ГОСТ Р МЭК 61511-2-2011 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата введения 01.08.2012

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения"

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью "Корпоративные электронные системы" на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 октября 2011 г. N 469-ст

Настоящий стандарт идентичен международному стандарту МЭК 61511-2:2003* "Безопасность функциональная. Системы безопасности, приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1" (IEC 61511-2:2003 "Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1").

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

4 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В

случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Введение

Приборные системы безопасности уже в течение многих лет используют для выполнения функций безопасности в промышленных процессах. Для эффективного применения приборных систем безопасности при выполнении функций безопасности необходимо, чтобы они соответствовали определенному минимальному уровню стандартизации.

Область применения настоящего стандарта - приборные системы безопасности, применяемые в промышленных процессах. Он также рассматривает вопросы интерфейса между такими системами и другими системами безопасности, которые выявляются в результате проведения оценки опасностей и рисков, присущих промышленному процессу. Приборная система безопасности включает в себя датчики, логические решающие устройства и исполнительные элементы.

В основе настоящего стандарта лежат две фундаментальные концепции, необходимые для его применения: концепция жизненного цикла безопасности и концепция уровней полноты безопасности. Жизненный цикл безопасности формирует центральную структуру, объединяющую большинство положений настоящего стандарта.

Настоящий стандарт рассматривает приборные системы безопасности, использующие электрические/электронные/программируемые электронные технологии. Если для логических устройств используют другие принципы действия, то следует применять основные положения настоящего стандарта. Настоящий стандарт также рассматривает датчики и исполнительные элементы приборной системы безопасности независимо от принципа их действия. Настоящий стандарт является конкретизацией общего подхода к вопросам обеспечения безопасности, представленного в МЭК 61508, для промышленных процессов.

Настоящий стандарт устанавливает подход, минимизирующий стандартизацию деятельности для всех стадий жизненного цикла безопасности. Этот подход был принят в целях реализации рациональной и последовательной технической политики. Цель настоящего стандарта - дать представление о том, как выполнять требования МЭК 61511-1.

Чтобы облегчить применение настоящего стандарта, номера разделов и подразделов идентичны соответствующим номерам разделов и подразделов МЭК 61511-1 (исключая приложения).

В большинстве ситуаций безопасность эффективнее всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. При необходимости он может быть дополнен системами защиты, основанными на применении различных технологий (например, химических, механических, гидравлических, пневматических, электрических, электронных, термодинамических (пример - гаситель пламени), программируемых электронных), с помощью которых достигается любой установленный остаточный риск. Любая стратегия обеспечения безопасности должна рассматривать

каждую конкретную приборную систему безопасности в контексте других систем защиты. Для облегчения применения такого подхода настоящий стандарт:

- требует, чтобы выполнялась оценка опасностей и рисков для определения общих требований к безопасности;

- требует, чтобы выполнялось распределение требований к безопасности в (по) приборной(ым) системе(ам) безопасности;

- реализует подход, который применим ко всем приборным методам обеспечения функциональной безопасности;

- подробно рассматривает применение определенных действий, таких, как руководство работами по безопасности, которые могут быть применены ко всем методам обеспечения функциональной безопасности.

Настоящий стандарт по приборным системам безопасности для промышленных процессов:

- охватывает все стадии жизненного цикла безопасности - от разработки первоначальной концепции, проектирования, внедрения, эксплуатации и технического обслуживания вплоть до утилизации;

- дает возможность, чтобы существующие или новые стандарты в разных странах, регламентирующие конкретные промышленные процессы, были с ним гармонизированы.

Настоящий стандарт призван привести к высокому уровню согласованности (например, основных принципов, терминологии, информации) в рамках конкретных промышленных процессов. Это принесет преимущества как в плане безопасности, так и в плане экономики.

На рисунке 1 представлена общая структура настоящего стандарта.

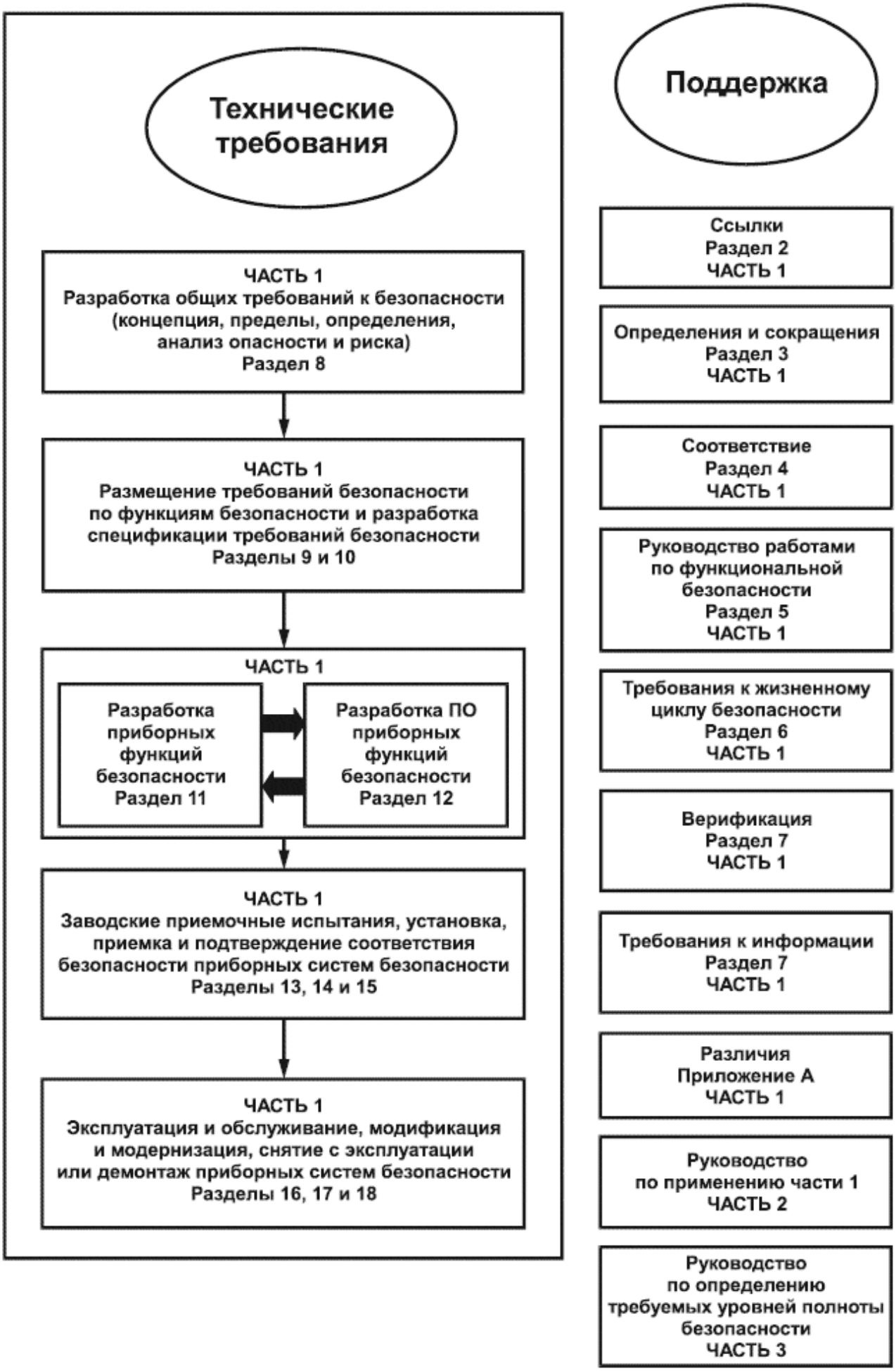


Рисунок 1 - Общая структура настоящего стандарта

1 Область применения

Настоящий стандарт содержит руководство по установлению требований, разработке, монтажу, эксплуатации и техническому обслуживанию функций безопасности приборных систем безопасности и соответствующих приборных систем безопасности в соответствии с МЭК 61511-1. Настоящий стандарт построен так, что каждый его номер раздела и подраздела совпадает с содержательно связанным номером раздела и подраздела МЭК 61511-1 (за исключением приложений).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты*:

МЭК 61508-2:2000 Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 2. Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью (IEC 61508-2:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems)

МЭК 61508-3:1998 Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 3. Требования к программному обеспечению (IEC 61508-3:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements)

МЭК 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения (IEC 61508-4:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4:1998, Definitions and abbreviations)

МЭК 61511-1:2003 Безопасность функциональная. Приборные системы безопасности для технологических процессов в промышленности. Часть 1. Термины, определения и технические требования (IEC 61511-1:2003, Functional safety - Safety instrumented systems for process industry sector - Part 1: Framework, definitions, system, hardware and software requirements)

3 Сокращения и определения

Дополнительные требования не предусмотрены, за исключением пунктов 3.2.68 и 3.2.71 МЭК 61511-1.

3.2.68 Функция безопасности должна предотвращать появление конкретного опасного события, например "предотвращать превышение давления в емкости #ABC456, уровня 100 бар". Функция безопасности может быть реализована:

a) отдельной приборной системой безопасности (ПСБ), или

b) одной или несколькими ПСБ и/или другими слоями защиты.

В случае b) каждая ПСБ или другой слой защиты должны быть способны к выполнению

функции безопасности, а полная их комбинация должна обеспечить требуемое снижение риска (заданную безопасность процесса).

3.2.71 Функции безопасности ПСБ формируются из функции безопасности, имеют соответствующий уровень полноты безопасности (УПБ) и выполняются конкретной ПСБ, например "закрыть клапан #XY123 в течение 5 с, если давление в емкости #ABC456 достигнет 100 бар". Необходимо отметить, что компоненты ПСБ могут быть использованы для выполнения более чем одной функции безопасности ПСБ.

4 Соответствие настоящему стандарту

Дополнительные требования не предусмотрены.

5 Управление функциональной безопасностью

5.1 Цель

Целью раздела 5 МЭК 61511-1 является установление требований к выполнению таких управляющих действий, которые необходимы для уверенности в том, что цели, связанные с функциональной безопасностью, достигаются.

5.2 Требования

5.2.1 Общие требования

5.2.1.1 Дополнительные требования не предусмотрены.

5.2.1.2 Если организация несет ответственность за выполнение одного или нескольких действий, необходимых для функциональной безопасности, и она выполняет работы в соответствии с процедурами обеспечения качества, то многие действия, описанные в данном разделе, уже выполняются в целях достижения качества. В таких случаях, возможно, нет необходимости повторять эти действия в целях обеспечения функциональной безопасности. При этом следует провести критический анализ принятых процедур обеспечения качества, чтобы установить достижение цели функциональной безопасности.

5.2.2 Организация и ресурсы

5.2.2.1 Внутри компании, стройки, завода или проекта следует определить организационную структуру, связанную с ПСБ; следует ясно понимать и знать роли и ответственность каждого элемента этой структуры. В рамках структуры должны быть определены индивидуальные роли, включая их описание, и цель. Для каждой роли должны быть строго определены ответственность и конкретные обязанности. Кроме того, должно быть установлено, кто и кому представляет индивидуальные отчеты. Целью должно быть обеспечение того, что каждый специалист в организации понимает свою роль и обязанности, связанные с работами по ПСБ.

5.2.2.2 Следует установить требования к подготовленности и знаниям, необходимым для выполнения всех работ жизненного цикла безопасности, связанных с ПСБ; для каждого уровня подготовки следует определить уровни компетентности. Следует оценить имеющиеся и требуемые трудовые ресурсы (численность персонала) по каждому уровню

подготовки и компетентности. В случае выявления различий между ними следует разработать календарные планы достижения необходимых уровней компетентности. При нехватке подготовленных кадров может быть проведен дополнительный набор опытного персонала.

5.2.3 Оценка риска и управление риском

Требования, установленные в МЭК 61511-1 (пункт 5.2.3) состоят в том, что должны быть выявлены опасности, оценены риски и определено необходимое снижение риска. Признано, что существует большое число различных методов для выполнения таких оценок. МЭК 61511-1 не предлагает конкретного метода. Вместо этого специалисту рекомендуется ознакомиться с обзором ряда методов по этой проблеме в МЭК 61511-3. Дополнительные указания даны в 8.2.1 настоящего стандарта.

5.2.4 Планирование

Цель данного пункта состоит в том, чтобы гарантировать, что в рамках всего проекта адекватное планирование безопасности было проведено так, что на каждой стадии жизненного цикла (например, техническое проектирование, эксплуатация) предусмотрены все необходимые действия. Настоящий стандарт не требует, чтобы такие действия по планированию имели какую-то конкретную структуру, но требует, чтобы они периодически дополнялись и критически оценивались.

5.2.5 Реализация и контроль

5.2.5.1 Цель данного пункта - обеспечить, чтобы выполнялись такие эффективные процедуры управления, которые:

- гарантируют удовлетворительные решения по всем рекомендациям, вытекающим из анализа опасностей, из оценки риска, из других действий по оценке и проверке, а также из действий по верификации и подтверждению соответствия;

- позволяют установить, что ПСБ работает в соответствии с ее спецификацией требований к безопасности в течение всего времени ее эксплуатации в течение срока службы.

5.2.5.2 Необходимо отметить, что в данном контексте в состав поставщиков могут входить подрядчики, выполняющие проектирование, и подрядчики, обеспечивающие обслуживание, а также поставщики отдельных компонентов.

5.2.5.3 Следует периодически проводить критический анализ характеристик ПСБ, чтобы убедиться в том, что исходные допущения, принятые при составлении спецификации требований к безопасности, сохраняются. Например, следует периодически оценивать интенсивность отказов различных компонентов ПСБ, чтобы убедиться, что она остается на принятом исходном уровне. Если интенсивности отказов оказались хуже, чем первоначально определенные, то может понадобиться модификация проекта. Аналогично должна быть проанализирована интенсивность запросов на срабатывание ПСБ. Если интенсивность запросов окажется выше первоначально принятой, то может потребоваться уточнение УПБ.

5.2.6 Оценка, аудит и проверки

Проведение оценок и аудитов является средством, направленным на выявление и

устранение ошибок. Приведенные ниже положения поясняют различие между этими двумя видами действий.

Оценка функциональной безопасности имеет своей целью установить, являются ли меры предосторожности, принятые на рассматриваемых стадиях жизненного цикла, достаточными для достижения безопасности. Суждение выносят исполнители оценки в отношении решений, принятых лицами, ответственными за реализацию функциональной безопасности. Например, оценка, сделанная перед вводом в эксплуатацию, может быть посвящена вопросу о том, достаточны ли принятые процедуры обслуживания.

Аудиторы функциональной безопасности определяют по проектной или эксплуатационной документации, были ли выполнены необходимые процедуры с установленной частотой и лицами, обладающими необходимой компетентностью. Аудиторы не обязаны делать выводы о достаточности рассматриваемой ими работы. Однако если они осознают, что внесение изменений может принести дополнительные преимущества, то соответствующие сведения следует включать в отчет.

Необходимо отметить, что во многих случаях может быть пересечение между работой исполнителя оценки и аудитора. Например, аудитор может встретиться с необходимостью не только установить, получил ли оператор необходимую подготовку, но и вынести дополнительно суждение о том, привела ли подготовка к требуемому уровню компетентности.

5.2.6.1 Оценка функциональной безопасности

5.2.6.1.1 Оценка функциональной безопасности (ОФБ) является основной процедурой, демонстрирующей, что ПСБ выполняет предъявляемые к ней требования, связанные с ее функциями безопасности и УПБ. Основная цель такой оценки состоит в том, чтобы продемонстрировать с помощью независимой оценки процесса разработки системы его соответствие требованиям действующих стандартов и установившейся практике. Оценка ПСБ может быть необходима на различных стадиях жизненного цикла. Чтобы выполнить эффективную оценку, должна быть разработана процедура, которая определяет границы области применения этой оценки, вместе с указаниями по составу группы, выполняющей оценку.

Атрибутами хорошей установившейся практики ОФБ считаются следующие черты:

- для каждой ОФБ должен быть сгенерирован план, определяющий область применения оценки, исполнителей оценки, их компетентность и информацию, которая должна быть получена в результате их работы;

- ОФБ должна учитывать требования других стандартов и практического опыта, которые могут содержаться во внешних или внутренних корпоративных стандартах, в руководствах, процедурах или нормах и правилах. План ОФБ должен определять, что именно должно быть оценено в данной конкретной работе, системе или случае применения;

- частота ОФБ может быть различной для разработок разных систем, но, как минимум, ОФБ всегда должна выполняться перед тем, как потенциальные опасности начнут действовать на систему. Некоторые компании предпочитают проводить ОФБ до выполнения стадии сборки/установки, чтобы предотвратить дорогостоящие переделки на более поздних стадиях жизненного цикла;

- частоту и строгость проведения ОФБ следует определять с учетом таких факторов, как:

- сложность,

- значимость безопасности,

- предшествующий опыт, связанный с подобными системами,

- стандартизация конструктивных особенностей;

- перед проведением ОФБ следует обеспечить наличие достаточных данных о результатах проектирования, монтажа, действий по верификации и подтверждению соответствия. Наличие достаточного количества данных само по себе может быть критерием оценки. Данные должны представлять текущее или принятое состояние проекта или установки системы;

- исполнители ОФБ должны быть в достаточной мере независимыми;

- исполнители ОФБ должны обладать опытом и знаниями в области соответствующей технологии и применения оцениваемой системы;

- систематический и непротиворечивый подход к ОФБ следует соблюдать на всем жизненном цикле и для всех систем. Само проведение ОФБ является субъективной деятельностью, поэтому для устранения субъективности, насколько это возможно, должно быть создано подробное руководство (возможно, с использованием контрольных листов), являющееся приемлемым для данной организации.

Документы, создаваемые в ходе ОФБ, должны быть полными, а сделанные в них заключения следует согласовать со всеми лицами, ответственными за руководство работами по функциональной безопасности ПСБ, до перехода к выполнению следующей стадии жизненного цикла.

5.2.6.1.2 Чтобы увеличить объективность оценки, к ней необходимо привлечь специалиста, не участвовавшего в проектировании. Имеется потребность в специалисте высокого уровня (например, по опыту, образованию, служебному положению), для того чтобы убедиться в том, что все спорные вопросы приняты во внимание и учтены. Так же как предлагается в МЭК 61511-1 (примечание к подпункту 5.2.6.1.2), для некоторых крупных проектов или групп специалистов по оценке может оказаться необходимым иметь более одного старшего специалиста, независимого от группы разработчиков исходного проекта.

В зависимости от структуры компании и службы экспертизы внутри компании требование к независимости специалиста по оценке может быть выполнено путем привлечения внешней организации. Наоборот, другие компании, имеющие в своем составе организации, которые обладают опытом оценки и применения ПСБ, независимы и отделены (по управлению и по другим ресурсам) от лиц, ответственных за проект, могут использовать собственные ресурсы, удовлетворяющие требованиям независимой организации.

5.2.6.1.3 Объем работ по оценке зависит от размера и сложности проекта. Может оказаться возможным оценивать результаты различных стадий в одно и то же время. Это, в частности, справедливо в случаях внесения небольших изменений в текущий проект.

5.2.6.1.4 В некоторых странах ОФБ выполняют на стадии 3, которую часто называют предпроектным обзором безопасности (ППОБ).

5.2.6.1.5 Дополнительные требования не предусмотрены.

5.2.6.1.6 Дополнительные требования не предусмотрены.

5.2.6.1.7 Группа специалистов, занятая оценкой, должна иметь доступ к любой информации, которую она считает необходимой для проведения оценки. В состав такой информации следует включать сведения, полученные при оценках опасности и рисков, на стадиях разработки, монтажа, приемки и подтверждения соответствия.

5.2.6.2 Аудит и проверка

5.2.6.2.1 В данном подпункте дано руководство по проведению аудита системы с помощью примеров, иллюстрирующих соответствующие действия.

а) Виды аудита

Проведение аудита ПСБ обеспечивает полезной информацией руководство предприятия, а также инженеров, занятых обслуживанием и разработкой приборов. Оно придает руководству действенность и осведомленность о степени использования и эффективности применяемых ПСБ. Существует много различных видов аудита. Реальный тип, масштаб и частота проведения аудита в любом конкретном случае должны отражать возможное влияние таких действий на полноту безопасности.

Видами аудита являются:

1) собственно аудиты, как независимые, так и проводимые собственными силами;

2) контроль;

3) визиты безопасности (например, при обходе предприятия и разборе инцидента);

4) обследование ПСБ (по анкете).

Необходимо различать обследования и проверки, с одной стороны, и действия по аудиту - с другой. Обследование и проверка направлены на оценку выполнения конкретных действий на жизненном цикле (например, контролер проверяет выполнение работы по обслуживанию перед тем, как компонент будет вновь включен в работу). В отличие от них действия по аудиту являются более исчерпывающими и концентрируются на полной реализации ПСБ в отношении жизненного цикла безопасности. Аудит должен включать в себя определение того, выполнена ли программа обследований и проверок.

Аудиты и контроль могут быть выполнены силами собственного персонала компании, стройки, завода или проекта (например, внутренний аудит) или независимыми лицами (например, аудиторами компании, отделом обеспечения качества, контрольными органами, покупателями или третьими лицами).

Руководители различного уровня могут пожелать использовать соответствующие типы аудита, чтобы получить дополнительную информацию об эффективности внедрения ПСБ. Результаты аудитов могут быть использованы для определения неправильно выполняемых процедур, что приведет к улучшению их применения.

b) Стратегия аудита

Программы проведения аудита стройки, завода или проекта должны предусматривать повторяющиеся программы независимых и внутренних аудитов и контроля.

Повторяющиеся программы регулярно обновляются для отражения предыдущих характеристик и результатов аудита, а также существующих проблем и приоритетов. Они охватывают все связанные со стройкой/заводом/проектом действия и аспекты ПСБ, относящиеся к соответствующим периоду времени и полноте.

Первостепенное основание и дополнительная ценность аудитов состоят в том, что их проведение обеспечивает своевременное получение информации. Эти действия имеют своей целью повысить эффективность ПСБ, например, помочь минимизировать риск для работников и населения получить травму или погибнуть, способствовать повышению культуры безопасности труда, способствовать предотвращению любого возможного выброса вещества в окружающую среду.

В итоге стратегия проведения аудитов может иметь смешанный характер и устанавливаться руководством (заказчиком) так, чтобы играть роль обратной связи, дающей информацию, необходимую руководству для своевременных действий.

c) Процедура и протоколы аудита

Максимальная ценность проведения аудита может быть достигнута только при условии, что все стороны (включая аудиторов, кандидатов на участие, руководителей завода, руководителя отдела и т.д.) понимают необходимость каждого аудита и могут на него влиять. Последующее описание проведения процесса и протоколов аудита может помочь гарантировать некоторую последовательность в подходе к достижению этих целей. Она состоит из следующих пяти ключевых стадий процесса проведения аудита:

1) стратегия и программа аудита.

Следует ясно определить цель проведения каждого аудита и назначить группы его исполнителей с указанием роли и ответственности каждой из таких групп.

Необходимо иметь стратегию аудита.

Следует составить программу проведения аудитов.

Необходимо регулярно пересматривать процедуры аудита, программы и стратегию его проведения;

2) подготовка и предварительное планирование аудита.

Прежде чем проводить аудит, старший руководитель стройки, завода или проекта и/или соответствующий координатор аудита должны определить контактное лицо.

Аудиторам и контактному лицу следует на самой ранней стадии обсудить, понять и согласовать:

- границы области аудита;

- продолжительность проведения аудита;

- персонал, который следует привлечь;

- основу аудита или стандарт для его проведения;

- необходимость приложения особых усилий на подготовительной стадии и привлечения заводского персонала для повышения шансов на успешный аудит.

Рекомендуется следующее распределение времени на каждую стадию проведения аудита:

- подготовка аудита - 30%;

- проведение аудита - 40%;

- составление отчета с замечаниями - 20%;

- завершение аудита - 10%.

Аудитору следует подготовить к проведению аудита руководящие материалы, процедуры, инструкции и т.п., а также данные и, при необходимости, контрольные листы.

Аудитор должен придавать особое значение и объяснять, какие изменения в области аудита могут произойти в ходе его проведения, если будут обнаружены серьезные замечания или ошибки;

3) проведение аудита.

Аудитор должен проводить свою работу непрерывно в течение нескольких дней, в пределах установленного для аудита периода времени, учитывая возможные отвлечения от работы персонала стройки, завода или проекта.

В ходе проведения аудита следует периодически информировать контактное лицо о выявленных замечаниях, тем самым избегая возникновения непредвиденных обстоятельств по окончании работы.

Аудитору следует стараться привлечь заводской персонал к участию в процессе аудита, чтобы передать свои знания и понимание (процессов и замечаний) владельцу.

Успех аудита в значительной степени зависит от стиля работы аудитора - он должен стараться быть полезным, конструктивным, вежливым, собранным и объективным.

Как минимум, аудитор должен стараться выполнить согласованные объемы и сроки работ; все необходимые изменения следует обсуждать;

4) составление отчета с замечаниями.

Аудитору следует поддерживать тесные контакты как до конца проведения аудита, так и позже, вплоть до выпуска итогового отчета.

Соответствующему руководству должна быть предоставлена возможность прокомментировать проект отчета и замечания, а также при желании обсудить их на официальной встрече.

Нормальной практикой считается запрос плана действий стройки, завода или проектной

организации, связанный с замечаниями, включенными в отчет;

5) завершение аудита.

Отчеты по аудиту обычно требуют реакции в форме плана действий. Аудитор должен проверить, выполнен ли этот план удовлетворительно к установленной дате или к следующему аудиту в зависимости от обстоятельств.

