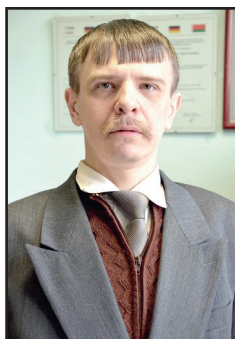




Метод для расчётных оценок характеристик безопасности железнодорожной автоматики



Константин БОЧКОВ



Дмитрий КОМНАТНЫЙ

*Бочков Константин Афанасьевич – Белорусский государственный университет транспорта, Республика Беларусь, Гомель.
Комнатный Дмитрий Викторович – Белорусский государственный университет транспорта, Республика Беларусь, Гомель*.*

Рассматривается проблема количественного анализа безопасности микроэлектронных и микропроцессорных систем железнодорожной автоматики и телемеханики. Проблема остаётся актуальной, так как предметом анализа безопасности являются редко происходящие, но очень опасные события. В качестве основных характеристик безопасности выбраны риск и значимость отказа. Определение значимости отказа выбрано по стандарту MIL-STD-1629A как наиболее адекватное. Приведены расчётные выражения для значимости отказа. Вероятность возникновения опасного отказа получена методом модельного анализа. Вероятность перерастания отказа в аварию предлагается рассчитывать методами сценарного анализа путём

построения древа событий. Приведены расчётные соотношения для рейтингов нарушений, позволяющие сравнивать опасные отказы и аварийные последовательности, в которые отказ может перерасти. Оценка риска эксплуатации систем железнодорожной автоматики выбрана не связанной с экономическими категориями, удобная для нормирования. Она основана на вероятностных представлениях о природе риска и рассчитывается методами теории вероятности. Разработанные расчётные соотношения и модели позволяют анализировать выполнение функций систем обеспечения безопасности движения поездов методами, общими для систем управления, но вместе с тем отражающими особенности работы железнодорожной автоматики.

Ключевые слова: железная дорога, системы железнодорожной автоматики, безопасность, риск, значимость отказа, рейтинги отказов, вероятность опасного отказа, нормирование риска.

*Информация об авторах:

Бочков Константин Афанасьевич – доктор технических наук, профессор, научный руководитель – заведующий НИЛ «Безопасность и электромагнитная совместимость технических средств» Белорусского государственного университета транспорта, Республика Беларусь, Гомель, bochkov1999@mail.ru, priemnay@belsut.gomel.by.

Комнатный Дмитрий Викторович – кандидат технических наук, доцент кафедры автоматики телемеханики и связи, докторант Белорусского государственного университета транспорта, Республика Беларусь, Гомель, toe4031@gstu.by.

Статья поступила в редакцию 17.02.2020, принята к публикации 28.05.2020.

For the English text of the article please see p. 169.

Успешная разработка и внедрение современных микроэлектронных и микропроцессорных систем железнодорожной автоматики и телемеханики (СЖАТ) требуют проведения анализа их безопасности количественными методами. Это объясняется тем, что в таких системах условия безопасности перевозочного процесса реализуются аппаратно-программными средствами. Применяемая элементная база имеет симметричные отказы, интенсивность которых значительно выше интенсивности отказов электромагнитных реле I класса надёжности. К тому же микроэлектронная элементная база имеет низкую устойчивость к электромагнитным помехам и вместе с тем эксплуатируется в сложной электромагнитной обстановке. Следовательно, обеспечить безопасность современных СЖАТ путём экспертных оценок аналогично системам, построенным на реле I класса надёжности, становится невозможным.

В опубликованных монографиях по железнодорожной автоматике [2–4] наиболее распространены методы анализа безопасности, созданные на основе моделей и представлений теории надёжности. Теория надёжности в настоящее время получила широкое развитие, поэтому естественны попытки использовать её для решения новых технических задач. По этому пути построения теории безопасности следуют авторы работ [5–7]. В методах анализа безопасности из [2–4] основной величиной, описывающей безопасность, является интенсивность потока отказов. Предполагается, что поток отказов – пуассоновский, интенсивность отказов является статистически устойчивой величиной. На основании этого подхода в [8; 9] использованы такие показатели безопасности, как средняя наработка до отказа, время пребывания системы в состоянии опасного отказа, коэффициент безопасности. Справедливо отмечается [10], что такие методы анализа безопасности не учитывают то обстоятельство, что опасные отказы, аварии и крушения являются редкими и даже уникальными событиями. Также не учитывается, что для перерастания опасного отказа в аварию требуется стечение нескольких неблагоприятных обстоятельств, которое также происходит достаточно

редко. Достоверное определение интенсивности опасных отказов представляет собой самостоятельную проблему.

