Общие положения обоснования функциональной безопасности интеллектуальных систем на железнодорожном транспорте

General provisions of the substantiation of functional safety of intelligent systems in railway transportation

Шубинский И.Б.[1]*, Розенберг Е.Н.[1]
Shubinsky I.B.[1]*, Rozenberg E.N.[1]
[1] АО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»), Москва, Российская Федерация
[1] Research and Design Institute for Information Technology, Signalling and Telecommunications in Railway Transportation (JSC NIIAS), Moscow, Russian Federation
**igor-shubinsky@yandex.ru*

Шубинский И.Б.

Розенберг Е.Н.

Резюме. Цель. *Материал статьи направлен на решение задачи объективной и уверенной оценки состояния функциональной безопасности (ФБ) интеллектуальных систем управления (ИСУ). Традиционные методы применительно к ИСУ не позволяют достаточно уверенно оценить реальное состояние ФБ вследствие их специфических особенностей. К этим особенностям относятся, в первую очередь, нечеткая архитектура ИСУ и изменяющиеся связи между элементами системы.* **Методы.** *Для обоснования ФБ ИСУ необходимо применять весь арсенал известных методов и средств, рекомендованных ГОСТ 33432-2015 [1], включая организационные меры, определяемые требованиями к политике, программе обеспечения безопасности и к доказательству безопасности. Проанализированы возможности доказательства ФБ ИСУ с помощью экспериментальных, экспертных, аналитических и технологических методов, методов имитационного моделирования. Установлены ограничения ряда методов применительно к обоснованию ФБ ИСУ.* **Результаты.** *Предложен эвристический графовый полумарковский (Марковский) метод для доказательства ФБ системы. Рекомендовано для обоснования ФБ ИСУ применять эвристический графовый метод в сочетании с технологическим методом, который определен стандартами ГОСТ Р МЭК 61508 [2–4] С их помощью возможно не только с уверенностью оценить состояние ФБ интеллектуальных систем, но и вырабатывать рекомендации по достижению приемлемых уровней безопасности таких систем.*

Abstract. Aim. *The paper aims to solve the problem of objective and confident functional safety (FS) evaluation of intelligent control systems (ICS). As regards ICS, the conventional methods, due to their particular features, do not allow for a sufficiently confident estimation of the actual state of FS. The above features include primarily the nondistinct architecture of ICS and the changing connections between the system elements.* **Methods.** *Substantiating ICS FS requires using the complete arsenal of known methods and means recommended in GOST 33432-2015 [1], including managerial measures defined by the requirements for the safety policy, program and case. The authors have analysed the capability to prove ICS FS using experimental, expert, analytical, technological, and simulation-based methods. The limitations of some methods as regards ICS FS substantiation have been established.* **Results.** *The authors suggest a heuristic graph-based semi-Markov (Markov) method of proving system FS. For the purpose of substantiating ICS FS, it is recommended using the heuristic graph-based method combined with the technological method defined in GOST R IEC 61508 [2–4]. They don't only allow confidently evaluating the FS of intelligent systems, but developing recommendations for achieving acceptable safety levels of such systems.*

Ключевые слова: *Безопасность функциональная, подтверждение безопасности, обоснование безопасности, программа обеспечения безопасности, доказательство безопасности, экспериментальный метод доказательства, экспертный метод, технологический метод доказательства, эвристический графовый полумарковский метод доказательства, доказательство с помощью имитационного моделирования.*
Keywords: *functional safety, safety confirmation, safety justification, safety program, safety case, experimental evidence, expert method, technological evidence, heuristic graph-based semi-Markov evidence, simulation-based evidence.*

Для цитирования: *Шубинский И.Б., Розенберг Е.Н. Общие положения обоснования функциональной безопасности интеллектуальных систем на железнодорожном транспорте // Надежность. 2023. №3. С. 38-45. https://doi.org/10.21683/1729-2646-2023-23-3-38-45*
For citation: *Shubinsky I.B., Rozenberg E.N. General provisions of the substantiation of functional safety of intelligent systems in railway transportation. Dependability 2023;3:38-45. https://doi.org/10.21683/1729-2646-2023-23-3-38-45*

Поступила: *17.05.2023* / **После доработки:** *29.06.2023* / **К печати:** *15.09.2023*
Received on: *17.05.2023* / **Revised on:** *29.06.2023* / **For printing:** *15.09.2023*

1.Введение

Использование накопленных знаний и формирование на их основе новых знаний – это научное направление получило свое развитие еще в 80-х годах прошлого века. Основная цель состояла в формировании экспертных оценок для решения многих прикладных задач, и, в первую очередь, для задач управления. Развитие вычислительных средств обеспечило возможность применения технологии Big Data для накопления и обработки огромных массивов неструктурированных данных. Чтобы работать с такими данными, применяют математическую статистику и методы машинного обучения с помощью алгоритмов Data Science, что позволяет формировать прогнозные модели и в итоге оптимально решать поставленные задачи.

