УДК 65.014.12

ОСОБЕННОСТИ РАЗРАБОТКИ СИСТЕМЫ МЕНЕДЖМЕНТА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНЖИНИРИНГОВОЙ КОМПАНИИ-ИНТЕГРАТОРЕ

Ю.Д.Индык, И.А.Можаева, А.В.Струков (АО «СПИК СЗМА»)

Инжиниринговая компания-интегратор включает в сферу своей деятельности полный комплекс работ от подбора контрольно-измерительных приборов и разработки проектной документации, обоснования проектных решений до сборки, наладки и обслуживания автоматизированных систем управления.

Специалисты компании-интегратора проводят:

- обследование технологических процессов и систем автоматизации;
- определение факторов риска технологического процесса;
- разработка задания на проектирование автоматизированных систем управления технологическими процессами (АСУТП);
- разработка проектной документации в соответствии с постановлением Правительства РФ №87;
- обоснование экономической эффективности, надежности и функциональной безопасности проектных решений;
- разработка прикладного программного обеспечения (ППО) для программируемых логических контроллеров и систем SCADA;
- сборка, тестирование, шеф-монтаж и пусконаладка оборудования.

Самым важным вопросом при выполнении всех указанных работ является обеспечение безопасности в целом и функциональной безопасности в частности.

Для повышения эффективности бизнеса, правильного определения и постановки целей, обеспечения их достижения при помощи людей и ресурсов, координации и контроля деятельности подразделений в организациях разрабатываются различные системы менеджмента. Для инжиниринговых компаний-интеграторов, работающих в области автоматизации промышленных процессов, наиболее характерными являются система менеджмента качества (СМК) и система менеджмента функциональной безопасности (СМФБ).

Функциональная безопасность (ФБ) как часть общей безопасности при использовании промышленного оборудования под управлением АСУТП обусловлена и зависит от правильного функционирования всех средств снижения риска, в том числе и систем противоаварийной автоматической защиты (ПАЗ).

Работы в области обеспечения ФБ проводятся на основе реализации двух основных концепций – концепции жизненного цикла безопасности (ЖЦБ) и концепции уровня полноты безопасности (УПБ).

Важно понимать, что ЖЦБ рассматривается как некоторый технический подход, который позволяет на систематической основе спланировать, выполнить и проконтролировать качество действий, направленных на достижение требуемого УПБ.

За последние годы особую актуальность получили работы, связанные с риск-ориентированным подходом при проектировании и эксплуатации систем противоаварийной автоматической защиты (ПАЗ).

Актуальные требования Ростехнадзора к проектированию и эксплуатации средств контроля, управления и ПАЗ для опасных производственных объектов (ОПО) включают в себя обязательные требования по проведению анализа опасностей и риска, а также необходимость оценки назначенного и достигнутого УПБ. Данные требования могут быть выполнены на основе методического подхода, изложенного в международных стандартах серии ГОСТ Р МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью».

Серия стандартов МЭК 61508 включает в себя 7 частей, которые в сумме содержат около 600 страниц текста. Стандарты представляют собой *верхний уровень* целого семейства отраслевых стандартов (рис.1), которые детализируют требования к функциональной безопасности для систем контроля и управления атомных станций (МЭК 61513), оборудования (МЭК 62061), приборных систем безопасности для промышленных процессов (МЭК 61511), систем безопасности дорожных транспортных средств (ИСО 26262), систем, связанных с безопасностью зданий и сооружений (МЭК 53195) и т.д.

Первая редакция МЭК 61508 была разработана с 1998 по 2000 годы. В Российской Федерации первая редакция была принята в качестве государственного стандарта ГОСТ Р МЭК 61508 в 2007 году. В настоящее время в мире действует вторая редакция МЭК 61508, выпущенная в 2010. В Российской Федерации вторая редакция МЭК 61508 также является актуальной с 2012 года (ГОСТ Р МЭК 61508–2012).

