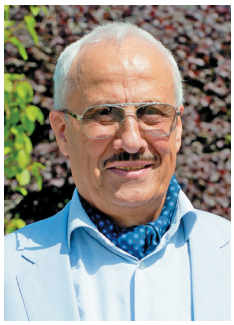
Оригинальная статья
https://doi.org/10.21683/1729-2646-2021-21-4-31-37

К оценке безопасности системы автоведения поездов

Игорь Б. Шубинский[1]*, Хендрик Шебе[2], Ефим Н. Розенберг[1]
[1]АО «НИИАС», Москва, Российская Федерация
[2]TÜV Rheinland, Кельн, Германия
**igor-shubinsky@yandex.ru*



Игорь Б. Шубинский

Хендрик Шебе

Ефим Н. Розенберг

Резюме. *В статье рассмотрена система автоведения в составе системы управления и безопасности локомотива, средств центра слежения (контроля) бортовых и стационарных средств технического зрения. Сосредоточено внимание на зависимости безопасности и надежности этой системы от характеристик надежности составных элементов и влиянии возмущающих погодных воздействий. Сформулированы критерии опасного и защитного отказа системы, построены графовые модели состояний безопасности и надежности системы автоведения. Приведены предпосылки для применения графового Марковского метода расчета безопасности и надежности сложных систем. Это позволило определить такие ключевые показатели безопасности системы автоведения, как среднее время до опасного отказа, вероятность опасного отказа, интенсивность опасных отказов. В результате исследования установлено, что безопасность системы автоведения зависит, главным образом, от уровней надежности средств технического зрения. При этом рост интенсивности опасных отказов системы ограничен величиной половины интенсивности отказов средства технического зрения. Установлено также то, что надежность системы автоведения определяется интенсивностью отказов системы управления и безопасности локомотива и интенсивностью отказов средств технического зрения.*
Проведенный анализ позволяет сделать вывод, что для достижения приемлемого уровня безопасности системы автоведения следует сосредоточить усилия на дублировании средств технического зрения, достижении функциональной безопасности бортового и стационарного средств технического зрения на уровне SIL 4, а также на регулярном сравнении результатов бортового и стационарного средств технического зрения, дублировании результатов сравнения, сглаживании этих результатов в процессе движения локомотива. Кроме того, целесообразно парирование возмущающих погодных воздействий путем повышения эффективности машинного обучения программных средств технического зрения

Ключевые слова: *система автоведения, техническое зрение, безопасность, надежность, Марковская модель, граф состояний, опасный отказ, защитный отказ.*

Для цитирования: *Шубинский И.Б., Шебе Х., Розенберг Е.Н. К оценке безопасности системы автоведения поездов // Надежность. 2021. №4. С 31-37. https://doi.org/10.21683/1729-2646-2021-21-4-31-37*

Поступила *27.07.2021 г.* / **После доработки** *16.11.2021 г.* / **К печати** *14.12.2021 г.*

Введение

Обеспечение безопасности сложной технической системы, обработка информации в которой осуществляется на уровне нейронных сетей, требует особых методов доказательства безопасности [1].

Главная проблема в разработке такого метода состоит именно в том, что вышеуказанная вычислительная система непостоянна в структуре алгоритма обработки информации, и к доказательству ее безопасности трудно применить классические методы вероятностной оценки в виде двух и более независимых аппаратно-программных обработчиков информации, применения разных программных продуктов в обработчиках и т.д. [2].

Именно поэтому дублирование таких обработчиков информации в виде камер технического зрения на локомотивах для безопасного определения препятствия на пути вряд ли получит требуемый уровень по безопасности, исходя из неизвестной величины времени тестирования такой самообучаемой, т.е. все время изменяемой, системы обработки ответственной информации.

В работе Брабанда и Шебе [1] предполагалось использовать статистические методы доказательства безопасности системы, а также обязательного наличия в структуре обрабатывающего комплекса дополнительного устройства, безопасность которого можно доказать традиционными способами за счет его неизменяемой структуры.

В работах Шубинского и Розенберга [3, 4] было предложено использовать так называемые многоуровневые структуры для доказательства безопасности, которые позволяют интегрировать безопасные и информационные системы с введением критерия обработки информации под требования безопасности. Данный подход хорошо себя зарекомендовал при разработке современных бортовых и стационарных систем безопасности. Также было использовано крайне важное свойство оценки безопасности системы – получение достоверной информации о предыстории состояния объекта с точки зрения безопасности.

Целесообразно применительно к задаче доказательства безопасности интеллектуальной системы с наличием нейронной сети применить принципы многоуровневой системы безопасности. Отличие при этом состоит в том, что нужно рассматривать не отдельный интеллектуальный прибор, например, камеру технического зрения на локомотиве, а весь комплекс технических средств в зоне движения локомотива.

