Оценка безопасности и бесперебойности работы системы управления маневровым локомотивом с техническим зрением

Estimating the safety and reliability of the control system of a locomotive with machine vision

Шубинский И.Б.[1], Розенберг Е.Н.[1], Панферов И.А.[1]*, Бояринова Н.А.[1], Кузьмин А.И.[1]
Shubinsky I.B.[1], Rozenberg E.N.[1], Panfiorov I.A.[1], Boyarinova N.A.[1], Kuzmin A.I.[1]
[1]АО «НИИАС», Москва, Российская Федерация
[1]JSC NIIAS, Moscow, Russian Federation

**i.panferov@vniias.ru*


Шубинский И.Б.


Розенберг Е.Н.


Панферов И.А.


Бояринова Н.А.


Кузьмин А.И.

Резюме. Цель. *Целью настоящей статьи является оценка показателей безопасности и бесперебойности комплекса технических средств, обеспечивающих управление локомотивом – маневровой автоматической локомотивной сигнализации (МАЛС). Повышение показателей достигается за счет использования дополнительного контроля, в качестве которого предлагается использование второго виртуального канала, позволяющего правильно обнаруживать отказы МАЛС, при этом не влияя на работу алгоритмов управления маневровым локомотивом.* **Методы.** *В данной статье применен графовый метод. С помощью модифицированного топологического полумарковского метода выведены формулы расчета средней наработки до отказа и коэффициента безопасности.* **Результаты.** *В представленной статье проведено отдельное рассмотрение среднего времени пребывания системы автоведения маневрового локомотива на уровне не ниже SIL3 и среднего времени работы до опасного отказа. Исследована зависимость данных показателей от интенсивности отказов технических средств МАЛС и интенсивности отказов технического зрения. С помощью графового метода проведена оценка уровня функциональной безопасности системы путем расчета коэффициента безопасности и коэффициента опасности. Исследованы зависимости данных коэффициентов от времени восстановления системы и вероятности обнаружения отказов составных элементов.*

Abstract. Aim. *The paper aims to evaluate the indicators of safety and reliability of the MALS suite of technology that ensures the control of locomotives. Increased indicators are achieved through the use of additional controls. As such, a second virtual channel is proposed. The latter allows detecting MALS failures without affecting the shunting engine control algorithms.* **Methods.** *The paper uses the graph method. Using a modified topological semi-Markov method, formulas were deduced for calculating the mean time to failure and the safety factor.* **Results.** *The paper individually examines the mean time of the automatic train operation system of a shunting engine remaining in at least SIL3 and mean time to hazardous failure. The authors research the dependence of the above indicators on the failure rate of the MALS equipment and the machine vision. Using the graph method, the level of the system's functional safety was evaluated by calculating the safety factor and the danger factor. The dependence of the above factors on the system recovery time and probability of detection of component failures was examined.*

Ключевые слова: *система управления локомотивом МАЛС, техническое зрение, бортовое устройство безопасности, графовая модель, функциональная безопасность.*
Keywords: *MALS locomotive control system, machine vision, onboard train protection system, graph model, functional safety.*

Для цитирования: *Шубинский И.Б., Розенберг Е.Н., Панферов И.А., Бояринова Н.А., Кузьмин А.И. Оценка безопасности и бесперебойности работы системы управления маневровым локомотивом с техническим зрением // Надежность. 2023. №1. С. 30-37. https://doi.org/10.21683/1729-2646-2023-23-1-30-37*
For citation: *Shubinsky I.B., Rozenberg E.N., Panfiorov I.A., Boyarinova N.A., Kuzmin A.I. Estimating the safety and reliability of the control system of a locomotive with machine vision. Dependability 2023;1:30-37. https://doi.org/10.21683/1729-2646-2023-23-1-30-37*

Поступила *18.01.2023* / **После доработки** *09.02.2023* / **К печати** *14.03.2023*
Received on: *18.01.2023* / **Revised on:** *09.02.2023/* **For printing:** *14.03.2023.*

Введение

Для решения одной из ключевых проблем на железнодорожном транспорте – создания беспилотных технологий – в настоящее время системы железнодорожной автоматики и телемеханики претерпевают новую стадию своего развития. В их состав наряду с традиционными средствами обеспечения функциональной безопасности вводятся достаточно сложные системы автоведения поездов [1]. Теперь для обеспечения безопасности движения уже нельзя ограничиваться алгоритмами управления, основанными только на логических и некоторых арифметических операциях. Технологическое развитие систем управления связано с решением сложных математических задач и в перспективе с массовым использованием для обработки информации нейронных сетей.

Простота технологических задач для первого уровня безопасности позволяла использовать хорошо отработанные методы обеспечения требований функциональной безопасности за счет дублирования аппаратных и программных средств [2]. При этом очевидным преимуществом использования более простых технических средств в виде жесткой логики и микроконтроллеров являлась простота контроля исправностей при онлайн-тестировании и, соответственно, возможность достижения требований уровней интенсивности опасного отказа [3].

В процессе разработки систем автоведения стало очевидно, что интенсивность их опасных отказов будет не выше SIL2. Применение опытных образцов таких систем на сети дорог ОАО «РЖД» показало, что в принципе это человеко-машинные комплексы, в которых техническим средствам автоведения нельзя в полной мере доверять безопасность движения поездов без участия оператора.

