ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61511-2— 2018

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 2

Руководство по применению МЭК 61511-1

(IEC 61511-2:2016, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 11 сентября 2018 г. № 586-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61511-2:2016 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1» (IEC 61511-2:2016 «Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1», IDT).

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

5 ВЗАМЕН ГОСТ Р МЭК 61511-2—2011

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартинформ, оформление, 2018

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Сокращения и определения 1
Приложение А (справочное) Руководство по МЭК 61511-1 2
Приложение В (справочное) Пример разработки прикладной программы логического решающего устройства ПСБ с помощью функциональных блок-схем 55
Приложение С (справочное) Что следует учесть при конвертировании из непрограммируемых (НР) технологий в ПЭ-технологии 71
Приложение D (справочное) Пример получения прикладной программы из схемы трубопроводов и контрольно-измерительных приборов (Т и КИП) 72
Приложение Е (справочное) Пример получения прикладной программы из схемы трубопроводов и контрольно-измерительных приборов (СТ и КИП) 75
Приложение F (справочное) Пример проекта ПСБ, иллюстрирующий каждую стадию ее жизненного цикла, с использованием языка линейно-лестничной логики при разработке прикладных программ 78
Приложение G (справочное) Руководство по применению методов прикладного программирования 142
Приложение ДА (справочное) Сведения о соответствии ссылочного международного стандарта национальному стандарту 154

Введение

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

Область применения комплекса стандартов МЭК 61511 — ПСБ, применяемые в промышленных процессах. Комплекс стандартов МЭК 61511 также рассматривает вопросы интерфейса между такими системами и другими системами безопасности, которые выявляются в результате проведения анализа опасностей и рисков, присущих промышленному процессу. ПСБ включает в себя датчики, логические решающие устройства и исполнительные элементы.

В основе комплекса стандартов МЭК 61511 лежат две фундаментальные концепции, необходимые для его применения: концепция жизненного цикла ПСБ и концепция уровней полноты безопасности (УПБ). Жизненный цикл ПСБ формирует базовую структуру, объединяющую большинство положений настоящего стандарта.

Настоящий стандарт рассматривает ПСБ, использующие электрические/электронные/программируемые электронные технологии. Если логические устройства основаны на неэлектрических технологиях, то для обеспечения выполнения требований функциональной безопасности следует применять основные положения настоящего стандарта. Комплекс стандартов МЭК 61511 также рассматривает датчики и исполнительные элементы ПСБ независимо от принципа их действия. Комплекс стандартов МЭК 61511 был разработан для конкретизации требований комплекса стандартов МЭК 61508 применительно к промышленным процессам. Комплекс стандартов МЭК 61511 является конкретизацией общего подхода к вопросам обеспечения безопасности, представленного в МЭК 61508, для промышленных процессов.

Комплекс стандартов МЭК 61511 устанавливает подход, минимизирующий стандартизацию деятельности для всех стадий жизненного цикла ПСБ. Этот подход реализует рациональную и последовательную техническую политику. Цель настоящего стандарта — дать представление о том, как выполнять требования МЭК 61511-1:2016.

Чтобы облегчить применение МЭК 61511-1:2016, номера разделов, приведенные в приложении А, идентичны соответствующим номерам разделов МЭК 61511-1:2016, за исключением символа «А».

В большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования процесса, который сам обеспечивает безопасность. Тем не менее иногда это невозможно или практически нецелесообразно. В таких случаях он может быть дополнен системами защиты, основанными на применении различных технологий [например, химических, механических, гидравлических, пневматических, электрических, электронных, термодинамических (например, гаситель пламени), программируемых электронных], с помощью которых достигается любой установленный остаточный риск. Любая стратегия обеспечения безопасности должна рассматривать каждую конкретную ПСБ в контексте других систем защиты. Для облегчения применения такого подхода МЭК 61511-1:2016:

- требует, чтобы выполнялась оценка опасностей и рисков для определения общих требований к безопасности;
- 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 по управлению безопасностью, которые могут быть применены ко всем методам обеспечения функциональной безопасности;
- охватывает все стадии жизненного цикла ПСБ — 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.

Комплекс стандартов МЭК 61511 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 комплекса стандартов МЭК 61511.

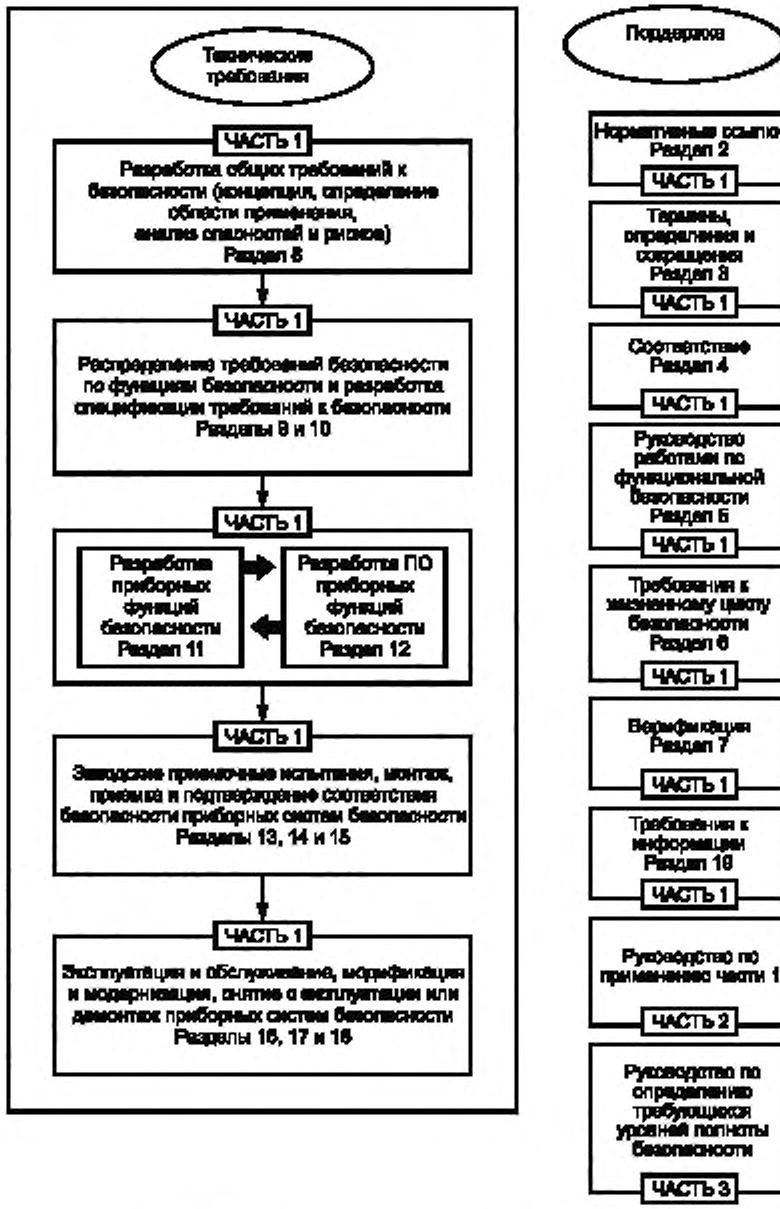


Рисунок 1 — Общая структура комплекса стандартов МЭК 61511

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 2

Руководство по применению МЭК 61511-1

Functional safety. Safety instrumented systems for the process industry sector.
Part 2. Guidelines for the application of IEC 61511-1

Дата введения — 2019—07—01

1 Область применения

Настоящий стандарт содержит руководство по установлению требований, разработке, монтажу, эксплуатации и техническому обслуживанию функций безопасности приборных систем безопасности (ФБ ПСБ) и реализующих их ПСБ в соответствии с МЭК 61511-1:2016.

Примечания

1 Справочное приложение А было построено так, что содержание каждого номера его раздела и подраздела совпадает с содержанием соответствующего номера раздела и подраздела МЭК 61511-1:2016 за исключением содержания тех номеров разделов и подразделов, которые следуют за символом «А».

2 Данное приложение А содержит материал, содержавшийся в теле первого издания настоящего стандарта. Те изменения, которые необходимы для обеспечения выполнения правил МЭК, целиком являются информационными.

3 Для получения максимальной пользы от данного руководства:

- следует изучать как руководящие указания раздела, так и руководящие указания конкретного подраздела (например, при необходимости применения руководящих указаний 5.2.6.1.3 следует учесть руководящие указания 5.2.6);
- если руководящие указания конкретного подраздела не предоставлены (например, отсутствуют какое-либо дальнейшие руководящие указания), то следует также обратиться к руководящим указаниям раздела, так как они могут быть применимы).

4 Примеры, представленные в приложениях настоящего стандарта, рассматривают только конкретные примеры реализации требований МЭК 61511 в конкретном случае, но пользователь должен сам убедиться, что выбранные им методы и технологии соответствуют его ситуации.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий международный стандарт (для датированной ссылки применяют только указанное издание ссылочного документа):

IEC 61511-1:2016, Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements (Безопасность функциональная. Приборные системы безопасности для технологических процессов в промышленности. Часть 1. Термины, определения и технические требования)

3 Сокращения и определения

В настоящем стандарте применены термины, определения и сокращения согласно МЭК 61511-1:2016 (раздел 3).

Издание официальное

Приложение А
(справочное)

Руководство по МЭК 61511-1

Примечание — Номера разделов и подразделов, представленные в приложении А, идентичны номерам разделов в МЭК 61511-1:2016. Это предназначено облегчить процесс предоставления перекрестных ссылок.

А.1 Область применения

Дополнительные требования не предусмотрены.

А.2 Нормативные ссылки

Дополнительные требования не предусмотрены.

А.3 Термины, определения и сокращения

Дополнительные требования не предусмотрены.

А.3.2.66 **функция безопасности** (safety function): Функция безопасности должна предотвращать появление конкретного опасного события, например «предотвращать превышение давления в емкости #ABC456, уровня 100 бар». Функция безопасности может быть реализована:

- отдельной ПСБ или
- одной или несколькими ПСБ и/или другими слоями защиты.

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).

А.3.2.67 **функция безопасности ПСБ** (safety instrumented function): Функции безопасности ПСБ (ФБ ПСБ) формируются из определенной функции безопасности, имеют соответствующий уровень полноты безопасности (УПБ) и выполняются конкретной приборной системой безопасности (ПСБ), например «закрыть клапан #XY123 в течение 5 с, если давление в емкости #ABC456 достигнет 100 бар». Устройства ПСБ могут быть использованы более чем в одной ПСБ.

А.4 Соответствие МЭК 61511-1:2016

Дополнительные требования не предусмотрены.

А.5 Управление функциональной безопасностью

А.5.1 Цель

Дополнительные требования не предусмотрены.

А.5.2 Руководящие указания к «Требованиям»

А.5.2.1 Общие требования

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 разделе 5 стандарта МЭК 61511-1:2016, 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.

А.5.2.2 Организация и ресурсы

Внутри компании, стройки, завода или проекта следует определить организационную структуру, связанную с ПСБ; следует ясно понимать и знать роли и ответственность каждого человека/подразделения 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 и кто назначает на должность. Целью должно быть обеспечение того, что каждый специалист в организации понимает свою роль и обязанности, связанные с работами по ПСБ.

Следует установить требования к подготовленности и знаниям, необходимым для выполнения всех работ на жизненном цикле ПСБ, 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. Лица, ответственные за определенную стадию жизненного цикла, должны быть доступны на всем ее протяжении, чтобы поддерживать передачу квалификации и опыта работы в жизненном цикле. При нехватке подготовленных кадров может быть проведен дополнительный набор опытного персонала.

А.5.2.2.1 Дополнительные требования не предусмотрены.

А.5.2.2.2 Дополнительные требования не предусмотрены.

А.5.2.2.3 Дополнительные требования не предусмотрены.

А.5.2.3 Оценка и управление рисками

Требования, установленные в МЭК 61511-1:2016 (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 61511-1:2016 не предлагает конкретного метода. Дополнительные указания даны в А.8.2.1 настоящего стандарта.

А.5.2.4 Планирование системы безопасности

Цель А.5.2.4 состоит в том, чтобы гарантировать, что в рамках всего проекта адекватное планирование системы 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.

А.5.2.5 Реализация и мониторинг

А.5.2.5.1 Цель МЭК 61511-1:2016 (пункт 5.2.5.1) — 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 (СТБ) в течение ее эксплуатационного срока службы.

А.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 устройств. Аппаратное и программное обеспечение компонентов ПСБ должно изготавливаться под управлением признанной системы управления качеством, например в соответствии с серией стандартов ИСО 9000.

Следует периодически проводить критический анализ характеристик ПСБ, чтобы убедиться в том, что исходные допущения, принятые при составлении СТБ, сохраняются. Например, следует периодически оценивать интенсивность отказов различных устройств 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.

А.5.2.5.3 Дополнительные требования не предусмотрены.

А.5.2.5.4 Дополнительные требования не предусмотрены.

А.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 (ОФБ) 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.

А.5.2.6.1 Оценка функциональной безопасности (ОФБ)

Оценка функциональной безопасности (ОФБ) является основной процедурой, демонстрирующей, что ПСБ выполняет предъявляемые к ней требования, связанные с ее функциями безопасности и значениями 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:

a) 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;

b) 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;

c) 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;

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

- сложность;
- значимость безопасности;
- предшествующий опыт, связанный с подобными системами;
- стандартизация конструктивных особенностей;

e) 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. Должно быть представлено подтверждение текущего или принятого состояния проекта или установки системы:

- следует обеспечить, чтобы исполнители ОФБ были 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;
- методы контроля должны показать, что функции прикладного программного обеспечения (ППО) соответствуют требованиям, вытекающим из опасностей процесса;
- функциональные испытания, показывающие, что ППО исполняет требуемые функции и, насколько это возможно, любые дополнительные функции как в ППО, так и во встроенном ПО, не приводят к опасным условиям;
- структурное тестирование (см. А.12.5.3), показывающее, что ППО выполняет требуемые функции за необходимое время, а также идентифицирующее наличие каких-либо не тестируемых областей ППО, которые (из-за того, что не испытывались) могут привести к возникновению опасных условий;
- анализ функциональных отказов и анализ по методу «что если», позволяющие показать, что функции ППО не приводят к опасным условиям;
- процедуры, демонстрирующие обеспечение управления и верификации процесса разработки, а также использование правильных версий ППО и встроенного ПО;
- должны быть установлены процедуры и план аудита.

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.

Чтобы увеличить объективность оценки, к ней необходимо привлечь специалиста, не участвовавшего в проектировании. Имеется потребность в специалисте высокого уровня (например, по опыту, служебному положению), для того чтобы убедиться в том, что все спорные вопросы приняты во внимание и учтены. Также, как предлагается в МЭК 61511-1:2016 (подпункт 5.2.6.1.2, примечание), 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 внутри себя 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.

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.

В некоторых странах ОФБ выполняют на стадии 3, которую часто называют предпроектным обзором безопасности (ППОБ). См. таблицу F.1, блок 10. Техническое задание для ОФБ должно быть согласовано на стадии планирования системы безопасности.

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 анализе опасностей и рисков, на стадиях разработки, монтажа, приемки и подтверждения соответствия.

А.5.2.6.1.1 Команда, выполняющая ОФБ, в некоторых случаях может состоять из одного человека, если этот человек обладает требующимися для этой деятельности навыками и опытом.

А.5.2.6.1.2 Число старших компетентных членов команды оценки может варьироваться в зависимости от размера приложения, охватываемых технологий, требований к коммуникациям (например, с пользователем/владельцем, интегратором, изготовителем), а также сроков проектирования.

Старший компетентный сотрудник должен обладать компетентностью в различных технологиях, которые могут быть использованы в приложении, применимых правилах и нормах, а также должен быть способен выполнять свою работу в установленные для проекта сроки.

А.5.2.6.1.3 Дополнительные требования не предусмотрены.

А.5.2.6.1.4 Дополнительные требования не предусмотрены.

А.5.2.6.1.5 Дополнительные требования не предусмотрены.

А.5.2.6.1.6 Инструментальные средства, используемые для проектирования, разработки, эксплуатации и обслуживания ПСБ, могут повлиять на полноту безопасности ПСБ, привнеся сбои в конечную систему. Такие средства могут привести к прямому «встраиванию» части своей функциональности в ПСБ (например, к появлению пользовательских библиотек, интерпретаторов) или же к тому, что они будут использоваться «в автономном режиме» (off-line), т. е. будут использоваться для генерации информации, которая может произвольно проверяться (например, средства вычисления переменных полей, средства для проведения испытаний). Такие средства также можно подсоединить к функционирующей ПСБ — например, в качестве средств обслуживания. Во всех таких случаях важно выявить возможные виды и последствия отказов, а также методы управления ими. Типичные подходы к управлению сбоями в инструментальных средствах включают:

- подтверждение прослеживаемости с национальными и международными стандартами (включая стандарты по калибровке и/или функциональные стандарты, в зависимости от характера средства);
- рассмотрение отчетов, содержащих опыт групп пользователей и накопленные данные предыдущего использования инструментального средства;
- анализ и функциональное тестирование результатов использования инструментального средства;
- использование принципа разнообразия для инструментальных средств разработки и/или испытания: например, использование кода, полученного от разных компиляторов, контроль результатов инструментального средства проектирования с помощью разных типов инструментальных средств проверки;
- инструментальное средство поставляется как составная часть устройства, удовлетворяющего требованиям МЭК 61508-2:2010 и МЭК 61508-3:2010.

В результате выполнения ОФБ будет проверена стратегия, которая должна быть направлена на поддержку целостности результатов инструментальных средств с учетом того, являются ли данные средства «встроенными» или «автономными», а также на получение заключения о том, был ли достигнут необходимый уровень доверия для этих инструментальных средств.

А.5.2.6.1.7 Дополнительные требования не предусмотрены.

А.5.2.6.1.8 Дополнительные требования не предусмотрены.

А.5.2.6.1.9 Дополнительные требования не предусмотрены.

А.5.2.6.1.10 Дополнительные требования не предусмотрены.

А.5.2.6.2 Аудит и проверка функциональной безопасности

a) Виды аудита

Проведение аудита ПСБ обеспечивает полезной информацией руководство предприятия, а также инженеров, занятых обслуживанием и разработкой устройств ПСБ. Это позволяет руководству быть активным участником и осведомленным о степени реализации 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:

- инспекции;
- визиты для оценки безопасности (например, при обходе предприятия и разборе инцидента);
- обследование ПСБ (по анкете).

Следует различать наблюдения и проверки, с одной стороны, и действия по аудиту — с другой. Наблюдение и проверка направлены на оценку выполнения конкретных действий на жизненном цикле (например, контролер проверяет выполнение работы по обслуживанию перед тем, как устройство будет вновь включено в работу). В отличие от них действия по аудиту являются более обширными и концентрируются на полной реализации ПСБ на всех стадиях их жизненного цикла. Аудит должен включать в себя определение того, выполнена ли программа наблюдения и проверки.

Аудиты и инспекции 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 ПСБ, а также текущих 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. Действия, выполняемые в процессе аудита, имеют своей целью повысить эффективность ПСБ, например помочь минимизировать риск для работников и населения получить травму или погибнуть, способствовать повышению культуры безопасности, 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

Общая цель аудита заключается в достижении определенного уровня соответствия МЭК 61511-1 и извлечении максимума информации в ходе проведения аудита, что может быть достигнуто 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. Эта последовательность 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, руководитель высшего звена 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;
  - основополагающие документы аудита или стандарт для его проведения;
  - необходимость дополнительных 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 заводскому персоналу и позволить ему принять участие в формировании заключений аудита;
- 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 провести заключительное заседание либо в конце проведения аудита, либо позже, но до выпуска итогового отчета;

- соответствующему руководству должна быть предоставлена возможность прокомментировать проект отчета и замечания, а также при желании обсудить их на заключительном заседании;

- нормальной практикой считается запрос плана действий стройки, завода или проектной организации, чтобы учесть замечания, включенные 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.

А.5.2.6.2.1 Дополнительные требования не предусмотрены.

А.5.2.6.2.2 ОФБ может быть проведена 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). Дополнительные требования см. в МЭК 61508-1:2010 (таблицы 4 и 5).

А.5.2.6.2.3 МЭК 61511-1:2016 (пункты 5.2.6.3, 5.2.6.4 и 5.2.6.5) придает особое значение той роли, которую играет управление изменениями в процессах проведения аудитов. Если первоначальный анализ опасностей предусматривает слои защиты, не связанные с ПСБ, которые должны быть реализованы, например в ОСУП (основная система управления процессом), или процедурами оператора с выдачей аварийных сигналов, то любые изменения этих систем должны контролироваться, чтобы гарантировать, что они не снижают уровень защиты, обеспечиваемый слоями защиты, не связанными с ПСБ. При этом очевидно, что незначительные изменения номеров версий или модификаций систем в ПСБ или интерфейсных систем могут привести к проблемам несовместимости между ППО, встроенным ПО, аппаратными средствами (например, представьте, как сложно восстановить раннюю версию программы ПО). Поэтому очень важно обеспечить управление не только отдельными элементами, но и всей конфигурацией элементов в целом. В частности, версии ППО и ПО должны соответствовать версиям аппаратных средств, а также рабочим процедурам и интерфейсу, для которых оно было спроектировано.

А.5.2.6.2.4 Дополнительные требования не предусмотрены.

А.5.2.7 Управление конфигурацией ПСБ

А.5.2.7.1 Для управления и поддержания прослеживаемости устройств на всех стадиях их жизненного цикла может быть установлен механизм идентификации, управления и учета для моделей или версий каждого устройства.

На возможно ранней стадии жизненного цикла ПСБ 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) уникальную идентификацию модели или версии и внутреннего статуса каждого изделия (включая встроенное и сервисное ПО и ППО) с указанием поставщика, даты и места применения, а также изменений модели или версии по отношению к исходной модели или версии;

c) идентификацию 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 каждой части ППО, которые в совокупности определяют законченное ППО;

g) обеспечение координации процесса добавления многочисленных ПСБ на одном или более объектах;

h) документально оформленную авторизацию ввода устройств в эксплуатацию;

i) авторизованный перечень подписей, допускающих ввод в эксплуатацию;

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

k) управление соответствующей сопроводительной документацией;

l) определение для каждой модели/версии устройства:

- функциональной спецификации,
- технической спецификации;

m) ссылку на процедуру управления изменениями.

Должны быть определены все подразделения и/или организации, участвующие в руководстве и обслуживании ПСБ, а границы их ответственности заданы и понятны.

По существу, требования к управлению конфигурацией ППО не отличаются от требований к устройствам аппаратных средств системы. Тем не менее ППО чаще заслуживает более строго подхода, чем требуется для отдельного устройства аппаратных средств, так как:

- более «логическая», чем «физическая», сущность ППО такова, что его фактическую конфигурацию трудно «рассматривать» иначе как через сопроводительную документацию;
- его проще модифицировать (практика выпуска нескольких различных версий программы за один день является стандартной для программистов);
- функциональные возможности приложения полностью зависят от корректной работы ППО, что делает его корректность ключевым фактором для корректной работы ПСБ в целом;
- оно может выполняться по-разному в зависимости от различных версий ПЭС (программируемой электронной системы), изменений в интерфейсах для связи с внешним миром, различия в диапазонах ввода и вывода и даже в зависимости от различных версий собственных средств разработки ППО;
- оно может быть предназначено для определенного набора спецификаций, конфигурации сборки, подсистемы ПСБ, окружения и размещения, но при этом его можно отличить только по версии и ревизии в управляемой конфигурации.

В дополнение к стандартным требованиям к управлению конфигурацией для обеспечения идентификации, управления изменениями и версиями, а также для совместимости элементов, типичные аспекты, которые следует использовать для поддержания управления ППО, включают:

- использование встроенных в ППО кодов, обеспечивающих возможность загрузки этого ППО только в предназначенный для него узел (хост) аппаратных средств (это в особенности полезно там, где на различных участках может использоваться множество различных конфигураций);
- использование информации о версии, требующейся для выполнения авторизации известным полномочным органом или органами, перед тем как станет возможно загружать в ПСБ новые версии программы;
- ведение учета о статусе и версии всех элементов, используемых в разработке, испытании и обслуживании ППО, связь которых с имеющими значение спецификациями и результатами верификации, связанными с конфигурацией, можно полностью проследить;
- поддержание резервного копирования для обеспечения возможности возвращения системы в предыдущую конфигурацию;
- использование управляемых циклов модификаций, позволяющих организовывать изменения в определенных версиях. Преимуществом этого является то, что множество различных версий могут находиться в разработке на разных стадиях готовности и не взаимодействовать друг с другом, а также позволяют циклу испытаний обеспечить определенную версию некоторым уровнем стабильности до того, как она будет внедрена на участке.

А.5.2.7.2 Дополнительные требования не предусмотрены.

А.6 Требования к жизненному циклу системы безопасности

А.6.1 Цели

Функциональная безопасность, достигнутая для любого объекта процесса, зависит от удовлетворительного выполнения ряда действий. Цель применения систематической концепции жизненного цикла ПСБ 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 61511-1:2016 типичный жизненный цикл системы безопасности представлен на рисунке 7 и в таблице 2, требования к каждой стадии жизненного цикла приведены в МЭК 61511-1:2016 (разделы 8—18).

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 МЭК 61511-1:2016 (раздел 6) состоит в том, чтобы даже при использовании другого жизненного цикла ПСБ были определены входные и выходные данные для каждой стадии жизненного цикла и были включены все существенные требования.

А.6.2 Руководящие указания к «Требованиям»

А.6.2.1 Особое внимание должно быть обращено на то, чтобы заранее определить жизненный цикл ПСБ для 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.

Должна быть идентифицирована иерархия ответственности каждой стадии жизненного цикла и с ней должны быть ознакомлены все вовлеченные стороны (например, субпоставщики, специалисты по системной интеграции, конечные пользователи). В результате этого все должны быть осведомлены о своей ответственности о том, как их деятельность связана между собой и со стадиями жизненного цикла, а также о том, как каждая сторона вносит свой вклад в выполнение общих требований к функциональной безопасности и к полноте безопасности.

А.6.2.2 Хотя настоящий стандарт этого не требует, обычно полезно на самой ранней стадии сформировать предполагаемый жизненный цикл ПСБ совместно с этапами жизненного цикла проекта, включая перечень блоков, показанных на рисунке 7 МЭК 61511-1:2016, которые применяются в проекте. После того как это будет сделано, чтобы начать работу в рамках жизненного цикла ПСБ, следует рассмотреть определенную информацию вместе с вопросом о том, кто, вероятно, способен эту информацию предоставить, для того чтобы конкретный персонал можно было назначить ответственным за жизненный цикл системы безопасности. В некоторых случаях может оказаться невозможным установить точную информацию по отдельным позициям раньше, 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 ПСБ.

А.6.2.3 Другой важной частью планирования жизненного цикла системы 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.

А.6.2.4 Поскольку детальное проектирование, верификация, подтверждение соответствия и доказательство о проведении испытания были выполнены на других стадиях жизненного цикла системы безопасности, то важно, чтобы после каждого изменения подтверждалось, что каждая стадия жизненного цикла безопасности системы остается неизменной, никаких новых опасностей не появляется и что приложение по-прежнему работает так, как от него требуется.

А.6.3 Руководящие указания к «Требованиям к жизненному циклу прикладной программы ПСБ»

А.6.3.1 Жизненный цикл ППО для ПСБ начинается на стадии 3 жизненного цикла ПСБ («СТБ ПСБ») и заканчивается с ОФБ стадии 3.

Если жизненный цикл ППО системы безопасности соответствует требованиям МЭК 61511-1:2016 (таблица 3), то допускается подстраивать глубину, число и размер стадий V-модели (см. рисунок А.1) для учета полноты безопасности и сложности проекта.

Тип используемого языка ППО и близость языка прикладным функциям могут сказываться на области применения стадий V-модели. Если для проектирования, реализации, верификации и подтверждения соответствия ППО используются ЯОИ, такие как язык лестничных диаграмм или язык диаграмм функциональных блоков из МЭК 61131-3:2013, то применимы только два уровня стандартной V-модели ППО:

- «разработка прикладного модуля», которая в V-модели интерпретируется как проектирование и реализация новой функции, и
- «проверка прикладного модуля», которая интерпретируется как верификация и испытание новой функции.

В тех случаях, когда новая функция должна быть записана на ЯПИ и, таким образом, необходим более подробный процесс разработки ППО (т. е. кодирования), разработчику следует выполнить все стадии и процедуры жизненного цикла, установленные в МЭК 61508-3:2010. СТБ ППО может быть частью СТБ ПСБ.

А.6.3.2 Выбор методов и способов должен зависеть от определенных обстоятельств. Факторы, учитываемые в принятии этого решения, вероятно, будут включать:

- размер ППО;
- степень сложности;
- УПБ реализуемых функций безопасности ПСБ (ФБ ПСБ);
- степень стандартизации инструментальных средств проектирования (например, средства конфигурации);
- тип прикладного языка (например, язык функциональных схем из приложения В; причинно-следственная диаграмма на рисунке D.2 и в таблице F.14; линейно-лестничная логика на рисунке F.11).

Примеры методов и мер см. в А.12.6.2.

А.6.3.3 Дополнительные требования не предусмотрены.

А.7 Верификация

А.7.1 Цель

Цель верификации состоит в обеспечении того, что действия, предусмотренные планом верификации на каждой стадии жизненного цикла ПСБ, действительно выполнены и что требуемые выходные результаты стадии, будь это документация, аппаратное средство или ППО, реализованы и соответствуют своим целям как конечным результатам стадий.

А.7.2 Руководящие указания к «Требованиям»

А.7.2.1 МЭК 61511-1:2016 признает, что организации будут иметь свои собственные процедуры верификации, и не требует, чтобы они всегда выполнялись одинаковым способом. Напротив, смысл МЭК 61511-1:2016 (раздел 7) состоит в том, что все действия по верификации планируются заблаговременно, вместе с любыми другими процедурами, мероприятиями и методами, которые должны применяться.

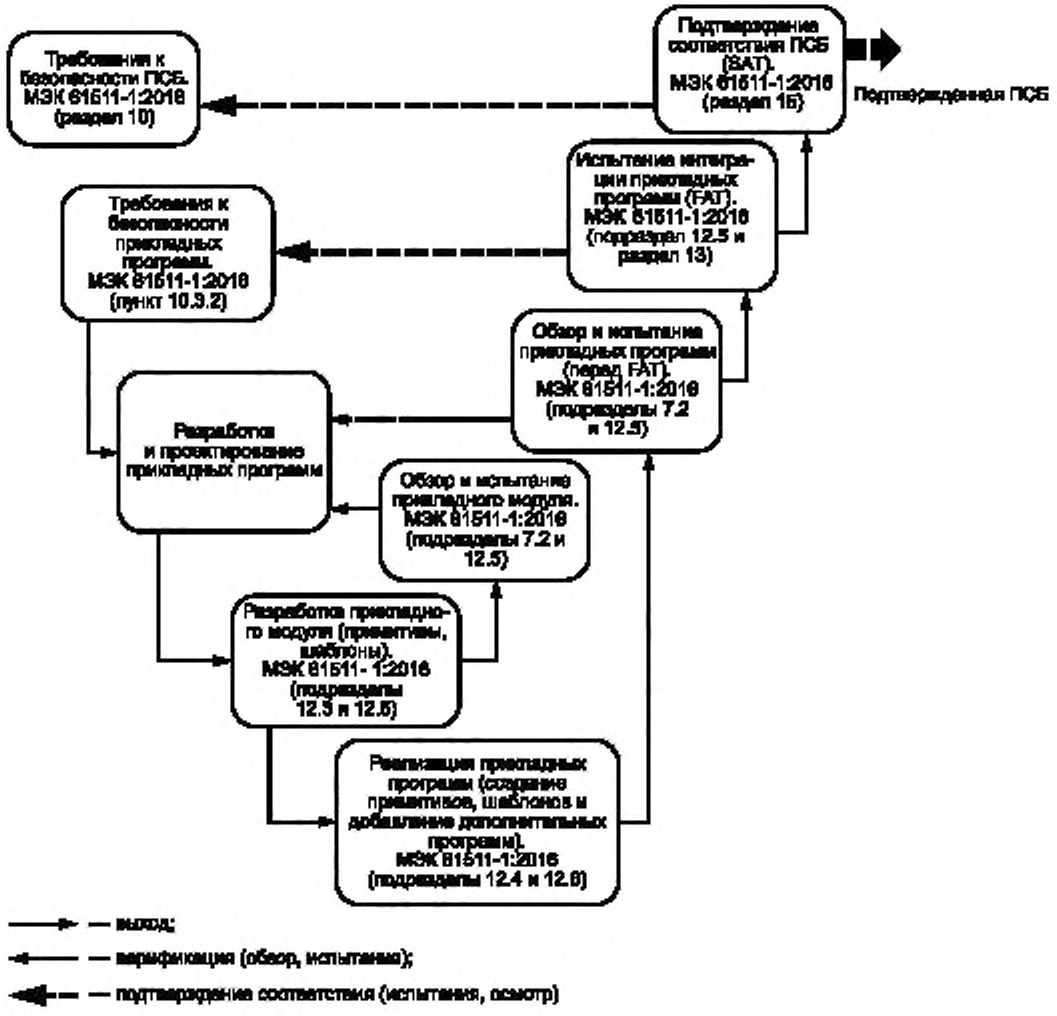


Рисунок А.1 — V-модель прикладной программы

А.7.2.2 Для того чтобы обнаружить и устранить ошибки, уже существующие в программах, рекомендуется проводить верификацию на всем жизненном цикле разработки. Вообще говоря, для того чтобы обеспечить проверяемость, рекомендуется, чтобы спецификации испытаний интеграции ППО были рассмотрены еще в ходе стадий проектирования и разработки. Область применения испытаний должна учитывать испытания, проводившиеся прежде.

Успешное завершение стадии должно подтверждаться с помощью верификации на каждой отделенной стадии цикла разработки ППО (включая, испытание). В общем случае верификацию проводит специальная группа, которая может состоять из одного или более человек (в зависимости от потребностей приложения).

Для снижения числа ошибок путем заранее принятых разумных ориентиров верификация должна проводиться квалифицированным участником, являющимся экспертом, не участвующим в разработке кода приложения, и в случае приложений с УПБ 3, участником, который представляет независимый отчет.

Если инструментальные средства разработки ППО 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, реализуемые ППО, и реакции 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 ППО, рекомендуется для более высоких значений УПБ проводить следующие дополнительные испытания:

- испытания, базирующиеся на особенностях внутренней структуры (например, внутренние алгоритмы, внутренние состояния);
- «стрессовое тестирование» (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 отображала то, что верификация и тестирование были выполнены и были успешными. Также рекомендуется:

- чтобы документация позволяла проведение оценки адекватности верификации и тестирования;
- чтобы документация позволяла бы независимому специалисту повторить испытания и оценить их достаточность.

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 проверку того, что соответствующие механизмы (например, защита паролем с уровнями доступа) предусмотрены и используются адекватно.

Система процесса может иметь одну или несколько встроенных систем, соответствующих разным стандартам (например, МЭК 62061:2005 для машинного оборудования, NFPA 85:2015 для печей). Требуется аккуратная интеграция оборудования, ППО и встроенного ПО. Достигнуть этого можно, например, если для систем, не связанных с промышленным процессом (т. е. для систем, которые должны соответствовать другим стандартам, таким как стандарты по машинному оборудованию, печам и т. п.), выполнять анализ опасностей и рисков как для промышленного оборудования, с целью обеспечения идентификации всех возможных опасностей и предоставления любой дополнительной идентифицированной защиты.

А.7.2.3 Дополнительные требования не предусмотрены.

А.7.2.4 Дополнительные требования не предусмотрены.

А.7.2.5 Когда жизненный цикл ППО достигнет стадий верификации и испытания, то любые изменения или модификации ППО могут искажать любые результаты, полученные на предыдущей стадии. Одним из способов решения этой проблемы является повторение всего жизненного цикла с самого начала, но это дорогостоящий способ, который привносит задержки в программу и почти в каждом случае предполагает большой объем совсем необязательной работы. Вместо этого с помощью анализа влияний следует идентифицировать области, которые могли пострадать, и сосредоточить усилия на обеспечении повторного подтверждения соответствия этих областей.

А.7.2.6 Важно, чтобы результаты верификации были пригодны для того, чтобы можно было показать, что на всех стадиях жизненного цикла ПСБ была проведена эффективная верификация.

А.8 Анализ опасностей и рисков процесса

А.8.1 Цели

Основная цель состоит в том, чтобы установить необходимость применения функций безопасности и соответствующие целевые меры отказов, которые необходимы, чтобы гарантировать безопасность процесса. Функции безопасности распределяются по слоям защиты в соответствии с требованиями раздела 9 МЭК 61511-1:2016. 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 защиты представлены на рисунке 9 МЭК 61511-1:2016.

А.8.2 Руководящие указания к «Требованиям»

А.8.2.1 Требования к проведению анализа опасностей и рисков устанавливаются только в терминах результатов. Это означает, что организация может использовать любой метод, который она считает эффективным и обеспечивающим результаты в виде ясного описания функций безопасности и соответствующих целевых мер отказов.

При проведении анализа опасностей и рисков следует устанавливать и рассматривать опасные события, которые могли произойти во всех обоснованных предсказуемых случаях (включая условия появления отказов и обоснованно предсказуемое неправильное применение). Следует рассмотреть прошлые инциденты, включая их причины, системные отказы и то, что было извлечено из уроков предотвращения повторения этих инцидентов.

Предварительный анализ опасностей и рисков в типичном проекте для промышленных процессов следует выполнять на ранней стадии разработки основных проектных решений для процесса. 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 технологического процесса, то для выполнения предварительного анализа опасностей и рисков обычно бывает достаточно этой информации. Необходимо признать, что в проекте могут появиться дополнительные опасные события, так как далее выполняется детальное проектирование. Поэтому после завершения построения технологической карты основного процесса и схемы его автоматизации может потребоваться окончательный анализ опасностей и рисков. Этот окончательный анализ обычно проводится с помощью формальной и полностью документируемой процедуры, такой как исследование опасности и работоспособности (HAZOP — см. МЭК 61882:2003). Она должна подтвердить, что разработанные слои защиты адекватно обеспечивают управление рисками на предприятии. В ходе этого окончательного анализа необходимо рассмотреть, не приводят ли отказы слоев защиты (или успешные активации слоев защиты) к каким-либо новым опасным событиям или запросам, и установить на этой стадии, не появилась ли необходимость введения новых функций безопасности. Другим более вероятным результатом является выявление дополнительных причин, которые приводят к опасным событиям, уже определенным на предварительной стадии. В таких случаях необходимо рассмотреть, нужна ли какая-либо коррекция функций безопасности и требований к целевым мерам отказа, установленным при предварительном анализе.

Подход, применяемый для выявления опасных событий, 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 ИСО 10418:2003 и API RP 14C:2001). Если проект более сложен или рассматривается новый процесс, то может оказаться необходимым применение более строгого подхода (например, по ИСО 31000:2009).

Примечание — Дополнительная информация о выборе соответствующих методов приведена в ИСО 17776:2000 «Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment».

При рассмотрении последствий событий, связанных с конкретными опасными событиями, следует проанализировать все возможные результаты события, а также частоту возникновения события с учетом вкладов в каждый результат. Ни один из ожидаемых результатов не должен игнорироваться или исключаться. 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 следует 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, чтобы 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 можно 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 опасное событие существует в период запуска, а персонал часто присутствует. Следует также обратить внимание на возможное увеличение численности людей, находящихся вблизи от опасного события, для исследования влияния симптомов разрастающегося события.

Должны быть оценены предполагаемые режимы работы промышленного процесса, в том числе запуск, постоянная работа, останов, обслуживание, циклы очистки. В ходе каждого из предназначенных режимов работы промышленного процесса следует учитывать обоснованно предсказуемые источники запросов на срабатывание ПСБ, такие как отказы оборудования, системы управления, других слоев защиты, ошибки обслуживания, ручное вмешательство (например, в функцию управления ОСУП в режиме ручного управления) и 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 (или последовательных скрытых) 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 причин, способных привести к идентифицированным опасным событиям, и какое значение частоты должно использоваться для таких событий. Необходимо также быть осторожным в тех случаях, когда принимается снижение частоты запросов за счет действий оператора. Такое допущение ограничивается возможностями человека (человеческим фактором) — скоростью

выполнения необходимых действий и сложностью решаемых задач. При допущении числа действий оператора более десяти раз в год следует проводить анализ надежности персонала. Если принимается, что снижение риска происходит более чем в 10 раз, то система должна проектироваться в соответствии с МЭК 61511-1:2016. В таком случае система, выполняющая функцию безопасности, будет включать в себя датчик, определяющий появление опасной ситуации, воспроизведение аварийной сигнализации, ответное действие оператора и оборудование, используемое оператором для прекращения любой ненормальной ситуации. 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 слоя защиты аварийной сигнализации должны быть подкреплены документально оформленным описанием необходимой реакции на сигнализацию и обоснованием того, что оператор имеет достаточно времени для корректирующего действия, а также уверенностью в том, что оператор подготовлен (изначально и с повторением обучения) к выполнению защитных действий.

Система аварийной сигнализации может быть использована как способ снижения риска путем снижения частоты запросов к ПСБ или в качестве отдельного слоя защиты, снижающего общий риск такого сценария. При проектировании такой системы аварийной сигнализации необходимо учесть следующее:

- датчик, применяемый в системе сигнализации, и исполнительные элементы, воздействующие на процесс, не используются для целей управления, если потеря управления приводит к запросу на срабатывание системы аварийной сигнализации. Это происходит в тех случаях, когда не был проведен анализ, указывающий на допустимость общего уровня риска. Следует рассмотреть проблемы отказов по общей причине и общего вида;
- датчик, применяемый в системе сигнализации, и исполнительные элементы, воздействующие на процесс, не заявляются как снижающая риск часть ПСБ для тех же опасных событий, если во время анализа снижения риска не учитываются отказы по общей причине;
- ограничения на снижение риска, которые можно требовать при проектировании и управлении системой аварийной сигнализации, такие как условия для защиты доступа, управление изменением и контроль, предупредительное обслуживание и испытание.

Примеры способов, которые могут применяться при установлении УПБ для ПСБ, даны в МЭК 61511-3:2016, 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 опасностей и рисков необходимо рассмотреть следующее:

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

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

c) дополнительные требования не предусмотрены;

d) необходимость снижения риска для каждого опасного события;

e) меры, предпринимаемые для снижения или устранения опасностей и рисков;

f) 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;

g) дополнительные требования не предусмотрены;

h) 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 опасностей и рисков, следует оформлять документально.

Может оказаться необходимым повторить проведение анализа опасностей и рисков на различных стадиях полного жизненного цикла ПСБ по мере того, как принимаемые решения и доступная информация становятся более совершенными. Следует периодически повторно подтверждать соответствие с помощью анализа опасностей и рисков и документально оформлять его проведение для обеспечения соответствия предположений реальному опыту эксплуатации [см. МЭК 61511-1:2016 (подпункт 5.2.5.3)] и текущему плану управления безопасностью [см. МЭК 61511-1:2016 (подпункт 5.2.5.1)].

А.8.2.2 ОСУП включает в себя все устройства, необходимые для управления промышленным процессом и соответствующим оборудованием желаемым образом [см. МЭК 61511-1:2016 (пункт 3.2.3)]. Устройства ОСУП, как правило, не квалифицированы в соответствии с МЭК 61511-1:2016 (пункт 11.2.4), что не позволяет допускать интенсивность опасных отказов меньше 10^{-5} в час.

Для промышленных процессов важной причиной запросов, которые должны быть рассмотрены при анализе опасностей и рисков, является отказ ОСУП. Необходимо отметить, что отказ ОСУП может быть вызван всем, от чего зависит корректная работа ОСУП: например, датчиком, клапаном, ошибкой оператора или логическим решающим устройством.

МЭК 61511-1:2016 устанавливает ограничение на интенсивность опасных отказов для самой ОСУП как инициирующего источника до 10^{-5} в час, если ОСУП не создавалась в соответствии с требованиями настоящего стандарта. Причина данного ограничения состоит в том, что система управления функциональной безопасностью, представленная в МЭК 61511-1:2016, и предписанные в ней меры и способы необходимы для снижения вероятности возникновения систематических отказов до достаточно низкого уровня, чтобы заявленная интенсивность опасных отказов поддерживалась на уровне меньше 10^{-5} в час. Такое ограничение обеспечивает, что высокие доверительные уровни не относятся к ОСУП, которые не отвечают требованиям МЭК 61511-1:2016.

А.8.2.3 Дополнительные требования не предусмотрены.

А.8.2.4 Дополнительные требования см. в ISA TR84.00.09:2013.

А.9 Распределение функций безопасности по слоям защиты

А.9.1 Цели

Для того чтобы определить потребность в ФБ ПСБ и соответствующие требования к их УПБ, важно рассмотреть запланированные (или установленные) слои защиты и насколько они снижают риски. Если необходим слой защиты ПСБ, то следует определить значение УПБ для каждой функции (или функций) безопасности ПСБ, распределенной для этой ПСБ.

А.9.2 Руководящие указания к «Требованиям к процессу распределения»

А.9.2.1 Первое требование состоит в том, чтобы идентифицировать используемые слои защиты и распределить снижение риска по функциям безопасности ПСБ. На практике часто функции безопасности распределяются только по ПСБ, в которых существуют проблемы применения разработок с внутренне присущей им безопасностью или систем, использующих другие технологии.

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

Как указывалось выше, действия по анализу опасности и риска и по распределению могут выполняться параллельно либо распределение может при некоторых обстоятельствах выполняться перед анализом 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 слоев 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.

А.9.2.2 Дополнительные требования не предусмотрены.

А.9.2.3 Если для реализации функции безопасности назначена ПБС, то необходимо будет учитывать режим ее реализации — с низкой частотой запросов или с высокой частотой запросов/непрерывный режим. В промышленных процессах функции безопасности часто реализуется режим с низкой частотой запросов, при котором частота запросов, как правило, невелика. Для таких случаев подходит таблица 4, приведенная в МЭК 61511-1:2016. Встречается также растущее число приложений, работающих в режиме с высокой частотой запросов, для которых более подходящим является режим работы с непрерывным запросом, так как опасные события, как правило, случаются, как только происходит отказ функционирования ПСБ. Для таких случаев применим МЭК 61511-1:2016 (таблица 5). Случаи режима работы с непрерывным запросом, в которых отказ привел бы к непосредственной опасности, редки. Функции управления горелкой или скоростью турбины могут относиться к приложениям, функционирующим в режиме с непрерывным запросом, которые должны соответствовать МЭК 61511-1:2016, если требующаяся средняя интенсивность отказов (для достижения указанной интенсивности опасных событий) меньше чем 10^{-5} в час.

МЭК 61511-1:2016 (таблица 4) определяет значения УПБ, выраженные в значениях средней вероятности отказа при наличии запроса ($ВОНЗ_{ср}$). Заданное значение $ВОНЗ_{ср}$ определяется 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 МЭК 61511-3:2016.

МЭК 61511-1:2016 (таблица 5) устанавливает УПБ, выраженный в значениях средней 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 5 МЭК 61511-1:2016, то его целевое значение базируется на частоте опасных отказов ПСБ. При применении таблицы 5 МЭК 61511-1: 2016 некорректно преобразовывать частоту опасных отказов в вероятность их появления при наличии запроса, используя интервал контрольной проверки или интенсивность запросов. Хотя при таком преобразовании единицы измерения могут казаться правильными, оно будет ошибочным и может привести к некорректному преобразованию таблицы 5 МЭК 61511-1:2016 и неполной спецификации требований, предъявляемых к УПБ функций безопасности.

Заданные значения средней вероятности отказов при наличии запроса или частоты опасных отказов применяются к ФБ ПСБ, а не к отдельным компонентам, устройствам или подсистемам ПСБ. Компонента, устройство или подсистема (например, датчик, логическое решающее устройство, исполнительный элемент) не могут иметь УПБ, установленные вне их связи с конкретной ПСБ. Однако компонент может обладать стойкостью к систематическим отказам, которая относится к мерам и способам, применяемым для снижения вероятности возникновения систематических ошибок, приводящих к опасным отказам ПСБ.

Результатом работ по анализу опасности и риска и распределению требований должно быть ясное описание функций, которые будут выполнены защитными слоями. В случае ПСБ подобное описание должно включать в себя режим работы, т. е. непрерывный, с высокой или низкой частотой запросов, а также требования УПБ для всех ФБ ПСБ. Такое описание формирует основу для составления СТБ ПСБ. Описание функций безопасности должно быть ясным настолько, насколько это необходимо для понимания функциональных требований и требований полноты 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.

А.9.2.4 Необходимо полностью понимать смысл таблиц 4 и 5, приведенных в МЭК 61511-1:2016. В частности, значения $ВОНЗ_{ср}$, которые могут быть приняты для одиночной ФБ ПСБ, ограничены пределом 10^{-5}, что связано со снижением риска в 10^5 раз (УПБ 4). Анализ безотказности может показать, что достижение интенсивности случайных отказов технических средств, не превышающей 10^{-b}, возможно, но в МЭК 61511-1:2016 принимается, что систематические отказы и отказы по общей причине будут ограничивать реально достигаемое сокращение рисков. 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 ФБ ПСБ в секторе промышленных процессов. При этом следует рассмотреть возможность устранения или сокращения опасности у ее источника за счет внедрения не основанных на ПСБ мер снижения вероятности возникновения причин опасных событий или использования нескольких независимых ФБ ПСБ с более низким уровнем полноты безопасности. Для случаев использования нескольких ФБ ПСБ следует учитывать зависимость одних ФБ ПСБ от других, включая влияние синхронной контрольной проверки. Один из методов рассмотрения этого влияния заключается в применении комплексного подхода к моделированию общей системы [см. МЭК 61511-3:2016 (приложение J)].

А.9.2.5 Дополнительные требования не предусмотрены.

А.9.2.6 Чтобы достичь более высоких уровней снижения риска (например, превышающих 10^3), можно использовать несколько ФБ ПСБ. При этом важно, чтобы каждая из ФБ ПСБ могла независимо выполнять функцию безопасности и чтобы независимость между ФБ ПСБ была достаточно обоснованной.

Кроме того, при использовании нескольких ФБ ПСБ следует учитывать отказы по общей причине. При этом должны выполняться все остальные требования, установленные в МЭК 61511-1:2016, включая требования к минимальной отказоустойчивости, приведенные в МЭК 61511-1:2016 (таблица 6).

Чтобы проиллюстрировать, как можно совместно использовать несколько ФБ 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 ФБ ПСБ, имеющую $ВОНЗ_{ср}$, равную $3{,}05 \cdot 10^{-4}$. Такая ФБ ПСБ дает снижение риска, равное приблизительно $3{,}3 \cdot 10^3$.

Было бы неправильно предполагать, что совместное использование двух таких систем приведет к сокращению риска, равному $10 \cdot 10^6$ ($3{,}3 \cdot 10^3 \cdot 3{,}3 \cdot 10^3$). 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), а также зависимости, вызванные синхронизированной контрольной проверкой, 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 нерезервированной системы, построенной на устройствах, отличающихся от применяемых в первой системе настолько, насколько это возможно (чтобы свести к минимуму проблемы, связанные с потенциально существующими общими причинами). Тем не менее

использование различающихся компонентов, может усложнить процесс обслуживания. Должен быть проведен тщательный анализ для выбора наилучшего решения для конкретного приложения.

Более подробное руководство по оценке зависимости и общих причин между слоями защиты приведено в МЭК 61511-3:2016 (приложение J).

А.9.2.7 Руководство по оценке зависимостей и влияния общих причин между слоями защиты приведено в МЭК 61511-3:2016 (приложение J).

А.9.2.8 Дополнительные требования не предусмотрены.

А.9.2.9 Дополнительные требования не предусмотрены.

А.9.3 Руководящие указания к «Требованиям к основной системе управления процессом как к слою защиты»

А.9.3.1 ОСУП при определенных условиях может считаться слоем защиты.

ФБ ПСБ не могут быть реализованы в ОСУП, если ОСУП не была спроектирована в соответствии с МЭК 61511-1:2016. В МЭК 61511-1:2016 (пункт 11.2.4) установлено: «Если не предполагается квалифицировать ОСУП как удовлетворяющую комплексу стандартов МЭК 61511, то ПСБ должна быть спроектирована так, чтобы ОСУП была отделена и независима до такой степени, чтобы не нарушалась полнота безопасности ПСБ». Для проектирования и управления ОСУП как ПСБ требуется применение требований к ее жизненному циклу, представленных в МЭК 61511-1:2016, включая требования к анализу опасностей и рисков, проектной документации, управлению функциональной безопасностью, подтверждению соответствия изменений и управлению изменениями.

Если не выполнены требования МЭК 61511-1:2016 (пункты 9.3.4 и 9.3.5) и не проведен дополнительный количественный анализ риска в соответствии с МЭК 61511-1:2016, то сокращение риска может быть распределено только на один слой защиты ОСУП. Подобный анализ нетривиален и включает в себя подробную оценку всего проекта ОСУП целиком, включая оборудование, программное обеспечение, коммуникации, источники питания, интерфейсы и т. п. Такой анализ, как минимум, должен учитывать целостность оборудования, разделение слоев защиты для предотвращения отказов по общим причинам, управление систематическими ошибками прикладного программирования, защиту доступа к аппаратному и программному обеспечению, управление изменениями, взаимодействия операторов, управление конфигурацией и периодическое подтверждение соответствия.

Если предполагается использование защитного слоя ОСУП, то следует провести оценку проекта и управления ОСУП для обеспечения такой вероятности возникновения отказов по общей причине, отказов общего типа и систематических отказов между слоем защиты ОСУП и инициирующим источником, а также между защитным слоем ОСУП и другими защитными слоями, которая является достаточно низкой по сравнению с общими требованиями к сокращению риска ОСУП.

А.9.3.2 Снижение риска менее чем в 10 раз может быть поручено защитным слоям ОСУП, без необходимости выполнять ее в соответствии с требованиями МЭК 61511-1:2016. Это позволяет использовать ОСУП для некоторого снижения риска без необходимости обеспечивать соответствие таких слоев защиты требованиям МЭК 61511-1:2016.

Заявленное для защитного слоя ОСУП снижение риска ≤ 10 следует обосновать путем анализа возможностей ОСУП по снижению риска (выполненного с помощью анализа безотказности или используя данные о прежнем использовании) и анализа процедур, используемых для конфигурирования, модификации и режимов эксплуатации и обслуживания.

Любой защитный слой ОСУП должен быть документально оформлен в функциональной спецификации, описывающей проектирование, обслуживание, контроль, проверку и работу ОСУП для достижения распределенного снижения риска.

Сбои, связанные с устройствами защитного слоя ОСУП, могут быть выявлены при выполнении процесса, автоматизированной диагностике, во время действий по обеспечению механической работоспособности или при инициации другого опасного события, но не того, где этот слой используется для снижения риска. Обнаружение сбоя должно привести к тому, что защитный слой ОСУП выполнит заданное действие для достижения или поддержания безопасного состояния. Заданное действие (реакция на сбой), требующееся для достижения или поддержания безопасного состояния, может состоять, например, из безопасного прекращения процесса (или той части процесса, которая полагается на неисправную подсистему ПСБ в снижении риска) или из определенной компенсирующей меры, обеспечивающей безопасную работу, пока завершаются ремонтные работы. Реакция на сбой должна быть реализована за время меньшее, чем время безопасности процесса.

Если распределение требований по снижению риска затрагивает защитный слой ОСУП, то важно обеспечить безопасность доступа и управление изменениями. Для управления доступом к защитному слою в ОСУП и его модификацией должно использоваться административное управление. Для обхода защитного слоя ОСУП (например, перевода функции ОСУП в ручной режим) требуется подтверждение, а компенсирующие меры должны быть готовы к использованию до осуществления обхода, чтобы обеспечить поддержание требующегося снижения риска. Должны быть предоставлены средства для подтверждения соответствия функций защитного слоя после того, как в ОСУП были внесены изменения, способные повлиять на работу защитного слоя ОСУП.

А.9.3.3 Дополнительные требования не предусмотрены.

А.9.3.4 Снижение риска, которое может быть возложено на защитный слой ОСУП, также ограничено степенью независимости между защитным слоем ОСУП, другими защитными слоями и источником опасного события.

Подробный анализ всей ОСУП в целом должен продемонстрировать, что устройства управления и защитные устройства в ОСУП достаточно независимы и разделены, причем настолько, что можно было бы сделать вывод, что вероятность того, что отказ ОСУП (как инициирующего источника) приведет к отказу защитного слоя ОСУП, достаточно мала. В таких случаях правильным может быть использование защитного слоя ОСУП, даже если ОСУП может служить инициатором опасного события.

Если проектирование и управление ОСУП не выполняются в соответствии с МЭК 61511-1:2016, то в случаях, когда ОСУП является источником нарушения, ответственность за одно опасное событие может возлагаться не более чем на один защитный слой ОСУП. На рисунке А.2 показана независимость защитного слоя ОСУП и источника нарушения в ОСУП.

Например, рассмотрим случай, в котором контур управления расходом выполняет роль источника, инициирующего нарушения. Этот источник включает в себя датчик расхода, логическое решающее устройство ОСУП и управляющий клапан. Для того чтобы назначить снижение риска сбросу давления в ОСУП, датчик давления следует соединить с независимым логическим решающим устройством ОСУП, приводящим в действие независимый исполнительный элемент (например, выпускной клапан факельной системы). Защитный слой может также быть аварийным сигналом и функцией реакции оператора.

Если заявляется, что ОСУП является источником, инициирующим нарушения, и защитным слоем для одного и того же опасного события, то проектирование и управление всего ОСУП (включая любые ее устройства, показанные на рисунке А.2) должно осуществляться таким образом, чтобы она могла поддерживать требующуюся от нее среднюю интенсивность отказов (например, $\leq 10^{-5}$/ч $\cdot \leq 10^{-1} = \leq 10^{-6}$/ч). Такое заявление должно быть подтверждено посредством проведения количественного анализа ОСУП, учитывающего вероятность возникновения отказов по общей причине и отказов общего вида между устройствами, образующими ОСУП. Отказы по общей причине, вызванные произвольными систематическими отказами, могут ограничить способность ОСУП в достижении заявленной средней интенсивности отказов.

Если проектирование и управление ОСУП не выполняются в соответствии с МЭК 61511-1:2016, то в случаях, когда инициирующий источник нарушения не связан с ОСУП, ответственность за одно опасное событие может возлагаться не более чем на два защитных слоя ОСУП. На рисунке А.3 показана независимость двух защитных слоев ОСУП, распределенных в ОСУП.

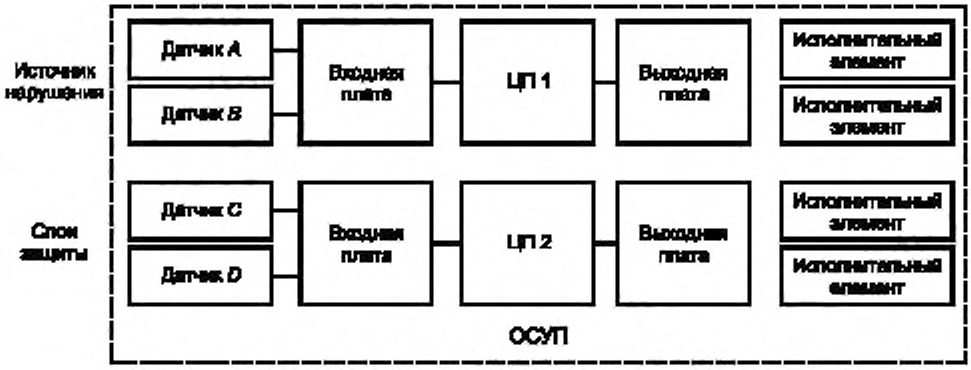


Рисунок А.2 — Независимость слоя защиты ОСУП и источника нарушений в ОСУП

А.9.3.5 Если заявляются два защитных слоя ОСУП для одного и того же опасного события, то проектирование и управление всей ОСУП (включая любые ее устройства, показанные на рисунке А.3) должно осуществляться таким образом, чтобы она могла поддерживать требующуюся от нее среднюю интенсивность отказов (например, $\leq 1/10 \cdot \leq 1/10 = \leq 1/100$). Условия и замечания в МЭК 61511-1:2016 (пункты 9.4.1 и 9.4.2) применимы к обоим слоям защиты ОСУП. Заявленное снижение риска должно быть подтверждено посредством проведения количественного анализа ОСУП, учитывающего вероятность возникновения отказов по общей причине и отказов общего вида между устройствами, образующими ОСУП. Отказы по общей причине, вызванные произвольными систематическими отказами, могут ограничить способность ОСУП в достижении заявленного сокращения риска.

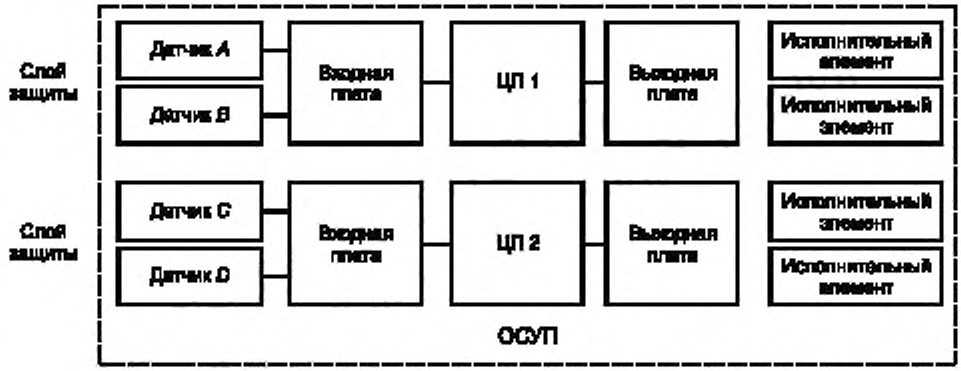


Рисунок А.3 — Независимость двух слоев защиты, распределенных в ОСУП

А.9.4 Руководящие указания к «Требованиям к предотвращению отказов по общей причине, отказов общего вида и зависимых отказов»

А.9.4.1 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.

А.9.4.2 При проведении оценки возможности появления отказов по общей причине, отказов общего типа и зависимых отказов применимы приведенные ниже положения. Широта, строгость и глубина оценки будет зависеть от значения УПБ предполагаемой функции. При УПБ 3 или УПБ 4 влияние отказов по общей причине, отказов общего типа и зависимых отказов может быть доминирующим. Поэтому следует рассмотреть:

- независимость между слоями защиты. Должен быть выполнен анализ режимов и влияния отказа, чтобы установить, может ли одиночное 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. 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 компонент ОСУП и ПСБ должно быть максимально физически разделено и подчинено функциональным потребностям, таким как точность и время отклика.

А.10 Спецификация требований к безопасности ПСБ

А.10.1 Цель

Разработка СТБ ПСБ является одной из самых важных процедур на всем жизненном цикле ПСБ. Именно с помощью такой спецификации пользователь может определить, как он хотел бы запроектировать и реализовать в ПСБ каждую из ФБ ПСБ.

Полное подтверждение соответствия ПСБ выполняется с использованием этой спецификации.

А.10.2 Руководящие указания к «Общим требованиям»

СТБ ПСБ может быть отдельным документом или сборником нескольких документов, включающим процедуры, рисунки или положения стандартов предприятия. Такие требования могут быть разработаны группой, занимающейся анализом опасности и риска, и/или самой группой разработчиков.

А.10.3 Руководящие указания к «Требованиям к безопасности ПСБ»

А.10.3.1 Как указано в МЭК 61511-1:2016, существует ряд требований к проекту, которые следует определить в проекте раньше, чем будут рассмотрены ФБ ПСБ, обеспечивающие желательную защиту.

Некоторые положения, посвященные СТБ, сводятся к следующему:

а) прежде всего следует определить ФБ ПСБ и ее значение УПБ. Примером ФБ ПСБ служит функция «Защитить реактор от превышения давления путем открытия клапанов сброса при высоком давлении». Типичное описание функции будет содержать следующее:

- параметры процесса, необходимые для того, чтобы выявить опасные условия.

Пример — Обнаружение возрастания давления выше определенного значения. Значение параметра, при котором начинаются защитные действия, устанавливается вне его рабочего диапазона, но оно не должно превышать значения, которое приводит к опасной ситуации. 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, и время, когда они должны быть выполнены. 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 нужно будет знать, что именно необходимо для успешной работы. Например, в нагревательных устройствах может оказаться достаточным снизить расход менее чем на 10 % на 1 мин. Другим примером может быть необходимость останова объекта в течение нескольких секунд;
- действия, не требующиеся для предотвращения опасного события, 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, не связанные с безопасностью, действия от действий, необходимых для предотвращения условия опасной ситуации, чтобы минимизировать стоимость и ограничить рабочий диапазон ПСБ тем, что крайне необходимо;
- любые выявленные состояния процесса или последовательности операций ПСБ, которые должны быть предотвращены, так как они могут приводить к опасным ситуациям. После завершения проектирования ПСБ требуется провести дополнительный анализ риска для рассмотрения возможности возникновения новых опасностей или дополнительных причин уже идентифицированных опасностей, вызванных частичными отказами или ложным срабатыванием ПСБ;

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 ее также следует установить. При выборе исполнительных элементов можно рассмотреть преимущества разнообразных решений (например, прекращение подачи продукта и расхода пара для снижения давления);

c) в самом начале можно определить требования к желательному интервалу проведения контрольной проверки с тем, чтобы они могли быть учтены в проекте ПСБ. Например, если контрольная проверка 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.

Следует рассмотреть:

- длительность испытания;
- состояние испытываемого устройства (в автономном режиме/в рабочем режиме);
- состояние процесса во время испытания;
- выявление отказов по общей причине;
- предотвращение ошибок (таких как сохранение изолированности ПСБ после выполнения испытания);
- требования к документации испытаний;
- требования к архивированию;
- необходимость гарантировать осведомленность управляющих о том, что запланировано;
- необходимость обеспечить осведомленность прилегающих и других подверженных влиянию территорий о приближающемся проведении испытания;
- техническую квалификацию и опыт персонала, разрабатывающего процедуры испытания;
- техническую квалификацию и опыт персонала, выполняющего процедуры испытания;

d) максимальное допустимое время реакции ПСБ начинается, когда процесс достигает условий срабатывания и заканчивается в последний момент, когда исполнительные элементы, достигающие своих безопасных состояний, все еще могут предотвратить опасность. 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 помещения для управления, так и на месте, то это следует указать в спецификации. Также следует определить любое требование, связанное с независимостью ключей ручного останова от логического устройства ПСБ;

e) следует установить 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 СТБ;

f) если существует заданная частота ложных срабатываний, то ее также следует указать как часть СТБ, 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 их также следует привести как часть СТБ;

i) следует установить виды отказов и реакцию ПСБ на обнаружение неисправностей. Например, передающее устройство может быть сконфигурировано 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. См. также МЭК 61511-1:2016 (подраздел 11.3), посвященный требованиям по обнаружению неисправностей.