Действительно, работа камеры на локомотиве с заранее созданной программой обработки информации о препятствии на пути зависит не только от принятых ранее мер по обучению нейронной сети, но и от конкретных факторов, влияющих на исправность аппаратных средств камеры, сбоев программного обеспечения и т. д. Кроме того, следует отметить, что влияние внешней среды – снег, туман, дождь – приводит к изменению показателей зоны обнаружения препятствия, что впрямую влияет на безопасность, т. к. связано с длиной тормозного пути поезда.

В данных условиях применяется дополнительный контроль за ситуацией впереди поезда из специального диспетчерского центра, где за несколькими локомотивами наблюдает машинист-оператор [5].

Сложность этого метода состоит в том, что критическим звеном становится реакция машиниста-оператора, а он сам зависит от устойчивости видеоизображения камеры на борту и надежности средств широкополосной радиосвязи в данной точке.

С другой стороны, разделение процесса обработки информации на два подпроцесса – в виде внутренней интеллектуальной обработки информации на борту для принятия решения о свободности пути и в виде передачи исходной визуальной информации машинисту-оператору для принятия им решения – позволяет повысить безопасность. Критерием здесь является то, что бортовая система должна иметь большую вероятность ложной тревоги, а машинист-оператор может исправить эту ситуацию путем специальной команды, передаваемой по радиоканалу на локомотив. На практике без применения этого принципа беспилотные системы останавливались бы, например, из-за пластикового пакета на пути.

Следует отметить, что в состав комплекса входят и стационарные устройства, контролирующие свободность пути в местах с плохой видимостью [5]. Информация от этих стационарных систем передается на локомотив в режиме реального времени, что значительно повышает безопасность движения поездов. Таким образом, примененная модель является упрощенной, но она позволяет аналитически проанализировать проблему. В этом состоит превосходство данного подхода к построению модели исследования по сравнению с более сложными моделями. Интересной особенностью взаимодействия стационарных и локомотивных устройств технического зрения является то, что они в одинаковой ситуации состояния внешней среды могут видеть одни и те же объекты, в прямой их видимости или с различных, в том числе инверсных точек наблюдения.

Наличие объектов, определяемых двумя независимыми системами, позволяет использовать это свойство для взаимного контроля интеллектуальных технических средств, особенно для выработки корректного решения бортовыми интеллектуальными системами, которые работают в более тяжелых уровнях эксплуатации (скорость движения, ограничения по зоне видимости и т. д.). Результат сравнения объектов может быть сформирован в виде сравнения обработанных стационарными и подвижными камерами в виде заранее обработанных моделей изображения, а может содержать предполагаемую инверсию изображения одного и того же объекта, если на него осуществляется направление камер технического зрения с противоположных точек. Такое заранее сформированное свойство для системы безопасности сравнения результатов позволяет повысить уровень независимости при обработке информации. Каждое техническое средство, в том числе видеокамеры, содержит элементы внутреннего тестирования как обязательный фактор при расчете уровня их безопасной работы. Учитывая, что в интеллектуальной системе при использовании нейронных систем трудно однозначно говорить о полноте тестирования, то целесообразно задействовать

фактор самодиагностики по заранее известным объектам наблюдения. Например, рядом с железнодорожными путями, в зоне сканирования камеры технического зрения или лидаров, находятся светофоры, шкафы управления, мачты электроснабжения и связи, которые четко привязаны к координатам пути, тем более если на локомотиве будет применяться 3D карта объектов инфраструктуры.

Таким образом, фиксация этих объектов позволяет фактически тестировать камеры и датчики на локомотиве с учетом параметров дистанции обнаружения и расшифровки видов объектов. Если частота контроля таких объектов достаточно высока, то на расстоянии движения локомотива между этими точками можно рассчитать вероятность отсутствия отказов или искажения алгоритма обработки информации на подвижном объекте. Достоинством этого метода является полнота обработки информации, когда совместно с внутренними тестированиями аппаратных средств можно добиться требуемого уровня безопасности системы. Сама система в этом случае представляется как «черный ящик», но с абсолютно известными выходными результатами в абсолютно известной координате пространства.

Концептуальная модель безопасности системы автоведения поездов

В составе системы автоведения локомотива содержатся следующие ключевые средства:

- средства системы управления и безопасности локомотива;
- технические средства центра слежения (контроля);
- стационарные средства «технического зрения»;
- бортовые средства «технического зрения».