На железнодорожном транспорте эти технологии также получили применение [5–8 и многие др.]. Особенно важную роль они играют в задачах автоведения подвижного состава. Здесь сформировалась достаточно общая архитектура автоматизированной системы управления, основанной на знаниях. Структура такой системы приведена на рис. 1.

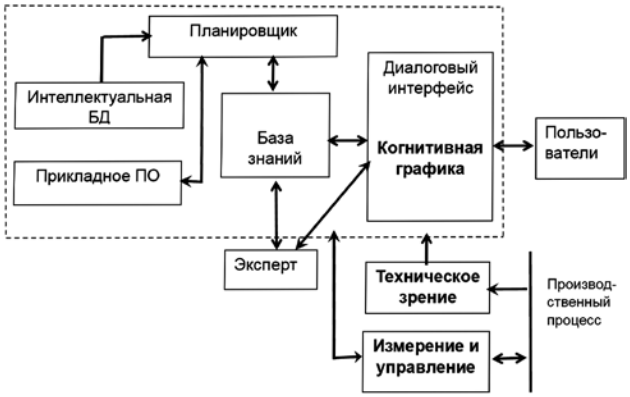

Рис. 1. Структурная схема интеллектуальной автоматизированной системы управления

Типовая часть интеллектуальной автоматизированной системы управления (ИСУ) (на рис. 1 обведена штриховой линией) содержит базы знаний и данных, планировщик, прикладное программное обеспечение (ПО) и диалоговый интерфейс. Эта часть системы имеет статичную структуру, практически не подвергается внешним возмущающим воздействиям, оперирует алгоритмами с постоянными параметрами и т.д. Автоведение подвижного состава управляется с помощью ИСУ, содержащей наряду с типовой частью развитые средства технического зрения, адаптивного управления и когнитивной графики (на рис. 1 эти средства системы обозначены жирным шрифтом). Они формируются на основе методов машинного обучения нейронных сетей. В ИСУ на железнодорожном транспорте в интересах оптимизации стоимости и функциональной безопасности стали применяться такие новые технологии как виртуальные каналы обработки информации, цифровые двойники, в также их сочетания совместно со средствами автоведения. Все это в совокупности и определяет следующие специфические особенности ИСУ:

Нечеткая архитектура системы;

1. Наличие технического зрения и зависимость от погодных условий;

2. Тесное информационное взаимодействие системы с реальным миром по информационным каналам связи;

3. Наличие большого и не всегда определенного количества уязвимостей в системе, тесно связанной с внешней средой;

4. Высокая вероятность изменения внешних воздействий из реального мира и изменения поведения системы при этом;

5. Изменение параметров алгоритмов управления в результате обучения нейронных сетей с помощью поступающих информационных потоков и накопленных баз данных;

6. Разветвленное программное обеспечение как типовой части системы, так и, особенно, средств обнаружения и управления движением подвижного состава.

Здесь следует отметить, что одной из ключевых особенностей ИСУ является то, что наряду с нечеткой архитектурой существенно изменяются связи в системе. Последнее обстоятельство значительно ограничивает возможности доказательства безопасности интеллектуальной системы.

2. Постановка задачи

При большой неопределенности как в архитектуре, так и в условиях функционировании системы, весьма проблематично доказывать ее функциональную безопасность, опираясь на традиционные методы, например, приведенные в СТО РЖД 1.19.009-2009 [9], которые широко применялись к устройствам и простым системам с установленном и ограниченным количеством уязвимостей. В ИСУ практически невозможно экспериментальным или/и расчетным путем доказать соответствие

уровня безопасности заданным требованиям (см. раздел 3 данной статьи). Следовательно, нужно изыскивать все доступные способы, чтобы убедиться в возможности (или невозможности) эксплуатировать ИСУ с приемлемым уровнем безопасности. Хорошим подспорьем в этом отношении могут служить рекомендации стандартов ГОСТ Р МЭК 61508-1-2012 (разделы 6, 8) [2], ГОСТ Р МЭК 61508-2-2012 [3], ГОСТ IEC 61508-3-2018 [4], ГОСТ Р /МЭК 62279-2016 [10]. В этих стандартах для оценки уровня функциональной безопасности сложных программно-аппаратных комплексов предложено наряду с традиционными подходами к доказательству учитывать технологию проектирования и изготовления, организацию работ по обеспечению качества и функциональной безопасности этих комплексов и их составных частей. Эти мероприятия и процедуры совместно решают задачи *обоснования безопасности*. Составная часть обоснования безопасности предусматривает подтверждение соответствия заданным требованиям, что в значительной мере реализуется с помощью методов доказательства безопасности. Развитие этого подхода в сочетании с накопленным методическим материалом на железнодорожном транспорте нашло отражение в стандарте ГОСТ 33432-2015 [1].

Применительно к интеллектуальным системам с указанными в разделе 1 особенностями в данном стандарте рекомендован следующий состав работ по обоснованию безопасности:

Разработка политики обеспечения функциональной безопасности (ФБ);

Разработка программы обеспечения ФБ;

Разработка доказательства ФБ.

