

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Главный редактор:

Шубинский Игорь Борисович – доктор технических наук, профессор, эксперт Научного совета при Совете Безопасности РФ, генеральный директор ЗАО «ИБТранс» (Москва, Россия)

Заместители главного редактора:

Шебе Хендрик – доктор естественных наук, главный эксперт по надежности, эксплуатационной готовности, ремонтпригодности и безопасности, TÜV Rheinland InterTraffic (Кёльн, Германия)

Ястребенецкий Михаил Анисимович – доктор технических наук, профессор, начальник отдела Национальной академии наук Украины «Государственный научно-технический центр ядерной и радиационной безопасности» (Харьков, Украина)

Ответственный секретарь:

Замышляев Алексей Михайлович – доктор технических наук, заместитель Генерального директора АО «НИИАС» (Москва, Россия)

Технический редактор:

Новожилов Евгений Олегович – кандидат технических наук, начальник отдела АО «НИИАС» (Москва, Россия)

Председатель редакционного совета:

Розенберг Игорь Наумович – доктор технических наук, профессор, Генеральный директор АО «НИИАС» (Москва, Россия)

Сопредседатель редакционного совета:

Махутов Николай Андреевич – доктор технических наук, профессор, член – корреспондент РАН, главный научный сотрудник Института машиноведения им. А.А. Благонравова, председатель Рабочей группы при Президенте РАН по анализу риска и проблеме безопасности (Москва, Россия)

РЕДАКЦИОННЫЙ СОВЕТ:

Аврамович Зоран Ж. – доктор технических наук, профессор, профессор Института транспорта Университета г. Белград (Белград, Сербия)

Баранов Леонид Аврамович – доктор технических наук, профессор, заведующий кафедрой «Управления и защиты информации» Российского университета транспорта (МИИТ) (Москва, Россия)

Бочков Александр Владимирович – кандидат технических наук, заместитель начальника отдела анализа и ранжирования объектов контроля Управления «Аналитический центр», ООО «Газпром газнадзор» (Москва, Россия)

Бочков Константин Афанасьевич – доктор технических наук, профессор, научный руководитель – заведующий НИЛ «Безопасность и ЭМС технических средств (БЭМС ТС), УО «Белорусский государственный университет транспорта» (Гомель, Белоруссия)

Гапанович Валентин Александрович – кандидат технических наук, президент НП «Объединение производителей железнодорожной техники» (Москва, Россия)

Каштанов Виктор Алексеевич – доктор физико-математических наук, профессор, профессор департамента прикладной математики Национального исследовательского университета «Высшая школа экономики» (Москва, Россия)

Климов Сергей Михайлович – доктор технических наук, профессор, начальник управления 4 Центрального научно-исследовательского института Министерства обороны РФ (Москва, Россия)

Кофанов Юрий Николаевич – доктор технических наук, профессор, профессор Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики» (Москва, Россия)

Кришнамурти Ачътха – доктор физико-математических наук, профессор, почетный профессор Департамента математики Университета науки и технологий (Кочин, Индия)

Лецкий Эдуард Константинович – доктор технических наук, профессор, заведующий кафедрой «Автоматизированные системы управления» Российского университета транспорта (МИИТ) (Москва, Россия)

Нетес Виктор Александрович – доктор технических наук, профессор ФГБОУ ВО «Московский технический университет связи и информатики» (МТУСИ) (Москва, Россия)

Папич Любиша – доктор технических наук, профессор, директор Исследовательского центра по управлению качеством и надежностью (DQM), (Приевор, Сербия)

Поляк Роман А. – доктор физико-математических наук, профессор, приглашенный профессор Школы математических наук технологического Университета Технион (Хайфа, Израиль)

Соколов Борис Владимирович – доктор технических наук, профессор, заместитель директора по научной работе Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), (Санкт-Петербург, Россия)

Уткин Лев Владимирович – доктор технических наук, профессор, заведующий кафедры «Телематика» (при ЦНИИ РТК) Санкт-Петербургского политехнического университета Петра Великого (Санкт-Петербург, Россия)

Юркевич Евгений Викторович – доктор технических наук, профессор, Главный научный сотрудник лаборатории Технической диагностики и отказоустойчивости ИПУ РАН. (Москва, Россия)

УЧРЕДИТЕЛЬ ЖУРНАЛА:

ООО «Журнал «Надежность»

Зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Регистрационное свидетельство ПИ № 77-9782 от 11 сентября 2001 года.

Официальный печатный орган Российской академии надежности

Издатель журнала

ООО «Журнал «Надежность»

Генеральный директор

Дубровская А.З.

Адрес: 109029, г. Москва,

ул. Нижегородская, д. 27, стр. 1, оф. 209

ООО «Журнал «Надежность»

www.dependability.ru

Отпечатано в ОАО «Областная типография

«Печатный двор». 432049, г. Ульяновск,

ул. Пушкирева, 27.

Подписано в печать 08.06.2019

Объем , Тираж 500 экз, Заказ №

Формат 60х90/8, Бумага глянцев

Статьи рецензируются.

Статьи опубликованы в авторской редакции. Мнение членов редакционного совета может не совпадать с точкой зрения авторов публикаций. Перепечатка материалов допускается только с письменного разрешения редакции. Рукописи не возвращаются.

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ» (АО «НИИАС») И ООО «ИЗДАТЕЛЬСКИЙ ДОМ «ТЕХНОЛОГИИ»

СОДЕРЖАНИЕ

Структурная надежность. Теория и практика

- Геча В.Я., Барбул Р.Н., Сидняев Н.И., Бутенко Ю.И.** Методология оценки надежности космических аппаратов при проектной и конструкторской проработке 3
- Антонов А.В., Чепурко В.А., Черняев А.Н.** Исследование модели учета отказов по общей причине бета-фактора 9
- Михайлов В.С.** Оценка гамма-процентного срока для биномиального плана испытаний 18

Функциональная надежность. Теория и практика

- Иванов А.И., Куприянов Е.Н., Туреев С.В.** Нейросетевое обобщение классических статистических критериев для обработки малых выборок биометрических данных 22
- Розенберг Е.Н., Коровин А.С., Пенькова Н.Г.** Модель оценки эффективности диагностических средств в бортовых устройствах 28

Функциональная безопасность и живучесть. Теория и практика

- Баранов Л.А., Кульба В.В., Шелков А.Б., Сомов Д.С.** Индикаторный подход в управлении безопасностью объектов инфраструктуры железнодорожного транспорта 33
- Ефимов В.В.** К вопросу о терминологии живучести авиационных конструкций 42

Управление рисками. Теория и практика

- Попов В.Г., Сухов Ф.И., Боландова Ю.К.** Экономическая оценка аварийного риска воздействия природных чрезвычайных ситуаций при движении поездов 48
- Гнеденко – Форум** 54

Методология оценки надежности космических аппаратов при проектной и конструкторской проработке

Владимир Я. Геча, Акционерное общество «Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы» имени А.Г. Иосифьяна», Российская Федерация, Москва

Руслан Н. Барбул, Акционерное общество «Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы» имени А.Г. Иосифьяна», Российская Федерация, Москва

Николай И. Сидняев, Московский государственный технический университет им. Н.Э. Баумана, Российская Федерация, Москва

Юлия И. Бутенко, Московский государственный технический университет им. Н.Э. Баумана, Российская Федерация, Москва



Владимир Я. Геча



Руслан Н. Барбул



Николай И.
Сидняев



Юлия И. Бутенко

Резюме. В статье рассматриваются вопросы эксплуатационной надежности космических систем (КС), эффективности сложных многоцепочных систем, использования резервирования при конструировании космических аппаратов (КА). Представлены методики прогнозирования надежности создаваемых устройств, проектирование устройств с заданной надежностью и сравнение надежности различных КС. С этой целью излагаются фундаментальные вопросы из теории надежности для проектирования КС, методы сбора и обработки данных о надежности аппаратуры по результатам эксплуатации и специальных испытаний на надежность. Разработаны методы, математические модели и проведен анализ структуры аппаратуры на этапе проектирования и при изготовлении. Приведены расчетные соотношения при различных видах резервирования в испытаниях, продления сроков эксплуатации блоков КА, основа которых – методология оценки остаточного ресурса. Систематизированы и изучены существующие методы анализа надежности. Изложены проблемы неопределенности информации по входным данным при расчетах классическими методами. Изучено влияние отклонения внешних воздействий от номинальных значений, непостоянность интенсивности отказов, нелинейный характер влияния внешних факторов на надежность. Исследован характер влияния внешних факторов на надежность и степень учета факторов в существующих методах. Отмечено, что качественные, организационно-технические (конструктивные и программные) требования по надежности, задаваемые в ТЗ для каждой стадии создания элементов КС в целом, должны выполняться и подтверждаться на соответствующей стадии работ. Представлены методики оценки ресурса технических объектов, среди которых важное место занимают методики, основанные на физических предположениях расходования ресурса. Отмечена важность экономического аспекта исследования проблемы продления сроков эксплуатации КС.

Ключевые слова: надежность, методики, ресурс, проектирование, космический аппарат, оценка ресурса.

Формат цитирования: Геча В.Я., Барбул Р.Н., Сидняев Н.И., Бутенко Ю.И. Методология оценки надежности космических аппаратов при проектной и конструкторской проработке // Надежность. 2019. №2. С. 3-8. DOI: 10.21683/1729-2646-2019-19-2-3-8

Введение

Стадии проектирования, начиная с разработки технического задания на систему и кончая выпуском технической документации на опытное производство, являются ключевыми в общей проблеме обеспечения надежности космического аппарата (КА). Важной работой, регламентирующей взаимоотношения всех участников разработки КА, является обоснование программы обеспечения надежности (ПОН) изделия в целом, его составных частей и элементов, а также выработка и согласование порядка подтверждения требований по надежности на всех стадиях создания [1-4]. С этой целью используют модели ПОН, типовые ПОН и модели (процедуры) подтверждения надежности. После выбора основных проектных, схемных и конструкторско-технологических решений перед окончательным оформлением проекта службой надежности предприятия совместно с подразделениями-разработчиками осуществляется оценка (экспертиза) результатов проектирования с позиций обеспечения надежности и корректировка принятых решений [5-8].

КА представляет собой сложный многокомпонентный комплекс, содержащий в себе как аппаратные, так и программные средства [9-12]. Соответственно, возникает необходимость оперативного контроля их характеристик и анализа состояния в процессе эксплуатации. Надежность является одной из важнейших характеристик технической системы [3]. Согласно ГОСТ, под надежностью принято понимать свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях эксплуатации, технического обслуживания, ремонта, хранения и транспортирования [4]. Поскольку КА имеет сложную структуру (а, следовательно, и сложный характер взаимосвязей между отдельными компонентами), усложняется и сам процесс получения численных значений показателей надежности [5-8].

Методологические аспекты и цели поставленной задачи

Для предупреждения и выявления отказов конструктивного, производственного и эксплуатационного характера и защиты от их последствий элементов системы применяют различные методы и средства. Если в результате предварительных исследований эффективности системы определен объем потребности в данном виде изделий и требуемый уровень гарантии выполнения задач при их применении, тогда минимально необходимый уровень надежности изделий можно определить однозначно в результате оценки и минимизации суммарных затрат ресурсов на создание и применение, т. е. на выполнение программы в целом [6, 7].

Разработка системы ограниченного применения (десятки образцов). В этом случае приходится учитывать все составляющие суммарных затрат: затраты на раз-

работку системы, на изготовление и на эксплуатацию всего парка изделий, обеспечивающих выполнение задачи не менее $N_{тр}$ раз (потребное количество изделий) с гарантией не ниже $\gamma_{тр}$ [9-12]. Задание требований по надежности системы и ее элементов включает:

- выбор номенклатуры показателей надежности;
- нормирование надежности (установление требуемых количественных значений показателей надежности элементов системы);
- нормирование доверительных вероятностей или средних квадратичных отклонений, с которыми нормативные значения показателей надежности системы должны быть подтверждены к моменту завершения государственных испытаний;
- формирование для элементов системы организационных и технических требований по обеспечению надежности;
- установление порядка подтверждения требования по надежности по стадиям создания элементов системы.

В общей постановке задача нормирования надежности формулируется следующим образом [8, 9, 13].

Пусть КА состоит из N элементов, объединенных определенной структурой и выполняющих определенные функции. При этом известны [9, 10, 14]: вид совместной плотности распределения моментов отказов элементов КА (τ_i), $f_s\{\tau_i; i=1, N\}$; требуемое значение (или ряд значений) показателя надежности системы P ; функции связи надежности и рассматриваемых факторов $\Phi_l\{P_i; i=1, N, \Phi_v, v=1, S\}$, $l=1, L$; функции распределения времени безотказной работы составных частей $F_i = P_i\{f(\tau_i)\}$, $i=1, N$; целевая функция (функционал) $g = g\{P_i, i=1, N\}$, где P_i – точечное значение оценки надежности i -го элемента; Φ_v – рассматриваемый v -й фактор; S – число рассматриваемых факторов; L – число функций связи.

Необходимо найти такие значения надежности элементов, которые оптимизируют целевую функцию g [1, 9].

Если необходимо спроектировать КА с минимальной стоимостью или массой, то в качестве целевой функции выбирают стоимость или массу $g = C$, $C = C\{P_i, i=1, N\}$, или $g = M$, $M = M\{P_i, i=1, N\}$.

В процессе решения отыскивают вектор $P = \{P_1, P_2, \dots, P_i, \dots, P_N\}$, минимизирующий C или M , т. е. $C(\bar{P}) = \min C(\bar{P})$; $\bar{P} = \{P_1, P_2, \dots, P_i, \dots, P_N\}$, или $M(\bar{P}) = \min M(\bar{P})$; $\bar{P} = \{P_1, P_2, \dots, P_i, \dots, P_N\}$ при $\Phi(P) \geq \Phi_0$. Если ставится задача максимизации функции $\Phi(P)$ при заданных ограничениях на стоимость (или массу), то $g = \Phi$; $\Phi = \Phi\{P_i, i=1, N\}$. Решают задачу отыскания вектора P , максимизирующего $\Phi(P)$, т. е. $\Phi(\bar{P}) = \max \Phi(P)$ при $C(\bar{P}) \leq C_0$, или $\Phi(\bar{P}) = \max \Phi(P)$ при $M(\bar{P}) \leq M_0$. Часто нормирование производят при условии не только выполнения требований по надежности системы, но и требований по безопасности. Тогда задачу решают, используя в качестве функции $\Phi(\bar{P})$ функцию безопасности, т. е. $B = \Phi(\bar{P})$, а затем проверяют условие $B = \Phi(\bar{P}) \geq P_B$. Если оно выполняется, то решение зада-

чи окончено, если не выполняется, то решение задачи продолжают, начиная с вектора $P = \bar{P}_p$, т. е. вектора, удовлетворяющего решению на первом этапе.

Методы конкретной реализации задач

При создании изделий космической техники, не имеющих аналогов и прототипов, вместо жестких нормативных значений показателей надежности разрабатывают алгоритмы и методики задания и нормирования количественных требований по надежности, учитывающие специфику использования КА и элементов [15, 16], а также реальные ограничения.

Рассмотрим область применения вероятностных показателей надежности как основы для обеспечения гарантий в зависимости от объема программы применения КА [4, 5, 7]. Пусть целью единичной программы создания и применения спутника одноразового использования является удовлетворение потребности в $N_{тр}$ таких изделий. Необходимое время работы спутников задано, в качестве показателя надежности изделия используется вероятность безотказной работы R . Известна зависимость уровня надежности изделия от затрат в рамках программы обеспечения надежности $R = R_1 R_2 R_3$, где $R_1 = 1 - (1 - R_{10}) \exp[-\alpha_1 (C_1 - C_{10})]$ – составляющая надежности, учитывающая влияние отказов комплектующих изделий с учетом резервирования; $R_2 = 1 - (1 - R_{20}) \exp[-\alpha_2 (C_2 - C_{20})]$ – составляющая надежности, учитывающая уровень производства и контроля готовой продукции; $R_3 = 1 - (1 - R_{30}) \exp[-\alpha_3 (N_{от} - N_{от0})]$ – составляющая надежности, учитывающая уровень отработанности; R_{10}, R_{20}, R_{30} – начальные (минимальные) уровни составляющих R_1, R_2, R_3 , соответствующие минимальным реализуемым затратам $C_{10}, C_{20}, N_{от0}$ средств C_1, C_2 и изделий $N_{от}$, затраченных на экспериментальную отработку; $\alpha_1, \alpha_2, \alpha_3$ – параметры, определяющие темп роста составляющих показателя R при увеличении затрат.

Возможные варианты решений и стратегий строятся с учетом того, что обеспечить достижение поставленной цели можно как за счет увеличения расхода средств на обеспечение более высокого уровня надежности каждого образца, так и за счет расширения программы изготовления изделий [14].

Так как при изготовлении N КА число КА N_y успешно выполнивших свою задачу, случайно, речь может идти об обеспечении практической гарантии с уровнем γ , где $\gamma = P\{N_y \geq N_{тр}\}$. Каждое решение задается вектором составляющих R_1, R_2, R_3 или соответствующих затрат $C_1, C_2, N_{от}$, что однозначно определяет уровень R . Для заданных γ и $N_{тр}$ с учетом известного R однозначно можно определить число изготавливаемых КА $N_{Г} = f(N_{тр}, \beta, R)$, гарантирующих успешную реализацию программы. Суммарные затраты на реализацию программы C_{Σ} могут быть определены на основе зависимости $C_{\Sigma} = (C_1 + C_2)(N_{от} + N_{Г})$. Смысл рациональности

(оптимальности) принимаемого решения при задании необходимого уровня надежности изделия и выделении средств на обеспечение надежности заключается в минимизации суммарных затрат разработку и изготовление необходимого количества КА [11, 15], гарантирующего успешную работу $N_y \geq N_{тр}$ изделий. В качестве множества исходов используем пространство элементарных событий. Каждое из элементарных событий ω_i состоит в том, что в результате применения N КА произошло ровно $N_y = i$ успехов. С точки зрения достижения поставленной цели все множество исходов W можно разделить на два подмножества W_1 и W_2 такие, что

$$\forall (i = 0, 1, \dots, N) (w_i \in W_1) \leftrightarrow (i \geq N_{тр});$$

$$\forall (i = 0, 1, \dots, N) (w_i \in W_2) \leftrightarrow (i < N_{тр}).$$

С учетом этого вероятность события $w_i \leftrightarrow \{N_y = i\}$ при известной вероятности безотказной работы КА определяют по формуле [4]:

$$P\{w_i\} = C_N^i R^i (1 - R)^{N-i}.$$

Эта формула задает вероятностную меру на пространстве W . Событие W_1 является объединением всех ω_i при $i \geq N_{тр}$, поэтому его вероятность определяется как сумма вероятностей этих элементарных событий

$$P\{W_1\} = \sum_{i=N_{тр}}^N C_N^i R^i (1 - R)^{N-i}.$$

Эта вероятность и дает уровень практической гарантии успешного выполнения программы. Для обеспечения заданного уровня гарантии γ при известных значениях R и $N_{тр}$ можем увеличивать N и этим самым заново определять пространство W_1 до тех пор, пока не добьемся выполнения условия $P\{W_1\} \geq \gamma$ [2]. При этом величина N и будет равна искомому значению $N_{Г}$. Таким образом, получим возможные пути построения функционального соответствия $\phi: R \rightarrow N$. Если множество R принять за пространство стратегий, среди которых необходимо выбрать значение $R_{оп}$, обеспечивающее минимум суммарных затрат на про реализацию программы $C_{\Sigma \min}$, соответствие ϕ решает часть задачи: для каждого R определяет $N_{Г}$. Решение усложняется тем, что надежность R может быть обеспечена различными сочетаниями составляющих R_1, R_2, R_3 . В каждом частном случае может быть поставлена и решена задача вспомогательной оптимизации, например, найти вектор R_1, R_2 , обеспечивающий $R' = R_1 R_2$ при минимуме стоимости $C = C_1 + C_2$. Описание процедуры поиска экстремума приведено в работах [2, 9] в составе программы, определяющей зависимость удельных затрат $C_{уд} = C_{\Sigma} / N_{тр}$ и удельных нормированных затрат $C_{уд.н} = C_{уд} / C_0$, где $C_0 = C_{10} + C_{20}$, от объема потребности $N_{тр}$ для конкретных вариантов исходных данных [11]. Кроме этого, по результатам вычислений может быть определена доля

затрат на компенсацию статистической неустойчивости результата относительно математического ожидания

$$\Delta C_\gamma = \frac{C}{C_\Sigma} \left(N_\Gamma - \frac{N_{\text{тр}}}{R} \right),$$

а также доля затрат на обеспечение надежности

$$\Delta C_R = 1 - \Delta C_\gamma - \frac{C_0}{C_\Sigma} (N_{\text{тр}} + N_{\text{от0}}).$$

Анализ последних двух формул позволяет выделить области значений массовости продукции с различными возможностями использования вероятностных требований в качестве основы для обеспечения гарантии успеха [1, 4, 12]. Для изделий массового производства ($N_{\text{тр}} > 10^3$) дополнительные затраты на обеспечение гарантированного результата, компенсирующие статистическую неустойчивость случайных явлений относительно средних, составляют единицы процентов от суммарной стоимости программы и незначительную часть суммарных расходов на программу обеспечения надежности. Для изделий серийного производства ($N_{\text{тр}} > 10^2$) затраты на компенсацию неустойчивости составляют до 10% суммарных расходов и порядка 20% расходов по программе обеспечения надежности. Для изделий мелкосерийного производства ($N_{\text{тр}}$ – десятки) затраты на компенсацию неустойчивости составляют до 25% суммарных расходов и до 50% стоимости ПОН. Наконец, для уникальных изделий ($N_{\text{тр}}$ – единицы) затраты на компенсацию статистической неустойчивости путем увеличения объема программы изготовления могут в несколько раз превышать первоначально планируемую стоимость программы, что является явно неприемлемым путем обеспечения гарантированного результата. Результаты анализа показывают возможности использования явления стохастического детерминизма для обеспечения гарантий. В условиях рассмотренного выше примера зависимость достигнутого уровня надежности изделия от затрачиваемых средств предполагается заданной в виде функционального соответствия $\phi: C \rightarrow R$ со свойствами:

$$\forall (s_i, s_j \in S) \exists (w_i = \phi(s_i), w_j = \phi(s_j)) : [w_i, R_w, w_j] \rightarrow [s_i, R_s, s_j],$$

что позволяет однозначно находить наилучшую стратегию распределения затрат, обеспечивающую максимум показателя R с точностью до задания допустимой ошибки процедуры поиска экстремума.

Единственный вид учитываемой неопределенности заключен в неоднозначности функционального соответствия, т. е. в случайности числа успехов. Принцип гарантированного результата позволяет устранить эту неоднозначность путем введения уровня практической гарантии и построения области $f: R \times N \rightarrow N_\Gamma$.

Следующий шаг приближения постановки задачи к реальной жизни состоит в учете неоднозначности соответствия $\phi: C \rightarrow R$, которое в достаточно общем случае может быть задано совместным распределением констант, входящих в соотношения. Последовательное применение принципа гарантированного результата

основано на построении доверительного интервала $[R(C), 1]$ с уровнем практической гарантии обеспечения $\gamma_{\text{об}}$. Причем практическая гарантия успешной реализации программы γ зависит теперь как от гарантии обеспечения $\gamma_{\text{об}}$, так и от гарантии успешного применения $\gamma_{\text{пр}}$: $\gamma = \gamma_{\text{об}} \gamma_{\text{пр}}$. При такой постановке задачи становится актуальным исследование вопроса о целесообразности использования стратегии экспериментального подтверждения достигнутого уровня надежности [2].

Пусть с целью подтверждения некоторого уровня надежности R_n планируется испытать n КА. Результаты каждого исхода испытаний $\{n, m\}$, где m – число успешных испытаний, случайны и в предположении независимости исходов имеют вероятности

$$P\{n, m\} = \binom{n}{m} R_{\text{об}}^{n-m} (1 - R_{\text{об}})^m,$$

где $R_{\text{об}}$ – уровень обеспеченной надежности. Для каждого исхода $\{n, m\}$ можно построить условную плотность байесовской оценки подтвержденного уровня надежности R_n

$$\phi_{\text{усл}}(R_n/n, m) = \frac{R_n^{n-m} (1 - R_n)^m \phi(R_n)}{\int_0^1 R_n^{n-m} (1 - R_n)^m \phi(R_n) dR_n}.$$

Средневзвешенная условная плотность распределения оценки подтвержденного уровня надежности будет:

$$\bar{\phi}_{\text{усл}}(R_n) = (n+1)! n! \times R_{\text{об}}^{n-m} (1 - R_{\text{об}})^m R_n^{n-m} \times \sum \frac{(1 - R_n)^m}{(m!)^2 [(n-m)!]^2}.$$

Используя эту зависимость, можно получить функциональное соответствие $\phi: R_{\text{об}} \times n \times R_n \rightarrow \gamma_n$. Для подтверждения уровня R_n при испытаниях n изделий с надежностью $R_{\text{об}}$ целесообразно использовать зависимость вида:

$$\gamma_n = (n+1) \sum_{m=0}^n R_{\text{об}}^{n-m} (1 - R_{\text{об}})^m \left[\frac{n}{m!(n-m)!} \right]^2 \int_{R_n}^1 z^{n-m} (1-z)^m dz.$$

При больших n (порядка 20 и более) и $m \geq 1$ вычисление γ_n можно упростить, используя нормальную аппроксимацию апостериорной плотности распределения с дисперсией $\sigma^2 = R_{\text{об}}(1 - R_{\text{об}})/n$. Так, например, результаты решения задачи выбора оптимальных значений $R_{\text{об}}$, n , γ_n , C , N_Γ для уровня гарантии $\gamma = 0,9$ для различных объемов программы применений изделий свидетельствуют о недостаточной эффективности использования только вероятностных показателей для планирования программ создания уникальных изделий. В то же время для программ с объемом применения изделий более сотни для обеспечения гарантии 0,9 оптимальная доля затрат на подтверждение надежности составляет 10%, 5% и 2% полных затрат для объема применения 100, 500 и 2000 шт. соответственно; при этом разница между обеспеченным и подтвержденным уровнем гарантии снижается от 0,15 до 0,06.

Расчеты показывают, что подтверждение надежности более эффективно при больших объемах программ применения. При малых объемах программы целесообразнее расходовать средства на обеспечение надежности. Вид зависимости $R_{06} = f(C)$ определяется на основе опыта реализации ПОН изделий-аналогов, что не исключает возможности появления новых непредвиденных проблем, типов отказов и т.п. В этих условиях целесообразной является разработка в составе ПОН эффективных защитных мероприятий, которые благодаря повышению уровня организации процесса применения КА могут обеспечить решение задачи при большем уровне начальной неопределенности.

Выводы

Предложен новый подход к анализу эксплуатационной надежности многокомпонентных космических систем (КС), позволяющий существенно улучшить и упростить решение задач анализа и контроля надежности. Одним из достоинств разработанной методики является то, что в ситуациях, когда еще не накопилось достаточно статистической информации, источником первоначальных данных для настройки модели надежности являются экспертные суждения, а в дальнейшем – используются данные, поступающие в ходе эксплуатации. Тем самым на всех стадиях жизненного цикла системы удается поддерживать модель надежности в актуальном состоянии.

Систематизированы и изучены существующие методы анализа надежности. Выявлены проблемы недостатка информации при расчетах классическими методами, игнорирование таких факторов, как влияние отклонения режима работы или внешних воздействий от номинальных значений, непостоянность интенсивности отказов, нелинейный характер влияния внешних факторов на надежность. Изучен характер влияния внешних факторов на надежность и степень учета данных факторов в существующих методах. Сформулирована задача анализа надежности. Качественные, организационно-технические (конструктивные и программные) требования по надежности, задаваемые в ТЗ для каждой стадии создания элементов и КС в целом, должны выполняться и подтверждаться на соответствующей стадии работ. Для их подтверждения не требуется статистический эксперимент, и в этом их большое преимущество. Значительному сокращению затрат на экспериментальные исследования КА и вообще созданию высоконадежных изделий на стадиях проектно-конструкторской разработки способствуют создаваемые в отдельных отраслях ракетно-космической отрасли проектные нормы надежности – системы количественных и качественных требований и правил, выполнение которых обязательно при разработке КА. Следует при этом отметить, что предлагаемый метод оценки рассмотрен только для изделий космической техники в составе КС, который может послужить отправной точкой для разработки

частных методик оценки экономической эффективности продления сроков эксплуатации конкретных типов и видов космической техники.

Библиографический список

1. Гнеденко Б.В. Математические методы в теории надежности [Текст] / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. – М.: Наука, 1965. – 524 с.
2. Сидняев Н.И. Теория планирования эксперимента и анализ статистических данных: учебное пособие [Текст] / Н.И. Сидняев. – М.: Издательство Юрайт, ИД Юрайт, 2011. – 399 с.
3. Морозов Д.В., Чермошенцев С.Ф. Методика повышения надежности функционирования системы управления беспилотного летательного аппарата в полете при возникновении отказа в бортовой контрольно-проверочной аппаратуре [Текст] // Надежность. – 2019; – №19(1). – С.30-35.
4. Сидняев Н.И. Модели и методы оценки остаточного ресурса изделий радиоэлектроники [Текст] / Н.И. Сидняев, Г.С. Садыхов, В.П. Савченко – М.: Издательство МГТУ им. Н.Э. Баумана, 2015. – 382 с.
5. Morris S.F. Use and application of MIL-HDBK-217 [Text] / S.F. Morris // Solid Slate Technology. – 1990. – Vol. 33. – No. 6. – Pp. 65-69.
6. Сидняев Н.И. Математическое моделирование оценки надежности объектов сложных технических систем [Текст] / Н.И. Сидняев. // Проблемы машиностроения и надежности машин. – 2003. – № 4. – С.24-31.
7. Brennom T.R. Should us MIL-HDBK-217 be 8888 [Text] / T.R. Brennom // IEEE Trans. Reliab. – 1988. – Vol. 37. – No. 5. – Pp. 474-475.
8. Сидняев Н.И. Обзор и исследование физики отказов для оценки показателей надежности радиоэлектронных приборов современных РЛС [Текст] / Н.И. Сидняев // Физические основы приборостроения. – 2017. – Т. 6. – № 2(23). – С. 4-52.
9. Барлоу Р. Математическая теория надежности [Текст] / Р. Барлоу, Ф. Прошан. – М.: Советское радио, 1969. – 488 с.
10. РД 50-690-89. Методические указания. Надежность в технике. Методы оценки показателей надежности по экспериментальным данным [Текст]. – Введ. 1991-01-01. – М.: Гос. комитет СССР по управлению качеством продукции и стандартам, 1990.
11. Сидняев Н.И. Факторы космической погоды, влияющие на бортовые элементы низкоорбитальных космических аппаратов [Текст] / Н.И. Сидняев, Л.А. Макриденко, В.Я. Геча, В.Н. Онуфриев / Вопросы электромеханики. Труды ВНИИЭМ. Труды Четвертой международной научно-технической конференции «Актуальные проблемы создания космических систем дистанционного зондирования Земли». – М.: АО «Корпорация «ВНИИЭМ», 2016. – С. 90-10.
12. Похабов Ю.П. Что понимать под расчетом надежности уникальных высокоответственных систем при-

менительно к механизмам одноразового срабатывания космических аппаратов [Текст] // Надежность. – 2018; – №4. – С.28-35.

13. **Антонов С.Г., Климов С.М.** Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий [Текст] // Надежность. – 2017. – №17(1). – С.32-39.

14. **Сидняев Н.И.** О современных подходах развития теории эффективности космических систем [Текст] / Н.И. Сидняев, В.Я. Геча, Р.Н. Барбул / Системы управления полным жизненным циклом высокотехнологичной продукции в машиностроении: новые источники роста: Всероссийская научно-практическая конференция (Москва, 18 апреля 2018 г.): материалы конференции / Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет). – М.: Издательство МГТУ им. Н.Э. Баумана, 2018. – С. 69-75.

15. **Климов С.М., Поликарпов С.В., Федченко А.В.** Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий [Текст] // Надежность. – 2017. – №17(3). – С.32-40.

16. **Колобов А.Ю., Дикун Е.В.** Интервальные оценки безотказности единичных космических аппаратов [Текст] // Надежность. – 2017. – №17(4). – С.31-35.

Сведения об авторах

Владимир Я. Геча – доктор технических наук, профессор, заместитель генерального директора, Акционерное общество «Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы» имени А.Г. Иосифьяна», Российская Федерация, Москва, e-mail: vniiem@orc.ru, vniiem@vniiem.ru

Руслан Н. Барбул – старший научный сотрудник, заместитель генерального директора по качеству и надежности, Акционерное общество «Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы» имени А.Г. Иосифьяна», Российская Федерация, Москва, e-mail: vniiem@orc.ru, vniiem@vniiem.ru

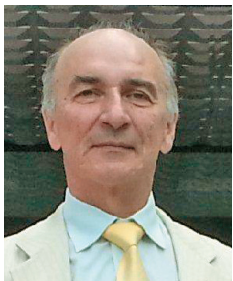
Николай И. Сидняев – доктор технических наук, профессор, заведующий кафедрой, Московский государственный технический университет им. Н.Э. Баумана, Российская Федерация, Москва, e-mail: Sidn_ni@mail.ru

Юлия И. Бутенко – кандидат технических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Российская Федерация, Москва, e-mail: iuliabutenko2015@yandex.ru

Поступила: 17.12.2018

Исследование модели учета отказов по общей причине бета-фактора

Александр В. Антонов, АНО ДПО Техническая академия Росатома, Российская Федерация, Обнинск
Валерий А. Чепурко, АО РАСУ, Российская Федерация, Москва
Алексей Н. Черняев, АО РАСУ, Российская Федерация, Москва



Александр В.
Антонов



Валерий А.
Чепурко



Алексей Н.
Черняев

Резюме. Цель. Отказы по общим причинам (ООП) представляют собой зависимые отказы группы из нескольких элементов, происходящие одновременно или в течение короткого промежутка времени (т.е. почти одновременно), вследствие действия одной общей причины (например, резкое изменение климатических условий эксплуатации, затопление помещения эксплуатации и пр.). Зависимый отказ – это множественный отказ нескольких элементов системы, вероятность которого не может быть выражена просто как произведение вероятностей безусловных отказов отдельных элементов. Для расчета вероятностей ООП существуют несколько различных общепринятых моделей: модель греческих букв, альфа-, бета-фактора и различные их вариации. Наиболее простой с точки зрения моделирования зависимых отказов и проведения дальнейших расчетов надежности является модель бета-фактора. Остальные модели при моделировании подразумевают комбинаторный перебор зависимых событий в группе из n событий, который при большом числе n становится трудозатратным. В статье для выбранных структурных схем надежности подробно разобрана методика расчета вероятности отказа системы с учетом ООП для модели бета-фактора. **Цель** данной статьи состоит в подробном анализе методики бета-фактора для трех структурных схем надежности, в исследовании влияния параметров модели на конечный результат, в нахождении ограничений применимости модели бета-фактора. **Методы.** Для выполнения расчетов применялись численные методы решения уравнений, аналитические методы исследования функций. **Выводы.** В статье подробно разобрана методика расчета ненадежности с учетом ООП по модели бета-фактора для трех структурных схем. В первом примере для выбранной структурной схемы из n параллельных элементов с одинаковой надежностью аналитически показано, что учет ООП не обязательно приводит к увеличению ненадежности. Во втором примере с основным соединением из n элементов с одинаковой надежностью показано, что учет ООП в зависимости от значения параметров приводит как к увеличению, так и к уменьшению ненадежности. Обнаружено существование множества значений параметров модели бета-фактора, приводящих к недопустимым значениям вероятности отказа системы. Эти множества значений соответствуют относительно большим значениям параметров модели и, с практической точки зрения, в расчетах реальных систем с высоконадежными составляющими вряд ли достижимы. В третьем примере исследуется классическая схема-мостик с двумя группами ООП. Показано сложное неоднозначное влияние параметров модели бета-фактора на вероятность отказа. Как и во втором примере, обнаружены ограничения на применимость модели бета-фактора.

Ключевые слова: отказ по общей причине, отказ по всевозможным причинам, независимые отказы, зависимые отказы, несовместные события, бета-фактор, функция ненадежности.

Формат цитирования: Антонов А.В., Чепурко В.А., Черняев А.Н. Исследование модели учета отказов по общей причине бета-фактора // Надежность. 2019. №2. С. 9-17. DOI: 10.21683/1729-2646-2019-19-2-9-17

Введение

Современный анализ надежности сложных систем не обходится без учета возможности отказов по общей причине (ООП). ООП – это отказ двух или более конструкций, систем или компонентов вследствие единичного конкретного события или единичной конкретной причины [1]. Одновременный отказ двух или более конструкций, систем или компонентов вызывается определенными недостатками, заложенными в процессе проектирования или производства, ошибками при эксплуатации или в процессе технического обслуживания, которые проявляются в результате воздействия природных явлений, эксплуатационных процессов на атомной станции, действий человека или любых внутренних событий в системе контроля и управления [2]. В качестве примера можно привести блокировку ряда систем безопасности вследствие принятия неправильного решения персоналом на Чернобыльской АЭС. Существующая классификация ООП подразумевает отказы, обусловленные внутренним или внешним воздействием, отказы вследствие ошибок персонала, отказы общего вида из-за общности конструкции или условий работы.

Существует несколько вероятностных методик учета ООП: модели альфа-фактора, греческих букв, бета-фактора и другие. Одна из наиболее простых – модель бета-фактора, которая рассматривает либо единичные независимые отказы элементов группы, объединенные общей причиной (ООП-группы), либо одновременный отказ всех элементов ООП-группы. Остальные модели рассматривают возможность того, что откажут произвольные подгруппы в ООП-группе. В этом случае в зависимости от модели определенным образом находится вектор параметров, соответствующих вероятности ООП подгруппы заданного объема. Поскольку модель бета-фактора подразумевает ООП всей группы одновременно, она содержит единственный параметр β .

Целью данной работы является исследование того, как учет ООП, по модели бета-фактора влияет на вероятность отказа различных структурных схем. Помимо обнаружения зависимости вероятности отказа системы от параметра модели β , в каждом случае проводится анализ вероятности отказа на предмет обнаружения возможных ограничений модели.

ООП в параллельных структурах

Проанализируем надежность параллельной (резервированной) с точки зрения надежности структуры с учетом ООП. Пусть система состоит из n параллельных равнонадежных элементов с вероятностью отказа q каждый. Очевидно, что без учета ООП вероятность отказа системы будет равна q^n .

Предположим, что по общей одинаковой причине могут отказать все n элементов. В этом случае возможны будут следующие события: i_j – независимый отказ j -го элемента, C – зависимый ООП всех элементов.

Согласно предположениям модели бета-фактора, отказ любого элемента группы может произойти либо по независимой, либо по общей, одинаковой для всех элементов, причине, т.е. события i_j и C будут несовместными. При этом вероятности этих событий будут пропорциональны q – вероятности отказа элемента по всевозможным (total) причинам

$$P(C) = \beta q, \quad P(i_j) = (1 - \beta)q, \quad j = 1, \dots, n. \quad (1)$$

Неотрицательный коэффициент пропорциональности β зависит от множества факторов, таких, как структура системы, способ резервирования, условия эксплуатации и т. д. Обычно этот коэффициент достаточно мал и технические системы содержат высоконадежные элементы, т.е. вероятность отказа q тоже мала. В таких условиях применение модели бета-фактора обычно не приводит к парадоксальным или даже невозможным результатам. При относительно больших значениях β и q вполне возможно их получить.

Логическая функция работоспособности с учетом ООП будет выглядеть следующим образом:

$$Y_s = \overline{(i_1 \wedge i_2 \wedge \dots \wedge i_n) \vee C},$$

вероятность отказа $Q(Y_s)$ будет определяться выражением

$$Q(Y_s) = 1 - P(Y_s) = \\ = P(i_1 \wedge i_2 \wedge \dots \wedge i_n) + P(C) = ((1 - \beta)q)^n + \beta q. \quad (2)$$

Исследуем (2) на предмет выявления возможных проблем с проводимыми расчетами.

Поскольку $0 \leq (1 - \beta)q \leq 1$, то $((1 - \beta)q)^n \leq (1 - \beta)q$. Следовательно, вероятность отказа (2) не будет превышать единицы. Т.е. условие нормировки для параллельной структуры будет выполнено.

Проверим общепринятое мнение о том, что учет ООП в резервируемых структурах приводит к увеличению вероятности отказа системы. Для этого определим значения параметров модели ООП, при которых достигается относительное увеличение надежности системы с параллельной структурой при учете ООП. Для увеличения надежности, очевидно, должно выполняться требование

$$Q(Y_s) = ((1 - \beta)q)^n + \beta q < q^n.$$

После упрощения получаем условие:

$$\left(\frac{\beta}{1 - (1 - \beta)^n} \right)^{\frac{1}{n-1}} = q_{\beta, n} < q. \quad (3)$$

При выполнении (3) надежность параллельной структуры, рассчитанная с учетом ООП, будет выше надежности без такого учета. На рисунке 1 приведены

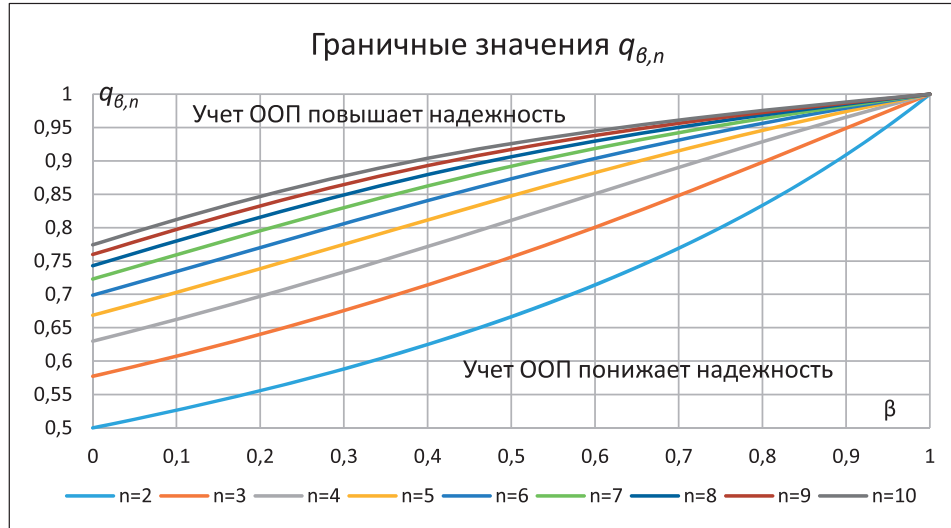


Рисунок 1 – Граничные значения $q_{\beta,n}$.

графики зависимости функции $q_{\beta,n}$ от параметра β при различных n .

Предположим, что параметр $\beta > 0$. Тогда, если вероятность по всевозможным причинам q будет меньше граничной $q_{\beta,n}$, то учет ООП приведет к уменьшению надежности резервируемой системы. Этот эффект обычно и ожидается в качестве естественной реакции модели бета-фактора на учет ООП. В том случае, если $q = q_{\beta,n}$, учет ООП никак не скажется на надежности системы. И, наконец, если $q > q_{\beta,n}$, учет ООП приведет, как ни странно, к увеличению надежности системы. Возьмем, к примеру, $\beta = 1/4$, $q = 3/4$, $n = 2$. Вероятности отказов с учетом и без учета ООП будут равны $((1-\beta)q)^n + \beta q = \frac{129}{256}$ и $q^n = \frac{9}{16} = \frac{144}{256}$ соответственно.

Чтобы разобраться с этим эффектом, рассмотрим крайнюю ситуацию. Предположим, что $q = 1$, т.е. вероятность отказа одного элемента по всевозможным причинам равна 1. В этом случае вероятность отказа без учета ООП будет также равна 1. В случае если $n \geq 2$ и $\beta \in (0,1)$, учет ООП приведет к следующему результату

$$(1-\beta)^n + \beta < 1.$$

Вероятности одного независимого отказа и ООП любого элемента будут равны, соответственно, $(1-\beta)\beta$. Получается, что единичную вероятность отказа модель бета-фактора разложила на две составляющие, обусловленные причиной отказа. Если бы система состояла из одного элемента, то никакого уменьшения вероятности не произошло бы: $(1-\beta) + \beta = 1$. Для резервированной структуры произошло уменьшение вероятности отказа, вызванное «жесткостью» предположений модели бета-фактора. Отказ j -го элемента есть дизъюнкция несовместных событий $i_j \vee C$. Отказ системы – конъюнкция $\bigwedge_{j=1}^n (i_j \vee C)$. Если бы были возможны события вида $i_1 \wedge i_2 \wedge i_n \wedge C_{3,4,\dots,n-1}$ – отказали по независимой причине

1-й, 2-й и n -й элементы, а остальные – по общей причине, и все возможные комбинаторные варианты перебора таких событий, имеющиеся в других моделях учета ООП (модель альфа-фактора, греческих букв и т.д.), то вероятность, возможно, была бы больше. Однако в модели бета-фактора события такого рода невозможны, поскольку, к примеру, невозможно событие $C_{3,4,\dots,n-1}$.

С другой стороны, смену поведения функции надежности (или ненадежности) при различных значениях параметров можно объяснить достаточно просто, проведя качественный анализ функции ненадежности, анализируя, в частности, производные этой функции по q и β .

Производная функции $Q(Y_s)$ по q будет определяться выражением.

$$\frac{\partial Q(Y_s)}{\partial q} = nq^{n-1}(1-\beta)^n + \beta > 0 \text{ при } \beta \in (0,1),$$

т.е. увеличение ненадежности элемента приводит к увеличению ненадежности параллельной системы в целом.

Теперь возьмем производную по другому параметру

$$\frac{\partial Q(Y_s)}{\partial \beta} = -nq^n(1-\beta)^{n-1} + q. \quad (4)$$

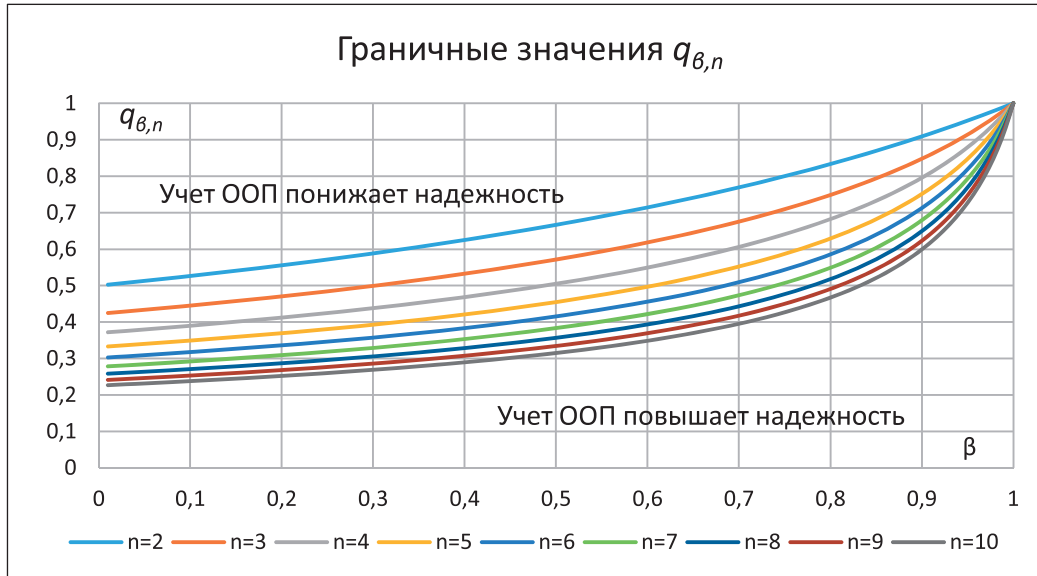
Проанализируем (4). Производная равна 0 в критической точке

$$\beta_{\text{крит.}} = 1 - \frac{1}{q} \left(\frac{1}{n} \right)^{\frac{1}{n-1}} = 1 - \frac{1}{q} \exp \left(-\frac{\ln n}{n-1} \right). \quad (5)$$

Критическая точка достижима в том случае, если $\beta_{\text{крит.}} \in (0,1)$. Условие $\beta_{\text{крит.}} < 1$ очевидно выполняется, а $\beta_{\text{крит.}} > 0$ происходит тогда и только тогда, когда

$$q > \exp \left(-\frac{\ln n}{n-1} \right).$$

Заметим, что

Рисунок 2 – Граничные значения $q_{\beta,n}$.

$$\lim_{\beta \rightarrow 0+} q_{\beta,n} = \lim_{\beta \rightarrow 0+} \left(\frac{\beta}{1 - (1-\beta)^n} \right)^{\frac{1}{n-1}} = \exp\left(-\frac{\ln n}{n-1}\right).$$

Таким образом, при $q \in \left(0, \exp\left(-\frac{\ln n}{n-1}\right)\right]$ производная

(4) для любых значений β будет положительной, т.к. $\frac{\partial Q(Y_s)}{\partial \beta} \Big|_{\beta=1} = q > 0$ и критическая точка находится вне отрезка $[0, 1]$. Следовательно, увеличение β будет приводить, как этого и следовало ожидать, к увеличению ненадежности.

В том случае, если $q \in \left(\exp\left(-\frac{\ln n}{n-1}\right), 1\right]$, будет существовать точка экстремума (5), причем, т.к. производная (4) будет положительной при $\beta=1$, критическая точка будет точкой минимума. Тогда $\frac{\partial Q(Y_s)}{\partial \beta} \Big|_{\beta=0} < 0$ и функция ненадежности будет парадоксально убывать по параметру β . Таково строгое обоснование поведения функции ненадежности.

ООП в последовательных структурах

В этом разделе проанализируем надежность последовательной (основной) с точки зрения надежности структуры с учетом ООП. Пусть система состоит из n последовательных равнонадежных элементов с вероятностью отказа q каждый. Без учета ООП ВБР системы будет равна $P(Y_s) = (1-q)^n$.

Логическая функция работоспособности с учетом ООП будет выглядеть следующим образом

$$Y_s = \overline{i_1 \vee i_2 \vee \dots \vee i_n \vee C}.$$

ВБР с учетом ООП

$$P(Y_s) = P(\overline{i_1} \wedge \overline{i_2} \wedge \dots \wedge \overline{i_n}) - P(C) = (1 - (1-\beta)q)^n - \beta q. \quad (5)$$

Так же, как и в случае с параллельной структурой, учет ООП может как уменьшить, так и увеличить надежность основного соединения. Для определения граничных значений $q_{\beta,n}$, очевидно, необходимо решить алгебраическое уравнение

$$(1 - (1-\beta)q)^n - \beta q = (1-q)^n. \quad (6)$$

На рисунке 2 приведены графики зависимости функции $q_{\beta,n}$ от параметра β при различных n . Решение уравнения (6) получено численным методом деления отрезка пополам.

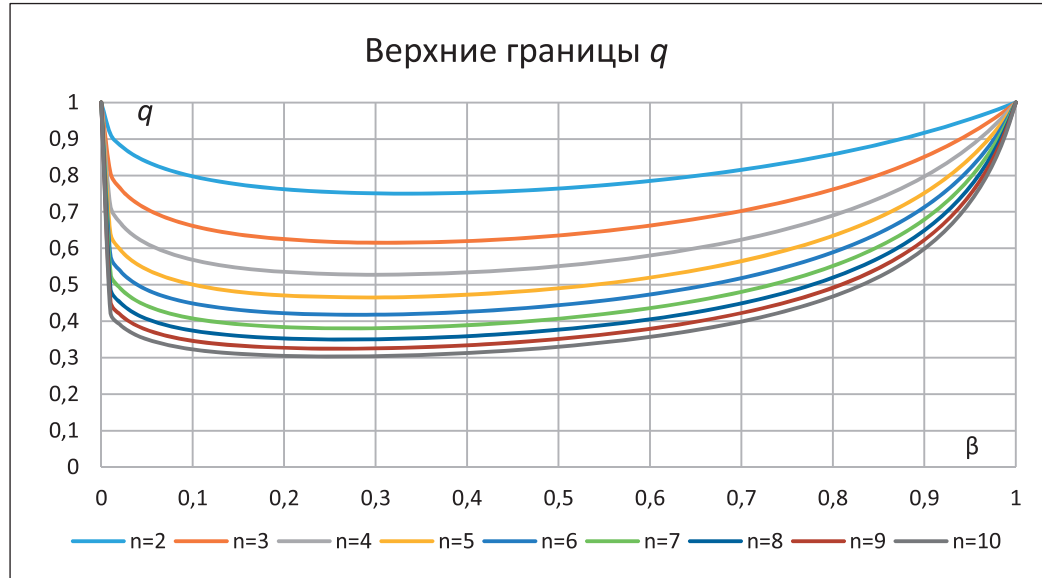
Если вероятность по всевозможным причинам q будет меньше граничной $q_{\beta,n}$, то учет ООП приведет к увеличению надежности последовательной системы. В том случае, если $q = q_{\beta,n}$, учет ООП никак не скажется на надежности системы. И, наконец, если $q > q_{\beta,n}$, учет ООП приведет к уменьшению надежности системы.

Возьмем, как и ранее, к примеру, $\beta = \frac{1}{4}$, $q = \frac{3}{4}$, $n = 2$. Вероятности отказов с учетом и без учета ООП будут равны $1 - (1 - (1-\beta)q)^n + \beta q = \frac{255}{256}$ и $1 - (1-q)^n = \frac{15}{16} = \frac{240}{256}$ соответственно.

Смену поведения функции надежности (или ненадежности) при различных значениях параметров, как и выше, попробуем объяснить, проведя качественный анализ функции ненадежности, анализируя, в частности, производные этой функции по q и β .

Производная функции $Q(Y_s)$ по q будет определяться выражением

$$\frac{\partial Q(Y_s)}{\partial q} = n(1-\beta)(1 - (1-\beta)q)^{n-1} + \beta > 0 \text{ при } \beta \in (0, 1).$$

Рисунок 3 – Допустимые значения q .

Увеличение ненадежности элемента приводит к увеличению ненадежности параллельной системы в целом.

Производная по другому параметру

$$\frac{\partial Q(Y_s)}{\partial \beta} = -nq(1-(1-\beta)q)^{n-1} + q. \quad (7)$$

Проанализируем (7). Производная равна 0 в критической точке

$$\beta_{\text{крит.}} = 1 - \frac{1}{q} \left(1 - \left(\frac{1}{n} \right)^{\frac{1}{n-1}} \right) = 1 - \frac{1}{q} \left(1 - \exp \left(-\frac{\ln n}{n-1} \right) \right). \quad (8)$$

Критическая точка достижима в том случае, если $\beta_{\text{крит.}} \in (0,1)$. Условие $\beta_{\text{крит.}} < 1$ очевидно выполняется, а $\beta_{\text{крит.}} > 0$ происходит тогда и только тогда, когда

$$q > 1 - \exp \left(-\frac{\ln n}{n-1} \right).$$

Таким образом, при $q \in \left(0, 1 - \exp \left(-\frac{\ln n}{n-1} \right) \right]$ производная (7) для любых значений β будет отрицательной,

т.к. $\left. \frac{\partial Q(Y_s)}{\partial \beta} \right|_{\beta=1} = q - nq < 0$ при $n \geq 2$ и критическая точка

находится вне отрезка $[0,1]$. Следовательно, увеличение β будет приводить, как этого и следовало ожидать, к уменьшению ненадежности.

В том случае, если $q > \exp \left(-\frac{\ln n}{n-1} \right)$, будет существовать точка экстремума (8), причем, т.к. производная (7) будет отрицательной при $\beta=1$, критическая точка будет

точкой максимума. Тогда $\left. \frac{\partial Q(Y_s)}{\partial \beta} \right|_{\beta=0} > 0$ и функция не-

надежности будет возрастать по параметру β .

В отличие от параллельной структуры, в последовательной для каждого β существуют предельные значения вероятности отказа по всевозможным причинам для каждого элемента, превышение которых может привести к недопустимым значениям вероятности отказа системы. Для нахождения этих значений необходимо решить уравнение

$$(1-(1-\beta)q)^n - \beta q = 0. \quad (9)$$

Недопустимо высокое значение вероятности отказа напрямую связано с предположениями модели бета-фактора. С точки зрения алгебры логики из появления события C следует то, что не произошло отказов по независимым причинам, т.е. $C \Rightarrow \bar{i}_1 \vee \bar{i}_2 \vee \dots \vee \bar{i}_n$. В этом случае

$$P(\bar{i}_1 \wedge \bar{i}_2 \wedge \dots \wedge \bar{i}_n) \geq P(C), \text{ т.е.}$$

$$(1-(1-\beta)q)^n \geq \beta q.$$

Так, к примеру, в случае $n = 2, 3, 4, 5, 10, 50, 100$ областью допустимых значений вероятности q будет область под графиком кривой на рисунке 3.