Рисунок 1 – Стандарты серии «Функциональная безопасность»

Первые три части стандарта МЭК61508 имеют похожую структуру: раздел 5 описывает требования к документации, раздел 6 – к управлению ФБ, раздел 7 – к процедурам оценивания ФБ.

Основные цели менеджмента ФБ определены в стандарте МЭК 61508-1. Первая цель состоит в определении обязанностей в управлении ФБ для тех, кто несет ответственность

за системы, связанные с безопасностью, или за одну или более стадий ЖЦБ. Вторая цель – определение действий, выполняемых ответственными за управление ФБ.

Такие цели следуют из общего определения менеджмента как скоординированной деятельности по руководству и управлению организацией. В это же время менеджмент функциональной безопасности – это менеджмент применительно к процессам разработки и проектирования систем ПАЗ на основе риск-ориентированного подхода**.**

Для инжиниринговых компаний-интеграторов, работающих в области автоматизации промышленных процессов различных отраслей промышленности, включая химическую, нефтеперерабатывающую, нефтегазодобывающую, целлюлозно-бумажное производство, фармацевтику, пищевые продукты и неядерную энергетику, более детализированными и актуальными являются требования к управлению ФБ, изложенными в стандартах серии МЭК 61511. Раздел 5 «Управление функциональной безопасностью» данного стандарта определяет перечень действий, необходимых для достижения целей ФБ. Кроме того в разделе сформулированы требования к наличию как системы управления качеством, так и системы управления функциональной безопасностью:

«5.2.2 Любой поставщик изделий или услуг для организации, несущей общую ответственность за одну или более стадий полного жизненного цикла ПСБ, должен передавать изделия или услуги, как специально предназначенные для этой организации и иметь систему управления качеством. При этом следует установить процедуры, чтобы продемонстрировать адекватность такой системы.

Если поставщик делает какие-либо заявления о функциональной безопасности для своего изделия или услуги, которые используются организацией для демонстрации соответствия требованиям настоящего стандарта, то поставщик должен иметь систему управления функциональной безопасностью. При этом следует установить процедуры, чтобы продемонстрировать адекватность такой системы».

В идеале система менеджмента организации должна состоять из двух отдельных, но дополняющих друг друга систем: системы менеджмента качества и системы менеджмента функциональной безопасности. СМК и СМФБ должны соответствовать размеру, характеру и сложности деятельности организации в области обеспечения процессов проектирования, ввода в эксплуатацию и сопровождения систем ПАЗ.

Первым шагом при внедрении СМФБ в организации является разработка плана внедрения. Это должна быть реалистичная стратегия внедрения СМФБ, отвечающая потребностям организации и определяющая подход к управлению процессами ФБ.

Содержание плана включает:

- определение политики безопасности;
- описание компонентов СМФБ;
- формирование обязанностей сотрудников компании в области ФБ;
- определение политики отчетности по задачам ФБ;
- разработка методик измерения характеристик и показателей СМФБ;
- планирование программ обучения сотрудников компании.

Для обеспечения требуемого качества производственных процессов и произведенной продукции в качестве основного документа СМФБ разрабатывается стандарт предприятия (СТП) «Система менеджмента функциональной безопасности».

Целями разработки и внедрения указанного СТП являются

- обеспечение риск-ориентированного подхода к созданию систем ПАЗ;

- формирование единого порядка создания и модернизации систем ПАЗ, обеспечивающего взаимодействие участников работ на всех этапах жизненного цикла указанных систем;
- обеспечение непрерывной поддержки правильного функционирования систем ПАЗ технологических процессов за счет правильной организации работ по созданию и модернизации указанных систем.

В стандарте в рамках модели ЖЦБ описаны процессы жизненного цикла систем ПАЗ, их организация и обеспечение, планирование, оценка и аудит ФБ, подтверждение соответствия системы безопасности, управление изменениями и конфигурацией системы.