А.10.3.2 Дополнительные требования не предусмотрены.

А.10.3.3 Данный пункт связан с руководящими указаниями к требованиям безопасности прикладного программирования. СТБ ППО идентифицирует минимальные возможности функционала ППО ПЭ, а также ограничивает разработку любого функционала, который может привести к небезопасной ситуации. Требования безопасности ППО, которые уже были указаны в требованиях для ПСБ, не должны повторяться отдельно, как СТБ для ППО.

СТБ ППО, как правило, учитывает системную архитектуру ПСБ. Системная архитектура определяет основные устройства, подсистемы ПСБ, встроенное ПО и ППО, а также то, как они взаимосвязаны и как достигаются требующиеся характеристики, в особенности полнота безопасности. Примеры модулей встроенного ПО включают в себя операционные системы, базы данных и коммуникационные подсистемы ПСБ. Примеры модулей ППО включают прикладные функции, дублируемые по всему предприятию.

Архитектура ППО должна также определяться лежащей в основе архитектурой подсистем(ы) ПСБ, предоставленной поставщиком(ами). Архитектура ППО не должна сводить на нет эффект от избыточности оборудования, например если процессор не избыточен (например, 1 из 1), а есть избыточность датчиков (например, 2 из 3), то соответствующее ППО должно обеспечивать требующееся голосование датчиков (т. е. 2 из 3).

Подробные требования по безопасности, предъявляемые к каждой функции безопасности ПБС, устанавливаются обычно с помощью логических диаграмм или причинно-следственных диаграмм [см. рисунок D.2 (приложение D)]. Во многих случаях для определения требований могут быть использованы языки программирования, предлагаемые поставщиком логического устройства. Обычно используют языки функциональных блок-диаграмм или язык причинно-следственных матриц. Специализированные форматы, такие как универсальный язык моделирования (UML), также являются доступными и полезными, когда предполагается использовать методы проверки моделей. Поставляемый выбранный язык должен подходить для конкретного применения. При определении подробных требований использование языков, предлагаемых поставщиком, 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.

Правильным решением может быть реализация дополнительных требований помимо необходимых для функционального поведения базовой отдельной ФБ ПСБ (например, для управления остановом и запуском установки), либо в ОСУП, либо в полностью отдельной от ФБ ПСБ части прикладной программы, с явными адресациями к ПСБ. В дополнение к этому ППО может включать в себя функции для реализации полной архитектуры ПСБ, сквозной диагностики и поведения в аварийных условиях. Например, архитектура датчиков (с правилами голосования: 1 из 2, 2 из 3 и т. д.), связанная с ФБ ПСБ, вместе с принципом безопасности «останов по отключению питания» или «останов по включению питания» определяет, как в ППО должно быть реализовано голосование датчиков. Важно обеспечить, что никакая комбинация дополнительных функций не смогла привести к переопределению основных прикладных функций безопасности.

Если для реализации функций ФБ ПСБ используются несколько ПСБ, то в документации должно быть объяснено, какие функции должны быть реализованы в каждой ПСБ. Если для реализации одной ФБ ПСБ используются несколько ПСБ (например, объединяются две ФБ ПСБ с более низким значением УПБ для достижения более высокого значения УПБ), то следует документально оформить взаимодействие и независимость каждой ФБ ПСБ [(см. приложение F (раздел F.4) и МЭК 61511-3:2016 (приложение J)].

Примечания

1 СТБ ППО идентифицирует минимальные возможности функций ППО ПЭ, а также ограничивает разработку любых функций, которые приведут к небезопасной ситуации.

2 Требования безопасности ППО, которые уже были установлены в требованиях для ПСБ, не должны повторяться.

3 Архитектура системы определяет основные устройства и подсистемы ПСБ встроенного ПО и ППО, а также то, как они взаимосвязаны и как достигаются требующиеся характеристики, в частности полнота безопасности.

4 Архитектура ППО может учитывать лежащую в основе архитектуру подсистем(ы) ПСБ, предоставленную поставщиками(ом). Архитектура ППО не должна сводить на нет эффект от избыточности оборудования — например, если процессор не избыточен (например, 1 из 1), а есть избыточность датчиков (например, 2 из 3), то соответствующее ППО должно обеспечивать требующееся голосование датчиков (т. е. 2 из 3).

5 ПСБ, как правило, состоит из трех архитектурных подсистем ПСБ: датчиков, логического решающего устройства и исполнительных элементов. Кроме того, подсистемы ПСБ могут иметь избыточные устройства для достижения требующегося уровня полноты.

6 Архитектура аппаратных средств ПСБ с избыточными датчиками может накладывать дополнительные требования на логическое решающее устройство ПСБ (например, реализацию логики 1oo2).

По любым привлекшим внимание противоречиям, разногласиям и упущениям в СТБ ПСБ следует обращаться к разработчикам ППО. Например, о влиянии порядка выполнения ФБ ПСБ в ППО. Другим примером может быть вопрос о реакции ППО на прекращение питания.

Примечания

1 Проектировщики ППО могут проверять информацию в спецификации для обеспечения однозначности, согласованности и понятности требований. Любые недостатки в указанных требованиях к безопасности могут быть идентифицированы для проектировщика ПСБ.

2 Так как требования к безопасности ППО и возможная архитектура ППО становятся более точными, то это может повлиять на архитектуру аппаратных средств ПСБ (см. рисунок А.4), и поэтому может быть важным тесное взаимодействие между разработчиком архитектуры ПСБ, поставщиком подсистемы ПСБ и разработчиком ППО.

СТБ ППО должна охватывать все функции, необходимые для всех режимов работы защищаемого процесса, включая разрешения на пуск, работу, остановку и дополнительно периодическое испытание ФБ ПСБ. Обычно это требует определения возможности перехода в режим техобслуживания, чтобы датчики и исполнительные элементы могли проверяться без останова процесса. Факторы, которые следует рассмотреть, включают:

a) функциональные и временные требования, необходимые для выполнения ФБ ПСБ, установленные пользователем;

b) интерфейсы ППО с процессом и персоналом;

c) связь между опасностями процесса и функциями, выполняемыми ППО;

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

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

f) платформу технических средств и встроенного ПО, на которых реализуется ППО, а также конфигурацию аппаратных средств и встроенного ПО;

g) опасности, которые могут появляться в процессе в результате функционирования системы, частью которой является ПО (например, не удовлетворяющие техническим условиям виды отказов аппаратных средств при отключении питания);

h) ограничения на методы и процедуры, которыми могли бы пользовать разработчики, полученные из инструкции по безопасности при обслуживании логического устройства;

i) проверки целостности и непротиворечивости данных, например сквозные проверки коммуникационных каналов, контроль выхода за указанные границы на входах датчиков, контроль выхода данных за указанные границы для параметров и использование разнообразия при выполнении прикладных функций;

j) критерии обнаружения и реакция на обнаруженные сбои аппаратных средств логического решателя и на отказы проверок целостности и логической непротиворечивости данных.

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



Рисунок А.4 — Связь системы, аппаратных средств ПСБ и прикладной программы ПСБ

А.10.3.4 В случае ФЯП устройств (например, датчиков с элементами ИИ, интеллектуальных преобразователей, графических панелей ЧМИ) требования для конфигурации устройств могут быть установлены как часть СТБ.

А.10.3.5 Разделы B.1, F.17, F.20 и G.2 содержат дополнительные руководящие указания по реализации требований МЭК 61511-1:2016 (пункт 10.3.3) и примерный вид требований к безопасности ППО. Предоставленные дополнительные руководящие указания будут различаться в зависимости от охвата области применения, языка ППО и прикладного процесса, сложности, что позволяет отразить разнообразие существующих возможностей, которые, как правило, позволяют осуществлять подобную реализацию.

А.10.3.6 Пример структурирования требований безопасности ППО см. приложение В (пункт В.3.3.1) и приложении F (шаг F.3).

А.11 Проектирование и разработка ПСБ

А.11.1 Цель

Цель раздела А.11.1 — предоставить руководящие указания по разработке ПСБ. Каждая ФБ ПСБ имеет свой собственный УПБ. Устройство ПСБ, например логическое решающее устройство, может использоваться несколькими ФБ ПСБ с различными УПБ.

А.11.2 Руководящие указания к «Основным требованиям»

А.11.2.1 Дополнительные требования не предусмотрены.

А.11.2.2 Руководящие указания к ППО см. в приложении А (пункт 12.2.4).

А.11.2.3 Если ППО ПСБ должно реализовывать ФБ ПСБ с различными УПБ, то их следует четко промаркировать. Это позволит сделать ППО каждой ФБ 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.

А.11.2.4 Иногда ОСУП дополнительно использует устройства ПСБ по эксплуатационным причинам. В МЭК 61511-1:2016 (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:

а) чтобы уменьшить число отказов по общей причине, отказов общего типа и систематических отказов, сводя к минимуму влияние отказа ОСУП на ПСБ.

Примечание — Разделение ПСБ и ОСУП согласуется с концепцией слоев защиты. Отдельная ПСБ является независимым слоем защиты в тех случаях, когда происходит отказ ОСУП;

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

Примечания

1 Обычно к ПСБ предъявляют более жесткие требования, чем к ОСУП, и назначение ОСУП не связано с выполнением таких же жестких требований, как предъявляемые к ПСБ. Однако неуправляемые изменения в ОСУП могут привести к увеличению запросов на срабатывание ПСБ.

2 Разделение ПСБ и ОСУП позволяет осуществлять раздельное обслуживание этих систем, часто различным обслуживающим персоналом.

3 Если ОСУП объединена с ПСБ, то для соблюдения требований к управлению изменениями ПСБ и управлению конфигурацией можно ограничить доступ к программированию или функциям конфигурации ОСУП.

4 Могут быть предоставлены средства для подтверждения соответствия ПСБ после внесения изменений в какие-либо устройства, разделяемые ОСУП и ПСБ;

c) чтобы облегчить идентификацию и управление ПСБ-устройствами, делая подтверждение соответствия и оценку функциональной безопасности ПСБ более простой и понятной;

d) для поддержки защиты доступа и повышения кибербезопасности ПСБ таким образом, чтобы внесение поправок в функции или данные ОСУП не влияло на ПСБ.

Примечания

1 Управление разделяемыми интерфейсами и устройствами может осуществляться как управление компонентами и устройствами ПСБ, если конфигурация аппаратных средств и ПО не обеспечивает функциональное разделение.

2 Следует уделить особое внимание ограничениями на запись, чтобы предотвратить неавторизированную или непреднамеренную запись в ПСБ;

e) чтобы сократить число исследований, которые требуются для того, чтобы обеспечить надлежащие проектирование, верификацию и управление ПСБ и ОСУП.

Примечание — Если отказ общего оборудования может вызвать запрос к ПСБ, то можно провести анализ, чтобы убедиться, что средняя полная интенсивность отказов соответствует ожидаемой. Такой анализ может охватывать все устройства ПСБ и ОСУП, такие как датчики, логические решающие устройства, исполнительные элементы, средства коммуникаций данных, сервисные программы, станции операторов и инженерные рабочие станции.

Если какое-либо устройство ОСУП разделено между ОСУП и ПСБ, то следует провести дополнительный анализ для демонстрации того, что в процессе проектирования и управления этим устройством ОСУП:

- обеспечивает выполнение функциональных требований к функции ОСУП и к ФБ ПСБ.

Примечание — Отказ какого-либо внешнего для ПСБ аппаратного средства или программного обеспечения не может повлиять на корректное функционирование ФБ ПСБ;

- соответствует требованиям к полноте, необходимой для достижения целевой средней интенсивности отказов для объединенных вместе систем.

Примечания

1 Отказ устройства ОСУП не может стать источником, инициирующим опасное событие или опасный отказ (или прекращение/обход) ФБ ПСБ, защищающей от конкретного события, для которого она была создана, если нет резервного устройства, способного запустить ПСБ. Для оценки влияния использования ОСУП и ПСБ общего устройства может быть проведен анализ.

2 Вероятность возникновения отказов по общей причине, отказов общего типа или зависимых отказов, таких как засорение свинцовых линий, обслуживающая деятельность, включая обходы, неправильно управляемые запорные клапаны линии и т. д., может быть оценена и определена как достаточно низкая;

- управление осуществляется в соответствии с МЭК 61511-1:2016, включая проведение контрольной проверки, защиту доступа и управление изменениями.

Разделение между ПСБ и ОСУП может быть реализовано по принципу идентичности или по принципу разнообразия. Применение принципа разделения идентичного 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 разделением идентичного (идентичное разделение), которое помогает при случайных отказах, разделение с разнообразием дает дополнительный выигрыш в снижении вероятности систематических отказов, влияющих на несколько каналов одновременно, и/или отказов по общей причине и тем самым сокращает отказы, коррелированные для нескольких каналов.

Разделение идентичного 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 устройства, не использовавшиеся ранее данной эксплуатационной организацией.

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

- засорение разъемов измерительных цепей и линий импульсных сигналов;
- коррозия и эрозия;
- неисправности аппаратных средств, вызванные окружающей средой;
- ошибки программного обеспечения;
- энергоснабжение и источники электропитания.

Примечание — Средства обеспечения (например, энергоснабжение) могут подвергаться анализу традиционными методами исследования безотказности. Применение коэффициента «бета» не относится к данному случаю.

- ошибки человека.

Существуют четыре зоны, в которых обычно следует обеспечить разделение между ПСБ и ОСУП:

- датчики на объекте;
- исполнительные элементы;
- логическое устройство;
- 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 и
- работами, выполняемыми на ОСУП (например, при ее техническом обслуживании, эксплуатации или модификации).

Если необходимы процедуры, обеспечивающие отсутствие опасных воздействий на ПСБ, то разработчику ПСБ следует 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.

Примечание — 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 (т. е. 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 61511-1:2016 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.

Общие датчики (например, передающее устройство, анализатор и переключатель) должны питаться от ПСБ. Следует также рассмотреть компенсирующие меры, применяемые в периоды, когда общее (разделяемое) устройство неисправно по причине обнаруженных отказов, обслуживания или проведения испытаний. Чтобы добиться более высокого значения УПБ, обычно необходимо использовать отдельные датчики ПСБ с идентичным или разнообразным резервированием, чтобы удовлетворить требуемой полноте безопасности.

Если в ПСБ используется отдельный одинарный датчик, то может оказаться предпочтительным использовать его и для ввода сигнала в ОСУП через подходящие разделители или другими способами, гарантирующими, что никакой отказ ОСУП не приводит к опасному отказу ПСБ. 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 или другими способами, гарантирующими, что никакой отказ ОСУП не приводит к опасному отказу ПСБ. При этом, применяя в ОСУП соответствующие алгоритмы, такие как «среднее из трех», можно повысить безопасность, сокращая интенсивность запросов к ПСБ.

В случае УПБ функций безопасности ПСБ равного УПБ 2, УПБ 3 или УПБ 4, чтобы выполнить требования к отказоустойчивости аппаратных средств и добиться необходимой полноты безопасности в ПСБ обычно необходимо использовать отдельные датчики ПСБ с идентичным или разнообразным резервированием.

b) Исполнительные элементы

Аналогично датчикам использование единого исполнительного элемента как в ОСУП, так и в ПСБ требует проведения дальнейшего рассмотрения и анализа, так как отказ единого исполнительного элемента может привести к опасной ситуации.

Примечание — Например, единый клапан, используемый и для ОСУП, и для ПСБ может привести к запросу в случае, когда происходит отказ открытого клапана, и к опасному отказу ПСБ, если клапан не закрывается, как это определено, в случае поступления запроса.

В случаях, когда как функциями ОСУП, так и функциями ПСБ используется единый исполнительный элемент, требования МЭК 61511-1:2016 обычно выполняются только в том случае, если диагностика исполнительного элемента может значительно снизить интенсивность опасных отказов, а ПСБ способна за установленное время перевести процесс в безопасное состояние.

На практике достичь этого для приложений с УПБ 1 трудно, даже когда проектирование общего исполнительного элемента гарантирует то, что действие ПСБ перекрывает действие ОСУП. Следует также рассмотреть компенсирующие меры, применяемые в периоды, когда разделяемое устройство неисправно по причине обнаруженных отказов, обслуживания или проведения испытаний. В случае значения УПБ функций безопасности ПСБ равного УБП 2, УПБ 3 или УПБ 4, чтобы добиться требующейся полноты безопасности в ПСБ, обычно необходимо использовать отдельные исполнительные элементы ПСБ с идентичным или разнообразным резервированием. Перекрывание действия ОСУП действием ПСБ, например, может быть достигнуто для пневматического клапана при непосредственном соединении ПСБ с соленоидом, приводимым в действие клапаном, который выполняет дренаж воздуха из исполнительного механизма клапана, находящегося, например, между исполнительным механизмом и позиционером клапана. В случае клапанов с электрическим управлением разводка может быть выполнена так, что ПСБ будет помещать клапан управления в безопасное состояние и поддерживать его в нем до переустановки.

Если применяются резервные исполнительные элементы, то исполнительные элементы могут быть соединены как с ПСБ, так и с ОСУП. Даже при наличии избыточных исполнительных элементов следует рассмотреть отказы по общей причине, возникающие между ОСУП и ПСБ. Проведение испытаний избыточных клапанов с временным сдвигом, реализуя соответствующую процедуру, может сократить последствия отказов по общей причине.

Если исполнительным элементом является клапан, то следует дополнительно рассмотреть следующее:

- клапан проектируется таким образом, что отказ ОСУП, способный привести к тому, что ПСБ не может осуществлять действия с общим клапаном, невозможен;
- проект клапана таков, что он функционально совместим как с обслуживанием ПСБ, так и с обслуживанием ОСУП.

Примечание — Этого может быть сложно добиться, так как многие клапаны ОСУП устанавливаются «открытыми для потока», а многие клапаны ПСБ устанавливаются «закрытыми для потока». Требования к питанию исполнительного механизма клапана ПСБ могут отличаться от требований для клапана управления;

- требования к останову.

Примечание — Уровень процесса утечки в клапане управления может считать приемлемым, если он не влияет на способность ФБ ПСБ выполнять установленную для нее функцию и предотвращать опасность;

- проект общего исполнительного элемента должен обеспечить, чтобы действие ПСБ перекрывало действие ОСУП;
- эксплуатационную безотказность клапанов при их применении в аналогичных процессах;
- виды опасных отказов клапанов;
- эксплуатационные условия, обеспечивающие полноту ПСБ.

Примечание — Например, клапаны обхода могут быть зафиксированы в закрытом состоянии и могут находиться под контролем процедур управления и аналогично клапаны, расположенные в обратных трубопроводах (например, гидравлических), могут быть пружинными, зафиксированными в закрытом состоянии;

- требования к контрольной проверке.

Примечание — Можно рассмотреть требования к проведению любых испытаний клапана при неполном ходе или на действующем процессе и то, как они могут влиять на работу.

c) Логическое решающее устройство

Возможности достигнуть разделения и независимости с помощью логических решающих устройств ОСУП или ПСБ различаются в зависимости от технологии, используемой в приложении (т. е. логическое решающее устройство может быть электрическим, электронным и программируемым электронным).

Электрические технологии

Многие промышленные процессы ранее и в настоящее время применяют ОСУП на основе пневматической технологии и ПСБ на основе электрической технологии. Разделение и независимость в таких применениях легко достижимы с помощью этих технологий, так как для их реализации требуются различные конструкции, различное размещение оборудования и отдельные коммуникации.

Электронные технологии

Многие промышленные процессы ранее и в настоящее время применяют ОСУП на основе электронной технологии, не обладающей возможностями реализации на средствах встроенного программирования, а ПСБ — на основе электрической технологии. Разделение и независимость в таких применениях легко достижимы с помощью этих технологий. Использование электронных ПСБ без встроенных программируемых электронных технологий также является целесообразным методом.

Программируемые электронные технологии (ПЭ)

Некоторые приложения для своих ОСУП применяют ПЭ-технологии и электрические технологии для своих ПСБ. Эти конфигурации, по сути, являются разделенными и независимыми, так как коммуникации разводятся отдельно, а универсальность физической реализации не дает преимуществ.

В настоящее время предпочтительный технический план для ОСУП/ПСБ в промышленном процессе заключается в использовании ПЭ-технологии как для ОСУП, так и для ПСБ. Подобная конфигурация предоставляет максимальную гибкость, так как она позволяет удаленно изменять ППО программы ОСУП и ПСБ, а также осуществлять обмен информацией между ОСУП и ПСБ. К сожалению, в случаях поддержания разделения и независимости между ОСУП и ПСБ эти характеристики могут иметь обратный эффект, чего можно избежать проведением анализа на стадиях проектирования жизненного цикла системы безопасности и демонстрацией функциональной безопасности (например, за счет разнообразия технологий).

СТБ [МЭК 61511-1:2016 (раздел 10)] содержит руководящие указания по достижению разделения и независимости ОСУП и ПСБ с такой технологией. Усилия в данной области были подкреплены за счет введения новых средств, обеспечивающих дополнительную защиту для ОСУП и ПСБ. Практические конфигурации систем управления ОСУП/ПСБ и средства обеспечения защиты, предоставляющие различные уровни разделения и независимости между ОСУП и ПСБ, см. в ISA TR84.00.09:2013.

Некоторые поставщики логических решающих устройств ПЭ предоставляют контроллеры, в которых ОСУП и ПСБ размещены в одном физическом корпусе. Перед применением такого подхода следует провести тщательный анализ руководства по безопасности логического решающего устройства и того, как его требования к работе и обслуживанию ОСУП и ПСБ соответствуют критериям управления безопасностью средств процесса и СТБ.

d) 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, рекомендуется применять строгие правила маркировки и процедуры обслуживания, способные минимизировать возможность ошибок, вызванных отключением ПСБ на период обслуживания.

Примечание — Останов по включению питания выполняется с помощью цепей ПСБ, выходы и устройства которой 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 систем останова по включению питания, так и для систем останова по отключению питания, если не потребуется их разделение по другим причинам (например, для снижения электромагнитных помех). Для систем останова по включению питания следует предусмотреть дополнительную противопожарную защиту кабельных лотков, проходящих в огнеопасных зонах.

А.11.2.5 Все операторы, сотрудники обслуживающего персонала, контролеры и руководители играют свою роль в обеспечении безопасного функционирования объекта. Однако люди могут совершать ошибки или могут быть не способны справиться с задачей, и как приборы и оборудование, они подвержены «сбою» или «отказу».

Вследствие этого деятельность человека тоже влияет на разработку и полноту системы. Для производственного 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 накопленной статистике и результатам исследований их 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:

CCPS/AIChE Human Factors Methods for Improving Performance in the Process Industries (1st edition), John Wiley & Sons (2007), ISBN 0 4701 1754 0;

Guidelines for Preventing Human Error in Process Safety (1st edition), John Wiley & Sons (2004), ISBN 08169 0461 8;

CCPS/AIChE Guidelines for Chemical Process Quantitative Risk Analysis (second edition), New York: American Institute of Chemical Engineers (2000), 0 8169 0720 X;

HSE Reducing error and influencing behavior, HSG48, Health and Safety Executive, London (2009), ISBN 978 0 7176 2452 2.

ISA TR84.00.04:2015 part 1, Annex B, Guidelines on the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511).

А.11.2.6 Дополнительные требования не предусмотрены.

А.11.2.7 МЭК 61511-1:2016 (пункт 11.2.7) 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.

Пример функции, обеспечивающей сохранение процесса в безопасном состоянии после его перевода в это состояние, приведен на рисунке F.11, лист 4, строка 1.

А.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. Средства ручного управления исполнительным элементом ПСБ могут учитываться при реализации требований полноты функции безопасности, но следует надлежащим образом рассмотреть значимые человеческие факторы, а также отказы по общей причине. Требования к ручному останову обычно устанавливают в СТБ.

При необходимости процедура аварийного останова в чрезвычайной ситуации может быть включена в ПЭ логическое решающее устройство. В некоторых случаях ручной останов может создать для объекта дополнительный риск (например, там, где требуется установление упорядоченной последовательности останова); в таком случае ручной останов может служить входными данными для ПСБ, чтобы та выполнила установленный поэтапный останов ПСБ (например, когда требуется выполнить последовательность действий по останову), если такое решение представляется подходящим группе специалистов по анализу опасностей и рисков.

А.11.2.9 В МЭК 61511-1:2016 (пункт 11.2.9) указано на необходимость выполнения анализа независимости между ПСБ и другими слоями защиты, а не только между ПСБ и ОСУП [см. МЭК 61511-1:2016 (рисунок 9)].

Проведение контрольной проверки между ПСБ и защитным слоем с временным сдвигом поможет снизить вероятность возникновения совпадающих по времени отказов.

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 61511-1:2016.

Если один тип аппаратных средств используется как для ОСУП, так и для ПСБ, а отказ общего оборудования по общей причине может привести к опасному событию, вызывающему запрос на ПСБ, то следует провести анализ, позволяющий убедиться в том, что полная средняя интенсивность отказов соответствует ожидаемой интенсивности. Необходимо установить опасности, связанные с опасными отказами общего оборудования.

В МЭК 61511-1:2016 (пункт 11.2.9) также указывается на необходимость обеспечить в проекте интерфейса между ПСБ и другими системами поддержку требующейся независимости, т. е. спроектированная в ПСБ не связанная с безопасностью независимость не должна подвергаться негативному влиянию со стороны ОСУП. Например, если данные приложения, сгенерированные для использования в ОСУП или в других не связанных с ПСБ устройствах, а также в инструментальных средствах применяются при проектировании ПСБ, т. е. вероятность распространения некоторого общего отказа от одной системы на другую. Другим примером может быть ППО, позволяющее реализовать в системе механизм перекрытия управления ОСУП без отдельного «разрешающего» переключателя, отделенного от ОСУП. Другие примеры связаны с созданием «зеркального» представления, когда данные приложения «утекают» в другую систему и перекрывают запуск.

А.11.2.10 В МЭК 61511-1:2016 (пункт 11.2.10) представлены предупреждающие руководящие указания по применению общих устройств как для ОСУП, так и для ПСБ. Слова «достаточно низка» в примечании к пункту 11.2.10 МЭК 61511-1:2016 означают, что интенсивность опасных отказов совместно используемого оборудования, объединенная с вероятностью отказов других (отличных от ПСБ) слоев защиты, соответствует принятому корпорацией критерию допустимого риска.

А.11.2.11 В тех случаях, когда исполнительные элементы при потере питания не переходят в безопасное состояние (например, системы останова по включению питания), следует рассмотреть достаточность средств ручного управления для перевода объекта в такое состояние.

А.11.2.12 Дополнительные требования не предусмотрены.

А.11.2.13 Целью руководства по безопасности является документальное оформление всей необходимой информации, связанной с тем, как устройство, подсистема ПСБ или система могут применяться безопасным образом.

Примечания

1 Руководство по безопасности предназначено охватить информацию как от производителя, так и от конечного пользователя и может быть надлежащим образом структурировано, например на разделы по аппаратным средствам, встроенному ПО и ППО.

2 Для элементов, связанных с МЭК 61508, вкладом производителя является инструкция по безопасности, соответствующая требованиям МЭК 61508-2:2010 (приложение D).

Руководство по безопасности должно включать, но не ограничиваться следующей информацией:

a) краткое описание элемента и его топологии (схемы), включая аппаратные средства и ПО.

Примечание — Любое снижение или увеличение отказоустойчивости аппаратных средств в соответствии с МЭК 61511-1:2016 (пункт 11.4.4), может быть обосновано в руководстве по безопасности;

b) идентификация ревизий и ограничений, связанных с ППО.

Примечание — Более подробную информацию о программировании приложений можно найти в разделе 12 МЭК 61511-1: 2016;

c) идентификация ревизий аппаратных средств и встроенного ПО;

d) описание на уровне операций, включая определение безопасного состояния и отказоустойчивой работы.

Примечание — Можно рассмотреть различные режимы работы, такие как запуск, нормальная работа, замедленная работа и режим запросов;

e) список всех допущений, связанных с работой, обслуживанием и испытаниями.

Примечание — Эти допущения могут включать условия использования, предупредительное обслуживание, указания по проведению контрольной проверки, а также последующие действия при сбоях диагностики;

f) список всех предельных значений и ограничений, связанных с функцией(ями) безопасности элемента.

Примечание — Предельные значения и ограничения включают (но этим не ограничиваются) настройку конфигурации, ограничения на условия окружающей среды и процесс;

g) режимы отказов и соответствующие интенсивности отказов устройств(а).

Примечание — Интенсивности отказов могут быть получены у производителя или из опыта эксплуатации;

h) другие параметры, требующиеся для анализа безотказности, такие как полезный срок службы, времена ремонта и, если необходимо, интенсивности отказов по общей причине;

i) реакция(и) (или поведение) на обнаруженные отказы и предупреждения;

j) инструкции производителя по эксплуатации и обслуживанию и, если применимы, рекомендации по интервалам контрольных проверок;

k) меры, принятые для предотвращения и управления систематическими отказами, включая отказы ПО и, если применимы, отказы по общей причине;

l) информация о том, как каждый режим отказа может быть выявлен с помощью обычных функциональных проверок и диагностики, включая интервалы диагностических проверок;

m) руководство по безопасности должно включать ограничения на использование устройства вместе с подробностями конфигурации, интерфейсов, установки, диагностики, средним временем ремонта, реакцией на сбои, а также интервалами проведения испытаний и ограничениями языка ППО.

A.11.2.14 Дополнительные требования не предусмотрены.

A.11.3 Руководящие указания к «Требованиям к поведению системы при обнаружении отказа»

A.11.3.1 Дополнительные требования не предусмотрены.

A.11.3.2 Дополнительные требования не предусмотрены.

A.11.4 Руководящие указания к «Требованиям к отказоустойчивости аппаратных средств»

A.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, так как такие отказы не происходят в одни и те же моменты времени (главным образом в аппаратных средствах).

МЭК 61511-1:2016 определяет, что промышленные процессы нуждаются в многоуровневых системах безопасности, и принимает концепцию УПБ для каждого слоя защиты в зависимости от требующегося снижения риска возникновения конкретного опасного события. Так как слои защиты различаются, то нельзя утверждать, что все УПБ обеспечивают отказоустойчивость. Однако при выборе архитектуры системы безопасности для конкретного УПБ важно гарантировать, 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 безотказности.

Требования, представленные в МЭК 61511-1:2016 (пункт 11.4.1), 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:

a) сложность устройств, используемых в ПСБ или подсистеме ПСБ;

b) устройство будет более устойчиво к систематическим сбоям во время работы, если было получено четкое понимание характера его сбоев и он был учтен в выборе устройства, установке и конфигурировании устройства, а также в определении методик работы и обслуживания;

c) данные об отказах из опыта эксплуатации;

d) уровень полноты безопасности, необходимый для используемого приложения;

e) мера того, насколько неисправности ведут к нарушению условий безопасности или насколько они могут быть выявлены диагностикой так, чтобы можно было предпринять определенные действия;

f) число ложных срабатываний, вызванных безопасными отказами, которое, как правило, возрастает с повышением отказоустойчивости, что, в свою очередь, может привести к новой опасности или служить дополнительной причиной для уже существующей опасности, или же они становятся недопустимыми в зависимости от целевой интенсивности ложных срабатываний;

g) отказы по общей причине и систематические отказы, которые могут значительно снизить преимущества, которые ожидаются от отказоустойчивости;

h) реально достигаемая отказоустойчивость, которая может быть снижена до нуля, если восстановление после опасных отказов занимает слишком много времени (например, архитектура 2oo3, сбои в которой не исправляются менее чем за 0,8 MTTF, хуже, чем архитектура 1oo1);

i) возможность резервирования, которая может не быть осуществима для всех функций;

j) различные ФБ ПСБ, которые реализует ПСБ (или ее подсистема).

Примечания

1 От подсистем ПСБ может потребоваться выполнение ими функций при высокой или низкой частоте запросов в зависимости от режима работы. Может быть установлено, что ФБ ПСБ должна закрывать клапан в ответ на определенные отклонения от процесса. Как для случаев ручной, так и для автоматической перенастройки ПСБ может сохранять клапан в безопасном состоянии до тех пор, пока ей не будет приказано выполнить обратное. Требования к отказоустойчивости аппаратных средств при работе ПСБ в случае обработки опасного события могут быть установлены в соответствии с режимом низкой частоты запросов, а в случае работы ПСБ во время останова — в соответствии с режимом высокой частоты запросов.

2 Минимальная отказоустойчивость аппаратных средств определена для сокращения числа возможных недостатков в проекте ФБ ПСБ, связанных с числом допущений, сделанных при проектировании ФБ ПСБ, и отсутствием точно установленной интенсивности отказов устройств, используемых в различных приложениях процесса.

А.11.4.2 Для применения требований к отказоустойчивости аппаратных средств необходимо хорошее понимание концепции подсистемы ПСБ [см. МЭК 61511-1:2016 (пункт 3.2.78)].

Требования к отказоустойчивости аппаратных средств применяются ко всей ПСБ или к подсистемам ПСБ, от которых требуется выполнение ФБ ПСБ, а не к отдельным устройствам внутри подсистемы. Например, в случае сенсорной ПСБ-подсистемы, состоящей из нескольких резервных датчиков, требования к отказоустойчивости применяются к сенсорной ПСБ-подсистеме в целом, а не к отдельным датчикам.

А.11.4.3 В МЭК 61508 были рассмотрены факторы, описанные в пункте А.11.4.1, и была установлена допустимая величина отказов, которая требуется в МЭК 61500-2:2010, посредством двух путей, называемых 1_H и 2_H. При подготовке настоящего стандарта, ориентированного на сектор промышленных процессов, было принято, что путь 2_H лучше адаптирован под сектор промышленных процессов. Тем самым требования к отказоустойчивости в МЭК 61511-1:2016 основаны на пути 2_H МЭК 61508-2:2010. Путь 1_H из МЭК 61508-2:2010 может применяться как альтернативный. Следует отметить, что при разработке подсистем ПСБ, чтобы удовлетворить требованиям готовности процесса (например, целевой интенсивности ложных отказов), может потребоваться большее резервирование компонент, чем это указано в МЭК 61511-1:2016 (таблица 6).

Выполнение оценки путем 1_H для достижения соответствия МЭК 61511 должно учитывать целевую рабочую среду. В случае внешних устройств рабочая среда, как правило, оказывает большее влияние на подтверждаемую интенсивность отказов, которая также может влиять на распространение безопасных и опасных отказов.

А.11.4.4 Отказоустойчивость может обеспечиваться неидентичными резервными устройствами (например, когда реализовано разнообразие в резервировании). Отказоустойчивость аппаратных средств ПСБ в действительности определяется самой короткой комбинацией независимых сбоев устройств, которая приводит к общему опасному сбою данной ПСБ. Если ПСБ была разделена на независимые подсистемы ПСБ, то значение отказоустойчивости ее аппаратных средств равно минимальному значению отказоустойчивости аппаратных средств ее ПСБ-подсистем.

Требования к отказоустойчивости аппаратных средств могут быть ослаблены, когда ПСБ ремонтируется в неавтономном режиме. Тем не менее ключевые параметры, связанные с любым ослаблением требований, должны быть предварительно оценены (например, выполнено сравнение длительности MTTR или испытания с вероятностью возникновения запроса во время ремонта или испытаний). Это должно быть включено в вычисление измерений вероятности ($ВОНЗ_{ср}$, ВОВЧ), связанных с принятыми УПБ.

В зависимости от выбранной архитектуры снижение отказоустойчивости аппаратных средств может привести к повышению риска возникновения опасного события. Риск продолжения работы при известном сбое должен быть оценен для того, чтобы определить необходимость компенсирующих мер.

Определенные единичные отказы/сбои могут быть исключены, если очевидно, что вероятность их возникновения очень низка благодаря свойствам, присущим проекту и конструкции [см. МЭК 61511-1:2016 (подраздел 3.2)], т. е. их вклад в целевую меру отказов суммы опасных отказов последовательно соединенных устройств, для которой требуется исключение сбоев, не должен превышать 1 %. Любые подобные исключения сбоев/отказов должны быть обоснованы и документально оформлены. В таком случае обычно нет необходимости ограничивать полноту безопасности любых ФБ ПСБ, несущих эти единичные отказы/сбои (основываясь на отказоустойчивости аппаратных средств).

Примечания

1 В случае внешнего проводного соединения является распространенной практикой допускать, что данные внешнего устройства включают в себя внешнее проводное соединение от внешнего устройства до окончания линии, так как внешнее проводное соединение обладает гораздо более низкой интенсивностью опасных необнаруженных отказов, чем внешнее устройство. В общем, отказоустойчивость аппаратных средств обеспечена для проводного соединения только в том случае, когда отказоустойчивость аппаратных средств необходима для внешнего

устройства. Для других форм коммуникаций сигналов может потребоваться определение отказоустойчивости аппаратных средств для средств передачи сигнала отдельно, так как интенсивность опасных необнаруженных отказов в рабочей среде выше. Для таких форм коммуникаций средства коммуникаций сигналов могут нуждаться в большей отказоустойчивости аппаратных средств, чем та, которая требуется для внешних устройств.

2 Устройства системы, выполняющие уникальные функции, которые обычно не требуются для успешной работы ПСБ (например, интерфейсы оператора, инженерные станции, системы управления обслуживанием и устройства регистрации данных), чья вероятность негативного влияния на корректную работу ПСБ мала, как правило, не учитываются в анализе.

Если определенные отказы могут быть исключены (в соответствии с вышеуказанными критериями), то минимальная отказоустойчивость аппаратных средств (HFT) может быть сокращена [см. МЭК 61511-1:2016 (пункт 11.4.6)].

А.11.4.5 Таблица 6 в МЭК 61511-1:2016 устанавливает минимальную допустимую отказоустойчивость для систем и подсистем ПСБ. Требование отказоустойчивости зависит от требуемого значения УПБ для ФБ, реализуемой ПСБ. При установлении отказоустойчивости аппаратных средств разрешено принимать допущения, что ПСБ или подсистема ПСБ 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 отказоустойчивости аппаратных средств также не требуется.

А.11.4.6 Отказоустойчивость является предпочтительным решением для получения необходимой уверенности в том, что была достигнута надежная архитектура. В случаях применения МЭК 61511-1:2016 (пункт 11.4.6) целью обоснования является демонстрация того, что предложенная альтернативная архитектура с пониженной отказоустойчивостью аппаратных средств является эквивалентным или лучшим решением (например, посредством других подлежащих верификации средств, таких как сертификация или нечто подобное). Оно должно предоставлять свидетельства того, что:

a) выполнение требований отказоустойчивости аппаратных средств в МЭК 61511-1:2016 (пункт 11.4.5) может привнести дополнительные отказы, которые повлекут за собой понижение общей безопасности, и

b) если отказоустойчивость аппаратных средств снижена до нуля, то виды отказов, идентифицированные в ПСБ, выполняющей ФБ, могут быть исключены, так как интенсивность(и) опасных отказов идентифицированного(ых) вида(ов) отказов очень низкие в сравнении с целевой мерой отказов для рассматриваемой ФБ ПСБ.

Примечания

1 Примеры реализации снижения отказоустойчивости аппаратных средств включают: организацию резерва [например, аналитическая избыточность — замена выхода отказавшего датчика на вычисления физических результатов на выходах других датчиков; использование более надежных элементов той же технологии (если доступны)]; переход на более надежную технологию; снижение последствий отказов по общей причине, используя разные технологии; увеличение границ рабочих режимов проекта; внесение ограничений на условия окружающей среды (например, для электронных компонентов); снижение неуверенности при оценке безотказности посредством сбора большего числа отзывов об эксплуатации или экспертных мнений и т. п.

2 Отказоустойчивость аппаратных средств эффективна только тогда, когда имеется высокая вероятность обнаружения отказа и ремонта одной части перед отказом других резервных частей. При работе с системами, расположенными в удаленных или труднодоступных местах (например, подводная ПСБ), где обслуживание затруднено (если вообще возможно), польза от отказоустойчивости аппаратных средств снижается. В подобных случаях ПСБ может быть спроектирована с повышенной устойчивостью к отказам, используя скорее более безотказные встроенные компоненты, чем отказоустойчивость аппаратных средств.

3 Общая безопасность процесса может быть снижена, если в целях повышения отказоустойчивости установлен дополнительный промышленный комбинированный пускатель двигателя для пуска при полном напряжении (т. е. комбинация выключателя с плавким предохранителем и электромагнитного пускателя с управляющим трансформатором и реле управления, обеспечивающая также защиту от короткого замыкания и перегрузки с помощью подключения и отключения питания к трехфазному реверсивному или нереверсивному двигателю). Это связано с увеличением числа компонентов при использовании нескольких пускателей двигателя в противовес использованию одного пускателя двигателя, приводящему:

- к большему числу ложных срабатываний;
- большей сложности проекта (например, увязка защиты от перегрузки и короткого замыкания) и увеличению числа трудностей, связанных с получением полноценных знаний о поведении и режимах отказов резервных пускателей двигателя;
- возросшей потребности в обслуживании, контроле и испытании;
- росту подверженности высокому напряжению;
- большему числу сбоев на каждом этапе, вызванных недостатком синхронизации (как правило, вызванных ошибками монтажа) между комбинированным пускателями двигателя для пуска при полном напряжении;
- росту подверженности электрическим дугам;
- большему количеству требующихся перезапусков.

Дополнительное обоснование использования единичного комбинированного промышленного пускателя двигателя для пуска при полном напряжении вместо резервирования представлено следующими факторами:

- режимы отказов всех компонентов четко определены;
- поведение пускателя двигателя в условиях сбоя может быть установлено;
- промышленные ручные пускатели или промышленные комбинированные пускатели двигателя для пуска при полном напряжении не прибегают к помощи ПО для выполнения установленных им функций;
- имеется достаточное количество надежных данных по отказам для того, чтобы продемонстрировать, что заявленные интенсивности отказов для обнаруженных и необнаруженных опасных отказов позволяют количественно оценить случайные отказы аппаратных средств;
- низкое значение *MTTFdu* промышленных комбинированных пускателей двигателя для пуска при полном напряжении;
- использование процедур количественной оценки для верификации использования единичного промышленного комбинированного пускателя двигателя для пуска при полном напряжении оправданно.

А.11.4.7 Дополнительные требования не предусмотрены.

А.11.4.8 Дополнительные требования не предусмотрены.

А.11.4.9 Дополнительные требования не предусмотрены.

А.11.5 Руководящие указания к «Требованиям к выбору компонентов и подсистем»

А.11.5.1 Цели

Дополнительные требования не предусмотрены.

А.11.5.2 Руководящие указания к «Общим требованиям»

Проблемы перехода от непрограммируемых технологий к ПЭ-технологии представлены в приложении С.

А.11.5.2.1 Существуют определенные соображения по выбору устройств и подсистем, применяемых в ПСБ. Первое мнение состоит в том, что устройства должны быть разработаны в соответствии с МЭК 61508-2:2010 (требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью) и МЭК 61508-3:2010 (требования к ПО). Второе мнение сводится к тому, что следует использовать устройства и подсистемы ПСБ, о которых известно, что они надежно и широко применяются в аналогичных задачах и окружающих условиях на протяжении их полезного срока службы. Полезный срок службы — это период времени, в который интенсивность отказов устройства в значительной степени постоянна. Вероятностный расчет результирующего значения $ВОНЗ_{ср}$ для всей ПСБ (которое должно удовлетворять требованию УПБ каждой ФБ, реализованной в этой ПСБ) основан на этих интенсивностях отказов. По окончании полезного срока службы интенсивности отказов могут постепенно возрастать, например из-за старения.

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

a) достаточно надежна, чтобы можно было достичь общей целевой $ВОНЗ_{ср}$ или целевой интенсивности опасных отказов ФБ ПСБ;

b) отвечает требованию ограничений архитектуры;

c) имеет достаточно низкую вероятность систематических сбоев;

d) в случае электрических устройств они должны иметь соответствующую интенсивность отказов или же их выбор должен быть основан на результатах предыдущего использования.

Требование перечисления c) может быть выполнено либо в соответствии с МЭК 61508-2:2010 и МЭК 61508-3:2010, либо на основании требований к предшествующему использованию, установленных в МЭК 61511-1:2016 (пункт 11.5.3).

Практический подход к выбору устройств, используемых в приложениях безопасности, заключается в применении комбинации свидетельств соответствия с МЭК 61508-2:2010 и МЭК 61508-3:2010, а также эксплуатационного опыта. Такой подход гарантирует, что выбираемые устройства проектируются, изготавливаются и настраиваются для использования в системах безопасности, а также успешно функционируют в предназначенном для них применении (например, учитывают отказы, внесенные приложением).

Процедуры для демонстрации того, что устройство соответствует МЭК 615-8-2:2010 и МЭК 61508-3:2010, не включают в себя рассмотрение возможных режимов опасных отказов интерфейсов, установки, энергопитания или коммуникационных интерфейсов процесса, могут не включать полное описание границ устройства и иногда ограничиваются Э/Э/ПЭ-частью устройства. Отказы, связанные с технологическими процессами, значительно преобладают в датчиках, включая отказы из-за подключенных технологических линий, незадействованных линий, коррозии и проникновении газа, а также отказы в клапанах из-за повреждения седла, закупоривания, смещения и коррозии (включая отложения на штоке). По этой причине устройства, разработанные в соответствии с МЭК 61508-2:2010 и МЭК 61508-3:2010, должны подвергаться оценке для обеспечения работы этого устройства в приложении, для которого оно предназначено. Оценка может включать сбор информации о предыдущем использовании или моделирование испытания статистических образцов.

При выборе устройств пользователю следует рассмотреть методы защиты от систематических отказов. Для устройства, разработанного в соответствии с МЭК 61508-2:2010 и МЭК 61508-3:2010, существует большое количество методов и мер, которые должны быть внедрены производителем во время разработки устройства, чтобы снизить возможность возникновения систематического отказа. С другой стороны, для данного устройства данно-

го применения история предыдущего использования, основанная на значительном документально оформленном опыте, может использоваться для демонстрации достаточно низкой вероятности опасных систематических отказов, связанных с предназначенным применением, и потому надлежащей защиты от них.

А.11.5.2.2 Дополнительные требования не предусмотрены.

А.11.5.3 Руководящие указания к «Требованиям выбора компонентов и подсистем на основе опыта их предшествующего применения»

А.11.5.3.1 Многие пользователи обладают устройствами, допущенными для применения на их объекте. Датчики и клапаны, которые уже показали неспособность функционировать желаемым образом, больше не используются в качестве допущенных для применения устройств.

Оценка этих устройств должна содержать особенности версии устройства и документально оформленные данные по контролю процесса эксплуатации. Кроме того, изготовитель должен установить процесс внесения изменений, учитывающий влияние зафиксированных отказов и реализуемых изменений.

TSA TR84.00.04:2015 и рекомендация NAMUR NE130 («Предшествующее использование» — устройства для систем ПСБ») содержат указания по квалификации внешних устройств, по поддержанию контроля их процессов управления изменениями, а также наблюдению и документальному оформлению их рабочих характеристик. Результаты могут быть собраны в форме согласования на устройство.

Если подобной формы не существует, 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.

А.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 использовать 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.

А.11.5.3.3 Дополнительные требования не предусмотрены.

А.11.5.4 Руководящие указания к «Требованиям к выбору устройств, программируемых на фиксированном языке программирования (ФЯП) (например, внешних устройств), на основе опыта их применения»

А.11.5.4.1 Дополнительные требования не предусмотрены.

А.11.5.4.2 Дополнительные требования не предусмотрены.

А.11.5.4.3 Дополнительные требования не предусмотрены.

А.11.5.4.4 Данный подпункт разъясняет дополнительные требования, применяемые при попытках квалифицировать устройство, программируемое на ФЯП, как способное обеспечить УПБ 3.

А.11.5.5 Руководящие указания к «Требованиям к выбору устройств, программируемых на языке программирования с ограниченной изменчивостью (ЯОИ) (например, логических решающих устройств), на основе опыта их применения»

А.11.5.5.1 Дополнительные требования не предусмотрены.

А.11.5.5.2 Дополнительные требования не предусмотрены.

А.11.5.5.3 Дополнительные требования не предусмотрены.

А.11.5.5.4 Дополнительные требования не предусмотрены.

А.11.5.5.5 Дополнительные требования не предусмотрены.

А.11.5.5.6 Дополнительные требования не предусмотрены.

А.11.5.6 Руководящие указания к «Требованиям для выбора устройств, использующих язык программирования с полной изменчивостью (ЯПИ) (например, логических решающих устройств)»

Дополнительные требования не предусмотрены.

А.11.6 Внешние устройства

А.11.6.1 Дополнительные требования не предусмотрены.

А.11.6.2 Дополнительные требования не предусмотрены.

А.11.6.3 Дополнительные требования не предусмотрены.

А.11.7 Интерфейсы

А.11.7.1 Руководящие указания к «Общим требованиям»

К интерфейсам пользователей ПСБ относятся интерфейсы оператора и интерфейсы обслуживания/разработки. Данные или информация, которой обмениваются ПСБ и рабочие места операторов, может быть как связанной с ПСБ, так и справочной.

Если действие оператора является частью ФБ 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 ФБ ПСБ.

Передача данных, не являющихся частью ФБ ПСБ (например, индикация действительного значения сигнала датчика функции безопасности ПСБ при условии, что функция срабатывания реализована внутри ФБ 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).

А.11.7.2 Руководящие указания к «Требованиям к интерфейсу оператора»

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

- дисплеи;
- панели, содержащие лампочки, кнопки и переключатели;
- сигнальные устройства (визуальные и звуковые);
- принтеры (не должен быть единственным средством вывода информации);
- любую их комбинацию.

a) 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 СТБ.

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

Интерфейс оператора ОСУП может быть использован для обеспечения автоматической регистрации событий ФБ 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. Расположение любых панелей должно рассматриваться с точки зрения областей, подверженных любым возможным опасностям.

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 ФБ 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.

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 устройства 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.

A.11.7.2.1 Дополнительные требования не предусмотрены.

A.11.7.2.2 Дополнительные требования не предусмотрены.

A.11.7.2.3 Дополнительные требования не предусмотрены.

A.11.7.2.4 Дополнительные требования не предусмотрены.

A.11.7.2.5 Дополнительные требования не предусмотрены.

A.11.7.2.6 Дополнительные требования не предусмотрены.

A.11.7.2.7 Дополнительные требования не предусмотрены.

A.11.7.3 Руководящие указания к «Требованиям к интерфейсу обслуживания/разработки»

A.11.7.3.1 Дополнительные требования не предусмотрены.

A.11.7.3.2 Дополнительные требования не предусмотрены.

A.11.7.3.3 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 ППО логического решающего устройства ПСБ;

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

d) наблюдение за системными ресурсами ПСБ и диагностической информацией;

e) изменение уровней безопасности ПСБ и доступа к переменным ППО.

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

Такие интерфейсы должны предоставлять средства для копирования ППО 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.

A.11.7.3.4 Дополнительные требования не предусмотрены.

A.11.7.4 Руководящие указания к «Требованиям к коммуникационным интерфейсам»

A.11.7.4.1 Два интерфейса могут выглядеть одинаково, лишь бы интерфейс обслуживания/разработки не мог использоваться для управления процессом. ПО обслуживания/разработки не должно использоваться в качестве интерфейса оператора.

A.11.7.4.2 Дополнительные требования не предусмотрены.

A.11.7.4.3 Дополнительные требования не предусмотрены.

A.11.7.4.4 Дополнительные требования не предусмотрены.

A.11.8 Руководящие указания к «Требованиям к проектированию обслуживания или испытаний»

A.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 (например, входов, выходов), так как использование подобных технических решений может угрожать нарушением цельности ПСБ. В проекте системы должны рассматриваться технические и процедурные требования к испытанию ПСБ, необходимые для проведения полных системных испытаний датчиков, логического решающего устройства и исполнительных элементов на безопасность.

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

Необходимо отметить, что любое ограничение межпроверочного интервала исполнительных элементов должно быть учтено при вычислении значений $ВОНЗ_{ср}$ для ФБ ПСБ.

A.11.8.2 Дополнительные требования не предусмотрены.

А.11.8.3 Байпасы могут привести к снижению уровня безопасности ПСБ. Такое снижение защиты можно ослабить следующими приемами:

- применением паролей и/или ключа блокирования переключателей. В некоторых проектах могут быть предусмотрены запираемые шкафы, содержащие соответствующие средства для обхода;
- явным выделением обходных схем, которое может быть дополнено либо опечатыванием положений клапана, либо установкой знаков безопасности, указывающих на важность соответствующей позиции;
- четко установленными процедурами или средствами (например, основное устройство включения и отключения байпаса) для управления применением байпаса или его отключения;
- использованием байпасов, обладающих функцией ограничения времени, которая автоматически отключает байпас — подобная функция снижает риск того, что при завершении испытания или обслуживания остаются включенные байпасы.

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, что риск останется приемлемым. Если это невозможно, то 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, т. е. 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.

А.11.8.4 В ПСБ могут использоваться таймеры, ограничивающие продолжительность байпаса, например посредством автоматической перенастройки и/или аварийного сигнала оператору; в ПСБ может предоставляться логика, позволяющая автоматически перенастроить любые блокировки и выходы за граничные значения, например недостаток давления при запуске насоса.

А.11.8.5 Дополнительные требования не предусмотрены.

А.11.8.6 Процедура принудительного изменения состояния входов и выходов в ПЭ ПСБ не должна использоваться в качестве части ППО. Например, неконтролируемое принудительное изменение состояния входов и выходов через редактирование памяти в логическом решающем устройстве в режиме онлайн с помощью инструментов программистов во время функционирования программы часто применяется при разработке программы для изучения предлагаемых модификаций ППО. Тем не менее подобная практика не должна применяться на действующем процессе, так как она замаскирует «настоящий» входной статус переменных, поступающих с предприятия, и/или будет передавать ложные выходы устройствам на предприятии. При любом исходе логическое решающее устройство не будет контролировать предприятие предсказуемым образом. Более того, такие незначительные модификации прикладной программы могут быть легко не замечены, оставаясь в программе, когда в них уже нет необходимости.

А.11.9 Руководящие указания к «Количественной оценке случайного отказа»

А.11.9.1 Пользователи и разработчики должны руководствоваться методиками, представленными в приложении J МЭК 61511-3:2016; приложении В МЭК 61508-6:2010; ИСО 12489; ISA TR84.00.02:2002; приложении В МЭК 61508-3:2010; МЭК 61025 (дерево сбоев); МЭК 61078 (блок схемы надежности); МЭК 61165 (графы Маркова); МЭК 62551 (сети Петри); МЭК 62502 (дерево событий), которые обеспечивают, что функционирование разрабатываемой ПСБ удовлетворяет требованиям, связанным со случайными отказами аппаратных средств.

В течение интервалов контрольных проверок вероятность опасного отказа при наличии запроса, ВОНЗ(t), постоянно растет с течением времени. Поэтому после того, когда она превышает свое среднее значение, она все время остается выше него до конца интервала контрольной проверки. В некоторых случаях это значение может даже превысить верхний предел УПБ, соответствующий этому среднему значению, и неизменно оставаться выше него. Таким образом, когда необходим высокий уровень полноты безопасности, одни лишь средние значения могут создавать ложное впечатление безопасности, поэтому следует осуществить верификацию, например верификацию того, что риск, соответствующий пиковым значениям, согласуется с критериями риска организации пользователя.

За выполнением ФБ ПСБ в режиме работы по запросу (например, закрытие клапана, чтобы предотвратить сверхдавление) довольно часто сразу следует другая ФБ ПСБ, которая для своего выполнения использует те же компоненты, но действует в непрерывном режиме работы (например, предотвращение открытия клапана, пока давление на его входе превышено, за счет клапана противоточного типа). Поэтому для режима работы ФБ ПСБ, действующей по запросу, следует учитывать частоту возникновения опасности, связанную с отказом, при котором ПСБ не удержит процесс в безопасном состоянии.

А.11.9.2 Оцениваемые интенсивности отказов могут быть определены с помощью количественного анализа видов отказов проекта, используя данные по отказам, полученные из признанного промышленного источника или из опыта предыдущего использования в такой же среде, как и для целевого применения. В консервативных целях в вычислениях может использоваться верхний доверительный предел для входных данных, равный 70 %.

Следует отметить, что общая интенсивность необнаруженных отказов отказоустойчивых элементов зависит от времени и возрастает на интервалах контрольных проверок. Отказоустойчивые элементы могут иметь интенсивности отказов, зависящие от времени.

Пример — Элемент, состоящий из двух похожих компонентов A и B с одинаковой интенсивностью необнаруженных отказов λ, обладает общей интенсивностью необнаруженных отказов A, увеличивающейся от 0 до λ с увеличением времени.

При количественной оценке влияния случайных отказов аппаратных средств ПСБ (или подсистемы этой ПСБ) со значением отказоустойчивости аппаратных средств, равным нулю, которая реализует ФБ ПСБ, действующую в режиме высокой частоты запросов или с непрерывными запросами, доверие (предпочтение) должно быть отдано только диагностике, если:

- сумма интервала диагностических проверок и времени реакции, позволяющей перейти в безопасное состояние или поддерживать его, должна быть меньше, чем время безопасности процесса; или
- в режиме с высокой частотой запросов отношение частоты диагностических проверок к частоте запросов равно или превышает 100.

Процедура проведения контрольной проверки и анализ безотказности средств выполнения контрольной проверки включает, например:

- продолжительность контрольных проверок;
- состояние процесса (действующий или остановлен) во время контрольной проверки;
- состояние испытываемого устройства во время контрольных проверок (в автономном или не автономном режиме); если испытываемое устройство находится в автономном режиме (т. е. недоступно) во время контрольной проверки — то это может иметь важное значение для его $ВОНЗ_{ср}$;
- охват контрольной проверкой, когда контрольные проверки не эффективны на 100 %. Это подразумевает идентификацию отказов, которые, по своему существу, никогда не могут быть обнаружены контрольными проверками;
- отказ, который может быть вызван самими контрольными проверками (например, отказ из-за изменения состояния, необходимого для цели тестирования);
- возможность проведения контрольных проверок с временным сдвигом для аналогичных дублирующих устройств для того, чтобы устранить связь между контрольными проверками устройств;
- возможность для контрольной проверки вернуть неверный результат о состоянии ПСБ:
  - на контрольную проверку оказал воздействие сбой, связанный с самой контрольной проверкой;
  - ошибки человека при проведении контрольных проверок (например, реальный отказа не обнаружен, потеря теста, прошедшее контрольную проверку или ремонт устройство остается в автономном режиме после завершения этой проверки или ремонта и т. д.).

Если интервал проведения контрольных проверок для вычислений вероятностей в явном виде не определен, то значение MTTR отдельных обнаруживаемых опасных отказов может быть вычислено как половина интервала контрольной проверки плюс MRT рассматриваемого отказа.

Большинство методик в приложении А.11.9.1 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 (примеры расчета охвата диагностикой см. в МЭК 61508-2:2010, приложение С, и МЭК 61508-6:2010, приложение С).

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 степень диагностического охвата, так и период проведения диагностических проверок (интервала диагностических проверок). Дополнительные указания см. в МЭК 61508-2:2010 приложение С, и ISA TR84.00.02:2015.

Если ПСБ является единственным слоем защиты и используется для выполнения функции безопасности в непрерывном режиме, то интервал диагностических проверок следует сделать 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 интервала диагностических проверок и времени реакции, позволяющего перейти в безопасное состояние, должна быть меньше, чем время безопасности процесса. В соответствии с МЭК 61511-1:2016 (подпункт 3.2.52.1) 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 ФБ ПСБ не выполняется.

Критичные и потенциально критичные неисправности в общих устройствах (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 видов отказа.

Для каждой реализуемой диагностики интервал проведения проверок и действие, вызванное выявленной неисправностью, должны удовлетворять СТБ.

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 систематические ошибки (такие 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 — см. примечание ниже). 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 устройства передачи датчика, выходной сигнал которого перестал изменяться.

Примечание — Отбор среднего значения обладает преимуществом по отношению к среднему арифметическому от трех датчиков, потому что среднее арифметическое искажается неправильно функционирующим устройством. Как бы там ни было, отбор среднего значения не работает, если два датчика выдают неверные результаты измерений, и в таком случае можно рассмотреть отказы общего вида;

3) если применено перечисление 2) или было проведено сравнение между аналоговыми датчиками в ПСБ и сравнимыми показателями параметров процесса, полученными другими датчиками в системах, таких как ОСУП, то возможное улучшение охвата диагностикой будет зависеть от конкретных приложений и должно подвергаться анализу, оценке и документальному оформлению. Если требуется, чтобы степень диагностического охвата должна быть больше 90 %, то должны подвергаться анализу и документально оформляться источники отказов по общей причине (ООП).

Примечания

1 Используя сравнение, любое несоответствие может, по крайней мере, автоматически сгенерировать аварийный сигнал. Порог срабатывания для подобной аварийной сигнализации несоответствия может быть установлен в соответствии с документально зафиксированным отклонением переменной соответствующего процесса. Подобные сравнения выявляют как отказ датчиков ПСБ, так и отказ датчиков, не связанных с ПСБ. В дальнейшем ложные тревоги или ложные срабатывания, сгенерированные отказами датчиков, не связанных с ПСБ, могут подвергнуться анализу перед внедрением подобного решения.

2 Улучшение диагностического охвата за счет сравнения подобного типа может применяться для увеличения интервала контрольной проверки;

4) могут быть введены временные задержки для предотвращения случайных срабатываний аварийной сигнализации из-за различия времени реакции датчиков на изменения в процессе, связанных 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;

5) 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 значитель-

ные 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 комплекса 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.

Должна также учитываться уверенность в данных о безотказности, используемых для вычисления целевой меры. Использование 70%-ных верхних доверительных границ входных параметров безотказности гарантирует выполнение консервативных вычислений, и это обсуждается в МЭК 61511-1:2016 (пункт 11.9.4).

А.11.9.3 Дополнительные требования не предусмотрены.

А.11.9.4 Значения данных по безотказности, используемые при количественной оценке последствий случайных отказов аппаратных средств, всегда известны только с числовыми погрешностями. Таким образом, оценивание влияния этих погрешностей на целевую меру полезно при определении требований УПБ.

Погрешность (см. примечание) заданного параметра безотказности (например, интенсивности отказов) может быть оценена посредством:

a) статистического анализа;

b) применения экспертной оценки там, где это требуется;

c) выполнения определенных тестов.

Согласно общему правилу числовые погрешности уменьшаются с ростом доступной обратной информации об эксплуатации.

Таким образом, параметр безотказности является не столько хорошо определяемым детерминированным значением, сколько случайной переменной с большим или маленьким разбросом, отклоняющимся от ее среднего значения, как это показано на рисунке А.5.

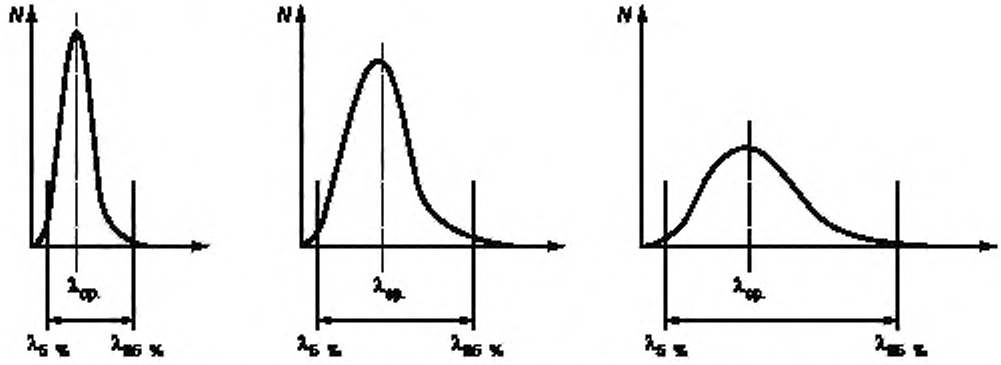


Рисунок А.5 — Иллюстрация погрешности для параметра безотказности

Чем более острое распределение, тем меньше погрешность параметра. На рисунке А.5 погрешность возрастает слева направо.

В пределе, если параметр полностью известен, кривая будет представлять из себя простую вертикальную прямую линию (т. е. обобщенная функция Дирака).

Как показано на рисунке А.5, погрешность параметра безотказности λ может быть оценена по его доверительному интервалу, например, на 90%-ной отметке: действительное среднее значение λ с вероятностью 90 % попадает в интервал $[\lambda_{5\ \%}, \lambda_{95\ \%}]$ (λ с вероятностью 5 % будет лучше, чем $\lambda_{5\ \%}$, и с вероятностью 5 % будет хуже, чем $\lambda_{95\ \%}$).

Чисто статистически среднее значение параметра безотказности может быть оценено с помощью «оценки максимальной вероятности», а доверительные границы $[\lambda_{5\ \%}, \lambda_{95\ \%}]$ могут быть вычислены с помощью функции χ^2 (хи-квадрат), представленной таблично в сборниках по статистике.

Испытание, в котором n отказов, наблюдаемых за накопленное время наблюдения T, дает среднее значение, равное n/T, и 90%-ный доверительный интервал, равный $\left[\frac{1}{2T}\chi^2_{0,95,\ 2n}, \frac{1}{2T}\chi^2_{0,05,\ 2(n+1)}\right]$. Ширина данного интервала

сжимается, т. е. точность увеличивается, когда увеличивается накопленное время наблюдения и/или число наблюдаемых отказов (справа налево на рисунке А.5).

Для обработки статистических наблюдений, экспертной оценки и результатов конкретных тестов может также использоваться Байесовский подход. Он может применяться для формирования соответствующих функций распределения вероятностей при моделировании методом Монте-Карло.

При широком доверительном интервале (т. е. в случае немногочисленной информации от пользователей об эксплуатации) следует реализовать процесс сбора данных о безотказности как можно быстрее, а вероятностные прогнозы целевых вероятностных показателей должны периодически обновляться с помощью собранных данных о безотказности.

Примечание — МЭК 61511 включает в себя вероятностные вычисления, выполнение которых нуждается в точных данных о безотказности. Он не может быть реализован надлежащим образом без сбора данных о безотказности от пользователей. Выявленная нехватка данных по безотказности — это возможность начать сбор конкретных данных по безотказности для их восполнения. Если это не приносит пользы для текущей ПСБ, то будет полезным для следующей.