Концептуальная модель безопасности системы автоведения локомотива содержит описание состояний надежности и безопасности составных средств системы, их взаимосвязи, а также влияние возмущающих погодных воздействий. Эта модель представлена в виде графа состояний безопасности системы (рис. 1).

При построении модели безопасности системы принят следующий критерий ее **опасного отказа**: отказ всех средств «технического зрения» и центра слежения (контроля) или необнаруженный отказ системы управления и безопасности локомотива. Критерий **защитного отказа**: отказ стационарных средств технического зрения, центра слежения (контроля) и влияние возмущающих погодных воздействий или обнаруженный отказ системы управления и безопасности локомотива.

Все множество состояний системы, согласно графу состояний на рис. 1, разделяется на следующие подмножества:

- подмножество работоспособных состояний S_p={0, 2, 3, 4, 5};
- подмножество защитных состояний $S_З$={1, 8};
- подмножество опасных состояний $S_О$={6, 7}.

Работоспособные и защитные состояния образуют множество исправных состояний.

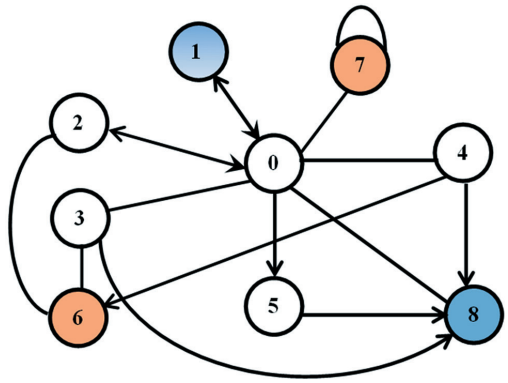


Рис. 1. Граф состояний безопасности системы автоведения поездов

Состояния графа: 0 – исправное состояние, возмущающих погодных воздействий нет; 1 – обнаруженный отказ системы управления и безопасности локомотива – **защитный отказ;** 2 – отказ технических средств центра слежения (контроля); 3 – отказ стационарных средств технического зрения; 4 – отказ бортовых средств технического зрения; 5 – возмущающие погодные воздействия; 6 – отказ всех средств «технического зрения» и центра слежения (контроля) – **опасный отказ** системы автоведения; 7 – необнаруженный отказ системы управления и безопасности локомотива – **опасный отказ;** 8 – отказ стационарных средств технического зрения, центра слежения (контроля) и возмущающие погодные воздействия – **защитный отказ.**

Переходы в модели в исправных состояниях, требующие пояснения: 1-0, 2-0, 3-0, 8-0 – восстановления технических средств после их отказов; 3-8 – отказ средств центра слежения при условии отказа стационарных средств «технического зрения»; 4-8 – отказ средств центра слежения при условии отказа бортовых средств «технического зрения»; 7-8 – отказ стационарных средств «технического зрения» при условии возмущающих погодных воздействий.

При математическом описании модели будем исходить из следующих соображений. Система новая, еще не имеет аналогов, статистических данных о ней нет. Поэтому законы распределения случайных величин в системе не установлены. Исходя из имеющегося опыта в отношении систем управления на железнодорожном транспорте, можно с большой долей уверенности предположить, что отказы электронных устройств, таких как устройства системы управления и безопасности локомотива, технических средств центра слежения (контроля) и средств технического зрения, распределены по экспоненциальному закону. Эта предпосылка не распространяется на случайные величины времени восстановления устройств после отказов и, тем более, на случайные погодные возмущающие воздействия. Проблема возмущающих воздействий теоретически исследована в работах Шебе и Фиртла [6], эти модели также применимы к возмущающим погодным воздействиям. Чтобы обеспечить адекватность результатов, авторы вынуждены были применить

сложное математическое описание случайного процесса возмущающих воздействий на систему управления движением локомотива. Эти обстоятельства затрудняют их практическое использование в математическом моделировании безопасности системы автоведения.

При отсутствии практических сведений весьма проблематично строить прогнозы относительно количественных значений показателей безопасности системы автоведения. В данной работе мы стремимся в условиях большой неопределенности выявить наиболее существенные факторы, влияющие на безопасность системы. Этой цели соответствует применение предпосылки о простейших потоках случайных событий в системе автоведения. Простейшие потоки отличаются свойствами ординарности, стационарности и отсутствия последействия. Их применение вследствие большой неопределенности исходных условий, с одной стороны, не способствуют точности прогнозирования характеристик безопасности поведения системы. С другой стороны, полученные при этом выходные результаты можно расценивать в качестве гарантированных снизу предпосылок (как наихудший случай) к построению безопасной системы автоведения путем нейтрализации выявленных наиболее значимых негативных факторов. Таким образом, примененная модель является упрощенной, но она позволяет выполнить анализ проблемы. Это – превосходство данного подхода по сравнению с более сложными моделями.

