Результаты апробации обновленного комплекса показали сокращение времени анализа и повышение достоверности расчетов, что подтверждает эффективность предложенных решений.

Модернизированный программный комплекс может применяться в лабораторных и проектных исследованиях при проведении FMECA-анализа систем ЖАТ, а также в составе методик доказательства функциональной безопасности микропроцессорных систем управления.

Список литературы

1 **Харлап, С. Н.** Обзор существующих средств автоматизации FMECA-анализа / С. Н. Харлап, В. Л. Катков, Е. П. Литвинов // Инновационное развитие транспортного и строительного комплексов : материалы Междунар. науч.-практ. конф., посвящ. 70-летию БелИИЖТа – БелГУТа, Гомель, 16–17 нояб. 2023 г. : в 2 ч. Ч. 1 / М-во трансп. и коммуникаций Респ. Беларусь, Бел. ж. д., Белорус. гос. ун-т. трансп. ; под общ. ред. Ю. И. Кулаженко. – Гомель : БелГУТ, 2023. – С. 234–236.

2 Особенности методов анализа видов и последствий отказов устройств ЖАТ / С. Н. Харлап, Д. Д. Медведев, С. И. Хоменко [и др.] // Проблемы безопасности на транспорте : материалы XII Междунар. науч.-практ. конф., посвящ. 160-летию Белорусской железной дороги, Гомель, 24–25 нояб. 2022 г. : в 2 ч. Ч. 1 / М-во трансп. и коммуникаций Респ. Беларусь, Бел. ж. д., Белорус. гос. ун-т. трансп. ; под общ. ред. Ю. И. Кулаженко. – Гомель : БелГУТ, 2022. – С. 227–230.

3 **Харлап, С. Н.** Программное обеспечение для проведения анализа FMECA микроэлектронных систем железнодорожной автоматики / С. Н. Харлап, В. Л. Катков // Проблемы безопасности на транспорте : материалы X Междунар. науч.-практ. конф., Гомель, 26–27 нояб. 2020 г. : в 5 ч. Ч. 1 / М-во трансп. и коммуникаций Респ. Беларусь, Бел. ж. д., Белорус. гос. ун-т. трансп.; под общ. ред. Ю. И. Кулаженко. – Гомель : БелГУТ, 2020. – С.43–44.

4 **Харлап, С. Н.** Программное обеспечение для автоматической классификации последствий отказов при проведении FMECA-анализа устройств СЖАТ / С. Н. Харлап, В. Л. Катков, Е. П. Литвинов // Научно-технические аспекты комплексного развития железнодорожного транспорта : материалы X Междунар. науч.-практ. конф. : в 2 ч. Ч. 1 – Донецк: ДИЖТ, 2024. – С. 140–145.

5 **Харлап, С. Н.** Программный комплекс для автоматического построения дерева отказов по результатам выполнения FMECA-анализа устройств СЖАТ / С. Н. Харлап, Е. П. Литвинов // Проблемы безопасности на транспорте : материалы XIII Междунар. науч.-практ. конф., посвящ. Году качества : в 2 ч. Ч. 1 / М-во трансп. и коммуникаций Респ. Беларусь, Бел. ж. д., Белорус. гос. ун-т. трансп.; под общ. ред. Ю. И. Кулаженко. – Гомель : БелГУТ, 2024. – С. 233–235.

УДК 656.25

МЕТОД КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ДОСТИЖИМОГО УРОВНЯ ПОЛНОТЫ БЕЗОПАСНОСТИ СИСТЕМ ЖАТ НА ОСНОВЕ АРХИТЕКТУРНЫХ ОГРАНИЧЕНИЙ

С. Н. ХАРЛАП, О. И. ЯКОВЦЕВА
Белорусский государственный университет транспорта, г. Гомель

Развитие высокоскоростного железнодорожного движения предъявляет повышенные требования к надёжности и функциональной безопасности систем железнодорожной автоматики и телемеханики (ЖАТ). Критически важной задачей становится оценка рисков отказов, способных привести к авариям, человеческим жертвам и значительным финансовым потерям. В этой связи ключевой задачей разработчиков является обеспечение соответствия систем строгим требованиям международных стандартов функциональной безопасности, таких как МЭК 61508 [1], которые предписывают достижение высоких уровней полноты безопасности.

Разработка систем ЖАТ традиционно ведётся по V-образной модели жизненного цикла [2]. Данная модель предполагает последовательное прохождение этапов: анализ требований, проектирование архитектуры, детальное проектирование, кодирование (реализация), затем интеграция компонентов и, наконец, этапы верификации (проверка соответствия проекту) и валидации (проверка соответствия исходным требованиям заказчика и реальным условиям эксплуатации).

