УДК 51-74

СИСТЕМЫ МЕНЕДЖМЕНТА РИСКА И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНЖИНИРИНГОВОЙ КОМПАНИИ-ИНТЕГРАТОРЕ

Ю.Д. Индык, И.А. Можаева, А.В. Струков (ООО "СПИК СЗМА")

Система менеджмента функциональной безопасности (СМФБ) – это система управления процессами обеспечения функциональной безопасности (ФБ) в организации. Инжиниринговая компания ООО "СПИК СЗМА" является интегратором систем автоматизации промышленных процессов и 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. Особенностью современного этапа развития инжиниринговых компаний является внедрение риск-ориентированного подхода к процессам автоматизации промышленных объектов, наличие персонала, имеющего практический опыт реализации процедур анализа риска.

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 функциональной безопасности (СМФБ) и система менеджмента качества (СМК) [1].

ГОСТ Р ИСО 9001-2015 "Системы менеджмента качества. Требования" использует процессный подход и понятия "риск" и "риск-ориентированное мышление" по отношению к процессам разработки, внедрения и улучшения системы менеджмента качества организации. Процессный подход включает в себя систематическое определение и менеджмент процессов и их взаимодействия для наиболее эффективного достижения целей компании.

Понятие "риск" рассматривается как влияние неопределенности на результаты деятельности компании, а риск-ориентированное мышление не только позволяет определить факторы, которые могут вызвать отклонение результатов от запланированных, но и разработать средства и методы для их минимизации [2]. Управление рисками в менеджменте качества решает задачу обеспечения конкурентоспособности и выживаемости компании.

Стандарт ИСО 9001 не содержит требования к построению полноценной модели риск-менеджмента, но подразумевает наличие "мышления, основанного на рисках" в целом ряде элементов модели системы менеджмента качества.

Различные части системы менеджмента организации, включая СМК, СМФБ, систему менеджмента информационной безопасности, могут быть интегрированы в единую систему менеджмента. В то же время, эффективность системы менеджмента организации в существенной степени зависит от степени интеграции СМФБ и модели риск-менеджмента в структуру СМК.

На рис.1 условно показана взаимосвязь СМК и СМФБ.

Рисунок 1 – Системы менеджмента качества и функциональной безопасности

Компания-интегратор систем автоматизации промышленных процессов рассматривает понятие риска в свете требований регулятора: "Разработка …средств контроля, управления и противоаварийной зашиты (далее – ПАЗ) должны быть обоснованы в проектной документации, документации на техническое перевооружение результатами анализа опасностей технологических процессов… с использованием методов анализа риска аварий на опасных производственных объектах…" [3].

Выполнение требований регулятора, связанных с риск-ориентированным подходом в обеспечении промышленной безопасности, при использовании систем ПАЗ относится к области функциональной безопасности. Функциональная безопасность, 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 ПАЗ.

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, изложенные в стандартах серии МЭК 61511 [4].

Раздел 5 стандарта МЭК 61511-1 "Управление функциональной безопасностью" определяет перечень действий, необходимых для достижения целей ФБ.

Требования к СМФБ охватывают следующие действия, которые необходимы для достижения целевых показателей функциональной безопасности (рис.2):

- организация и ресурсы;
- оценка и управление рисками;
- планирование системы ФБ;
- реализация и мониторинг;
- оценка, аудит и проверки;
- управление конфигурацией ПАЗ.

Рисунок 2 – Действия в СМФБ

Конкретизация требований к указанным действиям оформляется в таких документах, как "Стандарт предприятия. Система менеджмента функциональной безопасности" и "Политика в области функциональной безопасности".

Политику и стратегию обеспечения безопасности необходимо определять с методами их достижимости, учитывая, что в рамках СМК компании разработаны и действуют такие документы, как "Матрица компетентности и взаимозаменяемости", которая определяет служебные обязанности сотрудников компании, в том числе и в процессах, связанных с обеспечением функциональной безопасности, и "Матрица компетенции и мониторинга", определяющая обязанности сотрудников компании в конкретном проекте.

Управление компетенциями является весьма важным направлением в деятельности компании и обеспечивается, например, функционированием учебного центра. Организация образовательного процесса и режим функционирования определяется в СМК в "Положении об образовательном подразделении".

Конкретные позиции при рассмотрении компетенций персонала описываются в соответствующих рабочих инструкциях. В общем виде требования к компетенциям персонала на различных этапах и стадиях жизненного цикла ПАЗ определяются, например, в рабочей инструкции "Оценка функциональной безопасности".