С целью учёта редкости событий аварий в [11] предлагается рассматривать участки законов распределения плотности вероятности величин, характеризующих опасные отказы, с большими значениями этих величин и малыми вероятностями их появления. Однако при таком подходе возникает проблема определения параметров и характеристик законов распределения либо из теоретических соображений, либо из данных опыта.

Следовательно, разработка методов анализа безопасности СЖАТ представляет собой крупную научно-техническую проблему, исчерпывающее решение которой в настоящее время ещё не получено. Соответственно, целью данной работы является дальнейшее развитие методов анализа безопасности СЖАТ.

РЕЗУЛЬТАТЫ

Для достижения поставленной цели требуется, в первую очередь, ввести основные величины, характеризующие свойство безопасности СЖАТ. В [12] указано, что такими величинами в теории безопасности систем управления ответственными технологическими процессами являются риск и значимость отказа. Там же изложены общие методы определения этих величин. Применительно к СЖАТ на основании [12] могут быть предложены модификация таких методов количественных расчётов значимости отказа и риска, а также способы рейтингового анализа нарушений безопасности и нормирования риска.

Наиболее адекватное определение значимости отказа C приведено в методике из стандарта MIL-STD-1629A. Хотя этот стандарт и отменён официально, заменён на стандарт MIL-STD-2070, но его методы и модели продолжают широко использоваться при проведении анализа безопасности ответственных технических систем, в частности, летательных аппаратов [1; 12; 13]. В указанных стандартах значимость отказа определяется как вероятность перерастания исходного опасного отказа в аварийную ситуацию:

$$C = P(I_0) P(E/I_0), \quad (1)$$

где $P(I_0)$ – вероятность отказа;





$P(E/I_0)$ – вероятность перерастания опасного отказа в аварию.

Такое определение учитывает, что не каждый опасный отказ влечёт за собой аварийную ситуацию; для развития аварийной ситуации должно произойти стечение нескольких неблагоприятных обстоятельств. Это стечение случается достаточно редко. Следовательно, приведённое определение значимости отказа устраняет отмеченный выше недостаток существующих методов анализа безопасности.

Значимость отказа имеет математический смысл вероятности возникновения аварийной ситуации по причине данного опасного отказа, поэтому её нормирование должно осуществляться по стандарту ГОСТ Р МЭК 61508-2-2012, в котором установлены уровни SIL и соответствующие значения вероятностей опасного отказа выполнения функции безопасности. В частности, для систем железнодорожной автоматики установлен уровень безопасности SIL 4 по ГОСТ 33894-2016.

Вероятность опасного отказа на основании [14] определяется по формуле:

$$P(I_0) = P_{hw}(T_{mi}) P_{sw}(T_{mi}) P_{op}(T_{mi}) P_{emd}(T_{mi}), \quad (2)$$

где P_{hw} – вероятность того, что время t с момента вступления поезда на маршрут до момента отказа аппаратуры СЖАТ не меньше времени пребывания поезда на маршруте;

P_{sw} – вероятность того, что время t с момента вступления поезда на маршрут до момента отказа программно-математического обеспечения СЖАТ не меньше времени пребывания поезда на маршруте;

P_{op} – вероятность того, что время t с момента вступления поезда на маршрут до момента отказа оператора СЖАТ не меньше времени пребывания поезда на маршруте;

P_{emd} – вероятность того, что время t с момента вступления поезда на маршрут до момента отказа аппаратуры СЖАТ под действием электромагнитных помех не меньше времени пребывания поезда на маршруте;

T_{mi} – время пребывания поезда на маршруте, с.

Вероятности P_{hw} , P_{sw} , P_{op} рассчитываются по формулам:

$$P_{hw}(T_{mi}) = \exp\left[-T_{mi} \sum_{m=1}^{m_0} \lambda_m (1 - v_m)\right], \quad (3)$$

$$P_{sw}(T_{mi}) = \exp\left[-a T_{mi} \sum_{m=1}^{m_0} \lambda_m\right], \quad (4)$$

$$P_{op}(T_{mi}) = \exp\left[-T_{mi} \sum_{m=1}^{m_0} \lambda_m (1 - v_m)\right], \quad (5)$$

где λ – интенсивность отказов 1/с;

v – коэффициент, учитывающий парирование опасного отказа устройствами самоконтроля [14];

a – коэффициент, учитывающий пребывание программно-математического обеспечения в пассивном состоянии;

m_0 – число возможных отказов.

