Оригинальная статья / Original article
https://doi.org/10.21683/1729-2646-2022-22-3-44-52

О методе обеспечения функциональной безопасности системы с одноканальной обработкой информации

On a method for ensuring functional safety of a system with single-channel information processing

Шубинский И.Б.[1], Розенберг Е.Н.[1], Коровин А.С.[1], Пенькова Н.Г.[1]*
Igor B. Shubinsky[1], Efim N. Rozenberg[1], Alexander S. Korovin[1], Natalia G. Penkova[1]*
[1]АО «НИИАС», Москва, Российская Федерация
[1]JSC NIIAS, Moscow, Russian Federation
**N.Penkova@vniias.ru*


Шубинский И.Б.


Розенберг Е.Н.


Коровин А.С.


Пенькова Н.Г.

Резюме. Цель *данной статьи – снижение стоимости оборудования системы управления движением локомотивов, которое достигается за счет применения структуры с одноканальным источником информации (в данном случае счетчиков осей) и двухканальным приемником информации (в данном случае бортовой системы управления) взамен традиционной структуры, где формирующее и принимающее устройства должны быть не менее чем двухканальными. При этом для обеспечения безопасности системы заложенный в наиболее широко применяемую многоканальную структуру механизм обнаружения отказов путем сравнения результатов работы между каналами бортового устройства дополняется программной реализацией проверяющих алгоритмов, позволяющих обеспечить соответствующий уровню полноты безопасности SIL4 уровень правильного обнаружения отказа одноканального устройства (в данном случае счетчика осей). Этот уровень в основном характеризуется количественным показателем «вероятность правильного обнаружения» и, чтобы добиться поставленной цели, необходимо вычислить допустимый и в то же время достижимый диапазон данной вероятности и параметров эффективности проверяющих алгоритмов, функцией от которых она является.* **Методика.** *В статье показаны две модели безопасности системы управления движением локомотива: традиционная структура с двухканальным формирующим и принимающим устройством и структура с одноканальным источником и двухканальным приемником информации. Графовые модели содержат аналогичные состояния, имея различия только в параметрах модели. С помощью топологического метода [1], применительно к условиям данной задачи, в обеих моделях выведены формулы расчета средней наработки системы до опасного отказа, интенсивности и вероятности возникновения опасных отказов. Определены значения исходных данных, в том числе вероятностей правильного обнаружения отказа бортовой системы и счетчика осей, и выполнены расчеты значений этих показателей безопасности, позволяющих отнести систему к одному из четырех дискретных уровней полноты функциональной безопасности.* **Результаты.** *В представленной статье произведено нормирование вероятностных показателей эффективности программных и аппаратных средств обнаружения отказа для структуры с одноканальным источником и двухканальным приемником информации. При этом под нормированием показателей понимается процесс установления их предельно допустимых значений, обеспечивающих количественные показатели безопасности (среднюю наработку системы до опасного отказа, интенсивность и вероятность опасного отказа системы) не хуже, чем у традиционной структуры с двухканальными формирующим и принимающим устройствами. Выявлены наиболее значимые для обеспечения безопасности из-за сильного влияния на уровень правильного обнаружения отказа (в данном случае счетчика осей) параметры эффективности. Полученные результаты показали возможность сокращения аппаратных затрат с сохранением выполнения требований безопасности при использовании одноканальных источников информации (в данном случае счетчиков осей) и двухканальных приемников информации (в данном случае бортовой системы управления), имеющих в своем составе программное обеспечение, которое дает возможность обеспечить соответствующий высокий уровень правильного обнаружения отказа (в данном случае счетчика осей).*

Abstract. *The paper* **Aims** *to reduce the cost of onboard train control systems by using an architecture with a single-channel source of information (in this case, axle counters) and a two-channel receiver of information (in this case, an on-board control system) instead of the conventional architecture, whereas the generator and receiver are to have at least two channels. Additionally, in order to ensure the system's safety, the failure detection mechanism embedded in the most common multichannel architecture that involves comparing the outputs of the onboard unit's channels is complemented by software verification algorithms that enable a SIL4-compliant level of correct failure detection of the single-channel device (in this case, an*

axle counter). This level is primarily characterized by the quantitative indicator "probability of correct detection" and achieving the goal requires calculating the acceptable and, at the same time, achievable range of this probability and the performance parameters of the verification algorithms, of which it is a function. **Methods.** *The paper shows two safety models of an onboard train control system, i.e., the conventional architecture with two-channel generating and receiving devices and the architecture with a single-channel source and a two-channel receiver of information. The graph models feature similar states and only differ in terms of the model parameters. By applying the topological method [1] to the conditions of the problem, within both models, formulas were derived for calculating the mean time to hazardous failure, rate and probability of hazardous failures. Input values were identified, including the probabilities of correct detection of failure of the on-board system and axle counter, the values of those safety indicators were calculated, allowing to attribute the system to one of the four discrete safety integrity levels.* **Results.** *The paper defines the probabilistic performance indicators of failure detection software and hardware for an architecture with a single-channel source and a two-channel receiver of information. Indicator definition involves setting maximum permissible values that enable the quantitative safety indicators (mean time to hazardous failure, rate and probability of hazardous failures) not worse than those of a conventional architecture with two-channel generating and receiving devices. The efficiency parameters that are the most safety-critical due to their significant effect on correct failure detection (in this case, the axle counter) are identified. The findings show that it is possible to reduce hardware-related costs without compromising compliance with the safety requirements when using single-channel sources (in this case, axis counters) and two-channel receivers of information (in this case, an on-board control system) that feature software enabling an appropriately high level of correct failure detection (in this case, of an axle counter).*

Ключевые слова: *бортовые системы управления, счетчики осей, графовая модель, функциональная безопасность.*
Keywords: *onboard control systems, axle counters, graph model, functional safety.*