Для проверки выполнения плана действий могут быть использованы соответствующие следящие системы стройки/завода/проекта.

Замечания каждой группы аудиторов следует периодически рассматривать и широко информировать о результатах этого рассмотрения.

Замечания и/или результаты аудитов могут быть использованы для пересмотра частоты их проведения и применены руководством как входная информация для анализа ПСБ.

5.2.6.2.2 Настоящий подпункт придает особое значение той роли, которую играет управление изменениями в процессах проведения аудитов.

5.2.7 Управление конфигурацией ПСБ

5.2.7.1 Требования

5.2.7.1.1 Для управления и поддержания возможности оперативного контроля устройств на всех стадиях их жизненного цикла может быть установлен механизм идентификации, управления и отслеживания для моделей или версий каждого устройства.

На возможно ранней стадии жизненного цикла безопасности каждому устройству следует присвоить уникальный объектный идентификатор. В некоторых случаях более ранние модели или версии устройств могут оставаться в эксплуатации и обслуживании. В качестве первого шага следует составить программу управления конфигурацией, которая может охватывать следующие аспекты:

a) обеспечение процедуры идентификации всех устройств на всех стадиях жизненного цикла;

b) уникальная идентификация модели, версии и внутреннего статуса каждого изделия (включая программные) с указанием поставщика, даты и места применения, а также изменений модели или версии по отношению к исходной модели или версии;

c) идентификация и отслеживание всех действий и изменений, проведенных по результатам замеченных отказов и выполненных аудитов;

d) управление вводом в эксплуатацию, определяющее статус и модель/версию соответствующих устройств;

e) меры безопасности, которые должны быть предприняты, чтобы обеспечить отсутствие неавторизованных перенастроек или изменений в действующих ПСБ;

f) определение версий каждого программного средства, которые в совокупности определяют законченное устройство;

g) обеспечение координации процесса добавления многочисленных ПСБ на одном или

более объектах;

h) оформленная документально авторизация ввода устройств в эксплуатацию;

i) зарегистрированный перечень подписей, допускающих ввод в эксплуатацию;

j) стадии или фазы, на которых устройства находятся под управлением конфигурацией;

k) управление соответствующей сопроводительной документацией;

l) определение для каждой модели/версии устройства:

- функциональной спецификации,

- технической спецификации;

m) установление того, что все подразделения и/или организации, участвующие в руководстве и обслуживании ПСБ, определены и границы их ответственности подписаны и понятны.

6 Требования к жизненному циклу безопасности

6.1 Цель

Функциональная безопасность, достигнутая для любого объекта процесса, зависит от удовлетворительного выполнения ряда действий. Цель применения систематической концепции жизненного цикла безопасности к ПСБ состоит в том, чтобы все действия, необходимые для достижения функциональной безопасности, были выполнены и чтобы можно было показать другим, что они выполнены в правильном порядке. В МЭК 61511-1 типичный жизненный цикл безопасности представлен на рисунке 8 и в таблице 2, требования к каждой стадии жизненного цикла приведены в пунктах 8-16 МЭК 61511-1.

Настоящий стандарт признает, что установленные действия могут быть структурированы разными способами, обеспечивающими выполнение всех требований. Подобная реструктуризация может быть предпочтительной, если она позволяет добиться лучшей интеграции работ, связанных с безопасностью, в обычные проектные процедуры. Цель раздела 6 МЭК 61511-1 состоит в том, чтобы даже при использовании другого жизненного цикла безопасности были определены входные и выходные данные для каждой стадии жизненного цикла и были включены все существенные требования.

6.2 Требования

6.2.1 Особое внимание должно быть обращено на то, чтобы заранее определить жизненный цикл безопасности той ПСБ, которую будут использовать. Опыт показывает, что здесь часто возникают проблемы, даже если эта работа хорошо и своевременно спланирована и получены согласования со всеми несущими ответственность лицами, подразделениями и организациями. В лучшем случае некоторые работы будут пропущены или потребуют переделки; в худшем случае безопасность может быть поставлена под угрозу.

6.2.2 Хотя настоящий стандарт этого не требует, обычно полезно на самой ранней стадии составить предполагаемый жизненный цикл безопасности ПСБ в проектируемом

жизненном цикле процесса, включая перечень блоков, показанных на рисунке 8 МЭК 61511-1, которые применяют в проекте. После того как это будет сделано, следует рассмотреть информацию, необходимую для начала работ по безопасности, вместе с вопросом о том, кто, вероятно, способен эту информацию предоставить. В некоторых случаях может оказаться невозможным установить точную информацию по отдельным позициям ранее, чем на поздних этапах разработки. В таких случаях может оказаться необходимым сделать оценки, основанные на предшествующем опыте, и затем подкрепить их более поздними данными. В подобной ситуации важно предусмотреть это в жизненном цикле безопасности.

6.2.3 Другой важной частью планирования жизненного цикла безопасности является определение методов, которые будут применяться на каждой стадии. Определение таких методов важно потому, что часто приходится использовать специфические методы, которые требуют привлечения лиц или подразделений, обладающих уникальным умением или опытом. Например, в конкретном случае применения последствия отказа могут зависеть от максимального развиваемого давления; и единственный способ, которым его можно определить, состоит в том, чтобы разработать динамическую модель процесса. Требования к информации, необходимой для динамического моделирования, дадут важный импульс процессу разработки.

7 Верификация

7.1 Цель

Цель верификации состоит в обеспечении того, что действия, предусмотренные планом верификации на каждой стадии жизненного цикла безопасности, действительно выполнены и что требуемые выходные результаты стадии, будь это документация, аппаратное средство или программное обеспечение, реализованы и соответствуют своему назначению.

7.1.1 Требования

7.1.1.1 МЭК 61511-1 признает, что организации будут иметь свои собственные процедуры верификации, и не требует, чтобы они всегда выполнялись одинаковым способом. Напротив, смысл данного пункта состоит в том, что все действия по верификации планируются заблаговременно, вместе с любыми другими процедурами, мероприятиями и методами, которые должны применяться.

7.1.1.2 Дополнительные требования не предусмотрены.

7.1.1.3 Важно, чтобы результаты верификации были пригодны для того, чтобы можно было показать, что на всех стадиях жизненного цикла безопасности была проведена эффективная верификация.

8 Анализ опасностей и рисков процесса

8.1 Цель

Общая цель состоит в том, чтобы установить необходимость применения функций безопасности (например, для слоев защиты) и соответствующие уровни качества их выполнения (сокращение риска), которые необходимы, чтобы гарантировать

безопасность процесса. Обычно промышленные технологические процессы обеспечиваются несколькими слоями безопасности так, чтобы отказ одного слоя не вызывал или не допускал опасных последствий на другом слое. Типичные слои безопасности представлены на рисунке 9 МЭК 61511-1.

8.2 Требования

8.2.1 Требования к проведению анализа опасностей и рисков устанавливаются только на основе конкретной задачи. Это означает, что организация может использовать любой метод, который она считает эффективным и обеспечивающим результаты в виде ясного описания функций безопасности и соответствующие уровни качества их выполнения.

При проведении анализа опасности и риска следует устанавливать и рассматривать опасности и опасные события, которые могли произойти во всех обоснованных предсказуемых случаях (включая условия появления отказов и обоснованное предсказуемое неправильное применение).

Предварительный анализ опасностей и рисков в типичном проекте для промышленных процессов следует выполнять на ранней стадии разработки основных проектных решений по процессу. На этой стадии принимается допущение о том, что опасности устранены или снижены до практически разумного предела путем применения принципов внутренней безопасности и хорошей инженерной практики (эти действия по снижению опасности лежат вне области применения МЭК 61511). Для ПСБ такой предварительный анализ опасностей и рисков важен потому, что создание, проектирование и реализация ПСБ являются сложными задачами и могут потребовать длительного времени. Другая причина, требующая более раннего выполнения этой работы, состоит в том, что информация о структуре системы потребуется до того, как будут разработаны блок-схемы базового процесса и его автоматизации.

Если построена технологическая карта процесса и доступны все исходные данные процесса, то для выполнения предварительной оценки опасности и риска обычно бывает достаточно этой информации. Необходимо признать, что в проекте могут появиться дополнительные опасности, так как далее выполняется детальное проектирование. Поэтому после завершения построения технологической карты базового процесса и его автоматизации может потребоваться окончательная оценка опасности и риска. Этот окончательный анализ обычно проводится с помощью формальной и полностью документируемой процедуры, такой, как исследование опасности и работоспособности (HAZOP). Она должна подтвердить, что разработанные уровни безопасности адекватно обеспечивают безопасность предприятия. В ходе этого окончательного анализа необходимо рассмотреть, не приводят ли отказы в системах безопасности к каким-либо новым опасностям, и установить на этой стадии, не появилась ли необходимость введения новых функций безопасности. Другим более вероятным результатом является выявление дополнительных событий, которые приводят к опасностям, уже определенным на предварительной стадии. В таких случаях необходимо рассмотреть, нужна ли какая-либо коррекция функций безопасности и требований к качеству их выполнения, установленных при предварительном анализе.

Подход, применяемый для выявления опасностей, зависит от рассматриваемого случая применения. Для некоторых простых процессов, по которым имеется большой опыт эксплуатации типовых разработок, таких, как простые морские устьевые (нефтегазодобывающие) вышки, может оказаться эффективным использование ранее разработанных промышленных вопросников (например, анкеты анализа безопасности,

приведенные в [1] и [2]). Если проект более сложен или рассматривается новый процесс, может оказаться необходимым применение более структурированного подхода (например, по [3]).

Примечание - Дополнительная информация о выборе соответствующих методов приведена в [4].

При рассмотрении последствий событий, связанных с конкретными отказами, следует проанализировать все возможные результаты отказов, а также частоту отказов с учетом вкладов в каждый результат. Ни один из ожидаемых результатов не должен игнорироваться или исключаться из анализа риска. Воздействие на трубопроводы или емкости давления, превышающего проектное, не всегда будет приводить к катастрофическим потерям содержимого. Во многих случаях оборудование будет подвергаться испытаниям давлением, превышающим проектное, и единственным последствием может быть утечка воспламеняющегося вещества, приводящая к возможности возгорания. При оценке последствий следует проконсультироваться с лицами, ответственными за механическую целостность установки. Им потребуется учесть не только исходные процедуры испытаний давлением, но и испытания на коррозию, если предусмотрена программа борьбы с ней. Если оценки последствий базируются на таких допущениях, то важно, чтобы это было ясно заявлено и соответствующие процедуры были включены в систему управления безопасностью.

При дальнейшем рассмотрении последствий следует оценить число лиц, которые могут подвергаться конкретной опасности. Надо быть внимательным при использовании такого статистического подхода, так как он не будет справедлив во всех случаях, в таких, где опасность существует только во время запуска оборудования, когда необходимый штат сотрудников всегда присутствует. Во многих случаях оперативный и обслуживающий персонал будет находиться в опасной зоне только изредка, и это обстоятельство следует принять во внимание при прогнозировании последствий. При использовании подобного статистического подхода необходимо проявлять осторожность, так как он может быть применим не во всех случаях (в таких, например, когда опасность существует только в период запуска, а персонал присутствует все время). Следует также обратить внимание на возможное увеличение численности людей, находящихся вблизи от опасного события для исследования влияния симптомов разрастающегося события.

При оценке возможных источников запросов на срабатывание ПСБ такая оценка должна охватывать следующие ситуации: запуск, постоянная работа, останов, ошибки обслуживания, ручное вмешательство (например, в режиме ручного управления), потеря ресурсов (например, сжатого воздуха, охлаждающей воды, сжатого азота, электроэнергии, пара, отходящего тепла и т.д.).

При рассмотрении частоты запросов в некоторых сложных случаях может потребоваться провести анализ дерева ошибок. Это часто бывает необходимо, когда серьезные последствия являются результатом одновременных отказов, вызванных более чем одним событием (например, когда предохранительный коллектор не рассчитан на срабатывание по наихудшему случаю из всех источников). Требуется принять решение о том, следует ли включать ошибки оператора в список событий, способных привести к опасности, и какое значение частоты должно использоваться для таких событий. Ошибки оператора часто подлежат исключению, если его действия требуют разрешающего подтверждения или предусмотрены средства блокировки доступа, предотвращающие непредумышленные действия.

Необходимо также быть осторожным в тех случаях, когда принимается снижение частоты запросов за счет действий оператора. Такое допущение должно быть ограничено возможностями человеческого фактора, такими, как скорость выполнения необходимых действий и сложность решаемых задач. Если оператор должен действовать по результатам аварийной сигнализации и принимается, что снижение риска происходит более чем в 10 раз, то систему в целом следует разрабатывать в соответствии с МЭК 61511-1. Система, выполняющая функцию безопасности, будет тогда включать в себя датчик, определяющий появление опасной ситуации, воспроизведение аварийной сигнализации, ответное действие оператора и оборудование, используемое оператором для прекращения любой опасности.

Следует отметить, что снижение риска менее чем в 10 раз может быть принято без необходимости соответствия МЭК 61511. Если принимается такое допущение, то следует тщательно рассмотреть возможности человеческого фактора. Любые требования по снижению риска с помощью аварийной сигнализации должны быть подкреплены документально оформленным описанием необходимой реакции на сигнализацию и тем, что оператор имеет достаточно времени для корректирующего действия, а также уверенностью в том, что оператор подготовлен к выполнению защитных действий.

Система аварийной сигнализации может быть использована как способ снижения риска путем снижения частоты запросов к ПСБ при условиях:

- датчик, применяемый в системе сигнализации, не используется для целей управления, если потеря управления приводит к запросу на срабатывание функции безопасности ПСБ;

- датчик, применяемый в системе сигнализации, не используется как часть ПСБ;

- учтены ограничения на снижение риска, которое можно требовать от основной системы управления процессом (ОСУП), и отказы с общей причиной.

Примеры способов, которые могут применяться при установлении УПБ для ПСБ, даны в МЭК 61511-3 [5], где содержатся также указания о том, что следует рассмотреть при выборе метода, используемого в конкретном случае применения.

При установлении того, требуется ли снижение риска, необходимо располагать заданными характеристиками безопасности процесса и окружающей среды. Они могут быть установлены для конкретного объекта или эксплуатирующей компании и будут сравниваться с уровнем риска, существующим при отсутствии дополнительных функций безопасности. После установления потребности в сокращении риска следует рассмотреть, какие функции требуется выполнить, чтобы вернуть процесс в безопасное состояние. Теоретически функции могут быть описаны в общем виде без ссылки на конкретную технологию. Например, в случае защиты от превышения давления функция может быть определена как предотвращение того, что давление превзойдет установленное значение. Тогда такая функция может быть выполнена как предохранительным клапаном, так и ПСБ. Если функция описана в общем виде, то выбор используемого способа ее реализации будет проведен на следующем этапе жизненного цикла (распределение функций безопасности ПСБ по слоям защиты). На практике в зависимости от выбранного типа системы функциональные требования будут различными, поэтому данная и следующая стадии в некоторых случаях могут быть объединены.

Подводя итог, можно сказать, что в ходе анализа опасности и риска необходимо рассмотреть следующее:

- каждое определенное опасное событие и последовательность событий, которые их составляют;

- последствия и возможность появления последовательностей событий, вызванных каждым опасным событием; они могут быть выражены количественно или качественно;

- необходимость снижения риска для каждого опасного события;

- меры, предпринимаемые для снижения или устранения опасностей и рисков;

- допущения, принятые в ходе анализа рисков, включая оценки интенсивностей запросов и отказов оборудования; должно быть подробно раскрыто любое допущение, принятое для эксплуатационных ограничений или вмешательств человека;

- ссылки на ключевую информацию о связанных с безопасностью системах на каждой стадии жизненного цикла ПСБ (например, в работах по верификации или оценке соответствия).

Используемую информацию и получаемые результаты, составляющие анализ опасности и риска, следует оформлять документально.

Может оказаться необходимым повторить проведение оценки опасности и риска на различных стадиях полного жизненного цикла безопасности ПСБ по мере того, как принимаемые решения и доступная информация становятся более совершенными.

8.2.2 Для промышленных процессов важной причиной запросов, которые должны быть рассмотрены во многих приложениях, является отказ ОСУП. Необходимо отметить, что отказ ОСУП может быть вызван датчиком, клапаном или системой управления.

Иногда системы управления, используемые для промышленных процессов, имеют резервные процессоры, но датчики и клапаны остаются нерезервными. При назначении интенсивности отказов ОСУП существует важное ограничение, которое надо осознать. МЭК 61511-1 устанавливает ограничение на интенсивность опасных отказов, связанных с конкретной опасностью, которое может составлять до 10^{-5} в час, но при условии, что система создается в соответствии с требованиями настоящего стандарта. Причина данного ограничения состоит в том, что если принимается более низкая интенсивность опасных отказов, то она должна лежать в диапазоне интенсивностей отказов, приведенном в таблице 4 МЭК 61511-1. Ограничение обеспечивает, что высокие доверительные уровни не относятся к системам, которые не отвечают требованиям МЭК 61511-1.

8.2.3 Дополнительные требования не предусмотрены.

9 Распределение функций безопасности по слоям защиты

9.1 Цель

Для того чтобы определить потребность в ПСБ и значения соответствующих УПБ, важно

рассмотреть существующие (или требующиеся) другие уровни защиты и насколько значительную защиту они обеспечивают. После рассмотрения других уровней защиты следует определить необходимость применения уровня защиты в виде ПСБ. Если такой уровень необходим, то следует определить УПБ для функции (или функций) безопасности этой ПСБ.

9.2 Требования к процессу распределения

9.2.1 Первое требование состоит в том, чтобы согласовать используемые слои защиты и распределить задания на качество работы по функциям безопасности ПСБ. На практике часто функции безопасности распределяются только по ПСБ, так как в таких существуют проблемы применения разработок с внутренне присущей им безопасностью и систем, работающих на других принципах действия.

Примерами таких проблем являются ограничения, связанные с воспламеняемостью или с защитой от экзотермических реакций. Любое решение по использованию приборных систем вместо традиционных подходов, таких, как предохранительные клапаны, требуется подкрепить разумными доводами, которые покажутся вескими надзорным органам.

Как указывалось выше, действия по оценке опасности и риска и по распределению могут выполняться параллельно, либо распределение может при некоторых обстоятельствах выполняться перед оценкой опасности и риска. Решения по распределению функций безопасности ПСБ по слоям защиты часто принимаются на основе практического опыта организации-пользователя. Следует также учесть хорошую установившуюся промышленную практику. Решения, принимаемые по ПСБ, должны допускать наличие других уровней защиты. Например, если установлены предохранительные клапаны и они спроектированы и смонтированы в соответствии с промышленными нормами, то может быть решено, что их достаточно для достижения адекватного снижения риска. ПСБ в таких случаях будут только ограничивать давление на уровнях, при которых размер или качество работы предохранительного клапана (клапанов) будут для данного применения недостаточны или будут лишь предотвращать выбросы в атмосферу.

9.2.2 Дополнительные требования не предусмотрены.

9.2.3 Если функция безопасности реализована как функция безопасности ПСБ, то необходимо будет учитывать режим ее реализации - по запросам или по непрерывному запросу. В большинстве случаев в промышленных процессах реализуется режим по запросам, причем частота запросов невелика. Для таких случаев подходит таблица 3, приведенная в МЭК 61511-1. Встречаются случаи с частыми (например, свыше одного раза в год) запросами, для которых более подходящим является режим работы с непрерывным запросом, так как вероятность появления опасного отказа будет определяться прежде всего интенсивностью отказов ПСБ. Для таких случаев применима таблица 4 МЭК 61511-1. Случаи режима работы с непрерывным запросом, в которых отказ привел бы к непосредственной опасности, редки. Система управления горелкой или скоростью турбины может относиться к системе, функционирующей в режиме с непрерывным запросом, если системы защиты недостаточны для всех видов отказов такой системы управления.

Таблица 3 МЭК 61511-1 определяет УПБ, выраженные в значениях средней вероятности отказа при наличии запроса (ВОНЗ^{ср}). Заданное значение $^{ВОНЗ}{}_{ср}$ будет определяться

требуемым сокращением риска, которое, в свою очередь, может быть найдено путем сравнения риска процесса без ПСБ с величиной допустимого риска. Его можно определить в количественной или качественной форме способами, приведенными в [5].

Таблица 4 МЭК 61511-1 устанавливает УПБ, выраженные в значениях заданной частоты опасных отказов при выполнении функции безопасности ПСБ. Эта частота будет определяться приемлемой интенсивностью отказов ПСБ с учетом последствия отказа в конкретном случае применения. Если для определения требуемого УПБ используется таблица 4 МЭК 61511-1, то его целевое значение базируется на частоте опасных отказов ПСБ. При применении таблицы 4 МЭК 61511-1 некорректно преобразовывать частоту опасных отказов в вероятность их появления при наличии запроса, используя межпроверочный интервал или интенсивность запросов. Хотя при таком преобразовании единицы измерения могут быть правильными, оно будет ошибочным и может привести к невыполнению требований, предъявляемых к УПБ функций безопасности.

Заданные значения средней вероятности отказов при наличии запроса или частоты опасных отказов применяются к функции безопасности ПСБ, а не к отдельным компонентам или подсистемам. Компонент или подсистема (например, датчик, логическое решающее устройство, оконечный элемент) не могут иметь УПБ, установленные вне их применения в конкретной ПСБ. Однако компонент или подсистема могут иметь независимый максимальный УПБ, характеризующий ее возможности.

Результатом работ по оценке опасности и риска и по распределению требований должно быть ясное описание функций, которые будут выполнены системами безопасности, включая возможные ПСБ и требования к УПБ (вместе с режимом работы, непрерывным или по запросам) для каждой функции безопасности ПСБ. Такое описание формирует основу для составления спецификации требований к безопасности ПСБ. Описание функций должно быть ясным настолько, насколько это необходимо для того, чтобы обеспечить поддержание безопасности.

На данной стадии реализации нет необходимости определять структуру для подсистем датчиков и клапанов. Решения по таким структурам достаточно сложны, и определение, требует ли конкретная подсистема датчиков голосующую группу 2oo3, а подсистема клапанов голосующую группу 1oo2, будет зависеть от многих факторов.

9.2.4 Необходимо полностью понимать смысл таблиц 3 и 4, приведенных в МЭК 61511-1. В частности, значения $ВОНЗ^{ср}$, которые могут быть приняты для одиночной функции безопасности ПСБ, ограничены пределом 10^{-5}, что связано со снижением риска в 10^{5} раз (УПБ 4). Анализ надежности может показать, что достижение интенсивности случайных отказов технических средств, не превышающей 10^{-5}, возможно, но в МЭК 61511-1 принимается, что систематические отказы и отказы по общей причине будут ограничивать реально достигаемое качество функционирования. Настоятельно рекомендуется, чтобы в тех случаях, когда анализ риска показывает необходимость столь значительного снижения риска, была бы принята во внимание трудность достижения УПБ 4 для функции безопасности ПСБ в секторе промышленных процессов. При этом следует рассмотреть возможность использования нескольких независимых ПСБ с более низким УПБ.

К примечанию 4. Чтобы достичь более высоких уровней снижения риска (например, превышающих 10^{3}), можно использовать несколько ПСБ. При этом важно, чтобы каждая

из ПСБ могла независимо выполнять функцию безопасности и чтобы независимость между ПСБ была достаточно обоснованной. Например, может оказаться нецелесообразным объединять контур давления, обладающий УПБ 2, с контуром уровня, имеющим УПБ 1, чтобы реализовать функцию безопасности по превышению давления, отвечающую требованию к снижению риска, равному 10^3 , так как в тот момент, когда датчик уровня обнаружит повышение уровня, сосуд уже может находиться под давлением, превышающим установленное ограничение.

Кроме того, при использовании нескольких ПСБ следует учитывать отказы по общей причине. При этом должны выполняться все остальные требования, установленные в МЭК 61511-1, включая требования к минимальной отказоустойчивости, приведенные в таблице 5.

Чтобы проиллюстрировать, как можно совместно использовать несколько ПСБ для достижения более высоких уровней снижения риска, рассмотрим следующий пример.

Пусть комплект датчиков, соединенных по схеме "2 из 3", группа логических устройств со структурой "2 из 3" и соединение исполнительных устройств "1 из 2" образуют ПСБ, имеющую $\text{ВОНЗ}_{\text{ср}}$, равную $3{,}05 \times 10^{-4}$. Такая ПСБ дает снижение риска, равное приблизительно $3{,}3 \times 10^3$.

Было бы неправильно предполагать, что совместное использование двух таких систем приведет к сокращению риска, равному 10×10^6 ($3{,}3 \times 10^3$ x$3{,}3 \times 10^3$). Факторы, связанные с общими причинами, такие, как применение аналогичных принципов действия, разработка обеих систем по той же самой функциональной спецификации, человеческие факторы (например, программирование, монтаж, обслуживание), внешние факторы (например, коррозия, закупоривание, замерзание воздухопроводов, попадание молнии), будут ограничивать качество работы системы. Необходимо также принимать во внимание любые компоненты, используемые этими двумя системами совместно.

Более подходящим решением могло бы быть использование второй нерезервной системы, построенной на компонентах, отличающихся от применяемых в первой системе настолько, насколько это возможно (чтобы свести к минимуму проблемы, связанные с потенциально существующими общими причинами).

Например, рассмотрим ПСБ, содержащую одиночный выключатель, релейную логику и одиночный исполнительный элемент, которые составляют систему с $\text{ВОНЗ}^{\text{ср}}$, равной $7{,}7 \times 10^{-3}$. Такая система дает снижение риска, равное приблизительно $1{,}3 \times 10^2$.