Характеристики электромагнитных помех, воздействующих на СЖАТ, имеют вероятностную природу [15]. Неоднократно предпринимались экспериментальные исследования законов распределения плотности вероятности характеристик электромагнитных помех [15; 16]. Поэтому вероятность отказа аппаратуры СЖАТ под действием электромагнитных помех рационально рассчитывать на основании известной модели «нагрузка–устойчивость» [15]:

$$P_{emd} = \int_0^{\infty} f_N(U) F_R(U) dU, \quad (6)$$

где U – напряжение помех, В;

$f_N(U)$ – функция плотности вероятности распределения уровня помех;

$F_R(U)$ — функция вероятности уровня помехоустойчивости аппаратуры СЖАТ.

Вероятность перерастания опасного отказа в аварию определяется путём анализа деревьев событий аварийных последовательностей по [12; 17]. Также задача расчёта вероятности перерастания опасного отказа в аварию решается в [18; 19]. Таким образом, при расчёте вероятности перерастания опасного отказа в аварию осуществляется сценарный анализ, рассматриваются конкретные пути реализации аварии. При расчёте вероятности опасного отказа осуществляется модельный анализ опасного отказа на основе моделей для расчёта вероятности отказов, вызванных различными причинами. Эти этапы анализа безопасности систем управления ответственными технологическими процессами, в том числе СЖАТ, являются обязательными [11].

Для сравнительного анализа нарушений безопасности вводятся понятия рейтингов нарушений [12].

Рейтинг $R = \sum_{i=1}^L Q_i$ отражает вероятность развития данного опасного отказа по всем L аварийным последовательностям.

Максимальный рейтинг $R_{max} = \max(Q_i)$ отражает вероятность развития наиболее вероятной аварийной последовательности для данного опасного отказа.

Средний рейтинг $R_{mdl} = R/L$ отражает вероятность развития всех возможных аварийных последовательностей для данного опасного отказа.

Завершающим этапом анализа безопасности систем управления ответственными технологическими процессами, в их числе и СЖАТ, является оценка риска эксплуатации. При оценке риска желательно не использовать экономические категории и «политические» соображения [20], а вместо этого получить численную оценку, удобную для нормирования. Такая оценка предложена в [21] и осуществляется по формуле:

$$\rho = \frac{1}{\frac{1}{P_{mf}} - 1}, \quad (7)$$

где P_{mf} — вероятность сбоя аппаратуры.

Так как значимость отказа имеет математический смысл вероятности возникно-

вения аварийной ситуации по причине данного опасного отказа, то применительно к рассматриваемому в статье методу анализа безопасности выражение (7) преобразуется к:

$$\rho = \frac{1}{\frac{1}{C} - 1}, \quad (8)$$

где C — значимость отказа.

В [21] обоснованы граничные значения риска, которые определяют области нормальной и аварийной работы технической системы и позволяют нормировать значения риска при эксплуатации СЖАТ:

- $0 < \rho < 1$ — ограниченная безопасность;
- $\rho = 1$ — критическое состояние, наличие отказов;
- $\rho > 1$ — опасное состояние, угроза аварии;
- $\rho \gg 1$ — запредельное состояние, угроза катастрофы.

ВЫВОДЫ

Итак, в статье сформулирован метод анализа безопасности СЖАТ, приведены соотношения для расчёта величин, характеризующих безопасность эксплуатации СЖАТ, описан сценарный и модельный анализ безопасности СЖАТ.

Отличительными чертами предлагаемого метода являются:

1. Учитываются основные исходные события, могущие привести к браку в поездной работе, аварии, крушению: отказы аппаратной части по причине ограниченной надёжности элементной базы, ошибки программно-математического обеспечения, ошибки оператора, воздействие электромагнитных помех.

2. Учитываются неаддитивность факторов, влияющих на опасный отказ, критичность совокупности факторов и другие аспекты перерастания опасного отказа в аварийную ситуацию.

3. Развитие аварийной ситуации характеризуется параметрами, которые можно просто определить в практике эксплуатации. Не используется общий поток опасных отказов, распределение плотности вероятности в области хвостов распределения, оценка которых осложнена редкостью соответствующих событий.

4. Показатели безопасности и риска позволяют осуществить нормирование, не



привлекая экономические категории, обоснованно сравнивать аварийные последовательности в аспекте безопасности с учётом наиболее вероятных, вероятных, и в среднем. Учитываются и возможные исходные события, и пути перехода в аварию, и возможное конечное происшествие.

5. Редкость и даже уникальность аварийной ситуации не влияет на выбор математического описания; аварийные ситуации учитываются в дереве событий.

6. Используется методика анализа, общая для систем управления ответственными технологическими процессами, осуществляются сценарный и модельный анализ риска, необходимый для всех технических систем.

7. Вероятности исходных событий рассчитываются по хорошо апробированным методам теории надёжности, характеристики аварийных ситуаций – специфическими адекватными методами теории безопасности.

8. Реализуется принцип принятия решения на основе фактов [10].

