_{DU}$	$\lambda_{DD}.T_P$
1oo3	$\lambda_{DU}^3.T_P^2$	$\lambda_{DD}^3.T_P^3/4$
2oo3	$3.\lambda_{DU}^2.T_P$	$\lambda_{DD}^2.T_P^2$
3oo3	$3.\lambda_{DU}$	$3.\lambda_{DD}.T_P/2$
1oo4	$\lambda_{DU}^4.T_P^3$	$\lambda_{DD}^4.T_P^4/5$
2oo4	$4.\lambda_{DU}^3.T_P^2$	$\lambda_{DD}^3.T_P^3$
3oo4	$6.\lambda_{DU}^2.T_P$	$2.\lambda_{DD}^2.T_P^2$
4oo4	$4.\lambda_{DU}$	$2.\lambda_{DD}.T_P$

Таблица 14. Подсчет PFH/PFD (невыявленные отказы)

12.17. Учет отказов с общей причиной (Common Cause Failures, CCF)

Отказы по общей причине (CCF) – это отказы, которые могут быть вызваны одной причиной, но влияют одновременно на более чем один канал. Они могут быть вызваны системной ошибкой, например ошибкой проектной спецификации или внешним воздействием, таким как экстремальная температура, которая может привести к отказу компонентов в обоих резервированных каналах. В обязанности разработчика системы входит принятие мер по минимизации вероятности отказов по общей причине с использованием соответствующих приемов проектирования.

Вклад CCF в параллельных резервных трактах учитывается путем включения коэффициента β. Интенсивность отказов CCF, включенная в расчет, равна β x общую частоту отказов одного из резервных трактов.

Модель с использованием коэффициента β [IEC 61508-6, приложение D] является предпочтительной методикой по причине ее объективности и предоставляемой ею трассируемости при подсчете β. Модель была скомпилирована таким образом, что она задает ряд специальных вопросов, которым затем присваиваются баллы с использованием объективной инженерной оценки. Максимальное количество баллов для каждого вопроса определяется в модели путем сравнения результатов различных оценок с известными данными об отказах при эксплуатации.

Полученные баллы сведены в двух столбцах. В столбце A представлены баллы для тех характеристик системы защиты от CCF, которые усиливаются при увеличении частоты диагностики (автотест или контрольная проверка). В столбце B представлены баллы для тех характеристик, которые не усиливаются при увеличении частоты диагностики.

Модель позволяет изменить количество баллов, меняя частоту и зону охвата диагностического теста. Баллы из столбца A умножаются на коэффициент C, который выводится с учетом данных диагностики. Окончательный коэффициент β находится затем из общей исходной оценки.

Исходная оценка = (A * C) + B

Отношение между β и исходной оценкой фактически представляет собой отрицательную показательную функцию, поскольку отсутствуют данные, оправдывающие отход от предположения о том, что, когда β убывает (улучшается), следующие улучшения становится все труднее получить.

Если конкретный вопрос неприменим к оцениваемой системе, вводится значение 100 или 0% в зависимости от того, что больше подходит для данной системы.

Ниже приводятся типичные ограничивающие условия, которые рассматриваются с целью оценки вклада CCF:

- резервированные каналы физически разделены;
- различные технологии, напр. один канал электронный, а другой релейный;
- установленная система работы на месте должна обеспечивать анализ отказов;
- установленные процедуры обслуживания должны предотвращать повторную маршрутизацию при прокладке кабелей;
- доступ персонала ограничен;
- рабочая среда находится под контролем, оборудование нормировано во всем диапазоне условий окружающей среды.

Конечно, реальное поведение во время работы будет зависеть от конкретной установки и конструкции, принятых практик эксплуатации и техобслуживания, но при словии принятия правильных практик проектирования модель предоставляет трассируемую оценку вклада CCF.

С учетом значений CCF в формулах для PFD и PFH [таблица 13 и 14] можно использовать следующий метод. Используемые уравнения являются упрощенной формой стандартных уравнений, их вывод приводится в пункте [19.6].

Для выявленных отказов:

$PFD1oo1 = \lambda_{DD}.MDT$	См. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DD}^2.MDT^2 + \beta.\lambda_{DD}.MDT$	См. IEC 61508-6, B.3.2.2.2

Для невыявленных отказов:

$PFD1oo1 = \lambda_{DU}.T_P/2$	См. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DU}^2.T_P^2/3 + \beta.\lambda_{DU}.T_P/2$	См. IEC 61508-6, B.3.2.2.2

где λ_{DD} – частота опасных выявленных отказов, λ_{DU} – частота опасных невыявленных отказов, а β – вклад отказов по общей причине. T_P – интервал между контрольными проверками, а MDT – среднее время простоя.

Общая форма этих уравнений для различных конфигураций, как для систем в непрерывном режиме, так и для систем в режиме управления, рассматривается в пункте [19.7].

12.18. Значения частоты отказов

При расчетах PFD и SFF в анализе используется основная гипотеза IEC 61508-6, приложение B.3, согласно которой интенсивность отказов компонента считается константной на протяжении всего срока службы системы.

Значения частоты отказов, используемые в расчетах, можно получить с помощью анализа видов, последствий и диагностики отказов (FMECA) на основе эксплуатационных данных или данных, публикуемых в отраслевых изданиях. Используемые значения частоты отказов следует сравнить с доступными данными для аналогичных по сложности и техническим характеристикам модулей. Такой метод гарантирует консервативный подход к моделированию надежности и дает уверенность в том, что вычисленные показатели надежности будут достигнуты в реальности.

Частоты отказов и их источники обсуждаются в пункте 14.8.

12.19. Моделирование 1oo2, 1oo2D и горячее резервирование

В следующих примерах показаны RBD, моделирующие некоторые типичные конфигурации системы.

1oo2

Система 1oo2 представляет собой архитектуру 1 из 2, в которой каждый из двух каналов может выполнять функцию безопасности. Это устойчивая к сбоям конфигурация, в которой отказ одного канала не влияет на работоспособность.

Если отказ канала является опасным невыявленным отказом, он не будет обнаружен системой диагностики и сообщение о сбое не появится. Однако функция безопасности по-прежнему будет работать, поскольку 1 оставшийся канал может инициировать отключение. Если отказ канала является опасным выявленным отказом, как правило, появляется сообщение об отказе.

Пример RBD показан в пункте 12.20.

1oo2D

Архитектура системы 1oo2D имеет два канала, соединенные параллельно, и каждый канал имеет диагностическую схему для обнаружения отказов с большим диагностическим охватом. При нормальной работе системы для выполнения операции выключения необходимо согласие обоих каналов. Исправный канал управляет системой, если диагностическая схема другой стороны обнаруживает отказ.

С точки зрения моделирования надежности при опасных выявленных отказах система 1oo2D работает как конфигурация 1oo2 и частоту отказов и PFD системы при выявленных отказах можно смоделировать как 1oo2.

Опасный невыявленный отказ одного из каналов в системе 1oo2D блокирует работу системы, поэтому частоту отказов системы и PFD нужно моделировать как 2oo2 для невыявленных отказов. Другими словами, должны работать оба канала.

Пример RBD показан в пункте 12.21.

Горячее резервирование

Архитектура системы горячего резервирования имеет два канала, соединенные параллельно, из которых один канал является ведущим и управляет функцией безопасности. Другой канал ведет себя как горячий резерв, т. е. при обнаружении опасного отказа в ведущем канале резервный канал принимает на себя управление функцией безопасности.

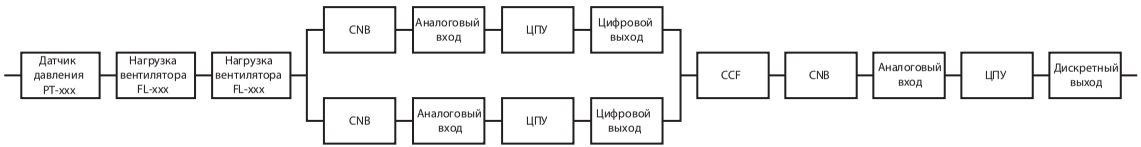
С точки зрения моделирования надежности при опасных выявленных отказах система горячего резервирования работает как конфигурация 1oo2 и частоту отказов и PFD системы при выявленных отказах можно смоделировать как 1oo2.

Опасный невыявленный отказ одного из каналов блокирует работу системы, поэтому частоту отказов системы и PFD нужно моделировать как 1oo1 для невыявленных отказов. Другими словами, функция безопасности не может работать в случае невыявленного отказа ведущего канала, а для невыявленных отказов не существует резервирования. Пример RBD показан в пункте 12.22.

Интенсивность отказов системы 1oo2

CCF										5%
Кол-во	1	1	1	1	2	1	1	1		
Конфигурация	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2	1oo2		
λDD (диагностика)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07		5,25E-08	
λDD*Кол-во	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07		5,25E-08	
λDD для ветви			1,16E-06				1,01E-06		5,25E-08	
MDT			24				24		24	
Итого λDD			1,16E-06				4,93E-11		5,25E-08	
λDU (контрольная проверка)	3,66E-07	2,00E-07	2,00E-07	9,10E-09	3,28E-08	2,26E-08	1,54E-08		5,84E-09	
λDU*Кол-во	3,66E-07	2,00E-07	2,00E-07	9,10E-09	6,56E-08	2,26E-08	1,54E-08		5,84E-09	
λDU для ветви			7,66E-07				1,13E-07		5,84E-09	
Период контрольной проверки, T			8760				8760		8760	
Итого λDU			7,66E-07				1,11E-10		5,84E-09	
λS (диагностика)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07		5,84E-08	
λS*Кол-во	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07		5,84E-08	
λS для ветви			2,63E-03				1,13E-06		5,84E-08	
MDT			24				24		24	
Итого λS			2,63E-03				2,25E-06		5,84E-08	
Итого λDD	1,21E-06									
Итого λDU	7,72E-07									
Итого λS	2,63E-03									
Итого λSYS	**2,63E-03**	**/ч**								

Интенсивность отказов системы 1oo2D

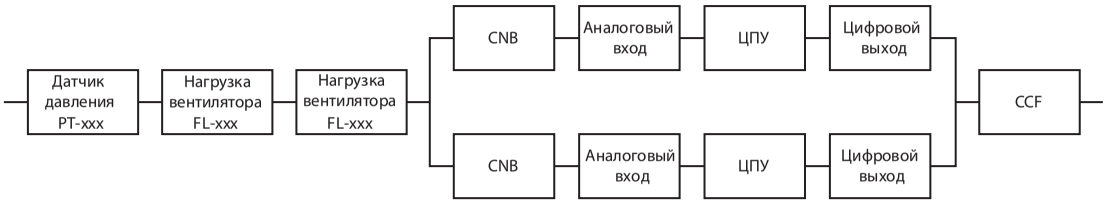


CCF								5%				
Кол-во	1	1	1	1	2	1	1		2	4	2	2
Конфигурация	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2		2oo2	2oo2	2oo2	2oo2
λ.DD (диагностика)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08				
λ.DD*Кол-во	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08				
λ.DD для ветви			1,16E-06				1,01E-06	5,25E-08				
MDT			24				24	24				
Итого λ.DD			1,16E-06				4,93E-11	5,25E-08				
λ.DU (контрольная проверка)	3,66E-07	2,00E-07	2,00E-07						9,10E-09	3,28E-08	2,26E-08	1,54E-08
λ.DU*Кол-во	3,66E-07	2,00E-07	2,00E-07						1,82E-08	1,31E-07	4,52E-08	3,07E-08
λ.DU для ветви			7,66E-07									2,25E-07
Период контрольной проверки, T			8760									8760
Итого λ.DU			7,66E-07									9,87E-04
λ.S (диагностика)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08				
λ.S*Кол-во	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08				
λ.S для ветви			2,63E-03				1,13E-06	5,84E-08				
MDT			24				24	24				
Итого λ.S			2,63E-03				2,25E-06	5,84E-08				
Итого λ.DD	1,21E-06											
Итого λ.DU	9,88E-04											
Итого λ.S	2,63E-03											
Итого λ.SYS	**3,62E-03**	**/ч**										

Кол-во	1	1	1	1	2	1	1		1	1	2	1	1
Конфигурация	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2		1oo1	1oo1	1oo1	1oo1	1oo1
λDD (диагностика)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08					
λDD*Кол-во	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08					
λDD для ветви			1,16E-06				1,01E-06	5,25E-08					
MDT			24				24	24					
Итого λDD			1,16E-06				4,93E-11	5,25E-08					
λDU (контрольная проверка)	3,66E-07	2,00E-07	2,00E-07						9,10E-09	3,28E-08	2,26E-08	1,54E-08	
λDU*Кол-во	3,66E-07	2,00E-07	2,00E-07						9,10E-09	6,56E-08	2,26E-08	1,54E-08	
λDU для ветви			7,66E-07									1,13E-07	
Периодичность проверки			8760									8760	
Итого λDU			7,66E-07									4,93E-04	
λS (диагностика)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08					
λS*Кол-во	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08					
λS для ветви			2,63E-03				1,13E-06	5,84E-08					
MDT			24				24	24					
Итого λS			2,63E-03				2,25E-06	5,84E-08					
Итого λDD	1,21E-06												
Итого λDU	4,94E-04												
Итого λS	2,63E-03												
Итого λSYS	**3,13E-03**	**/ч**											

Интенсивность отказов системы Hot Syandby

Доступность сложной системы



CCF								5%
Кол-во	1	1	1	1	2	1	1	
Конфигурация	1oo1	1oo1	1oo1	1oo2	1oo2	1oo2	1oo2	
λDD (диагностика)	1,16E-06	0,00E+00	0,00E+00	8,19E-08	2,95E-07	2,03E-07	1,38E-07	5,25E-08
λDD*Кол-во	1,16E-06	0,00E+00	0,00E+00	8,19E-08	5,90E-07	2,03E-07	1,38E-07	5,25E-08
λDD для ветви			1,16E-06				1,01E-06	5,25E-08
MDT			24				24	24
Итого λDD			1,16E-06				4,93E-11	5,25E-08
λDU (контрольная проверка)	3,66E-07	2,00E-07	2,00E-07	9,10E-09	3,28E-08	2,26E-08	1,54E-08	5,84E-09
λDU*Кол-во	3,66E-07	2,00E-07	2,00E-07	9,10E-09	6,56E-08	2,26E-08	1,54E-08	5,84E-09
λDU для ветви			7,66E-07				1,13E-07	5,84E-09
Период контрольной проверки,T			8760				8760	8760
Итого λDU			7,66E-07				1,11E-10	5,84E-09
λS (диагностика)	2,15E-06	3,00E-07	3,00E-07	9,10E-08	3,28E-07	2,26E-07	1,54E-07	5,84E-08
λS*Кол-во	0,00E+00	0,00E+00	2,63E-03	9,10E-08	6,56E-07	2,26E-07	1,54E-07	5,84E-08
λS для ветви			2,63E-03				1,13E-06	5,84E-08
MDT			24				24	24
Итого λS			2,63E-03				2,25E-06	5,84E-08

Итого λDD	=	1,21E-06	Ср (DD)	=	0,99997
Итого λDU	=	7,72E-07	Ср (DU)	=	0,99328
Итого λS	=	2,63E-03	Ср (S)	=	0,94062

Итого λSYS = 2,63E-03 /ч
Доступность = 0,9343

12.24. Листок с примерными данными

Данные по частоте отказов, использованные в прежних схемах RBD, должны быть видны в отчете и показывать трассируемость до источника. Ссылка на источник, если речь идет об опубликованных данных, должна быть настолько подробной, чтобы позволить третьим лицам независимо проверить данные. Здесь может быть указан идентификатор документа, номер ISBN, если таковой имеется, страница и номер элемента.

Таблица 15 представляет собой типичную таблицу с данными для схем RBD, рассмотренных в предыдущих примерах.

Описание	Номер по каталогу	λОбщ.	λD	λDD	λDU	λS	Комментарий/ источник
Датчик давления, PT-xxx	PT-xxx	3,68E-06	1,53E-06	1,16E-06	3,66E-07	2,15E-06	Инструкции по технике безопасности изготовителя PT-xxx, M-xxx-xxx, Month-20xx
Токовый трансформатор FL-xxx для нагружения вентилятора	FL-xxx	5,00E-07	2,00E-07	0,00E+00	2,00E-07	3,00E-07	FARADIP-THREE V6.4, база данных о надежности. Technis, 26 Orchard Drive, Tonbridge, Kent TN10 4LG, ISBN 0-951-65623-6.
Comms. Module ControlNet CNB	1756-CNB	1,82E-07	9,10E-08	8,19E-08	9,10E-09	9,10E-08	Документ Allen-Bradley «Using ControlLogix in SIL2 Applications» (Использование ControlLogix в SIL2)
Модуль аналоговых входов	1756-AI16	6,56E-07	3,28E-07	2,95E-07	3,28E-08	3,28E-07	Документ Allen-Bradley «Using ControlLogix in SIL2 Applications» (Использование ControlLogix в SIL2)
ЦПУ ControlLogix	1756-L63	4,52E-07	2,26E-07	2,03E-07	2,26E-08	2,26E-07	Документ Allen-Bradley «Using ControlLogix in SIL2 Applications» (Использование ControlLogix в SIL2)
Модуль дискретных выходов	1756-OB32	3,07E-07	1,54E-07	1,38E-07	1,54E-08	1,54E-07	Документ Allen-Bradley «Using ControlLogix in SIL2 Applications» (Использование ControlLogix в SIL2)

Таблица 14. Подсчет PFH/PFD (невыявленные отказы)

12.25. Моделирование противопожарных и газовых систем (систем F&G)

При моделировании систем F&G важно иметь правильное представление о нечувствительности к сбоям. Моделирование СПАЗ или аналогичных систем, как правило, следует конфигурации логического решающего устройства. Например, надежность датчиков давления, данные которых о превышении давления оцениваются системой СПАЗ по схеме «любой из двух» (1oo2), будет моделироваться как 1oo2. То же самое не всегда верно для систем F&G.