Основываясь на приведенных предпосылках, примем экспоненциальными распределения отказов $F_i(t)$ и восстановлений $Q_i(t)$ составных технических средств:

$F_i(t) = 1–\exp(–\lambda_i t)$, $i = 1...4$; $Q_i(t) = 1–\exp(–\mu_j t)$,

где λ_1 – интенсивность отказов системы управления и безопасности локомотива; λ_2 – интенсивность отказов средств центра слежения (контроля); λ_3 – интенсивность отказов стационарных средств технического зрения; λ_4 – интенсивность отказов бортовых средств технического зрения; μ_1 – интенсивность восстановления отказов системы управления и безопасности локомотива; μ_2 – интенсивность восстановления отказов средств центра слежения (контроля); μ_3 – интенсивность восстановления отказов бортовых средств технического зрения; μ_4 – интенсивность восстановления отказов стационарных средств технического зрения и средств центра слежения (контроля).

Предполагается, что отказ системы управления и безопасности локомотива обнаруживается с вероятностью правильного обнаружения α. Вероятность пропуска отказа системы локомотива есть $\bar{\alpha} = 1 - \alpha$. Вероятность ложного обнаружения ничтожно мала.

Исходя из указанных выше предпосылок, примем закон распределения случайных погодных возмущающих воздействий в виде $H(t)=1–\exp(–\gamma t)$, где γ – интенсивность их влияния на безопасность системы автоведения.

При приведенных предпосылках поведение системы автоведения в отношении ее безопасности представляется Марковским случайным процессом.

С этой целью находим входные параметры модели безопасности системы в подмножествах исправных (работоспособных и защитных) состояний согласно графу на рис. 1.

Функции распределения безусловного времени пребывания системы, представленной графом состояний на рис. 1, в исправных состояниях имеют следующие выражения:

$$F_0(t) = 1 - \exp\left(-\left[\gamma + \sum_{i=1}^{4} \lambda_i \right] \cdot t \right); \; F_1(t)=1–\exp(–\mu_1 t);$$

$$F_2(t)=1–\exp(–[\lambda_3+\mu_2]\cdot t); \; F_3(t)=1–\exp(–[\lambda_2+\lambda_4+\mu_3]\cdot t);$$

$$F_4(t)=1–\exp(–[\gamma+\lambda_2]\cdot t);$$

$$F_5(t)=1–\exp(–\lambda_4 t); \; F_8(t)=1–\exp(–\mu_4 t). \qquad (1)$$

Опасные состояния 6 и 7, а также входящие в эти состояния дуги, исключены из математического описания, поскольку исследуется процесс поведения системы автоведения до попадания в опасные состояния.

Математические ожидания времени пребывания системы в исправных состояниях:

$$T_0 = \int_0^\infty \left(1 - F_0(t)\right) dt = \frac{1}{\gamma + \sum_{i=1}^{4} \lambda_i}; \; T_1 = \int_0^\infty e^{-\mu_1 t} dt = \frac{1}{\mu_1};$$

$$T_2 = \int_0^\infty e^{-\lambda_3 t} e^{-\mu_2 t} dt = \frac{1}{\lambda_3 + \mu_2};$$

$$T_3 = \int_0^\infty e^{-\lambda_2 t} \cdot e^{-\lambda_4 t} \cdot e^{-\mu_3 t} dt = \frac{1}{\lambda_2 + \lambda_4 + \mu_3};$$

$$T_4 = \int_0^\infty e^{-\gamma t} e^{-\lambda_2 t} dt = \frac{1}{\gamma + \lambda_2};$$

$$T_5 = \int_0^\infty e^{-\lambda_4 t} dt = \frac{1}{\lambda_4}; \; T_8 = \int_0^\infty e^{-\mu_4 t} dt = \frac{1}{\mu_4}. \qquad (2)$$

Вероятности переходов между состояниями i, j системы определяются по формуле $p_{ij} = \int_0^\infty \lambda_{ij} [1 - F_i(t)] dt$, где λ_{ij} – интенсивность перехода системы из состояния i в состояние j. Например, интенсивность перехода из начального состояния 0 в состояние 1 (рис. 1) обнаруженного отказа системы управления и безопасности локомотива равна $\lambda_{01}=\alpha\cdot\lambda_1$, тогда как интенсивность перехода из состояния 0 в состояние 7 необнаруженного отказа этой системы (опасный отказ системы) вычисляется как $\lambda_{07} = \bar{\alpha} \cdot \lambda_1$.