Возьмем, как и ранее, к примеру, $\beta=0,1$, $q=0,9$, $n=2$. Вероятности отказов с учетом и без учета ООП будут равны $1-(1-(1-\beta)q)^n + \beta q = 1,0539$ и $1-(1-q)^n = 0,99$ соответственно.

ООП в мостиковой схеме

Исследуем влияние параметров модели бета-фактора в мостиковой схеме. Структура мостиковой схемы представлена на рисунке 4. Предположим, что существует две различные общие причины для выхода из строя сразу нескольких элементов мостика:

– общая причина a , по которой одновременно могут отказать элементы 1 и 2;

– общая причина b , по которой одновременно отказывают элементы 3 и 4.

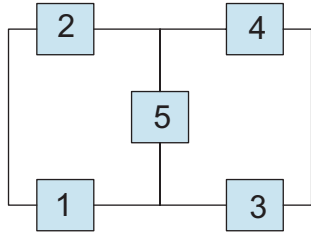


Рисунок 4 – Мостиковая схема

Таким образом, элементы 1 и 2 образуют первую ООП-группу, а элементы 3 и 4 – вторую. Получается так, что эти две группы не содержат одинаковых элементов, хотя, вообще говоря, такое вполне возможно, что один элемент может быть одновременно в нескольких ООП-группах. Такую ситуацию предполагается рассмотреть в следующей работе.

Пусть β_a и β_b – параметры модели бета-фактора в соответствующих группах. В этом случае возможны следующие события: i_1 – независимый отказ 1-го элемента, i_2 – независимый отказ 2-го элемента, C_a – зависимый ООП 1-го элемента и 2-го элемента (группы a) – рисунок 5. Таким же образом, в том же пространстве элементарных исходов можно изобразить события из второй ООП-группы: i_3 – независимый отказ 3-го элемента, i_4 – независимый отказ 4-го элемента, C_b – зависимый ООП 3-го элемента и 4-го элемента (группы b).

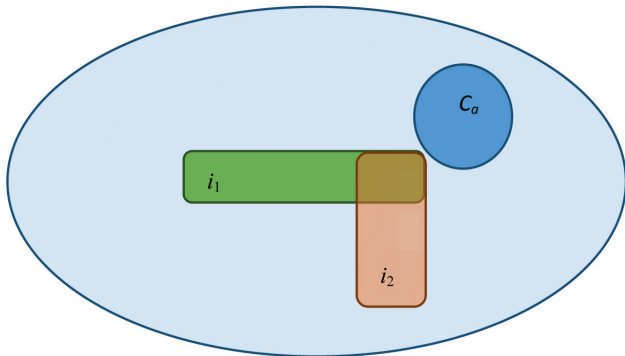


Рисунок 5 – События при ООП

На рисунке 5 изображено возможное взаимное расположение событий одной группы. Важно отметить, что несовместными (взаимоисключающими) будут пары событий: i_1 и C_a , i_2 и C_a , i_3 и C_b , i_4 и C_b . Обозначим событие x_k – k -й элемент работоспособен, $k = 1, \dots, 5$. Тогда $x_1 = i_1 \vee C_a$, $x_2 = i_2 \vee C_a$, $x_3 = i_3 \vee C_b$, $x_4 = i_4 \vee C_b$.

Логическая функция неработоспособности будет выглядеть следующим образом

$$\bar{Y}_s = [x_5 A] \vee [\bar{x}_{51} B], \quad (10)$$

где $A = (\bar{x}_1 \bar{x}_2) \vee (\bar{x}_3 \bar{x}_4)$ и $B = (\bar{x}_2 \vee \bar{x}_4)(\bar{x}_1 \vee \bar{x}_3)$.

Пусть все элементы равнонадежны и вероятности их отказов по всевозможным причинам равны q . В этом случае ненадежность мостика без учета ООП будет равна:

$$Q(Y_s) = q^3(2-q)^2 + q^2(1-q)(2-q^2) = 2q^5 - 5q^4 + 2q^3 + 2q^2. \quad (11)$$

Заменим участвующие в (10) события A и B , содержащие $\bar{x}_1, \bar{x}_2, \bar{x}_3$ и $\bar{x}_4$, на независимые и ООП события:

$$A = (\bar{x}_1 \bar{x}_2) \vee (\bar{x}_3 \bar{x}_4) = (i_1 i_2 \vee C_a) \vee (i_3 i_4 \vee C_b).$$

$$B = (\bar{x}_2 \vee \bar{x}_4)(\bar{x}_1 \vee \bar{x}_3) = (i_1 \vee i_3)(i_2 \vee i_4) \vee C_a \vee C_b.$$

Определим вероятности этих событий:

$$P(A) = f(\beta_a, q) + f(\beta_b, q) - f(\beta_a, q)f(\beta_b, q), \quad (12)$$

где $f(\beta, q) = (1-\beta)^2 q^2 + \beta q$.

Для расчета вероятности события B воспользуемся теоремой сложения, которая в случае несовместных событий одной ООП-группы даст следующий результат

$$P(B) = P((i_1 \vee i_3)(i_2 \vee i_4)) + P(C_a) + P(C_b) - P(i_1 i_2 C_b) - P(i_3 i_4 C_a) - P(C_a C_b) = g^2(\beta_a, \beta_b, q) + \beta_a q + \beta_b q - (1-\beta_a)^2 \beta_b q^3 - (1-\beta_b)^2 \beta_a q^3 - \beta_a \beta_b q^2,$$

где $g(\beta_a, \beta_b, q) = (1-\beta_a)q + (1-\beta_b)q - (1-\beta_a)(1-\beta_b)q^2$.

После подстановки полученных результатов и упрощения получим ненадежность мостика с учетом ООП

$$Q(Y_s) = c_5 q^5 + c_4 q^4 + c_3 q^3 + c_2 q^2 + c_1 q, \quad (13)$$

где коэффициенты полинома определяются выражениями:

$$c_5 = 2(1-\beta_a)^2(1-\beta_b)^2,$$

$$c_4 = (1-\beta_a)(1-\beta_b)(-5+3\beta_a+3\beta_b-\beta_a\beta_b),$$

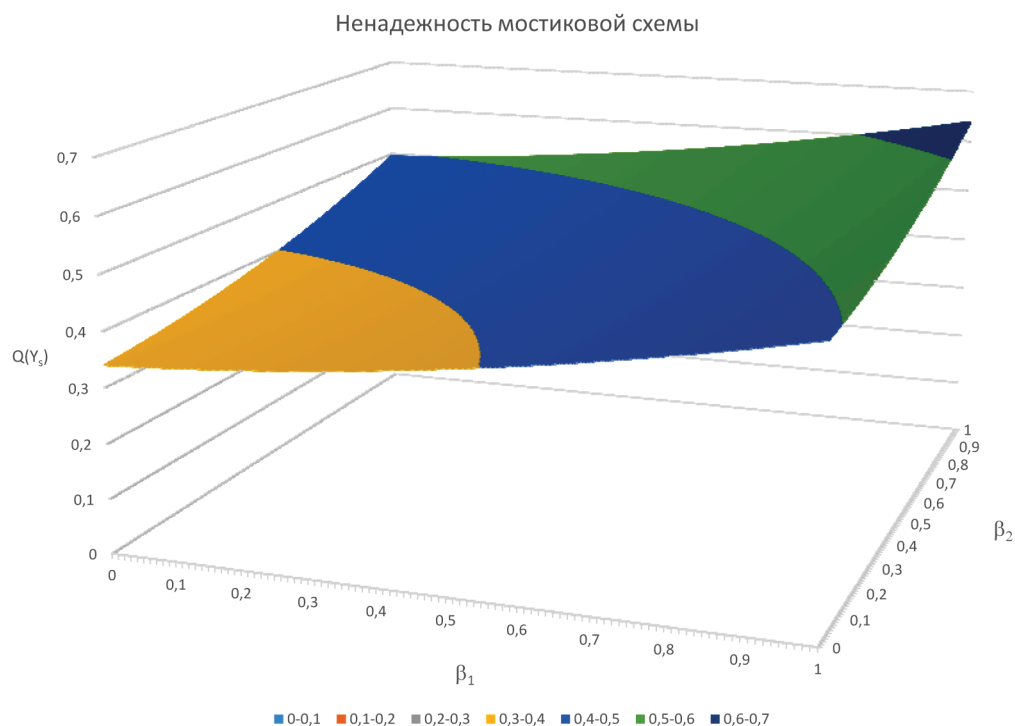
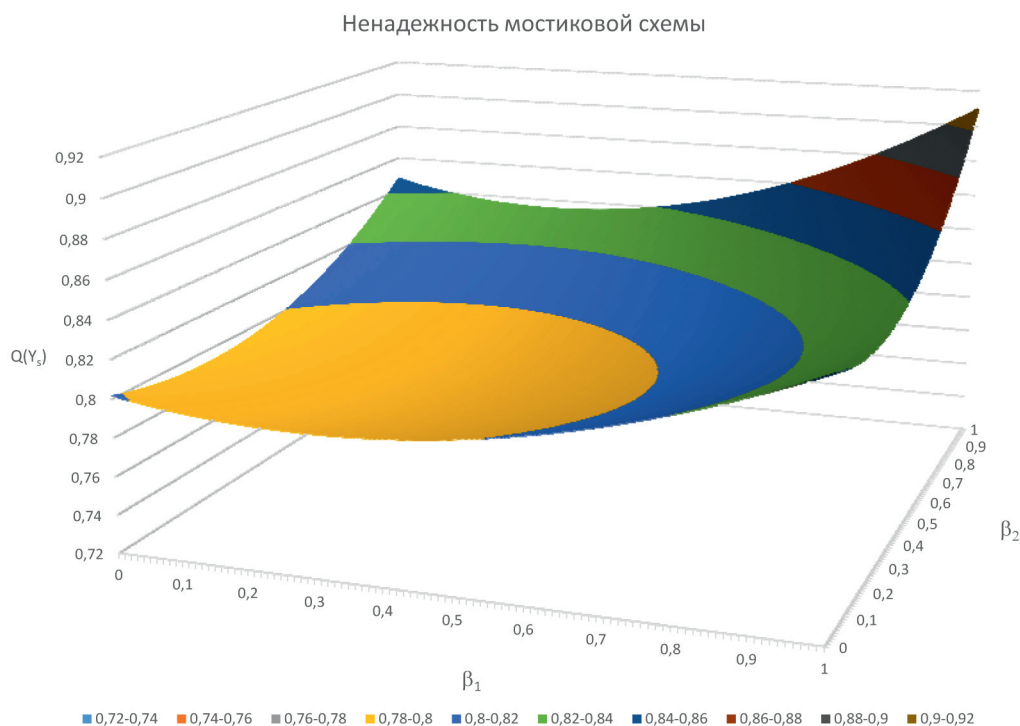
$$c_3 = 2-3\beta_a-3\beta_b+\beta_a\beta_b(6-\beta_a-\beta_b),$$

$$c_2 = (1-\beta_a)^2 + (1-\beta_b)^2 - \beta_a\beta_b,$$

$$c_1 = \beta_a + \beta_b.$$

В результате проведенных исследований функции (13) обнаружили следующие зависимости.

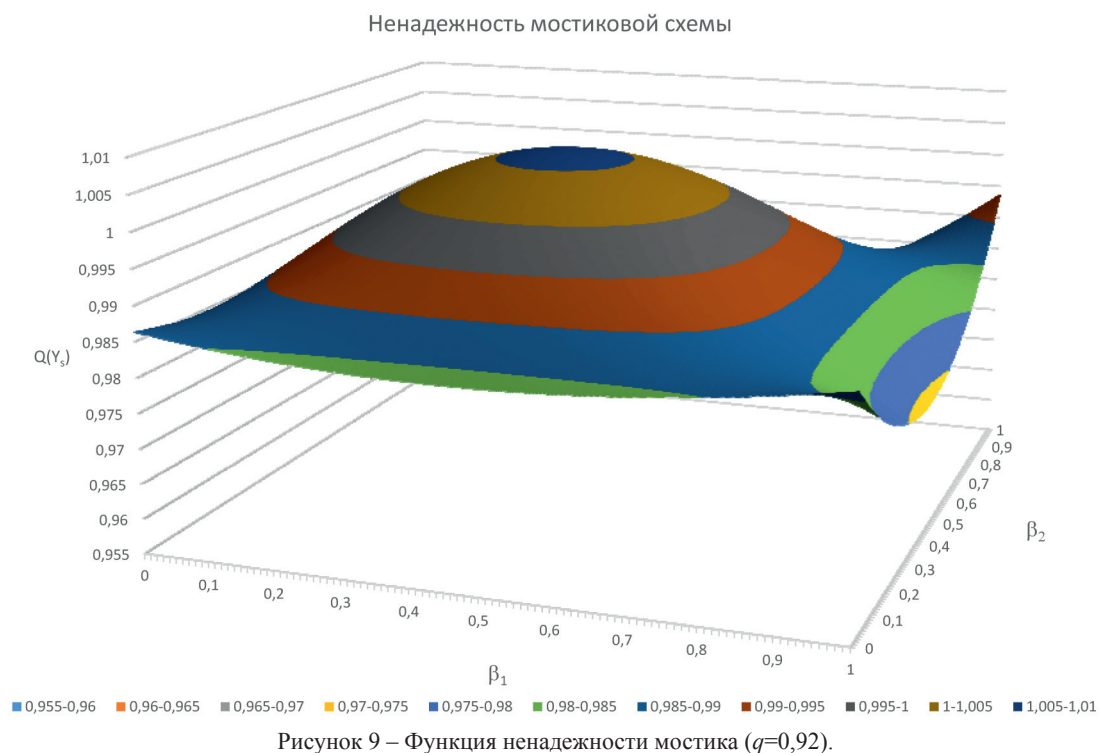
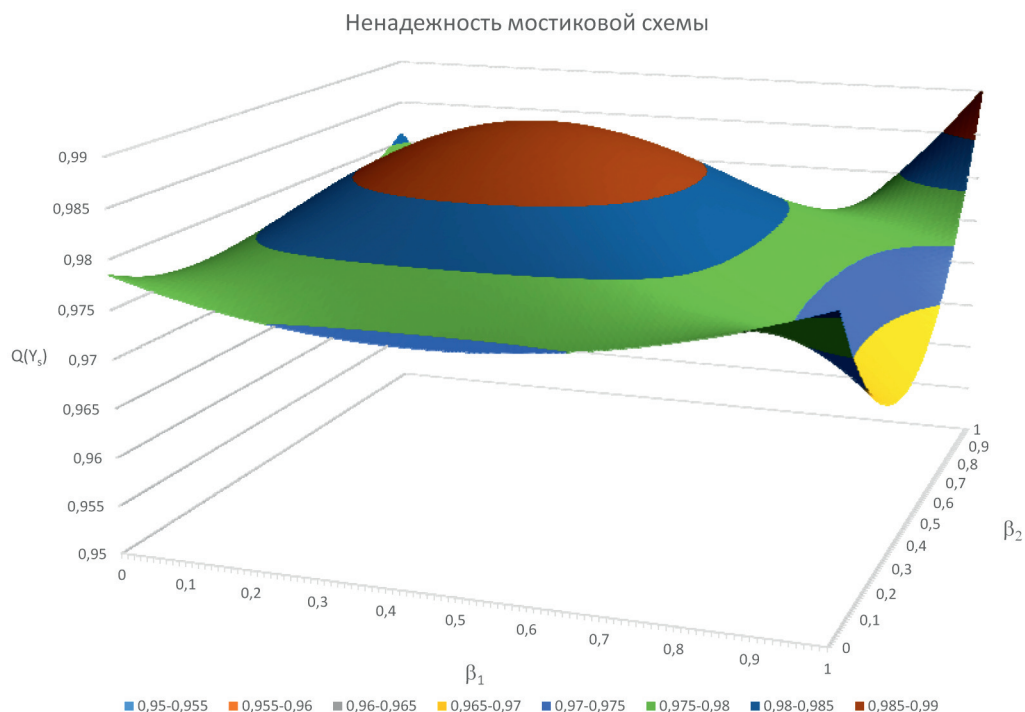
При $q \leq 0,5$ ненадежность $Q(Y_s)$ классически монотонно возрастает по каждому параметру β_a, β_b (рисунок 6). Т.е., при расчете мостика с высоконадежными элементами неожиданных эффектов не обнаружено.

Рисунок 6 – Функция ненадежности мостика ($q=0,3$).Рисунок 7 – Функция ненадежности мостика ($q=0,7$).

При $q \in (0,5, \approx 0,85)$ функция ненадежности имеет глобальный минимум. В окрестности точки $(0,0)$ ненадежность уменьшается при увеличении каждого параметра (рисунок 7). При достижении точки минимума дальнейшее увеличение параметров ООП приводит к увеличению ненадежности. При $\beta_a = \beta_b = 1$ достигается максимум ненадежности. Таким образом, при средней ненадежности составляющих мостик элементов

учет ООП может привести к снижению ненадежности системы в целом. Значение 0,85 получено визуально, для точных оценок необходимо аналитическое исследование (13).

При $q \in (\approx 0,85, \approx 0,91)$ функция ненадежности имеет сложную зависимость: четыре локальных граничных минимума и один максимум (рисунок 8). В окрестности точки $(0,0)$ ненадежность уменьшается при увеличении



каждого параметра. При достижении точки минимума дальнейшее увеличение параметров ООП приводит к увеличению ненадежности. Дальнейшее поведение зависит от конкретных значений параметров. При $\beta_a = \beta_b = 1$ достигается максимум ненадежности. При высокой ненадежности составляющих мостик элементов учет ООП может привести как к снижению (при малых β_a, β_b), так и к увеличению ненадежности системы в целом.

При $q \in (\approx 0,91, 1)$ функция ненадежности имеет прежнюю сложную зависимость: четыре локальных граничных минимума и один максимум (рисунок 9). В окрестности точки (0,0) ненадежность уменьшается при увеличении каждого параметра. При достижении точки минимума дальнейшее увеличение параметров ООП приводит к увеличению ненадежности. Дальнейшее поведение зависит от конкретных значений

параметров. При $\beta_a = \beta_b = 1$ достигается максимум ненадежности. Необходимо отметить, что существует область недопустимых значений параметров β_a, β_b , при которых ненадежность системы принимает значения большие единицы. Таким образом, не обязательно последовательная структура имеет недопустимые значения параметров модели бета-фактора.

Заключение

В статье проведено математическое исследование модели бета-фактора учета ООП. Исследования проводились на трех структурных схемах надежности: параллельной, последовательной и схеме типа мостик. Для двух последних схем обнаружилась проблема недопустимых значений параметров модели бета-фактора при высокой ненадежности элементов, составляющих систему. Для всех трех схем надежности показано, что необязательно увеличение параметров модели бета-фактора приводит к увеличению ненадежности.

Библиографический список

1. ГОСТ Р МЭК 61226-2011. Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления [Текст]. – Введ. 2011–09–26. – М.: Стандартинформ, 2011. – V, 22 с.: ил.
2. ГОСТ Р МЭК 62340-2011. Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине [Текст]. – Введ. 2012–07–01. – М.: Стандартинформ, 2012. – V, 18 с.
3. Антонов А.В. Анализ дерева отказов в среде программирования R [Текст] / А.В. Антонов, Е.Ю. Галивец, В.А. Чепурко, А.Н. Черняев // Надежность. – 2018. – № 18(1). – С. 4-13. DOI:10.21683/1729-2646-2018-18-1-4-13.
4. Антонов А.В. Анализ дерева отказов в среде программирования R. Учет отказов по общей причине [Текст] / А.В. Антонов, Е.Ю. Галивец, В.А. Чепурко, А.Н. Черняев // Надежность. – 2018. – № 18(3). – С. 3-9. DOI:10.21683/1729-2646-2018-18-3-3-9.
5. Перегуда А.И. Математическая модель надежности компьютерных сетей [Текст] / А.И. Перегуда, А.А. Перегуда, Д.А. Тимашев // Надежность. – 2013. – № 4. – С. 18-43. DOI:10.21683/1729-2646-2013-0-4-18-43.
6. Алпеев А.С. Надежность программного обеспечения управляющих систем и безопасность атомных станций [Текст] / А.С. Алпеев // Надежность. 2015;(4):75-80. <https://doi.org/10.21683/1729-2646-2015-0-4-75-80>.
7. Mosleh A. Procedures Guidelines in Modeling Common Cause Failures in Probabilistic Risk Assessment [Text] / A. Mosleh, D.M. Rasmuson, F.M. Marshall // NUREG/CR-5485. – University of Maryland, 1998.
8. O'Connor Andrew N. A General Cause Based Methodology for Analysis of Dependent Failures in System Risk and Reliability Assessments [Text] / A.N. O'Connor, A. Mosleh. – University of Maryland, 2013. – URL: <http://hdl.handle.net/1903/14285> (дата обращения 09.04.2019).
9. Smith C.L. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8: Technical Reference [Text] / C. L. Smith, S. T. Wood, W. J. Galyean, J. A. Schroeder, M. B. Sattison // NUREG/CR-7039 INL/EXT-09-17009. – Vol. 2. – U.S. Nuclear Regulatory Commission, Washington, D.C., 2011.
10. A.N. O'Connor. «A general cause based methodology for analysis of dependent failures in system risk and reliability assessments», 2013.

Сведения об авторах

Александр В. Антонов – доктор технических наук, профессор, главный эксперт Международного центра подготовки персонала Автономной некоммерческой организации дополнительного профессионального образования «Техническая академия Росатома», Российская Федерация, Москва, e-mail: AVAntonov@rosatomtech.ru

Валерий А. Чепурко – кандидат физико-математических наук, доцент, главный специалист отдела расчетных обоснований проектных решений АО РАСУ, Российская Федерация, Москва, e-mail: VAChepurko@rasu.ru

Алексей Н. Черняев – кандидат технических наук, заместитель технического директора – директор департамента проектирования АО РАСУ, Российская Федерация, Москва, e-mail: AlNChernyaev@rasu.ru

Поступила: 06.02.2019

Оценка гамма-процентного срока для биномиального плана испытаний

Виктор С. Михайлов, Федеральное государственное унитарное предприятие «Центральный научно исследовательский институт химии и механики им. Д.М. Менделеева» ФГУП «ЦНИИХМ», Российская Федерация, Москва



Виктор С. Михайлов

Резюме. В современном производстве высоконадежных, уникальных, сложных изделий стала обычной ситуация, в которой необходимо получить оценку гамма-процентного срока сохраняемости (ГПСС) или гамма-процентной наработки до отказа (ГПНДО) (далее – ГПС, понимая под этим соответственно ГПСС или ГПНДО) на основе испытаний, не давших отказов. Как правило, план испытаний относят к биномиальным испытаниям или к испытаниям с ограниченной наработкой и восстановлением. Под ГПНДО понимается наработка, в течение которой отказ не возникнет с вероятностью γ , выраженной в процентах. Аналогично, под ГПСС понимается календарная продолжительность хранения изделия, в течение и после которой изделие способно выполнять требуемую функцию с вероятностью γ , выраженной в процентах. **Цель работы.** Целью работы является нахождение такой оценки ГПС, которая будет простой и более эффективной по сравнению с традиционной и уступающей незначительно эффективной оценке, в случае существования последней, с точки зрения близости к расчетной оценке ГПС при использовании биномиального плана испытаний. **Методы исследования.** В основе исследования эффективных оценок лежит интегральный подход, использующий построение правила выбора (критерий) эффективной оценки, заданного на сумме значений абсолютных смещений оценок, выбранных из некоторого множества, от функции параметра закона распределения. **Выводы.** Полученная оценка ГПС является простой и более эффективной по сравнению с традиционной и уступает незначительно эффективной оценке, в случае существования последней, с точки зрения близости к расчетной оценке ГПС при использовании биномиального плана испытаний. Полученная оценка ГПС имеет существенные преимущества, а именно: оценка является эффективной на достаточно широком классе оценок; оценка позволяет получать значение по результатам испытаний, не давших отказов. Полученная оценка ГПС рекомендуется для безотказных испытаний, проводимых по биномиальному плану.

Ключевые слова: гамма-процентный срок сохраняемости; гамма-процентная наработка до отказа; экспоненциальное распределение; план испытаний; точечная оценка.

Формат цитирования: Михайлов В.С. Оценка гамма-процентного срока для биномиального плана испытаний // Надежность. 2019. №2. С. 18-21. DOI: 10.21683/1729-2646-2019-19-2-18-21

Введение

В современном производстве высоконадежных, уникальных, сложных изделий стала обычной ситуацией, в которой необходимо получить оценку гамма-процентного срока сохраняемости (ГПСС) или гамма-процентной наработки до отказа (ГПНДО) (далее – ГПС, понимая под этим соответственно ГПСС или ГПНДО) на основе испытаний, не давших отказов. Как правило, план испытаний относят к плану типа $NB\tau$ или NBt_i , где N – число испытываемых однотипных изделий; τ – наработка (одинаковая для каждого изделия); B (B) – характеристика плана, означающая, что работоспособность изделия после каждого отказа в течение срока испытаний не восстанавливается (восстанавливается) [1]. Под ГПНДО понимается наработка, в течение которой отказ не возникнет с вероятностью γ , выраженной в процентах [2]. Аналогично, под ГПСС понимается календарная продолжительность хранения изделия, в течение и после которой изделие способно выполнять требуемую функцию с вероятностью γ , выраженной в процентах

[2]. При условии подчинения наработки до отказа экспоненциальному закону распределения с параметром T_0 (средняя наработка до отказа, далее – СНДО), расчетное значение ГПС (далее – t_γ) вычисляется по формуле:

$$t_\gamma = -T_0 \ln(\gamma). \quad (1)$$

Постановка задачи

Рассмотрим случай проведения испытаний в соответствии с биномиальным планом.

Для биномиального плана испытаний достаточной статистикой является число наблюдаемых отказов (r) и суммарная наработка $S(R, N, \tau, t_i)$ [1, 4, 5], $R = r$ – случайное число отказов, t_i – моменты отказов, $i=1, 2, \dots, R$, тогда для биномиального плана испытаний случайная величина R (далее – с.в.), имеет биномиальное распределение $p_N(k)$ [3, ф-ла (1.4.55)] с параметрами N и p , $0 < p < 1$, т.е. с.в. R , равная числу успехов в серии из N независимых опытов, принимает целочисленные значения $0, 1, 2, \dots, N$ с вероятностями:

$$p_N(k) = C_N^k p^k (1-p)^{N-k}. \quad (2)$$

Функция распределения $F_R(r, N, p)$ биномиальной с.в. R примет вид

$$F_R(r, N, p) = \sum_{k=0}^r p_N(k). \quad (3)$$

С целью построения оценки ГПС ($\hat{t}_\gamma$) вполне естественным будет, если в качестве оценки параметра T_0 воспользоваться традиционной оценкой средней наработки до отказа, построенной для экспоненциального распределения [1, 5]:

$$T_{02} = \frac{S(R, N, \tau, t_i)}{r}, \text{ при } r > 0.$$

Однако полученная таким образом оценка $\hat{t}_{\gamma 2} = -T_{02} \ln(\gamma)$ имеет существенные недостатки, а именно:

- оценка является смещенной [1];
- оценка является не эффективной [1];
- оценка не позволяет получать значение t_γ по результатам испытаний, не давших отказов.

Для решения упомянутой выше задачи достаточно найти несмещенную эффективную оценку ($\hat{t}_{\gamma \text{эф}}$), если такая существует в классе состоятельных смещенных оценок. (Класс состоятельных оценок, в который входят и все оценки, полученные методом подстановки, включая и метод максимального правдоподобия, содержит в себе оценки с любым смещением, в том числе и с фиксированным – в виде функции от параметра или константы [3]). В ряде случаев найденные несмещенные эффективные оценки имеют весьма громоздкий вид со сложным алгоритмом вычисления [4]. Они также не всегда являются достаточно эффективными в классе всех смещенных оценок и не всегда имеют значительное преимущество перед простыми, но смещенными оценками, с точки зрения близости к оцениваемому показателю [6].

Цель работы

Целью статьи является нахождение оценки ГПС (далее – $\hat{t}_{\gamma 1}$), которая будет простой и более эффективной по сравнению с традиционной и уступающей незначительно эффективной оценке $\hat{t}_{\gamma \text{эф}}$ в случае существования последней, с точки зрения близости к t_γ при использовании биномиального плана испытаний.

Методы исследования и результаты

Рассмотрим класс оценок представимых в виде $\hat{t}_\gamma = -\hat{T}_0 \ln(\gamma)$, где $\hat{T}_0$ – оценка СНДО для биномиального плана испытаний.

В качестве инструмента для нахождения эффективной оценки будем использовать интегральные характеристики [6]. Аналогично [6] построим функционал (далее – $A(\hat{t}_\gamma)$) в основе которого лежит суммарный квадрат

отклонения ожидаемой реализации оценки $\hat{t}_\gamma$ от t_γ для всех возможных значений t_γ , T_0 , γ , N и τ :

$$A(\hat{t}_\gamma(R, N, \tau, t_i)) = \frac{1}{3} \sum_{\tau_j=1E+3}^{\tau_j=1E+5} \frac{1}{10} \sum_{N=10}^{\infty} \int_0^{\infty} \left(\frac{1}{T_0} \right)^2 \left\{ E\hat{t}_\gamma(R, N, \tau_j, t_i) - (-T_0 \ln(\gamma)) \right\}^2 \partial T_0, \quad (4)$$

где $E\hat{t}_\gamma$ – математическое ожидание оценки. В соответствии с формулой (3) математическое ожидание $E\hat{t}_\gamma(R, N, \tau, t_i)$ имеет вид:

$$\begin{aligned} E\hat{t}_\gamma(R, N, \tau, t_i) &= \sum_{k=0}^N p_N(k) \hat{t}_\gamma(k, N, \tau, t_i) = \\ &= \sum_{k=0}^N p_N(k) * (-\hat{T}_0 \ln(\gamma)). \end{aligned}$$

Эффективная оценка ГПС t_γ должна обладать минимальной величиной функционала $A(\hat{t}_\gamma)$.

Вынесем из-под знака интеграла выражение $-\ln(\gamma)$, тогда формула (4) примет вид:

$$A(\hat{t}_\gamma) = \ln^2(\gamma) V(\hat{T}_0), \quad (5)$$

где

$$\begin{aligned} V(\hat{T}_0(R, N, \tau)) &= \\ &= \frac{1}{3} \sum_{\tau_j=1E+3}^{\tau_j=1E+5} \frac{1}{10} \sum_{N=10}^{\infty} \int_0^{\infty} \left(\frac{1}{T_0} \right)^2 \{ E\hat{T}_0(R, N, \tau_j) - T_0 \}^2 \partial T_0. \end{aligned}$$

В соответствии с [6] функционал $V(\hat{T}_0)$ в формуле (5) принимает минимальное значение (а вместе с ним и функционал $A(\hat{t}_\gamma)$), если в качестве оценки параметра T_0 подставить его эффективную оценку, построенную на достаточно широком классе смещенных оценок. В этом случае для биномиального плана испытаний в качестве оценки параметра T_0 (СНДО) следует использовать явно заданную и эффективную оценку $\hat{T}_4$ из [6]:

$$\hat{T}_4 = \frac{\tau}{-\ln(1 - \hat{p}(R, N))}, \quad (6)$$

где оценка вероятности отказа $\hat{p}$ получается решением уравнения (см. формулу (3)):

$$F_R(r, N, \hat{p}) = \sum_{k=0}^r p_N(k, \hat{p}) = 0,5.$$

Тогда эффективная оценка ГПС $\hat{t}_{\gamma 1}$, построенная на достаточно широком классе оценок [6], примет вид (см. формулу (1)):

$$\hat{t}_{\gamma 1} = -\hat{T}_4 \ln(\gamma) \quad (7)$$

Для безотказных испытаний оценку $\hat{t}_{\gamma 1}$ можно применять и для плана типа NBт. Полученная таким образом оценка ГПС t_γ имеет существенные преимущества, а именно:

- оценка является эффективной на достаточно широком классе оценок [6];

- оценка позволяет получать значение t_γ по результатам испытаний, не давших отказов и проводимых по планам испытаний типа ЛБт или ЛВт.

Примеры

Пример 1. В качестве показателя надежности изделия используется гамма-процентная наработка до отказа t_γ ($\gamma=0,9$), которая не должна быть менее 1500 ч. По результатам безотказных испытаний одного изделия в течение 10000 ч требуется сделать оценку t_γ и проверку соответствия изделия требованиям к надежности.

Непосредственно из формул (6) – (7) следует, что оценка величины ГПНДО составит

$$\hat{t}_{\gamma 1} = -\hat{T}_4 \ln(\gamma) = -\ln(0,9) * \frac{\tau}{-\ln(1 - \hat{p}(R=0, N=1))} =$$

$$= 0,1053 * \frac{10000}{-\ln(1-0,5)} = 1519 \text{ ч.}$$

По результатам оценки t_γ можно сделать вывод о соответствии изделия требованиям к гамма-процентной наработке до отказа. Время, в течение которого откажет не более 10% изделий, составит 1519 ч, что соответствует требованиям к надежности изделия.

Приведем для сравнения традиционное решение примера 1.

Традиционно для испытаний, не давших отказов, параметр T_0 (вместо точечной оценки) оценивают по нижней доверительной границе (далее – НДГ) СНДО с доверительной вероятностью $\gamma = 0,9$. Тогда результат в соответствии с [5] составит:

$$T_{01n} = \frac{2t_\Sigma}{x^2(1-\alpha; 2r+1)} = \frac{2*1*10000}{2,71} = 7380 \text{ ч,}$$

где $x^2(1-\alpha; 2r+1)$ – квантиль χ^2 -распределения с $2r+1$ степенью свободы (для плана испытаний ЛВТ), ($\alpha = 1 - \gamma = 1 - 0,9 = 0,1$) – уровень значимости согласно ГОСТ Р 50779.26-2007;

$$\hat{t}_{\gamma 1} = -T_{01n} \ln(\gamma) = 0,1053 * 7380 = 777 \text{ ч.}$$

По результатам оценки t_γ традиционным методом можно сделать вывод о несоответствии изделия требованиям к гамма-процентной наработке до отказа. Время, в течение которого откажет не более 10% изделий, составит 777 ч, что не соответствует требованиям к надежности изделия.

Из сравнения традиционной $\hat{t}_{\gamma 1} = 777$ ($\gamma = 90\%$) и предлагаемой $\hat{t}_{\gamma 1} = 1519$ ($\gamma = 90\%$) оценок гамма-процентной наработки до отказа t_γ следует, что для испытаний, не давших отказов, традиционное оценивание с использованием нижних доверительных оценок, как и следовало ожидать, существенно занижает гамма-

процентную наработку до отказа t_γ в сравнении с предлагаемой оценкой $\hat{t}_{\gamma 1}$.

Пример 2. В условиях примера 1 по результатам испытаний десяти изделий произошел один отказ в конце испытаний, требуется сделать оценку v t_γ и проверку соответствия изделий требованиям к надежности.

Непосредственно из формул (6) – (7) следует, что оценка величины ГПНДО составит

$$\hat{t}_{\gamma 1} = \hat{T}_4 \ln(\gamma) = -\ln(0,9) * \frac{\tau}{-\ln(1 - \hat{p}(R=1, N=10))} =$$

$$= 0,1053 * \frac{10000}{-\ln(1-0,16226)} = 5947 \text{ ч.}$$

По результатам оценки t_γ можно сделать вывод о соответствии изделия требованиям к гамма-процентной наработке до отказа. Время в течение которого откажет не более 10% изделий составит 5947 час, что соответствует требованиям к надежности изделия.

Приведем для сравнения традиционное решение примера 2.

Традиционно параметр T_0 оценивают в соответствии с [5] по формуле:

$$T_{01} = \frac{t_\Sigma}{R+1} = \frac{10*10000}{2} = 50000 \text{ ч.}$$

Тогда

$$\hat{t}_{\gamma 1} = -T_{01} \ln(\gamma) = 0,1053 * 50000 = 5265 \text{ ч.}$$

По результатам оценки t_γ традиционным методом можно сделать вывод о соответствии изделия требованиям к гамма-процентной наработке до отказа. Время, в течение которого откажет не более 10% изделий, составит 5265 час, что соответствует требованиям к надежности изделия.

Оценка СНДО T_{01} уступает по своей эффективности оценке $\hat{T}_4$ [6]. Следовательно, оценка гамма-процентной наработки до отказа $\hat{t}_{\gamma 1}$ эффективнее традиционной оценки гамма-процентной наработки до отказа $\hat{t}_{\gamma 1}$. Тогда из сравнения традиционной $\hat{t}_{\gamma 1} = 5265$ ($\gamma = 90\%$) и предлагаемой $\hat{t}_{\gamma 1} = 5947$ ($\gamma = 90\%$) оценок гамма-процентной наработки до отказа t_γ следует, что традиционное оценивание $\hat{t}_{\gamma 1}$, как и следовало ожидать, существенно занижает гамма-процентную наработку до отказа t_γ в сравнении с предлагаемой оценкой $\hat{t}_{\gamma 1}$.

Пример 3. В качестве показателя надежности изделия используется гамма-процентный срок сохраняемости t_γ ($\gamma=0,9$), который не должен быть менее одного года. По результатам безотказного хранения одного изделия в течение 10 лет требуется сделать оценку t_γ и проверку соответствия изделия требованиям к надежности.

Непосредственно из формул (6)–(7) следует, что оценка величины ГПСС составит

$$\hat{t}_{\gamma 1} = \hat{T}_4 \ln(\gamma) = -\ln(0,9) * \frac{\tau}{-\ln(1 - \hat{p}(R=0, N=1))} =$$

$$= 0,1053 * \frac{10}{\ln(1-0,5)} = 1,519 \text{ год.}$$

По результатам оценки t_{γ} можно сделать вывод о соответствии изделия требованиям к гамма-процентному сроку сохраняемости. Календарное время, в течение которого откажет не более 10% изделий, составит 1,519 года, что соответствует требованиям к надежности изделия.

Выводы

Полученная оценка ГПС $\hat{t}_{\gamma 1}$ является простой и более эффективной по сравнению с традиционной и уступает незначительно оценке $\hat{t}_{\gamma \text{эф}}$ в случае ее существования, с точки зрения близости к t_{γ} при использовании биномиального плана испытаний.

Полученная оценка ГПС $\hat{t}_{\gamma 1}$ имеет существенные преимущества, а именно:

- оценка является эффективной на достаточно широком классе оценок [6];
- оценка позволяет получать значение t_{γ} по результатам испытаний, не давших отказов.

Полученная оценка ГПС $\hat{t}_{\gamma 1}$ рекомендуется для безотказных испытаний, проводимых по биномиальному плану.

Библиографический список

1. Барзилович Е.Ю. Вопросы математической теории надежности [Текст] / Е.Ю. Барзилович, Ю.К. Беляев, В.А. Каштанов и др.: под ред. Б.В. Гнеденко. – М.: Радио и связь, 1983. – 376 с.
2. ГОСТ 27.002-2015. Надежность в технике. Термины и определения [Текст]. – Введ. 2016–06–21. – М.: Стандартинформ, 2016. – IV, 27 с.
3. Шуленин В.П. Математическая статистика. Часть 1. Параметрическая статистика [Текст]: учебник / В.П. Шуленин. – Томск: Издательство НТЛ, 2012. – 540 с.

4. Воинов В.Г. Несмещенные оценки и их применение [Текст] / В.Г. Воинов, М.С. Никулин. – М.: Наука, 1989. – 440 с.

5. ГОСТ Р 50779.26-2007. Статистические методы. Точечные оценки, доверительные, предикционные и толерантные интервалы для экспоненциального распределения [Текст]. – Введ. 2007–12–27. – М.: Стандартинформ, 2008. – IV, 27 с.

6. Михайлов В.С. Неявные оценки для плана испытаний типа НБт [Текст] / В.С. Михайлов // Надежность и качество сложных систем. – 2018. – №1(21). – С. 64-71.

7. Михайлов В.С. Нахождение эффективной оценки средней наработки на отказ [Текст] / В.С. Михайлов // Надежность. – 2016. № 4(59). – С. 40-42.

8. Ишков А.С. Методика оценки гамма-процентной наработки радиоэлектронных компонентов информационно-измерительных систем по результатам кратковременных испытаний [Текст] / А.С. Ишков, В.Д. Зуев // Надежность. – 2015. №2(53). – С. 82-89.

9. Швецова-Шиловская Т.Н. Расчетно-экспериментальный метод оценки показателей надежности технологического комплекса на основе результатов его испытаний с учетом априорной информации о надежности по результатам испытаний составных частей [Текст] / Т.Н. Швецова-Шиловская, Т.В. Громова, Ф.П. Соколов, В.Г. Ратушенко // Надежность. – 2013. №2(45). – С. 80-92.

10. Чумаков И.А. Оценки остаточного времени альтернирующего процесса. Общий подход к оценкам остаточного времени [Текст] / И.А. Чумаков, В.А. Чепурко, А.В. Антонов // Надежность. – 2013. №2(45). – С. 51-79.

Сведения об авторе

Виктор С. Михайлов – ведущий инженер, Федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт химии и механики им. Д.И. Менделеева» ФГУП «ЦНИИХМ», Российская Федерация, Москва, e-mail: Mvs1956@list.ru

Поступила: 25.11.2018

Нейросетевое обобщение классических статистических критериев для обработки малых выборок биометрических данных

Александр И. Иванов, АО «Пензенский научно-исследовательский электротехнический институт», Российская Федерация, Пенза

Евгений Н. Куприянов, ФБГОУ ВПО «Пензенский государственный университет», Российская Федерация, Пенза

Сергей В. Туреев, НИИ систем связи и управления, Российская Федерация, Москва



Александр И. Иванов



Евгений Н. Куприянов



Сергей В. Туреев

Резюме. Целью работы является повышение мощности статистических критериев за счет их совместного применения для снижения требований к объему тестовой выборки. **Методы.** Классические статистические критерии: хи-квадрат, Крамера фон-Мизеса и Шапиро-Уилка предложено объединять через использование эквивалентных им искусственных нейронов. Каждый нейрон выполняет сравнение входных статистик с заранее вычисленным порогом и имеет два выходных состояния. Это позволяет получать три разряда бинарного выходного кода сети из трех искусственных нейронов. **Результаты.** Показано, что каждый из этих критериев на малых выборках биометрических данных дает большие значения ошибок первого и второго рода при проверке гипотезы нормальности. Нейросетевое объединение трех рассматриваемых критериев позволяет существенно снизить вероятности ошибок первого и второго рода. Приведены результаты парных нейросетевых обобщений, а также неросетевого обобщения тройки рассматриваемых статистических критериев. **Выводы.** Дается прогноз ожидаемых вероятностей ошибок первого и второго рода для нейросетевых обобщений 10 и 30 классических статистических критериев для малых выборок, содержащих 21 опыт. Важным элементом технологии прогнозирования является симметризация задачи, когда вероятности ошибок первого и второго рода делаются одинаковыми и усредняются. Усредняются также модули коэффициентов парной корреляции выходных состояний сумматоров искусственных нейронов. Только в этом случае связь числа обобщаемых критериев с ожидаемыми вероятностями ошибок первого и второго рода становится линейной в логарифмических координатах.

Ключевые слова: статистические критерии: хи-квадрат, Крамера фон-Мизеса, Шапиро-Уилка; искусственные нейронные сети, малые выборки, проверка гипотезы нормального закона распределения данных.

Формат цитирования: Иванов А.И., Куприянов Е.Н., Туреев С.В. Нейросетевое обобщение классических статистических критериев для обработки малых выборок биометрических данных // Надежность. 2019. №2. С. 22-27. DOI: 10.21683/1729-2646-2019-19-2-22-27

Проблема контроля закона распределения данных малых выборок

Проблемы обеспечения надежности уникальных ответственных систем [1, 2] многогранны и могут быть решены только комплексом организационно-технических мероприятий. Особо ярко эти проблемы проявляются в нейросетевой биометрии. Каждый из нас имеет уникальный биометрический образ, который необходимо однозначно преобразовать в криптографический ключ или в длинный пароль доступа из случайных символов. Однозначность преобразования обеспечивается обучением нейронной сети, при этом обучающая выборка имеет близкий к нормальному многомерный закон распределения данных. Проблема состоит в том, что обучающие выборки малы. В частности стандартный алгоритм [3] обучения хорошо справляется со своей задачей на выборке в 20 примеров, если эта выборка корректно получена и не имеет выбросов (грубых ошибок).

В случае, когда выборка биометрических данных велика (200 опытов и более) проверить гипотезу нормальности их распределения не сложно. Можно воспользоваться хи-квадрат критерием или иным другим статистическим критерием [4]. Одной из проблем биометрии [5] является то, что ее пользователи не желают предъявлять автомату обучения искусственной нейронной сети [3] 200 и более примеров своего биометрического образа. Пользователи комфортно себя чувствуют, предъявляя обучающую выборку объемом от 10 до 20 примеров своего уникального биометрического образа, например, рукописного пароля или голосовой парольной фразы. Требования предъявить больше примеров для обучения, воспринимаются пользователями негативно.

Аналогичная ситуация возникает в ботанике, биологии, медицине. Селекционер ботаник или биолог в короткие сроки не имеет возможности получить выборку в 200 особей животных (экземпляров растений), обладающих нужными редкими свойствами. Достаточную для корректных статистических оценок выборку удастся

получить через достаточно длительный интервал времени, фактически выделив и закрепив желаемые редкие свойства в нескольких поколениях.

В медицине наблюдается аналогичная ситуация: для проверки статистических гипотез требуются большие выборки. Тематика статистической обработки малых выборок популярна, однако известные рекомендации [6, 7] не дают кардинальных улучшений ситуации. Как правило, добиться улучшения удастся, если применять несколько статистических критериев [8].

Можно попытаться усилить известные статистические критерии [9], однако этот путь не дает значительных улучшений. Как правило, новые статистические критерии или модификация старых по отдельности плохо работают.

Основной идеей данной работы является нейросетевое объединение классических статистических критериев [4, 10, 11]. Успехи, достигнутые российской нейросетевой биометрией, весьма и весьма значительны. Силами регуляторов отечественного рынка информационной безопасности создан пакет российских национальных стандартов ГОСТ Р 52633.xx, регламентирующих ряд очень жестких требований к нейросетевой биометрии. В рамках данной статьи мы фактически предпримем попытку переложить хорошо отработанные математические приемы нейросетевой биометрии в новые предметные области. При этом мы попытаемся показать, что рекордно жесткие требования регуляторов отечественного рынка информационной безопасности к вероятностям ошибок первого и второго рода будут выполнимы и в других предметных областях, если придерживаться основных рекомендаций пакета стандартов нейросетевой биометрии ГОСТ Р 52633.xx.

Синтез и настройка хи-квадрат нейрона с 5 входами

При проверке гипотезы нормальности на практике наиболее часто используется хи-квадрат критерий Пирсона. Для малой выборки объемом в 21 опыт формула для вычисления значения хи-квадрат критерия имеет следующий вид:

$$\chi^2 = 21 \cdot \sum_{i=1}^5 \frac{\left(\frac{n_i}{21} - \Delta \tilde{P}_i \right)^2}{\Delta \tilde{P}_i}, \quad (1)$$

где n_i – число опытов, попавших в i -тый интервал гистограммы, $\Delta \tilde{P}_i$ – ожидаемая вероятность попадания опытов в i -тый интервал гистограммы при нормальном законе распределения данных проверяемой выборки.

Заметим, что в соответствии с отечественными стандартизованными рекомендациями [10] среднее число опытов, попавших в каждый из интервалов гистограмм должно быть близко к 5. Именно по этой причине в формуле (1) используется суммирование по 5 интервалам гистограммы для малой выборки в 21 опыт.

При создании своей формулы в 1900 году Пирсон не мог воспользоваться вычислительной техникой. По этой причине он вынужден был искать асимптотические соотношения для бесконечно больших выборок. Сегодня ситуация изменилась, любой студент способен написать программу, воспроизводящую миллионы выборок объемом в 21 опыт. На рисунке 1 приведено распределение плотности вероятности значений хи-квадрат критерия для выборок с нормальным и равномерным законом распределения значений.

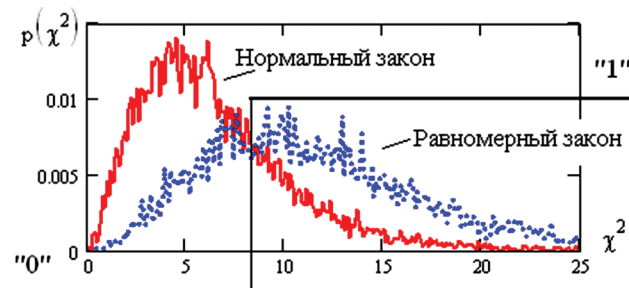


Рисунок 1 – Распределения значений хи-квадрат критерия для выборок объемом в 21 опыт с равномерным и нормальным законами распределения значений

Следует отметить, что искусственные нейроны настраиваются таким образом, чтобы эффективно разделять на два класса «нормальные» и «равномерные» входные данные [12]. На рисунке 1 пороговый элемент хи-квадрат нейрона делит континуум выходных на две области: «0» – «нормальные» данные и «1» – «равномерные» данные. Настройка выходного квантователя хи-квадрат нейрона выполняется исходя из условия равновероятного значения ошибок первого и второго рода $P_1 = P_2 = P_{EE} = 0,292$.

Для того, чтобы получить пять входных параметров хи-квадрат нейрона, необходимо выполнить сортировку данных проверяемой выборки по их значениям:

$$x = \text{sort}(x). \quad (2)$$

Кроме того, необходимо вычислить ширину интервалов гистограммы:

$$\Delta x = \frac{x_{20} - x_0}{5}. \quad (3)$$

Далее выполняют вычисление положения краев интервалов:

$$X_i = x_0 + \Delta x \cdot i \quad \text{при } i = 0, 1, \dots, 5. \quad (4)$$

Только после этого удастся подсчитать число попаданий в каждый из интервалов гистограммы и сформировать вектор входных параметров $\{n_1, n_2, \dots, n_5\}$ для нейрона (1). Итоговый результат подвергается квантованию:

$$\begin{cases} z(\chi^2) \leftarrow "0" & \text{если } \chi^2 \leq 7,72; \\ z(\chi^2) \leftarrow "1" & \text{если } \chi^2 > 7,72. \end{cases} \quad (5)$$

В итоге мы имеем полное формальное описание реализации хи-квадрат нейрона для выборки, состоящей из 21 опыта.

Синтез и настройка нейрона Шапиро-Уилка с 10 входами

Очевидно, что к той же выборке из 21 реализации может быть применен критерий Шапиро-Уилка [4, 11]. Его значение вычисляется по следующей формуле:

$$v^2 = \frac{1}{(\sigma(x))^2} \cdot \left\{ \sum_{i=0}^9 a_i \cdot (x_{20-i} - x_i) \right\}^2, \quad (6)$$

где x_i – упорядоченные значения, проверяемой выборки, $\sigma(x)$ – стандартное отклонение, a_i – табличные значения коэффициентов Шапиро-Уилка.

Распределения значений этого критерия для равномерного и нормального законов приведены на рисунке 2.

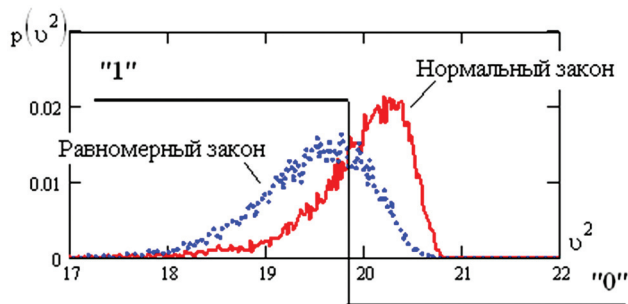


Рисунок 2 – Распределения значений критерия Шапиро-Уилка для выборок объемом в 21 опыт с равномерным и нормальными законами распределения значений

Если рассматривать функционал (6) как некоторый искусственный нейрон, то его выходами будут 10 разностей данных, исследуемой выборки, а выходной квантователь будет описываться следующими соотношениями:

$$\begin{cases} z(v^2) \leftarrow "0" & \text{если } v^2 \geq 19,8; \\ z(v^2) \leftarrow "1" & \text{если } v^2 < 19,8. \end{cases} \quad (7)$$

Такая настройка порога срабатывания квантователя обеспечивает одинаковые значения вероятности ошибок первого и второго рода $P_1 = P_2 = P_{EE} = 0,303$.

Синтез и настройка нейрона Крамера фон-Мизеса с 20 входами

Если сравнивать хи-квадрат нейрон (1) и нейрон Шапиро-Уилка (6) мы наблюдаем рост размерности их входной размерности (числа входов их сумматоров). Еще большей входной размерностью обладает нейрон Крамера фон-Мизеса:

$$\omega^2 = \sum_{i=0}^{19} \left(\frac{i+1}{21} - \tilde{P}(x_i) \right)^2 \cdot \frac{x_{i+1} - x_i}{x_{20} - x_0}. \quad (8)$$

Распределения значений на выходе сумматора нейрона Крамера фон-Мизеса приведены на рисунке 3.

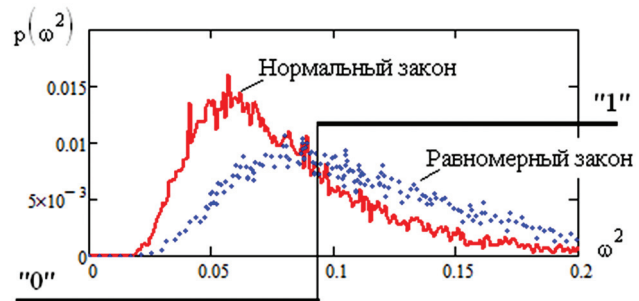


Рисунок 3 – Распределения значений критерия Крамера фон-Мизеса для выборок объемом в 21 опыт с равномерным и нормальными законами распределения значений

Настроенный выходной квантователь сумматора нейрона описывается следующим образом:

$$\begin{cases} z(\omega^2) \leftarrow "0" & \text{если } \omega^2 \leq 0,087; \\ z(\omega^2) \leftarrow "1" & \text{если } \omega^2 > 0,087. \end{cases} \quad (9)$$

Такая настройка порога срабатывания квантователя обеспечивает одинаковые значения вероятности ошибок первого и второго рода $P_1 = P_2 = P_{EE} = 0,342$.

Совместное использование трех статистических критериев

Описанные выше статистические критерии линейно независимы (имеют модули коэффициентов корреляции менее единицы):

$$\begin{cases} \text{corr}(\chi^2, v^2) \approx +0,559; \\ \text{corr}(\chi^2, \omega^2) \approx -0,708; \\ \text{corr}(\omega^2, v^2) \approx -0,667. \end{cases} \quad (10)$$

Отсутствие полной линейной зависимости (10) выходных состояний трех критериев позволяет объединить их для совместного использования. В этом случае выходной код трех нейронов «000» будет соответствовать трехкратному подтверждению гипотезы нормальности данных, исследуемой выборки. Инверсное состояние этого кода «111» будет соответствовать трехкратному подтверждению гипотезы равномерного закона распределения данных малой выборки.

По аналогии с практикой применения нейросетевых преобразователей биометрия-код будем принимать решение о принятии одной из двух гипотез по большинству состояний «0» или «1» в выходном коде сети трех нейронов. В этой ситуации каждому из четырех кодовых состояний «нормальное» распределение будет соответствовать своя вероятность ошибок, эти данные сведены в таблицу 1.

Таблица 1. Вероятности появления ошибок для кодовых состояний «нормальное» распределение

Код	«000»	«001»	«010»	«100»
P_1	0,0404	0,0423	0,0441	0,0621

Получается, что принятие кодов таблицы 1 как некоторого комплексного признака «нормальности» данных может привести к ошибкам, возникающим с вероятностью от 0,0404 до 0,0621. Наблюдается примерно 7-ми кратное снижение вероятности принятия ошибочных решений при использовании совокупности трех статистических критериев по сравнению с их применением поодиночке.

Эффект повышения точности оценок при увеличении размеров группы нейросетевого обобщения статистических критериев

В настоящее время созданы и применяются десятки статистических критериев [4, 10, 11]. Предположительно для каждого из них может быть собран эквивалентный искусственный нейрон. Более того, в последнее время активизируются работы по созданию новых, ранее неизвестных статистических критериев [13-17]. Первые успехи в этом направлении позволяют надеяться на то, что к десяткам уже созданных статистических критериев в ближайшие годы удастся добавить десятки совершенно новых критериев. То есть, через несколько лет мы можем получить пакет из сотни различных статистических критериев и их нейронов-аналогов.

Возникает вопрос: до какого уровня можно снизить вероятность появления ошибок при нейросетевом обобщении коллекции из 100 и более статистических критериев? Ответить на этот вопрос можно, опираясь на накопленный технологический опыт обработки данных нейросетевой биометрии.

Для прогнозов могут быть использована технология симметризации нейронных сетей [18, 19]. Для ее реализации усредним вероятности появления ошибок трех рассмотренных ранее нейронов $(0,292+0,303+0,342)/3 = 0,312$. Далее усредним модули коэффициентов корреляции между выходными состояниями трех нейронов (10): $E(|\text{corr}(\cdot)|) = 0,645$. Будем исходить из того, что все 100 обобщаемых критериев имеют симметричную матрицу коэффициентов корреляции со значениями элементов вне ее диагонали 0,645.