Комбинация программируемой ПСБ с простой релейной ПСБ дает теоретическое снижение риска, равное $4{,}3 \times 10^5$ ($3{,}3 \times 10^3$ x$1{,}3 \times 10^2$). При такой комбинации, как показано выше, функционирование теоретически возможно (так как любая ПСБ может остановить процесс), хотя и здесь должны быть учтены факторы общей причины, и достигаемое снижение риска будет из-за них несколько ниже.

9.3 Дополнительные требования для уровня полноты безопасности 4

9.3.1 Дополнительные требования не предусмотрены.

9.3.2 Дополнительные требования не предусмотрены.

9.4 Требования к основной системе управления процессом как к слою защиты

9.4.1 ОСУП при определенных условиях может считаться слоем защиты. Если функции ОСУП выполняются в целях снижения риска процесса, то сама ОСУП может рассматриваться как средство снижения определенных рисков.

9.4.2 Снижение риска менее чем в 10 раз может быть поручено приборной системе без необходимости выполнять ее в соответствии с требованиями МЭК 61511-1. Это позволяет использовать ОСУП для некоторого снижения риска без необходимости обеспечивать соответствие таких систем требованиям МЭК 61511-1. Любое заявленное требование следует подвергнуть проверке путем анализа полноты ОСУП (определенной с помощью анализа надежности и данных о качестве функционирования) и анализа процедур, используемых для конфигурирования, модификации и режимов эксплуатации и обслуживания. Если распределение требований по снижению риска затрагивает функции ОСУП, то важно обеспечить безопасность доступа и управление изменениями. Снижение риска, которое может быть возложено на функции ОСУП, также определяется степенью независимости между функциями ОСУП и источником нарушения. На рисунке 2 показана такая независимость.

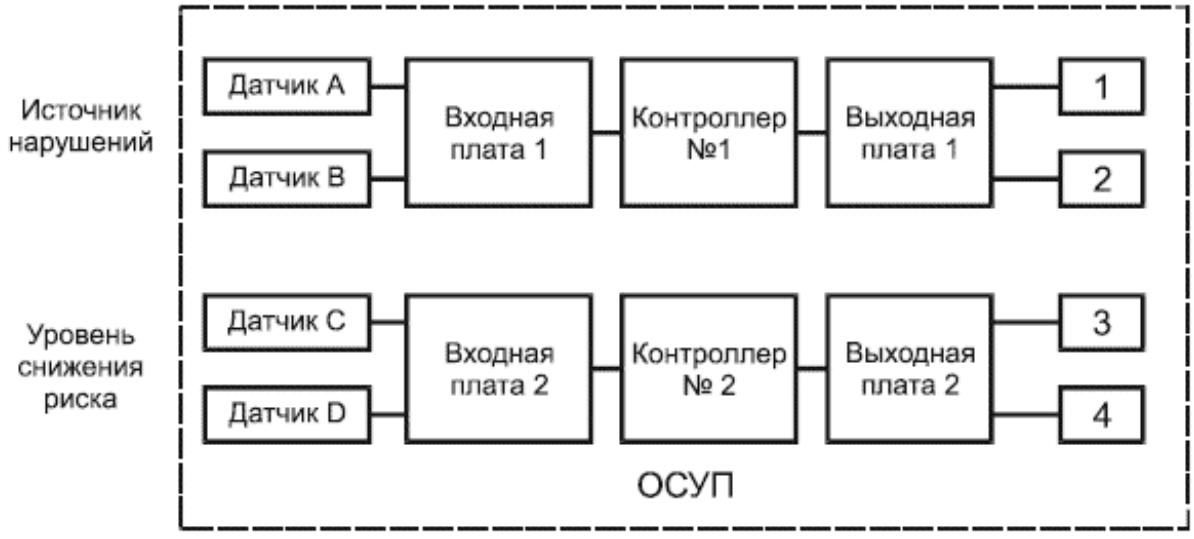


Рисунок 2 - Функция ОСУП и независимость источника нарушений

Например, рассмотрим случай, в котором контур управления расходом выполняет роль источника нарушения. Этот источник включает в себя датчик расхода, контроллер и управляющий клапан. Для того чтобы распределить снижение риска между контуром управления давлением и ОСУП, датчик давления следует соединить с независимым контроллером, воздействующим на независимый исполнительный элемент (например, выпускной клапан факельной системы).

9.5 Требования к предотвращению отказов по общей причине, отказов общего типа и зависимых отказов

9.5.1 Важно рассмотреть на ранней стадии вопрос о том, существует ли какая-либо причина отказов, являющаяся общей между резервными компонентами на каждом уровне

(например, между двумя предохранительными клапанами давления одной и той же емкости), между разными слоями защиты или между слоями защиты и ОСУП. Примером может служить ситуация, в которой отказ устройства ОСУП может привести к запросу на срабатывание ПСБ, в составе которой используется устройство с теми же характеристиками. В таких случаях необходимо установить, существует ли правдоподобный вид отказов, способных привести к одновременному отказу обоих устройств. Если такая общая причина отказов установлена, то могут быть предприняты следующие действия:

a) общая причина может быть ослаблена путем внесения изменений в проект ПСБ или ОСУП. Двумя эффективными методами снижения возможности отказов по общей причине являются разнообразие проектов и физическое разделение. Обычно такой подход предпочтителен;

b) при определении достаточности снижения общего риска следует принять во внимание возможность событий, связанных с общей причиной отказов. Может потребоваться построение анализа дерева ошибок, которое отражает как причины запроса, так и отказы системы защиты. В таком дереве ошибок могут быть представлены отказы по общей причине, а их влияние на общий риск может быть оценено количественно с помощью соответствующих методов моделирования.

Следует отметить, что любые датчики или исполнительные механизмы, являющиеся общими для ОСУП и ПСБ, очень часто порождают отказы по общей причине, и подходить к таким устройствам с общими элементами следует так, как указано в данном подпункте.

9.5.2 При проведении оценки возможности появления отказов по общей причине, отказов общего вида и зависимых отказов применимы приведенные ниже положения. Широта, строгость и глубина оценки будет зависеть от УПБ предполагаемой функции. При УПБ, равном 3 и выше, влияние отказов по общей причине, отказов общего вида и зависимых отказов может быть доминирующим. Поэтому следует рассмотреть:

- независимость между слоями защиты. Должен быть выполнен анализ влияния режима отказа, чтобы установить, может ли одинарное событие вызвать отказ больше чем одного слоя защиты или отказ ОСУП и слоя защиты. Глубина и строгость анализа будут зависеть от величины риска;

- разнообразие между слоями защиты. Целью является обеспечение разнообразия между слоями защиты и ОСУП, но это не всегда достижимо. Примером может служить защита от превышения давления, когда контур управления давлением в ОСУП может быть источником запросов. И в ОСУП, и в ПСБ требуется реализовать измерение давления, а выбор подходящего для этого оборудования ограничен. Некоторое разнообразие может быть достигнуто путем применения оборудования разных изготовителей, но если датчики в ПСБ и ОСУП подсоединяются к объекту по одинаковым схемам, такое разнообразие может быть ограниченным;

- физическое разделение между различными слоями защиты. Физическое разделение будет снижать влияние отказов по общей причине благодаря физическим причинам. Подключение измерительных компонентов ОСУП и ПСБ должно быть максимально физически разделено и подчинено функциональным потребностям, таким, как точность и время отклика.

10 Спецификация требований к безопасности ПСБ

10.1 Цель

Разработка спецификации требований к безопасности ПСБ является одной из наиболее важных процедур на всем жизненном цикле безопасности. Именно с помощью такой спецификации пользователь может определить, какие функции безопасности он хотел бы запроектировать и реализовать в ПСБ.

Полное подтверждение соответствия ПСБ выполняется с использованием этой спецификации.

10.2 Общие требования

10.2.1 Спецификация требований к безопасности ПСБ может быть отдельным документом или сборником нескольких документов, включающим процедуры, рисунки или положения стандартов предприятия. Такие требования могут быть разработаны группой, занимающейся оценкой опасности и риска, и/или самой группой разработчиков.

10.3 Требования к безопасности ПСБ

10.3.1 Как указано в МЭК 61511-1, существует ряд требований к проекту, которые должны быть определены в проекте раньше, чем будут рассмотрены функции безопасности ПСБ, обеспечивающие желательную защиту.

Спецификации требований к безопасности для отдельных подсистем могут также быть получены из этой полной спецификации.

Некоторые положения, посвященные спецификациям требований по безопасности, сводятся к следующему:

а) прежде всего необходимо определить функцию безопасности ПСБ и ее УПБ. Примером функции безопасности ПСБ служит функция "Защитить реактор от превышения давления путем открытия клапанов сброса при высоком давлении". Типичное описание функции будет содержать следующие элементы:

- измерения, необходимые для того, чтобы выявить появление условий опасных событий. Простым примером может быть повышение давления до определенного значения, подлежащего определению. Значение параметра, при котором начинаются защитные действия, должно быть вне его рабочего диапазона, но не превышать значения, которое приводит к опасному событию. Необходимо установить допустимые пределы для показателей быстродействия системы и точности измерения. При выборе этих пределов их необходимо обсудить с лицами, ответственными за разработку и создание ПСБ;

- действия, которые должны быть выполнены для предотвращения условия опасного события. Простым примером может служить снижение расхода пара, подаваемого в теплообменник на определенное время. Следует отметить, что обычно неэффективно предусматривать прекращение подачи пара в теплообменник. Проектировщику следует знать, что именно необходимо для успешной работы. Например, в нагревательных устройствах может оказаться достаточным снизить расход менее чем на 10% на одну минуту. Другим примером может быть необходимость останова объекта в течение нескольких секунд;

- действия, не требующиеся для предотвращения опасной ситуации, но которые могут быть выгодны по эксплуатационным причинам. Такими действиями могут быть формирование аварийных сигналов, отключение устройств, увеличивающих или уменьшающих поток, для сокращения запросов на другие системы защиты или действия по быстрому запуску, после того как источник опасности будет устранен. Важно отделить подобные действия от действий, необходимых для предотвращения условия опасной ситуации, чтобы минимизировать стоимость и ограничить рабочий диапазон ПСБ, что крайне необходимо. Чем шире выбран диапазон, тем труднее показать, что общая вероятность отказа по запросу соответствует требованиям, связанным с установленным уровнем полноты безопасности;

- любые выявленные состояния процесса или последовательности операций ПСБ, которые должны быть предотвращены, так как они могут приводить к опасным ситуациям;

b) спецификация требований по безопасности должна устанавливать безопасное состояние процесса для каждой определенной функции, выраженное в терминах конкретных технологических условий: какие потоки должны быть включены или остановлены, какие клапаны процесса должны быть открыты или закрыты, какими должны быть рабочие состояния любого вращающегося оборудования (насосы, компрессоры, перемешивающие устройства). Если для приведения процесса к безопасному состоянию необходимо установление некоторой упорядоченной последовательности состояний, то она также должна быть установлена.

Примечание - При выборе исполнительных элементов следует рассмотреть преимущества разнообразных решений (например, прекращение подачи продукта и расхода пара для снижения давления);

c) в самом начале следует определить требования к желательному интервалу проведения проверочных испытаний, с тем чтобы они могли быть учтены в проекте ПСБ. Например, если проверочные испытания должны выполняться только во время плановых остановов (например, каждые три года), то в проекте может потребоваться предусмотреть большее резервирование, чем в случае проведения ежегодных испытаний;

d) следует установить требования к возможности ручного перевода процесса в безопасное состояние. Например, если существует требование о том, чтобы оператор мог вручную остановить часть оборудования как из операторной, так и на месте, то это необходимо указать в спецификации. Также необходимо определить любое требование, связанное с независимостью ключей ручного останова от логического устройства ПСБ;

e) необходимо перечислить все требования, предъявляемые к повторному запуску процесса после останова. Например, некоторые пользователи применяют электронные ключи перезапуска, установленные в главном зале управления или на месте, а другие предпочитают применять соленоиды с запорными рычагами. Если к подобным действиям по перезапуску существуют специфические требования, то они должны составлять часть спецификации требований по безопасности;

f) если существует заданная частота ложных срабатываний, то ее также следует указать как часть спецификации требований по безопасности, так как она будет фактором, влияющим на проект ПСБ;

g) интерфейс между ПСБ и оператором должен быть описан полностью, включая

аварийную сигнализацию (предаварийные сигналы о неисправности устройства, сигналы останова, перепуска и диагностики устройства), графики, фиксируемые последовательности событий;

h) может оказаться необходимым предусмотреть обходные каналы (обходы), позволяющие проводить испытания или обслуживание ПСБ на действующем объекте. Если существуют специфические требования к обходу таких устройств, как ключи и пароли, то они также должны быть приведены как часть спецификации требований по безопасности;

i) следует установить виды отказов и реакцию ПСБ на обнаружение неисправностей. Например, передающее устройство может быть спроектировано таким образом, что при его отказе возникают условия срабатывания либо при его отказе не возникает условий срабатывания. Если при его отказе не возникает условий срабатывания, то важно, чтобы оператор получал сигнал об отказе передающего устройства и был обучен необходимым корректирующим действиям для получения отремонтированного передающего устройства как можно быстрее. См. также пункт 11.3 МЭК 61511-1, посвященный требованиям по обнаружению неисправностей.

10.3.2 Дополнительные требования не предусмотрены.

11 Проектирование и разработка ПСБ

11.1 Цель

Цель данного раздела - предоставить руководство по разработке ПСБ. Каждая функция безопасности ПСБ имеет свой собственный УПБ. Компонент ПСБ, например логическое решающее устройство, может использоваться несколькими функциями безопасности ПСБ с различными УПБ.

11.2 Основные требования

11.2.1 Дополнительные требования не предусмотрены.

11.2.2 Дополнительные требования не предусмотрены.

11.2.3 Дополнительные требования не предусмотрены.

11.2.4 В МЭК 61511-1 (раздел 11) содержится ряд проектных требований к ПСБ. Одно из них касается независимости между ПСБ и ОСУП.

Обычно ПСБ отделяется от ОСУП по следующим причинам:

a) чтобы уменьшить влияние ОСУП на ПСБ, особенно в тех случаях, когда они совместно используют общее оборудование. Например, если ОСУП и ПСБ используют общий клапан для задач управления и останова, то событие, состоящее в опасном отказе этого клапана, не даст возможности ПСБ выполнить функцию автоматического останова;

b) чтобы сохранить гибкость ПСБ к изменениям, обслуживанию, испытаниям и документальному оформлению.

Примечание - Обычно к ПСБ предъявляют более жесткие требования, чем к ОСУП, и

назначение ОСУП не связано с выполнением таких же жестких требований, как предъявляемых к ПСБ. Однако следует отметить, что неуправляемые изменения в ОСУП могут привести к увеличению запросов на срабатывание ПСБ;

c) чтобы облегчить подтверждение соответствия и оценку функциональной безопасности ПСБ;

d) если ОСУП объединена с ПСБ, то для соблюдения требований к управлению процессом внесения изменений может потребоваться ограничение доступа к программированию или функциям конфигурации ОСУП.

Если отказ общего оборудования может вызвать запрос к ПСБ, то следует провести анализ, чтобы убедиться, что полная интенсивность отказов соответствует ожидаемой. Полная интенсивность отказов будет равна сумме интенсивностей опасных отказов общих компонентов оборудования и интенсивности отказов по запросу от других источников (включая опасные отказы независимых частей ПСБ).

Разделение между ПСБ и ОСУП может быть реализовано по принципу идентичности или по принципу разнообразия. Применение принципа идентичного разделения означает использование той же самой технологии реализации и для ОСУП, и для ПСБ, тогда как применение принципа разнообразного разделения означает использование для реализации ОСУП и для ПСБ различных технологий от одного или разных изготовителей.

По сравнению с идентичным разделением, которое помогает при случайных отказах, разнообразное разделение дает дополнительный выигрыш в снижении вероятности систематических отказов и отказов по общей причине.

Идентичное разделение между ПСБ и ОСУП может иметь некоторые преимущества при проектировании и техническом обслуживании, так как снижает вероятность ошибок технического обслуживания. Это особенно важно, если должны применяться различные компоненты, не использовавшиеся ранее данной эксплуатационной организацией.

Идентичное разделение между ПСБ и ОСУП может быть приемлемым для применений с УПБ 1, УПБ 2 и УБП 3, хотя при этом необходимо рассмотреть источники и последствия отказов по общей причине и уменьшить возможность их появления. Некоторыми примерами отказов по общей причине являются:

a) засорение разъемов измерительных цепей и соединительных линий;

b) коррозия и эрозия;

c) неисправности аппаратных средств, вызванные окружающей средой;

d) ошибки программного обеспечения;

e) энергоснабжение и источники электропитания;

f) ошибки человека.

Разнообразное разделение предлагает дополнительный выигрыш в снижении возможности систематических ошибок (фактор, особенно важный в случаях с УПБ 3 и УПБ 4) и отказов с общей причиной.

Существует четыре зоны, в которых обычно следует обеспечить разделение между ПСБ

и ОСУП:

1) датчики на объекте;

2) исполнительные элементы;

3) логическое устройство;

4) разводка (меж)соединений.

Физическое разделение между ОСУП и ПСБ может не потребоваться, если поддерживается их независимость, а комплекс оборудования и применяемые процедуры обеспечивают, чтобы ПСБ не подвергалась опасным воздействиям, вызванным:

- отказами ОСУП;

- работами, выполняемыми на ОСУП (например, при ее техническом обслуживании, эксплуатации или модификации).

Если необходимы процедуры, обеспечивающие отсутствие опасных воздействий на ПСБ, то разработчик ПСБ должен установить их.

a) Датчики на объекте.

Использование единого датчика для ОСУП и ПСБ требует проведения дополнительного рассмотрения и анализа, так как отказ этого единого датчика может привести к опасному событию. Например, единый датчик уровня, используемый как в ОСУП, так и в качестве источника сигнала о превышении предельного уровня в ПСБ, может сформировать запрос, если датчик выходит из строя и "занижает" уровень (то есть дает сигнал о том, что уровень ниже значения, заданного для контроллера). В результате контроллер будет подавать сигнал на открытие клапана. Так как тот же датчик используется и для ПСБ, то он не обнаружит превышения уровня.

В случаях, когда для функций как ОСУП, так и ПСБ используется единый датчик, требования МЭК 61511-1 обычно выполняются только в том случае, если диагностика датчика может эффективно снизить интенсивность опасных отказов, а ПСБ способна за установленное время перевести процесс в безопасное состояние. На практике этого достичь трудно даже в случаях с УПБ 1. Чтобы добиться требуемого УБП функций безопасности ПСБ, равного УПБ 2, УПБ 3 или УПБ 4, обычно необходимо использовать идентичное или разнообразное резервирование датчиков.

Примечание - Если в ПСБ используется отдельный одинарный датчик, то может оказаться предпочтительным повторить его для ввода сигнала в ОСУП через подходящие разделители. Такая схема может способствовать улучшению охвата диагностикой, обеспечивая сравнение сигналов датчиков ОСУП и ПСБ.

В тех случаях, когда в ПСБ используются резервные датчики, они могут быть подключены также к ОСУП через подходящие разделители. При этом, применяя в ОСУП соответствующие алгоритмы, такие как "среднее из трех", можно повысить безопасность, сокращая интенсивность запросов к ПСБ.

b) Исполнительные элементы.

Аналогично датчикам использование единого клапана как в ОСУП, так и в ПСБ требует

проведения дальнейшего рассмотрения и анализа. Вообще говоря, если отказ клапана приводит к запросу на срабатывание ПСБ, использование общего клапана и для ПСБ, и для ОСУП не рекомендуется.

В случаях, когда и для ОСУП, и для ПСБ используется единый клапан, требования МЭК 61511-1 обычно выполняются только в том случае, если диагностика клапана может значительно снизить интенсивность опасных отказов, а ПСБ способна за установленное время перевести процесс в безопасное состояние.

На практике этого достичь трудно даже в случаях применения с УПБ 1. Чтобы добиться требуемого УПБ функций безопасности ПСБ, равного УПБ 2, УПБ 3 или УПБ 4, в ПСБ обычно необходимо использовать отдельные клапаны с идентичным или разнообразным резервированием.

В случаях, когда и для ОСУП, и для ПСБ используется единый клапан, разработчик должен обеспечить, чтобы действие ПСБ перекрывало действие ОСУП. Это обычно достигается путем прямого подключения ПСБ к соленоидному клапану, непосредственно отсекающему источник энергии, например между исполнительным механизмом и позиционером.

В тех случаях, когда в ПСБ используются резервные клапаны, они могут быть подключены также и к ОСУП.

Примечание - Даже при наличии резервных клапанов важно рассмотреть отказы по общей причине, свойственной и ОСУП, и ПСБ.

Для определения требований к клапану необходимо дополнительно рассмотреть:

- требования к останову;

- эксплуатационную надежность клапанов при их применении в аналогичных процессах;

- виды опасных отказов клапанов;

- эксплуатационные условия, которые делают клапан менее эффективным (например, наличие открытых клапанов байпаса);

- требования к проверочным испытаниям.

c) Разводка (меж)соединений.

Что касается подачи питания для отключения систем и соответствующей разводки соединений к периферийным ("полевым") устройствам, то разводка соединений для ОСУП с соответствующими периферийными устройствами обычно отделена от разводки соединений между ПСБ и связанными с нею периферийными ("полевыми") устройствами на объекте, так как это позволяет избежать возможности случайного отключения функций безопасности без предупреждения об этом. Типовые правила по проектированию таких систем предписывают применение отдельных многоканальных кабелей и соединительных коробок для ПСБ и ОСУП. В тех случаях, когда разводка соединений не разделена, предлагается применять строгие правила маркировки и процедуры обслуживания, способные минимизировать возможность ошибок, вызванных отключением на период обслуживания.

Примечание - Подача питания для отключения относится к цепям ПСБ, выходы и устройства которых при нормальной работе обесточены. Подача питания (например, электричества или воздуха) приводит к активации отключения.

Система монтажа кабелей (например, кабельные лотки, кабелепроводы) может быть общей как для обесточенных систем, так и для систем под напряжением, если не потребуется их разделение по другим причинам (например, для снижения электромагнитных помех). Для систем подачи питания для отключения может быть предусмотрена дополнительная противопожарная защита кабельных лотков, проходящих в огнеопасных зонах.

11.2.5 Дополнительные требования не предусмотрены.

11.2.6 См. требования 11.8 настоящего стандарта, а также примечание к пункту 11.2.5 МЭК 61511-1.

Все операторы, сотрудники обслуживающего персонала, контролеры и руководители играют свою роль в безопасном функционировании объекта. Однако люди могут совершать ошибки или могут быть не способны справиться с задачей и, так же как аппаратура и оборудование, являются субъектами неправильного срабатывания или отказа.

Вследствие этого деятельность человека тоже является элементом разработки системы. Для оперативного и обслуживающего персонала особенно важен человеко-машинный интерфейс (ЧМИ), отражающий состояние ПСБ.

Анализ надежности персонала (АНП) определяет условия, приводящие к ошибкам людей, и дает оценки интенсивностей ошибок по прошлой статистике и результатам исследований поведения. Некоторые примеры ошибок человека, вносящих свой вклад в риск безопасности химических процессов, включают в себя:

- необнаруженные ошибки при проектировании;

- ошибки эксплуатации (например, неправильная уставка);

- неправильное техническое обслуживание (например, замена клапана на неисправный экземпляр);

- ошибки в калибровке, тестировании или интерпретации выходных сигналов систем управления;

- невыполнение должных действий при аварии.

Примечание - Дополнительные указания можно найти в [6]-[8].

11.2.7 Этот подпункт посвящен возможной опасности, которая может возникать, если ПСБ автоматически перезапускает процесс сразу после устранения условий срабатывания. Следует проанализировать каждую функцию безопасности ПСБ, чтобы определить, как ее надо перенастроить после срабатывания. Обычно повторный запуск возможен только после ручного вмешательства оператора.

11.2.8 Могут быть предусмотрены средства ручного вмешательства, независимые как от логического устройства ПСБ, так и от системы управления ОСУП, позволяющие

оператору в случае аварии начать останов. Требования к ручному останову обычно устанавливают в спецификации требований по безопасности.

При необходимости процедура аварийного останова в чрезвычайной ситуации может быть включена в программируемую логику решающего устройства ПСБ (например, когда требуется выполнить последовательность действий по останову), если такое решение представляется подходящим группе специалистов по АНП.

11.2.9 Данный пункт указывает на необходимость провести анализ независимости между ПСБ и другими слоями защиты, а не только между ПСБ и ОСУП (см. МЭК 61511-1, рисунок 9).

В некоторых случаях может быть допустимо неполное разделение между ОСУП и ПСБ. В частности, это возможно, если отказ общего оборудования не будет формировать запрос к ПСБ. В таких случаях необходимо применять общее или раздельное оборудование в соответствии с МЭК 61511-1.

Если отказ общего оборудования может привести к запросу на ПСБ, тогда следует провести анализ, позволяющий убедиться в том, что полная интенсивность отказов соответствует ожидаемой интенсивности. Полная интенсивность отказов будет равна сумме интенсивности опасных отказов общих компонентов и интенсивности отказов по запросу от других источников (включая опасные отказы независимых частей ПСБ). Чтобы установить опасности, связанные с опасными отказами общего оборудования, необходимо рассмотреть следующие случаи:

a) если один из компонентов резервной схемы используется как часть ОСУП, то рассматривают опасности, вызванные появлением опасных отказов общего оборудования, учитывая, что функционирование ПСБ ухудшилось из-за отказавших приборов;

b) если общие компоненты не резервированы, то рассматривают опасности, вызванные появлением опасных отказов общего оборудования, принимая, что ПСБ не срабатывает.