Таким образом,

$$p_{01} = \frac{\alpha\lambda_1}{\gamma + \sum_{j=1}^{4} \lambda_j}; \; p_{0i} = \frac{\lambda_i}{\gamma + \sum_{j=1}^{4} \lambda_j}, \; i = 2,3,4;$$

$$p_{05} = \frac{\gamma}{\gamma + \sum_{j=1}^{4} \lambda_j}; \; p_{10} = p_{58} = p_{80} = 1; \; p_{20} = \frac{\mu_2}{\lambda_3 + \mu_2};$$

$$p_{30} = \frac{\mu_3}{\lambda_2 + \lambda_4 + \mu_3}; \; p_{38} = \frac{\lambda_2}{\lambda_2 + \lambda_4 + \mu_3}; \; p_{48} = \frac{\gamma}{\lambda_2 + \gamma}. \qquad (3)$$

Результаты анализа показателей безопасности системы автоведения поездов

Используя графовый Марковский метод расчета безопасности сложных систем Шубинского [7], можно определить такие ключевые показатели безопасности системы автоведения, как среднее время до опасного отказа $T_{\text{ОП}}$, вероятность опасного отказа $G_{\text{ОП}}(t)$, интенсивность опасных отказов $\lambda_{\text{ОП}}$.

Ключевой показатель безопасности – среднюю наработку до опасного отказа $T_{\text{ОП}}$ системы определяют с помощью метода [8] по формуле

$$T_{\text{ОП}} = \frac{T_1 \Delta G^1_{S_{\text{ОП}}} + \sum_{(k)} \sum_{i,j} l^{ij}_k \Delta G^j_k T_j}{\Delta G_{S_{\text{ОП}}}}, \quad (4)$$

где $\Delta G^1_{S_{ОП}}$ – вес разложения графа без начальной вершины 1 и множества опасных состояний $S_{\text{ОП}}=\{6,7\}$ и связанных с ними дуг графа; $\Delta G_{S_{\text{ОП}}}$ – вес разложения графа без множества опасных состояний и связанных с ними дуг графа; l^{ij}_k – вес k-го пути из вершины i в вершину j; ΔG^j_k – вес разложения графа без вершин, расположенных на k-ом пути и без вершины j в множестве неопасных состояний $S_{\text{Н}}=\{0,1,2,3,4,5,8\}$.

Веса разложений можно определить с помощью формулы Мейсона [8]

$$\Delta G = 1 - \sum_i C_i + \sum_{ij} C_i C_j - \sum_{ijk} C_i C_j C_k + ...,$$

где веса контуров находят в множестве неопасных состояний (рис. 1)

$$C_1=p_{01}\cdot p_{10};\ C_2=p_{02}\cdot p_{20};\ C_3=p_{03}\cdot p_{30};\ C_4=p_{03}\cdot p_{38}\cdot p_{80};$$
$$C_5=p_{04}\cdot p_{48}\cdot p_{80};\ C_6=p_{05}\cdot p_{58}\cdot p_{80}. \quad (5)$$

Все контуры пересекающиеся, т.к. имеют общую вершину 0.

Руководствуясь графом на рис. 1 и подставляя выражения (1), (2), (3) в формулу (4), находим в множестве неопасных состояний $S_{\text{Н}}=\{0,1,2,3,4,5,8\}$

$$T_{\text{ОП}} = \frac{T_0 + \sum_{i=1}^{5} p_{0i} T_i + (p_{03}p_{38} + p_{04}p_{48} + p_{05}p_{58})\cdot T_8}{\Delta G_{S_{\text{ОП}}}}, \quad (6)$$

где вес разложения графа без опасных состояний $\Delta G_{S_{\text{ОП}}} = 1 - \sum_{i=1}^{6} C_i$ и веса контуров вычисляются по формуле (5).

Поскольку в реальных системах управления между интенсивностями восстановлений и отказов электронных средств имеет место соотношение $\lambda_i << \mu_i$, то с погрешностью, не превышающей первого порядка малости, можно существенно упростить формульные выражения исходных параметров модели. При этом следует принять во внимание, что интенсивность восстановления стационарных электронных средств, таких как центр слежения (контроля) и технического зрения, практически одинаковы, а некоторые отклонения в пределах десятков процентов неощутимо влияют на конечные результаты в условиях отмеченного выше соотношения между интенсивностями отказов и восстановлений. Тогда $\mu_2=\mu_4=\mu$ и $\mu_1=\mu_3=k\mu$, $(0<k\leq 1)$, где k – коэффициент учета логистических задержек в восстановлении отказов бортовых средств системы автоведения.