Очевидно, что все достоинства предлагаемого в статье метода и преодолеваемые им трудности анализа безопасности непосредственно применимы к вопросам эксплуатации СЖАТ, обеспечения функциональной безопасности этих систем. При этом осуществляется дальнейшее развитие теории СЖАТ на основе уже достигнутого уровня [14; 17].

Поэтому допустимо заключить, что результаты настоящей статьи могут найти применение для доказательства безопасности современных микропроцессорных и микроэлектронных СЖАТ, что является актуальной научно-практической задачей и необходимым этапом разработки и внедрения таких систем.

ЛИТЕРАТУРА

1. MIL-STD1629A 24 November 1980 Military Standart Procedures for Performing a Failure Mode, Effects and Criticality Analysis. Washington, DC, Department of Defense; Washington, DC: Department of defense, 1980, 25 p. [Электронный ресурс]: <https://www.fmea-fmea.com/milstd1629.pdf>. Доступ 27.03.2020.
2. Сапожников В. В., Елкин Б. Н., Кокурин И. М. [и др.] Станционные системы автоматики и телемеханики: Учебник / Под ред. В. В. Сапожникова. – М.: Транспорт, 1997. – 432 с.
3. Андрес Э., Долгий И. [и др.] Системы автоматики и телемеханики на железных дорогах мира: Учеб. пособие. [Пер. с англ.] / Под ред. Т. Тега и С. Власенко. – М.: Интекст, 2010. – 496 с.

4. Сапожников В. В. [и др.] Сертификация и доказательство безопасности систем железнодорожной автоматики / Под ред. В. В. Сапожникова. – М.: Транспорт, 1997. – 288 с.

5. Шубинский И. Б., Новожилов Е. О. Метод нормирования показателей надёжности объектов железнодорожного транспорта // Надёжность. – 2019. – Т. 19. – № 4 – С. 17–23.

6. Шубинский И. Б., Замышляев А. М., Проневич О. Б. Графовый метод оценки производственной безопасности на объектах железнодорожного транспорта // Надёжность. – 2017. – Т. 17. – № 1. – С. 40–45.

7. Маковеев О. Л., Костюнин С. Ю. Оценка параметров безопасности и безотказности систем контроля и управления // Надёжность – 2017. – Т. 17. – № 1. – С. 46–52.

8. Braband, J. A practical guide to safety analysis methods. Signal + Draht, 2001, Vol. 93, No. 9, pp. 41–44.

9. Braband, J., Lennartz, A. Systematic Process for the Definition of Safety Targets for Railway Signalling Applications. Signal + Draht, 1999, No. 9, pp. 53–57.

10. Негрей В. Я. Развитие методов оценки безопасности перевозочного процесса на железнодорожном транспорте // Вестник БелГУТ. Наука и транспорт. – 2002. – № 2. – С. 12–16.

11. Махутов Н. А., Пермяков В. Н., Аметханов Р. С. и др. Анализ рисков и обеспечение защищённости критически важных объектов нефтегазохимического комплекса. – Тюмень: Тюм. ГНГУ, 2013. – 560 с.

12. Александровская Л. М. [и др.] Безопасность и надёжность технических систем. – М.: Университетская книга, Логос. – 2008. – 378 с.

13. MIL-STD2070 15 April 1983 Military Standart Procedures for Performing a Failure Mode, Effects and Criticality Analysis for Aeronaut and ICAL Equipment. Washington, DC, Naval Publications and Form center, 1983, 24 p.

14. Лисенков В. М. Безопасность технических средств в системах управления движением поездов. – М.: Транспорт, 1992. – 160 с.

15. Бочков К. А. Теория и методы контроля электромагнитной совместимости микроэлектронных систем обеспечения безопасности движения поездов / Дис... док. тех. наук. – М.: МИИТ, 1993. – 379 с.

16. Бестемьянов П. Ф. Методика статистического моделирования электромагнитных помех в каналах автоматики и телемеханики на железнодорожном транспорте // Электротехника. – 2016. – № 9. – С. 2–8.

17. Лисенков В. М. Статистическая теория безопасности движения поездов. – М.: ВИНТИ РАН, 1999. – 232 с.

18. Баранов Л. А., Кульба В. В., Шелков А. Б., Сомов Д. С. Индикаторный подход в управлении безопасностью объектов железнодорожного транспорта // Надёжность. – 2018. – Т. 18. – № 2. – С. 34–42.

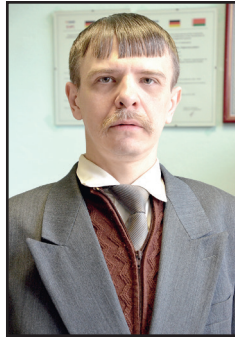
19. Проневич О. Б., Швед В. Э. Алгоритм расчёта и прогнозирования показателей функциональной безопасности систем электроснабжения железнодорожного транспорта // Надёжность – 2018. – Т. 18. – № 3. – С. 46–55.

