УДК **629.33** DOI **10.46960/1816-210X_2025_3_95**
EDN **YWKUBQ**

АНАЛИЗ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ДЛЯ БЛОКОВ УПРАВЛЕНИЯ, НЕ ИМЕЮЩИХ ФУНКЦИЙ НА УРОВНЕ ТРАНСПОРТНОГО СРЕДСТВА

П.К. Захаров
ORCID: **0009-0006-6372-8295** e-mail: **pavel.zaharov@nami.ru**
Научный Центр Российской Федерации
Федеральное государственное унитарное предприятие «НАМИ»
Москва, Россия

И.Б. Лепеева
ORCID: **0009-0006-7819-2702** e-mail: **irina.lepeeva@nami.ru**
Научный Центр Российской Федерации
Федеральное государственное унитарное предприятие «НАМИ»
Москва, Россия

П.С. Рогов
ORCID: **0000-0001-9758-7554** e-mail: **petr.rogov@nami.ru**
Научный Центр Российской Федерации
Федеральное государственное унитарное предприятие «НАМИ»
Москва, Россия

Представлен модернизированный адаптированный подход к анализу функциональной безопасности электронных компонентов транспортных средств, не имеющих собственных целей безопасности (ЦБ), но влияющих на безопасность транспортного средства в целом. Рассмотрен двусторонний подход к исследованию компонентов (одновременный проход V-модели согласно ISO 26262 снизу-вверх и сверху-вниз). Выполнен анализ безопасности блока распределения низковольтного питания LVDCU с помощью предлагаемого метода. Для восьми различных реализаций блока LVDCU рассчитаны вероятностные метрики для случайных отказов аппаратных средств, по численным значений которых определена лучшая реализация с точки зрения функциональной безопасности. Подробно рассмотрена стадия разработки спецификации технических требований по безопасности, выполнен анализ вероятности нарушения ЦБ связанных с блоком систем вследствие случайных отказов аппаратных компонентов (АК). Выполнено прогнозирование метрик охвата диагностикой одиночных и скрытых сбоев. Полученный алгоритм позволяет произвести качественный и количественный анализ безопасности электронного компонента, не имеющего собственных целей безопасности, без потери поля покрытия возможных опасностей и недопущения неоправданного снижения ASIL, учитывая его межсистемное применение в архитектуре транспортного средства.

***Ключевые слова*:** межсистемный компонент, функциональная безопасность, аппаратный компонент, требования безопасности, программное обеспечение, вероятностная метрика для случайных отказов аппаратных средств; анализ видов и последствий отказов, анализ опасностей и оценка рисков, уровень полноты безопасности транспортного средства, метрика единичных сбоев, метрика скрытого сбоя.

ДЛЯ ЦИТИРОВАНИЯ: Захарова, П.К. Анализ функциональной безопасности для блоков управления, не имеющих функций на уровне транспортного средства / П.К. Захарова, И.Б. Лепеева, П.С. Рогов // Труды НГТУ им. Р.Е. Алексеева. 2025. № 3. С. 95-107. DOI 10.46960/1816-210X_2025_3_95 EDN: YWKUBQ

© Захаров П.К., Лепеева И.Б., Рогов П.С., 2025

FUNCTIONAL SAFETY ANALYSIS FOR CONTROL UNITS WITHOUT VEHICLE-LEVEL FUNCTIONS

P.K. Zakharov
ORCID: **0009-0006-6372-8295** e-mail: **pavel.zaharov@nami.ru**
State Scientific Center of the Russian Federation Federal State Unitary Enterprise «NAMI»
Moscow, Russia

I.B. Lepeeva
ORCID: **0009-0006-7819-2702** e-mail: **irina.lepeeva@nami.ru**
State Scientific Center of the Russian Federation Federal State Unitary Enterprise «NAMI»
Moscow, Russia

P.S. Rogov
ORCID: **0000-0001-9758-7554** e-mail: **petr.rogov@nami.ru**
State Scientific Center of the Russian Federation Federal State Unitary Enterprise «NAMI»
Moscow, Russia

Abstract. This article presents a modernized adapted approach to analysing the functional safety of electronic components of vehicles that do not have their own safety goals, but affect the safety of the vehicle as a whole. A two-way approach to component analysis is considered (simultaneous bottom-up and top-down pass of the V-model according to ISO 26262). The low voltage distribution control unit (LVDCU) safety analysis was performed using the proposed method. Probabilistic metrics for random hardware failures are calculated for eight different LVDCU implementations, and the numerical values are used to determine the best implementation from a functional safety perspective. The stage of development of the specification of technical requirements for safety is considered in detail, and an analysis of the probability of violation of the safety goal of the systems connected with the component due to accidental failures of hardware components is performed. Forecasting of diagnostic coverage metrics for single and hidden failures has been completed. The obtained algorithm makes it possible to perform a qualitative and quantitative analysis of the safety of an electronic component that does not have its own safety goals, without losing the coverage field of possible hazards and preventing an unjustified reduction in ASIL, taking into account its intersystem application in the vehicle architecture.

Key words: intersystem component; functional safety, hardware, safety requirements, software, probabilistic metric for random hardware failures, failure modes and effects analysis, hazard analysis and risk assessment, automotive safety integrity level, single-point fault metric, latent-fault metric.