Указанные изменения в исходных параметрах касаются функций распределения $F_1(t) \cong 1-\exp(-k\mu\cdot t)$, $F_2(t) \cong 1-\exp(-\mu\cdot t)$, $F_3(t) \cong 1-\exp(-k\mu\cdot t)$, математических ожиданий $T_2 \cong \frac{1}{\mu}$ и $T_1 \cong T_3 \cong \frac{1}{k\mu}$, вероятностей переходов $p_{20} \cong p_{30} \cong 1$, $p_{38} \cong \frac{\lambda_2}{k\mu}$.

Действительно, по требованиям нормативного документа, NPRD-2011 camera sub-assembly [9] интенсивность отказов средств технического зрения должна составлять $\lambda_2 = \lambda_4 = 2{,}3\cdot 10^{-5}$, а центра слежения (контроля) $\lambda_3 = 2{,}8\cdot 10^{-5}$. Согласно EN 50129 [10] интенсивность отказов системы управления и безопасности локомотива должна соответствовать уровню SIL 4, т.е. $\lambda_1 \leq 10^{-8}$. При этом согласно IEC 61508-2 (A4, первая строка) [12] вероятность пропуска отказа должна быть меньше уровня $\bar{\alpha} \leq 0{,}01$. Интенсивность восстановления отказов электронных программируемых средств системы автоведения в большинстве случаев превышает значение $\mu \geq 2$, что превышает интенсивности отказов на 4 и более порядков. Это позволяет в пределах приемлемой погрешности исключать из формульного выражения те составляющие суммирования, которые на несколько порядков меньше других членов этих сумм.

Указанные соображения позволяют раскрыть формульное выражение (6) среднего времени до опасного отказа системы автоведения до приемлемого прикладного математического выражения

$$T_{\text{ОП}} = \frac{\dfrac{k\mu + \alpha\lambda_1 + \lambda_3 + k(\lambda_2+\lambda_4)}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)k\mu} + \dfrac{\gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)\lambda_4} + \left[\dfrac{\lambda_3\cdot\lambda_2}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)k\mu} + \dfrac{\lambda_4\cdot\gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)(\lambda_2+\gamma)} + \dfrac{\gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)}\right]\cdot\dfrac{1}{\mu}}{\Delta G_{S_{\text{ОП}}}},$$

где

$$\Delta G_{S_{\text{ОП}}} = 1 - p_{01}p_{10} - p_{02}p_{20} - p_{03}p_{30} - p_{03}p_{38}p_{80} - p_{04}p_{48}p_{80} - p_{05}p_{58}p_{80} \cong 1 - \frac{\alpha\lambda_1 + \lambda_2 + \lambda_3 + \gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)} - \frac{\lambda_3}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)}\frac{\gamma}{(\gamma+\lambda_2)} - \frac{\lambda_4}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)}\frac{\lambda_2}{k\mu}. \quad (7)$$

После преобразования формулы (7) находим, что с погрешностью, не превышающей первого порядка малости, среднее время до опасного отказа системы автоведения может быть представлено в виде

$$T_{ОП} \cong \frac{\lambda_4(\gamma+\lambda_2+\lambda_4)+\gamma\cdot(\gamma+\lambda_2)}{\lambda_4(\overline{\alpha}\cdot\lambda_1+\lambda_4)(\gamma+\lambda_2)}, \qquad (8)$$

Предельное значение наработки системы автоведения поезда до опасного отказа имеет место при отсутствии деструктивных возмущающих погодных условий ($\gamma \to 0$) и при выполнении требований IEC 61508-2 [11] ($\alpha \to 0$). Подставляя эти значения в формулу (8), получаем результат математического моделирования. Он свидетельствует о том, что безопасность системы автоведения зависит, главным образом, от уровней надежности средств технического зрения, т.е.

$$T_{ПРЕД} \le \frac{\lambda_2+\lambda_4}{\lambda_2\lambda_4} = \frac{1}{\lambda_4}+\frac{1}{\lambda_2}.$$

При близких значениях интенсивности отказов стационарных и бортовых средств технического зрения данное выражение преобразуется к виду

$$\lambda_2 \cong \lambda_4 = \lambda;\ \text{следовательно}\ T_{ПРЕД} \le \frac{2\lambda}{\lambda^2} = 2\cdot T,$$

где T – среднее время до отказа средства технического зрения.

Так как поток опасных отказов системы многократно разрежен относительно потока неопасных отказов исходного объекта, который является простейшим, то согласно работам [12, 13] многократно разреженный случайным образом простейший поток отказов также является простейшим с постоянным параметром

$$\lambda_{ОП} = 1/T_{ОП} = \frac{\lambda_4(\overline{\alpha}\cdot\lambda_1+\lambda_4)(\gamma+\lambda_2)}{\lambda_4(\gamma+\lambda_2+\lambda_4)+\gamma(\gamma+\lambda_2)}. \qquad (9)$$

В пределе интенсивность опасных отказов системы автоведения стремится к величине

$$\lambda_{ОП} \to \frac{\lambda_2\cdot\lambda_4}{\lambda_2+\lambda_4} \cong \frac{\lambda}{2}(\lambda_2 \approx \lambda_4), \qquad (10)$$

то есть, к половине величины интенсивности отказов средства технического зрения.

