*Надежность, том 26, №2, 2026 / Dependability 2, 2026*
*Транспортные и транспортно-технологические системы страны, ее регионов и городов, организация производства на транспорте*
*УДК 656.25:656.2.08*
*Оригинальная статья*
*https://doi.org/10.21683/1729-2646-2026-26-2-9-16*

# Об отказобезопасности критически важных систем высокоскоростного движения

## On the fail-safety of critical systems in high-speed rail

**Гапанович В.А.[1], Шубинский И.Б.[2]***
**Gapanovich V.A.[1], Shubinsky I.B.[2]***

*[1] Ассоциация «Объединение производителей железнодорожной техники» (ОПЖТ), Москва, Россия*
*[2] АО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»), Москва, Российская Федерация*
*[1] Association "Union of Industries of Railway Equipment" (UIRE), Moscow, Russia*
*[2] Research and Design Institute for Information Technology, Signalling and Telecommunications in Railway Transportation (JSC NIIAS), Moscow, Russian Federation*
** igor-shubinsky@yandex.ru*

*Гапанович В.А.*

*Шубинский И.Б.*

**Резюме. Цель**. *Установить приемлемые архитектуры отказобезопасности критически важных систем высокоскоростного движения, определить их возможности и ограничения.* **Методы.** *Построение и исследование ряда математических моделей надежности и функциональной безопасности систем. Выбор приемлемых архитектур отказобезопасности критически важных систем высокоскоростного движения.* **Результаты.** *Анализ надежности широко распространенной на практике архитектуры безопасности* **2oo3** *аналитически и численно показал, что с помощью мажоритарной логики удается существенно повысить достоверность результатов (среднее время до функционального отказа мажорированной системы в 2 раза превышает этот показатель в исходном объекте). Вместе с тем, безотказность системы, а, следовательно, ее отказобезопасность, ниже, чем у исходного объекта. Поэтому такая архитектура приемлема не выше уровня SIL3. Возможно для обеспечения этого уровня отказобезопасности предпочтение отдавать альтернативной архитектуре* **(1oo2)P** *вследствие отсутствия в ней восстанавливающих органов и переключающих устройств. Она формируется из двух параллельно работающих компонент, каждая из которых построена по схеме постоянного дублирования. Однако при этом не следует забывать, что в такой системе сохраняется риск ложного срабатывания. Показано, что для обеспечения отказобезопасности на уровне SIL4 можно применять гибридные мажоритарные архитектуры (***2oo3)P** *или* **2oo4.** *Вместе с тем следует учитывать, что существенную часть мажоритарных структур отказобезопасности критически важных систем составляют переключательные схемы, обеспечивающие отключение отказавших и включение резервных компонент. Это обстоятельство отрицательно сказывается на эффективности мажоритарного резервирования, поскольку связано с применением дополнительных средств и процедур. Причина этого недостатка состоит в том, что и при аппаратной, и при программной организации механизм маскирования сбоев, т.е. голосование, определение неисправного канала, его блокирование и последующее включение в нормальную работу, используется в каждом такте работы системы вне зависимости от наличия или отсутствия сбоев. Эти временные потери при практической реализации достигают 30-50%. К недостаткам мажорирования при его реализации следует отнести также большое количество связей между каналами и определенные трудности при проектировании. Указанные ограничения оказывают негативное, но не определяющее влияние на выбор приемлемой архитектуры отказобезопасности. Их следует учитывать для каждого конкретного объекта и условий его применения*

**Abstract. Aim.** *To identify acceptable fail-safety architectures for critical high-speed rail systems, as well as their capabilities and limitations***. Methods.** *Construction and study of several mathematical models of system dependability and functional safety. Selection of acceptable faail-safety architectures for critical high-speed rail systems.* **Results.** *An analytical and numerical analysis of the dependability of the widely used 2oo3 safety architecture has shown that majority logic can significantly improve the reliability of the results (mean time to functional failure of a majority system is twice that of the original object). However, the system's dependability, and, consequently, its fail-safety, is lower than that of the original object. Therefore, such an architecture is not acceptable beyond SIL3. For the purpose of ensuring this level of fail-safety, the alternative* **(1oo2)P** *architecture may prove to be preferable as it lacks restoring organs and switching devices. It is made of two components that operate in parallel, each of which uses a hot standby setup. However, one should not forget that such systems are prone to false alarms. It has been shown that hybrid majority architectures* **(2oo3)P** *or*

**2oo4** *can provide SIL4 fail-safety. However, it should be noted that a significant portion of the majority setups that ensure fail-safety of critical systems are switching circuits designed for disconnecting failed components and activating backup components. This circumstance affects the effectiveness of majority redundancy, as it requires the use of additional tools and procedures. This shortcoming is due to the fact that in both hardware and software implementations, the fault masking mechanism, i.e., voting, faulty channel identification, blocking thereof, and then resuming normal operation, is repeated in every system cycle, regardless of the presence or absence of faults. Practically, the associated time losses are as high as 30 to 50%. The disadvantages of majority redundancy also include the large number of connections between channels and certain design difficulties. These limitations have a negative, but not decisive, effect on the selection of an acceptable fail-safety architecture. They should be taken into account given each specific object and its operating conditions.*

