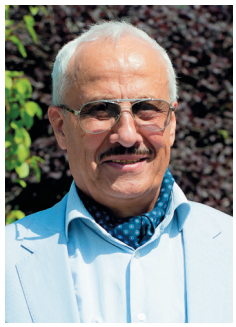
Оригинальная статья
https://doi.org/10.21683/1729-2646-2021-21-1-38-44

О функциональной безопасности сложной технической системы управления с цифровыми двойниками

Игорь Б. Шубинский[1]*, Хендрик Шебе[2], Ефим Н. Розенберг[1]
[1]*АО «НИИАС», Москва, Российская Федерация*
[2]*T V Rheinland, Кельн, Германия*
**igor-shubinsky@yandex.ru*



Игорь Б. Шубинский

Хендрик Шебе

Ефим Н. Розенберг

Резюме. Цель *данной статьи заключается в оценке преимуществ применения технологии цифровых двойников по сравнению со стандартными подходами построения безопасной двухканальной системы.* **Методы.** *Система описывается с помощью Марковской модели. Эта модель позволяет определить количественные характеристики безопасности при наличии в системе защитных отказов.* **Результаты.** *Выведены основные количественные показатели безопасности системы как среднее время до опасного отказа и среднее время до защитного отказа, а также количественные соотношения основных и дополнительных затрат для партии продукции.* **Заключение.** *Преобразование исходного объекта в систему с цифровыми двойниками позволяет значительно снизить интенсивность опасных отказов. Данный эффект может быть получен не только с помощью технологии цифровых двойников, но и вследствие переводов системы в состояния защитных отказов при каждом событии несовпадения результатов работы исходного объекта и/или цифровых двойников. Установлено, что среднее время до защитного отказа системы при этих условиях не меньше среднего времени до отказа исходного объекта. Это означает, что при достижении высокой эффективности повышения безопасности есть возможность сохранить надежность системы на уровне не ниже уровня надежности исходного объекта. Введение в состав системы цифровых двойников – это новый, еще не апробированный подход к обеспечению безопасности системы. Решение о целесообразности дополнительных затрат принимают совместно заказчик и разработчик системы. При этом надо учитывать, что при большой партии изготавливаемых технических систем нивелируется влияние дополнительных затрат и сохраняется эффект значительного повышения безопасности систем.*

Ключевые слова: *цифровой двойник, функциональная безопасность, система управления*

Формат цитирования: *Шубинский И.Б., Шебе Х., Розенберг Е.Н. О функциональной безопасности сложной технической системы управления с цифровыми двойниками // Надежность. 2021. №1. С. 38-44. https://doi.org/10.21683/1729-2646-2021-21-1-38-44*

Поступила *07.10.2020 г.* / **После доработки** *04.02.2021 г.* / **К печати** *22.03.2021 г.*

1. Введение

Рассматривается система управления, которая должна работать с высоким уровнем функциональной безопасности. Возможные решения по построению системы управления приведены в стандарте IEC 61508 [1]. Применительно к системам управления и/или обеспечения безопасности движения на железнодорожном транспорте, многие рекомендации по функциональной безопасности аппаратуры и программ приведены в стандартах EN 50128 [2], EN 50129 [3], а также в работах [4–10 и др.]. Ключевые решения состоят в применении многоканальности аппаратуры и многоверсионности программ, что приводит, естественно, к существенному удорожанию системы и нередко ограничивает возможности ее многосерийного изготовления. Нельзя не отметить определенные сложности при модернизации и модификации такой системы вследствие необходимости перепроектирования ее избыточных средств под изменившиеся потребности. Они возникает на железнодорожном транспорте в связи с перепрофилированием данной системы на другой объект подвижного состава, изменением грузонапряженности пути, изменением класса железнодорожной линии и др.

В настоящее время актуальна задача построения дешевых в серийном производстве систем управления и обеспечения безопасности движения, которые при этом соответствуют повышенным требованиям функциональной безопасности. В данной статье изучается возможность создания системы управления и/или обеспечения безопасности движения в составе исходного объекта уровня полноты безопасности УПБ1 или УПБ2 и внешнего контура цифровых двойников, предназначенного для достижения желаемого уровня функциональной безопасности.