Политика обеспечения ФБ должна быть сформирована в организации разработчике ИСУ и является общей при разработке всех изделий этой организации. Она должна предусматривать решение следующих основных вопросов:

- цели и задачи обеспечения ФБ;
- принципы и подходы к обеспечению ФБ;
- принципы управления рисками, связанными с ФБ;
- организация обеспечения ФБ.

Для управления рисками в работе [11] предложено применять материалы проекта ATO-RISK, заказанного немецким центром исследований железнодорожного транспорта. Этот проект направлен на определение критерия приемлемости рисков для автоматизированного вождения по железной дороге. Как описано в работе [11], для оценки уровня риска проводится явный анализ риска в зависимости от функции, либо используются справочные системы. Явный анализ рисков проводится путем оценки различных сценариев на основе полуколичественного подхода с помощью матрицы баллов риска. В матрице качественно дифференцируют ожидаемую степень ущерба в соответствии с классами аварий. Указанный подход может быть рекомендован при решении задач формирования политики безопасности ИСУ.

Программа работ по обеспечению ФБ и доказательство ФБ разрабатываются для каждого изделия автономно и предназначены для представления заказчику в качестве доказательства того, что изделие выполнено качественно, согласно требованиям стандартов по ФБ и соответствует заявленному уровню полноты безопасности (УПБ).

Программа работ по обеспечению ФБ наряду с разделами «Нормативные ссылки», «Характеристика объекта», «Порядок отчетности», «Порядок корректировки» содержит два следующих ключевых раздела:

- Мероприятия по обеспечению ФБ;
- Организация работ по обеспечению ФБ.

На рис. 2 приведен перечень работ по реализации ключевых разделов Программы работ по обеспечению безопасности (ПОБ).

Важно подчеркнуть, что наряду с решением задач по обеспечению ФБ, анализу опасностей и управления рисками, верификации и валидации ИСУ большое значение придается вопросам организации работ. Эти работы предусматривают подготовку и аттестацию должностных лиц в области ФБ, организацию взаимодействия с соисполнителями и заказчиком, организацию материально-технического обеспечения.

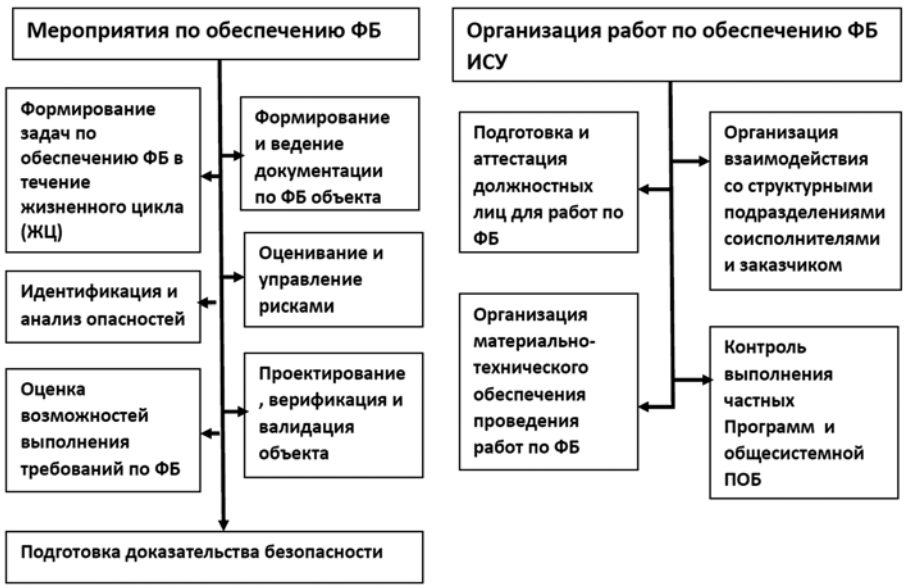

Рис. 2. Перечень работ по реализации разделов ПОБ

Конечная цель мероприятий по обеспечению ФБ ИСУ состоит в подготовке доказательства безопасности.

В состав работ по доказательству ФБ (рис. 3) входят отчеты не только по состоянию ФБ, но и о принятых разработчиком ИСУ мерах по управлению качеством и обеспечению ФБ. Эти отчеты

позволяют заказчику оценить уровень и качество производства ИСУ, включая поставки комплектующих, организацию и технологический уровень работ по обеспечению ФБ, результаты оценки рисков, глубину и качество работ по верификации и валидации требованиям ФБ.

Заключение о соответствие ИСУ требованиям ФБ формируется на основе материалов отчета о состоянии ФБ с учетом указанных раннее отчетов по мерах по управлению качеством и ФБ. Это очень существенный момент. Дело в том, что нечеткая архитектура ИСУ, изменение параметров алгоритмов управления в результате обучения нейронных сетей и другие особенности функционирования интеллектуальных систем не способствуют гарантированной оценке состояния их ФБ. Использование материалов отчетов о принятых мерах по управлению качеством и ФБ значительно усиливает информационное описание системы и повышает уверенность в достоверности оценки состояния ее ФБ.