Для цитирования: *Шубинский И.Б., Розенберг Е.Н., Коровин А.С., Пенькова Н.Г. О методе обеспечения функциональной безопасности системы с одноканальной обработкой информации // Надежность. 2022. №3. С. 44-52. https://doi.org/10.21683/1729-2646-2022-22-3-44-52*
For citation: *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;3: 44-52. https://doi.org/10.21683/1729-2646-2022-22-3-44-52*

Поступила *19.06.2022 г.* / **После доработки** *30.06.2022 г.* / **К печати** *19.09.2022*
Received on: *19.06.2022* / **Revised on:** *30.06.2022* / **For printing:** *19.09.2022.*

Введение

Структура системы обеспечения безопасности движения поездов на электронной (микропроцессорной) элементной базе основывается на принципе многоканальности при обработке информации. Соответственно, если рассматривать передачу информации от источника к приемнику, то формирующее информацию устройство и принимающее ее должны быть как минимум двухканальными.

Опыт построения таких устройств на железнодорожном транспорте на настоящий момент уже достаточен, чтобы подтвердить тезис об обязательности двухканальности в структуре системы безопасности. Более 30 тысяч бортовых устройств КЛУБ-У, более 300 станций с микропроцессорной централизацией, более 1000 км микропроцессорной автоблокировки. За период свыше 30 лет эксплуатации этих устройств не было ни одного случая опасного отказа систем.

Вместе с тем, очевиден вопрос об использовании не только аппаратной, но и информационной избыточности.

В работе [2] рассмотрен принцип дуальности программного обеспечения при обработке ответственной информации, когда предполагается для конкретной задачи создание не менее двух разных алгоритмов и последующее построение разных программных кодов. К наиболее известным примерам применения такой технологии следует отнести бортовые и стационарные устройства фирмы Бомбардье, хотя для более ответственных систем эта фирма использует принцип сочетания двухканальных аппаратных средств с двухверсионным программированием.

В статье оценена возможность применения нового подхода к организации безопасного движения поездов с помощью одноканальных счетчиков осей, при котором информация от текущего счетчика осей сравнивается с предусмотренной в приемнике информацией. Процедуры сравнения информации выполняют функции второго канала счетчика осей и, таким образом, можно говорить о наличии в системе двухверсионного программирования. А также о наличии в системе не только двухканальной бортовой системы управления поездом, но и в определенной мере двухканального счетчика осей.

Постановка задачи

Представим, что в локомотивном устройстве, выполненном со всеми требованиями функциональной безопасности, записана определенная, единственная информация. Такая информация, например, может быть в виде количества осей поезда, который следует по перегону.

Условие безопасности состоит в том, что на пути поезда расположено k пунктов счетчиков осей, которые, подсчитав количество прошедших точку осей поезда, передают эту информацию на локомотив для сравнения с информацией, записанной в безопасное бортовое устройство. При совпадении результата сравнения количества измеренных осей поезда с заранее известной информацией на борту по координате i-го ($i = 1,2,\ldots,k$) счетного пункта принимается решение с заданным уровнем безопасности, что участок за хвостом поезда свободен. Каждый i-ый счетный пункт из последовательности подряд расположенных свободных участков имеет свою географическую координату и, соответственно, суммирование расстояний между этими координатами определяет дистанцию между головой последующего поезда и последним счетным пунктом за хвостом впереди идущего поезда. Если информация не совпала, то участок занятый первичным поездом удлиняется до следующей счетной точки.

Здесь и далее общеизвестный вопрос о передаче информации между поездами по цифровому каналу передачи ответственной информации не рассматривается, так как предполагается соответствие требованию уровня безопасности (кодирование, криптошифрование и т.д.).

Возникает вопрос о целесообразности наличия традиционного решения – двухканального источника информации в виде счетчика осей поезда. Действительно, среди всего многообразия отказов счетчика осей существует только одна опасная ситуация, когда ошибка в подсчете количества осей поезда будет замаскирована таким отказом счетчиков осей, который в результате приведет к совпадению с информацией на борту локомотива. Очевидно, что здесь действует целый ряд условий – разное количество осей поездов, полное многообразие отказов устройства счета осей на пути, среди которых должно проявиться единственное маскирующее событие.

Правомерен вопрос о возможности использования одноканальных источников информации (в данном случае счетчиков осей) вместо двухканальных, значительно сокращая аппаратные затраты, при этом имея в качестве опорного двухканальное устройство получателя (в данном случае приемник информации на локомотиве). Задача состоит в том, чтобы оценить, сохраняется или нет приемлемый уровень функциональной безопасности системы при переходе в ней от двухканальных счетчиков осей к одноканальным счетчикам, но с регулярным применением информационной избыточности в качестве второго канала счетчика осей.

Описание моделей

Исследуем две модели безопасности, где первая модель – для исходной двухканальной организации счетчиков осей, а вторая – для системы с одноканальными счетчиками и с реализацией информационной избыточности

Модель 1

Бортовая система управления построена по требованиям уровня полноты безопасности SIL 4 – это двухканальная двухверсионная система. Все k счетчиков осей имеют двухканальную архитектуру, что позволяет обеспечить их безопасность на уровне SIL 3. Принято, что отказы аппаратуры каналов бортовой системы управления и счетчиков осей независимы и распределены по экспоненциальному закону с интенсивностями отказов соответственно $\lambda_{П}$ и $\lambda_{Сч}$. Заданное число счетчиков осей на пути следования локомотива равно k. В свою очередь, отказ каналов передачи данных также распределен по экспоненциальному закону с интенсивностью $\lambda_{К}$. Эта предпосылка уместна для электронной аппаратуры. Вероятности правильного обнаружения отказов бортовой системы и счетчика осей равны соответственно α_1 и α_2. Эти вероятности являются комплексной оценкой эффективности обнаружения отказов этих систем. Они совместно учитывают возможности встроенного контроля и операций сравнения данных двух каналов. События этих двух способов контроля зависимы. Правильность сравнения данных двух каналов оценивается вероятностями α_{11} и α_{21} соответственно относительно бортовой системы и счетчика осей. Эффективность встроенного контроля этих систем оценивается вероятностями правильного обнаружения отказов α_{12} и α_{22} соответственно. Следовательно, вероятности правильного обнаружения отказов бортовой системы и счетчика осей соответственно равны