Стандарт «Система менеджмента функциональной безопасности» применяется совместно со следующими документами СМК.

- Программа улучшения качества продукции;
- Положение об СМК организации;
- Положение о документированной информации СМК;
- Положение о внутреннем аудите СМК;
- Положение о несоответствиях и корректирующих действиях;
- Положение об организации обучения;
- Производство проектной продукции;
- Внесение изменений в проектную документацию автоматизации технологических процессов взрывоопасных производств химической, нефтехимической, нефтеперерабатывающей промышленности и других объектов;
- Архив проектно-сметной документации.

Действия, относящиеся к управлению ФБ, применяются на соответствующих этапах жизненного цикла ПАЗ. При этом в рамках СМФБ разрабатываются документы (процедуры, рабочие инструкции, положения), реализуемые как на отдельных, так и на всех стадиях жизненного цикла ПАЗ.

На всех этапах ЖЦБ вместе с СТП «Система менеджмента функциональной безопасности» применяются следующие документы:

- план жизненного цикла ПАЗ;
- верификация безопасности;
- матрица компетентности и взаимозаменяемости;
- матрица распределения ответственности и мониторинга.

Для отдельных этапов и стадий ЖЦБ разрабатываются процедуры (рабочие инструкции, методики, руководства), которые обеспечивают быстрое и точное выполнение действий, относящихся к процессам ФБ.

В табл.1 приведен краткий перечень рабочих инструкций, разработанных в рамках СМФБ, для соответствующих этапов и стадий жизненного цикла ПАЗ.

Структура, формат и уровень детализации рабочих инструкций (РИ) соответствуют потребностям персонала компании и зависят от сложности выполняемых работ, применяемых методов, уровня подготовки, квалификации и навыков персонала. В РИ указывается последовательность выполнения операций, которая точно отражает установленные требования и соответствующую деятельность.

Таблица 1 – Документы СМФБ на этапах ЖЦБ

Этап ЖЦБ	Документы СМФБ	Разделы «Плана ЖЦ ПАЗ»
1. Анализ опасностей и рисков	СМК-РИ01-ФБ Проведение исследований опасностей и работоспособности объекта проектирования HAZOP	5.1
2. Распределение функций безопасности по слоям защиты	СМК-РИ02-ФБ Проведение анализа риска и распределение функций безопасности по слоям защиты (LOPA)	5.2
3. Спецификация требований безопасности к СПАЗ	СМК-РИ03-ФБ Разработка спецификации требования безопасности (СТБ) к ПАЗ	5.3
4. Проектирование и разработка СПАЗ	СМК-РИ05-ФБ Процедура верификации УПБ	5.4
5. Установка, ввод в действие и подтверждение соответствия	СМК-РИ04-ФБ Оценка функциональной безопасности	5.5

Рабочая инструкция «Проведение исследований опасностей и работоспособности объекта проектирования» определяет порядок проведения исследований опасностей и работоспособности объекта (HAZOP) специалистами компании, проводимых с целью выявления опасностей и последствий их реализации, принятых мер защиты, определения тяжести последствий и оценки вероятности по матрице оценки рисков, а также для формирования рекомендаций в случае среднего или высокого риска.

Особое внимание уделяется вопросам организационно-технического обеспечения риск-сессий, формированию рабочей группы исследования, оборудованию помещения для проведения заседаний групп, описывается пример матрицы оценки риска.

В приложениях РИ приводятся шаблоны проверочных листов этапа сбора исходных данных и разработки Технического задания, подготовки и проведение риск-сессий и отчета HAZOP.

РИ «Проведение анализа слоев защиты (АСЗ/LOPA)» устанавливает порядок анализа слоев защиты объекта – АСЗ (англ. LOPA – Layer Of Protection Analysis procedure) с целью определения уровней полноты безопасности (УПБ) функций безопасности, реализуемых в ПАЗ. Основными задачами исследования является определение достаточности контуров безопасности ПАЗ и установление требований по надежности выполнения функций безопасности к отдельным контурам безопасности ПАЗ.