Под цифровым двойником понимается изделие, содержащее:

- математическую модель исходного объекта;
- программную реализацию модели, которая реализует все рабочие функции исходного объекта;
- результаты верификации модели и доказательства ее адекватности исходной системе, а также перечень опасных и потенциально опасных состояний с определением допустимой длительности опасных отказов исходного объекта;
- эксплуатационную документацию.

В целом цифровой двойник можно представить как сложное средство диагностики.

2. Архитектура технической системы с цифровым двойником

Архитектура цифрового двойника приведена на рис. 1. Она чем-то схожа с архитектурой сложной технологической управляемой системы, предложенной в работе [11], но не повторяет ее.

Цифровой двойник формируется в виде компьютерной модели, состоящей из трех взаимосвязанных уровней:

- *объектный*, содержащий в себе компьютерную модель технических средств системы управления, участвующих в реализации алгоритма функционирования системы, с подключенными к ней моделями исполнительных и измерительных устройств;
- *логический*, который содержит имитационную модель алгоритма функционирования системы управления и/или обеспечения безопасности движения;
- *визуальный*, на котором осуществляется визуализация данных, а также формирование задающих воздействий, представляющих собой команды пользовательского управления.

Обеспечение адекватности виртуальной модели реальному объекту на железнодорожном транспорте является ключевым элементом построения системы обеспечения безопасности движения [12]. Рассмотрим в качестве объекта систему железнодорожной автоматики и телемеханики. Системы автоматической блокировки

Рис. 1. Архитектура цифрового двойника

и электрической (микропроцессорной) централизации на станции содержат датчики информации о параметрах работы рельсовых цепей (уровень напряжения на входах приемников). Описание работы этих датчиков является самостоятельной сложной задачей, поскольку выбирается оптимум из режимов контроля наличия поездов на участке, контроля излома рельсов, уровня сигналов для локомотивной сигнализации. Вместе с тем, данные процессы хорошо изучены и сведены к типовым нормам, обеспечивающим безопасность движения. Соответственно для моделирования в виртуальной модели их математическое описание может быть использовано для предиктивной диагностики событий непрерывного процесса их функционирования. Для следующего уровня виртуальной модели, представляющей дискретно-событийную работу моделируемого объекта, достаточно иметь только значение выхода процесса за нормы работоспособности и безопасности.

Дискретно-событийная работа в виртуальной модели хорошо представляется дискретным автоматом, для которого также разработаны критерии обеспечения безопасности, основанные на монотонности функций управления. Аналогично может быть построена виртуальная модель работы отдельных систем на подвижном составе. Так, работа тормозной магистрали поезда в режиме торможения сводится к открытию клапанов, что приводит к потере давления в магистрали и срабатыванию тормозов в поезде. Сам процесс описывается сложными дифференциальными уравнениями распространения потока воздуха по всей длине поезда. Для оценки последствий в части обеспечения безопасности достаточно иметь критерии снижения давления в хвостовом вагоне за заданное время. Учитывая, что сам режим торможения может разделяться на виды служебного, полного служебного и экстренного торможения, в виртуальной модели необходимо сформировать их варианты. Следует заметить, что само механическое воздействие тормозных колодок на колеса из-за разрядки тормозной магистрали можно описать предельными временными характеристиками, влияющими на длину тормозного пути.

Для следующего уровня виртуальной модели – уровня описания работы прибора безопасности, достаточно иметь временные отметки начала открытия клапана торможения и завершения снижения скорости поезда или его остановки.

Таким образом, в виртуальной модели цифрового двойника совмещены упрощенные непрерывные математические модели непрерывных процессов в преобразовании информации и связанные с ними дискретно-событийные модели.

Внешний контур рассматриваемой системы управления и/или обеспечения безопасности движения формируется с помощью двух однотипных цифровых двойников по двухканальной схеме с независимыми входами и выходами каналов и безопасным компаратором. Способы построения двухканальной схемы для обеспечения функциональной безопасности описаны в указанных выше стандартах.

