УДК 656.25

*В. Ф. КУСТОВ, кандидат технических наук, Украинский государственный университет железнодорожного транспорта, г. Харьков*

# РАЗРАБОТКА ТРЕБОВАНИЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ДЛЯ УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

Рассматриваются вопросы разработки требований функциональной безопасности к решающим элементам каналов резервирования, кратным опасным отказам резервированных систем железнодорожной автоматики, а также определения допустимой наработки до опасного отказа каждого канала резервирования максимально допустимого времени устранения опасных отказов в каналах резервирования для достижения заданного уровня функциональной безопасности.

**Введение.** Обеспечение и доказательство функциональной безопасности систем железнодорожной автоматики является наиболее сложным и дорогостоящим этапом в процессе разработки и обоснованно считается одним из главных факторов возможности допуска их в эксплуатацию. Недостаточный учет отдельных факторов функциональной безопасности, как показывает практика, приводит к значительному ущербу. Так, только из-за просчетов в функциональной безопасности самолета Боинг-737 Max 8 и связанных с ними крупных крушений, унесших 346 жизней, и экономических последствий, ущерб, по оценкам специалистов, для всемирно известной фирмы «Boeing» составил более 20 млрд дол.

Для обеспечения безопасности систем железнодорожной автоматики (СЖА) разработаны нормативные показатели функциональной безопасности (ФБ) для систем в целом, например, [1, 2] и для отдельных их функций безопасности [3, 4]. Также разработаны требования по ФБ к допустимым периодам диагностирования для наиболее часто используемых способов резервирования в СЖА [5]. Учитывая, что во многих случаях ФБ зависит от правильности применения решающих элементов («И», «ИЛИ», «n» из «m»), используемых на выходах и входах каналов резервирования для подачи ответственных сигналов на объекты управления или от объектов контроля, необходимо определять допустимые вероятности или интенсивности опасных отказов этих важных устройств. К сожалению, в некоторых разработках СЖА, даже введенных в эксплуатацию, недопустимо используются варианты решающих элементов «ИЛИ» для подачи управляющих воздействий на стрелочные электродвигатели или лампы разрешающих сигналов светофоров, решающие элементы «И» для подачи сигналов на лампы запрещающих светофоров. В ряде случаев в двух комплектных структурах нагруженного резервирования для обеспечения безопасности используется в каждом комплекте правильный вариант «2» из «2» с решающим элементом «И», но на выходе для повышения готовности используется решающий элемент «ИЛИ», который в 2 раза снижает ФБ СЖА, т. к. позволяет реализовать опасный отказ любого из его комплектов. Это может быть допустимым только при соответствующем запасе по ФБ каждого из комплектов СЖА.

Для обеспечения ФБ важным является также учет кратных отказов, которые могут иметь недопустимую вероятность появления, например из-за одновременного электромагнитного воздействия на все каналы нагруженного резервирования (при неконтролируемых отказах помехозащитных средств) или теплового воздействия на них при отказах систем вентиляции или кондиционирования в шкафах управления, а также при эксплуатации электронных компонентов СЖА в напольных конструктивах (путевых ящиках, муфтах и т. п.), допускающих общий недопустимый перегрев в нескольких каналах резервирования одновременно.

Важным является и определение допустимых значений наработки до опасного отказа каждого канала резервирования и времени устранения опасных отказов в каналах резервирования для достижения заданных уровней ФБ.

Целью настоящей статьи является определение допустимых значений функциональной безопасности решающих элементов резервированных структур, кратных отказов каналов резервирования СЖА, допустимых значений наработки до опасного отказа каждого канала резервирования и времени устранения опасных отказов в каналах резервирования при экспоненциальном законе распределения опасных отказов.

## 1 Определение допустимых значений функциональной безопасности решающих элементов резервированных структур

Максимально допустимое значение периода диагностирования опасных отказов в каждом канале резервирования для наиболее широко применяемых структур систем ЖАТ с мажоритарным резервированием «2» из «3» и нагруженным дублированием «2» из «2» определяется с учетом ФБ решающих элементов и кратных опасных отказов в различных каналах резервирования СЖА согласно работе [5] по следующим выражениям:

$$T_{д.2v3}=\frac{\lambda_{оп.доп}-6\lambda^2_{оп.1}T_у-\lambda_{кр.оп}-n_{рэ}\lambda_{1.оп.рэ}-n_{рэ}\lambda_{кр.оп.рэ}}{6\lambda^2_{оп.1}}; \quad (1)$$

$$T_{д.2v2}=\frac{\lambda_{оп.доп}-2\lambda^2_{оп.1}T_у-\lambda_{кр.оп}-n_{рэ}\lambda_{1.оп.рэ}-n_{рэ}\lambda_{кр.оп.рэ}}{2\lambda^2_{оп.1}}, \quad (2)$$