Рабочая инструкция "Оценка функциональной безопасности" определяет требования к планированию процедур оценки функциональной безопасности (ОФБ) и к компетенциям персонала на различных стадиях ОФБ. Для проектной организации одной из важнейших стадий ОФБ является стадия 1, которая реализуется после выполнения процедур анализа опасностей и риска и назначения уровней полноты безопасности (этапы 1 и 2 жизненного цикла безопасности) и составления спецификации требований к безопасности ПАЗ (этап 3). На этой стадии обеспечивается и проверяется полнота учета требований к рабочим характеристикам ПАЗ, которые обеспечивают достижение заданных показателей качества функционирования ПАЗ, в том числе и показателей функциональной безопасности. Для проведения процедуры ОФБ на стадии 1 жизненного цикла безопасности при необходимости может быть назначена команда специалистов, способная провести техническую, прикладную и эксплуатационную экспертизу, необходимую для конкретного проекта. Эта команда специалистов должна провести анализ работы, выполненной на всех этапах жизненного цикла ПАЗ до оцениваемой стадии.

Для выполнения работ на стадии 1 (анализ опасностей и рисков) разрабатывается рабочая инструкция "Проведение исследований опасностей и работоспособности объекта проектирования", основными разделами которой являются:

- планирование исследования;
- организационно-техническое обеспечение;
- правила проведения (методология) HAZOP на этапе проектирования;
- правила проведения (методология) HAZOP на действующей АСУТП;
- требования к отчету.

Информация, полученная в результате реализации процедуры исследований опасностей и работоспособности объекта проектирования, является входной для процедур определения требуемых уровней полноты безопасности. В зависимости от характера имеющейся к началу второго этапа жизненного цикла ПАЗ информации, разрабатываются рабочие инструкции "Метод анализа слоев защиты" или "Методы, основанные на графе рисков".

Особенностью рабочей инструкции "Метод анализа слоев защиты" является наличие приложений, содержащих большой объем справочной информации о частотах появления исходных причин опасных событий, о влиянии человеческого фактора на развитие аварии, описание видов и частот отказов оборудования. В качестве источников для такой информации могут быть использованы документы Ростехнадзора (Руководства по безопасности, материалы сайта Ростехнадзора "Уроки, извлеченные из аварий"), Приказы МЧС, стандарты и справочники.

Рабочая инструкция "Методы, основанные на графе рисков" описывает, в частности, порядок калибровки графа риска с использованием расчетных значений уровней допустимого риска по категориям "Жизнь и здоровье персонала", "Материальные потери" и "Окружающая среда". В отличие от традиционной матрицы риска, граф риска позволяет при оценке временных характеристик опасных событий учитывать влияние условных модификаторов, таких, например, как продолжительность действия риска, коэффициент занятости, вероятность возгорания, коэффициент уязвимости.

Основным требованием стандарта МЭК 61511 является требование проектирования систем ПАЗ в соответствии со спецификацией требований к ПАЗ. Наряду с техническим заданием на создание АСУТП, документ "Спецификация требований к системе ПАЗ", разработанный на основе соответствующей рабочей инструкции, определяет все требования, необходимые для проектирования ПАЗ, в том числе и требования, связанные с реализацией риск-ориентированного подхода. Структура документа включает в себя три основных группы требований:

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

Общие требования к ПАЗ включают описание действий для обнаружения и парирования отказов элементов подсистемы сенсоров, отказов ПЛК и конечных элементов. К общим требованиям относятся требования к интерфейсам инженерных станций и станций операторов, требования к шкафам ПАЗ, электропитанию и заземлению.

Общие требования к функциям безопасности ПАЗ определяют режим работы (например, по запросу с низкой интенсивностью запросов), с отключением или подачей питания, описываются схемы структурной избыточности и алгоритмы их возможной деградации, а также программные байпасы обслуживания датчиков.

Основой для формирования общих и специальных требований к функциям безопасности ПАЗ являются 29 требований к безопасности ПАЗ, приведенных в разделе 10 стандарта МЭК 61511-1.

Одним из важнейших документов в структуре СМФБ компании-интегратора является рабочая инструкция "Процедура верификации уровня полноты безопасности".

В общем виде процедура верификации контура ПАЗ включает в себя следующие шаги:

1 Формирование (подготовка) исходных данных, необходимых для расчета вероятности отказа на запрос.

