Автоматизированное вождение поездов – валидация анализа рисков

Automated train driving: risk analysis validation

Хендрик Шебе
Hendrik Schabe
TUV Rheinland, Кельн, Германия
TUV Rheinland, Cologne, Germany
dr.hendrik.schaebe@gmail.com

Хендрик Шебе

Резюме. Цель. *Статья посвящена описанию валидации анализа рисков в рамках исследовательского проекта по автоматизированному ведению поезда.* **Методы.** *Валидация проводилась с использованием нескольких различных методов. Полученные результаты сопоставлялись с результатами, полученными из других источников. Кроме того, был проведен независимый анализ рисков с использованием альтернативного метода MEM (минимальная эндогенная смертность).* **Результаты.** *Валидация показала, что результаты, полученные в рамках проекта, являются достоверными. Подтвержден уровень полноты безопасности (SIL) 1 или 2 для систем, заменяющих машиниста поезда.* **Выводы**. *Показано, что для валидации результатов анализа рисков целесообразно использовать различные методы. При этом необходимо учитывать, что будут получены сопоставимые, но не идентичные результаты.*

Abstract. Aim. *The paper is dedicated to describing the validation of risk analysis as part of an automated train control research project.* **Methods.** *Validation was performed using several different methods. The obtained results were compared with those obtained from other sources. Additionally, an independent risk analysis was performed using the alternative MEM (minimum endogenous mortality) method.* **Results.** *The validation showed that the project's findings are reliable. Safety Integrity Levels (SIL) 1 or 2 were confirmed for train driver substitution systems.* **Conclusions.** *It was shown that various methods should be used for the purpose of risk analysis validation. It must be taken into account that comparable, but not identical results will be obtained.*

Ключевые слова: *анализ рисков, валидация, автоматизированное вождение.*
Keywords: *risk analysis, validation, automatic driving.*

Для цитирования: *Шебе Х. Автоматизированное вождение поездов – валидация анализа рисков // Надежность. 2024. №1. С. 65-72. https://doi.org/10.21683/1729-2646-2024-24-1-65-72*
For citation: *Schabe H. Automated train driving: risk analysis validation. Dependability 2024;1:65-72. https://doi.org/10.21683/1729-2646-2024-24-1-65-72*

Поступила: *18.08.2023* / **После доработки:** *30.01.2024* / **К печати:** *15.03.2024*
Received on: *18.08.2023* / **Revised on:** *30.01.2024* / **For printing:** *15.03.2024*

1. Введение

Данная статья посвящена валидации анализа рисков для проектов автоматизированного ведения поезда. Как правило, в таких проектах машинист заменяется технической системой. Анализ рисков используется для получения требований к допустимой частоте функциональных отказов (Tolerable Functional Failure Rate, TFFR) и, соответственно, уровню полноты безопасности (Safety Integrity Level, SIL). В данной статье мы сосредоточимся на перекрестной валидации результатов, полученных с помощью различных методов.

В разделе 2 описывается общий подход к валидации. В разделе 3 представлены различные действия по валидации, которые были предприняты. В четвертом разделе сделаны общие выводы.

Многие результаты настоящей работы были получены в рамках проекта ATO-RISK по заказу Немецкого центра исследований железнодорожного транспорта (DZSF). Более подробную информацию можно найти в итоговом отчете [1].

2. Общий подход к валидации

Результаты, относящиеся к валидации, были получены с использованием двух подходов:

а) Для GoA 2 (Grade of automation 2 – степень автоматизации 2) для определения допустимого уровня риска учитывается способность машиниста и предполагается, что впоследствии машинист будет заменен технической системой. Определена вероятность отказа по требованию (PFD).

б) Для GoA 3 / 4 (Grade of automation 3 / 4 – степень автоматизации 3 / 4) рассматривалась непосредственно техническая система, реализующая определенные функции машиниста поезда. Был получен показатель допустимой частоты функциональных отказов TFFR.

Валидация состояла из трех частей:

• сравнение результатов для GoA 2 с данными из других источников и сравнение результатов для GoA 3 / 4 с результатами из других источников;

• перекрестное сравнение результатов обоих подходов с использованием интенсивности требования;

• сравнение результатов со значениями, полученными по третьему, независимому, принципу.

Для GoA 2 использовались две процедуры определения вероятности ошибки: процедуры по Хинчину и RARA, см. [2]. Эти две процедуры были выбраны как наиболее подходящие для определения вероятности ошибки человека. При этом процедура по Хинчину была модифицирована, так как оценка вероятности человеческой ошибки по Хинчину не является консервативной для установления целевых показателей безопасности. RARA является более современным методом, и можно предположить, что полученные этим методом результаты являются более реалистичными [2]. Вероятности человеческих ошибок были получены для нескольких функций. Для последующего сравнения использовался значительно сокращенный набор функций, поскольку для сравнения были необходимы также результаты для GoA 3 / 4.