Первым подходом для обработки погрешности, описанной выше, является использование пессимистических входных данных о безотказности. Это гарантирует, что несмотря на недостаток точности, оценка целевого показателя (ВОЗН$_{ср}$ или ВОЧ) не является оптимистичной. Это может быть выполнено посредством применения к входным параметрам безотказности некоторых верхних доверительных границ, более высоких, чем обычные средние значения. Предполагается, что использование верхних доверительных границ в 70 % ($\lambda_{70\,\%} > \lambda_{ср}$), как правило, предоставляет приемлемый доверительный уровень. Это показано на рисунке А.6, демонстрирующем, что «консервативность» входных данных снижается с увеличением точности (уменьшается разница между $\lambda_{70\,\%} - \lambda_{ср}$).

Примечания

1 Для испытания с n наблюдаемыми отказами за накопленное время наблюдения T верхняя доверительная граница может быть вычислена с помощью функции χ^2. Например, $\lambda_{70\,\%}$ может быть оценена как $\lambda_{0.7} = \frac{1}{2T}\chi^2_{0,3,\ 2(n+1)}$, т. е. в 70 % случаев фактическое значение ниже (т. е. лучше), чем это. Такая верхняя доверительная граница существует, даже когда не наблюдается никаких отказов. Она всегда является пессимистической по сравнению с $\lambda_{ср}$, но она становится все менее и менее пессимистической с увеличением T и/или n (см. рисунок А.6).

2 Вычисления, выполненные при верхних доверительных границах для входных параметров в 70 %, не дают верхние доверительные границы в 70 % для всего результата (например, ВОЗН$_{ср}$). Вычисления, выполненные таким образом, гарантируют только консервативность результата.

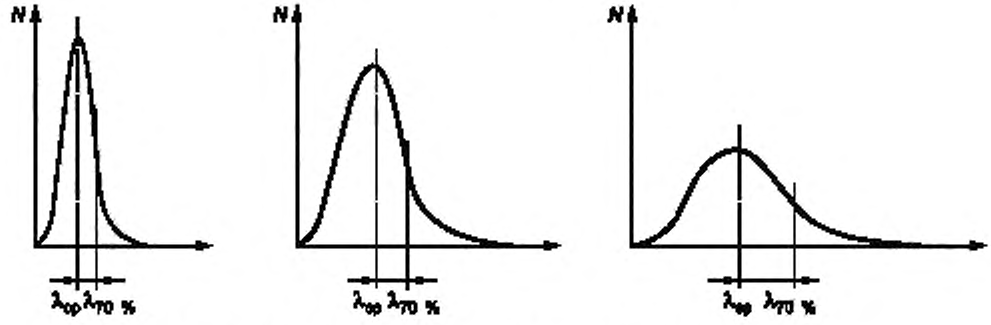


Рисунок А.6 — Демонстрация верхней доверительной границы в 70 %

Предыдущий подход предполагает только одно вычисление вероятностной цели (т. е. ВОЗН$_{ср}$) но уровень консервативности неизвестен. Поэтому, если требуется узнать этот уровень консервативности, то может быть использован другой подход. Он предполагает использование всех распределений входных параметров безотказности вместо только отдельных значений, таких как $\lambda_{70\,\%}$. Может применяться моделирование так называемым методом Монте-Карло, который выполняет следующее:

a) использует случайные числа для моделирования вероятностных распределений значений входных параметров безотказности и

b) архивирует несколько (например, 100) вычислений вероятностной цели с различными наборами случайных чисел.

Это дает статистическую выборку (т. е. гистограмму) целевого результата (например, ВОЗН$_{ср}$), которая может быть обработана для получения соответствующего вероятностного распределения, а также соответствующего среднего значения и доверительных уровней (см. рисунок А.7).

Рисунок А.7 демонстрирует функцию плотности вероятности (фпв) и соответствующую ей интегральную функцию распределения (ифр), которые могут быть получены в результате моделирования методом Монте-Карло. Это показывает распределение $ВОЗН_{ср}$ вокруг его среднего значения $[ВОЗН_{ср}]_{ср}$.

Примечание — $ВОЗН_{ср}$ сама по себе является случайной переменной в связи с лежащими в основе ее формирования вероятностными законами. Вычисление, приведенное выше, по существу, предоставляет только распределение из-за неопределенностей входных параметров безотказности.

$[ВОЗН_{ср}]_{ср}$ может применяться вместо классического $ВОЗН_{ср}$, но его консервативность не может быть доказана. Оно, скорее всего, будет близко к медианному значению (т. е. с вероятностью 50 % фактическое значение будет лучше, чем $(ВОЗН_{ср})_{50\ \%}$, и с вероятностью 50 % фактическое значение будет хуже него).

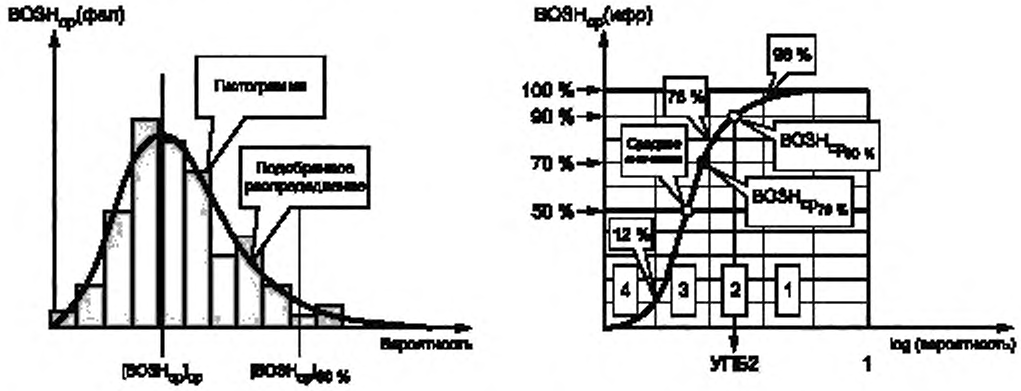


Рисунок А.7 — Типичное вероятностное распределение целевых результатов, полученных моделированием методом Монте-Карло

Кривая «ифр» на рисунке А.7 демонстрирует, что значение $ВОЗН_{ср}$ имеет шанс в 12 % попасть в диапазон, связанный с УПБ 4 (шанс в 88 % быть в диапазоне УПБ 3 или хуже), имеет шанс в 78 % быть в диапазоне УПБ 3 или лучше (шанс в 22 % быть в диапазоне УПБ 2 или хуже), а также имеет шанс в 96 % быть в диапазоне УПБ 2 или лучше (4 % шанс быть в диапазоне УПБ 1 или хуже) и т. д.

В консервативных целях может быть выбран доверительный уровень 90 %. Так как $ВОЗН_{ср\ 90\ \%}$ лежит в области УПБ 2, то для данного примера это ведет к значению УПБ 2. Следует отметить, что для доверительного уровня в 70 % тот же пример выдает значение УПБ 3.

А.11.9.5 Дополнительные требования не предусмотрены.

А.12 Разработка прикладной программы ПСБ

А.12.1 Цель

Примеры того, как определяется разработка ППО для одной или нескольких функций безопасности в ПСБ, см. в приложении В (раздел В.1) и приложении F (раздел F.20).

А.12.2 Руководящие указания к «Общим требованиям»

А.12.2.1 Раздел 12 в МЭК 61511-1:2016 подходит для разработки и модификации программ ППО с требованием к УПБ до значения УПБ 3. Опыт показывает, что имеется незначительная разница между методами разработки с требованиями УПБ 1, УПБ 2 и УПБ 3 при использовании ЯОИ в удовлетворяющем требованиям МЭК 61511-1:2016 логическом решающем устройстве, применяя соответствующее руководство по безопасности.

Различия между УПБ 1, УПБ 2 и УПБ 3 может быть в применяемых методах испытания и верификации для различных УПБ. См. А.7.2.2.

А.12.2.2 Например, прикладной программист в процессе обнаружения неточностей и для обеспечения гарантии, что он понимает намеченное требование, должен также анализировать информацию в логическом представлении [см., например, приложение F (разделы F.15 и F.17)], а не в виде последовательности команд.

А.12.2.3 Настоящий стандарт ограничивается рассмотрением требований для ППО, разрабатываемых с помощью ЯОИ. Под «разработкой ППО» понимают проектирование и реализацию прикладной логики системы безопасности для ПЭ, выбранной в соответствии с МЭК 61511-1:2016 (подраздел 11.5).

А.12.2.4 Настоящий стандарт также рассматривает применение устройств, использующих фиксированный язык программирования (ФЯП), например управление вводом параметров в микропроцессорных датчиках — см., например, приложение С и таблицу F.13.

А.12.2.5 Для ФБ ПСБ и функций, не связанных с безопасностью, следует использовать отдельное ППО.

Одним из способов показать их адекватную независимость может быть выполнение всех следующих положений:

a) ФБ ПСБ понятно промаркированы в ППО, как прикладные коды ФБ ПСБ;

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

c) все переменные, используемые при реализации ФБ ПСБ, промаркированы;

d) все прикладные программы, реализующие функции, не связанные с ПСБ, промаркированы как коды функций, не связанных с ПСБ;

e) все ППО, использующие переменные, не связанные с безопасностью, и переменные ФБ ПСБ, удовлетворяют следующим условиям:

f) ППО (включая все функции и функциональные блоки), не связанное с безопасностью, не должно осуществлять запись в переменные ФБ ПСБ, используемые в ППО безопасности, и

g) ППО безопасности, реализующее ФБ ПСБ, не зависит от каких-либо переменных, не связанных с безопасностью;

h) все ППО безопасности (включая переменные и данные) защищено от любых изменений ППО, не связанного с безопасностью, и

i) если безопасное ППО и ППО, не связанное с безопасностью, совместно используют одни и те же ресурсы (например, ЦПУ, ресурсы операционной системы, память, шины), то функция безопасности ПСБ (например, время реакции) безопасного ППО никогда не должно оказаться под угрозой.

А.12.2.6 См. руководящие указания к А.11.2.8. Если ППО не имеет функции ручного сброса, то это должно быть определено в СТБ.

Рассматривает опасность, которая может возникнуть, если прекращается подача электропитания ПСБ, а восстановление электропитания не может поддерживать безопасное состояние процесса. См. также пункт А.11.2.8 и МЭК 61511-1:2016 (пункт 12.2.5). В случае останова по включению питания см. также МЭК 61511-1: 2016 (пункт 11.6.2).

А.12.2.7 Дополнительные требования не предусмотрены.

А.12.2.8 Помогает уменьшить сложность ППО и гарантирует рассмотрение всех входов и выходов при каждом сканировании. См. также ISA TR84.00.09. Также помогает обеспечить достижение требований к времени отклика — см. МЭК 61511-1:2016 (пункт 10.3.2).

А.12.2.9 Обеспечивает использование надлежащего ППО. Следует рассмотреть как вопрос обеспечения защиты хранения и поиска, так и вопрос длительности хранения старых версий с учетом производственных и нормативных требований. Также следует рассмотреть вопрос сохранения аппаратных средств и встроенного ПО, необходимых для работы старых версий ППО. Перед внесением каких-либо модификаций в ППО должно быть проверено, что ППО, работающее в машинном оборудовании, идентично контрольному экземпляру. Перед восстановлением данных пользователя должно быть проверено, что используются данные пользователя надлежащей версии. См. пункт А.5.2.7.

А.12.2.10 Дополнительные требования не предусмотрены.

А.12.3 Руководящие указания к «Проектированию прикладной программы»

А.12.3.1 Рабочие режимы могут включать рабочие функции, такие как ручная функция, полуавтоматическая, автоматическая, функция запуска, пакетной обработки, испытания и обслуживания. См. приложение F (разделы F.14 и F.27).

А.12.3.2 Примеры входной информации для проектирования ППО см. в приложении F (раздел F.13). Пример СТБ для ПСБ см. на шаге F.3. Пример методов и инструментальных средств для разработки проекта ППО см. в приложении F (раздел F.20) и на шаге F.3.

Прикладному программисту и проектировщикам ПСБ может потребоваться обсудить входную информацию для проектирования ППО.

А.12.3.3 Для того чтобы облегчить проведение ОФБ, ППО должно быть прослеживаемым до спецификации требований к безопасности ПСБ. Например, его структуру надо организовать таким образом, чтобы она демонстрировала как реализуются ПСБ, а идентификаторы должны отражать практическую реализацию, используя наименования тегов входа/выхода, основанные на реальности. ППО должно также сопровождаться комментариями, описывающими функции процесса. См. также МЭК 61511-1:2016 (пункт 5.2.6) и примеры на рисунке F.11. Проектирование ППО должно описывать устройство и подсистемы ППО ПСБ, а также как они взаимосвязаны и как достигаются требующиеся атрибуты, в особенности полнота безопасности. Примеры ППО устройств включают прикладные функции, продублированные во всей программе (например, последовательности управления насосом), обмен информацией с входом/выходом на заводской установке и с коммуникационными модулями, любые функции уровня ППО, которые взаимодействуют с лежащими в основе ПЭ-устройствами (например, использование нескольких ПСБ для достижения функций резервирования, и/или поведение при обнаружении ошибки, и/или последовательности запуска/останова).

Проведение ОФБ для ППО поможет идентифицировать ошибки на ранней стадии, также как обеспечить устойчивость ППО к отказам. ОФБ ППО может включать:

a) подтверждение того, что ППО не выходит за ограничения, установленные в инструкции по безопасности, и соответствует любым стандартам кодирования для конкретного приложения и стилям программирования систем безопасности;

b) анализ отказов поведения ППО; он включает идентификацию функций, выполняемых ППО, их возможные функциональные отклонения (например, как в «химическом» HAZOP — слишком большой/маленький, слишком рано/поздно, противоположно/отсутствует/никакое и т. д.), оценку влияния отказа каждой прикладной функции и идентификацию любых мер по смягчению ущерба, защищающих от функциональных отказов.

Примечание — Многие функции ППО являются ФБ ПСБ, и анализ их отказов может быть частью анализа отказов системы. Тем не менее в ППО могли быть идентифицированы дополнительные функции или же они могли быть идентифицированы во время самого анализа функциональных отказов для защиты от отказов ФБ ПСБ (например, такие функции, как управление насосами, голосование на входах процесса, например голосование «огонь и газ» или «температура и давление», ответное действие на отказ).

A.12.3.4 Примеры методов проектирования прикладной программы приведены ниже:

a) см. рисунок F.11, лист 4, строчка 1;

b) см. примеры ППО в разделе F.20 (таблицы F.8—F.14 включительно). Структура ППО должна согласовываться со структурой процесса (например, на химическом объекте прикладное программное обеспечение для каждого участка процесса должно быть сгруппировано вместе и внутри каждого участка процесса следует распределить программное обеспечение между оборудованием для обеспечения понимания и обслуживания);

c) правильный порядок выполнения и сетевых, и логических операций должен быть определен внутри каждой программы, а также должны быть определены последовательность и требуемые скорости выполнения всех прикладных программ. Следует подтвердить, что скорости выполнения программ ППО были согласованы с требуемыми временами реакции процесса, приведенными в СТБ ППО;

d) примеры описания стандартных библиотечных модулей можно найти на рисунке F.11, лист 1;

e) примеры описания специальных библиотечных модулей можно найти в B.4.1; любые заказные функции и функциональные блоки должны быть спроектированы и разработаны; заказные разработанные функциональные блоки весьма желательны, так как в прикладных программах могут быть запрограммированы, испытаны и повторно использованы повторяющиеся операции. Следует сконфигурировать модули ввода/вывода и области памяти для переменных данных;

f) распределение памяти, как правило, выполняется автоматически при выполнении прикладного программирования в ПЛК; распределение памяти достигается посредством разбиения различных частей ППО (например, аварийные сигналы, входы, выходы, логика безопасности, логика, не связанная с безопасностью, свободная область для дальнейшего развития) на их отдельные «ступеньки» — пример см. на рисунке F.11; если разбиение должно выполняться вручную, то при управлении памятью следует проявлять осторожность, что можно делать за счет:

- распределения эквивалентных переменных по предназначенным для них страницам, чтобы не смешивать константы и переменные, входные и выходные переменные, физические переменные и промежуточные переменные;
- разделения типов переменных, чтобы, например, не смешивать целочисленные с двоичными;
- предотвращения мультиплексирования переменных простых типов в более сложные типы переменных, например, вкладывания нескольких двоичных переменных в целочисленные или в байты, следуя правилу «один адрес в памяти для одной переменной»;

g) например, глобальной переменной в прикладной программе можно описать предупредительную сигнализацию, такую как аварийный сигнал о превышении температуры, который изменяется в зависимости от составляющих пакета данных в процессе; другим примером может быть предельное значение, при котором формируется аварийный сигнал о воспламенении газа, которое используется в противопожарных и газовых системах защиты и которое равно, например, 20 % от нижнего взрывоопасного предела (НВП); примером защиты целостности может служить функциональность основного логического решающего устройства, разрешающая только одной команде ППО переписывать значения глобальной переменной; дополнительные соображения на тему использования глобальных переменных см. в G.3.4.3, G.3.4.4, G.7.2.4, G.7.3.1 и G.7.3.2;

h) желательно разделить функции безопасности и функции, не связанные с безопасностью, по разным программам так, чтобы основной акцент мог быть сделан на программах безопасности и чтобы можно было легко продемонстрировать, что функции, не связанные с безопасностью, не оказывают влияния на функции безопасности; на рисунке B.13 приведен пример анализа независимости ФБ ПСБ; в СТБ должно быть указано, какая ФБ ПСБ и какие другие функции будут включены в рассматриваемую программу; желательно также ограничить размер программ безопасности небольшим числом функций, чтобы наивысший уровень полноты требовался бы только критически важным функциям безопасности;

i) на рисунке F.11, листах 1 и 2, приведен пример описания ввода и вывода; должны быть созданы наименования для всех переменных ввода/вывода и памяти;

j) на рисунках B.6 и B.12 приведены примеры спецификации ЧМИ ПСБ;

k) должны быть определены коммуникационные переменные для систем, внешних к ПСБ; если эти переменные размещаются в памяти, то они должны быть приписаны к соответствующим областям памяти так, чтобы коммуникационная подсистема ПСБ могла иметь к ним доступ; переменные, которые могут изменяться другими системами, внешними к ПСБ, должны быть аккуратно определены и, как правило, размещаться в специальной

области памяти, предназначенной для чтения или записи; на рисунке В.13 проиллюстрирован пример обмена данными между ПСБ и ОСУП;

l) необходимо определить способы диагностики датчиков и исполнительных элементов, а также организацию периодических проверок, которые будут зависеть от резервирования датчиков и исполнительных элементов; организация проверок должна быть определена тщательно и предусматривать соответствующую аварийную сигнализацию в ходе проведения проверки; примеры реализации диагностик см. на рисунке F.11, лист 3, строки А1—А6, лист 4, строки 4, 6, 8 и 10, лист 5, строки 17—20;

m) обращение с аварийными сигналами и их записью следует осуществлять с осторожностью, как и рассмотрение их влияния на снижение риска; более того, должен быть определен подход, связанный с переопределением обслуживания; некоторые пользователи будут требовать, чтобы для обслуживания к цифровым входам были подсоединены переключатели, в то время как другие будут использовать управляемый ввод данных в ПСБ из рабочей станции; в любом случае должны быть обеспечены безопасные процедуры, предотвращающее непреднамеренные переопределения обслуживания/обходы аварийной сигнализации; типичные примеры диаграммы аварийной сигнализации см. на рисунке F.11, лист 3; установление приоритетов аварийных сигналов см. в приложении F (раздел F.14) и таблице F.13; типичные примеры интерфейсов операторов см. на рисунке F.11, лист 2, строки DI1, DI2 и DI3;

n) примеры проверки целостности прикладных данных и подтверждения соответствия датчиков включают:

- проверку выхода входных/выходных данных за границы заданных диапазонов, например значения датчика, вышедшего за границы заданного диапазона;
- подтверждение соответствия передаваемых прикладных данных, например внешний сторожевой таймер, внешние алгоритмы циклической проверки избыточностью (CRC) и
- сравнение значений датчиков и отправку сигналов об отклонениях;

o) проверки конфигурации системы могут выполняться посредством структурных испытаний (подробное описание структурных испытаний см. в перечислении b) А.12.5.3; кроме того, требуется проявлять осторожность, чтобы обеспечить уникальность наименования тегов, включая их уникальность среди контроллеров;

p) один из примеров управления сложностью приведен в В.4.3.3.1, где сложность ППО ограничена при помощи иерархической организации из трех слоев модулей (см. также рисунок В.9);

q) на рисунке F.11, лист 3, строки D01, D02 и D03, лист 4, строки 1 и 2, а также лист 5, строки 12 и 16—20, показан пример управления сбоями входов/выходов ПСБ и подсистем ПСБ;

r) примером испытания при действующем процессе с автоматической блокировкой может служить испытание клапана при неполном ходе на выходе физического процесса — см. также А.16.3.1.2 и А.16.3.1.3;

s) на рисунке В.6 приведен пример интерфейса для обслуживания переключателей при их автономном тестировании;

t) внесение изменений в ПСБ должны выполняться автономно — безопасность процесса внесения изменений, как правило, основано на:

- предотвращении изменений ППО в логическом решающем устройстве на действующем процессе; это, как правило, можно обеспечить запрещением редактирования кода логического решающего устройства посредством переключателей и паролей аппаратных средств;
- предотвращении доступа к ссылке на загрузку ППО;
- внутренних характеристиках среды разработки ППО и встроенных в них функций безопасности, включая контроль синтаксиса, проверки соответствия, прослеживаемость и управление версиями;

u) спецификации требований безопасности ППО, как правило, содержатся в документе или наборе документов, организованном иерархически, чтобы обеспечить постепенное уточнение требований, которые изменяются от СТБ до самых подробных спецификаций реализации, таких как отображение памяти. Документация на ППО, предусмотренная логическим решающим устройством, не является адекватным вариантом СТБ для ПСБ.

А.12.3.5 Соображения по надлежащему подходу к разработке проекта прикладных программ включают:

a) см. приложение F (пункты F.17 и F.27);

b) внедренное ППО должно реализовывать все функции, описанные в спецификации требований безопасности ППО, и все другие неустановленные поведения должны быть идентифицированы и не должны влиять на полноту безопасности;

c) указания по возможным способам избежать неоднозначности см. в А.12.6 и приложении G. ППО должно быть реализовано таким образом, чтобы оно помогало операторам и эксплуатационному персоналу понимать и взаимодействовать с ПСБ (там, где требуется). Например, описание аварийных сигналов, требующихся времен реакции, рабочей нагрузки оператора и т. п. Функции должны поддерживать деятельность по обслуживанию, включая использование переопределений и байпасов;

d) указания по избавлению от ошибок проектирования см. в А.12.6.

А.12.4 Руководящие указания к «Реализации прикладной программы»

А.12.4.1 При возможности ППО всегда должно базироваться на апробированных модулях ППО, которые могут включать библиотечные функции и четко определенные правила для объединения модулей ППО (см. приложение В, подпункты В.4.3.3.1, В.4.3.3.2.1 и В.4.3.4.1 и рисунок В.9). На рисунке F.11, лист 1, приведен пример части ППО, использующей блоки стандартных функций, предоставленные поставщиком и прошедшие оценку безопасности.

А.12.4.2 Чтобы понять, как может быть реализовано каждое требование МЭК 61511-1:2016, см. следующие ссылки:

Примечание — Приложение F является примером, основанным на втором издании МЭК 61508 и МЭК 61511.

a) разработчик ППО — нижняя часть рисунка F.11, угловой штамп;

b) описание цели ППО: разделы F.1, F.2, F.3, F.4, а также F.5.1 и F.5.2;

c) дополнительные требования не предусмотрены;

d) дополнительные требования не предусмотрены;

e) прослеживаемость до СТБ ППО — таблица F.12;

f) идентификация каждой ФБ ПСБ и ее УПБ — таблица F.11;

g) идентификация и описание используемых символов, включая логические условные обозначения, стандартные библиотечные функции, функции библиотеки приложений — рисунок F.11, лист 1;

h) для идентификации сигналов ввода и вывода логического решающего устройства ПСБ см. таблицы F.9 и F.10;

i) если вся ПСБ задействует коммуникации, то описание потока информации в коммуникациях см. на рисунке F.12;

j) описание структуры программы, включая описание порядка логической обработки данных по отношению к подсистемам ввода/вывода ПСБ см. в В.1. Там же приведены типичные ограничения, устанавливаемые временами сканирования;

k) если это требуется для спецификации ФБ ПСБ, информацию о средствах обеспечения корректности эксплуатационных данных и данных, отправляемых по коммуникационному каналу, см. на рисунке F.11, лист 5, строки 17, 18, 19, 20; и

l) информацию по идентификации версий и истории изменений см. на нижней части листа на рисунках F.4—F.11.

А.12.4.3 Повторное использование библиотечных функций ППО должно демонстрировать удовлетворительное функционирование в похожих приложениях, включая свидетельства того, что одинаковые библиотечные функции продемонстрировали удовлетворительное функционирование в похожих условиях использования. Примером разработанной прежде библиотечной функции ППО, используемой на множестве технологических объектов, является ППО-модуль, выполняющий функции пуска, останова и самоподхвата двигателя, которые можно встретить в мгновенной функции управления трехфазным двигателем.

А.12.4.4 Чтобы создать устойчивое и надежное ППО, следует с вниманием отнестись к его структуре. Можно использовать способ, при котором в основной проект логического решающего устройства добавляется резервирование на уровне приложения, а функции разделяются между несколькими входами/выходами (например, структурирование управлением клапана) и порядком обработки переменных входа и выхода.

А.12.5 Руководящие указания к «Требованиям к верификации прикладной программы (проверка и тестирование)»

А.12.5.1 Дополнительные требования не предусмотрены.

А.12.5.2 Компетентность в таком контексте означает, что человек обладает профессиональной технической квалификацией и образованием (например, имеет степень магистра или бакалавра или аналогичную степень), что он/она ознакомлен с используемым языком программы и инструментальными средства проектирования и реализации, что он/она является опытным прикладным программистом. Более того, он/она должен обладать знаниями по функциональной безопасности, особенно для промышленных процессов. Он/она должен уметь распознать небезопасную, по сути, логику (например, применение логических схем ИЛИ, либо инверторов при переходе в безопасное состояние при отключении питания, либо применение логических схем И при переходе в безопасное состояние при включении питания). См. F.28.

А.12.5.3 Во время испытания должны выполняться все области ППО для того, чтобы обеспечить корректное функционирование и гарантировать, что одна область приложения не оказывает неблагоприятного влияния на другую часть программы. ППО должно проверяться для всех значений данных из разрешенного диапазона, чтобы гарантировать, что система будет функционировать корректно, находясь в этом диапазоне. Проверки за пределами этого диапазона также должны быть выполнены, чтобы подтвердить, что ППО не выполняет непредназначенные ему функции, которые подвергают риску его требования к безопасности.

Проверка ППО должна включать такие методы, как контроль, сквозной контроль и формальный анализ. Она должна использоваться совместно с моделирование и испытанием для того, чтобы обеспечить, что ППО гарантированно удовлетворяет связанной с ним спецификации.

Испытание может быть выполнено методом «черного ящика» (выполнение испытания без знания внутренней структуры ППО), например функциональное испытание, или методом «белого ящика» (выполнение испытания, используя знания внутренней структуры ППО). В обоих случаях важно продемонстрировать, как результаты испытания удовлетворяют требованиям, но в случае испытания методом «белого ящика» легче идентифицировать «непредвиденное» поведение.

Проверки ППО на соответствие требованиям, полученным на стадиях проектирования и формирования спецификаций, могут сначала проводиться на симуляторе, а затем — на логическом решающем устройстве. Целями

проверок на начальных этапах (симулирование и тестирование на соответствие требованиям проектных спецификаций) являются:

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

b) проверить ППО для широкого набора условий и последовательностей их выполнения, чтобы показать, что оно остается устойчивым при неожиданном поведении;

c) структурное тестирование включает три основные стадии разработки и испытания ППО (уровни разработки модуля, интеграции и тестирования всей системы).

Структурные тестирования ППО предназначены подвергать критической оценке решения, принятые ППО с помощью тестовых сценариев, основанных на структуре и логике проекта. Полное структурное тестирование проверяет структуры данных ППО (такие как таблицы конфигурации, типовые решения, подпрограммы, функции), а также его логику управления и логику процедур на уровнях испытаний, рассмотренных ниже.

Структурные тестирования должны выполняться на уровнях тестирования модуля, интеграции и системы. Здесь под «модулем» подразумевается наименьший отдельно компилируемый (или ему эквивалентный) созданный код, такой как процедура, подпрограмма, класс, метод или таблица базы данных. Структурное тестирование гарантирует, что утверждения и решения ППО полностью проверяются выполнением кода. Например, оно подтверждает, что операторы цикла ППО ведут себя на граничных значениях своих данных, как и предполагалось. Для конфигурируемого ППО целостность данных в таблицах конфигурации оценивается на влияние этих данных на поведение программы. На уровне модуля структурное тестирование также включает идентификацию «мертвого кода», т. е. кода, выполнения которого нельзя добиться никакой последовательностью кода.

Структурное тестирование интеграции должны выполняться после верификационных испытаний всех используемых модулей и до структурного тестирования на уровне системы. Верификация ППО подтверждает, что выход каждой стадии разработки ППО является правильным по отношению к (т. е. согласуется с) входам(и) для данной стадии. Испытание работоспособности подтверждает, что окончательный продукт ППО, работающий на предназначенных для него аппаратных средствах и в предназначенной для него среде, соответствует предполагаемому продукту, определенному в спецификациях этого продукта и требованиях к ППО.

Структурное тестирование на уровне модулей

Модуль компилируется и устанавливаются связи с драйвером и заглушками в соответствии с требованиями. Драйвером заменяется любой фактический блок, который по прошествии некоторого времени вызовет тестируемый модуль, и если драйвер передает данные тестируемому модулю, то он настроен на передачу значений переменных тестового сценария, таких как максимальные, минимальные и другие номинальные значения, а также значения «стресс-тестов». Заглушки используются вместо любых модулей, вызываемых тестируемым модулем. Как и драйвер, заглушки возвращают данные тестируемому модулю, они также передают значения «стресс-тестов» и номинальных данных там, где это необходимо. Интерфейсы драйверов и заглушек, включая их имена, являются такими же, как и интерфейсы реальных модулей, что позволяет набору этих модулей связываться с тестируемым модулем без внесения в него изменений.

Структурное тестирование на уровне модулей может выполняться на реальных целевых аппаратных средствах, на программе-эмуляторе или программе-симуляторе используемых аппаратных средств или на совершенно другом процессоре, если этого требует ситуация. Последнее возможно, например, если реально используемые аппаратные средства не обладают возможностью определить результаты испытаний модулей, но код был написан на алгоритмическом языке высокого уровня. Таким образом, ППО на языке высокого уровня может быть скомпилировано и установлены связи для работы на другом логическом решающем устройстве, поддерживающем чтение результатов испытаний там, где целевое логическое решающее устройство не может поддерживать испытания.

Структурное тестирование (также известное как испытание методом «белого ящика») выполняется над объектом испытаний, в данном случае — модулем, посредством его внутреннего анализа для определения поведения этого объекта, например посредством определения всех возможных ветвей кода. Основная цель структурного тестирования на уровне модуля заключается в проверке соответствия ППО проекту, включая его логику, корректность алгоритмов и точность (в отличие от параллельного ППО или ручных вычислений), а также корректность блоков инженерных данных. Это требует, чтобы для каждого модуля выполнялись тестирование всех его ветвей, полное тестирование ППО (включая верификацию отсутствия мертвого кода) и «стресс-тесты» (для обнаружения, например, как условий переполнения или потери значащих разрядов, так и номинальных и максимальных значений данных управления циклом). Для разработки критериев приемки (технических условий) используется рабочий проект.

Среда для структурных испытаний на уровнях интеграции и системы

Лучшего всего проводить структурные испытания интеграции и системы на фактически применяемых аппаратных средствах и в реальной среде, насколько это практически возможно. Существует несколько причин для этого, но две наиболее значимые это: a) ППО может обладать малозаметными условиями, как плохими, так и хорошими, которые проявляют себя только при работе с реально используемыми аппаратными средствами; b) готовая ПСБ, включающая предназначенные аппаратные средства и ППО, должна проходить подтверждение соответствия при работе на таких аппаратных средствах, а структурные тестирования должны приблизить разработку ППО к ее завершению. Тем не менее выполнение структурных испытаний частично или целиком в

моделируемой среде имеет свои безусловные основания. Существуют две наиболее распространенные конфигурации при реализации возможностей моделирования: эмуляция логического решающего устройства и моделирование среды или моделирование как логического решающего устройства, так и среды. Принципиальными преимуществами использования моделирования среды и иногда логического решающего устройства считают следующие:

- возможность установить полностью известные входные значения с предварительно определенными результатами для установления критериев приемки каждого испытания;
- симулятор упрощает установление на входах значений, которые выше, ниже и равны предельным значениям критических данных;
- легко установить недопустимые входные значения для испытания всех возможных условий ошибок и отказов;
- можно сразу увидеть результаты каждого испытания.

Структурное тестирование на уровне интеграции

Структурное тестирование интеграции проверяет объединение функционально совместимых модулей верифицированных частей ППО (которые включают части ППО на уровне модулей, прошедшие структурные испытания) посредством компиляции и/или объединения и установления связей между этими частями вместе с любыми требующимися драйверами и заглушками. Затем эта структура загружается в реальную или смоделированную среду для выполнения. Это позволяет специалисту, проводящему испытание, сосредоточиться на одном выбранном наборе функций для подтверждения его правильной работы, включая все внутренние и внешние интерфейсы. После завершения испытания каждого набора функций следующий набор функций может либо подвергнуться отдельному испытанию или быть добавлен к (т. е. связан с) другому(им) уже испытанному(ым) набору(ам). Регрессионное тестирование (т. е. выполнение выбранного подмножества предыдущих, успешно выполненных сценариев испытаний) должно выполняться на уже испытанных наборах для подтверждения того, что новый набор функций не оказывает на них неблагоприятного влияния.

Последовательный (инкрементальный) подход

Последовательный подход для структурных испытаний на уровне интеграции является наилучшим для разработчиков ППО (в отличие от проведения испытаний для подтверждения соответствия третьей стороной — см. ниже), в особенности если ППО является большой и сложной программой. При таком подходе выбранные небольшие, функционально совместимые части ППО компилируются, связываются и испытываются. Такой подход применяется независимо от метода разработки ППО на жизненном цикле, включая любой из следующих трех методов. В «потоковом» методе разрабатываются все требования, затем выполняется проектирование и, наконец, выбранные цепочки выполняемых задач кодируются и подвергаются структурным испытаниям. При «спиральном» методе сначала происходит обсуждение основного устройства ППО системы, а затем разрабатываются требования, проект и код, а структурное тестирование устройства выполняется до обсуждения и разработки следующего основного устройства. Наконец, в последовательном методе разработки все спецификации и требования могут быть разработаны, но проект и его реализация выполняются по одной функции в каждый отдельный момент времени.

В любом случае, если операционная система была уникальным образом разработана специально для испытываемой системы, то она должна сначала пройти структурное испытание. Сама по себе эта часть кода должна быть разбита на функционально совместимые наборы, если она является большой и/или сложной; в противном случае она может подвергнуться структурному испытанию как отдельная сущность. Вторая часть ППО, подвергаемая испытанию, как правило, является уникальным разделом ввода/вывода. Если имеются разнообразные устройства ввода/вывода, то они могут подвергаться структурным испытаниям раздельно. Но часто лучшим решением является выбор цепочки, включающей как способность ввода данных, так и способность наблюдать результат вывода каждого структурного тестирования. Третьим шагом является выбор и структурное тестирование функционально совместимой части приложения и утилит, необходимых для поддержания этого приложения. Затем осуществляется выбор следующей функционально совместимой части ППО и связанных с ней прикладных утилит для следующего структурного тестирования и т. д. Все функции, испытанные прежде, должны подвергнуться регрессионному тестированию по мере необходимости.

Во время проверки формат данных в ППО должен быть верифицирован для подтверждения:

- полноты (например, все функции безопасности были реализованы и все состояния для каждой функции безопасности были рассмотрены);
- внутренней непротиворечивости (например, для всей программы должны поддерживаться единая согласованность и гарантия того, что логика безопасности понятна, не требует разъяснений и визуально отделена от логики, не связанной с логикой ФБ ПСБ, такой как создание отчетов о состоянии);
- защиты от несанкционированного изменения (например, должны применяться два уровня защиты: один уровень на станции прикладного программирования для предотвращения внесения изменений в исходный код приложения без надлежащих полномочий, а второй уровень для защиты ППО от загрузки в ПСБ без надлежащих полномочий);
- согласованности функциональным требованиям (например, обеспечение того, что каждое функциональное требование было правильно интерпретировано);

- согласованности со структурами данных (например, обеспечение читаемости структур данных и использования одного формата во всем ППО);

- совместимости с базовым встроенным программным обеспечением (например, в аспектах последовательности выполнения, времени выполнения программы);

- правильности значений данных (например, использование правильных типов данных, таких как целочисленные или с плавающей запятой, логические и т. п.);

- функционирования в пределах известных безопасных границ (например, проверка диапазона в приложении для поддержания значений в ожидаемом и испытанном диапазоне);

- наличия возможности внесения безопасных изменений.

ППО также должно быть верифицировано для обеспечения защищенности изменяемых параметров от:

- недопустимых или неопределенных начальных значений (например, необходимо обеспечить, чтобы все изменяемые значения, которые могут быть введены, обладали значением по умолчанию, позволяющим обеспечить поддержание ППО в рабочем диапазоне, в случае если пользователь не вводит никаких значений);

- ошибочных значений (например, обеспечить сигнал тревоги или завершить работу, если значение выходит за пределы диапазона, проверенного или ожидаемого процессом);

- несанкционированных изменений (например, необходимо обеспечить предотвращение внесения пользователем несанкционированных изменений или значения не могут быть изменены из-за сбоя в другой системе);

- искажения данных (например, необходимо обеспечить защиту данных от искажения, связанного с любой задачей или системой, не имеющей отношения к безопасности).

Коммуникации, интерфейсы процесса и ППО, связанное с ними, должно подвергаться верификации для обнаружения отказов, обеспечения защиты от подтверждения правильности данных при искажении сообщений, если это уже не было обеспечено устройством, соответствующим МЭК 61508.

Время реакции приложения должно проверяться для всех функций безопасности, чтобы гарантировать, что маршрут данных через приложение позволяет выполнить требование ко времени безопасности процесса. Например, логическая структура может предполагать прохождение ППО через несколько циклов перед завершением выполнения функции безопасности.

А.12.5.4 Дополнительные требования не предусмотрены.

А.12.5.5 После начала формальных проверок все изменения функций ППО и данных о конфигурации должны быть осуществлены в строгом соответствии с установленной процедурой проведения модификаций.

А.12.5.6 Дополнительные требования не предусмотрены.

А.12.6 Руководящие указания к «Требованиям к методологии и инструментам прикладной программы»

А.12.6.1 Дополнительные руководящие указания см. в МЭК 61508-3:2010, приложение D, и ISA TR84.00.09. Дополнительные рассуждения см. также в приложении G. Программисту не следует делать заключений, кроме тех, что определены в инструкции по безопасности: например, что он может использовать возможности компьютера, отсутствующие в инструкции по безопасности. В идеале компьютер должен быть сконфигурирован для обеспечения выполнения подобных ограничений.

Для некоторых ПЭ-систем полный диапазон функций конфигурации может включать общие функции управления, зависящие от алгоритмов, постоянство предсказуемой реакции которых сложно доказать, например функции, использующие алгоритмы с недостоверным завершением (например, рекурсия) или способные привести к исключениям при выполнении программы (например, 'tg 90 градусов'). Для такого типа систем производитель, как правило, предоставляет «ПЭ-инструкцию», определяющую, какие из функций могут применяться для приложений безопасности. Кроме того, там, где используются ПЭ-системы, может потребоваться ограничить способ использования инструментальных средств во избежание тех из них, о которых известно, что они могут приводить к сбоям в работе (подобное, как правило, может быть выявлено в обсуждениях пользователей на интернет-форумах), а также ограничить сложность функций программирования до тех, надежное поведение которых было доказано. В подобном случае в любую инструкцию для ПЭ, поставляемую с ПЭ-системой, потребуется добавить дополнительные процедуры для ограничения использования инструментальных средств (например, для указания хорошей практики программирования, идентификации небезопасных свойств [например, неопределенных языковых функций, незавершающихся алгоритмов)], определить проверки для обнаружения сбоев в конфигурации и указать процедуры для документального оформления ППО, направленные на обеспечение предсказуемости ППО. Если архитектура ПСБ не определена в инструкции для ПЭ, то процедуры должны также включать способ обеспечения отказоустойчивости, например резервирование и разнообразие. Следует рассмотреть необходимость определения любых дополнительных ограничений ППО, таких как сторожевые таймеры, проверки данных.

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.

Типичными разделами инструкции по безопасности ПЭ являются:

a) уровни полноты безопасности, для которых подходит устройство или система;

b) ожидаемое поведение каждой стандартной функции (т. е. для обеспечения четко определенного синтаксиса и семантики используемого языка программирования);

c) правила и ограничения, нацеленные на ограничение использования «небезопасных» свойств прикладного языка и набора инструментов;

d) требования и ограничения для инструментальных средств и языков программирования;

e) использование встроенных сторожевых таймеров;

f) руководство для программиста о том, как использовать средства программирования для проверки правильности применения переменных данных. Необходимо также рассмотреть схему распределение памяти, выполнение проверки индикаторов состояния и проверки правильности входных величин.

А.12.6.2 Набор методов и способов, используемых для разработки ППО, должен быть идентифицирован, и должно быть приведено обоснование их выбора.

Типичный набор средств, поддерживающий прикладное программирование, приведен в приложении Е (раздел Е.1).

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 персонала, вовлеченного в разработку, обслуживание и использование системы;
- обеспечение гарантии 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 — дополнительные указания см. в приложении Е (разделы Е.2 и Е.3);
- детерминированный порядок выполнения и обновления элементов данных.

Методы и способы для устранения сбоев включают проверку, испытание путем моделирования, анализ и аналитическое доказательство — см. также МЭК 61511-1:2016 (подраздел 12.5).

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

- способы проверок и обработку особых ситуаций в ходе функционирования;
- использование внешних баз данных поставщика и полных отчетов о неисправностях;
- мониторинг отчетов об отказах ПСБ и результатов процесса, а также их влияния на ПСБ;
- отображение ключевых функций ПСБ в других системах;
- использование дубликата ППО ПСБ в процессе обучения персонала.

Методы и инструментальные средства для управления модификациями включают: управление конфигурацией и управление версиями, базы данных управления требованиями, обновление исполнительных документов, управление документами и управление изменениями, трассируемость и прослеживание ответственности за изменение, автоматические наборы тестов.

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

- 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;
- предсказуемость поведения подсистем ПСБ;
- совместимость отказоустойчивой архитектуры между проектом ППО и аппаратными средствам.

Среда разработки приложения ПЭ и язык должны соответствовать МЭК 61508-3:2010 (таблица А.3).

Там, где решено использовать инструментальные средства, не поставляемые как часть ПЭ-системы, следует рассмотреть возможности достижения следующего:

- простоты организации ППО;
- предоставления комментариев, встроенных в ППО для объяснения его функций и ожидаемого поведения;
- способов повышения охвата диагностикой до максимального значения и его демонстрации;
- гарантии свойств, важных для ПФБ (например, время выполнения в наихудшем случае);
- наличия соответствующих комментариев и описаний на естественном языке;
- разумной структуризации, отражающей данное применение;
- общности стиля с другими связанными прикладными программами.

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).

Следует рассмотреть доступность инструментальных средств (не обязательно тех, которые используются во время начальной разработки системы) для предоставления соответствующих сервисов на протяжении всего срока жизни ПСБ.

Дополнительное подробное рассмотрение характеристик среды программирования и инструментальных средств см. в приложении Е.

А.13 Заводские приемочные испытания (ЗПИ)

А.13.1 Цели

Целью заводского приемочного испытания (часто включающего в себя испытание интеграции ППО) является демонстрация того, что ПСБ способна реализовывать все требующиеся ФБ ПСБ за требующееся время реакции, соответствует другим функциональным требованиям СТБ и исключает предсказуемое нежелательное поведение.

А.13.2 Руководящие указания к «Рекомендациям»

А.13.2.1 Заводские приемочные испытания (ЗПИ) рекомендуются для логических устройств, которые выполняют ФБ ПСБ и имеют довольно сложную логику или структуру с резервированием (например, «1 из 2», «2 из 3» и т. д.).

А.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.

А.13.2.3 Дополнительные требования не предусмотрены.

А.13.2.4 Дополнительные требования не предусмотрены.

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

А.13.2.6 Дополнительные требования не предусмотрены.

А.13.2.7 Дополнительные требования не предусмотрены.

А.14 Установка и ввод в действие ПСБ

А.14.1 Цели

Дополнительные требования не предусмотрены.

А.14.2 Руководящие указания к «Требованиям»

А.14.2.1 Дополнительные требования не предусмотрены.

А.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.

А.14.2.3 Хотя МЭК 61511-1:2016 рассматривает ввод в действие как отдельную стадию, признается, что объект, опыт проектировщиков и требования проекта могут потребовать проведения ввода в действие за несколько стадий. Конфигурирование инструментальных средств включает настройки, обеспечивающие надлежащее функционирование, соответствующее СТБ или инструкции по безопасности (например, дампирование, линеаризация).

А.14.2.4 Должна быть оформлена документация, демонстрирующая соответствие требующимся конфигурациям (т. е. требования в соответствии с СТБ или инструкцией по безопасности).

А.14.2.5 Дополнительные требования не предусмотрены.

А.15 Подтверждение соответствия безопасности ПСБ

А.15.1 Цель

Цель подтверждения соответствия безопасности ПСБ — подтвердить соответствие ПСБ требованиям, установленным в СТБ. Действия по подтверждению соответствия следует выполнять до введения ПСБ в эксплуатацию.

А.15.2 Руководящие указания к «Требованиям»

А.15.2.1 Дополнительные требования не предусмотрены.

А.15.2.2 План подтверждения соответствия ППО должен быть включен как часть общего плана подтверждения соответствия ПСБ или подсистемы ПСБ.

А.15.2.3 Дополнительные требования не предусмотрены.

А.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 ППО прошло испытания успешно и все проблемы, выявленные в ходе ЗПИ, решены.

Будет 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 ФБ ПСБ выполняются должным образом и что интерфейс оператора обеспечивает его необходимой информацией.

А.15.2.5 Дополнительные требования не предусмотрены.

А.15.2.6 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 после установки и ввода в эксплуатацию всей системы.

А.15.2.7 Дополнительные требования не предусмотрены.

А.15.2.8 Принудительно задавать значения входов и выходов, не выводя ПСБ из обслуживания, должно быть запрещено, если не добавлены одобренные заводом процедуры и не обеспечена безопасность доступа. Любое подобное принудительное изменение должно объявляться или вызывать аварийный сигнал сообразно обстоятельствам.

О прекращении обслуживания должно быть объявлено.

А.16 Эксплуатация и обслуживание ПСБ

А.16.1 Цели

Дополнительные требования не предусмотрены.

А.16.2 Руководящие указания к «Требованиям»

А.16.2.1 Должен быть утвержден план обслуживания ПСБ. План обслуживания должен содержать описание всех возможных режимов с ограниченной функциональностью ПСБ, вызванных отказом в ПСБ или обслуживанием. Следует идентифицировать компенсирующие меры для этих режимов и разработать планы обслуживания. Все действия по обслуживанию должны записываться.

А.16.2.2 В случае, когда отказ и/или байпас ФБ ПСБ реализуется в действующем процессе, вероятность перехода процесса в небезопасное состояние увеличивается. Поэтому должны существовать процедуры для:

- диагностики ситуации отказов, в особенности модели отказов, которая предписывает предпринять соответствующие меры по снижению риска и одновременно предупредить операторов;
- идентификации мер компенсации, позволяющих продолжение работы на допустимом уровне безопасности.

Примечания

1 Пример средств для тестирования диагностики должен вносить искусственный сбой.

2 Анализ видов и последствий отказов является важным набором инструментальных средств для анализа рисков и его рекомендуется использовать;

- осуществления байпаса при выполнении контрольной проверки. Следует применять строго установленные процедуры эксплуатации и меры ослабления рисков для запуска и отключения байпаса (например, получение одобрения перед применением байпаса, предупреждение операторам во время использования байпаса, контроль контура управления перед возвращением в состояние полной работоспособности). Операторы должны быть надлежащим образом обучены методам и процедурам, применяемым для испытания диагностики. Если применяется испытание методом внесения сбоя, то следует рассмотреть отрицательное влияние этого метода, чтобы гарантировать, что по возвращении в состояние полной работоспособности ФБ ПСБ и УПБ системы по-прежнему соответствуют требованиям функциональной безопасности.

Если диагностика указывает на отказ, выявленный тестированием, использующим внесение сбоя, то следует провести надлежащий анализ, чтобы определить причину и влияние данного отказа на ФБ ПСБ и его УПБ и выполнить соответствующие действия:

a) в соответствии с процедурой обслуживания следует решить проблему, связанную со случайным отказом аппаратных средств (например, продолжить обслуживать устройство или сменить его), или

b) необходимо возвратиться на соответствующую стадию жизненного цикла и продолжить в соответствии с процессом управления изменениями, чтобы решить проблему, связанную с отказом системы (например, в случае необнаруженной ошибки при проектировании).

А.16.2.3 Следует рассмотреть следующее:

- причины запроса компенсирующих мер;
- инструкцию по использованию компенсирующих мер и
- каким образом компенсирующие действия приведут процесс к безопасному состоянию, время реакции и последствия в случае отказа выполнения компенсирующих мер;
- следует применять строго установленные процедуры эксплуатации и меры ослабления рисков для запуска и отключения байпаса (например, получение одобрения перед применением байпаса, предупреждение операторам во время использования байпаса, контроль контура управления перед возвращением в состояние полной работоспособности). Операторы должны быть надлежащим образом обучены.

А.16.2.4 Дополнительные требования не предусмотрены.

А.16.2.5 Дополнительные требования не предусмотрены.

А.16.2.6 Дополнительные требования не предусмотрены.

А.16.2.7 Дополнительные требования не предусмотрены.

А.16.2.8 Дополнительные требования не предусмотрены.

А.16.2.9 Дополнительные требования не предусмотрены.

А.16.2.10 Дополнительные требования не предусмотрены.

А.16.2.11 Процедуры контрольных проверок для датчиков и исполнительных элементов должны включать в себя полное испытание их интерфейса для управления газом/жидкостью в технологическом процессе. Испытание, выполненное посредством удаленного доступа, должно оказать влияние на рабочие характеристики ФБ ПСБ.

Примечание — Неавтономное испытание является возможным при использовании местного интеллектуального устройства.

А.16.2.12 Дополнительные требования не предусмотрены.

А.16.2.13 Предположения, сделанные во время определения УПБ, могут повлиять на значение УПБ системы.

Оперативное управление производством должно проверять и верифицировать предположения, сделанные во время определения УПБ, включая загруженность, вероятность предотвращения, процедуры для того, чтобы избежать запросов или снизить их число, а также процедуры, применяемые в случае сигналов, предупреждающих об опасности.

Если подобные предположения отклоняются от фактических текущих условий, то следует провести новый анализ рисков.

А.16.3 Контрольная проверка и осмотр

А.16.3.1 Руководящие указания к «Контрольной проверке»

А.16.3.1.1 Интервал между проведением контрольной проверки следует выбирать из условия достижения средней вероятности отказа при наличии запроса, установленной СТБ.

А.16.3.1.2 Контрольная проверка ПСБ должна отражать реальные рабочие условия так точно, как это возможно. Контрольная проверка должна выполняться перед любой регулярной деятельностью по обслуживанию, которая, скорее всего, исказит любые достоверные результаты тестов.

Контрольную проверку ПСБ предпочтительно проводить в виде комплексного испытания, т. е. весь контур ПСБ должен испытываться целиком. Контрольная проверка может быть выполнена либо как полное комплексное испытание (т. е. контур целиком), либо методом сегментирования (сериями перекрывающих друг друга испытаний на уровне устройств, т. е. датчиков, логических решающих устройств и исполнительных элементов). Контрольная проверка должна включать, но не ограничиваться, верификацией следующих условий:

a) последовательностей логики работы, например представленных диаграммами причинно-следственных связей;

b) работы всех устройств ввода, включая внешние датчики и модули ввода ПСБ;

c) логики, связанной с каждым устройством входа;

d) логики, связанной с объединенными входами;

e) значений, вызывающих останов (уставки) всех входов;

f) функции аварийного сигнала;

g) скорости реакции ПСБ, когда она необходима;

h) работы модулей выхода ПСБ и всех исполнительных элементов;

i) вычислительных функций, выполняемых ПСБ;

j) временного режима и скорости устройств выхода;

k) функционирования ручных действий, приводящих процесс в безопасное состояние;

l) функционирования диагностики, инициированной пользователем;

m) готовности ПСБ к работе после испытания, например после сброса любой блокировки или ручной коррекции.

Если тестирование контура ПСБ невозможно по причинам безопасности или эксплуатационным причинам, то можно выполнить частичное тестирование для устройств или подсистем, являющихся частью контура ПСБ. Некоторые элементы могут быть протестированы в условиях процесса эксплуатации, блокируя входной сигнал или перекрывая выходное действие. Такие элементы, как прямоточные клапаны, приводящие к останову процесса, могут, таким образом, подвергаться испытанию во время запланированных периодов останова.

В тех случаях применения, когда выполняется частичное испытание, необходимо прописать тестовые процедуры, проверяющие все элементы контура:

- проведение проверок исполнительных элементов при останове объекта;
- проведение проверок ПСБ на срабатывание выходных устройств, насколько это практически возможно (например, срабатывание выходного реле отключения, 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 ФБ ПСБ.

Все способы, связанные с резервными архитектурами, должны подвергаться проверочному испытанию для демонстрации того, что все каналы работают правильно, а не только те, которых достаточно для инициации выхода. Это часто требует обеспечения специальных условий для облегчения испытания.

Полное испытание контура ПСБ должно проводиться в заранее определенные временные интервалы.

Те части, которые не были охвачены тестированием, должны быть подтверждены другими способами, например, если невозможно выявить опасные отказы посредством контрольных проверок, то такой элемент должен тщательно проверяться в заранее определенные временные интервалы.

Испытание клапана при неполном ходе может восприниматься как функциональное испытание, охватывающее долю возможных отказов, а не как самотестирование с обеспечением диагностического охвата. Обнаруженная доля отказов должна быть надлежащим образом документально оформлена, используя анализ видов, последствий и диагностики отказов (FMEDA) или подобный ему.

А.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) устройства. После завершения проектирования для этого проекта могут быть проведены расчеты, определяющие максимально допустимый интервал между проверками, позволяющий достигнуть эксплуатационного УПБ, установленного для ФБ 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).

Следует обратить внимание, что $ВОНЗ_{ср}$ является вероятностью, зависящей от времени, которая с увеличением времени возрастает. Таким образом, в случае больших временных интервалов контрольных проверок эта вероятность может быть очень высокой, даже если в среднем целевой УПБ достигнут, и это может стать очень ненадежным индикатором риска. Такое не может быть допустимо, но проведение испытаний с временным сдвигом в какой-то мере смягчает последствия этой проблемы.

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, устройства и степень диагностического охвата, 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.

Кроме того, остановы, связанные с фактическими запросами к ПСБ, во время ее работы могут «засчитываться» в качестве контрольных проверок (полностью или частично) при заданных условиях, таких как:

- информация в том виде, в каком она была зарегистрирована во время соответствующей контрольной проверки, эквивалентна документам по останову;
- останов охватывает все части ПСБ и если это не так, то устройства или подсистемы ПСБ, которые не были активны, должны испытываться отдельно;
- останов происходит в заранее определенное временное окно перед следующей запланированной контрольной проверкой, которая после него может быть отменена.

Если эти условия выполнены, то следующую запланированную контрольную проверку можно пропустить.

При выборе интервала между контрольными проверками следует рассмотреть интенсивность запросов (для систем, работающих в режиме по запросам), интенсивности отказов для каждого из проверяемых компонентов и общие требования к рабочим характеристикам системы.

А.16.3.1.4 Дополнительные требования не предусмотрены.

А.16.3.1.5 Дополнительные требования не предусмотрены.

А.16.3.1.6 Дополнительные требования не предусмотрены.

А.16.3.1.7 Дополнительные требования не предусмотрены.

А.16.3.2 Руководящие указания к «Осмотру»

Как указано в МЭК 61511-1:2016, осмотр ПСБ отличается от контрольной проверки. В то время как контрольная проверка обеспечивает правильную работу ПСБ, визуальный осмотр требуется для того, чтобы проверить механическую целостность установки.

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

Примечания

1 Осмотр может выявить возникающие отказы, которые не обнаруживаются контрольной проверкой.

2 Компонент, подсистема или система ПСБ, находящаяся в неудовлетворительном состоянии, обладает большей вероятностью иметь высокую интенсивность отказов (λ), чем та, которую приняли в результате вычислений ВОНЗ$_{ср}$ и остаточного риска. Неудовлетворительное состояние любых подобных элементов может быть устранено.

А.16.3.3 Руководящие указания к «Документальному оформлению контрольной проверки и осмотра»

Важно, чтобы результаты контрольных проверок 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 устройства.

Например, если при контрольных проверках 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 контрольных проверок. Если история показывает наличие повторяющихся отказов, следует рассмотреть вопрос о перепроектировании ПСБ с использованием датчика другого типа.

А.17 Модификация ПСБ

А.17.1 Цели

Под модификацией в основном понимают изменения, вносимые на этапе эксплуатации ПСБ.

А.17.2 Руководящие указания к «Требованиям»

А.17.2.1 Любое изменение ПСБ (подсистемы или компонентов) является модификацией, если это изменение не являлось равнозначной заменой. Подобные модификации могут включать проблемы, связанные:

- с новым интервалом проведения контрольной проверки или ее процедурами;
- компонентами с различными характеристиками, например в случае замены устаревших компонентов;
- изменениями уставок;
- изменениями в условиях работы;
- изменениями в рабочих процедурах;
- изменениями в прикладном программном обеспечении или встроенном;
- исправлениями систематических отказов;
- интенсивностью отказов более высокой, чем желаемая;
- повышенной интенсивностью запросов.

А.17.2.2 Дополнительные требования не предусмотрены.

А.17.2.3 Там, где это представляется возможным, следует избегать модифицирования ППО ПСБ при действующем процессе. Если требуется осуществить модификацию при действующем процессе, то следует документально оформить и одобрить всю процедуру целиком в соответствии с планированием безопасности.

А.17.2.4 Дополнительные требования не предусмотрены.

А.17.2.5 Дополнительные требования не предусмотрены.

А.17.2.6 Дополнительные требования не предусмотрены.

А.17.2.7 Дополнительные требования не предусмотрены.

А.17.2.8 Дополнительные требования не предусмотрены.

А.18 Снятие с эксплуатации ПСБ

А.18.1 Цели

Дополнительные требования не предусмотрены.

А.18.2 Руководящие указания к «Требованиям»

А.18.2.1 Дополнительные требования не предусмотрены.

А.18.2.2 Дополнительные требования не предусмотрены.

А.18.2.3 Дополнительные требования не предусмотрены.

А.18.2.4 Дополнительные требования не предусмотрены.

А.18.2.5 Дополнительные требования не предусмотрены.

А.19 Требования к информации и документации

А.19.1 Цели

Примеры структуры документов см. в МЭК 61508-1:2010, приложение А, а более подробное — в МЭК 61506. Документация может предоставляться в различном виде (например, бумажном, на пленке или любом носителе данных, позволяющем отображение на экранах и дисплеях). Только в целях иллюстрации в приложениях приведено множество разнообразных примеров документации.

А.19.2 Руководящие указания к «Требованиям»

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

a) результаты анализа опасностей и риска;

b) распределение слоев защиты;

c) допущения, используемые при определении требований к полноте;

d) СТБ-спецификации;

e) логику применения;

f) проектную документацию;

g) информацию и/или документацию по изменениям;

h) записи результатов верификации и подтверждения соответствия;

i) процедуры ввода в эксплуатацию и подтверждения соответствия ПСБ;

j) эксплуатационные процедуры ПСБ;

k) процедуры обслуживания ПСБ;

l) процедуры контрольных проверок;

m) результаты проведения оценок и аудитов.

А.19.2.2 Системы ПСБ следует идентифицировать и документально оформить таким образом, чтобы было проведено четкое различие между ними и другими системами, не связанными с безопасностью, такими как ОСУП.

А.19.2.3 Дополнительные требования не предусмотрены.

А.19.2.4 Дополнительные требования не предусмотрены.

А.19.2.5 Дополнительные требования не предусмотрены.

А.19.2.6 Дополнительные требования не предусмотрены.

А.19.2.7 Дополнительные требования не предусмотрены.

А.19.2.8 Типичный список документов, предусмотренный в результате выполнения проекта ПСБ, см. в приложении F (раздел F.26).

А.19.2.9 Дополнительные требования не предусмотрены.

Приложение В
(справочное)

Пример разработки прикладной программы логического решающего устройства ПСБ с помощью функциональных блок-схем

В.1 Общие положения

Следующие примеры описывают:

- метод организации действий, связанных с разработкой ППО, удовлетворяющий МЭК 61511-1:2016 (подраздел 6.3);
- формирование СТБ ППО на основе СТБ ПСБ, тем самым отвечая на вопрос МЭК 61511-1:2016 (пункт 10.3.2);
- разработку и реализацию двух функций останова в ППО, удовлетворяющих МЭК 61511-1:2016 (пункты 7.2.2 и 11.5.2, раздел 12 и пункт 15.2.2).

В.2 Принципы разработки и подтверждения соответствия прикладных программ

Чтобы помочь инженерам, разрабатывающим ППО, спроектировать такие ФБ ПСБ, эффективность которых можно предсказать и полнота безопасности которых будет соответствовать запрошенной (например УПБ 3) необходимо иметь эффективную методологию разработки.

При традиционном подходе инженеры по проектированию ППО способны провести полное испытание проекта ППО только на последних этапах проектирования, когда уже доступна реальная структура аппаратных средств. Такой метод является очень неэффективным, так как при обнаружении ошибки на данном этапе им придется вернуться к соответствующей стадии проектирования, чтобы исправить эти ошибки и выпустить новую версию, что, в свою очередь, приведет к значительному увеличению временных и денежных затрат, связанных с разработкой конечного продукта.

Традиционный поход к созданию спецификации ППО, основанный на тексте, недостаточно эффективен при работе с расширенными, сложными требованиями к безопасности, которые, как правило, представлены в спецификациях на ФБ ПСБ.

Наиболее эффективным инструментом для решения таких проблем является проектирование, основанное на модели (MBD). MBD является математическим и визуальным методом рассмотрения проблем, связанных с проектированием сложных систем безопасности, и этот метод успешно применяется во множестве приложений. Он предоставляет эффективный подход для преодоления трудностей стадии разработки жизненного цикла системы безопасности. Данный подход и этот пример включают следующие шаги:

- моделирование СТБ ППО с помощью:
  - идентификации рассматриваемых элементов ПСБ;
  - описания их поведения, используя надлежащий язык моделирования;
- анализ и синтез поведения предусмотренной реализации СТБ ППО с учетом их выполнения;
- демонстрацию соответствия реализации ППО требованиям СТБ, необходимую для документального оформления процесса подтверждения соответствия и выполнения требований МЭК 61511-1:2016 (подраздел 12.5 и раздел 15).

Это позволяет найти и исправить ошибки на ранних стадиях проектирования ППО, когда влияние временных и финансовых факторов минимально. В методологии MBD повторное проектирование выполняется более легко как для обновления ППО, так и для разработки более развитого ППО с расширенными возможностями. MBD предоставляет общую среду проектирования для всех разработчиков, облегчая общие коммуникации, анализ данных и верификацию ППО для различных групп разработчиков.

Текстовые спецификации и симуляция применялись довольно долгое время, но они очень неэффективны и неадекватны при работе с расширенными и сложными характеристиками ФБ ПСБ, так как эти средства по своей сути абсолютно не представимы графически и не имеют математического аппарата для оценки результата. В связи с ограничениями графических инструментальных средств инженеры по проектированию привыкли во многом полагаться на традиционное текстовое программирование и математические модели. И это являлось основной причиной неуверенности в обеспечении полноты безопасности, так как разрабатываемые модели в программах, основанных на тексте, являлись не только сложными и требующими больших затрат времени, но и были значительно подвержены ошибкам. Отладка модели и исправление ошибок являлось трудоемким процессом. Требовалось множество прогонов и исправления ошибок для достижения окончательной модели без сбоев, так как функциональная модель претерпевает незаметные изменения при ее преобразовании для различных стадий проектирования. На сегодняшний день подобные трудности преодолеваются при помощи специальных средств графического моделирования, поддерживаемых пакетами для разработки программ, удовлетворяющими МЭК 61511-1:2016 (подраздел 12.6) и охватывающими весь жизненный цикл ППО системы безопасности, представленный в МЭК 61511-1:2016 (пункт 6.3.1). Это позволяет в едином репозитарии как разрабатывать спецификации, так и осуществлять этап реализации, в результате появляется возможность подтвердить свойства полноты безопасности при достаточно низких затратах по сравнению с ручными методами. Подобные общие принципы разработки ППО, представленные данным примером, легли в основу реализации практики проектирования, основанной на модели.

Для поддержки проектирования и подтверждения соответствия будут последовательно реализованы, постепенно интегрированы и использованы следующие модели:

- функциональные модели:
  - модель функциональной архитектуры аппаратных средств;
  - модель физической архитектуры аппаратных средств;
  - модель функциональной архитектуры ППО;
  - модель архитектуры ППО;
- модели свойств безопасности:
  - временных свойств;
  - свойств полноты безопасности;
  - модель проверки.

Эти модели интегрируются постепенно для того, чтобы последовательно продемонстрировать соответствие ППО спецификациям СТБ ППО.

Эти модели применяются:

- для проектирования как реализации спецификации, а именно подробной спецификации функциональной полноты и полноты безопасности;
- разработки ППО с автоматической компиляцией;
- выполнения полуавтоматического испытания при проверке модели, предназначенного для верификации соответствия каждого модуля ППО функциональным спецификациям и спецификациям безопасности;
- выполнения подтверждения соответствия, предоставляя исчерпывающую информацию о степени охвата испытанием и результатах испытаний.

B.3 Описание приложения

B.3.1 Общие положения

В данном примере рассматривается часть ПСБ, предназначенная для установки по производству сжиженного природного газа (LNG).