Класс таких систем, решающих задачи безопасности движения на станции при маневровой работе, относится к уровню SIL2. Это связано с тем, что скорости передвижения состава при маневровой работе значительно меньше, чем при поездной работе [4]. Вместе с тем следует учитывать тяжелый характер работы машиниста на маневровом локомотиве и, по возможности, автоматизировать некоторые его функции. Таким образом, даже при присутствии машиниста на локомотиве необходимо в перспективе ставить задачи выполнения требования на уровне, близком к SIL3 или вводить новую детализацию градации уровня общения безопасности движения SIL2+. Этот технический уровень средств обработки информации может быть достигнут с помощью операционной системы реального времени и высокопроизводительных микропроцессоров. Здесь сразу возникает проблема достоверности обработки информации и полноты онлайн-тестов. Стремление использовать сложные микропроцессорные комплексы, с одной стороны, и желание иметь резерв по их избыточности, с другой стороны, затрудняет такой контроль. Действительно, в структуре обработки информации используется малый объем памяти и ограниченный набор команд. В этих условиях нельзя обеспечить высокий уровень гарантий полноты теста, поскольку многие элементы структуры обработки информации не задействованы. Это, в свою очередь, приводит к ограничениям в обеспечении приемлемого уровня правильного обнаружения отказов маневровой автоматической локомотивной сигнализации (МАЛС).

2. Постановка задачи. Модель исследования

2.1. Постановка задачи

В настоящее время система управления маневровым локомотивом МАЛС одноканальная, что не позволяет поднять его уровень полноты безопасности выше УПБ2. За счет использования информационной избыточности [5] возможно создание виртуального второго канала, с помощью которого предлагается дополнительно контролировать работу этой микропроцессорной системы. Это позволит достичь обеспечения высокой вероятности правильного обнаружения отказов МАЛС. Контроль должен строиться таким образом, чтобы не влиять на работу алгоритма управления маневровым локомотивом. С помощью программы прибора безопасности (ПБ), формируется упорядоченная последовательность машинных команд, которые в системе МАЛС отображаются в виде последовательности контрольных сигнатур, что позволяет дополнительно контролировать работу сложных устройств МАЛС и таким образом повысить его УПБ.

Развивая этот принцип, можно теперь использовать данные устройства уровня SIL2 или SIL3 для контроля еще более сложного устройства с видеокамерами и нейронными сетями. Здесь необходимо отметить, что само это сложное устройство, на примере МАЛС, реализует задачи типа не проезда маневрового сигнала, которые совпадают с типовой задачей МАЛС и дополнительно обнаруживают препятствия через техническое зрение. Выделив базовую технологическую задачу по обработке информации, можно ее использовать в виде функционального теста для аппаратуры сложного беспилотного комплекса. Это можно представить в виде сегмента в пространстве возможных решений беспилотных систем.

Таким образом, сами рабочие сигналы становятся функциональным тестом еще более сложной системы [6]. Кроме того, в рамках рассматриваемой системы следует дополнительно контролировать программно-аппаратные средства технического зрения путем сравнения показаний датчиков технического зрения на борту и на стационаре [7]. Такая иерархическая структура может быть полезна для сокращения аппаратных затрат и упрощения доказательства безопасности по сравнению с реализацией всех функций в одном процессоре. Нужно отметить, что без применения инновационных решений возникает проблема в обеспечении надежности системы, так как средства технического зрения существенно увеличивают объем аппаратуры системы, что сказывается на снижении ее уровня надежности.

2.2. Модель исследования

Любую информацию, которую можно промоделировать в виде объектов и связей между ними, удобно представить в форме графов. Графы широко применяются для визуализации информации, т.е. преобразования больших и сложных видов абстрактной информации в интуитивно понятную визуальную форму.

При построении модели авторы основывались на следующих критериях:

защитный отказ – отказали МАЛС и средства технического зрения (ТЗ), управление локомотивом передается машинисту;

опасный отказ – отказали МАЛС, средства ТЗ и ПБ, полный останов маневрового локомотива. Вопрос критичности опасного отказа в статье не обсуждается – это предмет отдельного рассмотрения.

На рис. 1 представлен граф состояний функциональной безопасности процесса взаимодействия МАЛС с ПБ и ТЗ.

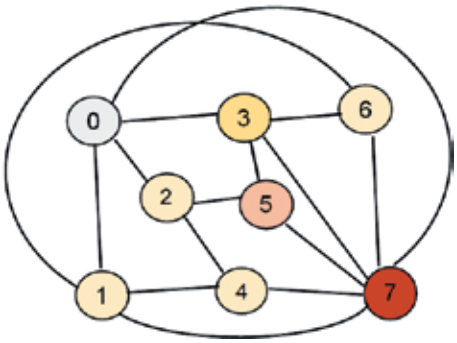

Рис. 1. Граф состояний

Состояния модели системы

Модель системы имеет следующие состояния (см. рис. 1):

0 – Все объекты системы управления исправны;

1 – Отказал и восстанавливается ПБ, остальные средства системы исправны;

2 – Отказал МАЛС, остальные средства системы исправны;

3 – Отказали и восстанавливаются средства ТЗ, остальные средства системы исправны;

4 – Отказали МАЛС и ПБ, восстанавливается МАЛС;

5 – Отказали ТЗ и МАЛС, управление локомотивом передается машинисту (защитный отказ);

6 – Отказали ТЗ и ПБ;

7 – Отказали все три системы. **Опасный отказ.**

Состояния безопасности системы на рис. 1 помечены следующими цветами:

В модели системы предусмотрены следующие переходы:

0-1 – отказ ПБ; 0-2 – обнаруженный отказ МАЛС с помощью встроенных средств контроля и/или сигнатурного анализа; 0-3 – обнаруженный отказ ТЗ с помощью встроенных средств контроля и/или путем сравнения результатов работы с программой МАЛС; 0-5 – необнаруженный отказ ТЗ; 0-7 и 1-7 – необнаруженный отказ МАЛС; 1-4 – отказ УМС при условии отказа ПБ; 1-6 – отказ ТЗ при условии отказа ПБ; 1-0 – восстановление работоспособности ПБ; 2-4 – отказ ПБ при условии отказа МАЛС; 2-5 – отказ ТЗ при условии отказа УМС; 3-5 – отказ МАЛС при условии отказа ТЗ; 3-6 – отказ ПБ при условии отказа МАЛС; 3-0 – восстановление работоспособности ТЗ; 4-7 – отказ ТЗ при условии отказов МАЛС и ПБ; 4-1 – восстановление работоспособности МАЛС; 5-7 – отказ ПБ при условии отказов МАЛС и ТЗ; 6-7 – отказ МАЛС при условии отказов ТЗ и ПБ; 7-0 – переход в исходное состояние в результате возможной модификации МАЛС, если приемлем риск опасного отказа.

Принятые предпосылки и допущения

1. Потоки отказов ПБ, бортовой системы управления маневровым локомотивом МАЛС и средствами ТЗ – простейшие, с параметрами $\lambda_{ПБ}$, $\lambda_{М}$, $\lambda_{ТЗ}$ соответственно. Это допущение основывается на том, что указанные устройства являются электронными и, как показала обширная практика эксплуатации подобных устройств, параметры потоков их отказов постоянны.

2. Отказы устройств в системе взаимно независимы.

3. Времена восстановления всех составных устройств распределены по экспоненциальному закону.

4. Интенсивности восстановления отказавших устройств в системе примерно равны μ, поскольку все устройства системы – электронные и их обслуживает одна ремонтная бригада.

5. Средства контроля на несколько порядков надежнее рабочих устройств, по этой причине принято считать их идеально надежными.

6. Вероятности ложного обнаружения отказов ничтожно малы.

7. Комплексные вероятности правильного обнаружения отказов МАЛС и ТЗ равны $\alpha_{М}$ и $\alpha_{ТЗ}$ соответственно. Вероятность правильного обнаружения прибора безопасности обеспечена на высоком уровне, т.е. $\alpha_{ПБ} \to 1$.

8. Интенсивность восстановления работоспособности ТЗ ($\mu_{ТЗ}$) определяется как средневзвешенное значение интенсивности восстановления обнаруженных отказов ТЗ и необнаруженных между техническими обслуживаниями ($T0$ – средняя периодичность технического обслуживания), т.е. $\mu_{ТЗ} = \alpha_{ТЗ} \cdot \mu + \frac{\alpha_{ТЗ}}{T0}$.

При указанных предпосылках и допущениях поведение системы описывается Марковским случайным процессом.

Функции распределения времени пребывания в состояниях графа модели

В соответствие с принятыми предпосылками и допущениями и на основании графа (рис. 1) модели функции распределения времени пребывания в состояниях графа имеют следующий вид:

$$F_0(t) = 1 - \exp[-(\lambda_{ПБ} + \lambda_М + \lambda_{ТЗ}) \cdot t];$$
$$F_1(t) = 1 - \exp[-(\mu + \lambda_М + \lambda_{ТЗ}) \cdot t];$$
$$F_2(t) = 1 - \exp[-(\lambda_{ПБ} + \lambda_{ТЗ}) \cdot t];$$
$$F_3(t) = 1 - \exp[-(\lambda_{ПБ} + \lambda_М + \mu_{ТЗ}) \cdot t];$$
$$F_4(t) = 1 - \exp[-(\mu + \lambda_{ТЗ}) \cdot t];\ F_5(t) = 1 - \exp[-\lambda_{ПБ} \cdot t];$$
$$F_6(t) = 1 - \exp[-\lambda_М \cdot t];\ F_7(t) = 1 - \exp(-\mu_1 \cdot t), \quad (1)$$

где μ_1 – интенсивность восстановления системы управления МАЛС после опасного отказа.

Математические ожидания времени пребывания системы в состояниях графа модели:

$$T_i = \int_0^\infty [1 - F_i(t)]dt;\ T_0 = \frac{1}{\lambda_{ПБ} + \lambda_М + \lambda_{ТЗ}};$$

$$T_1 = \frac{1}{\mu + \lambda_М + \lambda_{ТЗ}};\ T_2 = \frac{1}{\lambda_{ПБ} + \lambda_{ТЗ}};$$

$$T_3 = \frac{1}{\lambda_{ПБ} + \lambda_М + \mu_{ТЗ}};\ T_4 = \frac{1}{\mu + \lambda_{ТЗ}};$$

$$T_5 = \frac{1}{\lambda_{ПБ}};\ T_6 = \frac{1}{\lambda_М};\ T_7 = \frac{1}{\mu_1}. \quad (2)$$