В целом консервативный анализ обычно бывает можно провести, не опираясь на предположения о зоне действия детектора и резервирования в схеме сигнализации, но на практике это может привести к пессимистичному анализу и невозможности достичь поставленных целей. При возникновении таких сложностей детальное знание угрозы позволяет разработать модель, лучше отвечающую целям, и с ее помощью выполнить более реалистичный анализ надежности.

Системы F&G не только защищают людей, но могут также использоваться для защиты активов от коммерческого риска или производственного объекта от экологического риска, а исполнительная операция, требуемая функцией SIF для обеспечения этой защиты, определяет подходящую модель для использования.

При моделировании функции SIF системы F&G для определения соответствия целям надежности аппаратных средств, напр. PFD, необходимо принимать решения, точно определяющие моделируемую конфигурацию оборудования.

Типичные данные C&E для функции SIF системы F&G включают следующее:

a) любой газовый детектор из шести (1oo6) в состоянии тревоги расценивается как единичная утечка газа и активирует сигнал тревоги в диспетчерской;
b) любые два газовых детектора из шести (2oo6) в состоянии тревоги расцениваются как подтвержденная утечка газа и активируют звуковую и световую сигнализацию на месте, а также генерируют СПАЗ на предприятии.

Однако для правильного моделирования необходимо понимать функцию SIF и угрозу, от которой она защищает. Исполнительная операция, требуемая функцией SIF, определит нужную модель для использования.

12.26. Моделирование конфигураций детекторов для систем F&G

На практике оператор будет исследовать каждую газовую тревогу, чтобы определить, является она реальной, ложной или вызвана сбоем детектора. Исполнительная операция запускается только в результате сигнала о подтвержденной утечке газа, и в этом случае гарантируется эвакуация персонала завода в безопасное место. Это

функция безопасности с необходимым УПБ, поэтому рассмотренный выше случай b) должен стать отправной точкой в нашем моделировании надежности: сигнал о подтвержденной утечке газа гарантирует эвакуацию персонала в безопасное место.

На рис. 44 схематически изображены шесть детекторов присутствия газа, расположенных в некоторой зоне, логическое решающее устройство со схемой 2oo6 сконфигурировано таким образом, что оно запускает исполнительную операцию только в том случае, если 2 детектора из 6 чувствуют газ.

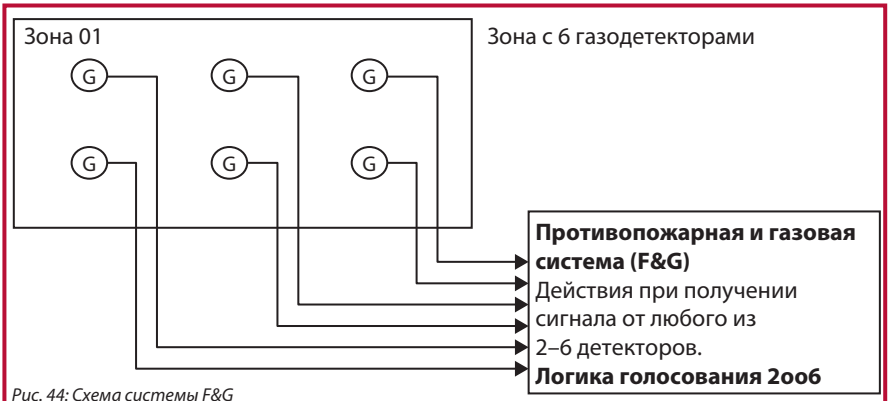


Рис. 44: Схема системы F&G

Однако задачей моделирования функций SIF в отличие от задач PFD является подсчет вероятности того, что на утечку газа не последует реакция. Утечка газа, достаточно большая, чтобы представлять опасность, может произойти только в зоне действия, скажем, половины из 6 детекторов, рис. 45.

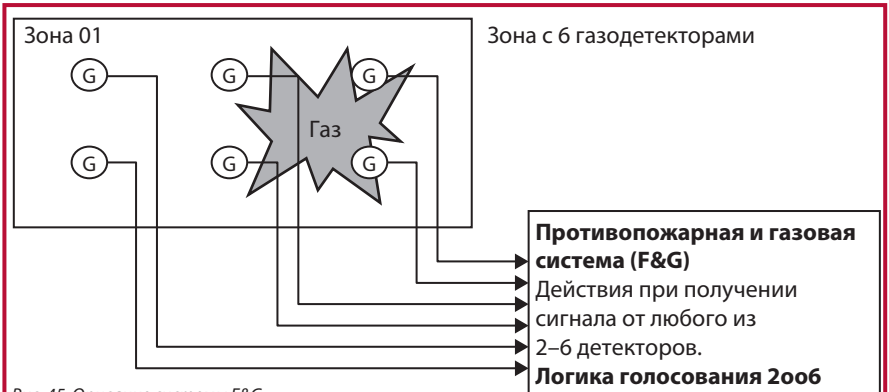


Рис. 45: Описание системы F&G

На практике требуется запуск исполнительной операции как можно раньше, т. е. когда как минимум два датчика покрыты облаком газа. В этом случае следовало бы смоделировать датчики со схемой 2oo2 без резерва. Следовательно, отказ датчика был бы уже недопустим. Если цели достигаются конфигурацией без резерва, такой подход считается консервативным, потому что он не основывается на справедливости каких-либо предположений о зоне действия датчиков.

В реальности PFD подсистемы датчиков часто оказывается лучше расчетного значения для конфигурации без резерва, потому что зоны действия датчиков обычно частично перекрываются из-за своего местоположения и отказ одного датчика может не повлиять на работоспособность системы.

Поэтому при моделировании надежности специалист, занимающийся анализом, должен оценить максимально допустимый размер утечки газа (газового облака) до запуска исполнительной операции и подсчитать, сколько датчиков окажутся в это время под облаком.

В данном примере, если допустить настолько сильную утечку газа, что облако покроет 3 датчика, прежде чем будет запущена исполнительная операция, в логической схеме «2 из 6» можно допустить отказ одного из датчиков. Иными словами, надежность обнаружения утечки газа можно моделировать как 2 из 3.

12.27. Влияние неверного моделирования на PFD

В приведенном выше примере, где газовые детекторы имеют логическую схему 2oo6, некоторые специалисты поддаются искушению смоделировать надежность системы как 2oo6 вместо 2oo3 или даже 2oo2. Очевидно, что результирующее расхождение в общей PFD функции безопасности и ее производительности по отношению к УПБ между конфигурациями с резервированием и без него может быть значительным.

При наличии некоторых предпосылок для нечувствительности к сбоям, напр. при моделировании 2oo3 или 2oo4, результирующие различия в общей PFD функции безопасности и ее производительности по отношению к целям SIL будут невелики. PFD для конфигураций с резервированием ограничена отказами по общей причине, так что улучшения PFD незначительны, когда нечувствительность к сбоям технического обеспечения (HFT) возрастает выше 1.

Однако, если на основании расположения детекторов и допустимых размеров газового облака перед запуском исполнительной операции нельзя сделать вывод о нечувствительности к сбоям, результирующее расхождение между конфигурациями с резервированием и без него может быть значительным, рис. 46.

Примечание. PFD вычисляется для типичных значений частоты отказов датчиков и времени ремонта и предполагает вклад отказов по общей причине для конфигураций с резервированием. Нечувствительность к сбоям, равная нулю, представляет в этом примере конфигурацию 2oo2, нечувствительность к сбоям 1 представляет 2oo3, 2 представляет 2oo4, и так далее.

Результаты показывают, что в зависимости от архитектуры или выбранной HFT для моделирования вычисленная PFD попадет на УПБ SIL1, SIL2 или SIL3.

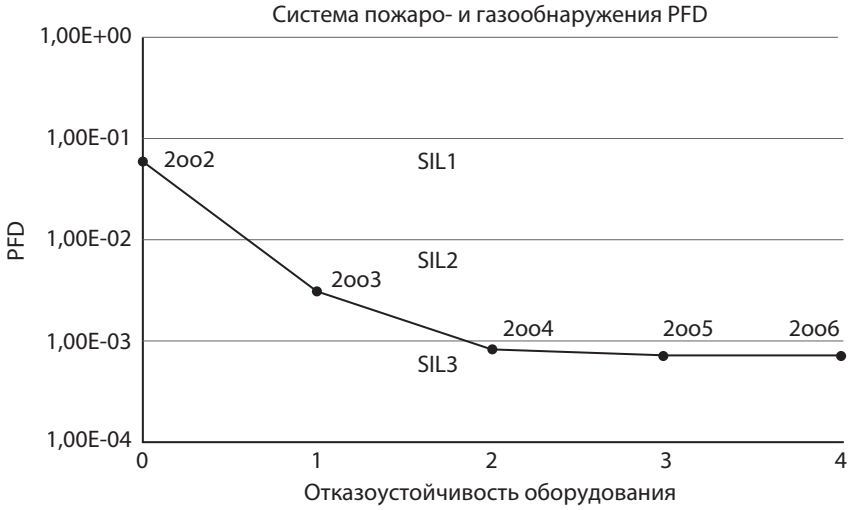


Рис. 46: Расчет PFD системы F&G

12.28. Влияние неверного моделирования на архитектуру

Неверное моделирование сильнее повлияет на архитектурную производительность функции безопасности. Для заданной доли безопасных отказов (SFF) производительность уровня SIL подсистемы детекторов зависит от ее HFT.

Например, для детектора типа B с долей SFF от 60 до 90% можно говорить о следующих возможностях архитектурного уровня SIL.

HFT	Конфигурация	SIL (архитектура)
0	2oo2	SIL1
1	2oo3	SIL2
2	4oo4	SIL3

Опять же, если специалист, проводящий анализ, предполагает конфигурацию 2oo6 на основании логической схемы, оптимистическая архитектура подсказывает уровень SIL3, в то время как в действительности применим только более низкий уровень.

12.29. Моделирование конфигураций сигнализации для систем F&G

Для защиты персонала от пожара и утечек газа служит подтвержденный сигнал тревоги. Звуковые и зрительные сигналы тревоги – это все, что требуется, чтобы обеспечить эвакуацию персонала в безопасное место. Поэтому в случаях угрозы для безопасности, конфигурация на выходе должна лишь позаботиться о наличии зрительных и звуковых сигнальных устройств.

Для систем F&G типичную исполнительную операцию можно определить как активацию зрительных 6oo6 И звуковых 4oo4 сигналов тревоги. При моделировании таких конфигураций, как правило, бывает трудно достичь чего-нибудь лучше, чем цель PGD уровня SIL1, что связано с числом включенных устройств. Кроме того, из-за очень низкой SFF у сигналов тревоги и проблесковых маячков их архитектурная производительность в недублированных конфигурациях обычно не поднимается выше SIL1.

Помня о том, что в зоне может находиться работающее оборудование, которое может помешать увидеть проблесковый маячок или заглушить звуковой сигнал, необходимо стремиться к такому расположению сигнализации, при котором персонал, находящийся в опасной зоне, постоянно мог бы видеть и слышать более чем одно сигнальное устройство. Если это условие выполняется, специалист, занимающийся анализом, может выиграть от такой нечувствительности к отказам в моделировании надежности конфигурации сигналов тревоги.

Конфигурация сигнальных устройств 6oo6 может покрывать 2 или 3 отдельные зоны, притом что в каждой зоне может быть по 2 или 3 сигнальных устройства. Поэтому специалист должен решить на основании схемы завода, какая нечувствительность к сбоям допустима в каждой зоне, и построить соответствующую модель, рис. 47.

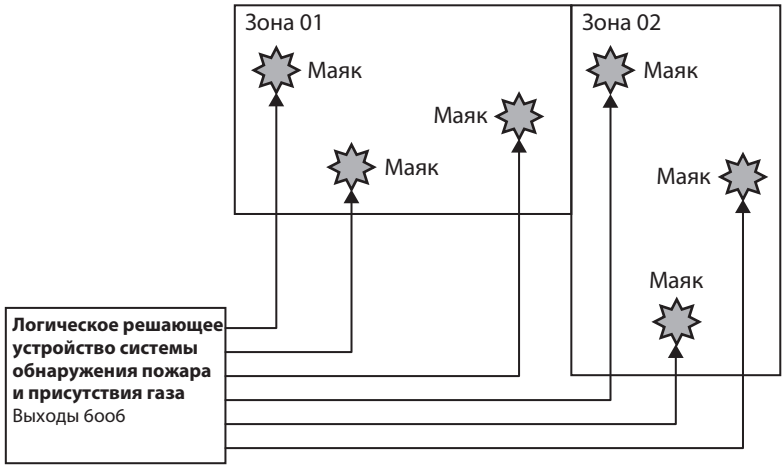


Рис. 47: Пример схемы системы сигнализации

Самое главное – это решить, сколько проблесковых маячков находятся в поле зрения и сколько из них могут отказать, не нанося вреда функции безопасности. На основании нашей учебной схемы было решено, что в каждой зоне два маячка из 3 присутствующих в зоне постоянно находятся в поле зрения.

В случае такой схемы разумным было бы смоделировать каждую зону 1 как 1oo2, так как человеку достаточно увидеть один маячок. Однако, поскольку защищены должны быть обе зоны, их обе нужно включить в модель, т. е. 1oo2 + 1oo2.

В качестве другого примера рассмотрим 6 проблесковых маячков в одной зоне, для которой было установлено, что в любое время 4 из 6 маячков попадают в поле зрения, рис. 48. Тогда требуется, чтобы работал 1 маячок из 4, и можно смоделировать сигналы тревоги как 1oo4.

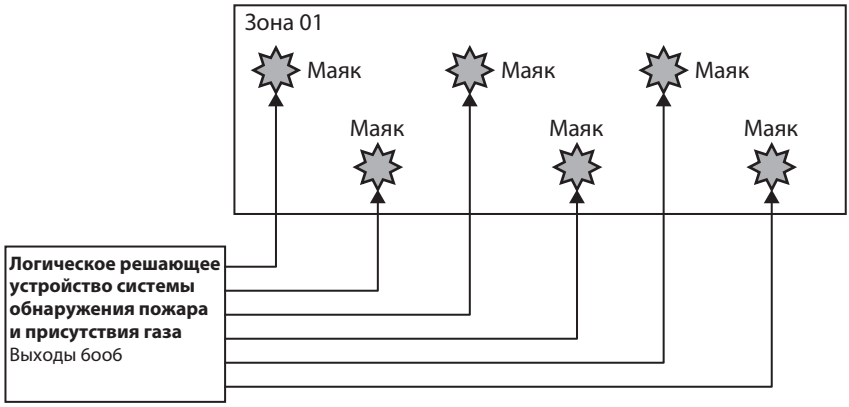


Рис. 48: Пример схемы системы сигнализации (1 зона)

12.30. Входные сигналы F&G в системах аварийного отключения

До сих пор не упоминалось о требовании создать на заводе систему аварийного отключения (СПАЗ) в случае подтвержденного возгорания или утечки газа. Включать ли отключение СПАЗ как часть в функцию SIF F&G, будет зависеть от последствий угрозы и требуемой защиты.

Если угроза приводит к риску для личной безопасности, можно утверждать, что сигналов тревоги достаточно для обеспечения защиты. Обычно отключения F&G также генерируют входной сигнал в СПАЗ, но во многих случаях это происходит для того, чтобы предотвратить эскалацию угрозы и защитить активы. Отключение СПАЗ также может быть инициировано в качестве хорошего средства управления, которое позволяет выполнить запуск после разрешения угрозы под большим контролем. Система F&G предназначена для защиты от огня и газа; СПАЗ предназначена для защиты от других угроз. При условии, что система F&G выполняет свои задачи по снижению риска, для аварийного отключения (СПАЗ) не должно быть причин, помимо описанных выше. Поэтому СПАЗ, как правило, не включается в SIF F&G.

Однако имеются исключения. Когда угроза влечет за собой ущерб для окружающей среды или имущества, сами по себе сигналы тревоги не обеспечивают защиту, поэтому бывает необходимо изолировать предприятие после обнаружения пожара или утечки газа. В таких случаях необходимо включить отключение и изоляцию как требующиеся в моделировании надежности функций SIF системы F&G.

12.31. Обзор

Как видим, моделирование входной подсистемы может дать оптимистичные результаты, если конфигурация логической схемы смоделирована лучше, чем нечувствительность к сбоям детекторов. Тот же метод дает очень пессимистичные результаты при моделировании выходных подсистем. Между двумя подсистемами принятый метод моделирования может привести к большому разбросу в значениях PFD и архитектурной производительности и, следовательно, к большому разбросу в заявленных уровнях SIL.

Поэтому необходим взвешенный подход к моделированию систем F&G, а также четкое понимание приемов моделирования и анализируемых угроз и систем. Тем самым можно достичь точной оценки снижения риска, предоставляемого системой F&G, и не вводить в заблуждение конечного потребителя оптимистичными заявками.

13. Проверка уровней (SIL)

13.1. Соответствие целям уровня полноты безопасности

Многие люди спрашивают, что нужно сделать, чтобы показать соответствие. Недостаточно приобрести компоненты с сертификатом уровня полноты безопасности и думать, что тем самым автоматически достигается соответствие. Вообще, поскольку норма не является предписывающей, невозможно предоставить контрольный перечень того, что нужно сделать. По правде сказать, то, насколько много или мало делается, зависит от разных вещей. Конкретные действия будут зависеть от объема доступной информации и данных, глубина анализа или строгость принятых мер должна устраивать заказчика и органы надзора, но прежде всего необходимо чувствовать, что сделано достаточно.

Если случится авария и кто-нибудь погибнет, сможете ли Вы посмотреть в глаза их близким и сказать, что сделали все от вас зависящее?

Предлагаемый план проверки соответствия отвечает требованиям IEC 61511-1, 10 и 12. В них содержатся следующие подпункты, как показано на рис. 49:

- требования к поведению системы при обнаружении неисправности [13.2];
- аппаратная отказоустойчивость [13.3];
- выбор компонентов и подсистем [13.4];
- полевые устройства [13.5];
- оператор, персонал сопровождения и интерфейсы связи с системой SIS [13.6];
- требования к техническому обслуживанию и разработке тестирования [13.7];
- вероятность отказа функции SIF [13.8];
- прикладное ПО [13.9].