Типичные события приведены в табл. 1. Для RARA было выбрано значение 50 %, что соответствует среднему значению весовых коэффициентов.

Табл. 1. Основные результаты, полученные для GoA 2 – значения PFD

Функция	Метод RARA с 50-процентным взвешиванием	Метод Хинчина (модифицированный)
Предотвращение столкновения с препятствиями	$8{,}64 \times 10^{-3}$	$1{,}00 \times 10^{-3}$
Обнаружение пониженного значения трения и реакция	$1{,}98 \times 10^{-2}$	$5{,}00 \times 10^{-3}$

Приведенная величина PFD является средней, так как это – величина, усредненная по всем рассматриваемым лицам в сопоставимых ситуациях.

Табл. 2. Соответствующие результаты для GoA 3 / 4 – значения TFFR

Функция	TFFR
Предотвращение столкновения с препятствиями или людьми (здесь требования определяются людьми)	9×10^{-7} 1/ч
Обнаружение пониженного значения трения и реакция	10^{-7} 1/ч

В табл. 2 приведены полученные количественные результаты для ситуации GoA 3 / 4 [3].

3. Действия по валидации

В этом разделе описываются действия по валидации. На первом этапе результаты сравнивались с другими источниками вероятности или частоты человеческих ошибок. На втором этапе была проведена перекрестная валидация результатов, полученных для GoA 2 и GoA 3 / 4. Необходимо отметить следующие аспекты:

• для GoA 2 в качестве эталонной системы рассматривается действующий машинист поезда и его деятельность, в то время как для GoA 3 / 4 применяется явный анализ рисков, выполненный с использованием стандарта. Уже в силу этих различий в процедурах определения критериев приемлемости риска полученные результаты могут быть различны, см., например, [3];

• рассматривая машиниста поезда, необходимо учитывать, что он, как правило, параллельно выполняет множество функций, а заменяющие его технические системы – только одну или несколько. Поэтому интенсивность требования машинисту может отличаться от интенсивности требования заменяющей его технической системе.

• для машиниста поезда определяется вероятность человеческой ошибки в виде вероятности отказа по требованию (PFD). Такое описание человеческих ошибок соответствует уровню техники. Строго говоря, машинист поезда работает непрерывно, выполняя разные функции, так что отдельная функция может выполняться им лишь эпизодически и по требованию. Это создает проблему, если необходимо пересчитать вероятность ошибки (PFD) машиниста поезда в допустимую частоту функциональных отказов (TFFR).

3.1. Сравнение с показателями человеческих ошибок из других источников

Для проверки значений PFD и TFFR, полученных для ситуаций GoA 2 и GoA 3 / 4, были использованы дополнительные источники. Следует отметить, что значения, используемые для перекрестной проверки, являются лишь вторичными по качеству, поскольку в самом проекте были использованы наиболее представительные значения.

3.1.1. PFD для машиниста

Из табл. 3.2 [4, стр. 41] были использованы строки 4 (показания манометра) и 6 (реакция), что дает результат для PFD, равный

$$PFD = \frac{5000 + 1800}{1000000} = 6{,}8 \times 10^{-3}.$$

Это значение PFD находится примерно на том же уровне, что и значения, определенные для GoA 2

(см. табл. 1, где приведены значения от 10^{-3} до 8×10^{-3}). Отметим, что сопоставимость задач GoA 2 и GoA 4 весьма ограничена.

3.1.2. Уровень человеческих ошибок

Вероятности человеческих ошибок Диллон приводит в табл. 3-3 [5, гл. 3.10] (они воспроизведены в табл. 3).

Табл. 3 Вероятности человеческих ошибок по Диллону [5]

Ошибка / Задача	Вероятность ошибки за месяц работы завода	Интенсивность ошибок, 1/ч
Неправильная работа	0,0300	$4{,}167 \times 10^{-5}$
Непонимание / неправильное толкование требований	0,0074	$1{,}028 \times 10^{-5}$
Неправильная настройка	0,0260	$3{,}611 \times 10^{-5}$

Из приведенной выше табл. 3 видно, что уровень человеческих ошибок находится в диапазоне примерно от 10^{-5} 1/ч до 4×10^{-5} 1/ч, т.е. даже выше диапазона SIL 1. Таким образом, если для GOA 3 / 4 (когда техническая система заменяет машиниста поезда) требуется показатель в диапазоне SIL 1 или даже SIL 2, то это значение является консервативным.