Вероятности переходов между состояниями графа модели

Вероятности переходов между состояниями *i* и *j* графа определяются с помощью следующего выражения:

$$p_{ij} = \int_0^\infty \lambda_{ij}[1 - F_{ij}(t)]dt. \quad (3)$$

Интенсивности переходов между состояниями графа находятся по графу (рис. 1) с учетом принятых предпосылок и допущений:

$$\lambda_{01}=\lambda_{24}=\lambda_{36}=\lambda_{ПБ};\ \lambda_{02}=\lambda_{14}=\lambda_{35}=\alpha_М\lambda_М;\ \lambda_{03}=\alpha_{ТЗ}\lambda_{ТЗ};$$
$$\lambda_{16}=\lambda_{25}=\lambda_{47}=\lambda_{ТЗ};\ \lambda_{37} = \lambda_{17} = \overline{\alpha}_М\lambda_М;\ \lambda_{10}=\lambda_{41}=\mu;\ \lambda_{30}=\mu_{ТЗ};$$
$$\lambda_{67}=\lambda_М;\ \lambda_{70}=\mu_1.$$

Согласно формуле (3) и выражениям (1) вероятности переходов между состояниями графа имеют следующий вид:

$$p_{01} = \frac{\lambda_{ПБ}}{\lambda_{ПБ}+\lambda_М + \lambda_{ТЗ}};\ p_{02} = \frac{\alpha_М\lambda_М}{\lambda_{ПБ}+\lambda_М + \lambda_{ТЗ}};$$

$$p_{07} = \frac{\overline{\alpha_М}\lambda_М + \overline{\alpha_{ТЗ}}\lambda_{ТЗ}}{\lambda_{ПБ}+\lambda_М + \lambda_{ТЗ}};\ p_{03} = \frac{\alpha_{ТЗ}\lambda_{ТЗ}}{\lambda_{ПБ}+\lambda_М + \lambda_{ТЗ}};$$

$$p_{10} = \frac{\mu}{\mu + \lambda_М + \lambda_{ТЗ}};\ p_{14} = \frac{\alpha_М\lambda_М}{\mu + \lambda_М + \lambda_{ТЗ}};$$

$$p_{17} = \frac{\overline{\alpha_М}\lambda_М}{\mu + \lambda_М + \lambda_{ТЗ}};\ p_{16} = \frac{\lambda_{ТЗ}}{\mu + \lambda_М + \lambda_{ТЗ}};$$

$$p_{24} = \frac{\lambda_{ПБ}}{\lambda_{ПБ} + \lambda_{ТЗ}};\ p_{25} = \frac{\lambda_{ТЗ}}{\lambda_{ПБ} + \lambda_{ТЗ}};$$

$$p_{30} = \frac{\mu_{ТЗ}}{\mu_{ТЗ} + \lambda_М + \lambda_{ПБ}};\ p_{35} = \frac{\alpha_М\lambda_М}{\mu_{ТЗ} + \lambda_М + \lambda_{ПБ}};$$

$$p_{37} = \frac{\overline{\alpha_М}\lambda_М}{\mu + \lambda_М + \lambda_{ПБ}};$$

$$p_{36} = \frac{\lambda_{ПБ}}{\mu_{ТЗ} + \lambda_М + \lambda_{ПБ}};\ p_{41} = \frac{\mu}{\mu + \lambda_{ТЗ}};$$

$$p_{47} = \frac{\lambda_{ТЗ}}{\mu + \lambda_{ТЗ}};\ p_{57} = p_{67} = p_{70} = 1. \quad (4)$$

Результирующие показатели функциональной безопасности системы

Данная модель позволяет исследовать функциональную безопасность системы автоведения маневрового локомотива послойно, т.е. оценивать время до понижения уровня полноты безопасности в зависимости от отказов составных элементов и достижения полного опасного отказа (опасный отказ второго вида на рис. 1):

- *Среднее время пребывания системы на уровне SIL3* (состояние 0 на графе):

$$T_{SIL3}^{система} = T_0 = \frac{1}{\lambda_{ПБ} + \lambda_М + \lambda_{ТЗ}}; \quad (5)$$

- *Среднее время бесперебойной работы системы на уровне не ниже SIL 2 – среднее время до защитного отказа вида 1* (состояния 0, 1, 2, 3, 4, 6 на графе рис. 1) определяются с помощью топологического метода [8]

$$T_{\geq SIL2}^{система} = \frac{T_0 + (p_{01} + p_{02}p_{24}p_{41})T_1 + p_{02}T_2 + p_{03}T_3 + (p_{02}p_{24} + p_{01}p_{14})T_4 + (p_{03}p_{36} + p_{01}p_{16})T_6}{1 - p_{01}p_{10} - p_{02}p_{24}p_{41}p_{10} - p_{03}p_{30} - p_{14}p_{41} + p_{03}p_{30}p_{14}p_{41}}; \quad (6)$$

- Среднее время до опасного отказа (до необходимости полного останова локомотива)

$$T_{опасный} = \frac{T_0 + (p_{01} + p_{02}p_{24}p_{41})T_1 + p_{02}T_2 + p_{03}T_3 + (p_{02}p_{24} + p_{01}p_{14})T_4 + (p_{03}p_{36} + p_{01}p_{16})T_6 + (p_{02}p_{25} + p_{03}p_{35})T_5}{1 - p_{01}p_{10} - p_{02}p_{24}p_{41}p_{10} - p_{03}p_{30} - p_{14}p_{41} + p_{03}p_{30}p_{14}p_{41}}. \quad (7)$$