где $\lambda_{оп.доп}$ – допустимая интенсивность опасных отказов устройств или системы в целом (не одной ответственной функции); $\lambda_{оп.1}$ – интенсивность опасных отказов одного канала резервирования; $T_у$ – максимально допустимое гарантированное время устранения опасных отказов элементов в каналах резервирования СЖА или максимально допустимый период времени, за который будет гарантировано обеспечено полное исключение влияния выявленного опасного отказа в канале резервирования на безопасность ее функционирования в целом; $\lambda_{кр.оп}$ – интенсивность кратных опасных отказов каналов резер-

вирования; $n_{рэ}$ – количество решающих элементов устройства или системы; $\lambda_{1оп.рэ}$ – интенсивность однократных опасных отказов решающего элемента; $\lambda_{кр.оп.рэ}$ – интенсивность кратных опасных отказов решающего элемента.

Из этих выражений, с учетом $\lambda_{оп.рэ} = \lambda_{1.оп.рэ} + \lambda_{кр.оп.рэ}$ можно определить требования к допустимой общей интенсивности опасных отказов решающих элементов для системы ЖАТ с мажоритарным резервированием «2» из «3» и двухканальной дублированной структуры «2» из «2» с решающим элементом «И» для 1-го класса объектов (у которых опасный отказ наступает при несанкционированном появлении сигнала) и «ИЛИ» для 2-го класса объектов (у которых опасный отказ наступает при несанкционированном пропадании сигнала) соответственно:

$$\lambda_{оп.рэ2v3} = \frac{\lambda_{оп.доп} - 6\lambda^2_{оп.1}(T_{д.2v3} + T_у) - \lambda_{кр.оп}}{n_{рэ}}; \quad (3)$$

$$\lambda_{оп.рэ2v2} = \frac{\lambda_{оп.доп} - 2\lambda^2_{оп.1}(T_{д.2v3} + T_у) - \lambda_{кр.оп}}{n_{рэ}}. \quad (4)$$

При различной ФБ каналов резервирования дублированной структуры с нагруженным резервированием общую интенсивность опасных отказов решающих элементов можно определить из формулы для определения минимально допустимого периода диагностирования каждого канала резервирования, приведенной в работе [5]:

$$T_{д.2v2} = \frac{\lambda_{оп.доп} - 2\lambda_{оп.1}\lambda_{оп.2}T_у - \lambda_{кр.оп} - n_{рэ}\lambda_{1.оп.рэ} - n_{рэ}\lambda_{кр.оп.рэ}}{2\lambda_{оп.1}\lambda_{оп.2}}, \quad (5)$$

где $\lambda_{оп.1}$, $\lambda_{оп.2}$ – интенсивность опасных отказов первого и второго каналов резервирования соответственно.

С учетом $\lambda_{оп.рэ} = \lambda_{1.оп.рэ} + \lambda_{кр.оп.рэ}$ получим допустимую интенсивность опасного отказа для решающих элементов дублированной структуры с нагруженным резервированием:

$$\lambda_{оп.рэ2v2} = \frac{\lambda_{оп.доп} - 2\lambda_{оп.1}\lambda_{оп.2}(T_{д.2v3} + T_у) - \lambda_{кр.оп}}{n_{рэ}}. \quad (6)$$

Необходимо отметить, что в вышеуказанных выражениях коэффициенты 6 и 2 при интенсивностях опасных отказов каждого канала резервирования определяются не исходя из усредненного их значения за период контроля (соответственно коэффициенты 3 и 1), как предлагается во многих публикациях по расчету резервированных структур, а за весь период контроля исходя из наихудших условий, так как к концу периода контроля реальная интенсивность опасных отказов всей структуры будет в 2 раза больше, чем при усредненном значении общей интенсивности опасных отказов резервированной системы за период контроля, что дает недопустимую погрешность в расчетах безопасности.