2 Расчет по формулам стандарта ГОСТ Р МЭК 61508-6 в специальных программных приложениях вероятностей отказа на запрос элементов системы с архитектурой 1oo1 и 1oo2D.

3 Расчет вероятности отказа на запрос системы путем построения логических моделей в виде дерева неисправностей или структурной схемы надежности системы безопасности и моделирования надежности системы безопасности с учетом особенностей построения голосующих групп с учетом отказов по общим причинам.

Логический подход, как отмечено в стандарте МЭК 61508-6, использует логические функции (модели), которые связывают отказы отдельных компонентов с общим отказом системы. Для корректного использования коммерческих программных продуктов следует отделить графическое представление системы ПАЗ от вычислений показателей функциональной безопасности отдельных компонентов. Данные вычисления следует осуществлять на основе моделей Маркова, упрощенные выражения для которых приведены стандарте МЭК 61508-6 [5].

Основой для верификации контуров ПАЗ служит приближенная (удобная для инженерной практики) формула для расчета показателя функциональной безопасности *PFDavg* простейшей структуры 1oo1 (компонент без резервирования)

$$PFD_{avg\ 1oo1} = \lambda_{du}\left(\frac{TI}{2} + MTTR\right) + \lambda_{dd} \cdot MRT \approx \frac{\lambda_{du}}{2} TI, \qquad (1)$$

где λ_{du}, λ_{dd} – интенсивность опасных необнаруженных и опасных обнаруженных отказов соответственно;

TI – интервал межконтрольных проверок;

MTTR, MRT – среднее время восстановления и ремонта соответственно.

Стандарт МЭК 61508-6 приводит в той или иной степени приближения упрощенные формулы для расчета показателей функциональной безопасности для ограниченного числа архитектур: 1oo1, 1oo2, 1oo2D, 2oo2, 2oo3 и 2oo3. Реальная инженерная практика может использовать значительно более разнообразные архитектурные решения.

Рабочая инструкция "Процедура верификации уровня полноты безопасности" содержит описание универсальной методики для расчета надежности контуров ПАЗ с использованием аттестованного в Ростехнадзоре программного средства ПК АРБИТР.

Программное средство ПК АРБИТР также позволяет осуществить анализ возможных действий для достижения заданного уровня полноты безопасности в случае не подтверждения заданных характеристик.

Во-первых, программа проводит анализ чувствительности и расчет показателей значимости всех элементов контура безопасности с учетом отказов по общей причине. Таким образом, определяется вклад каждого элемента контура в формулу расчета показателя функциональной безопасности. Во-вторых, оценивается влияние возможных мер усовершенствования на выявленные критические компоненты. К возможным мерам относятся мероприятия по снижению влияния отказов по общим причинам, введение избыточных структурных элементов, сокращение периода межконтрольных проверок, проводимых с целью обнаружения и устранения опасных скрытых отказов.

В качестве примера рассмотрим задачу подтверждения заданного уровня полноты безопасности, приведенную в п.В.3.2.4 стандарта МЭК 61508-6.

Анализируется функция безопасности, для которой задан уровень полноты безопасности УПБ2. Вариант архитектуры всей системы включает одну группу из трех аналоговых датчиков давления с архитектурой 2oo3 на выходе. Логическая подсистема рассматриваемой системы представляет собой программируемую электронную систему с избыточной архитектурой 1oo2D и управляет одним закрывающим и одним дренажным клапанами. Для обеспечения функции

безопасности необходима работа как закрывающего, так и дренажного клапана. Межконтрольный интервал равен одному году. Архитектура всей системы безопасности представлена на рис.3.