FOR CITATION: P.K. Zakharov, I.B. Lepeeva, P.S. Rogov. Functional safety analysis for control units without vehicle-level functions. Transactions of NNSTU n.a. R.E. Alekseev. 2025. № 3. Pp. 95-107.
DOI 10.46960/1816-210X_2025_3_95 EDN: YWKUBQ

Введение

Современные дорожные транспортные средства в рамках постоянного технического прогресса наращивают в составе своей архитектуры электронные блоки. Внедрение все большего числа электронных компонентов направлено не только на улучшение комфорта и расширение мультимедийных возможностей для водителей и пассажиров, но и зачастую на увеличение уровня безопасности. Новые электронные блоки, интегрируемые в состав транспортного средства (ТС), обрабатывают большое количество разнородной информации, на основе которой принимаются решения о вмешательстве в процесс вождения, оказания воздействий на транспортное средство. В автомобильном секторе постоянно создаются и совершенствуются системы безопасности автотранспорта путем внедрения подобных электронных блоков. К ним относятся системы подушек безопасности, сложные системы, обеспечивающие помощь водителю в процессе движения автомобиля, системы предотвращения столкновений автомобиля с препятствием, а также различные системы предупреждения об опасностях во время

движения. Внедрение новых функций безопасности привело к резкому увеличению количества электронных систем на борту автомобиля. Поэтому при проектировании и разработке особо ответственных систем на первый план выходит необходимость исследования функциональной безопасности. Функции, влияющие на управление ТС, должны быть спроектированы с учетом строгих требований к безопасности, которые закладывают основу для надежной и безопасной эксплуатации на протяжении всего жизненного цикла (ЖЦ) ТС. Для соблюдения всего комплекса требований к функциональной безопасности на основе общеотраслевого стандарта IEC 61508 был создан комплекс стандартов ISO 26262, подробно описанный в статье Kuen-Long Lu and Yung-Yuan Chen [1]. Также исследованием функциональной безопасности (ФБ) сложных электронных и электрических компонентов в различных отраслях занимались А.С. Степанянц, И.Б. Шубинский, А.С. Шаракшанэ, А.С. Давлиева [2]), изучению ЖЦ ФБ посвящена квалификационная работа М.Д. Кнопфа [3].

ISO 26262 – стандарт, регламентирующий обеспечение функциональной безопасности автомобилей. Отдельные части стандарта описывают различные меры, которые должны предпринимать поставщики и производители автомобилей, чтобы минимизировать риск возникновения ошибок в используемых компонентах или программных инструментах, которые могут привести к сбоям в работе конечного продукта. Основная цель стандарта ISO 26262 – обеспечить проектирование электронных систем с новыми функциями, которые повышают надежность и позволяют контролировать и предотвращать опасные для жизни человека отказы в таких системах [4]. Актуальность применения подхода, описанного в ISO 26262, одним из первых была представлена Fabio Marchiò еще в 2014 г. в статье [5] в виде V-модели. Данный вид ЖЦ, состоящий из подэтапов, подробно рассмотрен в работе John O. Clark [6]. В настоящее время концепции V-модели при реализации ЖЦ функциональной безопасности придерживаются многие основные производители ТС и компонентов, несмотря на то, что формат данного цикла может не совпадать с ЖЦ основной разработки (например, *General Motors* использует модель *Waterfall* [7, 8].

ISO 26262 можно считать лучшей мировой практикой максимизации функциональной безопасности автомобильной электроники, несмотря на попытки применения новых гибких технологий, таких как *Agile* [9] или прототипный подход *Tesla* [7], также применяемый в сфере автомобилестроения. Все эти вариации направлены на адаптацию классического цикла ФБ по V-модели под нужды и возможности разработчика. Несмотря на это, все циклы берут свое начало на этапе «черного ящика» для системы и функциональности рассматриваемой системы на уровне ТС – это этап определения устройства. Как следует из самого определения по ISO 26262-1, устройством является система или несколько систем, реализующие некоторую функцию уровня транспортного средства. Следовательно, именно устройство является объектом с наивысшей степенью идентификации в процессе и отправной точкой для разработки безопасности конкретного продукта. Цели безопасности и уровень полноты безопасности ТС (*Automotive integrity safety level, ASIL*) устройство получает через анализ его функциональности. ASIL является атрибутом, указывающим степень вклада того или иного компонента в безопасность и уровень необоснованного риска, который необходимо сократить. Далее вся разработка системы проходит линейно (последовательно) сначала сверху-вниз по левой ветви V-модели, а затем снизу-вверх – по правой ветви.

Этот цикл прекрасно работает при наличии штатной отправной точки алгоритма в виде устройства с наличием функциональности на уровне транспортного средства. Но так бывает не всегда, и иногда в практике приходится сталкиваться с объектами, которые не имеют функциональности на уровне ТС, а, соответственно, не имеют своих ЦБ, но при этом оказывают явное воздействие на безопасность при внедрении их в архитектуру ТС. Такие компоненты носят наименование межсистемных компонентов, т.е. это отдельные объекты, одновременно связанные с рядом систем ТС, функционал которых распространяется на многие системы ТС

и служит для обеспечения должной работоспособности этих систем непосредственно уровня ТС. Данные компоненты могут быть рассмотрены в составе каждой из них при анализе функциональной безопасности. Именно такому блоку посвящено настоящее исследование.