В тех случаях, когда эти пункты делятся на более мелкие требования, они также показаны на рисунке.

Соответствие IEC 61511-1, 5: Управление функциональной безопасностью обсуждается также в разделе [18].

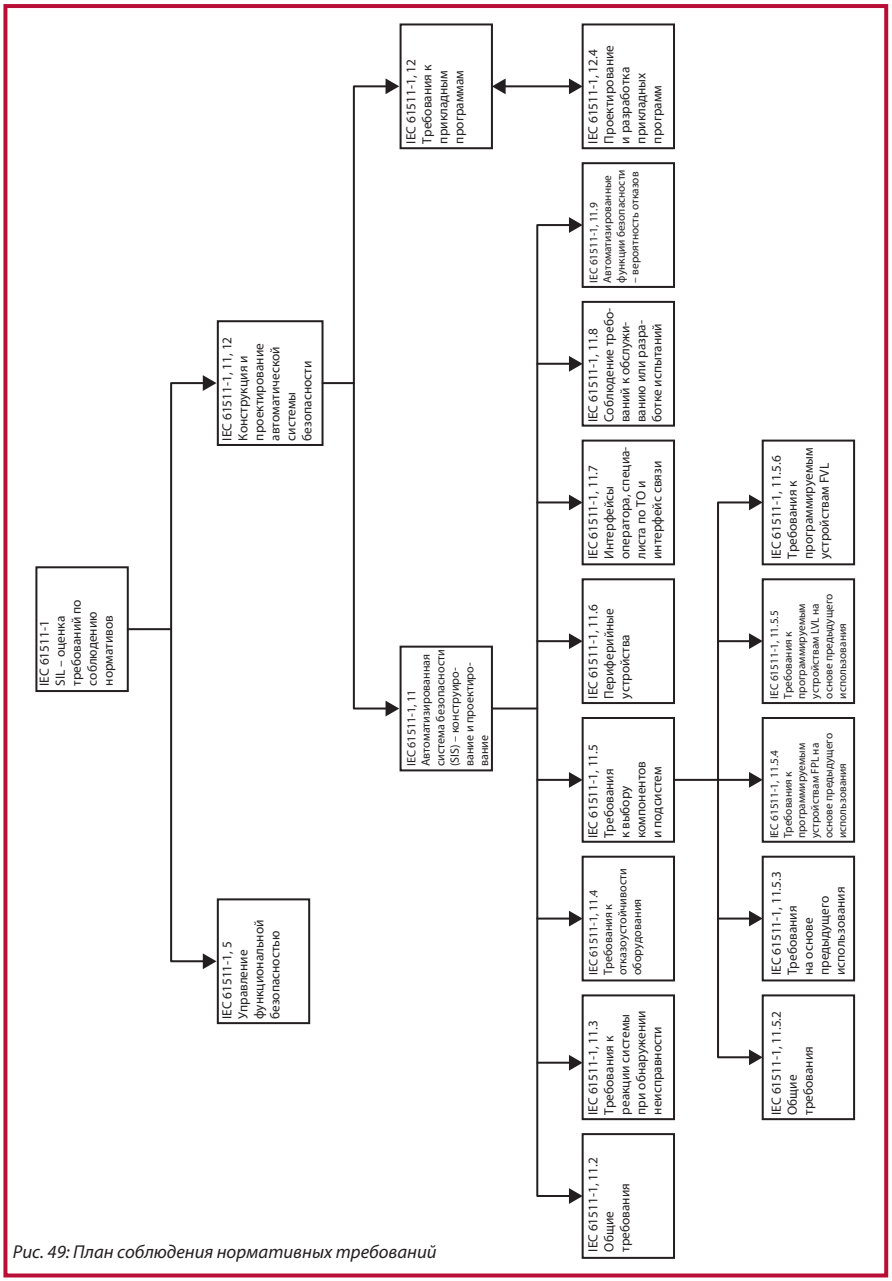


Рис. 49: План соблюдения нормативных требований

13.2. Требования к поведению системы при обнаружении неисправности IEC 61511-1, 11.1

Необходимо определить поведение системы при обнаружении неисправности. Оно может быть подробно описано, например, в спецификации SRS или проектной спецификации.

Ниже показаны типичные примеры тех параметров, которые можно включить в такое писание.

1. Все выходные блоки имеют схему 1oo2 по команде ПЛК и возвращаются к схеме 1oo1, если связь с ПЛК потеряна.
2. В программной спецификации утверждается принцип безопасности при аварии. Все элементы отключения SIS достигают отказа по принципу безопасности.
3. В случае системы СПАЗ использовалась функция отключения путем прекращения подачи энергии.
4. В случае системы F&G реализован метод выпуска огнегасящего состава по принципу срабатывания защиты при подаче питания. Об обнаружении отдельного опасного отказа в конфигурации с резервированием свидетельствует состояние тревоги. Система F&G продолжает работать в безопасном режиме в течение допустимого периода ремонта, также были приняты другие меры по снижению дополнительного риска, такие как предоставление фиксированного ручного спускания огнегасящего состава.

13.3. Требования по нечувствительности к сбоям технического обеспечения, IEC 61511-1, 11.4

13.3.1. Подход

Для соответствия требованиям по нечувствительности к сбоям технического обеспечения (HFT) требуется количественная оценка доли безопасных отказов (SFF) и архитектурных ограничений.

13.3.2. Доля безопасных отказов

В контексте полноты безопасности технического обеспечения самый высокий уровень SIL, который может быть заявлен для функции безопасности, ограничивается HFT и SFF подсистемы, исполняющей функцию безопасности.

Нечувствительность к сбоям технического обеспечения 1 показывает, что архитектура подсистемы такова, что опасный отказ одной из подсистем не мешает выполнению защитного действия, т. е. конфигурация 1oo2 или 2oo3 имеет HFT 1, а конфигурация 1oo3 или 2oo4 имеет HFT 2.

С учетом этих требований IEC 61508 [19.1] дает следующие уточнения:

- нечувствительность к сбоям технического обеспечения, равная N, означает, что N+1 сбоев могут вызвать потерю функции безопасности. При определении нечувствительности к сбоям технического обеспечения другие меры, которые могут контролировать влияние отказов, напр. сообщения об ошибках, не учитываются;
- если один сбой непосредственно приводит к еще одному или нескольким сбоям, все они рассматриваются как один сбой;
- при определении нечувствительности к сбоям технического обеспечения некоторые сбои могут исключаться при условии, что вероятность их появления очень мала относительно требований к полноте безопасности подсистемы. Такое исключение необходимо обосновать и документально подтвердить.

Используются следующие общие соотношения.

$$SFF = \Sigma (\Sigma \lambda_S + \Sigma \lambda_{DD})/(\Sigma \lambda_S + \Sigma \lambda_D)$$ См. IEC 61508-2.C.1

где:

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

Для каждого элемента необходимо вычислить функцию безопасности SFF. Полученное значение используется затем в таблице 16, чтобы определить соответствие SIL для уровня нечувствительности к сбоям технического обеспечения.

13.3.3. Ограничения архитектуры

IEC 61511-1, 11.4.5 предусматривает оценку нечувствительности к сбоям технического обеспечения с использованием требований IEC 61508-2, таблица 2 и 3.

В рамках IEC 61508 [19.1] подсистемы разделяются на типы A и B. Обычно, если типы отказов четко определены и поведение в условиях сбоя может быть полностью задано, а также имеются надежные эксплуатационные данные в достаточном количестве, подсистема причисляется к типу A. Если хотя бы одно из этих условий не выполняется, подсистема причисляется к типу B.

Простые механические устройства, такие как клапаны, в основном относятся к типу A. Логические решающие устройства обычно представляют собой тип B, поскольку они обладают способностью к обработке данных и их поведение в условиях сбоя не может быть полностью задано. Датчики могут принадлежать к типу A или B в зависимости от технологии и сложности устройства.

Архитектурные ограничения для функции безопасности обобщены в таблице 16.

Определение подсистемы типа A: Виды отказа всех составных частей определены однозначно, поведение подсистемы в условиях неисправности полностью определено, на месте собрано достаточно надежных фактических данных для подтверждения заявленной вероятности выявленных и невыявленных отказов.			
Доля безопасных отказов	Отказоустойчивость оборудования (N)		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% – <90%	SIL2	SIL3	SIL4
90% – <99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4
Определение подсистемы типа B: Виды отказа как минимум одной составной части определены неоднозначно или поведение подсистемы в условиях неисправности не определено в полной мере или на месте собрано недостаточно надежных фактических данных для подтверждения заявленной вероятности выявленных и невыявленных опасных отказов.			
Доля безопасных отказов (SFF)	Отказоустойчивость оборудования (N)		
	0	1	2
<60%	Не допускается	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

Таблица 16. Ограничения архитектуры

Примечание. Нечувствительность к сбоям технического обеспечения, равная N, означает, что N+1 сбоев могут вызвать потерю функции безопасности.

13.3.4. Пример

В этом примере, рис. 50, функция безопасности состоит из двух датчиков уровня, работающих в конфигурации 1oo2. Если один из датчиков фиксирует высокий уровень, ПЛК Allen Bradley обесточивает SOV, что позволяет клапану СПАЗ закрыться.

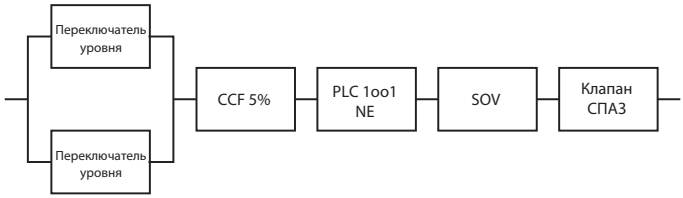
Анализ архитектурной производительности требует прежде всего определить, к какому типу, A или B, относится каждый из элементов. В большинстве случаев это можно сделать, используя определения из таблицы 16. Помните, чтобы отнести элемент к типу A, необходимо точно знать типы отказов и поведение элемента при

отказе, а также иметь очень хорошую статистику отказов. В противном случае элемент следует рассматривать как тип B.

Тогда данные об отказах для каждого элемента позволят подсчитать SFF. Тип элемента и SFF подписаны под каждым элементом на рис. 50.

HFT относится к уровню нечувствительности к сбоям для каждого элемента. Датчики уровня, работающие в конфигурации 1oo2, имеют HFT, равную 1. Все другие элементы не имеют нечувствительности к сбоям, и поэтому HFT у них равна 0.

Наконец, SIL, который может быть заявлен для архитектурной производительности каждого элемента, можно определить, используя информацию из таблицы 16.



Тип	A	B	A	A
SFF	0,40	0,95	0,72	0,25
ДЧО	1	0	0	0
Архитектурный уровень пригодности и безопасности	2	2	2	1
Допустимый уровень пригодности и безопасности (арх.)	1			
Общий разрешенный допустимый уровень пригодности и безопасности	**SIL1**			

Рис. 50: Функция отказа в случае возникновения опасной ситуации

Реле уровня – это тип A, поэтому применимы критерии для типа A. С SFF 0,40 и нечувствительностью к сбоям 1 датчики уровня соответствуют архитектурным ограничениям SIL2.

Аналогично можно оценить SOV и клапан СПА3. SOV, также тип A, имеет нечувствительность к сбоям 0 и SFF 0,72, что дает SIL2. Клапан СПА3, тип A, имеет нечувствительность к сбоям 0 и SFF 0,25, что дает SIL1.

Определение подсистемы типа A: Виды отказа всех составных частей определены однозначно, поведение подсистемы в условиях неисправности полностью определено, на месте собрано достаточно надежных фактических данных для подтверждения заявленной вероятности выявленных и невыявленных отказов.			
Доля безопасных отказов	Отказоустойчивость оборудования (N)		
	0	1	2
<60%	**SIL1 (значение**	**SIL2 (LT)**	SIL3
60% – <90%	**SIL2 (SOV)**	SIL3	SIL4
90% – <99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

Рис. 51. Архитектурные ограничения датчиков уровня

ПЛК относится к устройствам типа B. Это верно для большинства ПЛК, так как они управляются ПО и их поведение в случае отказа имеет элемент неопределенности, следовательно, не все условия, требуемые для типа A, выполняются.

Поэтому оценка ПЛК должна соответствовать требованиям для типа B, рис. 52.

Определение подсистемы типа B: Виды отказа как минимум одной составной части определены неоднозначно или поведение подсистемы в условиях неисправности не определено в полной мере или на месте собрано недостаточно надежных фактических данных для подтверждения заявленной вероятности выявленных и невыявленных опасных отказов.			
Доля безопасных отказов	Отказоустойчивость оборудования (N)		
	0	1	2
<60%	Не допускается	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	**SIL2 (ПЛК)**	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

Рис. 52. Архитектурные ограничения ПЛК

Подводя итоги, можно сказать, что архитектурная производительность SIL для каждого элемента показана на рис. 50, а SIL, который можно заявить для всей функции безопасности, – это SIL1. Архитектурная производительность SIL для всей функции безопасности ограничена самым низким из заявленных SIL.

13.4. Требования к выбору компонентов и подсистем, IEC 61511-1, 11.5

13.4.1. Подход

Выбор компонентов и подсистем для приложений технологического сектора может быть основан на оценке пригодности. В технических требованиях должны быть необходимые условия:

- для выбора компонентов и подсистем;
- для обеспечения возможности интеграции компонента или подсистемы в архитектуру SIF;
- для задания критериев приемлемости компонентов и подсистем.

13.4.2. Общие требования, IEC 61511-1, 11.5.2

Эту процедуру не следует использовать для приложений SIL4, но для всех остальных компонентов и подсистем необходимо обратить внимание на следующее.

Демонстрация пригодности должна включать оценку SIL, состоящую из подсчета PFD и архитектурных ограничений по сравнению с плановыми показателями.

Демонстрация пригодности должна также включать подробное изучение документации производителя к аппаратуре и установленному ПО. На практике сопроводительная документация к выбранным компонентам и подсистемам бывает в форме технических спецификаций, покрывающих функциональные и экологические аспекты эксплуатации. Поэтому FDS должна включать пункт, в котором обосновывается пригодность выбранных компонентов и подсистем, на основе сравнения спецификаций, предоставленных производителем, с функциональными требованиями.

Компоненты и подсистемы должны соответствовать «Спецификации требований к безопасности». На практике компоненты и подсистемы выбираются на основе их способности отвечать требованиям безопасности. Демонстрация соответствия носит оценочный характер, и требования к архитектурным ограничениям и PFD сохраняют свою силу.

13.4.3. Предшествующее применение, IEC 61511-1, 11.5.3

Прежде всего, выбор компонентов должен основываться на спецификации закупок от проверенных поставщиков.

Частью оценки поставщика должно стать рассмотрение QMS и систем управления конфигурацией производителя, которое также вносит свой вклад в доказательство пригодности, представленное в FDS.

Также в FDS должны содержаться сведения о накопленном объеме использования для всех выбранных компонентов и подсистем. Сведения могут основываться:

- на суммарном времени работы устройства для SIL1 и полевых устройств;
- суммарном времени работы устройства с указанием опасных отказов для SIL2 и сложных элементов.

Для логических решающих устройств с SIL3 требуется сертификация.

Требуемый накопленный объем использования для компонента или подсистемы зависит от заданной частоты отказов и отчетов о прежних отказах. Рис. 53 служит исключительно для ориентировки, на нем показано требуемое число накопленных устройство-лет (число устройств x годы в эксплуатации) для различных значений заданной частоты отказов.

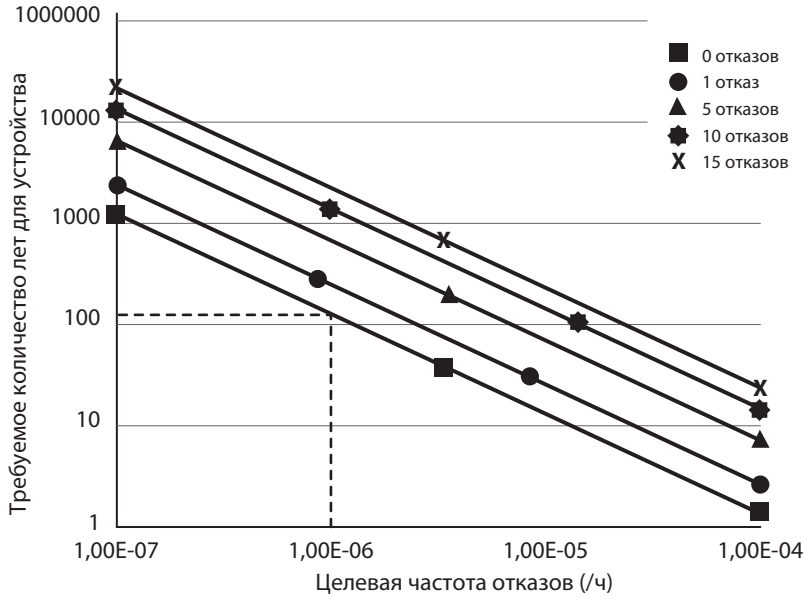


Рис. 53: Руководство по обязательному использованию

Например, если заданная интенсивность отказов составляет 1,00E-06/ч и в отчете зафиксировано 0 отказов, по рис. 53 находим примерно 137 устройство-лет, что достигается, например, при безотказной работе 14 устройств в течение 10 лет. Если в отчете о семействе по месту эксплуатации упоминаются отказы, реальная

интенсивность отказов устройства будет выше и, следовательно, для достижения той же заданной частоты отказов потребуется больше часов безотказной работы.

Рисунок основывается на распределении X^2-с границей доверительного интервала 70% и может служить только для ориентировки и для указания на то, когда будет накоплено достаточное число устройство-лет.

IEC 61511 также требует от производителя ведения отчетности о случаях возврата и внесенных в конструкцию изменениях, что позволяет оценить воздействие заявленных отказов.

На практике информация об отказах редко бывает доступна, поэтому в процессе выбора можно провести экспертизу компонентов и подсистем, чтобы быть уверенным, что они будут функционировать надлежащим образом. Такая экспертиза может потребовать консультаций с другими пользователями или с производителями и пользователями аналогичных устройств и приложений. Такие подкрепляющие доказательства должны быть отражены в FDS как часть пригодности компонентов и подсистем.