Еще одним упрощением является нормализация выходных состояний сумматоров нейронов, что противоречит данным, отображенным на рисунках 1, 2, 3, однако на данный момент только для этого упрощения существует положительный опыт использования симметризации.

Приняв все перечисленные выше допущения, мы приходим к блок-схеме численного эксперимента, отображенной на рисунке 4. Исходные данные для численного эксперимента получают от 100 программных генераторов псевдослучайных чисел с нормальным распределением.

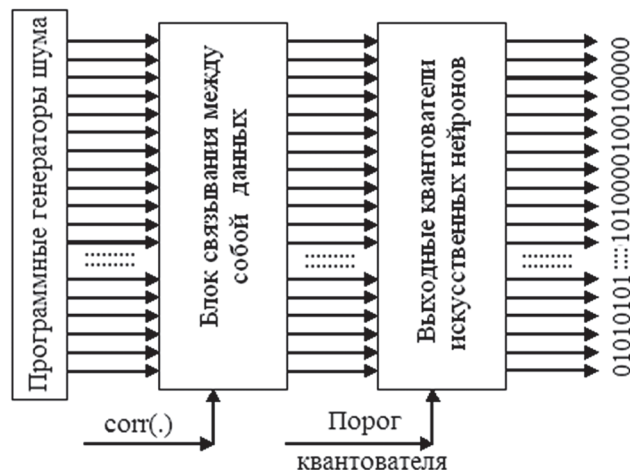


Рисунок 4 – Блок-схема решения задачи моделирования полностью симметричных искусственных нейронных сетей

Так как 100 программных генераторов дают независимые данные, их необходимо связать друг с другом и сделать одинаково коррелированными. Эту функцию выполняет второй слева блок на рисунке 4, реализующий произведение вектора независимых случайных чисел на симметричную связывающую матрицу:

$$\begin{bmatrix} 1 & a & \dots & a \\ a & 1 & \dots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \dots & 1 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{100} \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{100} \end{bmatrix} \quad (11)$$

В силу симметричности, связывающей матрицы преобразования (11), выходные данные оказываются одинаково коррелированными. Для того, чтобы получить заданное значение коэффициентов равной коррелированности $\text{corr}(y_i, y_{i+1}) = 0,645$ достаточно подбора значения всего одного параметра регулирования – a .

Следует отметить, что процедура симметризации связей и данных не может давать точных соответствий прогнозов и реальных данных. Если мы установим порог квантования блока эмуляции нейронов так, чтобы вероятность ошибок составляла 0,312, то тройки выходов совместно дадут общую ошибку 0,138. Этот результат примерно в 3 раза хуже реальных данных таблицы 1.

Для того, чтобы привести результаты к наблюдаемым данным, приходится значительно снизить равные вероятность ошибок каждого из нейронов с величины 0,312 до величины 0,141. В этом случае вероятность ошибок совместной работы группы из трех нейронов составит 0,0404.

Переход от обычных данных к данным с равной коррелированностью выгоден тем, что для этого частного случая в логарифмических координатах вероятности ошибок и число нейронов связаны линейной зависимостью, как это показано на рисунке 5.

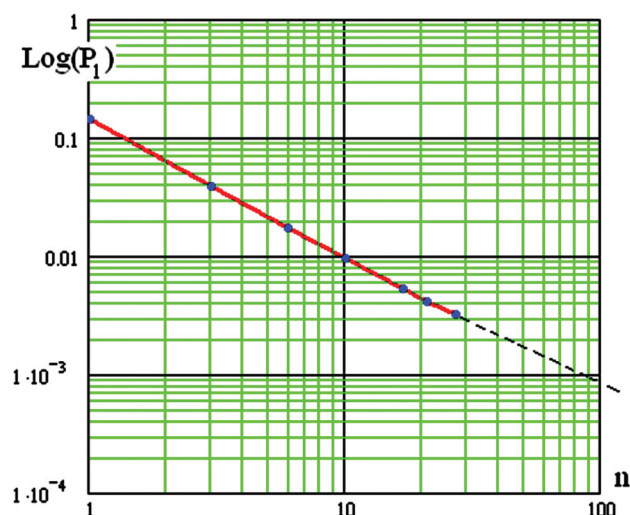


Рисунок 5 – Линия снижения вероятности ошибок первого рода из-за совместного применения нескольких статистических критериев с коэффициентами корреляции 0,645

Линия построена по 7 группам, состоящим из 1, 3, 6, 10, 16, 21, 27 нейронов. При проведении численного эксперимента использовалась выборка из 10 000 000 реализаций, время вычислений составляет примерно 9 минут на обычной вычислительной машине. Следует отметить, что применяя эту же вычислительную машину трудно провести численный эксперимент для группы из 100 нейронов, так как придется ждать несколько месяцев. Сократить время удастся путем экстраполяции (пунктирная линия на рисунке 5).

В конечном итоге прогнозируемое значение вероятности ошибок для нейросетевого обобщения 10 критериев должно составить $P_1 = 0,01$, а при обобщении 100 критериев вероятность ошибок должна снизиться до величины 0,0009. Столь существенное снижение вероятности ошибок является хорошим стимулом для организации работ по синтезу новых статистических критериев [13-17].

Заключение

Пирсон, создавший в 1900 году хи-квадрат критерий, по сути дела, начал революцию в статистической обработке. Путь развития, обнаруженный Пирсоном, оказался очень плодотворным и за прошедшие 119 лет, его последователями были созданы десятки разных статистических критериев.

Нейронные сети начали активно изучаться с середины XX века, однако только в начале XXI века эта технология обработки была доведена до промышленного применения и стандартизована [3].

Основным утверждением данной статьи является возможность объединения двух, казалось бы, разных ветвей математики. Для объединения вполне достаточно использовать стандартизованные в России технологии нейросетевой обработки биометрических данных, применив их к трем или более классическим

статистическим критериям. Для рассмотренной тройки статистических критериев этот подход дает снижение вероятности ошибок более чем в 7 раз. При этом становится очевидным тезис о целесообразности расширения номенклатуры существующих статистических критериев. Чем больше размер группы, обобщаемых нейронами статистических критериев, тем лучше должен быть конечный результат.

В этом контексте кардинально меняется подход к синтезу новых статистических критериев. После Пирсона математики старались найти новый критерий, мощность которого выше чем у его предшественников. Огромное число критериев, которые были исследованы, но имели относительно низкую мощность, не публиковалось. При нейросетевом объединении множества статистических критериев мощность каждого из них перестает играть основную роль. Крайне важным оказывается еще и то, каковы корреляционные связи добавленного критерия с группой других критериев. В нашем случае два объединяемых критерия имеют примерно одинаковую мощность, однако в этой группе присутствует особый критерий Шапиро-Уилка, который имеет низкую коррелированность с основными критериями хи-квадрат и Крамера-фон Мизеса.

Как следствие, необходимо повторить работы по исследованию возможного многообразия статистических критериев, принимая во внимание не только их относительную мощность, но и значения их коэффициентов корреляции в группах с другими, наиболее востребованными статистическими критериями. Новые статистические критерии с относительно низкой мощностью разделения гипотез ранее отбраковывались и не публиковались, теперь ситуация коренным образом изменилась. Куда важнее становится то, как новый критерий дополняет уже исследованные статистические критерии. Скорее всего, в ближайшее время потребуется создавать некоторую таблицу уровня родственности (коррелированности) уже известных и перспективных статистических критериев. Объединять в группы и создавать для них нейросетевые обобщения выгоднее всего линейно независимые (слабо коррелированные) статистические критерии.

Библиографический список

1. Похабов Ю.П. Проблемы надежности и пути их решения при создании уникальных высокоответственных систем [Текст] / Ю.П. Похабов // Надежность. – Том 19. – № 1. – С. 10-17.
2. Похабов Ю.П. Обеспечение надежности уникальных высокоответственных систем [Текст] / Ю.П. Похабов // Надежность. – Том 17. – № 3. – С. 17-23.
3. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа [Текст]. – Введ. 2012-04-01. – М.: Стандартинформ, 2012. – IV, 15 с.

4. **Кобзарь А.И.** Прикладная математическая статистика: для инженеров и научных работников [Текст] / А.И. Кобзарь. – М.: ФИЗМАТЛИТ, 2006 г. – 816 с.

5. **Язов Ю.К.** и др. Нейросетевая защита персональных биометрических данных [Текст] / Ю.К. Язов, В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров / Под ред. Ю.К. Язова. – М.: Радиотехника, 2012 г. – 157 с.

6. **Сухорученков Б.И.** Анализ малой выборки. Прикладные статистические методы [Текст] / Б.И. Сухорученков. – М.: Вузовская книга, 2010. – 384 с: ил.

7. **Дерффель К.** Статистика в аналитической химии [Текст] / К. Дерффель. – М.: Мир, 1994. – 258 с.

8. **Даев Ж.А., Нурушев Е.Т.** Применение статистических критериев для улучшения эффективности методов оценки рисков. // Надежность. – Том 18. – № 2. – С. 42-45.

9. **Ахметов Б.Б., Иванов А.И.** Оценка качества малой выборки биометрических данных с использованием более экономичной формы хи-квадрат критерия. // Надежность. – 2016. – № 2(57). – С. 43-48.

10. **Р 50.1.037-2002.** Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть I. Критерии типа χ^2 [Текст]. – М.: Госстандарт России, 2001. – 140 с.

11. **Р 50.1.037-2002.** Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть II. Непараметрические критерии [Текст]. – М.: Госстандарт России, 2002. – 123 с.

12. **Хайкин Саймон.** Нейронные сети: полный курс [Текст] / С. Хайкин. – М.: «Вильямс», 2006. – 1104 с.

13. **Серикова Н.И.** Оценка правдоподобия гипотезы о нормальном распределении по критерию Джини для числа степеней свободы, кратного числу опытов [Текст] / Н.И. Серикова, А.И. Иванов, Ю.И. Серикова. // Вопросы радиоэлектроники. – 2015. – № 1(1). – С. 85-94.

14. **Перфилов К.А.** Критерий среднего геометрического, используемый для проверки достоверности статистических гипотез распределения биометрических данных [Текст] / К.А. Перфилов. / Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. – Пенза, 2014. – Том 9. – С. 92-93. – URL: <http://www.pniei.penza.ru/RV-conf/T9/C92>.

15. **Иванов А.И.** Оценка соотношения мощностей семейств статистических критериев «среднего геометрического» на малых выборках биометрических

данных [Текст] / А.И. Иванов, К.А. Перфилов / XI Всероссийская научно-практическая конференция «Современные охраняемые технологии и средства обеспечения комплексной безопасности объектов». Пенза-Заречный. 20 октября 2016 г. – 2016. – С. 223-229.

16. **Иванов А.И.** Многомерный статистический анализ качества биометрических данных на предельно малых выборках с использованием критериев среднего геометрического, вычисленного для анализируемых функций вероятности [Текст] / А.И. Иванов, К.А. Перфилов, Е.А. Малыгина // Измерение. Мониторинг. Управление. Контроль. – 2016. – № 2(16). – С. 64-72.

17. **Иванов А.И.** Оценка качества малых выборок биометрических данных с использованием дифференциального варианта статистического критерия среднего геометрического [Текст] / А.И. Иванов, К.А. Перфилов, Е.А. Малыгина // Вестник СИБГАУ. – 2016. – №4(17). – С. 864-871.

18. **Малыгин А.Ю.** Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации [Текст] / А.Ю. Малыгин, В.И. Волчихин, А.И. Иванов, В.А. Фунтиков. – Пенза, Издательство Пензенского государственного университета, 2006. – 161 с.

19. **Ахметов Б.С.** Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации [Текст] / Б.С. Ахметов, В.И. Волчихин, А.И. Иванов, А.Ю. Малыгин. – Алматы, КазНТУ им. Сагпаева, 2013. – 152 с. – URL: <http://portal.kazntu.kz/files/publicate/2014-01-04-11940.pdf>

Сведения об авторах

Александр И. Иванов, доктор технических наук, доцент, ведущий научный сотрудник лаборатории биометрических и нейросетевых технологий АО «Пензенский научно-исследовательский электротехнический институт», Российская Федерация, Пенза, e-mail: ivan@pniei.penza.ru

Евгений Н. Куприянов, аспирант кафедры «Технические средства информационной безопасности» ФГБОУ ВО «Пензенский государственный университет», Российская Федерация, Пенза, e-mail: ibst@pnzgu.ru

Сергей В. Туреев, начальник научно-технического центра, НИИ систем связи и управления, Российская Федерация, Москва, e-mail: niissu@niissu.ru

Поступила: 22.01.2019

Модель оценки эффективности диагностических средств в бортовых устройствах

Ефим Н. Розенберг, АО «НИИАС», Российская Федерация, Москва

Александр С. Коровин, АО «НИИАС», Российская Федерация, Москва

Наталья Г. Пенькова, АО «НИИАС», Российская Федерация, Москва



Ефим Н.
Розенберг



Александр С.
Коровин



Наталья Г.
Пенькова

Резюме. Цель данной статьи – показать, что разработка, внедрение новых средств диагностики и улучшение существующих средств диагностики в бортовых устройствах позволяет добиться улучшения эксплуатационных характеристик и снижения вероятности перехода интеллектуальных систем железнодорожного транспорта в запрещенное состояние.

Методика. Для интеллектуальных систем железнодорожного транспорта наибольший интерес представляет построение аналитической модели оценки вероятности в связи с ее возможностью наглядной демонстрации учитываемых в модели факторов. Запрещенные события, которые приводят к нарушению работоспособности интеллектуальных систем железнодорожного транспорта, являются случайными, и их можно представить в виде случайного процесса. Случайный процесс развития системы, переход системы из разрешенного состояния в запрещенное состояние, изменение состояний системы во времени может быть описан полумарковским процессом. При оценке вероятности попадания системы в запрещенное состояние возникает вопрос выбора метода расчета. В статье показана возможность представления и решения полумарковской модели с помощью связанной графовой модели [3, 5], которая обладает высоким уровнем наглядности и является хорошо формализованным методом определения вероятности перехода системы в запрещенное состояние. Множество состояний системы и связи между ними представлены в виде ориентированного графа состояний, для которого определены топологические понятия [3]. Для определения влияния введения новых средств диагностики и улучшения существующих средств диагностики в бортовых устройствах на вероятность перехода интеллектуальных систем железнодорожного транспорта в запрещенное состояние используется теорема определения вероятности перехода системы из начального неопасного состояния в опасное состояние и приведена формула расчета этой вероятности. **Результаты.** Реализованный в представленной статье графовый метод демонстрирует, что применение дополнительных средств диагностики позволяет уменьшить вероятность попадания системы в запрещенное состояние, то есть, в состояние, когда отказ не будет обнаружен штатными или дополнительными средствами диагностики, более чем в 2 раза.

Ключевые слова: бортовые устройства безопасности, блок индикации, функциональная надежность, графовая модель.

Формат цитирования: Розенберг Е.Н., Коровин А.С., Пенькова Н.Г., Модель оценки эффективности диагностических средств в бортовых устройствах// Надежность. 2019. №2. С. 28-32. DOI: 10.21683/1729-2646-2019-19-2-28-32

Введение

Для планирования мероприятий по обработке запрещенных событий на железнодорожном транспорте широко применяется моделирование. Для интеллектуальных систем большие возможности предоставляет математическое моделирование. Методы математического моделирования подразделяют на две группы: аналитические и имитационные. В виду определенных недостатков метода имитационного моделирования [1], для интеллектуальных систем железнодорожного транспорта наибольший интерес представляет построение аналитической модели оценки вероятности в связи с возможностью наглядной демонстрации учитываемых в модели факторов. Запрещенные события, приводящие к нарушению работоспособности интеллектуальных систем железнодорожного транспорта, являются слу-

чайными, их можно представить в виде случайного процесса. Случайный процесс развития системы, переход системы из разрешенного состояния в запрещенное состояние, изменение состояний системы во времени может быть описан полумарковским процессом. Построение и решение полумарковских моделей в общем виде сводится к формированию системы однородных дифференциальных уравнений. Такой путь всегда чреват математическими трудностями. Поэтому в статье показана возможность представления и решения полумарковской модели с помощью связанной графовой модели [3, 5]. Такая модель обладает высоким уровнем наглядности, позволяет формализовать искомые состояния системы, а также пути перехода из разрешенного в запрещенное состояние, не требует применения сложного математического аппарата для формирования мероприятий по обработке запрещенных событий.

Постановка задачи

В настоящее время на железнодорожном транспорте одними из интеллектуальных систем на борту локомотива являются: устройство безопасности КЛУБ-У (унифицированное комплексное локомотивное устройство безопасности), комплекс БЛОК (безопасный локомотивный объединенный комплекс) и комплекс БЛОК-М (безопасный локомотивный объединенный комплекс масштабируемый). Устройство безопасности КЛУБ-У, комплекс БЛОК и комплекс БЛОК-М имеют свои блоки индикации, которые оснащены человеко-машинным интерфейсом. Блок индикации является программно-аппаратным устройством. Данное устройство предназначено для отображения информации, необходимой машинисту, помощнику машиниста, оператору, в случае беспилотного движения локомотива, сервисному персоналу при ведении локомотива и при проведении предрейсовой диагностики.

Отображаемая информация о допустимой скорости, целевой скорости, фактической скорости, профиле пути, расстоянии, о впередилежащей точке остановки, графике движения, впередиидущем поезде, показании запрещающего светофора, позволяет достигать цели по безопасному ведению локомотива – как соблюдение скоростного режима при штатной работе, так и прогнозирование безопасного режима ведения локомотива.

В процессе работы устройства возможно нарушение его работоспособности вследствие случайного отказа его аппаратной части, проявления систематической ошибки в его программе, ошибки машиниста, взаимодействующего с устройством, ошибки во входных данных. Любое нарушение работоспособности устройства расценивается как его отказ. Это приводит к отображению неактуальной информации и принятию машинистом неверных решений по соблюдению безопасного режима ведения локомотива.

В связи с этим уделяется большое внимание разработке и применению диагностических технических средств, позволяющих минимизировать вероятность попадания блока индикации в запрещенное состояние, которое приведет к нарушению работоспособности устройства отображения информации. Под запрещенным состоянием в данном случае понимается скрытый (не обнаруживаемый диагностическими средствами) отказ.

Блок индикации имеет внутренние средства диагностики, которые с приемлемой для обеспечения безопасности полнотой диагностического покрытия проверяют состояние работоспособности устройства индикации.

С помощью внутренних средств диагностики удается выявить ряд нарушений в работе блока индикации. Для расширения перечня выявляемых ошибок предлагается дополнительно перед каждой поездкой, машинистом или сервисным персоналом проводить предрейсовую диагностику блока индикации. Это, в том числе, позволяет предотвратить выход на линию локомотива с неисправным устройством безопасности.

Цель данной статьи – показать эффективность применения диагностических средств в человеко-машинном

взаимодействии, применительно к бортовым устройствам. А также продемонстрировать, что разработка, внедрение новых средств диагностики и улучшение существующих средств диагностики позволяет добиться улучшения эксплуатационных характеристик блока индикации и снижения вероятности перехода блока индикации в запрещенное состояние.

Описание моделей

Представим алгоритм работы блока индикации с внутренними средствами диагностики и предрейсовой диагностикой в виде блок-схемы (рисунок 1).

Построим граф состояний алгоритма работы блока индикации, представленного на рисунке 1.

События возникновения нарушений при работе блока индикации носят случайный характер. Представим исследуемые состояния алгоритмов работы блока индикации с помощью ориентированного графа состояний $G(S, H)$, где S – конечное множество состояний системы; H – конечное множество дуг между вершинами i, j (состояниями s_i, s_j). Состояния работы блока индикации можно описать следующим образом: если блок индикации находится в состоянии s_i , то с вероятностью p_{ij} он сможет перейти в состояние s_j .

На рисунке 2а представлен граф состояний, в котором для обнаружения отказа в работе блока индикации используются только внутренние средства диагностики. А на рисунке 2б представлен граф состояний, в котором для обнаружения отказа в работе устройства помимо внутренних средств диагностики блока индикации, добавляется еще предрейсовая диагностика блока индикации с участием машиниста или сервисного персонала. Для достижения цели нашей статьи исследуем граф на рисунке 2б. Граф имеет следующие состояния:

Состояние «S1» – отображение программой блока индикации текущей поездной обстановки;

Состояние «S2» – проверка наличия отказа внутренними средствами диагностики (программная проверка наличие ошибок в CAN, проверка на зависание контроллера программно переключением watchdog timer, программная проверка наличия блока индикации в конфигурации);

Состояние «S3» – устранение блоком индикации отказа, обнаруженного внутренними средствами диагностики (программный перезапуск CAN – интерфейса, аппаратный перезапуск контроллера с помощью watchdog timer, программный перезапуск программного обеспечения блока индикации);

Состояние «S4» – проверка наличия отказа с помощью предрейсовой диагностики блока индикации (правильность обработки команд, правильность отображения поездной обстановки, правильность установленной версии программного обеспечения, правильность значений параметров постоянных характеристик);

Состояние «S5» – устранение с помощью машиниста или сервисного персонала отказа, обнаруженного предрейсовой диагностикой (оперативное устранение

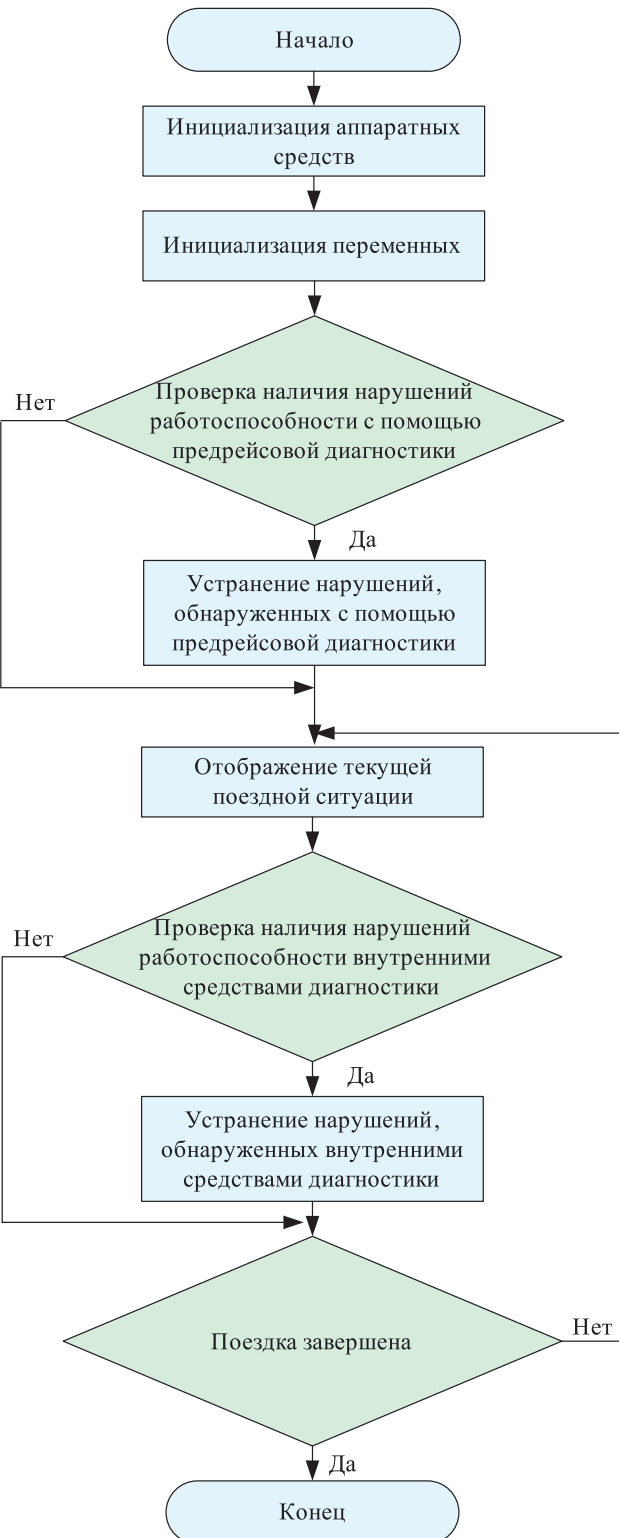


Рисунок 1 – Блок-схема алгоритма работы блока индикации с внутренними средствами диагностики и предрейсовой диагностикой.

обнаруженных ошибок, обновление программного обеспечения блока индикации, ввод правильных значений параметров постоянных характеристик);

Состояние «S6» – нахождение блока индикации в режиме со скрытым отказом.

S – полное множество состояний, $S = \{S1, S2, S3, S4, S5, S6\}$;

S_p – подмножество состояний не относящихся к запрещенным, $S_p = \{S1, S2, S3, S4, S5\}$;

$\bar{S}_p$ – подмножество запрещенных состояний, $\bar{S}_p = \{S6\}$.

При исправных внутренних средствах диагностики и средствах предрейсовой диагностики блока индикации обнаруживается факт отказа в работе блока индикации, после чего осуществляется перевод устройства в состояние устранения отказа.

Предполагается, что при обнаружении отказа устройство восстанавливается. В случае необнаружения отказа внутренними средствами диагностики и средствами предрейсовой диагностики блока индикации вследствие их отказа или недостаточной их эффективности, осуществляется перевод устройства в состояние скрытого отказа устройства (запрещенное состояние).

Состояния $S1$ и $S2$ являются разрешенными и находятся во множестве «штатный режим работы блока индикации в период эксплуатации по прямому назначению». Выбор значений вероятностей переходов $p11$ и $p12$ выполнен исходя из соотношения объема частей программы, реализующих функцию отображения текущей поездной обстановки и функцию проверки наличия отказов внутренними средствами диагностики. Рейс длится 10 часов (то есть каждые 10 часов требуется переход в состояние предрейсовой диагностики).

Выбор значения $p21$ определен фактической надежностью блока индикации в ходе его эксплуатации. По статистике отказ блока индикации – маловероятное событие (зафиксировано 70 отказов за 2018 год на всей сети железных дорог по данным эксплуатации, всего ориентировочно 11740 изделий). То, что в ходе эксплуатации отказ не зафиксирован, не означает, что блок все это время находился в работоспособном состоянии, он мог некоторую долю времени находиться в запрещенном состоянии скрытого отказа. Распределение значений вероятностей переходов $p23$ и $p26$ осуществлено исходя из эффективности реализованной в блоке внутренней диагностики. Обнаруживающая способность отказов внутренними средствами диагностики, реализованными в блоке индикации, в соответствии с ГОСТ Р 61508-7-2012, находится на уровне 0,5.

В таблице 1 представлены значения вероятностей переходов за один шаг из i -го состояния в состояние j (p_{ij}).

Таблица 1. Матрица переходных вероятностей

		Состояние						
		1	2	3	4	5	6	Σ
Состояние	1	0,72	0,18	0	0,1	0	0	1
	2	0,85	0	0,075	0	0	0,075	1
	3	1	0	0	0	0	0	1
	4	0,7	0	0	0	0,15	0,15	1
	5	1	0	0	0	0	0	1
	6	0	0	0	0	0	1	1

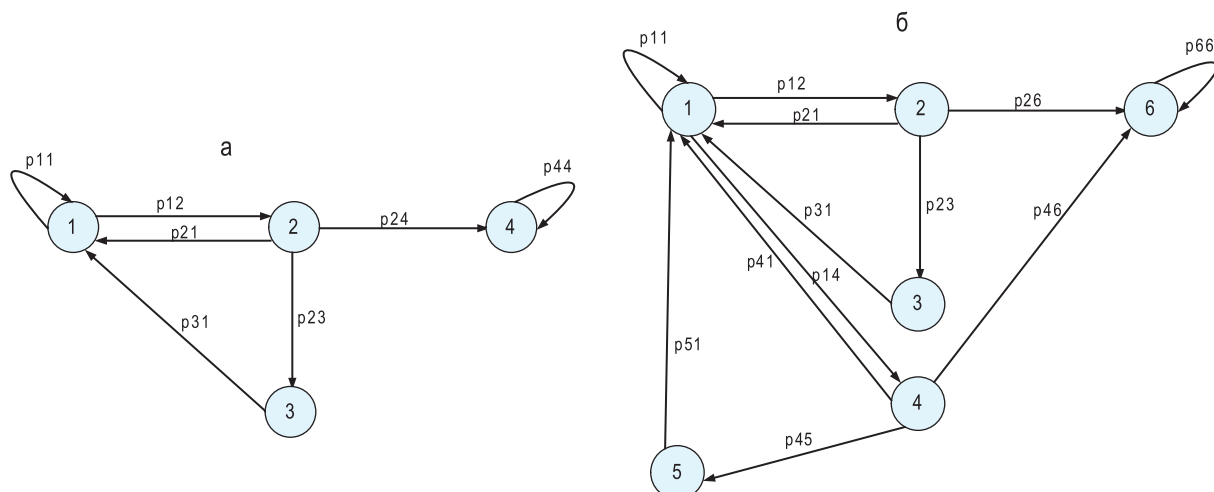


Рисунок 2 – Граф состояний: а) с внутренними средствами диагностики; б) с внутренними средствами диагностики и добавлением предрейсовой диагностики блока индикации с участием машиниста или сервисного персонала.

Задача состоит в определении влияния введения предрейсовой диагностики на вероятность перехода блока индикации в запрещенное состояние во время эксплуатации по назначению, когда используется только внутренняя диагностика.

Для решения этой задачи воспользуемся теоремой, которая гласит, что вероятность перехода системы из конкретного i -го начального неопасного состояния в любое опасное состояние f определяется выражением [5]

$$b_{if} = \frac{\sum_{f \in \bar{S}_p} \sum_k l_k^{if} \Delta G_k^f}{\Delta G_{\bar{S}_p}},$$

где l_k^{if} – k -ый путь, ведущий из неопасного состояния графа i в опасное состояние f ;

ΔG_k^f – вес разложения графа без f -й вершины и вершин графа, расположенных на k -ом пути;

$\Delta G_{\bar{S}_p}$ – вес разложения графа без вершин множества опасных состояний.

Приведем следующие топологические понятия, используемые для математического моделирования [3]:

- *путь* – это цепь последовательно соединенных однонаправленных дуг с началом в состоянии i и окончанием в состоянии j , вес пути

$$l_k^{ij} = \prod_{i,r,j \in S} p_{ir} p_{rj},$$

где p_{ir} – вероятность перехода за один шаг из состояния i в состояние r ;

p_{rj} – вероятность перехода за один шаг из состояния r в состояние j ;

- *замкнутый контур* – это цепь последовательно соединенных однонаправленных дуг, в которой выход конечной вершины в цепи соединен с начальной вершиной в цепи. Вес j -го контура определяется выражением:

$$C_j = \prod_{i,j \in S} p_{ij} p_{ji};$$

- *петля* – частный случай замкнутого контура, в ней входящие и исходящие дуги сливаются в одну дугу, вес петли $C_j = p_{ij}$;

- *разложение графа* – это часть графа, не содержащая выделенных вершин и связанных с ней дуг; вес разложения ΔG^i рассчитывается с учетом исключения из графа вершины i и связанных с ней дуг; вес разложения $\Delta G_{\bar{S}_p}$ рассчитывается с учетом дополнительного исключения из графа вершин множества $\bar{S}_p$ и связанных с ними дуг; вес разложения ΔG_k^f рассчитывается с учетом исключения из графа вершины f , а также вершин, расположенных на k -ом пути из начальной вершины в вершину f и связанных с ними дуг;

- *вес разложения* находится по формуле Мезона:

$$\Delta G = 1 - \sum_j C_j + \sum_{rj} C_r \cdot C_j - \sum_{irj} C_i \cdot C_r \cdot C_j + \dots$$

Для того чтобы оценить эффективность введения предрейсовой диагностики, рассчитаем условную вероятность перехода из исходного состояния «1» в запрещенное состояние «6», при условии, что штатные средства диагностики (внутренняя диагностика) отключены (пути $S1 \rightarrow S2 \rightarrow S6$ и $S1 \rightarrow S2 \rightarrow S3$).

В соответствии с теоремой оценки вероятности перехода из начального разрешенного состояния в запрещенное состояние, условная вероятность перехода из $S1$ в $S6$ определяется выражением:

$$b_{16/\bar{S}_{126}} = \frac{\sum_{f \in \bar{S}_p} \sum_k l_k^{16} \Delta G_k^6}{\Delta G_{\bar{S}_p}}.$$

Как видно из графа на рисунке 2б, количество k путей перехода из $S1$ в $S6$ при условии, что для обнаружения отказа в работе блока индикации используется только предрейсовая диагностика блока индикации с участием машиниста или сервисного персонала, равно 1.

Определение весов путей: $l_1^{16} = S1 \rightarrow S4 \rightarrow S6 = p_{14} p_{46}$.

Определение весов контуров:

$C1$: $S1 \rightarrow S1$, вес контура – p_{11} ;

$C2$: $S1 \rightarrow S2 \rightarrow S1$, вес контура – $p_{12} p_{21}$;

C3: $S1 \rightarrow S2 \rightarrow S3 \rightarrow S1$, вес контура – $p12 \cdot p23 \cdot p31$;

C4: $S1 \rightarrow S4 \rightarrow S1$, вес контура – $p14 \cdot p41$;

C5: $S1 \rightarrow S4 \rightarrow S5 \rightarrow S1$, вес контура – $p14 \cdot p45 \cdot p51$;

C6: $S6 \rightarrow S6$, вес контура – $p66$.

Для рассматриваемого случая вес разложения графа без вершин множества запрещенных состояний равен: $\Delta G_{\bar{S}_p} = 1 - (C1 + C2 + C3 + C4 + C5)$.

А вес разложения с учетом исключения из графа вершины «6», а также вершин, расположенных на k -ом пути из вершины «1» в вершину «6» и связанных с ними дуг равен: $\Delta G_1^6 = 1$.

Подставляя данные из таблицы 1 получаем, что условная вероятность перехода из состояния $S1$ в состояние $S6$:

$$b_{16/\bar{S}_{26}} = \frac{\sum_{f \in \bar{S}_p} \sum_k l_k^{16} \Delta G_k^6}{\Delta G_{\bar{S}_p}} =$$

$$= \frac{p14 * p46 * \Delta G_1^6}{1 - C1 - C2 - C3 - C4 - C5} = 0,53.$$

Поскольку исследуемые модели описывают полную группу событий, то вероятность попадания в единственное запрещенное состояние в обоих случаях равна 1. Таким образом, исходя из вычисленного значения условной вероятности $b_{16/\bar{S}_{26}}$, получаем, что введение предрейсовой диагностики блока индикации с участием машиниста или сервисного персонала позволяет уменьшить вероятность попадания блока индикации в запрещенное состояние во время рейса больше, чем в 2 раза (с 1 до 0,47).

Заключение

В данной статье показана эффективность добавления предрейсовой диагностики блока индикации с участием машиниста или сервисного персонала к внутренним средствам диагностики обнаружения отказа в работе блока индикации. Так, вероятность попадания в запрещенное состояние, то есть, в состояние, когда отказ не будет обнаружен штатными или дополнительными средствами диагностики, уменьшится более чем в 2 раза.

Благодарность

Авторы выражают благодарность профессору, доктору технических наук Шубинскому Игорю Борисовичу за оказанную помощь, ценные советы и замечания при написании настоящей статьи.

Библиографический список

1. Ивницкий В.А. Моделирование информационных систем железнодорожного транспорта. Учебное пособие [Текст] / В.А. Ивницкий. – М.: МИИТ, 2011. – 143 с.
2. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа [Текст] /

И.Б. Шубинский. – М.: ООО «Журнал «Надежность», 2012. – 296 с.

3. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза [Текст] / И.Б. Шубинский. – М.: Журнал Надежность, 2016. – 544 с.

4. Шубинский И.Б. О понятии функциональной надежности [Текст] / И.Б. Шубинский, Х. Шебе // Надежность. – 2012. – № 4. – С. 74-84.

5. Шубинский И.Б. Методы обеспечения функциональной надежности программ [Текст] / И.Б. Шубинский // Надежность. – 2014. – №4. – С. 87-101.

6. Шубинский И.Б. Графовый метод оценки производственной безопасности на объектах железнодорожного транспорта [Текст] / И.Б. Шубинский, А.М. Замышляев, О.Б. Проневич // Надежность. – 2017. – Т.17. – № 1. – С. 40-45.

7. Проневич О.Б. Алгоритм расчета и прогнозирования показателей функциональной безопасности систем электроснабжения железнодорожного транспорта [Текст] / О.Б. Проневич, В.Э. Швед // Надежность. – 2018. – № 18(3). – С. 46-55.

8. Розенберг Е.Н. Функциональная надежность программного обеспечения блока индикации комплекса БЛОК [Текст] / Е.Н. Розенберг, Н.Г. Пенькова, А.С. Коровин // Надежность. – 2017. – № 17(2). – С. 36-40.

9. Шухина Е.Е. Безопасный локомотивный объединенный комплекс БЛОК [Текст] / Е.Е. Шухина, В.И. Астрахан. – М.: 2013. – 103 с.

10. Зорин В.И. Унифицированное комплексное локомотивное устройство безопасности (КЛУБ-У) [Текст] / В.И. Зорин, В.И. Астрахан. – М.: ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2008. – 177 с.

11. ГОСТ Р МЭК 61508-7-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства [Текст]. – Введ. 2012-10-29. – М.: Стандартинформ, 2014. – V, 94 с.

Сведения об авторах

Ефим Н. Розенберг – профессор, доктор технических наук, первый заместитель Генерального директора АО «НИИАС». Российская Федерация, Москва, e-mail: info@vniias.ru

Александр С. Коровин – главный специалист сектора разработки микропроцессорных устройств АО «НИИАС». Российская Федерация, Москва, e-mail: A.Korovin@vniias.ru

Наталья Г. Пенькова – заместитель начальника центра безопасности и алгоритмической поддержки АО «НИИАС». Российская Федерация, Москва, e-mail: N.Penkova@vniias.ru

Поступила 08.04.2019

Индикаторный подход в управлении безопасностью объектов инфраструктуры железнодорожного транспорта

Леонид А. Баранов, Российский университет транспорта (МИИТ), Российская Федерация, Москва

Владимир В. Кульба, Институт проблем управления им. В.А. Трапезникова РАН (ИПУ РАН), Российская Федерация, Москва

Алексей Б. Шелков, Институт проблем управления им. В.А. Трапезникова РАН (ИПУ РАН), Российская Федерация, Москва

Дмитрий С. Сомов, ПАО Сбербанк, Российская Федерация, Москва



Леонид А. Баранов



Владимир В. Кульба



Алексей Б. Шелков



Дмитрий С. Сомов

Резюме. Целью настоящей статьи является разработка методов анализа и моделирования процессов возникновения и развития нештатных ситуаций на сложных технических объектах инфраструктуры железнодорожного транспорта. Приведены результаты анализа угроз, причин и последствий возникновения внезапных чрезвычайных ситуаций на сложных технических объектах инфраструктуры железнодорожного транспорта. Для решения задач обеспечения безотказного функционирования технических объектов, а также своевременной идентификации неполадок предложено использовать индикаторный подход, позволяющий осуществлять диагностирование и формальный анализ процессов возникновения и распространения неисправностей по элементам сложных технических систем. Для моделирования процессов распространения возникающих в результате технических неполадок возмущений (угроз возникновения чрезвычайных ситуаций) предложено использовать теоретико-графовый подход, предполагающий модельное и визуальное представление структуры исследуемой технической системы в виде ориентированного графа, отражающего взаимосвязи между ее элементами. Каждой вершине и дуге графа присваиваются некоторые параметры или функционалы, отражающие процессы взаимосвязанного функционирования элементов моделируемой системы. Распространение возмущений в системе моделируется импульсными процессами, запускаемыми в одной или нескольких исходных вершинах. В статье приведены разработанные формализованные модели распространения возмущений в технической системе на основе построения структурных компонент и матриц взаимосвязи. Введено понятие критического элемента технической системы, с использованием которого идентифицируется событие ее выхода из строя. Выделены два базовых критерия отказа технической системы: исключительный (система считается вышедшей из строя, если возмущение достигло любого из критических элементов) и абсолютный критерий (отказ наступает в случае, если возмущение достигло заданного подмножества критических элементов). В работе приведен аналитический пример, иллюстрирующий возможности предложенной модели распространения возмущений по структуре технической системы. Для решения задачи повышения эффективности диагностирования угроз возникновения чрезвычайных ситуаций на технических объектах инфраструктуры железнодорожного транспорта предложена модель использования структурно-интегрированных индикаторов, сущность которой состоит в том, что в структуре технической системы предлагается размещать индикаторы, оперативно передающие необходимую и достаточную информацию в случае возникновения нештатной ситуации. Основная задача при этом состоит в формировании некоторого множества индикаторов, основной целью которого является снижение информационной нагрузки и фокусировка внимания диспетчеров или операторов на ключевых с точки зрения обеспечения безаварийности и безопасности процессах, происходящих в технической системе. Выделены базовые критерии формирования множества индикаторов в сложной технической системе: максимум достоверности оценки последствий возникших возмущений, максимум точности определения причин возникновения нештатной ситуации, минимум времени обнаружения нештатной ситуации, минимум единовременных или текущих затрат. Приведена модифицированная графовая модель распространения возмущений в сложной технической системе, являющаяся основой для решения многокритериальных задач оптимального размещения индикаторов в структуре технических систем по критериям полноты, точности и своевременности обнаружения отказов различного типа. Автоматизация процессов формирования множества индикаторов с применением моделей распространения возмущений в технических системах позволит использовать предложенные методы в рамках развития методологии УРРАИ в части совершенствования технологий поддержки принятия решений в процессе управления объектами инфраструктуры железнодорожного транспорта.

Ключевые слова: управление, железнодорожный транспорт, объект инфраструктуры, техническая система, нештатная ситуация, датчики, индикаторы, моделирование.

Формат цитирования: Баранов Л.А., Кульба В.В., Шелков А.Б., Сомов Д.С. Индикаторный подход в управлении безопасностью объектов инфраструктуры железнодорожного транспорта // Надежность. 2019. №2. С. 33-41. DOI: 10.21683/1729-2646-2019-19-2-33-41

Введение

Актуальность проблем обеспечения высокого уровня безопасности на железнодорожном транспорте в настоящее время существенно возрастает. Железные дороги, являясь важнейшей составной частью транспортного комплекса России, играют исключительно важную роль в процессах социально-экономического развития страны, поскольку данному виду транспорта по объему и структуре грузовых и пассажирских перевозок фактически отсутствует альтернатива. Ведущая роль железнодорожного транспорта определяется также характерными для нашей страны значительными расстояниями перевозок, удаленностью основных объектов добывающей промышленности и источников сырьевых ресурсов от пунктов их переработки и потребления, а также морских портов, недостаточным развитием инфраструктуры других видов транспорта в имеющих стратегическое значение для развития нашей страны регионах Сибири и Дальнего Востока. От состояния, безопасности и качества работы железнодорожного транспорта зависят не только перспективы дальнейшего социально-экономического развития, но также возможности государства эффективно выполнять такие важнейшие функции, как защита национального суверенитета и безопасности страны, обеспечение потребности граждан в перевозках, создание условий для выравнивания уровня развития регионов и т.д.

В 2010 г. профильными организациями и подразделениями ОАО «Российские железные дороги» развернуты и в настоящее время активно продолжаются работы по созданию и широкому внедрению комплексной системы управления надежностью, ресурсами и функциональной безопасностью на железнодорожном транспорте УРРАН («Управление ресурсами, рисками и надежностью на стадиях жизненного цикла объектов инфраструктуры и подвижного состава») [1]. Данная система фактически реализует интегрированную технологию управления надежностью, ресурсами и функциональной безопасностью на железнодорожном транспорте и по сути является развитием методологий RAMS (безотказности, готовности, ремонтпригодности и безопасности) и LCC (стоимости жизненного цикла).

Основными стратегическими целями обеспечения безопасности на железнодорожном транспорте являются [2]:

1. Повышение эффективности основной деятельности, использования пропускных и провозных способностей инфраструктуры, технической надежности и готовности основных средств;

2. Обеспечение качества продуктов, услуг и процессов;

3. Обеспечение безопасности перевозок.

Производственно-технологический комплекс железнодорожного транспорта представляет собой широкомасштабную территориально распределенную многопрофильную инфраструктуру, включающей целый комплекс различных по назначению и решаемым технологическим задачам хозяйств ОАО «РЖД» (хозяйства пути и сооружений, автоматики и телемеханики, связи, электрификации и электроснабжения; локомотивное, вагонное и пассажирское хозяйства). При этом уровень сложности входящих в состав перечисленных хозяйств технических систем непрерывно возрастает, что неизбежно приводит к увеличению количества и разнообразия рисков различного типа, сопутствующих производству, наладке, техническому обслуживанию, эксплуатации и модернизации этих систем [3].

Обеспечение безопасности и надежности становится исключительно актуальным в условиях использования «беспилотных» транспортных средств. Международной ассоциацией общественного транспорта (International Association of Public Transport) рассматривается 5 уровней автоматизации управления движением поездов (от GO A0 до GO A4). При реализации уровня GO A4 на подвижном составе нет эксплуатационного персонала. В этих условиях централизованные системы автоматического управления движением поездов метрополитенов должны содержать подсистемы, обеспечивающие полноту, точность и своевременность обнаружения отказов различного типа и превентивное принятие решения [4].

В настоящее время с развитием современных технологий фактически происходит одновременное увеличение числа задействованных элементов в технических системах (размерностная сложность), рост разнообразия структур взаимодействия элементов таких систем (структурная сложность) и повышение разнообразия форм и способов этого взаимодействия (функциональная сложность). Это существенно повышает уровень сложности постановки и решения комплекса задач обеспечения надежного функционирования сложных технических систем (СТС), входящих в состав объектов инфраструктуры железнодорожного транспорта (ОИЖТ), поскольку в зависимости от их структурных и функциональных особенностей проявление рисков и характер распространения сбоев и отказов в рассматриваемых системах может быть различным [5]. При этом реализация рисков может заключаться в возможности нарушения нормального функционирования или выхода из строя как отдельного узла, так и всей системы в целом.

В настоящей работе основное внимание уделено разработке методов моделирования и анализа процессов

возникновения и развития нештатных ситуаций на объектах инфраструктуры железнодорожного транспорта на основе индикаторного подхода.

1. Моделирование процессов распространения возмущений по технической системе

Обширный опыт эксплуатации СТС различного класса и назначения показывает, что возникновению сбоев и отказов различной природы, а также возникающих по этой причине происшествий и аварийных ситуаций, которые далее для краткости будем называть внезапными чрезвычайными ситуациями (ВЧС), как правило, предшествует фаза накопления каких-либо дефектов в технологическом оборудовании или отклонений в протекании того или иного технологического процесса [6]. Длительность данной фазы может очень существенно различаться (от минут до суток). При этом на первом этапе сами по себе дефекты или отклонения не представляют непосредственной угрозы возникновения ВЧС. Происходящие на практике процессы накопления подобных отклонений от нормы связаны, как правило, либо с не наблюдаемостью работы элементов и подсистем СТС из-за отсутствия эффективных средств мониторинга и диагностики, либо, что бывает гораздо чаще, с тем, что персонал привыкает к такого рода отклонениям, поскольку они далеко не всегда приводят к авариям. На следующей фазе происходит внезапное так называемое инициирующее событие, которое приводит к лавинообразному развитию неблагоприятных процессов и возникновению ВЧС, последствия которой существенно усугубляются отсутствием организационно-технических механизмов противодействия, а также недостатком времени и ресурсов для его эффективного осуществления. Очевидно, что возникающая на третьей фазе как результат быстрого развития событий ВЧС в абсолютном большинстве случаев была бы невозможной без накопления отклонений и ошибок на первой стадии.

Таким образом, одной из основных задач обеспечения безотказного функционирования СТС является своевременная идентификация неполадок, иных нарушений в работе технической системы, предаварийных (аварийных) ситуаций и передача информации об их возникновении в системы визуализации, диспетчеризации и ситуационного управления различного уровня (лицам, принимающим решения (ЛПР), диспетчерам, операторам, и т.д.). Как правило, источниками информации о возможных нештатных отклонениях (неполадках) в работе СТС или их подсистем (узлов) являются датчики – элементы системы, способные регистрировать различные параметры состояния самой системы, ее окружающей среды, параметры функционирования СТС и др.

Возникающую в результате появления неполадок опасность возникновения сбоя, отказа, аварии, ВЧС или иного нарушения нормального функционирования

СТС, которое было зарегистрировано датчиком, будем называть угрозой. При этом будем предполагать, что возникновение некоторой угрозы приводит к возникновению процессов распространения возмущения по структурным элементам СТС в соответствии со схемой их взаимодействия. Поскольку угрозы в соответствии с приведенным выше определением могут иметь различную природу (тип, характер возникновения и проявления и т.п.), то и элементы СТС могут взаимодействовать между собой в процессе распространения возмущений различным образом. Как следствие, для каждого типа угрозы взаимодействие элементов системы будет происходить по различным схемам. Соответственно, по различным путям будет происходить и распространение возмущения по элементам СТС.

Технические системы высокой структурной, размерной и функциональной сложности обычно наделяются достаточно большим количеством датчиков, что существенно затрудняет осуществление качественного контроля их показаний, диагностирование возникающих нештатных ситуаций, а главное – своевременное принятие точных управляющих решений в случае отклонения их показаний от нормы и особенно – появления угрозы возникновения ВЧС. Таким образом, возникает задача выбора структуры информационной системы диспетчерского или ситуационного управления, позволяющей снизить нагрузку на оператора с целью увеличения скорости его реакции на возникающие нештатные ситуации без существенной потери уровня информированности о протекании наиболее существенных с точки зрения обеспечения безопасности процессов в СТС [5, 7–8].

При моделировании распространения возмущений, вызванного угрозой, будем использовать теоретико-графовый подход. Представление структуры исследуемой системы в виде графа в настоящее время достаточно широко используется в качестве одного из подходов к визуальному и модельному представлению связей между элементами различных, в том числе технических, систем. При этом в общем случае структура системы в зависимости от моделируемого процесса или явления может быть как жестко фиксированной, так и претерпевать определенные регулярные изменения (что характерно для динамических систем).

Суть рассматриваемого подхода заключается в том, что структура системы и взаимодействие ее элементов в процессе эксплуатации представляются в виде ориентированного графа. Каждой вершине и дуге графа присваиваются некоторые параметры и функционалы, адекватно описывающие процессы функционирования элементов моделируемой системы. Начальный импульс (возмущение), приложенный к одной или группе вершин, распространяется по всему графу, изменяя параметры вершин. При этом в общем случае может меняться и величина самого импульса в соответствии с функционалами, присвоенными дугам графа. В процессе моделирования используется дискретное время с фиксированным шагом Δt . Данный подход в моделиро-

вании динамических систем в настоящее время нашел применение в целом ряде предметных областей [9].

Пусть $A = \{a_1, a_2, \dots, a_n\}$ – множество элементов модели, где n – их число. В каждый момент времени любой элемент модели может принимать значения 0 или 1. Единица соответствует активированному состоянию (до элемента дошло возмущение), ноль соответствует неактивному состоянию. Состояние элемента a_i в момент времени t будем обозначать $a_i(t)$, а через $\bar{A}(t)$ будем обозначать вектор–строку $(a_1(t), a_2(t), \dots, a_n(t))$ состояний элементов модели. Множество датчиков образует подмножество элементов модели $A \supseteq D = \{d_1, d_2, \dots, d_{n_D}\}$, где n_D – количество датчиков.

Назовем матрицей смежности M квадратную бинарную матрицу $n \times n$, проиндексированную по обоим осям множеством элементов модели. В позиции (i, j) , $i, j \in \overline{1, n}$ матрицы смежности содержится запись 1 тогда и только тогда, когда между собой элементы a_i и a_j модели связаны отношением R_1 таким, что если в момент времени t_1 элемент a_i активен, то из этого следует, что в момент времени $t_2 = t_1 + \Delta t$ элемент a_j тоже будет активным. Иными словами, отношение R_1 задает пути распространения возмущения по системе. Отношение R_1 будем называть отношением смежности или отношением достижимости глубины 1. Наличие отношения смежности между элементами модели a_i и a_j будем обозначать $a_i R_1 a_j$, а отсутствие – $a_i \bar{R}_1 a_j$. В случае, если между элементами a_i и a_j отсутствует отношение смежности R_1 , в позиции (i, j) матрицы смежности M стоит 0. Будем считать, что отношение смежности обладает свойством рефлексивности, т.е. $\forall a \in A \quad a R_1 a$. В рамках модели это означает, что однажды активированный элемент остается активированным в течение всего времени моделирования. Для каждого выделенного типа угрозы может быть выделено свое отношение смежности R_1^1, R_1^2, R_1^3 , и т.д. Соответственно, каждому типу угрозы соответствует своя матрица смежности. Матрице смежности M соответствует оргграф причинно-следственных взаимосвязей элементов модели $G(A, R_1)$, вершинами которого является множество элементов модели, а дуга (a_i, a_j) соответствует единице в позиции (i, j) матрицы. Данный граф будем называть оргграфом взаимосвязи.

Активация элементов модели задается булевым уравнением $\bar{A}(t_{i+1}) = \bar{A}(t_i) \times M$. Другими словами, на последующих шагах активируются все элементы модели, соединенные дугами с уже активными элементами. При этом, поскольку диагональные элементы матрицы смежности равны 1, однажды активированные элементы остаются активированными в течение всего моделирования.

Среди множества элементов модели выбрано подмножество датчиков $D = \{d_1, d_2, \dots, d_{n_D}\}$. Датчики регистрируют заданные параметры СТС и сигнализируют о возникновении угрозы. Возмущение, вызванное данной угрозой, распространяется от датчиков к другим элементам системы по дугам графа взаимосвязи $G(A, R_1)$. Множество элементов модели, матрица взаимосвязи и

подмножество датчиков определяются совместно с проектировщиком системы по результатам анализа схемы функционирования системы на этапе ее разработки. Также среди элементов модели выделяется подмножество критических элементов $K = \{k_1, k_2, \dots, k_{n_K}\}$, определяющих критерий выхода системы из строя. Для каждого типа угрозы (раскраски ребер) можно рассматривать различные наборы критических элементов.

Моделирование начинается с момента t_0 активации первого датчика и продолжается либо до момента стабилизации (прекращения изменения состояния элементов модели), либо до выхода системы из строя в соответствии с выбранным критерием отказа системы.

Момент выхода системы из строя будем обозначать t_s . Критерий выхода системы из строя определяется критическими элементами. В зависимости от особенностей рассматриваемой системы или узла, а также других особенностей решаемой задачи можно выбирать различные критерии оценки выхода системы из строя. Среди них можно выделить два базовых критерия.

1. *Исключительный критерий выхода системы из строя.* Система считается вышедшей из строя, если возмущение достигло любого из критических элементов: $t_s = \min(t : \exists k \in K : k(t) = 1)$.

2. *Абсолютный критерий выхода системы из строя.* Система считается вышедшей из строя, если возмущение достигло заданного подмножества $K^* \subseteq K$ (в вырожденном случае – всех) критических элементов: $t_s = \min(t : \forall k \in K^* : k(t) = 1)$.

Можно также рассматривать и иные критерии, например, связанные с количеством, взаимным расположением и другими параметрами множества критических элементов, до которых дошло возмущение.

Для иллюстрации возможностей предложенной модели распространения возмущений по структуре СТС кратко рассмотрим условный упрощенный пример. Пусть структура системы включает 12 элементов, $n=12$, $A = \{a_1, a_2, \dots, a_{12}\}$. Элементы a_1 и a_2 являются датчиками, $d_1 = a_1$, $d_2 = a_2$, $D = \{d_1, d_2\} = \{a_1, a_2\}$, $n_D=2$. Элементы a_{11} и a_{12} являются критическими элементами, $k_1 = a_{11}$, $k_2 = a_{12}$, $K = \{k_1, k_2\} = \{a_{11}, a_{12}\}$, $n_K=2$. Задана матрица смежности M :

$$M = \begin{array}{c|cccccccccccc} & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Отношение R_1 , задаваемое матрицей M , формирует оргграф взаимосвязи $G(A, R_1)$, представленный на рисунке 1, где датчики обозначены символом окружности $\bigcirc$, а критические элементы – квадратом $\blacksquare$. Будем считать, что тип угрозы только один, соответственно, задано одно множество критических элементов, одно отношение смежности и один граф взаимосвязи.

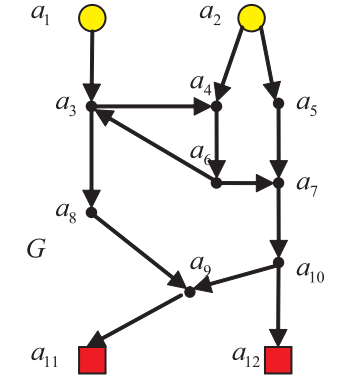


Рисунок 1 – Граф взаимосвязи G

Предположим, что в момент времени $t = t_0$ датчик $d_1 = a_1$ регистрирует угрозу. $a_1(t_0) = 1, a_{i \neq 1}(t_0) = 0, \bar{A}(t_0) = (1, 0, 0, \dots, 0)$.