11.2.10 Необходимо обеспечить предупреждающие указания по применению элементов, общих как для ОСУП, так и для ПСБ. Слова "достаточно низка" в примечании к пункту 11.2.10 МЭК 61511-1 означают, что интенсивность опасных отказов совместно используемого оборудования, умноженная на ВОНЗ других (отличных от ПФБ) слоев защиты, соответствует принятому корпорацией критерию допустимого риска.

11.2.11 В тех случаях, когда исполнительные элементы при потере питания не переходят в безопасное состояние (например, обеспечение срабатывающих систем питанием), следует рассмотреть достаточность средств ручного управления для перевода объекта в такое состояние.

11.3 Требования к поведению системы при обнаружении отказа

11.3.1 Дополнительные требования не предусмотрены.

11.3.2 Дополнительные требования не предусмотрены.

11.3.3 Дополнительные требования не предусмотрены.

11.4 Требования к отказоустойчивости аппаратных средств

11.4.1 Традиционный подход к разработке системы безопасности состоит в обеспечении того, что никакой одиночный сбой не приведет к невыполнению предполагаемой функции. У систем, построенных по таким структурам, как "1 из 2" или "2 из 3", отказоустойчивость равна единице, так как они способны функционировать даже при наличии в них одного опасного сбоя. Такие системы применяют в качестве стандартного подхода при построении систем безопасности, обеспечивая достаточную устойчивость при противостоянии случайным отказам аппаратных средств. Структуры с допустимым числом отказов защищают также от широкого ряда систематических отказов (главным образом в аппаратных средствах), так как такие отказы необязательно происходят в одинаковые моменты времени.

Настоящий стандарт определяет, что промышленные процессы нуждаются в многоуровневых системах безопасности, и принимает концепцию УПБ для каждого слоя защиты в зависимости от потребности в снижении риска в конкретных условиях применения. Так как слои защиты различаются, то нельзя утверждать, что все УПБ обеспечат им отказоустойчивость. Однако при выборе структуры для конкретного УПБ важно обеспечить, чтобы она была достаточно устойчива и к случайным сбоям аппаратных средств, и к систематическим сбоям. Для того чтобы обеспечить устойчивость к случайным сбоям аппаратных средств, следует провести анализ надежности.

Требования настоящего стандарта направлены на обеспечение того, чтобы структуры имели необходимую отказоустойчивость при случайных сбоях аппаратных средств и некоторых систематических сбоях. При определении необходимой степени отказоустойчивости необходимо рассмотреть следующий ряд факторов:

- сложность устройств, используемых в подсистеме. Устройство будет более устойчиво к систематическим сбоям, если хорошо известны виды его отказов, может быть определено его поведение в условиях отказа и имеется достаточно данных по его эксплуатационной надежности;

- мера того, насколько неисправности ведут к нарушению безопасных условий или насколько они могут быть выявлены диагностикой так, чтобы можно было предпринять определенные действия. Это свойство определяется через долю безопасных отказов устройства;

- требование к УПБ для рассматриваемого случая применения.

Международная рабочая группа, подготовившая МЭК 61508, рассмотрела указанные факторы и установила в МЭК 61508-2 величину допустимого числа отказов. При подготовке настоящего стандарта, ориентированного на сектор промышленных процессов, было принято, что требования к отказоустойчивости устройств, установленных на объекте, и непрограммируемых логических устройств могут быть упрощены, а в качестве альтернативных могут быть применены требования, установленные в МЭК 61511-1. Следует отметить, что при разработке подсистем, чтобы удовлетворить требованиям готовности, может потребоваться большее резервирование компонентов, чем это указано в таблицах 5 и 6.

Требования к отказоустойчивости аппаратных средств могут быть применены к отдельным компонентам или подсистемам, выполняющим требуемую функцию безопасности ПСБ. Например, в случае сенсорной подсистемы, включающей несколько

резервных датчиков, требование к отказоустойчивости применяется к подсистеме в целом, а не к отдельным датчикам.

11.4.2 Таблица 5 МЭК 61511-1 устанавливает минимальное допустимое число отказов для программируемых электронных логических устройств. Требование отказоустойчивости зависит от требуемого значения УПБ для данной ПСБ и доли безопасных отказов (ДБО) подсистемы. Сведения о ДБО логического решающего устройства обычно можно получить от его поставщика. Если логический решатель с программируемой электроникой применяется в условиях, которые не соответствуют принятым при расчетах ДБО, то следует тщательно рассмотреть утверждения, сделанные ДБО. В частности, должны быть проверены сделанные предположения, чтобы убедиться, что ограничения и характеристики окружающей среды, принятые при расчетах ДБО, соответствуют рассматриваемому случаю применения. Именно поэтому ДБО будут зависеть от ряда позиций, таких как подается или отключается питание подсистемы при ее срабатывании. Источники данных и допущений, принятых в ходе расчетов ДБО, следует документально оформлять. ДБО относится только к случайным отказам аппаратных средств. При установлении ДБО допускается принимать допущения, что подсистема была должным образом выбрана для применения и соответственно установлена, укомплектована персоналом и обслуживается таким образом, что отказы на ранних стадиях и связанные с ее развитием могут быть исключены из оценки. Рассмотрение человеческих факторов при определении ДБО также не требуется.

11.4.3 Таблица 6 МЭК 61511-1 устанавливает базовый уровень числа допустимых отказов для датчиков, исполнительных устройств и логических решающих устройств с непрограммируемой электроникой, имеющих предельный требуемый УПБ, приведенный в первой графе таблицы. Требования в таблице 6 основаны на требованиях, установленных в МЭК 61508-2 для устройств с программируемой электроникой с ДБО от 60% до 90%. Эти требования базируются на предположении, что доминирующим видом отказов являются отказы, происходящие в безопасном состоянии, или что опасные отказы выявляются.

11.4.4 Данным подпунктом разрешается при определенных условиях снижать на единицу допустимое число отказов любых подсистем, кроме программируемых электронных логических устройств. Эти условия применимы к таким устройствам, как клапаны или интеллектуальные датчики, и уменьшают вероятность систематических отказов так, что требования снижаются до уровня, установленного в МЭК 61508-2 для устройств с непрограммируемой электроникой.

11.4.5 В некоторых случаях допустимое число отказов может быть снижено путем соблюдения требований МЭК 61508-2. Этого можно достичь с помощью введения дополнительных диагностических операций, таких как сравнение сигналов или регулярные испытания на частичную перегрузку так, чтобы ДБО подсистемы составляла не менее 90%.

11.5 Требования к выбору компонентов и подсистем

11.5.1 Цели

Дополнительные требования не предусмотрены.

11.5.2 Общие требования

11.5.2.1 Существуют определенные соображения по выбору компонентов и подсистем, применяемых в ПСБ. Первое мнение состоит в том, что компоненты должны быть разработаны в соответствии с МЭК 61508-2 (требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью) и МЭК 61508-3 (требования к ПО). Второе мнение сводится к тому, что следует использовать компоненты и подсистемы, о которых известно, что они надежно и широко применяются в аналогичных задачах и окружающих условиях.

Какое бы мнение ни было выбрано, необходимо продемонстрировать, что компонент или подсистема:

a) достаточно надежны, чтобы можно было достичь общей заданной ВОНЗ или заданной интенсивности опасных отказов ПФБ;

b) отвечают требованию структурных ограничений;

c) имеют достаточно низкую вероятность систематических сбоев.

Требование перечисления c) может быть выполнено либо в соответствии с МЭК 61508-2 и МЭК 61508-3, либо путем предшествующего использования требований, установленных в 11.5 настоящего стандарта.

11.5.2.2 Дополнительные требования не предусмотрены.

11.5.2.3 Дополнительные требования не предусмотрены.

11.5.2.4 Дополнительные требования не предусмотрены.

11.5.3 Требования к выбору компонентов и подсистем на основе опыта их предшествующего применения

11.5.3.1 Внешних устройств (датчиков и клапанов), которые спроектированы в соответствии с требованиями МЭК 61508-2 и МЭК 61508-3, не очень много. Поэтому пользователи и проектировщики вынуждены рассчитывать на применение таких устройств, по которым имеется опыт предшествующего применения.

Многие пользователи располагают перечнем приборов, утвержденных или рекомендованных к применению для их потребностей. Такие перечни сформированы на основе широкого промышленного опыта успешного применения устройств в ОСУП. Применение датчиков и клапанов, по которым история функционирования отсутствует, нежелательно.

Обычно датчики и клапаны, приведенные в утвержденных или рекомендованных перечнях для ОСУП, могут также рассматриваться как имеющие опыт применения в ПСБ, оцениваемых по требованиям МЭК 61511-1. Такой перечень приборов должен содержать версию устройств и документально оформленные действия пользователя и изготовителя, связанные с возвратами приборов с объектов. Кроме того, изготовитель должен установить процесс внесения изменений, учитывающий влияние зафиксированных отказов и реализуемых изменений.

Если подобный перечень отсутствует, то пользователям и проектировщикам следует провести оценку датчиков и клапанов, чтобы убедиться, что эти приборы соответствуют желательному функционированию. Могут потребоваться консультации с другими

пользователями или проектировщиками, чтобы учесть результаты применения устройств в аналогичных случаях.

11.5.3.2 Необходимо отметить, что для более сложных устройств может оказаться затруднительным показать, что опыт, полученный в некотором применении, полезен в решаемой задаче. Например, опыт применения программируемых логических контроллеров (ПЛК) для случая, предусматривающего использование простой многоступенчатой логики, может не подойти для технических средств, которые будут использованы для выполнения сложных вычислений или обработки событий.

Вообще говоря, соответствующие аспекты работы периферийных устройств и логического решающего устройства различны.

Работу периферийных устройств характеризуют следующие аспекты:

- функциональное назначение (например, измерение, управляющее действие);

- рабочий диапазон;

- свойства процесса (например, свойства химических веществ, температура, давление);

- подключение к процессу.

Работу логических решающих устройств характеризуют следующие аспекты:

- версия и структура аппаратных средств;

- версия и конфигурация системного программного обеспечения;

- прикладное программное обеспечение;

- конфигурация ввода-вывода;

- быстродействие;

- интенсивность запросов процесса.

Работу всех устройств характеризуют следующие аспекты:

- электромагнитная совместимость (ЭМС);

- условия окружающей среды.

11.5.4 Требования к выбору компонентов и подсистем, программируемых на фиксированном языке программирования (ФЯП) (например, внешних устройств), на основе опыта их применения

11.5.4.1 Дополнительные требования не предусмотрены.

11.5.4.2 Дополнительные требования не предусмотрены.

11.5.4.3 Дополнительные требования не предусмотрены.

11.5.4.4 Данный подпункт разъясняет дополнительные требования, применяемые при попытках квалифицировать устройство, программируемое на ФЯП, как способное

обеспечить УПБ 3.

11.5.4.5 Данный подпункт устанавливает требования к инструкции по безопасности устройства с УБП 3, программируемого на ФЯП.

11.5.5 Требования к выбору компонентов и подсистем, программируемых на языке программирования с ограниченной изменчивостью (ЯОИ) (например, логических решающих устройств), на основе опыта их применения

11.5.5.1 В данном подпункте приведены дополнительные требования, предъявляемые к программируемым на ЯОИ электронным логическим устройствам, выполняющим функции безопасности ПСБ с УПБ 1 или УПБ 2. Логические решающие устройства с программируемой электроникой, использующие ЯОИ, выполняющие функции безопасности ПСБ с УПБ 3 и УПБ 4, должны быть выполнены согласно МЭК 61508-2 и МЭК 61508-3.

11.5.5.2 Дополнительные требования не предусмотрены.

11.5.5.3 Дополнительные требования не предусмотрены.

11.5.5.4 Дополнительные требования не предусмотрены.

11.5.5.5 В данном подпункте приведены дополнительные требования для используемых в применениях с УПБ 1 и УПБ 2 безопасно сконфигурированных логических решающих устройств, программируемых на ЯОИ. Дополнительные соображения приведены в приложении D.

11.5.5.6 В данном подпункте перечислены дополнительные требования для используемых в применениях с УПБ 2 безопасно сконфигурированных логических решающих устройств с программируемой электроникой, программируемых на ЯОИ.

11.5.5.7 Данный подпункт устанавливает требования к инструкции по безопасности устройства с УПБ 2, программируемого на ЯОИ.

11.5.6 Требования для выбора компонентов и подсистем, использующих язык программирования с полной изменчивостью (ЯПИ) (например, логических решающих устройств)

11.5.6.1 Дополнительные требования не предусмотрены.

11.6 Внешние устройства

11.6.1 Дополнительные требования не предусмотрены.

11.6.2 Дополнительные требования не предусмотрены.

11.6.3 Дополнительные требования не предусмотрены.

11.6.4 Дополнительные требования не предусмотрены.

11.7 Интерфейсы

К интерфейсам пользователей ПСБ относятся интерфейсы оператора и интерфейсы обслуживания/разработки. Данные или информация, которой обмениваются ПСБ и

рабочие места операторов, могут быть как связанными с ПСБ, так и справочными.

Если действие оператора является частью функции безопасности ПСБ, то все, что должно быть выполнено для реализации этого действия, необходимо рассматривать как часть функции безопасности ПСБ. В это действие, например, может быть включен аварийный сигнал, указывающий на то, что оператор должен остановить процесс. В этом примере выключатель останова (как и иные технические средства, обеспечивающие действия по останову) надо рассматривать как часть функции безопасности ПСБ.

Передача данных, не являющихся частью функции безопасности ПСБ (например, индикация действительного значения сигнала датчика функции безопасности ПСБ при условии, что функция срабатывания реализована внутри функции безопасности ПСБ), может осуществляться в ОСУП, если можно показать, что функции безопасности ПСБ не подвергаются риску (например, при реализации в ОСУП доступа к ним только в режиме чтения).

11.7.1 Требования к интерфейсу оператора

Интерфейсы оператора, использующиеся для обмена информацией между оператором и ПСБ, могут включать в свой состав:

- видеодисплеи;

- панели, содержащие лампочки, кнопки и переключатели;

- сигнальные устройства (визуальные и звуковые);

- принтеры (не должен быть единственным средством вывода информации);

- любую их комбинацию.

а) Видеодисплеи

Видеодисплеи ОСУП могут совместно использоваться функциями ПСБ и ОСУП, если они отображают только справочную информацию. Информация, критичная для безопасности, должна дополнительно индицироваться через ПСБ (например, если оператор выполняет часть функции безопасности).

Если во время аварийных ситуаций необходимо действие оператора, то темпы добавления и обновления данных на операторском дисплее должны соответствовать спецификации требований по безопасности.

Видеодисплеи, связанные с ПСБ, должны быть ясно определены в качестве таковых во избежание двусмысленности или возможного замешательства оператора в аварийной ситуации.

Интерфейс оператора ОСУП может быть использован для обеспечения автоматической регистрации событий функций безопасности ПСБ и функций формирования аварийных сигналов ОСУП.

Условия, подлежащие регистрации, могут включать:

- события, происходящие в ПСБ (такие, как срабатывание и предаварийные происшествия);

- доступна ли ПСБ к изменениям в программах;

- результаты диагностики (например, расхождение и т.п.).

Важно, чтобы оператор был готов к обходу любой части ПСБ с помощью процедуры, обрабатывающей аварийный сигнал, и/или рабочей процедуры. Например, обход исполнительного элемента в ПСБ (например, запорного клапана) может быть выполнен с использованием концевых переключателей обходимого клапана, которые включают аварийный сигнал на панели оператора, или установленных перемычек, или механических блокировок на обходимом клапане, которыми управляют рабочие процедуры. Вообще предлагается поддерживать эти аварийные сигналы обхода отдельно от ОСУП.

b) Панели

Панели должны быть расположены так, чтобы операторы имели к ним свободный доступ.

Панели должны быть устроены так, чтобы расположение кнопок управления, лампочек, индикаторов и других источников информации не запутывало оператора. Если выключатели останова для различных модулей процесса или оборудования выглядят одинаково и расположены вместе, то возможен останов не того оборудования, если оператор находится в состоянии стресса при аварийной ситуации. Выключатели останова должны быть физически разнесены и снабжены этикеткой с названием функции. Должны существовать средства проверки всех лампочек.

c) Принтеры и регистраторы

Принтеры, подключенные к ПСБ, не должны нарушать функцию безопасности ПСБ в случаях их неисправности, отключения, окончания бумаги или аномальной работы.

Принтеры полезны для распечатки последовательностей событий, результатов диагностики и других событий и аварийных сигналов, имеющих метки времени и даты и идентификационные номера. Следует предусматривать вспомогательные средства для формирования отчетов.

Если печать выполняется через буферную память (информация собирается, хранится и затем печатается по запросу или в заданное время), то емкость буфера должна быть такой, чтобы информация не была потеряна и чтобы функции ПСБ ни при каких обстоятельствах не нарушались из-за переполнения буферной памяти.

11.7.1.1 Чтобы быстро передать оператору критическую информацию, надо дать ему всю необходимую информацию на одном дисплее. Важно обеспечить логичность показаний, поэтому методы, порядок включения сигнализации и компоненты дисплея следует согласовывать с дисплеями ОСУП.

Важно также размещение информации по дисплеям. Необходимо избегать размещения большого количества информации на одном дисплее, так как это может привести операторов к ошибочному считыванию данных и выполнению неправильных действий. Чтобы направить внимание оператора на важную информацию, сокращая при этом вероятность его ошибок, необходимо использовать цвета, мигающие индикаторы и разумное расположение данных на экране дисплея. Сообщения должны быть ясными, четкими и однозначными.

Информация на дисплее должна быть сформирована так, чтобы данные могли быть

распознаны даже операторами, страдающими дальтонизмом. Например, информация, представленная красным или зеленым цветом, могла бы быть одновременно представлена графическим объектом с заливкой или без заливки соответственно.

11.7.1.2 Дополнительные требования не предусмотрены.

11.7.1.3 Дополнительные требования не предусмотрены.

11.7.1.4 Дополнительные требования не предусмотрены.

11.7.1.5 Дополнительные требования не предусмотрены.

11.7.2 Требования к интерфейсу обслуживания/разработки

11.7.2.1 Дополнительные требования не предусмотрены.

11.7.2.2 Интерфейсы технического обслуживания/разработки включают в свой состав средства программирования, испытаний и технического обслуживания ПСБ. Эти интерфейсы представляют собой устройства, которые используются для выполнения функций, таких как:

a) системное конфигурирование аппаратных средств;

b) разработка, документальное оформление и загрузка прикладного ПО логического решающего устройства ПСБ;

c) доступ к прикладному ПО для выполнения изменений, испытаний и контроля;

d) наблюдение за системными ресурсами ПСБ и диагностической информацией;

e) изменение уровней безопасности ПСБ и доступа к переменным прикладного ПО.

Интерфейсы технического обслуживания/разработки должны отображать действия и диагностическое состояние любых компонентов ПСБ (например, входных модулей, процессоров), включая связи между ними.

Такие интерфейсы должны предоставлять средства для копирования прикладных программ на носители для создания резервных копий.

Если подключенный с ПСБ для технического обслуживания/разработки персональный компьютер неисправен, выключен или отсоединен, то он не должен нарушать функции безопасности ПСБ.

11.7.2.3 Дополнительные требования не предусмотрены.

11.7.2.4 Дополнительные требования не предусмотрены.

11.7.3 Требования к коммуникационным интерфейсам

11.7.3.1 Дополнительные требования не предусмотрены.

11.7.3.2 Дополнительные требования не предусмотрены.

11.7.3.3 Дополнительные требования не предусмотрены.

11.7.3.4 Дополнительные требования не предусмотрены.

11.8 Требования к проектированию обслуживания или испытаний

11.8.1 В проекте ПСБ должно быть учтено, как система должна обслуживаться и проверяться. Если ПСБ должна проверяться на действующем процессе, то в проекте не должны предусматриваться отсоединение проводов, применение перемычек или вызов программных регистров, так как использование подобных технических решений может угрожать нарушением цельности ПСБ. В проекте системы должны быть предусмотрены технические и процедурные требования к ПСБ, необходимые для проведения полных системных испытаний датчиков, логического решающего устройства и исполнительных элементов на безопасность.

Важно определить, как будет проводиться обслуживание системы в действующем процессе. Например, если датчик или клапан должен оставаться в работе, то необходимо рассмотреть, как обслуживающее подразделение будет работать с этими устройствами, не вызывая случайных срабатываний, сохраняя безопасность процесса.

Необходимо отметить, что любое ограничение межпроверочного интервала

исполнительных элементов должно быть учтено при вычислении значений $ВОНЗ^{ср}$ для функции безопасности ПСБ.

11.8.2 Дополнительные требования не предусмотрены.

11.8.3 Установка байпасов может привести к снижению уровня безопасности ПСБ. Такое снижение можно ослабить следующими приемами:

a) применением паролей и/или ключа блокирования переключателей. В некоторых проектах могут быть предусмотрены запираемые шкафы, содержащие соответствующие средства для обхода;

b) явным выделением обходных схем, которое может быть дополнено либо опечатыванием положений клапана, либо установкой знаков безопасности, указывающих на важность соответствующей позиции.

Например, при конфигурации датчика по схеме "1 из 2" некоторые пользователи предпочитают иметь обход, охватывающий оба датчика одновременно, тогда как другие предпочитают иметь раздельные обходы для каждого датчика. Если оба датчика имеют обходы, необходимо предусмотреть меры, обеспечивающие приемлемый риск. Если это невозможно, следует вернуться на более раннюю стадию разработки.

Аналогично некоторые операции процесса не допускают изменения положения клапана на действующем объекте, либо установка средств обхода клапана может оказаться нецелесообразной. В таких случаях проект должен предусматривать проведение проверки ПСБ, насколько это практически возможно, то есть по крайней мере с помощью соленоидного клапана. При этом в проект может быть включен обход соленоида с обычной процедурой обработки аварийного сигнала или процедурами контроля этого обхода.

11.8.4 Дополнительные требования не предусмотрены.

11.9 Вероятность отказа функции безопасности ПСБ

11.9.1 Пользователи и разработчики должны руководствоваться методиками, представленными в приложении А, которые обеспечивают, что функционирование разрабатываемой ПСБ удовлетворяет требованиям, связанным со случайными отказами аппаратных средств.

11.9.2 Большинство методик в приложении А требует некоторой количественной оценки охвата диагностикой ПСБ. Диагностика - это автоматическое выполнение тестов для обнаружения сбоев в ПСБ, которые могут привести к безопасным или опасным отказам.

Конкретный метод диагностики обычно не позволяет обнаружить все возможные сбои. Эффективность используемой диагностики может быть оценена для набора сбоев, для которого предназначен этот метод диагностики. В подпунктах 7.4.4.5 и 7.4.4.6 МЭК 61508-2 рассмотрены требования к определению метода диагностики (см. также приложение 6 [9], где представлен пример расчета охвата диагностикой).

Повышение охвата диагностикой ПСБ может помочь выполнению требований, предъявляемых по УПБ. В этом случае при расчете вероятности отказов (в режиме запросов) или интенсивности отказов (в непрерывном режиме) ПСБ должны быть учтены как охват диагностикой, так и период проведения диагностических проверок (междиагностический интервал). Дополнительные указания см. в приложении В [9] или в [10].

Если ПСБ является единственным слоем защиты и используется для выполнения функции безопасности в непрерывном режиме, то междиагностический интервал должен быть таким, чтобы сбои в ПСБ были обнаружены за время, достаточное для обеспечения полноты ПСБ и выполнения действий, позволяющих в случае отказа в процессе или в ОСУП сохранить безопасное состояние.

Чтобы этого добиться, сумма междиагностического интервала и времени реакции, позволяющего перейти в безопасное состояние, должна быть меньше, чем время безопасности процесса. Время безопасности процесса определяется как время между отказом (потенциально способным привести к опасному событию), возникающим в процессе или в ОСУП, и появлением опасного события, если функция безопасности ПСБ не выполняется.

Критичные и потенциально критичные неисправности в общих компонентах (таких как центральный процессор, устройства памяти типов RAM или ROM) обычно препятствуют почти всему процессу обработки данных, и их гораздо труднее обнаружить, чем неисправность отдельного выходного устройства. Виды отказов, имеющих высокую вероятность, должны выявляться с большей достоверностью. Более того, следует учитывать выявляемость отказов данного вида.

Для каждой реализуемой диагностики интервал проведения проверок и действие, вызванное выявленной неисправностью, должны удовлетворять спецификации требований к безопасности.

Если такие диагностические средства не встроены в поставляемое оборудование, то на системном или прикладном уровне могут быть реализованы внешние средства диагностики, чтобы удовлетворить УПБ функции безопасности ПСБ.

Диагностика может не обнаружить систематических ошибок (таких, как ошибки в программах). Однако можно осуществить подходящие предупредительные меры, чтобы

обнаружить возможные систематические ошибки.