Объект исследования. Начало анализа

Объект исследования в настоящей работе – *Low Voltage Distribution Control Unit (LVDCU)*, который является частью низковольтной системы питания потребителей в ТС. LVDCU не является «системой» в понимании стандарта ISO-26262, но участвует в работе многих низковольтных устройств. Анализ LVDCU как межсистемного компонента должен выполнятся по другому алгоритму. Необходимо начинать с технической архитектуры низковольтной системы питания и зависимых внешних компонентов.

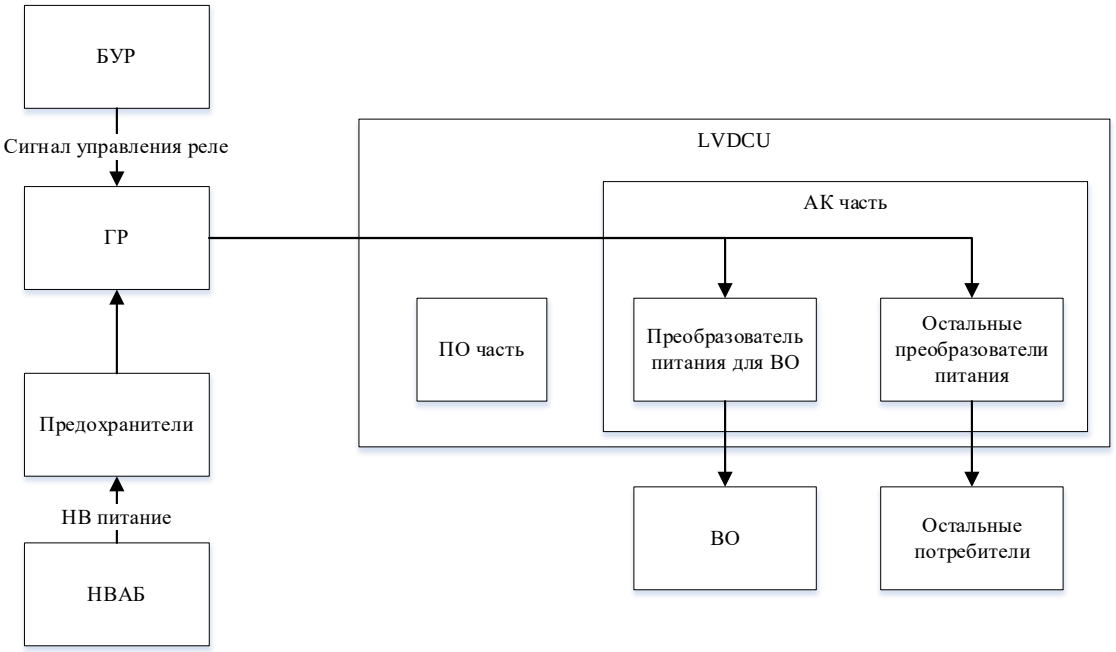

Рис. 1. Фрагмент технической архитектуры низковольтной системы питания и связанных компонентов

Fig. 1. Fragment of the technical architecture of the low-voltage power supply system and related components

На рис. 1 изображена часть технической архитектуры, показывающая участие LVDCU в питание внешнего освещения (ВО). Показанная техническая архитектура сконцентрирована на питании ВО, остальные компоненты не показаны и названы, как «остальные». Фрагмент технической архитектуры, показанный на рис. 1, состоит из блоков – технических компонентов. Каждый технический компонент состоит из аппаратных, программных и аппаратно-программных компонентов, которые выполняют одну задачу. Каждый технический компонент имеет отказы в соответствии с ISO-26262-5. Например, преобразователь питания имеет следующие отказы:

- нет напряжения;
- повышенное напряжение;
- пониженное напряжение;
- дрейф и колебания;
- перепады напряжения.

Отказы аппаратных компонентов (АК) и ошибки программного обеспечения (ПО) приводят к отказам технических компонентов. Объединение АК и ПО в технические компоненты упрощает анализ и позволяет объединить отказы, ведущие к одинаковым последствиям. LVDCU осуществляет распределение и защиту питания для многих систем. Одна из них ВО. Дальнейший анализ в данной статье сфокусирован на влиянии LVDCU в работу ВО, так как отказ ВО – наиболее опасное событие с точки зрения безопасности систем, на работоспособность которых влияет LVDCU. ВО включает в себя проводные соединения, фары и фонари. Принимается во внимание, что LVDCU питает ВО через одну линию: один преобразователь – ВО может полностью отказать из-за неисправности блока LVDCU. Отказ ВО приведет к множеству потенциальным опасностям. Соответствующие цели безопасности (ЦБ) представлены ниже:

- обнаружить/предотвратить полную потерю видимости дорожного пространства впереди ТС (ЦБ1);
- обнаружить/предотвратить потерю информировании о маневре ТС (ЦБ2);
- обнаружить/предотвратить потерю работоспособности стоп-сигналов (ЦБ3);
- обнаружить/предотвратить потерю видимости ТС спереди/сзади (ЦБ4).