Тогда, состояния элементов модели в момент времени $t = t_1 = t_0 + \Delta t$ вычисляются следующим образом:

$$\bar{A}(t_1) = \bar{A}(t_0) \times M = (1, 0, 1, 0, 0, \dots, 0).$$

На рисунке 2 изображен процесс распространения возмущений по дугам графа взаимосвязи G от активных элементов (выделены дополнительной окружностью) к неактивным, а также состояния соответствующих элементов модели в различные моменты времени. Возмущение распространяется по дугам графа от активных элементов к неактивным, преодолевая за один шаг времени одну дугу. Состояние элементов в произвольный момент времени определяется булевой формулой $\bar{A}(t_i) = \bar{A}(t_0) \times M^i$.

Строки состояний элементов для различных моментов времени имеют следующий вид:

$$\bar{A}(t_0) = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0);$$

$$\bar{A}(t_1) = (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0);$$

$$\bar{A}(t_2) = (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0);$$

$$\bar{A}(t_3) = (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0);$$

$$\bar{A}(t_4) = (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0);$$

$$\bar{A}(t_5) = (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0);$$

$$\bar{A}(t_6) = (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1).$$

Как видно из рассмотренного примера, в момент времени $t = t_4$ активируется первый критический элемент.

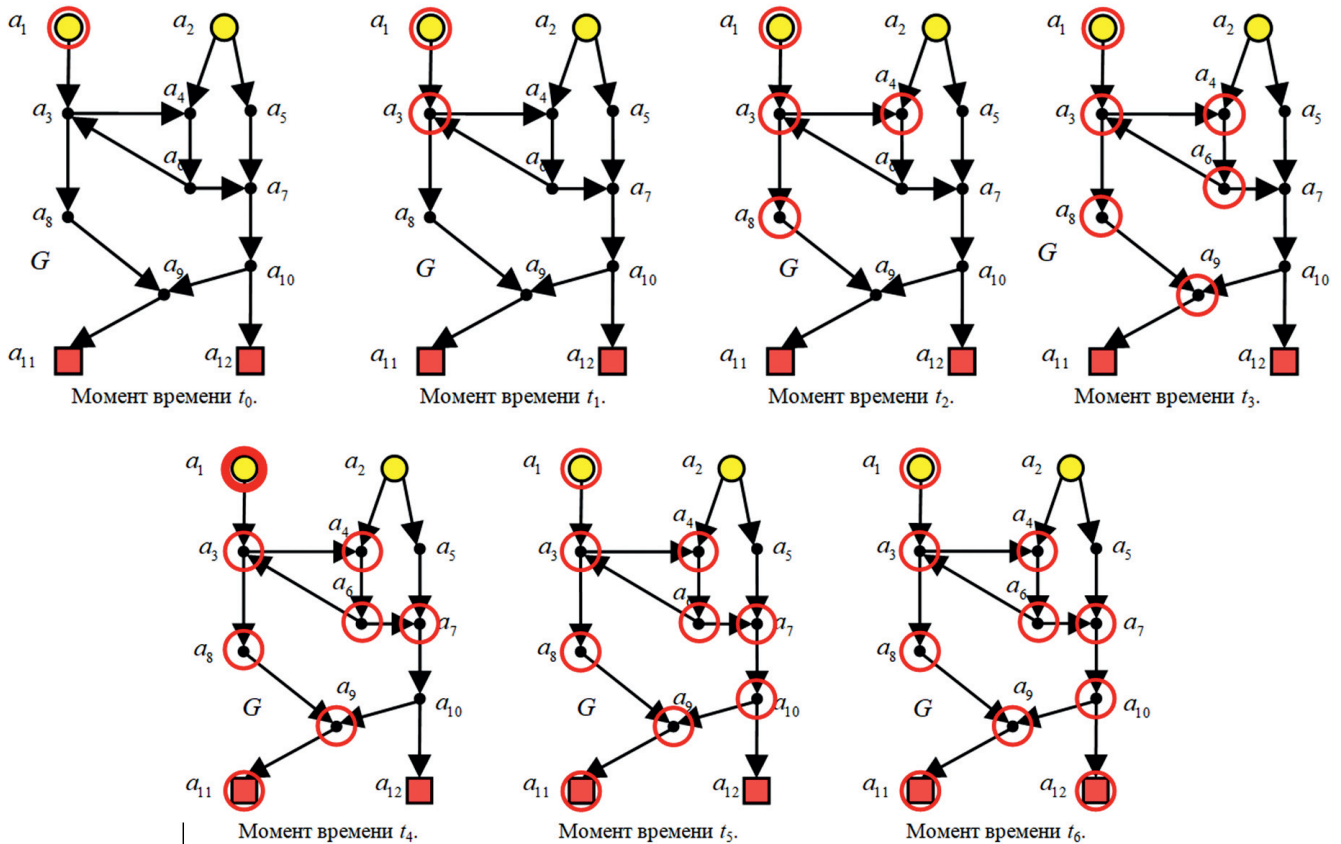


Рисунок 2 – Процесс распространения возмущений по системе

Если в системе используется исключительный критерий выхода системы из строя, то в момент времени t_4 система вышла бы из строя. При абсолютном критерии система выходит из строя в момент времени $t=t_6$.

2. Модели использования индикаторного подхода

Для решения задачи повышения эффективности диагностирования угроз возникновения ВЧС рассмотрим модель использования структурно-интегрированных индикаторов на технических ОИЖТ. Сущность индикаторного подхода состоит в том, что помимо датчиков в структуре технической системы предлагается размещать индикаторы, оперативно передающие необходимую и достаточную информацию в случае возникновения нештатной ситуации в СТС (угрозы возникновения ВЧС) в соответствующие системы визуализации, диспетчеризации или ситуационного управления с целью сигнализации ЛПР (оператору, диспетчеру и т.п.) о необходимости повышенного внимания к сложившейся ситуации или прямого вмешательства.

Основная задача в рамках данного подхода состоит в формировании некоторого множества индикаторов (здесь допустимо использование и общепринятого в организационном управлении и менеджменте понятия «панели индикаторов» [10]), основной целью которого является снижение информационной нагрузки и фокусировка внимания ЛПР (диспетчеров, операторов и т.д.) на ключевых с точки зрения целей задач обеспечения безаварийности и безопасности процессах, происходящих в СТС.

Индикаторы должны выбираться в структуре СТС таким образом, чтобы на основе значений отражаемых ими показателей (параметров) можно было достоверно судить о возникших отклонениях от штатного режима функционирования системы. Таким образом, рассматриваемый подход прежде всего должен в рамках систем контроля, диспетчеризации или ситуационного управления обеспечить оперативное предоставление ЛПР необходимой и достаточной информации о состоянии СТС в наглядной форме, а также возможности оперативного (в том числе сценарного) анализа альтернативных путей развития нештатной ситуации на заданном временном горизонте в управляемой технической системе, что в конечном итоге должно повысить эффективность принимаемых управленческих решений по обеспечению транспортной безопасности.

Для достижения указанных выше целей индикаторы должны быть расположены в структуре СТС таким образом, чтобы сигнализировать ЛПР о возникновении и развитии потенциально опасных ситуаций как можно раньше. Одновременно с этим необходимо отметить, что на ранних стадиях развития ситуации далеко не всегда до конца ясен возможный (наиболее вероятный, пессимистический, оптимистический и т.д.) сценарий развития нештатной ситуации, и, как следствие,

множество последствий может оказаться слишком широким, что не позволит достоверно спрогнозировать последствия и выработать правильное решение. В данном случае требуется оперативный и детальный мониторинг потенциально предаварийного состояния СТС с целью сбора дополнительной информации для ее последующего анализа и выработки соответствующей реакции на возникшие отклонения и угрозы возникновения ВЧС.

Безусловно, не менее важным критерием выбора определенного размещения индикаторов является и стоимость такого размещения. В зависимости от конкретной задачи необходимо учитывать не только количество индикаторов, но и их вес, объем, физическое расстояние между индикаторами, датчиками и т.д. Очевидно, что выбирая множество индикаторов нужно стремиться снизить их общее число, обеспечивая при этом минимально возможное снижение точности и информативности выдаваемых ими данных в системы визуализации, диспетчеризации или ситуационного управления.

На содержательном уровне можно выделить следующие основные критерии формирования множества индикаторов в сложной технической системе.

Достоверность оценки последствий. Набор индикаторов должен быть выбран таким образом, чтобы по их показаниям можно было судить о характере развития ситуации и возможных последствиях с максимальной точностью.

Точность определения причин. Показания индикаторов должны давать возможность не только оперативной идентификации и оценки последствий нештатных ситуаций, но и выявления причин их возникновения. Например, по показаниям индикаторов необходимо обеспечивать возможность определения, с какого узла (элемента) СТС началось распространение негативного воздействия, была ли причина возникших отклонений внешней или внутренней и т.д.

Время обнаружения нештатной ситуации. Индикаторы должны быть выбраны и расположены в структуре СТС таким образом, чтобы выявлять развивающиеся отклонения от нормального функционирования системы на как можно более ранних стадиях для максимизации резерва времени, необходимого на принятие решения оператором системы.

Объем затрат. Выбор и размещение индикаторов в структуре СТС должно быть осуществлено таким образом, чтобы минимизировать единовременные и текущие затраты.

Предложенные критерии в определенном смысле противоречивы, поскольку, например, для максимально точного определения причины возникновения нештатной ситуации, строго говоря, необходимо разместить индикаторы во всех элементах системы, но это приведет к росту стоимости и увеличению информационной нагрузки на ЛПР, росту затрат необходимого ЛПР времени на обнаружение нештатной ситуации и т.п.

Для решения задачи синтеза набора индикаторов модифицируем рассмотренную выше графовую модель распространения возмущений в СТС. Введем понятие времени прохождения дуги, под которым будем понимать положительное число, сопоставленное дуге графа взаимосвязи и означающее время, за которое возмущение перейдет из элемента модели, стоящего в начале дуги, в элемент, стоящий в конце дуги. Для записи времени прохождения дуг будем использовать матрицу временных взаимосвязей M_p , представляющую собой квадратную матрицу $n \times n$, проиндексированную по обеим осям элементами модели. При этом в позиции (i, j) , $i, j \in 1, n$ матрицы временных взаимосвязей размещено время прохождения дуги (a_i, a_j) , если такая дуга существует, и знак бесконечности ∞ , если такая дуга отсутствует.

Назовем матрицей временных расстояний N квадратную матрицу $n \times n$, проиндексированную по обеим осям элементами модели. При этом в позиции (i, j) , $i, j \in 1, n$ данной матрицы стоит временное расстояние между вершинами a_i и a_j графа. Матрица временных расстояний является результатом применения алгоритма нахождения кратчайших расстояний между вершинами Флойда-Уоршелла к матрице временных взаимосвязей [11].

Введем ряд определений, позволяющих сформулировать оптимизационную задачу размещения индикаторов в технической системе. Подмножество индикаторов будем обозначать $I = \{i_1, i_2, \dots, i_{n_i}\}$. Назовем множеством предшествования времени t вершины a множество всех элементов модели $Bef_t(a)$ таких, что элемент a достижим из них за время, не превышающее времени t . Множеством последствия времени t элемента a назовем множество всех элементов модели $Aft_t(a)$, достижимых из элемента a за время, не превышающее времени t .

Под индикаторным покрытием предшествования времени t будем понимать набор множеств предшествования времени t для всех индикаторов:

$$I_t^{Bef} = \{Bef_t(i_1), Bef_t(i_2), \dots, Bef_t(i_{n_i})\}.$$

Индикаторным множеством покрытия предшествования времени t будем называть объединение множеств элементов модели, входящих в индикаторное покрытие предшествования времени t , или, что то же самое, объединение множеств предшествования времени t всех индикаторов:

$$\overline{I_t^{Bef}} = \bigcup_{j=1}^{n_i} Bef_t(i_j).$$

Аналогично под индикаторным покрытием последствия времени t будем понимать набор множеств последствия времени t для всех индикаторов:

$$I_t^{Aft} = \{Aft_t(i_1), Aft_t(i_2), \dots, Aft_t(i_{n_i})\}.$$

Индикаторным множеством покрытия последствия времени t будем называть объединение множеств элементов модели, входящих в индикаторное покрытие

последствия времени t , или, что то же самое, объединение множеств последствия времени t всех индикаторов:

$$\overline{I_t^{Aft}} = \bigcup_{j=1}^{n_i} Aft_t(i_j).$$

Будем называть общим множеством покрытия предшествования набор множеств предшествования для всех индикаторов заданного для каждого индикатора времени:

$$I_T^{Bef} = \{Bef_{t_1}(i_1), Bef_{t_2}(i_2), \dots, Bef_{t_{n_i}}(i_{n_i})\},$$

где $T = \{t_1, t_2, \dots, t_{n_i}\}$ – набор времен множеств предшествования. Аналогично вводится понятие общего индикаторного покрытия последствия:

$$I_T^{Aft} = \{Aft_{t_1}(i_1), Aft_{t_2}(i_2), \dots, Aft_{t_{n_i}}(i_{n_i})\}.$$

Назовем диаметром общего покрытия максимум по всем временам набора

$$T : D(I_T^{Bef}) = D(I_T^{Aft}) = \max_{j \in n_i} (t_j).$$

Аналогично покрытиям времени введем понятие индикаторного множества общего индикаторного покрытия предшествования и последствия:

$$\overline{I_t^{Bef}} = \bigcup_{j \in n_i} Bef_t(i_j), \quad \overline{I_t^{Aft}} = \bigcup_{j \in n_i} Aft_t(i_j).$$

Будем считать, что решением задачи размещения индикаторов является некоторое подмножество элементов модели $I \subseteq A$. Введем ограничения на множество решений и получим, таким образом, множество допустимых решений.

Количество индикаторов должно быть ограничено. Это ограничение следует из требования снизить информационную нагрузку на оператора. Математически данное ограничение можно записать следующим образом: $|I| = n_i \leq N_i$, где N_i – некоторая константа, заданная при формулировании конкретной задачи.

Набор индикаторов должен покрывать все возможные угрозы, известные на этапе проектирования системы. Другими словами, в терминах рассматриваемой модели, не должно быть ситуаций, при которой возмущение, вызванное датчиком, достигнет критического элемента раньше, чем оно достигнет индикатора. Математическую интерпретацию данного ограничения можно записать следующим образом: $\forall d \in D : Alf(d) \cap K \neq \emptyset \exists i \in I : i \in Aft_s(d)$.

Таким образом, область допустимых решений должна удовлетворять следующим требованиям:

$$I \subseteq A,$$

$$|I| = n_i \leq N_i,$$

$$\forall d \in D : Alf(d) \cap K \neq \emptyset \exists i \in I : i \in Aft_s(d).$$

Сформулируем оптимизационные критерии для поиска оптимального решения среди допустимых решений.

1. *Критерий максимизации допустимого времени на принятие решения.* С точки зрения безопасности функционирования системы и предупреждения выхода ее из строя необходима как можно более ранняя сигнализация об угрозе. Данный критерий состоит в максимизации времени, прошедшего с момента активации критического элемента до наступления критического события и в терминах и обозначениях модели записывается следующим образом:

$$\min_{d \in D, k \in K} \left(\max_{i \in I \cap \text{Alf}(d)} (dis^t(d, k) - dis^t(d, i)) \right) \rightarrow \max.$$

2. *Полнота покрытия.* Для каждого набора индикаторов определено покрытие множествами предшествования и последствия. Для того чтобы иметь возможность судить как можно более полно о возможных причинах и последствиях текущей ситуации в системе необходимо выбрать индикаторы таким образом, чтобы множество покрытия предшествования и последствия охватывало как можно большую часть элементов модели. Математически это можно записать следующим образом:

$$|I^{Alt}| \rightarrow \max; |I^{Bef}| \rightarrow \max.$$

3. *Точность покрытия.* В предыдущем критерии используется покрытие без учета времени. Но для точного определения развивающейся ситуации необходимо, чтобы индикаторы находились «близко» по времени от возмущения, движущегося по системе. Для этого необходимо, чтобы минимальный диаметр покрытия предшествования или последствия, множество которого покрывает все множество покрытия предшествования I^{Bef} или последствия I^{Alt} был минимальным:

$$\min_{T: I_T^{Alt} = I^{Alt}} (D(I_T^{Alt})) \rightarrow \min; \min_{T: I_T^{Bef} = I^{Bef}} (D(I_T^{Bef})) \rightarrow \min.$$

Сформулируем задачу оптимизации размещения индикаторов.

Пусть задана модель распространения возмущения по технической системе: множество элементов модели $A = \{a_1, a_2, \dots, a_n\}$, подмножество датчиков $D = \{d_1, d_2, \dots, d_{np}\}$, подмножество критических элементов $K = \{k_1, k_2, \dots, k_{nk}\}$. Элементы модели связаны в граф взаимосвязей G , времена прохождения дуг заданы матрицей временных взаимосвязей M .

Требуется найти такое подмножество элементов модели (множество индикаторов) $I = \{i_1, i_2, \dots, i_{ni}\}$, чтобы выполнялись условия:

$$|I| = n_i \leq N_i,$$

$$\forall d \in D: \text{Alf}(d) \cap K \neq \emptyset \exists i \in I: i \in \text{Alf}_s(d).$$

$$\min_{d \in D, k \in K} \left(\max_{i \in I \cap \text{Alf}(d)} (dis^t(d, k) - dis^t(d, i)) \right) \rightarrow \max,$$

$$|I^{Alt}| \rightarrow \max; |I^{Bef}| \rightarrow \max,$$

$$\min_{T: I_T^{Alt} = I^{Alt}} (D(I_T^{Alt})) \rightarrow \min; \min_{T: I_T^{Bef} = I^{Bef}} (D(I_T^{Bef})) \rightarrow \min.$$

В виду ориентированности на системы высокой структурной, функциональной и размерностной сложности, а также учитывая противонаправленность сформулированных выше критериев, точные алгоритмы решения рассматриваемой задачи будут иметь слишком высокую вычислительную сложность. В силу этого решение данной задачи предложено осуществлять с использованием комбинации различных приближенных алгоритмов, строящих решения по отдельным критериям, либо модифицирующих некоторое заранее заданное по иным критериям эффективности размещение индикаторов [5, 12]. Существенная особенность практического применения алгоритмов решения рассматриваемой задачи заключается в том, что оно должно осуществляться с использованием интерактивных процедур взаимодействия с экспертами или специалистами в заданной предметной области. Такой подход позволяет значительно улучшить качество результатов решения поставленной задачи (вариантов размещения индикаторов) с точки зрения достижения поставленных целей.

Заключение

Основной целью предложенного индикаторного подхода является повышение надежности эксплуатируемых СТС и предотвращение ВЧС за счет раннего диагностирования отклонений от нормального функционирования технических систем. Индикаторный подход обеспечивает возможность снижения информационной нагрузки на ЛПР (диспетчера или оператора), одновременно с этим фокусируя его внимание на наиболее существенных с точки зрения обеспечения безопасности процессах на объекте управления. Рассматриваемый подход также, что не менее важно, позволяет локализовывать с необходимой точностью источники возникновения нештатных ситуаций.

Предложенные модели распространения возмущений в СТС являются основой для постановки и разработки формализованных методов решения задач своевременного выявления нештатных ситуаций в процессе эксплуатации СТС и предотвращения ВЧС. Разработанный индикаторный подход включает комплекс моделей и технологий анализа процессов воздействия угроз и распространения возмущений в сложных технических системах, а также методов решения многокритериальных задач оптимального размещения индикаторов в структуре СТС по критериям полноты, точности и своевременности обнаружения отказов различного типа.

Автоматизация процессов формирования множества индикаторов, а также обработки, визуализации и анализа

их показаний позволит использовать предложенные методы в рамках развития методологии УРРАН в части совершенствования технологий поддержки принятия решений в процессе управления ОИЖТ.

Библиографический список

1. Гапанович В.А. Развитие и внедрение технологии УРРАН на железнодорожном транспорте [Текст] / В.А. Гапанович // Надежность. – 2013. – № 4. – С. 3-17.
2. Гапанович В.А. Система адаптивного управления техническим содержанием инфраструктуры железнодорожного транспорта (проект УРРАН) [Текст] / В.А. Гапанович, И.Б. Шубинский, Е.Н. Розенберг, А.М. Замышляев // Надежность. – 2015. – № 2. – С. 4-22.
3. Кульба В.В. Методология исследования проблем обеспечения безопасности на железнодорожном транспорте [Текст] / В.В. Кульба, С.А. Косяченко, А.Б. Шелков // Управление большими системами. – 2012. – Специальный выпуск 38 «Проблемы управления на железнодорожном транспорте». – С. 5-19.
4. Баранов Л.А. Автоматическое управление движением поездов отечественных метрополитенов [Текст] / Л.А. Баранов // Мир транспорта. – 2018. – №3. – С. 156-165.
5. Кульба В.В. Использование сценарного и индикаторного подходов для управления живучестью, стойкостью и безопасностью сложных технических систем [Текст]: Научное издание / В.В. Кульба, Д.А. Кононов, С.А. Косяченко, А.А. Кочкаров, Д.С. Сомов. – М.: ИПУ РАН, 2011. – 116 с.
6. Быков А.А. О проблемах техногенного риска и безопасности техносферы [Текст] / А.А. Быков // Проблемы анализа риска. – 2012. – Том 9. – № 3. – С. 4-7.
7. Шульц В.Л. Управление техногенной безопасностью на основе сценарного и индикаторного подходов [Текст]: Научное издание / В.Л. Шульц, В.В. Кульба, А.Б. Шелков И.В. Чернов, Д.С. Сомов. – М.: ИПУ РАН, 2013. – 116 с.
8. Шульц В.Л. Методология управления техногенной безопасностью объектов инфраструктуры железнодорожного транспорта на основе индикаторного подхода [Текст] / В.Л. Шульц, В.В. Кульба, А.Б. Шелков, И.В. Чернов // Тренды и управление. – 2013. – № 3. – С. 4-23.
9. Модели и методы анализа и синтеза сценариев развития социально-экономических систем [Текст]: в 2-х кн. / Под ред. В.Л. Шульца, В.В. Кульбы. – М.: Наука, 2012. Кн. 1: –304 с. Кн. 2: – 358 с.
10. Эккерсон У. Панели индикаторов как инструмент управления. Ключевые показатели эффективности, мониторинг деятельности, оценка результатов [Текст] / У. Эккерсон. – М.: Изд-во Альпина Бизнес Букс, 2007. – 396 с.
11. Кормен Т. Алгоритмы. Построение и анализ [Текст]: 3-е издание / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн. – М.: Изд-во Вильямс, 2013. – 1324 с.
12. Кульба В.В. Применение структурно-интегрированных индикаторов в мониторинге сложных технических систем [Текст] / В.В. Кульба, Д.С. Сомов, А.А. Кочкаров. // Известия Южного федерального университета. Технические науки. – 2011. – № 3(116). – С. 52-65.

Сведения об авторах

Леонид А. Баранов – доктор технических наук, профессор, заведующий кафедрой, Российский университет транспорта (МИИТ), Российская Федерация, Москва, e-mail: baranov.miit@gmail.com

Владимир В. Кульба – доктор технических наук, профессор, заведующий лабораторией, Институт проблем управления им. В.А. Трапезникова РАН (ИПУ РАН), Российская Федерация, Москва, e-mail: kulba@ipu.ru

Алексей Б. Шелков – кандидат технических наук, ведущий научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН (ИПУ РАН), Российская Федерация, Москва, e-mail: abshelkov@gmail.com

Дмитрий С. Сомов – главный аналитик, ПАО Сбербанк, Российская Федерация, Москва, e-mail: somov.dmitry@gmail.com

Поступила: 27.02.2019

К вопросу о терминологии живучести авиационных конструкций

Вадим В. Ефимов, Московский государственный технический университет гражданской авиации, Российская Федерация, Москва



Вадим В. Ефимов

Резюме. Цель. Рассмотрены существующие определения живучести и эксплуатационной живучести авиационных конструкций. Сделана попытка дать однозначное определение живучести авиационных конструкций, которое в дальнейшем можно будет распространить и на летательный аппарат в целом и на другие сложные технические объекты. Основная задача настоящей работы состоит в том, чтобы четко разделить понятия надежности и живучести. Для обеспечения эффективности эксплуатации и безопасности полетов летательный аппарат должен обладать летной годностью – комплексной характеристикой летательного аппарата, определяемой реализованными в его конструкции принципами и решениями, позволяющей совершать безопасные полеты в ожидаемых условиях и при установленных методах эксплуатации. Ожидаемые условия эксплуатации описаны в Авиационных правилах – Нормах летной годности. Несмотря на то, что выполнение требований Норм летной годности обеспечивает достаточно высокий уровень безопасности полетов, особо ответственные элементы конструкции выполняют так, чтобы они оставались работоспособны даже в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации. Но надежность не может отвечать за работоспособность вне ожидаемых условий эксплуатации. Напрашивается вывод о том, что в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, за работоспособность должно отвечать другое свойство, а именно живучесть. **Методы.** При проведении настоящего исследования были использованы логический и вероятностный подходы. Были исследованы литературные источники, посвященные в основном проблемам надежности и живучести авиационных конструкций, а также других сложных технических объектов. Для наилучшего понимания различий и взаимосвязи понятий надежности и живучести был использован вероятностный подход. **Результаты.** После проведенного анализа литературных источников было сформулировано определение живучести как свойства объекта сохранять во времени способность выполнять требуемые функции в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, при установленных методах технического обслуживания, хранения и транспортирования. Кроме того, было предложено определение эксплуатационной живучести как свойства объекта сохранять во времени способность выполнять требуемые функции в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, в зависимости от методов технического обслуживания, хранения и транспортирования. При рассмотрении вероятностного подхода к разделению понятий надежности и живучести авиационных конструкций был использован известный ранее показатель реальной эффективности транспортного летательного аппарата, который представляется в виде математического ожидания показателя эффективности. Летательный аппарат может находиться либо в ожидаемых условиях эксплуатации, либо в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, третьего не дано. Тогда сумма вероятностей попадания летательного аппарата в эти условия должна равняться единице. Вероятность безотказной работы можно вычислить через вероятность противоположного события – вероятность отказа, которую можно представить в виде произведения вероятности попадания летательного аппарата в соответствующие условия эксплуатации и вероятности отказа в данных условиях. Для экстремальных условий, выходящих за рамки ожидаемых, можно использовать доработанные автором известные понятия поражаемости и уязвимости. **Выводы.** Получено определение живучести, имеющее четкое отличие от понятий надежности и отказобезопасности. Кроме того, предложено понятие эксплуатационной живучести, которое введено по аналогии с ранее введенным понятием эксплуатационной надежности.

Ключевые слова: живучесть, эксплуатационная живучесть, надежность, отказ, безотказность, отказобезопасность, авиационная конструкция, летательный аппарат.

Формат цитирования: Ефимов В.В. К вопросу о терминологии живучести авиационных конструкций // Надежность. 2019. №2. С. 42-47. DOI: 10.21683/1729-2646-2019-19-2-42-47

Введение

Любой летательный аппарат (ЛА) характеризуется широким набором свойств и параметров, среди которых присутствуют эксплуатационные свойства – совокупность свойств ЛА, которые проявляются в процессе эксплуатации. К ним относятся: надежность, живучесть, безопасность и эксплуатационная технологичность. Если термины надежности, безопасности и эксплуатационной технологичности рассмотрены в специальной литературе достаточно подробно и последовательно, а по некоторым терминам существуют даже соответствующие стандарты, то термин «живучесть» не имеет однозначной и общепринятой формулировки. Это относится не только к терминологии живучести ЛА, но и к терминологии живучести других объектов [1–5].

В настоящей работе сделана попытка дать однозначное определение живучести авиационных конструкций, которое в дальнейшем можно будет распространить и на ЛА в целом и на другие сложные технические объекты. Основная задача настоящей работы состоит в том, чтобы четко разделить понятия надежности и живучести, провести между ними четкую границу.

Основные понятия и определения теории живучести авиационных конструкций

Для обеспечения эффективности эксплуатации и безопасности полетов ЛА должен обладать летной годностью, которая закладывается при его создании и поддерживается в эксплуатации. *Летная годность* – это комплексная характеристика ЛА, определяемая реализованными в его конструкции принципами и решениями, позволяющая совершать безопасные полеты в ожидаемых условиях и при установленных методах эксплуатации [6]. В Нормах летной годности самолетов транспортной категории [7] дается определение *ожидаемым условиям эксплуатации* – это условия, которые известны из практики или возникновение которых можно с достаточным основанием предвидеть в течение срока службы ЛА с учетом его назначения. Эти условия включают в себя параметры состояния и факторы воздействия на ЛА внешней среды, эксплуатационные факторы, влияющие на безопасность полета.

Ожидаемые условия эксплуатации не включают в себя:

- экстремальные условия, встречи с которыми можно надежно избежать путем введения эксплуатационных ограничений и правил;
- экстремальные условия, которые возникают настолько редко, что требование выполнять Нормы летной годности в этих условиях привело бы к обеспечению более высокого уровня летной годности, чем это необходимо и практически обосновано.

Летная годность зависит от *надежности* ЛА, в том числе от надежности его конструкции, которая, в свою очередь, определяется прочностью конструкции.

На этапе проектирования ЛА его летная годность по условию прочности обеспечивается правильным выбором конструктивных решений, выполнением расчетов на прочность, жесткость и усталость, проведением соответствующих испытаний.

В процессе эксплуатации ЛА из-за усталостных и коррозионных повреждений, разрушения неметаллических материалов, попадания в экстремальные условия эксплуатации, выходящие за рамки ожидаемых условий, возможна потеря летной годности по условию прочности конструкции. В связи с этим при эксплуатации ЛА необходимо поддержание его летной годности путем проведения соответствующих мероприятий при техническом обслуживании и ремонте.

Несмотря на то, что выполнение требований Норм летной годности обеспечивает достаточно высокий уровень безопасности полетов, особо ответственные элементы конструкции выполняют так, чтобы они оставались работоспособны даже в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации. Но надежность не может отвечать за работоспособность вне ожидаемых условий эксплуатации, поскольку в соответствии с ГОСТ 27.002-2015 «Надежность в технике. Термины и определения» [8] надежность – это свойство объекта сохранять во времени способность выполнять требуемые функции в *заданных режимах и условиях применения*, технического обслуживания, хранения и транспортирования, а соответствии с терминологией Норм летной годности под заданными режимами и условиями применения следует понимать *ожидаемые условия эксплуатации*. Напрашивается вывод о том, что в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, за работоспособность должно отвечать другое свойство, а именно *живучесть*. Но подходит ли для этого какое-либо из существующих определений живучести? Рассмотрим существующую терминологию живучести авиационных конструкций и ЛА в целом.

В настоящее время терминология живучести не отражена в каком-либо ГОСТе. В предыдущей редакции вышеупомянутого ГОСТа по терминологии надежности (ГОСТ 27.002 – 89, [9]) существовало приложение, где было дано определение живучести, но не одно, а сразу три, что не способствовало однозначному пониманию этого термина. Приведем эти определения. Под живучестью понимают:

- 1) свойство объекта, состоящее в его способности противостоять развитию критических отказов из дефектов и повреждений при установленной системе технического обслуживания и ремонта,
- или
- 2) свойство объекта сохранять ограниченную работоспособность при воздействиях, не предусмотренных условиями эксплуатации,

или

3) свойство объекта сохранять ограниченную работоспособность при наличии дефектов или повреждений определенного вида, а также при отказе некоторых компонентов. Примером служит сохранение несущей способности элементами конструкции при возникновении в них усталостных трещин, размеры которых не превышают заданных значений.

Это своеобразная классификация существующих определений живучести. В литературе, посвященной живучести авиационных конструкций, нашли то или иное отражение все эти три типа определений, но наибольшее распространение получил третий из них. Приведем для примера определения живучести этого типа:

– живучесть – свойство конструкции сохранять прочность при наличии повреждений (в том числе усталостных) [10];

– живучесть – свойство конструкции выполнять свои функции, несмотря на полученные повреждения различной природы [11];

В соответствии с этими определениями, если возникло какое-либо повреждение, то работоспособность конструкции будет зависеть от ее свойства живучести. Но повреждение конструкции вполне может возникнуть в ожидаемых условиях эксплуатации. Это могут быть частичные отказы, причины которых кроются, например, в ошибках проектирования, некачественном изготовлении элементов конструкции. В качестве примера можно привести усталостные разрушения элементов, возникшие по причине ошибок в расчетах усталостной долговечности или по причине нанесения дефектов при изготовлении деталей, которые явились концентраторами напряжений.

Если конструкция имеет резервные элементы, т.е. создана с использованием принципа безопасного разрушения, то оставшиеся элементы конструкции обеспечат восприятие расчетной нагрузки, а значит, конструкция в целом останется работоспособной. Но тогда понятие живучести пересекается с понятием безотказности, которое является составной частью надежности. В соответствии с [8] *безотказность* – это свойство объекта непрерывно сохранять способность выполнять требуемые функции в течение некоторого времени или наработки в заданных режимах и условиях применения, т.е. в ожидаемых условиях эксплуатации, если использовать терминологию Норм летной годности. Как известно, одним из самых простых способов повышения безотказности является резервирование элементов. Если один или даже несколько параллельно работающих элементов (в случае многократного резервирования) откажут, то оставшиеся элементы обеспечат работоспособность объекта или его системы. Тогда в чем разница между вышеприведенными определениями живучести и безотказности? Очевидно, что разница может быть только в условиях эксплуатации, при которых возник дефект или частичный отказ. Если это произошло в ожидаемых условиях

эксплуатации, то за работоспособность должна отвечать надежность (безотказность), если это произошло в экстремальных условиях эксплуатации, выходящих за рамки ожидаемых условий, то за работоспособность должна отвечать живучесть. Но об этом в вышеприведенных определениях живучести ничего не говорится.

В некоторых работах вместе или вместо термина «живучесть» используется термин «эксплуатационная живучесть». Причем в это понятие также вкладывается различный смысл. Рассмотрим следующие определения:

– эксплуатационная живучесть – свойство, обеспечивающее нормальное выполнение заданных функций всеми системами ЛА в полете при наличии отказов или повреждений отдельных агрегатов, элементов, узлов [12];

– эксплуатационная живучесть авиационных конструкций – свойство конструкций ЛА обеспечивать безопасность эксплуатации по условиям прочности при частичном или полном разрушении силовых элементов из-за усталостных, коррозионных, случайных повреждений при эксплуатации, либо повреждений в процессе производства и ремонта [13].

Данные определения по смыслу ничем не отличаются от вышеприведенных определений живучести, а слово «эксплуатационная», по-видимому, используется для того, чтобы указать на то, что в данном случае речь не идет о боевой живучести, т.е. о живучести, связанной с воздействием боевых поражающих средств, а лишь о живучести, связанной с «обычной» эксплуатацией.

Но в некоторых работах [10, 11] в понятие «эксплуатационная живучесть» вкладывается иной смысл: эксплуатационная живучесть – обобщенный термин, характеризующий свойства конструкции и способы обеспечения ее безопасности по условиям прочности и включающий в себя допустимость повреждения и безопасность разрушения (повреждения). *Допустимость повреждения* – свойство конструкции и способ обеспечения ее безопасности по условиям прочности путем установления сроков первого и последующих осмотров конструкции в эксплуатации с целью обнаружения возможного повреждения и последующего ремонта конструкции или замены поврежденного элемента до наступления того состояния, когда снижение прочности окажется недопустимым. *Безопасность разрушения* (повреждения) – свойство конструкции и способ обеспечения ее безопасности по условиям прочности путем создания такой конструкции, при которой после возможного существенного повреждения или разрушения одного из основных силовых элементов остаточная прочность, несмотря на неотреставрированное состояние, не снизится более чем до допустимого уровня за интервал времени, в течение которого повреждение (разрушение) будет заведомо обнаружено.

Это определение достаточно громоздко и сложно для восприятия, но суть его сводится к тому, что живучесть – это свойство, обеспечивающее безопасность за счет

способности противостоять развитию критических отказов из возникших дефектов. Такое понятие эксплуатационной живучести можно отнести к первому типу определений в вышеприведенной классификации определений живучести. Но в данном случае оно пересекается с гостированным понятием *отказобезопасности* – свойства воздушного судна в целом и/или его функциональных систем, характеризующего способность обеспечивать безопасное завершение полета в ожидаемых условиях эксплуатации при возможных отказах на борту воздушного судна [14].

В связи со всем вышеизложенным наиболее логичным и последовательным представляется второй тип определений живучести. В работе [15] дается наиболее близкое ко второму типу определение: живучесть – свойство самолета сохранять работоспособное состояние при воздействии поражающих средств и нерасчетных нагрузок, а также при наличии накопившихся повреждений.

Если из данного определения исключить слова «а также при наличии накопившихся повреждений», то его можно считать вполне приемлемым.

Таким образом, по аналогии с вышеприведенным определением надежности можно дать следующее определение живучести: *живучесть* – это свойство объекта сохранять во времени способность выполнять требуемые функции в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, при установленных методах технического обслуживания, хранения и транспортирования.

Итак, любой объект и ЛА, в частности, может находиться либо в ожидаемых условиях эксплуатации, либо в экстремальных условиях эксплуатации, выходящих за рамки ожидаемых, третьего не дано. В ожидаемых условиях эксплуатации за работоспособность объекта отвечает надежность, в экстремальных – живучесть.

Понятие «эксплуатационная живучесть» также имеет право на существование. Если рассмотреть определение надежности и вышеприведенное рекомендуемое в настоящей работе определение живучести, то и в том и в другом случае рассматриваются установленные методы технического обслуживания, хранения и транспортирования. Но реальные условия эксплуатации характеризуются значительным разнообразием и нестабильностью из-за различия климатических условий, уровня подготовки летного и технического состава, материально-технической базы, организации технического обслуживания и ремонта и др. Таким образом, методы и условия технического обслуживания, хранения и транспортирования объекта могут отличаться от заданных. В связи с этим в работе [16] было введено понятие *эксплуатационной надежности*, которое можно сформулировать следующим образом: это свойство объекта сохранять во времени способность выполнять требуемые функции в ожидаемых условиях эксплуатации в зависимости от методов и условий технического обслуживания, хранения и транспортирования. По аналогии с данным определением можно сформулировать

определение *эксплуатационной живучести* – свойства объекта сохранять во времени способность выполнять требуемые функции в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, в зависимости от методов технического обслуживания, хранения и транспортирования.

Таким образом, надежность и живучесть оказываются взаимосвязанными, но четко разделенными понятиями, каждое из которых имеет свою зону ответственности.

Для лучшего понимания этого разделения рассмотрим различие и взаимосвязь надежности и живучести, используя вероятностный подход.

Вероятностный подход к разделению понятий надежности и живучести авиационных конструкций

Для того чтобы лучше разобраться в различии и взаимосвязи понятий надежности и живучести, используем подход, описанный в работе [15].

Рассмотрим показатель реальной эффективности транспортного ЛА, который можно представить в виде математического ожидания:

$$W = W_0 P_{\text{над}} P_{\text{жив}},$$

где W_0 – показатель исходной эффективности, определяемый функциональными свойствами ЛА (в основном, его летно-техническими характеристиками), при его абсолютной надежности и живучести. Это может быть, например, показатель производительной отдачи [17] $W_0 = m_{\text{ком}} L / m_0$, где $m_{\text{ком}}$ – максимальная масса коммерческой нагрузки, L – дальность полета при максимальной массе коммерческой нагрузки, m_0 – максимальная взлетная масса ЛА;

$P_{\text{над}}$ – показатель надежности (вероятность сохранения работоспособности в ожидаемых условиях эксплуатации);

$P_{\text{жив}}$ – показатель живучести (вероятность сохранения работоспособности в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации).

Показатель надежности можно представить в виде произведения вероятностей:

$$P_{\text{над}} = P_{\text{г}} P_{\text{п}} P_{\text{б/отк}},$$

где $P_{\text{г}}$ – коэффициент готовности;

$P_{\text{п}}$ – вероятность выполнения полета при условии нахождения ЛА в работоспособном состоянии;

$P_{\text{б/отк}}$ – вероятность безотказной работы за время выполнения полета в ожидаемых условиях эксплуатации.

Рассмотрим последовательно эти вероятности.

Для того чтобы ЛА мог выполнить полетное задание, изначально он должен находиться в работоспособном состоянии, что зависит от его свойства готовности. Количе-

ственно это оценивается соответствующей вероятностью P_p , которая называется коэффициентом готовности.

Чтобы выполнить полетное задание, ЛА, будучи в работоспособном состоянии, должен выполнять полет. Это зависит от многих причин, в том числе организационного характера, но если говорить только о свойствах ЛА, то это зависит, например, от технических возможностей его пилотажно-навигационного оборудования (возможность обеспечения полета в темное время суток, в сложных метеословиях). Возможность выполнения полета при условии нахождения ЛА в работоспособном состоянии оценивается соответствующей условной вероятностью P_n .

Однако в полете могут возникнуть *особые ситуации* – ситуации, возникающие в полете в результате воздействия неблагоприятных факторов или их сочетаний и приводящие к снижению безопасности полета [7], в том числе к авариям и катастрофам, в результате чего полетное задание не может быть выполнено. К неблагоприятным факторам относят отказы, экстремальные условия эксплуатации, ошибки экипажа и обслуживающего персонала.

В данной классификации неблагоприятных факторов под отказами обычно понимают нарушения работоспособности, возникающие в ожидаемых условиях эксплуатации. Это могут быть отказы, причины которых кроются в ошибках проектирования, некачественном изготовлении элементов конструкции и оборудования ЛА. Возможность появления подобных отказов оценивается соответствующей вероятностью $Q_{отк}$, а вероятность безотказной работы в ожидаемых условиях эксплуатации определяется по формуле:

$$P_{б/отк} = 1 - Q_{оуз} Q_{отк}, \quad (1)$$

где $Q_{оуз}$ – вероятность попадания ЛА в ожидаемые условия эксплуатации.

Поскольку, как было сказано выше, ЛА может находиться либо в ожидаемых условиях эксплуатации, либо в экстремальных условиях, выходящих за рамки ожидаемых условий эксплуатации, а третьего не дано, то сумма вероятностей попадания ЛА в эти условия должна равняться единице:

$$Q_{оуз} + Q_{эуз} = 1,$$

где $Q_{эуз}$ – вероятность попадания ЛА в экстремальные условия эксплуатации.

К счастью, $Q_{оуз} \gg Q_{эуз}$, причем $Q_{оуз} \cong 1$, в связи с чем в формуле (1) ее обычно опускают.

Но отказы могут быть также следствием попадания ЛА в экстремальные условия, выходящие за рамки ожидаемых условий эксплуатации. То есть отказы могут являться следствием нерасчетных внешних воздействий (например, воздействие одиночных порывов ветра, скорость которых превосходит значения, установленные Нормами летной годности, что может привести к

разрушению элементов конструкции или появлению остаточных деформаций, воздействие повышенной непрерывной атмосферной турбулентности, параметры которой также указаны в Нормам летной годности, что может привести к преждевременному израсходованию ресурса и, как следствие, к усталостному разрушению элемента конструкции, воздействие боевых поражающих средств), ошибок экипажа (например, грубая посадка или превышение максимально допустимого полетного значения перегрузки при маневре, что может привести к разрушению элементов конструкции или появлению остаточных деформаций) или ошибок обслуживающего персонала (например, нанесение дефектов на элементы конструкции при неаккуратном выполнении работ по техническому обслуживанию и ремонту и, как следствие, к преждевременному усталостному разрушению). В данном случае за выполнение полетного задания отвечает уже живучесть.

В соответствии с [15] живучесть ЛА определяется поражаемостью и уязвимостью. Доработаем формулировки этих понятий в соответствии с вышеизложенными соображениями. Тогда *поражаемость* – это свойство ЛА, характеризующее возможность его попадания в экстремальные условия, выходящие за рамки ожидаемых условий эксплуатации (показателем поражаемости является вероятность попадания ЛА в экстремальные условия эксплуатации – $Q_{эуз}$). *Уязвимость* – это свойство ЛА, характеризующее возможность нарушения его работоспособного состояния в результате воздействий, не предусмотренных ожидаемыми условиями эксплуатации (показателем уязвимости является вероятность потери работоспособности ЛА при условии воздействия, не предусмотренного ожидаемыми условиями эксплуатации – $Q_{уяз}$). С учетом этого по аналогии с формулой (1) выражение для показателя живучести, т.е. вероятности сохранения работоспособности в экстремальных условиях, имеет вид:

$$P_{жив} = 1 - Q_{эуз} Q_{уяз}.$$

Заключение

В настоящей работе сделана попытка дать однозначное определение живучести авиационных конструкций. Полученное определение можно распространить на ЛА в целом, а также на другие сложные технические объекты.

Выделять боевую живучесть в отдельное понятие не имеет смысла, т.к. воздействие на объект поражающих средств вполне укладывается в понятие воздействия неблагоприятных факторов.

Достоинством полученного определения живучести является его четкое отличие от гостированных понятий надежности и отказобезопасности.

Кроме того, предложено понятие эксплуатационной живучести, которое введено по аналогии с понятием эксплуатационной надежности.

По мнению автора настоящей работы, назрела необходимость закрепить понятие живучести в соответствующем ГОСТе или, по крайней мере, выпустить приложение к ГОСТ 27.002-2015, подобно приложению к ранее действовавшему ГОСТ 27.002-89, но с учетом изложенных в настоящей работе предложений.

Библиографический список

1. Черкесов Г.Н. Анализ функциональной живучести структурно-сложных технических систем [Текст] / Г.Н. Черкесов, А.О. Недосекин, В.В. Виноградов // Надежность. – 2018. – №18(2). – С. 17-24. DOI:10.21683/1729-2646-2018-18-2-17-24
2. Черкесов Г.Н. Описание подхода к оценке живучести сложных структур при многоразовых воздействиях высокой точности [Текст] / Г.Н. Черкесов, А.О. Недосекин // Надежность. – 2016. – № 16(2). – С. 3-15. DOI:10.21683/1729-2646-2016-16-2-3-15
3. Зарубский В.Г. Особенности организации процесса функционального диагностирования управляющего компьютера повышенной живучести [Текст] / В.Г. Зарубский // Надежность. – 2016. – № 16(3). – С. 35-38. DOI:10.21683/1729-2646-2016-16-3-35-38
4. Юркевич Е.В. Особенности информационной поддержки в обеспечении живучести космического аппарата при электрофизических воздействиях [Текст] / Е.В. Юркевич, Л.Н. Крюкова, С.А. Салтыков // Надежность. – 2016. – № 16(4). – С. 30-35. DOI:10.21683/1729-2646-2016-16-4-30-35
5. Климов С.М. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий [Текст] / С.М. Климов, С.В. Поликарпов, А.В. Федченко // Надежность. – 2017. – № 17(3). – С. 32-40. DOI:10.21683/1729-2646-2017-17-3-32-40
6. Смирнов Н.Н. Сохранение летной годности воздушных судов [Текст] / Н.Н. Смирнов Н.Н., Ю.М. Чинючин, С.П. Тарасов. – М.: МГТУ ГА, 2005. – 78 с.
7. Авиационные правила. Часть 25. Нормы летной годности самолетов транспортной категории: утв. Постановлением 23-ей сессии Совета по авиации и использованию воздушного пространства 5 сентября 2003 года. – М.: ОАО «Авиаиздат», 2004. – 237 с.
8. ГОСТ 27.002-2015. Надежность в технике. Термины и определения [Текст]. – Введ. 2016–06–21. – М.: Стандартинформ, 2016. – IV, 27 с.
9. ГОСТ 27.002-89. Надежность в технике. Термины и определения [Текст]. – Введ. 1990-07-01. – М.: ИПК Издательство стандартов, 1990. – 38 с.
10. Арепьев А.Н. Вопросы эксплуатационной живучести авиаконструкций [Текст] / А.Н. Арепьев, М.С. Громов, В.С. Шапкин. – М.: Воздушный транспорт, 2002. – 424 с.
11. Бутушин С.В. Обеспечение летной годности воздушных судов гражданской авиации по условиям прочности [Текст] / С.В. Бутушин, В.В. Никонов, Ю.М. Фейгенбаум, В.С. Шапкин. – М.: МГТУ ГА, 2013. – 772 с.
12. Смирнов Н.Н. Основы теории технической эксплуатации летательных аппаратов [Текст]: Часть 2 / Н.Н. Смирнов. – М.: МГТУГА, 2003. – 87 с.
13. Авиация: энциклопедия / Гл. ред. Г. П. Свищев. – М.: Большая Российская энциклопедия, 1994. – 736 с.
14. ГОСТ Р 56079-2014. Изделия авиационной техники. Безопасность полета, надежность, контролепригодность, эксплуатационная и ремонтная технологичность. Номенклатура показателей [Текст]. – Введ. 2014-07-14. – М.: Стандартинформ, 2014. – II, 14 с.
15. Анцелиович Л.Л. Надежность, безопасность и живучесть самолета [Текст] / Л.Л. Анцелиович. – М.: Машиностроение, 1985. – 296 с.
16. Герасимова Е.Д. Эксплуатационная надежность и режимы технического обслуживания ЛА и АД [Текст] / Е.Д. Герасимова, Н.Н. Смирнов, И.Ф. Полякова. – М.: МГТУГА, 2002. – 58 с.
17. Шейнин В.М. Весовое проектирование и эффективность пассажирских самолетов. Т. 2. Расчет центровки и моментов инерции самолета. Весовой анализ [Текст] / В.М. Шейнин, В.И. Козловский. – М.: Машиностроение, 1977. – 208 с.

Сведения об авторе

Вадим В. Ефимов – доктор технических наук, доцент, профессор Московского государственного технического университета гражданской авиации, Российская Федерация, Москва, e-mail: efimowww@yandex.ru

Поступила: 19.11.2018

Экономическая оценка аварийного риска воздействия природных чрезвычайных ситуаций при движении поездов

Владимир Г. Попов, Российский университет транспорта (МИИТ), Российская Федерация, Москва

Филипп И. Сухов, Российский университет транспорта (МИИТ), Российская Федерация, Москва

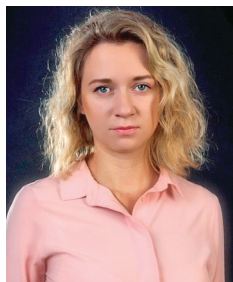
Юлия К. Боландова, Российский университет транспорта (МИИТ), Российская Федерация, Москва



Владимир Г. Попов



Филипп И. Сухов



Юлия К. Боландова

Резюме. Цель. Статья посвящена вопросу оценки риска транспортного происшествия, обусловленного воздействием природных чрезвычайных ситуаций, при движении поездов по определенному маршруту. Постоянно увеличивающаяся антропогенная нагрузка на окружающую среду неизбежно приводит к изменениям климата, которые в свою очередь провоцируют увеличение числа экстремальных погодных явлений. Последние, как правило, инициируют техногенные аварии и катастрофы. Оценка факторов климатического риска, количественно характеризующих последствия влияния на инфраструктуру железнодорожного транспорта, служит отправным моментом для управления рисками бедствий и адаптации человеческой деятельности к постоянно изменяющемуся климату. **Методы.** Авторы данной статьи предлагают метод оценки риска, учитывающий влияние различных видов природных чрезвычайных ситуаций, воздействующих на подвижной состав в процессе его следования. В основе этого метода лежат элементы теории вероятностей и математической статистики. Благодаря разработанной методике можно произвести оценку риска транспортного происшествия, вызванного природными чрезвычайными ситуациями, при движении поездов не только для конкретного участка железной дороги, но и для определенного маршрута или направления на сети железных дорог. **Результаты.** Для маршрута «Невинномысская – Туапсе», состоящего из 6 участков Северо-Кавказской железной дороги, один из которых был поврежден в результате выпадения обильных осадков 24-25 октября 2018 года, был рассчитан риск транспортного происшествия в результате воздействия на социотехническую систему этого направления трех видов ЧС природного характера, а именно:

- наводнения;
- урагана с силой ветра более 22 м/с;
- сильного дождя.

Параметры этих чрезвычайных ситуаций охарактеризованы следующими составляющими:

- частота возникновения среди других видов ЧС;
- среднее годовое число природных ЧС;
- характерный пространственный масштаб природной ЧС;
- характерное время действия природной ЧС.

Условные вероятности воздействия на социо-техническую систему железнодорожного транспорта события, имеющего характерный пространственный и временной масштаб, и приведшего к транспортному происшествию с поездом, были оценены из предположения, что поток поездов в пространстве подчиняется нормированному закону Эрланга k -го порядка. Риск транспортного происшествия при движении поезда в четном и нечетном направлениях по i -му участку j -ой железной дороги, вызванного опасным воздействием природного ЧС m -го вида определен с учетом совместности событий. С помощью метода дисконтирования получено уравнение для оценки математического ожидания экономического ущерба от нарушений безопасности движения, что позволило оценить экономическую составляющую риска. **Выводы.** В результате предложен метод оценки риска транспортного происшествия вследствие воздействия природной ЧС, приведен пример оценки данного риска, включая эту экономическую составляющую, для направления движения «Невинномысская – Туапсе».

Ключевые слова: аварийный риск, аварийные ситуации, чрезвычайные ситуации, железнодорожный транспорт, чрезвычайные ситуации природного характера, грузовые железнодорожные перевозки, нарушения безопасности движения.

Формат цитирования: Попов В.Г., Сухов Ф.И., Боландова Ю.К. Экономическая оценка аварийного риска воздействия природных чрезвычайных ситуаций при движении поездов // Надежность. 2019. №2. С. 48-53. DOI: 10.21683/1729-2646-2019-19-2-48-53

Современная мировая статистика свидетельствует о растущем во всем мире ущербе от опасных погодных и климатических явлений. Из диаграммы (рис. 1) видно, что 90% самых тяжелых экономических потерь приходится не на геофизические явления, такие, как извержения вулканов, цунами и землетрясения, а на метеорологические, климатические и гидрологические явления окружающей среды: паводки, наводнения, сильный ветер, ливневые дожди, град, засухи [1].

Следует отметить, что опасные явления климата могут инициировать техногенные чрезвычайные ситуации (ЧС). К большим социальным и экономическим потерям привели сели, сопровождавшие мощный циклон с проливными дождями 6–9 августа 2002 г. на Черноморском побережье России, в районе г. Новороссийска. По данным оперативных сводок МЧС России, 6 августа мощные грязекаменные потоки, общий объем которых превышал 15 тыс. м³, разрушили 300 метров железной дороги на участке между Сочи и Туапсе, а также проходящую рядом автотрассу. Было заблокировано движение 47 пассажирских поездов. Прямой экономический ущерб от рассматриваемого бедствия составил, по предварительным оценкам, более 71 млн долл. [2].

В результате выпадения обильных осадков 24–25 октября 2018 г. (275–330 мм) в трех муниципальных образованиях Краснодарского края повреждены два автомобильных и один железнодорожный мост, участки автомобильных дорог «Туапсе – Майкоп» и «Джубга – Сочи», железнодорожное полотно на перегонах «Туапсе – Кривенковская» и «Туапсе – Адлер». Были отменены 36 и задержаны 39 пассажирских поездов.

Бесперебойная и безопасная работа железнодорожного транспорта во многом зависит от условий климата. Оценка факторов климатического риска, количественно характеризующих последствия влияния на инфраструктуру железнодорожного транспорта, служит отправным моментом для управления рисками бедствий и адаптации человеческой деятельности к постоянно изменяющемуся климату.

Оценка риска состоит в его количественном измерении [3], чтобы количественно оценить риск, требуются проведение анализа вероятностей возникновения опасностей и последствий реализации этих опасностей.

Основной задачей управления рисками на железнодорожном транспорте является достижение и поддержание допустимого уровня риска при обеспечении функциональной безопасности объектов инфраструктуры и подвижного состава [4]. Последнее время особое внимание уделяется вопросам надежности подвижного состава и разработкам систем и методов оценки и управления рисками для решения задач по обеспечению безопасности транспортных процессов [5–8]. Однако в последних исследованиях, посвященных этой проблеме, система функционирования инфраструктуры железнодорожного транспорта рассматривается в отрыве от окружающей среды. В данной статье предлагается метод оценки риска транспортного происшествия, учитывающий влияние различных видов ЧС природного характера.

Под транспортным происшествием в данной статье понимаются крушения, аварии, а также сходы и столкновения железнодорожного подвижного состава, не имеющие последствий крушения и аварии, в соответствии с



Рисунок 1 – Количество природных катастроф за период 1980–2016 гг.

классификацией Приказа Минтранса от 18 декабря 2014 года № 344 [10].

