УДК 656.25
DOI: https://doi.org/10.30932/1992-3252-2020-18-164-173

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 С 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:

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

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:

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

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

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

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

где λ – интенсивность отказов 1/с;

ν – 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 $R = \sum_{l=1}^{L} Q_l$ отражает вероятность развития данного опасного отказа по всем L аварийным последовательностям.

Максимальный рейтинг $R_{max} = max(Q_l)$ 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:

$$\rho = \frac{1}{\frac{1}{P_{mlf}} - 1}, \qquad (7)$$

где P_{mlf} – вероятность сбоя аппаратуры.

Так как значимость отказа имеет математический смысл вероятности возникновения аварийной ситуации по причине данного опасного отказа, то применительно к рассматриваемому в статье методу анализа безопасности выражение (7) преобразуется к:

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

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;
- $\rho >> 1$ – 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 распределений, 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-fmeca.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 Applicatioins. 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.: ВИНИТИ 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.