Уровень полноты безопасности транспортного средства (УПБТС) определяется после выполнения анализа опасностей и оценки рисков (АОиОР). АОиОР выполнялся при анализе безопасности ВО и указан в данной статье в качестве справочных материалов. В результате АОиОР определен УПБТС С для ЦБ, связанных с отказами ВО. Фрагмент АОиОР представлен в табл. 1.

Таблица 1.
Фрагмент АОиОР

Table 1.
Fragment of the failure mode and effects analysis

Условия применения	**Неисправность**	**Опасность**	**Потенциальные последствия**	**Тяжесть последствий**	**Вероятность воздействия**	**Управляемость**	**УПБТС**	**ЦБ**
Любые условия, любая дорожная ситуация, темное время суток, любая дорожная ситуация, любая скорость ТС	Нет освещения дорожного полотна перед ТС (при наличии запросе на включение)	Потеря видимости дорожного пространства впереди ТС	Возможно столкновение с дорожной инфраструктурой в результате потери видимости	S3: переднее столкновение с объектами дорожной инфраструктуры на высокой скорости	E3: передвижение в темное время суток занимает 1-10 % от всего времени эксплуатации ТС	C3: более 90 % водителей смогут сменить траекторию движения и миновать объекты на низкой скорости, но на высокой скорости (>80 км/ч) менее 90 % водителей смогут предотвратить столкновение	C	Обнаружить/предотвратить полную потерю видимости дорожного пространства впереди ТС

Анализ аппаратных компонентов объекта исследования

Следующим шагом анализа функциональной безопасности LVDCU является анализ на уровне АК. Цели анализа на уровне АК:

- определение причин отказов технических компонентов на уровне АК;

- определение вероятности отказов технических компонентов;
- расчет вероятностной метрики для случайных отказов аппаратных средств (BMCOA);
- расчет метрики единичных сбоев (MOC);
- расчет метрики скрытого сбоя (MCC).

BMCOA представляет количественный анализ, который вычисляет нарушение соответствующих ЦБ случайными отказами АК. Результаты количественного анализа сравниваются целевым значением. Для определения интенсивности отказов АК стандарт ISO-26262-5-2021 предполагает использование следующих справочников: SN 29500, IEC 61709, MIL HDBK 217 F notice 2, RIAC FMD-2016, MIL HDBK 338, A. Birolini «Reliability Engineering – Theory and Practice». Последний используется по умолчанию в данной статье для определения видов и распределения отказов АК. Виды и распределение отказов некоторых АК дополнены справочником MIL HDBK 338. Также в данной статье по умолчанию интенсивности отказов АК определены в соответствии со справочником SN29500. Для уточнения интенсивности отказов некоторых АК использовался справочник MIL HDBK 217 F. Интенсивность отказа измеряется в единицах измерения *Failure In Time* (FIT). Единица измерения FIT определяется выражением:

$$1\ \text{FIT} = 1 \times 10^{-9}\ \text{ч}^{-1} \quad (1)$$

Результаты определения интенсивностей отказов АК сведены в таблицу спецификации АК, фрагмент которой представлен в табл. 2.

Таблица 2.
Фрагмент спецификации АК

Table 2.
Fragment of the hardware component specification

Название	Описание	Идентификатор	Количество	Описание элемента из справочника	Спецификация	Интенсивность отказа, FIT	Вид отказа	Распределение отказа, %	Распределение отказа, FIT
GRM31CR61H106KA12	Capacitor C1206 10mcF 50V X5R ±10% Murata	C1, C2, C20	3	Handbook: Edition SN29500-1, Note 1: Category: Passive components (Part 4), subcategory: Capacitor Type: Ceramic MDK/MDC (z. B. X7R, X5R) Quality grade: GP	Rated voltage 50V Operating voltage 5V Ambient temperature 40°C	0,80759	Short	70	0,56531
							Open	10	0,08079
							Drift+	10	0,08079
							Drift-	10	0,08079
MPZ1608S102A	Ferrite filter L0603 1kOhm 0,8A 25% TDK	L1	1	Handbook: Edition SN29500-1, Note 1: Category: Passive components (Part 4), subcategory: Inductors Type: Inductors for EMV application <= 3A	Ambient temperature 40°C	1,26273	Short	60	0,75764
							Open	40	0,50509

Таблица 2 (окончание).
Фрагмент спецификации АК

Table 2 (continued).
Fragment of the hardware component specification

Название	Описание	Идентификатор	Количество	Описание элемента из справочника	Спецификация	Интенсивность отказа, FIT	Вид отказа	Распределение отказа, %	Распределение отказа, FIT
AC0603 FR-071M8L	Resistor R0603 1,8MOhm 0,1W 1% Yageo	R14	1	Handbook: Edition SN29500-1, Note 1: Category: Passive components (Part 4), subcategory: Resistor Type: Metal film	Ambient temperature 40°C	0,14156	Open	40	0,05662
							Drift+	30	0,04247
							Drift-	30	0,04247

Определение интенсивностей отказов технических компонентов

Для определения интенсивностей отказов технических компонентов необходимо выявить сеть причин и последствий между отказами АК и техническими компонентами. Анализ видов и последствий отказов (АВПО) предусмотрен стандартом ISO-26262 для определения сети причин и последствий. После проведения АВПО между отказами АК и неисправностями технических компонентов будет сформирована сеть причин и последствий. Результаты АВПО должны быть добавлены в АВПО системы, на работоспособность которой влияет межсистемный компонент, для дополнения структуры системы и определения корреляции причин и последствий между межсистемным компонентом и системой.