Для характеристики ЧС природного характера введем следующие обозначения:

$C_{j,i,m}$ – событие, представляющее собой ЧС m -го вида, природного характера, произошедшее в географическом районе России, на территории которого находится i -й участок j -ой железной дороги;

$D_{j,i,m}$ – событие, характеризующее воздействие ЧС природного характера m -го вида (события $C_{j,i,m}$) на социотехническую систему железнодорожного транспорта на i -ом участке j -ой железной дороги и приводящее к транспортному происшествию;

$B_{j,i,m} = D_{j,i,m} \times C_{j,i,m}$ – транспортное происшествие [10], вызванное воздействием ЧС природного характера m -го вида на социотехническую систему железнодорожного транспорта на i -ом участке j -ой железной дороги;

$N_{j,i,m}$ – среднее годовое число природных ЧС m -го вида, происходящих в географическом районе России, на территории которого находится i -й участок j -ой железной дороги ($m = 1, 2, \dots, M$), 1/год;

$L_{j,i,m}$ – характерный пространственный масштаб природного ЧС m -го вида, происходящего в географическом районе России, на территории которого находится i -й участок j -ой железной дороги ($m = 1, 2, \dots, M$), км;

$T_{j,i,m}$ – характерное время действия природного ЧС m -го вида, происходящего в географическом районе России, на территории которого находится i -й участок j -ой железной дороги ($m = 1, 2, \dots, M$), ч;

Оценка вероятности транспортного происшествия при движении поезда в четном направлении по i -му участку j -ой железной дороги, вызванного природной ЧС m -го вида, производится по формуле:

$$\begin{aligned} R''(B_{j,i,m}) &= R''(D_{j,i,m} \times C_{j,i,m}) = \\ &= P''(C_{j,i,m}) \cdot P''(D_{j,i,m} | C_{j,i,m}), \end{aligned} \quad (1)$$

где $P''(D_{j,i,m} | C_{j,i,m}) = P''(L_{j,i,m} | C_{j,i,m}) \cdot P''(T_{j,i,m} | C_{j,i,m})$.

$P''(C_{j,i,m})$ – вероятность возникновения в данном географическом районе природного ЧС m -го вида, характерного пространственного масштаба – $L_{j,i,m}$ за среднее время нахождения поезда, движущего в четном направлении по i -му участку, протяженностью $L_{j,i}$ [9];

$$P''(C_{j,i,m}) = 1 - \exp\left(-\frac{N_{j,i,m} \cdot t''_{j,i}}{365 \cdot 24}\right), \quad (2)$$

где $t''_{j,i} = L_{j,i} / V''_{j,i}$, $V''_{j,i}$ – участковая скорость движения поездов на i -ом участке j -ой железной дороги в четном направлении, км/час;

$P''(L_{j,i,m} | C_{j,i,m})$ – условная вероятность воздействия на социотехническую систему железнодорожного транспорта события $C_{j,i,m}$ характерного пространственного масштаба $L_{j,i,m}$, приведшего к транспортному происшествию с поездом, движущимся в четном направлении на i -ом участке j -ой железной дороги [9]

$$\begin{aligned} P''(L_{j,i,m} | C_{j,i,m}) &= 1 - \exp(-k_x \lambda''_x L_{j,i,m}) \sum_{k=0}^{k_x-1} \frac{(k_x \lambda''_x L_{j,i,m})^k}{k!}; \\ \lambda''_x &= 1 / \Delta \bar{X}''_{j,i}, \end{aligned} \quad (3)$$

где k_x – порядок нормированного распределения Эрланга;

$\Delta \bar{X}''_{j,i} = V''_{j,i} \times \Delta \bar{T}''_{j,i}$ – средний пространственный интервал между поездами, движущимися в четном направлении на i -ом участке j -ой железной дороги, км;

$\Delta \bar{T}''_{j,i}$ – средний временной интервал между поездами, движущимися в четном направлении на i -ом участке j -ой железной дороги, ч;

$P''(T_{j,i,m} | C_{j,i,m})$ – условная вероятность воздействия на социотехническую систему железнодорожного транспорта события $C_{j,i,m}$ характерного временного масштаба $T_{j,i,m}$, приведшего к транспортному происшествию с поездом, движущимся в четном направлении на i -ом участке j -ой железной дороги [9]

$$\begin{aligned} P''(T_{j,i,m} | C_{j,i,m}) &= 1 - \exp(-k_t \lambda''_t T_{j,i,m}) \sum_{k=0}^{k_t-1} \frac{(k_t \lambda''_t T_{j,i,m})^k}{k!}; \\ \lambda''_t &= 1 / \Delta \bar{T}''_{j,i}, \end{aligned} \quad (4)$$

где k_t – порядок нормированного распределения Эрланга

В выражении (1), записанном для оценки вероятности транспортного происшествия при движении поезда в нечетном направлении по i -му участку j -ой железной дороги $R'(B_{j,i,m})$, соответствующие значения $P'(C_{j,i,m})$, $P'(L_{j,i,m} | C_{j,i,m})$, $P'(T_{j,i,m} | C_{j,i,m})$ определяются по формулам, аналогичным для четного направления движения поездов при соответствующей замене данных.

Тогда вероятность транспортного происшествия $R(B_{j,i,m})$ при движении поездов в четном и нечетном направлениях по i -му участку j -ой железной дороги, вызванного опасным воздействием природного ЧС m -го вида, можно определить по формуле (с учетом совместности событий):

$$R(B_{j,i,m}) = R''(B_{j,i,m}) + R'(B_{j,i,m}) - R''(B_{j,i,m}) \times R'(B_{j,i,m}). \quad (5)$$

Из формул (1), (5) можно получить следующие оценки вероятности транспортного происшествия при движении поезда.

I. Оценку вероятности транспортного происшествия при движении поезда по i -му участку j -ой железной дороги, вызванного всеми возможными природными ЧС M видов ($m = 1, 2, 3, \dots, M$), произведем по следующим формулам:

при движении поезда в четном направлении

$$R''(B^M_{j,i}) = \sum_{m=1}^M \phi_m \cdot R''(B_{j,i,m}), \quad (6)$$

при движении поезда в нечетном направлении

$$R'(B_{j,i}^M) = \sum_{m=1}^M \phi_m \cdot R'(B_{j,i,m}^M), \quad (7)$$

при движении поездов в четном и нечетном направлениях

$$R(B_{j,i}^M) = R''(B_{j,i}^M) + R'(B_{j,i}^M) - R''(B_{j,i}^M) \cdot R'(B_{j,i}^M), \quad (8)$$

где ϕ_m – частота возникновения ЧС m -го вида среди других видов ЧС, $\sum_{m=1}^M \phi_m = 1$;

$B_{j,i}^M$ – транспортное происшествие – событие, последовавшее после воздействия всех возможных M видов ЧС природного характера на социотехническую систему железнодорожного транспорта на i -м участке j -ой железной дороги.

II. Оценку вероятности транспортного происшествия при движении поезда по I ($i = 1, 2, 3, \dots, I$) участкам j -ой железной дороги, вызванного природной ЧС m -го вида, произведем по следующим формулам:

при движении поезда в четном направлении

$$R''(B_{j,m}^I) = 1 - \prod_{i=1}^I [1 - R''(B_{j,i,m}^I)], \quad (9)$$

при движении поезда в нечетном направлении

$$R'(B_{j,m}^I) = 1 - \prod_{i=1}^I [1 - R'(B_{j,i,m}^I)], \quad (10)$$

при движении поездов в четном и нечетном направлениях

$$R(B_{j,m}^I) = 1 - \prod_{i=1}^I [1 - R(B_{j,i,m}^I)], \quad (11)$$

где $B_{j,i}^I$ – транспортное происшествие – событие, последовавшее после воздействия ЧС m -го вида природного характера на социотехническую систему железнодорожного транспорта на I ($i = 1, 2, 3, \dots, I$) участках j -ой железной дороги.

III. Оценку вероятности транспортного происшествия при движении поезда по I ($i = 1, 2, 3, \dots, I$) участкам j -ой железной дороги, вызванного всеми возможными ЧС природного характера, произведем по следующим формулам:

при движении поезда в четном направлении:

$$R''(B_j^{I,M}) = 1 - \prod_{i=1}^I [1 - R''(B_{j,i}^M)], \quad (12)$$

при движении поезда в нечетном направлении:

$$R'(B_j^{I,M}) = 1 - \prod_{i=1}^I [1 - R'(B_{j,i}^M)], \quad (13)$$

при движении поездов в четном и нечетном направлениях:

$$R(B_j^{I,M}) = 1 - \prod_{i=1}^I [1 - R(B_{j,i}^M)], \quad (14)$$

где $B_j^{I,M}$ – событие, последовавшее после воздействия всех возможных M видов ЧС природного характера

на социотехническую систему железнодорожного транспорта на I ($i = 1, 2, 3, \dots, I$) участках j -ой железной дороги.

IV. Оценку вероятности транспортного происшествия при движении поезда по I участкам ($i = 1, 2, 3, \dots, I$) железных дорог ($j = 1, 2, 3, \dots, J$), вызванного всеми возможными ЧС природного характера, произведем по следующим формулам:

при движении поезда в четном направлении

$$R''(B^{J,I,M}) = 1 - \prod_{j=1}^J [1 - R''(B_j^{I,M})], \quad (15)$$

при движении поезда в нечетном направлении

$$R'(B^{J,I,M}) = 1 - \prod_{j=1}^J [1 - R'(B_j^{I,M})], \quad (16)$$

при движении поездов в четном и нечетном направлениях

$$R(B^{J,I,M}) = 1 - \prod_{j=1}^J [1 - R(B_j^{I,M})], \quad (17)$$

где $B^{J,I,M}$ – транспортное происшествие – событие, последовавшее после воздействия всех возможных M видов ЧС природного характера на социотехническую систему железнодорожного транспорта на I ($i = 1, 2, 3, \dots, I$) участках J ($j = 1, 2, 3, \dots, J$) железных дорог.

Если в формулах (9) – (14) в качестве I взять все участки j -ой железной дороги, то можно получить соответствующие оценки аварийных рисков для j -ой железной дороги в целом ($j = 1, 2, 3, \dots, J$). Если в формулах (15) – (17) взять I участков ($i = 1, 2, 3, \dots, I$) J железных дорог ($j = 1, 2, 3, \dots, J$), то можно получить соответствующие оценки аварийных рисков для различных маршрутов и направлений движения поездов.

Для экономической оценки последствий транспортного происшествия воспользуемся данными работ [11–16]. Согласно [10] транспортные происшествия – нарушения безопасности движения (НБД) поездов – подразделяются на крушение – B_1 , аварию – B_2 ; транспортное происшествие (сход или столкновение поезда без последствий крушения или аварии) – B_3 .

Используя метод дисконтирования [11] и статистические данные работ [12, 13], можно записать уравнение для оценки математического ожидания экономического ущерба от НБД B_n ($B_n = B_1, B_2, B_3$):

$$Y(B_n) = Y_0(B_n)(1+r)^p, \quad (18)$$

где $Y_0(B_1) = 2 \cdot 10^6$ руб., $Y_0(B_2) = 0,5 \cdot 10^6$ руб., $Y_0(B_3) = 7 \cdot 10^3$ руб. – средние значения экономического ущерба от одного события видов B_1, B_2, B_3 в ценах 2000 г.;

$p = \Gamma - 2000$ – условный номер года;

Γ – календарный год анализа риска;

r – норма дисконтирования ($r = 0,1-0,12$).

Практическая невозможность прогнозных оценок экономического ущерба от возникновения НБД определенного вида B_n при воздействии природных ЧС на со-

циотехническую систему железнодорожного транспорта и приводящих к транспортным происшествиям при движении поездов, заставляет обращаться к использованию консервативных допущений и апостериорных статистических данных по НБД поездов. С учетом этого можно записать уравнение

$$Y(B) = \sum_{n=1}^3 \alpha_n \cdot Y(B_n), \quad (19)$$

где α_n – относительные частоты появления определенного вида НБД B_n ($n = 1, 2, 3$), которые по данным работ [14, 16] можно оценить как $\alpha_1 = 0,01$, $\alpha_2 = 0,1$, $\alpha_3 = 0,89$.

Тогда экономическую оценку риска транспортного происшествия с поездом при движении по i -у участку j -ой железной дороги, вызванного природной ЧС m -го вида, можно получить по формулам:

в четном направлении $R''_3(B_{j,i,m}) = R''(B_{j,i,m}) \cdot Y(B)$;
в нечетном направлении $R'_3(B_{j,i,m}) = R'(B_{j,i,m}) \cdot Y(B)$;
в четном и нечетном направлениях

$$R_3(B_{j,i,m}) = R(B_{j,i,m}) \cdot Y(B). \quad (20)$$

Экономическую оценку рисков для случаев $B_{j,m}^I \cdot B_j^{I,M}$; $B_{j,i}^{I,M}$ (для I участков на одной железной дороге или на J железных дорогах) можно получить аналогично, умножив соответствующие вероятности возникновения транспортных происшествий (формулы (6) – (17)) на величину ущерба $Y(B)$.

Оценим вероятности транспортного происшествия $R(B_{j,i}^M)$ при движении поездов по маршруту «Невинномысская – Туапсе», состоящего из 6 участков ($i = 1, 2, 3, \dots, 6$) Северо-Кавказской железной дороги в результате воздействия на социотехническую систему этого направления трех видов ЧС природного характера, а именно:

– наводнения ($m = 1$); частота возникновения среди других видов ЧС $\phi_1 = 0,06$; среднее годовое число $N_1 = 1$; характерный пространственный масштаб $L_1 = 15$ км; характерное время действия $T_1 = 1$ ч;

– урагана с силой ветра более 22 м/с ($m = 2$); частота возникновения среди других видов ЧС $\phi_2 = 0,11$; среднее годовое число природных ЧС $N_2 = 2$; характерный пространственный масштаб природного ЧС $L_2 = 300$ км; характерное время действия $T_2 = 120$ ч;

– сильного дождя ($m = 3$); частота возникновения среди других видов ЧС $\phi_3 = 0,83$; среднее годовое число природных ЧС $N_3 = 15$; характерный пространственный масштаб природного ЧС $L_3 = 1$ км; характерное время действия $T_3 = 3$ ч.

Результаты расчета приведены в таблице 1.

Пользуясь формулой (14), произведем оценку вероятности транспортного происшествия при движении поездов по 6 ($i = 1, 2, 3, \dots, 6$) участкам Северо-Кавказской железной дороги ($j = 1$), вызванного тремя опасными состояниями ($M = 3$) объектов окружающей среды: $R(B_{j,i}^{6,3}) = 4,295 \cdot 10^{-4}$. При этом математическое ожидание экономического ущерба от НБД в пересчете на 2019 год составит $Y(B) = 429474,42$ руб. (формула (19)).

Тогда экономическая оценка риска транспортного происшествия с поездом при движении по 6 участкам ($i = 1, 2, 3, \dots, 6$) Северо-Кавказской железной дороги ($j = 1$) составит (по аналогии с формулой (20)):

$$R_3(B_j^{I,M}) = R(B_j^{I,M}) \cdot Y(B) = R(B_1^{6,3}) \cdot Y(B) = \\ = 4,295 \cdot 10^{-4} \cdot 429474,42 \approx 184,45 \text{ руб.}$$

Если, например, рассматривать стоимость транспортировки 1 т опасного груза по этому маршруту, составляющую по приблизительным расчетам 6000 руб., то полученная экономическая оценка может рассма-

Таблица 1 – Результаты расчета вероятностей транспортного происшествия

i	Наименование участка	Длина участка, км	Размер движения, поездов/сут	Наводнение ($m = 1$; $\phi_1 = 0,06$; $N_1 = 1$; $L_1 = 15$; $T_1 = 1$)	Ураган с силой ветра более 22 м/с ($m = 2$; $\phi_2 = 0,11$; $N_2 = 2$; $L_2 = 300$; $T_2 = 120$)	Сильный дождь ($m = 3$; $\phi_3 = 0,83$; $N_3 = 15$; $L_3 = 1$; $T_3 = 3$)	Вероятность $R(B_{j,i}^M)$
				Вероятность $R(B_{j,i,m})$	Вероятность $R(B_{j,i,m})$	Вероятность $R(B_{j,i,m})$	
1	Невинномысская – Армавир Ростовский	77	46	$1,506 \cdot 10^{-4}$	$9,058 \cdot 10^{-4}$	$1,028 \cdot 10^{-9}$	$1,087 \cdot 10^{-4}$
2	Армавир Ростовский – Курганная	40,5	40	$5,165 \cdot 10^{-5}$	$4,765 \cdot 10^{-4}$	$2,122 \cdot 10^{-10}$	$5,552 \cdot 10^{-5}$
3	Курганная – Белореченская	63,8	41	$8,830 \cdot 10^{-5}$	$7,506 \cdot 10^{-4}$	$3,944 \cdot 10^{-10}$	$8,786 \cdot 10^{-5}$
4	Белореченская – Комсомольская	19,8	42	$2,961 \cdot 10^{-5}$	$2,33 \cdot 10^{-4}$	$1,44 \cdot 10^{-10}$	$2,741 \cdot 10^{-5}$
5	Комсомольская – Кривенковская	87,6	42	$1,31 \cdot 10^{-4}$	$1,03 \cdot 10^{-3}$	$6,361 \cdot 10^{-10}$	$1,212 \cdot 10^{-4}$
6	Кривенковская – Туапсе	18,2	77	$8,89 \cdot 10^{-5}$	$2,142 \cdot 10^{-4}$	$7,187 \cdot 10^{-9}$	$2,89 \cdot 10^{-5}$

триваться как страховая сумма при управлении риском (обработке риска) путем его передачи.

Библиографический список

1. Доклад о климатических рисках на территории Российской Федерации [Текст] / Под ред. д.ф.-м.н. В.М. Катцова. – Санкт-Петербург, 2017. – 106 с.
2. Оценка и управление природными рисками: тематический том [Текст] / Под ред. А.Л. Рагозина. – М.: Издательская фирма «КРУК», 2003. – 320 с.
3. **Акимов В.А.** Основы анализа и управления риском в природной и техногенной сферах [Текст] / В. А. Акимов, В. В. Лесных, Н. Н. Радаев. – М.: Деловой экспресс, 2004. – 352 с.
4. **ГОСТ 33433-2015.** Безопасность функциональная Управление рисками на железнодорожном транспорте [Текст]. – Введ. 2016-09-01. – М.: Стандартинформ, 2016. – IV, 34 с.
5. **Володарский В.А.** О надежности подвижного состава, прошедшего ремонт [Текст] / В.А. Володарский, А.И. Орленко // Надежность. – 2015. – №1(52). – С. 25-28.
6. **Замышляев А.М.** Функциональная зависимость между количеством вагонов в сходе из-за неисправностей вагонов или пути и факторами движения [Текст] / А.М. Замышляев, А.Н. Игнатов, А.И. Кибзун, Е.О. Новожилов // Надежность. – 2018. – №18(1). – С. 53-60.
7. **Даев Ж.А.** Применение статистических критериев для улучшения эффективности методов оценки рисков [Текст] / Ж.А. Даев, Е.Т. Нурушев // Надежность. – 2018. – №18(2). – С. 42-45.
8. **Аксенов В.А.** Совершенствование системы управления рисками для решения задач по обеспечению безопасности производственных процессов [Текст] / В.А. Аксенов, Д.Л. Раенок, А.М. Завьялов // Надежность. – 2013. – №3. – С. 103-120.
9. **Попов В.Г.** Оценка аварийного риска при движении поездов в результате воздействия чрезвычайных ситуаций природного характера, возникающих в окружающей среде [Текст] / Попов В.Г., Сухов Ф.И., Боландова Ю.К. // Наука и техника транспорта. – 2018. – №4. – С. 115-120.
10. Приказ Минтранса РФ от 18 декабря 2014 г. №344 Об утверждении положения о классификации,

порядке расследования и учета транспортных происшествий и иных событий, связанных с нарушением правил безопасности движения и эксплуатации железнодорожного транспорта (Зарегистрировано в Минюсте РФ 26.02.2015 № 36209).

11. **Легасов В.А.** Дисконтирование и компромисс между поколениями [Текст] / В.А. Легасов, В.Ф. Демин, Я.В. Шевелев // Проблемы анализа риска. – 2005. – Т. 2. – №2. – С. 141-146.
12. **Красковский А.Е.** Экономические механизмы управления безопасностью движения [Текст] / А.Е. Красковский // Железнодорожный транспорт. – 2002. – №5. – С. 29-33.
13. **Попов В.Г.** Индекс прогноз и индекс отклик [Текст] / В.Г. Попов, Ф.И. Сухов // Мир транспорта. – 2007. – Т. 5. – №3. – С. 130-133.
14. **Попов В.Г.** Метод оценки уровня безопасности движения и аварийного риска при перевозке грузов по железным дорогам [Текст] / В.Г. Попов // Транспорт: наука, техника, управление. – 2008. – №7. – С. 1-5.
15. **Попов В.Г.** Метод оценки аварийного риска при перевозке нефти и нефтепродуктов по железным дорогам [Текст] / В.Г. Попов, С.В. Петров // Безопасность жизнедеятельности. – 2010. – №11. – С. 39-43.
16. **Попов В.Г.** Оценка риска от аварийных происшествий. [Текст] / Попов В.Г., Сухов Ф.И., Петров С.В. // Мир транспорта. – 2012. – Т. 10. – №6. – С. 150-155.

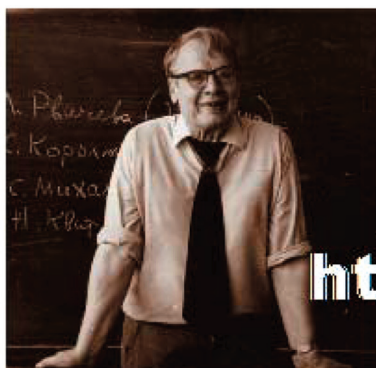
Сведения об авторах

Владимир Г. Попов – доктор технических наук, профессор, заведующий кафедрой «Химия и инженерная экология», Российский университет транспорта (МИИТ), Российская Федерация, Москва, e-mail: vporov_miit@mail.ru

Филипп И. Сухов – кандидат технических наук, доцент кафедры «Химия и инженерная экология», Российский университет транспорта (МИИТ), Российская Федерация, Москва, e-mail: philipp.sukhov@mail.ru

Юлия К. Боландова – аспирант, ассистент кафедры «Химия и инженерная экология», Российский университет транспорта (МИИТ), Российская Федерация, Москва, e-mail: jbolandova@gmail.com

Поступила: 17.12.2018



<http://Gnedenko-Forum.org/>

Дорогие коллеги!

В 2005 году была основана неформальная Ассоциация специалистов по надежности, прикладной вероятности и статистике (I.G.O.R.), которая имеет свой сайт в Интернете GNEDENKO FORUM. Сайт назван в честь выдающегося математика Бориса Владимировича Гнеденко (1912-1995). Целью Форума является улучшение профессиональных и персональных контактов специалистов по математической статистике, теории вероятностей и их важных ветвей, как Теория надежности и контроля качества, Теория массового обслуживания, Теории управления запасами и т.п.

Начиная с января 2006 года Форум издает ежеквартальный Международный электронный журнал

«Надежность: Теория и приложения» (“Reliability: Theory & Applications”).

Журнал зарегистрирован в Библиотеке Конгресса США (ISSN 1932-2321). Все права сохраняются за авторами, так что статьи затем могут быть свободно опубликованы в любых других изданиях или представлены на конференции.



**Вступайте в Форум
Гнеденко!**

**Добро
пожаловать!**
В наших рядах уже более
500 специалистов
из **44** стран мира.

Для вступления в
Форум присылайте
фото и краткое резюме
по адресу:

к.т.н. Александр Бочков,
a.bochkov@gmail.com

Membership is free.

ЗАЯВКА НА ПОДПИСКУ НА ЖУРНАЛ «НАДЕЖНОСТЬ»

с № _____ 20__ г. по № _____ 20__ г., количество экз. _____

Полное наименование организации	
Юридический адрес предприятия (индекс, страна, адрес)	
Почтовый адрес предприятия (индекс, страна, адрес)	
ИНН/КПП	
Расчетный счет	
Банк	
Корреспондентский счет	
БИК	
Контактное лицо: Ф.И.О., должность	
Телефон/факс, e-mail	

Реквизиты: ООО «Журнал «Надежность»

Адрес редакции: 109029, г. Москва, ул. Нижегородская, д.27, стр.1, оф. 209

Тел./факс: (495) 967-77-02 , e-mail: evgenya.patrikeeva@yandex.ru

ИНН 7709868505 КПП 770901001

р/с 40702810100430000017, ПАО «УРАЛСИБ БАНК» г. Москва

к/с 30101810100000000787

Адрес доставки:

Кому: _____

Куда: _____

Для оформления подписки на журнал «Надежность» заполните заявку и отправьте ее по факсу или электронной почте.

По всем вопросам, связанным с подпиской, обращайтесь в редакцию журнала.

Стоимость годовой подписки 4180-00 руб, в т.ч. НДС 10%.

Периодичность – 4 номера в год.

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ

АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ И ПРОЕКТНО-
КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ НА
ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ»
(АО «НИИАС»)



АО «НИИАС» – ведущее предприятие ОАО «РЖД» в области создания комплексов и систем обеспечения безопасности движения, управления движением, геоинформационного обеспечения, мониторинга состояния подвижного состава и инфраструктуры железных дорог



Цели:

- ☐ эффективность,
- ☐ безопасность
- ☐ надежность перевозок



Основные направления деятельности

- Интеллектуальные системы управления
- Технологии управления перевозками и транспортного обслуживания
- Системы автоматики и телемеханики
- Центры автоматизированного управления
- Информационные системы
- Геоинформационные системы и спутниковые технологии
- Системы транспортной безопасности
- Системы управления инфраструктурой
- Системы управления топливно-энергетическими ресурсами
- Испытания, сертификация и экспертиза
- Информационная безопасность
- Нормативно-правовое обеспечение



www.vniias.ru

THE JOURNAL IS PUBLISHED WITH PARTICIPATION AND SUPPORT OF JOINT-STOCK COMPANY RESEARCH & DESIGN INSTITUTE ON RAILWAY TRANSPORT (JSC NIAS)

JSC NIAS is RZD's leading company in the field of development of train control and safety systems, traffic management systems, GIS support technology, railway fleet and infrastructure monitoring systems

Mission:

- efficiency, transportation
- safety,
- reliability



Key areas of activity

- Intellectual control and management systems
- Transportation management systems and transport service technology
- Signalling and remote control systems
- Automated transportation management centers
- Railway transport information systems
- Geoinformation systems and satellite technology
- Transport safety systems
- Infrastructure management systems
- Power consumption and energy management systems
- Testing, certification and expert assessment
- Information security
- Regulatory support



www.nias.ru

SUBSCRIBER APPLICATION FOR DEPENDABILITY JOURNAL

Please subscribe us for 20_____ from No. _____ to No. _____ number of copies _____

Company name	
Name, job title of company head	
Phone/fax, e-mail of company head	
Mail address (address, postcode, country)	
Legal address (address, postcode, country)	
VAT	
Account	
Bank	
Account number	
S.W.I.F.T.	
Contact person: Name, job title	
Phone/fax, e-mail	

Publisher details: Dependability Journal Ltd.

Address of the editorial office: office 209, bldg 1, 27 Nizhegorodskaya Str., Moscow 109029,
Russia Phone/fax: 007 (495) 967-77-02, e-mail: evgenya.patrickeeva@yandex.ru
VAT 7709868505 Account 890-0055-006
Account No. 40702810100430000017
Account No. 30101810100000000787

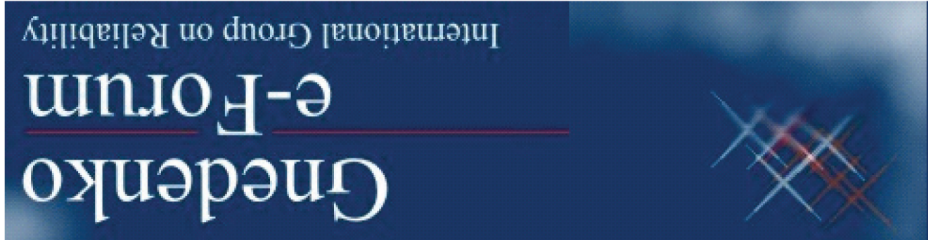
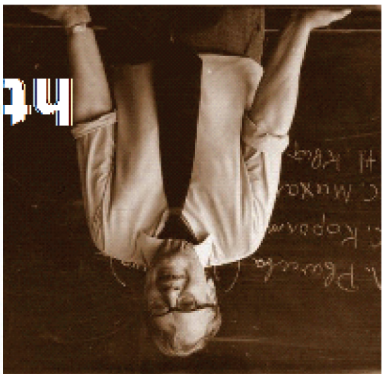
Address of delivery:

To whom: _____

Where: _____

To subscribe for Dependability Journal, please fill in the application form and send it by fax
or email.

In case of any questions related to subscription, please contact us.
Cost of year subscription is 4180 rubles, including 18 per cent VAT.
The journal is published four times a year.



Gnedenko e-Forum
International Group on Reliability

<http://Gnedenko-Forum.org/>

Dear colleagues!

In 2005 the informal Association of Experts in Reliability, Applied Probability and Statistics (I.G.O.R.) was established with its own Internet website GNEDENKO FORUM. The site has been named after the outstanding mathematician Boris Vladimirovich Gnedenko (1912-1995). The Forum's purpose is an improvement of personal and professional contacts between experts in the mathematical statistics, probability theory and their important branches, such as reliability theory and quality control, the theory of mass service, storekeeping theory, etc. Since January 2006, the Forum has published a quarterly international electronic magazine

"Reliability: Theory and Applications":

The magazine is registered with the Library of Congress in the USA (ISSN 1932-2321). All rights reserved for authors so that articles can be freely published in any other publications or presented at conferences.

Join Gnedenko Forum!

Welcome!

More than **500** experts
from **44** countries
worldwide have already
joined us!

To join the Forum, send a
photo and a short CV to the
following address:
Alexander Bochkov, PhD
a.bochkov@gmail.com

Membership is free.

with the rail transportation of oil and petroleum products]. Life safety 2010;11:39-43 [in Russian].

[16] Popov V.G., Sukhov F.I., Petrov S.V. Accident risk assessment. World of Transport and Transportation 2012;6;150-155 [in Russian].

About the authors

Vladimir G. Popov, Doctor of Engineering, Professor, Head of Department of Chemistry and Ecological Engineering, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: vpopov_miti@mail.ru

Philipp I. Sukhov, Candidate of Engineering, Senior Lecturer, Department of Chemistry and Ecological Engineering, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: philipp.sukhov@mail.ru

Yulia K. Bolandova, post-graduate student, teaching assistant, Department of Chemistry and Ecological Engineering, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: jbolandova@gmail.com

Received on: 17.12.2018

- [11] Legasov V.A., Demin V.F., Shevelev Ya. V. Diskontirovanie i kompromiss mezhdu pokoleniyami [Discounting and compromise between generations]. Issues of Risk Analysis 2005;2(2):141-146 [in Russian].
- [12] Kraskovskiy A.E. Ekonomicheskie mekhanizmy upravleniya bezopasnostyu dvizheniya [Economic mechanisms of traffic safety management]. Zhелеznodorozhny transport 2002;5:29-33 [in Russian].
- [13] Popov V.G., Sukhov F.I. Indeks prognoz and indeks otklik [Prediction index and response index]. World of Transport and Transportation 2007;5(3):130-133 [in Russian].
- [14] Popov V.G., Petrov S.V. Metod otsenki urovnya bezopasnosti dvizheniya i avariynogo riska pri perevozke gruzov po zheleznyy dorogam [Method of assessment of traffic safety and accidental risk associated with carriage of goods by rail]. Transport: science, equipment, management 2008;7:1-5 [in Russian].
- [15] Popov V.G., Petrov S.V. Metod otsenki avariynogo riska pri perevozke nefi i nefteproduktov po zheleznyy dorogam [Method of assessment of accidental risk associated

Table 1. Calculation data of transportation accident probability

<i>t</i>	Name of line	Length of line, km	Amount of traffic, per day	Probability $R(B_{f,l,m}^{f,l,m})$	Probability $R(B_{f,l,m}^{f,l,m})$	Probability $R(B_{f,l,m}^{f,l,m})$	Probability $R(B_{f,l,m}^{f,l,m})$
1	Arnavit Rostovsky – Nevinnomysskaya	77	46	1,506·10 ⁻⁴	9,058·10 ⁻⁴	1,028·10 ⁻⁹	1,087·10 ⁻⁴
2	Arnavit Rostovsky – Kurgannaya	40,5	40	5,165·10 ⁻⁵	4,765·10 ⁻⁴	2,122·10 ⁻¹⁰	5,552·10 ⁻⁵
3	Kurgannaya – Belorechenskaya	63,8	41	8,830·10 ⁻⁵	7,506·10 ⁻⁴	3,944·10 ⁻¹⁰	8,786·10 ⁻⁵
4	Belorechenskaya – Komsomolskaya	19,8	42	2,961·10 ⁻⁵	2,33·10 ⁻⁴	1,44·10 ⁻¹⁰	2,741·10 ⁻⁵
5	Komsomolskaya – Krivenkovskaya	87,6	42	1,31·10 ⁻⁴	1,03·10 ⁻³	6,361·10 ⁻¹⁰	1,212·10 ⁻⁴
6	Krivenkovskaya – Tupase	18,2	77	8,89·10 ⁻⁵	2,142·10 ⁻⁴	7,187·10 ⁻⁹	2,89·10 ⁻⁵

– hurricane with wind strength over 22 mps ($m = 2$),

frequency as compared to other types of emergencies $\Phi_2 = 0.11$, average annual number of natural emergencies N_2

duration $T_f = 120$ h, characteristic spatial scale $L_2 = 500$ km, characteristic

of emergences $\phi_3 = 0,83$, average annual number of natural
emergences $N = 15$ characteristic spatial scale $L = 1$ km
— heavy rain ($m = 5$), frequency as compared to other types
za i upravleniya riskom v prirodnykh tekhnologiyakh
[Basics of the natural and man-made risk analysis and manage-
ment]. Moscow: Delovoy ekspres. 2004. In Russian]

[4] GOST 33433-2015. Functional safety. Risk management on railway transport. Moscow: Standartinform, 2016.

Using formula (14), let us estimate the probabilities of a transportation accident involving trains on 6 [5] Volodarsky V.A., Orlenko A.I. On the depend-

($t = 1, 2, 3, \dots, 6$) lines of the North Caucasus Railway ($f = 1$) caused by three hazardous states ($M = 3$) of environmental

objects: $R(B_{63}^1) = 4,295 \cdot 10^4$. The mathematical expectation of the economic damage of TSD calculated as of 2019 will

amount to $Y(B) = 429474.42$ rub (formula (19)). Then, the estimate of the economic risk of a transportation and the traffic factors. Dependability 2018;18(1):53-60.

[7] Dayev Zh.A., Nurushev E.I. Application of statistical criteria for improving the efficiency of risk assessment of the North Caucasus Railway ($f = 1$) will be (similarly) [Zhurnal Dnepropetrovskogo nauchno-issledovatskogo universiteta. Tekhnicheskie nauki. 2018. № 49. S. 45–46].

$$R(\beta_{i_M}^{i_M}) = R(\beta_{6_3}^6) \cdot Y(B) = R(\beta_{6_3}^6) \cdot Y(B) =$$
$$= 24,295 \cdot 10^{-4} \cdot 429474,42 \approx 184,45 \text{ rub.}$$

If, for instance, we consider the case of transportation of 1 of hazardous freight on this route that amount to ap- of natural emergencies in the environment. Science and

approximately 6000 rub, the obtained economic estimate can be considered as the amount of coverage for the purpose of Technology in Transport 2018;4:115-120 [in Russian].

risk management (risk treatment) by means of transfer.

References

[1] Katsov V.M., editor. Doklad o klimaticheskikh riskakh i drugikh opasnykh posledstviyakh izmeneniya klimata i drugoye. Moscow: Voenizdat, 2007. 120 p.

ma territorii Rossiyskoy Federatsii [Report on the climate-related risks in the Russian Federation]. Saint Petersburg, by the Ministry of Justice of the Russian Federation on 30.03.2015. URL: <http://36.03.2015> (36.03.2015).

26.02.2015, no. 36209).

For the economic assessment of the consequences of transportation accidents let us use the information set forth in [11–16]. According to [10], transportation accidents, i.e. traffic safety disturbances (TSD) are subdivided into train wrecks, B_1 , train accidents, B_2 , transportation accidents (derailment or collision without consequences in the form of train wreck or train accident), B_3 .

Using the discounting method [11] and statistical data of [12, 13], we can write the estimation equation of the mathematical expectation of economic damage caused by TSD as $B_n(B_n = B_1, B_2, B_3)$:

$$Y(B_n) = Y_0(B_n)(1 + r)^p, \quad (18)$$

where $Y_0(B_1) = 2 \cdot 10^6$ rubles, $Y_0(B_2) = 0.5 \cdot 10^6$ rubles, $Y_0(B_3) = 7 \cdot 10^3$ rubles are the average values of economic damage caused by one event of types B_1, B_2, B_3 in 2000 rubles,

$p = Y - 2000$ is the conventional year,

Y is the calendar year of risk analysis,

r is the rate of discounting ($r = 0, 1-0, 12$).

The practical impossibility of predictive estimation of the economic damage caused by TSD of type B_n associated with

the effect of natural emergencies on socio-technical railway systems and causing transportation accidents involving moving trains forces us to resort to using conservative assumptions and a posteriori statistical data on the TSD that affect trains. Given the above, the equation can be written as follows:

$$Y(B) = \sum_{n=1}^3 \alpha_n \cdot Y(B_n), \quad (19)$$

where α_n is the relative rates of TSD of type B_n ($n = 1, 2, 3$) that according to [14, 16] can be estimated as $\alpha_1 = 0, 01$, $\alpha_2 = 0, 1$, $\alpha_3 = 0, 89$.

Then, the economic estimate of the risk of transportation accident affecting a train on the i -th line of the j -th railway caused by a natural emergency of the m -th type can be obtained using the following formulas:

$$\begin{aligned} \text{up } R''(B_{j,i,m}^E) &= R''(B_{j,i,m}^E) \cdot Y(B), \\ \text{down } R'_E(B_{j,i,m}^E) &= R'_E(B_{j,i,m}^E) \cdot Y(B), \\ \text{up and down } R_E(B_{j,i,m}^E) &= R(B_{j,i,m}^E) \cdot Y(B). \end{aligned} \quad (20)$$

The economic estimate of risks for cases $B_{j,i,m}^E, B_{j,i,m}^E, B_{j,i,m}^E$ (for i lines in one railway or j railways) can be obtained similarly by multiplying the corresponding probability of a transportation accident (formulas (6) – (17)) by the size of damage $Y(B)$.

Let us estimate the probability of transportation accident $R(B_{j,i}^{E,M})$ involving trains on the Nevinnomysskaya – Tuapse line of 6 sections ($i = 1, 2, 3, \dots, 6$) of the North Caucasus Railway caused by the effect of three types of natural emergencies below on the socio-technical system:

– flood ($m = 1$), frequency as compared to other types of emergencies $\phi_1 = 0, 06$, average annual number $N_1 = 1$, characteristic spatial scale $L_1 = 15$ km, characteristic duration $T_1 = 1$ h,

$$R'(B_{j,i,m}^E) = 1 - \prod_{i=1}^I [1 - R'(B_{j,i,m}^E)], \quad (10)$$

for up and down trains

$$R(B_{j,i,m}^E) = 1 - \prod_{i=1}^I [1 - R(B_{j,i,m}^E)], \quad (11)$$

where $B_{j,i}^{E,M}$ is a transportation accident, an event that followed the effect of a natural emergency of the m -th type on the socio-technical railway system on i ($i = 1, 2, 3, \dots, I$) lines of the j -th railway.

III. We will estimate the probability of a transportation accident affecting a train moving along i ($i = 1, 2, 3, \dots, I$) lines of the j -th railway caused by all possible natural emergencies using the following formulas:

for an up train:

$$R''(B_{j,i,M}^E) = 1 - \prod_{i=1}^I [1 - R''(B_{j,i}^E)], \quad (12)$$

for a down train:

$$R'(B_{j,i,M}^E) = 1 - \prod_{i=1}^I [1 - R'(B_{j,i}^E)], \quad (13)$$

for up and down trains:

$$R(B_{j,i,M}^E) = 1 - \prod_{i=1}^I [1 - R(B_{j,i}^E)], \quad (14)$$

where $B_{j,i}^{E,M}$ is an event that followed the effect of all possible M types of natural emergencies of the socio-technical railway system on i ($i = 1, 2, 3, \dots, I$) lines of the j -th railway. IV. We will estimate the probability of a transportation accident affecting a train on i ($i = 1, 2, 3, \dots, I$) lines of j ($j = 1, 2, 3, \dots, J$) railways caused by all possible natural emergencies using the following formulas:

for an up train

$$R''(B_{j,i,M}^E) = 1 - \prod_{j=1}^J [1 - R''(B_{j,i}^E)], \quad (15)$$

for a down train

$$R'(B_{j,i,M}^E) = 1 - \prod_{j=1}^J [1 - R'(B_{j,i}^E)], \quad (16)$$

for up and down trains

$$R(B_{j,i,M}^E) = 1 - \prod_{j=1}^J [1 - R(B_{j,i}^E)], \quad (17)$$

where $B_{j,i}^{E,M}$ is a transportation accident, an event that followed the effect of all possible M types of natural emergencies on the socio-technical railway system on i ($i = 1, 2, 3, \dots, I$) lines of j ($j = 1, 2, 3, \dots, J$) railways. If in formulas (9) to (14) for i we take all the lines of the j -th railway, we can obtain the corresponding estimates of accidental risk for the j -th railway as a whole ($j = 1, 2, 3, \dots, J$). If in formulas (15) to (17) we take i ($i = 1, 2, 3, \dots, I$) lines of j ($j = 1, 2, 3, \dots, J$) railways, we can obtain the corresponding estimates of accidental risks for various routes.

$B_{j,i,m} = D_{j,i,m} \cdot H_{j,i,m}$, a transportation accident [10] caused by the effect of a natural emergency of the m -th type on the sociotechnical railway system on the i -th line of the j -th railway,

$N_{j,i,m}$, the average yearly number of natural emergencies of the m -th type that occur in the Russian geographical region where the i -th line of the j -th railway ($m = 1, 2, \dots, M$) is situated, 1/year,

$L_{j,i,m}$, the characteristic spatial scale of a natural emergencies of the m -th type that occurs in the Russian geographical region where the i -th line of the j -th railway ($m = 1, 2, \dots, M$) is situated, km,

$T_{j,i,m}$, the characteristic duration of a natural emergency of the m -th type that occurs in the Russian geographical region where the i -th line of the j -th railway ($m = 1, 2, \dots, M$) is situated, h,

We will estimate the probability of a transportation accident affecting an up train on the i -th line of the j -th railway caused by a natural emergency of the m -th type using the following formulas:

$$R''(B_{j,i,m}) = R''(D_{j,i,m}) \times C_{j,i,m} = P''(C_{j,i,m}) \cdot P''(D_{j,i,m} | C_{j,i,m}), \quad (1)$$

where $P''(D_{j,i,m} | C_{j,i,m}) = P''(L_{j,i,m} | C_{j,i,m}) \cdot P''(T_{j,i,m} | C_{j,i,m})$ is the probability of occurrence in the specific geographical region of a natural emergency of the m -th type with the characteristic spatial scale $L_{j,i,m}$ within the average time of presence of an up train on the i -th line with the length of $L_{j,i}$ [9],

$$P''(C_{j,i,m}) = 1 - \exp\left(-\frac{N_{j,i,m} \cdot T_{j,i,m}}{365 \cdot 24}\right) \quad (2)$$

where $T_{j,i,m} = L_{j,i} / V''$, V'' is the up service speed on the i -th line of the j -th railway, $P''(L_{j,i,m} | C_{j,i,m})$ is the conditional probability of the effect on the sociotechnical railway system of event $C_{j,i,m}$ with characteristic spatial scale $L_{j,i,m}$ causing a transportation accident involving an up train on the i -th line of the j -th railway [9]

$$P''(L_{j,i,m} | C_{j,i,m}) = 1 - \exp(-k_x \lambda'' T_{j,i,m})^k; \quad (3)$$

$$\lambda'' = 1 / \Delta X_{j,i}^{\lambda''},$$

where k_x is the kind of the standard Erlang distribution, $\Delta X_{j,i}^{\lambda''} = V'' \times \Delta T_{j,i}^{\lambda''}$ is the average spacing of up trains on the i -th line of the j -th railway, km, $\Delta T_{j,i}^{\lambda''}$ is the average headway between up trains on the i -th line of the j -th railway, h,

$P''(T_{j,i,m} | C_{j,i,m})$ is the conditional probability of the effect on the sociotechnical railway system of event $C_{j,i,m}$ with characteristic duration $T_{j,i,m}$ that caused a transportation accident involving an up train on the i -th line of the j -th railway [9]

for a down train

$$R''(B_{j,i,m}) = 1 - \prod_{i=1}^I [1 - R''(B_{j,i,m})] \quad (9)$$

for an up train

using the following formulas:

j -th railway caused by a natural emergency of the m -th type accident affecting a train on I ($i = 1, 2, 3, \dots, I$) lines of the

II. We will estimate the probability of a transportation accident affecting a train on the i -th line of the

$B_{j,i,m}$ is a transportation accident, an event that followed the effect of all possible M types of natural emergencies on the sociotechnical railway system on the i -th line of the

out of all the other types of emergencies, $\sum_{m=1}^M \phi_m = 1$,

where ϕ_m is the frequency of emergencies of the m -th type

$$R(B_{j,i,m}) = R''(B_{j,i,m}) + R'(B_{j,i,m}) - R''(B_{j,i,m}) \cdot R'(B_{j,i,m}), \quad (8)$$

for up and down trains

$$R'(B_{j,i,m}) = \sum_{m=1}^M \phi_m \cdot R'(B_{j,i,m}), \quad (7)$$

for a down train

$$R''(B_{j,i,m}) = \sum_{m=1}^M \phi_m \cdot R''(B_{j,i,m}), \quad (6)$$

for an up train

$(m = 1, 2, 3, \dots, M)$ using the following formula:

I. We will estimate the probability of a transportation accident affecting a train on the i -th line of the j -th railway caused by all possible natural emergencies of M types

affecting a moving train.

Out of formulas (1), (5), we can obtain the following estimates of the probability of a transportation accident affecting a moving train.

$$R(B_{j,i,m}) = R''(B_{j,i,m}) + R'(B_{j,i,m}) - R''(B_{j,i,m}) \times R'(B_{j,i,m}). \quad (5)$$

(accounting for the jointness of events):

the m -th type can be identified using the following formula way caused by a hazardous effect of a natural emergency of

affecting up and down trains on the i -th line of the j -th railway, the probability $R(B_{j,i,m})$ of a transportation accident

appropriate data.

Then, the probability $R(B_{j,i,m})$ of a transportation accident according to formulas similar to those for up trains subject to cording to formulas similar to those for up trains subject to

In formula (1) written to estimate the probability of a transportation accident involving a down train on the i -th line of the j -th railway $R'(B_{j,i,m})$, the corresponding values

$$P'(C_{j,i,m}), P'(L_{j,i,m}), P'(T_{j,i,m}) \text{ are identified according to formulas similar to those for up trains subject to} \quad (4)$$

$$\lambda'' = 1 / \Delta T_{j,i}^{\lambda''},$$

Risk assessment consists in its quantitative measurement [3]. Quantitative estimation of risk requires the analysis of the probabilities of occurrence of hazards and consequences of such hazards' realization.

The main purpose of risk management in railway transportation consists in achieving and maintaining the acceptable level of risk while ensuring the functional safety of infrastructure facilities and rolling stock [4]. As of late, special emphasis is placed on the matters of dependability of rolling stock and development of systems and methods of risk estimation and management aimed at ensuring the safety of transportation processes [5-8]. However, the latest research into this matter examines the system of railway infrastructure operation separately from the environment. The authors propose a method of transportation accident risk assessment that takes into consideration the effect of various natural emergencies.

A transportation accident is understood as train wrecks, train accidents, as well as derailments and collisions of rolling stock that do not cause train wrecks and accidents in accordance with the classification of the Decree of the Ministry of Transportation of the Russian Federation no. 344 of December 18, 2014 [10].

Let us introduce the following notations for the purpose of characterizing natural emergencies:

$C_{j,i,m}$, an event that is a natural emergency of the m -th type that occurred in the Russian geographical region where the i -th line of the j -th railway is situated,

$D_{j,i,m}$, an event that characterizes the effect of a natural emergency of the m -th type (event $C_{j,i,m}$) on the socio-technical railway system on the i -th line of the j -th railway and causes a transportation accident,

Today's world statistics show growing damage caused by hazardous weather and climate events around the globe. The diagram (Figure 1) shows that 90% worst economic losses are caused not by geophysical phenomena, such as volcano eruptions, tsunamis and earthquakes, but meteorological, climate and hydrological events, i.e. floods, strong winds, heavy rains, hail, droughts [1].

Importantly, hazardous climate events can initiate industrial emergencies. Significant social and economic losses were caused by mudflows that accompanied a deep depression with showers between August 6 and 9, 2002 around Novorossiysk on the Black Sea coast of Russia. According to operational messages of the EMERCOM of Russia, on August 6 power-ful mud-and-stone flows with the total volume over 15 thousand m³ destroyed 300 meters of railway track between Sochi and Tuapse, as well as the nearby motorway. 47 passenger trains were blocked. According to preliminary estimations, direct economic damage amounted to USD 71 mln. [2].

As the result of abundant precipitations on October 24 and 25, 2018 (275-330 mm) in three municipalities of the Krasnodar Krai, harm was inflicted on two road bridges and one railway bridge, sections of the Tuapse – Maykop and Dzhubga – Sochi motorways, roadbed in the Tuapse – Krivenskaya and Tuapse – Adler railway lines. 36 passenger trains were cancelled and 39 were delayed.

Fault-free and safe operation of railway transportation largely depends on the climate conditions. The assessment of the factors of climate-related risk that quantitatively characterize their effect on the railway infrastructure is the starting point of calamity risk management and adaptation of human activities to the ever-changing climate.

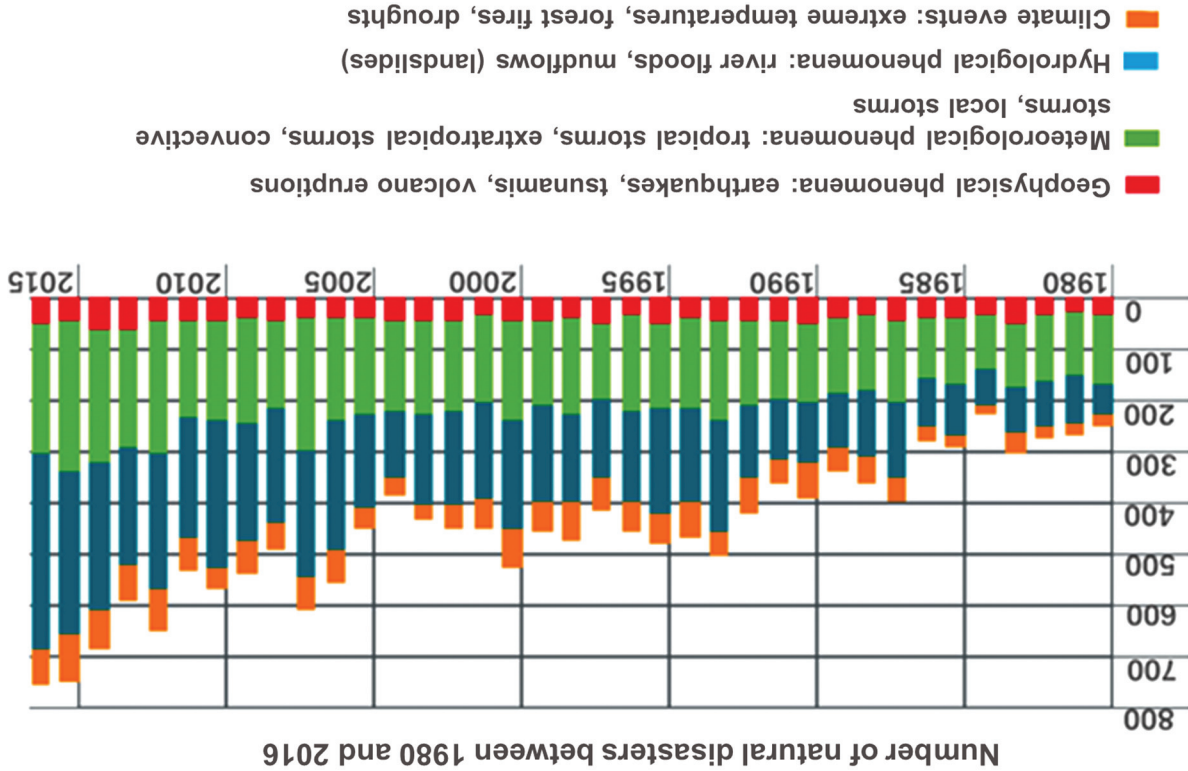


Figure 1. Number of natural disasters between 1980 and 2016

Economic assessment of the accidental risk of natural emergencies for train traffic

Vladimir G. Popov, Russian University of Transport (MILT), Russian Federation, Moscow
 Filipp I. Sukhov, Russian University of Transport (MILT), Russian Federation, Moscow
 Yulia K. Bolandova, Russian University of Transport (MILT), Russian Federation, Moscow

Abstract. Aim. The paper is dedicated to the evaluation of the risk of transportation accidents caused by natural emergencies affecting train traffic on a specific line. The ever-growing anthropogenic burden on the environment inevitably causes climate change that, in turn, gives rise to higher numbers of extreme weather events. The latter usually cause industrial accidents and disasters. The assessment of the factors of climate-related risk that quantitatively characterize their effect on the railway infrastructure is the starting point of calamity risk management and adaptation of human activities to the ever-changing climate. **Methods.** The authors propose a method of risk assessment that takes into consideration the effect of various natural emergencies that affect rolling stock in motion. The method is based on elements of the probability theory and mathematical statistics. The developed method enables the assessment of the risk of a transportation accident caused by natural emergencies specific to not only a line, but a route on a railway network. **Results.** For the Nevinnomysskaya – Tuapse line that includes 6 sections of the North Caucasus Railway, one of which was damaged due to abundant precipitations on October 24 and 25, 2018, the risk of transportation accident caused by the effects of three types of natural emergencies on the sociotechnical system of this line has been calculated:

- flood,
- hurricane with wind strength of over 22 mps,
- heavy rain.

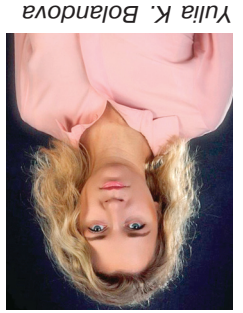
The parameters of such emergencies are characterized by the following factors:

- frequency as compared to other types of emergencies,
- average annual number of natural emergencies,
- characteristic spatial scale of the natural emergency,
- characteristic duration of the natural emergency.

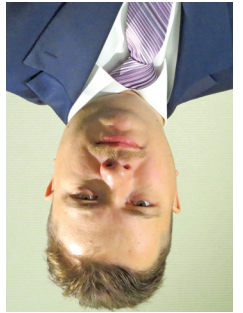
The conditional probabilities of the effects on the railway sociotechnical system of an event that has characteristic spatial scale and duration and has caused a transportation accident involving a train were estimated based on the assumption that a train flow in space follows the normal Erlang distribution of the k -th kind. The risk of transportation accident involving up and down trains travelling along the i -th line of the j -th railway caused by a hazardous effect of a natural emergency of the m -th type is identified subject to the jointness of events. Using the discounting method, an equation was obtained for estimating the mathematical expectation of economic damage by traffic safety disturbances, which allowed estimating the economic component of the risk. **Conclusions.** As the result, a method is proposed for estimation of the risk of transportation accidents caused by natural emergencies, an example is provided of such risk estimation, including the economic component, for the Nevinnomysskaya – Tuapse line.

Keywords: accidental risk, accidents, emergencies, railway transportation, natural emergencies, railway freight transportation, traffic safety disturbances.