Вероятность опасного отказа с погрешностью, не превышающей первого порядка малости, определяется в виде

$$G_{ОП}(t) \cong \lambda_{ОП}\cdot t \to \frac{\lambda}{2}t.$$

Результаты анализа показателей надежности системы автоведения поездов

Модель надежности системы автоведения трансформируется из концептуальной модели безопасности этой системы (рис. 1) путем исключения из нее опасных состояний и связанных с ними дуг. Граф состояний модели надежности приведен на рис. 2.

Для решения задачи анализа надежности данной системы ограничимся определением среднего времени

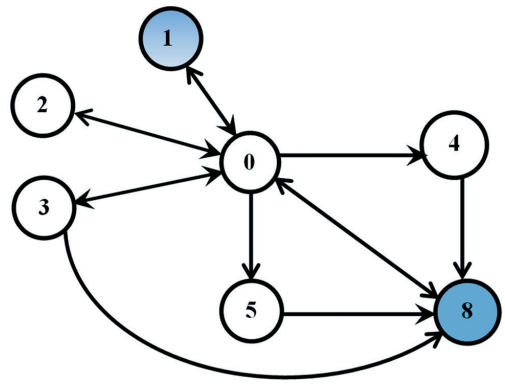


Рис. 2. Граф состояний надежности системы автоведения поездов

ее пребывания в множестве работоспособных состояний $S_р = \{0, 2, 3, 4, 5\}$. Этот показатель есть не что иное, как средняя наработка системы до защитного отказа. Целесообразность анализа именно этого показателя обусловлена тем, что для повышения безопасности стремятся в каждом тревожном случае переводить систему в защитное (нерабочее) состояние. Поэтому важно установить, какие факторы оказывают определяющее влияние на надежность системы с техническим зрением при построении ее с данной архитектурой.

Руководствуясь графом на рис. 2, с помощью метода [7] находим

$$T_З = \frac{T_0 + p_{02}T_2 + p_{03}T_3 + p_{04}T_4 + p_{05}T_5}{1 - p_{02}p_{20} - p_{03}p_{30}}.$$

При принятых в пп. 2 и 3 предпосылках и допущениях данное выражение представляется в виде

$$T_З = \frac{(\lambda_2+\gamma)(\lambda_4+\gamma)+\lambda_4^2}{\lambda_4(\lambda_2+\gamma)(\lambda_1+\lambda_4+\gamma)} + \frac{\lambda_2\mu_3+\lambda_3\mu_2}{\mu_2\mu_3(\lambda_1+\lambda_2+\gamma)}. \qquad (11)$$

Как отмечалось ранее в п. 2, согласно нормативным требованиям документа NPRD-2011 camera sub-assembly [9] интенсивность отказов средств технического зрения должна составлять $\lambda_2 = \lambda_4 = 2{,}3\cdot10^{-5}$, а центра слежения (контроля) – $\lambda_3 = 2{,}8\cdot10^{-5}$. Следовательно, с приемлемой для оценки точностью можно принять, что $\lambda_2 \cong \lambda_3 \cong \lambda_4 = \lambda$. Кроме того, средства технического зрения и центра слежения в подавляющем большинстве содержат электронные средства, интенсивность восстановления которых находится примерно на одинаковом уровне $\mu \ge 2$. Следовательно, можно принять, что $\mu_2 \cong \mu_3 = \mu$ и выражение (11) преобразуется к виду

$$T_З = \frac{(\lambda+\gamma)^2+\lambda_4^2}{\lambda(\lambda+\gamma)(\lambda_1+\lambda+\gamma)} + \frac{2\lambda}{\mu(\lambda_1+\lambda+\gamma)}. \qquad (12)$$

Как и при оценке безопасности системы, примем что предельное значение наработки системы автоведения поезда до защитного отказа имеет место при отсутствии деструктивных возмущающих погодных условий ($\gamma \to 0$). Тогда формула (12) примет следующий вид:

$$T_З \to \frac{2}{\lambda_1+\lambda}\left(1+\frac{\lambda}{\mu}\right).$$

Как отмечалось в п. 2, в данной задаче имеет место условие $1 >> \frac{\lambda}{\mu}$. Учитывая это, находим предельную оценку надежности системы автоведения поездов по критерию средней наработки до защитного отказа

$$T_3 \to \frac{2}{\lambda_1 + \lambda}. \quad (13)$$

Следовательно, надежность системы автоведения определяется интенсивностью отказов системы управления и безопасности локомотива (λ_1) и средств технического зрения (λ). Именно эти объекты системы автоведения должны быть в центре внимания при обеспечении приемлемого уровня надежности системы.