**Ключевые слова.** *Киберфизическая система, отказобезопасность, безотказность, функциональная надежность, архитектура отказобезопасности, мажоритарная логика система с гибридной мажоритарной логикой*
**Keywords***: Cyber-physical system, fail-safety, reliability, functional dependability, fail-safety architecture, majority logic, hybrid majority logic system*

**Для цитирования:** *Гапанович В.А., Шубинский И.Б. Об отказобезопасности критически важных систем высокоскоростного движения // Надежность. 2026. №2. С. 9-16. https://doi.org/10.21683/1729-2646-2026-26-2-9-16*
**For citation:** *Gapanovich V.A., Shubinsky I.B. On the fail-safety of critical systems in high-speed rail. Dependability 2026;2: 9-16. https://doi.org/10.21683/1729-2646-2026-26-2-9-16*

**Поступила:** *03.01.2025* / **После доработки:** *15.01.2026* / **К печати:** *25.05.2026*
**Received on:** *03.01.2025* / **Revised on:** *15.01.2026* / **For printing:** *25.05.2026*

## Введение

Для выполнения функций безопасности на железнодорожном транспорте в течение многих лет используются системы, состоящие из электрических и/или электронных элементов.

В критически важных системах высокоскоростного движения безопасность достигается в большинстве своем за счет использования нескольких составных устройств и даже систем, в которых применяются различные технологии (например, механические, гидравлические, пневматические, электрические, электронные, программируемые электронные). Так, например, локомотив состоит из множества взаимосвязанных между собой систем, содержащих, в том числе, критически важные системы, непосредственно обеспечивающие безопасность движения. К ним можно отнести: локомотивные приборы безопасности; системы автоматического пожаротушения и системы обнаружения возгораний; электронную (программируемую) часть управления тормозами. В мотор-вагонном подвижном составе в состав критически важных систем можно отнести также системы управления внешними и внутренними дверьми.

Любая стратегия безопасности должна, следовательно, учитывать не только все элементы, входящие в состав отдельных систем (например, датчики, управляющие устройства и исполнительные механизмы), но также и все подсистемы безопасности, входящие в состав общей системы обеспечения безопасности. Таким образом, для критически важных систем высокоскоростного движения недостаточно ограничиваться задачами анализа и синтеза отдельных функций безопасности – необходимо комплексно решать задачи безопасности на системном уровне. При этом следует руководствоваться основными документами Международной электротехнической комиссии в области внедрения системного управления RAMS в железнодорожной отрасли IEC 62278-1 и IEC 62278-2 и особенно Техническими отчетами IEC 62278-3:2025 и 62278-4:2025. В дополнение к стандарту IEC 62278 Техническим комитетом МЭК ТК 9 выпущен Технический отчет [1]. Эта часть IEC 62278 содержит указания по применению требований RAM в частности к подвижному составу и проведению мероприятий RAM в течение стадий жизненного цикла системы от приглашения к участию в тендере до демонстрации на стадии эксплуатации.

Необходимо отметить одно важное изменение в обновленной редакции IEC 62278-1:2025 [2]. В определении введен конкретный объект стандартизации «Физическое устройство». Из этого следует, что требования функциональной безопасности [3] применимо и для киберфизических систем, а не только к программному обеспечению и архитектуре логических контроллеров микропроцессорных систем управления. Это обстоятельство позволяет с точки зрения функциональной безопасности рассматривать критически важные системы высокоскоростного движения как киберфизические системы [4], содержащие (рис. 1):

- вычислительную компоненту в составе с прикладной логикой, прикладной вычислительной платформой и системной вычислительной платформой;
- прикладную компоненту с целевыми физическими объектами и процессами;
- датчики и исполнительные устройства.