B.3.2 Описание процесса

Процесс, описанный в данном примере, является одним из процессов терминала сжиженного природного газа. Целью данной установки является получение LNG с кораблей для хранения и подготовки LNG к вводу в газораспределительную сеть.

B.3.3 Функции безопасности ПСБ

B.3.3.1 Общие положения

ПСБ для описанного выше процесса включает 7 ФБ ПСБ с УПБ 3 и 64 ФБ ПСБ с УПБ 2. Основное внимание в примере сосредоточено на одной ФБ ПСБ с УПБ 3 и одной ФБ ПСБ с УПБ 2. Приведенная ниже информация может рассматриваться как часть СТБ и применяться в качестве входных данных для СТБ ППО.

B.3.3.2 ФБ ПСБ 02.01 — Аварийный останов разгрузки LNG

Часть процесса, охватываемая этой функцией, представлена на рисунке B.1.

Целью этой функции с УПБ 2 является изоляция судна от объекта в случае, если в одном из трех резервуаров LNG выявлено сверхвысокое давление.

Запрос функции возникает, когда обнаруживается сверхвысокое давление и срабатывает реле датчика давления (датчики на рисунке B.1 не показаны) в любом из трех резервуаров LNG. Затем в результате выполнения функции происходит закрытие трех клапанов (XV1008, XV2008 и XV3008). Если затем по истечении заданного периода времени сверхвысокое давление по-прежнему не снижается, то закрываются два дополнительных клапана (XV1014 и XV2014). Клапаны останутся закрытыми до переустановки системы, даже если сигнал о сверхвысоком давлении исчезнет.

B.3.3.3 ФБ ПСБ 06.02 — Аварийное закрытие впускного клапана ORV

Часть процесса, обслуживаемая данной функцией, представлена на рисунке B.2.

Целью этой функции с УПБ 3 является отключение каждой открытой стойки выпаривателя (ORV) посредством закрытия впускного клапана XV1001 и запорного клапана XV1013 в случае обнаружения очень низкой температуры (датчики на рисунке B.2 не показаны) на отводящем трубопроводе с помощью реле датчика температуры. Эти клапаны не должны закрываться одновременно, чтобы избежать захвата газа в контуре между клапанами. Клапаны останутся закрытыми до переустановки системы, даже если сигнал об очень низкой температуре исчезнет. Закрытие обоих запорных клапанов приводит к опасному состоянию. Предотвращение опасного состояния соответствует УПБ 2.

B.3.4 Снижение риска и эффект «домино»

Анализ рисков устанавливает, что запрос к обеим ФБ ПСБ в одно и то же время может быть опасен и не должен происходить.

B.4 Выполнение жизненного цикла прикладной программы системы безопасности

B.4.1 Общие положения

Настоящий подраздел последовательно описывает:

- входные данные, необходимые для разработки СТБ ППО, получаемые из СТБ;
- разработку СТБ ППО (МЭК 61511-1:2016, пункт 10.3.2);

- проектирование архитектуры ППО (МЭК 61511-1:2016, раздел 12);
- моделирование, проектирование и испытание ППО (МЭК 61511-1:2016, пункты 12.3 и 12.4);
- испытание и моделирование интеграции ППО (МЭК 61511-1:2016, пункты 12.4 и 12.5);
- создание ППО;
- участие в подтверждении соответствия ПСБ (МЭК 61511-1:2016, раздел 15).

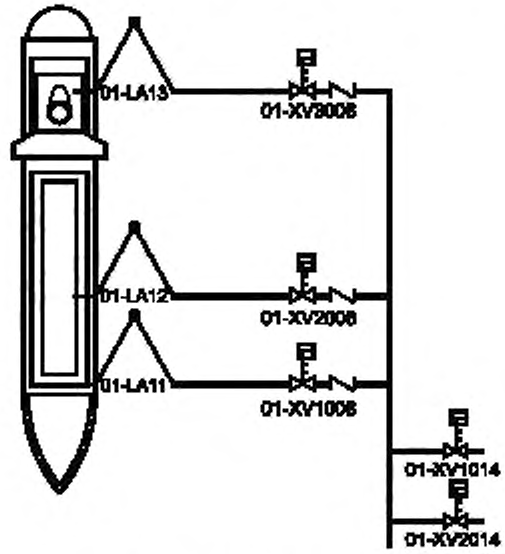


Рисунок В.1 — Технологическая схема для ФБ ПСБ 02.01

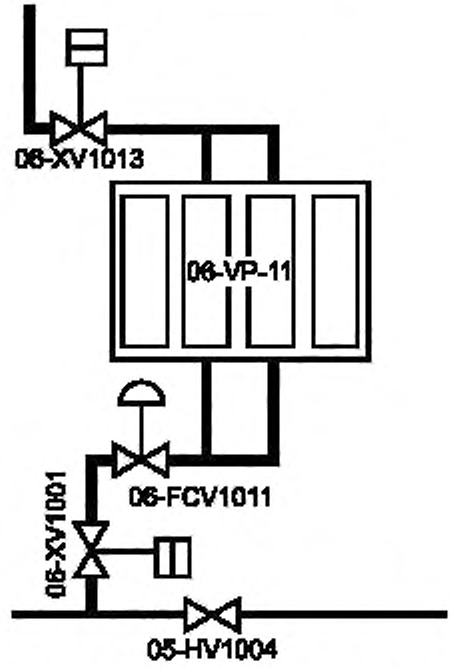


Рисунок В.2 — Технологическая схема для ФБ ПСБ 06.02

В.4.2 Входные данные для разработки СТБ прикладной программы

В.4.2.1 Общие положения

Далее представлены входные данные, получаемые от предыдущих стадий жизненного цикла.

В.4.2.2 Функциональная спецификация

Функциональная спецификация, возникающая из уточнения требований, описанных на рисунках В.1 и В.2, представлена на рисунке В.3. Эти схемы описывают ожидаемое поведение ФБ ПСБ перед принятием любых решений о будущих необходимых аппаратных средствах и прикладном программном обеспечении для реализации этих функций.

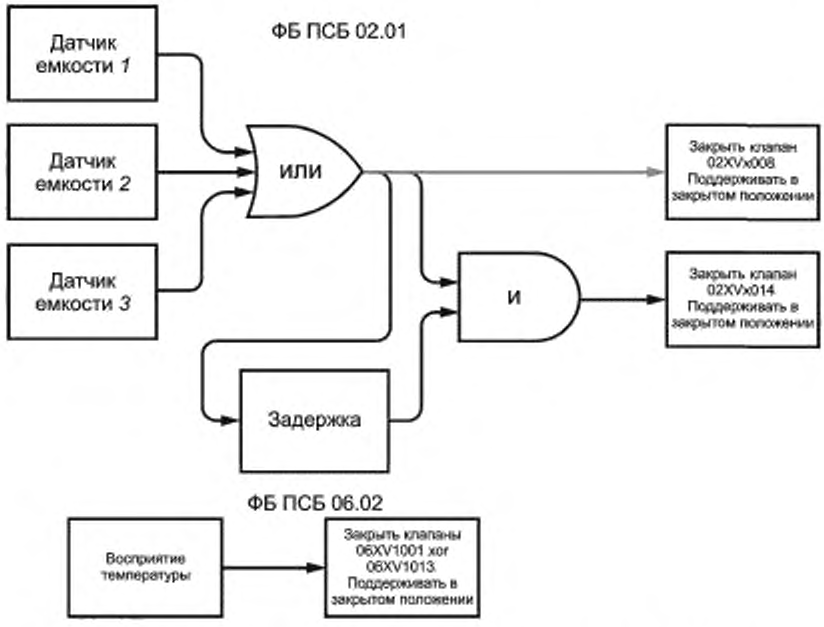


Рисунок В.3 — Функциональная спецификация ФБ ПСБ 02.01 и ФБ ПСБ 06.02

В.4.2.3 Функциональная архитектура аппаратных средств

Эти схемы показывают архитектуру аппаратных средств, необходимую для реализации ФБ ПСБ перед применением ограничителей HFT и каких-либо других требований СТБ.

ФБ ПСБ 02.01

Функциональная архитектура аппаратных средств представлена на рисунке В.4.

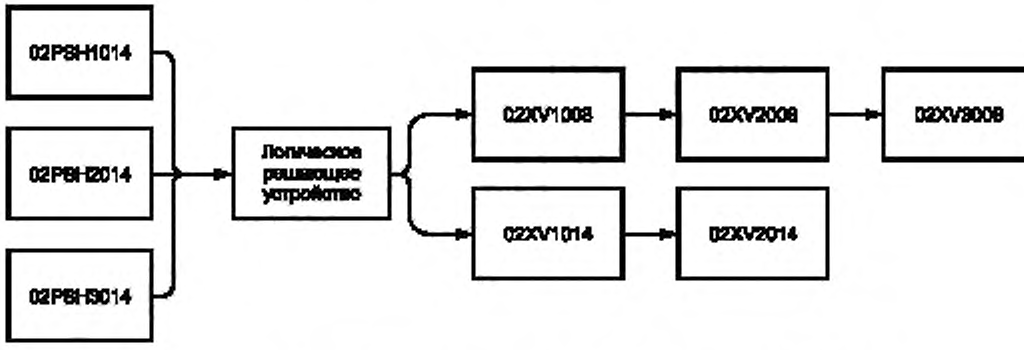


Рисунок В.4 — Функциональная архитектура аппаратных средств ФБ ПСБ 02.01

ФБ ПСБ 06.02
Функциональная архитектура аппаратных средств представлена на рисунке В.5.

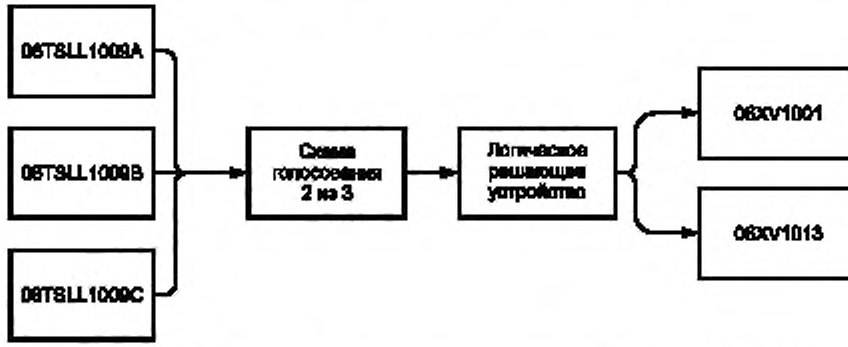


Рисунок В.5 — Функциональная архитектура аппаратных средств ФБ ПСБ 06.02

В.4.2.4 Типичная спецификация аппаратных средств для соленоидных клапанов (SOV)/клапанов с электроприводом (MOV)

Схема трубопроводов и контрольно-измерительной аппаратуры, как правило, описывает все интерфейсы аппаратных средств и ППО устройства. На рисунке В.6 показаны интерфейсы аппаратных средств и ППО, предназначенные для реализации с SOV как в ОСУП, так и в ПСБ.

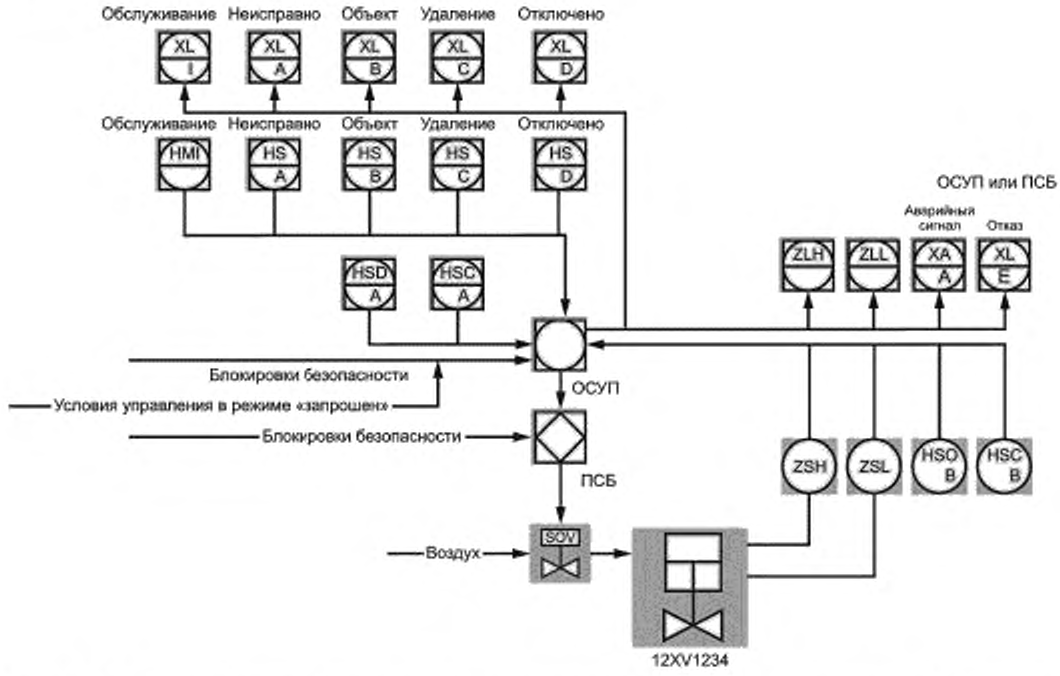


Рисунок В.6 — Спецификация аппаратных средств для реализации с SOV, выделенная из схем трубопроводов и контрольно-измерительной аппаратуры

В.4.2.5 Спецификация архитектуры аппаратных средств на физическом уровне

Уточнение полученных требований, описанных на рисунках В.4 и В.5, ведет к определению реальных аппаратных средств, предназначенных для использования, и их окончательной архитектуре, как это представлено на рисунках В.7 и В.8.

Примечания

1 Описание применения требований к отказоустойчивости аппаратных средств, полученных из требований в МЭК 61511-1:2016 (раздел 11), в настоящем примере не обсуждается.

2 В данном примере канал связи между ОСУП и ПСБ является дискретным (реализован аппаратно).

ФС ПСБ 02.01

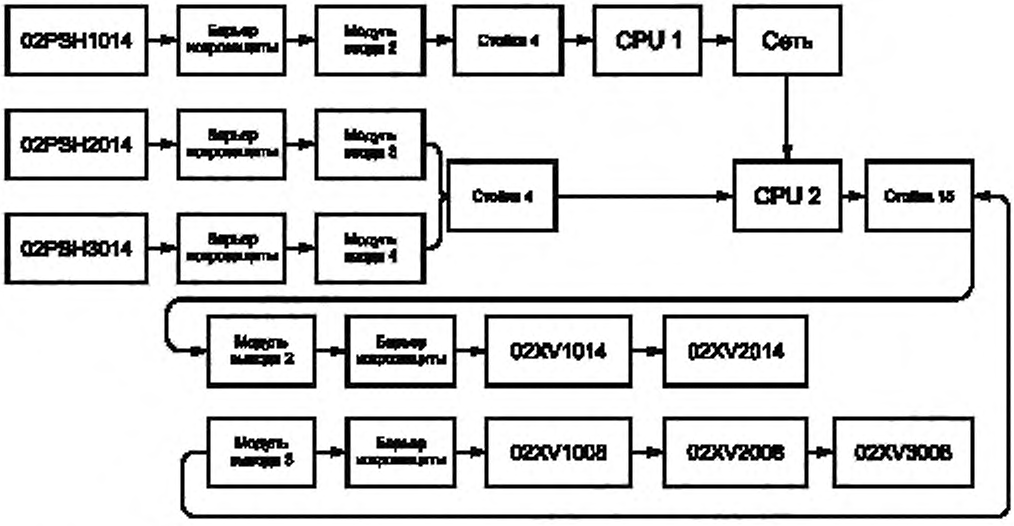


Рисунок В.7 — Физическая архитектура аппаратных средств ФБ ПСБ 02.01

ФС ПСБ 06.02

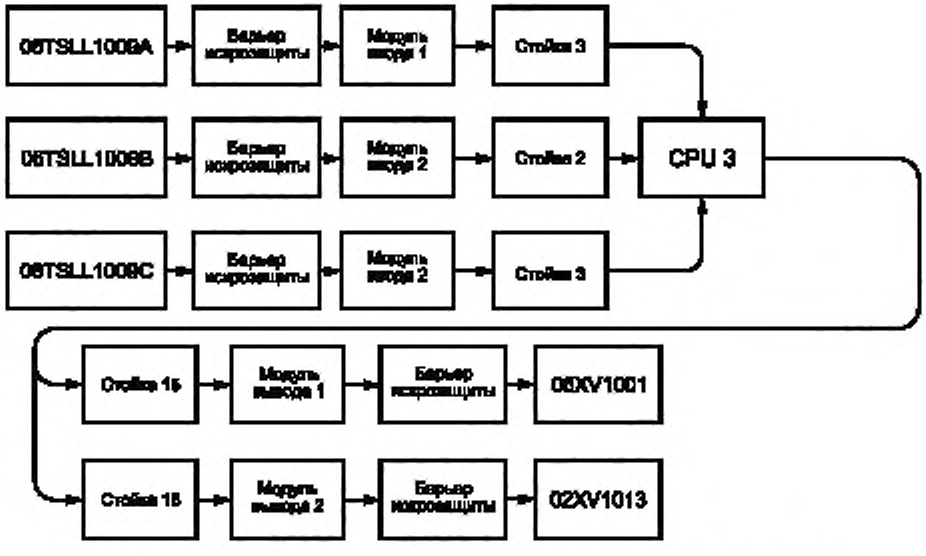


Рисунок В.8 — Физическая архитектура аппаратных средств ФБ ПСБ 06.02

В.4.3 Проектирование и разработка прикладной программы

В.4.3.1 Общие положения

Настоящий пункт включает примеры для описания следующих шагов:

- разработка СТБ ППО;
- проектирование функциональной архитектуры ППО;

- функциональное проектирование, моделирование и испытание ППО;
- моделирование и испытание интеграции ППО.

В.4.3.2 СТБ прикладной программы

В.4.3.2.1 Общие положения

СТБ ППО может быть организована следующим образом:

- функциональные требования, соответствующие ожидаемым поведениям:
  - требования к устройствам (датчикам и исполнительным устройствам);
  - требования к блокировкам каждой ФБ ПСБ;
  - требования к блокировкам между ФБ ПСБ;
- требования к полноте безопасности, соответствующие поведениям, которых следует избегать:
  - на уровне устройства;
  - на уровне ФБ ПСБ;
  - на более высоком уровне, таком как уровень объекта (завода).

В.4.3.2.2 Спецификация функциональных требований к прикладной программе

В.4.3.2.2.1 Функциональные требования к устройству

Функциональные требования к устройству могут быть описаны для каждого типа устройства и разделены на требования:

- к базовым эксплуатационным режимам устройства и
- функциональной спецификации устройства.

Пункт В.4.3.2 содержит пример для SOV.

Общие рабочие режимы исполнительных устройств: конечный автомат для рабочих режимов соленоидного клапана (SOV) определен в таблице В.1.

Таблица В.1 — Спецификация режимов работы

Название состояния	Описание
Запрос	Когда условия безопасности генерируют последовательность действий по безопасности, то поступает запрос на управление клапаном логикой более высокого уровня. Подобный запрос имеет наивысший приоритет по сравнению с любым другим рабочим режимом. Затем устройство фиксируется в запрошенном режиме. Его отдельные компоненты становятся недоступны, а клапан управляется только логикой более высокого уровня. Когда логика снимает условия безопасности, осуществляется принудительный переход из рабочего режима в режим УДАЛЕНИЯ, после этого оператор может изменить режим работы
Удаление	Управление клапаном осуществляется с помощью команд открытия и закрытия человеко-машинного интерфейса ОСУП. Это состояние является начальным
Локальное	Управление клапаном осуществляется с помощью командных кнопок открытия и закрытия, расположенных рядом с клапаном
Неисправен	Данный режим возможен, только если клапан уже находится в своем безопасном положении. Все локальные и удаленные команды оператора становятся недоступны. Управление осуществляется с помощью условий безопасности
Обслуживание	Данный режим возможен, только если клапан уже находится в безопасном положении. Осуществляется принудительный переход в состояние «Неисправен», и все аварийные сигналы блокируются

Функциональная спецификация SOV.

Устройство является запорным электромагнитным клапаном, управляемым от ПСБ и ОСУП.

Предполагается, что в случае опасности, от которой защищает ФБ ПСБ, SOV имеет единственное и постоянное безопасное положение. Это положение закрытое.

SOV является автономным устройством: он воспринимает отдельные команды от ОСУП и может при определенных обстоятельствах находиться под управлением логики более высокого уровня. Логика управления таким устройством, как SOV, называется «типовым набором».

Типовой набор для данного SOV позволяет реализовать следующее:

- команды открытия и закрытия от станций оператора ОСУП;
- локальные команды открытия и закрытия, поступающие от объекта через ОСУП;
- переход в безопасное положение, инициированный ПСБ или ОСУП;
- передачу по кабелю команды открытия и закрытия из ПСБ;
- выбор рабочего режима на станции оператора ОСУП с помощью программируемого переключателя;
- реорганизацию команд в следующих случаях:
  - реорганизацию команд при получении информации от концевых переключателей при инициализации;
  - реорганизацию команд при блокировках логики более высокого уровня в запрошенном режиме;
  - реорганизацию команд по командам объекта в режиме объекта;
  - реорганизацию команд при безопасном состоянии в случае действий по обеспечению безопасности;

- работу в состоянии обслуживания;
- визуализацию положения клапана на основе информации от двух концевых переключателей;
- генерацию аварийного сигнала о конфликте (при открытии или закрытии, одновременном распознавании обоих концевых переключателей, отказе концевого переключателя). Чтобы избежать генерации ложных аварийных сигналов о конфликте, информация концевого переключателя задерживается, чтобы позволить ПСБ передать команду в ОСУП;
- обнаружение отказов ОСУП и ПСБ;
- модификацию настройки и параметров настройки.

Параметры: задержка обнаруженного конфликта.

Доступ только на уровне обслуживания.

B.4.3.2.2.2 Функциональные требования к ФБ ПСБ

Функциональные требования для каждой функции безопасности описаны в СТБ.

B.4.3.2.2.3 Функциональные требования к блокировкам между ФБ ПСБ

На данном уровне функциональные требования отсутствуют.

B.4.3.2.3 Спецификация требований к полноте безопасности

B.4.3.2.3.1 Требования к полноте устройства

Существуют следующие требования к полноте безопасности устройства:

- никакая комбинация блокировок не должна мешать команде устройства, реализующей переход в его безопасное положение при появлении запроса;
- никакая комбинация блокировок не должна задерживать команду SOV более чем на 100 мкс;
- никакая комбинация блокировок не должна приводить к неопределенному или нестабильному состоянию физического устройства при выполнении команды;
- все условия перехода конечного автомата должны быть исчерпывающими и исключительными;
- должны быть определены действия каждого условия конечных автоматов.

B.4.3.2.3.2 Требования к полноте ФБ ПСБ

Существуют следующие требования к полноте ФБ ПСБ:

- если входные данные действительны, то никакая комбинация блокировок не должна помешать ФБ направить запрос типовому набору ППО для SOV;
- никакая комбинация блокировок не должна задерживать запрос к SOV более чем на 100 мкс;
- никакая комбинация блокировок не должна приводить к неопределенному или нестабильному состоянию физического устройства при выполнении команды.

B.4.3.2.3.3 Требования к полноте блокировок между ФБ УПБ

Существуют следующие требования к полноте ФБ ПСБ:

- никакая комбинация блокировок или запросов не должна приводить к одновременному запросу к ФБ ПСБ 02.01 и ФБ ПСБ 06.02.

B.4.3.3 Проектирование функциональной архитектуры прикладной программы

B.4.3.3.1 Проектирование архитектуры

Деятельность по проектированию архитектуры ППО должна обеспечить, чтобы результирующая архитектура:

- соответствовала МЭК 61511-1:2016 (пункт 12.4.4);
- никаким образом не ухудшала систематическую полноту архитектуры аппаратных средств, заданную в СТБ.

Архитектура ППО строится иерархически. Предлагаются следующие уровни и модули ППО:

- типовой набор для ППО устройств: в данном примере рассматриваются соленоидные клапаны; датчики давления и температуры. Эти модули содержат логику, необходимую для управления устройством, сбора и обработки входных данных, стандартных сложных функций, таких как голосование;
- логика ФБ ПСБ: блокирование модулей ППО для реализации ожидаемого поведения ФБ ПСБ;
- логика объекта: блокирование ФБ ПСБ.

Эти модули ППО описаны с помощью графического языка автоматизированной среды проверки моделей и представляют собой модели, отражающие ожидаемое поведение разрабатываемых модулей ППО. Все эти модули представляют завершенное ППО, которое создано для ФБ ПСБ, и может быть скомпилировано и загружено в целевые логические решающие устройства.

Список необходимых модулей (ограничен рассматриваемым примером):

- типовой набор SOV;
- голосование «2 из 3»;
- обработка коммуникаций сети;
- обработка датчиков;
- логика ФБ ПСБ 02.01;
- логика ФБ ПСБ 06.02.

Все модули объединены (интегрированы) в соответствии со структурой, описанной на рисунке B.9.

B.4.3.3.2 Требования к полноте безопасности, полученные из архитектуры

B.4.3.3.2.1 Общие положения

Данная архитектура никаким образом не должна подвергать риску систематическую полноту безопасности физических аппаратных средств, определенную в B.4.3.3.1.

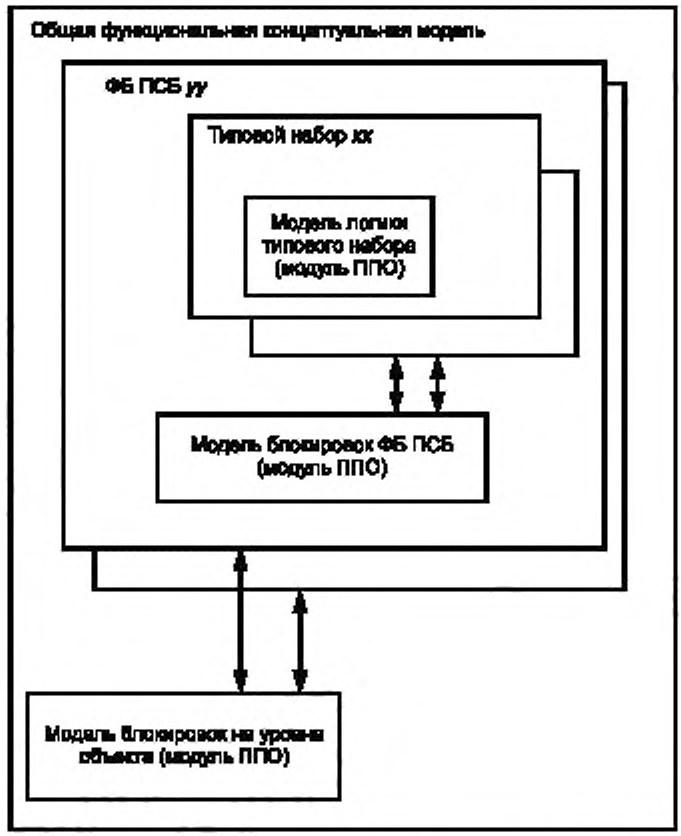


Рисунок В.9 — Иерархическая структура интеграции моделей

Эта проблема далее более подробно не обсуждается, так как она непосредственно зависит от характеристик выбранных логических решающих устройств. Но, как минимум, выясняется, что для ФБ ПСБ 02.01 есть необходимость анализа последствий распределения модулей ППО между CPU 1 и CPU 2 на систематическую полноту безопасности этой ФБ ПСБ. Для этого требуется анализ комбинаций видов отказов аппаратных средств вместе с видами отказов ППО. Такой анализ, как правило, выполняется с помощью построения дерева отказов, включая в него отказы, характерные для модулей ППО (независимые от аппаратных средств, на которых оно установлено), и направлен на определение того, существует ли отказ системы вследствие отказа одного элемента, который негативно влияет на ОАС.

Кроме того, определение архитектуры ППО позволяет определить выводимые из нее СТБ ППО, которые необходимо распределить для каждого модуля ППО.

В.4.3.3.2.2 Требования к целостности устройства

Требования к устройству:

- все условия перехода конечного автомата должны быть исчерпывающими и исключительными;
- действия каждого условия конечного автомата должны быть определены.

В.4.3.3.2.3 Требования к полноте функции безопасности ПСБ

Выводимые требования:

- никакая комбинация динамических значений переменных, обеспечивающих интерфейс между блокировками ФБ ПСБ и связанными с ней модулями, не должна приводить к неопределенному или нестабильному состоянию ФБ ПСБ.

Примечание — Это требование не повторяет требование В.4.3.3.1. В.4.3.3.1 связан с логикой функционального статического поведения. Настоящее требование связано с логикой динамического поведения, распределенного между двумя CPU и возникающего из проекта архитектуры.

В.4.3.3.2.4 Требования к полноте на уровне объекта

Никаких производных требований.

В.4.3.4 Функциональное проектирование, моделирование и испытание прикладной программы

В.4.3.4.1 Проектирование и испытание функциональных моделей модулей прикладной программы

Необходимые модули ППО, идентифицированные в архитектуре ППО, моделируются в автоматизированной среде разработки и проверки моделей. Помимо этого, создаются модели для описания:

- поведения физических устройств;
- поведения человеко-машинного интерфейса;
- необходимых свойств безопасности устройств;
- необходимых свойств безопасности ФБ ПСБ;
- необходимых свойств безопасности на уровне объекта;
- физического поведения объекта (блокировка техническими жидкостями);
- части логики ОСУП.

Это необходимо для обеспечения требующихся свойств моделируемых ФБ ПСБ их функциональным и физическим контекстом.

Все модули ППО интегрируются в одну функциональную модель для проверки в соответствии со структурой, описанной на рисунке В.10.

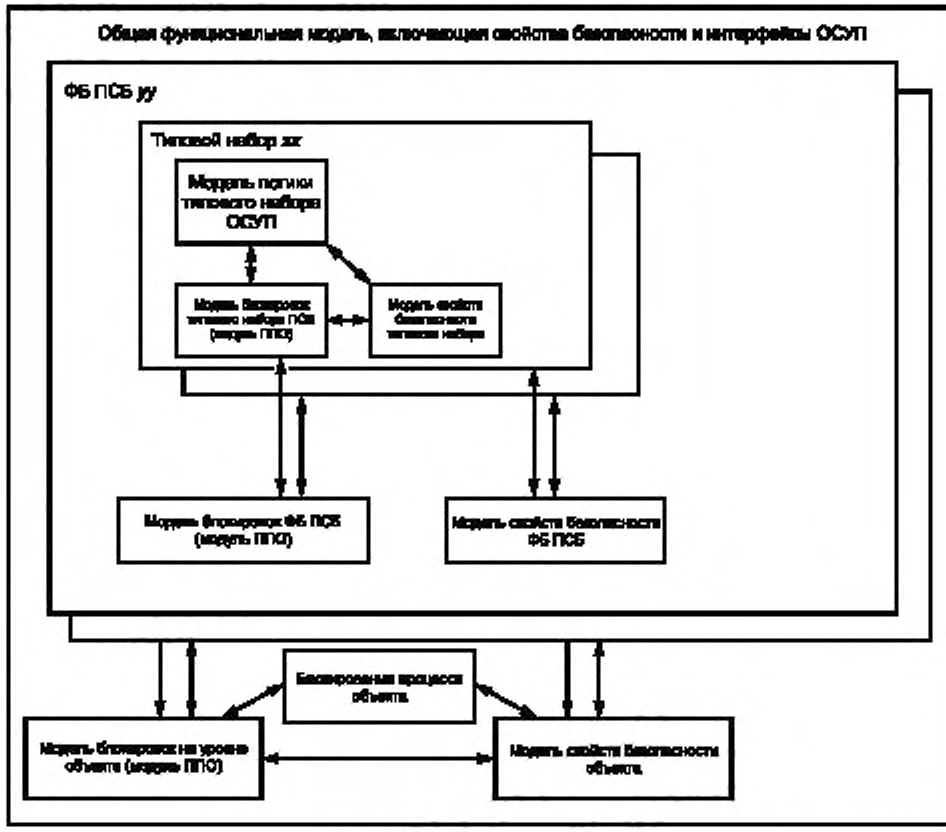


Рисунок В.10 — Иерархическая структура интеграции моделей, включающая модели свойств безопасности и логики ОСУП

В.4.3.4.2 Описание моделей

В.4.3.4.2.1 Уровень прикладных программ типового набора

Модель логики управления SOV из ОСУП.

Уточнение требований к режимам работы из таблицы В.1 позволяет получить подробное описание проекта логики управления SOV, представленное с помощью диаграммы состояний.

Пример таблицы переходов состояний приведен в таблице В.2.

Из таблицы переходов состояний В.2 может быть получена диаграмма переходов состояний, представленная на рисунке В.11.

Таблица В.2 — Таблица переходов состояний

Состояния/Следующие состояния	Условие перехода	Действие
Запрос		
Удаление	!12HS1234D	
Удаление		
Запрос	12HS1234D	
Объект	12HS1234B ∩ !12HS1234D	
Отключено	12HS1234A ∩ !12HS1234D ∩ 12ZSL1234	
Объект		
Запрос	12HS1234D	
Удаление	12HS1234C ∩ !12HS1234D	
Отключено	12HS1234A ∩ !12HS1234D ∩ 12ZSL1234	
Отключено		
Запрос	12HS1234D	
Удаление	12HS1234C ∩ !12HS1234D	
Объект	12HS1234B ∩ !12HS1234D	

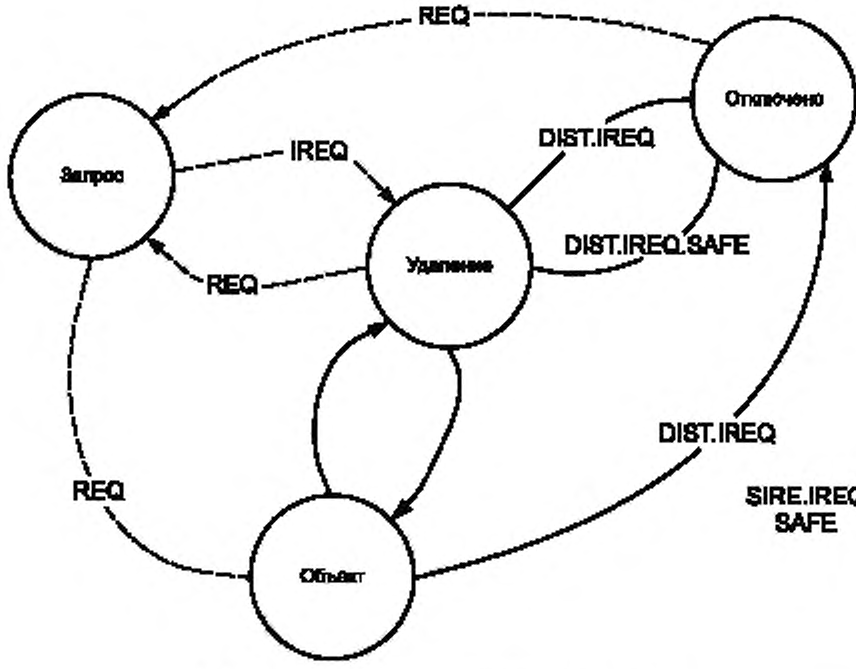


Рисунок В.11 — Диаграмма переходов состояний

Результатом графической спецификации поведения SOV, соответствующей требованиям к интерфейсу на рисунке В.6 и рисунку В.11, является описание функционального блока, представленное на рисунке В.12.

Моделирование функций и интерфейсов ЧМИ не требуется, так как они являются только выходами и не повлияют на поведение SOV. Таким образом, рисунок В.12 может быть упрощен (см. рисунок В.13).

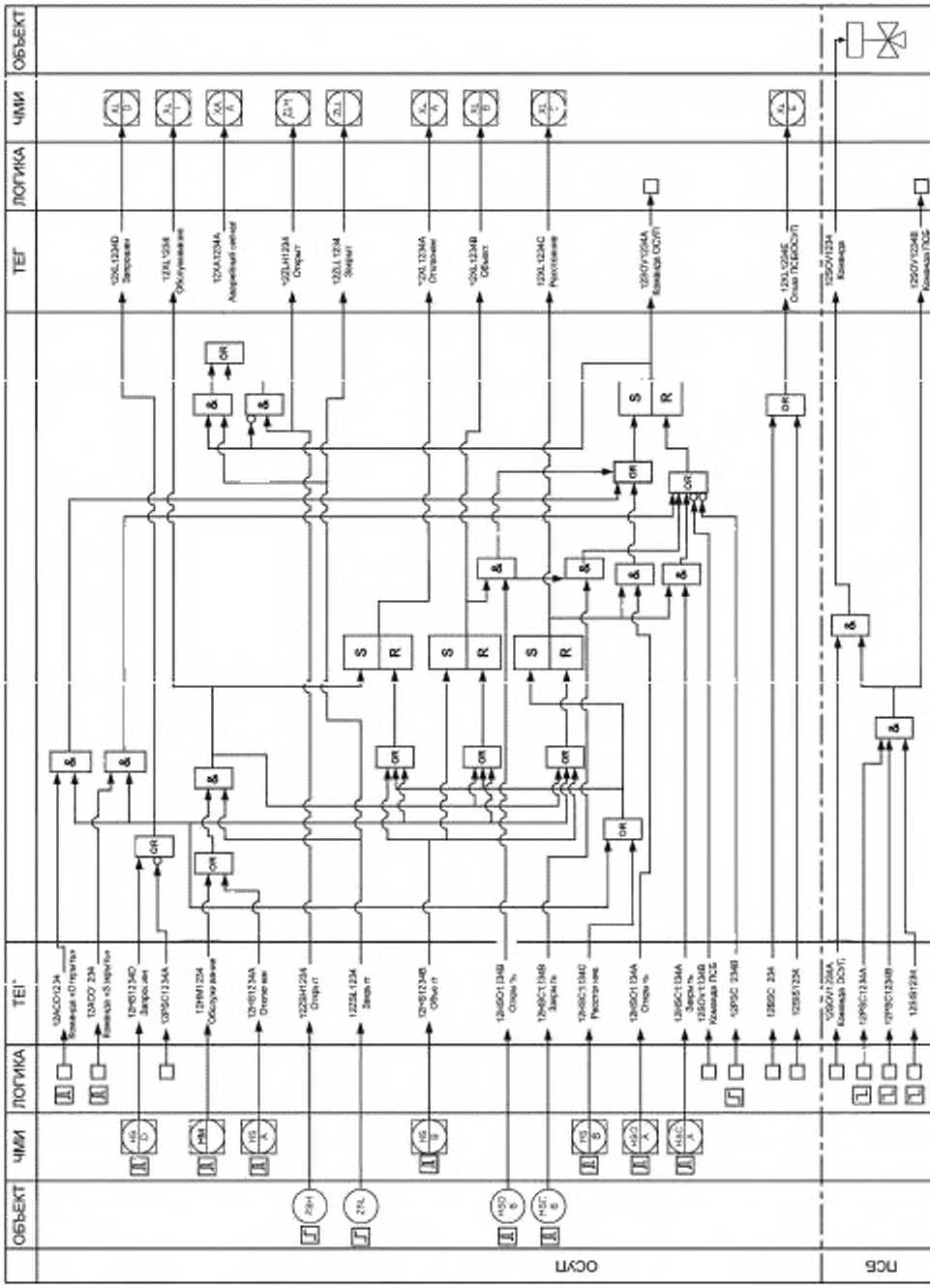


Рисунок В.12 — Структурная схема типового набора SOV

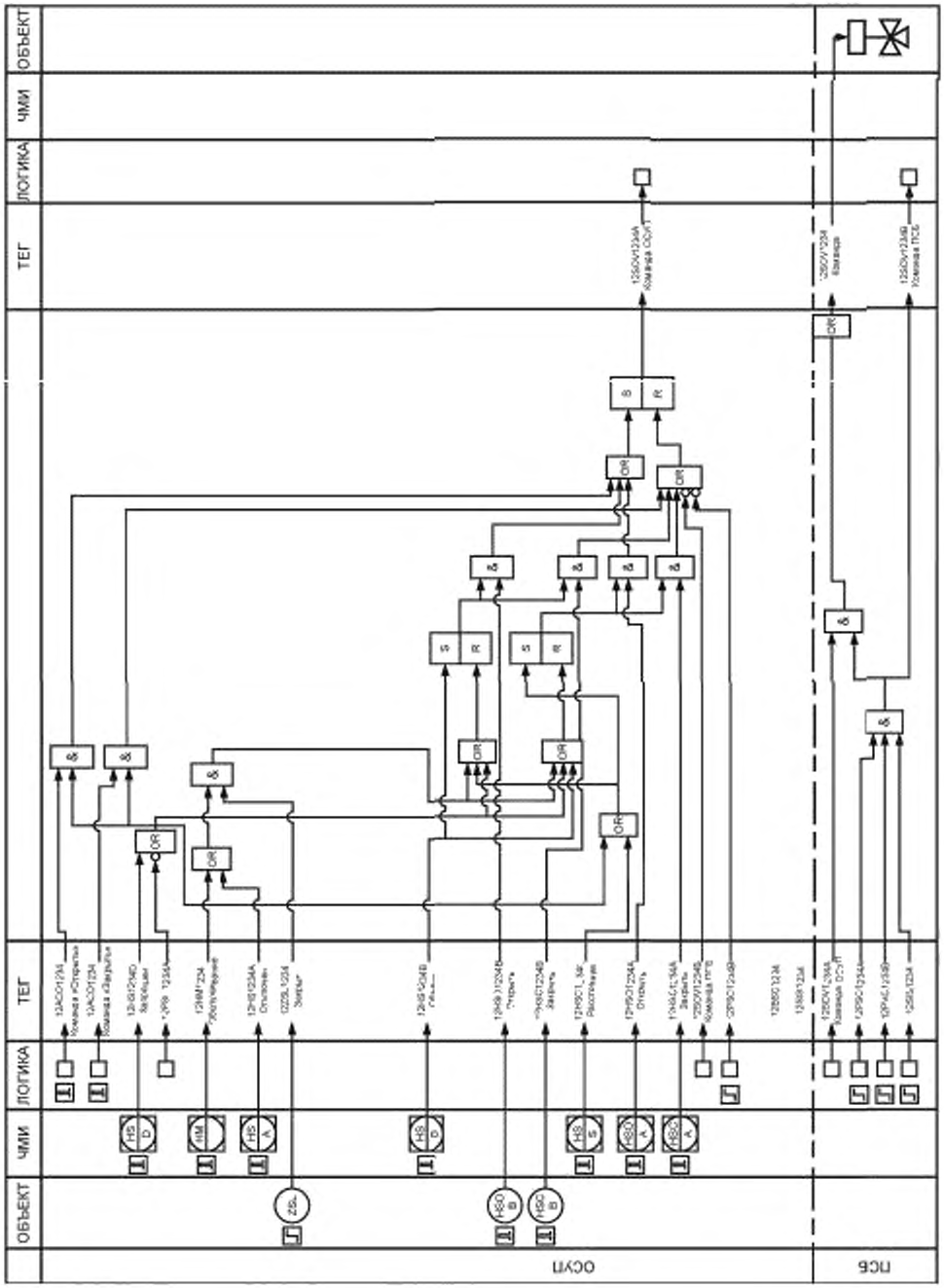


Рисунок В.13 — Упрощенная структурная схема модели типового набора SOV

Спецификация на рисунке В.13 должна быть реализована на графическом языке автоматизированной среды проверки модели. Реализация учитывает необходимость отделения части логики, связанной с ОСУП, от части, связанной с ПСБ. Результат такой реализации, например, приведен на рисунке В.14 (для ОСУП) и на рисунке В.15 (для ПСБ). Моделирование ОСУП требуется, в частности, когда между ОСУП и ПСБ существует интерфейс, необходимый для доказательства независимости ФБ ПСБ от ОСУП и подтверждения выполнения требований к полноте безопасности, например требования о том, что ОСУП ни в коем случае не может заблокировать ФБ ПСБ. Большинство средств проверки модели позволяют непосредственно исполнять такую проверку модели без выполнения шага, описанного на рисунках В.12 и В.13, которые приведены здесь для ясности понимания.

Продолжение моделирования.

Такой же подход применяется для моделирования:

- свойств безопасности данного SOV;
- других необходимых типовых наборов, которые будут использоваться в данном примере:
    - голосования «2 из 3»;
    - свойств безопасности «2 из 3»;
    - обработки сетевых коммуникаций;
    - свойств безопасности сетевых коммуникаций;
    - обработки датчиков;
    - свойств безопасности датчиков.

В.4.3.4.2.2 Уровень функции безопасности ПСБ

Такой же подход применим на уровне ФБ ПСБ для моделирования:

- блокировок ПСБ 02.01;
- свойств безопасности ПСБ 02.01;
- блокировок ПСБ 06.02;
- свойств безопасности ПСБ 06.02.

В.4.3.4.2.3 Уровень объекта

Такой же подход применим на уровне ФБ ПСБ к моделированию:

- блокировок объекта;
- свойств безопасности объекта;
- объекта.

В.4.3.4.3 Результаты тестирования моделей и исправление дефектов

Средство проверки моделей независимо запускают модели с целью обнаружения нарушений безопасного поведения. Если средство проверки моделей находит ошибки, то модели, в которых они обнаружены, корректируются и выполняются снова, пока эти систематические сбои проектирования не будут устранены.

В.4.3.5 Моделирование интеграции прикладной программы и тестирование

Предыдущие шаги позволили инженеру ППО:

- описать архитектуру ППО;
- описать содержание функциональных модулей ППО;
- продемонстрировать, что спецификации архитектуры и модулей:
    - соответствуют функциональным спецификациям ППО;
    - соответствуют спецификациям полноты безопасности ППО.

Недостаточно продемонстрировать, что концепция ППО является подходящей при интегрировании ППО в целевую архитектуру физических аппаратных средств, так как функциональное поведение ППО будет также зависеть от характеристик архитектуры физических аппаратных средств.

Эта стадия проектирования заключается в добавлении моделей, описывающих влияние распределения ППО в архитектуре целевых физических аппаратных средств, чтобы проверить, что СТБ по-прежнему выполняются. В случае их невыполнения модули ППО, и/или архитектуры ППО, и/или даже физическая архитектура будут модифицированы. Шаг, представленный на рисунке В.10, может быть пропущен, если физическая архитектура аппаратных средств известна на ранних стадиях жизненного цикла разработки ППО.

Последующие модели разрабатываются и добавляются в модель проверки в рамках следующей структуры, как описано на рисунке В.16.

В.4.4 Производство прикладных программ

Некоторые рабочие среды ППО позволяют генерацию прямого загружаемого кода из моделей, уже подвергавшихся проверкам. Некоторые из них, кроме этого, соответствуют МЭК 61508.

В.4.5 Верификация и тестирование прикладной программы

Если невозможно автоматически сгенерировать загружаемый код из прежде используемого средства или средства, соответствующего МЭК 16508, то ППО генерируется вручную и тестируется.

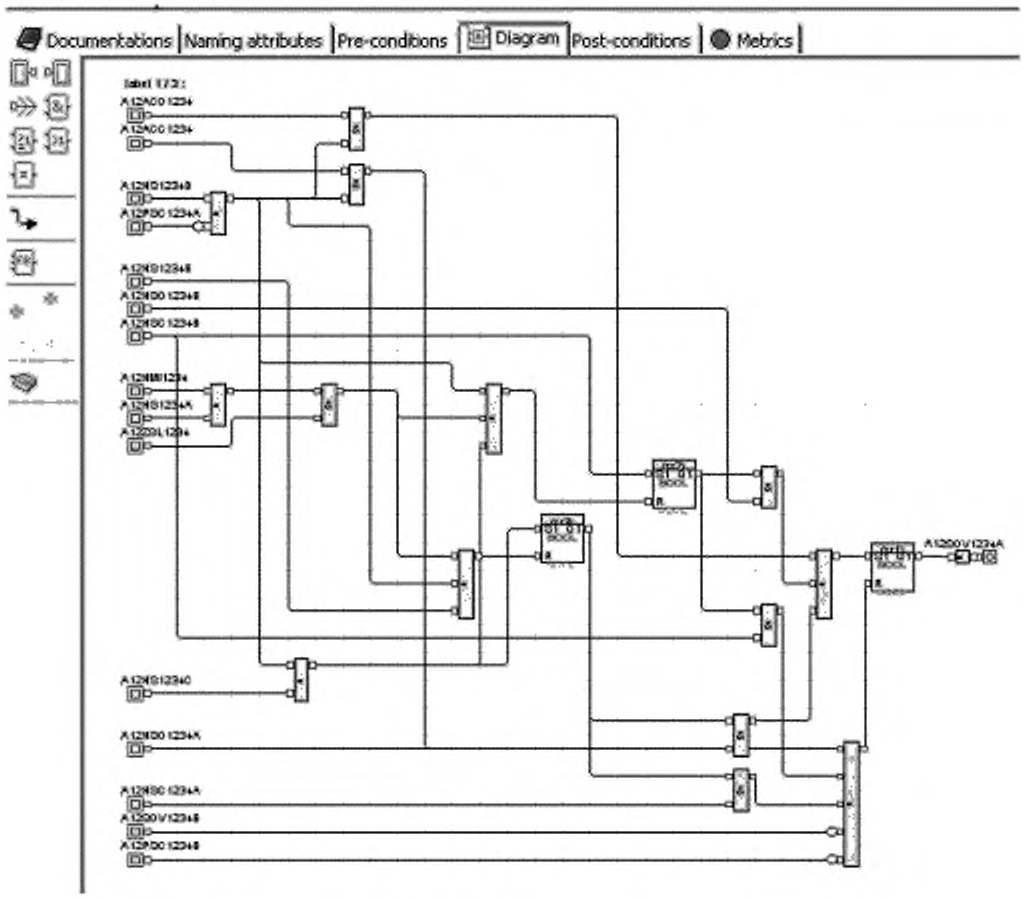


Рисунок В.14 — Реализация структурной схемы модели типового набора (для ОСУП)

Реализация модели логики управления SOV из ПСБ.

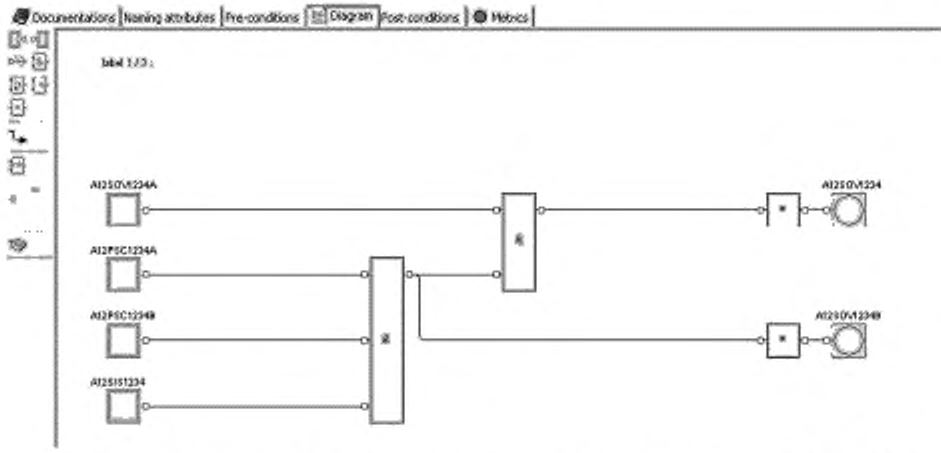


Рисунок В.15 — Реализация модели прикладных программ типового набора SOV (для ПСБ)

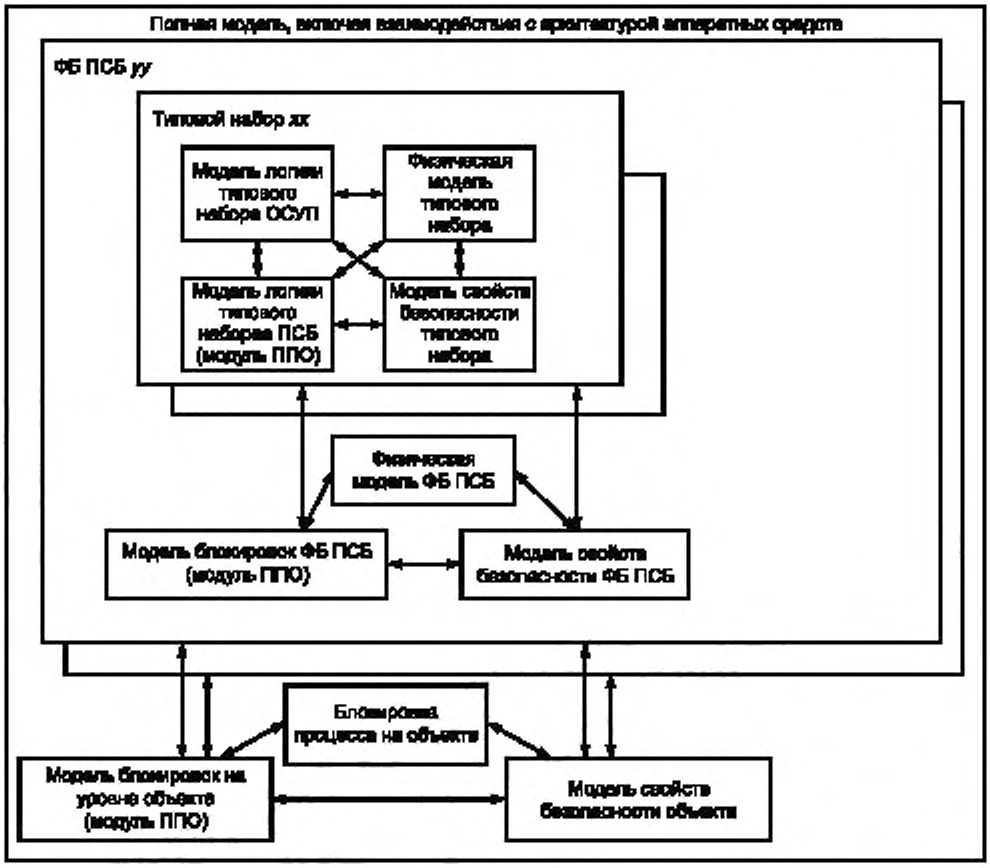


Рисунок В.16 — Полная модель для заключительной проверки модели реализации

В.4.6 Подтверждение соответствия

Для ППО, генерируемого автоматически из моделей с помощью средства, соответствующего МЭК 61511-1:2016, (пункт 12.6), подтверждение соответствия заключается в верификации документации средства проверки модели посредством анализа этой документации, чтобы убедиться, что все функциональные свойства и свойства полноты безопасности, описанные в СТБ ППО, были в действительности продемонстрированы.

В случае ППО, генерируемого вручную, подтверждение соответствия заключается в верификации того, что реализация строго соответствует предположениям моделей и тому, что все функциональные свойства и свойства полноты безопасности, описанные в СТБ ППО, были в действительности продемонстрированы в ходе испытаний.

Приложение С
(справочное)

Что следует учесть при конвертировании из непрограммируемых (НР) технологий в ПЭ-технологии

Многие объекты технологического комплекса используют электрические или полупроводниковые устройства для проектирования ПСБ. Для подобных производственных объектов может возникнуть желание получить преимущества, предлагаемые ПЭ-технологией, поэтому для них могут быть запланированы модификации их ПСБ или дополнения к их ПСБ с использованием ПЭ-устройств. Перед выполнением такого перехода или во время его выполнения среди прочего стоит учитывать следующее:

a) ПЭ-устройства для систем ПСБ не должны применяться, если на объекте не могут быть осуществлены успешная верификация и подтверждение соответствия, а также успешное использование, эксплуатация и обслуживание ПЭ-устройств в их ОСУП;

b) ПЭ-устройства для систем ПСБ не должны применяться, если на объекте нет возможностей для использования, проектирования, модификации и обслуживания ППО для ПЭ-устройств;

c) должна быть проведена проверка для установления того, какие из существующих возможностей приложения объекта могут быть использованы для ППО ПСБ, например, такие как:

- навыки и опыт (например, опыт программирования, функциональность, готовность); возможность переноса навыков работы с ППО на объекте на ПСБ; знание менеджмента и участие в поддержке ПЭ;
- возможности обеспечения защиты, так как они связаны с разрешением доступа (местным и удаленным);
- использование прикладного языка на существующем производственном объекте;
- модули (например, существующие алгоритмы управления, такие как запуск/останов/проверка двигателя, сравнение реального положения со статусом команды положения);
- реакция и задержки в реальном времени при переходе с жестко закодированных систем на ПЭ-системы;
- интерфейсы (например, существующие, подтвержденные, надежные интерфейсы для связи с DCS, ЧМИ, сети, электрические интерфейсы, интерфейсы с устройством синхронизации);
- документация (например, способность к представлению функциональности для четкого описания ППО обслуживающему персоналу/операторам);
- поддержка выявления неисправностей в ПЭ и ППО 24/7;
- охват (доступность поддержки 24/7);
- реакция (например, время до разрешения проблемы);
- симулятор (например, для анализа, модификации, разработки ППО и обучения его использованию в автономном режиме);
- возможности проведения испытаний (например, подход к проведению испытания на объекте и возможности проведения испытаний, необходимых для ППО);
- опыт оператора (работы с ПЭ и ППО);
- процедуры байпаса на объекте (а также их реализация и управление с помощью прикладного программирования);
- конвертация решения ЧМИ объекта из технологии НР в технологию ПЭ;
- обучение (готовность, охват прикладного программирования, ЧМИ);
- инструментальные средства (например, программирования, разработки, проведения испытаний); поддержка для служебных программ;
- поддержка управления (существующая, достаточная, осознание необходимости поддержки всеми сторонами);
- управление процедурой изменения, включая управление модификациями ППО, управление защищенным хранилищем и конфигурацией и обеспечение возможности повторного подтверждения соответствия там, где были применены изменения, или там, где они могут влиять на ППО;
- дальнейшее улучшение/обновление/моральный износ систем(ы);
- корпоративные/объектные стандарты прикладного программирования и ввод в действие промышленных норм и правил;
- совместимость с родственными ПЭ-решениями для взаимного обмена опытом, процессами, оборудованием и т. п.

Приложение D
(справочное)

Пример получения прикладной программы из схемы трубопроводов и контрольно-измерительных приборов (Т и КИП)

В настоящем приложении проиллюстрирован переход от схемы Т и КИП процесса разделения нефти и газа к ППО. На рисунке D.1 представлена схемы Т и КИП. На рисунке D.2 представлена функция безопасности с помощью диаграммы причинно-следственных связей. На рисунке D.3 показано преобразование диаграммы причинно-следственных связей в ППО при помощи программирования методом функциональных блоков.

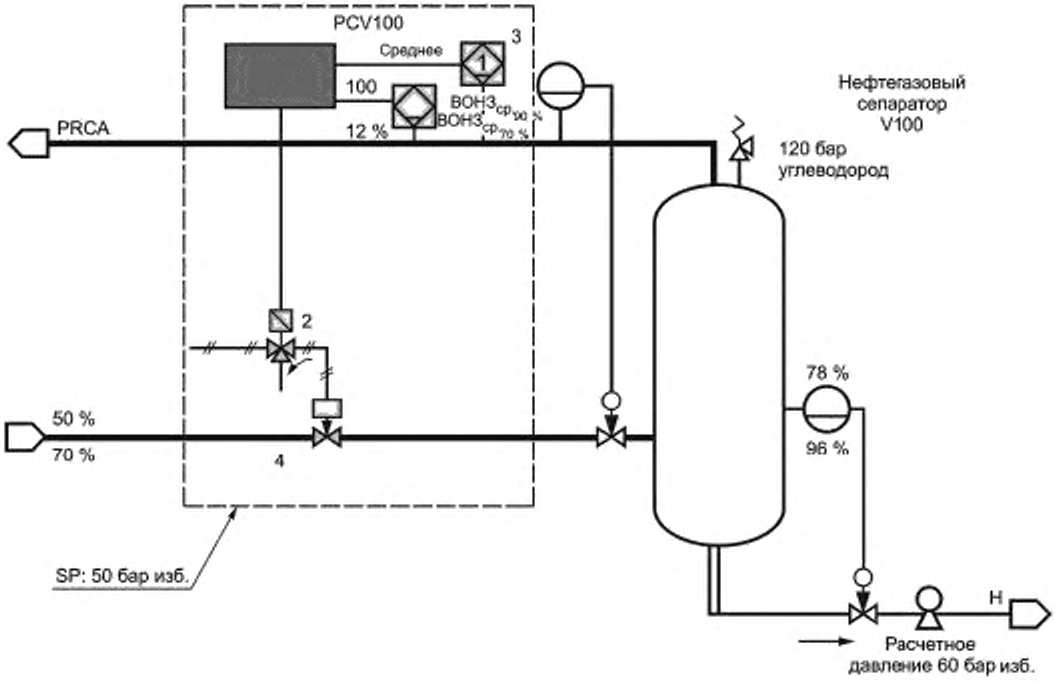


Рисунок D.1 — Пример схемы Т и КИП для сепаратора нефти и газа

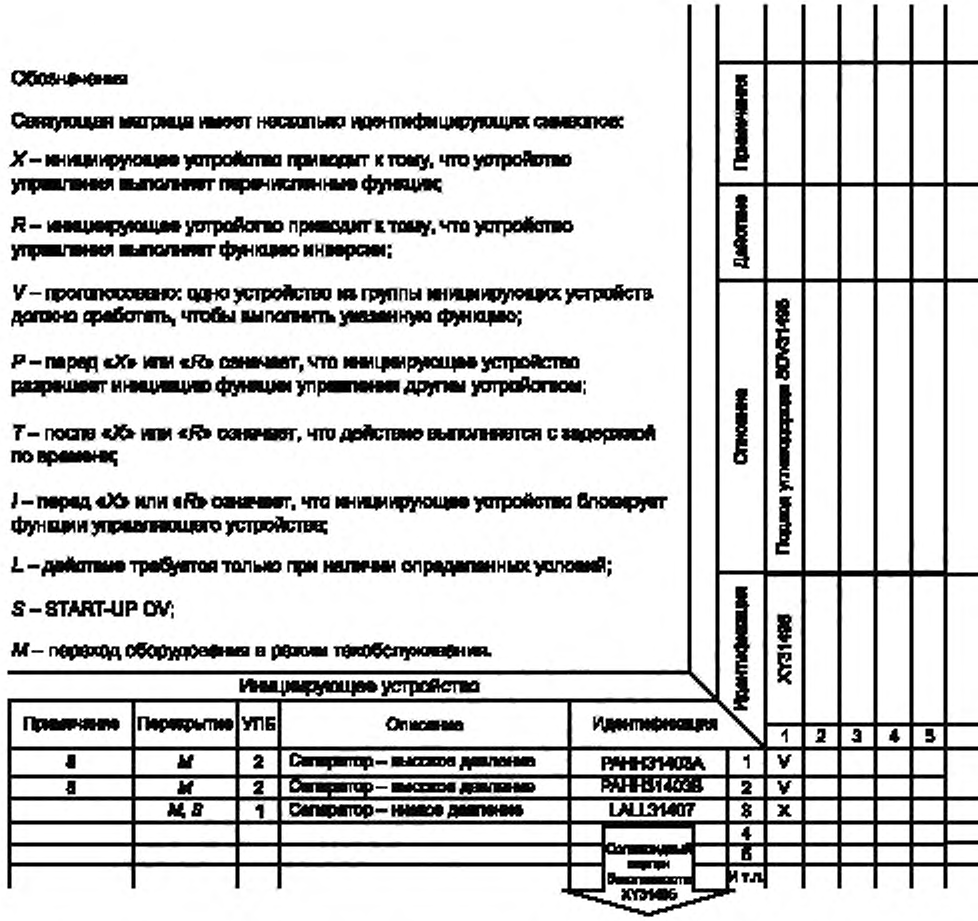


Рисунок D.2 — Пример (части) причинно-следственной диаграммы системы противоаварийной защиты

Ниже приведен пример ППО для ФБ ПСБ с двумя аналоговыми сигналами со схемой голосования «1 из 2», посылаемыми от датчиков давления и цифровым выходом к одиночному исполнительному элементу. Концепция безопасности — переход в безопасное состояние по отключению питания (DTS). Язык программирования — язык функциональных блоков.

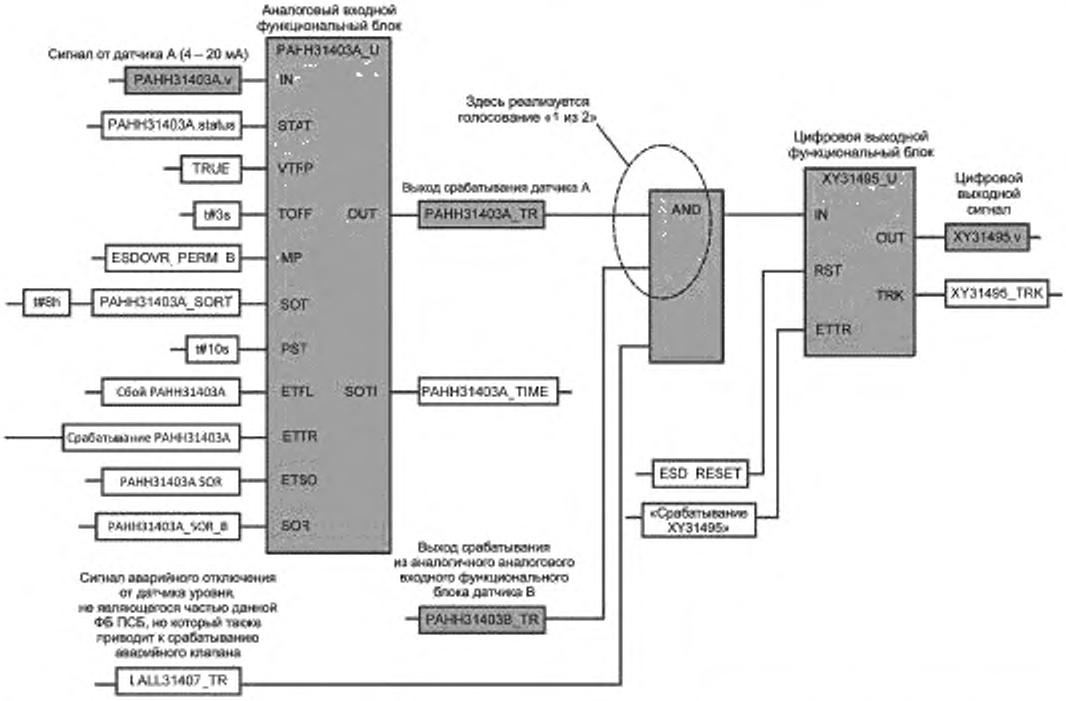


Рисунок D.3 — Пример (части) прикладной программы для ПЛК системы безопасности, запрограммированной методом функциональных блоков

Приложение Е
(справочное)

Пример получения прикладной программы из схемы трубопроводов и контрольно-измерительных приборов (СТ и КИП)

Е.1 Типовой набор инструментальных средств прикладного программирования

Как правило, набор инструментальных средств, поддерживающий программирование ПЭ, включает следующие средства:

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

b) редакторы языков. Эти редакторы использует прикладной программист при разработке программ, выполняющих все необходимые для данной системы функции (связанные и не связанные с безопасностью);

c) библиотеки функций и функциональных блоков, уже подвергавшихся оценке. Такие функции и функциональные блоки могут быть использованы в ППО;

d) средства разработки пользовательских функций и функциональных блоков. Некоторые поставщики предоставляют такую среду разработки, которая позволяет пользователю разрабатывать собственные функции и функциональные блоки, поддерживаемые прикладными языками. Такие функции и функциональные блоки должны быть тщательно проверены до применения в ППО;

e) средства планирования работы ППО. Такие средства планирования поддерживают настройку порядка требуемой последовательности выполнения программ и скорости их выполнения;

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

g) средства эмуляции. Некоторые поставщики предоставляют среду разработки, способную эмулировать все ППО на компьютере, поддерживающем эту среду. Это позволяет проводить проверки ППО в автономном режиме 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 на реальном функциональном блоке, 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 «выполнено», «неисправность» или «работа»; и часто доступна более детальная информация о неисправностях в системе.