$$\alpha_1 = \alpha_{11} + \alpha_{12} - \alpha_{11}\alpha_{12} \text{ и} \quad (1)$$

$$\alpha_2 = \alpha_{21} + \alpha_{22} - \alpha_{21}\alpha_{22}. \quad (2)$$

Предполагается, что вероятности ложного обнаружения ничтожно малы, а отказы каналов передачи данных гарантированно и своевременно обнаруживаются.

Модель безопасности системы управления движением локомотива приведена на рис. 1.

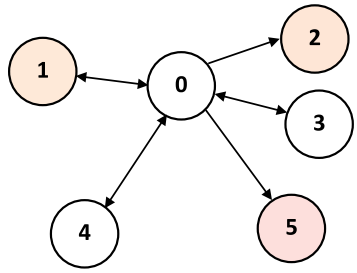

Рис. 1. Модель безопасности системы управления движением локомотива.

Состояние системы:

0 – исправное работоспособное состояние бортовой системы управления, всех счетчиков осей и средств передачи данных;

1 – обнаруженный отказ канала бортовой системы управления локомотива, восстановление работоспособности канала, защитный отказ;

2 – необнаруженный отказ канала бортовой системы управления локомотива, опасный отказ;

3 – отказ канала передачи данных, восстановление работоспособности канала;

4 – обнаруженный отказ счетчика осей, восстановление работоспособности канала;

5 – необнаруженный отказ счетчика осей, опасный отказ.

Множества состояний системы:

$S_{\text{Р}}=\{0,3,4\}$ – работоспособные состояния; $\overline{S}_{\text{Р}}=\{1,2,5\}$ – неработоспособные состояния; $S_{\text{Р}}\bigcup\overline{S}_{\text{Р}}=S$; S_1 – защитное состояние; $S_{\text{ОП}}=\{2,5\}$ – опасные состояния, $\overline{S}_{\text{ОП}}=\{0,1,3,4\}$ – неопасные состояния; $S_{\text{ОП}}\bigcup\overline{S}_{\text{ОП}}=S$.

Математические ожидания времени ($T_0, T_1, T_2, T_3, T_4, T_5$) пребывания системы, описываемой моделью 1, в приведенных на рис. 1 состояниях графа определяются выражениями (3):

$$T_0=\frac{1}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}},\ T_1=T_3=T_4=\frac{1}{\mu},$$

$$T_2=\frac{1}{\lambda_{\text{П}}+\lambda_{\text{К}}+2k\lambda_{\text{СЧ}}},$$

$$T_5=\frac{1}{2\lambda_{\text{П}}+(k-1)2\lambda_{\text{СЧ}}+\lambda_{\text{СЧ}}+\lambda_{\text{К}}}, \qquad (3)$$

где $\lambda_{\text{П}}$ – интенсивность отказов бортовой системы управления локомотивом, $\lambda_{\text{СЧ}}$ – интенсивность отказов одного счетчика осей, $\lambda_{\text{К}}$ – интенсивность отказов каналов передачи данных между бортовой системой управления и счетчиком осей, k – количество счетчиков осей на данном участке (например, 10).

Вероятности переходов p_{ij} между вершинами графа определяются выражениями (4):

$$p_{01}=\frac{\alpha_1 2\lambda_{\text{П}}}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}},\ p_{02}=\frac{(1-\alpha_1)2\lambda_n}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}},$$

$$p_{03}=\frac{\lambda_{\text{К}}}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}},\ p_{04}=\frac{\alpha_2\cdot 2k\lambda_{\text{СЧ}}}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}},$$

$$p_{05}=\frac{(1-\alpha_2)\cdot 2k\lambda_{\text{СЧ}}}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}},\ p_{10}=p_{30}=p_{40}=1. \qquad (4)$$

Веса контуров:

$$C_1=p_{01}p_{10},\ C_2=p_{03}p_{30},\ C_3=p_{04}p_{40}. \qquad (5)$$

Веса разложений графа в множестве неопасных состояний:

$$\Delta G=1-C_1-C_2-C_3,\ \Delta G_0=1,\ \Delta G_1=1-C_2-C_3,$$

$$\Delta G_3=1-C_1-C_3,\ \Delta G_4=1-C_1-C_2. \qquad (6)$$

Средняя наработка системы до опасного отказа определяется согласно топологическому методу [1] применительно к условиям данной задачи по следующей формуле:

$$T_{\text{ОП}}=\frac{T_0+p_{01}T_1\Delta G_1+p_{03}T_3\Delta G_3+p_{04}T_4\Delta G_4}{\Delta G}. \qquad (7)$$

Подставляя формулы (6) в формулу (7), находим в развернутом виде выражение средней наработки исследуемой системы до опасного отказа:

$$T_{\text{ОП}}=\frac{T_0+p_{01}T_1(1-C_2-C_3)+p_{03}T_3(1-C_1-C_3)+p_{04}T_4(1-C_1-C_2)}{1-C_1-C_2-C_3}. \qquad (8)$$