Существенным недостатком этого подхода является то, что проектные решения, принятые на ранних этапах, могут быть полноценно проверены лишь на стадии валидации, когда опытный образец уже создан. Это создаёт высокие риски того, что выявленные на финальной стадии несоответствия требованиям безопасности потребуют дорогостоящего пересмотра проекта и возврата к предыдущим этапам разработки.

Сложность прогнозирования уровня полноты безопасности

Функциональная безопасность – комплексный показатель, включающий:

1 **Защиту от систематических отказов** (ошибки проектирования): обеспечивается строгим соблюдением регламентированных стандартами процедур на всех этапах разработки. Риски здесь минимальны при корректном выполнении всех предписанных мероприятий.

2 **Защиту от случайных аппаратных отказов:** характеризуется **интенсивностью опасных отказов** и **долей безопасных отказов**. Именно количественная оценка этих показателей на ранних стадиях проектирования представляет наибольшую сложность.

До завершения разработки системы точно спрогнозировать достигаемый УПБ затруднительно. Это зачастую приводит разработчиков к одной из двух неоптимальных стратегий:

1 Слепое следование прошлому опыту без точной количественной оценки.

2 Применение избыточного набора методов защиты «на всякий случай», что ведёт к удорожанию и снижению конкурентоспособности продукта.

Для решения этой проблемы предлагается использовать на ранних этапах проектирования концепцию **архитектурных ограничений**, изложенную в стандарте МЭК 61508 [3]. Данный подход позволяет формализовать требования к структуре системы и дать первоначальную количественную оценку её потенциала по обеспечению безопасности.

Ключевая идея метода заключается в том, что максимально достижимый уровень полноты безопасности для программируемого электронного компонента (отнесённого по стандарту к Типу B – сложные компоненты, такие как микроконтроллеры и ПЛИС) не является произвольным. Он определяется двумя фундаментальными параметрами, закладываемыми на этапе архитектурного проектирования:

1 **Уровень отказобезопасности *N*** – этот параметр определяется аппаратной архитектурой системы и обозначает количество отказов, которые система может выдержать без перехода в опасное состояние:

1) ***N* = 0.** Одноканальная архитектура (1oo1 – «one out of one»). Одиночный отказ элемента может привести к опасному отказу системы. Это архитектура без избыточности;

2) ***N* = 1.** Двухканальная архитектура. Сюда относятся как дублированные системы (1oo2 – система обеспечивает безопасность, если функционирует хотя бы один канал из двух), так и мажоритарные системы (2oo3 – система обеспечивает безопасность, если функционируют хотя бы два канала из трёх). Один опасный отказ может быть перекрыт избыточным каналом;

3) ***N* = 2.** Троированная архитектура (3oo3 – система обеспечивает безопасность, если функционирует хотя бы один канал из трех). Система может парировать опасные отказы в двух каналах.

2 **Доля безопасных отказов (ДБО)** – это расчётный показатель, выражаемый в процентах. Он характеризует эффективность всех применяемых в системе диагностических механизмов. ДБО показывает, какая часть всех возможных отказов компонента будет обнаружена и обработана таким образом, что система перейдёт в безопасное состояние. Формула для расчёта ДБО выглядит следующим образом:

$$\text{ДБО} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}},$$

где λ_S – интенсивность безопасных отказов (отказы, которые не приводят к потере функции безопасности или сразу же её обнаруживают); λ_{DD} – интенсивность опасных отказов, которые обнаруживаются встроенными диагностическими средствами; λ_{DU} – интенсивность опасных отказов, которые не обнаруживаются диагностикой (самая критичная категория).

Поскольку уровень отказобезопасности *N* выбирается на этапе разработки концепции и является фиксированным, ключевой переменной величиной становится доля безопасных отказов. Её сложно оценить экспертным путём.

Для решения этой задачи предлагается метод количественного расчёта ДБО на основе выбранных аппаратных средств и программных механизмов контроля и диагностики. Это позволит ещё на стадии проектирования спрогнозировать максимально достижимый УПБ для выбранной архитектуры системы, а также решить обратную задачу – подобрать оптимальный набор аппаратных и программных мер для достижения целевого УПБ.

Для практической реализации данного метода предлагается разработать специализированное программное обеспечение, которое автоматизирует расчёты и минимизирует риски недостижения требуемых показателей безопасности на поздних стадиях разработки.

Алгоритм оценки достижимого УПБ [4]:

1 *Выбор архитектуры* – разработчик в интерфейсе программы выбирает целевую аппаратную архитектуру системы (1oo1, 1oo2, 2oo3, 3oo3), что определяет параметр *N*.

2 *Выбор компонентов* – пользователь выбирает из встроенной базы данных конкретные аппаратные компоненты, планируемые к применению в оцениваемом проекте. Для каждого компонента в базе данных хранятся данные по интенсивности отказов (λ), разбитые на категории (λ_S, λ_D и т. д.).