ПЭ-систему создают в среде программирования, поддерживающей кодирование ППО, конфигурирование параметров приложения и интерфейсов, а также тестирование/мониторинг выполнения ППО. Многие ПЭ-системы, предназначенные для использования в приложениях безопасности, будут поддерживаться предназначенным для этого набором инструментальных средств вместе с руководством, которое будет описывать, как использовать инструментальные средства для обеспечения гарантированного достижения для ППО предназначенного для него уровня полноты. Среда проектирования и прикладной язык должны обладать характеристиками, которые облегчают:

- реализацию абстрагирования, модульного принципа организации и другие характеристики управления сложностью; при возможности следует создавать ППО на основе хорошо проверенных модулей, которые могут включать в себя библиотечные функции пользователя и четко заданные правила для интеграции модулей;
- выражение для представления:
  - функционала, в идеале в виде логического описания или алгоритмических функций;
  - потока информации между модулями устройств, реализующих прикладные функции;
  - требований к установлению последовательностей;
  - обеспечения того, что ФБ ПСБ всегда функционирует в заданных временных ограничениях;
  - предотвращения неопределяемого поведения;
  - гарантии того, что внутренние элементы данных ошибочно не дублируются, все используемые типы данных определены и выполняется надлежащее действие в случае, если данные выходят за границы установленного диапазона или являются неверными;
  - допущений при проектировании и зависимостей между ними;
- понимание разработчиками и другими специалистами, кому требуется понимать проект, как функционала приложения, так и ограничений технологии;

- верификацию и подтверждение соответствия, включая ППО, функционал интегрированного приложения, интерфейс вместе с ПСБ и конфигурацией ее аппаратных средств, зависящей от приложения;
- модификацию ППО. Сюда включают модульную организацию, прослеживаемость и документацию.

Е.2 Правила и ограничения для проектирования прикладных программ

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

a) разделить ППО на отдельные ФБ ПСБ со своим УПБ для каждой ФБ ПСБ;

b) разобраться в архитектуре аппаратных средств каждой ФБ ПСБ и продублировать эту архитектуру аппаратных средств для каждого ППО ФБ ПСБ;

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

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

e) не объединять ППО одной ФБ ПСБ с прикладными программами любой другой ФБ ПСБ;

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

g) обеспечить документальное оформление ППО, согласованное с функциональным описанием, содержащимся в документации ППО;

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

i) тщательно проверить (например, моделированием, просмотром или проверкой) каждый модуль ППО и провести повторный независимый анализ (привлекая на этой и на всех последующих стадиях подразделения по эксплуатации и обслуживанию);

j) тщательно проверить комбинации модулей, образующие подсистемы процесса ПСБ, и провести их повторный независимый анализ;

k) тщательно испытать ППО ПСБ в целом и провести его повторный независимый анализ;

l) использовать ППО при проведении проверки аппаратных средств (например, для подтверждения правильности подсоединения входов/выходов к датчикам/исполнительным элементам);

m) включить проверки ППО в прогоны процесса (например, выполнение процесса без загрузки опасных материалов).

Пример — Сквозные проверки в каналах связи коммуникаций, контроль граничных значений на входах датчиков, контроль граничных значений данных для параметров и разнообразное выполнение прикладных функций;

n) обеспечить доступность персонала сопровождения ППО при любой работе с ППО (например, при вводе в эксплуатацию);

o) не допускать взаимные блокировки между ФБ ПСБ.

Е.3 Правила и ограничения для прикладного программирования

Ниже приведены некоторые правила, которые следует учитывать для прикладного программирования ПЭ логических решающих устройств, применимость которых зависит от приложения:

a) запрещается использовать функции SKIP (пропустить) и JUMP (перепрыгнуть);

b) запрещается использовать функции NOT (отрицание);

c) запрещается использовать косвенную адресацию;

d) запрещается использовать алгоритмы сжатия;

e) запрещается использовать логику, основанную на результатах арифметических вычислений;

f) запрещается использовать логику вместе с устройствами, запоминающими внутреннее состояние (например, с триггерной памятью);

g) запрещается использовать текстовые переменные в ФБ ПСБ;

h) запрещается использовать функции или подпрограммы, включающие передачу переменных или параметров;

i) запрещается индивидуальная настройка библиотечных функций;

j) запрещается использовать прерывания;

k) запрещается блокировка данных;

l) запрещается размещение логических переменных внутри целочисленных переменных;

m) запрещается логическая инверсия физического состояния датчиков или исполнительных устройств;

n) запрещается разбиение блокировок ФБ ПСБ по нескольким логическим решающим устройствам;

o) запрещается использовать любые функции сетевых коммуникаций, кроме пассивных функций;

p) настоятельно рекомендуется использовать методы программирования, проверенные на объекте и прошедшие оценку безопасности;

q) настоятельно рекомендуется использовать стандартизированные модули (например, «типовые наборы»);

r) настоятельно рекомендуется использовать алфавитно-цифровые описатели устройств для описания задачи и перекрестных ссылок для каждого датчика, исполнительного элемента (например, для соленоидных клапанов, клапанов, двигателей, аварийных сигналов), ПСБ и т. д., согласующиеся и связанные с проектными чертежами (например, схемы Т и КИП, компоновочные чертежи, логические диаграммы);

s) настоятельно рекомендуется использовать одобренные объектом и уже прежде проходившие оценку функции безопасности логического решающего устройства (например, аварийный останов, световые завесы, предохранительные затворы);

t) настоятельно рекомендуется разделять программирование логического решающего устройства ПЭ на три отдельные области: входной контур, контур логики, выходной контур:

- входные контуры следует изображать вертикально в формате ступенчатой диаграммы, чтобы у каждой ступеньки слева находились датчики, а справа — входные модули; каждый датчики должен быть подключен отдельно;
- логические диаграммы должны изображаться вертикально в формате ступенчатой диаграммы (или на надлежащем ЯОИ), чтобы у каждой ступеньки слева были входы, а справа — выход;
- выходные диаграммы следует изображать вертикально в формате ступенчатой диаграммы, чтобы у каждой ступеньки слева был выход логического решающего устройства, а справа — исполнительный элемент; каждый исполнительный элемент должен быть подключен отдельно;

u) подход к проектированию должен, как правило, базироваться на останове по отключению питания для перевода процесса в безопасное состояние; в случае систем, которым требуется останов по включению питания, требуются специальные меры предосторожности;

v) адресация входов/выходов логического решающего устройства и программирование логического решающего устройства должны быть организованы для зеркального отображения приложения процесса (например, начальное программирование и назначение входов/выходов должны быть связаны с циклом запуска приложения и продолжаться во время его разработки в таком же формате, какой диктует технологический процесс, заканчиваясь на функции останова);

w) функции поддержки, такие как контрольные испытания, ручное управление, байпас, аварийные сигналы и диагностика, должны быть идентифицированы как таковые и отделены от ФБ ПСБ;

x) следует обеспечить необходимые запасные входы/выходы, память и производительность обработки так, чтобы при будущих требованиях к модификации/расширению была возможность поддерживать ясность и способность для необходимого прикладного программирования;

y) диаграммы должны содержать перекрестные ссылки на местоположение многократного использования любого компонента ППО (например, входа, выхода, внутреннего регистра);

z) следует обеспечить соответствие порядка обработки в рамках ППО реакции в реальном времени.

Приложение F
(справочное)

Пример проекта ПСБ, иллюстрирующий каждую стадию ее жизненного цикла, с использованием языка линейно-лестничной логики при разработке прикладных программ

Примечание — Данный пример используется с разрешения ISA и AIChE CCPS, *Guidelines for Safe Automation of Chemical Processes*, New York, 1993, доступного по адресу: AIChE, 345 East 47th Street, New York, NY 10017, Tel: (212) 705-7657. Данный пример был модифицирован, чтобы соответствовать требованиям МЭК 61511.

F.1 Обзор

В настоящем приложении представлен пример, иллюстрирующий реализацию каждой стадии жизненного цикла системы безопасности с помощью многоступенчатой логики в соответствии с МЭК 61511.

Это третья редакция данного примера. Первая редакция была выпущена CCPS до издания МЭК 61508 и МЭК 61511. Вторая редакция была выпущена ISA (TR84.00.04, часть 2) и соответствовала первым изданиям МЭК 61508 (2000) и МЭК 61511 (2003). Третья редакция соответствует комплексам стандартов МЭК 61508(2010) и МЭК 61511(2016). Кроме того, данный пример был разбит на разделы, соответствующие стадиям жизненного цикла системы безопасности, представленным на рисунке 7 в МЭК 61511-1:2016.

Настоящее приложение предназначено продемонстрировать один из методов для соблюдения требований МЭК 61511. Пользователю следует обратить внимание на то, что комплекс стандартов МЭК 61511 обусловлен потребностями практической деятельности и что для достижения соответствия могут применяться многие методы. Некоторые из методов, используемых в данном примере, включают: причинно-следственный («что если») и HAZOP методы для анализа опасностей и рисков, анализ уровней защиты (АУЗ) для распределения функций безопасности по слоям защиты, анализ дерева сбоев для верификации УПБ, а также многоступенчатую логику для документального оформления требований ППО. Чтобы выполнить требования стандартов на каждом шаге жизненного цикла системы безопасности могут применяться и другие методы и инструментальные средства.

В данном примере рассмотрен химический процесс, похожий на тот, что представлен в CCPS AIChE, *Guidelines for Safe Automation of Process Applications*, 1993.

В рассматриваемом примере выбирается подсистема ПСБ процесса и к ней применяются философия, процедуры, методы проектирования, а также методология верификации, рассматриваемые в МЭК 61511.

Данный пример демонстрирует документацию «от появления идеи (концепции) до устранения (списывания)» для каждой ФБ ПСБ. Знание истории этой документации обеспечивает аудиторов и персонал объекта средствами, позволяющими проследить весь путь ФБ ПСБ на всех стадиях жизненного цикла ПСБ, начиная от анализа опасностей процесса (АОП), создавшего ее. Каждая ФБ ПСБ четко идентифицирована в каждом документе для облегчения прослеживания между стадиями жизненного цикла. Очень важная часть системы безопасности — это способность демонстрировать другим (например, аудиторам, регулирующим органам, страховым компаниям), что каждая ФБ ПСБ обеспечивает адекватное снижение риска.

Данный пример не является полным проектом для процесса полимеризации, так как для получения автоматизированного проекта, обеспеченного системой безопасности с высоким уровнем полноты, требуется куда более подробное рассмотрение.

Все приведенные ссылки связаны с информацией в данном примере, если не указано обратное.

F.2 Описание проекта

F.2.1 Общие положения

Рассмотрим процесс полимеризации винилхлоридного мономера (ВХМ)

$$CH_2 = CHCl$$

для получения поливинилхлорида (ПВХ)

$$[-CH_2\text{-}CHCl\text{-}]_n.$$

В процессе участвует опасный реагент ВХМ, являющийся воспламеняемым и обладающий токсичными продуктами горения, а также являющийся известным канцерогеном. Процесс также иллюстрирует дозировочную операцию большего масштаба, выполняемую полунепрерывным способом во время периода осуществления полимеризации, приблизительно равного десяти часам. Также представляется упрощенное описание шагов процесса.

F.2.2 Концептуальное планирование

При принятии бизнес-решения о производстве определенного продукта, в данном примере — поливинилхлорида, формируется начальная команда проекта. Данная команда начинает с оценивания возможных путей процесса для определения технологии, которая будет удовлетворять потребностям производства при выполнении обязанностей по обеспечению здоровья, безопасности, защищенности и защиты окружающей среды.

F.2.3 Анализ опасностей процесса

На самых ранних стадиях оценки процесса и определения проекта команда по анализу опасностей процесса начинает тесно взаимодействовать с проектировщиками. Для проектов, связанных с опасными материалами, команда

будет включать не только инженеров по проектированию процесса, но также специалистов по здравоохранению и безопасности. Этой команде часто требуется общение с другими специалистами, такими как химики, обслуживающий персонал, консультанты или подрядчики по проектированию, у которых есть опыт работы с таким же или похожими процессами, а также с лицами, лицензирующими процесс. В данном примере с самого начала считаем, что имеем дело с хорошо отработанным процессом. Поэтому мы сосредоточимся на вопросах процесса проектирования, которые влияют или непосредственно связаны с проектированием систем управления процессом и защитных блокировочных систем. Более подробная информация о вопросах, связанных с этим процессом проектирования, может быть найдена в следующих документах из Центра безопасности химических процессов Американского института инженеров-химиков (Center for Chemical Process Safety, American Institute of Chemical Engineers):

- *Guidelines for Hazard Evaluation Procedures;*
- *Guidelines for Chemical Process Quantitative Risk Analysis;*
- *Guidelines for Safe Storage and Handling of High Toxic Hazard Material;*
- *Guidelines for Vapor Release Mitigation;*
- *Guidelines for the Technical Management of Chemical Process Safety.*

F.3 Упрощенное описание процесса

Производство ПВХ из мономера является относительно несложным. Основным элементом технологического процесса является корпус реактора, в котором происходит полимеризация, выполняющаяся примерно в течение десяти часов, при этом содержимое реактора механически перемешивается, а выделяемое в результате реакции тепло удаляется с помощью циркуляции охлаждающей воды, поступающей в кожух реактора. Так как процесс предполагает загрузку реактора очередной партией, технологические системы проектируются с большим количеством параллельно работающих модулей реактора так, чтобы технологический процесс мог выполняться полунепрерывно. Для простоты в данном примере рассмотрен один из модулей, учитывая, что реальный производственный объект, как правило, содержит несколько параллельных модулей, работающих последовательно.

На рисунке F.1 представлена упрощенная технологическая схема процесса для типичного предприятия, производящего ПВХ. Если корпус реактора был открыт для обслуживания после завершения обработки и выгрузки последней партии, то его прежде всего необходимо очистить, чтобы избавиться от любых остатков воздуха (кислорода) в паровом пространстве для минимизации окислительной реакции мономера, которая производит HCl и может привести к механической коррозии корпуса реактора и снижению качества итогового продукта. В противном случае первым шагом должна быть обработка корпуса реактора антифоулянтом, чтобы предотвратить полимеризацию на стенах реактора. За этим шагом следует загрузка корпуса деминерализованной водой и поверхностно-активными присадками.

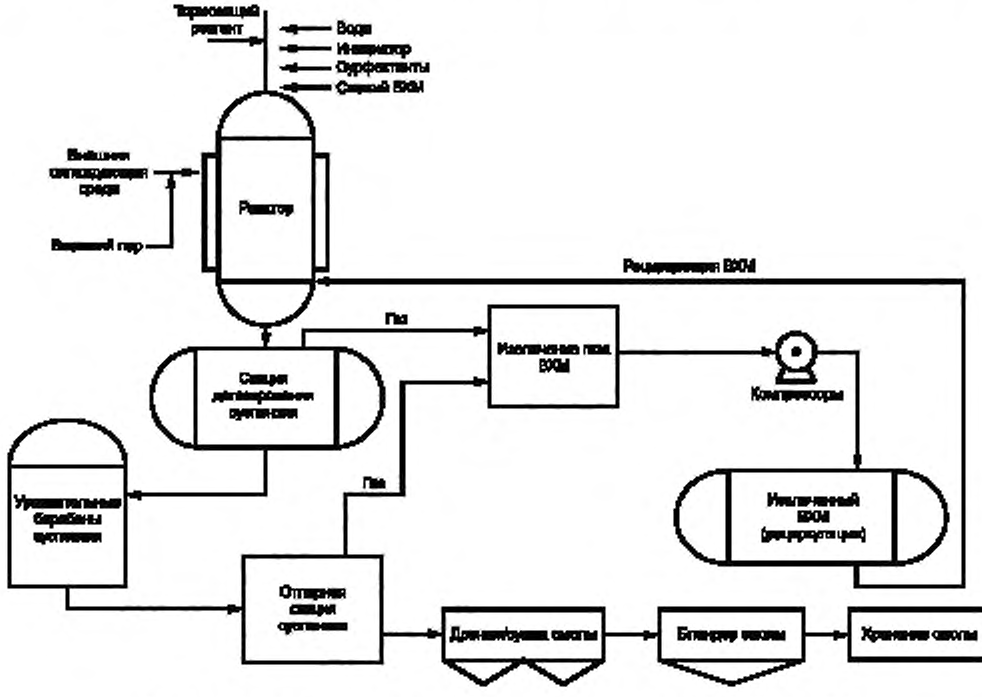


Рисунок F.1 — Упрощенная технологическая схема процесса получения ПВХ

Далее осуществляется загрузка жидким мономером винилхлорида (ВХМ) под давлением его насыщенного пара (примерно 3,86 бар избыточного давления при 21 °С — 56 фунт/кв. дюйм избыточного давления при 70 °F).

Инициатором реакции является пероксид, растворяемый в растворителе. Так как он достаточно активен, то его хранят при низкой температуре в специальном бункере. Небольшие его количества отбираются для ежедневного использования в процессе и хранят в холодильнике. Он первый вводится в небольшой загрузочный бак, связанный с реактором, для обеспечения добавления только корректного количества.

После того как был введен инициатор реакции, в кожух реактора добавляется нагретая паром вода, чтобы поднять температуру примерно до 54,5—60 °С, или до 130—140 °F (в зависимости от стандартного рецепта загрузки для конкретной категории продукта), и далее реакция будет продолжаться со скоростью, удовлетворяющей требованиям. Для удержания ВХМ в воде во взвешенном состоянии (контроль размера частиц), улучшения распределения тепла в партии и получения однородного продукта необходимо перемешивание. Так как реакция является экзотермической, то для управления температурой реактора в кожухе корпуса циркулирует охлаждающая вода. Условия внутри реактора тщательно контролируются на протяжении примерно восьми часов, которые требуются для завершения полимеризации.

Реакция завершается, когда снижается давление в реакторе, подавая сигнал о том, что большая часть мономера вступила в реакцию. Полимер, вступивший в реакцию, выгружается из реактора, и выполняются процессы его дальнейшей обработки для последующего использования ВХМ, отпаривания, дренажа и сушки.

F.4 Техническое проектирование

Проверяются все конкретные локальные требования, идентифицируются применимые правила и нормы и утверждаются общие директивы по риску. Проверяются производственные требования (например, воздух, охлаждающая вода, электропитание) и подтверждается их адекватность для заданного применения.

F.5 Применение МЭК 61511

F.5.1 Общие положения

После завершения предварительного планирования (см. разделы F.2—F.4) начинается выполнение МЭК 61511.

Для настоящего примера стратегией проектирования является инициализация проекта жизненного цикла (см. рисунок F.2) и разбиение стадий жизненного цикла на десять шагов, согласующихся с рисунком F.2 и таблицей F.1 (обзор жизненного цикла системы безопасности). На данном этапе проекта может быть полезно использовать таблицу жизненного цикла для назначения ответственных лиц за каждую стадию жизненного цикла, как это показано в таблице F.1.

F.5.2 Шаг F.1. Оценка опасностей и рисков

См. стадию жизненного цикла ниже в таблице F.2.

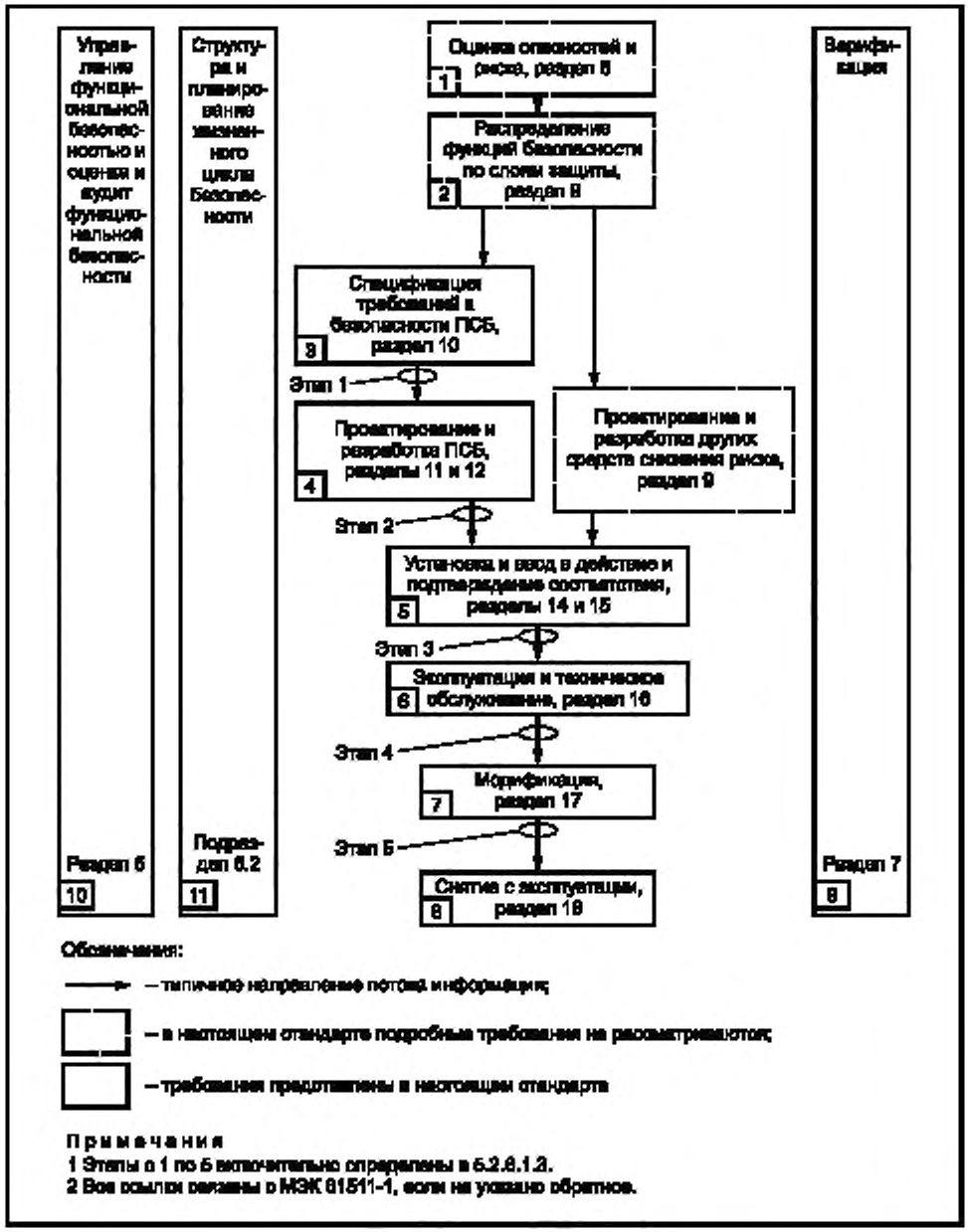


Рисунок F.2 — Стадии жизненного цикла ПСБ и этапы ОФБ

Таблица F.1 — Обзор жизненного цикла ПСБ

Стадия или деятельность жизненного цикла системы безопасности		Цель	Раздел или подраздел требований МЭК 61511-1 2016	Вход	Выход	Ответственный
Рисунок F.2, блок №	Заголовок					
1	Анализ опасностей и рисков	Определить: опасности и опасные события процесса и связанного с ним оборудования, последовательность событий, ведущую к опасному событию, риски процесса, связанные с опасным событием, требования к снижению риска и функции безопасности, необходимые для достижения требующегося снижения риска	8	Технологический процесс, размещение оборудования, состав персонала, цели безопасности	Описание опасностей, требуемой(ых) функции(й) безопасности и соответствующего снижения риска	Группа анализа опасности процесса (PHA), см. F.2.2
2	Распределение функций безопасности по слоям защиты	Распределение функций безопасности по слоям защиты, а для каждой ФБ ПСБ назначить УПБ		Описание необходимой ФБ ПСБ и соответствующих требований к полноте безопасности	Описание распределения требований к безопасности (см. МЭК 61511:2016, раздел 9)	Группа анализа опасности процесса (PHA), см. F.2.2
3	СТБ ПСБ	Установить для каждой ПСБ требования к ФБ ПСБ и их полноте безопасности, необходимые для достижения требуемой функциональной безопасности	10	Описание распределения требований к безопасности (см. МЭК 61511:2016, раздел 9)	Требования к безопасности ПСБ; требования к безопасности ППО	Группа E & I
4	Проектирование и разработка ПСБ	Спроектировать ПСБ, отвечающую требованиям к ФБ ПСБ и полноте безопасности	11 и 12.4	Требования к безопасности ПСБ; требования к безопасности ППО	Проект ПСБ, соответствующий требованиям к безопасности ПСБ; планирование испытания интеграции ПСБ	Группа E & I
5	Установка, ввод в действие и подтверждение соответствия ПСБ	Интеграция и испытание ПСБ; подтвердить соответствие ПСБ всем требованиям к безопасности в части требуемых ФБ ПСБ и полноты безопасности	12.3, 14, 15	Проект ПСБ; план испытания интеграции ПСБ; требования к безопасности ПСБ; план подтверждения соответствия безопасности ПСБ	Полное функционирование ПСБ в соответствии с требованиями к безопасности ПСБ на основе результатов испытаний интеграции ПСБ; результаты деятельности по монтажу, приемке и подтверждению соответствия	Группа сборки

Окончание таблицы F.1

Стадия или деятельность жизненного цикла системы безопасности		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход	Ответственный
Рисунок F.2. блок №	Заголовок					
6	Эксплуатация и техническое обслуживание ПСБ	Обеспечить поддержание функциональной безопасности ПСБ в процессе эксплуатации и обслуживания	16	Требования к ПСБ; проект ПСБ; план эксплуатации и технического обслуживания ПСБ	Результаты деятельности по эксплуатации и техническому обслуживанию	Группа по эксплуатации
7	Модификация ПСБ	Провести изменения, улучшения и настройку ПСБ, обеспечивающие достижение и поддержание требуемого УПБ	17	Скорректированные требования к безопасности ПСБ	Результаты модификации ПСБ	Группа по эксплуатации
8	Снятие с эксплуатации	Обеспечить правильную проверку, организацию работ и сохранность ФБ ПСБ	18	Информация о фактическом состоянии требований безопасности и процесса	ФБ ПСБ, выведенная из использования	Группа по эксплуатации
9	Верификация ПСБ	Провести испытания и оценить результаты конкретной стадии, чтобы обеспечить правильность и соответствие изделий исходным для данной стадии регламентирующим документам	7, 12.5	План верификации ПСБ для каждой стадии	Результаты верификации ПСБ для каждой стадии	Группа по эксплуатации
10	ОФБ ПСБ	Обследовать ПСБ и дать заключение о достигнутой функциональной безопасности	5	Планирование ОФБ ПСБ; требование к безопасности ПСБ	Результаты ОФБ ПСБ	Группа по эксплуатации

Таблица F.2 — Жизненный цикл ПСБ. Блок 1

Обзор					
Стадия жизненного цикла системы безопасности или деятельность		Цель	Раздел или лодраздел требований МЭК 61511-1: 2016	Вход	Выход
Рисунок 2, блок 1	Анализ опасностей и рисков	Определить: опасности и опасные события процесса и связанного с ним оборудования; последовательность событий, ведущую к опасному событию; риски процесса, связанные с опасным событием; требования к снижению риска и функции безопасности, необходимые для достижения требующегося снижения риска	8	Технологический процесс, размещение оборудования, состав персонала, цели безопасности	Описание опасностей, требуемой(ых) функции(й) безопасности и соответствующего снижения риска

F.5.3 Идентификация опасности

Процесс идентификации опасности начинается во время анализа бизнес-решений (см. раздел F.2). Он является одной из самых важных функций группы анализа опасности процесса и продолжается до тех пор, пока этот процесс не будет передан на производство, где выполняются анализ эксплуатационной безопасности и программы аудита.

F.5.4 Предварительное оценивание опасности

Первым шагом в любом планировании разработки технологического процесса являются идентификация общих параметров процесса производства, определение его безопасности и опасностей окружающей среды (или опасных событий) и выявление возможностей сделать процесс изначально более безопасным. Для этого требуется информация о физических или опасных свойствах всего исходного сырья, промежуточных веществ, продуктов реакций и отходов, участвующих в возможных альтернативных процессах. Для данного примера, в котором определенный полимер создается из своего мономера, выбор базового реагента невелик. Доступные альтернативные процессы различаются раствором-средой, суспензией и эмульсией полимеризации. Набор важных свойств ВХМ приведен в таблице F.3 (в «реальном» примере должна использоваться самая последняя версия списка данных безопасности материала ВХМ).

Как бы там ни было, условия реакции и инициатор (а также любые присадки) должны выбираться осторожно, чтобы они обеспечивали безопасное управление скоростью реакции, позволяющее предотвратить неуправляемые реакции, и в то же время позволяли получать адекватное качество и повышать производительность. Выбранная технология предполагает полимеризацию в воде, но при этом требует малых доз относительно опасного жидкого инициатора. Опасности, связанные с инициатором, также требуют особого внимания, но они не рассматриваются в данном упрощенном примере.

F.5.5 История происшествий

Далее выполняется идентификация опасностей. В данном примере основные опасности связаны с воспламеняемостью и токсичностью продуктов сгорания ВХМ. В реальном проекте предприятия также были бы важными факторами подверженность персонала опасностям и ограничения диапазона рабочих температур ВХМ во внешней среде. Для простоты эти факторы в данном примере не рассматриваются. На первом шаге полезно провести обзор истории прошлых происшествий, связанных с аналогичными технологическими процессами.

Таблица F.3 — Некоторые физические свойства винилхлорида

Формула: CH_2 = CHCl Синонимы: винилхлоридный мономер (VCM); Monochloroethylene; Chlorethene; vinyl chloride (VCl). Поставляется в форме сжатого сжиженного газа; упругость паров по Рейду = 5,17 бар абсолютного давления (75 фунтов на кв. дюйм). Газ, бесцветный, запах сладковатый; молекулярный вес = 62,5; Sp. Grav. (vap) = 2,16. Точка кипения при нормальных условиях = –13,4 °C (7,1 F); удельная плотность (liqNBP) = 0,97; держится и закипает на поверхности воды. Критическая *T* = 431 K (317 °F); критическое *P* = 55,4 бар абсолютного давления (775 фунтов на кв. дюйм); температура плавления = –154 °C (–245 °F). Скрытая теплота испарения = 372,16 кдж/кг/160 британских тепловых единиц/lb; Теплота сгорания = 18924 кдж/кг/8136 британских тепловых единиц/lb. Теплота полимеризации = 1695,6 кдж/кг/729 британских тепловых единиц/lb; как правило, стабилен в обычных условиях; полимеризуется при наличии воздуха, солнечного света, влаги, теплоты или инициаторов свободно радикальной полимеризации, если не стабилизован ингибиторами

Окончание таблицы F.3

Опасности возгорания Пределы воспламеняемости на воздухе: 3,6—33 %. Точка возгорания: –61 °С (–108 °F) (открытый тигель); самовозгорание T = 472 °С (882 °F). Разлив быстро испаряется, закипает и производит облако газа тяжелее, чем воздух, которое может воспламеняться от искры. В огне возникают ядовитые газы (HCl, CO и т. п.). Может взрываться, если возгорает в замкнутом пространстве. Наружное возгорание контейнера может привести к взрыву в результате расширения паров кипящей жидкости (BLEVE)
Опасности для здоровья Испарения, раздражающие глаза, нос и горло. При вдыхании вызывает головокружение, трудности дыхания и может привести к серьезным неблагоприятным последствиям и даже к смерти. Длительное или интенсивное воздействие может привести к негативным последствиям для легких, печени и почек. Признан канцерогеном для человека по решению Федерального агентства по охране труда и здоровья США (OSHA), Международного агентства онкологических исследований (IARC) и Национальным институтом США Национальной токсикологической программы (NTP). Предельная допустимая концентрация: 5 мг/м^3. Допустимый уровень воздействия по решению OSHA: 1 мг/м^3 (временное среднее значение), 5 мг/м^3 (среднее значение предельного отклонения в течение любого периода времени, не превышающее 15 мин). Порог ощущения запаха: 260 мг/м^3. Контакт с веществом в жидком состоянии может вызвать обморожение
Загрязнение воды Предел для технологической воды: 10 мг/м^3. Предел для выпускаемой воды 1 мг/м^3
Выбросы в атмосферу Предел для технологических выбросов в атмосферу: 10 мг/м^3 (местный стандарт). Предел для среднегодовой концентрации вредных веществ на территории объекта: 0,2 мг/м^3 ВХМ в воздухе
Реакция на выброс Выдать предупреждение «Высокая степень воспламеняемости, удалить источник возгорания»; обеспечить вентиляцию. Остановить поток. Покинуть опасную зону, разрешить ее посещение только со средствами индивидуальной защиты. К большим очагам пожара не приближаться; потушить малые очаги с помощью огнетушащего порошка или CO_2. Остудить водой контейнер, подвергшийся возгоранию. Запретить сброс в канализационные системы, чтобы избежать взрывов

Можно найти ссылку на описание происшествия на объекте по производству ПВХ, в котором погибли четыре человека и десять получили ранения. Это происшествие было вызвано выгрузкой партии из неверного корпуса реактора, что привело к выбросу мономера в помещение, где находились параллельно работающие реакторы. По-видимому, испарения ВХМ воспламенились из-за искры от электрического машинного оборудования или из-за статического электричества, и в помещении здания произошел взрыв реакторов.

В следующем происшествии рабочий ошибочно открыл крышку люка действующего реактора, произошел выброс большого количества винилхлорида, который воспламенился и привел к возникновению пожара и гибели лица, занимавшегося обслуживанием, а также двух неквалифицированных рабочих.

В другом происшествии осуществлялась загрузка реактора 946 л (250 галлонами) ВХМ при открытом донном клапане реактора. Хотя в результате этого выброса возникла серьезная опасность, но воспламенения не произошло и пострадавших не было. Отмечаются другие происшествия, например взрыв во время работ по техническому обслуживанию насоса винилхлорида (в связи с загрязнением полимерным пероксидом, которое возникло в результате трех одновременно произошедших непредусмотренных ситуаций). Также был случай выброса ВХМ из газоочистителя на предприятии по производству ВХМ в связи с проблемами технического обслуживания, вызванными забитым клапаном во время периодической перезагрузки. Воспламенение ВХМ привело к одной смерти и нескольким раненым.

Также отмечались случаи выбросов ВХМ и пожаров, связанные с перевозкой. Сход с рельсов 16 вагонов около Хьюстона в США привел к утечке ВХМ из цистерны объемом 182 000 л (48 000 галлонов) и мгновенному воспламенению. По истечении 45 минут горения взорвался вагон с ВХМ, убив пожарника и ранив 37 человек большим огненным шаром. После взрыва большие фрагменты цистерны были обнаружены в 120 м (400 футах) от места происшествия.

Кроме этого, для каждого известного серьезного происшествия, как правило, существуют сообщения о бесчисленных небольших происшествиях. Следует уделять внимание возможным незначительным выбросам, так как вместе они могут приводить к серьезным происшествиям. В особенности это касается легко воспламеняющегося

находящегося под давлением материала, воспламенение небольших выбросов которого может приводить к серьезным отказам, если это приведет к нагреву других устройств системы. Поэтому полнота безопасности системы ВХМ должна иметь высокий уровень.

F.6 Предварительные решения по безопасности проектируемого промышленного процесса

Для данного примера желаемый темп производства ПВХ — 90 млн кг (200 млн фунтов) в год, или приблизительно 10 400 кг/ч (23 000 фунтов). Основываясь на известной кинетике реакции при температуре реакции в 60 °С (140 °F), соответствующее время цикла равно 8 ч. При определении емкости реактора в обосновании, как правило, уделяют определенное внимание тому факту, что величина опасности при катастрофическом отказе резервуара связана с количеством опасного материала. В одном из двух предельных случаев можно использовать один реактор для производства партии 81,6 т (180 000 фунтов) ПВХ в 40 % суспензионной смеси, для чего потребуется реактор, вмещающий 189 000 л (50 000 галлонов). Это будет неразумно, так как резервирование невозможно и имеется большой объем воспламеняемого материала под высоким давлением. Кроме того, так как емкость не распределена, то производимые партии будут большими и редкими и им потребуется сопутствующее оборудование, размер которого предназначен для больших объемов материала. Более того, такому реактору потребуется решение по добавлению большого количества опасного раствора инициатора, а работа с достаточно большим объемом такого материала вновь поднимает вопрос об обеспечении безопасности.

В другом предельном случае можно использовать большое количество, например десять, небольших реакторов, каждый из которых спроектирован с расчетом на производство партии в 8,16 т (18 000 фунтов) [примерно 18 900 л (5000 галлонов)]. В первом предельном случае используется большой объем материалов, во втором случае партии небольшие, команды переключения будут выполняться более часто, но имеется куда больше соединительных проводов, клапанов и сложностей в управлении. Компромиссные решения будут зависеть от производственных потребностей, готовности оборудования, стоимости, а также от обеспечения безопасности.

Выполнение таких исследований ведет к выбору числа параллельно работающих реакторов и размера реакторного модуля. В настоящее время это позволяет обеспечить возможности для любого будущего расширения емкости. В рассматриваемом примере решено установить три параллельных реактора, каждый из которых обладает емкостью 64 400 л (17 000 галлонов). Объем раствора инициатора, равный 20 л (5 галлонам), при расчете на партию является количеством, которое обеспечивает безопасное управление. Максимальный объем материала ВХМ в реакторе примерно равен 27,2 т (60 000 галлонов).

Температура реакции выбирается с расчетом достижения желаемого молекулярного веса, который зависит от конечного использования. Чтобы предотвратить выход реакции из-под контроля и обеспечить стабильное функционирование реактора, применяется надлежащее управление температурой охлаждающей воды. Стабильное управление температурой реакции полимеризации требует небольшого температурного различия между охлаждающей водой и температурой реакции. В данном примере температура нагретой охлаждающей воды является достаточно высокой, чтобы обеспечить небольшую разницу температур по сравнению с температурой реакции 60 °С (140 °F). Нагретая охлаждающая вода поступает из хорошо известного источника высокой надежности, в достаточном количестве и под предусмотренным давлением.

Для рассматриваемого примера было принято, что предохранительные и выпускные клапаны связаны с газоочистителем, чтобы выбросы не несли экологические последствия.

F.7 Выявленные опасности для промышленного процесса

Основными кратковременными опасностями, связанными с выбросом ВХМ, являются пожары и взрывы, сопровождаемые возникновением токсичных продуктов горения. Такие типы опасностей включают в себя:

a) факельное горение: утечка из системы, находящейся под давлением, воспламеняется и формирует горящую струю, которая может затронуть и повредить другое оборудование. [Грубо говоря, длина струи приблизительно в 150 раз больше диаметра выходного отверстия — струя из отверстия 50 мм (2 дюйма) может достигать примерно 9 м (30 футов) в длину.];

b) вспышка газовоздушной смеси: выбрасываемая под давлением жидкость вспыхивает, создавая воспламеняемый газ, переходящий в источник возгорания. При возгорании пламя возвращается, перемещаясь по облаку воспламеняемого газа (струя дыма в таком случае может быть существенно больше, чем струя пламени);

c) пожар разлития: остаточная жидкость из-под гидроизоляции стыков создает лужу, которая может загореться, а высота пламени может быть в три раза больше ширины лужи;

d) BLEVEs (взрыв в результате расширения паров кипящей жидкости): внешнее возгорание может привести к отказу бака с наддувом, заполненного ВХМ, или связанного с ним трубопровода, вызванному слабостью металла. Подобный отказ может привести к катастрофическому отказу бака, возникновению огненного шара и возможному разбросу осколков. Защита от избыточного давления с помощью предохранительного клапана не предотвращает BLEVE;

e) взрывы: утечка воспламеняющегося газа в замкнутое пространство с последующим возгоранием может привести к взрывам или детонациям со значительным избыточным давлением;

f) отказ гидросистемы: переполнение бака с последующим расширением жидкости в результате ее нагревания может привести к разрушению любого парового пространства и быстрому росту давления. Может произойти неожиданный отказ бака;

g) разрушение от коррозии под напряжением: воздух (кислород) в системе может повысить присутствие ионов хлорида и может привести к потере целостности металла;

h) токсичные продукты сгорания: продукты сгорания ВХМ включают фосген, хлорид водорода и монооксид углерода, а также другие токсины (эти продукты сгорания присутствуют после пожара, в особенности, если пожар произошел в замкнутом пространстве);

i) выход из-под контроля реакции полимеризации: полимеризация ВХМ может привести к разрушению реактора с выбросом ВХМ и нанесению значительного ущерба.

Кроме того, ВХМ, будучи известным канцерогеном для человека, представляет опасность при его длительном воздействии, поэтому воздействие его паров на персонал контролируется регулирующим органом, OSHA PEL (временное среднее значение предельного воздействия на персонал) которого равно 1 мг/м^3 в воздухе в течение 8 ч (предельное значение 5 мг/м^3 в течение 15 мин). Далее федеральные и местные регулирующие органы утверждают предел уровней выброса из технологической вентиляции и устанавливают системы очистки воды предприятия. На количество остаточного ВХМ в ПВХ также устанавливаются строгие ограничения.

Существуют несколько менее кратковременные опасности, связанные с вдыханием паров ВХМ и возможным отключением охлаждения воспламеняющейся жидкости. Персоналу требуется защита как от вдыхания этих паров, так и от возможного обморожения.

На данном этапе оценки определения масштабов опасных зон предназначены для определения размера возможных крупных происшествий. Выброс 27,2 т (60 000 фунтов) ВХМ может привести к пожароопасному облаку пара, объем которого примерно равен 120 м^3 (400 куб. футов). Так как ВХМ является тяжелым газом и может содержать аэрозоли, полученные в результате воспламенения, то крупное паровое облако наиболее вероятно примет дискообразную форму, но по-прежнему может обладать воспламеняемым следом 300—450 м (1000—1500 футов) в диаметре. Это указывает на то, что максимально опасное происшествие, связанное с одним реактором, может сказаться не только на объекте, но и заполнить воспламеняемым газом достаточно большое замкнутое пространство. Используя критерии оценки, рассмотренные в таблице F.8, такие последствия должны считаться, как минимум, «тяжелыми» и, скорее, «обширными» в зависимости от конкретных рассматриваемых данных. В консервативных целях группа анализа опасности процесса рассматривает эти последствия как входящие в категорию «обширные».

Примечание — Хранение ВХМ в резервуарах на объекте не рассматривается в данном упрощенном примере.

F.8 Стратегия проекта технологического процесса

Подробная проработка проекта требует определения базовых технологических процедур и стратегий технического обслуживания производства. На рисунке F.3 представлена предварительная схема Т и КИП, предназначенная помочь этому процессу. Пошаговые действия этого процесса предоставлены ниже:

a) предварительное откачивание воздуха. Если реакторы были открыты для технического обслуживания, то следует удалить кислород из системы в целях обеспечения качества и целостности металла;

b) подготовка реактора. Пустой реактор промывается водой под высоким давлением, проводится проверка на возможность утечки через люк и обработка антифоулянтами;

c) заправка деминерализованной водой. Добавляется контролируемая порция воды. Добавление большего количества может повлечь за собой гидравлическое переполнение; а меньшего — может негативно сказаться на качестве и привести к потенциальной потере контроля над реакцией. На этом шаге также вносятся все поверхностно-активные средства или другие добавки;

d) заправка ВХМ. В реактор добавляется точная порция ВХМ;

e) нагрев реактора. Из загрузочного бака в партию добавляется инициатор, а в охлаждающую воду, циркулирующую в кожухе реактора, добавляется пар до тех пор, пока партия не достигнет температуры, при которой продолжается реакция [примерно на 5,5 °C (10 °F) ниже температуры реакции в стационарном режиме];

f) реакция. Паровая система отключается, и охлаждающая вода циркулирует в кожухе реактора для управления температурой, отводя тепло полимеризации, пока протекает реакция;

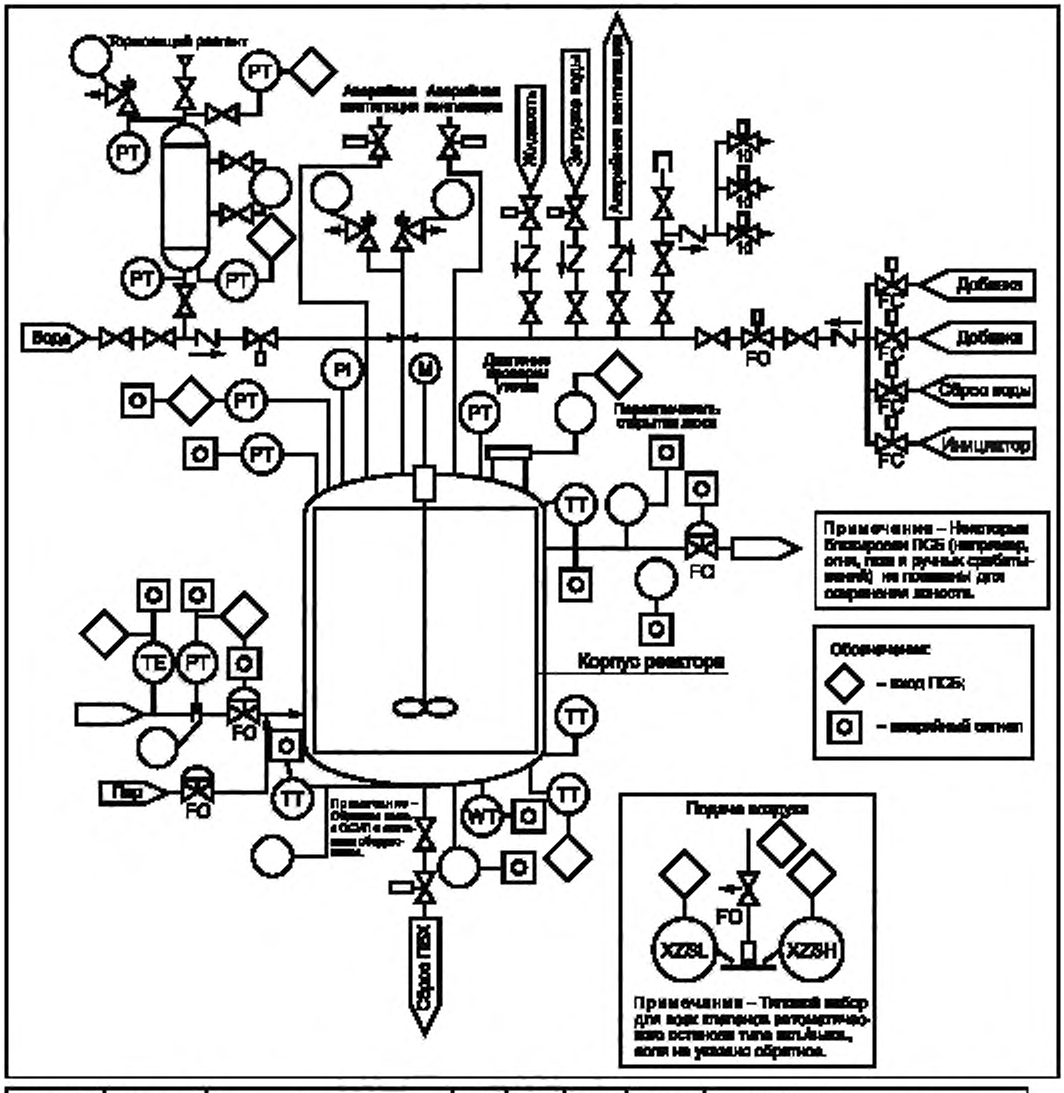
g) завершение. Если давление в реакторе начинает падать, так как большая часть ВХМ была разрушена полимеризацией, то партия будет выгружена;

h) разгрузка реактора. Содержимое реактора выгружается под давлением в расположенную далее по технологической цепочке емкость для временного содержания, где осуществляется удаление газа из системы для последующего отпаривания и сушки. Для предотвращения оседания в реакторе смолистых веществ во время процедуры выгрузки работает аппарат для перемешивания. ВХМ, не вступивший в реакцию, извлекается для повторного использования.

В случае аварийной ситуации используются две дополнительные технологические системы. В случае потери контроля над реакцией или наличия возможности возникновения такой ситуации полимеризация может быть быстро остановлена добавлением в партию химического реагента, тормозящего реакцию (агента, останавливающего реакцию). Тем не менее для надлежащего распределения такого реагента, чтобы позволить ему быстро остановить полимеризацию, необходимо перемешивание партии. Если происходит отказ аппарата для перемешивания, то в течение одной или двух минут должен быть добавлен реагент, тормозящий реакцию, чтобы обеспечить его смешивание перед тем, как пропадет водоворот жидкости в реакторе. В качестве запасного варианта содержимое реактора может быть

перемешано с помощью «барботажа» реактора — сбросом давления, приводящим к появлению поднимающихся пузырьков внутри находящейся в резервуаре жидкости. Оба этих события запускаются оператором.

Вторая технологическая схема предотвращения аварийной ситуации реализуется автоматической системой сброса давления. В случае потери контроля над реакцией ее можно безопасным образом ограничить сбросом давления в реакторе с помощью системы вентиляции. Отвод тепла при парообразовании кипящей массы реакции позволяет безопасным образом отводить тепло из реактора. Производительность аварийной вентиляционной системы определяется пиковой потребностью в вентиляции системы реактора.



Проект #	Редакция #	Редакция	R/S/D	CHKD	APPD	Дата	Проект # YYYY	Дата:
							Начертил:	
							Проверил:	
							Одобрил:	
							DWG# XXXXX1	

Рисунок F.3 — Пример предварительной схемы Т и КИП для модуля реактора ПВХ

Наименования трубопровода показаны для простоты как объединенные. См. рисунок F.11 для уточнения наименований.

F.9 Предварительная оценка опасностей

F.9.1 Общие положения

После того как проект был разработан довольно подробно, группа анализа опасности процесса подвергает проект предварительной оценке опасностей. Эта оценка считается предварительной, так как проект еще не завершен. Группа анализа опасности процесса для более простых частей технологического процесса выполняет анализ методом возможных ситуаций/таблиц контрольных проверок (см. таблицу F.4), а для более сложных — выполняет HAZOP (см. таблицу F.5).

По результатам идентификации опасностей и из истории прошлых происшествий можно сделать вывод, что в реакторе, реализующем технологический процесс в данном примере, возможны события различной степени тяжести от «незначительного» до «существенного» в соответствии с таблицей F.8.

Кроме того, для обеспечения целостности конструкции необходимо рассмотреть соответствие строгим требованиям ликвидации аварии, чтобы предотвратить распространение выбросов ВХМ, которые могут представлять опасность для здоровья и безопасности рабочих. Результаты анализа этой опасности должны быть надлежащим образом документально оформлены, в особенности учитывая последовательность событий, которые могут привести к неуправляемым выбросам.

В таблицах F.4 и F.5 показаны только частичные списки опасностей, относящихся к рассматриваемому примеру. Типичный проект будет обладать куда более обширным списком элементов «что если» и HAZOP.

На основе этих результатов соответствующая группа экспертов анализа опасности по технологическому процессу и его автоматизации создает список случайных событий, в которых ФБ ПСБ была предложена в качестве меры снижения опасности.

В таблице F.6 приведен неполный список случайных событий и стратегий их предотвращения, на основе которых предлагаются стратегии блокировок и действия, предназначенные помочь в дальнейшем определении или в создании дополнительных независимых слоев защиты. Таблица F.6 подготовлена и одобрена командой анализа опасностей технологического процесса (см. раздел F.2).

После того как опасности были идентифицированы, группа анализа опасности процесса формирует следующие рекомендации:

a) реализовать следующую превентивную стратегию ПСБ для случаев потери контроля над реакцией:

- если в реакторе поднимается температура или давление, то у оператора достаточно времени, чтобы удаленно добавить реагент, тормозящий реакцию.

Примечание — Так как аппарат перемешивания не работает, то после добавления тормозящего реагента, чтобы смешать его с реагирующей массой, требуется выполнить барботаж реактора (см. строки 2 и 3 в таблице F.6);

- если это не поможет установить контроль над реакцией, то при очень высокой температуре или давлении ФБ ПСБ для сброса давления откроет аварийные выпускные клапаны, что позволит безопасным образом вернуть контроль над реакцией;

b) в случае потери контроля, которая происходит из-за неисправности аппарата перемешивания (см. строки 2 и 3 таблицы F.6), в дополнение к рекомендациям, приведенным в перечислении a), требуется дополнительная защита:

- на прекращение перемешивания (низкий ток в цепи) оператору будет указывать аварийный сигнал, и после добавления тормозящего реагента требуется выполнить барботаж реактора, чтобы смешать тормозящий реагент с реакционной массой,

- согласно рекомендации в перечислении a) функция открытия аварийных выпускных клапанов ФБ ПСБ будет запасным вариантом для управления потерей контроля над реакцией;

c) нарушения, такие как низкий расход или отсутствие охлаждающей воды, контролируются защитой, описанной в перечислении a). Если низкий расход охлаждающей воды был вызван прекращением подачи питания на насосы, то оператор получает аварийный сигнал о низком расходе, призывающий его включить паротурбинный привод насоса подачи воды;

d) перегрузка реактора водой или ВХМ может привести к переполнению и возможному гидравлическому повреждению реактора из-за большого давления. Подобного повреждения можно избежать, предотвращая перегрев партии, если весовые камеры или уровень заполнения реактора превышают «высший» предел, установленный для этого шага добавления партии в ОСУП. Запасным вариантом при очень высоком давлении в реакторе является ФБ ПСБ, которая для сброса давления открывает аварийные выпускные клапаны;

e) отказ предохранителя от утечки аппарата перемешивания реактора приводит к опасному выбросу ВХМ. Чтобы защитить реактор от подобной опасности рекомендуется при высоком давлении в предохранителе от утечки аппарата перемешивания активировать ФБ ПСБ аварийного сброса давления;

f) так как система реагента, тормозящего реакцию, является очень важной в управлении реакцией, выходящей из-под контроля, то команда рекомендует также использование блокировок в ОСУП, гарантирующих необходимое наличие тормозящего реагента. Блокировки ОСУП не позволяют загрузку ВХМ в реактор в случае, если уровень жидкости в баке с тормозящим реагентом низкий или если давление азотной подушки на бак является низким.

F.9.2 Шаг F.2. Распределение функций безопасности

В таблице F.7 представлены ключевые элементы при распределении функций безопасности.

Таблица F.4 — Метод «что если»/список контрольных проверок (подготовлена и одобрена командой анализа опасностей промышленного процесса, см. F.2)

Что если. .	Опасность	Последствие	Мера обеспечения безопасности	Исходный №	Рекомендация	Выполнил
Происходит отказ подачи электропитания на всей территории (питание контрольно-измерительного оборудования от ИБП сохраняется)	Потеря контроля над реакцией из-за потери возможности перемешивания. На нее указывает отключение двигателя аппарата перемешивания, низкий расход охладителя, высокое давление в реакторе и высокая температура в реакторе	Потеря контроля над реакцией приводит к повышению давления и разгерметизации	Добавление реагента, тормозящего реакцию, и выполнение барботирования реактора, чтобы вернуть контроль над реакцией. Снижение давления в реакторе — ПСБ (с помощью предохранительного клапана давления, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
Ошибка стандартного рецепта загрузки — используются две дозы инициатора	Высокая концентрация инициатора приводит к потере контроля над реакцией. На это указывают высокая температура реактора и высокое давление	Потеря контроля над реакцией приводит к перегрузке давлением и разгерметизации	Добавление реагента, тормозящего реакцию. Разгерметизировать реактор — ПСБ (с помощью предохранительного клапана давления, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
Происходит нарушение предохранителя от утечки в аппарате перемешивания реактора	Выброс ядовитых газов ВХМ. На это указывают высокое давление на предохранителе от утечки реактора и детектор дыма на территории	Ядовитые газы ВХМ воспламеняемы	Дополнительная вентиляция в области предохранителя от утечки реактора. Снижение давления в реакторе в случае высокого давления на предохранителе от утечки — ПСБ		Определить требующийся УПБ с помощью АУЗ	
Примечание — Это только частичный список опасностей.						

Таблица F.5 — HAZOP (подготовлена и одобрена командой анализа опасностей промышленного процесса, см. раздел F.2)

Справочное слово (GW)	Отклонение	Причина	Последствие	Мера безопасности	Исходный №	Рекомендация	Выполнил
Нет	Отсутствие потока	Отказ системы управления охлаждающей водой	В итоге происходит потеря контроля над реакцией из-за высокой температуры в реакторе и/или высокого давления	Добавление реагента, тормозящего реакцию. Разгерметизировать реактор — ПСБ (с помощью предохранительного клапана давления, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
		Насос останавливается в связи с отказом подачи питания на насос	В итоге происходит потеря контроля над реакцией из-за высокой температуры в реакторе и/или высокого давления	Помимо электропитания у насоса имеется паровой привод. Добавить реагент, тормозящий реакцию. Разгерметизировать реактор — ПСБ (с помощью предохранительного клапана давления, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
Нет	Отсутствие перемешивания	Отказ привода двигателя аппарата перемешивания	Пониженная температура охлаждения, неоднородность приводят к потере контроля над реакцией. На это указывают высокая температура в реакторе, высокое давление и низкая сила тока в двигателе аппарата перемешивания	Добавление реагента, тормозящего реакцию, и выполнение барботирования реактора, чтобы вернуть контроль над реакцией. Разгерметизировать реактор — ПСБ (с помощью предохранительного клапана, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
Больше	Более высокая температура	Отказ управления температурой приводит к перегреву во время парового обогревания	Высокая температура ведет к потере контроля над реакцией. На это указывают высокое давление и температура в реакторе	Добавление реагента, тормозящего реакцию. Разгерметизировать реактор — ПСБ (с помощью предохранительного клапана давления, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
Больше	Более высокий уровень	Отказ управления уровнем приводит к переполнению реактора	С ростом температуры реактор заполняется жидкостью, возможно гидравлическое повреждение реактора и выброс ВХМ. На это указывают высокий уровень загрузки, большой вес загрузки или высокое давление в реакторе	Сравнить высокий уровень и вес с рецептом. Разгерметизировать реактор — ПСБ (с помощью предохранительного клапана давления, размер которого соответствует событию)		Определить требующийся УПБ с помощью АУЗ	
Примечание — Это только частичный список опасностей.							

Таблица F.6 — Частичная сводка оценки опасностей для разработки стратегии ФБ ПСБ

№	Инициирующее событие	Нарушение процесса	Затронутая переменная процесса	Превентивная стратегия
1	Отказ средств управления охлаждающей водой	Потеря охлаждения приводит к потере контроля над реакцией	Низкий расход охлаждающей воды. Высокая температура реактора. Высокое давление в реакторе	Добавление реагента, тормозящего реакцию. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
2	Отказ привода двигателя аппарата перемешивания	Снижение эффективности охлаждения, неравномерность температуры ведет к потере контроля над реакцией	Низкая сила тока в двигателе аппарата перемешивания. Высокая температура реактора. Высокое давление в реакторе	Добавление реагента, тормозящего реакцию, и выполнение барботирования реактора, чтобы вернуть контроль над реакцией. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
3	Отказ подачи электропитания на всей территории (но питание контрольно-измерительного оборудования от ИБП сохраняется)	Потеря контроля над реакцией из-за потери возможности перемешивания	Двигатель аппарата перемешивания отключен. Низкий расход охлаждающей жидкости. Высокое давление в реакторе. Высокая температура реактора	Добавление реагента, тормозящего реакцию, и выполнение барботирования реактора, чтобы вернуть контроль над реакцией. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
4	Остановка насоса охлаждающей воды, отказ подачи питания на насос	Прекращение охлаждения приводит к потере контроля над реакцией	Низкий расход охлаждающей воды. Высокая температура реактора. Высокое давление в реакторе	Паровые приводы на насосах. Добавление реагента, тормозящего реакцию. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
5	Ошибка стандартного рецепта загрузки — используются две загрузки инициатора	Высокая концентрация инициатора приводит к потере контроля над реакцией	Высокое давление в реакторе. Высокая температура реактора	Добавление реагента, тормозящего реакцию. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
6	Отказ системы управления приводит к переполнению реактора	С ростом температуры реактор заполняется жидкостью, возможно гидравлическое повреждение реактора и выброс ВХМ	Высокий уровень загрузки. Большой вес загрузки. Высокое давление в реакторе	Сравнить уровень и вес с рецептом. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
7	Отказ управления температурой приводит к перегреву во время парового обогревания	Высокая температура ведет к потере контроля над реакцией	Высокое давление в реакторе. Высокая температура реактора	Добавление реагента, тормозящего реакцию. Разгерметизация реактора (ПСБ). Предохранительные клапаны давления (независимый слой защиты)
8	Отказ предохранителя от утечки аппарата перемешивания реактора	Отказ предохранителя утечки ведет к опасному выбросу ядовитых газов ВХМ	Высокое давление в предохранителе от утечки реактора. Обнаружение ядовитых газов на территории, где происходит реакция	Дополнительная вентиляция в области предохранителя от утечки реактора. Разгерметизация реактора в случае высокого давления на предохранителе от утечки (ПСБ)

Таблица F.7 — Жизненный цикл ПСБ. Блок 2

Обзор					
Стадия или деятельность жизненного цикла системы безопасности		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок 7, блок 2	Распределение функций безопасности по слоям защиты	Распределение функций безопасности по слоям защиты и для каждой ФБ ПСБ, связанного с ней УПБ	9	Описание требующейся ФБ ПСБ и связанные с ней требования к полноте безопасности	Описание распределения требований к безопасности (см. раздел 9 МЭК 61511-1:2016)

F.10 Определение уровня полноты безопасности ФБ ПСБ

С помощью предложенного списка ФБ ПСБ на собрании группы анализа опасности процесса определяется требующийся УПБ для каждой ФБ ПСБ. Будет использован метод анализа уровней защиты (АУЗ). Описание метода АУЗ см. в МЭК 61511-3:2016, приложение F. Дополнительное руководство представлено в AIChE, CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment,* 2001.

F.11 АУЗ для рассматриваемого примера

В данном разделе объясняется переход от данных, представленных в частичной сводке информации по оценке опасностей (см. таблицу F.6), к результатам АУЗ (см. таблицу F.9).

Ниже представлено описание сценария АУЗ.

Событие 1. Отказ управления подачей охлаждающей воды.

Этот сбой оборудования инициирует потерю контроля над реакцией, которая может привести к катастрофическому разрыву реактора. Влияние такого события оценивается как «существенное», что согласно примечанию 1 к таблице F.8 приводит к допустимой интенсивности, равной 10^{-b}/год для одиночного сценария. Несколько отказов в системе управления могут привести к такому сбою оборудования, а опыт работы указывает на то, что подобный тип сбоя случается примерно один раз в 10 лет. Согласно таблице F.6 методом защиты служит добавление тормозящего реагента, но потеря контроля над реакцией может происходить слишком быстро и оператор может не успеть среагировать на аварийный сигнал. Этот слой защиты не рассматривается для снижения риска. На производственной площади, как правило, присутствуют люди, поэтому предполагаются негативные последствия для персонала, связанные с данным событием. Эффективность предохранительных клапанов давления (ПКД) оценивается только на 90 %, так как забивание клапанов является распространенной проблемой при таком событии. Так как ПКД находятся на одном трубопроводе выгрузки, то их консервативно рассматривают как отдельный независимый слой защиты (НСЗ). Это приводит к значению вероятности возникновения промежуточного события, равному 10^{-2} в год. Согласно консервативным предположениям, используемым в данном примере, только ПКД квалифицируются как независимый слой защиты. Группа анализа опасности процесса выполняет анализ всех рисков для обеспечения безопасности технологического процесса и принимает решение, что ФБ ПСБ является надлежащим решением. Как показано в таблице F.9, для этого требуется ФБ ПСБ с УПБ 3.

Примечание — ПКД подбираются в соответствии с документацией на корпус реактора, но как продемонстрировано с помощью АУЗ (используя критерии корпоративного риска в таблице F.8), они не оказываются достаточной защитой, обеспечивающей целевое снижение риска в рассматриваемом сценарии. Это замечание типично для всех сценариев АУЗ в данном примере.

Событие 2. Отказ привода двигателя аппарата перемешивания.

Это нарушение инициирует выход реакции из-под контроля, который похож на Событие 1, с тем исключением, что так как перемешивание прекратилось, то требуется дополнительный шаг — барботаж реактора (см. F.8), чтобы установить контроль над реакцией посредством добавления тормозящего реагента. И снова эта потеря контроля может случиться так быстро, что оператор может не успеть среагировать, поэтому никакого снижения риска от реакции оператора на аварийный сигнал не происходит. Несколько отказов в системе управления или в самом аппарате перемешивания могут привести к такому сбою оборудования, а опыт работы указывает на то, что подобный тип сбоя случается примерно один раз в 10 лет. ФБ ПСБ S-1 является единственной эффективной ФБ ПСБ для данного события, и ей требуется УПБ 3.

Событие 3. Прекращение обычного электропитания на всей территории.

Несмотря на то что это нарушение обладает очевидными отличиями от События 2, выбор УПБ для ФБ ПСБ приводит к похожему результату, как и в случае События 2.

Событие 4. Прекращение подачи питания на насос с охлаждающей водой.