3.1.3. Уровень полноты безопасности машиниста по SIRF

В приложении C к [6] приведены допущения по SIL-классификации машиниста: SAS 1, т.е. уровень полноты безопасности SIL 1. SAS не соответствует непосредственно SIL, поскольку последний определен только для технических систем. Однако в табл. 8 [7] SAS для программного обеспечения должен быть переведен в точно соответствующий SIL. Таким образом, если заменить машиниста техническими системами, то эти технические системы должны иметь уровень SIL 1.

3.2. Перекрестная валидация вероятностей человеческих ошибок по отношению к интенсивности отказов технических систем

Для GoA 2 была выведена вероятность PFD, а для GoA 3 / 4 – частота TFFR. При сравнительной оценке принято, что человеческая ошибка соответствует неготовности системы.

PFD – это вероятность возникновения неисправности или даже человеческой ошибки, в каждом случае связанная с требованием. В математическом смысле это условная вероятность, а именно, вероятность отказа при условии возникновения требования. Допустимая частота функциональных отказов (TFFR) – это допустимый коэффициент функциональных отказов технической системы. TFFR имеет смысл интенсивности, поэтому для выведения TFFR не требуется значение интенсивности требования. Обе величины можно сравнивать, поскольку они относятся, с одной стороны, к вероятности отказа машиниста (PFD), а с другой – к интенсивности опасных отказов технической системы (TFFR), которая должна заменить машиниста. Связь между PFD и TFFR может быть установлена следующим образом (см., например, [8]):

$$\text{TFFR} = \text{PFD} \times \text{интенсивность требования}.$$

Существует несколько способов определения указанной интенсивности требования. Они описаны ниже.

3.2.1. Расчет интенсивности требования по статистике BEU

Для выведения интенсивности требования используется так называемая статистика BEU [9]. Она показывает следующие результаты за период 4,5 года (с 01.01.2017) – табл. 4.

Табл. 4. Результаты статистики BEU

Тип события	Подтип события	Количество соответствующих событий
Коллизия	Столкновение с неподвижным транспортным средством	5
	Столкновение с объектом, движущимся в том же направлении	1
	Столкновение с объектом в калибровочном профиле	4
	Коллизия с другими стационарными объектами	21
	Взаимодействие с животными	5
Личный несчастный случай	Столкновение с движущимся железнодорожным составом	353
Всего		389

Суммарное количество аварий соответствует интенсивности 389 / 4,5 = 86,4 аварий/год. При среднем количестве 22900,5 пассажирских и 2650,5 грузовых поездов в сутки (среднее значение для 2019 и 2020 годов [10]) и принятии средней продолжительности поездки пассажирского поезда 2 ч, а грузового – 5 ч, получается следующий результат по количеству поездо-часов в год

$$(22900,5 \times 2 + 2650,5 \times 5) \times 365,25 = 21569290,9\,ч.$$

Только 64% всех поездов принадлежат Deutsche Bahn (DB), это также необходимо учесть, так как статистика аварий относится ко всем поездам (не только к по-

ездам DB), а пробег – только к поездам DB. Это дает интенсивность

$$\frac{0,64\times 86,4}{21569290,9\,h} = 2,56\times 10^{-6}\,1/\text{ч}.$$

Существует множество ситуаций, когда появляется требование машинисту, но аварии впоследствии не происходит. Это может произойти потому, что машинист успешно среагировал, или потому, что другие обстоятельства предотвращают аварию. Таким образом значение, приведенное выше, еще не является интенсивностью требования.

Поэтому необходимо ввести коэффициент, показывающий, насколько чаще возникает требование машинисту, чем авария. В отчете [1] для GOA 3 / 4 этот коэффициент был оценен как 10. Последующие расчеты в разделе 3.4 настоящей статьи показывают, что этот коэффициент может принимать даже значение 25.

В результате интенсивность требования (при указанном коэффициенте, равном 10…25) составит

$$\mu_{BEU} = 2,56\times 10^{-5}\,1/\text{ч} \quad \ldots \quad 6,41\times 10^{-5}\,1/\text{ч},$$

в зависимости от того, какое из значений используется.

3.2.2. Интервал проверки

Предполагается, что техническая система ежегодно подвергается тщательной проверке (proof test), в ходе которой выявляются все «спящие» (скрытые) отказы. С другой стороны, требование машинисту воспринять ситуацию и впоследствии отреагировать может предъявляться реже, чем раз в год. В частности, учитывая большое количество функций, выполняемых машинистом, все требования к машинисту распределяются между многими функциями, поэтому интенсивность требований к каждой функции становится соответственно низкой.