13.4.4. Программируемые устройства с фиксированным языком программы (FPL), IEC 61511-1, 11.5.4

В тех случаях, когда необходимо использовать программируемые компоненты и подсистемы с FPL (напр., полевые устройства), для приложений SIL1 и SIL2 должны соблюдаться все общие требования [13.4.2], требования по предшествующему применению [13.4.3] и следующие требования к программируемым компонентам и подсистемам с FPL.

Кроме того, для каждого выбранного компонента в FDS должно приводиться обоснование выбора компонентов FPL, в котором подтверждается, что компонент отвечает указанным требованиям по функциональности, включая:

a) характеристики входных и выходных сигналов;
b) режимы использования;
c) использованные функции и конфигурации;
d) неиспользованные свойства обычно не влияют на функции безопасности.

Для приложений SIL3 требуется официальное заключение.

В качестве альтернативы, которой пользуются некоторые системные интеграторы, можно достать устройство FPL, соответствующее SIL3. Эти устройства должны уже иметь официальное заключение, выданное соответствующей организацией, и сертификат SIL3 вместе с набором подкрепляющей документации.

В ней должно доказываться, что устройство способно выполнять требуемую функцию и что вероятность опасных отказов в результате случайных сбоев аппаратуры или системных сбоев технического и программного обеспечения достаточно мала. Также к устройству должно прилагаться руководство по технике безопасности с перечнем ограничений при эксплуатации и техобслуживании.

13.4.5. Программируемые устройства с языком с ограниченной варьируемостью (LVL), IEC 61511-1, 11.5.5

В тех случаях, когда необходимо использовать программируемые компоненты и подсистемы с LVL (напр., логические решающие устройства), для приложений SIL1 и SIL2 должны соблюдаться все общие требования [13.4.2], требования по предшествующему применению [13.4.3], требования к программируемым устройствам с FPL [13.4.4] и следующие требования к программируемым компонентам и подсистемам с LVL.

В документации должно содержаться обоснование того, что там, где между функциональным разрезом и физической средой в прежнем состоянии и функциональным разрезом и физической средой при использовании в функции безопасности имеется различие, FDS должна констатировать эти отличия и доказывать отсутствие негативных влияний на PFD.

Для приложений SIL1 или 2 можно использовать программируемое электронное (PE) решающее устройство с безопасной конфигурацией (которое является серийным PE логическим решающим устройством общего назначения, конфигурированным специально для использования в приложениях безопасности) при условии, что это обосновывается в документации.

Спецификации, предоставляемые производителем, должны демонстрировать доступность необходимой информации по техническому и программному обеспечению, чтобы обеспечить понимание поведения системы в случае отказа. Для этого в FDS должны быть перечислены все опасные типы отказов с указанием мер диагностики и защиты, если таковые имеются. В FDS должны быть также указаны средства защиты от несанкционированных или непредусмотренных изменений.

Для приложений логических решающих устройств с SIL2 FDS должна утверждать способы защиты от следующих сбоев по время выполнения программы:

a) текущий контроль последовательности программы;
b) защита кода от изменений или обнаружение отказов путем контроля в режиме онлайн;
c) проверка ошибок или многовариантное программирование;
d) проверка диапазона переменных или проверка значений на правдоподобие;

e) модульный подход;
f) для установленного ПО использовался подходящий тип кодирования.

Кроме того, необходимо продемонстрировать следующее:

g) было проведено тестирование в типовых конфигурациях на тестовых примерах, репрезентативных для намеченных функциональных разрезов;
h) использовались проверенные сертифицированные модули ПО и компоненты;
i) система подверглась динамическому анализу и тестированию;
j) система не использует искусственный интеллект или динамическую реконфигурацию;
k) выполнено тестирование с применением имитации отказа, а его результаты отражены в документации.

Для приложений с SIL2 в FDS должны быть указаны ограничения эксплуатации, техобслуживания и обнаружения неисправностей, включая конфигурации PE логических решающих устройств и намеченных функциональных разрезов.

Для приложений с SIL3 в документации должна быть представлена аттестация SIL для любых логических решающих устройств с LVL.

13.4.6. Программируемые устройства с языком с полной варьируемостью (FVL), IEC 61511-1, 11.5.6

В документации должна быть представлена аттестация SIL для любых логических решающих устройств с FVL.

13.5. Полевые устройства, IEC 61511-1, 11.6

При выборе полевых устройств должны соблюдаться все общие требования [13.4.2], требования по предшествующему применению [13.4.3] и следующие требования к полевым устройствам. В соответствующих случаях должны также соблюдаться требования к программируемым устройствам с FPL.

Полевые устройства выбираются и устанавливаются с целью минимизации отказов, которые могут стать причиной неточности информации из-за условий, порождаемых условиями процесса и окружающей среды. К условиям, которые необходимо учитывать, относятся: коррозия, замерзание материала в трубах, взвешенные наносы, полимеризация, синтез, перепады температуры и давления, конденсация в импульсных линиях с сухим коленом и недостаточная конденсация в импульсных линиях с мокрым коленом.

Рабочая документация полевых устройств должна показывать, как компонент справляется со всеми указанными требованиями в смысле функциональности в различных условиях процесса и окружающей среды, а FDS должна подтверждать предоставленные сведения. FDS должна также подтверждать, что все контуры отключения при подаче питания с дискретным входом/выходом применяют метод для обеспечения целостности цепи и полноты подачи энергии, т. е. текущий контроль линии.

«Умные» датчики должны быть защищены от записи, чтобы предотвратить несанкционированное внесение изменений через систему дистанционного управления, однако по результатам соответствующего анализа безопасности можно использовать и вариант «чтение/запись».

13.6. Оператор, персонал сопровождения, интерфейсы связи, IEC 61511-1, 11.7

Все интерфейсы связи должны отвечать следующим требованиям.

Конструкция интерфейса связи SIS должна гарантировать, что любой отказ интерфейса связи не скажется негативно на способности SIS приводить процесс в безопасное состояние. Это должно быть подтверждено в документации проекта.

Документация должна также подтверждать:

a) прогнозируемую частоту отказов коммуникационных сетей;
b) что связь с BPCS и внешними устройствами не повлияет на SIF;
c) что интерфейс связи обладает достаточной прочностью, чтобы противостоять электромагнитным помехам, включая скачки напряжения, не вызывая при этом опасных отказов SIF;
d) что интерфейс связи подходит для коммуникации между устройствами, отнесенными к различным потенциалам заземления. ПРИМЕЧАНИЕ. Может потребоваться материал-заменитель (напр., волоконная оптика).

13.7. Техническое обслуживание или требования к разработке тестирования IEC 61511-1, 11.8

SIS должна быть спроектирована таким образом, чтобы тестирование можно было проводить в сквозном режиме или по частям. При этом следующее рассматривается как приемлемое:

- контрольная проверка в режиме онлайн – разработка тестирования должна обеспечивать обнаружение невыявленных отказов;
- устройства для тестирования и обвода – при обводе любого участка SIS с целью техобслуживания или проверки оператору должен быть направлен сигнал тревоги;

- форсирование входов или выходов без перевода SIS в режим офлайн недопустимо, если на месте отсутствуют соответствующие процедуры и способы защиты. Как и в случае обвода, при форсировании входов/выходов оператору должен быть направлен сигнал тревоги.

13.8. Вероятность отказа SIF, IEC 61511-1, 11.9

См. раздел [14].

13.9. Требования прикладному ПО, IEC 61511-1, 12

В IEC 61511-1, 12 перечисляются требования для всех типов ПО, входящего в состав SIS или используемого при создании SIS. Здесь определены требования к жизненному циклу системы безопасности прикладного ПО, позволяющие гарантировать, что:

- определены все виды деятельности, требующиеся для разработки прикладного ПО;
- полностью определены инструменты ПО, которые используются для разработки и проверки прикладного ПО, т. е. сервисной программы;
- составлен план достижения целей функциональной безопасности.

Общим требованием является определение применимых фаз жизненного цикла системы безопасности ПО, которые следует принять к рассмотрению, и занесение в документацию всей необходимой информации. К документации относится:

- спецификация требований к безопасности ПО – аналогична требованиям к аппаратному обеспечению, необходимо составить спецификацию с четким и хорошо структурированным перечнем всех требований к безопасности ПО, что позволит группе разработчиков создать соответствующее ПО;
- планирование проверки безопасности ПО – это должно быть частью планирования проверки SIS в целом;
- проектирование и разработка – необходимо разработать прикладное ПО, отвечающее требованиям к проектированию системы, перечисленным в SRS ПО, по функциям безопасности и уровням полноты безопасности. Необходимо использовать нужные языки, инструменты программирования и поддержки, помогающие при верификации, проверке, оценке и внесении изменений. Конструкция должна быть поделена на модули и структурирована таким образом, чтобы это позволяло проводить тестирование и вносить изменения. Для проверки правильности функционирования следует выполнить соответствующее тестирование модулей ПО. Заметьте, что проверка должна выполняться для каждой фазы жизненного цикла системы безопасности ПО:

- интеграция – протестированное и проверенное ПО нужно интегрировать в подсистему SIS и еще раз протестировать, чтобы продемонстрировать его соответствие требованиям SRS при работе на аппаратной части;
- проверка безопасности ПО – это должно быть частью проверки SIS в целом (фаза 5);
- внесение изменений – любое внесение изменений в проверенное ПО должно выполняться под контролем, чтобы сохранить целостность ПО.

14. Вероятность отказа SIF, IEC 61511-1, 11.9

14.1. Соответствие стандарту

В предшествующих главах указано на то, что необходимо установить меру заданной надежности, чтобы быть уверенным, что общий риск не превышает максимально допустимый риск.

Также было показано, что мера заданной надежности может выражаться в SIL, и, чтобы соответствовать стандарту, необходимо не только продемонстрировать, что функция безопасности отвечает количественным целевым показателям, но и провести соответствующие проверки.

Соответствие стандарту требует, чтобы достигалась та мера заданной надежности, которая отвечает применяемому SIL.

14.2. Требования к заданной надежности SIL

PFD для каждого SIL зависит от режима работы, в котором предполагается использовать SIS, с учетом частоты делаемых запросов. Режимы описываются в пункте [6.9] и делятся на следующие виды.

Режим управления, в котором указанное действие запускается условиями процесса или другими командами. В случае опасного отказа функции автоматизированной защиты (SIF) потенциальная опасность возникнет только при отказе основной системы управления процессом (BPCS).

Непрерывный режим, в котором в случае опасного отказа SIF потенциальная угроза наступает без дальнейших отказов, если только не предприняты действия по ее предотвращению.

На основе этих критериев можно получить следующие заданные значения надежности, см. таблицу 17.

Уровень SIL	**Режим управления –** вероятность отказа по требованию	**Непрерывный режим** Количество отказов в час
SIL4	$\geq 10^{-5}$, но $<10^{-4}$	$\geq 10^{-9}$, но $<10^{-8}$
SIL3	$\geq 10^{-4}$, но $<10^{-3}$	$\geq 10^{-8}$, но $<10^{-7}$
SIL2	$\geq 10^{-3}$, но $<10^{-2}$	$\geq 10^{-7}$, но $<10^{-6}$
SIL1	$\geq 10^{-2}$, но $<10^{-1}$	$\geq 10^{-6}$, но $<10^{-5}$

Таблица 17. Требуемая величина PFD для SIL и интенсивность отказа

14.3. Подсчет PFD для функции безопасности в режиме управления

При подсчете надежности предполагается, что отказы происходят в случайном порядке с постоянной частотой и что после отказа неисправный элемент остается недоступным, пока отказ не будет обнаружен и устранен.

При подсчете PFD по сути дела подсчитывается вероятность того, что SIS будет недоступна в тот момент, когда к ней поступит запрос. Для резервированной системы 1oo2 при условии, что произошел отказ одного канала, PFD представляет собой вероятность того, что второй канал также откажет в период простоя первого.

Следующие общие соотношения могут быть полезны при подсчете PFD. Используемые уравнения являются упрощенной формой стандартных уравнений, их вывод приводится в пункте [19.6].

Для выявленных отказов:

$PFD1oo1 = \lambda_{DD}.MDT$	См. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DD}^2.MDT^2 + \beta.\lambda_{DD}.MDT$	См. IEC 61508-6, B.3.2.2.2

Для невыявленных отказов:

$PFD1oo1 = \lambda_{DU}.T_P/2$	См. IEC 61508-6, B.3.2.2.1
$PFD1oo2 = \lambda_{DU}^2.Tp2/3 + \beta.\lambda_{DU}.T_P/2$	См. IEC 61508-6, B.3.2.2.2

где λ_{DD} – частота опасных выявленных отказов, λ_{DU} – частота опасных невыявленных отказов, а β – вклад отказов по общей причине, пункт [12.17]. T_P – интервал между контрольными проверками, а MDT – среднее время простоя.

Общие формы этих уравнений для различных конфигураций, для систем как с непрерывным режимом, так и с режимом управления, рассмотрены в [12.9].

14.4. Значения частоты отказов

При расчетах PFD и SFF в анализе используется основная гипотеза IEC 61508-6, приложение B.3, согласно которой интенсивность отказов компонента считается константной на протяжении всего срока службы системы.

Значения частоты отказов, используемые в расчетах, могут быть получены через FMECA, из эксплуатационных данных путем квантификации или по ссылке на опубликованные данные в промышленных источниках. Используемые значения частоты отказов следует сравнить с доступными данными для аналогичных по сложности и техническим характеристикам модулей. Такой метод гарантирует

консервативный подход к моделированию надежности и дает уверенность в том, что вычисленные показатели надежности будут достигнуты в реальности.

Частоты отказов и их источники обсуждаются в пункте 14.8.

14.5. Моделирование надежности

В этом примере из [6.5] выделены процесс и SIF, рис. 54.

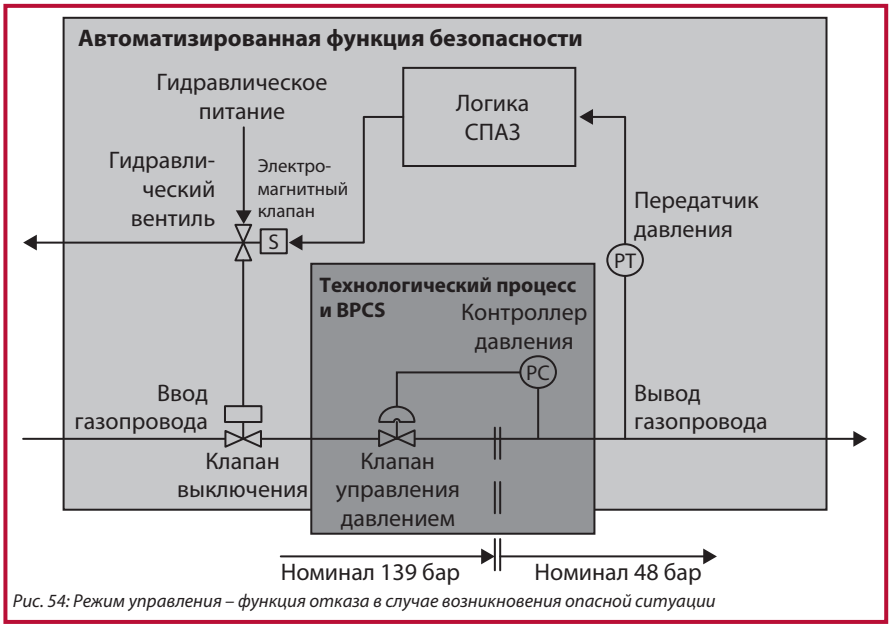


Рис. 54: Режим управления – функция отказа в случае возникновения опасной ситуации

Подсчет PFD легче всего выполняется с помощью техники блок-схемы расчета надежности (Reliability Block Diagram, RBD). В RBD схемы показывают элементы или компоненты, необходимые для надежной системы, и не обязательно отображают физические планировки и связи. Моделирование RBD описано в IEC 61508-6, дополнение B, 4.2.

Здесь приведена RBD для описанной SIS, рис. 55.

	Передатчик давления	Логика СПАЗ	Электромагнитный клапан	Клапан выключения
λDD	2,64E-07	3,42E-06	0,00E+00	0,00E+00
MTD	48	48	48	48
PFD конфигурации	1,27E-05	1,64E-04	0,00E+00	0,00E+00
λDU	4,00E-08	1,63E-07	6,00E-07	4,64E-06
Период контрольной проверки	8760	8760	8760	8760
PFD конфигурации	1,75E-04	7,14E-04	2,63E-03	2,03E-02
PFD (выведено)	177E-04			
PFD (не выведено)	2,38E-02			
PFD	2,40E-02			
Допустимый уровень пригодности и безопасности (PFD)	SIL1			

Рис. 55: Режим управления – функция безопасности

Эта RBD иллюстрирует подсчет PFD. Элементы ниже – значения для λ_{DD} (интенсивность опасных обнаруженных отказов), λ_{DU} (интенсивность опасных необнаруженных отказов), MDT, среднее время простоя и период контрольной проверки T.

14.6. Пример оценки уровня полноты безопасности модификации форполимерной петли режима управления

Ниже описан пример оценки SIL PFD и архитектурная производительность SIF.

Область задачи

СПАЗ-функция S-005 предотвращает неуправляемую реакцию в 39-R-050 и, таким образом, защищает от утечку из реактора, которая может привести к травмам оператора и последующему экологическому ущербу. В настоящий момент функция безопасности S-005 инициируется при регистрации высокой температуры или высокого давления в реакторе; при этом стравливающий клапан ROV0503 открывается для сброса давления.

Существовали понятные опасения, что ROV0503 может не обеспечить достаточной пропускной способности в случае стравливания, и поэтому СПАЗ-действие функции S-005 было изменено и стало задействовать дополнительный стравливающий клапан ROV0501.

Кроме того, в ходе программы обновления были добавлены два ручных выключателя (разрешительный выключатель HS0900 и выключатель обхода автоматики HS2004) для целей техобслуживания.

Цели

В составе этой SIS клиент эксплуатирует большое количество сенсоров и стремится уменьшить связанные с ними издержки. Таким образом, этот анализ имеет следующие цели.