2 **Определение допустимых значений функциональной безопасности кратных отказов каналов резервирования СЖА.**

Допустимые значения интенсивностей кратных опасных отказов каналов резервирования для СЖА с мажоритарным резервированием «2» из «3» и двухканальной дублированной структуры «2» из «2» также можно определить из выражений (3) и (4):

$$\lambda_{кр.оп2v3} = \lambda_{оп.доп} - 6\lambda^2_{оп.1}(T_{д.2v3} + T_у) - \lambda_{оп.рэ2v3}; \quad (7)$$

$$\lambda_{кр.оп2v2} = \lambda_{оп.доп} - 2\lambda^2_{оп.1}(T_{д.2v3} + T_у) - \lambda_{оп.рэ2v2}. \quad (8)$$

При наличии $n$ – числа возможных кратных опасных отказов в резервированной СЖА – допустимые (максимальные) значения их интенсивностей опасных отказов будут рассчитаны следующим образом:

$$\lambda_{кр.оп2v3} = \frac{\lambda_{оп.доп} - 6\lambda^2_{оп.1}(T_{д.2v3} + T_у) - \lambda_{оп.рэ2v3}}{n_{кр.оп}}; \quad (9)$$

$$\lambda_{кр.оп2v2} = \frac{\lambda_{оп.доп} - 2\lambda^2_{оп.1}(T_{д.2v3} + T_у) - \lambda_{оп.рэ2v2}}{n_{кр.оп}}. \quad (10)$$

3 **Определение допустимых значений функциональной безопасности отдельных каналов резервирования.**

Минимально допустимые наработки до опасного отказа одного канала резервирования мажоритарной структуры «2» из «3» и двухканальной дублированной структуры «2» из «2» с безопасным решающим элементом «И» предлагается определять, с учетом работ [5–7] и формул (1), (2) по следующим выражениям:

$$T_{оп.1.2v3} = \sqrt{\frac{6(T_д + T_у)}{\lambda_{оп.доп} - \lambda_{кр.оп} - n\lambda_{1.оп.рэ} - n\lambda_{кр.оп.рэ}}}; \quad (11)$$

$$T_{оп.1.2v2} = \sqrt{\frac{2(T_д + T_у)}{\lambda_{оп.доп} - \lambda_{кр.оп} - n\lambda_{1.оп.рэ} - n\lambda_{кр.оп.рэ}}}. \quad (12)$$

При различной ФБ каналов резервирования дублированной структуры, с учетом максимально допустимых фиксированных значений $T_д$, $T_у$ и $\lambda_{оп1.max}$ = const, $\lambda_{оп2.max}$ = = const, минимально допустимая наработка до опасного отказа каждого из каналов резервирования системы определяется следующим образом:

$$T_{оп.1.min} = \frac{2\lambda_{оп.2}(T_д + T_у)}{\lambda_{оп.доп} - \lambda_{кр.оп} - n\lambda_{1.оп.рэ} - n\lambda_{кр.оп.рэ}}; \quad (13)$$

$$T_{оп.2.min} = \frac{2\lambda_{оп.1}(T_д + T_у)}{\lambda_{оп.доп} - \lambda_{кр.оп} - n\lambda_{1.оп.рэ} - n\lambda_{кр.оп.рэ}}. \quad (14)$$

При отсутствии кратных опасных отказов и опасных отказов решающих элементов минимально допустимые наработки до опасного отказа одного канала резервирования мажоритарной структуры «2» из «3» и двухканальной дублированной структуры «2» из «2» с безопасным решающим элементом «И» будут определяться с учетом работ [5–7] по следующим выражениям:

$$T_{оп.1.2v3} = \sqrt{\frac{6(T_д + T_у)}{\lambda_{оп.доп}}}; \quad (15)$$

$$T_{оп.1.2v2} = \sqrt{\frac{2(T_д + T_у)}{\lambda_{оп.доп}}}, \quad (16)$$

Расчет по формулам (15), (16) производится без необходимости определения интенсивности опасных отказов элементов, поэтому при отсутствии кратных опасных отказов и опасных отказов решающих элементов имеет максимальную достоверность.

В случае появления опасного отказа в канале резервирования ранее расчетного значения по формулам (13)–(16) принимается решение о просчетах ФБ на этапах допуска СЖА в эксплуатацию и принимаются экстренные меры по устранению таких просчетов.