20. Малкин В. С. Надёжность технических систем и техногенный риск. – Ростов н/Д: Феникс, 2010. – 452 с.

21. Сосновский Л. А. Риск. Механотермодинамика необратимых повреждений. – Гомель: БелГУТ, 2004. – 317 с.



Method for Calculating Safety Features of Railway Automation Devices



Konstantin A. BOCHKOV

Dmitry V. KOMNATNIY

*Bochkov, Konstantin A., Belarusian State University of Transport, Republic of Belarus, Gomel.
Komnatniy, Dmitry V., Belarusian State University of Transport, Republic of Belarus, Gomel*.*

ABSTRACT

The problem of quantitative analysis of safety of microelectronic and microprocessor systems of railway automation and telemechanics is considered. The problem remains relevant, since the subject of safety analysis is rarely occurring, but extremely dangerous events. The risk and significance of failure are selected as the main safety features of these systems. The way to identify a failure was chosen according to MIL-STD-1629A standard, as the most adequate. Calculated expressions for significance of a failure are proposed. The probability of a dangerous failure is calculated by the method of model analysis. It is proposed to calculate the probability of a failure further developing into an accident

using scenario analysis methods by constructing event trees. Calculated ratios for ratings of violations are suggested, allowing to compare dangerous failures and emergency sequences developed from a failure. The risk assessment of operation of railway automation systems was selected not related to economic categories, and thus convenient for rationing. It is based on probabilistic concepts of the nature of risk and is calculated using the methods of probability theory. The developed design ratios and models make it possible to analyze performance of the functions of train traffic safety systems by methods common to control systems, at the same time reflecting the features of operation of railway automation.

Keywords: railway, railway automation systems, safety, risk, significance of a failure, ratings of failures, probability of dangerous failure, risk regulation.

*Information about the authors:

Bochkov, Konstantin A. – D.Sc. (Eng), Professor, Scientific Supervisor – Head of the Research Laboratory of Safety and electromagnetic compatibility of technical means of Belarusian State University of Transport, Republic of Belarus, Gomel, bochkov1999@mail.ru, priemnay@belsut.gomel.by.

Komnatniy, Dmitry V. – Ph.D. (Eng), Associate Professor of the Department of Automation of Telemechanics and Communications, D.Sc. student of Belarusian State University of Transport, Republic of Belarus, Gomel, toe4031@gstu.by.

Article received 17.02.2020, accepted 28.05.2020.

For the original Russian text of the article please see p. 164.

Successful development and implementation of modern microelectronic and microprocessor railway automation and telemechanics systems (RATS) require quantitative analysis of their safety. This is due to the fact that in such systems, safety conditions of the transportation process are implemented by hardware and software tools. The applied element base has symmetrical failures, the intensity of which is much higher than the failure rate of electromagnetic relays of I class of reliability. In addition, the microelectronic element base has low immunity to electromagnetic interference and, at the same time, operates in a complex electromagnetic environment. Consequently, it becomes impossible to ensure safety of modern RATS through expert assessments, similar to systems built on relays of I class of reliability.

In the published monographs on railway automation [2–4], the most common methods of safety analysis are based on models and representations of the theory of reliability. The theory of reliability has now been widely developed, therefore, attempts to use it to solve new technical problems are natural. The authors of [5–7] follow this path of constructing a safety theory. In safety analysis methods from [2–4], the main value describing safety is the rate of failure. It is assumed that the failure flow is Poisson, and the failure rate is statistically stable. On the basis of this approach, in [8; 9] such safety indicators as mean time to failure, the time the system remains in a state of dangerous failure, and safety factor. It is fairly noted [10] that such methods of safety analysis do not take into account the fact that dangerous failures, accidents and crashes are rare and even unique events. It is also not considered that a combination of several unfavorable circumstances is required for development of a dangerous failure into an accident, which also occurs quite rarely. Reliable determination of intensity of dangerous failures is an independent problem.

In order to take into account rarity of accident events, in [11] it is proposed to consider sections of the probability density distribution laws of quantities characterizing dangerous failures, with large values of these quantities and low probabilities of their occurrence. However, with this approach, the problem arises of determining the parameters and characteristics of distribution laws either

from theoretical considerations or from experience data.

Consequently, development of methods for analyzing safety of RATS is a major scientific and technical problem, an exhaustive solution of which has not yet been obtained. Accordingly, the *objective* of this work is further development of methods for analyzing safety of RATS.

Results.