3 *Выбор методов диагностики* – для каждого компонента пользователь активирует методы диагностики и самоконтроля, которые планируется использовать в проекте. Программа обладает обширным каталогом таких методов с предрасчитанной эффективностью (коэффициентом покрытия диагностики – DC), регламентированной стандартами (МЭК 61508-2 [3], МЭК 61508-6 [4]).

4 *Расчёт ДБО* – программа на основе выбранных компонентов и активированных для них диагностических методов вычисляет совокупную долю безопасных отказов для всей системы.

5 *Определение УПБ* – по соответствующей таблице стандарта МЭК 61508-2 программа определяет итоговый, максимально достижимый УПБ для выбранной конфигурации.

Разработчик может проверить, как повлияет на итоговый УПБ добавление других методов диагностики или переход к другой архитектуре, например от дублированной к троированной. Это позволяет найти экономически оптимальное решение, гарантированно удовлетворяющее требованиям по безопасности.

Ключевые особенности работы программы:

Интерактивность: пользователь может настраивать параметры устройства и выбирать методы диагностики (рисунок 1).

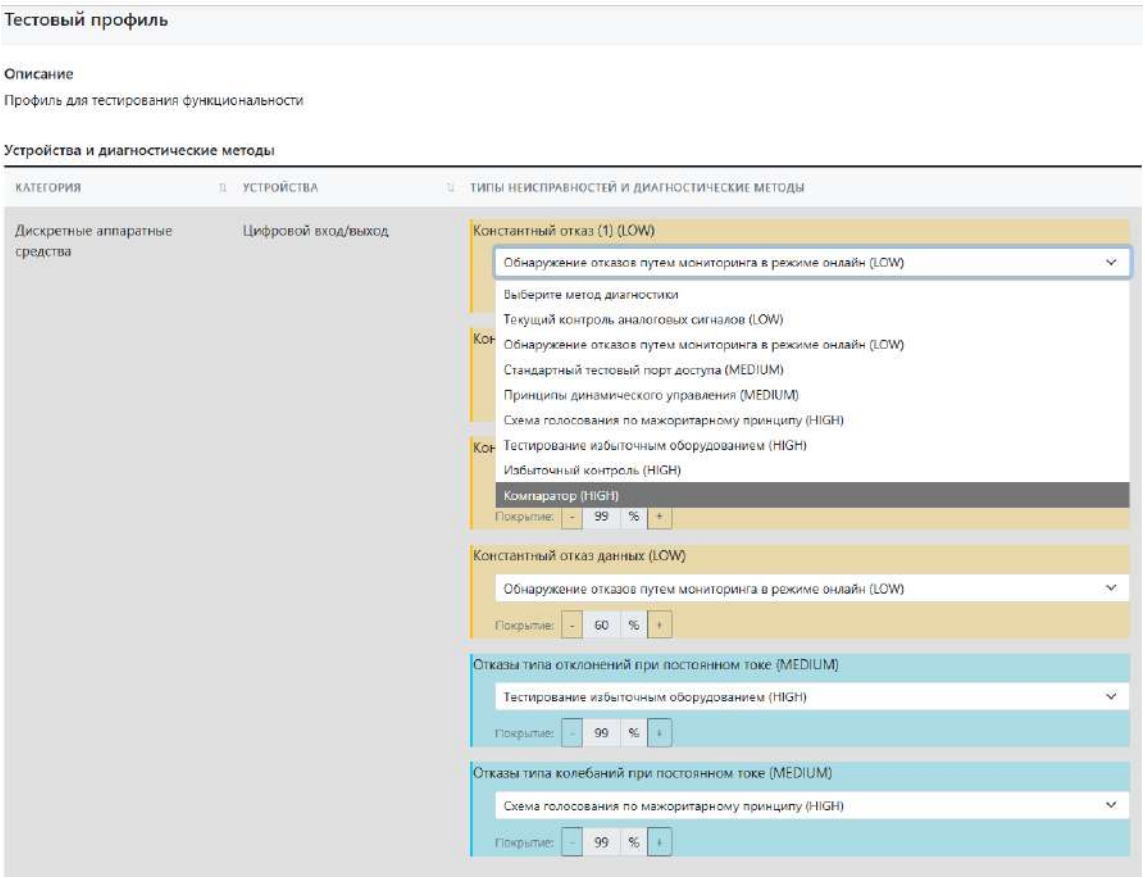

Рисунок 1 – Пример конфигурации системы и выбора диагностик

Автоматизация: расчёты выполняются автоматически на основе выбранных данных.

Соответствие стандартам: программа использует данные из ГОСТ Р МЭК 61508-2 [3] и МЭК 61508-6 [4] для обеспечения точности анализа.