Внешний контур связан с исходной одноканальным объектом каналом связи, защищенным от помех и от несанкционированного доступа (рис. 2):

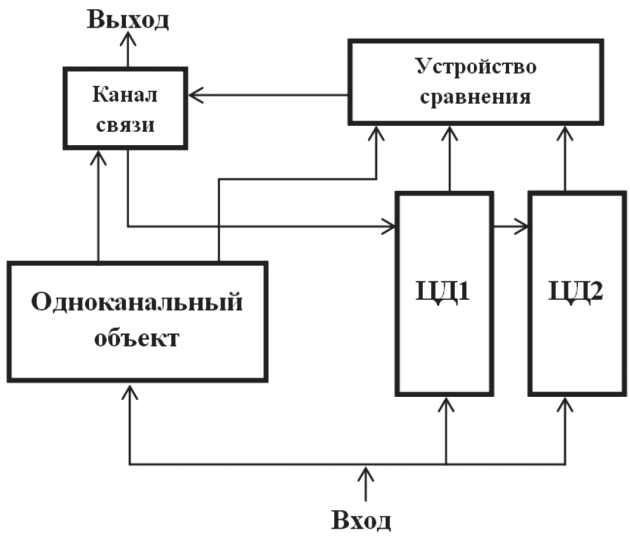


Рис. 2. Укрупненная структурная схема технической системы с цифровым двойником

3. Оценка эффективности ответственной технической системы с цифровым двойником

Система, схема которой приведена на рис. 2, относится к категории ответственной технической системы (например, системы управления и/или обеспечения безопасности движения), к которой предъявляются повышенные требования по функциональной безопасности. Введение цифровых двойников в состав ответственной технической системы вызывает опасения и требует углубленного обоснования безопасности этой системы. В IEC 61508 [1] рекомендован базовый показатель функциональной безопасности объекта – интенсивность опасного отказа λ. Тогда в качестве показателя эффективности системы с цифровым двойником можно рассматривать отношение интенсивности опасного отказа исходной системы λ_O – одноканального объекта (рис. 2) к вероятности опасного отказа системы с цифровым двойником λ_C. Чем больше это отношение, тем эффективнее применение технологии цифровых двойников в ответственных системах.

Для фиксированных интервалов времени показатель эффективности применения технологии цифровых двойников имеет следующий вид: $Э = \lambda_O / \lambda_C$.

Для определения интенсивности опасного отказа системы в целом λ_C приняты *следующие предпосылки:*

- система управления и/или обеспечения безопасности движения работает при высокой интенсивности запросов;

- надежность одноканального объекта определяется интенсивностью отказа λ_1;

- исходный объект контролируется с вероятностью правильного обнаружения отказа α. Цифровой двойник

также контролируется с вероятностью α. Вероятность пропуска отказа $\bar{\alpha}$. Средства контроля идеально надежны. Вероятность ложной тревоги пренебрежимо мала;

- адекватность цифрового двойника исходному объекту оценивается по результатам его верификации. Предполагается, что оба цифровых двойника адекватно имитируют работу исходного объекта. Соответствующий уровень полноты безопасности должен обеспечиваться с помощью стандартов IEC 61508 [1], часть 3, или EN 50128 [2].

- надежность цифрового двойника определяется систематическими отказами его программного средства. Отказы проявляются при определенных наборах входных данных. Предполагается, что эти наборы разнообразны и случайны. Отсюда следует возможность оценивать надежность цифрового двойника интенсивностью отказа λ_2. Предполагается также, что надежность цифрового двойника гораздо выше надежности исходного объекта, т.е. $\lambda_2 << \lambda_1$.

- в случае обнаруженного отказа объекта передается команда на замену его путем подключения двух цифровых двойников. При этом принято, что правильная и своевременная передача команды осуществляется с вероятностью ν;

- устройство сравнения и узел связи в защищенном исполнении идеально надежны (если это предположение не обеспечено, то возможно включить в интенсивности отказов λ_1 и λ_2 соответствующие доли, вызванные устройством сравнения);

- приняты показательные распределения отказов и восстановлений объекта. Это обусловлено тем, что в системах управления и/или обеспечения безопасности движения в подавляющем большинстве содержится электрическое/электронное оборудование;

- случайные события отказов объекта и цифровых двойников взаимно независимы;

- интенсивности устранения отказа объекта и систематического отказа цифрового двойника равны μ, поскольку осуществляются одной ремонтной бригадой.