Для определения множественных и единичных отказов необходимо провести анализ дерева отказов (АДО). Алгоритм выполнения АДО для системы и его иерархия описаны в ISO-26262. АДО должен начинаться с опасности, к которой могут привести неисправности, определенные на уровне ТС, уточняющиеся по мере проведения анализа на различных уровнях анализа система. При анализе системы архитектура АДО дополняется и уточняется. Структура АДО показана на рис. 2.

Для межсистемного компонента дерево АДО начинается с отказов технических компонентов. Результаты должны быть добавлены в АДО системы для дополнения влияния межсистемного компонента на систему и завершения дерева отказов. АДО определило множественные и одиночные отказы АК межсистемного компонента LVDCU. На основе результатов АДО интенсивности отказов технических компонентов были рассчитаны и структурированы. В табл. 3 указан фрагмент отказов технических компонентов, влияющих на работоспособность ВО (применительно ко всем ЦБ). По результатам определения интенсивностей отказов технических компонентов было обнаружено, что для предварительной концептуальной реализации системы суммарная интенсивность отказов, которая приведет к полному отключению ВО (нарушению всех ЦБ), равна 121,7 FIT. Это значение не учитывает интенсивности отказов компонентов ВО (фары, фонари и т.д.), проводных соединений и других компонентов, участвующих в питании потребителей низковольтно системы питания (низковольтную аккумуляторную батарею (НВАБ), блок управления реле (БУР) и т.д.). Интенсивность отказа 121,7 превышает максимальное значение для УПБТС С, установленное ISO-26262, равное 100 FIT.

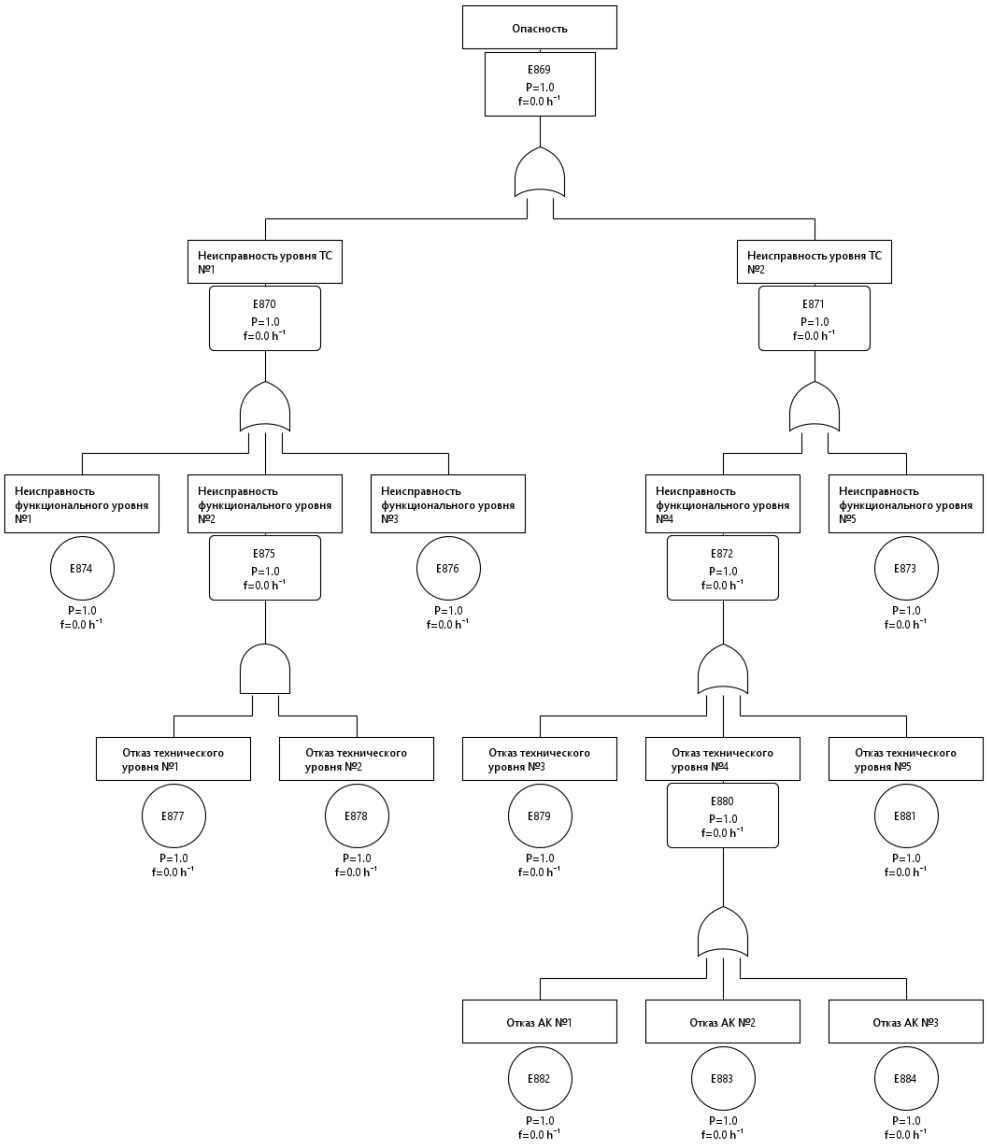

Рис. 2. АДО для системы

Fig. 2. Fault tree analysis for a system

Таблица 3.