1. Определить, какие элементы следует включить в анализ измененной СПАЗ-функции безопасности S-005.
2. Построить RBD для определения PFD и архитектуры S-005.
3. Предложить концепцию контрольного испытания (промежутки между испытаниями для сенсоров, ручных выключателей, логики и стравливающих клапанов), позволяющую достичь целей (таблица 18), минимизировав частоту испытаний сенсоров.

Примечание. Клиент заявил, что промежутки между контрольными испытаниями для любого элемента не должны превышать 36 месяцев. С инженерной точки зрения клиента не устраивает, что части SIS не будут проверяться в течение долгого времени.

Разрешительный сигнал и обход автоматики

С СПАЗ S-005 ассоциированы два выключателя – HS2004 и HS0900.

Очевидно, что HS0900 используется для подачи катализатора в реактор и, соответственно, его неверное положение или отказ в неверном положении не создают фактора риска. HS2004 блокирует аварийный останов в функции S-005. Если HS2004 будет непреднамеренно оставлен в положении обхода автоматики после техобслуживания или даст сбой в этом положении, функция безопасности S-005 окажется отключена.

Конфигурация оборудования

Логическое решающее устройство основано на конфигурации тройного модульного резервирования (Triple Modular Redundant, TMR) с принятием решения по 2 элементам из 3 (2 out of 3, 2oo3). На рис. 56 представлена схема конфигурации оборудования.

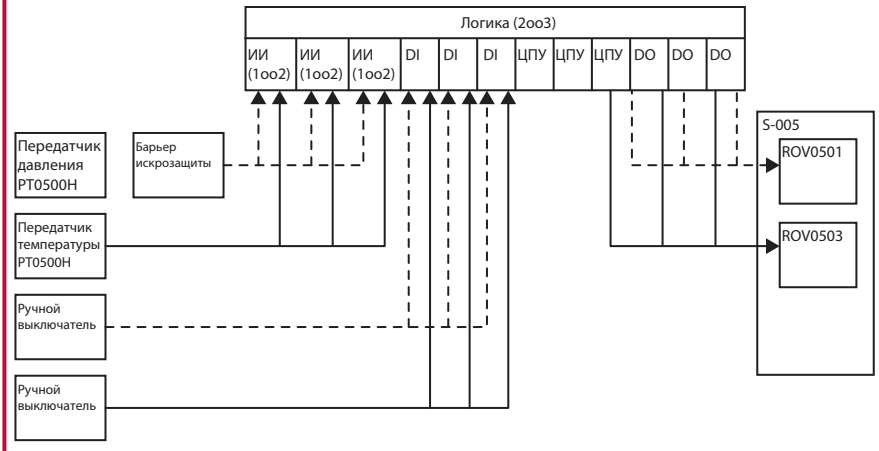


Рис. 56: Схема оборудования

Анализ функций безопасности

В таблице 18 представлены намеченные цели SIL и PFD.

Контур	**Инициатор**	**Действие СПАЗ**	**Необходимые условия для предотвращения опасности**	**Целевое значение PFD**	**Целевое значение SIL**
1	Высокое давление [PT0500H] или высокая температура [TT0504HH]	Активация S-005	ROV0503 и ROV0501 разомкнуты	5,56E-03	SIL2

Таблица 18. Функции безопасности для анализа

Диагностическое покрытие

Предполагается, что все необнаруженные виды ошибок будут выявлены в контрольном испытании, т. е. при полном исполнении функции SIS.

Среднее время простоя

В этом анализе следует использовать MDT, равное 72 ч.

Период контрольной проверки

Интервалы между контрольными испытаниями следует выбрать таким образом, чтобы достичь целей, при этом максимизировав промежуток между контрольными испытаниями для сенсоров.

Учет отказов с общей причиной (Common Cause Failures, CCF)

CCF – это отказы, которые могли быть порождены одной причиной, но одновременно влияют более чем на один канал. Они могут быть вызваны системной ошибкой, например ошибкой проектной спецификации или внешним воздействием, таким как экстремальная температура, которая может привести к отказу компонентов в обоих резервированных каналах.

Вклад CCF в нагруженные резервные пути должен учитываться в модели путем включения β-фактора. Интенсивность CCF-отказов, включенная в расчет, равна β x общая интенсивность отказов одного из резервных путей. β-факторы, используемые в анализе, подытожены в таблице 19.

Избыточная конфигурация	***β* Фактор**	**Обоснование**
Датчики PT0500, TT0504	3%	Поскольку датчики основаны на различных технологиях и измеряют различные переменные процесса, вероятность отказов, обусловленных общей причиной, ограничивается самим процессом, механизмом крепления датчиков и способом прокладки проводов и изоляции соединений датчиков. В связи с этим считается, что величина 3% обеспечивает достаточный запас.
Логика PLC TMR	5%	Отказы в избыточной конфигурации TMR, обусловленные общей причиной, редки, однако, следуя консервативному подходу, применяется значение 5%.

Таблица 19: β факторы

Компоненты типа A

Следующие элементы могут быть отнесены к типу A:

- барьер искрозащиты (устройство развязки электропитания передатчика; PB0500);
- датчик температуры (TT0504);
- ручной выключатель (HS0900, HS2004);
- стравливающие клапаны преполимеризации.

Компоненты типа B

Следующие элементы были отнесены к типу B:

- модули логики ПЛК;
- датчики давления (PT0500).

Значения частоты отказов компонентов

Анализ должен предполагать постоянные интенсивности отказов, поскольку ожидается, что эффекты ранних отказов будут ликвидированы соответствующими процессами. Эти процессы включают использование освоенных изделий из утвержденных источников, внутреннее тестирование перед поставкой и расширенное эксплуатационное и функциональное тестирование в рамках установки, наладки и пуска. Данные по рекламационным возвратам на других сходных проектах показывают, что отказы в начальном периоде эксплуатации не приводят к значительному количеству возвратов; таким образом, можно считать используемые методы успешными.

Также предполагается, что компоненты не эксплуатируются дольше их срока эксплуатации; это обеспечивает отсутствие отказов из-за износа механизмов. Значения частоты отказов (в отказах/час), которые можно использовать в модели при подсчете PFD, λ_{DD} и λ_{DU}, сведены в таблице 20. Значения частоты отказов были получены нескольких источников.

Элемент/ тег	Описание	λ	λD	λDU	λDD	λS	SFF
Устройства ввода							
PT 0500	Датчик давления (IS)	1,5E-06	1,4E-06	6,0E-07	7,5E-07	1,5E-07	0,60
PT 0501	Датчик давления (IS)	1,5E-06	1,4E-06	6,0E-07	7,5E-07	1,5E-07	0,60
PB 0500	Барьер – для PT выше (не-IS)	2,1E-07	6,3E-08	6,3E-08	0,0E+00	1,5E-07	0,70
PB 0501	Барьер – для PT выше (не-IS)	2,1E-07	6,3E-08	6,3E-08	0,0E+00	1,5E-07	0,70
FT 0041	Расходомер Кориолиса	2,6E-06	2,2E-06	9,0E-07	1,3E-06	4,0E-07	0,65
TT 0504	3-проводный РДТ с установленным впереди передатчиком	2,0E-06	1,4E-06	4,0E-07	1,0E-06	6,0E-07	0,80
HS 2004	Переопределяющий переключатель	2,00E-06	8,00E-07	8,00E-07	0,00E+00	1,20E-06	0,60
HS0900	Разрешающий переключатель	2,00E-06	8,00E-07	8,00E-07	0,00E+00	1,20E-06	0,60
Логические устройства							
ЦПУ	ЦПУ	1,51E-06	5,16E-07	6,42E-09	5,09E-07	9,91E-07	1,00
Модуль цифровых входов 32pt	Модуль цифровых входов 32pt	2,19E-08	1,09E-08	9,91E-11	1,08E-08	1,09E-08	0,99
Модуль аналоговых входов 32pt	Модуль аналоговых входов 32pt	1,40E-08	7,00E-09	9,86E-11	6,90E-09	7,00E-09	0,99
Модуль цифровых выходов 16pt	Модуль цифровых выходов 16pt	2,95E-08	1,47E-08	9,93E-11	1,46E-08	1,47E-08	0,99
Устройства вывода							
39-PM-050	Состояние работы насоса от контактора при нормально разомкнутом контакте реле	3,0E-07	2,0E-07	1,95E-07	0,00E+00	1,05E-07	0,35
ROV 0501	Перепускной клапан AOV (FO), включая SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734
ROV 0503	Перепускной клапан AOV (FO), включая SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734
ROV 0404	AOV (FC) включая SOV	9,72E-06	3,03E-06	3,03E-06	0,00E+00	6,69E-06	0,688
ROV 0405	Перепускной клапан AOV (FO), включая SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734
ROV 0406	Перепускной клапан AOV (FO), включая SOV	5,07E-06	1,35E-06	1,35E-06	0,00E+00	3,72E-06	0,734

Таблица 20. Значения частоты отказов (1/ч.) и расчет SFF

Одно возможное решение

Этот анализ имеет следующие цели.

1. Определить, какие элементы следует включить в анализ измененной СПАЗ-функции безопасности S-005.
2. Построить RBD для определения PFD и архитектуры S-005.
3. Предложить концепцию контрольного испытания (промежутки между испытаниями для сенсоров, ручных выключателей, логики и стравливающих клапанов), позволяющую достичь целей (таблица 18), минимизировав частоту испытаний сенсоров.

В RBD на рис. 57 приведены элементы, необходимые в составе функции безопасности. Нет нужды включать в оценку функции безопасности HS0900, так как его отказ не может помешать работе функции безопасности. Если HS0900 откажет или будет оставлен в неправильном положении, это не создаст фактора риска.

HS2004 же следует включить в оценку, поскольку, если он будет непреднамеренно оставлен в положении обхода автоматики после техобслуживания или даст сбой в этом положении, функция безопасности S-005 окажется отключена.

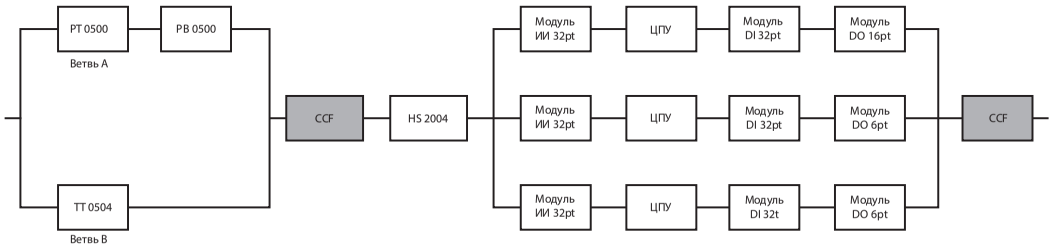
Расчет PFD потребовал некоторой рассудительности в отношении установки промежутков между контрольными испытаниями, Tp. Стояло требование максимизировать промежутки вплоть до 3 лет, пока это не мешает достижению цели PFD. Здесь может быть много возможных решений, и на практике это обычно обсуждается с клиентом. Возможная концепция контрольного испытания представлена в таблице 21.

Периодичность контрольных испытаний (датчики)	24	мес.	17 520	час
Периодичность контрольных испытаний (рубильник)	6	мес.	4380	час
Периодичность контрольных испытаний (логические схемы)	36	мес.	26 280	час
Периодичность контрольных испытаний (клапаны)	3	мес.	2190	час

Таблица 21. Возможные интервалы между контрольными испытаниями

Эти интервалы между контрольными испытаниями обеспечивают расчетную PFD 4,91E-03 против целевой 5,56E-03; PFD и архитектурная производительность удовлетворяют цели SIL2.

Рис. 57: RBD решения



Доля CCF			3%						5%
Кол-во	1	1		1	1	1	1	1	1
Конфигурация		1oo2						2oo3	
λ.DD [Ветвь A]	7,50E-07	0,00E+00	2,25E-08	0,00E+00	6,90E-09	5,09E-07	1,08E-08	1,46E-08	2,71E-08
λ.DD [Ветвь B]	1,00E-06	0,00E+00							
λ.DD для ветви			2,25E-08	0,00E+00				5,42E-07	2,71E-08
MDT		72	72	72				72	72
КонфигурацияPFD		3,89E-09	1,62E-06	0,00E+00				4,56E-09	1,95E-06
λ.DU [Ветвь A]	6,00E-07	6,30E-08	1,99E-08	8,00E-07	9,86E-11	6,42E-09	9,91E-11	9,93E-11	3,36E-10
λ.DU [t-Ветвь B]	4,00E-07	0,00E+00							
λ.DU для ветви			1,99E-08	8,00E-07				6,72E-09	3,36E-10
Период контрольной проверки, T		17 520	17 520	4380				26 280	26 280
Конфигурация PFD		2,71E-05	1,74E-04	1,75E-03				3,11E-08	4,41E-06

PFD (выведено)	3,58E-06
PFD (не выведено)	4,91E-03
PFD	4,92E-03
Допустимый уровень пригодности и безопасности (PFD)	2

Тип	B	A	A	B	B	B
SFF	0,60	0,70	0,60	>99	>99	>99
Резервирование	1	0	0	1	1	1
Архитектурный уровень пригодности и безопасности	2	2	2	3	3	3
Допустимый уровень пригодности и безопасности (арх.)	2					

14.7. Отслеживаемость данных по интенсивности отказо .

При выполнении расчетов PFD важно, чтобы все расчеты были наглядными, а все используемые данные отслеживались до источника. Microsoft Excel – полезный инструмент в этом плане, так как удовлетворяет обоим этим требованиям и позволяет представлять разрабатываемую модель надежности в графическом виде, как на рис. 57.

Таблица позволяет каждой ячейке данных указывать на таблицу с данными, где могут быть представлены все собранные данные по интенсивности отказов и источникам данных. Пример таблицы с данными представлен в таблице 22. Важно, что ссылка на источник данных достаточно детализирована, это дает возможность в любой момент проверить и подтвердить используемые значения.

При использовании формата Excel удобно также перечислять списком типы компонентов и предполагаемые MDT и Tp, используемые в расчете. Это дает возможность легко изменять интервалы между контрольными испытаниями – эффект на PFD при этом будет подсчитываться автоматически.

Наименование/ номер по каталогу	**λ**	**λD**	**λDD**	**λDU**	**λS**	**Тип**	**SFF**	**MDT**	**Tp**	**Источник данных**
PT0500	1,35E-06	8,18E-07	7,50E-07	6,80E-08	5,27E-07	B	0,95	4380	4380	exida [14.8.2]
SIL3 Логическое устройство	5,57E-06	2,23E-06	2,21E-06	2,20E-08	3,34E-06	B	1,00	168	4380	Sintef [14.8.8]
Модуль аналоговых входов	1,07E-06	5,34E-07	5,08E-07	2,60E-08	5,34E-07	B	0,98	168	4380	Sintef [14.8.8]
Модуль цифровых выходов	5,26E-07	2,63E-07	2,50E-07	1,30E-08	2,63E-07	B	0,98	168	4380	Sintef [14.8.8]
12" клапан HIPPS	5,29E-06	2,12E-06	0,00E+00	2,12E-06	3,17E-06	A	0,60	730	4380	Oreda 2002 [14.8.6]

Таблица 22. Типичная таблица с данными

14.8. Источники данных по интенсивности отказов

14.8.1. Подход

Данные по интенсивности отказов следует получать только из надлежащих источников, в зависимости от сферы применения. Здесь перечислены использованные источники данных, подходящие для данного сектора.

14.8.2. Exida.com Safety Equipment Reliability Handbook, 2007, 3rd Edition Volume 1 – Sensors, ISBN 978-0-9727234-3-5/Volume 2 – Logic Solvers and Interface Modules, ISBN 978-0-9727234-4-2/Volume 3 – Final Elements, ISBN 978-0-9727234-5-9

14.8.3. Handbook of Reliability Data for Electronic Components used in Telecommunications Systems, HRD-5.

14.8.4. Hydrocarbon Leak and Ignition Database Report No. 11.4/180 May 1992

14.8.5. IEEE Standard 500-1984. Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data.

14.8.6. OREDA, The Offshore Reliability Data Handbook 4th Edition 2002 ISBN 82-14-02705-5

14.8.7. Parloc 2001: 5th Edition, The Institute of Petroleum, published by the Energy Institute ISBN 0 85293 404 1.

14.8.8. Reliability Data for Control and Safety Systems, 2006 Edition, PDS Data Handbook, SINTEF, ISBN 82-14-03898-7.

14.8.9. Reliability Technology, AE Green and AJ Bourne, Wiley, ISBN 0-471-32480-9.

15. Установка, сдача в эксплуатацию и валидация, IEC 61511-1, 14, 15

15.1. Фазы жизненного цикла

На рис. 58 показана актуальная фаза жизненного цикла.

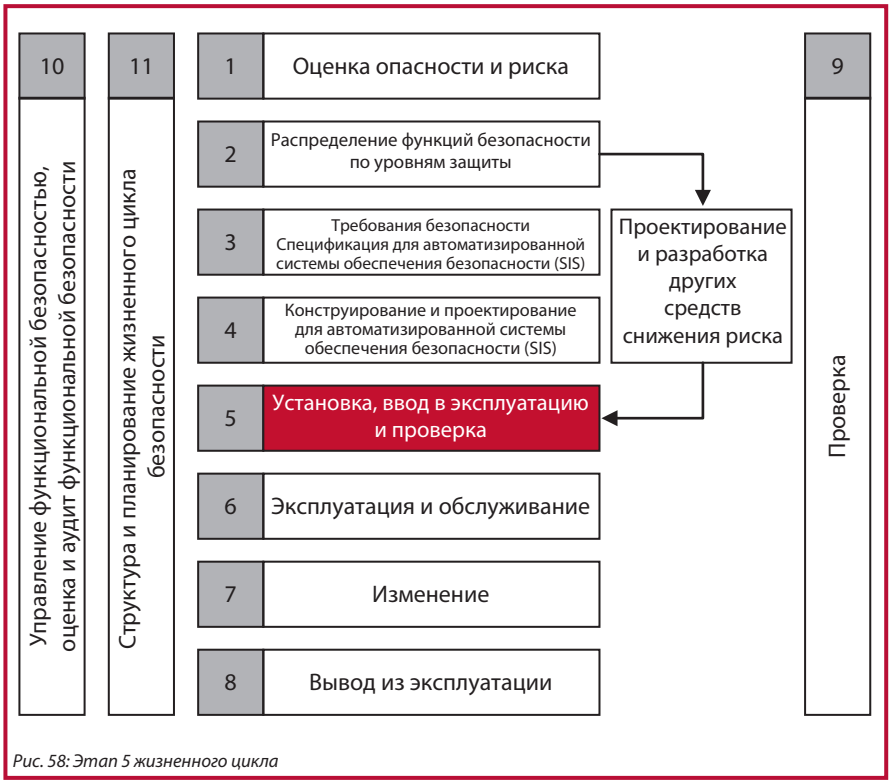


Рис. 58: Этап 5 жизненного цикла

Цели фаз определенные в IEC 61511-1, 14 и 15, таковы:

- установить SIS в соответствии с техническими характеристиками и документацией [15.2];
- сдать SIS в эксплуатацию для подготовки к окончательной валидации системы [15.3];
- подтвердить, что установленная и введенная в эксплуатацию SIS соответствует требованиям, определенным в SRS [15.4].