- интенсивности устранения опасных отказов γ определяются длительностью существования скрытых (необнаруженных средствами контроля) отказов;

- предполагается, что времена восстановления системы распределены по показательному закону (это – общепринятое предположение в таких системах; однако даже если функция распределения времени восстановления отличается от экспоненциальной, это мало влияет на стационарные характеристики системы, см., например, книгу Гнеденко и Коваленко [13]).

Рассмотрим модель возможной организации обеспечения безопасности системы.

Критерии защитного отказа системы с цифровыми двойниками:

1. Не совпали результаты работы исходного объекта и цифровых двойников; причины – необнаруженный отказ исходного объекта или одного из цифровых двойников. Восстанавление системы.

2. Отказал один из цифровых двойников. Восстанавление системы.

Критерий опасного отказа системы с цифровым двойником:

Отказ объекта и ошибка в передаче команды на подключение цифровых двойников или отказ исходного объекта и цифровых двойников.

Граф состояний безопасности технической системы с цифровыми двойниками (см. рис. 2) согласно модели 1 показан на рис. 3.

Описание остояний:

1 – исправное состояние системы;

2 – обнаруженный отказ объекта;

3 – не совпали результаты работы объекта и его цифровых двойников вследствие не выявленного отказа объекта. Причина не совпадения результатов неизвестна. Система переводится в состояние *защитного отказа.* Производится восстановление системы;

4 – неправильная или несвоевременная передача команды управления на подключение цифровых двойников при правильно обнаруженном отказе объекта – *опасный отказ.* Отказ устраняется после обнаружения скрытого отказа;

5 – обнаружен отказ одного из двух цифровых двойников. Система переводится в состояние *защитного отказа.* Производится восстановление системы.

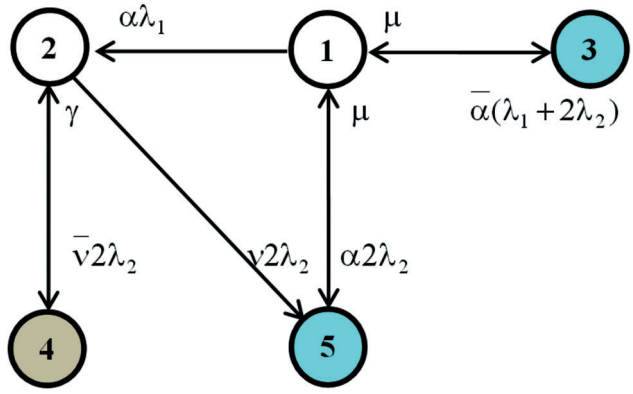


Рис. 3. Граф состояний безопасности системы с цифровыми двойниками

Дуги графа на рис. 3 помечены следующими параметрами: **1-2**: $\alpha\lambda_1$ – обнаруживаемый поток отказов исходного объекта; **1-3:** $\bar{\alpha}(\lambda_1+2\lambda_2)$ – не обнаруживаемый поток отказов объекта или цифровых двойников ; **1-5**: $\alpha 2\lambda_2$ – обнаруживаемый поток отказов цифровых двойников; **4-2:** γ – интенсивность существования скрытого опасного отказа; **2-4:** $\bar{\nu}2\lambda_2$ – разреженный с вероятностью не подключения $\bar{\nu}$ поток отказов цифровых двойников; **2-5:** $\nu 2\lambda_2$ – разреженный с вероятностью подключения ν поток отказов цифровых двойников; **3-1, 5-4:** μ – интенсивность восстановления системы.

Модель функциональной безопасности рассматриваемой системы на рис. 3 предусматривает следующую логику ее функционирования. Начальное состояние 1 – все элементы исправны. В случае обнаруженного отказа или сбоя в работе объекта происходит переход в состояние 2 и передается команда на замену его цифровыми двойниками на период времени, не влияющий на возникновение

опасных управляющих воздействий. При опасном или потенциально опасном отказе производится блокирование выходных сигналов объекта, как это показано в патенте [12]. Если отказал исходный объект и результаты работы цифровых двойников не совпадают, то система переводится в состояние защитного отказа 3. Если обнаружен отказ любого одного цифрового двойника, то при исправном объекте происходит переход системы из состояния 1 в состояние 5 защитного отказа. При отказавшем объекте при отказе любого одного цифрового двойника происходит переход из состояния 2 в состояние 4 опасного отказа (если произошла ошибка при подключении цифровых двойников) или в состояние 5 в случае безошибочного подключения цифровых двойников.