To achieve the stated objective, it is required, first of all, to introduce the basic values that characterize the safety property of RATS. In [12] it is indicated that such values in the theory of safety of control systems for responsible technological processes are associated with risk and significance of a failure. General methods for determining these values are also presented there. With regard to RATS, based on [12], the below described modification of such methods for quantitative calculations of significance of a failure and a risk, as well as methods for rating analysis of safety violations and risk regulation, can be proposed.

The most adequate definition of significance of a failure C is given in the methodology of MIL-STD-1629A standard. Although this standard has been officially canceled and replaced by MIL-STD-2070 standard, its methods and models continue to be widely used in safety analysis of critical technical systems, in particular, regarding aircrafts [1; 12; 13]. In these standards, significance of a failure is defined as the probability of an initial dangerous failure developing into an emergency:

$$C = P(I_0) \cdot P(E/I_0), \quad (1)$$

where $P(I_0)$ is probability of a failure;

$P(E/I_0)$ is probability of a dangerous failure developing into an emergency.

This definition takes into account that not every dangerous failure entails an emergency; for development of an emergency, a combination of several unfavourable circumstances must occur. This confluence is rare. Consequently, the above definition of significance of a failure eliminates the aforementioned drawback of existing methods of safety analysis.

The significance of a failure has the mathematical meaning of probability of an emergency due to a given dangerous failure, therefore, its regulation should be carried out in accordance with GOST R MEC61508-2-2012 standard, which establishes SIL levels and the corresponding values of probabilities of a



dangerous failure of a safety function. In particular, the safety level of SIL 4 has been set for railway automation systems in accordance with GOST 33894-2016.

The probability of a dangerous failure based on [14] is determined according to the formula $P(I_D) = P_{hw}(T_{mi}) P_{sw}(T_{mi}) P_{op}(T_{mi}) P_{emd}(T_{mi})$, (2) where P_{hw} is probability that time t from the moment the train enters the route until the moment when RATS equipment fails is not less than the time the train stays on the route;

P_{sw} is probability that time t from the moment the train enters the route until the moment of failure of the software and mathematical support of RATS is not less than the time the train stays on the route;

P_{op} is probability that the time t from the moment the train enters the route until the moment of failure of RATS operator is not less than the time the train stays on the route;

P_{emd} is probability that the time t from the moment the train enters the route until the moment when RATS equipment fails under the influence of electromagnetic interference is not less than the time the train stays on the route;

T_{mi} is time of train staying on the route, s.

The probabilities P_{hw} , P_{sw} , P_{op} are calculated according to the formulas:

$$P_{hw}(T_{mi}) = \exp \left[-T_{mi} \sum_{m=1}^{m_0} \lambda_m (1 - v_m) \right], \quad (3)$$

$$P_{sw}(T_{mi}) = \exp \left[-a T_{mi} \sum_{m=1}^{m_0} \lambda_m \right], \quad (4)$$

$$P_{op}(T_{mi}) = \exp \left[-T_{mi} \sum_{m=1}^{m_0} \lambda_m (1 - v_m) \right], \quad (5)$$

where λ is intensity of failures 1/s;

v is coefficient that takes into account parrying of a dangerous failure by self-control devices [14];

a is coefficient taking into account software stay in a passive state;

m_0 is the number of possible failures.

The characteristics of electromagnetic interference affecting RATS are of a probabilistic nature [15]. Experimental studies of laws of probability density distribution of characteristics of electromagnetic interference have been repeatedly undertaken [15; 16]. Therefore, it is rational to calculate the probability of a failure of RATS equipment under the influence of electromagnetic interference on the basis of the well-known «load–stability» model [15]:

$$P_{emd} = \int_0^{\infty} f_N(U) F_R(U) dU, \quad (6)$$

where U is interference voltage, V;

$f_N(U)$ is probability density function of the interference level distribution;

$F_R(U)$ is function of the probability of the interference immunity level of RATS equipment.



The probability of a dangerous failure developing into an accident is determined by analyzing the trees of events of emergency sequences according to [12; 17]. Also, the problem of calculating the probability of a dangerous failure developing into an accident is solved in [18; 19]. Thus, when calculating the probability of a dangerous failure developing into an accident, scenario analysis is carried out, and specific ways of accident emergence are considered. When calculating the probability of a dangerous failure, a model analysis of a dangerous failure is carried out on the basis of models to calculate the probability of failures caused by various reasons. These stages of safety analysis of control systems of critical technological processes, including RATS, are mandatory [11].

For a comparative analysis of safety violations, the concepts of ratings of violations are introduced [12].

The rating $R = \sum_{l=1}^L Q_l$ reflects the probability of a given dangerous failure development for all L emergency sequences.