Диагностику можно выполнить, используя разнообразные методы или их комбинацию, включая:

a) для датчиков:

1) могут быть предусмотрены диагностические сигналы, означающие, что выявлен полный отказ датчика с выходом его выходного сигнала за верхнюю или нижнюю границу диапазона измерений. Одним из путей, которым это может быть достигнуто, является использование аварийного сигнала, если значения датчика оказались вне его рабочего диапазона. Например, в применение, контролирующее высокую температуру и использующее резервные температурные датчики, чтобы диагностировать отказ датчика или потерю его сигнала, можно добавить аварийный сигнал, если значение сигнала датчика оказалось ниже нижнего уровня его рабочего диапазона;

2) если используют резервные датчики, то сравнение аналоговых значений позволяет выявить аномалии, происшедшие при нормальной работе. Если применяют три датчика, то можно использовать значение датчика, являющееся средним из этих трех датчиков (отбор среднего значения). Отбор среднего значения обладает преимуществом по отношению к среднему арифметическому от трех датчиков, потому что среднее арифметическое искажается неправильно функционирующим устройством. Значительные расхождения между показаниями устройств могут быть из-за:

- засорения разъемов измерительных цепей и соединительных линий;

- снижения давления в системе очистки;

- зарастания каналов ввода термопар;

- проблем с заземлением или энергопитанием;

- отсутствия реакции датчика, выходной сигнал которого перестал изменяться;

3) могут быть введены временные задержки для предотвращения случайных срабатываний аварийной сигнализации из-за различия времени реакции датчиков на изменения в процессе, связанного с размещением датчика или принципом его действия. Например, некоторые резервные датчики расхода могут иметь задержки от 1 до 2 с. Существует много пакетов программ, поставляемых продавцами датчиков, для контроля показаний резервных датчиков и вычисления стандартного отклонения, способных инициировать диагностическую сигнализацию;

4) другим способом диагностики датчика является сравнение с изменениями связанных переменных (например, показания накопительных расходомеров сопоставляются с изменениями уровня в емкости или с соотношениями давления и температуры);

b) для исполнительных элементов:

1) для проверки выполнения ожидаемых действий может быть проведено сравнение сигналов обратной связи, получаемых с выхода исполнительного элемента (такого, как сигнал конечного выключателя или сигнал от датчика положения), с требуемым состоянием. Чтобы отфильтровать сигнал, получаемый во время перемещения клапана (например, от полностью открытого до полностью закрытого положения), следует

использовать значительные временные задержки. Если клапан в ходе нормальной работы периодически меняет свое безопасное состояние (например, в операциях дозирования), то это сравнение сигнала обратной связи исполнительного элемента с требуемым его состоянием можно рассматривать только как диагностическую операцию;

2) некоторые клапаны, приводы, соленоиды и/или позиционеры могут обладать способностью к самодиагностированию;

c) для логических решающих устройств:

- в типовых случаях программируемые электронные логические устройства, подготовленные для задач безопасности или отвечающие требованиям серии стандартов МЭК 61508, включают в себя диагностические средства, выявляющие различные неисправности. Типы таких средств и их степень диагностируемости обычно описываются в руководствах по безопасности;

d) для внешних средств диагностики:

- примерами таких средств служат контрольные (сторожевые) таймеры и концевые мониторы.

В связи с примечанием к перечислению c) пункта 11.9.2 МЭК 61511-1, в котором рассмотрена степень доверия к данным по надежности, среднее время до отказа $T_{\text{ср}}$ обычно определяется путем регистрации числа отказов n , происшедших на образцах компонентов за накопленное число часов работы T . Уровень доверия к результирующему значению $T_{\text{ср}}$ может быть получен по критерию "Хи - квадрат" [11]. Это означает, что значение $T_{\text{ср}}$, которое должно применяться в расчетах надежности ПСБ, будет, вообще говоря, ниже, чем $T_{\text{ср}}$, рассчитанное как T/n . Такое снижение будет тем больше, чем выше требуемый уровень доверия и чем меньше число зафиксированных отказов. Однако, как правило, можно принимать, что при уровне доверительной вероятности 70% коэффициент снижения незначителен по сравнению с другими источниками неопределенностей, связанных с моделированием надежности.

12 Требования к прикладному ПО, включая критерии выбора сервисного ПО

В разделе 12 МЭК 61511-1 не делается различий в методах разработки прикладного программного обеспечения (ППО) для систем с УПБ 3 и с более низким УПБ, так как опыт показывает, что существует небольшая разница в методах, используемых для:

- программ, составленных на ФЯП или ЯОИ;

- логических устройств, отвечающих требованиям МЭК 61511-1;

- соответствующих руководств по безопасности.

При разных УПБ могут быть различия в испытаниях и верификации. Дополнительные указания см. в 12.7.2.3.

12.1 Требования к жизненному циклу безопасности ППО

12.1.1 Цели

12.1.1.1 Дополнительные требования не предусмотрены.

12.1.2 Требования

12.1.2.1 Дополнительные требования не предусмотрены.

12.1.2.2 К примечаниям 1 и 2 МЭК 61511-1. Если для разработки, реализации, верификации и подтверждения соответствия прикладных программ применяются ЯОИ, такие как язык ступенчатых диаграмм или функциональных блок-схем по [12], то применимы только два уровня стандартной V-модели ПО, показанные на рисунке 3. В этом случае принимается, что используемые функциональные блоки соответствуют МЭК 61508-3, и тогда:

- "разработка архитектуры ППО" применяется к ПО каждой функции безопасности ПСБ так, чтобы обеспечить совместимость проекта ПО со структурой аппаратных средств;

- "разработка ППО" интерпретируется как проектирование и реализация логики безопасности, построенной на ЯОИ в соответствии с МЭК 61508-3 и МЭК 61508-4;

- "проверка ППО" интерпретируется как верификация и испытание прикладных программ, и

- "интеграция ППО с подсистемами ПСБ" трактуется как интеграция и верификация каждой функции безопасности процесса, выполненной на ЯОИ.

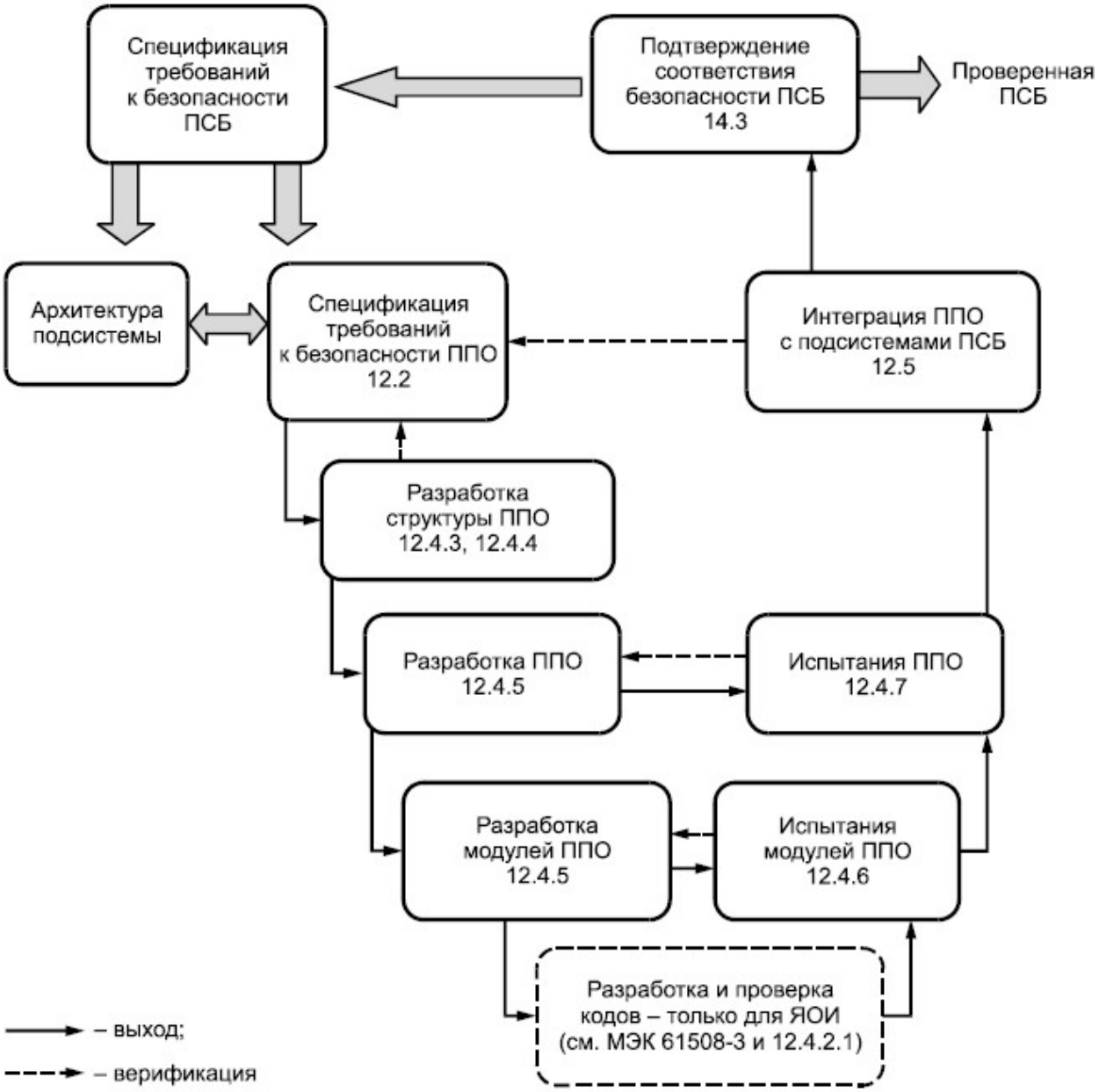
Пример жизненного цикла разработки ППО, используемого в ПЛК с УПБ 3, соответствующий МЭК 61508, приведен в приложении D.

Если необходимо реализовать новую "функцию" или "функциональный блок", используя элементы ЯОИ, соответствующие МЭК 61508 (например, выполнение общей последовательности выключения горелки или насоса), то тогда:

- "разработка прикладного модуля" по V-модели интерпретируется как проектирование и реализация новой функции, а

- "проверка прикладного модуля" интерпретируется как верификация и испытание новой функции.

В тех случаях, когда новая функция должна быть записана на ЯОИ и, таким образом, необходимо кодирование ПО, разработчику следует, как это показано на V-модели (рисунок 3), выполнить все фазы жизненного цикла и процедуры, установленные в МЭК 61508-3.



Примечание - Если не указано иное, то номера подразделов и пунктов, указанные на рисунке, соответствуют принятым в МЭК 61511-1.

Рисунок 3 - Жизненный цикл разработки ПО (V-модель)

12.1.2.3 Дополнительные требования не предусмотрены.

12.1.2.4 При выборе методов, способов и средств учитывают следующее.

Чтобы выбрать методы, способы и средства, которые могут содействовать созданию ПО с требуемым качеством, следует учитывать следующие ключевые для ППО параметры качества:

- простоту;

- наличие соответствующих комментариев и описаний на естественном языке;

- разумную структуризацию, отражающую данное применение;

- охват тестированием;

- понятность для персонала, участвующего в процессе сопровождения;

- общность стиля с другими связанными прикладными программами.

Подходы, используемые для определения ключевых параметров, предусматривают:

- обсуждения с посредниками, включая участников процессов эксплуатации и обслуживания;

- обзор текущей практики и промышленных стандартов;

- обзор рекомендаций изготовителей;

- анализ предшествующего опыта;

- обсуждение с ведущими специалистами.

Выбор методов, способов и средств оптимизации ключевых параметров качества проводят с учетом перечисленных ниже положений.

Следует выбирать такие методы и способы, которые минимизируют риск введения ошибок в ППО в течение его разработки. Это может потребовать рассмотрения следующих их аспектов:

- хорошо определенные синтаксис и семантика;

- пригодность для данного случая применения;

- понятность для разработчиков;

- гарантированность свойств, важных для ПФБ (например, время выполнения в наихудшем случае);

- наличие успешного опыта использования для аналогичных применений;

- правила и ограничения, направленные на ослабление влияния "небезопасных" особенностей метода.

Следует выбирать такие инструментальные средства реализации методов и способов, которые при их практическом применении снижают возможность ошибок человека. Для этого можно включить рассмотрение следующих вопросов:

- хорошее знание средств соответствующими участниками группы разработчиков;

- наличие успешного опыта использования средств в аналогичных применениях;

- правила и ограничения, направленные на ослабление влияния "небезопасных" особенностей средств;

- документально оформленный перечень всех средств (с указанием версии) и ПСБ;

- совместимость между различными инструментальными средствами и ПСБ;

- способность генерировать документацию для ППО.

Типичными примерами инструментальных средств, применяемых на различных стадиях жизненного цикла, являются:

- генераторы прикладных кодов;

- программы управления конфигурацией;

- программы статического анализа (например, программа проверки имени признака, программа проверки времени сканирования);

- симуляторы;

- испытательные средства, включающие программы проверки ПО;

- автоматизированное рабочее место проектировщика.

Могут быть рассмотрены другие методы, способы и средства, включающие измерения показателей (например, охвата тестами) и использование различных более углубленных средств верификации функции(й) (например, средства взаимной верификации).

Для того чтобы обнаружить и устранить ошибки, уже существующие в программах, рекомендуется проводить верификацию на всем жизненном цикле разработки. Типичные подходы к этой задаче описаны в 12.7.2.3.

Чтобы гарантировать, что оставшиеся в программах ошибки не приведут к неприемлемым результатам, необходимо рассмотреть:

- способы проверок и обработку особых ситуаций в ходе функционирования;

- использование внешних баз данных поставщика и общих отчетов о неисправностях;

- мониторинг отчетов об отказах ПСБ и результатах процесса, а также их влиянии на ПСБ;

- отображение ключевых функций ПСБ в других системах;

- использование дубликата ППО ПСБ в процессе обучения персонала.

Чтобы обеспечить возможность обслуживания ПО на всем жизненном цикле ПСБ, необходимо рассмотреть:

- программу управления изменениями (см. МЭК 61511-1, раздел 17);

- постоянную поддержку управления и обучение обслуживающего персонала;

- наличие средств поддержки и разработки на всем жизненном цикле ПСБ;

- наличие хорошо документально оформленных и, желательно, широко используемых методов помощи соответствующим возможностям и навыкам человека на протяжении всего жизненного цикла ПСБ;

- использование правил проведения разработки и документального оформления, направленных на облегчение понимания и ограничение влияния изменений в ПО;

- использование "встроенной" и обновляемой документации;

- способность к развитию и проверке в ходе функционирования.

12.1.2.5 Дополнительные требования не предусмотрены.

12.1.2.6 Дополнительные требования не предусмотрены.

12.1.2.7 Дополнительные требования не предусмотрены.

12.1.2.8 Дополнительные требования не предусмотрены.

12.2 Спецификация требований к безопасности ППО

12.2.1 Цель

12.2.1.1 Дополнительные требования не предусмотрены.

12.2.2 Требования

Общая структура ПСБ может налагать дополнительные функциональные требования на ПО конкретных функций безопасности ПСБ. Типичными примерами этого являются логика выбора "1 из 2" для резервных датчиков, а также установленные безопасные действия по обнаружению опасных отказов с помощью самодиагностики датчика. В примерах, приведенных в приложении В, перечислены такие требования, порожденные применяемой архитектурой.

ППО должно также учитывать диагностические операции, реализуемые ПЭС и разработанные для выполнения соответствующих действий, установленных в инструкции по безопасности логического устройства.

Подробные требования по безопасности, предъявляемые к каждой функции безопасности ПСБ, устанавливаются обычно с помощью логических диаграмм или причинно-следственных схем. Во многих случаях для определения требований могут быть использованы языки программирования, предлагаемые поставщиком логического устройства. Обычно используют языки функциональных блок-схем или язык матриц причин и следствий. Поставляемый выбранный язык должен подходить для конкретного применения. При определении подробных требований использование языков, предлагаемых поставщиком, часто может уберечь от ошибок, которые встречаются при переносе требований из других видов документации. Для того чтобы определить функции безопасности и функции, не связанные с безопасностью, а также требования к УПБ всех функций безопасности, следует широко использовать комментарии.

Все функции, необходимые для всех режимов работы защищаемого процесса, должна охватывать подробная спецификация требований к функциональной безопасности. Кроме того, следует обеспечить периодическое проведение проверок всех функций безопасности ПСБ. Обычно это требует определения дополнительных возможностей технического обслуживания, чтобы датчики и исполнительные элементы могли проверяться без останова процесса. Для документального оформления таких требований может быть использована методология, описанная в предыдущем подразделе.

Если для выполнения функций безопасности используется несколько ПСБ, то в

документации следует предусмотреть объяснение, какие функции выполняются каждой ПСБ. Если несколько ПСБ используются для реализации одной и той же функции безопасности, то в документации следует указать взаимодействие и независимость каждой ПСБ. Документация должна содержать сведения об ожидаемом УПБ, который должен быть обеспечен для каждой ПСБ.

Дополнительные указания см. в 10.2.1 и 10.3.1.

12.2.2.1 Дополнительные требования не предусмотрены.

12.2.2.2 До разработки ППО пользователь обеспечивает проведение оценки опасности и риска процесса, которое используется для установления требований к безопасности ПО в терминах функций безопасности ПСБ и их УПБ. После того как принято решение о программной реализации функции безопасности ПСБ, по любым привлекшим внимание конфликтам, разногласиям и упущениям в спецификации требований по безопасности следует обращаться к разработчикам ПО (например, по вопросу влияния порядка выполнения функции безопасности ПСБ в ПО). Другим примером может быть вопрос о реакции ППО на прекращение питания.

12.2.2.3 Требования к безопасности ППО должны разрабатываться как прослеживаемое соответствие спецификации требований к безопасности функции безопасности ПСБ. Необходимо обратиться к следующим факторам:

- функциональные и временные требования, необходимые для выполнения функции безопасности ПСБ, установленные пользователем;

- интерфейсы программной системы с процессом и персоналом;

- соотношение между опасностями процесса и функциями, выполняемыми ППО;

- ограничения на разрешенное поведение ППО, установленные так, чтобы процесс оставался в пределах безопасной области (например, неспособность работать при неверных входных значениях);

- допустимые функции сервисного ПО, выполняемые в логическом решающем устройстве (например, реализация приоритета логики безопасности и коммуникаций ввода/вывода, обработка ошибок и диагностика системы);

- платформа технических средств и системное ПО, на которых реализуется ППО, а также конфигурация технических средств и системного ПО;

- опасности, которые могут появляться в процессе в результате функционирования системы, частью которой является ПО (например, неподходящие виды отказов технических средств при отключении питания);

- ограничения на методы и процедуры, которыми могли бы пользоваться разработчики, вытекающие из инструкции по безопасности при обслуживании логического устройства.

Чтобы избежать трудностей на более поздних стадиях процесса разработки, важно также рассмотреть стратегию, с помощью которой можно показать, что требования к ППО выполнены.

Если в ПСБ используется ППО, то оценка функциональной безопасности может

включать:

- применение способов контроля, показывающих, что функции ППО соответствуют требованиям, вытекающим из опасностей процесса;

- функциональные испытания, показывающие, что ППО исполняет требуемые функции и, насколько это возможно, любые дополнительные функции ПО не приводят к опасным условиям;

- структурные испытания, показывающие, что ППО выполняет требуемые функции за необходимое время;

- анализ функциональных отказов и анализ по методу "что, если", позволяющие показать, что функции ППО не приводят к опасным условиям;

- аудит, показывающий, что процессы разработки и верификации проведены под контролем и что применена правильная версия ПО.

12.2.2.4 Дополнительные требования не предусмотрены.

12.2.2.5 Дополнительные требования не предусмотрены.

12.2.2.6 Дополнительные требования не предусмотрены.

12.3 Планирование подтверждения соответствия безопасности ППО

Дополнительные указания см. в 14.3.

12.3.1 Цель

12.3.2 Требования

12.3.2.1 Дополнительные требования не предусмотрены.

12.4 Проектирование и разработка ППО

12.4.1 Цели

12.4.1.1 Дополнительные требования не предусмотрены.

12.4.1.2 Дополнительные требования не предусмотрены.

12.4.1.3 Дополнительные требования не предусмотрены.

12.4.1.4 Дополнительные требования не предусмотрены.

12.4.1.5 Дополнительные требования не предусмотрены.

12.4.2 Общие требования

Существует ряд подходов к созданию безопасного ППО ПСБ. Однако независимо от того, какой подход используется для достижения безопасности ППО, принимается, что стадии жизненного цикла безопасности, предшествующие разработке прикладных программ

(например, оценка опасностей и рисков, разработка функционального описания, выбор технических и программных средств), выполнены правильно.

Если для выбранных устройств отсутствуют опыт применения, сопровождения или способность к выявлению неисправностей, то рекомендуется до осуществления приведенных далее подходов провести обучение и получить эксплуатационный опыт (предпочтительно - в безопасном применении). Чтобы повысить эффективность этих усилий, необходимо установить связь с другими пользователями таких же программируемых электронных (ПЭ) логических решающих устройств в той же самой среде. Степень уверенности в этом подходе является главным фактором в определении применения логического решающего устройства с ПЭ для приложения, использующего ПСБ.

Ниже приведен перечень указаний, подлежащих выполнению при разработке ППО ПСБ:

- разделить ППО на отдельные функции безопасности ПСБ со своим УПБ для каждой функции безопасности;

- разобраться в структуре технических средств каждой функции безопасности ПСБ и продублировать эти технические средства для каждого ППО функции безопасности ПСБ;

- не оптимизировать ППО, если это ведет к излишней сложности (это часто требует привлечения опытного программиста для интерпретации ППО);

- использовать методы разработки ППО, упомянутые в инструкциях поставщика (например, в руководстве по безопасности);

- не объединять прикладные программы одной функции безопасности ПСБ с прикладными программами любой другой функции безопасности ПСБ;

- использовать язык ППО (например, по типу или по функции), средства которого отработаны, понятны и способны к выявлению ошибок;

- обеспечить письменное описание ППО, согласованного с функциональным описанием, содержащимся в документации ППО;

- декомпозировать ППО на модули, согласованные с последовательностью процесса (например, первый модуль - это общее ПО, которое не связано с функцией безопасности ПСБ, но требуется в ПСБ; второй модуль - это первая функция безопасности ПСБ, относящаяся к запуску процесса; последний модуль - это последняя функция безопасности ПСБ, относящаяся к окончанию процесса);

- тщательно проверить (например, моделированием, просмотром или проверкой) каждый модуль ППО и провести повторный независимый анализ (привлекая на этом и на всех последующих стадиях подразделения по эксплуатации и обслуживанию); тщательно проверить комбинации модулей, образующие подсистемы процесса, и провести их повторный независимый анализ;

- тщательно испытать ППО ПСБ в целом;

- провести его повторный независимый анализ;

- использовать ППО для проведения проверки технических средств (например, для подтверждения правильности подсоединения входов/выходов к датчикам/исполнительным элементам);

- включить проверки ППО в прогоны процесса (например, выполнение процесса без загрузки опасных материалов);

- персонал сопровождения ППО должен быть доступен при любой передаче (например, при сдаче-приемке).

Документация ППО должна быть применима для определения пригодности этого ПО для УПБ каждой функции безопасности ПСБ. Для того чтобы установить соответствие ППО требованиям УПБ, следует провести независимый анализ.

Альтернативные подходы и дополнительные указания по этим вопросам приведены в МЭК 61508-3 и [9].

12.4.2.1 Дополнительные требования не предусмотрены.

12.4.2.2 Что касается указаний по выбору методов и средств разработки ППО, то системы с требованиями безопасности до УПБ 3 следует разрабатывать в соответствии с инструкциями, приведенными в руководстве по безопасности поставщика, как часть системы, соответствующей МЭК 61508. Для систем с УПБ 4 разработчик должен дополнительно подтвердить, что выбранные методы соответствуют требованиям МЭК 61508-3.

Что касается указаний по выбору методов и средств испытаний и верификации ППО, то системы с требованиями безопасности до УПБ 3 следует верифицировать в соответствии с указаниями, приведенными в 12.7. Для систем с УПБ 4 исполнитель верификации также должен подтвердить, что выбранные методы соответствуют требованиям МЭК 61508-3.

12.4.2.3 Дополнительные требования не предусмотрены.

12.4.2.4 Вообще говоря, для того чтобы обеспечить проверяемость, рекомендуется, чтобы спецификации испытаний интеграции ППО были рассмотрены еще в ходе стадий проектирования и разработки.

12.4.2.5 Если ППО ПСБ должно реализовывать функции безопасности ПСБ с различными УПБ, то их следует четко разделить и промаркировать. Это позволит сделать ПО каждой функции безопасности ПСБ прослеживаемым вплоть до каждого резервного датчика и каждого резервного исполнительного элемента. Это даст также возможность выполнять функциональное испытание и подтверждение соответствия функций в соответствии с УПБ. Маркировка должна идентифицировать функции безопасности ПСБ и УПБ.

Для функций безопасности ПСБ и функций, не связанных с безопасностью, следует использовать отдельные ПО. Одним из способов показать их адекватную независимость может быть выполнение всех следующих позиций:

a) функции безопасности ПСБ понятно промаркированы в ППО как прикладные коды функции безопасности ПСБ;

b) функции ПСБ, не связанные с безопасностью, явно отделены в ППО;

c) все переменные, используемые при выполнении функций безопасности ПСБ, промаркированы;

d) все коды прикладных программ, реализующих функции ПСБ, не связанные с безопасностью, промаркированы как коды функций, не относящихся к безопасности;

e) все коды прикладных программ, использующие переменные, не связанные с безопасностью, и переменные функции безопасности ПСБ удовлетворяют следующим условиям:

- коды прикладных программ (программы, функции и функциональные блоки), не связанные с безопасностью, не должны изменять переменные функции безопасности ПСБ, используемые в кодах прикладных программ безопасности;

- коды прикладных программ безопасности, реализующих функции безопасности ПСБ, не должны зависеть от любых переменных, не связанных с безопасностью;

f) все ППО (то есть коды и переменные) защищено от любых изменений ПО, не связанного с безопасностью;

g) если безопасное ППО и ППО, не связанное с безопасностью, совместно используют одни и те же ресурсы [например, центральное процессорное устройство (ЦПУ), ресурсы операционной системы, память, шины], то функция безопасности ПСБ (например, время реакции) безопасного ППО ни при каких обстоятельствах не должна оказаться под угрозой.

