Список литературы

1 **Аверкиев, С. А.** Системы технической диагностики и мониторинга на базе технических средств АСДК (СТДМ АСДК) : типовые материалы для проектирования 410422-ТМП / С. А. Аверкин. – 2007.

2 **Воронцов, В. Н.** Схемы переездной сигнализации для переездов, расположенных на перегонах при любых средствах сигнализации и связи АПС-04 : типовые материалы для проектирования 410407-ТМП / В. Н. Воронцов. – 2004.

3 **Калинин, В. С.** Инновации в железнодорожном транспорте : техническая документация / В. С. Калинин, А. И. Михайлов. – 2018.

4 Ефанов, Д. В. Микропроцессорная система диспетчерского контроля устройств железнодорожной автоматики и телемеханики : учеб. пособие / Д. В. Ефанов, Г. В. Осадчий. – 3-е изд. стер. – СПб. : Лань, 2023. – 180 с.

УДК 656.25

МОДЕРНИЗАЦИЯ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ АВТОМАТИЗАЦИИ ПРОВЕДЕНИЯ FMECA-АНАЛИЗА СИСТЕМ ЖАТ

С. Н. ХАРЛАП, Е. П. ЛИТВИНОВ

Белорусский государственный университет транспорта, г. Гомель

Современные микроэлектронные системы железнодорожной автоматики и телемеханики (ЖАТ) являются ключевыми элементами обеспечения безопасности движения поездов. Их проектирование и внедрение требуют обязательного подтверждения функциональной безопасности в соответствии с действующими нормативными документами и международными стандартами.

Одним из основных методов доказательства безопасности является анализ видов, последствий и критичности отказов (Failure Mode, Effects and Criticality Analysis – FMECA) [1], включающий определение критериев и видов отказов, их имитацию, анализ последствий и расчет интенсивности возникновения опасных отказов [2] для всей анализируемой системы.

Высокая сложность современных устройств и большое количество моделируемых отказов делают проведение FMECA-анализа трудоемкой задачей, подверженной риску систематических ошибок, связанных с человеческим фактором. Однако четкая последовательность этапов анализа позволяет эффективно автоматизировать данный процесс, что особенно актуально для систем ЖАТ, где необходимы высокая точность и воспроизводимость результатов.

С этой целью в 2025 году был разработан программный комплекс (ПК) для автоматизации проведения FMECA-анализа систем ЖАТ [3–5], включающий три модуля: CircuitAnalyzer, FailureAnalyzer и FailureTreeBuilder.

В ходе апробации программного комплекса были выявлены направления, требующие модернизации для повышения производительности и точности анализа. В первую очередь, это оптимизация вычислительных процессов моделирования отказов в модуле CircuitAnalyzer и расширение возможностей учета диагностируемости отказов сложных микросхем при расчете интенсивностей отказов в модуле FailureTreeBuilder комплекса.

Модуль CircuitAnalyzer выполняет автоматизированное моделирование отказов электронных компонентов исследуемых схем с использованием ядра схемотехнического симулятора SPICE. В исходной версии моделирование производилось последовательно, что при большом количестве элементов (до нескольких тысяч) приводило к значительным временным затратам.

Для устранения данного недостатка реализован механизм многопоточного моделирования отказов. Каждая модель отказа теперь может выполняться в отдельном потоке с параллельным использованием ядер центрального процессора. Такой подход позволил значительно увеличить производительность и сократить время выполнения анализа.

Однако использование всех ядер процессора без ограничений может приводить к снижению производительности из-за повышенной нагрузки на систему и конкуренции потоков за ресурсы процессора. Для обеспечения стабильности работы и возможности адаптации под вычислительные ресурсы конкретного компьютера реализован механизм семафора, позволяющий ограничивать количество одновременно выполняемых потоков.

Количество активных потоков

$$N_{\text{потоков}} = N_{\text{ядер процессора}} - 1. \quad (1)$$

Это решение обеспечивает рациональное распределение вычислительной нагрузки и предотвращает конфликт потоков при обращении к памяти и дисковым ресурсам. Таким образом, в зависимости от архитектуры вычислительной системы и числа ядер процессора, время выполнения полного цикла моделирования может сокращаться в несколько раз, при этом сохраняется возможность гибкой настройки параметров параллельности.

Реализация многопоточного моделирования позволила существенно повысить эффективность работы модуля CircuitAnalyzer, сохранив корректность и воспроизводимость получаемых результатов.

Модуль FailureTreeBuilder выполняет построение дерева опасных отказов и расчет интенсивности опасного отказа всей исследуемой системы. В ходе модернизации была доработана методика учета результатов экспертной оценки диагностируемости сложных микросхем.

В предыдущей версии комплекса интенсивность опасного отказа сложных элементов, например, микроконтроллеров, для которых невозможно выполнить поэлементное моделирование, рассчитывалась по справочным данным без учета диагностических возможностей аппаратного обеспечения:

$$\lambda_{оо} = \lambda_{справ}, \tag{2}$$

где $\lambda_{оо}$ – интенсивность опасного отказа, 1/ч; $\lambda_{справ}$ – справочная интенсивность отказов, 1/ч.

В модуль FailureTreeBuilder добавлена возможность задания коэффициентов диагностируемости – как общего для всей микросхемы, так и отдельных для каждого типа отказа, например, короткое замыкание на «плюс питания», короткое замыкание на «минус питания», короткое замыкание на соседний вывод, обрыв контакта. Эти коэффициенты указываются в таблице данных объекта исследования. Если значения не заданы, по умолчанию принимается коэффициент равный 1. Пример задания данных коэффициентов приведен на рисунке 1.

	K	L	M	N	O	P
след пин	Замыкание на след пин (Класс отказа)	Kd_Common	Kd_KzPlus	Kd_KzGnd	Kd_Break	Kd_KzNextPin
	защитный	0.9	0.7	0.8	0.6	0.5
	защитный					
	защитный					
	маскируемый					
	маскируемый					
	маскируемый					

Рисунок 1 – Пример задания коэффициентов диагностируемости

Модернизированная формула расчета интенсивности опасных отказов имеет вид

$$\lambda_{оо} = \lambda_{справ} (1 - K_{диаг}), \tag{3}$$

где $K_{диаг}$ – коэффициент диагностируемости для анализируемой микросхемы.

Таким образом, если устройство обладает средствами диагностирования отказов, то их влияние может быть учтено с помощью коэффициента диагностируемости. В этом случае интенсивность опасного отказа определяется по формуле (3).

Такой подход позволяет повысить точность оценки риска: при высокой диагностируемости значение коэффициента $K_{диаг}$ близко к единице, что приводит к уменьшению расчетной интенсивности опасных отказов, а при низкой диагностируемости, напротив, увеличивает её, отражая рост вероятности невыявленных опасных отказов.

Проведенные модернизации существенно расширили функциональные возможности и повысили эффективность работы программного комплекса для проведения FMECA-анализа. Основные результаты модернизации заключаются в следующем:

– реализация многопоточного моделирования отказов позволила ускорить вычисления в 2–8 раз в зависимости от числа ядер процессора;

– использование принципа семафора обеспечило гибкость настройки и стабильность работы при больших объемах моделирования;

– внедрение коэффициентов диагностируемости повысило точность оценки интенсивности отказов сложных микросхем и микроконтроллеров;

– модернизированный расчетный алгоритм позволил более корректно учитывать влияние диагностических систем на общую интенсивность опасных отказов.

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.