The maximum rating $R_{max} = \max(Q_l)$ reflects the probability of the most probable emergency sequence for a given dangerous failure.

The average rating $R_{mdl} = R/L$ reflects the probability of development of all possible emergency sequences for this dangerous failure.

The final stage in analysis of safety of control systems for critical technological processes, including RATS, is assessment of the operating risk. When assessing risk, it is desirable not to use economic categories and «political» considerations [20], but to obtain a numerical estimate that is convenient for rationing. Such an estimate was proposed in [21] and is carried out according to the formula:

$$\rho = \frac{1}{\frac{1}{P_{mf}} - 1}, \quad (7)$$

where P_{mf} is probability of equipment failure.

Since the significance of a failure has the mathematical meaning of the probability of an emergency due to a given dangerous failure, in relation to safety analysis method considered in the article, expression (7) is transformed into:

$$\rho = \frac{1}{\frac{1}{C} - 1}, \quad (8)$$

where C is significance of a failure.

In [21], the boundary values of risk are substantiated, which determine the areas of normal and emergency operation of the technical system and make it possible to normalize the risk values during operation of RATS:

- $0 < \rho < 1$ – limited safety;
- $\rho = 1$ – critical state, presence of failures;
- $\rho > 1$ – dangerous state, threat of an accident;
- $\rho \gg 1$ – transcendental state, threat of a catastrophe.

Conclusions.

So, the article formulates a method for analyzing safety of RATS, the ratios for calculating the values that characterize safety of RATS are described, a scenario and model analysis of safety of RATS are also suggested.

The distinctive features of the proposed method are:

1. The main initiating events that can lead to defects in train operation, accidents, crashes are considered: hardware failures due to limited reliability of the element base, errors in software and mathematical support, operator errors, exposure to electromagnetic interference.

2. The non-additivity of factors influencing the dangerous failure, criticality of the combination of factors and other aspects of development of a dangerous failure into an emergency situation are considered.

3. Development of an emergency is characterized by parameters that can be easily determined in operational practice. The general flow of dangerous failures and the probability density distribution in the region of distribution tails are not used since their assessment is complicated by rarity of the corresponding events.

4. Safety and risk indicators allow to carry out standardization without involving economic categories, to reasonably compare emergency sequences in terms of safety, considering the most probable, probable and average. Possible initiating events and paths of transition to an accident and a possible final event are also taken into account.

5. Rarity and even uniqueness of the emergency does not affect the choice of mathematical description; emergency situations are taken into account in the event tree.

6. The method of analysis is used, which is common for control systems of responsible technological processes, scenario and model risk analysis is carried out, which is necessary for all technical systems.

7. The probabilities of initiating events are calculated according to well-tested methods of the theory of reliability, characteristics of emergency situations are calculated with the specific adequate methods of safety theory.

8. The principle of decision making on the basis of facts is implemented [10].

It is obvious that all the advantages of the method proposed in the article and the difficulties of safety analysis solved by it are directly applied to the issues of operation of RATS, ensuring functional safety of these systems. At the same time, further development of the theory of RATS is carried out based on the already achieved level [14; 17].

Therefore, it is permissible to conclude that the results of this article can be used to prove safety of modern microprocessor and microelectronic RATS, which is an urgent scientific and practical task and a necessary stage in development and implementation of such systems.

REFERENCES

1. MIL-STD1629A 24 November 1980 Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis. Washington, DC, Department of Defense; Washington, DC: Department of Defense, 1980, 25 p. [Electronic resource]: <https://www.fmea-fmea.com/milstd1629.pdf>. Last accessed 27.03.2020.

2. Sapozhnikov, V. V., Elkin, B. N., Kokurin, I. M. [et al]. Station automation and telemechanics systems: Textbook [Stantsionnie sistemy avtomatiki i telemekhaniki: Uchebnik]. Ed. by V. V. Sapozhnikov. Moscow, Transport publ., 1997, 432 p.

3. Andres, E., Dolgiy, I. [et al]. Automation and telemechanics systems on the world's railways: Study guide [Sistemy avtomatiki i telemekhaniki na zheleznnykh dorogakh mira: Ucheb. posobie] [Trans. from English]. Ed. by T. Tega and S. Vlasenko. Moscow, Intekst publ., 2010, 496 p.

4. Sapozhnikov, V. V. [et al]. Certification and safety proof of railway automation systems [Sertifikatsiya i dokazatelstvo bezopasnosti sistem zheleznodorozhnoi avtomatiki]. Ed. by V. V. Sapozhnikov. Moscow, Transport publ., 1997, 288 p.

5. Shubinsky, I. B., Novozhilov, E. O. Method of standardization of indicators of reliability of railway transport facilities [Metod normirovaniya pokazatelei nadezhnosti ob'ektov zheleznodorozhnogo transporta]. *Nadezhnost'*, 2019, Vol. 19, Iss. 4, pp. 17–23.