В идеальном случае взаимовлияние между кодами ППО (функций безопасности ПСБ и функций, не связанных с безопасностью) и всеми переменными (функций безопасности ПСБ и функций, не связанных с безопасностью) должно автоматически проверяться с помощью разрабатываемого ППО. Если эта возможность недоступна, то разработчики ППО и другие лица, выполняющие верификацию и подтверждение соответствия ППО, должны проверять все прикладные коды и связанные с ними переменные на соответствие приведенным выше правилам разделения.

12.4.2.6 Дополнительные требования не предусмотрены.

12.4.2.7 Дополнительные требования не предусмотрены.

12.4.3 Требования к архитектуре ППО

Варианты архитектуры ППО в типовых логических решающих устройствах ПСБ достаточно ограничены и вполне понятны при рассмотрении основных действий при разработке прикладных программ. Обычно разработчик при выполнении разработки и испытаний прикладных программ выполняет следующие основные действия:

a) выбор конфигурации модулей ввода/вывода и области памяти для переменных данных;

b) создание имен для всех входов/выходов и запоминаемых переменных. Наименования должны соответствовать соглашению непротиворечивости;

c) определение способа прекращения обслуживания. Некоторые пользователи будут требовать, чтобы для прекращения обслуживания к цифровым входам были подсоединены переключатели. Другие будут использовать управляемый ввод данных в

ПСБ из рабочей станции. В любом случае должно быть обеспечено безопасное управление, предотвращающее непреднамеренное прекращение обслуживания. О прекращении обслуживания должно быть объявлено;

d) определение способов диагностики датчиков и исполнительных элементов, а также организации периодических проверок. Они будут зависеть от резервирования датчиков и исполнительных элементов. Организация проверок должна быть тщательно определена и предусматривать соответствующую аварийную сигнализацию в ходе проведения проверки;

e) определение коммуникационных переменных для других систем, внешних к ПСБ. Если эти переменные размещаются в памяти, то они должны быть приписаны к соответствующим областям памяти так, чтобы коммуникационная подсистема могла иметь к ним доступ. Переменные, которые могут изменяться другими системами, внешними к ПСБ, должны быть аккуратно определены и, как правило, размещены в специальной области памяти, предназначенной для чтения и записи;

f) определение того, где и как регистрируются последовательности событий, и понимание их влияния на ПСБ;

g) разработка заказных функций и функциональных блоков. Такая возможность применения заказных функциональных компонентов весьма желательна, так как в прикладных программах могут быть запрограммированы, испытаны и повторно использованы повторяющиеся операции.

Примечание - Термины "функция", "функциональный блок" и "программа" определены в [12];

h) принятие решения о том, какие функции безопасности ПСБ и другие функции следует включить в данную программу. Желательно разделить функции безопасности и функции, не связанные с безопасностью, по разным программам так, чтобы основной акцент мог быть сделан на программах, критичных для безопасности. Желательно также ограничить размер одной программы небольшим числом функций;

i) составление прикладных программ. Структура прикладной программы должна соответствовать структуре процесса (например, на химическом объекте ППО для каждого участка процесса должно быть сгруппировано вместе; внутри каждого участка процесса следует обеспечить распределение ПО между оборудованием для облегчения понимания и обслуживания);

j) определение правильного порядка выполнения сетевых и логических операций внутри каждой программы, а также последовательности и требуемой скорости выполнения всех прикладных программ. Подтверждение того, что скорости выполнения прикладных программ согласованы с необходимыми временами реакции процесса, приведенными в спецификации требований к безопасности ПО;

k) проверка ППО с использованием контролирующих возможностей среды разработки (если возможно);

l) загрузка ППО в логическое устройство;

m) проверка всех входов и выходов логического устройства, ППО и интерфейсов с другими системами, внешними для ПСБ.

12.4.3.1 Дополнительные требования не предусмотрены.

12.4.3.2 Дополнительные требования не предусмотрены.

12.4.3.3 Дополнительные требования не предусмотрены.

12.4.3.4 Дополнительные требования не предусмотрены.

12.4.3.5 Примерами верификации полноты безопасности данных могут служить:

- проверка выхода входных/выходных данных за границы заданных диапазонов;

- подтверждение соответствия передаваемых прикладных данных;

- проверки согласованности наименований индексов (например, проверки многократного использования одного и того же имени индекса);

- проверки правильности прекращения обслуживания (например, при обслуживании и запуске);

- проверка правильности настроек и сигнализации.

12.4.4 Требования к средствам поддержки, руководству пользователя и прикладным языкам

Среда разработки представляет собой совокупность инструментальных средств, которые поддерживают процессы кодирования ППО, конфигурирования прикладных параметров и интерфейсов, а также проверки и контроля выполнения прикладных программ. Обычно такая среда включает в себя следующие средства:

a) редактор конфигурации. Этот редактор используется, чтобы сконфигурировать подсистему входов/выходов, входные/выходные переменные памяти и функции коммуникации;

b) языковые редакторы. Эти редакторы использует прикладной программист при разработке программ, выполняющих все необходимые в данной системе функции (связанные или несвязанные с безопасностью);

c) библиотеки сертифицированных функций и функциональных блоков. Такие функции и функциональные блоки могут быть использованы в прикладных программах;

e) средства разработки заказных функций и функциональных блоков. Некоторые поставщики предоставляют такую среду разработки, которая позволяет пользователю разрабатывать заказные функции и функциональные блоки, поддерживаемые прикладными языками. Такие функции и функциональные блоки должны быть тщательно проверены до применения прикладной программы;

e) средства планирования работы прикладных программ. Такие средства планирования поддерживают настройку порядка и скорости выполнения требуемых программ;

f) средства загрузки. Они позволяют разработчику загружать в логические устройства для исполнения ППО, библиотеки функциональных блоков, данные переменных и другую информацию о конфигурации;

g) средства эмуляции. Некоторые поставщики предоставляют среду разработки, способную эмулировать все прикладные программы на компьютере, поддерживающем эту среду. Это позволяет проводить проверки прикладных программ вне процесса их применения до того, как они будут загружены в логическое устройство;

h) средства мониторинга программ. Средства мониторинга позволяют пользователю просматривать данные, получаемые исполняемой программой, или на экране пользователя, или через реальный функциональный блок, или на экране программы многоступенчатых диаграмм. Среда разработки может также предоставлять возможность наблюдения за исполнением программы-эмулятора. Кроме того, могут контролироваться программы, исполняемые логическим устройством;

i) дисплеи диагностики логического устройства. Такие дисплеи показывают состояние модулей основного процессора, коммуникационных модулей и модулей ввода/вывода системы. Обычно для каждого модуля на экран выводятся состояния "переход", "неисправность" или "работа", и часто доступна более детальная информация о неисправностях в системе.

12.4.4.1 Дополнительные требования не предусмотрены.

12.4.4.2 Дополнительные требования не предусмотрены.

12.4.4.3 Дополнительные требования не предусмотрены.

12.4.4.4 Предпочтительны трансляторы прикладного языка, прошедшие проверку в использовании и/или сертифицированные на соответствие промышленным стандартам.

12.4.4.5 Дополнительные требования не предусмотрены.

12.4.4.6 Дополнительные требования не предусмотрены.

12.4.4.7 Пример руководства по безопасности

Компоненты и устройства, используемые в ПСБ, реализуемых в соответствии с настоящим стандартом, должны быть обеспечены документацией, которая содержит все известные аспекты установки, обслуживания, конфигурирования, программирования и эксплуатации, подлежащие рассмотрению, если компоненты или устройства должны отвечать спецификации требований к безопасности для данного применения.

Настоящий стандарт часто называют "руководство по безопасности" для компонента или устройства. Однако он может входить в состав стандартной инструкции по установке, инструкции по техническому обслуживанию и инструкции пользователя, предоставляемых поставщиком вместе с дополнительным документом, определяющим их использование в применениях с ПСБ, ограничения для этих применений, действия, которые следует предпринять при получении диагностических аварийных сигналов, и информацию, связанную с известными режимами отказов. Следует также определить те характеристики, конфигурации и/или типы программных операторов, которые не следует применять в тех случаях, когда компонент или устройство используется в ПСБ.

Программирование на ЯОИ допускает использование глобальных данных, поэтому руководство по безопасности должно содержать указания для программиста о том, как использовать средства программирования для тщательного анализа и проверки правильности применения переменных данных. Необходимо также рассмотреть

распределение памяти, выполнение проверки индексов состояния и проверки правильности входных величин.

Как часть руководства по безопасности либо как отдельный документ для конкретного применения могут также предоставляться инструкции и примеры, позволяющие группе программистов создавать программы похожего формата и стиля. Такие инструкции должны содержать сведения о тех деталях конкретных алгоритмов или функций, которые не должны использоваться в программах, если эти алгоритмы или функции могут вызвать нежелательное поведение, способное повлиять на безопасность.

Программиста следует предупредить, что он не должен принимать никаких допущений, кроме установленных в руководстве по безопасности (например, не использовать средства компиляции, отсутствующие в таком руководстве). В идеальном случае компилятор должен быть сконфигурирован таким образом, чтобы эти ограничения выполнялись автоматически.

Приведенный в таблице 1 пример построения и содержания руководства предназначен для типового логического устройства, соответствующего МЭК 61511.

Таблица 1 - Состав и содержание типичного руководства по безопасности

Разделы	Основное содержание
Введение	Общие сведения, требования к оборудованию, структура руководства, соглашения, документы, связанные с руководством, версия документа, терминология, обзор изделия
Установка	Среда в планируемом месте размещения, подключение к процессу, процедуры запуска, процедуры останова, модификации применения, реализация функций в уже действующей системе
Построение конфигурации и применения	Рассмотрение проекта*, возможности и функционирование, программа обучения
Текущее функционирование	Функционирование изделия, обзор эксплуатации, инструкции по эксплуатации
Обслуживание	Предупреждающее обслуживание, индикаторы оборудования, сообщения об ошибках, системная и прикладная сигнализация, обнаружение неисправностей и ремонт, выполняемый пользователем
Приложения	Системные сообщения, лист проверок, прикладные решения
Индексы	Индексы сообщений по безопасности
* Рассмотрение проекта охватывает все аспекты конфигурации и прикладного программирования, которые связаны с безопасностью конфигурации, и программируемой электроники логического решающего устройства. Оно должно включать следующие вопросы (но не ограничиваться ими): - времена обработки данных логическим устройством, интенсивность обновления входов/выходов, интенсивность передачи данных, последовательность действий логического устройства; - требования к управлению системной сигнализацией; - ограничения на конфигурацию и программирование.	

В примере приведены все самостоятельные разделы документа с указанием основных заголовков к содержанию каждого раздела.

12.4.4.8 Дополнительные требования не предусмотрены.

12.4.5 Требования к разработке ППО

Перед проведением разработки ППО необходимо проверить следующие требования:

- логическое устройство ПСБ и связанные с ним модули ввода/вывода должны соответствовать МЭК 61511-1;

- все ограничения и эксплуатационные процедуры, необходимые для соответствия МЭК 61511-1, должны быть предусмотрены в документации пользователя или в документах, выпущенных поставщиком логического устройства; обычно эти документы называют "руководство по безопасности";

- датчики и исполнительные элементы, используемые программируемой электроникой, должны соответствовать МЭК 61511-1;

- если выполняются периодические проверки на действующем процессе, то может быть обеспечена возможность прервать обслуживание, чтобы провести проверки датчиков и исполнительных элементов.

Обычно ППО пишется на языках программирования, предоставляемых поставщиком логического устройства или поставщиками интеллектуальных внешних устройств. ППО может быть написано на ЯПИ, например на языке машинных команд или языке С, на языке ЯОИ, например на языке функциональных блок-схем или языке многоступенчатых диаграмм, или на ФЯП, когда пользователь только вводит данные, необходимые для выполнения фиксированной программы.

Если ППО написано на ЯПИ, разработчику следует соблюдать требования и указания МЭК 61508-3. Если ППО написано на ЯОИ или ФЯП, то разработчик может следовать требованиям и указаниям МЭК 61511-1. При этом разработчик должен соблюдать ограничения и процедуры, установленные поставщиком логического устройства в руководстве по безопасности. При необходимости должны разрабатываться и использоваться также указания по программированию и правила кодирования/конфигурирования.

12.4.5.1 Дополнительные требования не предусмотрены.

12.4.5.2 Дополнительные требования не предусмотрены.

12.4.5.3 Например, глобальной переменной в прикладной программе можно описать сигнал нарушения безопасности, такой, как аварийный сигнал о превышении температуры, который изменяется в зависимости от дозирования группы составляющих в процессе.

Например, глобальной константой в прикладной программе можно описать верхнюю границу, при достижении которой запускается аварийный сигнал о воспламенении газа, которую используют в системах зажигания и газовой защиты и которая равна, например, 20% нижнего предела взрывоопасности.

12.4.5.4 Дополнительные требования не предусмотрены.

12.4.5.5 Дополнительные требования не предусмотрены.

12.4.5.6 Дополнительные требования не предусмотрены.

12.4.6 Требования к проверкам модулей ППО

Проверки ППО на соответствие требованиям, полученным на стадиях проектирования и составления спецификаций, могут сначала проводиться на симуляторе, а затем - на логическом решающем устройстве. Цели проверок на начальных этапах (симулирование и тестирование на соответствие требованиям проектных спецификаций):

- показать, что программные модули выполняют необходимые функции и не способны к выполнению любых запрещенных действий;

- проверить ПО для широкого набора условий и последовательностей их выполнения, чтобы показать, что оно остается устойчивым в нештатных состояниях.

Цель последующих проверок (комплексные и заводские приемочные испытания) - показать, что ППО отвечает предъявленным к нему требованиям на конкретных технических средствах и не нарушает установленных временных соотношений.

Заключительный этап проверок - это демонстрация того, что интегрированная система работает правильно в предполагаемой среде, с предполагаемыми физическими устройствами и интерфейсами и с разработанными эксплуатационными процедурами и может быть полностью реализована только в процессе установки и приемки всей системы.

После начала формальных проверок все изменения функций ПО и данных о конфигурации должны быть осуществлены в строгом соответствии с установленной процедурой проведения модификаций.

12.4.6.1 Дополнительные требования не предусмотрены.

12.4.6.2 Дополнительные требования не предусмотрены.

12.4.6.3 Дополнительные требования не предусмотрены.

12.4.7 Требования к комплексным испытаниям ППО

12.4.7.1 Дополнительные требования не предусмотрены.

12.4.7.2 Дополнительные требования не предусмотрены.

12.4.7.3 Дополнительные требования не предусмотрены.

12.5 Интеграция ППО с подсистемой ПСБ

12.5.1 Цель

12.5.1.1 Дополнительные требования не предусмотрены.

12.5.2 Требования

12.5.2.1 Испытания интеграции могут быть проведены на любой стадии подтверждения соответствия ПСБ.

12.5.2.2 Дополнительные требования не предусмотрены.

12.5.2.3 Дополнительные требования не предусмотрены.

12.6 Процедуры модификации ПО на ФЯП и ЯОИ

12.6.1 Цель

12.6.1.1 Дополнительные требования не предусмотрены.

12.6.2 Требования к модификации

Всегда, когда это возможно, следует избегать внесения изменений в ПСБ на действующем процессе. Если такие изменения все-таки требуются, то вся процедура должна быть оформлена документально и выполнена в соответствии с планом безопасности.

Для внесения любых изменений в программируемые ПСБ рекомендуется следующая процедура:

a) планирование и ресурсы. Процесс внесения изменений в программируемую ПСБ должен быть управляемым, планируемым и обеспеченным ресурсами на уровне, достаточном для безопасной реализации изменений;

b) анализ влияний. Необходимая модификация может потребовать проведения полной оценки опасности и риска, включая все возможные влияния неизменяемых частей системы (анализ влияний на безопасность);

c) разработка. Разработка модификации должна быть проведена по всему жизненному циклу, представленному в МЭК 61511-1;

d) верификация. Перед установкой изменения должна быть выполнена полная верификация технических средств и ПО вне процесса. Если граница для изменяемого ПО ясно очерчена и контролируема, то до сдачи-приемки требуется провести верификацию только очерченной части ППО;

e) установка и ввод в действие. Установка и ввод в действие изменения должны следовать процедурам, установленным для ПСБ в МЭК 61511-1;

f) подтверждение соответствия приемочных испытаний. Подтверждение соответствия системы (тестирование причин и следствий) должно быть выполнено для ее модифицированных частей до их включения в действие в составе действующей системы;

g) персонал. К выполнению модификаций следует допускать только определенный персонал, обладающий на основе его подготовки и проверки компетентностью в вопросах выполнения изменений;

h) модификации в автономном режиме. При осуществлении модификаций ППО в автономном режиме следует провести верификацию корректности используемых версий ППО, включая рабочие параметры.

12.6.2.1 Дополнительные требования не предусмотрены.

12.7 Верификация ППО

12.7.1 Цели

12.7.1.1 Дополнительные требования не предусмотрены.

12.7.1.2 Дополнительные требования не предусмотрены.

12.7.2 Требования

Спецификация требований к безопасности ППО будет включать:

- требования к функциям безопасности ПСБ (например, значения УПБ для функций безопасности ПСБ, логика, описанная диаграммами потоков или причинно-следственными диаграммами);

- временные ограничения (например, минимальные времена реакции выхода на входной сигнал);

- архитектурные ограничения (например, требования резервирования, коммуникационные интерфейсы и функциональные разделения).

Соответствие установленным требованиям обеспечивается проведением верификации на каждой стадии разработки ППО.

Верификация данных включает подтверждение того, что данные, используемые ППО, правильны и, где необходимо, уникальны (например, что имена индексам присвоены уникально, что данные не используются последующими функциями ошибочно и что константы, устанавливающие значение для аварийной сигнализации, актуальны и правильны).

Верификация защиты от несанкционированного изменения могла бы включать в себя проверку того, что соответствующие механизмы (например, защита паролем с уровнями доступа) предусмотрены и используются адекватно.

12.7.2.1 Дополнительные требования не предусмотрены.

12.7.2.2 Дополнительные требования не предусмотрены.

12.7.2.3 На каждой отдельной стадии разработки ППО (включая проведение проверок) верификация подтверждает, что эта стадия успешно выполнена. В общем случае верификацию проводит специальная группа, которая может состоять из одного или более человек.

Для снижения числа ошибок путем заранее принятых разумных ориентиров верификация должна включать:

- при УПБ 1 - экспертную оценку, выполненную другим участником группы разработчиков ППО;

- при УПБ 2 - экспертную оценку, выполненную лицом, не являющимся участником разработки;

- при УПБ 3 - экспертную оценку, выполненную лицом, представляющим независимое подразделение.

Если инструментальные средства разработки ПО включают некоторые автоматические операции верификации [например, проверку на повторное использование тэгов (имен переменных)], то группе верификации следует подтвердить, что такие средства используются должным образом и получаемые результаты правильны.

При любом УПБ рекомендуется, чтобы объем проверок охватывал все функции безопасности ПСБ ППО и реакцию ПСБ на все виды отказов (например, отказ питания, отказ процессора, отказ входного или выходного устройства и отказ коммуникаций). Однако для дальнейшего снижения количества любых ошибок, оставшихся в ПО, рекомендуется при более высоких УПБ проводить следующие дополнительные испытания:

- при УПБ 2 и УПБ 3 - испытания, базирующиеся на особенностях внутренней структуры (например, внутренние алгоритмы, внутренние состояния);

- при УПБ 3 - форсированные испытания (например, при значениях входных и/или внутренних переменных вне рабочих диапазонов, при неверных комбинациях входных сигналов, при неправильных последовательностях и нагрузках).

При любых УПБ рекомендуется, чтобы документация для выполнения верификации и тестирования была достаточна для того, чтобы показать, что верификация и тестирование были выполнены и были успешными. Однако при более высоких УПБ также рекомендуется:

- при УПБ 2 и УПБ 3 - чтобы документация была достаточна для проведения оценки адекватности верификации и тестирования;

- при УПБ 3 - чтобы документация была достаточна для того, чтобы независимый специалист мог повторить испытания и оценить их достаточность.

12.7.2.4 Дополнительные требования не предусмотрены.

13 Заводские приемочные испытания

13.1 Цель

13.1.1 Дополнительные требования не предусмотрены.

13.2 Рекомендации

13.2.1 Хотя проведение заводских приемочных испытаний (ЗПИ) не является требованием, они рекомендуются для логических устройств, которые выполняют функции безопасности ПСБ и имеют довольно сложную логику или структуру с резервированием (например, "1 из 2", "2 из 3" и т.д.).

13.2.2 Наиболее важная часть ЗПИ должна представлять собой хорошо определенную, хорошо прописанную и хорошо структурированную процедуру испытаний, которая устанавливает, как проверять прикладную логику и что контролировать после каждого шага.

Персонал, которому предстоит эксплуатировать процесс, следует привлекать к участию в ЗПИ, начиная с момента, когда ему дадут некоторую начальную подготовку для

эксплуатации ПСБ. Часто персонал также может сделать хорошие предложения и добавления к процедуре испытаний, которые не были видны при разработке.

13.2.3 Дополнительные требования не предусмотрены.

13.2.4 Дополнительные требования не предусмотрены.

13.2.5 В ходе ЗПИ следует проверить интерфейсы (например, коммуникации между ОСУП и ПСБ).

13.2.6 Дополнительные требования не предусмотрены.

13.2.7 Дополнительные требования не предусмотрены.

14 Установка и ввод в действие ПСБ

14.1 Цель

14.1.1 Дополнительные требования не предусмотрены.

14.2 Требования

14.2.1 Дополнительные требования не предусмотрены.

14.2.2 Установку ПСБ следует выполнять в соответствии с проектом и планом проведения установки. Любые отклонения от проекта необходимо подвергать должному критическому рассмотрению с участием проектировщиков, чтобы гарантировать, что все требования проекта выполнены. После того как ПСБ должным образом установлена, должна быть полностью выполнена процедура ввода в действие и затем необходимо начать действия по подтверждению соответствия.

14.2.3 Хотя МЭК 61511-1 рассматривает ввод в действие как отдельную стадию, признается, что объект, опыт проектировщиков и требования проекта могут потребовать проведения ввода в действие за несколько стадий.

14.2.4 Дополнительные требования не предусмотрены.

14.2.5 Дополнительные требования не предусмотрены.

15 Подтверждение соответствия безопасности ПСБ

15.1 Цель

15.1.1 Цель подтверждения соответствия безопасности ПСБ - подтвердить соответствие ПСБ требованиям, установленным в спецификации требований к безопасности. Действия по подтверждению соответствия следует выполнять до введения ПСБ в эксплуатацию.

15.2 Требования

15.2.1 Дополнительные требования не предусмотрены.

15.2.2 Дополнительные требования не предусмотрены.

15.2.3 Дополнительные требования не предусмотрены.

15.2.4 Если ПСБ уже прошла ЗПИ, то это может быть учтено в ходе подтверждения соответствия. Группа, выполняющая подтверждение соответствия, должна критически рассмотреть результаты ЗПИ, чтобы убедиться, что все ППО прошло испытания успешно и все проблемы, выявленные в ходе ЗПИ, решены.

Повторение испытаний ППО при окончательном подтверждении соответствия может не требоваться. Это положение применимо в следующих случаях:

- когда такой подход предусмотрен заранее и включен в план подтверждения соответствия;

- если ППО верифицировано на соответствие требованиям безопасности в ходе ЗПИ и

- применяемая версия ППО верифицирована на идентичность версии, прошедшей ЗПИ.

Однако очень важно убедиться в том, что какие-либо повреждения, вызванные транспортированием, хранением или настройкой, отсутствуют, что все датчики и исполнительные элементы подсоединены к логическому устройству правильно, что функции безопасности ПСБ выполняются должным образом и что интерфейс оператора обеспечивает его необходимой информацией. Настоятельно рекомендуется, чтобы подтверждение соответствия ПСБ включало в себя общие контрольные испытания системы, так как раздельные испытания логического устройства и внешних элементов неэквивалентны полной сквозной проверке системы.

15.2.5 Дополнительные требования не предусмотрены.

15.2.6 Дополнительные требования не предусмотрены.

15.2.7 Дополнительные требования не предусмотрены.

15.2.8 Дополнительные требования не предусмотрены.

16 Эксплуатация и обслуживание ПСБ

16.1 Цель

16.1.1 Дополнительные требования не предусмотрены.

16.2 Требования

16.2.1 Дополнительные требования не предусмотрены.

16.2.2 Дополнительные требования не предусмотрены.

16.2.3 Дополнительные требования не предусмотрены.

16.2.4 Дополнительные требования не предусмотрены.

16.2.5 Дополнительные требования не предусмотрены.

16.2.6 Дополнительные требования не предусмотрены.

16.2.7 Дополнительные требования не предусмотрены.

16.2.8 Дополнительные требования не предусмотрены.