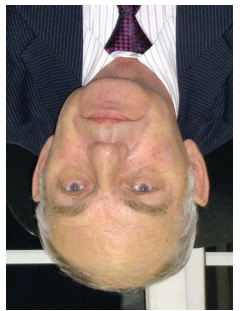
For citation: Popov VG, Sukhov FI, Bolandova YK Economic assessment of the accidental risk of natural emergencies to train traffic. *Dependability* 2019;2: 48-53. DOI: 10.21683/1729-2646-2019-19-2-48-53



Yulia K. Bolandova



Filipp I. Sukhov



Vladimir G. Popov

- obsluzhivaniya LA i AD [Operational dependability and maintenance conditions of aircraft and aircraft engines]. Moscow: MGТУ GA, 2013 [in Russian].
- [12] Smirnov NN. Osnovy teorii tekhnicheskoy ekspluatatsii letatelnykh apparatov: Chast 2 [Fundamentals of aircraft maintenance: Part 2]. Moscow: MGТУGA, 2003 [in Russian].
- [13] Svishchev GP, editor. Aviatstsia: entsiklopediya [Aviation: encyclopedia]. Moscow: Bolshaya Rossiyskaya entsiklopediya, 1994 [in Russian].
- [14] GOST R 56079-2014. Aircraft items. Flight safety, reliability, testability and maintainability. Indices nomenclature. Moscow: Standartinform, 2014 [in Russian].
- [15] Antseliovich LL. Nadezhnost, bezopasnost i zhivuchest samoleta [Dependability, safety and survivability of an airplane]. Moscow: Mashinostroenie, 1985 [in Russian].
- [16] Gerasimova ED, Smirnov NN, Poliakova IF. Ekspluatatsionnaya nadezhnost i rezhimy tekhnicheskogo
- the airworthiness of civilian aircraft in terms of strength].**

About the author

Vadim V. Efimov, Doctor of Engineering, Associate Professor, Professor, Moscow State Technical University of Civil Aviation, Russian Federation, Moscow, e-mail: efimovwww@yandex.ru

Received on: 19.11.2018

where $\tilde{Q}^{\text{ext}}$ is the probability of an aircraft encountering

extreme operating conditions.

Fortunately, $\tilde{Q}^{\text{exp}} \gg \tilde{Q}^{\text{ext}}$, while $\tilde{Q}^{\text{exp}} \approx 1$, so in formula

(1) it is usually omitted.

But failures may also be caused by an aircraft encoun-

tering extreme conditions beyond the expected operating

conditions. In other words, failures may be caused by

anomalous external effects (for instance, single gusts with

the speed higher than the value specified in the Airworthiness

Requirements, which can cause the destruction of structural

components or appearance of permanent deformations,

excessive continued air turbulence, whose parameters are

also specified in the Airworthiness Requirements, which

may cause premature depletion of operating life and, as con-

sequence, fatigue failure of a structural component, effects

of munition), crew error (for instance, hard touchdown or

excess of maximum allowed value of maneuver load factor,

which may cause the destruction of structural components

or occurrence of permanent deformations) or maintenance

error (for instance, damage to structural components as the

result of careless performance of service and repair opera-

tions and, as consequence, premature fatigue failure). In this

case mission performance relies on the survivability.

In accordance with [15], aircraft survivability is defined

by the perishability and vulnerability. Let us make improve-

ments to the definitions of these concepts in accordance with

the above considerations. Then, *perishability* is the property

of an aircraft that characterizes the possibility of it encoun-

tering extreme conditions beyond the expected operating

conditions (the indicator of perishability is the probability of

an aircraft encountering extreme operating conditions, $\tilde{Q}^{\text{ext}}$).

Vulnerability is the property of an aircraft that characterizes

the possibility of disruption of its operating conditions (the

indicator of vulnerability is the probability of loss of aircraft

operability under condition of effects beyond the expected

operating conditions, $\tilde{Q}^{\text{vul}}$). Given the above, similarly to

formula (1), the expression for the survivability indicator,

i.e. probability of retained operability under extreme condi-

tions, is as follows:

$$P^{\text{sur}} = 1 - \tilde{Q}^{\text{ext}} \tilde{Q}^{\text{vul}}.$$

Conclusion

In this paper, an attempt was made to unambiguously

define the survivability of aeronautical structures. The ob-

tained definition can be extended to an aircraft as a whole,

as well as other complex technical objects.

There is no point in singling out the concept of combat

survivability, since the effect of munitions is covered by the

concept of the effects of adverse factors.

The advantage of the obtained definition of survivability

consists in its clear difference from the standardized terms

for dependability and fail-safety.

Additionally, the concept of damage tolerance (operation-

al survivability) was proposed that was introduced similarly

to the concept of operational dependability.

References

- [1] Cherkesov GN, Nedosekin AO, Vinogradov VV. Functional survivability analysis of structurally complex technical systems. Dependability 2018;18(2):17-24. DOI:10.21683/1729-2646-2018-18-2-17-24.
- [2] Cherkesov GN, Nedosekin AO. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. Dependability 2016;16(2):3-15. DOI:10.21683/1729-2646-2016-16-2-3-15.
- [3] Zarubsky VG. Organization features of functional diagnosis of a control computer with improved survivability. Dependability 2016;16(3):35-38. DOI:10.21683/1729-2646-2016-16-3-35-38.
- [4] Yurkevich EV, Kriukova LN, Salykov SA. Aspects of information support in ensuring the survivability of spacecraft under electrophysical effects. Dependability 2016;16(4):30-35. DOI:10.21683/1729-2646-2016-16-4-30-35.
- [5] Klimov SM, Polikarpov SV, Fedchenko AV. Method of increasing fault tolerance of satellite communication networks under information technology interference. Dependability 2017;17(3):32-40. DOI:10.21683/1729-2646-2017-17-3-32-40.
- [6] Smirnov NN, Chiniuchin YuM, Tarasov SP. Sokhranenie letnoy godnosti vozdukhnykh sudov [Main-taining the airworthiness of aircraft]. Moscow: MGTU GA; 2005 [in Russian].
- [7] Aviatsonomnye pravila. Chast 25. Normy letnoy godnosti samoletov transportnoy kategorii: utv. Postanovleniem 23-ey sessii Soveta po aviatcii i ispolzovaniyu vozdukhnogo prostanstva 5 sentyabrya 2003 goda [Aviation rules. Part 25. Airworthiness Requirements for transport category airplanes: approved by Order of the 23-rd session of the Council for aviation and airspace management of September 5, 2003]. Moscow: Aviaizdat; 2004 [in Russian].
- [8] GOST 27.002-2015. Industrial product dependability. Terms and definitions. Moscow: Standartinform; 2016 [in Russian].
- [9] GOST 27.002-89. Industrial product dependability. General concepts. Terms and definitions. Moscow: Izdatel'svo standartov; 1990 [in Russian].
- [10] Arepiev AN, Gromov MS, Shapkin VS. Voprosy ekspluatatsionnoy zhivuchesti aviakonstruktsiy [Matters of damage tolerance of aerostuctures]. Moscow: Vozdushnyy transport; 2002 [in Russian].
- [11] Butushin SV, Nikonov VV, Feygenbaum YuM, Shapkin VS. Obespechenie letnoy godnosti vozdukhnykh sudov grazhdanskoy aviatsii po usloviyam prochnosti [Insuring

made in this paper.

In the author's opinion there is a long-standing need to stipulate the concept of survivability in an appropriate national standard or at least issue an annex to GOST 27.002-2015 similar to an annex to the previously effective GOST 27.002-89, but taking into account the proposals

P_{dep} is the dependability indicator (probability of retained operability under the expected operating conditions), P_{sur} is the survivability indicator (probability of retained operability under extreme conditions beyond the expected operating conditions). The dependability indicator can be represented as the product of probabilities:

$$P_{\text{dep}} = P_a P_f P_{\text{ff}}$$

where P_a is the availability coefficient, P_f is the probability of flight execution under conditions of the aircraft being operable, P_{ff} is the probability of no-failure during the flight under the expected operating conditions. Let us examine these probabilities. In order to perform the flight mission, an aircraft must be initially in the up state which depends on its availability. Quantitatively, that is evaluated with the corresponding probability P_a named availability coefficient.

In order to perform the flight mission, an aircraft, being in the up state, must conduct the flight. That depends on many factors, including managerial ones, but if we only talk about the aircraft properties, that depends, for instance, on the capabilities of the flight and navigation equipment (capability to ensure flights in nighttime, in poor weather conditions). The capability to conduct a flight under conditions of the aircraft being operable is defined by the corresponding conditional probability P_f .

However, during a flight, *special situations* may arise as the result of the effect of adverse factors or their combinations that cause reduced flight safety [7], including accidents and crashes that prevent the flight mission performance. Adverse factors include failures, extreme operating conditions, crew errors and maintenance errors. In this classification of adverse factors, failures are normally understood as disruptions of operability that occur under expected operating conditions. They may include failures caused by design flaws, poor quality of structural components and aircraft equipment manufacture. The possibility of such failures is estimated by the corresponding probability $\tilde{Q}_{\text{ff}}$, while the probability of no-failure under the expected operating conditions is identified according to formula:

$$P_{\text{ff}} = 1 - \tilde{Q}_{\text{ff}}^{\text{exp}} \quad (1)$$

where $\tilde{Q}_{\text{ff}}^{\text{exp}}$ is the probability of an aircraft encountering expected operating conditions. As an aircraft, as stated above, may be either in the expected operating conditions, or in extreme conditions beyond the expected operating conditions while no third option exists, the sum of the probabilities of an aircraft encountering such conditions must be equal to one:

$$\tilde{Q}^{\text{exp}} + \tilde{Q}^{\text{ext}} = 1,$$

conditions the operability of an item is the responsibility of dependability, while under extreme operating conditions it is the responsibility of survivability.

The concept of "damage tolerance (operational survivability)" has the right to exist as well. If we examine the definition of dependability and the above recommended definition of survivability, in both cases the specified methods of maintenance, storage and transportation are covered. But real operating conditions are characterized by a significant variety and instability due to the varied environmental conditions, level of training of the flight and maintenance personnel, physical infrastructure, organization of service and repair, etc. Thus, the methods and conditions of maintenance, storage and transportation of an item may differ from the specified ones. Due to that [16] introduced the concept of *operational dependability* that can be formulated as follows: the property of an item to retain in time the capability to perform the required functions under the expected operating conditions depending on the methods and conditions of maintenance, storage and transportation. Similarly to this definition the definition of *damage tolerance (operational survivability)* can be formulated as the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions depending on the methods of maintenance, storage and transportation. Thus, dependability and survivability are interrelated, yet clearly delimited concepts each of which has its own area of responsibility. In order to better understand this delimitation, let us examine the difference and correlation between the dependability and survivability using the probabilistic approach.

Probabilistic approach to the delimitation of the concepts of dependability and survivability of aeronautical structures

In order to ensure a better understanding of the differences and correlation between the concepts of dependability and survivability, let us use the approach described in [15]. Let us examine the indicator of operating efficiency of a transport aircraft that can be represented in the form of mathematical expectation:

$$W = W_0 P_{\text{dep}}^{\text{dep}} P_{\text{sur}}^{\text{sur}}$$

where W_0 is the initial efficiency indicator that is defined by the aircraft's functional properties (most importantly its performance), under conditions of its absolute dependability and survivability. That may be, for instance, the indicator of productive capacity [17] $W_0 = m_{\text{pl}} L / m_0$, where m_{pl} is the maximum mass of payload, L is the flight distance with the maximum mass of payload, m_0 is the maximum takeoff mass of the aircraft.

– survivability is the property of a structure to perform its functions despite the sustained damage of various nature [11].

In accordance with these definitions, in case of any damage the operability of a structure will depend on its survivability. But a structure may sustain damage under expected operating conditions. That may be the case of partial failures caused, among other things, by design flaws, poor quality of structural components manufacture. Examples include fatigue failure of elements due to miscalculations of fatigue endurance or defects caused at the stage of manufacture of parts that prove to be stress raisers.

If a structure has redundant elements, i.e. its design complies with the principle of safe destruction, the remaining structural components will ensure design load accommodation and the structure as a whole will remain operable. But then the concept of survivability overlaps with the concept of reliability that is a component of dependability. In accordance with [8], *reliability* is a property of an item to continuously retain the ability to perform the required functions during a certain period of time or operation time in specified modes and conditions of application, i.e. under the expected operating conditions in terms of the Airworthiness Requirements. As it is known, component redundancy is one of the simplest ways of improving reliability. If one or even several parallel elements (in case of multiple redundancy) fail, the remaining elements will ensure the operability of the item or its system. Then, what is the difference between the above definitions of survivability and reliability? It is obvious that the difference can only be in the operating conditions, under which a defect or partial failure occurred. If it happened under the expected operating conditions, the operability must be ensured by the dependability (reliability), if it happened under extreme operating conditions beyond the expected conditions, the operability must be ensured by the survivability. But the above definitions of survivability say nothing about that.

Some papers use the term “damage tolerance (operational survivability)” along or instead of “survivability”. The understanding of this term varies too. Let us examine the following definitions:

– damage tolerance (operational survivability) is a property that ensures normal performance of the specified functions by all systems of an aircraft in flight in case of failures or damage to individual assemblies, elements, units [12].

– damage tolerance (operational survivability) of aeronautical structures is a property of structures of an aircraft to ensure safe operation in terms of strength in case of partial or complete destruction of load-carrying elements due to fatigue, corrosion, accidental damage in operation, or damage caused in the process of manufacture and repairs [13].

In terms of their meanings, those definitions are no different from the above definitions of survivability, while the word “operational” is apparently used to indicate that in this case combat survivability is not implied – the latter

being the kind of survivability associated with the effects of munitions – and only survivability in “normal” operation is covered.

But in some works [10, 11] the concept of “damage tolerance (operational survivability)” implies something different:

damage tolerance (operational survivability) is a generalized term that characterizes the properties of a structure and ways of ensuring its safety in terms of strength and includes the allowability of damage and safety of destruction (damage). *Allowability of damage* is a property of a structure and way of ensuring its safety in terms of strength by designing a structure in which, after possible significant damage or destruction of one of the main load-carrying elements, the residual strength, despite the structure being unrepaired, will not go below the allowed level over an interval of time, within which the damage (destruction) will be undoubtedly identified.

This definition is quite cumbersome and complex, but essentially it comes down to survivability being the property that ensures safety through the capability to resist the development of critical failures out of defects. This understanding of damage tolerance (operational survivability) can be attributed to the first type of definitions in the above classification of definitions of survivability. But in this case, it overlaps with the standardized definition of *fail-safe*, the property of an aircraft as a whole and/or its functional systems that characterizes the capability to ensure safe completion of the flight in the expected operating conditions in case of possible failures onboard [14].

Given the above, the second type of definitions of survivability appears to be the most logical and consistent. In [15], a definition is set forth that is the closest to the second type: survivability is the property of an airplane to retain its operability when affected by projectiles and off-design loads, as well as subject to the existence of accumulated damage.

If we remove “as well as subject to the existence of accumulated damage” from this definition, it can be deemed quite acceptable.

Thus, similarly to the above definition of dependability, survivability can be defined as follows:

survivability is the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions under the specified methods of maintenance, storage and transportation.

Thus, any item or aircraft may be, among other things, either in the expected operating conditions, or in extreme operating conditions beyond the expected operating conditions. No third option exists. Under expected operating

Introduction

Any aircraft is characterized by a wide range of properties and parameters, including operating properties, i.e. the set of aircraft properties that manifest themselves in the course of operation. They include dependability, survivability, safety and maintainability. Whereas the terms dependability, safety and maintainability are covered in sufficient detail and with sufficient consistency in specialized literature, and some terms are even part of corresponding standards, the term "survivability" does not have an unambiguous and generally accepted definition. That is true not only in case of the aircraft survivability terminology, but that of other items as well [1–5].

In this paper, an attempt is made to unambiguously define the survivability of aeronautical structures that can subsequently be extended to an aircraft as a whole and other complex technical items. The primary goal of this paper is to clearly distinguish between the concepts of dependability and survivability.

Primary concepts and definitions of the theory of survivability of aeronautical structures

In order to ensure efficient operation and flight safety, an aircraft must possess airworthiness that is defined by its design and is maintained in operation. *Airworthiness* is a comprehensive characteristic of an aircraft defined by the implemented design principles and solutions that allows performing safe flights under expected conditions and under the established methods of operation [6]. Airworthiness Requirements of transport aircraft [7] define *expected operating conditions* as the conditions that are known from practice or whose occurrence can be reasonably predicted within the useful life of an aircraft subject to its purpose. Such conditions include state parameters and external factors that affect an aircraft, operational factors that affect flight safety.

The expected operating conditions do not include the following:

- extreme conditions that can be reliably avoided by introducing operating restrictions and rules,
- extreme conditions that occur so rarely, that observing the Airworthiness Requirements in such conditions would result in a higher level of airworthiness than required and practical.

Airworthiness depends on the *dependability* of the aircraft, including the dependability of its structure that, in turn, is defined by its strength.

At the stage of design, an aircraft's airworthiness in terms of strength is ensured by correct choice of design solutions, strength, stiffness and fatigue calculations and testing.

In the course of aircraft operation, fatigue and corrosion damage, destruction of non-metallic materials, exposure to extreme operating conditions beyond the

expected conditions may cause the loss of airworthiness in terms of structural strength. In this context, aircraft operation requires maintaining its airworthiness by means of appropriate measures as part of service and repair operations.

Despite the fact that compliance with the Airworthiness Requirements ensures a sufficiently high level of flight safety, the most vital structural components are designed in such a way as to remain operable even under extreme conditions beyond the expected operating conditions. But dependability cannot be responsible for operability outside the expected operating conditions, as in accordance with GOST 27.002-2015 Dependability in techniques. Terms and definitions [8] dependability is a property of an item to retain in time the ability to perform the required functions in *specified modes and conditions of application*, maintenance, storage and transportation, while in accordance with the terminology of the Airworthiness Requirements, the specified modes and conditions of application are to be understood as the *expected operating conditions*. Conclusion suggests itself that under extreme conditions beyond the expected operating conditions operability is to be ensured by another property, i.e. *survivability*. But does any of the existing definitions of survivability fit this purpose? Let us examine the existing terminology of survivability of aeronautical structures and aircraft as a whole.

Currently, terminology of survivability is not represented in any Russian national standard. In the previous version of the above standard (GOST 27.002-89, [9]) the dependability terminology was covered in an annex, in which survivability was defined, but it was done so in three different ways, which did not contribute to a clear understanding of the term. Let us take a look at those definitions. Survivability is understood as:

1) property of an item that consists in its ability to resist the development of critical failures from defects and damage under the adopted system of service and repair,

or

2) property of an item to retain limited operability when exposed to effects not provided for by the operating conditions,

or

3) property of an item to retain limited operability in the presence of defects or damage of a certain type, as well as in case of failure of some components. An example would be the retaining of the carrying capacity by structural components affected by fatigue cracks whose size does not exceed the specified values.

That is a classification of sorts of the existing definitions of survivability. In the literature dedicated to the survivability of aeronautical structures all of the three above definitions are used to various extents, but the third one is the most common. Let us give examples of the survivability definitions of this type:

– survivability is the property of a structure to retain strength when damaged (including fatigue damage) [10].

On the matter of the terminology of aeronautical structures survivability

Vadim V. Efimov, Moscow State Technical University of Civil Aviation, Russian Federation, Moscow



Vadim V. Efimov

Abstract. Aim. The paper examines the existing definitions of survivability and damage tolerance (operational survivability) of aeronautical structures. An attempt is made to unambiguously define the survivability of aeronautical structures that can subsequently be extended to an aircraft as a whole and other complex technical items. The primary goal of this paper is to clearly distinguish between dependability and survivability. In order to ensure efficient operation and flight safety, an aircraft must possess airworthiness, a comprehensive characteristic of an aircraft that is defined by the implemented design principles and solutions and that allows performing safe flights under expected conditions and under the established methods of operation. The expected operating conditions are described in the Aviation Regulations – Airworthiness Requirements. Despite the fact that compliance with the Airworthiness Requirements ensures a sufficiently high level of flight safety, the most vital structural components are designed in such a way as to remain operable even under extreme conditions beyond the expected operating conditions. But dependability cannot be responsible for operability outside the expected operating conditions. Conclusion suggests itself that under extreme conditions beyond the expected operating conditions operability is to be ensured by another property, i.e. survivability. **Methods.** This research was conducted using the logical and probabilistic approaches. The author examined literary sources primarily dedicated to the matters of dependability and survivability of aeronautical structures, as well as other complex technical items. In order to ensure an optimal understanding of the differences and correlation between the concepts of dependability and survivability, the probabilistic approach was used. **Results.** Upon the analysis of literary sources, survivability was defined as the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions depending on the methods of maintenance, storage and transportation. The probabilistic approach to the delimitation of the concepts of dependability and survivability of aeronautical structures was examined using the known indicator of operating efficiency of a transport aircraft that is represented as the mathematical expectation of the efficiency indicator. An aircraft may be either in the expected operating conditions or in extreme conditions beyond the expected operating conditions. No third option exists. Then, the sum of the probabilities of an aircraft encountering such conditions must be equal to one. The probability of no-failure can be calculated by means of the probability of the contrary event, i.e. the probability of failure that can be represented as the product of the probability of an aircraft encountering certain operating conditions and the probability of failure in such conditions. For the case of extreme conditions beyond the expected conditions the well-known concepts of perishability and vulnerability with the author's improvements can be used. **Conclusions.** A definition of survivability was obtained that is clearly different from the concepts of dependability and fail-safety. Additionally, the concept of damage tolerance (operational survivability) was proposed that was introduced similarly to the previously introduced concept of operational dependability.

Keyword: survivability, damage tolerance (operational survivability), dependability, failure, reliability, fail-safety, aeronautical structure, aircraft.

For citation: Efimov VV. On the matter of the terminology of aeronautical structures survivability. Dependability 2019;2: 42-47. DOI: 10.21683/1729-2646-2019-19-2-42-47

Control Sciences of the Russian Academy of Sciences,
Russian Federation, Moscow, e-mail: kulba@ipu.ru
Alexey B. Shelkov, Candidate of Engineering, Lead
Researcher, V.A. Trapeznikov Institute of Control Sci-
ences of the Russian Academy of Sciences, Russian
Federation, Moscow, e-mail: abshelkov@gmail.com
Dmitry S. Somov, Chief Analyst, Sberbank, Russian
Federation, Moscow, e-mail: somov.dmitry@gmail.com

Received on: 27.02.2019

Due to the orientation to the systems of high dimensional, structural and functional complexity and in light of opposing nature of the criteria formulated above, the precise algorithms for solving the problem in question will have too high computational complexity. Thus this problem is proposed to be solved using a combination of various approximate algorithms that create solutions according to individual criteria, or modify some existing indicator placement created based on other performance criteria [5, 12]. The practical application of this problem algorithms should be carried out using interactive procedures to collaborate with experts or specialists in a given subject area. Such approach can significantly improve the quality of the solution results (variants of indicator placement) in terms of achieving the set goals.

Conclusion

The main aim of the proposed indicator-based approach is to increase the dependability of CTS in operation and to prevent SE through the early diagnostics of the hazard of emergencies in technical systems. The indicator-based approach offers means to reduce the information-related stress and to concentrate dispatchers' or operators' attention on the processes that are most relevant in terms of safety. The approach also allows locating the sources of emergency situations with the required accuracy.

The proposed models of the disturbance propagation in the CTS are the basis for the formulation and development of formalized methods for timely detection of abnormal situations during the CTS operation and preventing SE. The developed indicator-based approach includes a set of models and technologies for analyzing the processes of hazard effect and disturbances propagation in complex technical systems, as well as methods for solving multi-criteria problems of optimal placement of indicators in the structure of the CTS based on criteria of completeness, accuracy and timeliness of detecting failures of various types.

References

- [1] Gapanovich V.A. Development and implementation of the URKAN technology on railway transport. Dependability 2013;4:11-17.
- [2] Gapanovich V.A., Shubinsky I.B., Rozenberg E.N., Zamyshlyayev A.M. System of adaptive management of railway transport infrastructure technical maintenance (URKAN project). Dependability 2015;2:14-22.
- [3] Kulba V.V., Kosyachenko S.A., Shelkov A.B. Methodology of research of railway transport safety problems. Large-Scale Systems Control 2012;38:5-19

About the authors

Leonid A. Baranov, Doctor of Engineering, Professor, Head of Department, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: baranov.miti@gmail.com

Vladimir V. Kulba, Doctor of Engineering, Professor, Head of Laboratory, V.A. Trapeznikov Institute of

sciences 2011;3(116):52-65 [in Russian].

use of structure-integrated indicators in complex technical systems monitoring. Izvestiya SFedU. Engineering

[12] Kulba V.V., Somov D.S., Kochkarov A.A. The Izdatelstvo Williams, 2013.

Introduction to Algorithms. Third edition. Moscow: Alpina Business Books; 2007.

[11] Cormen T., Leiserson C., Rivest R., Stein C. ing, Monitoring, and Managing your Business. Moscow: [10] Eckerson W. Performance Dashboards: Measuring, Monitoring, and Managing your Business. Moscow: Nauka; 2012 [in Russian].

systems]. Moscow: Nauka; 2012 [in Russian].

synthesis of development scenarios of socio-economic systems]. Moscow: Nauka; 2012 [in Russian].

icheskih sistem [Models and methods of analysis and analiza i sinteza scenariy razvitiya socialno-ekonom-

[9] Shults V.L., Kulba V.V., editors. Modeli i metody ment 2013;3:4-23 [in Russian].

facilities using indicator approach]. Trends and management 2013;3:4-23 [in Russian].

technogenic safety management of railway infrastructure transporta na osnove indikatsionnogo podhoda [Method of

nostyu ob'ektov infrastruktury zheleznodorozhnogo I.V. Metodologiya upravleniya tekhnogennoy bezopas-

[8] Shults V.L., Kulba V.V., Shelkov A.B., Chernov publication]. Moscow: ICS RAS; 2013 [in Russian].

using scenario and indicator approaches. A scientific Nauchnoe izdanie [Technogenic safety management

tyu na osnove scenariy i indikatsionnogo podhoda. I.V., Somov D.S. Upravlenie tekhnogennoy bezopasnos-

[7] Shults V.L., Kulba V.V., Shelkov A.B., Chernov of risk analysis 2012;9(3):4-7 [in Russian].

ogy-related risk and safety of the technosphere]. Issues bezopasnosti tekhnosfery [On the problems of technol-

[6] Bykov A.A. O problemah tekhnogennoy riska i [in Russian].

complex technical systems]. Moscow: ICS RAS; 2011

to controlling the survivability, durability and safety of system [Use of scenario and indicator-based approaches

stojkostyu i bezopasnostyu slozhnykh tekhnicheskikh indikatsionnogo podhoda dlya upravleniya zhivuchestvu,

Kochkarov A.A., Somov D.S. Ispolzovanie scenariy i [5] Kulba V.V., Kononov D.A., Kosyachenko S.A.,

165 [in Russian].

[4] Baranov L.A. Automatic control of metro trains. World of Transport and Transportation. 2018;16(3):156-

[in Russian].

In order to judge of the possible causes and consequences of the current situation most accurately, the selected indicators must allow for the precedence and afteraction sets to covers as much of the model elements as possible. Mathematically, it can be expressed as:

$$\left| \overline{I_{All}^I} \right| \rightarrow \max; \left| \overline{I_{Bef}^I} \right| \rightarrow \max.$$

3. *Accuracy of coverage.* In the previous criterion coverage is used without consideration of time. However, to accurately identify the developing situation, the indicators should be “close” to the propagating through the system disturbance in time. For that purpose, the minimal diameter of precedence or afteraction coverage (the set of which covers the whole set of precedence I_{Bef}^I or afteraction I_{All}^I) must be minimal:

$$\min_{T: I_{All}^I = I_{All}^I} \left(D \left(I_{All}^I \right) \right) \rightarrow \min; \min_{T: I_{Bef}^I = I_{Bef}^I} \left(D \left(I_{Bef}^I \right) \right) \rightarrow \min.$$

Let us formulate the task of optimizing the placement of indicators.

Let us suppose that the given model of disturbance propagation through a technical system is: the set of model elements is $A = \{a_1, a_2, \dots, a_n\}$, the subset of sensors is $D = \{d_1, d_2, \dots, d_{n_0}\}$, the subset of critical elements is $K = \{k_1, k_2, \dots, k_{n_k}\}$. The model elements are interconnected in relations graph G , edge passing times are given in the matrix of temporal relations M .

It is required to find such subset of elements (a set of indicators) $I = \{i_1, i_2, \dots, i_{n_i}\}$ that would comply with the following conditions:

$$|I| = n_i \leq N_i$$

$$\forall d \in D: AIf(d) \cap K \neq \emptyset \exists i \in I: i \in AIf_s(d).$$

$$\min_{d \in D, k \in K} \left(\max_{i \in I \cap AIf(d)} (dis'_i(d, k) - dis'_i(d, i)) \right) \rightarrow \max;$$

$$\left| \overline{I_{All}^I} \right| \rightarrow \max; \left| \overline{I_{Bef}^I} \right| \rightarrow \max;$$

$$\min_{T: I_{All}^I = I_{All}^I} \left(D \left(I_{All}^I \right) \right) \rightarrow \min;$$

$$\min_{T: I_{Bef}^I = I_{Bef}^I} \left(D \left(I_{Bef}^I \right) \right) \rightarrow \min.$$

Diameter of the overall coverage shall mean the maximum value of all times of a set.

$$T: D \left(I_{Bef}^I \right) = D \left(I_{All}^I \right) = \max_{j \leq n_j} \left(t_j \right).$$

Similar to the time coverage, the concept of the indicator set of the overall indicator coverage of precedence and afteraction is introduced:

$$\overline{I_{Bef}^I} = \bigcup_{j \leq n_j} Bgf_i \left(t_j \right), \overline{I_{All}^I} = \bigcup_{j \leq n_j} AIf_i \left(t_j \right).$$

Let us suppose that the solutions to the indicator localization problem is a subset of model elements $I \subseteq A$. With the introduction of some restrictions on the set of solutions the set of feasible solutions is obtained.

The number of indicators should be limited. This restriction derives from the requirement to reduce the information-related stress on the operator. Mathematically this restriction can be expressed as $|I| = n_i \leq N_i$, where N_i is some constant given in a specific task.

The set of indicators shall cover all possible threats known at the current stage of system development. In other words, in terms of the model in question, there should not be a situation in which the disturbance caused by the sensor reaches a critical element before it reaches the indicator. The mathematical interpretation of this restriction can be written as $\forall d \in D: AIf(d) \cap K \neq \emptyset \exists i \in I: i \in AIf_s(d)$

Thus, the region of feasible solutions must satisfy the afteraction requirements:

$$I \subseteq A,$$

$$|I| = n_i \leq N_i$$

$$\forall d \in D: AIf(d) \cap K \neq \emptyset \exists i \in I: i \in AIf_s(d).$$

Optimization criteria for finding the optimal solution among the feasible solutions are formulated.

1. *Criterion of maximizing the allowable time for decision making.* From the system's operational safety and failure prevention point of view the earliest possible threat detection is required. This criterion implies maximizing the time from the moment of activation of the critical element to the critical event. In terms and designations of the model it is written as follows:

$$\min_{d \in D, k \in K} \left(\max_{i \in I \cap AIf(d)} (dis'_i(d, k) - dis'_i(d, i)) \right) \rightarrow \max.$$

2. *Completeness of coverage.* For each set of indicators, coverage by precedence and afteraction sets is defined.

matrix is the result of applying the Floyd-Warshall algorithm for finding the shortest distances between the nodes to the matrix of temporal relations [11].

An optimization problem of placing indicators in a technical system is formulated using a series of definitions introduced below. A subset of indicators will be denoted by $I = \{i_1, i_2, \dots, i_{n_i}\}$. The set of time t precedence of element a shall mean a set of model elements $Bef_i(a)$, from which the element a can be reached in a time not exceeding time t . The set of time t precedence of element a shall mean a set of model elements $Bef_i^t(a)$, from which the element a can be reached in a time not exceeding time t . The set of time t precedence of element a shall mean a set of model elements $Aft_i(a)$, which can be reached from the element a in a time not exceeding time t .

Indicator coverage of time t precedence shall mean a set of time t precedence sets for all indicators:

$$I_{Bef}^t = \{Bef_i^t(i_1), Bef_i^t(i_2), \dots, Bef_i^t(i_{n_i})\}.$$

Indicator set of coverage of time t precedence shall mean the union of the set of model elements included in the indicator coverage of time t precedence, or, what is the same, the union of time t precedence sets for all indicators:

$$\overline{I_{Bef}^t} = \bigcup_{j=n_i}^{j=1} Bef_i^t(i_j).$$

Similarly, indicator coverage of time t afteraction shall mean a set of time t afteraction sets for all indicators:

$$I_{Aft}^t = \{Aft_i^t(i_1), Aft_i^t(i_2), \dots, Aft_i^t(i_{n_i})\}.$$

Indicator set of coverage of time t afteraction shall mean the union of the set of model elements included in the indicator coverage of time t afteraction, or, what is the same, the union of time t afteraction sets for all indicators:

$$\overline{I_{Aft}^t} = \bigcup_{j=n_i}^{j=1} Aft_i^t(i_j).$$

Overall set of coverage precedence shall mean the union of sets of time given for each indicator precedence for all indicators:

$$I_{Bef}^T = \{Bef_{i_1}^t(i_1), Bef_{i_2}^t(i_2), \dots, Bef_{i_{n_i}}^t(i_{n_i})\}.$$

where $T = \{t_1, t_2, \dots, t_{n_i}\}$ is a set of times of precedence sets. Similarly, the concept of overall indicator precedence coverage

$$I_{Aft}^T = \{Aft_{i_1}^t(i_1), Aft_{i_2}^t(i_2), \dots, Aft_{i_{n_i}}^t(i_{n_i})\}.$$

At the substantive level, the following main criteria for choosing the set of indicators in a complex technical system can be distinguished.

Reliability of consequence evaluation. The selection of the indicator set should allow for making judgment on the nature of the situation development and possible consequences with maximum accuracy based on their readings.

Accuracy of cause identification. Indicators should allow not only for timely detection and consequences assessment of abnormal situations, but also for identification of their causes. For example, indicators should show with which CTS node (element) the spread of the negative impact started, whether the cause of the deviations was external or internal, etc.

Abnormal situation detection time. Indicators' selection and localization in the structure of the CTS should allow for detecting deviation from normal operating at the earliest possible stages of their development in order to maximize the amount of time available for a decision made by system operator.

Cost. Indicators' selection and localization in the structure of the CTS should minimize one-time and current costs.

The proposed criteria are contradictory in a way. For example, in order to determine the cause of an abnormal situation as precisely as possible, strictly speaking, one should place indicators in all elements of the system, but this will increase the cost, the information-related stress on the decision maker, the time required for abnormal situation detection, etc.

To solve the problem of composing a set of indicators, the above graph model of disturbance propagation in the CTS is modified. The concept of edge passing time is introduced expressed as a positive number associated with the edge of the relation graph and meaning the time, during which the disturbance passes from the model element at the beginning of the edge to the element at the end of the edge. To register the edge passing times, the matrix of temporal relations M_t , which is a square matrix $n \times n$, indexed along both axes by the model elements. Positions (i, j) , $i, j \in 1, n$ of the temporal relations matrix contain edge passing time (a, a_j) , if such edge exists, and infinity sign ∞ , if such edge does not exist.

Temporal distances matrix N shall mean a $n \times n$ square matrix indexed along both axes by the set of model elements. Position (i, j) , $i, j \in 1, n$ of this matrix contains temporal distance between graph nodes a_i and a_j . The temporal distance

2. Models of using the indicator-based approach

For the purpose of more efficient diagnostics of emergency hazard, a model of application of structurally integrated indicators in railway infrastructure facilities will be considered. The indicator-based approach means that, in addition to the sensors, indicators are integrated within the structure of a technical system immediately delivering the required and sufficient information to the corresponding visualization, dispatching or situational management systems in case of emergency in order to inform the DM (dispatchers, operators, etc.) if increased attention to the situation or direct intervention are required.

The main task is to identify a set of indicators (the concept of "indicator dashboard" generally accepted in organizational management [10] can be used here) with the primary purpose of reducing the information-related stress and concentration of dispatchers' or operators' attention on the processes within a technical system that are most relevant in terms of accident-free and safe operation.

The values of the parameters reflected by the selected indicators should reliably demonstrate the deviations from the normal operation of the system. Thus, within the framework of control, dispatching or situational management, the approach under consideration is to first and foremost

provide the decision makers with the necessary and sufficient information on the status of the CTS in visual form, as well as ensure the possibility of operational (including scenario) analysis of alternative ways of emergency situation developing on a specific time horizon. Ultimately, it should improve the efficiency of management decisions on transport safety.

In order to achieve these objectives, the location of the indicators in the CTS structure should allow for informing the DS on the occurrence and development of a potentially dangerous situation at the earliest possible stage. At the same time, it should be noted that at the early stages of a situation's development, the possible (most probable, pessimistic, optimistic, etc.) scenario for an abnormal situation is not always clear. As a result, the set of consequences may be too broad, which does not allow reliably predicting the consequences and making the right decision. In this case, real-time and detailed monitoring of the potentially pre-emergency state of the CTS is required in order to collect additional information to analyze it and decide on the appropriate response.

Naturally, an equally important criterion for choosing a specific placement of indicators is the cost of such placement. Depending on the specific task, it is necessary to take into account not only the number of indicators, but also their weight, volume, physical distance between indicators, sensors, etc. When selecting a set of indicators, one should obviously strive to reduce their total number,

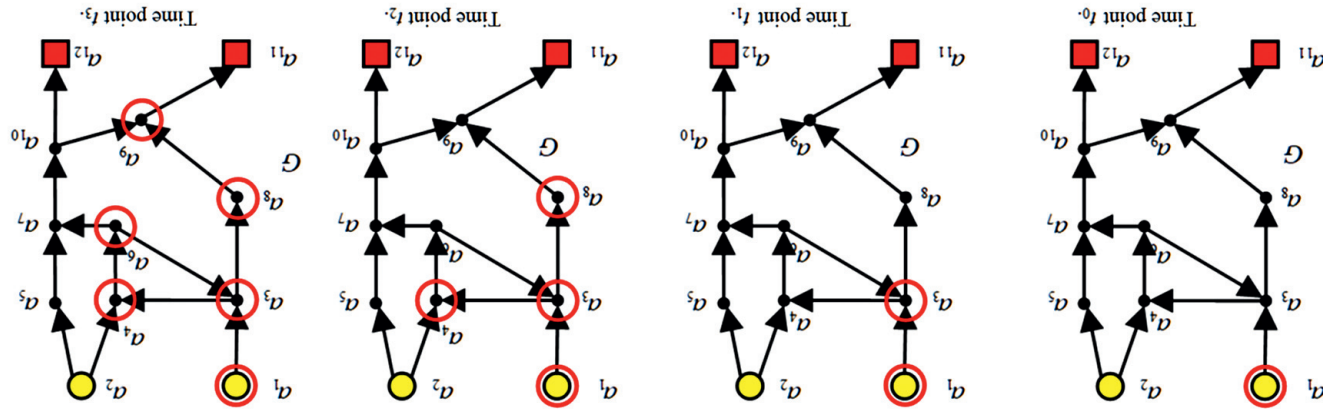


Figure 2. The process of disturbance propagation in the system

cal elements can be considered for each type of threat

Simulation starts at the moment of activation of the first sensor t_0 and continues either until the moment of stabilization (termination of change in the state of the model elements), or until the system fails in accordance with the selected system failure criterion.

The time of system failure will be designated as t_s . The criterion for system failure is determined by critical elements. Depending on the features of the system or node under consideration, as well as other features of the problem being solved, different criteria for evaluating the system failure can be selected. There are two basic criteria among them.

Exceptional criterion for system failure. The system is considered failed if the disturbance has reached any of the critical elements: $t_s = \min(t : \exists k \in K : k(t) = 1)$.

Absolute criterion for system failure. The system is considered failed if the disturbance has reached a given subset $K^* \subseteq K$ of (in the degenerate case of all) critical elements: $t_s = \min(t : \forall k \in K^* : k(t) = 1)$.

Other criteria can also be considered, for example, those related to the number, mutual arrangement and other parameters of the critical element set to which the disturbance has reached.

To illustrate the possibilities of the proposed model of disturbance propagation in the structure of a CTS, let us consider a simplified example. Let us suppose that the structure of the system include 12 elements, $n=12$, $A=\{a_1, a_2, \dots, a_{12}\}$. Elements a_1 and a_2 are sensors, $d_1 = a_1$, $d_2 = a_2$, $D=\{d_1, d_2\} = \{a_1, a_2\}$, $n_D=2$. Elements a_{11} and a_{12} are critical elements, $k_1 = a_{11}$, $k_2 = a_{12}$, $K=\{k_1, k_2\} = \{a_{11}, a_{12}\}$, $n_K=2$. The adjacency matrix M is defined as:

$$M = \begin{array}{c|cccccccccccc} & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} \\ \hline a_1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_2 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_3 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ a_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ a_9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ a_{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ a_{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ a_{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

The relation R_1 , defined by the matrix M forms the relation digraph $G(A, R_1)$ shown in Figure 1, where the sensors are designated by a circle ●, and the critical elements are indicated by a square ■. Let us suppose that there is only one type of threat, hence, only one set of critical elements, one adjacency relationship and one relationship graph are defined.

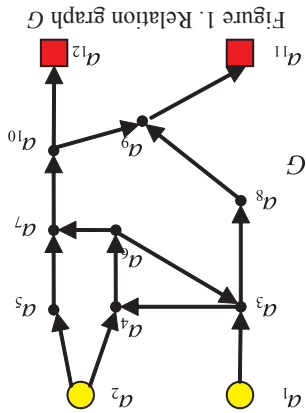


Figure 1. Relation graph G

Let us suppose that at time $t = t_0$ the sensor $d_1 = a_1$ registers a threat $a_1(t_0) = 1$, $a_{i \neq 1}(t_0) = 0$, $\underline{A}(t_0) = (1, 0, 0, \dots, 0)$. Then, the states of the model elements at the time point $t = t_1 = t_0 + \Delta t$ are calculated as follows:

$$\underline{A}(t_1) = \underline{A}(t_0) \times M = (1, 0, 1, 0, \dots, 0).$$

Figure 2 shows the process of disturbance propagation along the edges of the relation graph G from active elements (marked by an additional circle) to inactive ones, as well as the states of the corresponding model elements at different points in time. The disturbance spreads along the edges of the graph from the active elements to the inactive ones, covering one edge at a step. The state of the elements at a specific time point is determined by a Boolean formula $\underline{A}(t_i) = \underline{A}(t_0) \times M^i$.

The elements status lines for different points in time are as follows:

$$\begin{aligned} \underline{A}(t_0) &= (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0); \\ \underline{A}(t_1) &= (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0); \\ \underline{A}(t_2) &= (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0); \\ \underline{A}(t_3) &= (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0); \\ \underline{A}(t_4) &= (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0); \\ \underline{A}(t_5) &= (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0); \\ \underline{A}(t_6) &= (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1). \end{aligned}$$

As the above example shows, at the time point t_4 the first critical element is activated. If the system uses an exceptional criterion for system failure, then at the time point t_4 the system would fail. With absolute criteria, the system fails at the time point t_6 .

tion of dynamic systems has now found application, in a number of areas [9].

Let us assume that $A = \{a_1, a_2, \dots, a_n\}$ is a set of elements in a model, where n is their number. At any point in time any element can take on a value of 0 or 1. One stands for an active state (the disturbance has reached the element), zero stands for inactive state. The state of element a_i at the point of time t will be designated as $a_i(t)$, and the row-vector of states of model elements $(a_1(t), a_2(t), \dots, a_n(t))$ will be designated as $\bar{A}(t)$. The set of sensors constitute a subset of model elements $A \supseteq D = \{d_1, d_2, \dots, d_{n_p}\}$, where n_p is the number of sensors.

Adjacency matrix M shall mean $n \times n$ binary matrix, indexed along both axes by the set of model elements. Positions (i, j) , $i, j \in 1, n$ of the adjacency matrix contain 1 if and only if the relation R_1 between model elements a_i and a_j is such that when element a_i is active at the moment t_1 , the element a_j will also be active at the moment $t_2 = t_1 + \Delta t$. In other words, relation R_1 specifies the paths of disturbance propagation through the system. By relation R_1 we shall mean an adjacency relation or reachability of depth of 1 relation. The adjacency relation between model elements a_i and a_j will be designated as $a_i R_1 a_j$, and the absence of such relation will be designated as $a_i \bar{R}_1 a_j$. If there is no adjacency relation R_1 between elements a_i and a_j , there is a 0 in the position (i, j) of the adjacency matrix M . Let us suppose that the adjacency relation has reflexive property, i.e. $\forall a \in A \quad a R_1 a$. Within the model, this means that once activated, the element remains activated during the entire simulation time. For each specified type of threat, its own adjacency relationship can be defined, R_1, R_2, R_3 and so on. Accordingly, each type of threat has its own adjacency matrix. The adjacency matrix M corresponds to the digraph of the cause-effect relationships of the model elements $G(A, R_1)$, the nodes of which are the set of model elements, and the edge (a_i, a_j) corresponds to one in the matrix position (i, j) . This graph will be called the relationship digraph.

The activation of the model elements is described by the Boolean equation $\bar{A}(t_{i+1}) = \bar{A}(t_i) \times M$. In other words, all elements of the model connected by edges with already active elements are activated at further steps. In this case, once activated elements remain activated during the entire simulation, since the diagonal elements of the adjacency matrix are equal to 1.

Among the set of model elements the subset of sensors $D = \{d_1, d_2, \dots, d_{n_p}\}$ is selected. The sensors register the specified parameters of the CTS and indicate the occurrence of a threat. The disturbance caused by this threat spreads from the sensors to other elements of the system along the edges of the correlation graph $G(A, R_1)$. The set of model elements, the correlation matrix and the subset of sensors are determined together with the system designer according to the results of the system operation scheme analysis at the development stage. The subset of critical elements $K = \{k_1, k_2, \dots, k_{n_k}\}$ that determine the criterion for system failure is also selected among the elements of the model. Different sets of criti-

other disorders in the technical system, pre-emergency (emergency) situations and the transfer of information on their occurrence to the visualization, dispatching and situational management systems at various levels (to decision makers (DM), dispatchers, operators, etc.). The sources of information on possible abnormal deviations (malfunctions) in CTS or their subsystems (nodes) operation are sensors, elements of the system that can register various parameters of the system state, environment, parameters of the CTS operation, etc.

The resulting risk of malfunction, failure, accident, SE or other disruption of the normal CTS operation, registered by the sensor, is called a threat. In this case, the occurrence of a certain threat presumably leads to the processes of disturbance propagation along the structural elements of CTS accordance with their interaction scheme. Since, in accordance with the definition above, threats can be of different nature (type, nature of occurrence and manifestation, etc.), the CTS elements can interact with each other in various ways during the disturbance propagation process. As a result, schemes of interaction between elements will be different for each type of threat. Hence, the disturbances will also propagate through the elements of the CTS along different paths.

Technical systems of high structural, dimensional and functional complexity usually include a large number of sensors, which makes it significantly more difficult to monitor their readings, diagnose abnormal situations, and most importantly, make timely accurate control decisions in the event of reading deviation from the norm and especially the threat of SE occurrence. Thus, problem of choosing the structure of the dispatching or situational management information system arises. It should allow reducing the operator's stress in order to increase the emergency response rate without a significant loss of awareness about safety critical processes [5, 7-8].

For the purpose of simulating the processes of propagation of the disturbances that occur as the result of malfunctions, the theoretic graph approach will be used. The representation of the structure of a technical system in the form of a graph is widely used for visualization and modeling of the correlations between system elements. At the same time, the structure of the system can be rigidly fixed or undergo certain regular changes (which is typical of dynamic systems) depending on the process or phenomenon being simulated.

In this approach the structure of a system and the interactions between its elements are represented in the form of a directed graph. Each node and edge of a graph is assigned certain parameters and functionals that reflect the processes of operation of the simulated system elements. The initial pulse (disturbance) applied to one or several nodes is propagated through the whole graph changing the parameters of the nodes. In the general case, the magnitude of the pulse itself can change as well in accordance with the function-als assigned to the edges of the graph. The simulation uses discrete time with a fixed step Δt . This approach to simula-

Being a crucial part of the Russian transportation industry railways play an essential role in the process of the country's socio-economic development, since this type of transport has practically no alternative in terms of the volume and structure of freight and passenger traffic. The leading role of railway transportation is also determined by the country's specific characteristics, including significant transport distances, remoteness of primary mining facilities and sources of raw materials from the points of processing and consumption, as well as seaports, insufficient infrastructure development of other types of transport in Siberia and the Far East, which are of strategic importance for the national development. The condition, safety and quality of rail transportation define not only the prospects for further social and economic development, but also the nation's ability to effectively perform such essential functions as protecting its sovereignty and security, providing citizens with transportation and creating conditions for more even economic development of individual regions, etc.

The URKAN integrated system for management of resources, risks and dependability of railway infrastructure facilities at lifecycle stages is being developed and widely implemented by specialized organizations and divisions of the Russian Railways since 2010 [1]. Essentially, the system implements a comprehensive process of dependability, resources and functional safety management in railway transportation and is essentially an extended RAMS (reliability, availability, maintainability and safety) and LCC (life cycle cost) methodology.

The primary strategic railway safety objectives are [2]:

1. Improving the efficiency of the main activity, utilization of infrastructure, technical reliability and fixed assets availability,
2. Ensuring the quality of products, services and processes,
3. Ensuring transportation safety.

The system of railway facilities and processes is a massive geographically distributed multi-purpose infrastructure that includes JSC Russian Railways facilities (track and structures, signalling, communication, electrification and power facilities; locomotive, car and passenger facilities) that are different in purpose and solve different process-specific tasks. At the same time, the complexity of the technical systems included in the above facilities continuously increases, which inevitably leads to an increase in the number and variety of risks associated with the production, adjustment, maintenance, operation and upgrading of these systems [3].

Ensuring safety and dependability becomes especially important with the use of "driverless" vehicles. According to the International Association of Public Transport, there are 5 Grades of Automation of trains (from GOA0 to GOA4). When GOA4 level is implemented, there is no operational personnel onboard rolling stock. Under

1. Simulation of disturbance propagation in the technical system

Today, the technological development goes hand in hand with the increase in the number of elements involved in technical systems (dimensional complexity), the increase in the diversity of interaction structures of these elements (structural complexity) and the increase in the diversity of the forms and methods of this interaction (functional complexity). This significantly complicates the task of ensuring the reliable operation of complex technical systems (CTS) that are part of the railway infrastructure facilities, since, depending on their structural and functional features, the manifestation of the risks and the nature of failures and faults propagation in the considered systems may differ [5]. In this case, the realization of risks may take the form of the possibility of malfunctioning or failure of a separate node and the entire system. The aim of this paper is to develop the methods of analysis and simulation of the processes of occurrence and development of emergencies at complex railway infrastructure facilities from indicator-based approach point of view.

The extensive experience of operating CTS of various types and purposes shows that the occurrence of failures and faults of various nature, as well as incidents and emergencies they lead to (hereinafter referred to as sudden emergencies, or SE) is usually preceded by the stage of accumulation of defects in the equipment or deviations in a particular process [6]. The duration of this stage can vary significantly (from minutes to days). At the same time, at first the defects or deviations themselves do not pose an immediate threat of SE occurrence. In practice the processes of accumulation of such deviations are usually associated either with the unobservability of the CTS elements and subsystems due to the lack of effective monitoring and diagnostic tools, or, even more often, with the fact that personnel are accustomed to such deviations, since they do not always lead to accidents. At the next stage a sudden so-called initiating event occurs, which leads to an avalanche-like development of unfavorable processes and the occurrence of SE, the consequences of which are significantly aggravated by the lack of organizational and technical countermeasures, as well as lack of time and resources for their effective implementation. It is obvious that the SE, occurring at the third stage as a result of the rapid development of events, for the most part would be impossible without the accumulation of deviations and errors in the first stage.

Thus, one of the main tasks of ensuring the smooth operation of CTS is the timely identification of malfunctions,

Indicator-based approach to safety management of railway infrastructure facilities

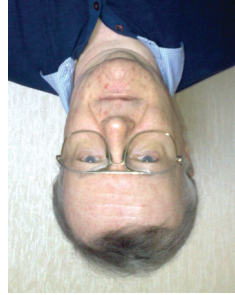
Leonid A. Baranov, Russian University of Transport (MILT), Russian Federation, Moscow
Vladimir V. Kulba, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS), Russian Federation, Moscow
Alexey B. Shelkov, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS), Russian Federation, Moscow
Dmitry S. Somov, Sberbank, Russian Federation, Moscow



Leonid A. Baranov



Vladimir V. Kulba



Alexey B. Shelkov



Dmitry S. Somov

Abstract. The Aim of this paper is to develop the methods of analysis and simulation of the processes of occurrence and development of emergencies at complex railway infrastructure facilities. It cites analysis data on the threats, causes and consequences of sudden emergencies at complex railway infrastructure facilities, as well as timely identification of faults, it is proposed to use the indicator-based approach that allows diagnosing and formally analyzing the processes of occurrence and propagation of malfunctions across the elements of complex technical systems. For the purpose of simulating the processes of propagation of the disturbances (hazards of emergencies) that occur as the result of malfunctions, it is proposed to use the theoretic graph approach that involves model and visual representation of the structure of a technical system under consideration in the form of a directed graph that shows the correlations between its elements. Each node and edge of a graph is assigned certain parameters or functionalities that reflect the processes of correlated operation of the elements of the simulated system. The propagation of disturbances within a system is simulated with pulse processes initiated in one or several nodes. The paper refers to the developed formalized models of disturbance propagation in a technical system based on the construction of structural components and correlation matrices. The authors introduce the concept of critical element of a technical system that helps identify the event of its failure. Two basic criteria of technical system failure, i.e. the exclusive (a system is considered to have failed if the disturbance has reached any of the critical elements) and absolute criterion (failure occurs if the disturbance has reached the specified subset of critical elements) are defined. The paper provides an analytical example that illustrates the capabilities of the proposed model of disturbance propagation within the structure of a technical system. For the purpose more efficient diagnostics of the hazard of emergencies in railway infrastructure facilities the paper proposes a model of application of structurally integrated indicators that consists in the integration of indicators within the structure of a technical system that would immediately deliver the required and sufficient information in case of emergency. The main task would be to identify a set of indicators with the primary purpose of reducing the information-related stress and concentration of dispatchers' or operators' attention on the processes within a technical system that are most relevant in terms of accident-free and safe operation. Basic criteria are identified for the generation of the set of indicators within a complex technical system: maximum of reliability of the disturbance consequences estimate, maximum of accuracy of emergency causes identification, minimum of emergency identification time, minimum of nonrecurrent and current costs. A modified graph model of disturbance propagation in a complex technical system is provided that is the prerequisite for solving the multicriterion problems of optimal location of indicators within the structure of a technical system in terms of completeness, accuracy and timeliness of detection of failures of various types. Automation of the processes of generation of indicator sets using models of disturbance propagation in technical systems will allow using the proposed methods as part of further development of the URRAN methodology in terms of improvement of the decision support in railway infrastructure facilities management.

Keywords: control, railway transportation, infrastructure facility, technical system, emergency, sensors, indicators, simulation.

For citation: Baranov LA, Kulba VV, Shelkov AB, Somov DS. Indicator-based approach to safety management of railway infrastructure facilities. Dependability 2019;2: 33-41. DOI: 10.21683/1729-2646-2019-19-2-33-41

- [2] Shubinsky I.B. Funktsionalnaya nadezhnost infor-matsionnykh sistem: Metody analiza [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal, 2012 [in Russian].
- [3] Shubinsky I.B. Nadiozhnie otkazoustoychivie infor-matsionnie sistemy. Metody sinteza [Dependable fail-safe information systems. Synthesis methods]. Moscow: Dependability Journal, 2016 [in Russian].
- [4] Shubinsky I.B. O poniatii funktsionalnoy nadezhnosti [On the concept of functional dependability]. Dependability 2012;4:74-84 [in Russian].
- [5] Shubinsky I.B. Methods of software functional dependability assurance. Dependability 2014;4:95-101.
- [6] Shubinsky I.B., Zamyshlyayev A.M., Pronevich O.B. Graph method for evaluation of process safety in railway facilities. Dependability 2017;17(1):40-45.
- [7] Pronevich O.B., Shved V.E. Algorithm of calculation and forecasting of functional safety indicators of railway power supply systems. Dependability 2018;18(3):46-55.
- [8] Rozenberg E.N., Penkova N.G., Korovin A.S. Functional dependability of the display unit software of the BLOK system. Dependability. 2017;17(2):36-40.
- [9] Shukhina E.E., Astrakhan V.I. Bezopasny lokomotivny obiedinenny kompleks BLOK [BLOK vital integrated onboard system]. Moscow, 2013 [in Russian].
- [10] Zorin V.I., Astrakhan V.I. Unifitsirovannoe kompleksnoe lokomotivnoe ustroystvo bezopasnosti (KLUB-U) [Standardized integrated onboard train protection system (KLUB-U)]. Moscow: Training and Methodology Centre for Railway Transport, 2008 [in Russian].
- [11] GOST R IEC 61508-7-2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 7. Techniques and measures. Moscow: Standartinform, 2014 [in Russian].
- About the authors**
- Elm N. Rozenberg**, Professor, Doctor of Engineering, First Deputy Director General, JSC NIAS Russia, Moscow, e-mail: info@vnias.ru
- Alexander S. Korovin**, Chief Specialist of Computer-Based Devices Development Sector, JSC NIAS, Russia, Moscow, e-mail: A.Korovin@vnias.ru
- Natalia G. Penkova**, Deputy Head of Safety and Algorithmic Support, JSC NIAS, Russia, Moscow, e-mail: N.Penkova@vnias.ru

Received on 08.04.2019

Acknowledgement

The authors express their gratitude to Prof. Igor B. Shubinsky, Doctor of Engineering, for his assistance, valuable advice and observations that contributed to this paper.