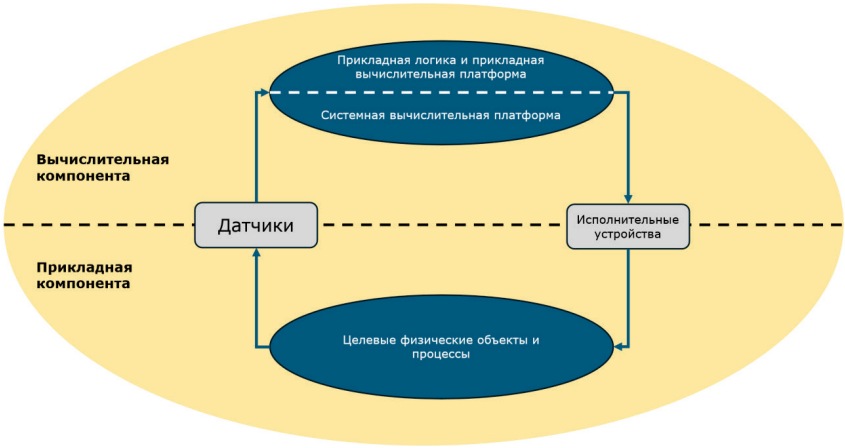


Рис. 1. Структурная модель киберфизических критически важных систем

## 1. Архитектуры отказобезопасности критически важных систем

Под безопасностью понимается отсутствие недопустимого риска или способность предмета, явления или процесса сохраняться при разрушающих воздействиях, или свойство критически важных систем сохранять свои параметры при воздействии опасностей, или способность системы функционировать, не переходя в опасное состояние и т.д. [5]. Все эти определения по существу сводятся к двум ключевым положениям: 1) при воздействии опасности система должна сохранять свои свойства и функционировать без происшествий; 2) риск опасного воздействия самой системы на окружающую среду не должен превышать допустимый уровень. Здесь под опасностью понимается угроза неблагоприятного (негативного) воздействия чего-либо на систему.

В зависимости от последствий можно отдельно рассматривать (рис. 2):

а) функциональную надежность системы, если она выполняет свою функцию (т.е. не теряет определенных свойств) в цепочке всех тех систем, которые участвуют в функции;

б) функциональную безопасность, если последствия не сведут к неприемлемым рискам.

Нарушения безопасности критически важной системы высокоскоростного движения вызваны событиями нарушений функционирования или эксплуатации самой системы. Существенными угрозами нарушения безопасности являются также информационные атаки и недекларированные возможности [6]. Отсюда следует, что *отказобезопасность – способность системы сохранять безопасное состояние в случае реализации угроз, связанных с нарушениями функционирования или эксплуатацией самой системы, а также с информационными атаками и недекларированными возможностями, и сохранять режим работы, не представляющий опасности для людей, окружающей среды или имущества*.

Возможные архитектуры отказобезопасности критически важных систем относительно их уровней полноты безопасности (SIL) и практические примеры в системах управления показаны в табл.1.

Коэффициент диагностического покрытия (Diagnostic Coverage, DC) – это количественный показатель в стандартах функциональной безопасности (IEC 61508), который показывает, какую долю опасных отказов компонента или системы способна обнаружить встроенная диагностика. Рекомендуемый минимальный DC (для аппаратных средств) SIL2 ≥ 90%. Для уровня SIL3 DC ≥ 99%, предполагается периодическое тестирование

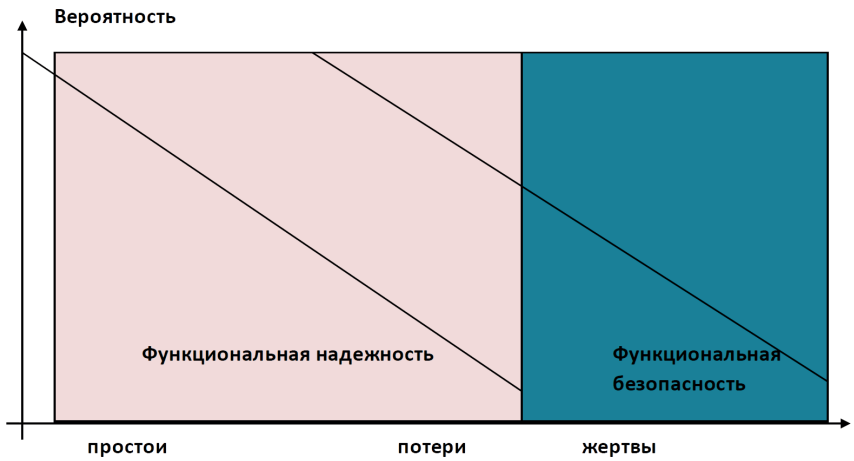


Рис. 2. Функциональная надежность и функциональная безопасность

**Табл. 1. Архитектуры отказобезопасности критически важных систем**

| Целевой уровень SIL | Типовая архитектура (сокращение) | Описание и логика работы | Практический пример в системе управления |
|---|---|---|---|
| **SIL 1** | **1oo1** (1 out of 1) | Одиночный канал. Без резервирования. Высокие требования к качеству компонентов и диагностике. | Простой датчик или привод с высокой собственной надежностью, где отказ маловероятен, а последствия минимальны. |
| **SIL 2** | **1oo1D** (1 out of 1 with Diagnostics) | Одиночный канал, но с **расширенной внутренней диагностикой** (DC ≥ 90%). Диагностика обнаруживает большинство отказов и переводит систему в безопасное состояние. | Контроллер с функцией самопроверки памяти, процессора и цепей ввода/вывода. При обнаружении сбоя инициируется аварийная остановка. |
| **SIL 2 / SIL 3** | **1oo2** (1 out of 2) | **Два параллельных канала**. Система срабатывает, если сработал **хотя бы один** канал. Высокая доступность, но есть риск ложного срабатывания. | Два независимых датчика давления. Если один показывает опасное значение — система останавливается. Используется, когда ложная остановка менее критична, чем пропуск опасности. |
| **SIL 3 / SIL 4** | **2oo3** (2 out of 3) | **Три параллельных канала**. Система срабатывает, если сработали **как минимум два** канала. Оптимальный баланс: отказоустойчивость (один канал может отказать) + защита от ложных срабатываний. | "Золотой стандарт" для критичных систем. Три процессорных модуля в системе управления движением поезда. Решение принимается по большинству, что исключает остановку из-за сбоя в одном модуле. |
| **SIL 4** | **2oo4** (2 out of 4) и другие комбинации | Высшая степень резервирования и отказоустойчивости. Может включать несколько уровней резервирования (аппаратное, временное, функциональное). | Критичные системы на АЭС или системы автоматического торможения поездов (например, ETCS Level 2). Часто сочетает дублированные контроллеры, работающие по схеме 2oo4, с независимыми цепями питания и датчиками. |