Для преобразования формулы (6) к явному виду с помощью выражений (2) и (4) учтем возможность упростить эти выражения, поскольку практически применительно к электронным средствам имеет место очевидное неравенство $\mu >>> \lambda$ и $\mu_{ТЗ} >> \lambda$. Следовательно, с погрешностью, не превышающей второго порядка малости, справедливы следующие выражения среднего времени пребывания в некоторых состояниях и ряда вероятностей переходов, т.е.

$$T_1 = T_3 = T_4 \cong \frac{1}{\mu};\ p_{10} = p_{30} \cong 1;\ p_{14} \cong \frac{\alpha_М \lambda_М}{\mu};$$

$$p_{14} = p_{35} \cong \frac{\alpha_М \lambda_М}{\mu_{ТЗ}};\ p_{16} \cong \frac{\lambda_{ТЗ}}{\mu};\ p_{36} \cong \frac{\lambda_{ПБ}}{\mu_{ТЗ}}.$$

При этих условиях выражение (6) преобразуется к явному виду (8), которое с погрешностью не менее первого порядка малости позволяет оценивать среднее время пребывания системы управления маневровым локомотивом с ТЗ и ПБ в состоянии функциональной безопасности на уровне не ниже SIL2

$$T^{система}_{\geq SIL2} \approx \frac{\lambda_{ПБ}(\overline{\alpha_М}\lambda_М + 2\lambda_{ПБ} + 3\lambda_{ТЗ}) + \lambda^2_{ТЗ}}{(\lambda_{ПБ} + \lambda_{ТЗ})[(\lambda_{ПБ} + \lambda_{ТЗ})(\lambda_М + \overline{\alpha_{ТЗ}}\lambda_{ТЗ}) - \alpha_М\lambda_М\lambda_{ПБ})]}. \quad (8)$$

Применение для контроля работы МАЛС с помощью прибора безопасности дополнительных процедур сигнатурного анализа, а также регулярное сравнение результатов работы МАЛС с результатами средств ТЗ дают основание принять параметры обнаружения отказов МАЛС и средств ТЗ близкими к единице ($\alpha_М \to 1, \overline{\alpha_М} \to 0$ и $\alpha_{ТЗ} \to 1, \overline{\alpha_{ТЗ}} \to 0$). При этих условиях формула (8) преобразуется к виду

$$T^{система}_{\geq SIL2} \approx \frac{\lambda_{ПБ}(2\lambda_{ПБ} + 3\lambda_{ТЗ}) + \lambda^2{}_{ТЗ}}{(\lambda_{ПБ} + \lambda_{ТЗ})\lambda_{ТЗ}\lambda_М}. \quad (9)$$

При указанных выше условиях выражение (7) преобразуется к явному виду (10), которое с погрешностью не менее первого порядка малости позволяет оценивать среднее время бесперебойной работы маневрового локомотива до полного его останова

$$T_{опасный} \approx \frac{\lambda_{ПБ}[(\overline{\alpha_М}\lambda_М + 2\lambda_{ПБ} + 3\lambda_{ТЗ}) + \lambda^2{}_{ТЗ}] + \alpha_М\lambda_М\lambda_{ТЗ}(1+\alpha_{ТЗ})}{(\lambda_{ПБ} + \lambda_{ТЗ})[(\lambda_{ПБ} + \lambda_{ТЗ})(\lambda_М + \overline{\alpha_{ТЗ}}\lambda_{ТЗ}) - \alpha_М\lambda_М\lambda_{ПБ})]}. \quad (10)$$

С учетом условий, при которых $\alpha_М \to 1, \overline{\alpha_М} \to 0$ и $\alpha_{ТЗ} \to 1, \overline{\alpha_{ТЗ}} \to 0$, формула (10) преобразуется к виду формулы (11)

$$T_{опасный} \approx \frac{\lambda_{ПБ}(2\lambda_{ПБ} + 3\lambda_{ТЗ}) + \lambda^2{}_{ТЗ} + 2\lambda_М\lambda_{ТЗ}}{(\lambda_{ПБ} + \lambda_{ТЗ})\lambda_{ТЗ}\lambda_М}. \quad (11)$$

На рис. 2 представлена графическая зависимость времени бесперебойной работы маневрового локомотива до полного останова от интенсивности отказов средств ТЗ и аппаратуры МАЛС. Для отслеживания зависимости интенсивность опасного отказа ПБ $\lambda_{ПБ} = 1 \times 10^{-7}$, что соответствует уровню полноты безопасности УПБ2.

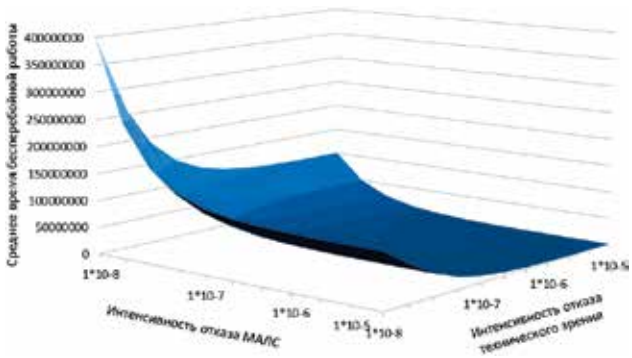

Рис. 2. Зависимость времени бесперебойной работы маневрового локомотива до полного останова от интенсивности отказов средств ТЗ и аппаратуры МАЛС

Ключевой задачей исследования является оценка уровня функциональной безопасности системы автоведения маневрового локомотива. Эта оценка в комплексном виде возможна путем исследования коэффициента безопасности данной системы. Этот коэффициент, согласно работе [8], в условиях данной задачи определяется в виде

$$K_Б = 1 - \overline{K_Б} = 1 - \pi_7 = 1 - \frac{T_7 a_7}{\sum_{i=0}^{7} T_i a_i}, \quad (12)$$

где $1-\pi_7$ – определитель графа во множестве неопасных ситуаций;

$a_i = \dfrac{\sum_k l_k^{0i} \Delta G_k^i}{\Delta G_0}$; $a_0 = 1$; ΔG_0 – вес разложения графа $G(S,П)$ без нулевой вершины, ΔG_k^i – вес разложения графа без вершины i и вершин, находящихся на k-м пути.