Сбой оборудования в Событии 4 похож на сбой оборудования в Событии 1. Вмешательство оператора может остановить выход реакции из-под контроля посредством запуска водяных насосов с паротурбинным приводом или добавления тормозящего реагента. И хотя это действие оператора полагается достаточно эффективным, никакое снижение риска, связанного с готовностью оператора, не учитывается. Анализ, представленный в таблице F.9, привел к выбору УПБ 3 для ФБ ПСБ S-1.

Событие 5. Двойная загрузка инициатора.

Это нарушение ведет к очень энергичному выходу реакции из-под контроля с высокой интенсивностью выделения тепла и стремительным ростом давления, несмотря на то что осуществляется подача охлаждающей воды. Рост давления должен быть достаточно быстрым для того, чтобы температура послужила действенной мерой для срабатывания ФБ ПСБ. Как ПКД, так и сбрасывающая давление ФБ ПСБ спроектированы для безопасного управления этим выходом операции из-под контроля. Из-за предусмотренных в проекте и процедурных мер обеспечения безопасности для реализации этого нарушения требуется очень маловероятная комбинация отказов. Поэтому средняя вероятность возникновения инициирующего события была выбрана равной 10^{-1}. Средняя вероятность, один не связанный с ПСБ НСЗ и «существенная» степень тяжести приводят к выбору УПБ 3 для ФБ ПСБ S-2.

Событие 6. Переполнение реактора, вызванное отказом системы управления.

Влияние этого нарушения заключается в гидравлическом воздействии большого давления на реактор, которое может привести к повреждению фланцевой прокладки или другому подобному выбросу. При большом количестве партий в год и их различающихся рецептах вероятность этого события определяется в среднем один раз в 10 лет. Команда приняла решение, что эффективность уровня ОСУП и аварийных сигналов датчиков массы с учетом вовлечения оператора составляет 90 % (10^{-1}), так как системы аварийной сигнализации располагаются на отдельном контроллере ОСУП. ПКД и ПСБ сброса давления эффективно устраняют это нарушение. «Серьезная» степень тяжести с умеренной вероятностью возникновения инициирующего события и двумя не связанными с ПСБ НСЗ указывали на то, что для ФБ ПСБ сброса давления подходит УПБ 1. Несмотря на то что для ФБ ПСБ определен УПБ 1, ФБ ПСБ S-2 следует проектировать с УПБ 3, как это требуется для События 5.

Событие 7. Отказ управления температурой во время этапа нагревания. Перегрев партии.

Это событие приводит к потере контроля над реакцией, подобно Событию 1. Последствия данного события и мероприятия по защите подобны рассмотренным для События 1 за исключением того, что датчик температуры не очень разумно использовать в мероприятиях по снижению риска данного события. Во время нагревания у оператора есть время добавить тормозящий реагент, чтобы предотвратить выход реакции из-под контроля. Однако, так как температурный датчик используется в системе управления, он может оказаться частью инициирующей причины данного события. Поэтому реакция оператора на аварийный сигнал о высокой температуре не будет являться НСЗ для данного события. ФБ ПСБ S-1 следует проектировать с УПБ 3, что уже требовалось для События 1.

Событие 8. Отказ предохранителя от утечки аппарата перемешивания.

Специальный предохранитель от утечки, используемый для данного реактора, ограничивает выбросы ВХМ до незначительных величин, если предохранитель отказывает. Существующей местной вентиляции будет достаточно, чтобы минимизировать пожаровзрывоопасность. Группа анализа опасности процесса решает, что степень тяжести «серьезная», и считает, что местная вентиляция эффективна на 90 % (10^{-1}). НСЗ отсутствует, степень тяжести «серьезная» и вероятность события высокая, поэтому согласно таблице F.9 подходящим считается УПБ 2.

F.12 Критерии допустимого риска

Критерии допустимого риска, использованные в данном примере, представлены в таблице F.8.

Эти критерии зависят от компании. Каждой компании при определении необходимых функций безопасности потребуется применять свои критерии риска и, если это потребуется, согласовывать их с местными органами власти.

Для простоты в данном примере допускается, что реактор постоянно находится в работе (100 % времени). В нем также не учитывается тот факт, что опасности существуют для каждого из трех реакторов.

После завершения АУЗ значения снижений правдоподобной вероятности событий для сценариев с 1 по 5 и 7 были просуммированы. Общая частота 6Е-5 удовлетворяет корпоративному критерию допустимой частоты для событий «существенной» степени тяжести, равной 10^{-4}, как показано в таблице F.8. Общее значение снижений частоты событий для сценариев 6 и 8 составляло 1.01Е-4, что соответствует корпоративному критерию допустимой частоты для событий «серьезной» степени тяжести, равной 10^{-3}.

Таблица F.8 — Классификация допустимого риска

Степень тяжести	Определение	Допустимая частота (событий/год) (см. примечание 1)
Существенная	Один или несколько смертельных исходов или же необратимые последствия для здоровья	10^{-4}
Серьезная	Несколько случаев необратимых телесных повреждений; 1 или 2 случая ограничения трудоспособности, или случай временной потери трудоспособности, или последствия средней тяжести для здоровья человека	10^{-3}
Незначительная	Незначительный ущерб для здоровья или обратимые последствия для здоровья	10^{-2}

Примечания

1 Представленные допустимые частоты предназначены для общего риска от всех опасностей. Допустимая частота для каждого сценария АУЗ устанавливается на один порядок ниже, чтобы учесть множественные опасности (т. е. каждому сценарию с «существенной» степенью тяжести назначается допустимая частота в 10^{-5}). Этот подход допустим для данного примера, так как рабочая зона, как правило, не занята людьми, а единственным человеком, подверженным опасностям, связанным с работой, является оператор, занимающийся плановым осмотром (осмотр выполняется одним человеком).

2 Данные таблицы F.8 должны быть определены в стандарте компании.

3 Компания в данном примере является корпорацией, работающей как в Великобритании, так и в США. Для проектов, реализованных в Великобритании, применяются дополнительные критерии риска. По мнению Управления по охране труда Великобритании риск, от опасного события должен быть снижен до такой степени, до которой стоимость любых дальнейших снижений риска несоразмерна получаемой выгоде. Ссылки: *Reducing Risk Protecting People*, HSE, ISBN No. 07176-2151-0, опубликовано в 2001; МЭК 61511-3.

gost.e-ecolog.ru

Таблица F.9 — Пример реактора ВХМ. Уровень полноты, основанный на АУЗ (подготовлено и одобрено группой анализа опасностей технологического процесса, см. раздел F.2)

№	Негативное событие	Степень тяжести/ допустимая частота	Инициирующая причина	Частота инициации (событий в год)	Защитные слои			Дополнительное ослабление	Промежуточная частота событий (событий в год)	Число НСЗ	Требуется ли ФБ ПСБ?	Уровень полноты безопасности ФБ ПСБ	Сниженная частота события (в год)	Примечание (имя ФБ ПСБ)
					Проект процесса	ОСУП	Аварийные сигналы и т. д.							
1	Разрыв реактора	Существенная/ 10^{-5}	Сбои управления охлаждающей H_2O	$1{,}0^{-1}$	Нет	Нет	Нет	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3}	$1{,}0^{-5}$	S-1
2	Разрыв реактора	Существенная/ 10^{-5}	Сбои привода двигателя аппарата перемешивания	$1{,}0^{-1}$	Нет	Нет	Нет	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3}	$1{,}0^{-5}$	S-1
3	Разрыв реактора	Существенная/ 10^{-5}	Потеря электропитания от основной системы на всей территории	$1{,}0^{-1}$	Нет	Нет	Нет	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3}	$1{,}0^{-5}$	S-1
4	Разрыв реактора	Существенная/ 10^{-5}	Отказ подачи питания на насос с охлаждающей водой	$1{,}0^{-1}$	Нет	Нет	Нет	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3}	$1{,}0^{-5}$	S-1
5	Разрыв реактора	Существенная/ 10^{-5}	Двойная загрузка инициатора	$1{,}0^{-1}$	Нет	Нет	Нет	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3}	$1{,}0^{-5}$	S-2
6	Гидравлическое повреждение реактора сверхвысоким давлением	Серьезная/$1{,}0^{-4}$	Переполненный реактор, отказ системы управления	$1{,}0^{-1}$	Нет	Нет	Аварийные сигналы уровня жидкости (400 LSH) и датчиков массы (300 WTH), 10^{-1}	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3} (требуется УПБ 1)	$1{,}0^{-6}$ (требуется 10^{-4})	S-2

Окончание таблицы F.9

№	Негативное событие	Степень тяжести/ допустимая частота	Инициирующая причина	Частота инициации (событий в год)	Защитные слои			Дополнительное ослабление	Промежуточная частота событий (событий в год)	Число НСЗ	Требуется ли ФБ ПСБ?	Уровень полноты безопасности ФБ ПСБ	Сниженная частота события (в год)	Примечание (имя ФБ ПСБ)
					Проект процесса	ОСУП	Аварийные сигналы и т. д.							
7	Разрыв реактора	Существенная/ 10^{-5}	Сбои в управлении температурой и избыточный пар	10^{-1}	Нет	Нет	Нет	PSVs 10^{-1}	10^{-2}	1 (ПКД)	Да	3 (Сброс давления) 10^{-3}	10^{-5}	S-1
8	Выброс ВХМ	Серьезная/10^{-4}	Сбои предохранителя от утечки на аппарате перемешивания	10^{-1}	Местная вентиляция предохранителя от утечки реактора, 10^{-1}	Нет	Нет	Нет	10^{-2}	0	Да	2 (Сброс давления) 10^{-2}	10^{-4}	S-3
Значения правдоподобной вероятности являются событиями в год. Остальные цифровые значения — это вероятности.														

F.13 Шаг F.3. Спецификации требований к безопасности ПСБ

F.13.1 Обзор

Таблица F.10 — Жизненный цикл безопасности ПСБ. Блок 3

Обзор					
Стадия или деятельность жизненного цикла системы безопасности		Цели	Раздел или подраздел требований МЭК 61511-1: 2016	Входы	Выходы
МЭК 61511-1: 2016, рисунок 7, блок 3	СТБ ПСБ	Установить для каждой ПСБ требования в терминах требуемых ФБ ПСБ и их значений полноты безопасности, необходимых для достижения требуемой функциональной безопасности	10	Описание распределения требований к безопасности (см. раздел 9 МЭК 61511-1:2016)	Требования к безопасности ПСБ; требования к безопасности ППО

Информация в СТБ, приведенная в данном примере, может быть оформлена в формате единого документа (см. таблицу F.10). Как альтернативный вариант могут использоваться несколько документов. Приведенные ниже требования предназначены только для данного примера.

F.13.2 Требования к входам

Информация в таблице F.11, ФБ ПСБ и связанные с ними УПБ являлись выходами шага 2 и использовались в разработке СТБ.

Таблица F.11 — Функции безопасности ПСБ и их УПБ

Идентификатор	Контролируемая переменная процесса	УПБ
S-1	Высокое давление и температура в реакторе	3
S-2	Высокое давление в реакторе	3
S-3	Высокое давление на предохранителе от утечки аппарата перемешивания	2

ОСУП выполняет функции оперативного управления для планового запуска и нормального останова. Они в данном примере не рассматриваются.

Группа анализа опасности процесса определила, что закупоривание является возможной проблемой в данном приложении. Команда проектировщиков должна учесть это замечание при проектировании ПСБ.

Никаких законодательных и нормативных требований, которые повлияли бы на проект ПСБ, не было идентифицировано.

F.13.3 Функциональные требования к безопасности

В таблице F.12 приведены безопасные состояния для каждой ФБ ПСБ и продемонстрирована функциональная связь между входами и выходами технологического процесса, включая требующуюся логику.

Таблица F.12 — Функциональная связь между вводами-выводами для ФБ ПСБ

ФБ ПСБ	УПБ	Датчик	Описание	Безопасное состояние исполнительного элемента
S-1	3	100PT 100PT1 100TT	Если давление в реакторе превышает 125 фунт/кв. дюйм или температура в реакторе превышает 200 °F	Открытый 100PV Открытый 100PV1
S-2	3	100PT 100PT1	Если давление в реакторе превышает 125 фунт/кв. дюйм	Открытый 100PV Открытый 100PV1
S-3	2	200PT	Если давление в предохранителе от утечки выше чем 10 фунт/кв. дюйм	Открытый 100PV Открытый 100PV1

В таблице F.13 для рассматриваемого технологического процесса представлены входные параметры датчиков ПСБ, их точки срабатывания, нормальный диапазон рабочих режимов и ограничения на условия эксплуатации.

Таблица F.13 — Датчики ПСБ, нормальный диапазон рабочих режимов и точки срабатывания

Маркировка	Диапазон калибровки	Нормальный диапазон рабочих режимов	Аварийный сигнал, предшествующий срабатыванию		Точка срабатывания	
100PT	0—200 фунт/кв. дюйм	60—100 фунт/кв. дюйм	115 фунт/кв. дюйм	При превышении	125 фунт/кв. дюйм	При превышении
100PT1	0—200 фунт/кв. дюйм	60—100 фунт/кв. дюйм	115 фунт/кв. дюйм	При превышении	125 фунт/кв. дюйм	При превышении
100TT	0—250 °F	125—175 °F	180 °F	При превышении	200 °F	При превышении
200PT	0—50 фунт/кв. дюйм	0—20 фунт/кв. дюйм	5 фунт/кв. дюйм	При превышении	10 фунт/кв. дюйм	При превышении

Все ФБ ПСБ проектируются для операции останова по отключению питания.

Исполнительные элементы переходят в их безопасное состояние при отключении питания, как это определено в таблице F.9. Чтобы удовлетворить требованиям архитектуры и требованиям к $ВОНЗ_{ср}$, исполнительные элементы собираются по схеме голосования (1oo2).

Время реакции — одна минута или менее — считается адекватным для каждой ФБ ПСБ, если не указано другое.

Для ПСБ используются датчики и логическое решающее устройство, оцененные в соответствии с МЭК 61508. Оцененные датчики также соответствуют требованиям для предшествующего использования.

Обзор, проведенный группой анализа опасности процесса, указывает на отсутствие комбинаций безопасных состояний технологического процесса, которые в случае, если они происходят одновременно, создают отдельную опасность.

Датчики обладают стойкостью к систематическим отказам SC 2, а логическое решающее устройство — SC 3.

Датчики для S-1 собраны по схеме голосования 1oo3, а для S-2 — 1oo2, чтобы обеспечить соответствие требованиям архитектуры и требованиям $ВОНЗ_{ср}$.

ЧМИ ОСУП будет служить основным человеко-машинным интерфейсом для ПСБ. Все функции отображения аварийных сигналов будут реализованы посредством ЧМИ ОСУП; не требуется никакой аппаратно-подключенной визуальной индикации. Интерфейс разработки/обслуживания будет размещен в безопасном месте.

В случае потери связи с ЧМИ у оператора имеется кнопка останова, установленная на панели, которую он будет применять для запуска последовательности действий, что необходимо для того, чтобы перевести процесс в безопасное состояние должным образом. Кнопка останова подключена к дискретным входам логических решающих устройств ПСБ и ОСУП и приводит к добавлению тормозящего реагента посредством действия ОСУП.

Группа анализа опасности процесса ознакомилась с руководством по безопасности выбранного логического решающего устройства ПСБ и определила, что ручная активация клапанов безопасности, независимая от логического решающего устройства, не требуется. Основываясь на этом выводе и нежелательных последствиях внезапного сброса давления технологического процесса, непосредственная ручная активация не включается в СТБ. См. логическую диаграмму (рисунок F.11).

Так как это пакетный режим, то процесс будет остановлен в случае обнаружения сбоев в ПСБ. То есть процесс не будет выполняться, если ПСБ работает в режиме ограниченной функциональности.

Аварийным сигналам, предшествующим срабатыванию, на которые оператор может среагировать, чтобы предотвратить останов систем, выполняемый ПСБ, должен быть назначен наивысший приоритет.

Все установки срабатываний ПСБ будут выполняться вручную. Переключатели ручной установки будут располагаться на панели оператора в помещении для управления.

Так как это пакетный режим и применяются надежные методы разработки систем управления, то интенсивность ложных срабатываний не рассматривается.

Дублирование (функциональное дублирование прикладной логики ПСБ в ОСУП) выполняется для борьбы с систематическими сбоями ППО. Было признано, что дублирование повышает интенсивность ложных срабатываний, но для процесса в пакетном режиме в данном примере ложные срабатывания не рассматриваются.

Обнаружение сбоев внешних устройств и ЧМИ с помощью диагностики предотвратит запуск очередной партии, но если партия обрабатывается, то поступит аварийный сигнал.

При останове процесса, инициированном ПСБ, все контуры управления ОСУП будут переведены в ручной режим и выходы установлены в безопасное состояние.

Каждая схема ПСБ (например, ввода-вывода, коммуникации, диагностики) должна контролироваться, чтобы гарантировать, что перед запуском ПСБ на них подано напряжение питания.

Каждый датчик перед запуском ПСБ должен автоматически проверяться на наличие несоответствующих значений (например, ниже 4 мА).

Режимы работы включают загрузку, выполнение реакции и выгрузку. Все функции ПСБ должны функционировать в каждом из режимов.

Не должно быть никаких перехватов управления, блокировок или байпасов.

Какие-либо особые требования для сохранения работоспособности ПСБ в случае значительного происшествия отсутствуют.

F.13.3.1 Требования к полноте безопасности

УПБ, требующийся для каждой ФБ ПСБ, определен в таблице F.9.

Ниже представлены характеристики аппаратных средств, необходимые для достижения требующегося УПБ:

- логическое решающее устройство с SC 3 (т. е. устройство со значением $ВОНЗ_{ср}$ между 0,001 и 0,0001), оцененное в соответствии с МЭК 61508;
- датчики и исполнительные элементы, которые должны быть выбраны в соответствии с МЭК 61508 и одобрены пользователем (см. ISA TR84.00.04, часть 1);
- все исполнительные элементы должны быть обеспечены датчиками положения и должно быть проверено, обеспечивается ли соответствие положения клапана команде логической схемы.

Ниже представлены характеристики диагностики, необходимые для достижения требующегося УПБ:

- диагностика предоставляется вместе с логическим решающим устройством;
- проверка верхнего и нижнего пределов на входах всех датчиков как в ПСБ, так и в ОСУП;
- сравнение диагностики на 100РТ и 100РТ1 как в ПСБ, так и в ОСУП;
- дублирование в ОСУП.

Реактор будет выключаться дважды в год для технического обслуживания в автономном режиме и испытания блокировок безопасности. Все слои защиты, идентифицированные в процессе АУЗ, которые обеспечивают снижение риска, должны тестироваться с такой же частотой.

Примечание — Так как режим работы является пакетным, то некоторые устройства ПСБ могут испытываться более часто (например, выпускные клапаны могут испытываться перед запуском каждой партии), если требуется достичь целевого $ВОНЗ_{ср}$.

На данном этапе вычисления для верификации УПБ, описанные в F.16, указывают на отсутствие необходимости более высокой частоты проведения испытаний. Тем не менее, если опыт эксплуатации показывает, что частота отказов устройства ФБ ПСБ выше, чем предполагается в вычислениях $ВОНЗ_{ср}$, то испытания некоторых устройств могут проводиться более часто.

Все ФБ ПСБ питаются от ИБП, чтобы снизить число ложных срабатываний. Так как это пакетный режим, то нет никаких дополнительных условий для предотвращения ложных срабатываний.

Отказы по общей причине будут минимизированы посредством:

- предоставления отдельных точек для резервных датчиков давления;
- предоставления отдельных линий для резервных выпускных клапанов;
- гарантии того, что аварийные сигналы, заявленные как НСЗ в событии 6 таблицы 7, совершенно независимы от ФБ ПСБ (т. е. для функций управления, аварийных сигналов и дублирования ОСУП применяются отдельные контроллеры распределенной системы управления);
- применения надежных инженерных практик (например, заземления, защиты от перенапряжения, источников питания, разнообразия), описанных в разделах F.18 и F.19;
- учета человеческого фактора (например, в связи с конфигурированием, калибровкой и испытаниями), используя разный персонал для проверки и принятия.

F.14 Функциональное описание и концептуальное проектирование

В настоящем разделе описано как функциональные требования к безопасности и требования к полноте безопасности интегрируются для обеспечения разработки архитектур ФБ ПСБ, верификации УПБ для каждой ФБ ПСБ и разработки ППО ПСБ.

F.14.1 Описательная часть логики системы реактора рассматриваемого примера

В данной ПСБ реализуются три автоматические ФБ ПСБ S-1, S-2 и S-3 (см. таблицу F.14).

- функции S-1 и S-2 ПСБ защищают от выхода реакции из-под контроля из-за высокой температуры/давления в реакторе, так как реакция является экзотермической, а высокое давление является результатом высокой температуры;

- если давление на датчиках 100PT или 100PT1 превышает 125 фунт/кв. дюйм или температура на датчике 100TT превышает 200 °F, то функция безопасности S-1 открывает выпускные клапаны реактора.

Так как рост давления происходит невероятно быстро в случаях переполнения реактора или добавления двойной дозы инициатора, то для предотвращения подобных событий используется ФБ ПСБ S-2. Достаточно медленная реакция температурного датчика может не обнаружить это невероятно быстрое событие, поэтому температурный датчик 100TT не включен в вычисления $ВОН3_{ср}$. Если давление на датчиках 100PT или 100PT1 превышает 125 фунт/кв. дюйм, то откроются выпускные клапаны.

Так как в данном применении используются идентичные интеллектуальные датчики давления, то должна учитываться вероятность того, что систематическая ошибка приведет к отказу обоих датчиков одновременно. Чтобы обнаружить значения датчиков, выходящие за верхнюю или нижнюю границу диапазона, или различающиеся между собой значения, осуществляется их диагностика логическими решающими устройствами как ПСБ, так и ОСУП. Степень диагностического охвата учитывается в вычислениях $ВОН3_{ср}$, как это описано в F.16.

Функция S-3 ПСБ открывает выпускные клапаны 100PV и 100PV1 в случае, когда давление в предохранителе от утечки превышает 10 фунт/кв. дюйм в соответствии с измерениями 2000PT.

Так как инициирующие причины для сценариев с 1 по 8 формируют запросы к устройствам одной ФБ ПСБ, то эти запросы должны суммироваться, чтобы определить режим работы каждой ФБ ПСБ. В данном примере их сумма равна до 0,8 запросов/год, что меньше, чем запрос в год для ФБ ПСБ. Поэтому каждая ФБ ПСБ будет работать в режиме с низкой интенсивностью запросов. Сравнение режима по запросу с режимом непрерывной работы см. в ISA TR84.00.04:2015 и A.9.2.3.

Таблица F.14 — Причинно-следственная диаграмма

Причинно-следственная диаграмма реактора (формат таблицы)						
Причина		Описание	Уставка срабатывания	Последствие		
Функция безопасности	Датчик/вход			Исполнительное устройство	Действие	Комментарий
S-1	100PT 100PT1	Давление в реакторе ИЛИ	> 125 фунт/кв. дюйм	100PV	OPEN	Сброс давления в реакторе
	100TT	Температура в реакторе	> 200 °F	100PV1	OPEN	Сброс давления в реакторе
S-2	100PT 100PT1	Высокое давление в реакторе	> 125 фунт/кв. дюйм	100PV 100PV1	OPEN OPEN	Сброс давления в реакторе
S-3	200PT	Давление в предохранителе от утечки реактора	>10 фунт/кв. дюйм	100PV 100PV1	OPEN OPEN	Сброс давления в реакторе

F.15 Вычисления для верификации УПБ

Для каждой ФБ ПСБ был создан схематический чертеж (т. е. диаграмма состояний, как показано на рисунках F.4, F.6 и F.8), учитывающий приведенные выше функциональные требования и требования к полноте безопасности, чтобы:

- описать то, как были выполнены функциональные требования и требования к полноте безопасности;
- проиллюстрировать, как архитектура ФБ ПСБ соответствует требованиям УПБ;
- продемонстрировать $ВОН3_{ср}$ для каждой подсистемы ФБ ПСБ (подсистемы датчиков, подсистемы логических решающих устройств или подсистемы исполнительных элементов);
- обеспечить основу для разработки архитектуры ПСБ;
- обеспечить основу для вычислений $ВОН3_{ср}$ для ФБ ПСБ.

Затем эти диаграммы состояний используются в разработке дерева отказов для каждой ФБ ПСБ с помощью доступного на рынке программного обеспечения. На выходе ПО для анализа дерева сбоев дается информация о $ВОН3_{ср}$ для ФБ ПСБ (см. рисунки F.5, F.7 и F.9). На данном этапе вычисленное значение $ВОН3_{ср}$ сравнивается с требующимся значением $ВОН3_{ср}$ (см. таблицу F.9, столбец 10); там, где вычисленное $ВОН3_{ср}$ не соответствовало требованиям таблицы 7, концептуальный проект был соответствующим образом изменен.

Каждый тип устройства ФБ ПСБ приведен в таблице F.15 вместе с его параметрами безотказности. Эти параметры были получены на основе предшествующего использования данных от поставщиков и баз данных отрасли, с акцентом на эксплуатационные данные.

Среднее время работы до опасного отказа (*MTTFd*):

Таблица F.15 — Показатели *MTTFd* устройств ПСБ из F.1

Предохранительный выпускной клапан	60 лет
Датчик давления	60 лет
Датчик температуры с термопреобразователем сопротивления (RTD)	60 лет
Соленоидный клапан	35 лет
Логическое решающее устройство ПСБ	2500 лет

Общая причина

Проблемы общей причины были решены с помощью методов, описанных в F.18. Остаточные отказы по общей причине были учтены добавлением факторов к дереву отказов для каждой ФБ ПСБ. Эти факторы были основаны на опыте работы на объекте. Как для выпускных клапанов, так и для соленоидных клапанов отказы по общей причине составляют 1 % общего числа опасных необнаруженных отказов; для датчиков отказы по общей причине были предварительно оценены в 2 % от общего числа опасных необнаруженных отказов [т. е. интенсивность опасных необнаруженных отказов датчиков, связанная с отказами по общей причине, равна 0,02·(1/60); в случае выпускных клапанов из-за отказов по общей причине — 0,01·(1/60); и в случае соленоидных клапанов по причине отказов по общей причине она равна 0,01·(1/35)].

Систематические сбои

Логическое решающее устройство ПСБ обладает стойкостью к систематическим отказам SC 3, которая включает отказы аппаратных средств, требования к архитектуре (отказоустойчивость) и отказы встроенного программного обеспечения. Следует отметить, что систематические отказы ППО не были учтены при оценке логического решающего устройства. Проблемы систематических отказов ППО логического решающего устройства были решены дублированием логики в ОСУП (см. диаграммы состояний на рисунках F.4, F.6 и F.8). Для снижения числа систематических отказов ППО ПСБ была использована ОСУП; однако вклад аппаратных средств ОСУП в $ВОЗН_{ср}$ не был учтен при анализе дерева отказов каждой ФБ ПСБ.

Примечание — Приведенная выше методика дополняет методы, определенные в МЭК 61511-1:2016, раздел 12.

Датчики давления и температуры являются интеллектуальными устройствами, они содержат программируемые (на фиксированном языке программирования) устройства и обладают стойкостью к систематическим отказам SC 2 в соответствии с МЭК 61508. Эти датчики используются в приложениях с УПБ 3 (т. е. для реализации ФБ ПСБ S-1 и ФБ ПСБ S-2). Для учета систематических отказов для каждой ФБ ПСБ с УПБ 3 был реализован ряд методов:

- для ФБ ПСБ S-1 при выборе оборудования учитывались его рабочие характеристики в предшествующем использовании, в то время как в процессе проектирования для обеспечения уровня систематических ошибок ПО уровню, соответствующему приложению с УПБ 3, были использованы разнообразие (температура и давление) и диагностика (см. F.14.1);
- для ФБ ПСБ S-2 анализ предшествующего использования (см. примечание), анализ дерева отказов (см. рисунок F.7) и диагностика использовались для обеспечения уровня систематических ошибок ПО датчиков уровню, соответствующему приложению с УПБ 3.

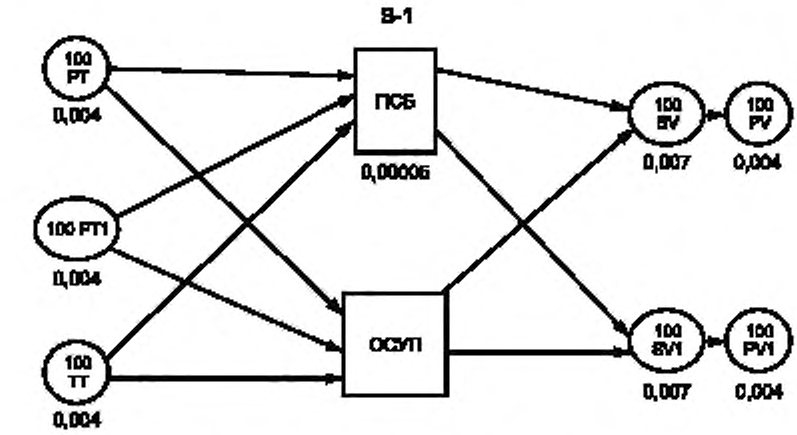
Примечание — На основе данных о предшествующем использовании команда предварительно оценила, что 2 % от всех отказов датчиков по общей причине были связаны со сбоями программного обеспечения. Дерево отказов, представленное на рисунке F.7, показывает, как в вычислениях $ВОН3_{ср}$ для ФБ ПСБ S-2 были учтены сбои программного обеспечения. Если доступных данных о предшествующем использовании было недостаточно, то альтернативным решением для пользователя будет связаться с производителем датчиков, чтобы получить гарантию того, что методы, использованные при разработке встроенного программного обеспечения, соответствовали руководящим указаниям, предоставленным в МЭК 61508 для программного обеспечения с УПБ 3.

Отказоустойчивость аппаратных средств (ОАС)

Для ФБ ПСБ S-1 и ФБ ПСБ S-2 отказоустойчивость для датчиков и клапанов была основана на требованиях МЭК 61511-1:2016, таблица 6 (УПБ 3).

Для ФБ ПСБ S-3 отказоустойчивость для датчиков и клапанов основана на требованиях МЭК 61511-1:2016, таблица 6 (УПБ 2).

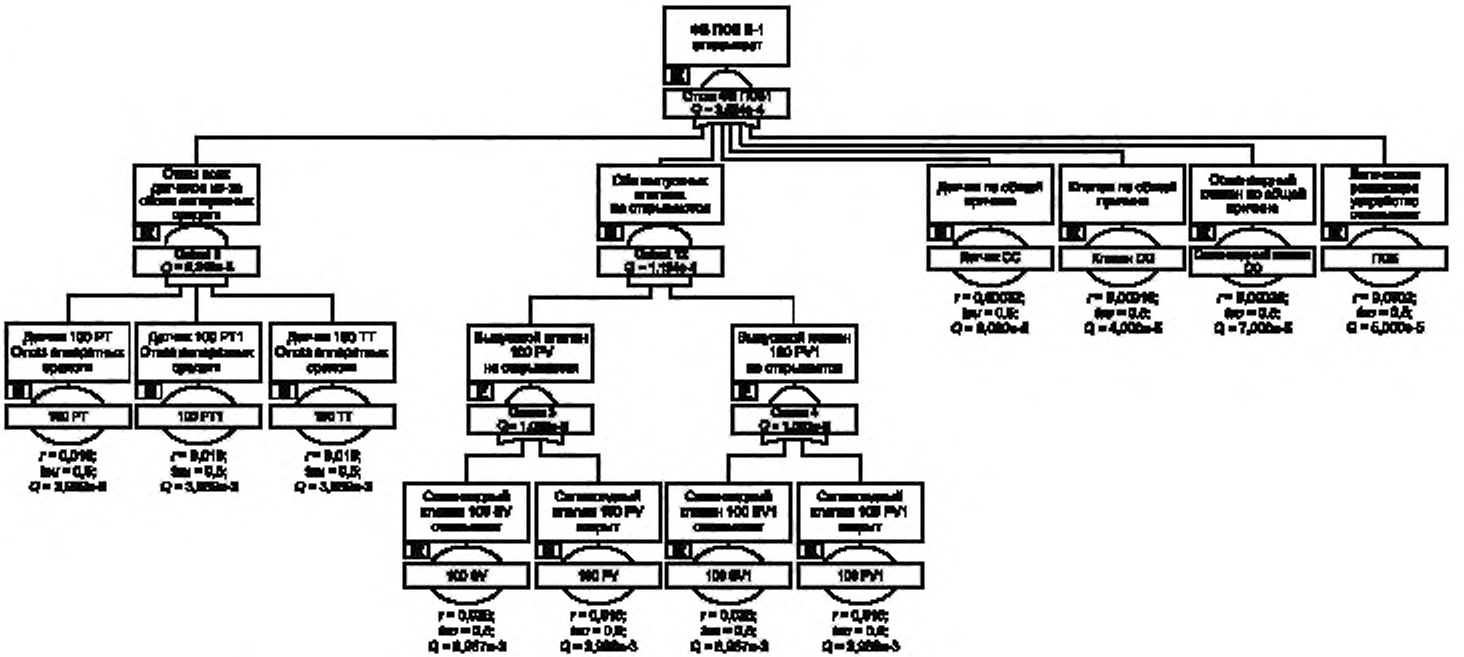
Логическое решающее устройство было спроектировано и прошло оценку третьей стороной в соответствии с требованиями МЭК 61508 (включая отказоустойчивость) для приложений с УПБ 3. Поэтому требования отказоустойчивости МЭК 61511 для ФБ ПСБ S-1, S-2 и S-3 выполнены.



Проект #	Ревизия #	Ревизия	ВНЗ	СНЗ	АРЗ	Лист	Проект ВУУУУ Начертил: Проверил: Одобрил: Отчет ХХХХХ1	Дата

Рисунок F.4 — Диаграмма состояний ФБ ПСБ S-1, на которой показаны $ВОНЗ_{ср}$ для каждого устройства ПСБ

На рисунке F.5 представлены вычисления для дерева отказов.



Проект #	Редакция #	Редакция	RVBD	CHKD	APPD	Дата	Проект # YYYY	Дата:
							Нарисовал:	
							Проверил:	
							Одобрил:	
							DWG# XXXXX1	

Обозначения

E — разрешающее событие,

Q — недоступность (ВОНЗ$_{cf}$);

r — интенсивность отказов (отказы в год)

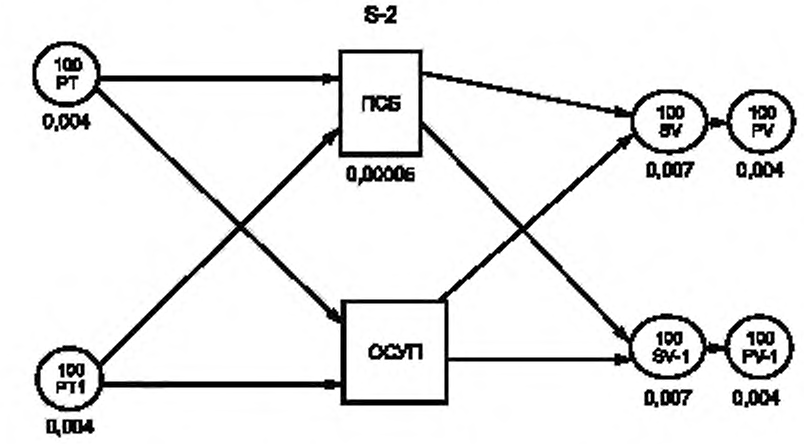
tau — интервал диагностической проверки (года).

Значение ВОНЗ$_{cf}$ для ФБ ПСБ S-1 округлено до 3.6e-4 и поэтому соответствует УПБ3

Рисунок F.5 — Дерево отказов S-1

ФБ ПСБ S-2

Если давление в реакторе превышает 125 фунт/кв. дюйм, то необходимо открыть выпускные клапаны 100PV и 100PV1. Требующийся УПБ = 3 (что предполагает $ВОНЗ_{ср}$ равную от 10^{-3} до 10^{-4}).

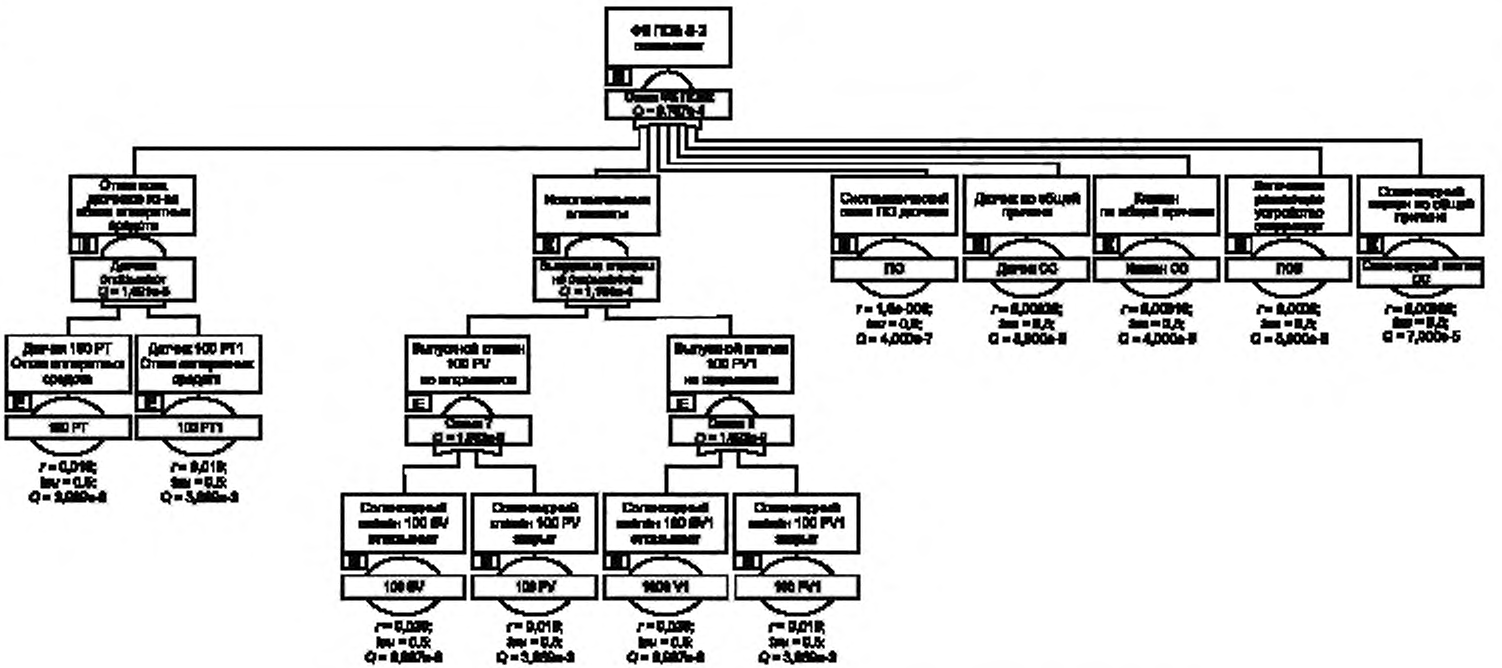


Проект #	Редакция #	Редакция	ВНЕС	СНКО	АРПО	Дата

Проект #/YYYY
Начертил:
Проверил:
Одобрил:
DWG#1000001
Дата:

Рисунок F.6 — Диаграмма состояний ФБ ПСБ S-2, на которой показаны $ВОНЗ_{ср}$ для каждого устройства ПСБ

На рисунке F.7 представлены вычисления для дерева отказов.



Проект #	Редакция #	Редакция	R/SD	CHKD	APPD	Дата

Проект # YYYY Дата:
Начертил:
Проверил:
Одобрил:
DWG# XXXXX1

Обозначения

E — разрешающее событие

Q — недоступность (ВОНЗ$_{ср}$);

r — интенсивность отказов (отказы в год)

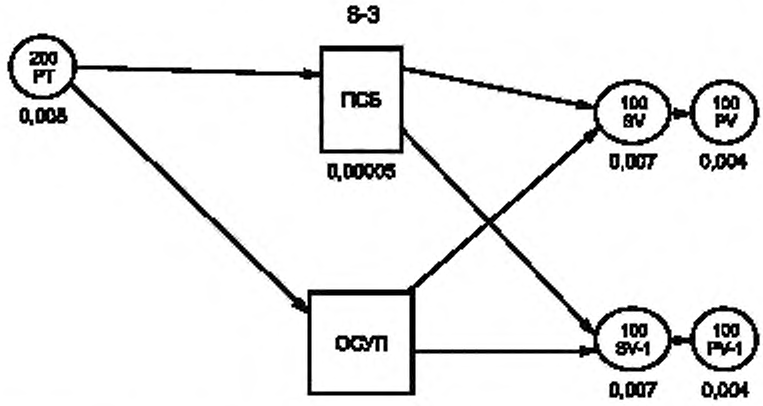
Iau — интервал диагностической проверки (года).

Значение ВОНЗ$_{ср}$ для ФБ ПСБ S-2 округлено до 3,8e-4 и поэтому соответствует УПБ3

Рисунок F.7 — Дерево отказов ФБ ПСБ S-2

ФБ ПСБ S-3

Если давление в предохранителе от утечки аппарата перемешивания выше чем 10 фунт/кв. дюйм, то необходимо открыть 100PV и 100PV-1. Требующийся УПБ = 2 (ВОНЗ$_{ср}$ равна от 10^{-2} до 10^{-3}).

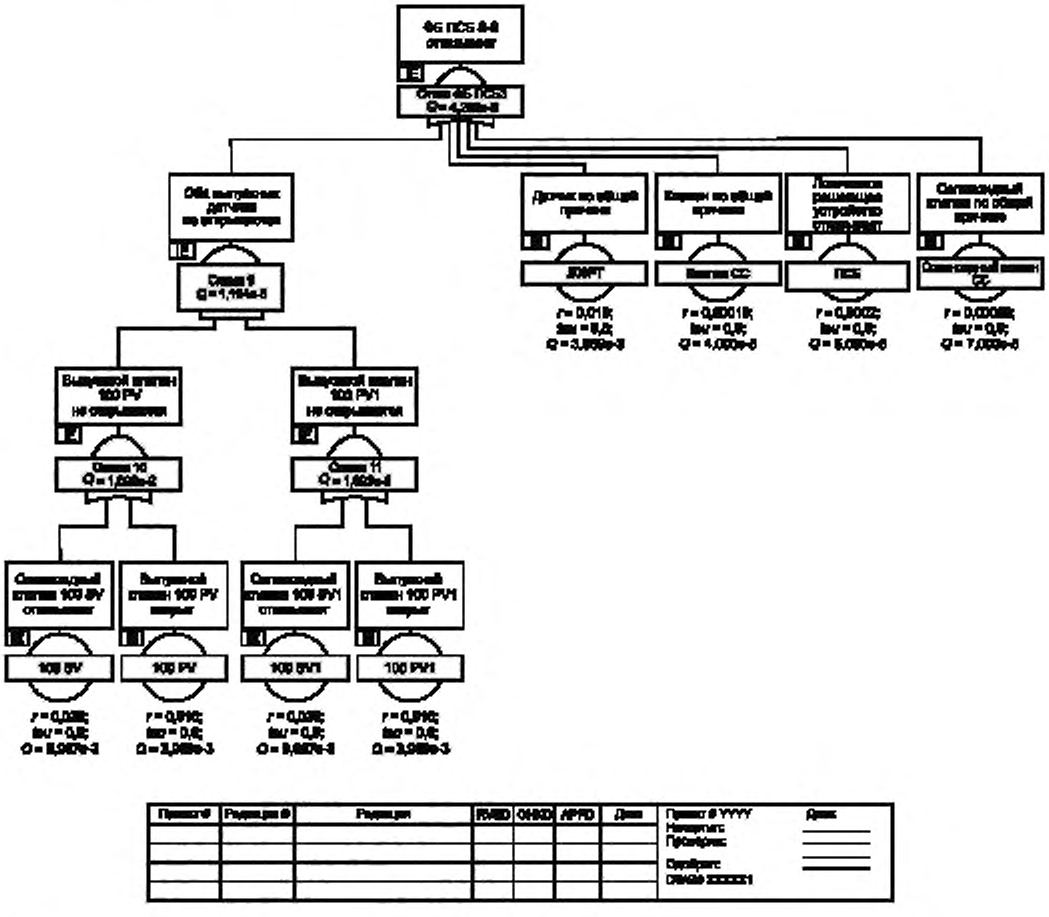


Проект #	Редакция #	Редакция	Внесл.	Спасл.	Апроб.	Дата

Проект #YYYY — Дата:
Начертил:
Проверил:
Одобрил:
DWG#XXXXX

Рисунок F.8 — Диаграмма состояний ФБ ПСБ S-3, на которой показаны ВОНЗ$_{ср}$ для каждого устройства ПСБ

На рисунке F.9 представлены вычисления для дерева отказов.



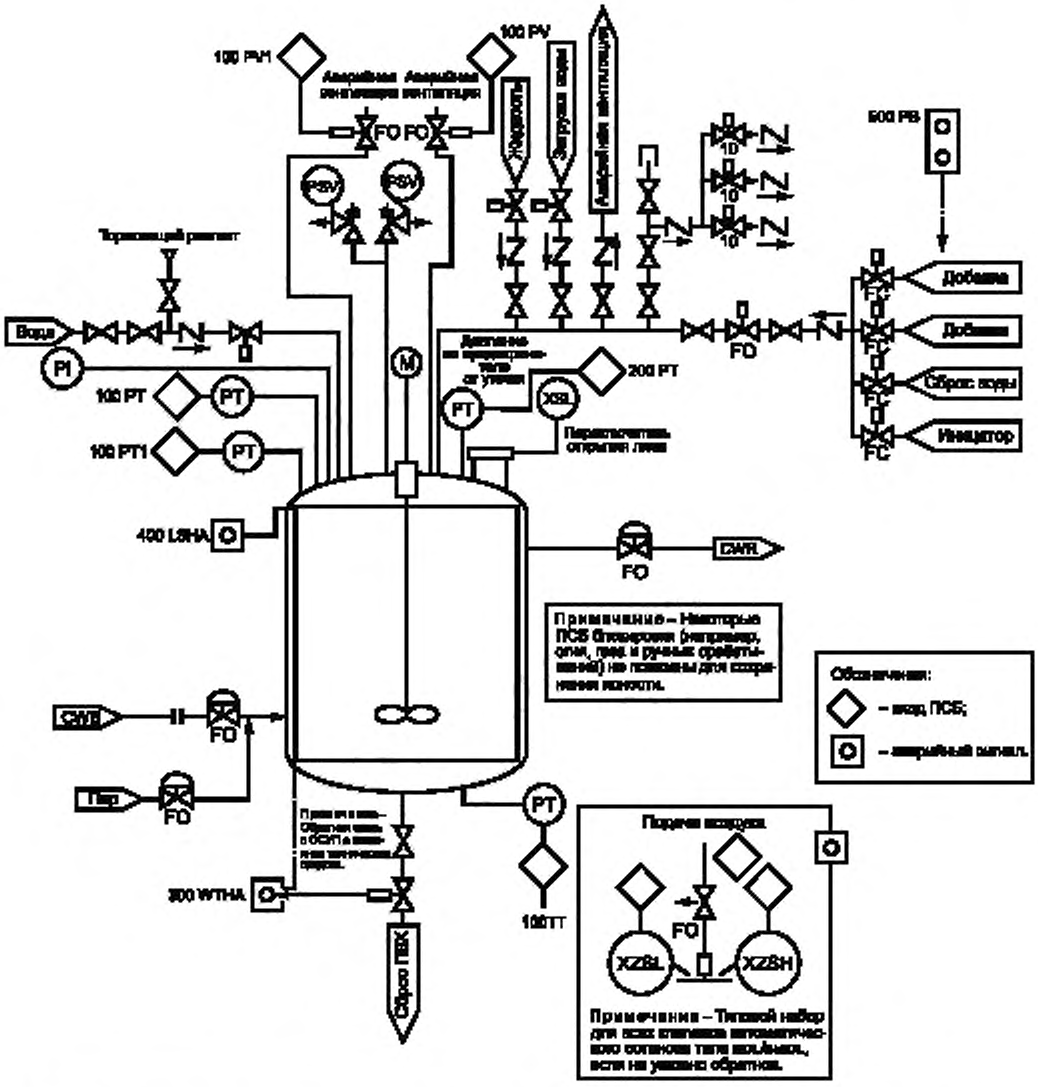
Обозначения.
E – разрешающее событие;
Q – недоступность (ВОНЗ$_{ср}$);
r – интенсивность отказов (отказы в год);
tau – интервал диагностической проверки (года).
Значение ВОНЗ$_{ср}$ для ФБ ПСБ S-3 округлено до 4,3e-3 и поэтому соответствует УПБ3.

Рисунок F.9 — Дерево отказов ФБ ПСБ S-3

F.16 Требования к прикладной программе

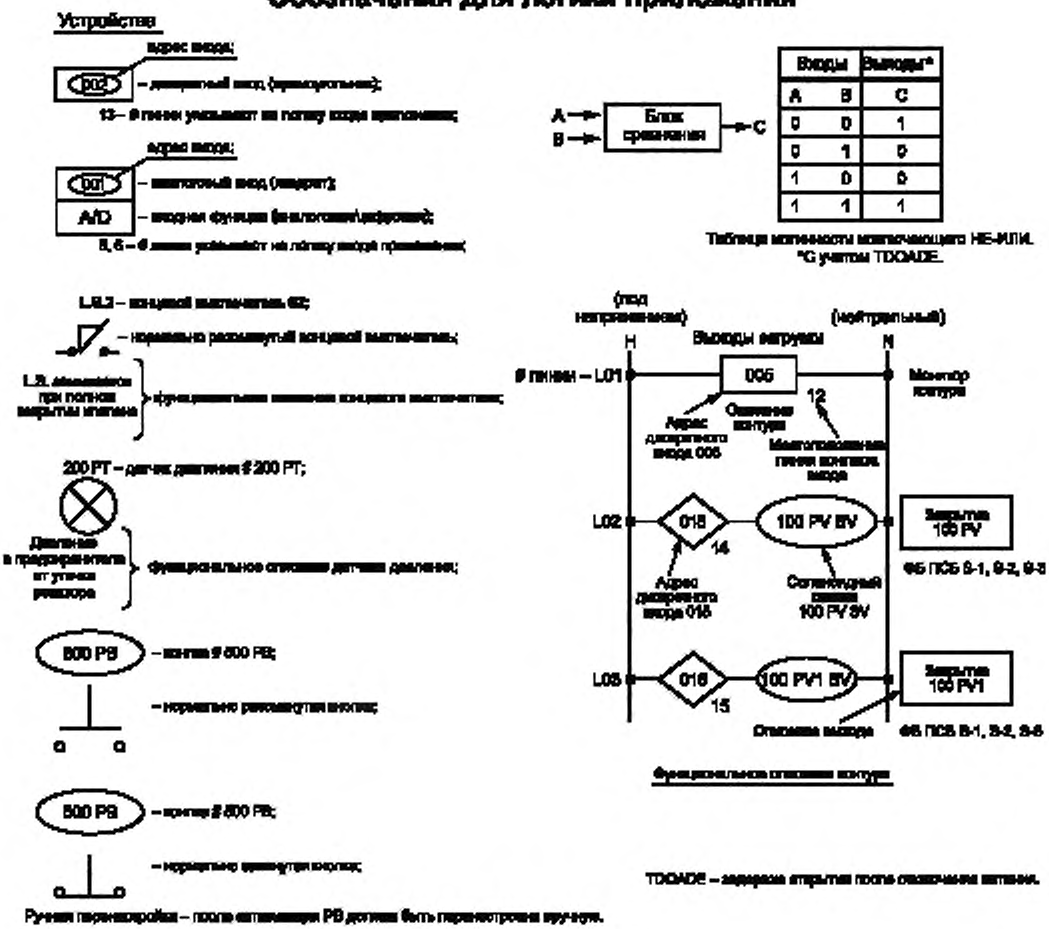
СТБ [в частности, описание логики (см. F.14.1], причинно-следственная диаграмма (см. таблицу F.14) и схема Т и КИП (см рисунок F.10) были использованы при разработке требований к ППО, как показано на ступенчатой диаграмме (см. рисунок F.11).

Ступенчатые диаграммы, отражающие функциональные требования для каждой ФБ ПСБ, показаны на рисунке F.11, листы 1—5. На ступенчатой диаграмме также показаны значения напряжения на линиях соединения, характеристики заземления, требования к замыкающим цепям и диагностика, предназначенная помочь проектировщику/программисту в разработке ППО.



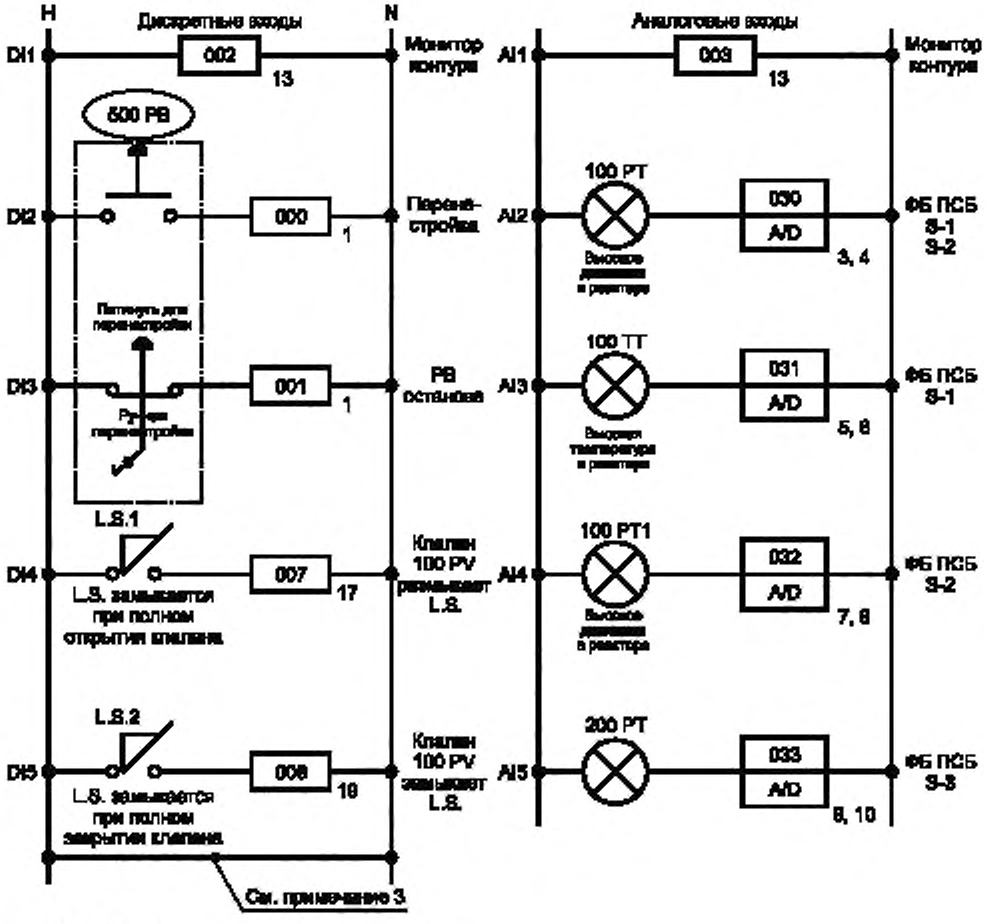
Проект #	Редакция #	Редакция	R/SD	CHKD	APPD	Дата	Проект # YYYY	Дата:
							Начертил:	
							Проверил:	
							Одобрил:	
							DWG# XXXXX1	

Рисунок F.10 — Схема Т и КИП для ФБ ПСБ модуля реактора ПВХ



Проект #	Редакция #	Редакция	RVBO	CHKD	APPD	Дата	Проект # YYYY	Дата:
							Начертил:	
							Проверил:	
							Одобрил:	
							DWG# XXXXX1	

Рисунок F.11 — Обозначения (1 из 5)

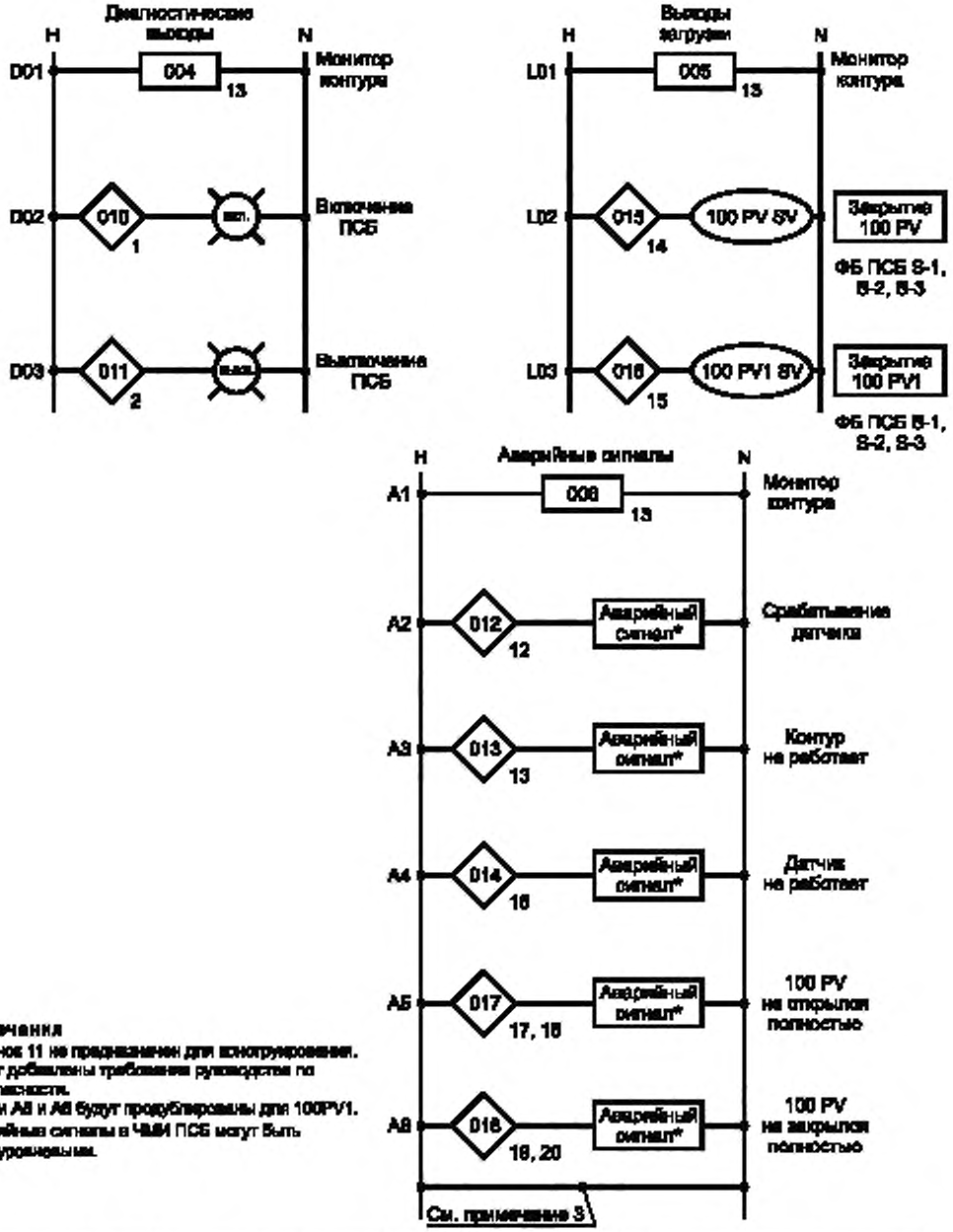


Примечания

1 Рисунок 11 не предназначен для конструирования.
2 Будут добавлены требования руководств по безопасности.
3 Линии DI4 и DI5 будут продублированы для 100PV1.

Проект #	Редакция #	Редакция	RVBD	CHKD	APPD	Дата	Проект # YYYY	Дата:
							Нарисовал:	
							Проверил:	
							Одобрил:	
							DWG# XXXXX1	

Рисунок F.11 — (2 из 5)



Примечания

1 Рисунок 11 не предназначен для конструирования.

2 Будут добавлены требования руководства по безопасности.

3 Линии A5 и A6 будут продублированы для 100PV1.

* Аварийные сигналы в ЧМИ ПСБ могут быть маркированными.

Проект #	Редакция Ф	Редакция	RVSD	CHKD	APPD	Дата

Проект # YYYY Дата:

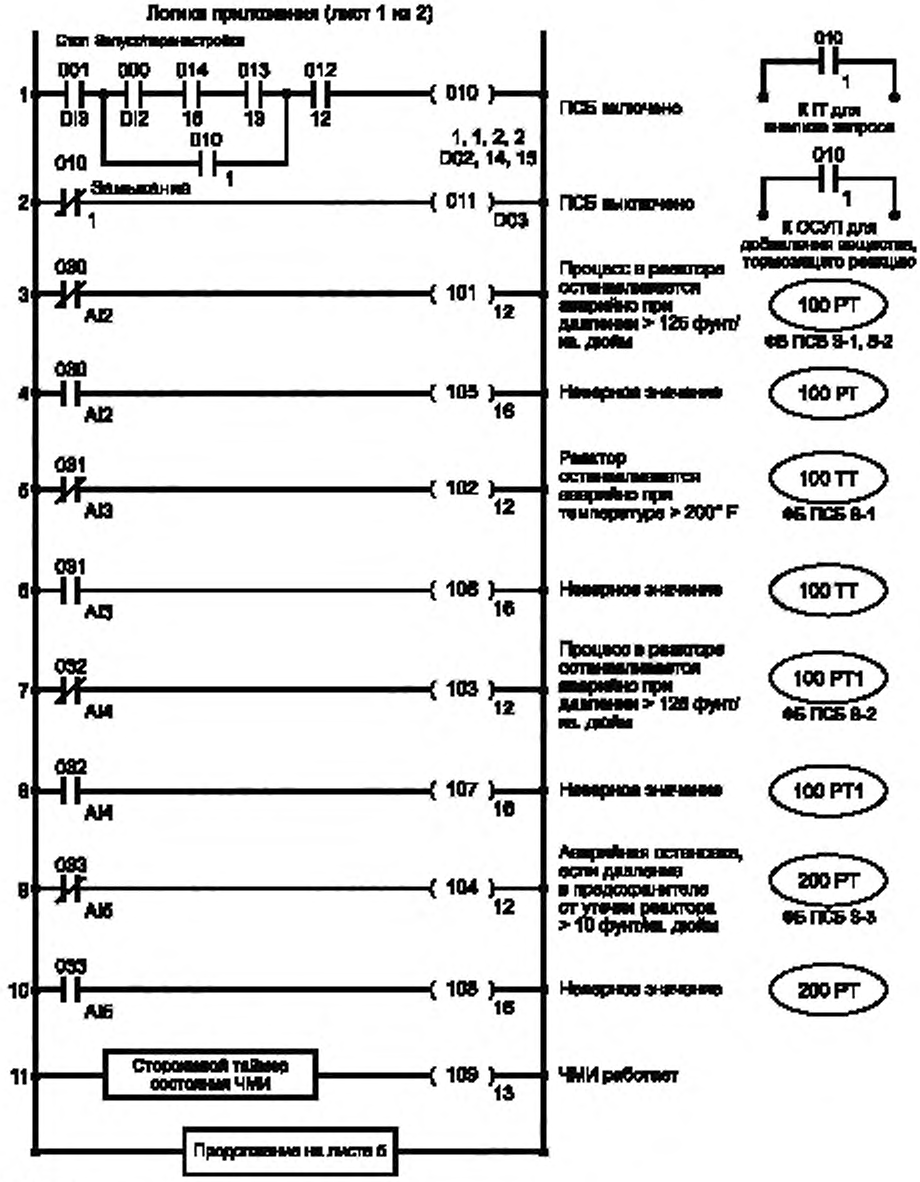
Начертил:

Проверил:

Одобрил:

DWG#XXXXX1

Рисунок F.11 — (3 из 5)



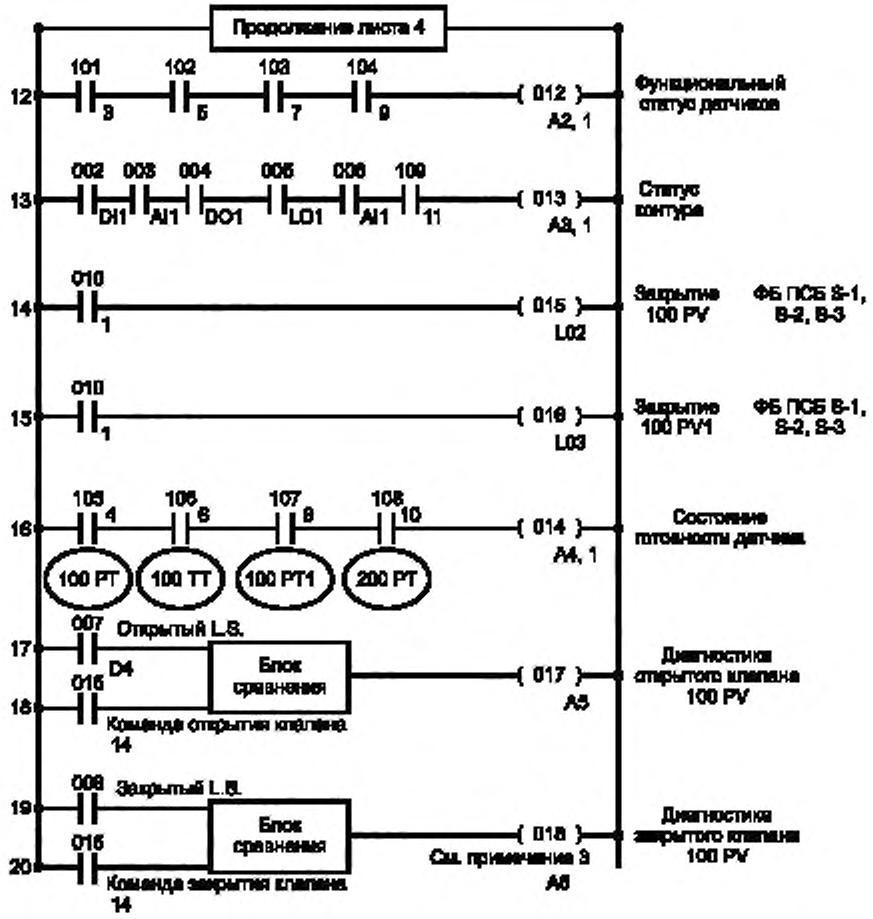
Примечания
1 Рисунок 11 не предназначен для конструирования.
2 Будут добавлены требования руководства по безопасности.