РИ подробно описывает методологию определения требуемых уровней полноты безопасности, обращая внимание на связь с результатами процедуры HAZOP, обеспечение независимости различных слоев защиты.

В приложениях приведены формы документов, используемых в процессе проведения анализа слоев защиты, примеры их оформления, количественные характеристики основных инициирующих опасных событий.

Основным документом в процессе проектирования систем ПАЗ, разрабатываемым на основе результатов анализа риска и с учетом технического задания Заказчика на создание АСУТП, является спецификация требований безопасности (СТБ).

Рабочая инструкция включает все требования к ПАЗ, содержащиеся в разделах 10 и 11 стандарта ГОСТ Р МЭК 61511-1–2018, и описывают последовательность документирования информации для формирования спецификации требований безопасности.

Структура документа включает в себя три группы требований:

- общие требования к ПАЗ;
- общие требования к функциям безопасности ПАЗ;

- специальные требования к функциям безопасности ПАЗ.

Целью такой структуры является обеспечение минимального количества повторяющейся или противоречивой информации путем фиксации детальных требований к проектированию, которые применяются к системе ПАЗ в целом и требований, которые применяются к каждой конкретной функции безопасности.

Согласно концепции ЖЦБ после определенных этапов необходимо осуществлять оценку полноты и корректности выполнения определенных действий по достижению каждой функцией безопасности ПАЗ необходимой функциональной безопасности и уровня полноты безопасности. Данная процедура называется оценкой функциональной безопасности (ОФБ).

Оценка функциональной безопасности – это исследование, основанное на фактах, выполняемое по утвержденной в установленном порядке методике, предназначенное для определения значения полноты безопасности связанных с безопасностью систем и средств, обеспечивающих выполнение заданной функции или функций безопасности.

Согласно ГОСТ Р МЭК 61511-1–2018 действия по ОФБ должны быть выполнены на определенных стадиях ЖЦБ (рис.2).