5. Заключение

Проведенный анализ позволяет сделать вывод, что для достижения приемлемого уровня безопасности системы автоведения следует сосредоточить усилия на следующем:

- дублирование средств технического зрения;
- достижение функциональной безопасности бортового и стационарного средств технического зрения на уровне SIL 4 (двухканальность и двухверсионность программного обеспечения, исполнение независимых каналов и др.);
- регулярное сравнение результатов бортового и стационарного средств технического зрения, дублирование результатов сравнения, сглаживание этих результатов в процессе движения локомотива.

При этом необходимо обеспечить выполнение требований стандарта EN 50129 к функциональной безопасности системы управления и безопасности локомотива на уровне SIL 4. Кроме того, целесообразно парирование возмущающих погодных воздействий путем повышения эффективности машинного обучения программных средств технического зрения.

Исследование подтвердило то обстоятельство, что безотказность системы управления и безопасности локомотива оказывает решающее влияние на надежность системы автоведения.

Библиографический список

1. Брабанд Й., Шебе Х. Оценка безопасности искусственного интеллекта // Надежность. 2020. Т. 19. № 4. С. 25-34.

2. Сапожников В.В., Сапожников Вл.В., Христов Х.А., Гавзов Д.В. Методы построения безопасных микроэлектронных систем железнодорожной автоматики / Под ред.: Сапожникова Вл.В. М.: Транспорт, 1995. 272 с.

3. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. М.: Журнал Надежность, 2017. 544 с.

4. Розенберг Е.Н. Многоуровневая система управления и обеспечения безопасности движения поездов: дис. … д-ра техн. наук. Моск. гос. ун-т путей сообщения (МИИТ), Москва, 2004.

5. Патент 2742960. Российская Федерация, МПК B61L 25/02. Бортовая информационная система: № 2020131633: заявл. 25.09.2020: опубл. 12.02.2021 Бюл. № 5 / Мыльников П.Д., Охотников А.П., Попов П.А.

6. Schäbe H., Viertl R. An Axiomatic Approach to Models of Accelerated Life Testing // Eng. Fract. Mechanics. 1995. Vol. 50. No. 2. P. 203-217.

7. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: Журнал Надежность, 2012. 212 с.

8. Mason S.J. Feedback Theory – Further Properties of Signal Flow Graphs //Proceedings of the IRE. 44: 920–926. doi:10.1109/jrproc.1956.275147

9. NPRD-2011 Nonelectronics Parts Reliability Data. Utica, N.Y.: Reliability Information Analysis Center, 2011.

10. EN 50129 Railway applications – Communication, signalling and processing system – Safety related electronic systems for signalling, 2018.

11. IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems,Parts 1-7, 2011;

12. Григелионис Б.И. О точности приближения композиции процессов восстановления пуассоновским процессом // Литов. матем. сб. 1962. Т. 2. № 2. С. 135-143.

13. Назаров А.А., Лопатин И.Л. Ассимптотические пуассоновские MAP-потоки // Известия Томского государственного университета (Управление, вычислительная техника и информатика). 2010. № 4(13). С. 72-78.

Сведения об авторах

Игорь Борисович Шубинский – доктор технических наук, профессор, заместитель руководителя НТК АО «НИИАС», ул. Нижегородская, д. 27, стр.1, Москва, Российская Федерация, 109029, тел. +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

Хендрик Шебе – доктор физико-математических наук, заведующий отделом анализа рисков и опасностей, TÜV Rheinland InterTraffic, Кельн, Германия, e-mail: schaebe@de.tuv.com

Ефим Наумович Розенберг – доктор технических наук, профессор, первый заместитель Генерального директора АО «НИИАС», ул. Нижегородская, д. 27, стр.1, Москва, Российская Федерация, 109029, e-mail: info@vniias.ru

Вклад авторов в статью

Шубинский И.Б. – разработка и решение моделей безопасности и надежности системы автоведения, анализ результатов.

Шебе Х. – анализ публикаций в области безопасности систем автоведения поездов, подготовка экспериментальных данных, участие в разработке моделей безопасности и надежности системы автоведения и анализе полученных результатов исследования.

Розенберг Е.Н. – постановка задачи исследования, участие в разработке модели безопасности системы автоведения, участие в анализе результатов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.