Это говорит о том, что интенсивность требования определяется интервалом проверки, то есть

$$\mu_{PT} = 1/8760\,\text{ч} = 1,14\times 10^{-4}\,1/\text{ч}.$$

3.2.3. Подход максимума

Теперь в качестве интенсивности требования выбирается максимальное значение из интенсивности требования машинисту поезда и интенсивности требования на основе коэффициента, соответствующего интервалу проверки

$$\mu = \max\left(\mu_{PT};\mu_{BEU}\right) = 1,14\times 10^{-4}\,1/\text{ч}.$$

Данный подход имеет следующие преимущества:

• в пункте 5.2.5 стандарта DIN VDE 831-103 [11] указано, что при определении TFFR следует учитывать коэффициент приблизительно 10, если техническая система испытывается примерно в 10 раз чаще, чем это требуется в эксплуатации. Таким образом, в данном случае, если техническое испытание проводится в 10 раз чаще, допускается TFFR, больший в 10 раз. При формировании максимума этот фактор учитывается независимо от конкретного значения TFFR;

• расчет интенсивности требования по BEU подвержен определенным неопределенностям, особенно при учете потенциально опасных ситуаций. При максимизации оказывается, что влияние этого фактора на интенсивность требования пренебрежимо мало, если только он не становится слишком большим.

3.2.4. Интенсивности требования согласно источнику [12]

В данном разделе будет проведена дополнительная проверка правдоподобия выше установленного значения интенсивности требования. В источнике [12] приведены частоты столкновений поездов с препятствиями в Нидерландах, а также частоты пожаров. Это типичные события, на которые приходится реагировать машинисту. В приложении C источника [12] приведены следующие данные (табл. 5).

Табл. 5. Различные события и их количество в Нидерландах

Событие	2020 г.	2016-2020 гг.
Столкновение поезда с препятствием	143	762
Пожар	24	259
Сумма	167	1021

Кроме того, данные об объемах перевозок приводятся в миллионах поездо-километров (табл. 6).

Табл. 6. Объем перевозок в Нидерландах и интенсивности событий

Размер	2020 г.	2016-2020 гг.
Количество поездо-километров, млн	151,7	795,4
Количество событий на 1 километр	$1,1\times 10^{-6}$ 1/ч	$1,28\times 10^{-6}$ 1/ч
Интенсивность события при скорости движения поезда 80 км/ч, 1/ч	$8,8\times 10^{-5}$ 1/ч	$1,024\times 10^{-4}$ 1/ч

Теперь можно использовать эти данные в качестве приблизительной оценки того, как часто машинист должен реагировать на требование. Результаты, приведенные в табл. 6, подтверждают результат $1,14\times 10^{-4}$ 1/ч, представленный в разделе 3.2.3 настоящей работы.

3.2.5. Преобразование PFD в TFFR для GoA 2 и сравнение с результатами для GoA 3 / 4

Значения PFD (см. табл. 1) были пересчитаны в TFFR с применением соответствующих значений интенсивности требования, полученных выше. Результаты пересчета, а также величины, представленные в табл. 1 и 2, приведены в табл. 7.

Табл. 7. Результаты для GoA 2 и GoA 3 / 4

Функция	GOA 3 / 4 TFFR	GoA 2 PFD		GOA 2 TFFR	
		RARA 50%	Хинчин (мод.)	RARA 50%	Хинчин (мод.)
Предотвращение столкновения с препятствиями	$9{,}00 \times 10^{-7}$ 1/ч	$8{,}64 \times 10^{-3}$	10^{-3}	$9{,}85 \times 10^{-7}$ 1/ч	$1{,}14 \times 10^{-7}$ 1/ч
Обнаружение пониженного значения трения и реакция	10^{-7} 1/ч или ниже	$1{,}98 \times 10^{-2}$	$5{,}00 \times 10^{-3}$	$2{,}26 \times 10^{-6}$ 1/ч	$5{,}70 \times 10^{-7}$ 1/ч