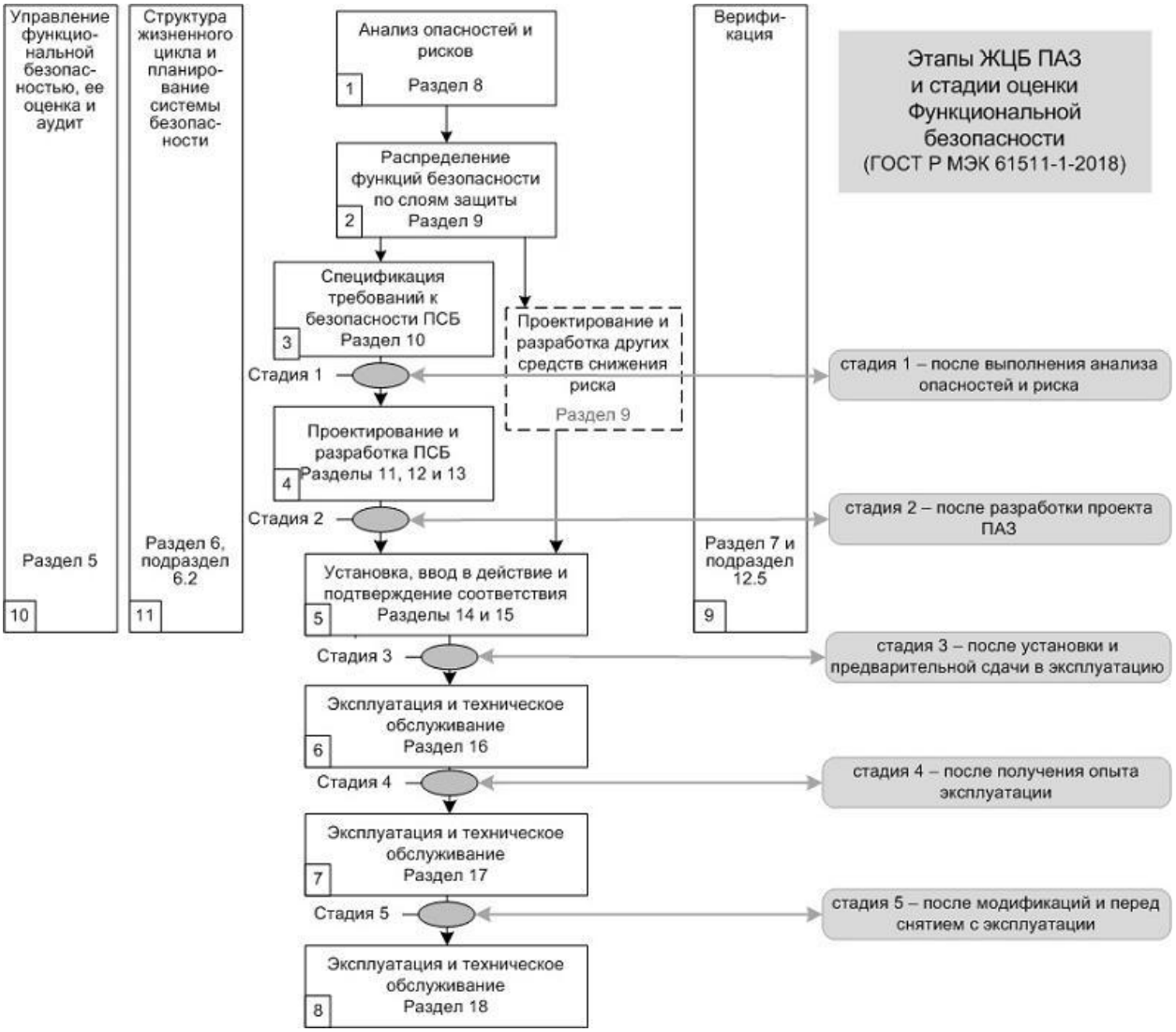

Рисунок 2 – Этапы жизненного цикла безопасности и стадии оценки функциональной безопасности

В рамках разработки СМФБ компании разработана РИ «Оценка функциональной безопасности».

Настоящая рабочая инструкция предназначена для проведения оценки функциональной безопасности системы ПАЗ. Процедура применяется на трех стадиях жизненного цикла ПАЗ (рис.2):

- стадия 1 – после этапов 1-3 («Анализ опасностей и риска», «Распределение функций безопасности по слоям защиты» и «Спецификация требований к безопасности ПАЗ»);
- стадия 2 – после этапа 4 «Проектирование и разработка ПАЗ»;
- стадия 3 – после этапа «Установка, ввод в действие и подтверждение соответствия».

РИ применяется со следующими документами СМК:

- СМК-СТП01 «Производство проектной продукции»;
- СМК-СТП02 «Производство инжиниринговых услуг»;
- СМК-СТП03 «Производство программной продукции»;
- СМК-СТП04 «Метрики для оценивания продукции и процессов»;
- СМК-СТП08 «Управление ресурсами»;
- СМК-СТП12 «Исходные данные для проектирования».

На стадии 1 после этапов 1, 2 и 3 ОФБ должна подтвердить, что анализ опасностей и рисков проведен полностью и правильно, а спецификация требований безопасности к ПАЗ содержит требования, достаточные для проектирования ПАЗ.

На стадии 2 после этапа 4 «Проектирование и разработка ПСБ» ОФБ обычно выполняется в форме отчета о выполнении в проектной документации требований ТЗ и СТБ. Кроме того отчет содержит результаты проектной оценки надежности контуров ПАЗ с подтверждением достигнутого уровня полноты безопасности.