При принятых экспоненциальных законах распределений и, следовательно, постоянных интенсивностях отказов и восстановлений, в исследуемой системе отсутствует последействие. Это означает, что поведение системы в будущем зависит от настоящего и не зависит от предыдущих ее состояний. При указанных предпосылках поведение системы описывается с помощью Марковского случайного процесса.

Для решения задачи предварительно определяют исходные данные:

- функции распределения времени пребывания системы в состояниях графа рис. 3

$$F_1(t)=1-\exp[-(\lambda_1+2\lambda_2)t];\ F_2(t)=1-\exp(-2\lambda_2 t);$$

$$F_4(t)=1-\exp(-\gamma\cdot t);\ F_3(t)=F_5(t)=1-\exp(-\mu\cdot t);$$

- математические ожидания времени пребывания системы в состояниях графа рис. 3 по формуле:

$$T_i=\int_0^\infty[1-F_i(t)]dt;\ T_i=\frac{1}{\lambda_1+2\lambda_2};\ T_2=\frac{1}{2\lambda_2};$$

$$T_4=\frac{1}{\gamma};\ T_3=T_5=\frac{1}{\mu};\qquad(1)$$

- вероятности переходов по формуле: $p_{ij}=\int_0^\infty\lambda_{ij}[1-F_i(t)]dt$, где λ_{ij} – интенсивность перехода системы из состояния i в состояние j:

$$p_{12}=\frac{\alpha\lambda_1}{\lambda_1+2\lambda_2};\ p_{13}=\frac{\overline{\alpha}(\lambda_1+2\lambda_2)}{\lambda_1+2\lambda_2};\ p_{15}=\frac{\alpha\cdot 2\lambda_2}{\lambda_1+2\lambda_2};$$

$$p_{24}=\overline{\nu};\ p_{25}=\nu;\ p_{31}=p_{42}=p_{51}=1;\qquad(2)$$

Ключевой показатель безопасности – среднюю наработку до опасного отказа $T_{\text{ОП}}$ системы можно определить с помощью топологического метода [14] по формуле

$$T_{\text{ОП}}=\frac{T_1\Delta G^1_{S_{\text{оп}}}+\sum_{(k)}\sum_{i,j}l^{ij}_k\Delta G^j_k T_j}{\Delta G_{S_{\text{оп}}}},\qquad(3)$$

где $\Delta G^1_{S_{\text{оп}}}$ – вес разложения графа без начальной вершины 1 и множества опасных состояний $S_{\text{ОП}}=\{4\}$ и связанных с ними дуг графа; $\Delta G_{S_{\text{оп}}}$ – вес разложения графа без множества опасных состояний и связанных с ними дуг графа; l^{ij}_k – вес k-го пути из вершины i в вершину j; ΔG^j_k – вес разложения графа без вершин расположенных на k-ом пути и без вершины j в множестве неопасных состояний $S_{\text{Н}}=\{1,2,3,5\}$.

Веса разложений можно определить с помощью формулы Мейсона [15]

$$\Delta G=1-\sum_i C_i+\sum_{ij}C_iC_j-\sum_{ijk}C_iC_jC_k+...,$$

где веса контуров находят в множестве неопасных состояний (рис. 3):

$$C_1=p_{13}\cdot p_{31}=\frac{\overline{\alpha}(\lambda_1+2\lambda_2)}{\lambda_1+2\lambda_2};\ C_2=p_{15}\cdot p_{51}=\frac{2\lambda_2}{\lambda_1+2\lambda_2};$$

$$C_3=p_{12}\cdot p_{25}=\frac{\alpha\nu\lambda_1}{\lambda_1+2\lambda_2}.$$

Все контуры пересекающиеся, т.к. имеют общую вершину1.