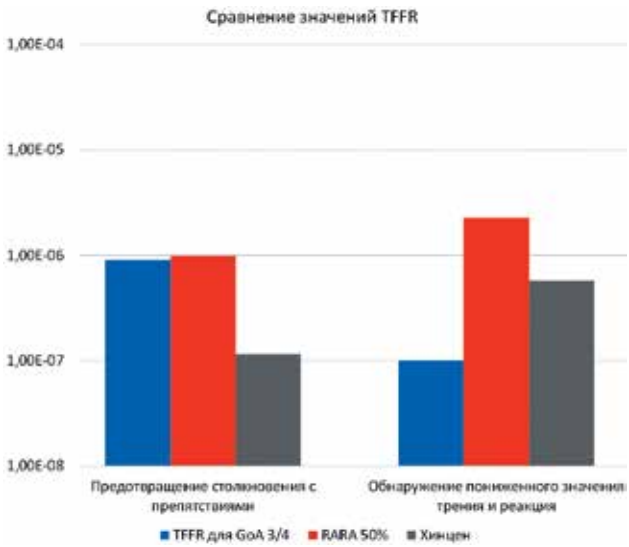

Рис. 1. Сравнение значений TFFR, полученных на основе различных принципов

Сравнение полученных результатов показывает следующее (см. рис. 1):

• результаты по RARA и Хинчину различаются между собой уже очень сильно, дальнейшее обсуждение причин см. в [2];

• для функции «Предотвращение столкновения с препятствиями» значение TFFR, определенное для GoA 3 / 4 по [11], и значение TFFR, полученное из PFD (GoA 2) на основе метода RARA, отличаются незначительно;

• для определения величины пониженного трения различия значительно больше, но значение TFFR, полученное для GoA 3 / 4, здесь гораздо более консервативно.

Следует отметить, что машинист не при всех обстоятельствах способен успешно реагировать:

• в силу объективных обстоятельств у него нет возможности вовремя затормозить, чтобы предотвратить столкновение, или

• он объективно не может заметить уменьшение коэффициента трения.

Это означает, что, строго говоря, вероятность эффективного отказа машиниста поезда

$$\text{PFD} \times p_E,$$

где p_E – вероятность того, что реакция машиниста является успешной.

Например, при высоких скоростях движения поезда у машиниста практически нет возможности предотвратить столкновение или существенно снизить последствия аварии.

На основе полученных результатов для GoA 2 мы имеем:

$$\text{TFFR} = \text{PFD} \times \mu.$$

Учитывая, что машинист поезда может успешно среагировать только с вероятностью p_E, получаем модифицированную формулу

$$\text{TFFR}_S = \text{PFD} \times p_E \times \mu + (1 - p_E) \times \mu.$$

В формуле для TFFR_S второй член учитывает те случаи, когда машинист по объективным причинам вообще не может среагировать, и авария происходит, даже если бы он среагировал идеально. Объем метода вывода критерия принятия риска представлен на рис. 2.

Рис. 2. Объект анализа риска в соответствии с GOA 2 и GOA 3 / 4

Можно отметить, что

$$\text{TFFR} < \text{TFFR}_S,$$

$$\text{PFD} \times \mu < \text{PFD} \times p_E \times \mu + (1 - p_E) \times \mu,$$

$$0 < (1 - \text{PFD}) \times (1 - p_E).$$

3.3. Результаты перекрестной валидации

Рассмотренные в предыдущих разделах вопросы показали, что:

• предположения о вероятности человеческой ошибки обоснованы и согласуются с результатами, полученными из других источников;

• обоснованы предположения об интенсивности требования машинисту (примерно раз в год) для корректной реализации преобразования PFD в TFFR;

• значения TFFR для машиниста, рассчитанные на основе PFD и интенсивности требования, являются достаточно консервативными по сравнению с показателями опасных отказов человека, которые встречаются в литературе;

• технические системы, которые должны заменить машиниста поезда для выполнения функции обнаружения препятствий, как правило, должны иметь уровень SIL 1 или выше.

3.4. Сравнительный расчет TFFR по принципу MEM

Далее проводится сравнительный и упрощенный расчет. В качестве примера рассматривается только функция машиниста по обнаружению препятствия и последовательному реагированию.

Сравнительный расчет отличается от других, описанных выше, по двум аспектам:

1. Использование статистических величин из Нидерландов. Преимущественно используются статистические данные из Нидерландов, это сделано по двум причинам. С одной стороны, эти значения доступны в хорошем качестве и с высокой степенью детализации, а с другой – они получены из разных источников. Кроме того, железнодорожные системы обеих стран хорошо сопоставимы.

2. Использование другого метода для получения критериев приемлемости рисков. Здесь в качестве процедуры выведения критериев приемлемости риска рассматривается принцип MEM (Minimum Endogenous Mortality), см. Приложение A4 к [13]. В предыдущих анализах этот метод не использовался.