References

- [1] Ivitsky V.A. Modelirovaniye informatsionnykh sistem zheleznodorozhnogo transporta. Uchebnoye posobiye [Simulation of information systems of the railway industry. Study guide]. Moscow: MIIIT, 2011 [in Russian].

Conclusion

This paper shows the efficiency of adding pre-trip diagnostics of the display unit by the driver or service personnel to the inbuilt tools for diagnosing failures in the display unit. Thus, the probability of a system's transition into a forbidden state, i.e. a state when the failure will not be detected by the inbuilt or additional diagnostic tools, will be reduced more than twice.

Conclusion

As the considered models describe a complete group of events, the probability of hitting the only forbidden state is in both cases 1. Thus, based on the calculated value of conditional probability $b_{16/S_{26}}$, we conclude that adding pre-trip diagnostics of the display unit by the driver or service personnel allows reducing the probability of the display unit transitioning into a forbidden state during the trip more than twice (from 1 to 0.47).

$$b_{16/S_{26}} = \frac{\Delta G_{sp}}{\sum_{k \in S_{26}} \Delta G_k^{16}} = \frac{p_{14} * p_{46} * \Delta G_1^{16}}{1 - C_1 - C_2 - C_3 - C_4 - C_5} = 0,53.$$

As the considered models describe a complete group of events, the probability of hitting the only forbidden state is in both cases 1. Thus, based on the calculated value of conditional probability $b_{16/S_{26}}$, we conclude that adding pre-trip diagnostics of the display unit by the driver or service personnel allows reducing the probability of the display unit transitioning into a forbidden state during the trip more than twice (from 1 to 0.47).

By substituting data from Table 1 we obtain the conditional probability of transition from state S_1 to state S_6 :

edges equals to: $\Delta G_1^{16} = 1$.

in the k -th path from node "1" to node "6" and connected of node "6" out of the graph, as well as the nodes situated The weight of resolution accounting for the exclusion $\Delta G_{sp}^{16} = 1 - (C_1 + C_2 + C_3 + C_4 + C_5)$.

For the considered case, the weight of graph resolution without the nodes of the forbidden state set equals:

C6: $S_6 \rightarrow S_6$, circuit weight is p_{66} .

C5: $S_1 \rightarrow S_4 \rightarrow S_5 \rightarrow S_1$, circuit weight is $p_{14} * p_{45} * p_{51}$.

C4: $S_1 \rightarrow S_4 \rightarrow S_1$, circuit weight is $p_{14} * p_{41}$.

- *path* is a chain of series-connected unidirectional edges with the beginning in the state i and the end in the state j , the path weight being

$$l_{ij}^k = \prod_{r \in S} p_{ij}^r p_{ij}^r$$

where p_{ij}^r is the probability of one-step transition from state i into state j , p_{ij}^r is the probability of one-step transition from state r into state j ;

- *closed circuit* is a chain of series-connected unidirectional edges, in which the output of the final node in the circuit is connected to the initial node of the circuit. The weight of the j -th circuit is identified by the formula:

$$C_j = \prod_{i,j \in S} p_{ij}^i p_{ij}^j$$

- *loop* is a case of closed circuit, in which the incoming and outgoing edges merge into one edge, the weight of a loop is $C_j = p_{jj}^j$;

- *graph resolution* is a part of a graph that does not contain defined nodes and connected edges; the weight of resolution ΔG_i^j is calculated subject to the exclusion of node i and connected edges out of the graph; the weight of resolution ΔG_i^j is calculated subject to the exclusion of node i out of the graph, as well as the nodes situated in the k -th path from the initial node to j and connected edges;

- the *weight of resolution* is found using Mason's formula:

$$\Delta G = 1 - \sum_j C_j + \sum_{j_1, j_2} C_{j_1} \cdot C_{j_2} - \sum_{j_1, j_2, j_3} C_{j_1} \cdot C_{j_2} \cdot C_{j_3} + \dots$$

In order to evaluate the efficiency of introducing pre-trip diagnostics, let us calculate the conditional probability of transition from the initial state "1" into the forbidden state "6", provided that the inbuilt diagnostic tools (internal diagnostics) are disabled (paths $S1 \rightarrow S2 \rightarrow S6$ and $S1 \rightarrow S2 \rightarrow S3$).

In accordance with the theorem for evaluation of the probability of system transition from the initial allowed state into a forbidden state, the conditional probability of transition from $S1$ to $S6$ is defined with the formula:

$$b_{16/S126} = \frac{\sum_{f \in S_p} l_{16}^k \Delta G_k^f}{\Delta G_{S_p}^{S_p}}$$

As it can be seen in the graph in Figure 2b, the number k of transition paths from $S1$ to $S6$ - provided that display unit failure detection relies only on pre-trip diagnostics of the display unit by the driver or service personnel - equals 1. Identification of path weights: $l_{16}^1 = S1 \rightarrow S4 \rightarrow S6 = p_{14} \cdot p_{46}$.

Identification of circuit weights:

$C1: S1 \rightarrow S1$, circuit weight is p_{11}^1 ;

$C2: S1 \rightarrow S2 \rightarrow S1$, circuit weight is $p_{12} \cdot p_{21}^1$;

$C3: S1 \rightarrow S2 \rightarrow S3 \rightarrow S1$, circuit weight is $p_{12} \cdot p_{23} \cdot p_{31}^1$.

States $S1$ and $S2$ are allowed and belong to the set "normal

diagnostics is to be initiated).

The value p_{21}^1 is selected based on the actual depend-

ability of the display unit in the course of its operation.

Statistically, a failure of the display unit is a low-probability event (70 failures were registered in 2018 throughout

the railway network based on operational data, the total number of systems being 11740). The fact that a failure

has not been registered in the course of operation does not mean that the unit is operational the whole time. It may

have been in a forbidden state of hidden failure for some period of time. The values of probabilities of transitions

p_{23}^1 and p_{26}^1 were distributed based on the efficiency of the internal diagnostic tools implemented in the unit.

The failure detectivity by the inbuilt diagnostic tools implemented in the display unit are at 0.5 in accordance

with GOST R 61508-7-2012.

Table 2 shows the values of probabilities of one-step transitions from the i -th state to state j (p_{ij}^i).

Table 1. Transition probabilities matrix

	State					
	1	2	3	4	5	6
1	0,72	0,18	0	0	0	0
2	0,85	0	0	0	0	0
3	1	0,075	0	0	0	0
4	1	0	0	0,15	0,15	0
5	1	0	0	0	0	0
6	1	0	0	0	0	0
Σ	6	5	4	5	6	1

The problem consists in the identification of the effect of introduction of pre-trip diagnostics on the probability of display unit transitioning into a forbidden state during intended operation, when only in-built diagnostic tools are used. In order to solve this problem, let us use theorem that states that the probability of system transition from the specific i -th initial non-hazardous state into any hazardous state f is defined by formula [5]

$$b_{ij}^k = \frac{\sum_{f \in S_p} l_{ij}^k \Delta G_k^f}{\Delta G_{S_p}^{S_p}}$$

where l_{ij}^k is the k -th path leading from a non-hazardous state of graph i into a hazardous state f ;

ΔG_k^f is the weight of graph resolution without the f -th node and graph nodes situated on the k -th path;

$\Delta G_{S_p}^{S_p}$ is the weight of graph resolution without the nodes of the hazardous state set.

Let us set forth the following topological concepts used in mathematical simulation [3]:

Let us represent the operation algorithm of a display unit with inbuilt diagnostic tools and pre-trip diagnostics in the form of a flow diagram (figure 1). Let us construct the graph of the operation algorithm of the display unit shown in Figure 1. Events of irregularities of display unit operation are random in their nature. Let us represent the considered operation algorithms of the display unit with a directed state graph $G(S, H)$, where S is the finite set of system states, H is the finite set of edges between nodes i, j (states s_p, s_j). The states of display unit operation can be described as follows: if the display unit is in state s_p , then with probability p_{ij} it can transition into state s_j .

Figure 2a shows a state graph in which only the inbuilt diagnostic tools are used for detection of display unit failure. Figure 2b shows a state graph in which the detection of system failures involves not only the inbuilt display unit diagnostic tools, but additionally pre-trip diagnostics of the display unit by the driver or service

Models description

The display unit has inbuilt diagnostic tools that verify the operability of the display unit with a level of diagnostic coverage that is sufficient to ensure safety. Inbuilt diagnostic tools are able to detect a number of irregularities in the display unit operation. In order to extend the list of detectable errors, it is proposed to introduce additional pre-trip diagnostics by the driver or service personnel to be conducted before each trip. Among other things, that will allow preventing locomotives with faulty safety devices to be cleared for operation. The aim of this paper is to show the efficiency of diagnostic tools in man-machine interaction in the context of onboard systems. It is also to demonstrate that the development, deployment of new diagnostic tools and improvement of the existing diagnostic tools enables better operational characteristics of the display unit and reduced probability of its transition into a forbidden state.

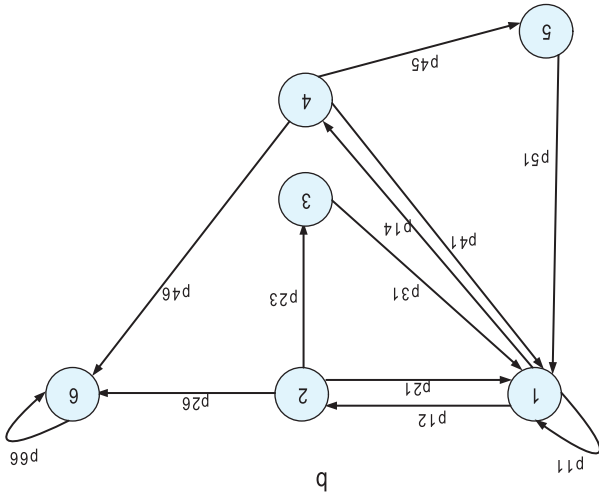
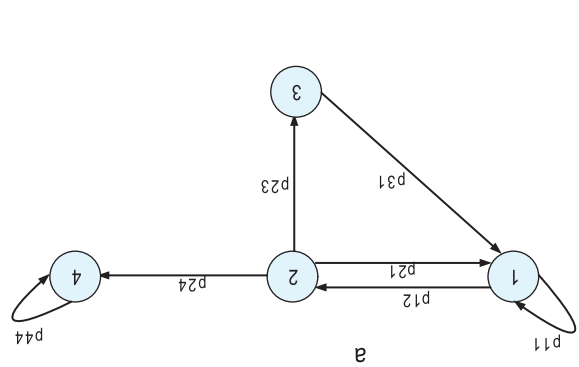


Figure 2. State graph: a) with inbuilt diagnostic tools and added pre-trip diagnostics of the display unit by the driver or service personnel.

personnel. In order to attain the goal of this paper, let us consider the graph in Figure 2b. The graph has the following states:

State S_1 , display of the current operational situation by the display unit software;

State S_2 , testing for failures by inbuilt diagnostic tools (software check for CAN errors, software check for controller freeze by watchdog timer switching, software check of display unit being present in the configuration);

State S_3 , elimination by the display unit of failures detected by the inbuilt diagnostic tools (software reboot of CAN interface, hardware controller reboot by means of watchdog timer, hardware reboot of display unit software);

State S_4 , testing for failures by means of pre-trip diagnostics of display unit (correctness of command processing, correctness of operational situation display, correctness of installed version of software, correctness of parameter values of constant characteristics);

State S_5 , elimination by the driver or service personnel of failures detected by means of pre-trip diagnostics (immediate elimination of detected errors, display unit software update input of correct parameter values of constant characteristics);

State S_6 , i.e. display unit being in a state with a hidden failure.

S is the complete set of states, $S = \{S_1, S_2, S_3, S_4, S_5, S_6\}$;

S_p is the subset of non-forbidden states, $S_p = \{S_1, S_2, S_3, S_4, S_5\}$;

$\bar{S}_p$ is the subset of forbidden states, $\bar{S}_p = \{S_6\}$.

Provided that the display unit's inbuilt and pre-trip diagnostic tools are operable, the existence of failure in the display unit is identified and the system is put into failure elimination mode.

It is assumed that in case of failure detection the system is restored. In case of non-detection of failure by the inbuilt and pre-trip diagnostic tools of the display unit due to their failure or insufficient efficiency the system is put into hidden failure mode (forbidden state).

Introduction

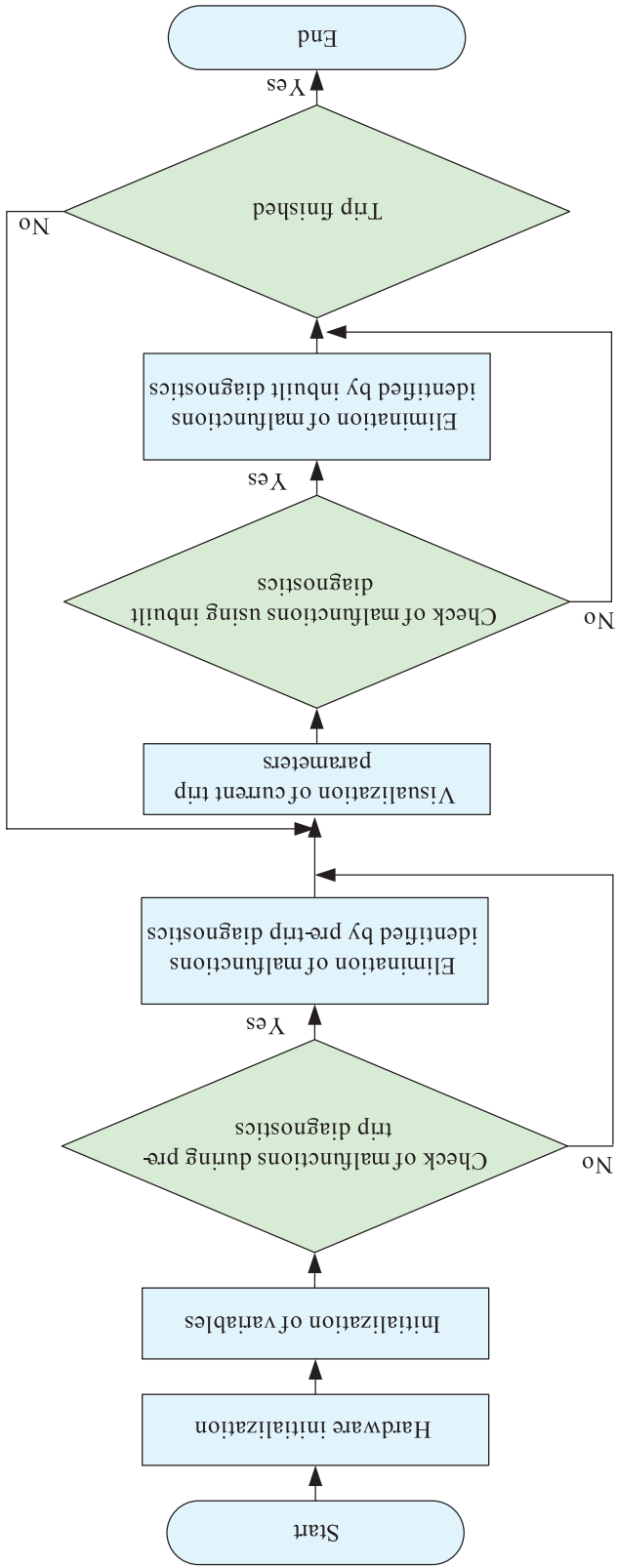
probability of the display unit transitioning into a forbidden state that causes disruption of display unit operability. A forbidden state, in this case, is understood as a hidden (not detected by diagnostic tools) failure.

Simulation is widely used in the railway industry for planning of forbidden state handling. In case of intelligent systems, mathematic simulation is advantageous. Methods of mathematic simulation are subdivided into two groups: analytical and simulation modeling. Due to certain shortcomings of simulation modeling [1], in the context of intelligent railway systems, the construction of the analytical model of probability evaluation is of principal interest due to the feasibility of demonstration of the factors that are taken into consideration by such model. Forbidden events that cause inoperability of intelligent railway systems are random; they can be represented as a random process. A random process of system development, transition from an allowed state into a forbidden state, system state changes in time can be described with a semi-Markovian process. In general, the construction and solution of semi-Markovian models comes down to building a system of homogeneous differential equations. This procedure always involves mathematical difficulties. For this reason the paper shows the feasibility of representation and solution of semi-Markovian models with a coupled graph model [3, 5]. Such models are highly visual, allow formalizing the wanted system states, as well as paths of transition from allowed into hazardous states, does not require the use of complex mathematics in the preparation of measures of forbidden event handling.

Problem definition

Currently, the Russian railway industry employs the following intelligent onboard systems: KLUB-U (standardized integrated onboard train protection system), BLOK (vital integrated onboard system) and BLOK-M (scalable vital integrated onboard system). The KLUB-U, BLOK and BLOK-M systems have their own display units equipped with man-machine interfaces. A display unit is a hardware and software system. This system is to ensure information display to the driver, assistant driver, operator in case of driverless operation, service personnel in case of locomotive driving and pre-trip diagnostics. The display of information on the permitted speed, target speed, actual speed, track profile, distance, stopping point ahead, train schedule, train ahead, stop aspect enables safe locomotive driving in terms of observation of speed limits in normal operation and prediction of safe mode of locomotive driving. In the process of operation, system operability may be disrupted due to a random hardware failure, manifestation of a systematic failure in its software, driver's error while interacting with the system, input data error. Any disruption of system operability is regarded as its failure. This causes the display of incorrect information and wrong decisions by the driver in terms of safety of locomotive driving. That is why great attention is paid to the development and application of diagnostic tools that allow minimizing the

Figure 1. Flow diagram of the operation algorithm of a display unit with inbuilt diagnostic tools and pre-trip diagnostics



Model of efficiency assessment of diagnostic tools of onboard equipment

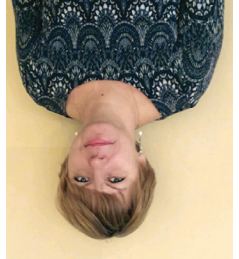
Effim N. Rozenberg, JSC NIIS, Russian Federation, Moscow
 Alexander S. Korovin, JSC NIIS, Russian Federation, Moscow
 Natalia G. Penkova, JSC NIIS, Russian Federation, Moscow



Effim N. Rozenberg



Alexander S. Korovin



Natalia G. Penkova

Abstract. The Aim of this paper is to show that the development, deployment of new diagnostic tools and improvement of the existing diagnostic tools in onboard equipment enables better operational characteristics and reduced probability of transition of intelligent railway systems into a forbidden state. **Method.** In the context of intelligent railway systems, the construction of the analytical model of probability evaluation is of principal interest due to the feasibility of demonstrating the factors that are taken into consideration by such a model. Forbidden events that cause inoperability of intelligent railway systems are random; they can be represented as a random process. A random process of system development, transition from an allowed state into a forbidden state, system state changes in time can be described with a semi-Markovian process. When assessing the probability of system transition into a forbidden state, the question arises as to the selection of a method of calculation. The paper shows the feasibility of representation and solution of a semi-Markovian model with the help of a coupled graph model [3, 5] that has a high level of visualization and is a well-formalized method of identification of the probability of a system's transition into a forbidden state. The set of system states and their connections are represented with a directed state graph with defined topological concepts [3]. In order to identify the effect of the introduction of new diagnostic tools and improvement of the existing diagnostic tools in onboard equipment on the probability of transition of intelligent railway systems into a forbidden state, the authors use the theorem of identification of the probability of system's transition from the initial unhazardous state into a hazardous state and set forth the formula to calculate this probability. **Results.** The graph method implemented in this paper shows that the use of additional diagnostic tools reduces more than twice the probability of a system's transition into a forbidden state, i.e. a state when the failure will not be detected by the inbuilt or additional diagnostic tools.

Keywords: onboard train protection systems, display unit, functional dependability, graph model

For citation: Rozenberg EN, Korovin AS, Penkova NG. Model of efficiency assessment of diagnostic tools of onboard equipment. *Dependability* 2019;2: 28-32. DOI: 10.21683/1729-2646-2019-19-2-28-32

comprehensive facility security assets. Penza-Zarechny,

2016. p. 223-229 [in Russian].

[16] Ivanov A.I., Perfilov K.A., Malygina E.A. Multivariate statistical analysis of the quality of biometric data on extremely small samples using the criteria of the geometric mean tests calculated for the analyzed probability functions. Measuring. Monitoring. Management. Control 2016;2(16):64-72 [in Russian].

[17] Ivanov A.I., Perfilov K.A., Malygina E.A. Evaluation of the quality of small samples of biometric data using a differential variant statistical test of the geometric mean. Vestnik SibGAU 2016;4(17):864-871 [in Russian].

[18] Malygin A.Yu., Volchikhin V.I., Ivanov A.I., Fun-tikov V.A. Bystrye algoritmy testirovaniya neyrosetevykh mekhanizmov biometricheskoy zaschity informatsii [Fast algorithms for testing of neural network mechanisms of biometric and cryptographic protection of information]. Penza, Penza State University Publishing 2006 [in Russian].

[19] Akhmetov B.S., Volchikhin V.I., Ivanov A.I., Malygin A.Yu. Algoritmy testirovaniya biometricheskoy zaschity informatsii [Algorithms for testing of biometric and neural network mechanisms of information protection]. Almaty: Satpayev KazNTU, 2013 [in Russian].

About the authors

Alexander I. Ivanov, Doctor of Engineering, Associate Professor, Lead Researcher of Laboratory of Biometric and Neural Network Technologies, Penza Research and Design Electrical Engineering Institute, Russian Federation, Penza, e-mail: ivan@pniel.penza.ru

Evgeny N. Kuprianov, post-graduate student, Department of Information Security Technology, Penza State University, Russian Federation, Penza, e-mail: ibst@pnzgu.ru
Sergey V. Turev, Head of Research and Technology Center, Research and Design Institute for Communications and Control Systems, Russian Federation, Moscow, e-mail: niissu@niissu.ru

Received on: 22.01.2019

[9] Akhmetov B.B., Ivanov A.I. Estimation of quality of a small sampling biometric data using a more efficient form of the chi-square test. Dependability 2016;16(2):43-48.

[10] R 50.1.037-2002. Rekomendatsii po standartizatsii. Prikladnaya statistika. Pravila proverki soglasia opytogo raspredeleniya s teoreticheskim. Chast I. Kriterii tipa χ^2 [Standardization recommendations. Applied statistics. Rules for compliance verification of experimental distribution with the theoretical one. Part I. Chi-square-type criteria]. Moscow: Gosstandart of Russia, 2001 [in Russian].

[11] R 50.1.037-2002. Prikladnaya statistika. Pravila proverki soglasia opytogo raspredeleniya s teoreticheskim. Chast II. Neparametricheskie kriterii [Applied statistics. Rules for compliance verification of experimental distribution with the theoretical one. Part II. Non-parametric tests]. Moscow: Gosstandart of Russia, 2002 [in Russian].

[12] Haykin S. Neural Networks: A Comprehensive Foundation. Moscow: Williams, 2006.

[13] Serikova N.I., Ivanov A.I., Serikova Yu.I. Otsenka pravdopodobia gipotezy o normalnom raspredelenii po kriteriu Dzhini dlia chisla stepeny svobody, kratnogo chislu opytov [Likelihood estimation of the hypothesis of normal Gini distribution for the number of degrees of freedom multiple of the number of experiments]. Voprosy radioelektroniki 2015;1(1):85-94 [in Russian].

[14] Perfilov K.A. Kriterii srednego geometricheskogo, ispolzuemy dlia proverki dostovernosti statisticheskikh gipotez raspredeleniya biometricheskikh dannyykh [Criteria of geometric mean used for validity verification of the statistical hypotheses of biometric data distribution]. Proceedings of the science and technology conference of the Penza information technology security cluster. Penza, 2014. Vol. 9. p. 92-93, <http://www.pniel.penza.ru/RV-conf/T9/S92> [in Russian].

[15] Ivanov A.I., Perfilov K.A. Otsenka sootnosheniya moshchnostey semeystva statisticheskikh kriteriev "srednego geometricheskogo" na malykh vyborkakh biometricheskikh dannyykh [Assessment of the relations of the strengths of the "geometric mean" family of statistical tests on small samples of biometric data]. XI All-Russian Science and Practice Conference Modern security technologies and

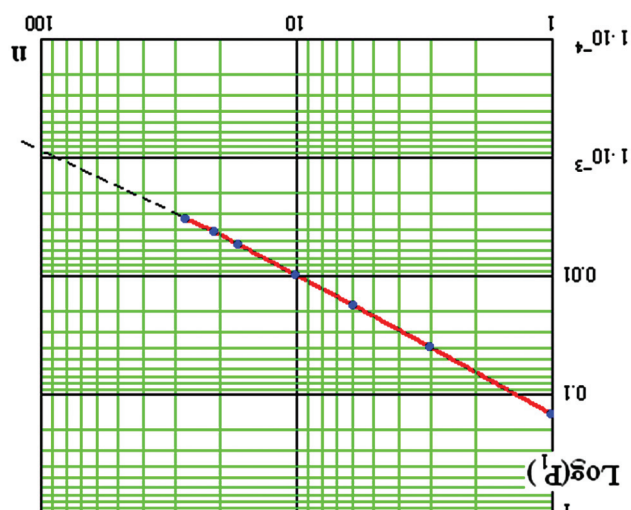
In this context, the approach to the synthesis of new statistical criteria is fundamentally changing. After Pearson, mathematicians were trying to find a new, more powerful criterion. A great number of analyzed criteria proved to have low power, and therefore were not published. With neural network integration of a set of statistical criteria, the power of each of them becomes secondary. The correlation relationships between the added criterion and the group of other criteria are also very important. In our case, two integrated criteria have almost the same power, but in this group there is a special Shapiro-Wilk criterion that has low correlation with the primary chi square and Cramér-von Mises criteria.

Thus, the possible diversity of statistical criteria is to be researched again, taking into account not only their relative power, but also the values of their correlation coefficients in groups with other relevant statistical criteria. New statistical criteria with relatively low power of hypothesis separation were previously rejected and not published, but now the situation has changed. It is more important to understand how the new criterion complements the already studied statistical criteria. Probably, it will be necessary to create a table of the level of affinity (correlation) of already known and promising statistical criteria in the nearest future. Linearly independent (weakly correlated) statistical criteria have to be grouped, and neural network integrations are to be created for them.

References

- [1] Pokhabov Yu.P. Problems of dependability and possible solutions in the context of unique highly vital systems design. Dependability 2019;19(1):10-17.
- [2] Pokhabov Yu.P. Ensuring dependability of unique highly vital systems. Dependability 2017;17(3):17-23.
- [3] GOST R 52633.5-2011. Information protection. Information protection technology. The neural network-code converter automatic training. Moscow: Standartinform; 2012 [in Russian].
- [4] Kobzar A.I. Prikladnaya matematicheskaya statistika: dia inzhenerov i nauchnykh rabotnikov [Applied mathematical statistics: for engineers and researchers]. Moscow: FIZMATLIT; 2006 [in Russian].
- [5] Iazov Yu.K., editor, Volchikhin V.I., Ivanov A.I., Funtikov V.A., Nazarov I.G. Neyrosetevaya zashchita personalnykh biometricheskikh dannykh [Neural network protection of biometric data]. Moscow: Radiotekhnika; 2012 [in Russian].
- [6] Sukhoruchenkov B.I. Analiz maloy vyborki. Prikladnye statisticheskie metody [Small sample analysis. Applied statistical methods]. Moscow: Vuzovskaya kniga; 2010 [in Russian].
- [7] Doerffel K. Statistics in analytical chemistry. Moscow: Mir; 1994.
- [8] Dayev Zh.A., Nurushiev E.T. Application of statistical criteria for improving the efficiency of risk assessment methods. Dependability 2018;2:42-45.

Figure 5. The line of decreasing probability of errors of the first kind due to application of several statistical criteria with correlation coefficients of 0,645



by means of extrapolation (dashed line in Figure 5). As the result, the predicted value of the error probability for a neural network generalization of 10 criteria should be $P_1 = 0,01$, and when summarizing 100 criteria the probability of errors should go down to 0,0009. Such a significant reduction of errors probability is a greater incentive for the synthesis of new statistical criteria [13-17].

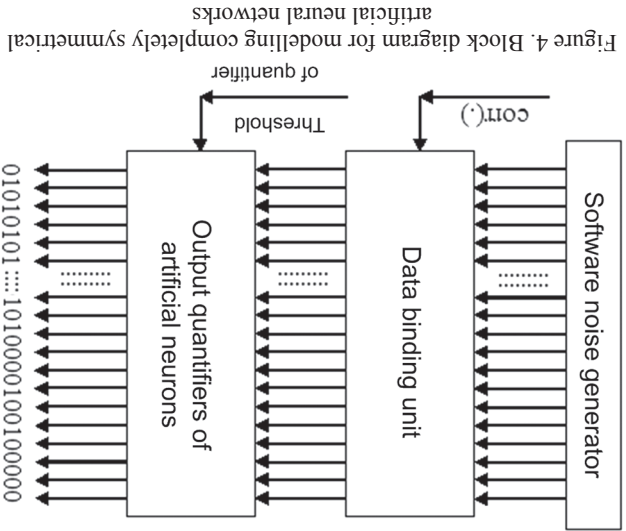
Conclusion

Pearson, who created the chi square criterion in 1900, essentially launched a revolution in statistical processing. The path of development discovered by Pearson proved to be very fruitful and over 119 years his followers have created dozens of different statistical criteria.

Neural networks have been a focus of scientific research since the middle of the 20-th century, but only at the beginning of the 21-st century this technology was implemented into the industry and standardized [3].

The key statement of this paper is that it is possible to combine two seemingly different branches of mathematics. Their integration only requires the neural network biometric data processing technologies that are standardized in Russia and are applied to 3 or more standard statistical criteria. In the case of the considered triple of statistical criteria, this approach reduces the probability of errors more than 7 times. In this case, thesis on expediency of expansion of nomenclature of the existing statistical criteria becomes obvious. The larger is the size of the group of statistical criteria generalized by neurons the better is the final result.

Another simplification is the normalization of the output states of neuron adders that contradicts the data presented in Figures 1, 2, 3, but at the moment only for this simplification there is a positive experience of using symmetrization. Figure 4 shows the block diagram of the numerical experiment. Initial data for the numerical experiment are obtained from 100 software generators of pseudorandom numbers with normal distribution.



As 100 software generators provide independent data, such data needs to be interconnected and correlated equally. Figure 4 shows that this function is performed by the second left block that multiplies the vector of independent random numbers and by a symmetric connecting matrix:

$$(11) \quad \begin{bmatrix} 1 & a & \dots & a \\ a & 1 & \dots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \dots & 1 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{100} \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{100} \end{bmatrix}$$

Due to the symmetry that connects the transfer matrix (11), the output data is correlated equally. To obtain a given value of coefficients of equal correlation $\text{corr}(y_i, y_{i+1}) = 0,645$, it suffices to find the value of one control parameter a . Let us note that the procedure of relations and data symmetrization cannot provide exact correspondences of predictions and real data. If we set the quantization threshold of the neuron emulation block in such a way that the error probability is 0,312, then the output triple will have a total error of 0,138. This result is about 3 times worse than the actual data in Table 1. Let us reduce the equal probability of errors of each neuron from 0,312 to 0,141 to match the results with the observed data. In this case the probability of errors of joint operation of three neurons will be 0,0404. The transition from normal data to data with the equal correlation is profitable as for this special case in logarithmic coordinates the error probabilities and number of neurons are connected by a linear dependence as shown in Figure 5.

Effect of increasing accuracy of estimates with the growing size of the group of neural network integration of statistical criteria

Then, if we consider the codes from Table 1 as some complex characteristic of "data normality" it can lead to errors arising with the probability from 0,0404 to 0,0621. There is about a 7-fold decrease in probability of taking wrong decisions, when using three statistical criteria in comparison with their application one by one.

Code	P_1
"000"	0,0404
"001"	0,0423
"010"	0,0441
"100"	0,0621

Table 1. Error probability for the code states "normal distribution"

Let us consider one of two hypotheses for the majority of states of "0" or "1" in the output code of the three neurons code by analogy with practical application of neural network converters, which is biometrics and code. In this case, each of the four code states "normal distribution" will correspond to its own probability of errors. Table 1 shows these data. The absence of a complete linear dependence (10) of the output states of the three criteria allows combining them for joint application. In this case, the output code of the three neurons "000" will correspond to a triple confirmation of the hypothesis of the data normality of the checked sample. The inverted state of this code "111" will correspond to the triple confirmation of the hypothesis of the uniform law of distribution of small sample data.

The question arises: up to what level is it possible to reduce the probability of errors by means of neural network integration of a collection composed of 100 and more statistical criteria? This question can be answered based on the accumulated technological experience in processing of neural network biometrics data. The neural network symmetrization technology can be used for prediction [18, 19]. To implement it, let us average the error probability of the three previously examined neurons $(0,292+0,303+0,342)/3 = 0,312$. Then, let us average the modules of correlation coefficients between the output states of the three neurons $(10): E(|\text{corr}(\cdot)|) = 0,645$. We proceed from the fact that all of the 100 integrated criteria have symmetric matrices of correlation coefficients with the elements' values outside its diagonal of 0,645.

neuron:

Let us sort the data of the checked sample according to their values to obtain five input parameters of chi square

$$(2) \quad x = \text{sort}(x).$$

At the same time, it is required to calculate the width of the histogram intervals:

$$(3) \quad \Delta x = \frac{x_{20} - x_0}{5}.$$

Furthermore, the position of the interval ends is calculated:

$$(4) \quad X_i = x_0 + \Delta x \cdot i \text{ when } i = 0, 1, \dots, 5.$$

Only after that, it is possible to calculate the number of hits for each of the histogram intervals and form a vector of input parameters $\{n_1, n_2, \dots, n_5\}$ for the neuron (1). The final result is quantized:

$$(5) \quad \begin{cases} z(\chi^2) \rightarrow "0" & \text{if } \chi^2 \leq 7,72; \\ z(\chi^2) \rightarrow "1" & \text{if } \chi^2 > 7,72. \end{cases}$$

As the result, we have a complete formal description of the chi square neuron implementation for a sample of 21 tests.

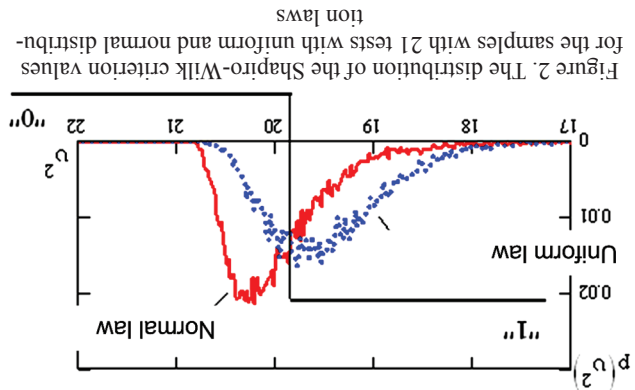
Synthesis and configuration of Shapiró-Wilk neuron with 10 inputs

Obviously, the Shapiró-Wilk criterion can be applied to the same sample of 21 tests [4, 11]. This criterion is calculated as following:

$$(6) \quad v_2 = \frac{1}{\sum_{i=0}^9 a_i \cdot (x_{20-i} - x_i)^2} \cdot \left(\sigma(x) \right)^2,$$

where x_i is the ordered values of the sample being checked, $\sigma(x)$ is the standard deviation, a_i is the table values of the Shapiró-Wilk coefficients.

Figure 2 shows the distribution of the values of this criterion for the uniform and normal laws.



If the functions of (6) are considered as some kind of artificial neuron, then its outputs will be 10 differences of

data of the sample being checked, and the output quantifier will be described as follows:

$$(7) \quad \begin{cases} z(v_2) \rightarrow "0" & \text{if } v_2 \geq 19,8; \\ z(v_2) \rightarrow "1" & \text{if } v_2 < 19,8. \end{cases}$$

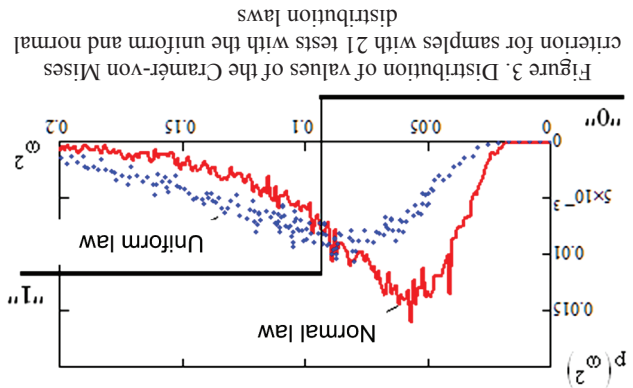
Such configuration of the threshold of the quantifier provides the errors probability of the first and second kind of $P_1 = P_2 = P_{EE} = 0,303$.

Synthesis and configuration of a Cramér-von Mises neuron with 20 inputs

If we compare the chi square neuron (1) and the Shapiró-Wilk neuron (6), we can see the growth of their input dimension (the number of inputs of their adders). The Cramér-von Mises neuron has an even higher input dimension:

$$(8) \quad \omega_2 = \sum_{i=0}^{19} \left(\frac{1}{i+1} - \tilde{P}(x_i) \right) \cdot \frac{x_{20} - x_0}{x_{i+1} - x_i}.$$

Figure 3 shows the distribution of values at the output of the Cramér-von Mises neuron adder.



The configured output quantifier of the neuron adder is described as follows:

$$(9) \quad \begin{cases} z(\omega_2) \rightarrow "0" & \text{if } \omega_2 \leq 0,087; \\ z(\omega_2) \rightarrow "1" & \text{if } \omega_2 > 0,087. \end{cases}$$

Such threshold configuration for quantifier operation provides the same values of errors probability of the first and second kind of $P_1 = P_2 = P_{EE} = 0,342$.

Joint application of three statistical criteria

The statistical criteria described above are linearly independent (they have modules of correlation coefficients less than 1):

$$(10) \quad \begin{cases} \text{corr}(\chi^2, v_2) \approx +0,559; \\ \text{corr}(\chi^2, \omega_2) \approx -0,708; \\ \text{corr}(\omega_2, v_2) \approx -0,667. \end{cases}$$

The problem of control of the data distribution law of small samples

The problems of ensuring the reliability of unique cri-

cal systems [1, 2] are multifaceted and can be solved only through a set of organizational and technical measures. These problems are especially prominent in neural network biometrics. Each of us has a unique biometric image that is to be transformed into a cryptographic key or long access password generated through random symbols. The uniqueness of the transformation is enabled by means of neural network learning, while the learning sample has a close to normal multidimensional data distribution law. The problem is that learning samples are small. In particular, the standard learning algorithm [3] is able to solve the task on samples of 20 examples, if this sample is obtained correctly and has no outliers (gross errors).

In cases of large biometrics data samples (200 tests and more) it is not difficult to test the hypothesis of normal distribution. The chi square criterion or any other statistical criterion can be used [4]. One of the problems of biometrics [5] is that its users do not wish to provide to an automatic neural network learning machine [3] 200 and more instances of their biometric image. Users feel satisfied having submitted a learning sample consisting of 10 to 20 examples of their unique biometric image, for example, a handwritten password or voice password. Users perceive negatively the requirements to present more than 20 examples.

The situation is similar in botany, biology, and medicine. A plan breeder or a biologist is not able to quickly get a sample of 200 animals (plant specimens) with necessary rare characteristics. A sufficient sample for correct statistical estimation can be obtained after a long period of time by selecting and consolidating the desired rare characteristics over several generations.

There is a similar situation in medicine. Large samples are required to test statistical hypotheses. The subject matter of statistical processing of small samples is very popular, but the well-known recommendations [6, 7] do not significantly improve the situation. As a rule, improvements are achieved through the application of several statistical criteria [8]. An attempt could be made to enhance the known statistical criteria [9], but this does not result in major improvements. As a rule, new statistical criteria or variants of earlier criteria individually provide poor results.

The main idea of this paper is the neural network integration of standard statistical criteria [4, 10, 11]. The progress achieved by the Russian neural network biometrics is very significant. Regulators of the Russian information security market have developed the GOST R 52633.xx Russian national series of standards that regulate a number of tough requirements for neural network biometrics. In this paper we will actually attempt to apply the well-developed mathematical techniques of neural network biometrics to new subject areas. At the same time, we will try to show that the very tough requirements of the Russian informa-

Synthesis and adjustment of the chi square neuron with 5 inputs

When testing the normality hypothesis in practice, the Pearson's chi square test is most often used. For a small sample with 21 tests, the formula for calculating the chi square criterion value is the following:

$$\chi^2 = 21 \cdot \sum_{i=1}^5 \left(\frac{n_i}{21} - \Delta \tilde{p}_i \right)^2, \quad (1)$$

where n_i is the number of tests in the i -th histogram interval; $\Delta \tilde{p}_i$ is the expected probability of tests being within the i -th histogram interval under the normal data distribution law of the checked sample.

Let us note that in accordance with the national standard recommendations [10], the average number of tests within each of the histogram intervals is to be close to 5. That is the reason why in formula (1) summation over 5 histogram intervals for a small sample of 21 tests is used.

When developing the formula in 1990, Pearson had no access to computer technologies. For this reason, he was forced to look for asymptotic relations for infinitely large samples. Today the situation has changed. Any student is able to write a program that can produce millions of samples of 21 tests. Figure 1 shows the probability density distribution of the chi square criterion values for samples with a normal and uniform value distribution law.

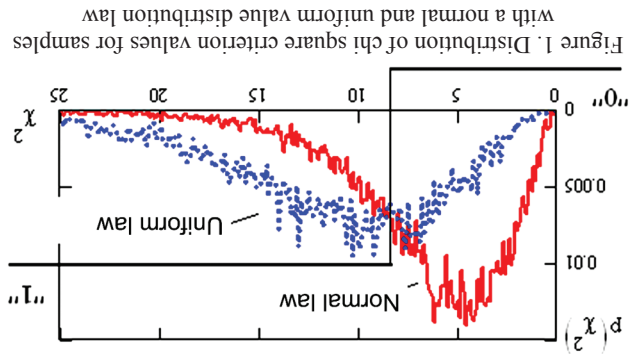


Figure 1. Distribution of chi square criterion values for samples with a normal and uniform value distribution law

Let us note that artificial neurons are configured in such a way as to effectively divide input data into two classes: normal and uniform [12]. Figure 1 shows that the threshold element of the chi square neuron divides the continuum of output elements into two areas: 0 is normal data and 1 is uniform data. The output quantifier of a chi square neuron is configured based on the condition of equally probable error values of the first and second kind of $P_1 = P_2 = P^{EE} = 0.292$.

Neural network integration of classical statistical tests for processing small samples of biometrics data

Alexander I. Ivanov, Penza Research and Design Electrical Engineering Institute, Russian Federation, Penza

Evgeny N. Kuprianov, Penza State University, Russian Federation, Penza

Sergey V. Tureev, Research and Design Institute for Communications and Control Systems, Russian Federation, Moscow



Alexander I. Ivanov



Evgeny N. Kuprianov



Sergey V. Tureev

Abstract. The Aim of this paper is to increase the power of statistical tests through their joint application to reduce the requirement for the size of the test sample. **Methods.** It is proposed to combine classical statistical tests, i.e. chi square, Cram-von Mises and Shapiro-Wilk by means of using equivalent artificial neurons. Each neuron compares the input statistics with a precomputed threshold and has two output states. That allows obtaining three bits of binary output code of a network of three artificial neurons. **Results.** It is shown that each of such criteria on small samples of biometric data produces high values of errors of the first and second kind in the process of normality hypothesis testing. Neural network integration of three tests under consideration enables a significant reduction of the probabilities of errors of the first and second kind. The paper sets forth the results of neural network integration of pairs, as well as triples of statistical tests under consideration. **Conclusions.** Expected probabilities of errors of the first and second kind are predicted for neural network integrations of 10 and 30 classical statistical tests for small samples that contain 21 tests. An important element of the prediction process is the symmetrization of the problem, when the probabilities of errors of the first and second kind are made identical and averaged out. Coefficient modules of pair correlation of output states are averaged out as well by means of artificial neuron adders. Only in this case the connection between the number of integrated tests and the expected probabilities of errors of the first and second kind becomes linear in logarithmic coordinates.

Keywords: statistical tests: chi square, Cram-von Mises, Shapiro-Wilk; artificial neural networks, small samples, normal law of data distribution hypothesis testing.

For citation: Ivanov AI, Kuprianov EN, Tureev SV. Neural network integration of classical statistical tests for processing small samples of biometrics data. Dependability 2019;2: 22-27. DOI: 10.21683/1729-2646-2019-19-2-22-27

The obtained estimate of GPL $t_{\gamma_1}^*$ is recommended for failure-free tests conducted using a binomial plan.

References

- [1] Barzilovich EYu, Beliaev YuK, Kashtanov VA et al., Gnedenko BV, editor. Voprosy matematicheskoi teorii na-dezhnosti [Matters of mathematical dependability theory]. Moscow: Radio i svyaz, 1983 [in Russian].
- [2] GOST 27.002-2015. Industrial product dependability. Terms and definitions. Moscow: Standartinform, 2016 [in Russian].
- [3] Shulenin VP. Matematicheskaya statistika. Chast 1. Parametricheskaya statistika: ochebnik [Mathematical statistics. Part 1. Parametric statistics: a textbook]. Tomsk: Izdatel'stvo NTU, 2012 [in Russian].
- [4] Voinov VG, Nikulin MS. Nesmeshchennye otsenki i ikh primeneniye [Unbiased estimates and their application]. Moscow: Nauka, 1989 [in Russian].
- [5] GOST R 50779.26-2007. Statistical methods. Point estimates, confidence intervals, prediction intervals and tolerance intervals for exponential distribution. Moscow: Standartinform, 2008 [in Russian].
- [6] Mikhailov VS. Implicit estimates for the MBT test plan. Reliability and quality of complex systems 2018, 1(21):64-71 [in Russian].
- [7] Mikhailov VS. Efficient estimation of mean time to failure. Dependability 2016, 4:40-42.
- [8] Ishkov AS, Zuev VD. Evaluation methodology of C-percentile time to failure of electronic components in information-measuring systems by short-term test results. Dependability 2015, 2:86-89.
- [9] Shvetsova-Shilovskaya TN, Gromova TV, Sokolov FP, Ratushenko VG. Computational and experimental method for estimating reliability indicators of technological complex based on the results of its testing using prior information on reliability derived from testing of its components. Dependability 2013, 2:87-92.
- [10] Chumakov IA, Chepurko VA, Antonov AV. Estimation of residual lifetime of alternating process. Common approach to estimations of residual lifetime. Dependability 2013, 2:65-79.

About the author

Viktor S. Mikhailov, Lead Engineer, D.I. Mendeleev Central Research and Design Institute of Chemistry and Mechanics, Russian Federation, Moscow, e-mail: Mvs1956@list.ru

Received on: 25.11.2018

Then,

$$t_{\gamma_1}^* = -T_0 \ln(\gamma) = 0,1053 * 50000 = 5265 \text{ h.}$$

Based on the conventional estimates of $t_{\gamma_1}^*$ it can be concluded that the product complies with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 5265 h, which is in line with the product dependability requirements.

The estimate of MTF T_0 is less efficient than estimate $\hat{T}_q$ [6]. Therefore, the estimate of gamma-percentile time to failure $t_{\gamma_1}^*$ is more efficient than the conventional estimate of the gamma-percentile time to failure $\hat{t}_{\gamma_1}^*$. Then, the comparison of the conventional $\hat{t}_{\gamma_1}^* = 5265$ ($\gamma = 90\%$) and proposed $t_{\gamma_1}^* = 5947$ ($\gamma = 90\%$) estimates of gamma-percentile time to failure $t_{\gamma_1}^*$ shows that the conventional estimation $\hat{t}_{\gamma_1}^*$, as expected, significantly underestimates the gamma-percentile time to failure $t_{\gamma_1}^*$ in comparison with the proposed estimation $t_{\gamma_1}^*$.

Example 3. As the dependability indicator of a product the gamma-percentile storing life t_{γ}^* ($\gamma=0,9$) is used, that must not be lower than one year. Based on the results of 10-year-long storage of one product it is required to estimate t_{γ}^* and verify the product's compliance with the dependability requirements.

Out of formulas (6) and (7) follows that the estimate of the GPL value will be

$$t_{\gamma_1}^* = \hat{T}_q \ln(\gamma) = -\ln(0,9) * \frac{-\ln(1 - \hat{p}(R = 0, N = 1))}{1} = 0,1053 * \frac{\ln(1 - 0,5)}{10} = 1,519 \text{ years.}$$

Based on the estimates of $t_{\gamma_1}^*$ it can be concluded that the product complies with the requirements for the gamma-percentile storing life. The calendar time within which not more than 10 % of products will fail will be 1,519 years, which is in line with the product dependability requirements.

Conclusions

The obtained estimate of GPL $t_{\gamma_1}^*$ is simple and more efficient as compared to the conventional one and not significantly inferior to estimate $\hat{t}_{\gamma_1}^*$, if such exists, in terms of proximity to $t_{\gamma_1}^*$ in case a binomial test plan is used. The obtained estimate of GPL $t_{\gamma_1}^*$ has significant advantages, i.e.:
- the estimate is efficient within a sufficiently wide range of estimates [6],
- the estimate allows obtaining value $t_{\gamma_1}^*$ based on the results of tests that did not produce any failures.

where

$$V(T_0^i(R, N, \tau)) = \frac{1}{\tau} \sum_{\tau_j=1}^{\tau} \sum_{N=10}^{10} \int_0^{\tau_j} \left(\int_0^{\tau_j} \{ET_0^i(R, N, \tau_j) - T_0^i\} \partial T_0 \right)$$

In accordance with [6] the functional $V(T_0^i)$ (along with the functional $A(T_0^i)$ in formula (5) assumes the minimal value, if the estimate of parameter T_0^i is substituted with its efficient estimate based on a sufficiently wide class of biased estimates. In this case, the implicit efficient estimate T_0^i from [6] should be used in the binomial test plan as the parameter of T_0^i (MTF):

$$T_0^i = \frac{-\ln(1 - \hat{p}(R, N))}{1} \quad (6)$$

where the probability of failure estimate $\hat{p}$ is obtained by solving the equation (see formula (3)):

$$F_R(r, N, \hat{p}) = \sum_{k=0}^r p^k (1-p)^{N-k} = 0.5,$$

Then, the efficient estimate of GPL $\hat{t}_{\gamma_1}$ based on a sufficiently wide range of estimates [6] will be as follows (see formula (1)):

$$\hat{t}_{\gamma_1} = -\hat{T}_0^i \ln(\gamma) \quad (7)$$

For failure-free tests the estimate $\hat{t}_{\gamma_1}$ can be used for the MTR as well. Thus obtained estimate of GPL $\hat{t}_{\gamma_1}$ has significant advantages, i.e.:

- the estimate is efficient within a sufficiently wide range of estimates [6],
- the estimate allows obtaining value $\hat{t}_{\gamma_1}$ based on the results of tests that did not produce any failures and conducted using test plans of types N/N or M/R .

Examples

Example 1. As the dependability indicator of a product the gamma-percentile time to failure t_{γ} ($\gamma=0.9$) is used, that must not be lower than 1500 h. Based on the results of 10000-hour-long failure-free tests of one product it is required to estimate t_{γ} and verify the product's compliance with the dependability requirements.

Out of formulas (6) and (7) follows that the estimate of the GPTF value will be

$$\hat{t}_{\gamma_1} = -\hat{T}_0^i \ln(\gamma) = -\ln(0.9) * \frac{-\ln(1 - \hat{p}(R = 0, N = 1))}{1} = 0.1053 * \frac{10000}{-\ln(1 - 0.5)} = 1519 \text{ h.}$$

Based on the estimates of t_{γ} it can be concluded that the product complies with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 1519 h, which is in line with the product dependability requirements.

For comparison, let us mention the conventional solution of example 1. Normally, for tests that did not produce any failures, parameter T_0^i (instead of point estimation) is estimated per the lower confidence contour (hereinafter referred to as LCC) of MTF with the confidence probability of $\gamma = 0.9$. Then, in accordance with [5] the result will be:

$$T_{0.1\%} = \frac{2\hat{\Sigma} x^2(1 - \infty; 2r + 1)}{2 * 1 * 10000} = \frac{2.71}{2} = 7380 \text{ h,}$$

where $x^2(1 - \infty; 2r + 1)$ is the quantile of the χ^2 distribution with a $2r + 1$ degree of freedom (for the NRT test plan), ($\alpha = 1 - \gamma = 1 - 0.9 = 0.1$) is the level of significance per GOST R 50779.26-2007.

$$\hat{t}_{\gamma_1} = -T_{0.1\%} \ln(\gamma) = 0.1053 * 7380 = 777 \text{ h.}$$

Based on the conventional estimates of t_{γ} it can be concluded that the product does not comply with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 777 h, which is not in line with the product dependability requirements.

The comparison of the conventional $\hat{t}_{\gamma_1} = 777$ ($\gamma = 90\%$) and proposed $\hat{t}_{\gamma_1} = 1519$ ($\gamma = 90\%$) estimates of gamma-percentile time to failure t_{γ} shows that for tests that did not produce any failures the conventional estimation using lower confidence estimates significantly underestimates the gamma-percentile time to failure t_{γ} in comparison with the proposed estimation $\hat{t}_{\gamma_1}$.

Example 2. In the conditions of example 1, based on the results of tests of ten products, one failure occurred at the end of the tests. It is required to estimate t_{γ} and verify the product's compliance with the dependability requirements.

Out of formulas (6) and (7) follows that the estimate of the GPTF value will be

$$\hat{t}_{\gamma_1} = \hat{T}_0^i \ln(\gamma) = -\ln(0.9) * \frac{-\ln(1 - \hat{p}(R = 1, N = 10))}{1} = 0.1053 * \frac{10000}{-\ln(1 - 0.16226)} = 5947 \text{ h.}$$

Based on the estimates of t_{γ} it can be concluded that the product complies with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 5947 h, which is in line with the product dependability requirements.

For comparison, let us mention the conventional solution of example 2. Normally, parameter T_0^i is estimated in accordance with [5] using the following formula:

$$T_{0.1} = \frac{\hat{\Sigma} t'_i}{R + 1} = \frac{10 * 10000}{2} = 50000 \text{ h.}$$

Introduction

In today's industry of highly dependable, unique, complex products, it is a commonplace situation when it is required to obtain an estimate of gamma-percentile storing life (GPSL) or gamma-percentile time to failure (GPTF) (hereinafter referred to as GPL, meaning GPSL or GPTF respectively) based on tests that did not produce any failures. Normally, a test plan is classified as type $N\tau$ or $NR\tau$, where N is the number same-type test objects, τ is the operation time (identical for each product), $N(R)$ is the characteristic of the plan that indicates that the product's operability after each failure within the testing time is not recovered (recovered) [1]. GPTF is understood as the operation time during which no failure occurs with the probability γ expressed as the total percentage [2]. Similarly, GPSL is understood as the total schedule time of product storage during and after which the product is able to perform the required function with the probability γ expressed as percentage [2]. If the time to failure complies with the exponential distribution law with parameter T_0 (mean time to failure, hereinafter referred to as MTF), the expected values of GPL (hereinafter referred to as t_γ) is calculated according to formula:

$$(1) \quad t_\gamma = -T_0 \ln(\gamma).$$

Problem definition

Let us consider the case of tests according to a binomial plan.

For a binomial plan, a sufficient statistic is (r) of observed failures and total operation time $S(R, N, \tau, t_i)$ [1, 4, 5], $R = r$ is the random number of failures, t_i is the moments of failures, $i = 1, 2, \dots, R$, then for a binomial test plan the random value R (hereinafter referred to as r.v.) has a binomial distribution $p^N(k)$ [3, formula (1.4.55)] with parameters N and p , $0 < p < 1$, i.e. r.v. R equal to the number of successful tests in a series of N independent tests, takes on whole-number values $0, 1, 2, \dots, N$ with probabilities:

$$(2) \quad p^N(k) = C_N^k p^k (1-p)^{N-k}.$$

Distribution function $F^R(r, N, p)$ of binomial r.v. R will be written as

$$(3) \quad F^R(r, N, p) = \sum_{k=0}^r p^N(k).$$

In order to estimate the GPL (t_γ) it would be quite natural to use the conventional mean time to failure estimate constructed for an exponential distribution as the estimate of parameter T_0 [1, 5]:

$$T_0^* = \frac{S(R, N, \tau, t_i)}{r}, \text{ if } r > 0.$$

However, thus obtained estimate $t_{\gamma^*} = -T_0^* \ln(\gamma)$ has significant disadvantages, i.e.:

- the estimate is biased [1],

Methods of research and results

The aim of this paper is to find such estimate of GPL (hereinafter referred to as t_γ) that would be simple and more efficient as compared to the conventional one and not significantly inferior to the efficient estimate $t_{\gamma^{est}}$, if such exists, in terms of proximity to t_γ in case a binomial test plan is used.