Важно обратить внимание на то, что на практике имеет место неравенство между интенсивностями отказов устройств системы λ_j и интенсивностью их восстановлений μ_j такое, что $\lambda_j<<\mu_j$. Отсюда следует, что согласно формулам (3) $T_0>>T_1,T_3,T_4$ и выражение (8) с погрешностью, не превышающей первого порядка малости, может быть преобразовано к следующему виду:

$$T_{\text{ОП}}\approx\frac{T_0}{1-C_1-C_2-C_3}. \qquad (9)$$

Вследствие утверждения о простейшем потоке опасных отказов справедливо следующее выражение интенсивности опасных отказов системы

$$\lambda_{\text{ОП}}\approx\frac{1-C_1-C_2-C_3}{T_0}. \qquad (10)$$

Вероятность опасного отказа системы для очевидного условия $\lambda_{\text{ОП}}<<1$ рассчитывается по формуле

$$Q_{\text{ОП}}(t)\approx\left[\frac{1-C_1-C_2-C_3}{T_0}\right]\cdot t. \qquad (11)$$

Преобразуем формулы (9), (10) и (11) к явному виду. С этой целью подставим в них аналитические выражения исходных параметров:

$$T_{ОП}\approx\frac{\frac{1}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}}}{\left(1-\frac{2\alpha_1\lambda_{\text{П}}}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}}-\frac{\lambda_K}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}}-\frac{2\alpha_2 k\lambda_{\text{СЧ}}}{2\lambda_{\text{П}}+2k\lambda_{\text{СЧ}}+\lambda_{\text{К}}}\right)}=$$

$$=\frac{1}{2(\overline{\alpha}_1\lambda_{\text{П}}+\overline{\alpha}_2 k\lambda_{\text{СЧ}})}, \qquad (12)$$

где $\overline{\alpha}_1=1-\alpha_1$ – вероятность необнаружения отказа бортовой системы управления локомотивом; $\overline{\alpha}_2=1-\alpha_2$ – вероятность необнаружения отказа счетчика осей.

В свою очередь, интенсивность опасных отказов равна:

$$\lambda_{\text{ОП}} \approx 2(\overline{\alpha}_1\lambda_{\text{П}} + \overline{\alpha}_2 \cdot k\lambda_{\text{СЧ}}) . \quad (13)$$

Вероятность опасного отказа системы

$$Q_{\text{ОП}}(t) \approx [2(\overline{\alpha}_1\lambda_{\text{П}} + \overline{\alpha}_2 \cdot k\lambda_{\text{СЧ}})]\cdot t . \quad (14)$$

Модель 2

Бортовая система управления локомотивом построена по требованиям уровня полноты безопасности SIL 4 – это двухканальная двухверсионная система. Все k счетчиков осей имеют одноканальную архитектуру, что позволяет существенно снизить стоимость. Однако есть опасение о достаточности полноты безопасности счетчиков осей и системы в целом. Чтобы обеспечить уровень полноты безопасности счетчиков осей не ниже SIL 3, как это имеет место при двухканальной архитектуре счетчиков осей, необходимо обеспечить соответствующий высокий уровень правильного обнаружения отказа счетчика осей.

Принятые допущения аналогичны тем, что указаны в модели 1.

В программном обеспечении бортовой системы и счетчиков осей предусмотрено определение текущего расположения локомотива и счетчика осей (их железнодорожные координаты), текущего времени прохождения локомотива над соответствующем счетчиком осей, расчет текущего номера счетчика осей и расчет количества осей проходящего локомотива. Эти результаты постоянно сравниваются. Правильное определение совпадения номера и расположения счетчиков осей к текущему расположению локомотива оценивается вероятностью β, а правильность определения совпадения результатов расчетов текущего времени и количества осей – вероятностью γ. Вероятность отсутствия ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей оценивается величиной ν. В свою очередь, (1 – ν) – вероятность ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей. Предполагается, что отказы каналов передачи данных гарантированно и своевременно обнаруживаются.

Граф модели 2 аналогичен графу модели 1. Имеют место аналогичные модели 1 состояния, но при этом существуют различия в параметрах моделей. Определим их.

Вероятности переходов p_{ij} между вершинами графа определяются выражениями:

$$p_{01} = \frac{\alpha_1 2\lambda_{\text{П}}}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}},\ p_{02} = \frac{(1-\alpha_1)2\lambda_n}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}},$$

$$p_{03} = \frac{\lambda_{\text{К}}}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}},\ p_{04} = \frac{\alpha_2^{\bullet}\cdot k\lambda_{\text{СЧ}}}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}},$$

$$p_{05} = \frac{(1-\alpha_2^{\bullet})\cdot k\lambda_{\text{СЧ}}}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}},\ p_{10} = p_{30} = p_{40} = 1, \quad (15)$$

где $\alpha_2^{\bullet} = \alpha_{22} + \nu(\beta+\gamma-\beta\gamma) - \alpha_{22}\nu(\beta+\gamma-\beta\gamma)$, α_{22} – вероятность правильного обнаружения отказов встроенными средствами контроля в счетчике осей; β – вероятность правильного совпадения результатов номера и расположения счетчиков осей к текущему расположению локомотива; γ – вероятность совпадения результатов расчетов текущего времени и количества осей; $\overline{\nu} = (1-\nu)$ – вероятность ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей.

Математические ожидания времени ($T_0, T_1, T_2, T_3, T_4, T_5$) пребывания системы, описываемой моделью 2, в приведенных на рис. 1 состояниях графа определяются выражениями (16):

$$T_0 = \frac{1}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}},\ T_1 = T_3 = T_4 = \frac{1}{\mu},$$

$$T_2 = \frac{1}{\lambda_{\text{П}} + \lambda_{\text{К}} + k\lambda_{\text{СЧ}}},\ T_5 = \frac{1}{2\lambda_{\text{П}} + (k-1)\lambda_{\text{СЧ}} + \lambda_{\text{СЧ}} + \lambda_{\text{К}}}. \quad (16)$$