Веса разложений графа рис. 3

$$\Delta G^1_{S_{\text{оп}}}=1;$$

$$\Delta G_{S_{\text{оп}}}=1-C_1-C_2-C_3=1-\frac{\overline{\alpha}(\lambda_1+2\lambda_2)+2\lambda_2+\alpha\nu\lambda_1}{\lambda_1+2\lambda_2}.(4)$$

Руководствуясь графом на рис. 3 и подставляя выражения (1), (2), (4) в формулу (3), находим в множестве неопасных состояний (1, 2, 5)

$$T_{\text{ОП}}=\frac{T_1+p_{12}T_2+p_{13}T_3+(p_{15}+p_{12}p_{25})\cdot T_5}{1-C_1}=$$

$$=\frac{\mu(\alpha\lambda_1+2\lambda_2)+\overline{\alpha}2\lambda_2(\lambda_1+2\lambda_2)}{2\lambda_2\mu\cdot[\alpha(\lambda_1+2\lambda_2)-\alpha(\lambda_1\nu+2\lambda_2)]}.\qquad(5)$$

Учитывая, что интенсивность отказов цифрового двойника λ_2 на 2-3 порядка меньше интенсивности отказов λ_1 исходного объекта и $\mu >> 2\lambda_2\lambda_1$, то выражение (5) с погрешностью, не превышающей одного порядка малости, может быть преобразовано к виду:

$$T_{\text{ОП}}\approx\frac{1}{2\lambda_2\overline{\nu}}.$$

Так как поток опасных отказов системы многократно разрежен относительно потока неопасных отказов исходного объекта, который является простейшим, то согласно работам [16, 17, 18] многократно разреженный случайным образом простейший поток отказов также является простейшим с постоянным параметром

$$\lambda_{\text{С}}=1/T_{\text{ОП}}=2\lambda_2\overline{\nu}.$$

Примечание. Для обеспечения важного предположения, а именно «интенсивность отказов цифрового двойника на 2-3 порядка меньше интенсивности отказов исходного объекта», важно, что программное обеспечение было создано с помощью методов, соответствующих более высоким уровням полноты безопасности, в частности на 2-3 уровня полноты безопасности выше.

Альтернативно, интенсивность отказов должна быть доказана статистическим путем [19].

При обеспечении требований стандарта EN 50159 [20] к безопасности канала связи вероятность своевременной и безошибочной передачи команды подключения цифровых двойников стремится к единице. Поэтому можно добиться близкой к 0 вероятности $\bar{\nu}$ ошибочной передачи команды управления цифровыми двойниками. Следовательно, путем применения цифровых двойников безопасность исходного объекта по показателю интенсивности опасных отказов может быть повышена на несколько порядков. Действительно, рассмотрим отношение интенсивностей опасных отказов исходного объекта ($\lambda_O = \lambda_1$) к интенсивности опасных отказов системы: $Э = \frac{\lambda_O}{\lambda_C} = \frac{\lambda_1}{2\lambda_2\bar{\nu}}$. Поскольку $\lambda_1 >> \lambda_2$ и $\bar{\nu}\to 0$, то наше утверждение справедливо.

Указанный эффект может быть получен не только путем применения технологии цифровых двойников, но и вследствие переводов системы в состояния защитных отказов при каждом событии изменения ее исходной архитектуры. Поэтому целесообразно сопоставить наработку системы до перехода в любое защитное состояние и наработку исходного объекта до отказа.

Определим среднюю наработку системы до защитного отказа. С этой целью в графе состояний рис. 3 нужно выделить состояния 3, 4, 5 (состояния опасного и защитных отказов) вместе с прилегающими к ним дугами. Тогда граф на рис. 3 преобразуется к виду, показанному на рис. 4.