Раскроем выражение (12) относительно коэффициента опасности $\overline{K_Б}$

$$\overline{K_Б} = \frac{T_7 \sum l_k^{07} \Delta G_k^7}{\sum_{i=0}^{7} T_i \sum l_k^{0i} \Delta G_k^i} =$$

$$= \frac{T_7 A}{\left(\begin{array}{c} T_0 + T_1(p_{01} + p_{02}p_{24}p_{41}) + T_2 p_{02}(1 - p_{14}p_{41}) + \\ + T_{03}p_{03}(1 - p_{14}p_{41}) + T_4(p_{02}p_{24} + p_{01}p_{14}) + \\ + T_5(p_{02}p_{25} + p_{03}p_{35}) + \\ + T_6(p_{03}p_{36}(1 - p_{14}p_{41}) + p_{01}p_{16}) + T_7 A \end{array}\right)}, \quad (13)$$

где

$$A = (p_{03}(p_{37} + p_{36}p_{67} + p_{35}p_{57}) + p_{02}p_{25}p_{57} + p_{07}) \cdot$$
$$\cdot(1 - p_{14}p_{41}) + p_{01}p_{14}p_{47} + p_{01}p_{17} + p_{02}p_{24}p_{47} + p_{01}p_{16}p_{67}.$$

Выражение (13) может быть представлено в явном виде с учетом очевидных неравенств $\mu >>> \lambda$ и $\mu_{ТЗ}, \mu_1 >> \lambda$, $\lambda_{ПБ} >> \lambda_{ТЗ}; \lambda_М$ и с учетом условий, при которых $\alpha_М \to 1, \overline{\alpha_М} \to 0$ и $\alpha_{ТЗ} \to 1, \overline{\alpha_{ТЗ}} \to 0$, формула (13) преобразуется к виду формулы (14)

$$\overline{K_Б} = \frac{\lambda_{ПБ}\lambda_{ТЗ}\lambda_М(2\lambda_{ПБ}\lambda_{ТЗ} + \lambda_М(1+\lambda_{ПБ}+\lambda_{ТЗ}) - \lambda_М^2\lambda_{ТЗ}}{\left(\begin{array}{c}\lambda_{ПБ}^2\lambda_{ТЗ}^2 + \lambda_{ПБ}\lambda_{ТЗ}\lambda_М(1+\lambda_{ПБ}+\lambda_{ПБ}\lambda_{ТЗ}) - \\ -\lambda_М^3\lambda_{ПБ}(1+\lambda_{ТЗ}+\lambda_{ТЗ}^2) + \\ +\lambda_М^2(\lambda_{ТЗ}+(1+2\lambda_{ПБ})(\lambda_{ПБ}+\lambda_{ПБ}\lambda_{ТЗ}+\lambda_{ТЗ}^2)\end{array}\right)}. \quad (14)$$

На рис. 3 представлен график зависимости коэффициента опасности (14) от интенсивностей отказов ТЗ и МАЛС. Опыт эксплуатации и разработки систем безопасности для маневровых составов и требования ГОСТ [9] позволяют принять интенсивность отказов ПБ на уровне УПБ2, т.е. $\lambda_{ПБ} = 10^{-7}$ 1/ч. Проследим динамику изменения коэффициента опасности (см. выражение (13)) от интенсивностей отказов МАЛС и ТЗ.

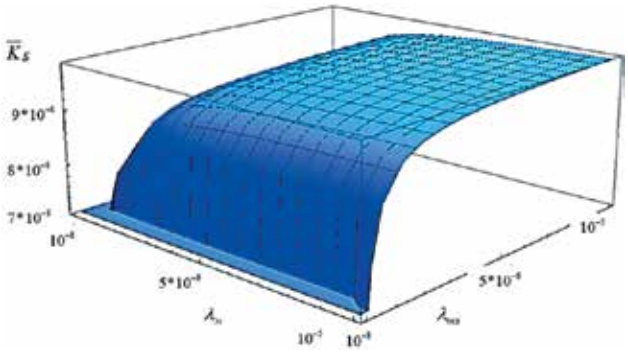

Рис. 3. График зависимости $\overline{K_Б}$ от $\lambda_М$ и $\lambda_{ТЗ}$

Из рис. 3 следует, что снижение интенсивностей отказов МАЛС и ТЗ даже на 3 порядка с SIL0 до SIL3 несущественно влияет на коэффициент опасности, диапазон изменения которого при этом меняется незначительно (менее 2%).