6. Shubinsky, I. B., Zamyshlyayev, A. M., Pronevich, O. B. A graph method for assessing industrial safety at railway transport facilities [Grafoviy metod otsenki proizvodstvennoi bezopasnosti na ob'ektakh zheleznodorozhnogo transporta]. *Nadezhnost'*, 2017, Vol. 17, Iss. 1, pp. 40–45.

7. Makoveev, O. L., Kostyunin, S. Yu. Assessment of safety parameters and reliability of monitoring and control systems [Otsenka parametrov bezopasnosti i bezotkaznosti sistem kontrolya i upravleniya]. *Nadezhnost'*, 2017, Vol. 17, Iss. 1, pp. 46–52.

8. Braband, J. A practical guide to safety analysis methods. SIGNAL + DRAHT, 2001, Vol. 93, No. 9, pp. 41–44.

9. Braband, J., Lennartz, A. Systematic Process for the Definition of Safety Targets for Railway Signalling Applications. SIGNAL + DRAHT, 1999, No. 9, pp. 53–57.

10. Negrei, V. Ya. Development of methods for assessing safety of the transportation process in railway transport [Razvitiye metodov otsenki bezopasnosti perevozhnogo protsessa na zheleznodorozhnom transporte]. *Bulletin of BelSUT. Science and transport*, 2002, Iss. 2, pp. 12–16.

11. Makhutov, N. A., Permyakov, V. N., Ametkhanov, R. S. [et al]. Risk analysis and security of critical objects of the petrochemical complex [Analiz riskov i obespechenie zashchishchennosti kriticheskikh vazhnykh ob'ektov neftegazokhimicheskogo kompleksa]. Tyumen, Tyum. SNSU, 2013, 560 p.

12. Aleksandrovskaya, L. M. [et al]. Safety and reliability of technical systems [Bezopasnost' i nadezhnost' tekhnicheskikh sistem]. Moscow, University book, Logos, 2008, 378 p.

13. MIL-STD2070 15 April 1983 Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis for Aeronaut and ICAL Equipment. Washington, DC, Naval Publications and Form center, 1983, 24 p.

14. Lisenkov, V. M. Safety of technical means in train traffic control systems [Bezopasnost' tekhnicheskikh sredstv v sistemakh upravleniya dvizheniem poezdov]. Moscow, Transport publ., 1992, 160 p.

15. Bochkov, K. A. Theory and methods of control of electromagnetic compatibility of microelectronic systems for ensuring safety of train traffic. D.Sc. (Eng) thesis [Teoriya i metody kontrolya elektromagnitnoi sovmestimosti mikroelektronnykh sistem obespecheniya bezopasnosti dvizheniya poezdov. Dis... doc. tekhn. nauk]. Moscow, MIIT publ., 1993, 379 p.

16. Bestemyanov, P. F. Methods of statistical modelling of electromagnetic interference in the channels of automation and telemechanics on railway transport [Metodika staticheskogo modelirovaniya elektromagnitnykh pomekh v kanalakh avtomatiki i telemekhaniki na zheleznodorozhnom transporte]. *Elektrotehnika*, 2016, Iss. 9, pp. 2–8.

17. Lisenkov, V. M. Statistical theory of train traffic safety [Statisticheskaya teoriya bezopasnosti dvizheniya poezdov]. Moscow, VINITI RAS, 1999, 232 p.

18. Baranov, L. A., Kulba, V. V., Shelkov, A. B., Somov, D. S. Indicator approach in safety management of railway transport facilities [Indikatornyi podkhod v upravlenii bezopasnostyu ob'ektov zheleznodorozhnogo transporta]. *Nadezhnost'*, 2018, Vol. 18, Iss. 2, pp. 34–42.

19. Pronevich, O. B., Shved, V. E. Algorithm for calculating and predicting indicators of functional safety of power supply systems for railway transport [Algoritm rascheta i prognozirovaniya pokazatelei funktsionalnoi bezopasnosti sistem elektrosnabzheniya zheleznodorozhnogo transporta]. *Nadezhnost'*, 2018, Vol. 18, Iss. 3, pp. 46–55.

20. Malkin, V. S. Reliability of technical systems and technogenic risk [Nadezhnost' tekhnicheskikh sistem i tekhnogennyy risk]. Rostov-on-Don, Phoenix publ., 2010, 452 p.

21. Sosnovsky, L. A. Risk. Mechanothermodynamics of irreversible damage [Risk. Mekhanotermodinamika neobratimyykh povrezhdeniy]. Gomel, BelSUT, 2004, 317 p. ●