оперативной памяти, контроль временных циклов, диагностика целостности программы

Основой для выбора полноты безопасности SIL является требование снижения риска до приемлемого уровня. Допустимый (приемлемый) уровень для пассажирского транспорта определяется как вероятность тяжелого или смертельного травмирования не более $10^{-6}$ в год (один случай на миллион лет в эксплуатации).

Уровень диагностического покрытия напрямую влияет на основные параметры системы:

- снижение вероятности опасного отказа
- повышение достигнутого уровня полноты безопасности SIL.

Для уровня SIL4 применяются все те же методы, что и для SIL3.Дополнительно реализуется полное аппаратное дублирование с постоянным сравнением выходов двух каналов, а также самодиагностика процессорного ядра, тестирование системы данных, контроль напряжения питания, избыточное вычисление со сравнениями.

Оценим достоинства и недостатки основных приведенных в табл.1 архитектур отказобезопасности систем.

*Архитектура 1oo1 (SIL1)* – простота и низкая стоимость. Однако низкая отказоустойчивость – отказ единственного канала ведет к отказу всей функции безопасности.

*Архитектура 1oo2 (SIL2/3)* – высокая вероятность корректного срабатывания. Однако повышенная вероятность ложного срабатывания, что может приводить к незапланированным остановам.

*Архитектура 2oo3 (SIL3/4)* – снижает вероятность ложного срабатывания. Однако относительно возможностей обеспечения надежности и безопасности требует дополнительного изучения (см. раздел 2).

*Архитектура 2oo4 (SIL4)* – высокая надежность и отказобезопасность. Позволяет системе продолжать безопасную работу при отказе двух каналов в определенных конфигурациях.

Ложные срабатывания систем управления существенно ограничивают возможности высокоскоростного движения поездов. Высокий уровень отказобезопасности и низкая вероятность ложного срабатывания являются ключевыми требованиями к критически важным система высокоскоростного движения поездов. Этим условиям отвечает архитектура *2oo4* (*SIL4*) и в определенной мере архитектура *2oo3* (*SIL3/4*).

## 2. Отказобезопасность мажоритарной архитектуры *2oo3*

Мажоритарной называется система выборов, при которой в число избранных попадают лишь кандидаты партии, получившей большинство голосов в данном округе. Этот подход применяется и в технике для повышения надежности ответственных объектов. Так, в критически важных системах широко применяется трехкратная структурная избыточность объектов в сочетании с восстанавливающим органом (ВО). На этой основе создается троированный мажоритарный объект (ТМО) с ВО, который определяет выходные результаты по *большинству голосов (мажоритарным методом)*. В результате реализуется логика 2/3 (совпадение хотя – бы двух выходных результатов из трех при трех параллельно работающих однотипных устройствах). В этом случае при условии идеальной надежности восстанавливающего органа вероятность безотказной работы и вероятность отказа ТМО соответственно равны:

$$P_{TMC}(t) = P^3(t) + 3P^2(t)G(t);$$

$$G_{TMC}(t) = 3P(t)G^2(t) + G^3(t),$$

где $P(t)$ и $G(t)$ – вероятности безотказной работы и вероятности отказа любого одного из трех параллельно работающих устройств.

В общем случае резервирования с логикой $n/m$, когда $n \geq 2$ и $n<m$ вероятность безотказной работы $N$ – го мажоритарного объекта (NMO) имеет следующий вид:

$$P_{NMO}(t) = P^m(t) + \binom{m}{1} P^{m-1}(t)G(t) + \\ + \binom{m}{2} \cdot P^{m-2}(t)G^2(t) + \ldots + \binom{m}{i} \cdot P^{m-i}(t)G^i(t) + \ldots \\ \ldots + \binom{m}{n} \cdot P^n(t)G^{m-n}(t) = \sum_{i=0}^{n} \binom{m}{i} \cdot P^{m-i}(t)G^i(t) \qquad (1)$$

При экспоненциальном законе распределения отказов с интенсивностью λ показатели безотказности ТМО имеют вид:

$$P_{TMC}(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t};$$

$$\lambda_{TMC}(t) = \frac{6\lambda(1-e^{-\lambda t})}{3-2e^{-\lambda t}}; \; T_{TMC} = \frac{5}{6\lambda}.$$

Приведенные выше значения показателей надежности мажоритарного объекта показывают, что мажоритарное резервирование может снизить его безотказность по отношению к исходному нерезервированному объекту. Вместе с тем, предполагается, что этот вид резервирования повышает достоверность передаваемой информации и, следовательно, повышает функциональную надежность исходного объекта. Убедимся в этом.