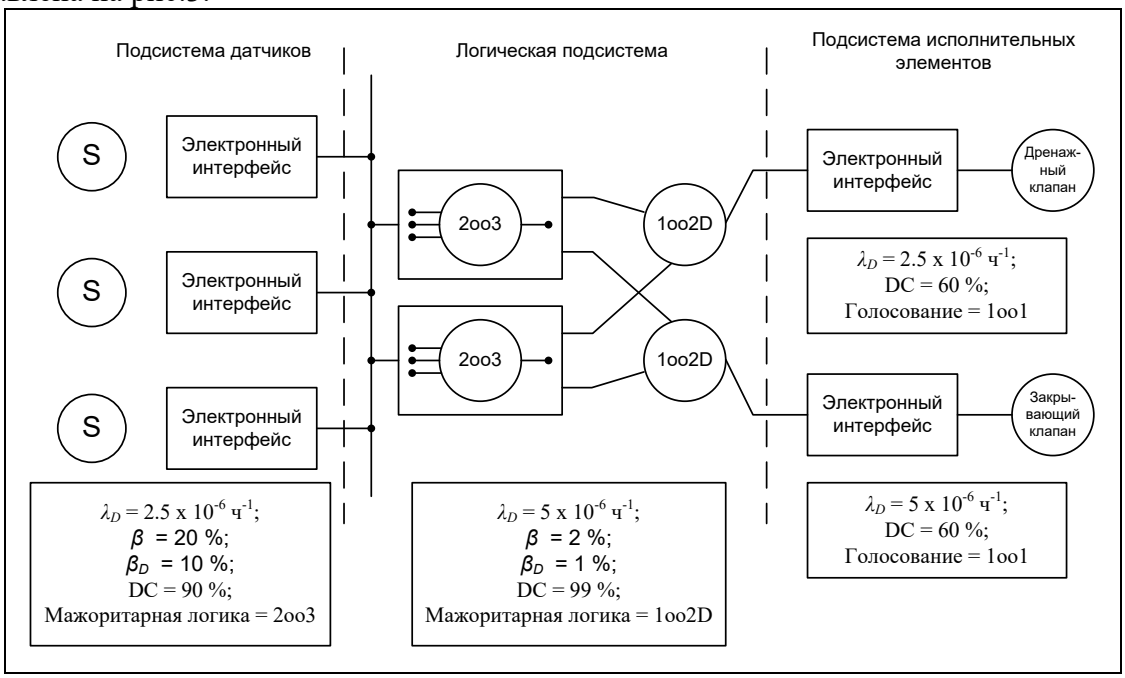

Рисунок 3 – Архитектура примера анализа контура безопасности

В примере рассматривается режим с низкой интенсивностью запросов, поэтому в качестве целевой меры отказов для функции безопасности рассчитывается средняя вероятность отказа на запрос *PFDavg*. Исходные данные для расчета показателя *PFDavg* приведены в прямоугольниках под соответствующими элементами схемы.

Расчетная схема в программной среде ПК АРБИТР приведена на рис.4.