15.2. Установка SIF

Требования к установке должны быть определены в «Плане установки, наладки и пуска» либо содержаться в общем плане проекта. Процедуры установки должны определять необходимые работы, технику и методы, персонал, ответственные подразделения или организации и график работ по установке.

15.3. Сдача SIF в эксплуатацию

SIS должна быть сдана в эксплуатацию в соответствии с планом и процедурами. Должен быть составлен протокол результатов испытаний и их соответствия критериям, определенным на этапе проектирования. Отказы должны быть исследованы и запротоколированы. Если в каких-то областях фактическая установка не соответствует проектной информации, следует исследовать различия и определить их влияние на безопасность.

15.4. Валидация SIF

Процедуры валидации должны включать в себя все режимы функционирования процесса и соответствующего оборудования, а также:

- пуск, штатный режим работы, останов;
- ручной или автоматический режим работы;
- режимы обслуживания, байпасы;
- синхронизацию;
- должностные обязанности;
- порядок поверки и калибровки.

Кроме того, валидация прикладного ПО должна включать следующее:

- определение ПО для каждого режима функционирования;
- используемую процедуру валидации;
- используемые инструменты и оборудование;
- критерии приемлемости.

Валидация должна подтверждать, что SIS нормально функционирует во всех режимах работы и не подвержена воздействию BPCS и иных подключенных систем. Валидация эксплуатационных качеств должна подтверждать работоспособность всех резервных каналов, байпасов, обходов при пуске оборудования и ручных систем останова.

При потере энергии (электрической, гидравлической или пневматической мощности) оборудование должно приходить в определенное или безопасное состояние. Диагностические сигнальные функции, определенные в SRS, должны функционировать и работать согласно указанному при недопустимых параметрах процессу, например

при входных значениях вне допустимого диапазона. По итогам валидации должен быть составлен соответствующий протокол с идентификацией элемента, оборудования, документации и результатов испытания, включая все несоответствия, а также запросы на анализы и изменения, сформированные по итогам.

16. Эксплуатация и техническое обслуживание, IEC 61511-1, 16

16.1. Фазы жизненного цикла

На рис. 59 показана актуальная фаза жизненного цикла.

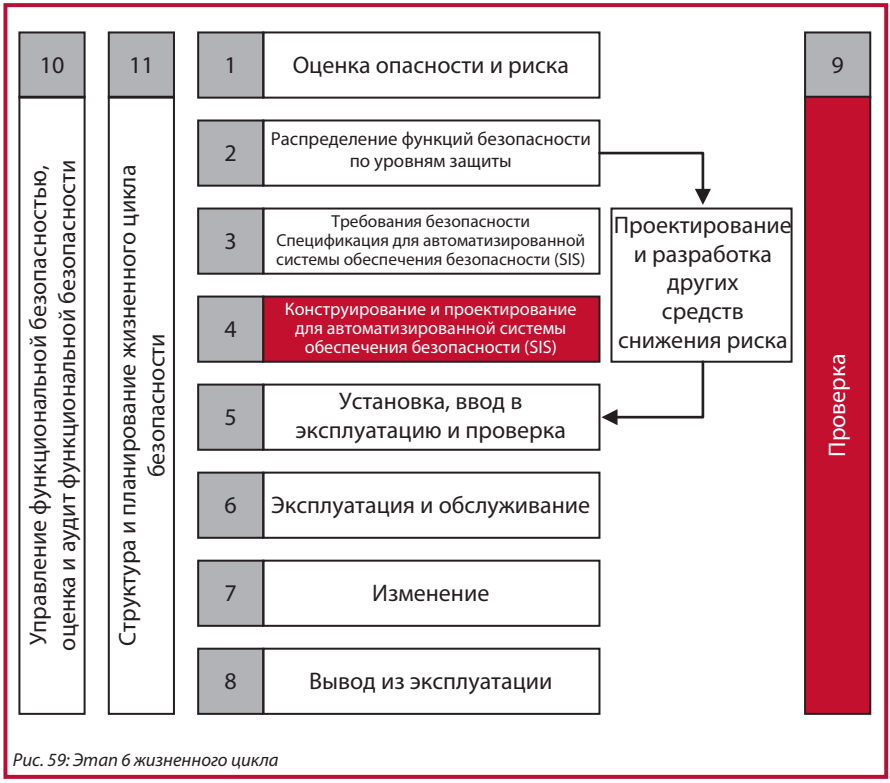


Рис. 59: Этап 6 жизненного цикла

Цели этой фазы, определенные в IEC 61511-1, 16.1, таковы:

- обеспечить соблюдение необходимого SIL каждой SIF во время эксплуатации и технического обслуживания [16.2];
- эксплуатировать и обслуживать SIS для соблюдения проектной функциональной безопасности [16.3].

16.2. Эксплуатация и обслуживание SIF (Operation and Maintenance, O&M)

Требования к O&M должны быть определены в «Плане эксплуатации и технического обслуживания» либо содержаться в общем плане проекта. Процедуры O&M должны

определять штатный режим деятельности, которого необходимо придерживаться для обеспечения функциональной безопасности. Этот режим должен включать требования для:

- контрольных испытаний;
- байпаса SIF для испытания или ремонта;
- штатного сбора данных, в т. ч. результатов проверок и испытаний в SIS, протоколов требований SIF, отказов и ремонтов, простоев из-за контрольных испытаний.

Процедуры контрольных испытаний должны быть разработаны так, чтобы испытывалась каждая SIF для выявления опасных отказов, остающихся необнаруженными при диагностике [16.4].

Должны иметься процедуры технического обслуживания для диагностики неисправностей, ремонта, повторной валидации системы после ремонта, мер при обнаружении рассогласования между ожидаемым и фактическим поведением, калибровки и обслуживания контрольно-испытательной аппаратуры, технической отчетности.

Должны иметься процедуры отчетности для отчетов об отказах, анализа систематических отказов и отказов с общей причиной, отслеживания ремонтных показателей.

16.3. Обучение по O&M

Обучение персонала, занятого в O&M, должно быть заранее запланировано и произведено в удобное время, чтобы SIS смогла эксплуатироваться и обслуживаться в соответствии с SRS. Обучение должно включать следующие разделы:

- факторы риска;
- граничные значения для отключения;
- меры противодействия в аварийной ситуации;
- действие всех байпасов и все ограничения при их использовании;
- режим ручного управления, например при запуске и останове, и все ограничения при его использовании;
- функционирование имеющегося оборудования аварийной сигнализации и диагностики.

16.4. Контрольное испытание

Процедуры контрольного испытания должны испытывать всю SIF – от датчиков до конечного действующего устройства. Интервал между контрольными испытаниями должен соответствовать использованному при квантификации PFD [14].

Допустимо испытывать разные элементы SIF с разными интервалами, если:

- расчетная PFD по-прежнему приемлема;
- испытания перекрывают друг друга так, что ни одна часть SIF не остается неиспытанной.

17. Модификация и вывод из эксплуатации, IEC 61511-1, 17, 18

17.1. Фазы жизненного цикла

На рис. 60 показаны актуальные фазы жизненного цикла.

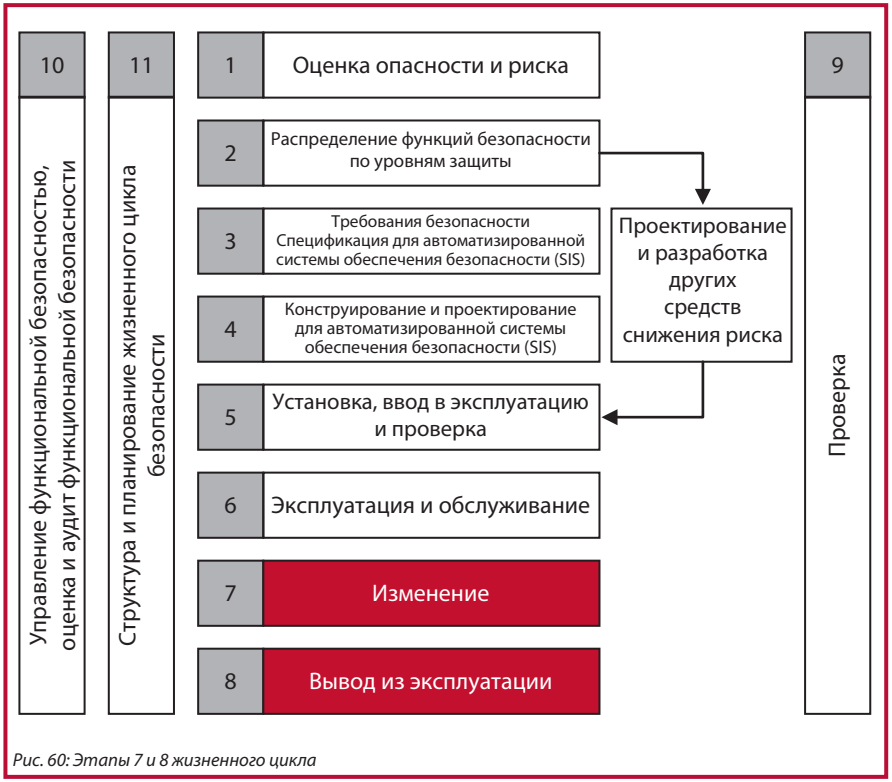


Рис. 60: Этапы 7 и 8 жизненного цикла

Цели этой фазы, определенные в IEC 61511-1, 17.1 и 18.1, – обеспечить, что:

- все модификации в любой SIF должным образом запланированы, проанализированы и утверждены перед внесением изменений [17.2];
- необходимая полнота безопасности соблюдается при любых изменениях, которые могут быть произведены [17.3];
- перед выводом из эксплуатации проведена необходимая проверка и получено разрешение, что обеспечивает соблюдение полноты безопасности в ходе вывода из эксплуатации [17.4].

17.2. Модификация SIF

Перед проведением любых модификаций следует иметь в наличии процедуры разрешения и контроля изменений. Обычно это выполняется с помощью запроса на внесение изменений (Change Request Note, CRN), который обычно составляет часть QMS.

Каждый запрос на внесение изменений должен описывать необходимое изменение и его обоснование. Запрос может быть инициирован O&M-персоналом в результате происшествий при эксплуатации или техническом обслуживании. Типичный процесс утверждения запросов на внесение изменений должен требовать подключения различных отделов организации для определения влияния изменения на проект, базу установленного оборудования, необходимую реализацию.

Если организация должна следовать требованиям функциональной безопасности, все изменения, помимо прочего, должны быть изучены компетентным лицом, например управлением по безопасности (Safety Authority, SA), для определения того, может ли изменение повлиять на безопасность; в этом случае будет требоваться соответствующий анализ воздействий.

17.3. Анализ воздействий

Результаты анализа могут потребовать пересмотра ранних этапов жизненного цикла; к примеру, может понадобиться пересмотреть выявленные факторы риска и оценку рисков. Работы по модификации нельзя начинать, пока этот процесс не будет завершен и пока SA не разрешит изменение.

Влияние изменений на SIF может оказать дальнейшее воздействие на O&M-персонал и потребовать дополнительного обучения.

17.4. Вывод SIF из эксплуатации

Вывод из эксплуатации должен осуществляться как плановая работа в составе фазы жизненного цикла 11 и может выполняться как модификация в конце срока реализации проекта.

В начале фазы вывода из эксплуатации должен быть произведен анализ воздействий для определения влияния вывода из эксплуатации на функциональную безопасность. Анализ должен включать ревизию идентификации опасностей и оценки рисков с особым вниманием к опасностям, которые могут возникнуть в ходе работ по выводу из эксплуатации.

18. Управление функциональной безопасностью, оценка и аудит функциональной безопасности

18.1. Фазы жизненного цикла

На рис. 61 показана актуальная фаза жизненного цикла.

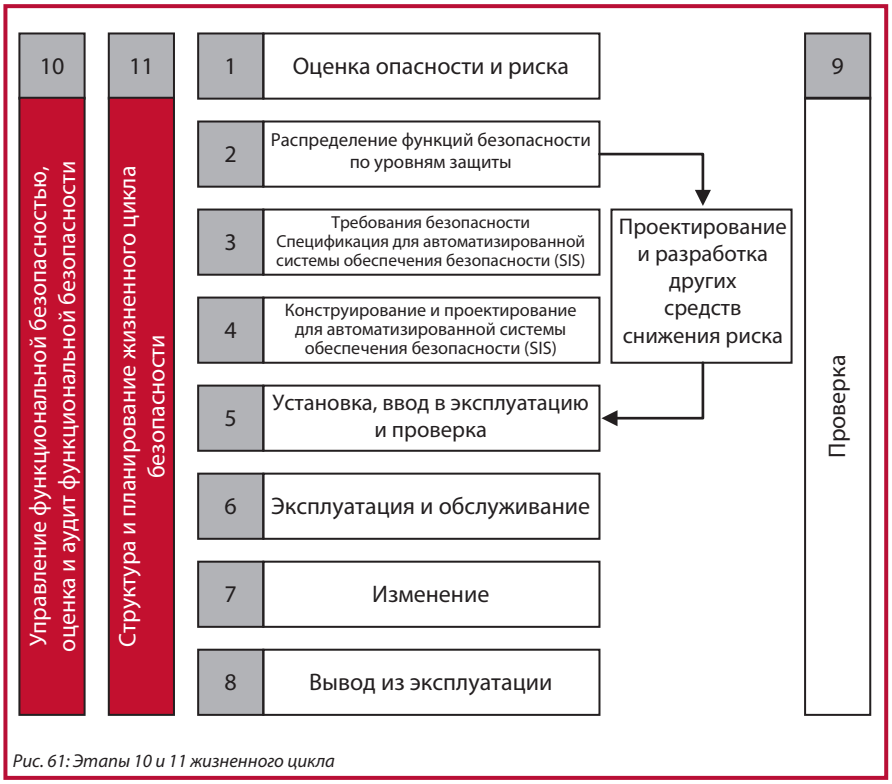


Рис. 61: Этапы 10 и 11 жизненного цикла

Цель этой фазы, установленная в IEC 61511-1, 5, – определить управленческие действия и документацию, необходимые для того, чтобы ответственные лица приняли должные меры по соответствующим фазам жизненного цикла.

Стандарт определяет общие требования к управленческим действиям и документации, необходимым для того, чтобы ответственные лица приняли должные меры по соответствующим фазам жизненного цикла.

Это означает, что для надлежащего завершения проектная документация должна содержать достаточную информацию для каждой фазы всего завершенного жизненного цикла, для последующих фаз и для деятельности по проверке.

Соответствие стандарту требует, чтобы спецификация содержала следующее:

- обязанности управляющих функциональной безопасностью;
- действия, которые должны быть предприняты лицами, имеющими соответствующие обязанности.

Работа по соответствию требованиям может быть реализована путем выработки процедур, охватывающих все требования, путем внедрения этих процедур и путем обеспечения наличия должной информации для эффективного управления функциональной безопасностью.

18.2. Управление функциональной безопасностью

Требования к управлению функциональной безопасностью сведены в таблице 23.

Большинство этих требований могут уже покрываться системой управления качеством (Quality Management System, QMS) организации. В следующих разделах рассматриваются некоторые области, которым обычно следует уделить внимание.

Управление требованиями функциональной безопасности	**Описание**
Общие требования IEC 61511-1, 5.2.1 Политика и стратегия должны разрабатываться вместе со средствами связи в пределах организации.	**Политика и связь** Необходимо разработать и довести до сведения всех сотрудников организации «Политику функциональной безопасности». Рекомендуется включить в политику конкретные цели функциональной безопасности, способы контроля их достижения и методы связи в пределах организации.
Чтобы обеспечить возможность замены решением SIS процессов в безопасном состоянии, должна быть в наличии «Система управления функциональной безопасностью».	Документ высокого уровня, описывающий «Систему управления функциональной безопасностью», должен связывать систему со всеми этапами жизненного цикла в рассматриваемом масштабе. В руководящем документе должны быть перечислены все процедуры, необходимые для реализации всех мер по обеспечению безопасности. Процедуры должны охватывать все управленческие и технические аспекты в рамках проекта. Процедуры должны содержать четкие описания производимых документов. Проекты следует контролировать в соответствии с «Планом обеспечения качества и безопасности», в котором должны быть определены действия, средства контроля и способы приемки по завершении.