ВО может реализоваться аппаратно или программно. Как правило, предпочтение отдается программному варианту реализации ВО, как более дешевому и гибкому варианту построения мажоритарного объекта. Вследствие простоты логики построения программы ВО есть возможность практически исключить алгоритмические и программные ошибки. Вследствие этого у некоторых специалистов создается иллюзия абсолютной надежности ВО. При этом упускается из виду то очень существенное обстоятельство, что функциональная надежность ВО и мажоритарного объекта в целом определяется не только ошибками в программе, но, главным образом, сбойными ошибками, которые возникают значительно чаще отказов аппаратуры и могут существенно понизить эффективность мажоритарного резервирования.

По существу восстанавливающий орган представляет собой для мажоритарной логики 2/3 программно реализованную структуру, показанную на рис.3

С помощью микроопераций $\wedge_1$, $\wedge_2$, $\wedge_3$ производится поразрядное сравнение выходных результатов работы цифровых однотипных устройств 1, 2 и 3. Количество бит в выходном результате обычно колеблется в пределах от 8 до 128. Эти цифры показывают число сравнений, которое нужно однократно выполнить каждой из трех микроопераций. В результате сравнений формируются 3 одиночных сигнала $X_i$ ($i$ = 1, 2, 3), каждый из которых представляет собой код 1 или 0.

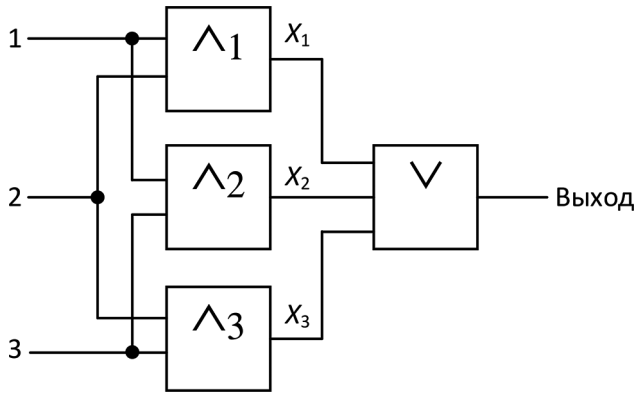

Рис. 3. Мажоритарная логика 2/3

Построим модель надежности мажоритарного объекта с восстанавливающим органом с логикой 2/3 в предположении, что микрооперации сравнения результатов работы цифровых однотипных устройств находятся под воздействием сбойных ошибок аппаратуры объекта и выполняются с вероятностью правильной однократной работы $p$. При этом для оценки сверху принимается, что алгоритмические и программные ошибки в микрооперациях отсутствуют и микрооперация дизъюнкции (рис. 3) также выполняется безошибочно вследствие большой избыточности по кодам 1 [7].

Вероятность функционального отказа мажоритарного объекта в момент времени $t_i$, $i$ = 0, 1, 2, …, определяется суммой вероятностей следующих событий:

- $G(A) = G^3(t_i) + 3G^2(t_i)P(t_i)$ – вероятность того, что все три устройства отказали или отказали два любых из трех устройств (при этом состояние надежности восстанавливающего органа не оказывает влияния);

- $G(Б) = P^3(t_i)(g^3 + 3g^2p)$ – вероятность того, что исправны все три устройства, но неправильно выполнены все три микрооперации восстанавливающего органа, или хотя бы две микрооперации из трех;

- $G(B) = 3P^2(t_i)G(t_i)(g^3 + 3g^2p + 3gp^2)$ – вероятность того, что при условии исправности двух любых из трех устройств неправильно выполнены либо все три микрооперации или две из трех или хотя бы одна из трех.

Вероятность отсутствия функционального отказа в работе мажоритарного объекта в момент времени $t_i$ равна:

$$P_{MO}(t_i) = 1 - G(A) - G(Б) - G(B) = \\ = P^2(t_i)[1 - g^2(1+2p) + G(t_i)p^2(2p-3g)].$$

Здесь подразумевается, что разность между соседними моментами времени $\Delta t = t_i - t_{i-1}$ есть такт обработки информации в системе.