Исходя из того, что минимальный эндогенный риск смертности для человека в возрасте от 5 до 15 лет составляет примерно 2×10^{-4} для отдельного человека в год, для одной технической системы выделяется бюджет риска в размере 10^{-5} на одного человека в год. Следующим шагом является выделение части бюджета риска для деятельности машинистов. Часто на сигнализацию выделяется около 10%, см. [4]. Эта доля используется для машиниста. Предполагается, что машинист несет полную ответственность за предотвращение столкновения, поскольку речь идет о препятствии на пути.

В результате получается значение допустимого риска

$$10\ \%\times10^{-5}\,1/год = 10^{-6}\,1/год = 1{,}14\times10^{-10}\,1/ч.$$

Речь идет о гибели одного человека, т.е. об индивидуальном риске. На следующем этапе рассчитывается индивидуальный риск, возникающий в результате отказа технической системы, заменяющей машиниста поезда.

Техническая система может иметь заданную TFFR и, как уже говорилось выше, раз в год подвергаться проверке. Тогда техническая система имеет PFD, равный

$$\text{PFD} = \text{TFFR} \times t / 2,$$

где t = 8760 ч – интервал проверки.

В качестве интенсивности требований системе принимается величина

$$\mu = 8{,}8 \times 10^{-5}\ 1/\text{ч}$$

из раздела 3.2.4.

Другим важным параметром является число погибших, которое можно ожидать в случае отказа технической системы. Здесь вновь используется [12]. За период с 2016 по 2020 год произошло 2 серьезных травмы и ни одного смертельного случая. Это относится к 45 значимым авариям (столкновение рельсовых транспортных средств, столкновение с препятствием, пожар). Значимые аварии – это аварии, отвечающие хотя бы одному из следующих критериев:

• имеется как минимум один тяжелораненый или погибший человек;

• сумма ущерба составляет не менее 150 000 евро;

• участок магистральной линии недоступен не менее 6 ч.

Для учета двух тяжелораненых используется понятие FWSI (fatalities and weighted severe injuries), см. [14]. Здесь тяжелые травмы добавляются к смертельным случаям с коэффициентом 0,1. Таким образом, вероятность смертельного исхода в таких авариях составляет

$$p_s = \frac{0{,}2}{45} = 4{,}44\times10^{-2}.$$

Следует отметить, что полученные выше вероятности подвержены статистической неопределенности, поскольку количество событий невелико. Кроме того, поскольку MEM является критерием индивидуального риска, необходимо также оценить вероятность смерти конкретного рассматриваемого человека. Мы предполагаем, что средняя наполняемость поезда составляет 50 пассажиров. Таким образом, вероятность того, что конкретный человек погибает в результате аварии, составляет,

$$q = \frac{1}{50} = 0{,}02.$$

Исходя из этого, для определения TFFR получено следующее неравенство:

$$\text{TFFR} \times \frac{t}{2} \times q \times p_s \times \mu < 1{,}14\times10^{-10}\,1/ч.$$

Это дает следующий результат:

$$\text{TFFR} < 3{,}33\times10^{-6}\,1/ч.$$

Следует отметить, что полученное значение очень хорошо согласуется с результатом, полученным для GoA 3 / 4. Согласование результатов, полученных с помощью MEM, с результатами других методов еще раз подтверждает результаты из [4].

На этом этапе следует указать на проблему метода MEM, см. также [15]. Результат зависит от многих факторов, которые часто приходится оценивать и которые затем влияют на конечный результат, особенно из-за их большого количества. Другие методы оказываются более устойчивыми. Они обходятся меньшим количеством факторов.

Вывод значений приемлемого риска по MEM также подтвердил другие значения, полученные для GoA 2 и GoA 3 / 4. Это показано на рис. 3.

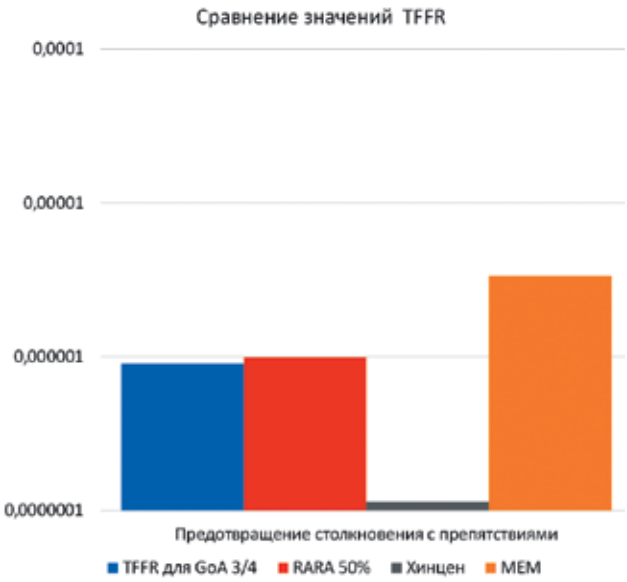

Рис. 3. Сравнение значений TFFR, полученных в результате выполнения различных пакетов работ.