Управление требованиями функциональной безопасности	**Описание**
Организация и ресурсы IEC 61511-1, 5.2.2 Лица, отделы, организации и прочие подразделения, ответственные за выполнение и контроль каждого из этапов жизненного цикла системы безопасности, должны быть определены и ознакомлены со своими обязанностями (включая в соответствующих случаях лицензирующие и регулятивные органы в сфере безопасности).	**Роли и ответственность** Все лица, отделы и организации, ответственные за контроль принятия мер по обеспечению безопасности, должны быть четко определены, а сферы их ответственности прояснены. Как правило, это осуществляется путем публикации организационных диаграмм с указанием отдельных лиц и их ролей. Обязанности каждой роли оформляются в виде должностных инструкций.
Лица, отделы и организации, принимающие участие в действия жизненного цикла системы безопасности, должны быть компетентны в областях, за которые несут ответственность.	**Компетентность** Компетентность всех упомянутых выше ответственных лиц должна быть документирована. Должны быть предусмотрены процедуры, обеспечивающие наличие у соответствующих ответственных лиц необходимых для выполнения порученных им действия знаний, навыков и опыта. Процедуры должны предусматривать контроль и оценку компетентности, а также потребностей в обучении. Документация по компетентности должна включать следующие сведения: а) инженерные знания (относящиеся к процессу, технологии, новизне и сложности сферы применения, датчикам и конечным элементам); б) адекватные управленческие и лидерские навыки, соответствующие роли в жизненном цикле системы безопасности; в) понимание потенциальных последствий событий; полнота обеспечения безопасности SIF; требования техники безопасности и соответствующие требования законов.
Оценка риска и управление риском IEC 61511-1, 5.2.3 Опасность должна быть определена, риск должен быть оценен, меры снижения степени риска должны быть определены.	**Определение SIL** См. раздел [6].
Планирование IEC 61511-1, 5.2.4 В ходе планирования обеспечения безопасности следует определить необходимые действия и исполнителей (лица, отделы, организация и пр. подразделения), ответственных за выполнение этих действий. Планы следует регулярно обновлять на протяжении жизненного цикла обеспечения безопасности.	**Планирование** Планирование должно обеспечить выполнение действий в рамках управления, контроля и оценки FS в соответствии с графиком и этапами жизненного цикла. Планирование может быть включено в план обеспечения качества проекта с описанием всех смежных действий, сроков и сфер ответственности отдельных лиц и организаций. Все действия по обеспечению безопасности могут включать ссылки на процедуры или рабочие методики, а также средства разработки и реализации.

Управление требованиями функциональной безопасности	**Описание**
Реализация и мониторинг IEC 61511-1, 5.2.5 Необходимо внедрить процедуры для своевременного отслеживания и соблюдения рекомендаций, возникающих на основе следующих элементов: а) анализ опасности и оценки риска; б) оценка и аудит; в) проверка и контроль; г) действия после происшествия.	**Реализация и мониторинг** Процедуры должны предусматривать формулирование рекомендаций на основе анализа и оценки действий, а также методы контроля и отслеживания процессов, от рекомендаций до реализации предложенных действий. Необходимо предусмотреть процедуру, которая обеспечивает соблюдение рекомендаций, разработанных в результате происшествий или угроз.
Следует предусмотреть процедуры оценки эффективности SIS в соответствии с требованиями безопасности, включая: а) сбор и анализ фактических данных в процессе эксплуатации; б) регистрацию потребностей в SIF с целью обеспечения верности предположений, сделанных в ходе определения SIL.	Если организация ответственна за этапы эксплуатации и технического обслуживания, должны быть предусмотрены процедуры оценки эффективности эксплуатации и технического обслуживания, включая: • систематические отказы; • повторяющиеся отказы; • оценку периодичности управления и отказов в соответствии с предположениями, сделанными на этапе проектирования или оценки FS. Требования к аудиту FS должны включать: периодичность, независимость, обязательный набор документов и дальнейшие действия.
Любой поставщик, предоставляющий организации изделия или оказывающий услуги, ответственный за один или несколько этапов жизненного цикла системы безопасности, должен предоставлять изделия или оказывать услуги в соответствии с требованиями организации и иметь внедренную у себя систему управления качеством. Следует предусмотреть процедуры обеспечения адекватности системы управления качеством поставленным задачам.	**Управление взаимоотношениями с поставщиками** Поставщики обеспечивают поставку продукции в соответствии с заказом и использованием соответствующей системы управления качеством. Как правило, закупки выполняются у поставщиков из утвержденного списка и контролируются согласно спецификациям закупок. Следует предусмотреть процедуры аудита утверждения поставщиков.
Оценка, аудит и контроль IEC 61511-1, 5.2.6 Следует определить и внедрить процедуры оценки функциональной безопасности, позволяющие судить о функциональной безопасности и полноте безопасности, обеспечиваемой автоматизированной системой безопасности. Процедуры должны предполагать назначение оценочной комиссии, включающей соответствующих специалистов с учетом области деятельности. В составе комиссии должен быть как минимум один старший специалист, не входящий в группу разработки проекта. Этапы жизненного системы безопасности, на котором выполняются действия по оценке функциональной безопасности, определяются в ходе планирования безопасности.	**Оценка функциональной безопасности** Действия по оценке FS – см. раздел [13]. Следует предусмотреть процедуры, позволяющие выполнять оценку функциональной безопасности. Требования демонстрации соответствия целям SIL и PFD (или PFH), поставленным в ходе определения SIL [6], изложены в разделе [11.1]. В организации может быть создана соответствующая группа специалистов при условии соблюдения требований в отношении компетентности и независимости. В случае использования услуг сторонней организации требования в отношении компетентности должны быть включены в процедуру управления поставщиками. Требования в отношении MTR должны быть включены в объем работ [8.6.6].

Управление требованиями функциональной безопасности	**Описание**
Перед идентификацией опасности необходимо провести не менее одной оценки функциональной безопасности и выполнить следующие действия: • оценка опасности и риска; • формулировка рекомендаций на основе оценки опасности и риска; • создание, производство и монтаж автоматизированной системы безопасности в соответствии с SRS; • реализация процедур обеспечения безопасности, эксплуатации и технического обслуживания; • проверка системы; • провести обучение персонала эксплуатации и техническому обслуживанию с предоставлением необходимых сведений об автоматизированной системе безопасности; • разработать стратегию дальнейшей оценки.	Оценка функциональной безопасности должна выполняться согласно плану обеспечения соответствия нормативным требованиям. В плане обеспечения качества и безопасности проекта должны быть указаны соответствующие пункты графика проекта или жизненного цикла системы безопасности, которые должны выполняться в то или иное время. Как минимум одна оценка функциональной безопасности должна быть выполнена, прежде чем на предприятии или в процессе будет зарегистрирован фактор опасности.
Следует разработать и внедрить процедуры аудита соответствия нормативным требованиям, включающие следующие положения: а) периодичность аудита; б) степень независимости лиц, отделов, организаций или иных подразделений, выполняющих работы и осуществляющих аудит; в) регистрация и дальнейшие действия.	Аудит функциональной безопасности должен подтвердить наличие в проекте соответствующих процедур и их реализацию. Как правило, аудит функциональной безопасности выполняется на ранних этапах жизненного цикла проекта с целью подтверждения присутствия всех процедур для всех аспектов безопасности. Последующие аудиторские проверки должны выполняться периодически в течение всего проекта, чтобы обеспечить соблюдение процедур, рекомендаций и дальнейших действий.
Управление конфигурацией SIS IEC 61511-1, 5.2.7 Следует разработать процедуры управления конфигурацией SIS на протяжении всего жизненного цикла. Следует определить указанные ниже элементы: а) этап, на котором реализуется формальный контроль конфигурации; б) метод идентификации компонентов (оборудования и программного обеспечения); в) процедуры предотвращения эксплуатации несанкционированных компонентов.	Управление конфигурацией Процедуры управления конфигурацией, инициацией изменений, утверждением и последующими действиями по запросам о внесении изменений, вероятно, уже существуют в рамках типовой системы управления качеством. Однако при рассмотрении изменений в функции безопасности следует выполнять анализ последствий, чтобы определить возможное влияние на безопасность и этап жизненного цикла, с которого следует начать повторную оценку. Возможно, потребуется разработка процедур анализа последствий и управления повторной оценкой.

Таблица 23. Требования к управлению функциональной безопасностью

18.3. Общие требования

Должна иметься политика и стратегия достижения функциональной безопасности на предприятии и должны быть определены средства доведения ее до всего предприятия.

Важно, чтобы на предприятии была разработана собственная политика функциональной безопасности, поскольку это потребует от руководства внимательно отнестись к значению функциональной безопасности для предприятия, уведомления о ней и создания культуры функциональной безопасности, охватывающей все предприятие и все виды его деятельности.

18.4. Организация и ресурсы

Для всех работников проекта должны быть определены их профессионализм и круг обязанностей. Профессионализм персонала должен записываться в реестре профессиональных навыков, а соответственно, должна иметься процедура его оценки для периодического обновления реестра на основании полученного опыта и для оценки потребностей в обучении. Требования к профессионализму должны быть определены для каждой роли проекта.

Для большинства предприятий с малым опытом в сфере функциональной безопасности может быть удобно назначить управление по безопасности (Safety Authority, SA), который будет отвечать за функциональную безопасность, корпоративную политику и связи, фазы жизненного цикла и планирование работ. SA должно быть независимым от проектов.

По всей вероятности, ему также может понадобиться создать и обслуживать реестр профессиональных навыков или переработать существующую систему для учета работ и обязанностей по функциональной безопасности.

18.5. Реализация и мониторинг проекта

При наличии работ, новых для области действий, например HAZOP, должна быть создана процедура для проведения HAZOP. Если, к примеру, разработка должна включать связанное с безопасностью прикладное ПО, должна иметься процедура по обеспечению разработки ПО в соответствии с фазой жизненного цикла 4 [11].

18.6. Управление конфигурацией и модификация

Процедуры для управления конфигурацией, инициации модификации, утверждения и обработки запросов на внесение изменений обычно уже существуют в типичной QMS.

Однако при рассмотрении изменений в функции безопасности следует выполнять анализ последствий, чтобы определить возможное влияние на безопасность и этап

жизненного цикла, с которого следует начать повторную оценку. Возможно, потребуется разработка процедур анализа последствий и управления повторной оценкой.

18.7. Эксплуатация и обслуживание (O&M)

В зависимости от фаз жизненного цикла, входящих в сферу охвата, может потребоваться внедрить процедуры для работы (в частности, сбора и хранения) с информацией, получаемой из факторов риска, происшествий и модификаций. Процедуры могут также описывать:

- меры в случае опасных происшествий;
- анализ выявленных факторов риска;
- деятельность по проверке.

Сбор данных и протоколирование могут быть необходимы, поскольку в ходе оценки безопасности могло быть предположено, что функция безопасности является, к примеру, системой режима по требованию. Мониторинг и частота требований для функции безопасности, таким образом, обеспечат определение и действенность соответствующих целей и показателей качества работы.

19. Ссылки

19.1. IEC 61508:2010, Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety Related Systems.

19.2. IEC 61511:2004: Functional Safety: Safety Instrumented Systems for the Process Industry.

19.3. Reducing Risks, Protecting People, HSE 2001, ISBN 0 7176 2151 0.

19.4. AIChE Centre for Chemical Process Safety, Layer of Protection Analysis (LOPA), 2001

19.5. IEC 61784-3:2010 Industrial Communications Networks. Profiles Part-3: Functional safety Fieldbuses – General Rules and profile Definitions.

19.6. Derivation of the Simplified PFDavg Equations, D Chauhan, Rockwell Automation (FSC).

19.7. General Reliability Calculations for MooN Configurations, KJ Kirkcaldy, Rockwell Automation (FSC).

19.8. Functional Safety: Safety Instrumented Systems for the Process Industry Sector. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).

20. Определения

2oo3	Логическая схема «два из трех» (2/3) – схема с тремя независимыми входами. Выход логической схемы находится в том же состоянии, что и любые два соответствующих входа. Например, цепь защиты с тремя датчиками, где для срабатывания аварийного останова требуется наличие сигнала от любых двух датчиков. Такая система «2oo3» называется устойчивой к единичному сбою (ДЧО = 1), то есть при отказе одного из датчиков система защиты останется работоспособной. Также возможны схемы 1oo1, 1oo2, 2oo2, 1oo3 и 2oo4.
ALARP (Анализ дерева событий)	Метод моделирования распространения отказов. В ходе анализа создается древовидная структура последовательных событий, начинающаяся от исходного события и демонстрирующая возможные последствия. Ветвление дерева происходит в результате промежуточных событий. Каждая ветвь представляет ситуацию с одним из возможных результатов. Включив в дерево все ветви, можно получить все возможные результаты.
D (Диагностика)	Некоторые логические решающие устройства, определяющие уровень безопасности, отмечены прописной буквой D («диагностика»). Они отличаются от обычных средств диагностики тем, что способны изменять свою архитектуру после обнаружения средством диагностики отказа. Наибольший эффект достигается в системах «1oo2D», которые способны переходить в режим «1oo1» после обнаружения неисправности. Таким образом, частота срабатывания такой системы значительно снижается.
E/E/PE Электрические, электронные и программируемые системы безопасности	См. 61508 и 61511.
FMECA	Анализ характера, последствий и важности отказов (FMECA) – подробный анализ различных состояния отказа и анализ важности конкретной единицы оборудования.
HAZOP	Анализ опасностей и пригодности к эксплуатации (АЭХОФ). Процедура анализа опасностей процесса, изначально разработанная ICI в 1970-х годах. Этот высокоструктурированный метод позволяет разделить процесс на различные узлы на основе операций для изучения поведения различных элементов каждого узла в диапазоне возможных отклонений от номинальных условий.
HSE (Великобритания)	Управление по вопросам охраны здоровья, техники безопасности и охраны труда
IEC	Международная электротехническая комиссия. Международная организация по стандартизации. Основная цель IEC – содействие международному сотрудничеству в вопросах стандартизации в области электротехники и электроники. Кроме этого, IEC регулярно публикует международные стандарты. См. 61508 и 61511. Анализ последствий позволяет выявить, какое воздействие изменение функции или компонента оказывает на другие функции или компоненты этой системы и других систем.
IEC 61508	Стандарт IEC, касающийся функциональной безопасности электрических, электронных и программируемых систем обеспечения безопасности. Основная цель стандарта IEC 61508 – использование автоматизированных систем безопасности для снижения риска до допустимого уровня путем соблюдения общих процедур жизненного цикла аппаратных и программных систем безопасности и ведения соответствующей документации. Этот стандарт, изданный в 1998 году и переизданный в 2000 году, используется в основном поставщиками оборудования для систем безопасности для подтверждения пригодности оборудования для использования в системах определенного уровня полноты.

IEC 61511	Стандарт IEC функциональной безопасности электрических, электронных и программируемых систем обеспечения безопасности в перерабатывающей промышленности. Подобно стандарту IEC 61508 он ориентирован на набор процессов жизненного цикла системы безопасности, направленных на управление рисками. Он был впервые опубликован IEC в 2003 году и принят в США в 2004 году под номером ISA 84.00.01-2004. В отличие от IEC 61508 этот стандарт ориентирован на пользователей автоматизированных систем безопасности в перерабатывающей промышленности.
IPL	Независимый уровень защиты. Это относится к различным методам снижения риска в процессах. Примерами могут служить предохранительные диафрагмы и предохранительные клапаны, которые независимо друг от друга снижают вероятность развития неблагоприятной ситуации в полномасштабную катастрофу с негативными последствиями. Для наибольшей эффективности предотвращения ущерба каждый такой уровень должен быть независим от других, иметь разумную вероятность срабатывания и возможность контроля работоспособности.
LOPA	Анализ уровней защиты. Метод оценки вероятности (периодичности) опасных результатов на основании периодичности исходных событий и вероятности отказов серии независимых уровней защиты, способных предотвратить ущерб.
MTTR	Среднее время восстановления работоспособности после отказа – средний период времени от отказа до возобновления работы по окончании ремонта. Этот период включает время, необходимое для обнаружения неисправности, начала ремонта и его завершения.
PFDavg	Средняя вероятность отказа по требованию – вероятность опасного отказа системы с невозможностью реализации функции безопасности при необходимости. PFD определяется как средняя или максимальная вероятность в заданный период времени. В стандартах IEC 61508/61511 и ISA 84.01 величина PFDavg используется в качестве опорной при определении SIL.
RRF	Коэффициент снижения риска – величина, обратная PFDavg.
SFF	Доля безопасных отказов – доля сбоев, приводящих к безопасному отказу или диагностике возможности небезопасного отказа. Доля безопасных отказов включает случаи диагностируемых опасных отказов, когда об этих отказах сообщается и за этим следует ремонт или останов.
SIF	Функция автоматизированной защиты – комплект оборудования, предназначенный для снижения вероятности возникновения определенной опасности (контур безопасности). Цели функции включают (1) автоматический перевод промышленного процесса в безопасное состояние в случае нарушения определенных условий, (2) разрешение процессу продолжаться безопасным способом, когда условия это позволяют (функция разрешения), (3) осуществление действий для смягчения последствий аварии на производстве. Включает элементы, обнаруживающие происшествие, принимающие решение о дальнейших действиях и выполняющие эти действия для перевода процесса в безопасное состояние. Возможности обнаружения, принятия решений и выполнения необходимых действий определяются уровнем полноты безопасности (SIL). См. SIL.
SIL	Уровень полноты безопасности – выраженная количественно цель степени безопасности, необходимой для обеспечения приемлемой вероятности опасности процесса. Определение целевого уровня SIL для процесса выполняется на основании оценки вероятности происшествий и тяжести последствий. В следующей таблице представлены уровни SIL для различных режимов эксплуатации.