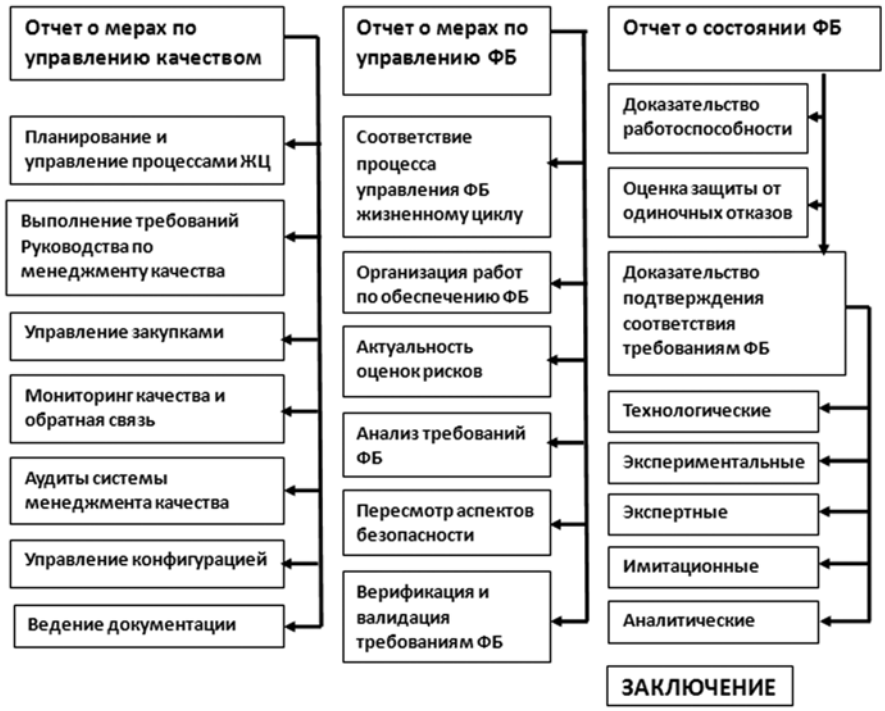

Рис. 3. Состав работ по доказательству ФБ

Непосредственно отчет о состоянии ФБ включает в себя как материалы исследования в отношении подтверждения соответствия заданным требованиям по ФБ, так и результаты экспериментальной оценки работоспособности и защищенности системы от одиночных отказов. Экспериментальная оценка производится на основе согласованной с испытательной лабораторией программы и методики испытаний.

Подтверждение соответствия заданным требованиям по ФБ играет ключевую роль в документе Доказательство ФБ системы. Вместе с тем, применительно к ИСУ подтверждение ее соответствия требованиям ФБ представляет собой достаточно сложную задачу. Рассмотрим этот вопрос более подробно.

3. Подтверждение соответствия ИСУ заданным требованиям по ФБ

Для подтверждения соответствия ИСУ требуемому уровню ФБ можно рекомендовать следующие методы:

- экспериментальные;
- экспертные;
- имитационные;
- аналитические;
- технологические.

Состав работ по доказательству ФБ приведен на рис. 3.

Экспериментальные методы позволяют наиболее объективно количественно оценить состояние ФБ системы при условии того, что установлена их реализуемость и достоверность. Вопрос реализуемости находится в прямой зависимости от требований к ФБ. Для характерного требования к уровню полноты безопасности ИСУ с частыми запросами на выполнение задач составляет УПБ 2, что соответствует требуемому диапазону значений интенсивности опасных отказов системы $\lambda_{ОП}=(10^{-7}–10^{-6})1/ч$. При этом вероятность опасных отказов системы в течение часа работы должна находиться в диапазоне значений $Q_{ОП}(1)=10^{-7}–10^{-6}$ [2]. При этих требованиях для экспериментального определения только одного опасного отказа потребуется провести не менее $N \geq \frac{1}{Q(1)} = (10^7 - 10^6)$ испытаний. Поскольку каждое испытание следует проводить в течение времени не менее одного часа, то для определения только одного опасного отказа потребуется затратить более 100 лет. При экспоненциальном распределении (что типично для распределения времени между опасными отказами) для получения достоверности испытаний на уровне доверительной вероятности 0,9 потребуется наблюдать не менее 10 событий опасных отказов, что вынудит увеличить время испытаний еще в несколько раз. Все это ставит под сомнение реализуемость применения экспериментальных методов испытаний.

Экспертные методы в принципе позволяют косвенно подтвердить или не подтвердить соответствие ИСУ заданным требованиям по ФБ. Естественно, что косвенная оценка не может быть самостоятельной – она должна использоваться как дополнение к другим оценкам. Технология экспертной оценки показателей сложных систем хорошо развита, так же, как и математический аппарат обработки мнений экспертов. Однако применение этих

методов к вопросам оценки уровня ФБ системы имеет ряд сложностей. Прежде всего, опыт эксплуатации ИСУ на железнодорожном транспорте еще незначителен. Накопленных знаний явно недостаточно. Следовательно, трудно рассчитывать на приемлемый уровень компетенции экспертов по этой тематике. Кроме того, в различных отраслях, в частности на железнодорожном транспорте, очень ограничен круг специалистов в области ФБ. Поэтому весьма проблематично подобрать достаточное число экспертов и оценить согласованность их мнений. Однако нужно стремиться к этому, что позволит в определенной мере использовать экспертные методы для подтверждения соответствия ИСУ.