16.3 Проверочные испытания и осмотр

16.3.1 Проверочные испытания

16.3.1.1 Интервал между проведением проверочных испытаний следует выбирать из условия достижения средней вероятности отказа при наличии запроса, установленной спецификацией требований к безопасности.

16.3.1.2 Дополнительные требования не предусмотрены.

16.3.1.3 Частота проведения контрольных испытаний должна быть согласована с применимыми рекомендациями изготовителей и хорошей инженерной практикой и быть более высокой, если необходимость этого установлена предшествующим опытом эксплуатации.

Существует ряд стратегий, используемых для выбора интервала между контрольными испытаниями функции безопасности ПСБ.

Например, некоторые пользователи предпочитают устанавливать интервал между контрольными испытаниями как можно более длительным, чтобы минимизировать затраты на техническое обслуживание и возможные последствия испытаний. В этих случаях разработчик ПСБ может предусмотреть повышенное резервирование оборудования, увеличение охвата диагностикой и более устойчивые к различным нарушениям (робастные) компоненты. После завершения проектирования для этого проекта могут быть проведены расчеты, определяющие максимально допустимый интервал между проверками, позволяющий достигнуть эксплуатационного УПБ, установленного для функции безопасности ПСБ. Недостатком такого метода разработки является то, что на предприятии у каждой системы будут различные межпроверочные интервалы, что может потребовать более строгого согласования. Он также может ухудшить показатели качества работы (например, $ВОНЗ^{ср} = 10^{-1}$ для систем с УПБ 1 и $ВОНЗ^{ср} = 10^{-2}$ для систем с УПБ 2).

Другие пользователи могут пожелать стандартизировать основные значения определяемых интервалов между испытаниями и проводить испытания всех систем, установленных на производственном объекте, через один и тот же интервал. Например, они могут пожелать испытывать каждую функцию безопасности ПСБ ежегодно, так как они ежегодно проектируют новую ПСБ. Предварительно выбирая интервал между контрольными испытаниями до начала проектирования, компании-пользователи могут затем предварительно выбрать архитектуру, компоненты и охват диагностикой, которые будут удовлетворять УПБ для большинства случаев применения. Установив эти характеристики в своих корпоративных стандартах, они могут снизить затраты на разработку для большинства применений. В этом случае следует провести расчеты для ПСБ, позволяющие убедиться, что при заранее выбранном интервале между контрольными испытаниями достигнут требуемый УПБ.

При выборе интервала между контрольными испытаниями следует рассмотреть интенсивность запросов (для систем, работающих в режиме по запросам), интенсивности

отказов для каждого из проверяемых компонентов и общие требования к качеству функционирования системы.

Примечание - В тех случаях применения, когда проверка срабатывания исполнительных элементов практически нецелесообразна, следует прописать процедуру, включающую:

- проведение проверок исполнительных элементов при останове объекта;

- проверки ПСБ на срабатывание выходных устройств, насколько это практически возможно (например, срабатывание выходного реле, соленоида останова или частичное перемещение клапана) в ходе испытаний на действующем объекте;

- учет любых ограничений во время испытаний исполнительных элементов при вычислении ВОНЗ^{ср} для функции безопасности ПСБ.

16.3.1.4 Дополнительные требования не предусмотрены.

16.3.1.5 Дополнительные требования не предусмотрены.

16.3.1.6 Дополнительные требования не предусмотрены.

16.3.2 Осмотр

Как указано в МЭК 61511-1, осмотр ПСБ отличается от контрольных испытаний. В то время как контрольные испытания обеспечивают правильную работу ПСБ, визуальный осмотр требуется для того, чтобы проверить механическую целостность установки.

Обычно осмотр проводят в то же время, что и контрольные испытания, но при желании их можно делать и чаще.

16.3.3 Важно, чтобы результаты контрольных испытаний и осмотра были оформлены документально для фиксации обнаруженных фактов. Какие-либо конкретные требования к тому, как долго эти результаты должны сохраняться, отсутствуют, но обычно длительность хранения должна быть достаточной для проведения переоценки предшествующих результатов, хранящихся в истории отказов компонентов.

Например, если при контрольных испытаниях было обнаружено, что датчик неисправен, то хорошей практикой считается сделать обзор результатов предшествующих испытаний, чтобы увидеть, были ли у этого датчика обнаружены неисправности в ходе проведения ряда аналогичных проверочных испытаний. Если история показывает наличие повторяющихся отказов, следует рассмотреть вопрос о перепроектировании ПСБ с использованием датчика другого типа.

17 Модификация ПСБ

17.1 Цель

17.1.1 Дополнительные требования не предусмотрены.

17.2 Требования

17.2.1 Дополнительные требования не предусмотрены.

17.2.2 Дополнительные требования не предусмотрены.

17.2.3 Дополнительные требования не предусмотрены.

17.2.4 Дополнительные требования не предусмотрены.

17.2.5 Дополнительные требования не предусмотрены.

17.2.6 Дополнительные требования не предусмотрены.

18 Снятие с эксплуатации ПСБ

18.1 Цель

18.1.1 Дополнительные требования не предусмотрены.

18.2 Требования

18.2.1 Дополнительные требования не предусмотрены.

18.2.2 Дополнительные требования не предусмотрены.

18.2.3 Дополнительные требования не предусмотрены.

18.2.4 Дополнительные требования не предусмотрены.

18.2.5 Дополнительные требования не предусмотрены.

19 Требования к информации и документации

19.1 Цели

19.1.1 Дополнительные требования не предусмотрены.

19.2 Требования

19.2.1 Перечень сведений и документов, которые могут быть использованы при реализации ПСБ, включает в себя:

a) результаты оценки опасностей и риска;

b) допущения, используемые при определении УПБ;

c) спецификации требований к безопасности;

d) логику применения;

e) проектную документацию;

a) информацию и/или документацию по изменениям;

g) записи результатов верификации и подтверждения соответствия;

h) процедуры сдачи-приемки и подтверждения соответствия ПСБ;

i) эксплуатационные процедуры ПСБ;

j) процедуры обслуживания ПСБ;

k) процедуры контрольных испытаний;

l) результаты проведения оценок и аудитов.

19.2.2 Дополнительные требования не предусмотрены.

19.2.3 Дополнительные требования не предусмотрены.

19.2.4 Дополнительные требования не предусмотрены.

19.2.5 Дополнительные требования не предусмотрены.

19.2.6 Дополнительные требования не предусмотрены.

19.2.7 Дополнительные требования не предусмотрены.

19.2.8 Дополнительные требования не предусмотрены.

19.2.9 Дополнительные требования не предусмотрены.

Приложение А

(справочное)

Примеры методов расчета вероятности отказа при наличии запроса для функции безопасности ПСБ

А.1 Общие сведения

Настоящее приложение посвящено ряду технических методов, применяемых для проведения расчетов вероятностей отказов ПСБ, разработанной и установленной в соответствии с МЭК 61511-1. Эти сведения по своей природе носят информационный характер, и их не следует интерпретировать как единственные методы оценки, которые могут быть использованы.

Применяемая методология основана на [9] (приложение В), [13]-[15] и [10].

А.2 Метод расчета по блок-схеме надежности

[13] и [9] (приложение В) иллюстрируют метод выполнения расчетов вероятностей отказов функций безопасности ПСБ по блок-схеме надежности, разработанный в соответствии с МЭК 61511-1 и настоящим стандартом.

А.3 Метод расчета по упрощенным уравнениям

В [10] представлен метод расчета по упрощенным уравнениям вероятности отказов функций безопасности ПСБ, разработанных в соответствии с МЭК 61511-1 и настоящим стандартом.

A.4 Метод анализа дерева неисправностей

В [14] и [10] показан метод проведения анализа дерева неисправностей для расчетов вероятностей отказов функций безопасности ПСБ, разработанных в соответствии с МЭК 61511-1 и настоящим стандартом.

A.5 Метод расчетов по моделям Маркова

В [15] и [10] иллюстрируется метод применения марковских моделей для расчетов вероятностей отказов функций безопасности ПСБ, разработанных в соответствии с МЭК 61511-1 и настоящим стандартом.

Приложение B

(справочное)

Разработка архитектуры типовой ПСБ

B.1 Основы

B.1.1 Введение

Приведенный ниже материал представляет собой пример, иллюстрирующий различные шаги, выполняемые в ходе разработки архитектуры ПСБ, отвечающей требованиям МЭК 61511-1. При разработке ПСБ применяют руководящие указания и практический опыт, а также стандартное оборудование, указанное ниже.

B.1.2 Руководящие указания и практика

В прошлом применения, связанные с безопасностью, называли "критичные приборные системы". Для них были составлены правила проведения разработок, типовые примеры и материалы лучшей практики, а также процедуры проверочных испытаний.

Существуют руководящие указания по определению требуемых функций безопасности ПСБ и их УПБ с помощью метода анализа уровней защиты [АУЗ - см. [5] (приложение F)], а также по проведению разработки и по резервированию приборов.

B.1.3 Приборное оснащение

При выборе приборного оснащения в случаях, связанных с безопасностью (ПСБ), для расчетов вероятности отказа при наличии запроса (ВОНЗ) используют информацию поставщика об охвате диагностикой и доле безопасных отказов (ДБО), а также информацию о качестве функционирования изделий, собранную на объектах.

B.1.4 Логическое решающее устройство

Технические средства, системное ПО и система проектирования логического устройства соответствуют УПБ 3 по МЭК 61508, и для разработки прикладных программ используется ЯОИ.

Руководство по безопасности системы содержит подробные указания по применению системы и разработке ППО.

Определяемые пользователем стандартные функции безопасности (например, выявление неисправности датчика, выбор варианта резервирования, такого как "1 из 2" или "2 из 3", безопасная перегрузка выхода) существуют в виде стандартных (шаблонов) прикладных программ, разрабатываемых пользователем.

B.2 Рабочий процесс

B.2.1 Введение

Все действия по разработке выполняются в соответствии с ранее установленным общим проектом рабочего процесса. Разработка ПСБ выполняется по своему собственному процессу, отдельные этапы которого встроены в общий процесс проектирования. Оценка функциональной безопасности проводится на соответствующих стадиях.

B.2.2 Типовые стадии жизненного цикла ПСБ

Разработка ПСБ требует выполнения типовых стадий, приведенных в таблице B.1. В дальнейшем будут обсуждаться только стадии 3, 4 и те части стадии 5, которые связаны с выбором архитектуры системы.

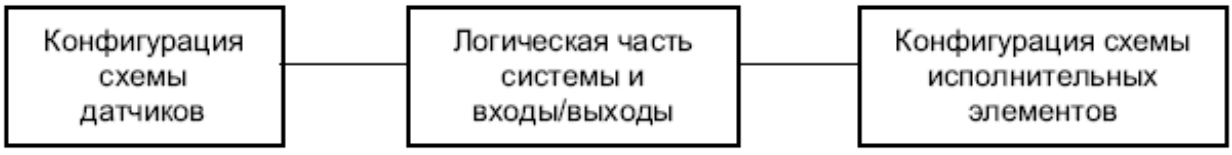
Таблица B.1 - Типовые стадии разработки ПСБ

Стадия	Наименование	Действие
1	Область применения	Определение оборудования процесса
2	Требования к функциональной безопасности оборудования процесса	Определение возможных опасностей, проведение анализа слоев защиты
3	Оценка требований к безопасности системы	Проектирование структуры ПСБ
4	Оценка требований к безопасности компонентов ПСБ	Определение технических средств ПСБ
5	Разработка ППО	Проектирование ПО ПСБ
6	Испытания и подтверждение соответствия ППО	Проведение испытаний ПСБ
7	Установка	Проведение установки на объекте
8	Ввод в действие	Окончательная приемка
9	Эксплуатация	Обеспечение выполнения процесса

B.2.3 Оценка требований безопасности

Доступная информация о результатах АУЗ: спецификация требований к безопасности и значения УПБ для ПСБ (например, УПБ для каждой ПФБ).

Модель, используемая для достижения УПБ:



Определение ВОНЗ: общая ВОНЗ (см. выше) остается в пределах, соответствующих УПБ.

Сокращенный метод: стандартные конфигурации схем приборного оснащения, включая схемы с резервированием (например, "1 из 2"), возможные диагностики и интервалы проверок могут быть представлены в таблицах, связанных с требованиями по УПБ. Такие таблицы должны быть основаны на реальных опытных данных и реальных проектах для различных процессов применений в пределах возможностей средств. Комбинируя альтернативные конфигурации системы с известными данными элементов блок-схем, можно провести выбор наиболее подходящего варианта.

Спецификация компонентов ПСБ: все компоненты системы имеют подтвержденные характеристики (например, ВОНЗ, ДБО, устойчивость к отказам, требования к систематическим отказам при определенном УПБ), установленные в МЭК 61511-1:

- датчики и исполнительные элементы выбраны согласно требованиям процесса, а их различные свойства проверены подразделением разработчиков на соответствие опыту эксплуатации;

- логические системы: входы и выходы определены согласно требованиям к датчикам и исполнительным элементам. Логическое устройство, язык прикладного программирования, инструментальные средства разработки и коммуникационный интерфейс являются частями утвержденной системы безопасности. Интерфейс оператора формируется в соответствии с требованиями конкретного применения.

B.2.4 Оценка требований к безопасности для компонентов ПСБ

На этой стадии все функции, предусмотренные в спецификации требований к безопасности, распределяются по компонентам системы, функциональным или программным. Требования к полноте безопасности будут определять соответствующие компоненты ПСБ и ее возможную архитектуру.

B.2.5 Требования к ППО, связанные с архитектурой

После выбора архитектуры ПСБ могут быть определены ППО, способные реализовать резервирование (например, "1 из 2"), и/или диагностические операции, требуемые для датчиков, логического устройства и исполнительных элементов.

B.2.6 Разработка ППО

Языком программирования является язык функциональных блок-схем (язык с ограниченной изменчивостью). Кодирование и испытание являются хорошо известными процессами. Кроме того, существуют некоторые ограничения на программирование функций безопасности, детально описанные в руководстве пользователя.

B.3 Пример 1

B.3.1 Введение

Приведенный ниже пример не основан на реальном сценарии и не рассматривает отказы по общей причине и на других слоях защиты. Пример составлен специально для того, чтобы продемонстрировать, как применяется ранее описанный процесс разработки ПСБ.

B.3.2 Сценарий опасности

Произошел отказ управления температурой на выходе реактора, нагреваемого паром, и

клапан управления паром открылся полностью.

B.3.3 Спецификация требований к безопасности и УПБ

Спецификация требований к безопасности: если давление в реакторе превзойдет 10 бар, следует за 20 секунд закрыть подачу пара в рубашку реактора, чтобы избежать экзотермической реакции. Действия оператора при этом не требуются. Необходимый уровень полноты безопасности - УПБ 3.

B.3.4 Архитектура системы

Компоненты системы: конфигурация датчика давления, конфигурация логического устройства, конфигурация исполнительного элемента. Проверенные практикой интеллектуальные датчики подсоединены непосредственно к входам логической системы. Клапан аварийного блока имеет встроенный соленоидный клапан и прямо подсоединен к выходу логической системы. Все данные о средних наработках на отказ (MTTF) получены из реального опыта эксплуатации.

Приборное оснащение:

датчики давления выполнены в соответствии с пунктом 11.4.4 МЭК 61511-1:

- среднее время наработки на отказ $T_{ср} = 10^5$ ч;

- охват диагностикой (ОД)=70%;

- доля безопасных отказов (ДБО)=90%;

- межпроверочный интервал - 1 год;

- среднее время восстановления $T_в = 8$ ч;

- клапан аварийного блока выполнен в соответствии с пунктом 11.4.4 МЭК 61511-1:

$T_{ср} = 8x10^4$ ч, ОД=0%, ДБО=80%, межпроверочный интервал - 6 мес, $T_в = 8$ ч.

Значения $ВОНЗ_{ср}$ для одинарных элементов:

- датчик: $2,2x10^{-3}$ (см. А.1) - неприемлемо;

- логическое устройство (резервное): $1,3x10^{-4}$, включая интерфейсы входа и выхода (из сертификата);

- клапан: $2,41x10^{-3}$ (см. А.1) - неприемлемо.

Выбор приемлемой архитектуры подсистемы датчиков: выбрана схема с резервированием "1 из 2".

Доля отказов по общей причине =10% (см. А.1).

ОД=90% (см. А.1).

Для схемы датчиков "1 из 2" новое значение ВОНЗ^{ср} =2,3x10^{-4} .

Проверка по таблице 6 и пункту 11.4.4 МЭК61511-1: реальное допустимое число отказов = $^{1\rightarrow}$ требованиям УПБ 3 соответствует.

Выбор приемлемой архитектуры подсистемы исполнительных устройств: выбрана схема с резервированием "1 из 2".

Доля отказов по общей причине =10% (см. А.1).

Для схемы исполнительных устройств "1 из 2" новое значение ВОНЗ^{ср} =4,65x10^{-4} .

Проверка по таблице 6 и пункту 11.4.4 МЭК 61511-1: реальное допустимое число отказов = $^{1\rightarrow}$ соответствует УПБ 3.

Проверка ВОНЗ^{ср} : датчик + логическое устройство + исполнительный элемент:

(2,3+1,3+4,7)x10^{-4} =8,3x10^{-4} .

В.3.5 Дополнительные структурные решения, связанные с безопасностью ПО

ПО подсистемы датчиков: в принятой выше схеме "1 из 2" применяется программа выбора сигнала датчика (существующий функциональный блок), которая закрывает клапан пара, если:

- один из двух датчиков выдает сигнал о наличии условия, превышающего установленное значение;

- средства диагностики обнаруживают опасный отказ.

ПО подсистемы исполнительных элементов: оба выхода на клапан пара обесточиваются по команде программы безопасности.

В.4 Пример 2

В.4.1 Введение

Аналогичный пример для более низкого значения УПБ.

В.4.2 Сценарий опасности

Произошел отказ управления температурой на выходе реактора, нагреваемого паром, и клапан управления паром открылся полностью.

В.4.3 Спецификация требований к безопасности и УПБ

Спецификация требований к безопасности: если давление в реакторе периодического действия превысит 10 бар, следует за 20 с закрыть подачу реагента "А" в реактор, чтобы избежать экзотермической реакции. Действия оператора при этом не требуются. Необходимый уровень полноты безопасности - УПБ 2.

В.4.4 Архитектура системы

Компоненты системы: конфигурация датчика давления, конфигурация логического устройства, конфигурация исполнительного элемента. Проверенные практикой интеллектуальные датчики подсоединены непосредственно к входам логической системы. Клапан аварийного блока имеет встроенный соленоидный клапан и прямо подсоединен к выходу логической системы. Все данные о средних наработках на отказ (MTTF) получены из реального опыта эксплуатации.

Приборное оснащение:

- датчики давления выполнены в соответствии с пунктом 11.4.4 МЭК 61511-1: $T_{ср} = 10^5$ ч, ОД=70%, ДБО=90 %, межпроверочный интервал - 1 год, $T_в = 8$ ч;

- клапан аварийного блока выполнен в соответствии с пунктом 11.4.4 МЭК 61511-1: $T_{ср} = 2{,}5x10^4$ ч, ОД=0%, ДБО=60%, межпроверочный интервал - каждая неделя (168 ч), $T_в = 8$ ч.

Значения ВОНЗ^{ср} для одинарных элементов:

- датчик: $2{,}2x10^{-3}$ (см. А.1) - приемлемо;

- логическое устройство (резервное): $1{,}3x10^{-4}$, включая интерфейсы входа и выхода (из сертификата);

- клапан: см. ниже (см. формулу в А.1).

Значение ВОНЗ^{ср} для одинарного датчика:

ВОНЗ^{ср} датчика при структуре "1 из 1" = $2{,}2x10^{-3}$.

Проверка по МЭК 61511-1 (таблица 6 и пункт 11.4.4): реальное допустимое число отказов = $0 \rightarrow$ соответствует УПБ 2.

Значение ВОНЗ^{ср} одинарного исполнительного элемента (см. формулу в А.1):

ВОНЗ$^{ср} = \lambda_D \times t_{CE}$, $\lambda_D = 1/(25000x2)$, $t_{CE} = 168/2+8$.

ВОНЗ^{ср} исполнительного элемента при структуре "1 из 1": $1{,}84x10^{-3}$.

Проверка по МЭК61511-1 (таблица 6 и пункт 11.4.4): реальное допустимое число отказов = $0 \rightarrow$ соответствует УПБ 2.

Проверка ВОНЗ^{ср} : датчик + логическое устройство + исполнительный элемент: $(2{,}2+0{,}1+1{,}8)x10^{-3} = 4{,}1x10^{-3}$.

В.4.5 Дополнительные структурные решения, связанные с безопасностью ПО

ПО подсистемы исполнительных элементов: выход на клапан пара обесточивается по команде программы безопасности.

Кроме того, предусматривается программа контроля, которая выполняется периодически (обычно каждые 8 ч), проверяет и фиксирует, что клапан все время находится в безопасном состоянии. Если при проверке будет обнаружен отказ или после последней проверки пройдет более 168 ч, выход логического устройства переводится в безопасное состояние (клапан аварийного блока закрыт) и ситуация сигнализируется. Наличие такой автоматической проверки позволяет при расчетах $ВОНЗ^{ср}$ принимать, что интервал между контрольными испытаниями составляет 168 ч.

Приложение С

(справочное)

Особенности применения программируемого логического контроллера безопасности

Настоящее приложение посвящено ряду ключевых вопросов, которые должен рассмотреть специалист, использующий в ПСБ небольшой (например, имеющий до 150 входов/выходов) программируемый логический контроллер (ПЛК) безопасности. Цель настоящего приложения - помочь специалисту провести начальное планирование разработки.

ПЛК безопасности представляет собой логическое решающее устройство ПСБ, сертифицированное на соответствие требованиям серии стандартов МЭК 61508. Для применения на конкретном объекте ко входам/выходам логического устройства ПСБ подсоединены датчики и исполнительные элементы, а также реализованы прикладные программы. Все средства, реализующие функции безопасности, связанные с отказами логического устройства ПСБ (например, проверки в режиме "он-лайн", управление во времени), встроены в систему. Необходимые проверки датчиков и исполнительных элементов реализованы в ППО; для некоторых функций предусмотрены проверенные функциональные блоки.

Считается, что для всех устройств известны данные о полноте безопасности (например, значения ВОНЗ, принятые пределы УПБ и т.д.). Данные о полноте безопасности логического устройства приведены в соответствующем руководстве.

С.1 Система

Логическим решающим устройством (рисунок С.1) ПСБ является ПЛК, разработанный специально для применения в случаях, связанных с безопасностью, и относящийся к типу, проверенному на выполнение требований серии стандартов МЭК 61508 до УПБ 3. ПЛК имеет входные и выходные интерфейсы для сигналов процесса, связанных с безопасностью, и коммуникаций с другими ПЛК безопасности. Он имеет также интерфейсы для сигналов и коммуникаций, не связанных с безопасностью. Система включает следующие компоненты:

- центральное процессорное устройство (ЦПУ) специального исполнения для функциональной безопасности технических средств, специальную операционную систему и встроенные функции управления отказами (для прикладного программирования и интеграции ПО, общее резервирование которого обеспечивается системой проведения разработок; программист работает только с одним ЦПУ);

- систему проектирования на языке с ограниченной изменчивостью (например, язык

функциональных блок-схем);

- библиотеку проверенных функциональных блоков;

- специальные средства конфигурации для выбора параметров функций безопасности ПСБ;

- средства подтверждения того, что загруженное выполняемое ППО идентично исходному ППО;

- руководство по безопасности.

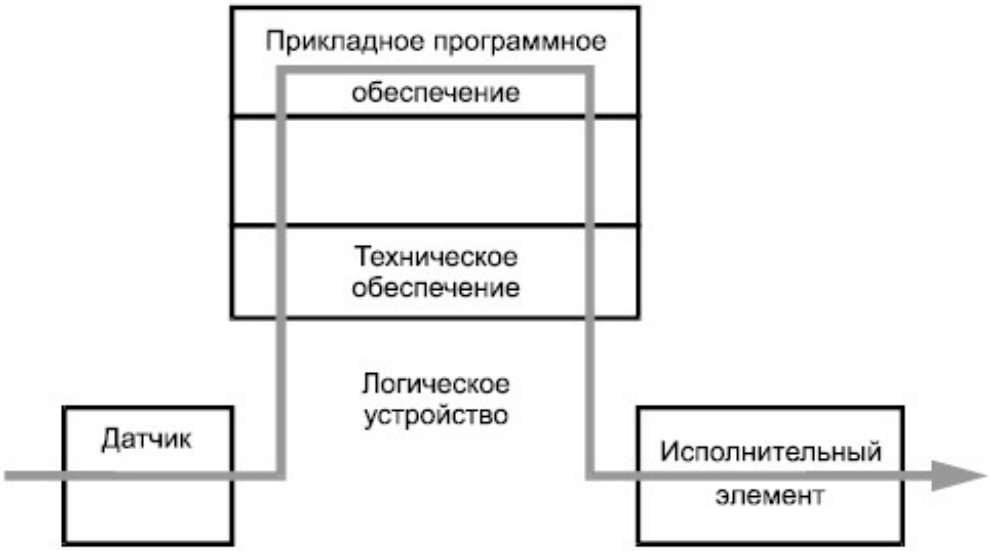


Рисунок С.1 - Логическое решающее устройство

С.2 Процесс работы

a) Спецификация требований к безопасности будет соответствовать настоящему стандарту, если рассмотрены следующие ключевые аспекты:

1) спецификации требований ко всем функциям безопасности ПСБ;

2) диапазоны аналоговых входов;

3) определение диагностических операций, выполняемых в режиме "он-лайн" для датчиков и исполнительных элементов;

4) описание реакции системы на обнаружение отказов разных видов;

5) определение параметров функций безопасности ПСБ (например, максимальная длительность цикла, максимально допустимое время существования несоответствия между сравниваемыми входами);

6) ограничения, приводимые в руководстве по безопасности;

b) спецификация требований к безопасности ППО должна быть получена в соответствии с перечислением a).