Фрагмент таблицы интенсивности отказов технических компонентов

Table 3.

Fragment of the table of failure rates of technical components

Технический компонент	Событие	Интенсивность отказа, FIT
Интегральная схема LVDCU	Короткое замыкание	6,21
	Обрыв	2,07
Управляющие АК	Нет сигнала на включение	57,43
Преобразователь питания для ВО	Нет напряжения	48,36
	Пониженное напряжение	4,84
	Повышенное напряжение	2,79
Все компоненты (сумма)	Все события	121,7

В предварительной концептуальной реализации архитектура системы низковольтного питания была составлена таким образом, что отказ БУР или главного реле (ГР) приводит к отключению питания ВО, так как LVDCU получает питания от БУР и ГР. Интенсивности отказов для БУР и ГР для питания ВО составляет 118,56 FIT. Суммарная интенсивность отказов LVDCU, БУР и ГР составляет 240,26 FIT, исключая проводные соединения, компоненты ВО и остальные связанные компоненты. Для увеличения безопасности системы были предложены следующие возможные варианты архитектуры системы ВО:

- предварительно концептуализировать реализацию (Реализация Р1);
- использовать запасную линию LVDCU для питания ВО (Р2);
- разделить питания стоп-сигналов и габаритных огней от остального ВО (Р3);
- разделить питания ВО (Р4);
- питать ВО через предохранитель напрямую от НВАБ (Р5);
- использовать реле времени для питания ВО (Р6);
- питать LVDCU напрямую от НВАБ (Р7);
- питать ВО через предохранитель напрямую от ГР (Р8).

В табл. 4 представлены интенсивности отказов для каждого из способа реализации.

Таблица 4.
Интенсивности отказов при различных реализациях питания

Table 4.
Failure rates for different power supply implementations

№ [1]	LVDCU	БУР + ГР	Сумм. мин. FIT [2]	ЦБ1 [3]	ЦБ2	ЦБ3	ЦБ4
Р1	121,7	118,56	240,26	240,26	240,26	240,26	240,26
Р2	92,37	118,56	210,93	210,93	210,93	210,93	210,93
Р3	92,37	118,56	210,93	240,26	240,26	240,17	210,93
Р4	92,37	118,56	210,93	210,93	240,26	210,93	210,93
Р5	12,25	-	12,25	12,25	12,25	12,25	12,25
Р6	≅ 0	118,56	118,56	118,56	118,56	118,56	118,56
Р7	121,7	-	121,7	121,7	121,7	121,7	121,7
Р8	12,25	118,56	130,81	130,81	130,81	130,81	130,81

[1] Номер реализации.
[2] Минимальная суммарная интенсивности отказа технических компонентов.
[3] Идентификационные номер ЦБ.

В результате перерасчетов интенсивности отказов ВО наиболее эффективным оказался вариант с питанием ВО напрямую от НВАБ через предохранитель. Таким образом, безопасность системы для требований, направленных на предотвращение отказа ВО, увеличилась в 19,6 раз. Данное значение учитывает только АК LVDCU, БУР и ГР в части питания ВО, но не проводные соединения и компоненты ВО.

Следующим этапом является *Failure Modes and Effects Diagnostic Analysis (FMEDA)*. По результатам FMEDA должны быть получены МОС и МСС.

МОС рассчитывается по выражению 2:

$$\text{МОС} = 1 - \frac{\sum(\lambda_{SPF} + \lambda_{RF})}{\sum \lambda}, \quad (2)$$

где λ_{SPF} – интенсивность отказов, связанных с одиночными сбоями элемента аппаратного средства, λ_{RF} – интенсивность отказов, связанных с остаточными сбоями элемента аппарат-

ного средства, $\sum \lambda_x$ – сумма всех значений λ_x связанных с безопасностью элементов аппаратных средств устройства для рассматриваемых метрик. Вычислением МОС для систем, которые включает межсистемный компонент, производится по выражению 3:

$$\text{МОС}_N = 1 - \frac{\sum_{i=1}^{N}(\lambda_{SPFi} + \lambda_{RFi})}{\sum_{i=1}^{N}\lambda_i}, \quad (3)$$

где N – количество всех компонентов в системе, λ_{xi} – интенсивность отказа i-ой системы, $\sum_{i=1}^{N}\lambda_{xi}$ – сумма всех влияющих на безопасность АК всех систем от 1 до N.