Методы имитационного моделирования – широко применяемые при разработке и испытаниях. Они основаны на методе Монте-Карло. Метод имитационного моделирования Монте-Карло позволяет с помощью датчиков псевдослучайных чисел смоделировать практически весь известный спектр входных, промежуточных и возмущающих воздействий на систему, обработать их путем программной имитации системы и сформировать выходные результаты в зависимости от смоделированных данных. Однако этот метод имеет крупный недостаток – разброс выходных результатов от реализации к реализации. Для сокращения разброса выходных результатов, т.е. уменьшения их дисперсии, необходимо большое количество реализаций модели, что, в свою очередь, приводит к резкому увеличению времени моделирования. Для сокращения времени моделирования разработан ряд методов понижения дисперсии. К ним относятся: модифицированный метод Монте-Карло (например, моделирование по ценности данных и результатов), метод дополняющих переменных, метод расслоенной выборки и др. Более эффективные результаты в понижении дисперсии обеспечивает метод взвешенного моделирования или иначе метод значимой выборки. На основе этого метода нами был разработан метод имитационного моделирования на основе полунатурных испытаний [12] путем искусственного введения в систему неисправностей (сбоев, помех, программных ошибок). Несмотря на очевидные успехи в области имитационного моделирования, эти методы имеют ряд существенных недостатков, вследствие которых их применение к исследованию ИСУ ограничено.

Основными ограничениями в применении методов имитационного моделирования применительно к ИСУ являются:

1. Требуется детальное описание моделируемой системы и ее особенностей, что для такой сложной системы (см. рис. 1) требует значительных усилий и связанного с ними большого объема работы;

2. Большая себестоимость создания имитационной модели системы;

3. Требуется доказательство адекватности модели реальной системе;

4. При каждом уточнении структуры системы и при доработках ее алгоритмов требуется выполнять работы, указанные выше в пп. 1 и 3, фактически это сводится к созданию новых имитационных моделей.

Аналитические методы – основной инструмент доказательства ФБ систем. Однако возможность их применения к задачам обоснования безопасности ИСУ вызывает определенные сомнения. Это связано, в первую очередь, с нечеткой архитектурой таких систем и, следовательно, трудностями (а порой невозможностью) формализовать задачи доказательства безопасности. Для преодоления этой проблемы нами предлагаются ***эвристические полумарковские (Марковские) графовые методы***. Дело в том, что решение неформализованных задач доказательства безопасности систем с нечеткой архитектурой базируется на эвристиках – *некоторых собственных представлениях человека, правилах, позволяющих сократить пространство перебора при поиске решения.*

Суть разработанных методов [13, 14, 15] состоит в сочетании эвристики в представлениях данных и математических моделей безопасности и надежности системы со строгими математическими методами анализа. Примерами возможностей графовых математических методов для анализа ФБ могут служить некоторые приведенные ниже формулы расчета ряда показателей безопасности:

- *вероятность первого попадания системы* из i-го начального неопасного состояния ($i \in S_H$, $S_H \cap \overline{S}_H = \varnothing$, $S_H \cap \overline{S}_H = S$) *в любое опасное состояние* $i \in \overline{S}_{ПБ}$ $i \in \overline{S}_H$ определяется выражением:

$$b_{if} = \frac{\sum\limits_{f \in \overline{S}_H} \sum\limits_{k} l_k^{if} \Delta G_k^i}{\Delta G_{\overline{S}_H}};$$

- *средняя наработка до защитного отказа*

$$T_З = \frac{T_0 \Delta G^0_{S_З \cup \overline{S}_н} + \sum\limits_{k} l_k^{0i} T_i \Delta G_k^i}{\Delta G_{S_З \cup \overline{S}_н}};$$

- *среднее время между опасными отказами*

$$T_Б = \frac{\sum\limits_{i \in S_H} \Delta G^i T_i}{\sum\limits_{i \in S_+} \Delta G^i \sum\limits_{j \in \overline{S}_H} p_{ij}};$$

- *коэффициент безопасности системы*

$$K_Б = \frac{\sum\limits_{i \in S_Н} \Delta G^i T_i}{\sum\limits_{j \in S} \Delta G^j T_j},$$

где $G(S, H)$ – ориентированный граф состояний, S – конечное множество вершин (состояний) системы; H – конечное множество дуг между вершинами i, j (состояния S_i, S_j); T_i – математическое ожидание безусловного времени пребывания системы в i-ом состоянии; p_{ij} – вероятность перехода из состояния i в состояние j графа; l_k^{if} – k-ый путь, ведущий из неопасного состояния

графа $i \in \overline{S}_H$ в опасное состояние $f \in \overline{S}_H$; – вес разложения графа без i-ой вершины и вершин графа, расположенных на k-ом пути; $\Delta G_{\overline{S}_Y}$ – вес разложения графа без вершин множества опасных состояний; $\Delta G_{S_З \cup \overline{S}_H}$ – вес разложения графа без множества опасных состояний $\overline{S}_H$ и множества защитных состояний $S_З$.