Контроль по допустимой наработке до опасного отказа каждого канала резервирования имеет большое значение, так как на каждом этапе доказательства безопасности имеется относительно высокая вероятность получения неверных выводов о реальной ФБ в процессе будущей их эксплуатации, например, по следующим причинам [5]:

– исходные данные для расчета ФБ не всегда имеют требуемую точность;

– стендовые испытания не позволяют провести все необходимые процедуры доказательства безопасности с достаточной достоверностью. Так, например, для крупных станций воспроизвести все технические и программные средства МПЦ на стенде в полном объеме практически невозможно;

– имитационные испытания путем моделирования на компьютере позволяют произвести проверку работоспособности и безопасности как отдельных каналов резервирования, так и их сочетаний, вплоть до проверки системы в целом, но при этом они не позволяют учитывать аппаратные особенности многих устройств и влияние всех дестабилизирующих факторов, а также имеют недостатки, присущие многим имитационным моделям;

– испытания в условиях эксплуатации при малой выборке испытуемых объектов и недостаточного времени испытаний не позволяют получить приемлемые уровни доверительной вероятности по полученным статистическим данным о реальной безопасности систем;

– экспертные оценки даже при высокой квалификации экспертов не могут дать полной информации о достаточности ФБ систем из-за сложности ее доказательства, в том числе и по вышеуказанным причинам.

**4 Определение допустимых значений максимального времени устранения опасных отказов в каждом канале резервирования**

На базе выражений (1) и (2) можно также определить требования по максимальному времени устранения опасных отказов в каждом канале резервирования мажоритарной структуры «2» из «3» и двухканальной дублированной структуры «2» из «2» для обеспечения заданных требований ФБ по допустимой интенсивности опасных отказов СЖА:

$$T_{у2\text{з}3} = \frac{\lambda_{оп.доп} - 6\lambda^2_{оп.1} T_{д2\text{з}3} - \lambda_{кр.оп} - n_{ро}\lambda_{1.оп.ро} - n_{ро}\lambda_{кр.оп.ро}}{6\lambda^2_{оп.1}}; \quad (17)$$

$$T_{у2\text{з}2} = \frac{\lambda_{оп.доп} - 3\lambda^2_{оп.1} T_{д2\text{з}3} - \lambda_{кр.оп} - n_{ро}\lambda_{1.оп.ро} - n_{ро}\lambda_{кр.оп.ро}}{6\lambda^2_{оп.1}}. \quad (18)$$

**Заключение**

Разработанные требования функциональной безопасности для устройств железнодорожной автоматики позволяют снизить риск появления опасных отказов и связанных с ними катастроф и аварий. Полученные результаты могут быть полезными не только для применения в сфере железнодорожного транспорта, но и для разработчиков в различных областях создания и эксплуатации систем, связанных с безопасностью (в авиации, космической технике, атомной и химической промышленности, медицине, системах военного назначения).

**Список литературы**


1 МГС ГОСТ 33894–2016. Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля – М. : Стандартинформ, 2019.

2 МГС ГОСТ 33895–2016. Системы железнодорожной автоматики и телемеханики на перегонах железнодорожных линий. Требования безопасности и методы контроля. – М. : Стандартинформ, 2019.

3 CENELEC – EN 50129. Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. – 2018. – 154 p.

4 ДСТУ 4178–2003. Комплексы техничных средств систем управления и регулирования движения поездов. Функциональная безопасность и надежность. Требования и методы испытаний. – Киев : Держспоживстандарт Украины, 2003.

5 **Кустов, В. Ф.** Особенности обеспечения функциональной безопасности микропроцессорных систем управления и контроля на железнодорожном транспорте / В. Ф. Кустов // Железнодорожный транспорт Украины. – 2015. – № 1. – С. 2–30.

6 **Кустов, В. Ф.** Математические модели функциональной безопасности микропроцессорных систем железнодорожной автоматики // Сб. науч. трудов УкрГАЖТ / В. Ф. Кустов. – Вып. № 116. – Харьков : УкрГАЖТ, 2010. – С. 65–71.

7 Ensuring railroad's digital automation systems resistance to dangerous states / S. Panchenko [et al.] // ICTE in Transportation and Logistics. ICTE Tol 2019, LNITI, 2020. – P. 120–128.


Получено 15.09.2020

**V. F. Kustov.** Development of functionalsafety requirements for devices of railway automation.

The article discusses the development of functional safety requirements for the decisive elements of redundancy channels, multiple dangerous failures of redundant railway automation systems, as well as determining the permissible operating time before a dangerous failure of each redundancy channel, the maximum permissible time for eliminating dangerous failures in the redundancy channels to achieve a given level.