Следовательно, вероятность функционального отказа в течение такта однократной обработки информации равна:

$$P_{MO}(\Delta t) = P^2(\Delta t)[1 - g^2(1+2p) + G(\Delta t)p^2(2p-3g)]. \quad (2)$$

Функция распределения времени до функционального отказа с учетом геометрического распределения ошибок в выполнении микроопераций восстанавливающего органа [7] имеет следующий вид: $F(n) = 1 - P_{MO}^{n}$. При этом математическое ожидание времени до функционального отказа мажоритарного объекта определяется в виде:

$$T_{\text{МОф}} = \frac{\Delta t}{1 - P_{\text{МО}}(\Delta t)}. \quad (3)$$

Учитывая, что геометрическое распределение есть дискретный аналог экспоненциального распределения, можно выразить интенсивность функциональных отказов мажоритарного объекта через величину, обратную средней наработке до его функционального отказа:

$$\lambda_{\text{МОф}} = \frac{1 - P_{\text{МО}}(\Delta t)}{\Delta t} =$$
$$= \frac{1 - P^2(\Delta t)[1 - g^2(1+2p) + G(\Delta t)p^2(2p-3g)]}{\Delta t}.$$

Для сравнения определим показатели функциональной надежности исходного объекта (цифрового устройства системы) без резерва, имея в виду, что результат работы устройства представляет собой массив информации, который считывается в каждом такте обработки информации. Вероятность безотказной работы устройства в течение длительности такта равна $P(\Delta t)$. Вероятность правильного однократного считывания массива информации определяем в виде $p_1 = p^{1/3}$. Эта связь с показателем правильного однократного выполнения микрооперации объясняется тем, что при выполнении микрооперации считываются массивы информации с двух устройств, после чего эти массивы сравниваются между собой. В результате при выполнении микрооперации выполняются три примерно равных действия считывания массива информации.

Отсюда вероятность функционального отказа в течение такта однократной обработки информации нерезервированным объектом равна $P_O(\Delta t) = P(\Delta t)p^{1/3}$. Другие два показателя функциональной безотказности имеют следующий вид:

$$T_{O\phi} = \frac{\Delta t}{1 - P(\Delta t)p^{\frac{1}{3}}}; \lambda_{O\phi} = \frac{1 - P(\Delta t)p^{\frac{1}{3}}}{\Delta t}. \quad (4)$$

Рассмотрим пример.

***Пример 1.*** Время такта обработки информации $\Delta t = 10^{-6}$ с. Показатели правильного однократного выполнения микрооперации сравнения результатов работы цифровых однотипных компонент находятся на уровне правильной однократной работы большой интегральной схемы и составляют согласно [7] $p = 1–5\times10^{-13}$; $g = 5\times10^{-13}$. Отказы составных компонентов обработки информации распределены по экспоненциальному закону с интенсивностью $\lambda = 10^{-6}$ 1/ч = $0{,}3\times10^{-9}$ 1/с. Требуется вычислить показатели функциональной безотказности мажоритарного объекта и объекта без резерва и сравнить эти результаты.

*Решение.* Вначале определяют вероятности безотказной работы и вероятности отказа исходного объекта в течение такта обработки информации:

$$P(\Delta t) = \exp(-\lambda\Delta t) = 1 - 0{,}3\cdot10^{-15}\ 1/\text{с};$$

$$G(\Delta t) = 1 - \exp(-\lambda\Delta t) = 0{,}3\cdot10^{-15}\ 1/\text{с}.$$

По формуле (2) находят вероятность правильной однократной работы мажоритарного объекта $P_{\text{МО}}(\Delta t) \approx 1–1{,}2\times10^{-15}$. Затем по формуле (3) определяют среднюю наработку до функционального отказа, а затем и интенсивность функциональных отказов мажоритарного объекта:

$$T_{\text{МОф}} = 8\cdot10^{8}\ \text{с} = 2\cdot10^{5}\ \text{ч};\ \lambda_{\text{МОф}} = 5\cdot10^{-6}\ 1/\text{ч}.$$

По формуле (4) определяют среднюю наработку до функционального отказа, а затем и интенсивность функциональных отказов исходного нерезервированного объекта:

$$P_{\text{О}}(\Delta t) \approx 1 - 3{,}2\cdot10^{-15};$$

$$T_{\text{Оф}} = 3{,}12\cdot10^{8}\ \text{с} = 0{,}87\cdot10^{5}\ \text{ч};\ \lambda_{\text{МОф}} = 11{,}5\cdot10^{-6}\ 1/\text{ч}.$$

Полученные результаты убедительно подтверждают справедливость высказанного ранее тезиса о том, мажоритарное резервирование с логикой 2/3 снижает структурную надежность (показатель средней наработки до структурного отказа $T_{\text{О}} = 1/\lambda$ исходного объекта снижается до значения $T_{\text{МО}} = 5/6\lambda$ у мажоритарного объекта). Однако большое достоинство мажоритарного резервирования в том, что оно существенно повышает функциональную надежность объекта (показатель средней наработки до функционального отказа мажоритарного объекта более чем в два раза превышает тот же показатель исходного нерезервированного объекта, т.е. $T_{\text{МОф}} / T_{\text{Оф}} > 2$).