Веса разложений графа рассчитываются по формуле Мэзона:

$$\Delta G = 1 - \sum_i C_i + \sum_{i,j} C_i C_j - \sum_{i,j,r} C_i C_j C_r + ...,$$

где C_i, C_j… – веса контуров на графе.

Принятые критерии опасного и защитного отказов.

Критерий опасного отказа в виде множества состояний опасного отказа $\overline{S_н} \subset S$, где $S_н \cap \overline{S_н} = \varnothing$, $S_н \cup \overline{S_н} = S$, множества работоспособных или неопасных состояний $S_н \subset S$, а также начальное состояние $0 \equiv S_0$ (или $i \equiv S_i$), где $S_i \subset S_н$;

Критерий защитного отказа в виде множества защитных состояний $S_З \subset S_н$, множества работоспособных или неопасных и незащитных состояний $\overline{S_З} \subset S_н$, где $S_З \cap \overline{S_З} = \varnothing$, $S_З \cup \overline{S_З} = S_н$, а также начальное состояние $0 \equiv S_0$ (или i $\equiv S_З$), где $S_i \subset \overline{S_З}$.

В условиях неопределенности или отсутствия некоторых данных и нечеткости архитектуры системы аналитическая оценка безопасности системы достигается путем многоэтапных расчетов, которые состоят в реализации следующей цепочки действий (рис. 4).

При наличии доверенных сведений и данных достаточно ограничиться только отдельными действиями, например построением графа, определением формульных выражений, расчетом и анализом результатов. Другие действия, например, экспертная оценка исходных данных, определение наиболее значимых факторов, упрощение расчетных формул, уточнение условий для построения графа, повторное построение (или повторные построения) графа ФБ ИСУ возникают по мере необходимости в зависимости от наличия или отсутствия информации, которой располагает оценщик ФБ системы. В работах [16–20] при аналитической оценке ФБ интеллектуальных систем с виртуальными каналами, цифровыми двойниками, систем автоведения подвижного состава, автоведения маневровых локомотивов соответственно нами выполнялись практически все указанные на рис. 4 действия, поскольку были недостаточно достоверные данные об архитектурах исследуемых систем, неполные сведения об исходных случайных величинах и их законах распределения. Вместе с тем, полученные результаты позволили не только в определенной мере оценить ожидаемые уровни полноты безопасности исследуемых систем, но, что особенно важно, и выработать рекомендации по достижению приемлемых уровней их функциональной безопасности. Полученные в указанных работах результаты согласуются с инженерными оценками безопасности исследуемых систем и соответствуют практическим наблюдениями за безопасностью опытных образцов интеллектуальных систем.

Вместе с тем, вследствие неполноты и нечеткости исходных данных и вследствие отмеченных выше специфических особенностей интеллектуальных систем эвристические графовые методы не в полной мере обеспечивают высокий уровень уверенности в результатах оценки состояния ФБ.

Для повышения уверенности при оценивании ФБ целесообразно руководствоваться рекомендациями стандартов ГОСТ Р / МЭК 61508-1,2-2012 [2, 3], ГОСТ IEC 61508-3-2018 [4], ГОСТ Р /МЭК 62279-2016 [10] и широко применять *технологические методы подтверждения соответствия требованиям* ФБ.

Оценка достигнутого уровня полноты безопасности (УПБ) для каждой функции безопасности аппаратных средств ИСУ возможна на основе рекомендации п. 7.4 ГОСТ Р / МЭК61508-2-2012.

Оценка меры примененных методов и средств по управлению отказами производится с помощью рекомендаций стандартов ГОСТ Р / МЭК 61508-2-2012 в части таблиц А.15–А.17 и ГОСТ Р /МЭК 61508-7-2012 в части приложений А, В.

Оценка примененных методов и средств по предотвращению систематических отказов может производиться в соответствии с приложениями В.1–В.4 стандарта ГОСТ Р / МЭК 61508-2-2012.