Преобразуем формулы (9), (10) и (11) к явной форме применительно к модели 2 с учетом выражений (15) и (16) параметров модели 2:

$$T_{ОП} \approx \frac{\dfrac{1}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}}}{\left(1 - \dfrac{2\alpha_1\lambda_{\text{П}}}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}} - \dfrac{\lambda_K}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}} - \dfrac{2\alpha_2^{\bullet}k\lambda_{\text{СЧ}}}{2\lambda_{\text{П}} + k\lambda_{\text{СЧ}} + \lambda_{\text{К}}}\right)} =$$

$$= \frac{1}{2\overline{\alpha}_1\lambda_{\text{П}} + \left(1-\alpha_2^{\bullet}\right)k\lambda_{\text{СЧ}}}, \quad (17)$$

$$\lambda_{\text{ОП}} \approx 2\overline{\alpha}_1\lambda_{\text{П}} + \left(1-\alpha_2^{\bullet}\right)k\lambda_{\text{СЧ}} . \quad (18)$$

Вероятность опасного отказа системы

$$Q_{\text{ОП}}(t) \approx [2\overline{\alpha}_1\lambda_{\text{П}} + \overline{\alpha}_2^{\bullet}\cdot k\lambda_{\text{СЧ}}]\cdot t . \quad (19)$$

Результаты исследования

Модель 1

Определение α_1 и α_2 осуществляется по формулам (1) и (2). Согласно исследованиям, которые описаны в работе [4], вероятность правильного обнаружения отказов встроенными средствами контроля в бортовой системе безопасности (должна соответствовать SIL 4) обеспечивается на уровне $\alpha_{12} = 0{,}9$, а в счетчиках осей для уровня SIL 3 достаточным является эффективность встроенных средств $\alpha_{22} = 0{,}8$. Таким образом, остаются неизвестными α_{11} и α_{21}. В работе [5] показана возможность вычислять вероятности комплексного обнаружения отказов α_1 и α_2 по следующим формулам:

$$\alpha_1 = \frac{\lambda_{\text{П}} - \lambda_{\text{ОП}}}{\lambda_{\text{П}}};\ \alpha_2 = \frac{\lambda_{\text{СЧ}} - \lambda_{\text{ОП}}}{\lambda_{\text{СЧ}}} . \quad (20)$$

В соответствии с требованиями четвертого уровня полноты безопасности SIL 4 бортовой системы безопасности $\lambda_{\text{оп}} = 10^{-9}$ 1/ч, а согласно требованиям третьего

уровня полноты безопасности SIL 3 счетчика осей $\lambda_{оп} = 10^{-8}$ 1/ч. На основании требований надежности к локомотивным устройствам, которые приведены в [6], а также с учетом практического опыта их эксплуатации, максимальные значения интенсивности отказа бортовой системы безопасности и счетчика осей $\lambda_{П} = ½ \cdot 10^{-5}$ 1/ч и $\lambda_{СЧ} = 10^{-5}$ 1/ч соответственно. Подставляя данные значения в формулы (20) для α_1 и α_2 получим, что $\alpha_1 = 0{,}9998$, а $\alpha_2 = 0{,}999$. Тогда по формулам (1) и (2) $\alpha_{11} = 0{,}998$, а $\alpha_{21} = 0{,}995$.

Линия связи должна быть надежной и ее вклад в опасный отказ всей системы не должен ухудшать достигнутого уровня безопасности поезда и счетчика осей, поэтому на основе практического опыта $\lambda_К = 10^{-7}$ 1/ч. В качестве примера количество счетчиков осей примем $k = 10$.

Подставив данные значениям в формулы (12) и (13), получим следующие результаты: $T_{оп} \approx 5 \cdot 10^6$ часов, что соответствует $\lambda_{оп} \approx 2{,}02 \cdot 10^{-7}$ 1/ч. Полученное значение $\lambda_{оп}$ соотносится с уровнем полноты безопасности SIL 3.

При необходимости достижения уровня полноты безопасности SIL 4 применительно к предложенной структуре системы целесообразно оценить влияние параметра α_2 и показателя надежности элементной базы счетчика осей $\lambda_{СЧ}$ на показатель функциональной безопасности системы $T_{оп}$. С этой целью построим графики (рис. 2) зависимостей показателя $T_{оп}$ от параметра α_2, который варьируется в диапазоне значений от 0,995 до 0,9998, при различных фиксированных значениях показателя надежности элементной базы счетчика осей, а именно $\lambda_{СЧ} = 10^{-5}$ 1/ч и $\lambda_{СЧ} = 10^{-6}$ 1/ч.

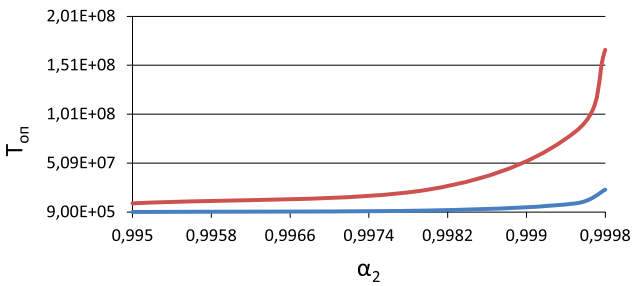

Рис. 2. График зависимости $T_{оп}$ от α_2 при $\lambda_{СЧ} = 10^{-5}$ 1/ч (синий график) и при $\lambda_{СЧ} = 10^{-6}$ 1/ч (красный график).