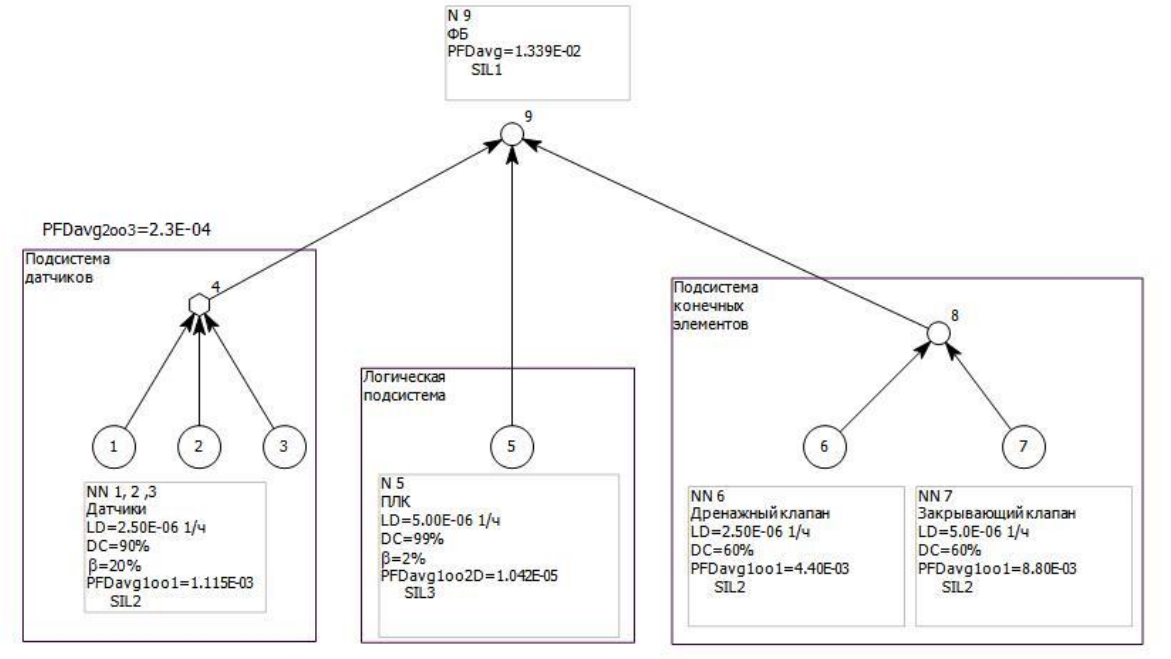

Рисунок 4 – Расчетная схема в программной среде ПК АРБИТР

Показатели $PFDavg_{1oo1}$ для датчиков и конечных элементов рассчитывались по формуле (1). Значение показателя $PFDavg_{2oo3}$=2.3E–04 для подсистемы датчиков с архитектурой 2oo3 с учетом бета модели отказов по общим причинам (β=20%) получено методом структурно-логического моделирования в программной среде ПК АРБИТР. Это значение совпадает со значением показателя, рассчитанного с помощью формулы, приведенной в разделе В.3.2.2.5 стандарта МЭК 61508-6.

Значение показателя $PFDavg_{1oo2D}$=1.04E–05 для логической подсистемы рассчитано по формуле раздела В.3.2.2.4 стандарта МЭК 61508-6.

Значение показателя $PFDavg_{2oo2}$=4.40E–03+8.80E–03=1.32E–02 рассчитано согласно указаниям раздела В.2.2.3 стандарта МЭК 61508-6.

Для всей функции безопасности показатель *PFDavg* согласно указаниям раздела 3.2 стандарта МЭК 61508 рассчитывается, как алгебраическая сумма показателей всех трех подсистем *PFDavgsys*=2.3E–04+1.04E–05+1.32E–02=1.3E–02.

Структурно-логическое моделирование в программной среде ПК АРБИТР дает результат 1.345E–02, что сравнимо с результатом раздела 3.2.4 стандарта МЭК 61508.

При анализе значимостей элементов схемы выявлено, что наибольший отрицательный вклад в значение показателя *PFDavgsys* вносит элемент №7 – закрывающий клапан.

На рис.5 приведен график отрицательных вкладов элементов схемы, полученный в программной среде ПК АРБИТР.

Рисунок 5 – Диаграмма отрицательных вкладов примера В.2.3.4

Так как полученное значение показателя *PFDavgsys*=1.3E-02 соответствует уровню полноты безопасности 1, то следует выбрать и осуществить подходящие меры усовершенствования контура ПАЗ относительно элемента №7 (закрывающий клапан): замена на более надежный элемент, дублирование клапана или уменьшение межконтрольного интервала.

Относительно приведенного примера следует добавить, что проведенные в компании исследования показали, что использование структурно-логического подхода для оценки надежности сложных контуров ПАЗ обеспечивает получение завышенной, то есть гарантированной оценки показателей функциональной безопасности.

В заключение приводим фрагмент документа СМФБ компании:

…ООО «СПИК СЗМА» устанавливает, планирует и обеспечивает следующие процессы жизненного цикла ПАЗ:

- Анализ опасностей технологических процессов;
- Распределение функций безопасности по уровням защиты и назначение для каждой функции безопасности ПАЗ соответствующего уровня полноты безопасности (УПБ);
- Разработка спецификации требований безопасности (СТБ) ПАЗ;

- Разработка проектной документации, отвечающей требованиям к функциям безопасности ПАЗ;
- Подтверждение соответствия требованиям функциональной безопасности ПАЗ требуемых функций безопасности и значений полноты их безопасности;
- Закупки, связанные со сборкой и испытаниями ПАЗ;
- Сборка и испытания ПАЗ с подтверждением требуемых функций безопасности и значений полноты их безопасности.

Литература

1 ГОСТ Р ИСО 9001–2015. Системы менеджмента качества. Требования.

2 Индык Ю.Д., Можаева И.А., Струков А.В. Особенности разработки системы менеджмента функциональной безопасности в инжиниринговой компании-интеграторе// Сборник трудов XXV Всероссийской научно-практической конференции "Актуальные проблемы защиты и безопасности". Т. 2:. ФГБУ РАРАН-Москва, НПО СМ – СПб. 2022 С.340–347

3 ФНиП "Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств", утверждены приказом Ростехнадзора №533 от 15.12.2020 г.

4 ГОСТ Р МЭК 61511-1. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения, технические требования.

5 ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. 2012. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3.