На стадии 3 после этапа 5 «Установка, ввод в действие и подтверждение соответствия» ОФБ подтверждает, что все проверки соответствия ПАЗ требованиям к безопасности с точки зрения функций автоматической защиты и необходимого уровня эксплуатационной безопасности выполнены полностью, протоколы испытаний контуров ПАЗ утверждены.

Кроме того, РИ «Оценка функциональной безопасности» описывает процедуры аудита функциональной безопасности, их периодичность, планирование и отчетность.

В некоторых случаях разработка СМФБ выполнялась в форме коррекции документов СМК, куда вносились добавления, относящиеся к процессам обеспечения функциональной безопасности на этапах проектирования и оказания инжиниринговых услуг.

В первую очередь были внесены изменения в основополагающий документ «Положение об СМК». Изменения указывали, что «…Действие системы менеджмента качества (СМК), описанной в настоящем Положении, распространяется на разработку, проектирование, производство, поставку, шеф-монтаж, пусконаладку и сервисное обслуживание программно-технических комплексов автоматизированных систем управления и противоаварийной автоматической защиты (ПАЗ) на основе риск-ориентированного подхода; разработку и сопровождение программных средств анализа надежности; проведение работ по анализу опасностей и работоспособности (HAZOP); оказание образовательных услуг и услуг в области менеджмента функциональной безопасности (ФБ)…».

Также изменения вносились, например, такие документы, как СТП «Управление ресурсами», в «Положение об организации обучения», где разработан и внесен подраздел «Обучение и проверка знаний по функциональной безопасности». Эти изменения направлены на выполнение требований стандарта ГОСТ Р МЭК 61508-1 к разработке процедур, которые гарантируют, что все специалисты компании, участвующие в жизненном цикле безопасности, будут иметь соответствующую компетентность, т.е. они должны пройти обучение, обладать техническими знаниями, опытом и квалификацией. В соответствии с этим разработаны учебные программы курсов повышения квалификации, направленные на приобретение обучаемыми умения работы с нормативными документами СМК и СМФБ, практических навыков реализации нормативных требований в повседневной деятельности.

Для конкретизации действий сотрудников компании при реализации текущего проекта по созданию системы ПАЗ составляется документ «План жизненного цикла ПАЗ», шаблон которого также входит в состав документов СМФБ.

Данный документ представляет собой руководство по выполнению проекта, которое обеспечивает и документирует планирование и реализацию процессов в соответствии с требованиями стандартов на каждом этапе проекта. В документе представлены работы, зоны ответственности и документы, которые должны отвечать требованиям стандарта ГОСТ Р МЭК 61511-1–2018, включая требуемые шаги по проверке (верификации) и валидации ПАЗ, а также необходимые действия по ОФБ ПАЗ.

После завершения отдельных этапов жизненного цикла «План жизненного цикла ПАЗ» дополняется номерами соответствующих документов. Это позволяет контролировать соблюдение требований стандартов, СТБ и технического задания на проектирование ПАЗ.

Для оценивания ФБ в ходе выполнения работ по текущему проекту проводятся периодические аудиты функциональной безопасности. Эти аудиты могут быть как внутренними, так и внешними. Внутренние аудиты проводятся в соответствии с Положением о внутреннем аудите СМК компании и требованиями раздела 5 стандарта МЭК 61511-1–2018. Целями аудита являются проверка информационных документов и записей для подтверждения наличия системы менеджмента функциональной безопасности, ее соответствия современным требованиям и строгого ее выполнения.

Результаты аудита также определяют направления постоянного улучшения как СМК, так и СМФБ. При этом дальнейшая интеграция в СМК требований стандартов в области функциональной безопасности является одним из условий и инструментов улучшения системы менеджмента качества организации. Построение интегрированных систем менеджмента позволяет обеспечить большую согласованность действий персонала внутри компании, минимизировать функциональную разобщенность, содействовать более высокой степени вовлечение персонала в процессы улучшения деятельности организации.