В отношении ПО ИСУ в стандарте ГОСТ IEC 61508-3-2018 рекомендованы следующие процедуры, относящиеся к технологическим методам подтверждения соответствия:

- оценка примененных методов и средств к спецификации и проектированию ПО для каждого УПБ (приложение А);

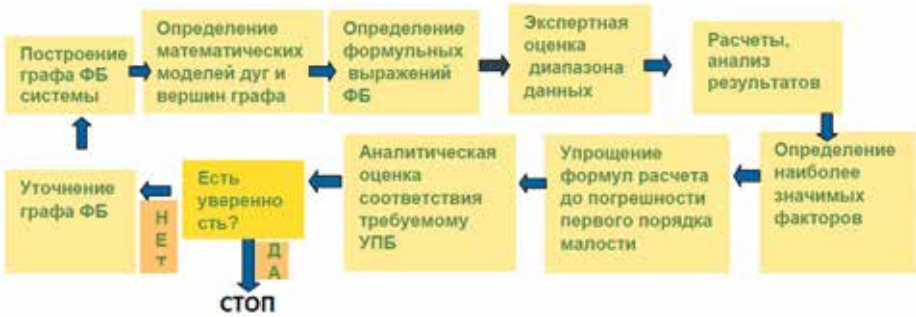

Рис. 4. Последовательность действий с помощью эвристических графовых методов

- оценка примененных методов и средств по предотвращению систематических отказов ПО (п. В.7);

- оценка качества интеграции ПО с аппаратными средствами ИСУ (приложения А, В);

- оценка руководства по безопасности ПО (приложение D)

4. Заключение

Обоснование ФБ ИСУ относится к категории задач исследования систем с неполными и недостаточно достоверными данными, с нечеткой архитектурой самих систем, с функционированием в условиях плохо формализованных воздействий на них. При этом сохраняется необходимость гарантированной оценки соответствия (или несоответствия) системы требованиям по ФБ. Для такой оценки необходимо использовать всю доступную информацию и все имеющиеся возможности для всесторонней оценки состояния ФБ ИСУ с учетом принятых мер при разработке и изготовлении системы. Целесообразно максимально реализовать возможности экспериментальных и экспертных методов, методов имитационного моделирования, аналитических и технологических методов подтверждения соответствия. Вследствие ограниченных возможностей экспериментальных и экспертных методов, а также методов имитационного моделирования, желательно акцентировать усилия на применении технологических и эвристических графовых методах. С их помощью возможно не только с уверенностью оценить состояние ФБ интеллектуальных систем, но и вырабатывать рекомендации по достижению приемлемых уровней безопасности таких систем.

Библиографический список

1. ГОСТ 33432-2015. Безопасность функциональная. Политика, Программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. М.: Стандартинформ, 2019. IV, 23 с.

2. ГОСТ Р / МЭК 61508-1-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования. М.: Стандартинформ, 2014. V, 52 с.

3. ГОСТ Р МЭК 61508-2-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам. М.: Стандартинформ, 2014. IV, 80 с.

4. ГОСТ IEC 61508-3-2018. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению. М.: Стандартинформ, 2018. V, 107 с.

5. Santur Y. Random forest based diagnosis approach for rail fault inspection in railways / Santur Y., Karakose M., Akin E. // National Conference on Electrical, Electronics and Biomedical Engineering. 2016. Pp. 714-719.

6. Famurewa S.M. Maintenance analytics for railway infrastructure decision support / Famurewa S.M., Zhang L., Asplund M. // Journal Qual. Maint. Eng. 2017. Vol. 23. Pp. 310–325.

7. Nakhaee M.C. The Recent Applications of Machine Learning in Rail Track Maintenance: A Survey / Nakhaee M.C., Hiemstra D., Stoelinga M., van Noort M. // Lecture Notes in Computer Science. 2019. Pp. 91–105.

8. Шубинский И.Б., Замышляев А.М., Проневич О.Б. и др. Применение методов машинного обучения для прогнозирования опасных отказов объектов железнодорожного пути // Надежность. 2020. № 20(2). С. 43-53.

9. СТО РЖД 1-19.009-2009 . Системы и устройства железнодорожной автоматики и телемеханики Доказательство безопасности.

10. ГОСТ Р /МЭК 62279-2016 Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах. М.: Стандартинформ, 2017. V, 95 с.

11. Braband J, Shabe H. Risk analysis for automated driving – validation and findings // Signal+ Draht. 2023. Vol. 115(4).

12. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. М.: «Журнал Надежность» , 2016. 546 с, ил.

13. Розенберг Е.Н. Многоуровневая система управления и обеспечения безопасности движения поездов : Дис. … д-ра техн. наук : 05.13.06, 05.22.08 : Москва, 2004. 317 с.

14. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность» , 2012. 216 с, ил.

15. Шубинский И.Б., Розенберг Е.Н. Функциональная безопасность систем управления на железнодорожном транспорте. Вологда: «Инфра-Инженерия», 2023, 360 с.

16. Шубинский И.Б., Шебе Х., Розенберг Е.Н. О функциональной безопасности сложной технической системы управления с цифровыми двойниками // Надежность. 2021. № 1. С. 38-44.

17. Розенберг Е.Н., Ольшанский А.М., Озеров А.В., Сафронов Р.А. Об использовании методов Big Data в области обеспечения функциональной безопасности // Надежность. 2022. № 22(2). С. 38-46.

18. Шубинский И.Б., Шебе Х., Розенберг Е.Н. К оценке безопасности системы автоведения поездов // Надежность. 2021. № 21(4). С. 31-37.