Проект #	Редакция #	Редакция	RVBD	CHKD	APPD	Дата

Проект # YYYY Дата:
Начертил:
Проверил:
Одобрил:
DWG# XXXXX1

Рисунок F.11 — (4 из 6)

Логика приложения (лист 2 из 2)



Примечания

1 Рисунок 11 не предназначен для конструирования.

2 Будут добавлены требования руководства по безопасности.

3 Линии 17, 18, 19 и 20 будут продублированы для 100 PV1.

Проект #	Редакция #	Редакция	RVSD	CHKD	APPD	Дата	Проект # YYYY	Дата:
							Начертил:	
							Проверил:	
							Одобрил:	
							DWG# XXXXX1	

Рисунок F.11 — (5 из 5)

F.17 Шаг F.4. Жизненный цикл ПСБ

Таблица F.16 — Жизненный цикл ПСБ. Блок 4

Стадия или деятельность жизненного цикла системы безопасности		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок 7, блок 4	Проектирование и разработка ПСБ	Спроектировать ПСБ, отвечающую требованиям к ФБ ПСБ и к полноте безопасности	11 и 12.4	Требования к безопасности ПСБ. Требования к безопасности ППО	Проект ПСБ, отвечающий требованиям к безопасности ПСБ. Планирование испытания интеграции ПСБ

В таблице F.16 предоставлены цели, входы, выходы и ссылка на связанные с ними разделы и подразделы для проектирования и разработки ПСБ.

F.18 Технология и выбор устройств

F.18.1 Общие положения

В настоящем разделе перечислены некоторые из ключевых параметров, применяемых в данном примере при выборе технологий и устройств:

a) группа анализа опасности процесса объекта одобряет все устройства, использованные в процессе эксплуатации ПСБ;

b) устройства низкой сложности, с которыми на объекте ознакомлены;

c) стойкость к систематическим отказам, подтвержденная документально оформленными источниками;

d) философия технического обслуживания и тестирования, согласующаяся со способностями/опытом персонала на объекте;

e) интерфейс оператора/технического обслуживания, основанные на существующих критериях объекта;

f) оценка стоимости и календарный план выполнения проекта с расчетом времени;

g) использование ОСУП для разнообразия ППО (дублирование);

h) все выбранные технологии прежде использовались на объекте (т. е. предшествующее использование), и обслуживающий персонал объекта обладает четким пониманием их функционирования;

i) режимы отказов и интенсивности отказов каждого компонента оборудования (включая источник данных) документально подтверждаются;

j) устойчивость к электромагнитным помехам на промышленном объекте;

k) защита от вибрации (например, вибрации, приводящей к раскреплению монтажных схем, отказы проводных соединений и устройств), предоставляемая с каждым компонентом оборудования.

F.18.2 Логическое решающее устройство

Параметры логического решающего устройства включают:

a) применение каждого перечисления из F.18.1;

b) логическое решающее устройство ПСБ оценивается в соответствии с МЭК 61508 и обладает стойкостью к систематическим отказам SC 3. Для прикладного программирования оно использует язык с ограниченной изменчивостью (т. е. линейно-лестничную логику);

c) расположение всех устройств логического решающего устройства в операторской производственного здания;

d) время безопасности процесса для всех ФБ ПСБ должно быть достаточно большим, чтобы адекватно соответствовать типичным временам реакции PLC;

e) опыт эксплуатации и обслуживания на объекте (т е. предшествующее использование) учитывался при выборе логического решающего устройства;

f) надлежащую интеграцию с ОСУП.

F.18.3 Датчики

Были использованы датчики вместо дискретных переключателей (за исключением переключателей положений клапанов) там, где использовались бесконтактные переключатели (чтобы воспользоваться преимуществами свойств бесконтактных устройств).

Датчики были дополнены диагностикой значений, выходящих из диапазона, и неверных значений в логических решающих устройствах ПСБ и ОСУП.

Данные по интенсивности отказов датчика были основаны на стойкости к систематическим отказам, которые были предоставлены в результате выполнения оценки по МЭК 61508 или данными о соответствии МЭК 61508, и было принято решение об использовании передового опыта по их установке.

Для каждого датчика были предоставлены отдельные переходники для крепления.

Применяемые датчики являются программируемыми (интеллектуальными) устройствами, обладающими следующими особенностями:

a) диагностика, удаленный доступ к информации по калибровке и описание свойств встроенных устройств более надежно обеспечивают, что соответствующее устройство установлено и правильно работает;

b) средства защиты (например, защита от записи, пароли, ключевые слова), ограничивающие доступ к настройке калибровки, которая может привести к непредвиденным изменениям, делающим устройство неспособным выполнять его функцию безопасности;

c) надлежащее время обновления датчика (т. е. задержка по времени между изменением в процессе и выходной реакцией датчика является допустимой);

d) там, где это целесообразно, датчики дополняются дренажными системам, вентиляцией и возможностью соединения с измерительной схемой;

e) выходы датчика (4—20 мА) непосредственно соединены с ПСБ и параллельно подключены к ОСУП.

F.18.4 Исполнительные элементы

Задействованные исполнительные устройства управления являются соленоидными клапанами и аварийными выпускными клапанами. Исполнительные устройства управления выполняют останов по отключению питания и переходят в свои безопасные состояния при прекращении подачи воздуха или электропитания (т. е. аварийные выпускные клапаны не открываются).

Исполнительные устройства управления были выбраны на основании опыта предшествующего использования.

F.18.5 Соленоидные клапаны

Соленоиды определяются с учетом следующего:

a) высокотемпературные формованные катушки класса H или F, предназначенные обеспечить более долгий срок службы в условиях непрерывной подачи питания (это типично для приложений с остановом при отключении питания);

b) высокая и низкая предельные температуры эксплуатации соленоида соответствуют или превышают условия среды, в которой он будет установлен;

c) пропускная способность выходного потока в вентиляцию через клапан, управляемый оператором, определяется так, чтобы она удовлетворяла требованиям временных спецификаций приложения (время реакции клапана меньше 10 сек является достаточным);

d) рейтинг выключения выходов логического решающего устройства достаточно низок, чтобы гарантировать то, что соленоидный клапан выпадет (будет опущен) в случае, когда выходы переходят в режим «выключено».

Среднее время до опасного отказа (*MTTFd*) для соленоидных клапанов было определено с помощью:

1) информации о предшествующем использовании, полученной из реального опыта эксплуатации (внутреннего и внешнего), а также из данных, предоставленных изготовителем;

2) информации о предшествующем использовании, указывающая на то, что в течение 140 лет использования в похожих приложениях случилось два опасных отказа соленоидных клапанов (клапан не позволял осуществлять выпуск/вентиляцию). Основываясь на этом, нижний доверительный предел *MTTFd* в 70 % (см. МЭК 61511-1:2016, примечания к пунктам 11.9.3 и 11.9.4 и TR84.00.04-1, TR84.00.09) был вычислен как 38,7 года. Для вычислений $ВОНЗ_{ср}$ было выбрано *MMTFd* в 35 лет.

F.18.6 Аварийные выпускные клапаны

Согласно спецификациям аварийные выпускные клапаны должны обеспечивать действие выпускных клапанов в случае утраты их работоспособности, а также когда рабочие сигналы не соответствуют требованиям функциональной безопасности. Основываясь на этом и оценивании группой анализа опасности процесса требований к любым другим действиям при отказах, было установлено, что аварийные выпускные клапаны открываются в случае:

a) потери питания;

b) потери подачи воздуха;

c) сигнала открытия, полученного соленоидным клапаном от логического решающего устройства ПСБ или логического решающего устройства ОСУП.

Кроме того, аварийные выпускные клапаны обладают следующими функциями:

1) предоставляется визуальная индикация фактического положения клапанов, включая:

- местную индикацию посредством индикатора позиции штока клапана;
- удаленную индикацию позиции клапана посредством концевых выключателей;

2) задействованы исполнительные механизмы с пружинным возвратом. Рассуждения о выборе размера этих механизмов и проектировании отказоустойчивой пружины включают в себя надлежащий анализ максимального требующегося давления отключения.

Примечание — В данном применении были задействованы запорные клапаны с протеканием под кнопкой клапана.

Контроль каждого клапана включает сравнение сигнала клапана с позицией клапана, сопровождаемого аварийным сигналом.

F.18.7 Модулирующие клапаны

Модулирующие клапаны не потребовались для ПСБ, рассмотренной в данном примере.

F.18.8 Клапаны байпаса

Анализ группы анализа опасности процесса определил, что клапаны байпаса не были необходимы, так как это пакетный режим работы, предоставляющий несколько возможностей автономного технического обслуживания. Это было согласовано с отделами эксплуатации и технического обслуживания, и они одобрили этот подход.

F.18.9 Человеко-машинные интерфейсы

F.18.9.1 Общие положения

Возможности интерфейса логического решающего устройства были спроектированы для связи с ОСУП с помощью функционально безопасного интерфейса для дублирования интерфейса оператора, аварийных сигналов, диагностики и взаимного обмена определенными значениями.

Следующие пункты были реализованы в интерфейсах ПСБ для связи с ОСУП:

- использование резервной панели ЧМИ;
- использование резервных коммуникационных каналов;
- использование сторожевого таймера внутриобъектных коммуникаций для интерфейсов, обрабатывающих критически важные данные (например, все данные, поступающие на операторскую панель ОСУП);
- кнопка останова (500PB) была установлена на одну из панелей ЧМИ и оснащена пластиковым покрытием безопасности, чтобы избежать непреднамеренных остановов.

Факторы, которые учитываются при проектировании интерфейса оператора, включают:

- требования к управлению аварийными сигналами;
- требования к реакции оператора;
- хорошую эргономику.

Изменения ППО (включая настройки срабатывания) ПСБ могут быть внесены только через инженерные панели ПСБ и при соблюдении надлежащих мер безопасности (см. раздел F.22).

F.18.9.2 Управление аварийными сигналами

Управление аварийными сигналами гарантирует, что проблемы и опасности предоставляются оператору таким образом, чтобы он мог своевременно и легко идентифицировать и понять их, используя заданный для этих аварийных сигналов приоритет, который отражает философию управления аварийными сигналами на объекте. Реализованные функции включают:

- аварийные сигналы, связанные с уровнями защиты, для которых значение снижения риска получено в результате АУЗ, имеют наиболее высокий приоритет. Эти аварийные сигналы (300WTHA и 400LSHA) должны проверяться с такой же частотой (два раза в год), как и ПСБ;
- аварийные сигналы перед срабатыванием, инициирующие действие оператора до действия ПСБ, имеют наиболее высокий приоритет;
- используются функции интерфейса оператора ОСУП, чтобы различать аварийные сигналы разных уровней приоритетов;
- используются аварийные сигналы перед срабатыванием и при срабатывании, чтобы помочь определить требования к реакции оператора;
- аварийные сигналы диагностики ПСБ отображаются на отдельном графическом устройстве ЧМИ.

F.18.9.3 Реакция оператора

Способность оператора реагировать на аварийные сигналы, инициированные ЧМИ, требует следующего:

- использование записи последовательности событий (SOE): при нормальном сканировании ОСУП обеспечивает правильную обработку аварийных сигналов «в порядке поступления»;
- использование аварийных сигналов, предшествующих срабатыванию: оператор может прибегнуть к корректирующему действию, перед тем как произойдет срабатывание (например, добавить тормозящий реагент, чтобы предотвратить выход реакции из-под контроля). В таких случаях предусматриваются аварийные сигналы, предшествующие срабатыванию. Аварийные сигналы, предшествующие срабатыванию и настройки срабатывания учитывают динамику процесса и реакцию датчиков.

F.18.9.4 Человеческие факторы

Человеческие факторы относятся к параметрам проектирования интерфейса, которые могут сказаться на способности оператора эффективно идентифицировать и отвечать на аварийные сигналы и информацию о состоянии объекта. В проекте реализовано:

- согласованное использование цветов, лампочек, типов, форм и размеров переключателей, размещение переключателей и т. д.;
- использование предохранительного колпачка на переключателе останова оператора (500PB), чтобы понизить вероятность случайного включения;
- переключатель останова с механическим воздействием оператора (потянуть, чтобы сбросить).

F.18.10 Разделение

F.18.10.1 Общие положения

Настоящий подраздел описывает разделение, присущее проекту каждой ФБ ПСБ.

Разделение выполняется, чтобы сократить число сбоев по общей причине и облегчить работу с проблемами защиты, которые могут возникнуть из-за непредвиденных изменений. Эти типы проблем могут сделать ПСБ

и ОСУП одновременно недоступными. Чтобы рассмотреть эти проблемы, реализуется подход к проектированию, согласующийся с обучением на объекте и опытом успешного использования.

F.18.10.2 Источники питания

Разделение контуров питания входов-выходов ПСБ от контуров питания, не связанных с ПСБ, должно реализовываться с помощью отдельного распределительного трансформатора для группового электрощита питания приборов ПСБ. Это обеспечивает защиту от сбоев по общей причине, связанных с проблемами заземления. Распределение источников питания ПСБ далее разделяется, чтобы обеспечить резервные источники питания [т. е. нормальный и бесперебойный источник питания (ИБП)] отдельной физической разводкой и распределительную сеть питания для входов, логических решающих устройств, источника(ов) питания входов-выходов, нагрузок на выходах и диагностики выходных схем.

Потребность в раздельных системах кабельных каналов (например, изоляционные трубы, кабельные короба, защитные кожухи и желоба для прокладки кабеля) отсутствует, так как проблемы электромагнитной совместимости (ЭМС) рассматриваются на постоянной основе при использовании хороших инженерных практик, чтобы достичь:

- максимальных уровней энергии приложения (480 V и ниже);
- спецификаций и размещения кабелей/кабельных каналов/оборудования;
- разделения проводников подачи питания и сигналов приборов (т. е. 4—20 мА) по разным кабелям;
- уникальной идентификации (т. е. цветного кодирования) оборудования ПСБ;
- охвата точек соединения терминальных устройств ПСБ;
- автоматизированного монтажа кабелей, позволяющего идентифицировать каждый проводник, кабель, систему кабельных каналов и точку соединения.

F.19 Отказы по общей причине и систематические отказы

F.19.1 Общие положения

В следующих подразделах (F.19.2—F.19.19) определено, как при проектировании учитываются отказы по общей причине и систематические отказы.

Методики проектирования, реализованные для предотвращения отказов по общей причине, включают разделение, разнообразие и экспертную оценку.

Методики, применяемые для предотвращения систематических ошибок, включают экспертную оценку, использование подходов к проектированию при наличии хорошего опыта предшествующего использования, разнообразия и диагностик сравнения.

F.19.2 Разнообразие

Разнообразие было достигнуто при помощи разного оборудования (логических решающих устройств ПСБ и ОСУП), различных проектных решений для выполнения общей функции (дублирование ППО ПСБ и ОСУП), различного встроенного ППО и разных программистов.

F.19.3 Ошибки спецификации

Ошибки спецификации [например, неверный диапазон температур окружающей среды, некорректный параметр (например, 0 °С когда предполагается 0 °F), ненадлежащее качество металла для группы контрольно-измерительных приборов] были идентифицированы и скорректированы при помощи экспертной оценки персоналом, ознакомленным с оцениваемой проблемой.

F.19.4 Ошибки проектирования аппаратных средств

Ошибки проекта аппаратных средств были рассмотрены в процессе использования оборудования ПСБ, которое соответствует критериям предшествующего использования при поддержке либо результатами выполнения оценки соответствия с МЭК 61508, либо данными о соответствии МЭК 61508, либо результатами анализа на объекте. Проектирование следует лучшим корпоративным практикам, руководству по безопасности для каждого сертифицированного устройства и руководству по применению для несертифицированного устройства, а также включенной экспертной оценке.

F.19.5 Ошибки проектирования программного обеспечения

ПЭ-оборудование было выбрано для использования, основываясь на предшествующем использовании и либо на результатах выполнения оценки соответствия с МЭК 61508, либо на данных о соответствии МЭК 61508. ППО было задействовано в ОСУП для «дублирования» ППО ПСБ, используя тем самым преимущества разнообразия встроенного программного обеспечения.

Чтобы сократить число систематических отказов, связанных со сбоями встроенного ПО, как в ПСБ, так и в ОСУП были реализованы выполнение сравнения двух датчиков давления и проверка их нижних и верхних предельных значений.

Управление систематическими ошибками ППО стало возможно при реализации нескольких перечисленных методов и мер, включая:

- язык с ограниченной изменчивостью для программирования всех прикладных программ, если недоступно программирование на языке с фиксированной изменчивостью (например, для датчиков, основанных на ПЭ, панели оператора, основанной на ПЭ);
- документально оформленную схему логики (см. рисунок F.11), которую может интерпретировать весь вовлеченный персонал, что обеспечивает не требующую объяснений, связанную с процессом документацию, включенную в документацию на ППО;

- оценки экспертов и средства моделирования, используемые для сокращения числа ошибок проектирования ППО;
- «дублирование» для непрерывного контроля рабочих параметров ППО и реализации разнообразия в программировании;
- требования производителя к руководству по безопасности.

F.19.6 Нагрузки окружающей среды, превышающие допустимые

При проектировании производственного помещения не учитывалось влияние землетрясения или падения самолетов, но оно было рассчитано выстоять при урагане пятого уровня. Рассмотренные условия окружающей среды, которым будет подвергаться ПСБ, включают:

- температуру;
- влажность;
- источники загрязнения;
- вибрацию;
- заземление;
- согласование линий питания;
- электромагнитную совместимость (ЭМС).

F.19.7 Температура

Экстремальная температура неблагоприятно влияет на устройства ПСБ, такие как логические решающие устройства, модули входов-выходов, датчики и исполнительные элементы. Проектные решения, связанные с влиянием температуры, реализованные в данном проекте, включают:

- рабочие температуры, указанные производителями;
- размещение оборудования в областях, где отклонения температуры удерживаются в рамках спецификаций производителя;
- защиту от погодных условий и контроль температуры для оборудования, установленного вне помещения;
- применение каплеотводных трубок или дренажа, или сушка воздухом системы КИП для снижения вероятности возникновения отказов, связанных с ледообразованием, должны быть реализованы надлежащим образом;
- сопроводительный обогрев там, где он требуется.

F.19.8 Влажность

Относительная влажность должна поддерживаться в соответствии с требованиями производителей (как правило, ниже 90 % для электронных систем). Чтобы снизить вредное влияние повышенной влажности (например, пар, открытый воздух), электронные блоки должны быть защищены конформным покрытием и их контакты должны быть обработаны водоотталкивающей смазкой, чтобы обеспечить газонепроницаемое соединение.

F.19.9 Источники загрязнения

Чтобы обеспечить защиту от возможного загрязнения, следует обеспечить следующее:

- надлежащую вентиляцию и защиту от пыли в ближайшем окружении;
- для оборудования, находящегося в агрессивной атмосфере, устанавливаются фильтры или применяются адсорбенты для систем HVAC (отопление, вентиляция, кондиционирование воздуха), а для всего остального оборудования реализуется продувка воздухом;
- для электронных устройств, установленный открыто на оборудовании, применяются вентилируемые шкафы и/или конформное покрытие и какой-нибудь метод защиты контактов в соединениях.

F.19.10 Вибрация

В здании присутствует некоторый уровень вибрации. Чтобы справиться с этой проблемой, все подключаемые устройства ПСБ (например, реле в системах подготовки «кубиков льда», панели входов-выходов) предоставляются вместе с жесткими блокировочными механизмами. Шкаф логического решающего устройства ПСБ использует виброизоляционные опоры, чтобы минимизировать передачу вибрации от шкафа на логическое решающее устройство.

F.19.11 Заземление

Заземление было спроектировано так, чтобы облегчить использование технологии программируемых электронных устройств посредством реализации:

- сопротивления системы заземления ниже 5 Ом;
- заземлений системы Уфера;
- электрически непрерывной стальной шины в здании;
- добавления к стальной шине в здании конической зоны молниезащиты с медными проводниками там, где они нужны.

F.19.12 Согласование линий питания

Согласование линий питания проектируется для обеспечения защиты ПСБ от сбоев в шинах питания, таких как отключение питания, грозовая помеха, падение напряжения, мгновенное падение напряжения, частичное нарушение энергоснабжения, бросок напряжения и импульсное повышение напряжения сети с большой амплитудой.

Защита от грозовой помехи обеспечивается реализацией защитных устройств, которые:

- скоординированы так, чтобы они могли противостоять способности (короткое замыкание, перегрузка) устройств быть защищенными;
- размещены для защиты каждого устройства ПСБ так же, как и конической зоны молниезащиты.

Существующая система распределения питания обладает некоторым гармоническим спектром. Система распределения питания ПСБ была спроектирована для защиты от гармоник.

Защита от перегрузки и короткого замыкания в ПСБ предоставляется вместе со следующими свойствами:

- отдельные предохранители для каждой схемы входа-выхода, чтобы ограничить последствия сбоя в этой схеме;
- согласование предохранителя на ответвлении схемы с предохранителем всей схемы, чтобы минимизировать вероятность отключения большой части структуры входов-выходов из-за сбоя низкого уровня.

F.19.13 Электромагнитная совместимость

Электронные и программируемые электронные системы используют сигналы низкого уровня, цифровые схемы, микропроцессоры, чипы памяти и т. п., на которые могут оказывать влияние электрические помехи, например электромагнитные помехи (ЭМП). ЭМП, генерируемые персональными коммуникационными системами, такими как переносные радиостанции, радиоприемники базовой станции, сотовые телефоны, персональные компьютеры, беспроводные модемы и частотно-регулируемые электроприводы, были оценены во время проектирования. ПСБ было спроектирована с учетом этих проблем за счет реализации следующего:

a) электротехнических шкафов, предоставляющих защиту ПСБ от внешних (за пределами шкафа) источников шума;

b) проекта кабельного канала и прокладки кабелей, обеспечивающего защиту ПСБ от внутренних (внутри шкафа) источников шума;

c) установки шумовых фильтров, где это требовалось.

Дополнительные методы ослабления ЭМП включают:

1) металлические электротехнические шкафы;
2) металлические барьеры;
3) экранирование кабелей и проводов;
4) монтаж витой парой;
5) надлежащее заземление;
6) надлежащее размещение устройства;
7) разводку соединений как можно дальше от источника ЭМП;
8) разнесение.

В соответствии с критериями выбора оборудования ПСБ требовалось, чтобы это оборудование было способно выдержать уровни ЭМП, которые обычно существуют в промышленной среде. Это было достигнуто за счет:

- спецификации оборудования, которое было спроектировано, построено и испытано в соответствии с применяемыми стандартами (например, МЭК 61131, TUV);
- установки оборудования в соответствии с руководствами по установке производителей.

F.19.14 Источники средств обеспечения

Электричество и сжатый воздух являются ключевыми средствами, обеспечивающими ПСБ. Содержание и качество их проектирования непосредственно связано с их готовностью обслуживать ПСБ. Независимо от проекта во время анализа опасности процесса предполагалось, что часть или все эти средства обеспечения недоступны.

Электроэнергетические компании и персонал объекта (например, связанный с силовой станцией, другими рабочими процессами) послужили консультантами в определении доступности существующих источников средств обеспечения. Основываясь на сделанных выводах, были спроектированы источники средств обеспечения, обладающие свойствами, предназначенными для улучшения их доступности (готовность), включая:

- сжатый воздух:
  - используется чистый, сухой качественный сжатый воздух;
  - исполнительным устройствам управления была предоставлена достаточная пневматическая энергия, чтобы обеспечить адекватное время работы при управлении исполнительными устройствами;
  - пневматическая энергия предоставлена с защитой от засорения, грязи, насекомых и заморозков;
  - длина и диаметр каналов передачи пневматической энергии и сигналов предназначены обеспечить удовлетворительные рабочие характеристики;
- электричество:
  - для логического решающего устройства ПСБ, входов, ЧМИ и диагностических выходов используется резервный источник питания;
  - для нагрузок двигателя предоставлена защита от низкого напряжения с задержкой по времени (30 циклов);
  - альтернативный источник питания обладает таким же качеством электроэнергии, как и основной;
  - альтернативные источники питания (например, ИБП) размещены так, чтобы каждый мог технически обслуживаться, не оказывая негативного влияния на функционирование других;

- в проект ПСБ была включена система, разрешающего пуска, которая требует готовности всех электрических цепей ПСБ.

F.19.15 Датчики

Чтобы минимизировать отказы по общей причине, для каждого датчика используется отдельный переходник для крепления.

F.19.16 Коррозия или биологическое обрастание, связанные с процессом

Рассматриваемый процесс обладает ограниченными возможностями для нарушения нормальных условий процесса, которые приводят к коррозии. Он также является процессом пакетной обработки, что облегчает реализацию требования очистить корпус реактора между циклами процесса. Никаких специальных требований к проекту реализовано не было.

F.19.17 Техническое обслуживание

Организация, занимающаяся техническим обслуживанием, участвовала в планировании, верификации и одобрении проекта. Особое внимание было уделено проекту, так как он связан с калибровкой, требованиями к обучению, применению байпасов и испытаниям.

F.19.18 Уязвимости неправильных действий

Эксплуатирующая организация участвовала в планировании, верификации и одобрении проекта. Особое внимание было уделено тому, как в результате проектирования были получены: упрощенные процедуры эксплуатации, требования к минимизации вмешательства оператора в производство, надлежащие режимы работы, обеспечивающие возможность прекращения обработки партии на ключевых интервалах, результаты тестирования ППО, гарантирующие обеспечение соответствия потребностям процесса, а также подтверждения того, что решение проблем управления аварийными сигналами/ЧМИ было удовлетворительным.

F.19.19 Архитектура ПСБ

В данном пункте рассматривается архитектура ПСБ. На рисунке F.12 предоставлена архитектура ПСБ. Цель данного пункта заключается в том, чтобы проиллюстрировать архитектуру ПСБ и ее связи с внешними устройствами (например, с ОСУП, ЧМИ, датчиками и исполнительными элементами процесса).

ОСУП взаимодействует с ПСБ через магистраль передачи данных. Тем не менее требования к защите требуют того, чтобы изменения уставок ПСБ и изменения конфигурации ПСБ могли выполняться только через предназначенный для этого инженерный пульт ПСБ. Инженерный пульт ПСБ должен непосредственно подсоединяться к ПСБ из аппаратной управления каждый раз, когда в уставки ПСБ или ее конфигурацию вносятся изменения.

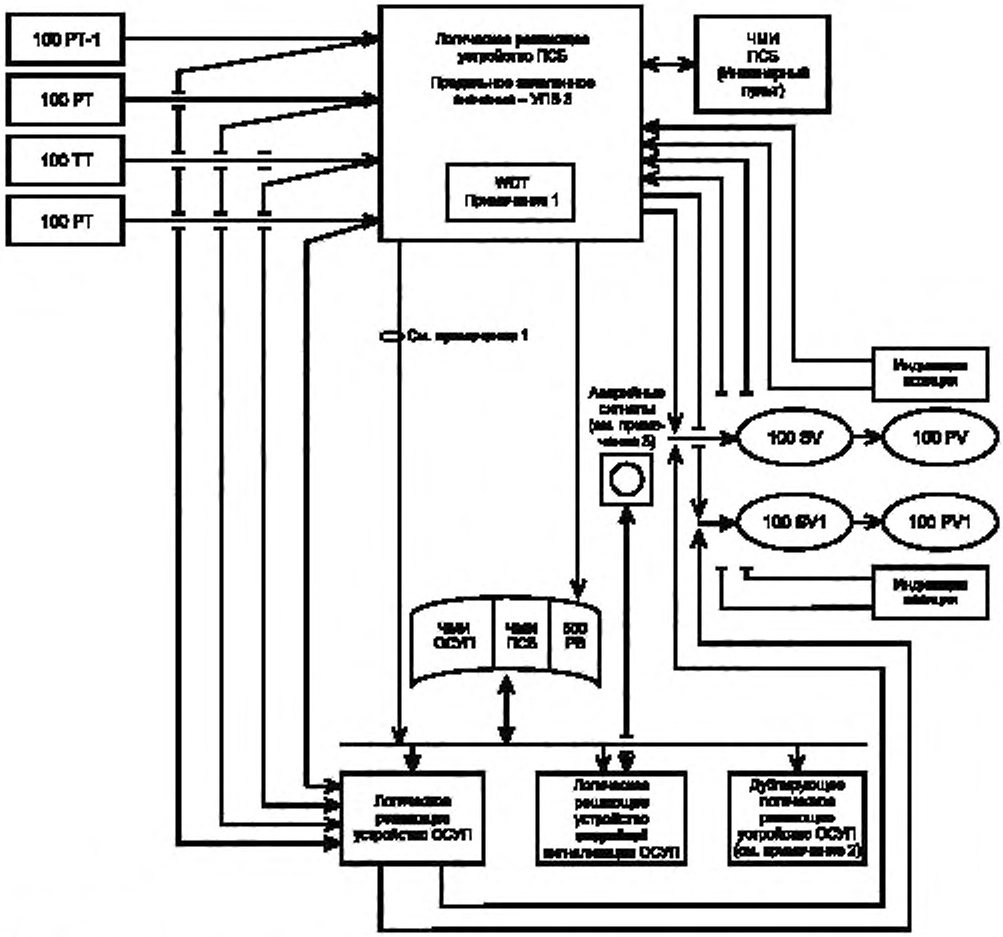
F.20 Особенности проекта прикладной программы ПСБ

Документация на ППО включает комментарии, которые являются достаточно подробными, позволяющими объяснить функцию каждого символа, каждой ФБ ПСБ и связь каждого символа с ФБ ПСБ. Комментарии являются достаточно полными и полезными персоналу по проектированию и техническому обслуживанию как для понимания функций ППО, так и для ориентации в нем.

F.21 Практика электромонтажа

Правильные способы электромонтажа являются незаменимыми в обеспечении желаемого уровня готовности ПСБ. Ниже приведен список способов электромонтажа, реализованных в данной ПСБ:

- цепи не имеют общих нулевых проводников или общих обратных проводов постоянного тока, чтобы минимизировать:
  - вероятность непреднамеренного разрывания цепи(ей) в случае, когда нулевой проводник или общий провод отключен или оборван;
  - возможность возникновения замыканий через цепь заземлений и ошибок разводки;
  - обеспечение дополнительными ответвлениями (10 % запасных, 20 % с промежутком);
- функции предохранителей входов-выходов включают:
  - использование схем входа-выхода с индивидуальными предохранителями для лучшей локализации сбоев и минимизации возможных негативных последствий по общей причине;
  - использование входов-выходов изолированного типа;
  - использование внешних плавких предохранителей (т. е. предохранителей входов-выходов внешних для ПЛК) там, где это требуется и где можно минимизировать удаление карты;
  - использование колодок с плавкими предохранителями (вместе с общей предохранительной вставкой/рубильником) в качестве средства обеспечения отключения в целях обслуживания;
- использование прозрачного стекла, устойчивого к ЭМП, чтобы позволить визуальный доступ к диагностической информации (например, к лампочкам входов-выходов);
- внутреннее (т. е. внутри шкафа с логическим решающим устройством) освещение и розетка с включением вилки с ее последующим поворотом для ПСБ, предназначенная устранить подключение в розетку приборов индуктивной связи;
- клеммы ПСБ идентифицируются, когда они расположены рядом с контактными выводами, не связанными с ПСБ;
- чтобы минимизировать магнитные помехи и помехи по общей причине там, где это было необходимо, применялся монтаж витой парой.



Примечания
1 Канал связи с ЧВИ ПСБ сопровождается коммуникационным WDT, обеспечивающим работу ЧВИ ПСБ во время рабочего цикла.
2 Дублирование прикладного ПО ПСБ.
3 Аварийные сигналы весовой камеры и уровня (800 WTA и 400 LSA (см. рисунок F.11)).

Проект #	Редакция #	Редакция	RVSD	CHKD	APPD	Дата

Проект # YYYY
Начертил:
Проверил:
Одобрил:
DWG# XXXXX1
Дата:

Рисунок F.12 — ПСБ для реактора ВХМ

F.22 Защита

Меры обеспечения защиты, предпринимаемые в проекте ПСБ, поддерживают полноту безопасности путем предотвращения несанкционированных и непреднамеренных модификаций любых функций ПСБ или устройств, включая логические решающие устройства, логику приложения, интерфейсы пользователя, датчики и исполнительные элементы. Для тех устройств (например, устройств интерфейса), которым сложнее управлять физическим доступом, должно быть реализовано применение административных процедур.

Были реализованы некоторые базовые методы обеспечения защиты:

- письменное разрешение с пояснением причин получения доступа;
- письменное разрешение, где идентифицированы личности, которым требуется доступ;
- определение требующегося обучения и/или уровня ознакомления с системой перед разрешением доступа;
- определение того, кто будет обладать доступом к системе, при каких обстоятельствах и для выполнения какой работы. Сюда включены процедуры, необходимые для управления байпасами при техническом обслуживании.

Свойства ПСБ, которые облегчают управление доступом. Примеры таких свойств проекта включают:

- строгую идентификацию устройств ПСБ посредством разноцветной маркировки;
- физическое распределение оборудования ПСБ и ОСУП (облегчая защиту замками связанных с ними шкафов);
- применение разнообразных технологий (что, как правило, требует и другого интерфейса для технического обслуживания).

Использование ПСБ, основанных на ПЭС, привнесло дополнительные проблемы защиты, связанные с относительной легкостью внесения изменений в логику приложения. Для этих систем были реализованы дополнительные функции, включая:

- ограничение доступа к интерфейсу разработки/обслуживания;
- утверждение административной политики/процедур, определяющих условия, при которых интерфейс технического обслуживания может быть подключен к системе во время нормального функционирования;
- использование программного обеспечения для поиска вирусов, а также надлежащих процедур обработки файлов и программ в инженерном пульте, чтобы помочь избежать искажения встроенной логики и/или логики приложений;
- использование служебного программного обеспечения ПСБ, которое отслеживает новые версии логики приложений и позволяет определять (по факту), когда было внесено изменение, кто его сделал и из чего оно состояло;
- отсутствие каких-либо внешних соединений ПСБ или ОСУП с Интернетом или телефонными линиями.

F.23 Шаг F.5. Установка, ввод в эксплуатацию и подтверждение соответствия ПСБ

Таблица F.17 — Жизненный цикл ПСБ. Блок 5

Стадия или деятельность жизненного цикла безопасности		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок F.7, блок 5	Установка, ввод в эксплуатацию и подтверждение соответствия ПСБ	Собрать и испытать ПСБ. Подтвердить соответствие во всех отношениях ПСБ требованиям безопасности в части требуемых ФБ ПСБ и требуемой полноты безопасности	12.3, 14, 15	Проект ПСБ. План испытания интеграции ПСБ. Требования к безопасности ПСБ. План для подтверждения соответствия безопасности ПСБ	Полное функционирование ПСБ в соответствии с проектом ПСБ. Результаты тестирования интеграции ПСБ. Результаты деятельности по установке, вводу в эксплуатацию и подтверждению соответствия

В таблице F.17 представлены цели, входы, выходы и ссылки на связанные с ними разделы и подразделы для установки, ввода в эксплуатацию и подтверждения соответствия ПСБ.

F.24 Установка

Установка ПСБ начинается с наличия проекта, производственного помещения, технологического оборудования, средств обеспечения (например, электричества) и приборного оборудования. Установка заканчивается переходом (т. е. передачей) ПСБ от построения до эксплуатации. Этот переход отражает принятие ПСБ отделом эксплуатации; в этот момент начинается запуск ПСБ в эксплуатацию (см. настоящий раздел).

Корпоративные функции по закупке и входному контролю были признаны адекватными для обеспечения принятия указанных устройств ПСБ в исправном состоянии в сопровождении надлежащей документации по их использованию в соответствии с МЭК 61511-1:2016 (подраздел 11.5). Временное хранение каждого устройства выполняется согласно руководству по безопасности производителя этого устройства и включает любые необходимые меры профилактического обслуживания оборудования.

Необходимо отметить, что существовала процедура обратного перехода в режим установки для реализации исправлений проблем, обнаруженных отделом эксплуатации; этот переход приводил к тому, что смежное оборудование оказывалось на разных стадиях завершения/приемки (т. е. в состоянии установки, а не в состоянии эксплуатации). Для данного проекта были использованы белая метка (для состояния эксплуатации) и зеленая метка (для состояния построения).

Каждое приборное средство было идентифицировано с помощью кодовой метки данного приборного средства. Для ПСБ были предоставлены следующие дополнительные идентификационные характеристики:

- все приборные средства ПСБ обеспечены визуальной идентификацией (т е. покрашены красным цветом) их статуса как устройства ПСБ;
- шкаф ПСБ обеспечен биркой с наименованием, ссылающейся на шифр чертежа ПСБ;
- ЧМИ-интерфейсы ПСБ идентифицированы (с помощью идентификации на первой странице программного обеспечения) как устройства, связанные с ПСБ;
- каждое устройство ФБ ПСБ было идентифицировано с помощью маркировки: # чертежа его контура и # ФБ ПСБ.

В установку ППО не входит сборка. ППО было разработано, испытано и верифицировано во время проектирования и было введено в ПСБ во время ввода системы в эксплуатацию.

Перед передачей отделу эксплуатации были выполнены следующие действия по верификации сборки:

- «прозвон» проложенной проводки для обеспечения надлежащего заземления и схемы соединения ПСБ;
- подача питания на средства управления (тем самым обеспечивая отсутствие коротких замыканий или перегрузок), включая входы-выходы;
- прямой пуск подачей полного напряжения (например, ступенчатым напряжением, «броском») на каждый двигатель и каждый клапан для обеспечения их работы в правильном направлении;
- проверка функциональности всех средств обеспечения (например, пневматической системы);
- выполнение «сквозного контроля» для проверки того, что установка завершена, безопасна и корректна;
- предоставление полной и исполнительно-технической документации ПСБ.

Отдел эксплуатации принимает участие в вышеописанной деятельности по верификации, чтобы:

- обрести понимание границ установки и размещения устройств ПСБ;
- обрести понимание размещения средств обеспечения и критически важных для них устройств [например, защиты от отключения, перегрузки и короткого замыкания (например, предохранители, автоматические выключатели)];
- иметь возможность предоставить необходимую подробную информацию для их плана ввода в эксплуатацию (см. раздел F.25);
- отдел технического обслуживания ознакомился с установкой ПСБ, работая под руководством отдела сборки, чтобы выполнить выбранные действия по верификации ПСБ, рассмотренные в настоящем разделе (например, «прозвон» ПСБ).

Завершенная установка верифицируется и принимается инспекционной группой, составленной из персонала сборки, эксплуатации и проектирования. После этого оборудование было промаркировано, чтобы отразить, что оборудование принято отделом эксплуатации и ему принадлежит (т. е. отдел эксплуатации несет ответственность за это оборудование).

F.25 Ввод в эксплуатацию

Ввод в эксплуатацию — это действия, выполняемые в период времени, начинающийся после завершения передачи (т. е. отделом сборки отделу эксплуатации) и заканчивающийся верификацией того, что ввод в эксплуатацию ПСБ завершен и можно перейти к подтверждению соответствия (см. раздел F.27). Для данного примера ввод ПСБ в эксплуатацию начался сразу же после ввода в эксплуатацию ОСУП.

Процедура ввода в эксплуатацию ПСБ включает идентификацию, построение графика, планирование, организацию, надзор и документальное оформление отладки системы аппаратных средств ПСБ, а также откладку операционных(ой) систем(ы) (т. е. встроенного ПО).

Ввод в эксплуатацию ПСБ рассматриваемого примера также называется «отладкой», так как это понятие лучше отражает основной вид деятельности, входящей в ввод в эксплуатацию. Отладка является пошаговой процедурой, обеспечивающей, что:

- подключение всех узлов ПСБ осуществлено правильно (включая заземление);
- все средства обеспечения (например, электроэнергия, сжатый воздух) функционируют надлежащим образом;
- все устройства ПСБ (например, датчики, логические решающие устройства, исполнительные элементы, ЧМ-интерфейсы, инженерные станции, коммуникационные системы) обеспечиваются питанием и функционируют надлежащим образом;
- настройки датчиков корректны.

Устройства с фиксированным языком программирования (ФЯП) (например, интеллектуальные датчики) были проверены в течение этого периода времени. Инженерная станция логического решающего устройства ПСБ и все ее возможности были задействованы во время отладки. Отдел обслуживания объекта был ключевым участником в этой деятельности при поддержке отделов сборки и проектирования, когда это требовалась. Отдел эксплуатации одобрил ввод в эксплуатацию, посчитав его завершенным и удовлетворительным, прежде, чем был выполнен переход к подтверждению соответствия.

F.26 Документация

Вся необходимая документация должна быть доступна персоналу. В связи с этим была проведена проверка обеспечения доступности и корректности всей документации перед переходом к подтверждению соответствия.

Окончательный список принятых документов включает в себя следующее:

- документацию по анализу рисков и опасностей [«что если» (см. таблицу F.4), HAZOP (см. таблицу F.5)];
- классификацию допустимого риска (см. таблицу F.8);
- документальное оформление распределения риска по слоям защиты — определение УПБ для каждой ФБ ПСБ (АУЗ);
- процедуру испытания для каждой ФБ ПСБ (см. раздел F.27);
- спецификацию требований к безопасности, включающую:
  - схемы Т и КИП;
  - логические диаграммы;
  - распечатку ППО;
  - руководства по безопасности;
  - обоснование безопасности органом оценки;
  - документальное оформление метода обоснования выбора оборудования;
  - инструкции по установке от производителя;
  - документацию на аппаратные средства ПСБ/ППО/установку/техническое обслуживание;
  - обоснование стойкости к систематическим отказам;
  - вычисления верификации УПБ (т. е. $ВОНЗ_{ср}$) для ФБ ПСБ, включая диаграммы состояний.

F.27 Подтверждение соответствия.5

Подтверждение соответствия — это действия, выполняемые в период времени, начинающийся после завершения ввода в эксплуатацию и заканчивающийся получением заключения о том, что ПСБ соответствует функциональным требованиям, заданным в СТБ.

Подтверждение соответствия ПСБ начинается после ввода в эксплуатацию ПСБ и подтверждения соответствия ОСУП.

Процедура подтверждение соответствия ПСБ включает идентификацию, составление графика, планирование, организацию, надзор и документальное оформление определенного набора действий. Эти действия для ПСБ включают:

- обкатку системы аппаратных средств;
- обкатку операционных(ой) систем(ы) (т. е. встроенного программного обеспечения);
- обкатку ППО;
- запуск (одобрение приемочного испытания и передача на производство, т. е. отделу эксплуатации).

Подтверждение соответствия данного примера ПСБ было разделено на «обкатку» и «запуск», чтобы лучше отразить основной вид деятельности, реализованный для подтверждения соответствия.

Обкатка — это пошаговая процедура, гарантирующая корректное функционирование ПСБ с неопасными материалами в технологическом процессе (например, использование воды вместо опасной жидкости), при этом управление процессом выполняется так, как если бы он реализовывал конечный продукт. Чтобы это было возможно, ППО логического решающего устройства ПСБ было установлено (см. раздел F.23) и испытано (см. раздел F.27) тщательным образом на всех его режимах работы (например, при запуске, действии, останове).

Производственный персонал являлся ключевым участником в этот период времени при поддержке персонала по обслуживанию и проектированию. При успешном завершении и одобрении обкатки отделом эксплуатации ПСБ передается на запуск.

Запуск является деятельностью, для которой требуется, чтобы отдел эксплуатации безопасным образом производил качественную продукцию при заранее одобренном цикле производства. Во время этой процедуры устройства ПСБ проверяются, чтобы обеспечить их надлежащее функционирование и способность выполнять их функцию безопасности, как установлено во время обкатки. После успешного завершения этой процедуры ее результаты были документально оформлены и отделом эксплуатации были окончательно утверждены. Подтверждение соответствия этого проекта ПСБ было завершено.

F.28 Испытание

Большая часть требующихся испытаний, обсуждаемых в настоящем разделе, была проведена во время начального подтверждения соответствия ПСБ. Процедуры испытаний, описанные ниже, также применяются для периодического тестирования и инспекции, описанной в разделе F.29, шаг 6.

Процедура испытания была составлена проектировщиком ПСБ. Эта процедура включает признание возникновения возможных происшествий, связанных с безопасностью, в результате проведения испытания ФБ ПСБ. В результате полученная процедура испытаний точно описывает, как безопасно выполнить испытания, а также количество/качество требующегося оборудования и персонала.

Испытание состояло из следующих действий:

- испытаний устройств;
- заводских испытаний и калибровки;
- моделирования;
- раздельного тестирования логики;
- автоматического тестирования;
- ручного тестирования;
- документального оформления состояния непосредственно перед началом поверки и состояния непосредственно после окончания поверки;
- подробной пошаговой процедуры.

Некоторые основные функции были протестированы не только ради настроек срабатывания и исполнительных управляющих устройств. Были проверены диагностические процедуры выявления ошибок, таких как потеря сигнала, формируют эти диагностические процедуры аварийные сигналы или переводят процесс в безопасное состояние. Была проверена логика с фиксацией состояния и его сброса в ФБ ПСБ, учитывая положение исполнительного управляющего устройства на сбросе. Положение возврата было документально оформлено и проверено.

Было испытано взаимодействие ПСБ с ОСУП. Были проверены показатели ФБ ПСБ, отправляемые в ОСУП, вместе с любыми другими действиями, выполняемыми при получении этих показателей. Дублирование логики ПСБ, выполняемое ОСУП, было испытано отдельно, чтобы подтвердить, что обе системы работают в соответствии с их проектами.

Общая процедура испытания ФБ ПСБ выглядит следующим образом:

- организация байпаса других ФБ ПСБ, которые необходимо обойти, чтобы испытать целевую ФБ ПСБ;
- моделирование нормальных условий работы:
    - моделирование приборных сигналов при нормальных рабочих условиях;
    - установка целевых исполнительных управляющих устройств в нормальное рабочее положение;
    - установка контроллеров и других устройств в нормальный рабочий режим;
- испытание ФБ ПСБ:
    - запись фактической точки срабатывания ФБ ПСБ;
    - верификация аварийного сигнала тревоги ФБ ПСБ и действий исполнительных управляющих устройств;
    - верификация действий ОСУП, связанных с ФБ ПСБ;
- сброс состояния ФБ ПСБ:
    - верификация сохранения действий ФБ ПСБ в безопасном состоянии;
- сброс ФБ ПСБ:
    - верификация сброса действий ФБ ПСБ в ее запроектированное состояние.

В процедуре примера полагается, что приборные средства прошли заводские испытания и откалиброваны. Этот пример процедуры написан скорее для одновременного тестирования всех функций ПСБ, чем для случая, в котором для каждой ФБ ПСБ имеется своя процедура. В первую очередь эта процедура проверяет основную функцию ПСБ и исполнительные управляющие устройства. Каждое действие по выполнению испытания предоставляет процедуру испытания в случае, если был заменен датчик или было внесено изменение в настройку срабатывания.

Важным ключевым фактором для успешного выполнения испытания на стадии подтверждения соответствия являлась заинтересованность персонала по эксплуатации и техническому обслуживанию в получении четкого понимания всех аспектов технологического процесса, ОСУП и ПСБ. Этот персонал включал:

- квалифицированного оператора пункта управления;
- квалифицированного электротехника и специалиста по приборам.

В таблице F.18, приведенной ниже, представлен список используемых типов приборных средств и некоторых процедур проведения испытания.

Таблица F.18 — Список используемых типов приборных средств и процедур проведения испытания

Давление:	
нормальные соединения	Обеспечение соединения дренажа/вентиляции и давления испытания на выходе клапана основного блока
выносные мембраны	Изолирующие клапаны и калибровочные кольца должны предоставляться для проведения испытания при действующем процессе. В подтверждении соответствия калибровки следует учитывать подъем (уровня) по отношению к клапану(ам) и определенную плотность заполняющей жидкости для капилляра
Температура:	
термопара	Проверка целостности устройства может быть выполнена только для определения работоспособности. Следует измерить значение в мВ на выходе при известной температуре и сравнить со стандартной кривой
резистивный температурный датчик (РТД)	Для проверки работоспособности устройства может быть измерено сопротивление. Верификацию сопротивления стоит проводить при известной температуре, сравнивая значения со стандартной таблицей калибровки данного устройства
системы с наполнением	Следует снять первичный датчик и поместить его в температурную ванну
биметаллический переключатель	Следует снять первичный датчик и поместить его в температурную ванну

Описанная далее процедура является примером для подтверждения соответствия функций ПСБ, включая диагностические аварийные сигналы. Этот пример не включает испытание функций ОСУП. Каждое устройство ПСБ (например, датчик, логическое решающее устройство, исполнительный элемент) тестировалось (или заменялось) по рекомендации производителя, что может быть не учтено в процедуре данного примера, но предполагается, что это было выполнено отдельно [см. ISA-TR84.00.03:2012, Mechanical Integrity of Safety Instrumented Systems (SIS)]. Примеры процедур проведения испытания можно найти в руководстве по безопасности производителя в разделе, посвященном контрольным испытаниям. Полная процедура испытания может также включать в себя испытание:

- действий ОСУП при активации функции безопасности, таких как переключение контроллеров в ручной режим;
- функций блокировки дублирования ОСУП;
- аварийных сигналов ОСУП при диагностике системы безопасности;
- аварийных сигналов ОСУП, распределенных в качестве слоев защиты в результате АУЗ.

Пример процедуры проверки блокировки реактора R1 приведен ниже.

В процедуре, приведенной ниже, цитируется NOMEX®[1)].

[1)] NOMEX® является примером подходящего изделия, доступного на рынке. Эта информация предоставляется для удобства пользователей настоящего стандарта и не означает поддержку данного изделия со стороны МЭК.

Заголовок:	Реактор R1 Процедура проверки блокировки	Подготовил:		ДАТА:	
		Проверил:		ДАТА:	
Область:		Техническое утверждение:		ДАТА:	
Критически важное обеспечение безопасности производственного процесса:	Да	Утвердил:		ДАТА:	

☐ АРХИВНАЯ КОПИЯ ☐ КОПИЯ ОБЪЕКТА

Отчет о результатах испытания

A. Испытанные датчики/переключатели:

Тип	Ноль	Диапазон	Единица измерения	Норма	Норма, мА	Аварийный сигнал	Аварийный сигнал, мА	Срабатывание	Срабатывание, мА	Устойчивость
100PT	0	200	PSIG	100	12	115	13.2	125	14	± 2 PSIG
100PT1	0	200	PSIG	100	12	115	13.2	125	14	± 2 PSIG
100TT	0	250	Deg F	125	12	180	15,52	200	16,8	± 2 Deg F
200PT	0	20	PSIG	2,5	6	5	8	10	12	± 1 PSIG

B. Испытанные исполнительные управляющие устройства

Тип	Положение
100PV	Открыт
100PV1	Открыт

C. Результаты испытания

Проверка первая:

_____ Все устройства прошли испытание.

_____ Для прохождения испытания потребовались корректирующие действия.

Дата завершения проверочной процедуры: _____.

D. Безопасность и здоровье

Защитное оборудование для персонала в соответствии с требованиями процедуры (например, защитные очки, шлем-каска, защитные ботинки).

E. Специальное защитное оборудование

Для защиты от световой вспышки требуется NOMEX®.

F. Условия, предшествующие испытанию, и блокировка

Должен быть проведен сброс реактора, и реактор должен быть заблокирован при помощи процедуры «запереть, отметить и проверить» (lock, tag & try).

Системы аварийного останова должны быть неактивны.

Там, где необходимо, должны быть установлены барьеры.

Информация (например, знаки, памятки, составление графиков, планирование) должна быть исчерпывающей.

G. Разрешения

Разрешение на разрыв линии для каждого измерительного преобразователя.

H. Специальное оборудование

Один генератор тока.
Одно переносной передатчик-коммутатор.

I. Габаритные чертежи

Схемы Т и КИП:
Схемы логики:
Чертежи E&I:

J. Штатная численность

Квалифицированный оператор пункта управления.
Квалифицированный специалист-электрик и специалист по приборам.

Каждая процедура испытания блокировки обладает своими уникальными требованиями к обеспечению безопасности. Следующий текст следует модифицировать, чтобы он соответствовал требованиям для конкретного применения.

Калибровка и осмотр

A. Инструментальное средство, прошедшее калибровку, или калибровка, прошедшая верификацию

Инструментальные средства, прошедшие калибровку в соответствии с их процедурами обслуживания.

Тип	Описание	Срабатывание	До проверки	Инициалы	Дата
100PT	Давление в реакторе север				
100PT1	Давление в реакторе юг				
100TT	Температура в реакторе				
200PT	Давление в предохранителе от утечки реактора				

B. Осмотренные инструментальные средства и исполнительные устройства управления

Внешние установки, осмотренные для обнаружения проблем с проводкой, трубопроводами, фильтрами, контрольно-измерительными приборами, соленоидами, изоляцией и технологическими соединениями.

Тип	Описание	До проверки	После проверки	Инициалы	Дата
100PT	Давление в реакторе север				
100PT1	Давление в реакторе юг				
100TT	Температура в реакторе				
200PT	Давление в предохранителе от утечки реактора				
100PV	Выпускной клапан реактора север				
100PV1	Выпускной клапан реактора юг				

Процедура испытания блокировки

Время начала процедуры проверки: _____Дата: _____
Процедура была выполнена:

Звание	Подпись	Дата
Оператор пункта управления		
Технический специалист E&I		
Технический специалист E&I		
Менеджер группы эксплуатации		

Общая структура для процедуры проверки блокировки

Технический специалист E&I:

A. Воспроизвести нормальные условия работы

_____ Убрать все блокировки ОСУП на 100PV и 100PV1.
_____ Обновить список проверки обхода для обхода #1.

Процедура проверки блокировки для РВ (кнопки) останова ПСБ реактора

Периодичность испытания:	6 мес
Цель испытания:	Ручной останов системы безопасности реактора открывает клапаны управления давлением в реакторе 100 V и 100PV1. Также следует провести испытание диагностики исполнительных управляющих устройств

A. Снять блокировку. (Оператор пункта управления.)

_____ Сбросить систему безопасности реактора нажатием кнопки сброса PB000.
_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.
_____ Проверить, что лампочка EA011 не горит, сигнализируя о том, что система безопасности реактора в неактивном режиме.

B. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Проверить, что диагностический аварийный сигнал закрытого выпускного клапана реактора EA18 не горит.
_____ Из ОСУП закрыть выпускной клапан реактора 100PV.
_____ Из ОСУП закрыть выпускной клапан реактора 100PV1.
_____ Установить все контроллеры ОСУП в нормальное рабочее положение.
_____ Установить все контроллеры ОСУП в нормальный рабочий режим.
_____ Установить все клапаны и двигатели ОСУП в нормальный рабочий режим.

C. Провести верификацию нормальных условий на объекте. (Оператор на объекте.)

_____ Провести верификацию на объекте закрытия выпускного клапана 100PV.
_____ Провести верификацию на объекте закрытия выпускного клапана 100PV1.

D. Провести испытание диагностического аварийного сигнала. (Технический специалист E&I.)

_____ Отсоединить сигнал от переключателя закрытого положения выпускного клапана реактора 100LSC.
_____ Проверить, что диагностический аварийный сигнал закрытого выпускного клапана реактора EA18 горит.
_____ Подсоединить сигнал от переключателя закрытого положения выпускного клапана реактора 100LSC.
_____ Проверить, что диагностический аварийный сигнал закрытого выпускного клапана реактора EA18 не горит.
_____ Отсоединить сигнал от переключателя закрытого положения выпускного клапана реактора 100LSC1.
_____ Проверить, что диагностический аварийный сигнал закрытого выпускного клапана реактора EA18 горит.
_____ Подсоединить сигнал от переключателя закрытого положения выпускного клапана реактора 100LSC1.
_____ Проверить, что диагностический аварийный сигнал закрытого выпускного клапана реактора EA18 не горит.

E. Провести испытание блокировки. (Оператор пункта управления.)

_____ Произвести останов системы безопасности реактора нажатием кнопки останова 500PB.

F. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка активности системы безопасности реактора EA010 не горит.
_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.
_____ Проверить, что диагностический аварийный сигнал об открытии выпускного клапана реактора EA17 не горит.
_____ Из ОСУП проверить, что выпускной клапан реактора 100PV открыт.
_____ Из ОСУП проверить, что выпускной клапан реактора 100PV1 открыт.
_____ Проверить, что все контроллеры ОСУП установлены в безопасное положение.
_____ Проверить, что все контроллеры ОСУП установлены в безопасный режим.
_____ Проверить, что все клапаны и двигатели ОСУП находятся в безопасном режиме.

G. Провести верификацию нормальных условий на объекте. (Оператор на объекте.)

_____ Провести верификацию на объекте, что выпускной клапан реактора 100PV открыт.
_____ Провести верификацию на объекте, что выпускной клапан реактора 100PV1 открыт.

H. Провести испытание диагностического аварийного сигнала. (Технический специалист E&I.)

_____ Отсоединить сигнал от переключателя открытого положения выпускного клапана реактора 100LSO.
_____ Проверить, что диагностический аварийный сигнал открытого выпускного клапана реактора EA17 горит.
_____ Подсоединить сигнал от переключателя закрытого положения выпускного клапана реактора 100LSO.
_____ Проверить, что диагностический аварийный сигнал открытого выпускного клапана реактора EA17 не горит.
_____ Отсоединить сигнал от переключателя открытого положения выпускного клапана реактора 100LSO1.
_____ Проверить, что диагностический аварийный сигнал открытого выпускного клапана реактора EA17 горит.
_____ Подсоединить сигнал от переключателя открытого положения выпускного клапана реактора 100LSC1.
_____ Проверить, что диагностический аварийный сигнал открытого выпускного клапана реактора EA17 не горит.

I. Сбросить блокировку. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.
_____ Проверить, что лампочка активности системы безопасности реактора EA010 горит.
_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, не горит.
_____ Проверить, что диагностический аварийный сигнал открытого выпускного клапана реактора EA17 не горит.

J. Провести верификацию условий переустановки на объекте. (Оператор на объекте.)

_____ Провести верификацию на объекте, что выпускной клапан реактора 100PV открыт.
_____ Провести верификацию на объекте, что выпускной клапан реактора 100PV1 открыт.

K. Провести верификацию условий переустановки. (Оператор пункта управления.)

_____ Из ОСУП проверить, что выпускной клапан реактора !00PV открыт.
_____ Из ОСУП проверить, что выпускной клапан реактора !00PV1 открыт.
_____ Проверить, что все контроллеры ОСУП установлены в безопасное положение.
_____ Проверить, что все контроллеры ОСУП установлены в безопасный режим.
_____ Проверить, что все клапаны и двигатели ОСУП находятся в безопасном режиме.

Процедура проверки блокировки давления в реакторе, датчик 100PT

ФБ ПСБ	S1, S2
Название события:	Превышение допустимого давления в реакторе
Классификация события.	УПБ 2
Периодичность испытания:	6 мес
Цель испытания:	Высокое давление в реакторе открывает клапаны управления давлением реактора 100PV и 100PV1

A. Провести диагностику (Технический специалист E&I.)

_____ Подключиться к датчику давления реактора 100PT при помощи ручного коммуникатора и провести диагностику датчика.
_____ Проверить, что ошибки диагностики отсутствуют.

B. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.
_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

C. Провести испытание блокировки. (Технический специалист E&I.)

_____ Отсоединить датчик давления реактора 100PT от системы безопасности.

D. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

E. Воспроизвести нормальные условия. (Технический специалист E&I.)

_____ Подсоединить моделирующее устройство к датчику давления реактора 100PT.

_____ Смоделировать давление 100 фунт/кв. дюйм (12 мА) на датчике давления реактора 100PT.

_____ Обновить список проверки обхода для обхода #2.

F. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, не горит.

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 активности системы безопасности реактора горит.

G. Провести испытание блокировки. (Технический специалист E&I.)

_____ Постепенно повысить уровень моделируемого сигнала на датчике давления реактора 100PT до 125 фунт/кв. дюйм (14 мА).

_____ Записать настройки, при которых произошло срабатывание блокировки: _____

H. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

I. Сбросить блокировку. (Технический специалист E&I.)

_____ Постепенно понизить уровень моделируемого сигнала на датчике давления реактора 100PT до 100 фунт/кв. дюйм (12 мА).

J. Провести верификацию условий переустановки. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора не горит.

K. Возвращение к текущим условиям. (Технический специалист E&I.)

_____ Отключить моделирующее устройство от датчика давления реактора 100PT.

_____ Присоединить датчик давления реактора 100PT к системе безопасности.

_____ Обновить список проверки обхода для обхода #2.

L. Провести верификацию текущих условий. (Оператор пункта управления.)

_____ Провести верификацию того, что датчик давления 100PT реактора считывает фактическое давление в реакторе.

Процедура проверки блокировки давления в реакторе, датчик 100PT1

ПСБ	S2
Название события:	Превышение допустимого давления в реакторе
Классификация события:	УПБ 2
Периодичность испытания:	6 мес
Цель испытания:	Высокое давление в реакторе открывает клапаны управления давлением реактора 100PV и 100PV1

A. Провести диагностику. (Технический специалист E&I.)

_____ Подключиться к датчику давления реактора 100PT1 при помощи ручного коммуникатора и провести диагностику датчика.

_____ Проверить, что ошибки диагностики отсутствуют.

B. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

C. Провести испытание блокировки. (Технический специалист E&I.)

_____ Отсоединить датчик давления реактора 100PT1 от системы безопасности.

D. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

E. Воспроизвести нормальные условия. (Технический специалист E&I.)

_____ Подсоединить моделирующее устройство к датчику давления реактора 100PT1.

_____ Смоделировать давление 100 фунт/кв. дюйм (12 мА) на датчике давления реактора 100PT1.

_____ Обновить список проверки обхода для обхода #3.

F. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, не горит.

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 активности системы безопасности реактора горит.

G. Провести испытание блокировки. (Технический специалист E&I.)

_____ Постепенно повысить уровень моделируемого сигнала на датчике давления реактора 100PT1 до 125 фунт/кв. дюйм (14 мА).

_____ Записать настройки, при которых произошло срабатывание блокировки: _____

H. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

I. Сбросить блокировку. (Технический специалист E&I.)

_____ Постепенно понизить уровень моделируемого сигнала на датчике давления реактора 100PT1 до 100 фунт/кв. дюйм (12 мА).

J. Провести верификацию условий переустановки. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора не горит.

K. Возвращение к текущим условиям. (Технический специалист E&I.)

_____ Отключить моделирующее устройство от датчика давления реактора 100PT1.

_____ Присоединить датчик давления реактора 100PT1 к системе безопасности.

_____ Обновить список проверки обхода для обхода #3.

L. Провести верификацию текущих условий. (Оператор пункта управления.)

_____ Провести верификацию того, что датчик давления 100PT1 реактора считывает фактическое давление в реакторе.

Процедура проверки блокировки температуры в реакторе, датчик 100TT

ПСБ	S1
Название события:	Превышение допустимой температуры в реакторе
Классификация события.	УПБ 2
Периодичность испытания:	12 мес
Цель испытания:	Высокая температура в реакторе открывает клапаны управления давлением реактора 100PV и 100PV1

A. Провести диагностику (Технический специалист E&I.)

_____ Подключиться к датчику температуры реактора 100TT при помощи ручного коммуникатора и провести диагностику датчика.

_____ Проверить, что ошибки диагностики отсутствуют.

B. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

C. Провести испытание блокировки. (Технический специалист E&I.)

_____ Отсоединить датчик температуры реактора 100TT от системы безопасности.

D. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

E. Воспроизвести нормальные условия. (Технический специалист E&I.)

_____ Подсоединить моделирующее устройство к датчику температуры реактора 100TT.

_____ Смоделировать температуру 125 F (12 мА) на датчике температуры реактора 100TT.

_____ Обновить список проверки обхода для обхода #4.

F. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, не горит.

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 активности системы безопасности реактора горит.

G. Провести испытание блокировки. (Технический специалист E&I).

_____ Постепенно повысить уровень моделируемого сигнала на датчике температуры реактора 100TT до 200 град. F (16,8 мА).

_____ Записать настройки, при которых произошло срабатывание блокировки: _____

H. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

I. Сбросить блокировку. (Технический специалист E&I.)

_____ Постепенно понизить уровень моделируемого сигнала на датчике температуры реактора 100TT до 125 град F (12 мА).

J. Провести верификацию условий переустановки. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора не горит.

K. Возвращение к текущим условиям. (Технический специалист E&I.)

_____ Отключить моделирующее устройство от датчика температуры реактора 100TT.

_____ Присоединить датчик температуры реактора 100TT к системе безопасности.

_____ Обновить список проверки обхода для обхода #4.

L. Провести верификацию текущих условий. (Оператор пункта управления.)

_____ Провести верификацию того, что датчик температуры реактора 100TT считывает фактическую температуру в реакторе.

Процедура проверки блокировки давления в предохранителе от утечки реактора, датчик 200PT

ПСБ	S3
Название события:	Превышение допустимого давления в предохранителе от утечки реактора
Классификация события:	УПБ 2
Периодичность испытания:	6 мес
Цель испытания:	Высокое давление в предохранителе от утечки реактора открывает клапаны управления давлением 100PV и 100PV1

A. Провести диагностику. (Технический специалист E&I.)

_____ Подключиться к датчику давления реактора 200PT при помощи ручного коммуникатора и провести диагностику датчика.

_____ Проверить, что ошибки диагностики отсутствуют.

B. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

C. Провести испытание блокировки. (Технический специалист E&I.)

_____ Отсоединить датчик давления реактора 200PT от системы безопасности.

D. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

E. Воспроизвести нормальные условия. (Технический специалист E&I.)

_____ Подсоединить моделирующее устройство к датчику давления в предохранителе от утечки реактора 200PT.

_____ Смоделировать давление 2,5 фунт/кв. дюйм (6 мА) на датчике давления в предохранителе от утечки реактора.

_____ Обновить список проверки обхода для обхода #5.

F. Воспроизвести нормальные условия. (Оператор пункта управления.)

_____ Проверить, что лампочка EA014, сигнализирующая о диагностическом аварийном сигнале датчика системы безопасности реактора, не горит.

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 активности системы безопасности реактора горит.

G. Провести испытание блокировки. (Технический специалист E&I.)

_____ Постепенно повысить уровень моделируемого сигнала на датчике давления в предохранителе от утечки реактора 200PT до 10 фунт/кв. дюйм (12 мА).

_____ Записать настройки, при которых произошло срабатывание блокировки: _____

H. Провести верификацию действий блокировки. (Оператор пункта управления.)

_____ Проверить, что лампочка EA011, сигнализирующая о неактивном состоянии системы безопасности реактора, горит.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора горит.