Требования к безопасности, относящиеся к техническим средствам ПЛК, описываются в

руководстве по безопасности. Ограничения затрагивают главным образом такие позиции, как предельные значения рабочих характеристик, размер памяти, время реакции.

Ограничения на архитектуру ПО или кодирование описываются в руководстве по безопасности. Они связаны с системой разработки ПЛК. Большинство ограничений заданы неявно языком с ограниченной изменчивостью;

c) разработка архитектуры ППО: проект архитектуры ППО должен точно соответствовать функциям безопасности ПСБ и видам действий, установленным для данного процесса;

d) разработка ППО: разработка ППО облегчается использованием существующих функциональных блоков;

e) интеграция: интеграция включает загрузку данных конфигурации (например, таблиц входов/выходов) и ППО, а также настройку всех параметров, значения которых отличаются от применяемых по умолчанию;

f) верификация: ППО подлежит верификации до или после интеграции системы. Верификация поддерживается средой разработки.

Приложение D

(справочное)

Пример методологии разработки ППО логического решающего устройства ПСБ

Настоящий пример иллюстрирует, как конкретный системный разработчик логического решателя ПСБ создает ППО для своих заказчиков. Создание этого ПО обычно выполняется как часть процесса интеграции всей системы, обсуждаемого далее.

Так как акцент делается на методологию разработки ППО безопасности, важно рассмотреть средства разработки ППО, языки программирования и стандарты кодирования, используемые при создании прикладных программ. Цель такого рассмотрения - показать набор типовых свойств инструментальных средств разработки программ, языков программирования и соответствующих языковых трансляторов, предоставленных в логике ПСБ.

Логическая часть ПСБ имеет средства разработки ППО, которые поддерживают ряд языков, установленных в [12], где определены языки программирования общего назначения для ПЛК. Так как [12] не связан с задачами безопасности, были приняты следующие решения:

- использовать языки с ограниченной изменчивостью, обычно применяемые для промышленных процессов;

- исключить использование языковых конструкций, не подходящих для применений, связанных с безопасностью;

- для дальнейшего ограничения языковых конструкций, применяемых на критичных объектах, использовать стандарт кодирования;

- встроить средства безопасного доступа и защиты файлов;

- поддерживать сертифицированные по [12] библиотеки функций, функциональных блоков и связанных с функциями процессов (например, обработка аналоговых данных, данных от датчиков пламени и загазованности);

- обеспечивать проведение третьей стороной сертификации средств разработки ППО, библиотек и трансляторов языков.

Эти решения рассмотрены подробнее в D.2, посвященном ППО разработки логического решателя ПСБ.

Пример стандарта кодирования, применяемого программистами логической части ПСБ, обсуждается в D.3. В D.4 приведены дополнительные требования, которые следует рассмотреть для средств разработки ПО.

D.1 Обзор процесса интеграции всей системы

Основные работы по интеграции ПСБ включают в себя:

a) интеграцию технического обеспечения.

Она состоит из монтажа частей логического решателя ПСБ в шкафах, имеющих соответствующие терминальные монтажные панели для подключения сигналов процесса к входным/выходным модулям логического решателя. Обычно сюда же включаются монтаж источников электропитания и подача электропитания на логический решатель и на внешние устройства;

b) определение логики применения.

Работы по интеграции логического решателя ПСБ могут также включать в себя подробное определение логики путем ее проработки с инженерами заказчика. Логика применения для каждой функции безопасности ПСБ определяется с учетом резервирования датчиков и исполнительных элементов. Интерфейс, используемый для проверки и обслуживания ПСБ на действующем процессе, определяется также с учетом эксплуатационных требований покупателя. Могут быть включены также дополнительные требования к логике, не связанной с безопасностью, но она должна быть строго отделена и спроектирована по тем же стандартам, что и функция безопасности;

c) реализацию ППО и конфигурирование технических средств.

Чтобы сконфигурировать технические средства входов/выходов логического решателя, а также коммуникационное оборудование ПСБ, используется сертифицированный на безопасность пакет разработки ППО для логического решателя ПСБ. Также реализуется и проверяется ППО каждой функции безопасности ПСБ и некритичное для безопасности ППО;

d) заводские приемочные испытания.

Многие покупатели проводят ЗПИ, чтобы проверить работу технических средств и ППО перед их отправкой на объект. При этом технические средства и ППО тщательно проверяют инженеры и другой персонал покупателя, занимающийся эксплуатацией;

e) установку ПСБ у покупателя.

Поставщик обеспечивает или проведение установки, или наблюдение за установкой на площадке объекта;

f) приемочные испытания на объекте.

Интерфейс каждого датчика и исполнительного элемента с логическими решателями ПСБ проверяют на функционирование и калибруют. Такие позиции, как ППО в целом и функции байпаса при обслуживании, проверяют повторно;

g) модификацию ППО и технических средств.

После проведения начальной установки и начала функционирования изменения в ППО и в техническом обеспечении проводятся строго по принятым на предприятии процедурам изменений.

D.2 ППО разработки логического решателя ПСБ

Как упомянуто ранее, в логическом решателе ПСБ использован пакет разработки ППО, основанный на языках [12]. Эти программные средства поддерживают следующие три языка: язык структурированных текстов, язык многоступенчатых диаграмм и язык функциональных блоков. Для каждого языка необходимы отдельные стандарты кодирования. Язык команд, аналогичный ассемблеру, не был включен, так как он не подходит для прикладных программистов. Это согласуется с таблицей С.1 [16].

На выбор языка в [12], что согласуется с требованиями, приведенными в 7.4.4 и таблице А.3 МЭК 61508-3 и в С.4 [16], наложен ряд дополнительных ограничений, включая следующие:

a) в [12] определены 20 типов данных (BOOL, SINT, INT, DINT, LINT, USINT, UINT, UDINT, ULINT, REAL, LREAL, TIME, DATE, TOD, DT, STRING, BYTE, WORD, DWORD, LWORD). Следует отметить, что существует восемь отдельных типов целочисленных данных. Чтобы поддерживать все эти типы данных, требуется поддержка большого количества функций преобразования и сокращения. Для применений, связанных с безопасностью, многие из приведенных типов данных не требуются. Поэтому число поддерживаемых типов данных было сокращено до 11. Для конкретного языка выбраны следующие типы поддерживаемых данных: BOOL, INT, DINT, DWORD, REAL, LREAL, STRING, TIME, DATE, TOD и DT. Это решение согласуется с рекомендациями МЭК 61508 по ограничению подмножества языков (см. МЭК 61508-3, таблица 3);

b) использование графических элементов управления исполнением (например, безусловные и условные переходы, безусловные и условные возвраты), принятых в МЭК 61508-3, не поддерживается, так как они могут приводить к появлению циклов и непреднамеренному обходу элементов, которые следовало бы выполнить (см. С.4.6 [16]);

c) не поддерживается ряд операторов языка структурированных текстов, так как они могут приводить к появлению циклов (например, FOR…END_FOR, WHILE…END_WHILE и REPEAT…END_REPEAT);

d) было наложено ограничение на то, чтобы язык не допускал доступ по записи к одной и той же глобальной переменной нескольких программ. Считывать значения глобальной переменной могут несколько программ, но для предотвращения конфликтов записывать значения этой переменной может только одна программа. Кроме того, если при

программировании ППО будет случайно запрограммирована запись значений глобальной переменной несколькими программами, то выдается соответствующее предупреждение;

e) программирование должно однозначно определять порядок выполнения всех элементов программы. Все языки имеют алгоритм, который устанавливает порядок выполнения и реализует его на каждом выполняемом элементе;

f) программирование должно обеспечить разделение программ, критичных и некритичных к безопасности. ПО предоставляет программисту возможность определить, какие программы связаны с безопасностью, а какие - нет. Программист также имеет возможность определять переменные, связанные и не связанные с безопасностью. При этом программы, не связанные с безопасностью, не могут иметь доступ по записи к переменным безопасности;

g) было признано, что использование переменных типа VAR_IN_OUT у многих прикладных пользователей приводит к серьезным затруднениям. Поэтому использование переменных типа VAR_IN_OUT нуждается в тщательном документальном оформлении либо язык программирования не должен их поддерживать.

D.3 Стандарты кодирования для прикладного программиста

Для того чтобы обеспечить разработку ППО безопасности, для разработчиков прикладных программ должны быть установлены стандарты кодирования. Ниже приведен ряд указаний для программистов, разрабатывающих прикладные программы и использующих для этого конкретное ПО разработки:

a) разработчику прикладных программ следует для реализации функций безопасности ПСБ использовать языки с ограниченной изменчивостью (язык функциональных блок-схем или язык многоступенчатых диаграмм). Даже эти языки должны быть ограничены (см. D.2 о подмножестве языков);

b) язык структурированных текстов является языком с полной изменчивостью, и его использование, если возможно, следует ограничить реализацией на нем функций и функциональных блоков. Такое ограничение было принято для того, чтобы эксплуатирующий персонал, не обладая профессиональными навыками в программировании, понимал программы безопасности;

c) размер программ следует ограничить до разумных пределов. Функции безопасности ПСБ, предназначенные для различных частей процесса, должны выполняться разными программами. В идеале одна программа должна охватывать только небольшое число функций безопасности ПСБ одной части процесса;

d) следует избегать смешивания имен. Например, если средства программирования поддерживают массивы, то программы, использующие массивы, должны проверять индексы массивов, чтобы убедиться, что они соответствуют допустимому диапазону;

e) если на объекте требуется применение логики, как критичной, так и некритичной для безопасности, то логику, некритичную для безопасности, следует реализовывать в отдельных программах и использовать правила разделения, встроенные в программу.

D.4 Другие требования к конфигурированию/программированию и функционированию систем безопасности

ПО для прикладного программирования имеет ряд особенностей, позволяющих пользователю получить доступ к информации логического решателя ПСБ. Однако необходимо, чтобы при этом была обеспечена безопасность разрабатываемого ПО и чтобы пользователь имел возможность проверять правильность выполнения программ. Некоторые из таких особенностей перечислены ниже:

a) средства программирования обеспечивают создание системы безопасного доступа, ограничивающей всех пользователей только теми функциями, которые соответствуют их роли (например, менеджер корпорации, руководитель объекта, руководитель проекта, инженер-проектировщик, старший программист, программист, оператор). Каждый пользователь регистрируется в системе со своим именем и паролем и после этого может работать на своем функциональном уровне. Система безопасного доступа предусматривает также отдельный уровень пользователя, занятого программированием безопасности, и отличный от него уровень для программирования, не связанного с безопасностью, так как компания пользователя может выразить желание дать возможность внесения изменений в программы безопасности на объекте только нескольким лицам;

b) предусматриваются защищенные или закрытые функции и библиотеки, которые недоступны программисту, либо он не может вносить в них изменения. Тем самым обеспечивается то, что библиотеки, прошедшие сертификацию или строгую проверку, не могут быть изменены без утверждения формального запроса на модификацию. Система безопасного доступа позволяет пользователю установить то должностное лицо верхнего уровня, которое имеет доступ или может изменять такие библиотеки (обычно это руководитель корпорации или объекта);

c) средства программирования также обеспечивают поддержку версий всех элементов разрабатываемого проекта. Любое изменение конфигурации системы, функции, функционального блока или программы приводит к изменению номера версии этого элемента. Это дает возможность пользователю быстро узнать, актуальна ли его документация на текущую дату, позволяет ему сосредоточиться на испытании только тех позиций, которые были изменены. Предусмотрены функции сравнения версий, с помощью которых пользователи могут выявить все изменения, включая непреднамеренные. Такие функции сравнения могут охватывать любые изменения в общей базе данных имен индексов и в списке исполняемых программ;

d) ПО обеспечивает защиту файлов путем вычислений и сравнений результатов циклического контроля с помощью избыточных кодов всех потоков данных, хранящихся в сложной файловой структуре данного проекта;

e) логический решатель ПСБ обеспечивает доступ к диагностической информации, благодаря чему программист может предпринять соответствующие действия, основанные на сведениях о реальном состоянии логического решателя;

f) логический решатель ПСБ предоставляет такие средства, которые в случае необходимости позволяют программисту проверять правильность выполнения арифметических операций;

g) средства программирования обеспечивают возможность эмулировать выполнение всех программ, разработанных на рабочей станции программиста. Это позволяет программисту проверить все разработанные программы в автономном режиме до того, как они будут загружены в логический решатель ПСБ. Такая проверка должна быть

обязательной в тех случаях, когда изменения проводятся в программе, выполняемой в режиме "он-лайн" на действующей системе;

h) ПО поддерживает динамический обмен данными, который может быть использован для связи с программами моделирования. Это дает возможность проводить дополнительные проверки прикладных программ в автономном режиме до их загрузки в контроллер безопасности.

D.5 Допущения

В данном подразделе рассмотрены допущения, связанные с аппаратными средствами и ПО, используемыми при разработке ППО. Обсуждаются также соответствующие процедуры и документация.

1) Логическое устройство ПСБ и связанные с ним модули ввода/вывода прошли оценку третьей стороны и признаны соответствующими серии стандартов МЭК 61508. Область сертификации по МЭК 61508, признанная третьей стороной, охватывает использование компонентов для функций безопасности ПСБ с УПБ 3.

2) Программирование ведется на языках с ограниченной изменчивостью, соответствующих [12], включая языки функциональных блок-схем, многоступенчатых диаграмм и структурированных текстов. Все функции и функциональные блоки, предоставляемые прикладными библиотеками, имеют атрибут, который определяет, может ли этот компонент использоваться в функциях безопасности или только для случаев, не связанных с безопасностью. При реализации функций безопасности ПСБ в прикладных программах, определяемых с атрибутом безопасности, могут быть использованы только функции и функциональные блоки, имеющие атрибут безопасности. Прикладные программы, обозначенные атрибутом "не связаны с безопасностью", могут использовать функции и функциональные блоки, имеющие атрибуты "не связаны с безопасностью" и "связаны с безопасностью".

3) Все языки программирования, поддерживаемые в [12], а также библиотеки функций и функциональных блоков с атрибутом безопасности должны быть сертифицированы на соответствие серии стандартов МЭК 61508.

4) Все ограничения сертифицирующей организации и рабочие процедуры предусмотрены в документации пользователя.

5) При периодических проверках всех элементов ПСБ необходимо игнорировать методологию обслуживания, что позволяет проводить проверки в режиме "он-лайн" без остановки управляемого процесса.

6) Все действия по интеграции системы выполняются с использованием серии стандартов ИСО 9000 или эквивалентных им процедур.

Приложение Е

(справочное)

Пример разработки внешне конфигурируемых диагностик для безопасно конфигурируемого программируемого электронного логического устройства

Программируемые электронные (ПЭ) логические устройства, проверенные на практике, должны обладать заложенными в них при проектировании значительными диагностическими возможностями. Диагностические операции могут быть реализованы как программными, так и аппаратными средствами и охватывать логическое устройство целиком, включая входные модули, центральный процессор, выходные модули и коммуникации [17].

Ниже приведен план, который может быть использован при реализации диагностирования конфигурируемых ПЭ логических устройств безопасности.

Е.1 Диагностирование ПЭ логического устройства внутренними средствами

Внутри ПЭ логических устройств, применяемых для промышленных процессов, имеются средства диагностики. В данном приложении они называются внутренними контрольными таймерами (ВКТ). В состав таких ВКТ входят поставляемые изготовителем программные, аппаратные, а также коммуникационные диагностические подсистемы, встроенные в ПЭ логическое устройство.

В ПЭ логических устройствах, применяемых для выполнения функции безопасности ПСБ, следует обеспечивать диагностику всех их элементов. Комплекс ВКТ может предоставлять выбираемые пользователем опции от отключения отдельной платы ввода или вывода до общей остановки системы. Диагностика, выполняемая ВКТ, проверяет те позиции логического устройства, которые изготовитель считает наиболее важными. Ограничения для применения ВКТ могут включать в себя следующие случаи:

- возможность отказа общего типа, при котором ВКТ выходит из строя по той же причине, что и логическое устройство, что приводит к неспособности ВКТ выполнять свои диагностические функции;

- реализация не может обеспечить пользователя диагностической информацией, связанной с типом сбоя логического устройства;

- невозможность контролировать внутренние состояния ПЭ логического устройства, включая устройства ввода/вывода, центральный процессор и коммуникации;

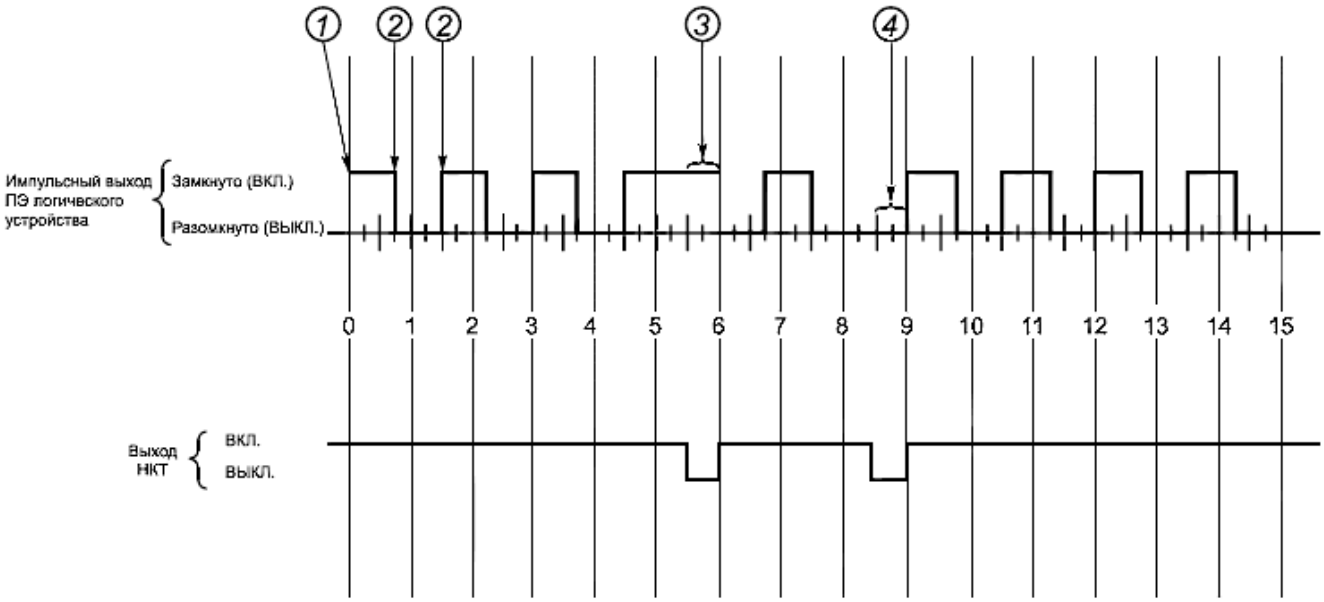
- невозможность контролировать модули ППО и их выполнение.

Е.2 Диагностирование ПЭ логического устройства внешними средствами

В ПЭ логических устройствах, выполняющих функции безопасности ПСБ, из-за ограничений, присущих ВКТ, может потребоваться применение наружных контрольных таймеров (НКТ). Использование НКТ ни в коей мере не снижает необходимости применения ВКТ для функции безопасности ПСБ.

Примерами часто используемых НКТ являются устройства контроля сигнала синхронизации логического устройства. Такой НКТ представляет собой устройство, непрерывно получающее импульсные сигналы в процессе выполнения ППО ПЭ логического устройства, и обычно работает следующим образом. В электронном логическом устройстве программно с помощью нескольких групп команд (раздельно хранящихся в специальных ячейках памяти) генерируется прямоугольный импульсный сигнал с заданным периодом. Этот прямоугольный сигнал подается на вход НКТ. На рисунке Е.1 представлена временная диаграмма, на которой показаны импульсный

выходной сигнал ПЭ логического устройства и выходной сигнал НКТ.



1 - включение синхронизирующего сигнала логического устройства; *2* - выключение и повторное включение синхронизирующего сигнала выполнены до окончания заданного в НКТ интервала времени (принята настройка 1 с), что обеспечивает высокий уровень сигнала на выходе НКТ. Высокий уровень сигнала на выходе НКТ остается до тех пор, пока управляющий импульсный сигнал меняет свое значение по крайней мере один раз в течение заданного интервала времени; *3* - если управляющий синхронизирующий сигнал остается включенным дольше предварительно заданного времени, то на выходе НКТ появляется низкий уровень сигнала (НКТ выключается); *4* - если управляющий синхронизирующий сигнал остается выключенным дольше предварительно заданного времени, то на выходе НКТ появляется низкий уровень сигнала (НКТ выключается)

Рисунок Е.1 - Временная диаграмма выхода НКТ

Если указанный прямоугольный импульсный сигнал, который управляет ПЭ логическим устройством, включается и отключается в заданной временной последовательности, то он обеспечивает высокий уровень сигнала на выходе (включение) НКТ. Встроенные в НКТ таймеры обычно реализуют функции временной задержки включения и временной задержки отключения. Настройки таймеров включения и отключения выбираются такими, чтобы ни одна задержка не выходила за пределы заданных временных параметров импульсного сигнала. Если это условие работы НКТ нарушается, то на выходе НКТ появляется низкий уровень сигнала (НКТ выключается) и функция безопасности ПСБ может быть отключена и/или дан аварийный сигнал. Длительность импульсов в этом импульсном сигнале может варьироваться путем изменений в соответствующей прикладной программе генератора колебаний.

Если в проекте применяется НКТ, то необходимо рассмотреть следующие его дополнительные особенности:

- для генерации синхронизирующего сигнала в ПЭ логическом устройстве используется тот же набор команд, что и в ППО функции безопасности ПСБ;

- цифровые входы ПЭ логического устройства могут использоваться для контроля состояния его входных шин при выявлении нештатного функционирования;

- размещение программ НКТ по различным областям памяти ПЭ логического устройства улучшает контроль функционирования памяти;

- передача сгенерированного синхронизирующего сигнала через систему коммуникации ПЭ логического устройства позволяет улучшить диагностику этой системы;

- возможная необходимость кнопок перезапуска. Такая кнопка требуется, если НКТ блокируется при пуске или останове. При разработке цепи перезапуска следует использовать как ВКТ, так и НКТ;

- возможная необходимость кнопок проверки. Такая кнопка может быть желательной при верификации функций НКТ;

- цифровые выходы ПЭ логического устройства могут использоваться для контроля состояния его выходных шин при выявлении нештатного функционирования;

- средства подавления скачков от контактов любых электромеханических реле для ослабления индуктивных наводок на электронику. Анализ использования дополнительной шины питания, удовлетворяющей требованиям:

- защиты от превышения напряжения;

- подавления электрических шумов;

- защиты от молнии;

- наличия аварийной сигнализации, разработанной специально для выявления срабатывания как ВКТ, так и НКТ.

Приложение ДА

(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 61508-2:2000	IDT	ГОСТ Р МЭК 61508-2-2007 "Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам"
МЭК 61508-3:1998	IDT	ГОСТ Р МЭК 61508-3-2007 "Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению"
МЭК 61508-4:1998	IDT	ГОСТ Р МЭК 61508-4-2007 "Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения"
МЭК 61511-1:2003	IDT	ГОСТ Р МЭК 61511-1-2011 "Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования"
Примечание - В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT - идентичные стандарты.		

Библиография

[1]	ISO 10418:2003	Petroleum and natural gas industries - Offshore production installations - Analysis, design, installation and testing of basic surface process safety systems
[2]	API RP 14C Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms/Edition: 7th . American Petroleum Institute/01-Mar-2001/	
[3]	IEC 60300-3-9:1995	Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems
[4]	ИСО 17776:2000	Petroleum and natural gas industries - Offshore production installations - Guidelines on tools and techniques for hazard identification and risk assessment
[5]	IEC 61511-3:2003	Functional safety - Safety instrumented systems for process industry sector - Part 3: Guidelines for the determination of the required safety integrity levels
[6]	CCPS/AIChE Guidelines for Improved Human Performance in Process Safety, New York: American Institute of Chemical Engineers (1994)	
[7]	CCPS/AIChE Guidelines for Chemical Process Quantitative Risk Analysis (second edition), New York: American Institute of Chemical Engineers (2000)	
[8]	HSE Reducing error and influencing behaviour, HSG48, Health and Safety Executive, London (1999), ISBN 0 7176 2452 8	
[9]	IEC 61508-6:2000	Functional safety of electrical/electronic/programmable electronic safety related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
[10]	ISA-TR84.00.02: Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques	
[11]	Smith, D. J., 2001, Reliability, Maintainability and Risk, 6th Edition, ISBN 0-7506-5168-7	
[12]	IEC 61131-3:1993	Programmable controllers - Part 3: Programming language
[13]	IEC 61078:2006	Analysis techniques for dependability - Reliability block diagram and boolean methods
[14]	IEC 61025:2006	Fault tree analysis (FTA)
[15]	IEC 61165:2006	Application of Markov techniques
[16]	IEC 61508-7:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures
[17]	CCPS, "Guidance for Safe Automation of Chemical Processes", AIChe, 345 East 47th Street, New York, New York 10017, ISBN 0-8169-0554-1, 1993	