Таким образом, можно утверждать, что [10] в принципе подходит для выведения критериев приемлемости рисков для проектов АТО.

4. Резюме

Определение вероятности человеческой ошибки для GoA 2 проводилось в соответствии с общепринятыми процедурами, применяемыми в железнодорожном секторе. То же самое относится и к определению значений TFFR для технических систем для GoA 3 / 4 для технической системы.

Валидация заключалась в сравнении результатов с другими источниками и различных перекрестных сравнениях. С одной стороны, сравнивались различные результаты, с другой стороны, был проведен независимый расчет с использованием MEM. Нельзя было ожидать, что будут получены точно такие же цифры. Результаты подтвержден в принципе. Причина этих различий была объяснена. Исследование показало, что результаты анализа риска могут быть подтверждены путем сравнения оценок, полученных различными методами. Это обосновывает выведенные требования безопасности – в нашем случае SIL 1 / SIL 2, которые должны применяться в случае замены человека-машиниста технической системой. Тем не менее, необходимо провести детальный анализ для каждой функции, подробнее см. в [1].

Библиографический список

1. Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene (ATO-RISK), Abschlussbericht. Bericht 40 (2023). Projektnummer 2020-19-S-1202. Deutsches Zentrum für Schienenverkehrsforschung, 2023. URL: https://www.dzsf.bund.de/SharedDocs/Downloads/DZSF/Veroeffentlichungen/Forschungsberichte/2023/ForBe_40_2023_ATO_Risk.pdf?__blob=publicationFile&amp%3Bv=3 (дата обращения 29.01.2024).

2. Adebahr F., Schäbe H. The Probability of Human Error and Failure Rates of Technical ATO Systems // Signal & Datacommunication. 2023. № 3. Pp. 21-29.

3. Braband J., Lindner L., Rexin F. Risk analysis for obstacle detection in automated driving // Signal & Datacommunication. 2023. № 3. Pp. 12-20.

4. Schäbe H. Different Approaches for Determination of Tolerable Hazard Rates // ESREL 2001, Torino, Conference Proceedings. 2001. Vol. 1. Pp. 435-442.

5. Dhillon B.S. Human Reliability, Error, and Human Factors in Engineering Maintenance with Reference to Aviation and Power Generation. CRC Press, 2009.

6. Dhillon B.S., Human Reliability, Error, and Human Factors in Power Generation. Springer, 2014.

7. Sicherheitsregelung Fahrzeug – Methode zum Festlegen und Nachweisen sicherheitsbezogener Anforderungen und Bewertung der Risiken im Rahmen der Umsetzung der CSM-RA und der EN 50126, Arbeitskreis APT/SIRF unter dem Lenkungskreis Fahrzeuge, 16.11.2021.

8. Braband J., Schäbe H., vom Hövel R. Вероятность отказа по требованию – почему и как (Probability of Failure on Demand, why and how) // Надежность. 2010. № 2. С. 2-10.

9. Auswertung Unfalldatenbank der Bundesstelle für Eisenbahnunfalluntersuchung (BEU) (01.01.2017 bis 26.04.2021), ausgewertet am 18.05.2021. Voigt, 2021.

10. Hilfeleistungseinsätze im Gleisbereich der DB AG. Deutsche Bahn AG, 2021. URL: https://www.deutschebahn.com/resource/blob/264996/345dad9c6bec2af95dc185d59c94afe1/notfallmanagement_leitfaden_hilfeleistungseinsatz-data.pdf (дата обращения 29.01.2024).

11. DIN VDE V 0831-103:2020-09. Electric signalling systems for railways. Part 103: Identification of safety requirements for technical functions in railway signalling.

12. Veiligheid van de spoorwegen. Jaarverslag Spoorwegveiligheid 2020. Inspectie Leefomgeving en Transport, 2020. URL: https://www.ilent.nl/binaries/ilt/documenten/jaarverslagen/2021/12/10/jaarverslag-spoorveiligheid-2020/Jaarverslag+Spoorwegveiligheid+2020.pdf (дата обращения 29.01.2024).

13. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety-2:2017.

14. Braband J., Schäbe H. Propagation of uncertainty in railway signaling risk analysis. In: Safety and Reliability of Complex Engineered Systems, in: Safety and Reliability of Complex Engineered Systems / Podofillini et al. (Eds). Proc. ESREL 2015, Taylor & Francis Group, London, 2015. Pp. 2623-2626.