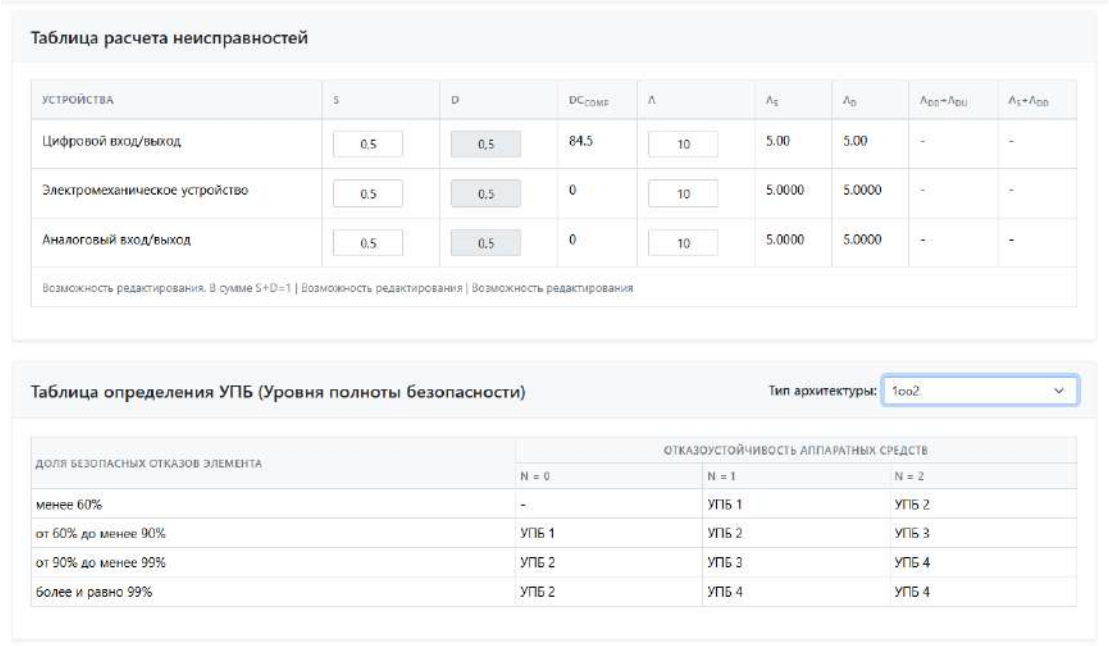

Рисунок 2 – Пример расчета неисправностей и УПБ

Данное программное обеспечение может стать эффективным инструментом для проектирования и анализа устройств с учетом требований функциональной безопасности. Оно поможет не только оценить текущее состояние проекта, но и принять обоснованные решения для его улучшения. Это особенно важно в контексте стандартов, таких как ГОСТ Р МЭК 61508-2-2012 [3], которые требуют строгого соблюдения норм безопасности для критически важных систем (рисунок 2).

Предлагаемое решение на основе метода архитектурных ограничений и специализированного ПО позволит реализовать комплексный подход к обеспечению функциональной безопасности систем ЖАТ на ранних этапах проектирования, минимизировать риски, оптимизировать затраты и гарантировать достижение требуемых уровней полноты безопасности.

Список литературы

1 ГОСТ Р МЭК 61508-1-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 1. Общие требования. – Введ. 01.08.2023. – М. : Стандартинформ, 2014. – 51 с.

2 ГОСТ 33432-2015. Политика, программа обеспечения безопасности. доказательство безопасности объектов железнодорожного транспорта. – Введ. 01.0.2016. – М. : Стандартинформ, 2019. – 24 с.

3 ГОСТ Р МЭК 61508-2-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 2. Требования к электрическим, электронным, программируемым электронным системам, относящимся к безопасности. – Введ. 01.08.2023. – М. : Стандартинформ, 2014. – 80 с.

4 ГОСТ Р МЭК 61508-6-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 6. Руководство по применению ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-3. – Введ. 01.08.2023. – М. : Стандартинформ, 2014. – 102 с.

УДК 656.259.12

МОДЕЛЬ И АЛГОРИТМ ВЫЯВЛЕНИЯ ОБРЫВА СТРЕЛОЧНЫХ СОЕДИНИТЕЛЕЙ, НЕ ОБТЕКАЕМЫХ СИГНАЛЬНЫМ ТОКОМ

Д. В. ШВАЛОВ, Е. С. РЕВЕНКО
Ростовский государственный университет путей сообщения, г. Ростов-на-Дону, Российская Федерация

Стрелочные соединители, не обтекаемые сигнальным током в нормальном режиме, устанавливаются на стрелочных переводах, входящих в состав разветвленных рельсовых цепей с неконтролируемыми ответвлениями. Такие соединители всегда дублируются в соответствии с действующи-