МСС рассчитывается по выражению 4:

$$\text{МСС} = 1 - \frac{\sum \lambda_{MPF,L}}{\sum(\lambda - \lambda_{SPF} - \lambda_{RF})}, \quad (4)$$

где $\lambda_{MPF,L}$ – интенсивность отказов, связанных с воспринимаемыми или выявляемыми множественными сбоями аппаратного средства. Вычисление полного МСС для систем, которые включают межсистемный компонент производится по выражению:

$$\text{МСС}_N = 1 - \frac{\sum_{i=0}^{N}\lambda_{MPF,L}}{\sum_{i=0}^{N}(\lambda - \lambda_{SPF} - \lambda_{RF})}. \quad (5)$$

Эти метрики являются относительными. Для использования FMEDA в анализе системы, которая включает межсистемный компонент, необходимо использовать таблицу FMEDA как часть таблицы FMEDA для ЦБ анализируемой системы, в работоспособности которой участвует LVDCU. Затем абсолютные значения метрик для межсистемного компонента будут уточнены. Пример фрагмента выполнения FMEDA представлен в табл. 5.

Таблица 5.
Пример фрагмента FMEDA для LVDCU для SG1

Table 5.
Example FMEDA fragment for LVDCU for SG1

Имя компонента	Интенсивность отказа, FIT	Потенциальные отказы	Распределение интенсивности отказа, FIT	Нарушает ЦБ	Механизм безопасности	ДО, %	SPF, FIT	Множественно нарушает ЦБ	Механизм безопасности	ДО, %	LF, FIT
VD2	1,015	Short	0,711	Да	-	-	0,711	Нет	-	-	-
		Open	0,203	Нет	-	-	-	Да	-	-	0,203
		Drift+	0,051	Нет	-	-	-	Да	-	-	0,051
		Drift-	0,051	Нет	-	-	-	Да	-	-	0,051
VD1	1,015	Short	0,812	Нет	-	-	-	Нет	-	-	-
		Open	0,203	Да	-	-	0,203	Нет	-	-	-

На рис. 3 изображена схема электрическая принципиальная, которая показывает соединения АК VD1 и VD2 для справочной информации.

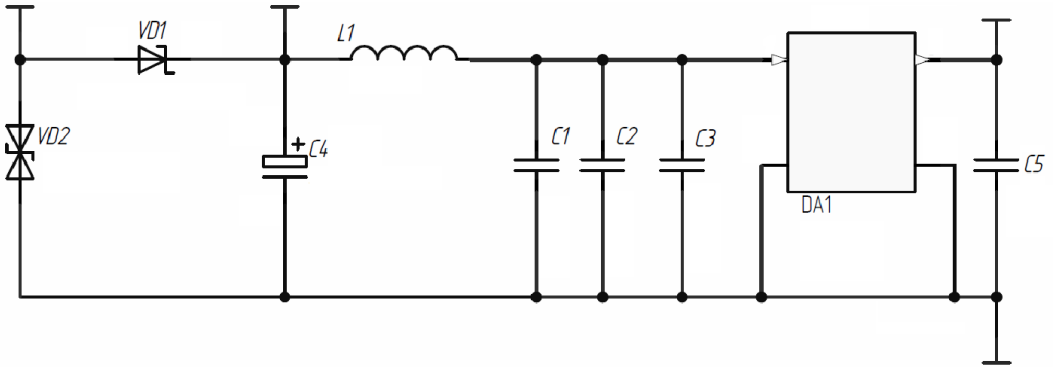

Рис. 3. Схема электрическая принципиальная

Fig. 3. Electrical schematic diagram

Продолжение анализа исследуемого объекта

Следующей стадией анализа ФБ LVDCU является разработка устройства на уровне ПО. Она включает в себя:

- спецификацию требования ФБ для ПО;
- архитектуру ПО;
- проектирование и реализацию ПО;
- интеграцию и верификацию ПО;
- тестирование ПО.

Из анализов ФБ для систем, в которых используется компонент, УПБТС для модулей ПО для межсистемных компонентов спускается по принципу «сверху-вниз». Анализ ПО межсистемного компонента должен проводится в соответствии с ISO-26262-6 и ISO-26262-9. На рис. 4 представлена схема распространения УПБТС для ПО межсистемного компонента.

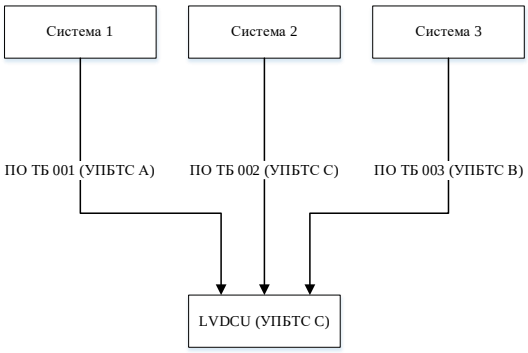

Рис. 4. Распространение УПБТС для ПО межсистемного компонента

Fig. 4. Extending the automotive safety integrity level to the intersystem component software

Следующей стадией является верификация ПО в соответствии с ISO-26262-6. Оно должно быть разработано в соответствии с требованиями ФБ, полученными в ходе анализа систем, работоспособность которых зависит от межсистемного компонента. Все требования из различных систем фокусируются на ПО межсистемного компонента. Проведение верификации ПО межсистемного компонента возможно без моделирования всей системы. Для определения влияния нарушения алгоритмов ПО на финальную систему должны быть проведены соответствующие испытания. ISO-26262-6 определяет список методов верификации для УПБТС и требований. Следующим этапом анализа являются интеграция и испытания. Они

должны быть проведены на уровне ПО/АК, техническом уровне, уровне системы. Полнота соответствия требований безопасности проверяется на всех уровнях анализа системы.