При низкой вероятности правильного выполнения микроопераций сравнения результатов работы компонент ($p \to 0$) функциональная надежность мажоритарного объекта ничтожно мала ($P_{\text{МО}}(\Delta t) \to 0$) даже при высокой вероятности безотказной работы составных однотипных компонент объекта ($P(\Delta t) \to 1$). Отсюда следует, что для обеспечения функциональной надежности мажоритарного объекта необходимо построить высоконадежный восстанавливающий орган.

## 3. Отказобезопасность систем с гибридными мажоритарными архитектурами

Недостаток мажоритарного резервирования заключается в нарушении алгоритма при отказе двух

из трех компонент (для троичной мажоритарной схемы), а в общем случае при отказе $n + 1$ компонент (для $n$-ированного мажоритарного объекта в системе). При нечетном числе компонент $N = 2n + 1$ объект еще сохраняет работоспособность при отказе $n$ компонент; если же откажет еще хотя бы одна компонента, то объект теряет свои функциональные возможности, хотя имеется $n$ исправных компонент. Для устранения этого существенного недостатка вводится в состав системы минимальная дополнительная избыточность.

Рассмотрим возможную архитектуру построения критически важной системы с гибридным мажоритарным резервированием.

***Архитектура (2oo3)P*** (для SIL3/4). Гибридное мажоритарное резервирование основывается на введении в состав мажоритарного объекта дополнительной однотипной резервной компоненты. Эта компонента не подключена к восстанавливающему органу. Она предназначена для замещения отказавших компонент из состава исходного мажоритарного объекта. Показатели структурной надежности данного объекта определяются на основании его критерия отказа, который определяется так. При трех основных и одном резервном однотипном компоненте обработки информации структурный отказ объекта наступает при наличии двух отказавших компонент или при наличии одного исправного основного компонента и также исправного резервного компонента, но подключение резервного вместо отказавшего основного компонента не было успешным (либо по причине пропуска отказа, либо по причине отказа переключающего устройства, либо из-за несвоевременного переключения на резерв).

Вероятность безотказной работы резервированных компонент троичного гибридного мажоритарного объекта может быть определена по формуле:

$$P_{(2oo3)P}(t) = P^3(t) + 3P^2(t)\cdot g(t)\cdot\left[1 + g(t)\cdot\gamma\right],$$

где $\gamma$ – вероятность успешного переключения на резерв.

При экспоненциальном законе распределения отказов компоненты средняя наработка до отказа системы [8]:

$$T_{(2oo3)P} = \int_0^\infty P_{(2oo3)P}(t)dt = \frac{10 + 3\gamma}{12\lambda}.$$

При успешных переходах на резерв ($\gamma \to 1$) средняя наработка до структурного отказа объекта может быть повышена до 30%. Действительно, при этих условиях $T_{(2oo3)P} = \dfrac{13}{12\lambda}$ и $T_{(2oo3)P} / T_{2oo3} = 1,3$.

***Архитектура 2oo4*** (для SIL4, см. табл. 1) основывается на применении адаптивных ВО, которые изменяют свой порог по мере выхода компонентов из строя. Например, при использовании мажоритарного резервирования с логикой 3/4 в случае отказа компоненты производится переход на логику 2/3.

Вероятность безопасной работы системы с этой архитектурой безопасности:

$$P_{2oo4}(t) = P^4(t) + 4P^3(t)G(t) + 6P^2(t)G^2(t).$$

При экспоненциальном законе распределения отказов компоненты критически важной системы средняя наработка до отказа системы:

$$T_{2oo4} = \int_0^\infty P_{2oo4}(t)\,dt = \frac{13}{12\lambda}.$$

Таким образом, архитектуры отказобезопасности с избыточностью типа **(2oo3)P** и **2oo4** обеспечивают практически одинаковый уровень средней наработки до отказа системы.

## Заключение

Критически важные системы высокоскоростного движения поездов представляют собой киберфизические системы, содержащие вычислительную компоненту в составе с прикладной логикой, прикладной вычислительной платформой и системной вычислительной платформой; прикладную компоненту с целевыми физическими объектами и процессами, датчики и исполнительные устройства. Для обеспечения отказобезопасности этих систем требуется тщательный отбор наиболее рациональных их архитектур.

Анализ надежности широко распространенной на практике архитектуры безопасности **2oo3** аналитически и численно показал, что с помощью мажоритарной логики удается существенно повысить достоверность результатов (среднее время до функционального отказа мажорированной системы в 2 раза превышает этот показатель в исходном объекте). Вместе с тем, безотказность системы, а, следовательно, ее отказобезопасность, ниже, чем у исходного объекта. Поэтому такая архитектура приемлема не выше уровня SIL3. Возможно для обеспечения этого уровня отказобезопасности предпочтение отдавать альтернативной архитектуре **(1oo2)P** вследствие отсутствия в ней ВО и переключающих устройств. Она формируется из двух параллельно работающих компонент, каждая из которых построена по схеме постоянного дублирования. Однако при этом не следует забывать, что в такой системе сохраняется риск ложного срабатывания.