19. Шубинский И.Б., Розенберг Е.Н., Коровин А.С. и др. О методе обеспечения функциональной безопасности системы с одноканальной обработкой информации // Надежность. 2022. № 22(3). С. 44-52.

20. Шубинский И.Б., Розенберг Е.Н., Панферов И.А. и др. Оценка безопасности и бесперебойности работы системы управления маневровым локомотивом с техническим зрением // Надежность. 2023. № 23(1). С. 30-37.

References

1. GOST 33432-2015. Functional safety. Policy and programme of safety provision. Safety proof of the railway objects. Moscow: Standartinform; 2019. (in Russ.)

2. GOST R / IEC 61508-1-2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements. Moscow: Standartinform; 2014. (in Russ.)

3. GOST R / IEC 61508-2-2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for electrical, electronic, programmable electronic safety-related systems. Moscow: Standartinform; 2014. (in Russ.)

4. GOST IEC 61508-3-2018. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3. Software requirements. Moscow: Standartinform; 2018. (in Russ.)

5. Santur Y., Karakose M., Akin E. Random forest based diagnosis approach for rail fault inspection in railways. In: Proceedings of the National Conference on Electrical, Electronics and Biomedical Engineering; 2016. Pp. 714-719.

6. Famurewa S.M., Zhang L., Asplund M. Maintenance analytics for railway infrastructure decision support. *Journal Qual. Maint. Eng.* 2017;23:310–325.

7. Nakhaee M.C., Hiemstra D., Stoelinga M., van Noort M. The Recent Applications of Machine Learning in Rail Track Maintenance: A Survey. *Lecture Notes in Computer Science* 2019. Pp. 91–105.

8. Shubinsky I.B., Zamyshliaev A.M., Pronevich O.B. et al Application of machine learning methods for predicting hazardous failures of railway track assets. *Dependability* 2020;2:45-53.

9. STO RZD 1-19.009-2009. [Railway automation systems and devices. Safety case]. (in Russ.)

10. GOST R / IEC 62279-2016. [Railways. Communications, signalling and data processing systems]. Moscow: Standartinform; 2017. (in Russ.)

11. Braband J., Shäbe H. Risk analysis for automated driving – validation and findings. *Signal+Draht* 2023;115(4):6-12.

12. Shubinsky I.B. [Dependable failsafe information systems. Synthesis methods]. Moscow: Dependability Journal; 2016. (in Russ.).

13. Rozenberg E.N. [Multi-level train control and protection system: Doctor of Engineering thesis]. 05.13.06, 05.22.08. Moscow; 2004. (in Russ.).

14. Shubinsky I.B. [Structural dependability of information systems. Analysis methods]. Moscow: Dependability Journal: 2012. (in Russ.).

15. Shubinsky I.B., Rozenberg E.N. [Functional safety of control systems in railway transportation]. Vologda: Infra-Inzheneria; 2023. (in Russ.)

16. Shubinsky I.B., Schäbe H., Rozenberg E.N. On the functional safety of a complex technical control system with digital twins. *Dependability* 2021;1:38-44.

17. Rozenberg E.N., Olshansky A.M., Ozerov A.V., Safronov R.A. Big data based methods for proof of functional safety. *Dependability* 2022;22(2):38-46.

18. Shubinsky I.B., Shäbe H., Rozenberg E.N. On the safety assessment of an automatic train operation system. *Dependability* 2021;21(4):31-37.

19. Shubinsky I.B., Rozenberg E.N., Korovin A.S. et al. On a method for ensuring functional safety of a system with single-channel information processing. *Dependability* 2022;22(3):44-52.

20. Shubinsky I.B., Rozenberg E.N., Panfiorov I.A. et al. Estimating the safety and reliability of the control system of a locomotive with machine vision. *Dependability* 2023;23(1):30-37.

Сведения об авторах

Шубинский Игорь Борисович – профессор, доктор технических наук, заместитель руководителя НТК АО «НИИАС», Москва, Российская Федерация, e-mail: igor-shubinsky@yandex.ru

Розенберг Ефим Наумович – профессор, доктор технических наук, первый заместитель Генерального директора АО «НИИАС», Москва, Российская Федерация, e-mail: info@vniias.ru

About the authors

Igor B. Shubinsky, Professor, Doctor of Engineering, Deputy Director of Integrated Research and Development Unit, JSC NIIAS, Moscow, Russian Federation, e-mail: igor-shubinsky@yandex.ru.

Efim N. Rozenberg, Professor, Doctor of Engineering, First Deputy Director General, JSC NIIAS, Moscow, Russian Federation, e-mail: info@vniias.ru.

Вклад авторов

Шубинский И.Б. – разработка эвристического графового полумарковского метода и порядка его практического применения в сочетании с технологическим методом оценки уровня полноты безопасности системы.

Розенберг Е.Н. – постановка задачи обоснования функциональной безопасности интеллектуальных систем управления и оценка ограничений в применении для этих целей статистических, экспертных методов, а также методов имитационного моделирования.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.