Исследуем зависимость коэффициента опасности системы от параметров интенсивности μ восстановления объектов и интенсивности μ_1 реанимации системы управления МАЛС после опасного отказа. Раннее установлено (см. график на рис. 3), что интенсивности отказов ТЗ и МАЛС не оказывают существенного влияния на безопасность системы. В соответствии с требованиями ГОСТ [9], средняя наработка до отказа систем, выполняющих функции управления железнодорожным подвижным составом на сортировочных горках, составляет 30 000 ч. Так как система управления МАЛС и ТЗ являются частями общей системы, то в данном исследовании показатели их интенсивности отказов принимаются равными $\lambda_М$=10^{-5}1/ч и $\lambda_{ТЗ}$=10^{-5}1/ч. Данные показатели могут быть достигнуты за счет использования современных аппаратных средств с высоким уровнем надежности. Трехмерный график зависимости коэффициента опасности системы от параметров μ и μ_1 представлен на рис. 4.

Из графика следует, что при увеличении интенсивности μ_1 восстановления системы после опасного отказа от 0,0059 1/ч до 1 1/ч (данный показатель соответствует времени восстановления системы от

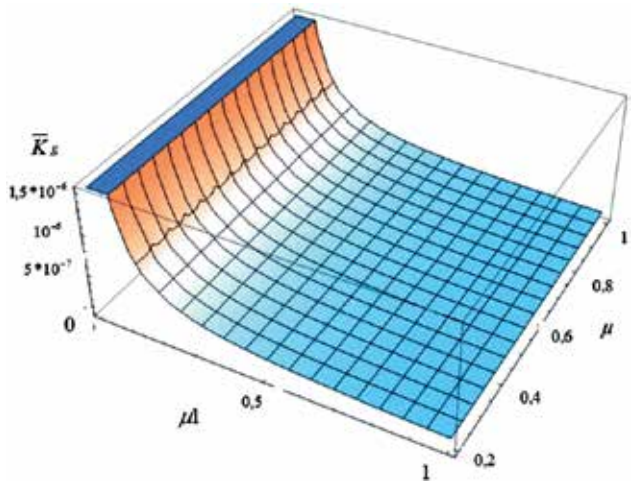

Рис. 4. График зависимости коэффициента опасности $\overline{K_Б}$ от μ и μ_1.

1 часа до недели, диапазон выбран исходя из характера неисправности; так, аппаратные отказы возможно устранить за час, имея запасной комплект, в то время как на исправление программных ошибок может понадобиться до 7 дней) коэффициент опасности уменьшается почти в 30 раз. Таким образом, своевременное и оперативное устранение неисправностей может существенно улучшить показатели безопасности системы.

Проанализируем влияние комплексных вероятностей правильного обнаружения отказов МАЛС ($\alpha_М$) и ТЗ ($\alpha_{ТЗ}$) на $\overline{K_Б}$. Рассмотрим 2 случая, когда интенсивность восстановления системы $\mu_1 \cong 0,0059$ 1/ч и $\mu_1 \cong 1$ 1/ч, данные интенсивности соответствуют времени восстановления системы после отказа 168 часов и 1 час соответственно и являются граничными значениями. Показатель интенсивности восстановления ТЗ выбран исходя из предположения, что неисправности устраняются за 24 часа, т.е $\mu \cong \mu_{ТЗ} \to 1/24$. Графики зависимости коэффициента опасности $\overline{K_Б}$ от $\alpha_{ТЗ}$ и $\alpha_М$ представлены на рис. 5.

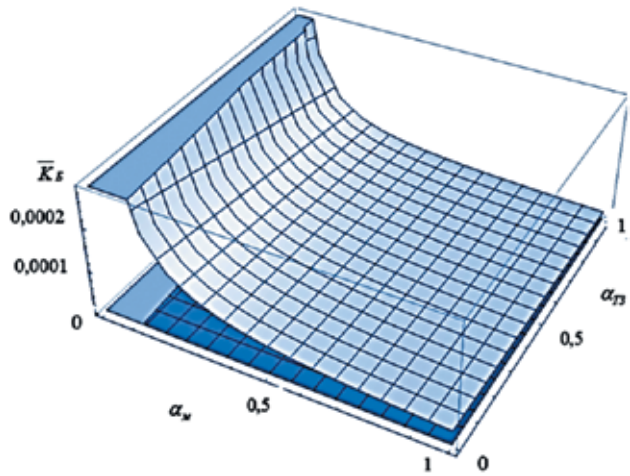

Рис. 5. Графики зависимости коэффициента опасности $\overline{K_Б}$ от $\alpha_{ТЗ}$ и $\alpha_М$ при $\mu_1 \cong 0,0059$ 1/ч (голубой график) и $\mu_1 \cong 1$ 1/ч (синий график).

Из данных графиков следует, что улучшение возможностей обнаружения отказов МАЛС и ТЗ, как было показано выше, позволяют в существенной мере улучшить временные показатели безопасности системы, но при этом незначительно влияют на снижение коэффициента опасности.

Практические результаты

Предложенная организация контроля за работой МАЛС и средств ТЗ, создание виртуального второго канала позволяет повысить функциональную безопасность системы управления маневровым локомотивом с ТЗ с уровня УПБ2 до УПБ3 и в течение достаточно длительного времени (более четверти от среднего времени наработки МАЛС до отказа) находиться на этом уровне функциональной безопасности системы.

При предложенной организации системы управления маневровым локомотивом с ТЗ среднее время ее исправной работы может возрасти почти в три раза при сохранении достигнутого уровня функциональной безопасности системы, при этом время бесперебойной работы локомотива до необходимости его полного останова по соображениям обеспечения безопасности может также увеличиться более чем в три раза. Этот важный результат может быть практически достигнут, несмотря на увеличение объема аппаратуры системы при введении в его состав средств ТЗ.