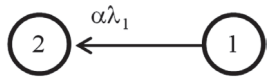


Рис. 4. Граф исследуемой системы без опасного и защитных состояний

Среднее время до защитного отказа находим по формуле (3), где все веса разложений равны 1 вследствие отсутствия контуров на графе рис. 4:

$$T_{ЗАЩ} = T_1 + p_{12}T_2 = \frac{1+\alpha\lambda_1}{\lambda_1 + 2\lambda_2}.$$

Тогда отношение среднего времени до защитного отказа к среднему времени до отказа исходного объекта с учетом соотношения $\lambda_1 >> \lambda_2$ определяется следующим образом

$$\frac{T_{ЗАЩ}}{T_1} \approx \frac{1+\alpha\lambda_1}{\lambda_1}. \qquad (6)$$

Таким образом, среднее время до защитного отказа системы не меньше среднего времени до отказа исходного объекта. Это означает, что в рассматриваемой модели при высокой эффективности в отношении повышения безопасности надежность системы сохраняется на уровне не ниже уровня надежности исходного объекта.

Введение в состав системы цифровых двойников – это новый, еще не апробированный подход к обеспечению безопасности системы. Естественно, он требует обоснования безопасности. Это связано с большими финансовыми затратами. С одной стороны, имеет место большой эффект в повышении функциональной безопасности системы. С другой стороны, возможны большие разовые затраты на создание алгоритма цифрового двойника $C_{АЦД}$ и на обоснование безопасности системы $C_{ОБ}$. С учетом отмеченных обстоятельств, оценим экономическую целесообразность данного подхода.

Пусть стоимость исходного объекта C_1. Стоимость системы с цифровыми двойниками $C_1 + \Delta C_1$. Объем партии выпускаемой продукции – m единиц. Стоимость партии из m систем с цифровыми двойниками составляет $C_{ПАР} = (C_1 + \Delta C_1)m + C_{АЦД} + C_{ОБ}$. Затраты на создание этой системы в совокупности с затратами на обоснование безопасности приемлемы в том случае, если выполняется следующее условие:

$$C_{ПАР} - C_1 m \le C_{ДОП}, \qquad (7)$$

где $C_{ДОП}$ – допустимые финансовые вложения на обеспечение желаемого уровня безопасности. Влияние дополнительных затрат на партию продукции можно оценить с помощью следующего выражения :

$$\frac{C_{ПАР}}{C_1 m} = \frac{(C_1 + \Delta C_1)m + C_{АЦД} + C_{ОБ}}{C_1 m}. \qquad (8)$$

При $m\to\infty$ выражение (8) преобразуется к виду

$$\lim_{m\to\infty} \frac{C_{ПАР}}{C_1 m} = \frac{C_1 + \Delta C_1}{C_1}. \qquad (9)$$

Поскольку затраты ΔC_1 на серийное изготовление цифровых двойников в системе значительно меньше затрат C_1 на изготовление исходного объекта, то выражение (9) стремится к 1. Это означает, что при большой партии изготавливаемых технических систем нивелируется влияние дополнительных затрат.

Решение о целесообразности дополнительных затрат совместно определяют заказчик и разработчик системы, исходя из потребности в обеспечении безопасности этой системы. Вместе с тем, затраты на обеспечение высокого уровня безопасности системы ориентировочно превышают в 10-50 раз стоимость исходного одноканального объекта, тогда как снижение интенсивности опасных отказов системы по сранению с этим показателем исходного объекта может составлять несколько порядков. Это обстоятельство может играть решающую роль в решении о применении технологии цифровых двойников в интересах обеспечения безопасности технической системы.

4. Заключение

Преобразование исходного объекта в систему с цифровыми двойниками позволяет значительно снизить интенсивность опасных отказов. Данный эффект может быть получен не только с помощью технологии цифровых двойников, но и вследствие переводов системы в состояния защитных отказов при каждом событии несовпадения результатов работы исходного объекта и/или цифровых двойников. Установлено, что среднее время

до защитного отказа системы при этих условиях не меньше среднего времени до отказа исходного объекта. Это означает, что при достижении высокой эффективности повышения безопасности есть возможность сохранить надежность системы на уровне не ниже уровня надежности исходного объекта.

Введение в состав системы цифровых двойников – это новый, еще не апробированный подход к обеспечению безопасности системы. Естественно, он требует основательного обоснования безопасности. Это связано с большими дополнительными финансовыми затратами. Решение о целесообразности дополнительных затрат принимают совместно заказчик и разработчик системы. При этом надо учитывать, что при большой партии изготавливаемых технических систем нивелируется влияние дополнительных затрат и сохраняется эффект значительного повышения безопасности систем.