_____ Проверить, что система безопасности реактора не будет переустановлена при нажатии кнопки сброса PB000.

I. Сбросить блокировку. (Технический специалист E&I.)

_____ Постепенно понизить уровень моделируемого сигнала на датчике давления в предохранителе от утечки реактора 200PT до 2,5 фунт/кв. дюйм (6 мА).

J. Провести верификацию условий переустановки. (Оператор пункта управления.)

_____ Переустановить систему безопасности реактора нажатием кнопки сброса PB000.

_____ Проверить, что лампочка EA010 горит, сигнализируя о том, что система безопасности реактора в активном режиме.

_____ Проверить, что лампочка EA012 аварийного сигнала о срабатывании датчика системы безопасности реактора не горит.

K. Возвращение к текущим условиям. (Технический специалист E&I.)

_____ Отключить моделирующее устройство от датчика давления в предохранителе от утечки реактора 200PT.

_____ Присоединить датчик давления реактора 200PT к системе безопасности.

_____ Обновить список проверки обхода для обхода #5.

L. Провести верификацию текущих условий. (Оператор пункта управления.)

_____ Провести верификацию того, что датчик давления в предохранителе от утечки реактора 200PT считывает фактическое давление в предохранителе от утечки реактора.

Общие положения завершения процедуры проверки блокировки

Технический специалист E&I:

A. Вернуть все остальные блокировки в рабочее состояние.

_____ Вернуть все блокировки ОСУП на 100PV и 100PV1 для применения в режиме эксплуатации.

_____ Обновить список проверки обхода для обхода #1.

Испытание и осмотр выполнены:

Должность	Подпись	Дата
Оператор пункта управления		
Технический специалист E&I		
Технический специалист E&I		
Менеджер эксплуатационной группы		

Время завершения процедуры проверки: _____Дата: _____

Осмотр и документальное оформление после испытания.

A. Провести верификацию того факта, что все изменения процедуры были проверены при участии менеджмента и одобрены.

B. Если какое-либо устройство выдало отказ, то указать корректирующее действие, которое потребовалось применить:

_____

_____

_____

Поставить все требующиеся подписи на архивной копии и на копии с записями об испытании системы безопасности. В таблице F.19 показано, как может быть документально оформлен проверочный лист, посвященный использованию моделирования/байпаса в процедурах проверки блокировки.

Таблица F.19 — Контрольный лист использования байпаса/моделирования в процедурах проверки блокировки

Байпас #	Контур	Место установки	Метод	Шаг установки	Подпись	Шаг удаления	Подпись
1	DCS	DCS	Флаг	1.1		7.1	
2	100PT	Датчик	Моделирующее устройство	3.4		3.10	
3	100PT1	Датчик	Моделирующее устройство	4.4		4.10	
4	100TT	Датчик	Моделирующее устройство	5.4		5.10	
5	200PT	Датчик	Моделирующее устройство	6.4		6.10	
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

F.29 Шаг F.6. Эксплуатация и техническое обслуживание ПСБ

Таблица F.20 — Жизненный цикл ПСБ. Блок 6

Стадия или деятельность жизненного цикла ПСБ		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок F.7, блок 6	Эксплуатация и техническое обслуживание ПСБ	Обеспечить поддержание функциональной безопасности ПСБ в процессе эксплуатации и технического обслуживания	16	Требования к ПСБ. Проект ПСБ. План эксплуатации и технического обслуживания ПСБ	Результаты деятельности по эксплуатации и техническому обслуживанию ПСБ

Обучение персонала по эксплуатации, техническому обслуживанию или другого технического персонала функциям как ОСУП, так и ПСБ выполняется до ввода системы в эксплуатацию и повторяется каждый раз, когда в систему вносятся изменения.

Новые элементы, которые следует рассмотреть, при обучении вопросам эксплуатации и технического обслуживания ПСБ, включают:

- терминологию (например, ПСБ, ФБ ПСБ, $ВОНЗ_{ср}$, УПБ, слои защиты);
- анализ опасностей и рисков;
- архитектуру [например, ЧМИ (с ПСБ и ОСУП), интерфейсы ПСБ (например, связь только для чтения из ОСУП)];

- требования документации (например, частота запросов к ФБ ПСБ/ПСБ, процедуры/методы/технические приемы, контрольные проверки и осмотры, результаты испытаний, идентификаторы оборудования вплоть до уровня версий, ответственные лица/отделы/организации);
- процедуры обхода;
- периодичность испытаний для ФБ ПСБ/ПСБ;
- функциональное описание ПСБ.

Был разработан журнал срабатываний ПСБ для операторов и технического обслуживающего персонала, чтобы позволить им вести запись запросов к ПСБ и отказов ПСБ. См. таблицу F.21, приведенную ниже.

Ложные срабатывания ФБ ПСБ включаются в этот журнал, но не рассматриваются как запросы к ПСБ.

Таблица F.21 — Журнал срабатываний ПСБ

Дата	ФБ ПСБ	По запросу/ ложное	Причина срабатывания	Отчет о серьезном происшествии #	Записал
5/18/08	S-2	По запросу	Ошибка оператора — перегруженный реактор	Отчет о серьезном происшествии # 18	L. Soft
8/03/08	S-3	Ложное	Отказ датчика 200PT	Отсутствует	J. Doe
2/28/09	S-1	По запросу	Отказ контура управления охлаждающим средством	Отчет о серьезном происшествии #43	T. Rex

Для идентификации повторяющихся проблем устройств ПСБ (обнаруживаемых во время испытаний) была установлена система отслеживания. Результаты заносятся в журнал, как это показано в таблице F.22.

Таблица F.22 — Журнал отказов устройств ПСБ

Дата	Устройство	Безопасный/опасный отказ	Описание отказа	Записал
3/21/07	100TT	Безопасный	Нарушена калибровка	T. Rex
5/18/08	100PV	Опасный	Застрял шток клапана — клапан не открывается	L. Soft
8/03/08	100PV	Опасный	Застрял шток клапана — клапан не открывается	J. Doe
2/28/09	100PV	Опасный	Застрял шток клапана — клапан не открывается	T. Rex

Как это указано в таблице F.20, выпускной клапан 100PV часто ломался. После третьего отказа анализ причины отказов определил, что клапан был дефектным. Его заменили, и с тех пор отказы не наблюдались.

Документальное оформление текущей реализации логики управления и безопасности как в ОСУП, так и в ПСБ осуществляется постоянно. Любые изменения вносятся в документацию во время их реализации. Бумажные копии документации, полностью описывающей системы и их функции, сохраняются как справочные материалы.

Была реализована программа аудита, для которой необходимо проведение исследования документации на систему как части анализа опасностей циклического процесса. Выпущен отчет, описывающий результаты аудита, а любые рекомендации аудита помечаются для последующего выполнения (каждый квартал) до тех пор, пока все они не будут реализованы. Аудит включает:

- проверку всех изменений, выполненных со времени последней проверки, и верификацию правильного статуса документации;
- проверку всех проблем, связанных с оборудованием или логикой, связанных с ПСБ, производимую со времени последней проверки, предназначенную установить возможные проблемы, развитие которых способно ухудшить функционирование системы в будущем;
- проверку того, как эксплуатационный персонал понимает функцию и работу системы;
- проверку журнала запросов к ПСБ, чтобы подтвердить соответствие допущенной частоте запросов, полученной в результате АУЗ;
- проверку результатов испытания ФБ ПСБ, чтобы подтвердить соответствие допущенной частоте отказов устройства, используемой в вычислениях $ВОНЗ_{ср}$.

Ниже приведен список необходимой документации, которая будет включена в аудит. Эта документация будет доступна персоналу, занимающемуся эксплуатацией, и ее актуальность будут поддерживать:

- документация по анализу опасностей и рисков [«что если» (таблица I.4), HAZOP (таблица F.5)];
- применяемая классификация допустимого риска (т. е., таблица F.8);

- документальное оформление распределения риска по слоям защиты — определение УПБ для каждой ФБ ПСБ (АУЗ) (т. е. таблица F.9);
- схемы Т и КИП (т. е. рисунки F.3—F.10);
- диаграмма системы ФБ ПСБ (т. е. рисунок F.12);
- распечатка ППО (линейно-лестничные диаграммы) [т. е. рисунок F.11 (листы 1, 2, 3, 4 и 5)];
- руководства по безопасности;
- документация на аппаратные средства/ППО/установку/техническое обслуживанию (например, таблица F.20, блок 6);
- документация о стойкости к систематическим отказам;
- вычисления для верификации УПБ (т. е. $ВОНЗ_{ср}$) для каждой ФБ ПСБ, включая диаграммы состояний (т. е. рисунки F.4—F.9);
- процедуры испытаний для каждой ФБ ПСБ;
- запросы к процессу для каждой ФБ ПСБ (т. е. таблица F.21);
- данные по отказам для устройств ФБ ПСБ (т. е. таблица F.22).

Периодические испытания и осмотр ПСБ выполняются с периодичностью, установленной при вычислениях $ВОНЗ_{ср}$ (т. е. каждые шесть месяцев). Слои защиты, идентифицированные в процессе АУЗ, также подвергаются испытанию каждые шесть месяцев.

Отдел эксплуатации ведет записи, в которых демонстрируется, что контрольные испытания и осмотры были выполнены в соответствии с требованиями. Эти записи должны включать в себя, как минимум:

a) описание выполненных испытаний и осмотров;

b) дату испытаний и осмотров;

c) имена людей, выполнявших испытания и осмотры;

d) серийный номер или другие уникальные идентификаторы испытываемой системы (например, номер контура, кодовую метку, номер оборудования и номер ФБ ПСБ);

e) результаты испытаний и осмотра (например, условия «до проверки» и «после проверки»);

f) текущее ППО, работающее в логическом решающем устройстве ПСБ.

F.30 Шаг F.7. Модификация ПСБ

Таблица F.23 — Жизненный цикл ПСБ. Блок 7

Стадия или деятельность жизненного цикла ПСБ		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок F.2, блок 7	Модификация ПСБ	Провести изменения, улучшения и настройку ПСБ, обеспечивающие достижение и поддержание требуемого УПБ	17	Скорректированные требования к безопасности ПСБ	Результаты модификации ПСБ

В таблице F.23 представлены цели, входы, выходы и ссылки на соответствующие разделы и подразделы, связанные с модификацией ПСБ.

На объекте утвержден функциональный процесс управления изменениями, согласующийся с OSHA 29 CFR 1910.119. Любая модификация ПСБ потребует повторного входа в жизненный цикл ПСБ на соответствующем шаге.

F.31 Шаг F.8. Снятие с эксплуатации ПСБ

Снятие с эксплуатации ключевых устройств рассмотрено в таблице F.24.

Таблица F.24 — Жизненный цикл ПСБ. Блок 8

Стадия или деятельность жизненного цикла ПСБ		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок F.2, блок 8	Снятие с эксплуатации	Обеспечить правильную проверку, организацию работ и сохранность ПСБ	18	Информация о технологическом процессе и требованиях к его безопасности	ФБ ПСБ, выведенная из использования

На объекте есть опыт снятия с эксплуатации опасных процессов и понимание потребности в анализе опасностей и рисков, а также в инженерном анализе с последующим планированием снятия с эксплуатации. По завершении

этих процессов перед выполнением снятия с эксплуатации необходимо получить соответствующие полномочия и составить календарный график работ.

F.32 Шаг F.9. Верификация ПСБ

Верификация (см. таблицу F.25) является деятельностью, выполняемой на протяжении всего жизненного цикла ПСБ.

Инженерный персонал, персонал по эксплуатации и персонал по техническому обслуживанию совместно управляют планированием верификации таким образом, чтобы каждая организация могла достичь своих целей.

Инженерный отдел применяет верификацию для обеспечения:

- корректности и согласованности с СТБ его проектов аппаратных средств, ППО и системы;
- вовлечения эксплуатационного отдела в выбранной деятельности по верификации (например, разработки ППО, визуализаций ЧМИ) на начальных стадиях, чтобы избежать сюрпризов во время окончательного одобрения (например, значительных доработок, задержек);
- предоставления отделу обслуживания возможности работать с ПСБ устройствами/подсистемами/системами, чтобы персонал отдела смог ознакомиться с документацией, расположением аппаратных средств, функциональностью ППО, что одновременно облегчает процесс верификации.

Эксплуатационный отдел применяет верификацию для того, чтобы:

- установить, что проект выполнен, как было запланировано, и осуществляется по графику;
- использовать ее в качестве входного материала для написания рабочих инструкций.

Отдел обслуживания применяет верификацию:

- для ознакомления своего персонала с процессом;
- идентификации областей, где требуется новое обучение/инструментальные средства;
- идентификации процедур установки, не согласующихся с нормами объекта;
- разработки процедур обслуживания.

Таблица F.25 — Жизненный цикл ПСБ. Блок 9

Стадия или деятельность жизненного цикла ПСБ		Цель	Раздел или подраздел требований МЭК 61511-1. 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок F.2, блок 9	Верификация ПСБ	Провести испытания и оценить результаты конкретного этапа, чтобы гарантировать их правильность и соответствие стандартам изделий, рассматриваемых на этом этапе	7, 12.5	План верификации ПСБ для каждой стадии	Результаты верификации ПСБ для каждой стадии

F.33 Шаг F.10. Управление функциональной безопасностью и ОФБ ПСБ

Таблица F.26 — Жизненный цикл ПСБ. Блок 10

Стадия или деятельность жизненного цикла ПСБ		Цель	Раздел или подраздел требований МЭК 61511-1: 2016	Вход	Выход
МЭК 61511-1: 2016, рисунок F.2, блок 10	Управление функциональной безопасностью и ОФБ ПСБ	Обеспечить надлежащее рассмотрение всех этапов жизненного цикла ПСБ и дать заключение о достигнутой функциональной безопасности	5	Планирование ОФБ ПСБ; требование к безопасности ПСБ	Результаты ОФБ ПСБ

F.34 Управление функциональной безопасностью

F.34.1 Общие положения

Управление функциональной безопасностью (см. таблицу F.26) в данной компании реализуется как часть программы управления безопасностью процесса (УБП). Обширные корпоративные стандарты учитывают все аспекты УБП, такие как механическая полнота, обеспечение качества и обучение. Эти стандарты требуют, что все

новые проекты, реализованные на производственных объектах компании, соответствуют требованиям МЭК 61511 там, где это применимо.

F.34.2 Компетентность персонала

Требуется менеджмент для обеспечения компетентности людей, отвечающих за выполнение и проверку каждого из действий в жизненном цикле ПСБ для задач, которые были им назначены. Это было достигнуто реализацией подхода, рассмотренного в МЭК 61511-1:2016 (пункт 12.5.2). Рассматривались следующие составляющие квалификации:

- опыт и обучение;
- инженерные знания о процессе;
- инженерные знания о технологии ПСБ;
- инженерные знания о безопасности (например, корпоративные стандарты функциональной безопасности);
- навыки управления и руководства;
- понимание возможных последствий события.

Дополнительно персонал по эксплуатации и техническому обслуживанию получил знания об опасностях, связанных с технологическим процессом, и был обучен эксплуатации ОСУП и ПСБ перед их запуском.

F.35 Оценка функциональной безопасности (ОФБ)

ОФБ (также именуемая проверкой безопасности перед запуском) была выполнена перед запуском технологического процесса см. МЭК 61511-1:2016 (пункт 5.2.6.1). Общая цель ОФБ заключалась в обеспечении функционирования ПСБ в соответствии с требованиями, определенными в СТБ, чтобы ПСБ могла безопасным образом перейти из стадии установки в стадию эксплуатации.

ОФБ не начинается, пока не завершатся и не будут приняты все работы по верификации.

Текущая ОФБ будет периодически выполняться, как это описано в разделе F.29, шаг 6.

Приложение G
(справочное)

Руководство по применению методов прикладного программирования

G.1 Цель данного руководства

В промышленном секторе выбор ПЭ-устройств, как правило, основывается либо на устройствах, соответствующих МЭК 61508 (например, «ПЛК безопасности»), поддерживаемых руководством по безопасности, либо на опыте их предшествующего использования.

Настоящее приложение представляет примеры факторов, называемых «общие свойства прикладного программирования систем безопасности», которые следует рассматривать в зависимости от обстоятельств, либо используя руководство по безопасности, предоставленное производителем, либо с помощью руководства по программированию, предназначенного для конкретного проекта. Эти примеры предназначены поддержать проект ППО в рамках области применения настоящего стандарта и внести свой вклад в достижение ожидаемой систематической полноты безопасности ППО.

Примечание — Это приложение было ранее определено как приложение А.

G.2 Общие свойства прикладного программирования систем безопасности

Настоящее приложение описывает общие, независящие от языка, свойства прикладного программирования системы безопасности. Эти свойства были определены в формате иерархической, трехуровневой структуры. Четыре свойства верхнего уровня представлены ниже.

Безотказность. Безотказность — это предсказуемая и согласованная работа ППО в условиях, указанных в задании на проектирование. Это свойство верхнего уровня является важным для безопасности, так как оно обеспечивает снижение вероятности внесения ошибок в ППО во время его реализации, которые приводят к сбоям в работе ППО.

Устойчивость. Устойчивость — это способность ППО работать допустимым образом в случае нештатных условий или событий в технологическом процессе. Это свойство верхнего уровня является важным для безопасности, так как оно повышает способность ППО справляться с исключительными условиями, восстанавливаться после внутренних отказов и предотвращать распространение ошибок, возникающих из необычных обстоятельств (не все из которых могли быть всецело определены в задании на проектирование).

Прослеживаемость. Прослеживаемость связана с обоснованностью анализа и идентификации ППО, а также процессов создания и разработки библиотеки устройств, т. е. с демонстрацией того, что полученное ППО является продуктом строго упорядоченного процесса реализации. Прослеживаемость также включает возможность связывания ППО с проектными документами более высокого уровня. Это свойство верхнего уровня является важным для безопасности, так как оно упрощает верификацию и подтверждение соответствия, а также другие вопросы обеспечения качества ППО.

Ремонтопригодность. Это средства, с помощью которых ППО снижает вероятность внесения сбоев во время изменений, выполняемых после ввода в эксплуатацию. Это свойство верхнего уровня является важным для безопасности, так как оно позволяет снизить вероятность некорректной работы в результате внесения ошибок во время адаптивного, корректирующего или полного сопровождения ППО.

G.3 Безотказность

G.3.1 Общие положения

В контексте ППО безотказность: 1) либо является вероятностью успешного выполнения в течение заданного промежутка времени и в заданных условиях; 2) либо вероятностью успешной работы по запросу. Факт выполнения ППО до его завершения является результатом его правильного поведения по отношению к системной памяти и логики ППО. То, что ППО своевременно выдает результат, зависит от того, что инженер по автоматизации обладает пониманием языковых конструкций и характеристик рабочей среды во время выполнения. Таким образом, установленные промежуточные свойства безотказности это:

- предсказуемость использования памяти. Существует высокая вероятность того, что ППО не «заставит» логическое решающее устройство обратиться к непредусмотренным или запрещенным ячейкам памяти;
- предсказуемость потока управления. Существует высокая вероятность того, что логическое решающее устройство выполнит инструкции в той последовательности, которая предполагалась программистом;
- предсказуемость во времени. Существует высокая вероятность того, что ППО, работающее в определенной рабочей среде, не будет выходить за рамки его ограничений по времени реакции и ограничений его возможностей. Что касается предсказуемости математического или логического результата, то существует высокая вероятность, что ППО, работающее в определенной рабочей среде, выдаст математический или логический результат, который предполагался инженером по автоматизации.

G.3.2 Предсказуемость использования памяти

G.3.2.1 Минимизация динамического распределения памяти

Динамическое распределение памяти используется в ППО для временного присваивания (распределения) памяти, когда это становится необходимо во время выполнения, и для освобождения памяти (также во время выполнения) других пользователей, когда она им больше не требуется. Проблема безопасности при динамическом распределении памяти в системе реального времени заключается в том, что ППО впоследствии может не освободить всю память или ее часть. Это может произойти либо из-за того, что:

- ППО распределяет память для себя, но в процессе нормального выполнения не освобождает ее, либо
- ППО, которое временно распределило память для своего использования, было прервано до выполнения освобождения памяти.

Каждая из этих двух ситуаций приведет к неизбежной потере всей применимой памяти и потери всех функций безопасности в сети. Поэтому динамическое распределение памяти в цифровых системах безопасности должно быть минимизировано.

Если динамического распределения памяти нельзя избежать, то применим МЭК 61508-3, и ППО должно учитывать положения, обеспечивающие, что:

- вся динамически распределенная во время конкретного цикла выполнения память освобождается в конце этого цикла и
- вероятность прерывания выполнения между точкой, в которой память динамически распределяется, и точкой, в которой она освобождается, минимальна (если не исключена полностью). ППО также должно быть способно обнаруживать любые ситуации, где динамически распределенная память не была освобождена, и освобождать подобную память.

Настоящий стандарт тем самым не рекомендует использовать косвенную адресацию. МЭК 61508-3 применим к ППО, использующему косвенную адресацию.

G.3.2.2 Минимизация страничной организации памяти и свопинга

Страничная организация памяти реализуется для части памяти и применяется для хранения редко используемых областей основной памяти. Если у ППО возникает потребность в этих областях памяти, то логическое решающее устройство считывает содержание одной части памяти и загружает его обратно в другую часть памяти. Свопинг процесса заключается в использовании части памяти для хранения образа памяти всего неактивного процесса (включая такие его области памяти, как пространство стека и динамическую память).

Если приходит время для выполнения процесса, то этот образ загружается из одной части памяти назад в основную память для использования логическим решающим устройством. В случае любого события конкретный объем используемой памяти и часть хранилища, используемого для свопинга, являются неопределяемыми.

Эти функциональные возможности не подходят для систем безопасности, так как подобные неопределенности в использовании основной памяти и хранилища могут повлечь за собой значительные задержки по времени реакции и использование сложных функций, управляемых прерываниями, для организации обмена в памяти.

Если логическое решающее устройство, которое поддерживает страничную организацию памяти или свопинг процесса, используется в ПСБ, то эта функция должна быть отключена на уровне логического решающего устройства. Для всех данных и всех ППО должно быть достаточно основной памяти. Если существуют какие-либо сомнения, что эти функции не были отключены, то применим МЭК 61508-3, и ППО должно быть способно обеспечить нахождение всех критически важных функций и их данных в основной памяти на протяжении всего периода выполнения. Подобные средства в ППО включают вызовы логического решающего устройства («пиннинг»), директивы инструментальных средств прикладного программирования и скрипты логического решающего устройства.

G.3.3 Предсказуемость потока управления

G.3.3.1 Общие положения

Поток управления определяет порядок, в котором выполняются операторы ППО. Предсказуемый поток управления позволяет осуществить однозначную оценку того, как программа будет функционировать в определенных условиях.

Связанные с этим базовые свойства это:

- максимизация структуры;
- минимизация сложности потока управления;
- инициализация переменных перед их использованием;
- по одной точке входа и точке выхода для подпрограмм;
- минимум неоднозначностей, связанных с интерфейсом;
- использование типизации данных;
- учет точности и достоверности;
- порядок очередности арифметических, логических и функциональных операторов;
- отказ от использования функций и процедур с побочными эффектами;
- разделение присваивания и анализа;
- надлежащая работа с программными контрольно-измерительными приборами;
- управление размером библиотек класса;

- минимальное использование динамического связывания;
- контроль перегрузки оператора.

G.3.3.2 Максимизация структуры

Следует избегать в ППО оператора GOTO или подобных операторов управления выполнением, способных привести к неструктурированному переходу выполнения от одной ветви ППО на другую. Проблема безопасности заключается в трудности отслеживания и понимания поведения времени выполнения. Конструкции GOTO могут повлечь за собой нежелательные побочные эффекты, так как они прерывают выполнение определенного сегмента ППО, не гарантируя, что последующее за этим выполнение будет удовлетворять всем условиям, которые привели ко входу в этот сегмент. Стандарты, не рекомендующие или даже запрещающие подобные практики, использовались уже более двадцати лет. Максимизация структуры осуществляется удалением конструкций GOTO и использованием ППО с надлежащей блочной структурой. Конструкции case, if…then… else, do, until и do while позволяют ветвление с определенным возвращаемым значением и не приводят к неопределенности потока управления, которое связано с GOTO или подобными конструкциями.

G.3.3.3 Минимизация сложности потока управления

На сложность потока управления указывает число уровней вложения, предназначенных для выполнения ветвлений или циклов. Чрезмерная сложность затрудняет прогнозирование потока ППО и препятствует проверке и обслуживанию. Более специфичная проблема безопасности заключается в том, что поток управления может быть непредсказуемым в случаях, когда возникают непредвиденные комбинации параметров. Чрезмерного использования вложения можно, как правило, избежать через применение функций или подпрограмм вместо включаемых ветвлений. В качестве меры профилактики безопасности следует установить определенное ограничение на вложения, включив его в проект или руководство по организации программирования.

Таким образом, МЭК 61511 ограничивает слои архитектуры ППО до двух:

- типовые наборы;
- блокировки.

МЭК 61508-3 применим к программам ППО, обладающим числом уровней вложения, превышающим этот установленный предел.

G.3.3.4 Инициализация переменных перед использованием

Если переменные не инициализируются присвоением определенного значения в начале цикла выполнения программы, то это снижает уровень безопасности, так как эти переменные могут содержать «мусор» для своих значений (остаток от предыдущего использования данной области памяти). Предсказуемость выполнения требует установки в ячейки памяти, выделенные под данные процесса, известных значений перед тем, как к ним будет получен доступ (установка и использование). Определенный результат использования неизвестных начальных значений переменной зависит от того, как эта переменная используется в ППО. МЭК 61508-3 применим к ППО, использующим неинициализированные переменные.

G.3.3.5 Одна точка входа и одна точка выхода для подпрограмм

Множественные точки входа и выхода в подпрограммах вносят неопределенность в поток управления так же, как это делают конструкции GOTO.

Предсказуемость потока выполнения повышается при использовании одной точки входа и одной точки выхода в каждой программе ППО. Так как предсказуемость потока выполнения является характеристикой, важной для безопасности, то использование нескольких точек входа и выхода в подпрограммах или функциях является нежелательным, даже если это поддерживается в языке. МЭК 61508-3 применим к программам ППО, обладающим несколькими точками входа и выхода.

G.3.3.6 Минимизация неоднозначности интерфейса

Сбои, связанные с интерфейсом, включают несоответствия в списках аргументов при вызове других подпрограмм, в коммуникациях с другими задачами или в передачах сообщений между объектами. Примером такого сбоя может служить инвертирование порядка аргументов при вызове подпрограммы. Предыдущие исследования отказов ППО продемонстрировали, что эта категория сбоев является достаточно значимой. Методы прикладного программирования, позволяющие снизить или устранить вероятность сбоев интерфейса, включают:

- упорядочивание аргументов для чередования разных типов данных (уменьшение шансов того, что два смежных аргумента будут поставлены в неправильном порядке);
- использование именных обозначений вместо обозначений порядка или позиции для языков, поддерживающих подобную систему обозначения;
- тестирование для определения допустимости входных аргументов в начале подпрограммы.

Для стандартных программ должны быть установлены адекватные начальные и конечные условия. Начальное условие является гарантией того, что все локальные переменные инициализированы, а все входные переменные успешно прошли проверку на допустимость. Конечное условие гарантирует, что все выходные переменные успешно прошли проверку на допустимость.

G.3.3.7 Использование типизации данных (структуры данных)

Использование структур данных, которые отличаются от тех, что были предназначены для использования в ППО, может привести к отказам, а подобные отказы, возникающие во время исключительной ситуации, могут оказывать особенно пагубное влияние на безопасность. Эту проблему можно решить объявлением типов данных.

Изначально основным преимуществом объявления типов данных являлось то, что это позволяло подготовить правильный объем памяти. Тем не менее типизация данных полезна для улучшенного определения интерфейсов, повышения удобочитаемости (для проверок) и для проверок во время компиляции и функционирования. Эти применения, изначально являвшиеся дополнительными, теперь стали основной мотивацией для типизации данных и привели к использованию строгой типизации данных, для которой требуются дополнительные объявления (типов данных), как минимум те, что входят в допустимый диапазон. Проблемы безопасности, связанные с типизацией данных, включают:

- ограничение использования анонимных типов (например, общий целочисленный тип или тип с плавающей запятой, не ограниченные снизу или сверху) в языках со строгой типизацией;
- предотвращение чрезмерного сдерживания ограничений на типы данных для того, чтобы избежать генерации ложных исключений или сообщений об ошибках (это является проблемой в языках со строгой типизацией);
- уменьшение числа преобразований типов и устранение неявных или автоматических преобразований типов (например, в назначениях или операциях над указателями);
- отказ от использования смешанных операций. Если подобные операции необходимы, то их следует четко идентифицировать и описать при помощи визуально выделенных комментариев в ППО;
- обеспечение того, что выражения, связанные с арифметическим вычислением или операциями отношений, обладают одним типом данных или надлежащим набором типов данных, для которого трудности преобразования сведены к минимуму.

Ограничение на использование косвенных ссылок, например для индексов массива, указателей или объектов указательного типа на ситуации, в которых какие-либо другие обоснованные альтернативы отсутствуют, а также проведение подтверждения соответствия неявно адресуемых данных перед настройкой или использованием обеспечивают корректность оцениваемых мест в памяти. Сильно типизированные указатели, индексы массива и типы доступа уменьшают возможность ссылки на недопустимые места в памяти.

G.3.4 Учет точности и достоверности

G.3.4.1 Общие положения

Реализация ППО должна обеспечивать адекватную точность и адекватную достоверность для предназначенного приложения системы безопасности. Это применимо как к измерениям физических свойств, так и к любым арифметическим значениям с плавающей запятой в рамках ППО. Проблемы с безопасностью возникают, когда заявленная точность переменных с плавающей запятой не поддерживается анализом, в особенности, когда разница между большими значениями незначительна (например, при вычислении интенсивности изменения на основе разницы между текущими и предыдущими значениями, в вычислениях дисперсий или при выполнении операций фильтрации, таких как «скользящее среднее»).

G.3.4.2 Порядок очередности арифметических, логических и функциональных операторов

Произвольный порядок очередности арифметических, логических и других операций варьируется от языка к языку. Разработчики или рецензенты могут делать некорректные выводы об очередности. Поэтому следует использовать механизмы обеспечения четкого объявления порядка выполнения операций.

G.3.4.3 Отказ от использования функций или процедур с побочными эффектами

Побочный эффект — изменение любой переменной, не возвращенной той функцией, которая сохраняет значение переменной после своего завершения. Побочными эффектами являются изменения файлов, регистров аппаратного обеспечения и т. п. Примером подобного побочного эффекта может служить изменение глобальной переменной, не входящей в список параметров функции. Побочные эффекты могут повлечь за собой проблемы, связанные с незапланированными зависимостями, и могут вызывать появление программных ошибок, которые сложно обнаружить.

G.3.4.4 Разделение присваивания и анализа

Операторы присваивания должны быть отделены от выражений анализа. Разделение может нарушаться, когда подпрограммы используются как часть анализа. Например, функция фильтрации может использоваться скорее как часть анализа, чем просто значение датчика. С этим свойством связано минимальное использование глобальных переменных, рассматриваемое ниже.

G.3.4.5 Надлежащее применение вспомогательных функций прикладной программы

Инструментальные средства ППО собирают и выводят определенные значения внутреннего состояния ППО во время выполнения, а также позволяют разработчику проверять корректную реализацию определенных аспектов спецификации. Конкретные проблемы, связанные с безопасностью, в этом случае:

- минимизация нарушений функционирования. Вспомогательные функции, которые нарушают нормальный поток выполнения, являются нежелательными в приложениях безопасности. Например, чрезмерная «запись» или другие выходные операторы могут привести к выполнению значительной части библиотечного ППО, связанного с выходными значениями; менее навязчивым подходом может быть запись этих значений в ячейки внешней памяти, в которых они позже смогут подвергаться обработке. Это также может проявиться при записи данных в двоичном формате для автономной обработки формата (т. е. при преобразовании удобочитаемого для человека текста в цифровой вид). Чтобы минимизировать различия в поведении между нормальным функционированием и тестированием, может быть разумно сохранять определенные вспомогательные функции ППО в фактической окружающей среде;

- обеспечение «видимости» вспомогательных функций в выполняющемся ППО. Некоторые средства ППО изменяют файлы объекта (или выполняемые файлы), сгенерированные логическим решающим устройством, чтобы внести вспомогательные функции. Это, как правило, является недопустимым в системах безопасности, так как влияние подобных изменений в ППО нельзя увидеть, и невозможно оценить это влияние на выполнение;

- соответствие руководству по вспомогательным функциям ППО. Осуществление проверки упрощается (и тем самым повышается уровень безопасности), если практики использования вспомогательных функций описаны в технических журналах, рассматривающих конкретный проект. В таких руководствах должно определяться, какие типы выходных механизмов будут использоваться, а при каких условиях их использования стоит избегать. Например, меры, описанные выше, для минимизации вмешательств в выполнение ППО конфликтуют с атрибутами абстракции данных и ограничения последствий ошибки, описанных далее в настоящем приложении.

G.3.4.6 Управление размером библиотек классов

Управление размером библиотеки класса является важным для предотвращения трудностей управления системой и снижения производительности по причине слишком большого числа классов или объектов. Если руководящие указания для конкретного проекта ограничивают число классов и объектов, и реализуемое ППО следует этим указаниям, то уровень безопасности повышается.

G.3.4.7 Минимальное использование динамического связывания

Связывание указывает на привязку имени к классу. Динамическое связывание позволяет откладывать связь имени/класса до тех пор, пока во время выполнения не будет создан объект, обозначенный этим именем. Непредсказуемость связывания имени/класса создает проблемы. Она также снижает предсказуемость поведения при выполнении объектно-ориентированной программы и усложняет ее отладку, понимание и отслеживание. Для приложений, имеющих критическое значение для безопасности, желательно устанавливать ограничения на динамическое связывание или устранять их вообще. МЭК 61508-3 применим для ППО, использующего динамическое связывание.

G.3.4.8 Управление перегрузкой операторов

Полиморфизм (перегрузка операторов) может повысить считываемость и снизить сложность, если для различных типов данных позволить использовать отдельную подпрограмму или отдельного оператора или поведение отдельного объекта. Однако в этом случае могут возникнуть проблемы с предсказуемостью, так как не ясно, каким образом логическое решающее устройство будет назначать ППО для различных полиморфизмов (например, каким образом операция умножения в многомерном массиве будет привязана к блокам задания коэффициентов или к одномерным массивам).

Поэтому для приложений, связанных с безопасностью, желательно иметь указания по использованию средств перегрузки операторов в ориентированных на конкретный проект или в организационных инструкциях по применению стандартов прикладного программирования, вместе с верификацией того, что ППО соответствует настоящему стандарту.

G.3.5 Предсказуемость во времени

G.3.5.1 Общие положения

Предсказуемость во времени критически важна в используемой системе безопасности, управляемой в реальном масштабе времени. Базовые свойства, связанные с объектно-ориентированным программированием, имеющие отношение к этому промежуточному свойству и уже описанные выше, следующие:

- управление размером библиотек классов;
- минимизация использования динамического связывания;
- управление перегрузкой операторов.

Два дополнительных базовых свойства, связанных с временными характеристиками, рассматриваются в следующих подпунктах:

- минимальное разбиение на задачи;
- минимальное использование обработки, управляемой прерываниями.

G.3.5.2 Минимальное разбиение на задачи

Несмотря на то что разбиение на задачи представляет собой привлекательную модель для одновременной обработки, ее использование является нежелательным в приложениях, имеющих критическое значение для безопасности, по следующим причинам:

- последовательность выполнения является неопределенной, если несколько других вызванных альтернатив ожидает выполнения, так как не всегда ясно, какой из вызовов будет выбран;

- разбиение на задачи допускает критически опасные временные ошибки, такие как появление состояния гонки и взаимоблокировки. Такие ошибки сложно отладить.

Таким образом, в системах безопасности без надлежащего обоснования использования разбиения на задачи следует избегать.

G.3.5.3 Минимальное использование обработки, управляемой прерываниями

Обработка, управляемая прерываниями, которая предназначена для принятия и обработки входной информации от объекта и оператора, может снизить среднее время реакции, но, как правило, приводит к недетерминированному максимальному времени реакции. Обработка, управляемая прерываниями, была причастна по крайней мере к нескольким происшествиям.

В справочных документах и стандартах, связанных с цифровыми системами безопасности, как правило, не рекомендуется или запрещается использование такой обработки (см. МЭК 60880:2006). Отказ от использования обработки, управляемой прерываниями, упрощает анализ синхронизации и поведения при выполнении, а также предотвращает недетерминированный подход ко времени реакции, присущий обработке, управляемой прерываниями.

G.4 Предсказуемость математических или логических результатов

Предсказуемость математических или логических результатов означает, что рассматриваемые результаты, полученные при завершении выполнения нижнего уровня ППО, являются результатами, которые предположил и на которые рассчитывал программист, написавший это ППО. Понятие «логические» предназначено для расширения понятия «результаты» для случая, в котором ППО может манипулировать логическими данными и выдавать логический результат. Поэтому ППО системы безопасности должно быть строго статическим. МЭК 61508-3:2010 применим для ППО, использующего память на триггерах с явным или неявным управлением.

Интенсивное использование блокировок изменяет предсказуемость результатов и повышает сложность демонстрации независимости между структурами ППО. ФБ ПСБ не должны блокировать друг друга.

Применение таймеров должно быть ограничено, а также следует исключать их последовательное включение или взаимоблокировки.

G.5 Устойчивость

G.5.1 Общие положения

Устойчивость относится к способности ППО продолжать выполнение в условиях, отличающихся от нормальных, или в случае других непредусмотренных условий. Синонимом устойчивости является живучесть. Устойчивость является важным свойством системы безопасности, так как непредусмотренные события могут произойти во время происшествия или в результате отклонения параметров от их номинальных значений, но способность ППО продолжать контролировать систему и управлять ею в подобных обстоятельствах является жизненно важной.

Промежуточными свойствами для устойчивости являются:

- управление применением разнообразия;
- управление применением обработки исключений;
- проверка ввода и вывода.

G.5.2 Управление применением разнообразия

G.5.2.1 Общие положения

Решение использовать разнообразные реализации ППО принимается на уровне проектирования и тем самым выходит за рамки области применения настоящего руководства. Тем не менее, если в проекте или в требованиях предусмотрено разнообразие, то его применение необходимо контролировать. Принципиальной проблемой использования разнообразия в ППО является вероятность того, что отказы ППО по общей причине могут привести к тому, что резервные системы безопасности откажут таким образом, что работа функция безопасности будет нарушена.

Вероятность возникновения отказов по общей причине между подпрограммами ППО, разработанными независимо друг от друга, достаточно сложно устранить. Любая общая спецификация может повлечь за собой отказы по общей причине. Такая же проблема существует при разработке тестовых данных для проверки ППО — специалисты по тестированию могут опустить те же нештатные или необычные случаи, которые упустили разработчики. Более того, при использовании подхода, при котором выходы нескольких версий ППО можно сравнивать в реальном времени (или иметь возможность сравнивать промежуточные результаты), проекты независимых команд-разработчиков могут быть чрезмерно специфицированы. Такие подробные общие спецификации могут привести к малой степени разнообразия в проекте ППО. Это часто обнаруживается в корпоративных стандартах программирования.

Кроме того, различные версии ППО, написанные независимо по одной и той же спецификации требований, эффективно защищают только от ошибок прикладного программирования (и иногда только от ограниченного набора таких ошибок). С другой стороны, эмпирические данные показывают, что большинство проблем безопасности (и большинство ошибок, встречающихся в ППО) возникают из-за ошибок в требованиях ППО, в особенности связанных с неправильным пониманием того, как должно ППО выполнять свои функции. ППО, предназначенное обеспечить резервирование, может не достигнуть своей цели и просто повторить эти ошибки. При проверке критически важного для безопасности ППО для определения отказов по общей причине основным является анализ разнообразия ППО.

Существует два базовых свойства:

- управление внутренним разнообразием;
- управление внешним разнообразием.

G.5.2.2 Управление внутренним разнообразием

Если применяется только внутреннее разнообразие, то интерфейсы ко всем версиям должны быть идентичны. Другими словами, любые данные датчика или параметры, поступающие от вызывающих процедур, должны идентично передаваться всем версиям, а выходные данные из любых версий должны приниматься и использоваться другими частями системы. Тем не менее внутренние операции и хранилище локальных данных должны использовать разнообразие в многомодульных версиях или реализациях. Применение внутреннего разнообразия упрощает объектно-ориентированный подход, при котором используются одинаковые сообщения и методы,

но внутренние алгоритмы и представления данных отличаются. Внутреннее разнообразие должно реализовываться в соответствии с проектом и руководящими принципами, ориентированными на конкретный проект. При этом должны рассматриваться:

- разнообразные алгоритмы. Использование различных алгоритмов, преобразований единиц измерения и параметров процесса (если в этом появляется потребность или это разрешено требованиями или проектом) делает вероятность отказа, связанного с проектированием или реализацией, минимальной;
- разнообразные способы подтверждения соответствия данных. Использование альтернативных схем для подтверждения соответствия данных датчика (или другого входного устройства) и выходных данных делает вероятность отказа, связанного с реализацией инженера-разработчика, минимальной;
- разнообразные стандартные программы обработки исключений. Эта мера снижает вероятность того, что ошибка в обработке исключений или выполнении произойдет одновременно во множестве версий;
- различные типы данных, структуры и распределение памяти. Эта мера снижает вероятность того, что непредвиденное взаимодействие между объектом, сгенерированным ППО с помощью инструментального средства прикладного программирования и логическим решающим устройством приведет к непреднамеренному перезаписыванию данных или ППО одновременно в нескольких версиях;
- разнообразные библиотеки и стандартные подпрограммы. Отказ от использования одинаковых стандартных программ в ППО, библиотечных стандартных программ, предоставляемых компилятором, и интерфейсов прикладного программирования, предоставляемых логическим решающим устройством. Эта мера снижает вероятность одновременного отказа, связанного с дефектом в таких стандартных программах;
- разнообразный порядок арифметических операций. Изменение порядка арифметических операций в преобразованиях, арифметических операторах и операторах присваивания при помощи коммутативных, ассоциативных и дистрибутивных свойств снижает вероятность одновременных отказов, связанных с непредвиденными условиями переполнения, созданными промежуточными результатами или проблемами числовой точности;
- разнообразный порядок операций ввода и вывода. Выполнение операций ввода-вывода в разном порядке снижает вероятность одновременных отказов, связанных с синхронизацией (например, взаимных блокировок), или отказов, управляемых данными (т. е. аварийного завершения программы из-за определенного значения данных).

Разнообразие ограничено тем фактом, что для данной платформы все эти языки действительно являются разнообразным представлением одинаковых алгоритмов. Использование разнообразия языков, таким образом, только ослабляет недостатки каждого языка перед компиляцией. Поэтому ППО может быть написано на двух разных языках для сравнения его поведения.

G.5.2.3 Управление внешним разнообразием

Там, где используется внешнее разнообразие, уровень безопасности повышается, если оно реализовано строго в соответствии с проектной документацией. Проектная документация должна отражать необходимость в разнообразии, подтверждаемую требованиями, анализом опасностей и другими подобными источниками. Внешнее разнообразие достигается при помощи разных интерфейсов для версий, и оно может совмещаться с внутренним разнообразием. Внешнее разнообразие необходимо, когда для разных версий используются разные языки и может также использоваться для получения данных от датчика через разные каналы. Неуправляемое или не специфицированное внешнее разнообразие может привести к быстрому росту числа интерфейсов, которые сказываются на безопасности из-за сложности обслуживания, тестирования, верификации и подтверждения соответствия.

G.5.3 Управление обработкой исключений

G.5.3.1 Общие положения

Обработка исключений решает проблемы, связанные с нарушениями нормальных состояний систем и входных данных. Средства обработки исключений в некоторых языках упрощают установление альтернативного пути обработки события, условия которого хотя и являются непредвиденными, но приводят к состояниям, которые заранее можно определить и впоследствии обработать. Проблемы, возникающие при появлении и обработке исключений, часто трудно решить в процедуре самой обработки исключения.

Базовые принципы обработки исключений:

- обработка на нижнем уровне;
- сохранение контроля за исполнением программы;
- единообразная обработка исключений.

G.5.3.2 Локальная обработка исключений

Обработка исключений сразу на нескольких уровнях может привести к неточной интерпретации места возникновения исключения. Этот системный сбой можно предотвратить, устанавливая обработку исключений на нижнем уровне.

G.5.3.3 Сохранение контроля за исполнением программы

Прерывание потока управления, являющегося внешним по отношению к подпрограмме, в которой возникло исключение, создает неопределенность в выполнении, следующем за обработкой исключения. Безопасность повышается за счет поддержания потока управления внешнего по отношению к модулю, ответственному за исключение.

G.5.3.4 Единообразная обработка исключений

Отсутствие единообразной обработки исключений может привести к неодинаковой обработке идентичных исключений в разных частях ППО. В худшем случае это может привести к появлению необработанных исключений.

Этих проблем можно избежать с помощью руководства по работе с исключениями, являющегося частью методических процедур прикладного программирования организации или конкретного проекта. Темы, включенные в данное руководство, это:

- общие и зависящие от проекта исключения, которые были определены и предусмотрены;
- определение мест обработки исключений ППО;
- перечисление всех предусмотренных побочных эффектов и верификация отсутствия каких-либо других побочных эффектов;
- обеспечение целостности данных критического состояния во время обработки исключения.

Очень важно заранее определить критерии того, что обрабатывать в исключениях, а что включить в алгоритм обработки самой программы.

G.5.4 Проверка ввода и вывода

G.5.4.1 Общие положения

Искажение данных, вызванное временным отказом или недействительным результатом, может иметь серьезные последствия для последующей обработки, если позволить его распространение. Базовые свойства, связанные с проверкой ввода и вывода, минимизируют подобные последствия посредством ограничения распространения ошибки. Два базовых свойства, рассмотренных в G.5.4.2 и G.5.4.3, это:

- проверка данных ввода и
- проверка данных вывода.

G.5.4.2 Проверка данных ввода

Данные ввода включают данные от другой стандартной программы, данные из внешней среды и данные, хранящиеся в памяти, полученные на предыдущей итерации. Достоверность данных должна проверяться перед обработкой. Подобные проверки снижают вероятность распространения некорректных результатов или искаженных данных. Как минимум, значения входных данных должны проверяться на тип данных и нарушение допустимого диапазона. Если возможно, то следует также выполнять проверки логической непротиворечивости данных. ППО должно иметь средства для обнаружения некорректного ввода и перевода модуля в известное состояние (т. е. заданное по умолчанию или ранее обоснованные значения) в соответствии с проектом более высокого уровня.

G.5.4.3 Проверка данных вывода

Данные вывода — будь это вывод во внешнюю среду, в другую стандартную программу или хранение таких данных для использования в последующей итерации — должны проверяться на достоверность. Как минимум, эта проверка на достоверность должна гарантировать, что значения имеют надлежащий тип данных и не выходят за допустимые диапазоны. Желательно выполнять проверки логической непротиворечивости данных. Однако подобные проверки логической непротиворечивости данных не должны быть настолько ограничивающими, что они ошибочно отбрасывают корректные значения.

Согласно проекту ППО оно должно также содержать средства для обработки отброшенных выходных значений.

G.6 Прослеживаемость

G.6.1 Общие положения

Как было ранее определено в настоящем приложении, прослеживаемость связана со свойствами безопасности ППО, которые поддерживают верификацию корректности и полноты на основе сравнения с проектом ППО. Промежуточные свойства прослеживаемости это:

- удобочитаемость;
- управление использованием встроенных функций (см. G.6.2);
- управление использованием скомпилированных библиотек (см. G.6.3).

Так как удобочитаемость также является промежуточным свойством ремонтопригодности, то она рассматривается в G.3.4.8. Последние два свойства и их значимость для безопасности рассматриваются в G.6.2 и G.6.3.

G.6.2 Управление использованием встроенных функций

Почти все языки включают встроенные функции для часто используемых задач программирования, чтобы довести до максимума продуктивность программиста. Тем не менее ограничения на эти функции и то, как они обрабатывают исключения, могут быть менее изучены, чем у конструкций базового языка. Поэтому использование подобных функций поднимает вопрос обеспечения безопасности.

Проблемы использования встроенных функций могут быть решены с помощью организационных или ориентированных на проект руководств. Используя сценарии регрессионного тестирования, можно установить соответствие с ожидаемыми результатами новых версий компиляторов и библиотек программ этапа исполнения. Поэтому следует сохранять тестовые сценарии, процедуры и результаты предыдущего тестирования для возможных встроенных функций. Тестирование также должно оценить поведение для граничащих и выходящих за допустимые границы условий (например, отрицательные аргументы в стандартной программе вычисления квадратного корня, некорректно прерванные строки для функции копирования строки и т. п.) в конкретной среде выполнения.

G.6.3 Управление использованием скомпилированных библиотек

Скомпилированные библиотеки являются стандартными программами, написанными и скомпилированными кем-либо, кроме группы разработки. Приложения скомпилированных библиотек включают операции ввода/вывода,

драйверы устройств или математические операции, не определенные в стандартном языке. Такие библиотеки могут предоставляться поставщиками инструментальных средств прикладного программирования, третьей стороной или другими подразделениями организаций-разработчиков. Проблемы, связанные с подобными функциями, похожи на проблемы встроенных функций.

Проблемы использования скомпилированных библиотек можно решать с помощью управления использованием функциональных вызовов к подобным библиотекам, следуя организационным руководствам или руководствам, связанным с проектом.

Подобно встроенным функциям следует сохранять и поддерживать тестовые сценарии, процедуры и результаты тестирования. Тестовые сценарии должны оценивать поведение для нормальных, выходящих за границы и предельных условий в конкретной среде выполнения. Для каждой новой версии скомпилированной библиотеки следует проводить регрессионное тестирование.

G.7 Ремонтопригодность

G.7.1 Общие положения

Ремонтопригодность ППО снижает вероятность того, что при осуществлении изменений будут внесены ошибки. Промежуточные свойства, связанные с ремонтопригодностью и влияющие на безопасность, включают:

- удобочитаемость. Те свойства ППО, которые облегчают понимание ППО персоналом проекта;
- абстракцию данных. То, насколько ППО можно разделить на разделы и модули, чтобы минимизировать сопутствующее негативное влияние и вероятность непреднамеренных побочных эффектов, связанных с изменениями ППО;
- функциональную связность. Надлежащее распределение в ППО функций на уровне проектирования устройств, с которыми работает ППО (одна процедура; одна функция);
- гибкость. То, насколько потенциально изменяемые области изолируются от остальной части ППО;
- переносимость. Главной проблемой для безопасности, связанной с переносимостью, является исключение нестандартных функций языка.

G.7.2 Удобочитаемость

G.7.2.1 Общие положения

Удобочитаемость обеспечивает понимание ППО квалифицированным персоналом разработчиков, не связанным с написанием этого ППО. Важность удобочитаемости для ремонтопригодности была продемонстрирована в исследованиях, в ходе которых было установлено, что для обнаружения сбоев в прикладных программах ручное чтение ППО («отладка за столом») более эффективно, чем структурное или функциональное тестирование. Разумно предполагать, что удобочитаемость также повысит идентификацию ППО, которое требуется изменять во время внепланового или адаптивного обслуживания, а также снизит вероятность создания новых сбоев во время такого обслуживания.

Для удобочитаемости не существует общих стандартов, которые можно назвать обязательными или рекомендовать. Тем не менее для ПСБ предполагается использовать организационные или связанные с конкретным проектом инструкции по стилю и практикам прикладного программирования (или связанные с ними руководства). Следующие базовые свойства связаны с удобочитаемостью:

- соблюдение правил использования отступов;
- использование описательных имен идентификаторов;
- комментирование и внутренняя документация;
- ограничение размера подпрограмм;
- минимизация многоязыкового программирования;
- уменьшение неясных или труднонаходимых конструкций программирования;
- уменьшение разброса взаимосвязанных устройств;
- уменьшение использования литералов.

G.7.2.2 Соблюдение правил использования отступов

Соответствующее использование отступов упрощает идентификацию объявлений, потоков управления, невыполняемых комментариев и другие конструкции ППО. Правила использования отступов обычно являются частью организационного или зависящего от конкретного проекта стиля программирования или стандартов. Важные проблемы структурирования текста, для которых нужны практики добавления отступов, связаны с обработкой:

- блоков программирования (последовательностей операторов, ограниченных операторами begin и end);
- комментариев;
- разветвляющихся конструкций (например, if... then... else, case-операторов, циклов и т. п.);
- множественных уровней вложения (например, цикл do в цикле do);
- объявления переменных и подпрограмм;
- директив инструментальных средств прикладного программирования;
- использования и управления исключениями.

G.7.2.3 Использование описательных имен идентификаторов

Имена для переменных, процедур, функций, типов данных, констант, исключений, объектов, методов, маркировок и других идентификаторов, которые нелегко понять, могут задерживать проверку и обслуживание. Проблемы безопасности, связанные с практиками именования, могут быть смягчены, если определить требования,

чтобы имена были описательными, согласованными и прослеживаемыми к документам более высокого уровня (например, уровня проекта ППО). Соглашения о наименованиях являются важной частью инструкции по стилю и практикам прикладного программирования.

Примеры рассматриваемых проблем включают:

- идентификация входных данных на объекте (например, должна ли переменная ссылаться на датчик или же ей следует именоваться loop1_hot_leg_TC1);
- как должны именоваться переменные цикла (например, «i.j.k» или более длинные названия);
- локальное переименование идентификаторов (например, «среднее число обычных процедур» переименовано как «среднее»);
- различие между разными категориями идентификаторов (например, суффикс _T на всех типах данных, чтобы отличать их от переменных);
- списки связанных с проектом терминов и зарезервированных слов (например, ограничения на использование понятий «аварийный сигнал», «предельное значение» и т. д.).

Следует избегать использовать одно имя для разных целей, если преимущества этого неочевидны, а в случае использования следует сопровождать это имя четкими, постоянными и недвусмысленными пояснениями. Множественное использование одного имени может сбивать с толку. Дополнительные проблемы могут возникнуть, если язык поддерживает предварительно скомпилированные модули. Переменная с одним именем в двух разных пактах программ, один из которых использует другой, может быть интерпретирована инструментальными средствами прикладного программирования не так, как это предполагал тот, кто написал программу. В некоторых случаях программист мог пропустить объявление имени в пакте программ. При этом другой пакет может использовать другую переменную с таким же именем таким образом, каким ему предназначено ее использовать. Если эта определенная ветвь или путь выполнения не встречается часто, то возможно, что подобный сбой не будет обнаружен до тех пор, пока он не вызовет отказ выполнения программы.

Использование зарезервированных слов для идентификаторов, выбираемых пользователем (в языках, где эта функция разрешена), неприемлемо.

G.7.2.4 Комментирование и внутренняя документация

Неполные комментарии, несогласованные форматы и комментарии, которые не обновляются, не отражают текущее состояние ППО, затрудняют проверку и вызывают проблемы для безопасности. Подобные проблемы могут быть сведены к минимуму с помощью руководящих указаний из стандартов по организации или проектированию ППО, которые регламентируют комментарии и внутреннюю (для ППО) документацию. Примеры вопросов, которые при их включении должны быть освещены во введении, включают:

- цель подпрограммы или модуля и как ее достигнуть;
- функции и требования к показателям эффективности, а также внешние интерфейсы, которые подпрограмма или модуль помогают реализовать;
- другие вызываемые подпрограммы или модули и их взаимозависимости;
- использование глобальных и локальных переменных и, если они используются, то адреса размещения в памяти и регистрах вместе с конкретными инструкциями по обслуживанию;
- ответственное подразделение или группу по программированию;
- дату создания модуля;
- дату выпуска последней версии, номер версии, номер отчета о проблеме и название, связанное с версией, предполагаемое поведение при отказе и связанную с ним информацию для всех основных сегментов ППО;
- входы и выходы, включая файлы данных, на которые даются ссылки во время записи модуля выполнения;
- комментарии о цели, области применения и ограничениях для каждого аргумента (для подпрограмм с аргументами).

Аналогичные примеры для документации в рамках ППО включают:

- ссылку на проектную документацию более высокого уровня в комментариях, связанных с объявлениями типов данных, переменных и констант;
- цель и ожидаемые результаты в начале ветки проекта и программирования блоков;
- подробные строчные комментарии, объясняющие необычные конструкции и отклонения от практик программирования.

G.7.2.5 Ограничение размера подпрограммы

В некоторых документах рекомендуются определенные ограничения по размеру для каждой подпрограммы и модуля ППО. Например, в среднем рекомендуется около 100 нерасширяемых операторов и максимум более 200 таких утверждений. Проблемы, связанные с размером подпрограмм, послужили одним из мотивирующих фактором для освоения структурированного программирования. Маленькие подпрограммы (одна или две страницы) легче проверять, чем многостраничные. Тем не менее ограничения на допустимый размер также должны учитывать характер программ и языка. В системах безопасности и управления технологического процесса данное ППО должно постоянно обрабатывать большое количество принятых данных и объявлений данных (с требующимися комментариями), и эти данные сами по себе могут занимать более одной страницы. Таким образом, определяющим фактором для данного базового свойства является скорее предоставление руководства по размерам, чем использование какого-то общего числового предела.

G.7.2.6 Минимизация многоязыкового программирования

Многоязыковое программирование [например, «последовательностная функциональная схема», ступенчатая диаграмма для булевой логики и «функциональный блок» для более сложных функций (масштабирования, вычисления среднего значения и т. п.)] усложняет работу по проверке и обслуживанию и поэтому является проблемой для обеспечения безопасности. Если подобной практики невозможно избежать, то можно минимизировать сложности за счет размещения ППО на «иностранном» языке рядом с программой на основном используемом языке, с которой оно взаимодействует (например, директива инструментального средства прикладного программирования для сборки на конвейере в подпрограмме обработки ввода, связанной с прерыванием), для повышения удобочитаемости.

Если от такой практики невозможно отказаться, то можно минимизировать трудности за счет размещения ППО на «иностранном языке», встроив его в подпрограмму на основном используемом языке, с которой это ППО взаимодействует (например, структурированный текст, встроенный в функциональный блок, в диаграмме функциональных блоков), для повышения удобочитаемости.

G.7.2.7 Уменьшение неясных или труднонаходимых конструкций программирования

Неясные конструкции прикладного программирования можно в общем охарактеризовать как использующие косвенные методы для уменьшения объема прикладного программирования или обработки логическим решающим устройством, необходимых для достижения результата. Подобные практики прикладного программирования создают проблемы для проверки и обслуживания и поэтому являются проблемами для безопасности. Например, сдвиг целочисленной переменной влево равносилен удваиванию ее значения. Тем не менее предыдущая языковая конструкция была бы неясной, если бы для проекта требовалось удваивание значения (т. е. предпочтительнее было бы выполнить умножение); последняя конструкция была бы неясной, если бы для проекта требовалось смещение значения влево (т. е. предпочтительнее было бы выполнить операцию сдвига в ППО, а не умножением на 2). Надлежащее комментирование может минимизировать влияние неясных или ограниченно неясных изменений в прикладных программах (например, сложение значения с ним самим, чтобы удвоить его).

Инверсии фактических положений датчика или исполнительного устройства, выраженных в логических состояниях, посредством функций «NOT» (отрицание) следует избегать, также как и мультиплексирования булевых переменных на целочисленных выходах и выходах с регистром-защелкой.

G.7.2.8 Уменьшение разброса взаимосвязанных устройств

Если взаимосвязанные устройства ППО распределены по программе, то при проведении проверки и обслуживания необходимо обращаться к нескольким местам в листинге ППО. Тем не менее характер этого распределения зависит от языка. Например, некоторые языки позволяют иметь спецификации интерфейса отдельно от тела ППО; другие предусматривают «прототипирование» для похожей цели. В языках со строгой типизацией данных желательно объединить все объявления типов в одном файле (или наборе файлов); в объектно-ориентированных языках желательно разделить базовые классы и производные классы. Специальное для проекта руководство по распределению взаимосвязанных устройств в ППО упрощает процесс проверки и повышает безопасность.

G.7.2.9 Уменьшение использования литералов

Литералы (т. е. фактическое число или строка в ППО) гораздо сложнее идентифицировать, чем имена, которым в начале каждого модуля присваиваются постоянные значения. Литералы влияют на безопасность, так как они снижают удобочитаемость и усложняют процесс обслуживания, в частности, если литерал связан с параметром процесса, который может настраиваться, или с коэффициент пересчета, который может изменяться во время повторной калибровки прибора. Гораздо легче изменить один набор значений в начале файла, чем гарантировать, что все литералы, связанные с подобным параметром, были полностью и корректно изменены во всех значимых файлах.

G.7.3 Абстракция данных

G.7.3.1 Общие положения

Абстракция данных — это комбинация данных и допустимых операций с данными в одной сущности, а также установление интерфейса, который разрешает доступ, обработку и хранение данных только с помощью допустимых операций. Абстракция данных вносит важный вклад в безопасность посредством сокращения или устранения побочных эффектов из-за изменений переменных либо во время выполнения, либо в ходе деятельности по обслуживанию ППО. Этот подход связан со следующими конкретными базовыми свойствами:

- минимизация использования глобальных переменных;
- минимизация сложности допустимых операций, определяющих интерфейс.

G.7.3.2 Минимизация использования глобальных переменных

Желательно ограничивать использование глобальных переменных в программах, связанных с безопасностью, так как они связаны с возможными побочными эффектами. Если переменные задаются и используются в рамках одной подпрограммы, то удобочитаемость повышается. Эти переменные можно сделать доступными для других подпрограмм с помощью стандартных и управляемых интерфейсов, сводящих к минимуму вероятность непреднамеренных взаимодействий. По тем же причинам следует избегать или осуществлять контроль над зависимостями между хранимыми внутренними данными разных подпрограмм.

Чтобы избежать возможных проблем с безопасностью, локальные переменные в разных программах не должны разделять одну область в памяти.

Следует избегать использования глобальных переменных в ППО, которые могут быть записаны из более чем одного логического экземпляра, так как это связано с возможными побочными эффектами.

G.7.3.3 Минимизация сложности интерфейсов

Интерфейсы являются частой причиной отказов ППО. Сложные интерфейсы трудно проверять и поддерживать, поэтому они являются нежелательными в программах, связанных с безопасностью. Характеристики, которые влияют на сложность, это:

- большое количество аргументов, используемых в вызывающих подпрограммах;
- использование кратких выражений, когда применяются различные режимы или опции;
- недостаток легко воспринимаемых ограничений и предположений для использования допустимых операций.

G.7.4 Функциональная связность

G.7.4.1 Общие положения

Функциональная связность означает четко определенную согласованность между функциями ППО и структурой устройств, с которыми оно работает. Функциональная связность обладает одним базовым свойством.

G.7.4.2 Одноцелевое назначение функций и процедур

Если каждая процедура, подпрограмма или функция реализуют только одну задачу или преследует только одну цель, указанную в проекте ППО, то процесс проверки и обслуживания упрощается.

Подпрограммы, функции или процедуры, выполняющие несколько задач, должны быть разделены и написаны как отдельные функции. Простым способом протестировать функцию на одноцелевое назначение — это проверка того, можно ли описать функцию одним предложением в следующей форме:

«глагол + цель(цели)».

МЭК 61511 предполагает, что типовые наборы будут повторяться, а ФБ ПСБ будет реализована на одном логическом решающем устройстве.

G.7.4.3 Одноцелевые переменные

Этот принцип функций, обладающих одной целью, следует применять и к переменным. Переменная должная использоваться только для одной цели.

G.7.5 Гибкость

G.7.5.1 Общие положения

Гибкость — это способность ППО приспосабливаться к изменениям функциональных требований. Гибкость расширяет абстракцию данных, способствуя изоляции областей возможных изменений. Для реализации гибкого ППО необходимо идентифицировать, что предположительно будет постоянным, а что будет изменяться, и выделить то, что будет изменяться, в легко идентифицируемые области, которые могут быть изменены с минимумом побочных изменений. У гибкости есть одно базовое свойство.

G.7.5.2 Изоляция изменяемых функций

При изоляции функций, которые могут быть изменены, что предотвращает влияние изменений на другое ППО или данные, упрощается процесс проверки и обслуживания. Во многих случаях подобные функции связаны с аппаратными средствами, которые должны меняться при смене платформы, системы или в случае, когда используются новые устройства вместо старых устройств, например для установки более мощного логического решающего устройства из той же линейки изделий изготовителя.

В значительной степени изоляция изменяемых функций является проблемой проектирования, связанной с абстракцией данных. Поэтому более подробное рассмотрение выходит за рамки настоящего стандарта.

G.7.5.3 Переносимость

G.7.5.4 Общие положения

С точки зрения безопасности преимущества переносимости заключаются в приверженности стандартным конструкциям программирования, которые приводят к предсказуемым и надежным результатам на ряде разных рабочих платформ. Таким образом, ППО, которое используется повторно или преобразуется для работы на другой платформе, будет легче обслуживать. Свойства, связанные с переносимостью, которые рассматривались в другом подразделе, включают:

- минимизацию использования встроенных функций;
- минимизацию использования скомпилированных библиотек;
- минимизацию использования динамического связывания;
- минимизацию разбиения на задачи;
- минимизацию использования асинхронных конструкций (прерываний).

Единственное базовое свойство, связанное с переносимостью, это отказ от использования нестандартных или «улучшенных» конструкций, ориентированных на конкретное инструментальное средство прикладного программирования или на инструментальное средство прикладного программирования в комбинации с платформой выполнения кода.

G.7.5.5 Разграничение нестандартных конструкций

Там, где необходимы нестандартные конструкции, их следует четко идентифицировать вместе с обоснованием их использования, ограничениями и зависимостями от версий.

Приложение ДА
(справочное)

Сведения о соответствии ссылочного международного стандарта национальному стандарту

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 61511-1:2016	IDT	ГОСТ Р МЭК 61511-1—2018 «Безопасность функциональная. Приборные системы безопасности для технологических процессов в промышленности. Часть 1. Термины, определения и технические требования»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

УДК 62-783:614.8:331.454:006.354 ОКС 13.110 Т51

Ключевые слова: безопасность функциональная, жизненный цикл систем, электрические компоненты, электронные компоненты, программируемые электронные компоненты и системы, системы, связанные с безопасностью, планирование функциональной безопасности, программное обеспечение, уровень полноты безопасности

БЗ 11—2017/55

Редактор *Р.Г. Говердовская*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Половой*

Сдано в набор 13.09.2018. Подписано в печать 02.10.2018. Формат 60 × 84 $^1/_8$. Гарнитура Ариал.
Усл. печ. л. 18,60. Уч.-изд. л. 18,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
www.jurisizdat.ru gost.e-ecolog.ru

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

gost.e-ecolog.ru