За счет предложенной организации работы МАЛС со средствами ТЗ, рационального использования возможностей программы ПБ и создания на ее основе последовательности контрольных сигнатур можно добиться гарантированного своевременного обнаружения отказов в системе и практически исключить скрытые отказы, что позволяет добиться указанного результата без применения конструктивных решений по повышению надежности аппаратуры системы.

Установлено, что определяющее влияние на коэффициент опасности системы оказывает время, связанное с восстановлением средств ТЗ. Совершенствование технологии ремонта и восстановления может существенно улучшить коэффициент безопасности системы. При этом улучшение комплексного показателя обнаружения отказов МАЛС и ТЗ позволят в существенной мере улучшить показатели безопасности системы в целом.

Библиографический список

1. Охотников А.Л., Попов П.А. Беспилотное управление локомотивом: вчера сегодня и завтра // Автоматика, связь, информатика. 2019. № 8. С. 12-17.

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

3. Швир В. Надежность электронных схем в устройствах СЦБ // Железные дороги мира. 1986. № 1. С. 59-67.

4. Калинин А.В. Управление маневровым локомотивом без участия машиниста. Основные принципы и перспективы развития технологии // Интеллектуальные ИТ управления ИТНОУ. 2017. № 1. С. 12-14.

5. Шубинский И.Б. О методе обеспечения функциональной безопасности системы с одноканальной обработкой информации / И.Б. Шубинский, Е.Н. Розенберг, А.С. Коровин, Н.Г. Пенькова // Надежность. 2022. № 22(3). С. 44-52. DOI: 10.21683/1729-26462022-22-3-44-52

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

7. Бортовая информационная система: пат. 2742960 Рос. Федерация. № 2020131633 / Мыльников П.Д., Охотников А.Л., Попов П.А.; заявл. 25.09.2020; опубл. 12.02.2021 Бюл. № 5.

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

9. ГОСТ 33435–2015. Устройства управления, контроля и безопасности железнодорожного подвижного состава. Требования безопасности и методы контроля. М.: Стандартинформ, 2016. IV, 45 с.

References

[1]. Okhotnikov A.L., Popov P.A. Self-driving: yesterday, today and tomorrow. *Automation, Communications, Informatics* 2019;8:12-17. (in Russ.)

[2]. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. Parts 1 – 7. 2011.

[3]. Shvir V. [Dependability of the electronic circuits in railway signalling devices]. *Rail International* 1986;1:59-67. (in Russ.)

[4]. Kalinin A.V. [Controlling a shunting engine without a driver. Key principles and prospects of the technology]. *[Intellektualniye IT upravleniya ITNOU]* 2017;1. (in Russ.)

[5]. Shubinsky I.B., Rozenberg E.N., Korovin A.S., Penkova N.G. On a method for ensuring functional safety of a system with single-channel information processing. *Dependability* 2022;22(3):44.https://doi.org/10.21683/1729-26462022-22-3-44-52.

[6]. Sapozhnikov V.V., Sapozhnikov Vl.V., Khristov Kh.A., Gavzov D.V. Sapozhnikov Vl.V., editor. [Design methods of vital computer-based railway automatics]. Moscow: Transport; 1995. (in Russ.)

[7]. Mylnikov P.D., Okhotnikov A.P., Popov P.A. [Onboard information systems]. Patent no. 2742960 dated 12.02.2021 bul. no. 5 N.

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

[9]. GOST 33435–2015. Control, monitoring and safety means of railway rolling stock. Safety requirements and control methods. (in Russ.)

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

Панферов Игорь Александрович – начальник отделения разработки систем интервального регулирования АО «НИИАС», Москва, Российская Федерация, e-mail: i.panferov@vniias.ru

Бояринова Наталья Александровна – главный специалист центра безопасности и алгоритмической поддержки АО «НИИАС», Москва, Российская Федерация, e-mail: n.boyarinova@vniias.ru

Кузьмин Андрей Игоревич – заместитель начальника отделения разработки систем интервального регулирования АО «НИИАС», Москва, Российская Федерация, e-mail: a.kuzmin@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.

Igor A. Panfiorov, Head of Unit for Train Separation Systems, JSC NIIAS, Moscow, Russian Federation, e-mail: i.panferov@vniias.ru.

Natalia A. Boyarinova, chief specialist, Centre for Safety and Algorithmic Support, JSC NIIAS, Moscow, Russian Federation, e-mail: n.boyarinova@vniias.ru.

Andrey I. Kuzmin, Deputy Head of Division for the Development of Train Separation Systems, JSC NIIAS, Moscow, Russian Federation, e-mail: a.kuzmin@vniias.ru.

Вклад авторов в статью

Шубинским И.Б. выполнена разработка математических моделей и формул расчета.

Розенбергом Е.Н. выполнена постановка задачи исследования.

Панферовым И.А. выполнен выбор и подготовка исходных данных, анализ и обзор результатов исследований, формулирование выводов.

Бояриновой Н.А. выполнены расчетные исследования, графическая визуализация результатов исследования, участие в выборе исходных данных для расчетного исследования и участие в анализе результатов.

Кузьминым А.И. выполнен анализ исходных данных для выполнения исследования, участие в анализе результатов исследования и анализе методов исследования.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.