SIS	Инструментальная система безопасности – реализация одной или нескольких автоматизированных функций безопасности. SIS представляет собой сочетание датчиков, логических цепей и оконечных элементов. Как правило, SIS имеет несколько функций с различными уровнями полноты безопасности (SIL), поэтому следует избегать описания системы с использованием единого уровня SIL. См. SIF.
Архитектура	Структура логики различных элементов автоматизированной функции безопасности. См. ограничения архитектуры, отказоустойчивость и 2oo3.
Базовая система контроля процессов	Система, реагирующая на входящий сигнал от процесса, связанного оборудования и/или оператора и генерирующая выходные сигналы, изменяющие процессы и работу связанного с ними оборудования требуемым образом. Система компонентного представления процессов предприятия не может реализовать автоматизированные функции безопасности уровня полноты 1 и выше, пока не будет отвечать проверенным на практике требованиям. См. проверенный на практике.
Безопасное состояние	Состояние процесса после выполнения действий, направленных на устранение опасности.
Безопасный отказ	Отказ без потенциальных негативных последствий для автоматизированной системы безопасности или возникновения состояния ошибки при выполнении функции. Ситуация, когда система безопасности или компонент выходит из строя так, что это приводит к нормальному аварийному останову системы или включению функции автоматической защиты при отсутствии опасности.
Блок-схема расчета надежности	Метод комбинирования вероятностей с целью оценки сложных вероятностей. Так как этот метод рассматривает «успешность» системы, может возникать путаница при использовании данных при моделировании множественных отказов.
Верификация SIL	Процесс расчета средней вероятности отказа по требованию (или вероятность опасного отказа в час) и ограничений архитектуры проекта системы безопасности с целью оценки соответствия требуемому уровню SIL.
Вероятность	Периодичность опасных событий, выраженная в количестве событий в год или на миллион часов. Один из двух компонентов, используемых при определении риска. Не следует путать с вероятностью в традиционном понимании.
Выход из строя безопасным образом (срабатывание защиты при отключении питания)	Функция устройства, позволяющая ему переходить в безопасное состояние в случае отключения электропитания или потери давления.
Диагностическое покрытие	Способность системы регистрировать отказы. Соотношение числа зарегистрированных отказов к общему числу отказов в системе.
Доля безопасных отказов	См. SFF.
Доступность	Вероятность того, что устройство работоспособно в данный момент времени. Это единица измерения работоспособности, выраженная в процентах. У большинства испытанных и отремонтированных компонентов систем безопасности кривая доступности имеет зубчатую форму и зависит от периодичности испытаний и ремонта. Таким образом, для вычисления средней вероятности отказа по требованию используется средняя доступность. См. PFDavg.
ДЧО	Отказоустойчивость оборудования (см. отказоустойчивость)

Закрытие при отказе	Условие, при котором привод закрывает клапан в случае отказа источника питания привода.
Занятость	Вероятность того, что в зоне поражения могут находиться люди. Определяется на основе принятых на предприятии правил в отношении персонала.
Интенсивность отказов	Количество отказов единицы оборудования за единицу времени. Обычно является постоянным значением. Возможно распределение по категориям, таким как безопасное/опасное, обнаруженное/необнаруженное, независимое/нормальное, с общей причиной. Для получения достоверных данных необходимо учитывать испытания на принудительный отказ и полный износ.
Контрольное испытание	Испытание компонентов системы безопасности с целью выявления отказов, не выявленных в ходе автоматической диагностики, т.е. опасных отказов, отказов диагностики, параметрических сбоев с последующим возвратом системы в состояние, подобное состоянию новой системы. Контрольное испытание является важным элементом жизненного цикла системы безопасности и необходимо для достижения требуемого уровня защиты на всем протяжении жизненного цикла.
Ложное отключение	См. безопасный отказ.
Лямбда	Интенсивность отказов системы. См. интенсивность отказов.
Надежность	1. Вероятность того, что устройство адекватно выполняет свою функцию в течение указанного периода времени в определенных условиях эксплуатации. 2. Вероятность того, что компонент оборудования или система адекватно выполняет свою функцию в течение указанного периода времени, как правило, в период эксплуатации, без необходимости корректирующего вмешательства.
Неполадки, произошедшие по одной причине	Случайное воздействие, приводящее к одновременному отказу нескольких компонентов по одной причине. Отличие от систематического отказа заключается в случайном и вероятностном характере неполадок при отсутствии постоянства и предсказуемости. См. систематический отказ.
Ограничения архитектуры	Ограничения, применяемые к оборудованию, выбранному для реализации функции автоматизированной безопасности независимо от расчетных рабочих характеристик подсистемы. Ограничения архитектуры описываются (в IEC 61508-2-Таблица 2 и IEC 61511-Таблица 5) в соответствии с требуемыми характеристиками SIL подсистемы, типом используемых компонентов и SFF компонентов подсистемы. Компоненты типа A – это простые устройства, не содержащие микропроцессоры, а компоненты типа B – это сложные устройства, содержащие микропроцессоры. См. отказоустойчивость.
Опасность	Вероятность ущерба.
Опасный отказ	Отказ компонента автоматизированной системы безопасности, препятствующий переходу системы в безопасное состояние при необходимости. См. состояние отказа.
Описание контрольных испытаний	Доля отказов, выявленных при обслуживании оборудования. В общем, предполагается, что при проведении контрольных испытаний все возникающие в системе неисправности устраняются (100-процентное покрытие периодическим тестированием).

Отказоустойчивость	Способность функционального модуля продолжать выполнять требуемую функцию в условиях случайных отказов или ошибок. Например, система принятия решений «1oo2» может продолжать работать, игнорируя один случайный отказ компонента. Отказоустойчивость – это одно из особых требований уровня полноты безопасности (SIL), оно подробно рассматривается в таблицах 2 и 3 части 2 стандарта IEC 61508 и пункте 11.4 стандарта IEC 61511 (ISA 84.01 2004).
Открытие при отказе	Условие, при котором привод открывает клапан в случае отказа источника питания привода.
Периодичность контрольных испытаний	Периодичность технического обслуживания оборудования.
Последствия	Масштаб ущерба или результатов опасного события. Один из двух компонентов, используемых при определении риска.
Причинно-следственная диаграмма	Метод, часто используемый для демонстрации зависимости между входными сигналами датчиков, функцией безопасности и требуемыми выходными сигналами. Часто применяется как элемент спецификации системы безопасности. Преимущества метода – простота и наглядность, недостатки – ограничения формата (некоторые функции нельзя представить в виде причинно-следственной диаграммы) и чрезмерное упрощение функции.
Проверенный на практике	Основание для использования компонента или системы в качестве уровня полноты безопасности (SIL) автоматизированной системы безопасности (SIS), которая не проектировалась с учетом требований стандартов IEC 61508. Для выявления наличия систематических ошибок в конструкции изделия метод требует достаточного времени наработки изделия, истории наблюдений, системы отчетности об отказах, наличия данных об отказах на местах. Стандарт IEC 61508 предусматривает все уровни истории эксплуатации, необходимые для каждого SIL.
Происшествие	Результат исходного события, распространению которого не препятствовали. Происшествие – это базовое описание нежелательного события с минимальным объемом информации. Например, термин «происшествие» используется при упоминании выбросов химических веществ или аварий, связанных с энергоносителями. Т.е. когда потенциал ущерба реализован, но результаты еще не приняли окончательную форму.
ПЦНУ	Практически целесообразный низкий уровень. Принцип обработки рисков, находящихся между высшим и низшим уровнями. Верхний предел – это настолько высокий риск, что он полностью исключается, а нижний предел – это риск, который не рассматривается из-за своей незначительности. Такой принцип учитывает как затраты, так и преимущества снижения риска, чтобы сделать риск «разумно низким».
Режим (высокой интенсивности)	(также «непрерывный режим» согласно IEC 61511). Аналогичен непрерывному режиму, только особое внимание уделяется автоматической диагностике. Разница между непрерывным режимом и режимом высокой интенсивности заключается в том, выполняется ли автоматическая диагностика быстрее, чем рабочий цикл защиты. Если диагностика выполняется медленнее, то системе доверять нельзя и включается непрерывный режим.

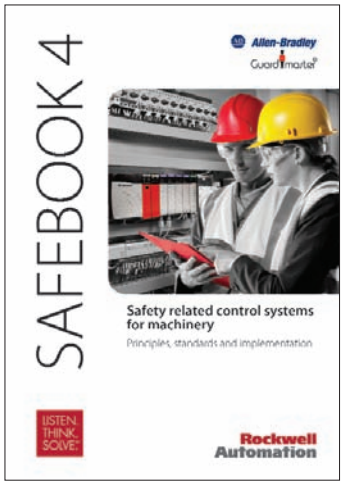
Режим (непрерывный)	Режим, когда требования активирования защитной функции возникают чаще, чем интервалы испытания функции автоматизированной защиты. Следует отметить, что в некоторых областях режим высокой интенсивности определяется по критерию возможности сокращения частоты несчастных случаев путем диагностики. В любом случае непрерывный режим – это режим, в котором частота нежелательных происшествий определяется частотой опасных отказов функций автоматизированной защиты (SIF). При отказе SIF необходимость в действии возникает за более короткий промежуток времени, чем при испытаниях, поэтому говорить о вероятности отказа не имеет смысла. Практически все опасные отказы SIF в непрерывном режиме обнаруживаются при запросе действия, а не путем испытания функции. См. режим низкой интенсивности, режим высокой интенсивности, SIL.
Режим (низкой интенсивности)	(также «режим управления» IEC 61511). Режим, когда требования активирования защитной функции возникают реже, чем интервалы испытания функции автоматизированной защиты. В перерабатывающей промышленности этот режим определен как режим, в котором запросы на активацию SIF возникают реже, чем один раз на два испытания. Режим низкой интенсивности – это наиболее распространенный режим в перерабатывающей промышленности. При определении уровня полноты безопасности для режима низкой интенсивности характер работы SIF оценивается по средней вероятности отказа по требованию (Probability of Failure on Demand – PFDavg). В этом режиме периодичность исходного события, измененная вероятностью отказа по требованию SIF, определяет периодичность срабатывания, а периодичность нежелательных происшествий определяется последующими уровнями защиты.
Резервирование	Использование нескольких элементов или систем, выполняющих одну и ту же функцию. Резервирование может быть обеспечено путем использования идентичных элементов (идентичное резервирование) или различных элементов (разнородное резервирование). Резервирование применяется для повышения надежности или доступности систем.
Система компонентного представления процессов предприятия (BPCS)	См. базовая система контроля процессов.
Систематический отказ	Отказ, который случается предсказуемым (а не случайным) образом по единой причине, которую можно устранить только путем внесения изменений в конструкцию, процесс, способ эксплуатации, документацию и прочие факторы. Поскольку математическое прогнозирование в этом случае невозможно, в жизненный цикл системы безопасности включается ряд процедур, предотвращающих возникновение таких отказов. Чем выше уровень полноты безопасности систем и компонентов, тем строже процедуры. Такие отказы невозможно предотвратить простым резервированием.
Случайный отказ	Отказ, происходящий внезапно и приводящий к поломке одного или нескольких узлов. Случайные отказы можно эффективно прогнозировать, используя статистику и данные о вероятности отказов по требованию для данного уровня безопасности. См. систематический отказ.
Состояния отказа	Характер неисправности. Неисправности обычно относят к одному из четырех состояний отказа: безопасное обнаруженное (SD), опасное обнаруженное (DD), безопасное необнаруженное (SU), опасное необнаруженное (DU) (см. ISA TR84.0.02).
Схема дерева неисправностей	Метод комбинирования вероятностей с целью оценки сложных вероятностей. Так как учитывается представление отказов системы, метод позволяет моделировать комбинированные состояния отказа. Расчет средней вероятности отказа следует выполнять с осторожностью.

Схема трубной обвязки и КИП	Чертежи трубопроводов и измерительной аппаратуры. На них представлена взаимосвязь производственного оборудования и контрольно-измерительных приборов, управляющих процессом. В непрерывных производствах схемы процессов составляются с помощью стандартного набора условных обозначений. Как правило, используются условные обозначения КИП, принятые Американским обществом приборостроителей (ISA) и опубликованные в стандарте S5. 1. 2. Основной эскизный чертеж, используемый при планировании системы контроля процессов.
Уровень защиты	См. IPL.
Функциональная безопасность	Предотвращение неприемлемого риска в ходе жизненного цикла системы безопасности. См. IEC 61508, IEC 65111, жизненный цикл системы безопасности, допустимый риск.

Сокращения

1oo1	1 out of 1 voting (Simplex) (логика голосования «1 из 1» (одинарная)).
1oo2	1 out of 2 (логика голосования «1 из 2»).
AI	Analogue Input (Аналоговый вход).
ANSI	American National Standards Institute (Американский национальный институт стандартов).
ALARP	As Low As Reasonably Practicable (настолько низкий, насколько это практически осуществимо).
BMS	Burner Management System (система управления работой котла).
BPCS	Basic Process Control System (ОСУП, Основная система управления процессом).
C&E	Cause and Effect (причина и следствие).
CBA	Cost Benefit Analysis (функционально-стоимостный анализ).
CCF	Common Cause Failure (отказы с общей причиной).
COMAH	Control Of Major Accident Hazards (контроль опасности возникновения крупномасштабных аварий).
Dangerous failure	Тип отказа, при котором отвечающая за безопасность система потенциально может оказаться в опасном или неработающем состоянии.
DCS	Distributed Control System (система распределенного управления, РСУ).
DD	Dangerous Detected (опасные обнаруженные [отказы]).
DI	Digital Input (цифровой вход).
DO	Digital Output (цифровой выход).
DU	Dangerous Undetected (опасные необнаруженные [отказы]).
E/E/PES	Electrical/Electronic/Programmable Electronic System (электрическая/электронная/программируемая электронная система).
ESD	Emergency Shutdown (ESD, Система противоаварийной автоматической защиты).
ESDV	Emergency Shutdown Valve (клапан аварийного отключения).
f/hr	Failures per hour (отказов в час).
F&G	Fire and Gas (пожарная и газовая опасность).
FC	Fail Closed (отказ в закрытом положении).
FDS	Functional Design Specification (технические требования к функциональному проектированию).
FMECA	Failure Modes, Effects and Criticality Analysis (анализ видов, последствий и критичности отказов, АВПКО).
FO	Fail Open (отказ в открытом положении).
FPL	Fixed Programmable Language (фиксированный язык программирования).
FSC	Functional Safety Capability (соответствие функциональной безопасности).
FVL	Full Variability Language (язык с полной варьируемостью).
HASAW	Health and Safety at Work Act (HSW) (Закон об охране здоровья и безопасности на рабочем месте (Великобритания)).
HAZAN	Hazard Analysis (анализ опасностей).
HAZOP	Hazard and Operability Study (HAZOP, Анализ эксплуатационных характеристик и опасных факторов).
HFT	Hardware Fault Tolerance (аппаратная отказоустойчивость).
HIPPS	High Integrity Pressure Protection System (система повышенной надёжности для защиты от превышения давления).
HSE	Health and Safety Executive (уполномоченный по вопросам охраны труда и безопасности).
I/O	Input/Output (ввод/вывод).
IEC	International Electrotechnical Commission (Международная электротехническая комиссия, IEC).
IPL	Independent Protection Layer (независимый уровень защиты).
ISA	International Society of Automation (Общество по приборам, системам и автоматизации).
LOPA	Layer of Protection Analysis (анализ уровня защиты).
LVL	Limited Variability Language (язык с ограниченной варьируемостью).
MDT	Mean Down Time (среднее время простоя).
MooN	M out of N (general case) («M из N» (общий случай)).
MTBF	Mean Time Between Failures (среднее время между отказами).
MTR	Maximum Tolerable Risk (максимальный допустимый риск).

MTTF	Mean Time To Failure (среднее время наработки на отказ).
MTTR	Mean Time To Repair (среднее время восстановления после отказа).
Non-SR	Non-Safety Related (не связанный с безопасностью).
O&M	Operation and Maintenance (эксплуатация и техническое обслуживание).
OPSI	Office of Public Sector Information (Управление публичной информации).
P&ID	Piping and Instrumentation Diagram (схема трубной обвязки и контрольно-измерительных приборов).
PA	Per Annum (за год).
PE	Programmable Electronic (программируемая электроника).
PFD	Probability of Failure on Demand (вероятность отказа при наличии запроса).
PFH	Probability of Failure per Hour (вероятность отказа при наличии запроса).
PSD	Process Shutdown (останов технологического процесса).
PT	Pressure Transmitter (датчик давления).
PTI	Proof Test Interval (интервал между контрольными испытаниями).
QMS	Quality Management System (система управления качеством).
R2P2	Reducing Risk Protecting People (снижение риска/защита людей).
RBD	Reliability Block Diagram (блок-схема расчета надежности).
RRF	Risk Reduction Factor (фактор уменьшения риска).
S	Safe (безопасный [отказ]).
SA	Safety Authority (управление по безопасности).
Safe failure	Тип отказа, при котором отвечающая за безопасность система потенциально не может оказаться в опасном или неработающем состоянии.
SFF	Safe Failure Fraction (доля безопасных отказов).
SIF	Safety Instrumented Function (Приборная функция безопасности).
SIL	Safety Integrity Level (уровень полноты безопасности).
SIS	Safety Instrumented System (SIS, Инструментальная система безопасности).
SOV	Solenoid Operated Valve (клапан с электромагнитным управлением).
SRS	Safety Requirements Specification (спецификация требований к безопасности).
STR	Spurious Trip Rate (частота ложных аварийных срабатываний).
TMR	Triple Modular Redundant (тройное модульное резервирование).
Tp	Proof Test Interval (интервал между контрольными испытаниями).
λ	Интенсивность отказов, отношение общего количества отказов к заданному временному отрезку.
λD	Интенсивность опасных (dangerous) отказов.
λDD	Интенсивность опасных отказов, выявленных (detected) при диагностике.
λDU	Интенсивность опасных отказов, не выявленных (undetected) при диагностике.
λS	Интенсивность безопасных (safe) отказов.



Также доступны:
Руководство по безопасности 4. Системы управления для обеспечения безопасности механизмов.
В этом руководстве рассматриваются принципы обеспечения безопасности механизмов, правовые аспекты, теория и практика безопасности.
Номер публикации: SAFEBK-RM002B

Чтобы получить экземпляр руководства, обратитесь к представителю Rockwell Automation или посетите веб-сайт www.rockwellautomation.com.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Америка: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Телефон: +1 414 382 2000, факс: +1 414 382 4444
Европа/Ближний Восток/Африка: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Телефон: +32 2 663 0600, факс: +32 2 663 0640
Азия: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Телефон: +852 2887 4788, факс: +852 2508 1846

Россия и СНГ: Rockwell Automation, Большой Строченовский переулок 22/25, офис 202, 115054 Москва, Телефон: +7 495 956 0464, факс: +7 495 956 0469, www.rockwellautomation.ru

Публикация: SAFEBK-RM003A-RU-P – Март 2013 г.