Заключение

Проведен анализ функциональной безопасности межсистемного компонента LVDCU. На стадии разработки устройства на уровне АК необходимые решения по увеличению безопасности улучшили BMCOA в 19,6 раз.

В результате настоящей работы были представлены выражения для расчета МОС и МСС для межсистемных компонентов, разработан и испытан алгоритм анализа ФБ применимый для межсистемных компонентов ТС. Стандартная методология ISO-26262 была адаптирована: требования АК и метрики должны быть реализованы в проекте по принципу «снизу-вверх» и применены в анализе всех систем, на работоспособность которых влияет межсистемный компонент; требования ФБ для модулей ПО наоборот должны быть проведены «сверху-вниз», из разных независимых систем.

Полученная измененная методология проведения анализа безопасности была апробирована и широко использована в таких проектах ФГУП НАМИ, как NAMI HYDROGEN [10] и AURUS MERLON [11].

Сокращения

ASIL / УПБТС	Automotive Safety Integrity Level / Уровень полноты безопасности транспортного средства
FIT	Failure In Time
FMD	Failure mode and Mechanism Distribution
FMEDA	Failure Modes and Effects Diagnostic Analysis
GP	General Purpose
HDBK	Handbook
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
L	Latent
LF	Latent Fault
LVDCU	Low Voltage Distribution Control Unit
MIL	Military
MPF	Multiple-Point Fault
RF	Residual Fault
RIAC	Reliability Information Analysis Center
SN	Siemens
SPF	Single-Point Fault
UTE	Utility Vehicle
АВПО	Анализ видов и последствий отказов
АДО	Анализ дерева отказов
АК	Аппаратный компонент
АОиОР	Анализ опасностей и оценка рисков
БУР	Блок управления реле
BMCOA	Вероятностная метрика для случайных отказов аппаратных средств
ВО	Внешнее освещение
ГР	Главное реле
ДО	Диагностический охват
ЖЦ	Жизненный цикл
КП	Комбинация приборов
МОС	Метрика единичных сбоев
МСС	Метрика скрытого сбоя

НВАБ	Низковольтная аккумуляторная батарея
ПО	Программное обеспечение
Р	Реализация
ТС	Транспортное средство
ФБ	Функциональная безопасность
ЦБ	Цель безопасности

Библиографический список

1. **Lu, K. L.** ISO 26262 ASIL-Oriented Hardware Design Framework for Safety-Critical Automotive Systems / K.L. Lu, Y.Y. Chen // IEEE International Conference on Connected Vehicles and Expo (ICCVE) – 2019. – ISBN 978-1-7281-0143-9
2. **Давлиева, А. С.** Оценка функциональной безопасности аппаратно-программных комплексов на основе ретроспективной, текущей и экспертной информации / А. С. Давлиева – Уфа: Уфимский государственный авиационный технический университет, 2022. – 139 с. – ISSN 2658-5014
3. **Knopf, M. D.** Comprehensive concept-phase system safety analysis for hybrid-electric vehicle utilizing automated driving function / M. D. Knopf – Fort Collins: Colorado State University, 2019. – 440 с.
4. **Самарин, А.** Функциональная безопасность электронных систем для автомобильного и промышленного рынка. Стандарты IEC 61508 и ISO 26262 и программа SafeAssure компании Freescale / А. Самарин // Компоненты и технологии. – 2015. – №8. – с. 128-134.
5. **Marchiò, F.** Automotive electronics: Application & technology megatrends / F. Marchiò // 40th European Solid State Circuits Conference (ESSCIRC) – 2014. – ISBN 978-1-4799-4378-4
6. **Clark, J. O.** System of Systems Engineering and Family of Systems Engineering From a Standards, V-Model, and Dual-V Model Perspective / J. O. Clark // 3rd Annual IEEE Systems Conference – 2009. – ISBN 978-1-4244-3462-6
7. Модели разработки ПО: Waterfall, V-model, Incremental, Iterative, Spiral model, Agile, Scrum, Kanban: сайт – URL: https://dzen.ru/a/ZawGm11Dd3_8rUTj (дата обращения 21.03.2025). – текст: электронный.
8. **Лепеева, И. Б.** Синтез методов ISO 26262 и ISO 21448 для повышения достоверности анализа опасностей и оценки рисков эксплуатации интеллектуальных систем помощи водителю / И. Б. Лепеева, П. С. Рогов // Труды НАМИ. – 2024. – №1. – с. 83-93 – ISSN 0135-3152
9. **Myklebust, T.** The Agile Safety Case / T. Myklebust, T. Stålhane – Cham: Springer Cham, 2018. – 235 с. – ISBN 978-3-319-70264-3
10. AURUS MERLON: официальный сайт – URL: https://merlon.nami.ru/ (дата обращения 17.02.2025). – текст: электронный.
11. NAMI HYDROGEN: официальный сайт – URL: https://hydrogen.nami.ru/ (дата обращения 17.02.2025). – текст: электронный.

Дата поступления
в редакцию: 18.04.2025

Дата принятия
к публикации: 25.07.2025