На основании графиков зависимостей на рис. 2 можно заключить, что путем усиления эффективности встроенного контроля счетчика осей за счет увеличения глубины фонового тестирования (памяти, портов ввода/вывода, обрабатывающего модуля) есть возможность достичь такого значения вероятности правильного обнаружения отказов счетчика осей α_2, которое обеспечивает более высокий уровень функциональной безопасности (функция $T_{оп}$ возрастает). Так, при $\lambda_{СЧ} = 10^{-5}$ 1/ч, выигрыш в $T_{оп}$ достигает одного порядка (от $5 \cdot 10^6$ часов до $2{,}4 \cdot 10^7$ часов). Соответственно интенсивность опасного отказа $\lambda_{оп}$ структуры в целом будет уменьшаться от $2{,}02 \cdot 10^{-7}$1/ч до $4{,}2 \cdot 10^{-8}$1/ч. При использовании в счетчике осей более надежной элементной базы с улучшенными до $\lambda_{СЧ} = 10^{-6}$ 1/ч показателями надежности, такие же показатели $T_{оп}$ и $\lambda_{оп}$ получим уже при комплексной вероятности обнаружения отказов счетчика осей на уровне $\alpha_2 = 0{,}998$.

Таким образом, для ответственных функций системы обеспечения безопасности бортового устройства, при $\lambda_{СЧ} = 10^{-5}$ 1/ч вероятность правильного обнаружения отказов счетчика осей α_2 должна быть не хуже 0,9998, а при $\lambda_{СЧ} = 10^{-6}$ 1/ч α_2 должна быть не хуже 0,998. При одновременном улучшении значений α_2 до 0,9998 и $\lambda_{СЧ}$ до 10^{-6} 1/ч полнота безопасности системы будет обеспечена на уровне SIL 4 (интенсивность опасного отказа системы $\lambda_{оп} \approx 6 \cdot 10^{-9}$ 1/ч.)

Модель 2

Как было показано выше, для достижения уровня полноты безопасности SIL 4 рекомендуемое значение параметра $\alpha_1 = 0{,}9998$. Вероятность правильного обнаружения отказов встроенными средствами контроля в счетчике осей $\alpha_{22} = 0{,}8$. На основании требований надежности к локомотивным устройствам, которые приведены в [6], а также с учетом практического опыта их эксплуатации, максимальные значения интенсивности отказа бортовой системы безопасности и счетчика осей $\lambda_{П} = ½ \cdot 10^{-5}$ 1/ч и $\lambda_{СЧ} = 10^{-5}$ 1/ч соответственно. Линия связи должна быть надежной и ее вклад в опасный отказ всей системы не должен ухудшать достигнутого уровня безопасности поезда и счетчика осей, поэтому на основе практического опыта $\lambda_К = 10^{-7}$ 1/ч. Примем количество счетчиков осей равным $k = 10$. Исходя из условий обеспечения уровня SIL 4, вероятность правильного обнаружения отказов счетчика осей $\alpha_2^{\bullet}$ должна быть не хуже 0,9998, что реально может быть достигнуто при следующих минимальных значениях исходных параметров β, γ и ν. Вероятность правильного определение совпадения результатов номера и расположения счетчиков осей к текущему расположению локомотива $\beta = \gamma = 0{,}99$, где γ – вероятность правильного определения совпадения результатов расчетов текущего времени и количества осей. Вероятность отсутствия ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей $\nu = 0{,}999$.

Подставив данные значения в формулы (17) и (18), получим следующие результаты: $T_{оп} \approx 4 \cdot 10^7$ часов, что соответствует $\lambda_{оп} \approx 2{,}4 \cdot 10^{-8}$ 1/ч.

Чтобы обеспечить уровень полноты безопасности счетчиков осей не ниже, чем это имеет место при их двухканальной архитектуре, необходимо обеспечить соответствующий высокий уровень правильного обнаружения отказа счетчика осей $\alpha_2^{\bullet}$. Вероятность правильного обнаружения отказов счетчика осей соответственно равна $\alpha_2^{\bullet} = \alpha_{22} + \nu(\beta + \gamma - \beta\gamma) - \alpha_{22}\nu(\beta + \gamma - \beta\gamma)$.

Исследуем индивидуальную степень влияния изменения параметров β, γ, ν и α_{22} на общую вероятность правильного обнаружения отказов счетчика осей $\alpha_2^{\bullet}$. Для этого рассмотрим влияние параметра β в диапазоне от 0,99 до 0,999 на $\alpha_2^{\bullet}$ при разных фиксированных значениях

ν, а также рассмотрим влияние параметра α_{22} в диапазоне от 0,8 до 0,99 на $\alpha_2^{\bullet}$ при тех же значениях ν. В обоих случаях примем β = γ. Для более наглядной демонстрации поведения функции неправильного обнаружения отказов счетчика осей построим графики зависимостей $1-\alpha_2^{\bullet}$ от β (рис. 3) и графики зависимостей $1-\alpha_2^{\bullet}$ от α_{22} (рис. 4).

Формулы (12) и (17) для моделей 1 и 2 отличаются только одним параметром – множителем при $k\lambda_{\text{сч}}$. Отсюда вытекает, что, чтобы средняя наработка до опасного отказа $T_{\text{оп}}$ системы с предложенной архитектурой (модель 2) была не хуже, чем у исходной системы, необходимо, как минимум, чтобы выполнялось равенство:

$$2\bar{\alpha}_2 = 1-\alpha_2^{\bullet} = 1-\alpha_{22}-\nu(\beta+\gamma-\beta\gamma)+\alpha_{22}\nu(\beta+\gamma-\beta\gamma).$$

При β = γ имеет место равенство $2\bar{\alpha}_2 = 1-\alpha_{22}-\nu(2-\beta)\beta(1-\alpha_{22})$.

Проведем исследование индивидуальной степени влияния изменения параметров β, γ, ν и α_{22} на общую вероятность правильного обнаружения отказов счетчика осей α_2. Рассмотрим влияние параметра β в диапазоне от 0,99 до 0,999 на $1-\alpha_2$ при разных фиксированных значениях ν, а также рассмотрим влияние параметра α_{22} в диапазоне от 0,8 до 0,99 на $1-\alpha_2$ при тех же значениях ν. Результаты расчетов показаны на графиках зависимостей (рис. 5 и рис. 6 соответственно).