15. Braband J. Risikoanalysen in der Eisenbahn-Automatisierung. Eurailpress, 2005. 136 p.

References

1. Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene (ATO-RISK), Abschlussbericht. Bericht 40 (2023). Projektnummer 2020-19-S-1202. Deutsches Zentrum für Schienenverkehrsforschung, 2023. URL: https://www.dzsf.bund.de/SharedDocs/Downloads/DZSF/Veroeffentlichungen/Forschungsberichte/2023/ForBe_40_2023_ATO_Risk.pdf?__blob=publicationFile&amp%3Bv=3 (дата обращения 29.01.2024).

2. Adebahr F., Schäbe H. The Probability of Human Error and Failure Rates of Technical ATO Systems // Signal & Datacommunication. 2023. № 3. Pp. 21-29.

3. Braband J., Lindner L., Rexin F. Risk analysis for obstacle detection in automated driving // Signal & Datacommunication. 2023. № 3. Pp. 12-20.

4. Schäbe H. Different Approaches for Determination of Tolerable Hazard Rates // ESREL 2001, Torino, Conference Proceedings. 2001. Vol. 1. Pp. 435-442.

5. Dhillon B.S. Human Reliability, Error, and Human Factors in Engineering Maintenance with Reference to Aviation and Power Generation. CRC Press, 2009.

6. Dhillon B.S., Human Reliability, Error, and Human Factors in Power Generation. Springer, 2014.

7. Sicherheitsregelung Fahrzeug – Methode zum Festlegen und Nachweisen sicherheitsbezogener Anforderungen und Bewertung der Risiken im Rahmen der Umsetzung der CSM-RA und der EN 50126, Arbeitskreis APT/SIRF unter dem Lenkungskreis Fahrzeuge, 16.11.2021.

8. Braband J., Schäbe H., vom Hövel R. Вероятность отказа по требованию – почему и как (Probability of Failure on Demand, why and how) // Надежность. 2010. № 2. С. 2-10.

9. Auswertung Unfalldatenbank der Bundesstelle für Eisenbahnunfalluntersuchung (BEU) (01.01.2017 bis 26.04.2021), ausgewertet am 18.05.2021. Voigt, 2021.

10. Hilfeleistungseinsätze im Gleisbereich der DB AG. Deutsche Bahn AG, 2021. URL: https://www.deutschebahn.com/resource/blob/264996/345dad9c6bec2af95dc185d59c94afe1/notfallmanagement_leitfaden_hilfeleistungseinsatz-data.pdf (дата обращения 29.01.2024).

11. DIN VDE V 0831-103:2020-09. Electric signalling systems for railways. Part 103: Identification of safety requirements for technical functions in railway signalling.

12. Veiligheid van de spoorwegen. Jaarverslag Spoorwegveiligheid 2020. Inspectie Leefomgeving en Transport, 2020. URL: https://www.ilent.nl/binaries/ilt/documenten/jaarverslagen/2021/12/10/jaarverslag-spoorveiligheid-2020/Jaarverslag+Spoorwegveiligheid+2020.pdf (дата обращения 29.01.2024).

13. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety-2:2017.

14. Braband J., Schäbe H. Propagation of uncertainty in railway signaling risk analysis. In: Safety and Reliability of Complex Engineered Systems, in: Safety and Reliability of Complex Engineered Systems / Podofillini et al. (Eds). Proc. ESREL 2015, Taylor & Francis Group, London, 2015. Pp. 2623-2626.

15. Braband J. Risikoanalysen in der Eisenbahn-Automatisierung. Eurailpress, 2005. 136 p.

Сведения об авторе

Хендрик Шебе – доктор естественных наук, главный эксперт по надежности, эксплуатационной готовности, ремонтопригодности и безопасности, TÜV Rheinland InterTraffic, Кельн, Германия, e-mail: dr.hendrik.schaebe@gmail.com

About the author

Hendrik Schäbe, Dr. rer. nat. habil., Principal Assessor RAMS, TÜV Rheinland InterTraffic, Cologne, Germany; e-mail: dr.hendrik.schaebe@gmail.com

Вклад автора в статью

Выполнен анализ литературы в области рисков функциональной безопасности технических систем и рисков, связанных с ошибками человека. Проведена валидация анализа рисков в рамках исследовательского проекта по автоматизированному ведению поезда, с применением различных методов. Показано, что результаты анализа риска подтверждаются путем сравнения оценок, полученных разными методами. Обосновано, что в случае замены человека-машиниста технической системой должны обеспечиваться требования безопасности SIL 1 / SIL 2.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.