Показано, что для обеспечения отказобезопасности на уровне SIL4 можно применять гибридные мажоритарные архитектуры (**2oo3)P** или **2oo4**. Вместе с тем следует учитывать, что существенную часть мажоритарных структур отказобезопасности критически важных систем составляют переключательные схемы, обеспечивающие отключение отказавших и включение резервных компонент. Это обстоятельство отрицательно сказывается на эффективности мажоритарного резервирования, поскольку связано с применением дополнительных средств и процедур.

Недостатком как аппаратного, так и программного способов мажорирования является значительное количество оборудования, даже в минимальном варианте при $n = 1$ (троирование). Другим недостатком способов мажорирования являются значительные потери производительности. При аппаратной реализации потеря производительности связана с необходимостью синхронизации процессов в резервированных каналах. При программной реализации быстродействие системы снижается из-за затрат времени на обмен информацией между каналами.

Причина этого недостатка состоит в том, что и при аппаратной, и при программной организации механизм маскирования сбоев, т.е. голосование, определение неисправного канала, его блокирование и последующее включение в нормальную работу, используется в каждом такте работы системы вне зависимости от наличия или отсутствия сбоев. Эти временные потери при практической реализации достигают 30-50%. К недостаткам мажорирования при его реализации следует отнести также большое количество связей между каналами и определенные трудности при проектировании.

Указанные ограничения оказывают негативное, но не определяющее влияние на выбор приемлемой архитектуры отказобезопасности. Их следует учитывать для каждого конкретного объекта и условий его применения.

## Список литературы

1. IEC 62278-3:2025. Железные дороги. Технические требования и демонстрация надежности, эксплуатационной готовности и безопасности.

2. IEC 62278-1:2025. Железнодорожные приложения – спецификация и демонстрация надёжности, доступности, ремонтопригодности и безопасности (RAMS) – Часть 1: Общий процесс RAMS.

3. ГОСТ 33358-2015 Безопасность функциональная. Системы управления и обеспечения безопасности движения поездов. Термины и определения. М.: Стандартинформ, 2018. III, 15 с.

4. Платунов А., Пинкевич В. Создание киберфизических систем: проблемы подготовки ИТ специалистов // Control Engineering (Россия). 2021. № 3(93). С. 64-70.

5. Шубинский И.Б. Функциональная безопасность систем управления на железнодорожном транспорте: монография / И.Б. Шубинский, Е.Н. Розенберг. М.; Вологда: Инфра-Инженерия, 2023. 360 с.

6. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберзащищенности систем управления // Надежность. 2014. № 2. С. 88-100.

7. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: Изд. Журнала «Надежность», 2012. 296 с.

8. Шубинский И.Б. Отказоустойчивость и отказобезопасность систем управления: монография. Москва; Вологда: Инфра-Инженерия, 2026. 340 с.

## References

1. IEC 62278-3:2025. Railways – Specification and demonstration of reliability, availability, and safety.

2. IEC 62278-1:2025. Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS process.

3. GOST 33358-2015 Functional safety. Control and safety systems for train operation. Terms and definitions. Moscow: Standartinform; 2018. (In Russ.)

4. Platunov A., Pinkevich V. [Creating cyberphysical systems: matters of IT worker training]. *Control Engineering (Russia)* 2021;3(93):64-70. (In Russ.)

5. Shubinsky I.B., Rozenberg E.N. [Functional safety of control systems in railway transportation]. Moscow; Vologda: Infra-Inzheneria; 2023. (In Russ.)

6. Gapanovich V.A., Rozenberg E.N., Shubinsky I.B. Some concepts of fail-safety and cyber protection of control systems. *Dependability* 2014;2:95-100.

7. Shubinsky I.B. [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal Publishing; 2012. (In Russ.)

8. Shubinsky I.B., Rozenberg E.N. [Fail-safety of control systems: a monograph]. Moscow; Vologda: Infra-Inzheneria; 2026. (In Russ.)

## Сведения об авторах

**Гапанович Валентин Александрович,** кандидат технических наук, президент Ассоциации «Объединение производителей железнодорожной техники».

**Шубинский Игорь Борисович,** доктор технических наук, профессор, главный эксперт АО «НИИАС», 119333, Москва, ул. Вавилова 48, кв.339.

## About the authors

**Valentin A. Gapanovich,** Candidate of Engineering, President of Association “Union of Industries of Railway Equipment”.

**Igor B. Shubinsky,** Doctor of Engineering, Professor, Chief Expert, JSC NIIAS, 48 Vavilova St., app. 339, 119333, Moscow.

## Вклад авторов

**Гапанович В.А.** сформулировал задачи обеспечения отказобезопасности критически важных объектов высокоскоростного движения как киберфизических систем, определил требования к их функциональной безопасности.

**Шубинский И.Б.** выполнил аналитическую и численную оценки функциональной надежности и отказобезопасности систем с мажоритарной логикой, в том числе гибридных мажоритарных систем.

## Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.