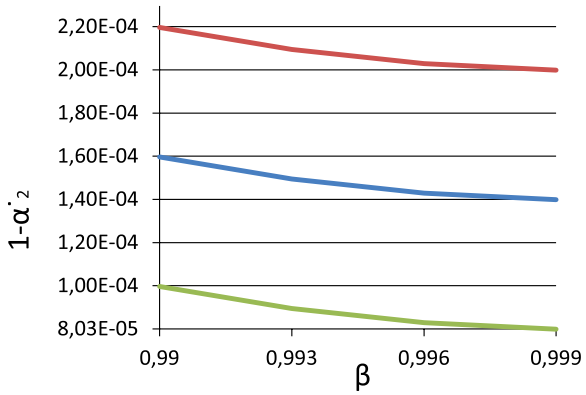

Рис. 3. График зависимости $1-\alpha_2^{\bullet}$ от β при ν = 0,999 (красный график), при ν = 0,9993 (синий график) и при ν = 0,9996 (зеленый график).

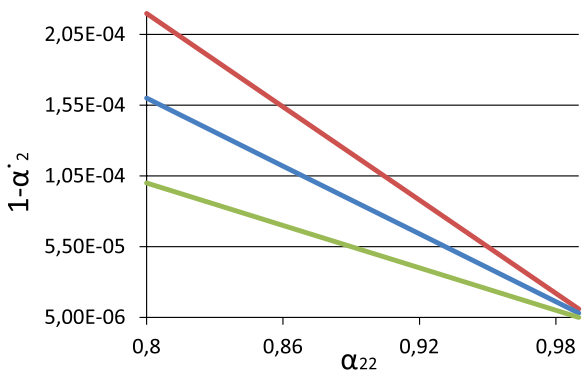

Рис. 4. График зависимости $1-\alpha_2^{\bullet}$ от α_{22} при ν = 0,999 (красный график), при ν = 0,9993 (синий график) и при ν = 0,9996 (зеленый график).

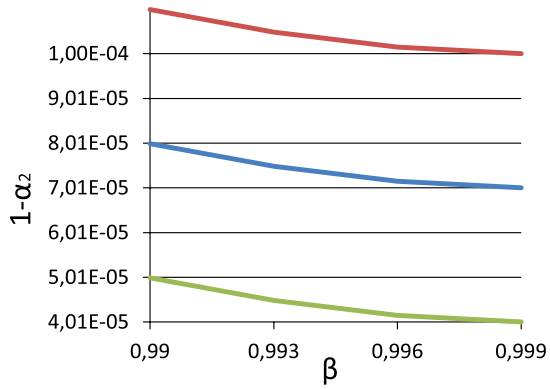

Рис. 5. График зависимости $1-\alpha_2$ от β при ν = 0,999 (красный график), при ν = 0,9993 (синий график) и при ν = 0,9996 (зеленый график).

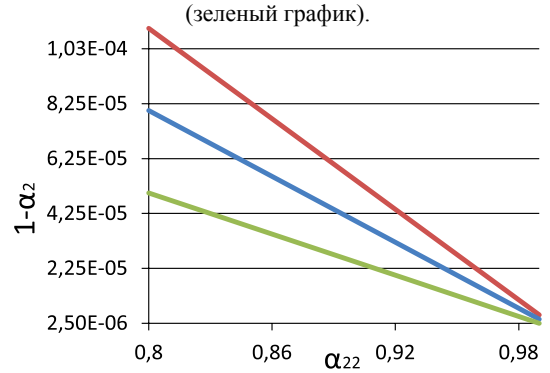

Рис. 6. График зависимости $1-\alpha_2$ от α_{22} при ν = 0,999 (красный график), при ν = 0,9993 (синий график) и при ν = 0,9996 (зеленый график).

Из полученных графиков зависимостей видно, что увеличение вероятности правильного определения совпадения результатов номера и расположения счетчиков осей к текущему расположению локомотива β несущественно влияет на уменьшение вероятности неправильного обнаружения отказа счетчика осей $1-\alpha_2^{\bullet}$ и $1-\alpha_2$. При этом путем усложнения алгоритмов формирования динамических данных для сравнения между бортовой системой локомотива и счетчиком осей, а также изменения количества бит, покрываемых кодом безопасности, например, CRC, можно добиться увеличения вероятности отсутствия ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей ν. А за счет увеличения глубины фонового тестирования (памяти, портов ввода/вывода, обрабатывающего модуля) можно получить более высокую вероятность правильного обнаружения отказов встроенными средствами контроля в счетчике осей α_{22}. Такие усовершенствования алгоритмов позволят уменьшить вероятность неправильного обнаружения отказа счетчика осей $1-\alpha_2^{\bullet}$ и $1-\alpha_2$ более чем на один порядок.

Учитывая выявленную степень влияния параметров β, ν и γ, рассмотрим поведение $T_{\text{оп}}$ в зависимости от ν в диапазоне от 0,999 до 0,9999 при фиксированных на минимальном значении β = γ = 0,99, α_{22} = 0,8 и построим график зависимости $T_{\text{оп}}$ от ν, рис. 7.

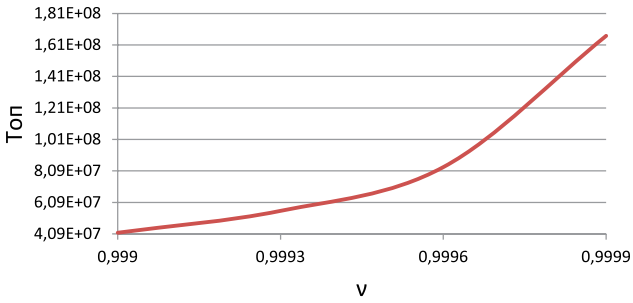

Рис. 7. График зависимости $T_{оп}$ от ν.