Библиографический список

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

2. EN 50128, Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems, 2011.

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

4. Schabe H. The Safety Philosophy behind CENELEC Rails Standards, Proceedings ESREL 2002,.Lyon, March 19-21, 2002. P. 788-790.

5. Hirao Y. Watanabe I. Safety technologies and management of railway signalling in Japan. Signal + Draht. 2000. №5.

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

7. Shubinsky I.B., Sheabe X. On the definition of functional reliability, Proceedings of the ESREL 2013, Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds) 2014 Taylor & Francis Group, London, ISBN 978-1-138-00123-7. P. 3021-3027.

8. Shubinsky I.B., Sheabe X., Rozenberg E.N. A short study on rebooting safe computers and the impact on safety, ESREL 2009, Proceedings Reliability, Risk and Safety, vol. 1. P. 175-178

9. Braband J. A practical guide to safety analysis methods/ Signal+Draht International. 2001.

10. Gulker J., Schabe H. Physical Principles of Safety. In ESREL 2006 ProceedingsSafety Reliability and Risk analysis, vol. 2. Rotterdam: Balkema, 2006. P. 1045–1050.

11. Дмитриев В.М., Ганджа Т.В., Зайченко Т.Н. Методика стратификации и интеграции компьютерной модели сложной технической управляемой системы // Информатика и системы управления. 2016. № 4(50).

12. Батраев В.В, Кудряшов С.В., Попов П.А., Розенберг Е.Н., Розенберг И.Н., Шухина Е.Е., Шубинский И.Б. Двухканальная система для регулирования движения железнодорожных транспортных средств. Патент РФ № 2726243. 2020. Бюл. № 19.

13. Гнеденко Б.В., Коваленко Б.В. Введение в теорию массового обслуживания, М.: Наука, 1987.

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

15. Mason Samuel J. Feedback Theory – Further Properties of Signal Flow Graphs // Proceedings of the IRE. 1956. Vol. 44. No. 7. P. 920–926. doi:10.1109/jrproc.1956.275147

16. Григелионис Б.И. О точности приближения композиции процессов восстановления пуассоновским процессом // Литов. матем. сб. 1962. Т. 2. № 2. С. 135-143.

17. Погожев И.Б. Оценка отклонения потока отказов в аппаратуре многофазового использования от пуассоновского потока // Кибернетику – на службу коммунизму, Т. 2. М.: Энергия, 1964. С. 228-245

18. Назаров А.А., Лапатин И.Л. Ассимптотические пуассоновские MAP-потоки // Известия Томского государственного университета. (Управление, вычислительная техника и информатика). 2010. № 4(13). С. 72-78.

19. Braband, J. Gall, H., Schäbe, H., Proven in Use for Software: Assigning an SIL Based on Statistics in: Handbook of RAMS in Railway systems – Theory and Practice, Qamar Mahboob, Enrico Zio (Eds.), 2018, Boca Raton, Taylor and Francis, Chapter 19. P. 337-350.

20. EN 50159 Railway applications Communication, signaling and processing systems Safety-related communication in transmission systems, 2010.

Сведения об авторах

Игорь Борисович Шубинский – доктор технических наук, профессор, заместитель руководителя НТК АО «НИИАС». Адрес: ул.Нижегородская, д. 27, стр.1, Москва, Российская Федерация, 109029, тел. +7 (495) 786-68-57; e-mail: igor-shubinsky@yandex.ru

Хендрик Шебе – доктор физико-математических наук, заведующий отделом анализа рисков и опасностей, TÜV Rheinland InterTraffic, Кельн, Германия; e-mail: schaebe@de.tuv.com

Ефим Наумович Розенберг – профессор, доктор технических наук, первый заместитель Генерального директора АО «НИИАС». Адрес: ул. Нижегородская, д. 27, стр.1, Москва, Российская Федерация, 109029; e-mail: info@vniias.ru

Вклад авторов в статью

Шубинским И.Б. выполнена разработка математической модели, проведен анализ результатов исследования.

Шебе Х. разработан граф состояний системы, определены ограничения предложенной модели.

Розенбергом Е.Н. выполнена постановка задачи исследования.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.