Из полученных расчетов и графика зависимости (рис. 7) видно, что при доведении вероятности отсутствия ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей ν до уровня, позволяющего обеспечить более высокий уровень функциональной безопасности (за счет усложнения алгоритмов формирования динамических данных для сравнения между бортовой системой локомотива и счетчиком осей, а также за счет изменения количества бит, покрываемых кодом безопасности, например, CRC), выигрыш в показателе безопасности $T_{оп}$ составляет более чем в 3 раза (от $4 \cdot 10^7$ часов до $1{,}7 \cdot 10^8$ часов). Соответственно интенсивность опасного отказа $\lambda_{оп}$ структуры в целом будет уменьшаться от значения $2{,}4 \cdot 10^{-8}$ 1/ч до значения $6 \cdot 10^{-9}$ 1/ч.

Сравнивая графики на рис. 2 и рис. 7 можно увидеть, что максимальное значение показателя безопасности $T_{оп}$ в модели 1, равное $1{,}7 \cdot 10^8$ часов, достижимо и для модели 2 при достижении параметров значений ν = 0,9999, β = γ = 0,99, α_{22} = 0,8.

Заключение

Полученные результаты показали, что для снижения стоимости оборудования системы управления движением поезда при сохранении уровня безопасности допустимо использование одноканальных источников информации (в данном случае счетчиков осей) и двухканальных приемников информации (в данном случае бортовой системы управления), имеющих при этом в своем составе программное обеспечение, позволяющее обеспечить соответствующий высокий уровень правильного обнаружения отказа (в данном случае счетчика осей). К указанным средствам обнаружения отказа относятся: определение текущего расположения локомотива и счетчика осей (их железнодорожных координат), текущего времени прохождения локомотива над соответствующем счетчиком осей, расчета текущего номера счетчика осей и расчета количества осей проходящего локомотива.

В представленной статье произведено нормирование вероятностных показателей эффективности программных и аппаратных средств обнаружения отказа для структуры с одноканальным источником и двухканальным приемником информации. При этом под нормированием показателей понимается процесс установления их предельно допустимых значений, обеспечивающих количественные показатели безопасности (среднюю наработку системы до опасного отказа, интенсивность и вероятность опасного отказа системы) не хуже, чем у традиционной структуры с двухканальными формирующим и принимающим устройствами. Выявлены наиболее значимые для обеспечения безопасности параметры эффективности средств правильного обнаружения отказа (в данном случае счетчика осей) (вероятность отсутствия ложного совпадения результатов расчетов бортовой системы локомотива и счетчика осей ν и вероятность правильного обнаружения отказов встроенными средствами контроля в счетчике осей α_{22}). Увеличение глубины фонового тестирования, усложнение алгоритмов вычисления динамических данных для сравнения между бортовой системой локомотива и счетчиком осей, а также изменение количества бит, покрываемых кодом безопасности, позволяют обеспечить высокий уровень правильного обнаружения отказа (в данном случае счетчика осей).

Библиографический список

1. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: ООО «Журнал «Надежность», 2012. 296 с.

2. Иыуду К.А. Надежность контроль и диагностика вычислительных машин и систем. М.: «Высшая школа», 1989. 216 с.

3. Шубинский И.Б. Методы обеспечения функциональной надежности программ // Надежность. 2014. №4. С. 87-101.

4. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: ООО «Журнал Надежность», 2012. 212 с.

5. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. М.: Журнал Надежность, 2016. 544 с.

6. Локомотивные устройства безопасности нового поколения. Технические требования. Утверждены Распоряжением ОАО «РЖД» от 30.12.2020 г. № 2995/р.

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

8. Харлап С.Н. Разработка микропроцессорного модуля управления для системы железнодорожной автоматики : учеб.-метод. пособие. Гомель: БелГУТ, 2015. 175 с.

9. BS EN 50128:2011. Railway applications – Communication, signaling and processing systems – Software for railway control and protection systems.

10. IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

References

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

2. Iyudu K.A. [Dependability supervision and diagnostics of computer systems].

3. Moscow: Vysshaya Shkola; 1989. (in Russ.)

4. Shubinsky IB. Methods of software functional dependability assurance. *Dependability* 2014;4:95-101.

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

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

7. [Next-Generation Onboard Train Protection Systems. Technical requirements]. Approved by Order of JSC RZD dated December 30, 2020. No. 2995/r.

8. 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.

9. Kharlap S.N. [Development of a computer-based control unit for a railway command and control system: a study guide]. Gomel: BelSUT; 2015. (in Russ.)

10. BS EN 50128:2011. Railway applications – Communication, signaling and processing systems – Software for railway control and protection systems; 2011.

11. IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems; 2010.

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

Коровин Александр Сергеевич – начальник сектора решения перспективных задач АО «НИИАС», Москва, Российская Федерация, e-mail: A.Korovin@vniias.ru

Пенькова Наталья Геннадьевна – заместитель начальника центра безопасности и алгоритмической поддержки АО «НИИАС», Москва, Российская Федерация, e-mail: N.Penkova@vniias.ru

About the authors

Igor B. Shubinsky, Professor, Doctor of Engineering, Deputy Director of Integrated Research and Development Unit, JSC NIIAS, 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.

Alexander S. Korovin, Head of Sector for Future-Oriented Solutions, JSC NIIAS, Moscow, Russian Federation, e-mail: A.Korovin@vniias.ru.

Natalia G. Penkova, Deputy Head of Centre for Safety and Algorithmic Support, JSC NIIAS, Moscow, Russian Federation, e-mail: N.Penkova@vniias.ru.

Вклад авторов в статью

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

Розенбергом Е.Н. выполнена постановка задачи исследования.

Коровиным А.С. выполнены расчетные исследования, анализ и обзор результатов исследований.

Пеньковой Н.Г. выполнены подготовка исходных данных для расчетного исследования и участие в анализе результатов исследований.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.