The Aim of the paper

In order to solve the above problem, it suffices to find an unbiased efficient estimate ($t_{\gamma^{est}}$), if such exists in the class of consistent biased estimates. (The class of consistent estimates that includes all estimates generated by the method of substitution, inclusive of the maximum likelihood method, contains estimates with any bias, including those with a fixed one, in the form of function of parameter or constant [3]). In some cases, the generated unbiased efficient estimates are quite lengthy and have a complex calculation algorithm [4]. They are also not always sufficiently efficient in the class of all biased estimates and not always have a considerable advantage over simple yet biased estimates in terms of proximity to the estimated value [6].

Let us consider the class of estimates that can be presented as $t_\gamma = -T_0 \ln(\gamma)$, where T_0 is the estimate of MTF for a binomial test plan.

In order to find the efficient estimate we will use integral characteristics [6]. Similarly to [6], let us construct a functional (hereinafter referred to as $A(t_\gamma)$) based on the total squared deviation of the expected estimate t_γ from t_i for all possible values t_p, T_0, γ, N and τ :

$$(4) \quad A(t_\gamma(R, N, \tau, t_i)) = \sum_{t_j=1}^{\infty} \frac{1}{10} \sum_{N=10}^{\infty} \int_0^{T_0} \left\{ E t_\gamma(R, N, \tau, t_i) - \left\{ \frac{1}{2} \int_0^{T_0} \partial T_0, \right\} \right\} (-(-T_0 \ln(\gamma))) dt_j =$$

$E t_\gamma(R, N, \tau, t_i) = \sum_{k=0}^N p^N(k) t_\gamma(k, \tau, t_i) =$

An efficient estimate of GPL t_γ must have the minimal value of functional of $A(t_\gamma)$.

Let us take $-\ln(\gamma)$ outside the integral sign, then the formula will become as follows:

$$(5) \quad A(t_\gamma) = \ln^2(\gamma) V(T_0^*),$$

Estimation of the gamma-percentile life for the binomial test plan

Viktor S. Mikhailov, D.I. Mendeleev Central Research and Design Institute of Chemistry and Mechanics, Russian Federation, Moscow



Viktor S. Mikhailov

Abstract. In today's industry of highly dependable, unique, complex products, it is a common-place situation when it is required to obtain an estimate of gamma-percentile storing life (GPL) or gamma-percentile time to failure (GPTF) (hereinafter referred to as GPL, meaning GPL or GPTF respectively) based on tests that did not produce any failures. Normally, a test plan is classified as binomial tests or tests with limited time and recovery. GPTF is understood as the operation time during which no failure occurs with the probability expressed as percentage. Similarly, GPL is understood as the total schedule time of product storage during and after which the product is able to perform the required function with the probability expressed as percentage. The **Aim** of this paper is to find such estimate of GPL that would be simple and more efficient as compared to the conventional one and not significantly inferior to the efficient estimate, if such exists, in terms of proximity to the GPL estimate in case a binomial test plan is used. **Methods of research.** The research of efficient estimates is based on the integrative approach that uses the construction of the choice rule (criterion) of efficient estimate specified on the vertical sum of biases of estimates selected out of a certain set based on the function of the distribution law parameter. **Conclusions.** The obtained estimate of GPL is simple and more efficient as compared to the conventional one and not significantly inferior to the efficient estimate, if such exists, in terms of proximity to the GPL estimate in case a binomial test plan is used. The obtained estimate of GPL has significant advantages, i.e. the estimate is efficient within a sufficiently wide range of estimates, it allows obtaining a value based on the results of tests that did not produce any failures. The obtained estimate of GPL is recommended for failure-free tests conducted using a binomial plan.

Keywords: gamma-percentile storing life, gamma-percentile time to failure, exponential distribution, test plan, point estimation.

For citation: Mikhailov VS. Estimation of the gamma-percentile life for the binomial test plan. Dependability 2019; 2: 18-21. DOI: 10.21683/1729-2646-2019-19-2-18-21

- [9] Smith C.L., Wood S.T., Galyean W.J., Schroeder J.A., Sattison M.B. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8: Technical Reference. NUREG/CR-7039 INL/EXT-09-17009; Vol. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission; 2011.
- [10] O'Connor A.N. A general cause based methodology for analysis of dependent failures in system risk and reliability assessments; 2013.
- [11] O'Connor A.N. A general cause based methodology for analysis of dependent failures in system risk and reliability assessments; 2013.

About the authors

Alexander V. Antonov, Doctor of Engineering, Professor, Chief Expert of the International Training Center, Rosatom Technical Academy, Russian Federation, Moscow, e-mail: AVAntonov@rosatomtech.ru

Valery A. Chepurko, Candidate of Physics and Mathematics, Associate Professor, Chief Specialist of Division for Justifying Calculations of Design Solutions, JSC RASU, Russian Federation, Moscow, e-mail: VAChepurko@rasu.ru

Alexey N. Cherniaev, Candidate of Engineering, Deputy Technical Director, Director of Design Department, JSC RASU, Russian Federation, Moscow, e-mail: AINCherniaev@rasu.ru

Received on: 06.02.2019

- [2] GOST R IEC 62340-2011. Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure. Moscow: Standartinform; 2012 [in Russian].
- [3] Antonov A.V., Galivets E.Yu., Chepurko V.A., Cherniaev A.N. Fault tree analysis in the R programming environment. Dependability 2018;18(1):4-13. DOI: 10.21683/1729-2646-2018-18-1-4-13.
- [4] Antonov A.V., Galivets E.Yu., Chepurko V.A., Cherniaev A.N. Fault tree analysis in the R programming environment. Accounting for common cause failures. Dependability 2018; 18(3):3-9. DOI: 10.21683/1729-2646-2018-18-3-3-9.
- [5] Pereguda A.I., Pereguda A.A., Timashev D.A. The mathematical model of computer networks' reliability. Dependability 2013;(4):31-43. DOI: 10.21683/1729-2646-2013-0-4-18-43.
- [6] Alpeev A.S. Dependability of control systems software and safety of nuclear power plants. Dependability 2015;(4):78-80. DOI: 10.21683/1729-2646-2015-0-4-75-80.
- [7] Mosleh A., Rasmussen D.M., Marshall F.M. Procedures Guidelines in Modeling Common Cause Failures in Probabilistic Risk Assessment. NUREG/CR-5485. University of Maryland; 1998.
- [8] O'Connor A.N. A General Cause Based Methodology for Analysis of Dependent Failures in System Risk and Reliability Assessments. University of Maryland; 2013, <<http://hdl.handle.net/1903/14285>> [accessed 09.04.2019].

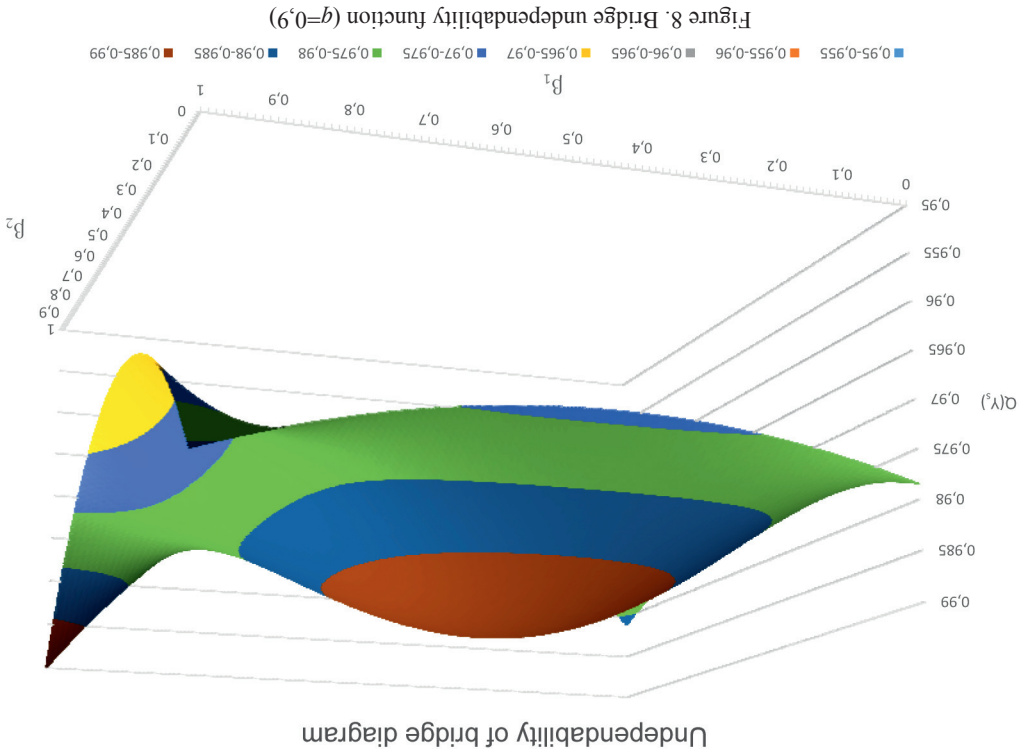
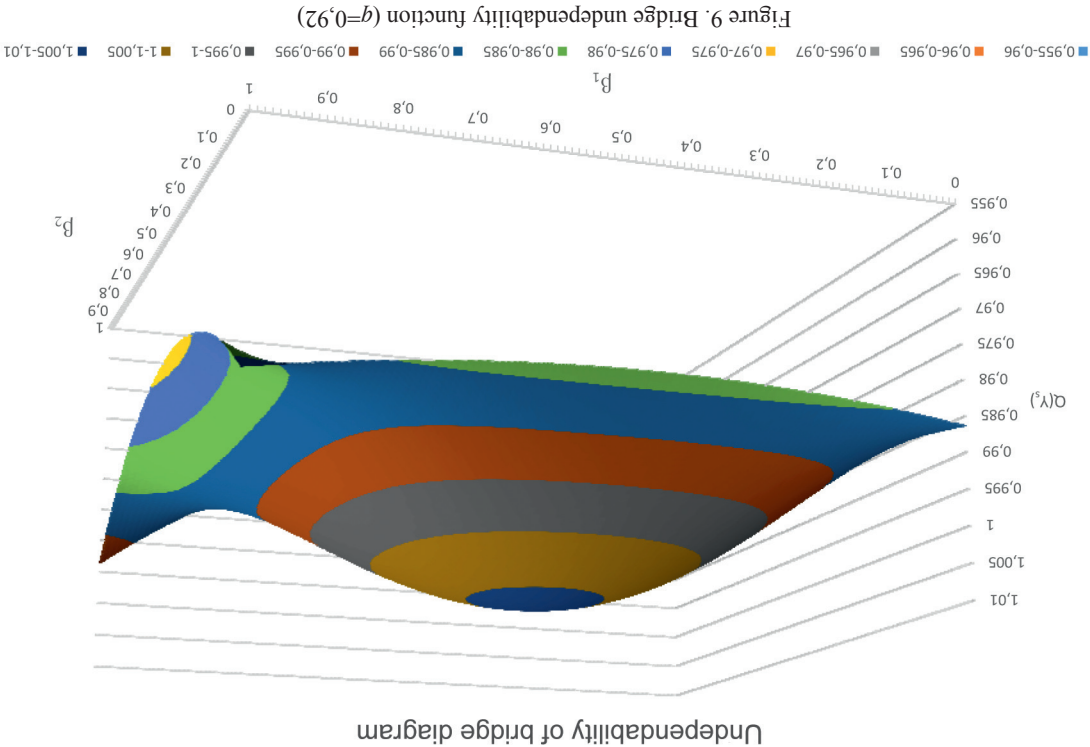
Conclusion

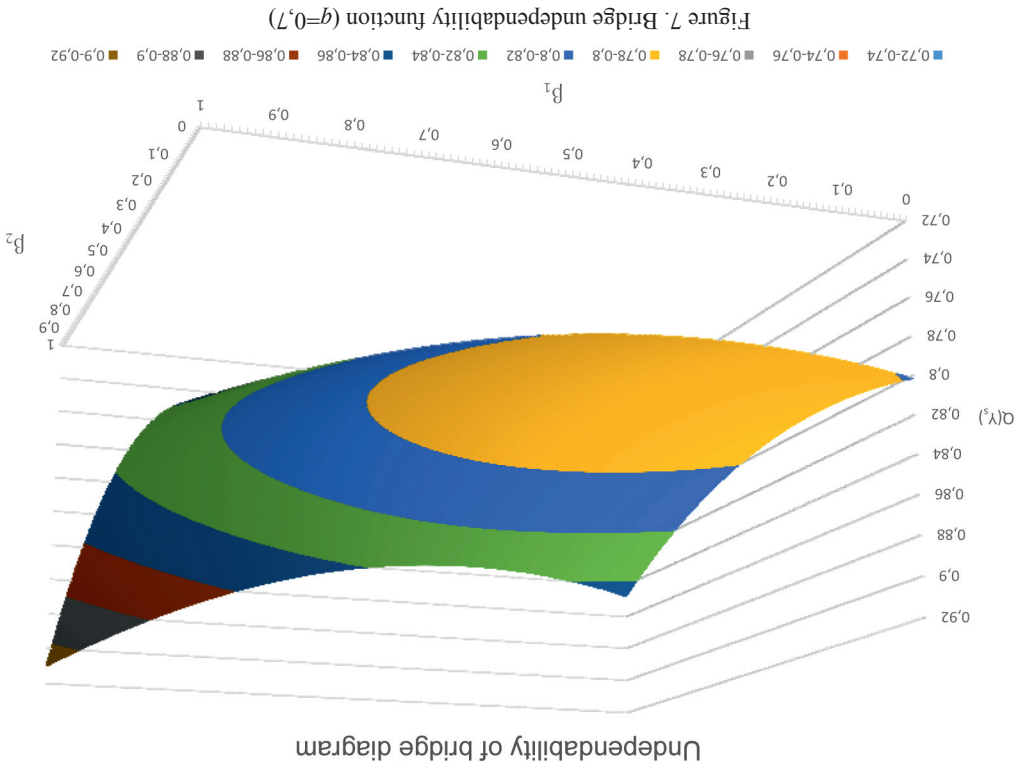
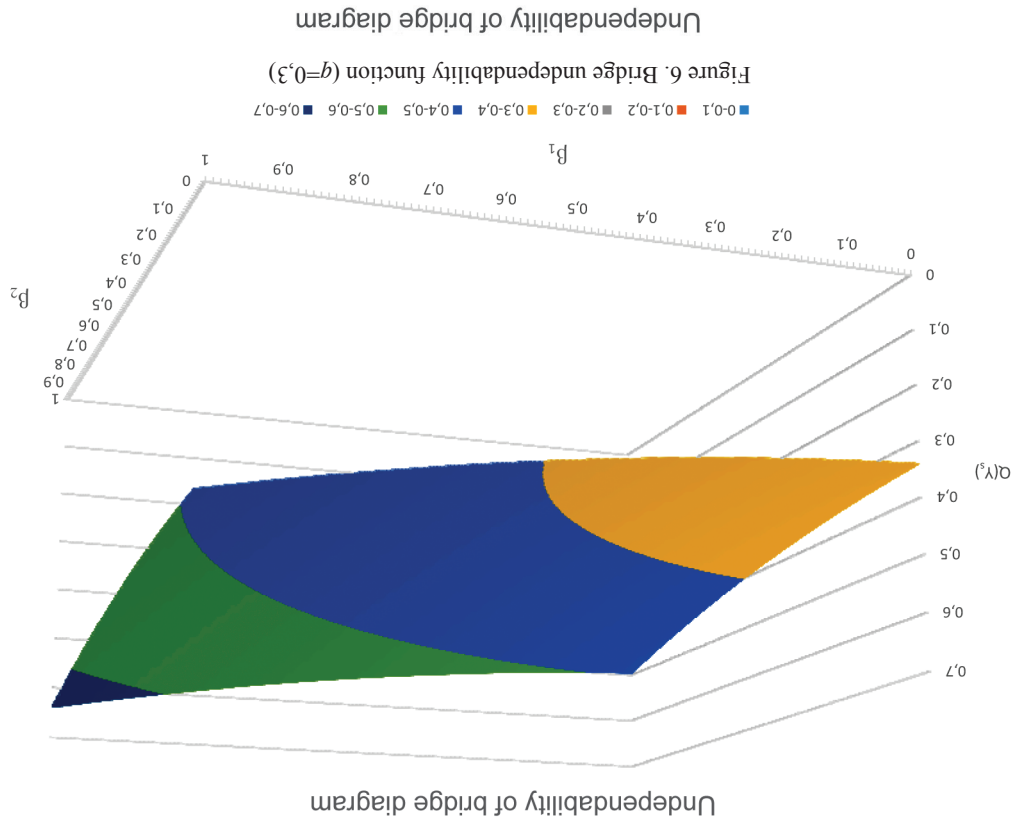
The paper conducts a mathematical research of the beta-factor model of accounting for CCF. The research covered three dependability diagrams: parallel, serial and bridge. The two latter diagrams reveal the problem of unacceptable beta factor model parameter values in case of high dependability of component elements. For all three dependability diagrams it is shown that increasing beta factor

References

[1] GOST R IEC 61226-2011. Nuclear power plants. Instrumentation and control systems important for safety. Classification of instrumentation and control functions. Moscow: Standartinform, 2011 [in Russian].

model parameters do not necessarily cause the growth of undependability.





case of low β_a, β_b or an increase of undependability of the system as a whole.

If $q \in (\approx 0.91, 1)$ the undependability function has, as previously, a complex dependence: four local boundary minimums and one maximum (figure 9). In the vicinity of point $(0,0)$ the undependability decreases if each parameter increases. When the minimum point has been reached, further increase of CCF parameters causes growing undependability. Further behaviour depends on the specific parameter values. If $\beta_a = \beta_b = 1$, maximum undependability is reached. It must be noted that there is a range of unacceptable values of parameters β_a, β_b under which the systems' undependability assumes a value higher than one. Thus, a serial structure does not necessarily have unacceptable beta-factor model parameter values.

Let β_a and β_b be parameters of the beta-factor model in the respective groups. In this case the following events are possible: i_1 is independent failure of the 1-st element, i_2 is independent failure of the 2-nd element, C_a is dependent CCF of the 1-st element and 2-nd element (group a). Similarly, the events from the second CCF group can be shown in this same sample space: i_3 is independent failure of the 3-rd element, i_4 is independent failure of the 4-th element, C_b is dependent CCF of the 3-rd element and 4-th element (group b).

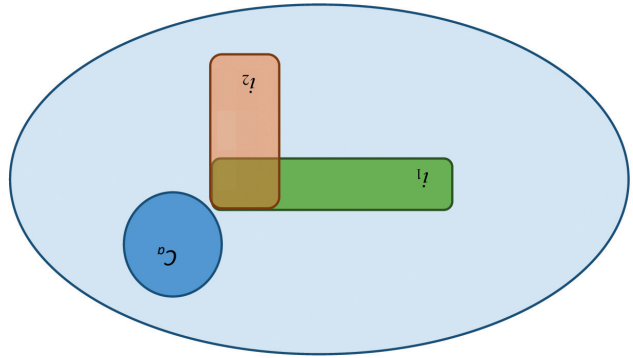


Figure 5. Events in case of CCF

Figure 5 shows possible mutual location of the events in a group. Importantly, antithetic (mutually exclusive) pairs of events will be the following: i_1 and C_a , i_2 and C_b , i_4 and C_b . Let us indicate the event x_k , the k -th element is operable, $k = 1, \dots, 5$. Then,

$$\overline{x_1} = i_1 \vee C_a, \overline{x_2} = i_2 \vee C_a, \overline{x_3} = i_3 \vee C_b, \overline{x_4} = i_4 \vee C_b.$$

The logic function of inoperability will be as follows

$$(10) \quad \overline{X_s} = [x_3 A] \vee [x_5 B],$$

where $A = (\overline{x_1} \overline{x_2}) \vee (\overline{x_3} \overline{x_4})$ and $B = (\overline{x_2} \vee \overline{x_4})(\overline{x_1} \vee \overline{x_3})$.

Let all the elements be equally dependable and the probabilities of their total cause failures be equal to q . In this case the undependability of the bridge regardless of CCF will be equal to:

$$(11) \quad \tilde{Q}(X_s) = q^3(2-q)^2(1-q)^2 + q^2(1-q)^2(2-q^2) = 2q^5 - 5q^4 + 2q^3 + 2q^2.$$

Let us substitute the events A and B involved in (1) and containing $\overline{x_1}, \overline{x_2}, \overline{x_3}$ and $\overline{x_4}$ with independent and CCF events:

$$A = (\overline{x_1} \overline{x_2}) \vee (\overline{x_3} \overline{x_4}) = (i_1 \vee i_2 \vee C_a) \vee (i_3 \vee i_4 \vee C_b).$$

$$B = (\overline{x_2} \vee \overline{x_4})(\overline{x_1} \vee \overline{x_3}) = (i_1 \vee i_3)(i_2 \vee i_4) \vee C_a \vee C_b.$$

Let us identify the probabilities of such events:

$$(12) \quad P(A) = f(\beta_a, q) + f(\beta_b, q) - f(\beta_a, q)f(\beta_b, q),$$

$$\text{where } f(\beta, q) = (1-\beta)q^2 + \beta q.$$

In order to calculate the probability of event B , let us use the addition theorem that, in the case of antithetic events of a CCF group will result in the following:

$$P(B) = P((i_1 \vee i_3)(i_2 \vee i_4)) + P(C_a) + P(C_b) - P(i_1 i_2 C_b) - P(i_3 i_4 C_a) - P(C_a C_b) = g^2(\beta_a, \beta_b, q) + \beta_a q + \beta_b q - (1-\beta_a)^2 \beta_b q^3 - (1-\beta_b)^2 \beta_a q^3 - \beta_a \beta_b q^2,$$

$$\text{where } g(\beta_a, \beta_b, q) = (1-\beta_a)q + (1-\beta_b)q - (1-\beta_a)(1-\beta_b)q^2.$$

Upon the substitution of the obtained results and simplification, we will obtain the bridge's undependability subject to CCF:

$$(13) \quad \tilde{Q}(X_s) = c_5 q^5 + c_4 q^4 + c_3 q^3 + c_2 q^2 + c_1 q,$$

where the polynomial coefficients are defined by the following formulas:

$$c_5 = 2(1-\beta_a)^2(1-\beta_b)^2,$$

$$c_4 = (1-\beta_a)(1-\beta_b)(-5+3\beta_a+3\beta_b-\beta_a\beta_b),$$

$$c_3 = 2-3\beta_a-3\beta_b+\beta_a\beta_b(6-\beta_a-\beta_b),$$

$$c_2 = (1-\beta_a)^2 + (1-\beta_b)^2 - \beta_a\beta_b,$$

$$c_1 = \beta_a + \beta_b.$$

As the result of the conducted research of function (13) the following dependences were identified.

If $q \leq 0.5$ undependability $\tilde{Q}(X_s)$ classically monotonically increases per each parameter β_a , β_b (figure 6). I.e. when calculating a bridge with highly dependable elements no unexpected effects were identified.

If $q \in (0.5, \sim 0.85)$ the undependability function has a global minimum. In the vicinity of point (0,0) the unpendability decreases if each parameter increases (figure 7). When the minimum point has been reached, further increase of CCF parameters causes growing unpendability. If $\beta_a = \beta_b = 1$ maximum unpendability is reached. Thus, in case of average unpendability of the bridge's component elements accounting for CCF may cause a reduction of unpendability of the system as a whole. The value 0.85 was

obtained visually, accurate estimation requires an analytical study of (13).

If $q \in (\sim 0.85, \sim 0.91)$ the unpendability function has a complex dependence: four local boundary minimums and one maximum (figure 8). In the vicinity of point (0,0) the unpendability decreases if each parameter increases.

When the minimum point has been reached, further increase of CCF parameters causes growing unpendability. Further behaviour depends on the specific parameter values. If $\beta_a = \beta_b = 1$ maximum unpendability is reached. In case of high unpendability of the bridge's component elements accounting for CCF may cause a reduction (in

$$1 - (1 - \beta)q^n \geq \beta q.$$

Thus, for instance, if $n = 2, 3, 4, 5, 10, 50, 100$ the range of acceptable values of probability q will be the area beneath the curve in figure 3.

Let us, as previously, take, for example, $\beta = 0,1$, $q = 0,9$, $n = 2$. The probabilities of failure accounting and not accounting for CCF will be equal to $1 - (1 - \beta)q^n + \beta q = 1,0539$ and $1 - (1 - q)^n = 0,99$ respectively.

CCF in bridge diagram

Let us research the effect of beta factor model parameters in a bridge diagram. The structure of a bridge diagram is shown in figure 4. Let us assume that there are two different common causes of failure of several bridge elements at once:

- common cause a that may cause simultaneous failure of elements 1 and 2,
- common cause b that causes simultaneous failure of elements 3 and 4.

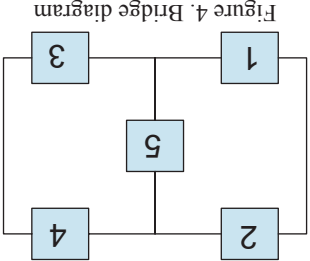


Figure 4. Bridge diagram

$$q > 1 - \exp\left(-\frac{n}{\ln n}\right).$$

Thus, if $q \in \left[0, 1 - \exp\left(-\frac{n}{\ln n}\right)\right]$, derivative (7) for any

$$\left.\frac{\partial \tilde{Q}(Y)}{\partial \beta}\right|_{\beta=1} = q - nq < 0$$

values of β will be negative, as

if $n \geq 2$ and the critical point is outside the interval $[0, 1]$. Therefore, increasing β will cause, as expected, decreasing undependability.

If $q > \exp\left(-\frac{n}{\ln n}\right)$, there will be a point of extremum

(8), and, as derivative (7) is negative for $\beta = 1$, the critical point will be the maximum point. Then, $\left.\frac{\partial \tilde{Q}(Y)}{\partial \beta}\right|_{\beta=0} > 0$ and

the undependability function will increase with respect to parameter β .

Unlike in the parallel structure, in the serial structure for each β there are limit values of the probability of failure due to any cause for each element, exceeding which may bring about unacceptable values of probability of system failure. In order to identify such values, the following equation must be solved:

$$1 - (1 - \beta)q^n - \beta q = 0. \quad (9)$$

An unacceptably high value of probability of failure is directly associated with the assumptions of the beta-factor model. In terms of logic algebra, out of the occurrence of event C follows that no independent cause failures took place, i.e. $C \Rightarrow i_1 \vee i_2 \vee \dots \vee i_n$. In this case

$$P(i_1 \vee i_2 \vee \dots \vee i_n) \geq P(C), \text{ i.e.}$$

Thus, elements 1 and 2 form the first CCF group, while elements 3 and 4 form the second one. Evidently, those two groups do not contain identical elements, although, in general, one element can simultaneously be part of several CCF groups. Such situation is to be considered in the next paper.

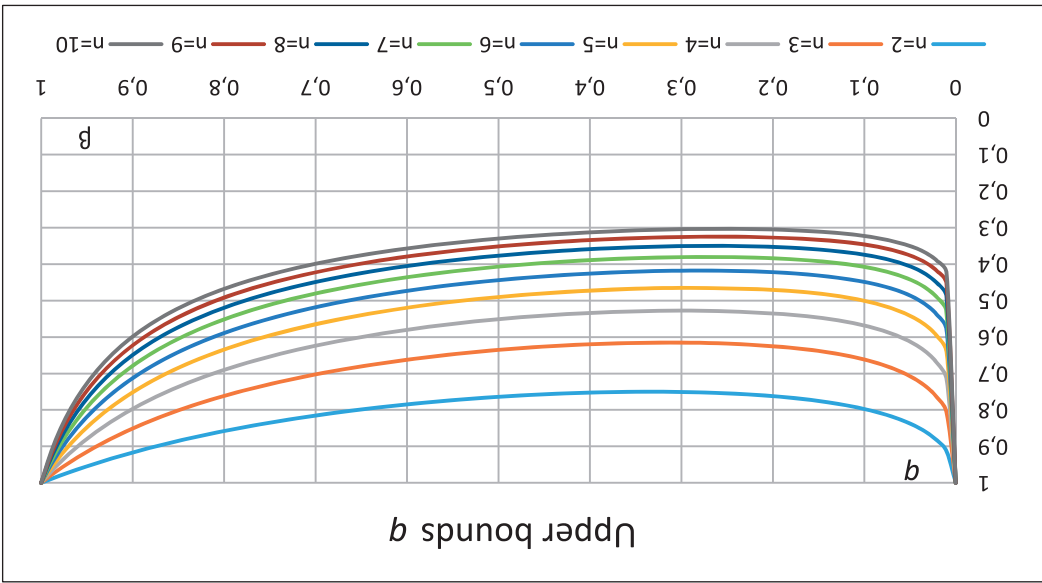


Figure 3. Acceptable values of q

CCF in serial structures

In this section, let us analyze the dependability of the serial (primary) structure in terms of dependability subject to CCF. Let the system consist of n serial equally dependable elements with the probability of failure q each. Not accounting for CCF, the system's PNF will be equal to $P(X_s) = (1 - q)^n$. The logic function of operability subject to CCF will be as follows:

$$(5), \text{ and, as derivative for } \beta=1, \text{ the critical point will be the minimum point. Then, } \left. \frac{\partial \bar{Q}(X_s)}{\partial \beta} \right|_{\beta=0} > 0 \text{ and the undependability function will paradoxically decrease with respect to parameter } \beta. \text{ That is the complete proof of the behaviour of the undependability function.}$$

If the probability for any reason q is lower than boundary $q_{\beta,n}$, accounting for CCF will cause increased dependability of a serial system. If $q = q_{\beta,n}$, accounting for CCF will not affect the dependability of the system. And finally, if $q > q_{\beta,n}$, accounting for CCF will cause decreased dependability of the system. Let us, as previously, take, for example, $\beta = \frac{1}{3}$, $q = \frac{4}{7}$, $n = 2$. The probabilities of failure accounting and not accounting for CCF will be equal to $\frac{240}{256}$ and $\frac{16}{256}$ respectively.

As above, let us try to explain the change of the behaviour of the dependability (or undependability) function under various parameter values by conducting a qualitative analysis addressing, among other things, the derivatives of q and β . The derivative of function $\bar{Q}(X_s)$ of q will be defined by the formula:

$$\frac{\partial \bar{Q}(X_s)}{\partial q} = n(1 - \beta)(1 - (1 - \beta)q)^{n-1} + \beta > 0 \text{ if } \beta \in (0, 1).$$

Growing undependability of the element causes growing undependability of a parallel system as a whole. Derivative per another parameter

$$(7) \quad \frac{\partial \bar{Q}(X_s)}{\partial \beta} = -nq(1 - (1 - \beta)q)^{n-1} + q.$$

Let us analyze (7). The derivative is equal to 0 in the critical point

$$(8) \quad \beta_{crit} = 1 - \frac{1}{1 - \frac{b}{n} \left(\frac{1}{1 - \frac{1}{n}} \right) - \exp\left(-\frac{b}{n-1}\right)}.$$

The critical point is attainable if $\beta_{crit} \in (0, 1)$. Condition $\beta_{crit} < 1$ is obviously fulfilled, while $\beta_{crit} > 0$ occurs when and only when

$$(6) \quad (1 - (1 - \beta)q)^n - \beta q = (1 - q)^n.$$

Figure 2 shows dependence graphs of function $q_{\beta,n}$ of parameter β under various n . The solution of equation (6) was obtained by means of the numerical method of segment bisection.

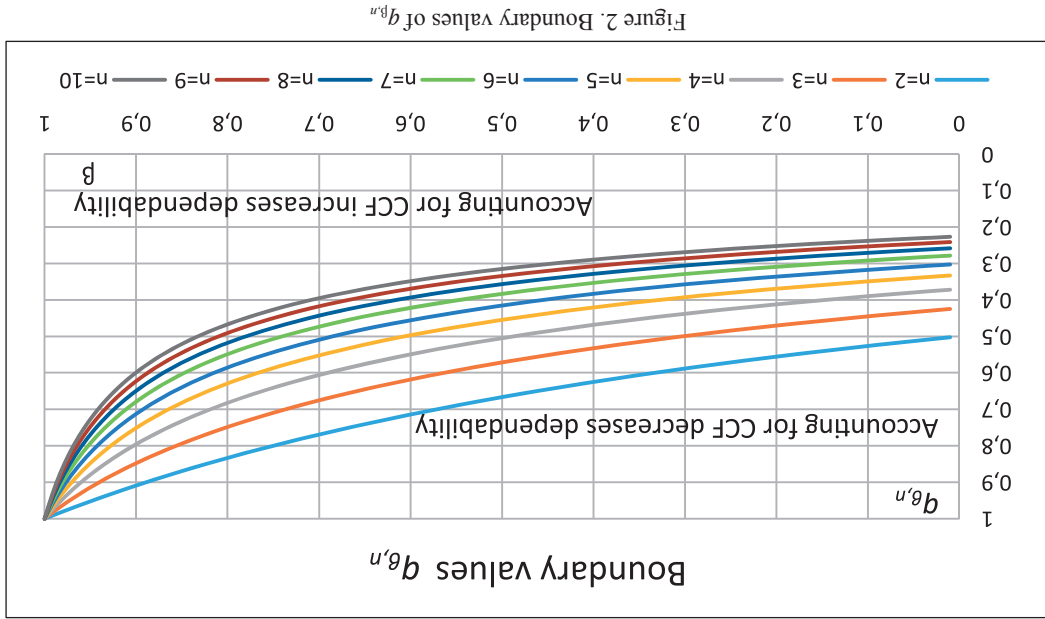
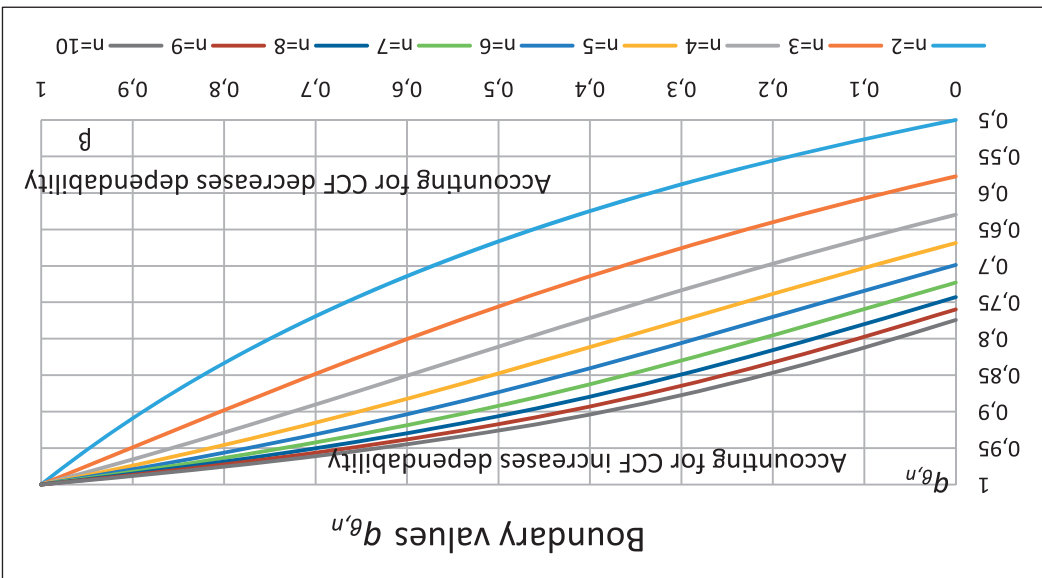


Figure 2. Boundary values of $q_{\beta,n}$

Figure 1. Boundary values of $q_{\beta,n}$

analyzing, among other things, the derivatives of q and β . The derivative of function $\tilde{Q}(X_s)$ of q will be defined by the formula:

$$\frac{\partial \tilde{Q}(X_s)}{\partial q} = nq^{n-1}(1-\beta)^n + \beta > 0 \text{ if } \beta \in (0,1),$$

i.e. growing unependability of the element causes growing unependability of a parallel system as a whole.

Now, let us take a derivative of another parameter

$$\frac{\partial \tilde{Q}(X_s)}{\partial \beta} = -nq^n(1-\beta)^{n-1} + q. \quad (4)$$

Let us analyze (4). The derivative is equal to 0 in the critical point

$$\beta_{crit.} = 1 - \frac{1}{n} \left(\frac{q}{1-\beta} \right)^{\frac{1}{n-1}} = 1 - \frac{1}{n} \exp \left(-\frac{n-1}{n} \right). \quad (5)$$

The critical point is attainable if $\beta_{crit.} \in (0,1)$. Condition $\beta_{crit.} > 0$ occurs when and only when

$$q > \exp \left(-\frac{n-1}{n} \right).$$

Let us note that

$$\lim_{\beta \rightarrow 0+} q_{\beta,n} = \lim_{\beta \rightarrow 0+} \left(\frac{1 - (1-\beta)^n}{\beta} \right)^{\frac{1}{n-1}} = \exp \left(-\frac{n-1}{n} \right).$$

Thus, if $q \in \left(0, \exp \left(-\frac{n-1}{n} \right) \right)$ [derivative (4) for any values of β will be positive, since $\frac{\partial \tilde{Q}(X_s)}{\partial \beta} > 0$ and the critical point is outside the interval $[0,1]$. Therefore, increasing β will cause, as expected, increasing unependability.

$$(1-\beta)^n + \beta < 1.$$

In order to get this effect clarified, let us examine an extreme situation. Let us assume that $q=1$, i.e. the probability of total cause failure of one element equals 1. In this case the probability of failure not accounting for CCF will be equal to 1 as well. If $n \geq 2$ and $\beta \in (0,1)$, accounting for CCF will have the following result

And finally, if $q > q_{\beta,n}$, accounting for CCF will, surprisingly, cause increased dependability of the system. Let us take, for example, $\beta=1/4$, $q=3/4$, $n=2$. The probabilities of failure accounting and not accounting for CCF will be equal to $\frac{129}{256} + \beta q = \frac{129}{256} + \frac{3}{4} \cdot \frac{1}{4} = \frac{16}{9}$ and $q^n = \frac{9}{16}$ respectively.

The probabilities of one independent failure and CCF of any element will be respectively equal to $(1-\beta)n\beta$. It turns out that the unitary probability of failure was decomposed by the beta-factor model into two components conditioned by the cause of failure. If the system consisted of one element, the probability would not decrease: $(1-\beta)+\beta=1$. In case of the redundant structure the probability of failure decreased due to the "rigidity" of the assumptions of the beta-factor model. The failure of j -th element is a disjunction of antithetic events $i_j \vee C$. System failure is a conjunction of $A_{n,i_j}^{j=1} (i_j \vee C)$. If an event of type $i_1 \vee i_2 \vee \dots \vee i_n \vee C_{3,4,\dots,n-1}$ (1-st, 2-nd and n -th elements failed due to an independent cause, the others failed due to the common cause) and all possible combinatorial enumerations of such events that are present in other models of accounting for CCF (alpha-factor model, Greek letters model, etc.) were possible, the probability would probably be higher. However, in the beta-factor model such events are impossible as, for instance, event $C_{3,4,\dots,n-1}$ is impossible. On the other hand, the change of behaviour of the dependability (or unependability) function under various parameter values can be explained quite simply by conducting a qualitative analysis of the unependability function,

Introduction

Today's dependability analysis of complex systems often includes taking into consideration possible common cause failures (CCFs). CCF is a failure of two or more structures, systems or components due to a single specific event or single specific cause [1]. A simultaneous failure of two or more structures, systems or components is caused by certain shortcomings associated with the design or manufacture, errors of operation or maintenance that manifest themselves as the result of natural effects, operational processes in a nuclear powerplant, human actions or internal events within the control and supervision system [2]. As an example, we can mention the blocking of a number of safety systems as the result of a wrong decision taken by the personnel of the Chernobyl NPP. The existing CCF classification includes failures caused by internal or external effects, failures caused by personnel's errors, general failures due to commonality of design or operating conditions.

There is a number of probabilistic methods of accounting for CCF, i.e. the alpha-factor model, Greek letter model, beta-factor model, etc. The beta-factor model is one of the simplest ones. It considers either single independent failures of a group's elements that have a common cause (CCF groups), or simultaneous failure of all elements of a CCF group. The other models consider the possible failure of random subgroups of a CCF group. In this case, depending on the specific model, in a certain manner, the vector is found of the parameters corresponding with the probability of CCF of a group of the specified size. As the beta-factor model involves the CCF of the whole group, it contains the single parameter β .

The aim of this paper is to investigate how accounting for CCF using the beta-factor model affects the probability of failure of various structure diagrams. Aside from finding the dependence between the probability of system failure and the model parameter β , in each case the probabilities of failure are analyzed to determine the possible limitations of the model.

CCF in parallel structures

Let us analyze the dependability of the parallel (backup) structure in terms of dependability subject to CCF. Let the system consist of n parallel equally dependable elements with the probability of failure q each. Obviously, not accounting for CCF, the system's probability of failure will be equal to q^n .

Let us assume that all n element can fail due to one common cause. In this case the following events will be possible: i_j , independent failure of the j -th element, C , dependent CCF of all elements.

According to the assumptions of the beta-factor model, a failure of any element of the group may occur due to an independent or common cause identical for all the elements, i.e. events i_j and C will be antithetic. The probabilities of

such events will be proportional to q , i.e. the probability of total cause failure of an element.

$$P(C) = \beta q, P(i_j) = (1 - \beta)q, j = 1, \dots, n. \quad (1)$$

Non-negative proportionality factor β depends on many factors, such as system structure, redundancy method, operating conditions, etc. Normally, this coefficient is quite low and technical systems contain highly dependable elements, i.e. the probability of failure q is also low. In this context, the use of the beta-factor model normally yields paradoxical or even impossible results. In case of relatively high values of β and q it is quite possible to attain them.

The logic function of operability subject to CCF will be as follows:

$$X_s = (i_1 \vee i_2 \vee \dots \vee i_n) \vee C,$$

the probability of failure $\bar{Q}(X_s)$ will be defined by the formula:

$$\bar{Q}(X_s) = 1 - P(X_s) =$$

$$= P(i_1 \vee i_2 \vee \dots \vee i_n) + P(C) = ((1 - \beta)q)^n + \beta q. \quad (2)$$

Let us examine (2) in order to identify possible problems with the calculations.

Whereas $0 \leq (1 - \beta)q \leq 1$, then $((1 - \beta)q)^n \leq (1 - \beta)q$. Therefore, the probability of failure (2) will not exceed one. I.e. the normalization requirement for the parallel structure will be fulfilled.

Let us verify the commonly held opinion that accounting for CCF in redundant structures causes increasing probability of failure of the system. For that purpose, let us identify the parameter values of the CCF model that enable a relative growth of dependability of a parallel structure system when accounting for CCF. Obviously, the following condition is to be fulfilled in order to enable a growth of dependability:

$$\bar{Q}(X_s) = ((1 - \beta)q)^n + \beta q < q^n.$$

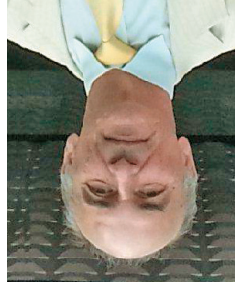
After a simplification we obtain the following condition:

$$(3) \quad \beta > q^{\frac{1}{n-1}} = q_{\beta, n}.$$

If (3) is fulfilled, the dependability of a parallel structure calculated subject to CCF will be higher than the dependability calculated otherwise. Figure 1 shows the dependence graphs of function $q_{\beta, n}$ of parameter β under various n . Let us assume that parameter $\beta > 0$. Then, if the total cause probability q is lower than boundary $q_{\beta, n}$, accounting for CCF will cause decreased dependability of a redundant system. This effect is what is normally expected as the natural reaction of the beta-factor model to accounting for CCF. If $q = q_{\beta, n}$, accounting for CCF will not affect the dependability of the

Study of the beta-factor model application for common cause failure modeling

Alexander V. Antonov, Rosatom Technical Academy, Russian Federation, Obninsk
Valery A. Chepurko, JSC RASU, Russian Federation, Moscow
Alexey N. Cherniaev, JSC RASU, Russian Federation, Moscow



Alexander V. Antonov



Valery A. Chepurko



Alexey N. Cherniaev

Abstract. Aim. Common cause failures (CCFs) are dependent failures of groups of certain elements that occur simultaneously or within a short period of time (i.e. almost simultaneously) due to a single common cause (e.g. a sudden change of climatic operating conditions, flooding of premises, etc.). A dependent failure is a multiple failure of several elements of a system, whose probability cannot be expressed as a simple product of the probabilities of unconditional failures of individual elements. CCA probabilities calculation uses a number of common models, i.e. the Greek letter model, alpha, beta factor and their variants. The beta-factor model is the most simple in terms of simulation of dependent failures and further dependability calculation. Other models, when used in simulation, involve combinatorial enumeration of dependent events in a group of n events that becomes labour-intensive if the number n is high. For the selected structure diagrams of dependability, the paper analyzes the calculation method of system failure probability with CCF taken into account for the beta-factor model. The Aim of the paper is to thoroughly analyze the beta-factor method for three structure diagrams of dependability, research the effects of the model parameters on the final result, find the limitations of beta-factor model applicability. **Methods.** The calculations were performed using numerical methods of solution of equations, analytical methods of function studies. **Conclusions.** The paper features an in-depth study of the method of undependability calculation for three structure diagrams that accounts for CCF and uses the beta-factor model. In the first example, for the selected structure diagram out of n parallel elements with identical dependability, it is analytically shown that accounting for CCF does not necessarily cause increased undependability. In the second example of primary junction of n elements with identical dependability, it is shown that accounting for CCF subject to parameter values both increased and decreased undependability. A number of beta factor model parameter values was identified that cause unacceptable values of system failure probability. These sets of values correspond to relatively high model parameter values and are hardly practically attainable as part of engineering of real systems with highly dependable components. In the third example, the conventional bridge diagram with two groups of CCFs is considered. The complex ambivalent effect of beta factor model parameters on the probability of failure is shown. As in the second example, limitations of the applicability of the beta-factor model are identified.

Keywords: common cause failure, total cause failure, independent failures, dependent failures, antithetic events, beta factor, undependability function.

For citation: Antonov AV, Chepurko VA, Cherniaev AN. Research of the beta-factor model of accounting for common cause failures. *Dependability* 2019;2: 9-17. DOI: 10.21683/1729-2646-2019-19-2-9-17

Nikolay I. Sidniyaev, Doctor of Engineering, Professor, Head of Department, Bauman Moscow State Technical University, Russian Federation, Moscow, e-mail: Sidn_ni@mail.ru
Yulia I. Butenko, Candidate of Engineering, Associate Professor, Bauman Moscow State Technical University, Russian Federation, Moscow, e-mail: iuliabutenko2015@yandex.ru

Received on: 17.12.2018

and Electromechanical Systems, Russian Federation, Moscow, e-mail: vniem@orc.ru, vniem@vniem.ru
Ruslan N. Barbul, Senior Researcher, Deputy Director General for Quality and Dependability, A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control and Electromechanical Systems, Russian Federation, Moscow, e-mail: vniem@orc.ru, vniem@vniem.ru

- [8] Sidniyev N.I. Obzor i issledovanie fiziki otkazov dlia osenki pokazateley nadezhnosti radioelektronnykh priborov sovremennykh RLS [Overview and research of physics of failure for the estimation of the dependability indicators of today's radar electronics]. Physical Bases of Instrumentation 2017;2(23):4-52 [in Russian].
- [9] Barlow R., Proschan F. Mathematical theory of reliability. Moscow: Sovetskoye radio; 1969.
- [10] RD 50-690-89. Metodicheskoe ukazaniye. Nadezhnost' v tekhnike. Metody osenki pokazateley nadezhnosti po eksperimentalnykh dannym [Guidelines. Dependability of technology. Methods of estimation of dependability indicators based on experimental data]. Moscow: State committee of the USSR for products quality management and standards; 1990 [in Russian].
- [11] Sidniyev N.I., Makridenko L.A., Gecha V.Ya., Onufriyev V.N. Faktory kosmicheskoy pogody, vliyayushchie na bortovye elementy nizkoorbitalnykh kosmicheskikh apparatov [Factors of space weather affecting the airborne devices of low-orbiting spacecraft]. In: Electromechanical matters. VNIIEM studies. Proceedings of the Fourth International Science and Technology Conference Topical Issues of the Design of Space-Based Earth Remote Sensing Systems. Moscow: VNIIEM Corporation; 2016. p. 90-100 [in Russian].
- [12] Pokhabov Yu.P. What should mean dependability calculation of unique highly vital systems with regards to single-use mechanisms of spacecraft. Dependability 2018;18(4):28-35.
- [13] Antonov S.G., Klimov S.M. Method for risk evaluation of functional instability of hardware and software systems under external information technology interference. Dependability 2017;17(1):32-39.
- [14] Sidniyev N.I., Gecha V.Ya., Barbul R.N. O sovremennykh podkhodakh razvitiya teorii effektivnosti kosmicheskikh sistem [On the modern approaches of the space systems efficiency theory]. In: Sistemy upravleniya polynym zhiznennym tsiklom vysokotekhnologichnoy produktii v mashinostroyeni: novye istochniki rosta: Vserossiyskaya nauchno-prakticheskaya konferentsiya [Proceedings of the All-Russian Science and Practice Conference Complete Lifecycle Management Systems of High-Technology Engineering Products]. Moscow: Bauman MSTU Publishing; 2018. p. 69-75.
- [15] Klimov S.M., Polikarpov S.V., Fedchenko A.V. Method of increasing fault tolerance of satellite communication networks under information technology interference. Dependability 2017;17(3):32-40.
- [16] Kolobov A.Yu., Dikoun E.V. Interval estimation of reliability of one-off spacecraft. Dependability 2017;17(4):23-26.

About the authors

Vladimir Ya. Gecha, Doctor of Engineering, Professor, Deputy Director General, A.G. Iosifian Research and Production Corporation Space Monitoring, Information, Control

References

- [1] Gnedenko B.V., Beliaev Yu.K., Soloviev A.D. Matematicheskie metody v teorii nadezhnosti [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965 [in Russian].
- [2] Sidniyev N.I. Teoriya planirovaniya eksperimenta i analiza statisticheskikh dannyykh: uchebnoe posobie [Experimental design theory and statistical data analysis: study guide]. Moscow: Izdatel'stvo Yuray; 2011 [in Russian].
- [3] Morozov D.V., Chernoshentsev S.F. Method of improving the functional dependability of the control systems of an unmanned aerial vehicle in flight in case of failure in the onboard test instrumentation. Dependability 2019;1:.... DOI: 10.21683/1729-2646-2019-19-1...
- [4] Sidniyev N.I., Sadykhov G.S., Savchenko V.P. Modeli i metody osenki ostatochnogo resursa izdeliy radioelektroniki [Models and methods of estimation of the residual operating life of electronics]. Moscow: Bauman MSTU Publishing; 2015 [in Russian].
- [5] Morris S.F. Use and application of MIL-HDBK-217. Solid State Technology 1990;33(6):65-69.
- [6] Sidniyev N.I. Matematicheskoe modelirovaniye osenki nadezhnosti ob'ektov slozhnykh tekhnicheskikh sistem [Mathematical simulation of dependability estimation of complex technical systems]. Problemy mashinostroyeniya i nadezhnosti mashin 2003;4:24-31 [in Russian].
- [7] Brennom, T.R. Should US MIL-HDBK-217 be 8888. IEEE Trans. Reliab. 1988;37(5):474-475.

The weight-average conditional density of the estimate of the confirmed level of dependability will be:

$$\phi^{com}(R_n/n, m) = \frac{\int_1^0 R_{n-m}^n (1 - R_n^n) \phi(R_n^n) dR_n^n}{R_{n-m}^n (1 - R_n^n) \phi(R_n^n)}.$$

where R_{dep} is the level of assured dependability. For each outcome $\{n, m\}$ a conditional density of the Bayesian estimate of the confirmed level of dependability R_n

$$P\{n, m\} = \binom{m}{n} R_{n-m}^{as} (1 - R_{n-m}^{as})^m,$$

of outcomes have the probability tests, are random and on the assumption of independence of each test $\{n, m\}$, where m is the number of successful level of dependability R_n it is planned to test n SC. The result Let us assume that for the purpose of confirming a certain level of dependability [2].

of the strategy of experimental confirmation of the achieved problem would suggest an investigation into the expediency successful application $\gamma_{ap} = \gamma_{as} \gamma_{dp}$. Such definition of the on both the guarantee of assurance γ_{as} and the guarantee of guarantee of successful program performance γ now depends level of practical guarantee of assurance γ_{as} . The practical the construction of a confidence interval $[\bar{R}(C), 1]$ with the application of the principle of guaranteed result is based on constants that make the correspondence. Consistent application of the principle of guaranteed result is based on general case, can be defined with a joint distribution of the uncertainty of correspondence $\phi: C \rightarrow R$ that, in a fairly The next step in accommodating the problem definition to the real-world problems consists in accounting for the

tion of domain $f: R \times N \rightarrow N_C$. introduction of the level of practical guarantee and construction of the number of successes. The principle of guaranteed result allows eliminating this uncertainty through the nature of the number of successes. The principle of guarantee of functional correspondence, i.e. the random uncertainty of considered uncertainty consists in the The only type of considered uncertainty consists in the the acceptable error of the extremum seeking procedure.

tion that ensures the maximum indicator R to the definition of which allows finding clearly the best strategy of cost allocation $\forall (s_i, s_j \in S) \exists (w_i = \phi(s_i), w_j = \phi(s_j)) : [w_i, R^w, w_j] \rightarrow [s_i R^s s_j]$, correspondence $\phi: C \rightarrow R$ with the following properties:

and the expired costs is assumed to be defined by functional guarantee. In the context of the above example, the dependence between the achieved level of product dependability shows the applicability of stochastic determinism in ensuring unacceptable way of ensuring a guaranteed result. Analysis initially planned cost of the program, which is obviously an scale manufacture can be several times higher than the the compensation of statistical instability through larger unique items (N_{req} of several units) the costs associated with of the total cost and up to 50% of the DP cost. Finally, for associated with the instability compensation account for 25% program. For low-volume items (N_{req} of tens) the costs as-

Conclusions

The paper proposes a new approach to the analysis of operational dependability of multicomponent space systems (SS) that allows significantly improving and simplifying the analysis and supervision of dependability. One of the advantages of the developed method is that in situations when there is still not enough statistical information, expert judgement is the source of input data for dependability model setting, while subsequently operational data is used. Thus, a system's dependability model is maintained up to date throughout its life cycle stages. The existing methods of dependability analysis are classified and examined. The authors acknowledged the problem of insufficiency of information for classical com-

Calculations show that confirmation of dependability is more efficient in cases of large scopes of application. In case of small scopes of application the priority funding should be directed towards ensuring dependability. The form of dependence $R_{as} = f(C)$ is defined based on the experience of the previous DP of similar products, which does not rule out the possibility of new unforeseen problems, types of failures, etc. In this context, it would be reasonable to develop efficient protection measures as part of DP that – by means of higher quality of SC application management – may enable the solution of the problem under a higher level of initial uncertainty.

$$\gamma_n = (n+1) \left(1 - R_{n-m}^{as} \right) \left(1 - R_{n-m}^{as} \right)^m \left[\frac{m! (n-m)!}{n!} \int_1^0 z^{n-m} (1-z)^m dz \right].$$

Using this dependence, the functional correspondence can be obtained, $\phi: R_{as} \times n \times R_n \rightarrow \gamma_n$. In order to confirm the level R_n while testing n products with dependability R_{as} , a dependence of the following type should be used:

$$\bar{\phi}^{com}(R_n^n) = (n+1)! n! \times R_{n-m}^{as} (1 - R_{n-m}^{as})^m \times \sum \frac{(m!)^2 [(n-m)!]^2}{(1 - R_n^n)^m}.$$

under the known probability of no-failure of SC is identified according to formula [4]:

$$P\{w_i\} = C_i^N R_i (1 - R)^{N-i}.$$

This formula defines the probability measure over the realm W . The event W_i is the union of all ω_i under $i \geq N_{\text{req}}$ therefore its probability is defined as the sum of probabilities of such sample events.

$$P\{W_i\} = \sum_{N=N_{\text{req}}}^i C_i^N R_i (1 - R)^{N-i}.$$

This probability ensures the level of practical guarantee

of successful program performance. In order to ensure the required level of guarantee γ under known values of R and N_{req} we can increase N thus redefining the space W_i until we obtain compliance with condition $P\{W_i\} \geq \gamma$ [2]. The value of N will be equal to the target value N_G . Thus, we will find the possible ways of constructing the functional correspondences $\phi: R \rightarrow N$. If the set R is taken as a space of strategies, out of which must be chosen the value R_{ed} that ensures the minimal total cost of program implementation $C_{\Sigma_{\text{min}}}$, correspondence ϕ solves a part of the problem: for each R it defines N_G . The solution is complicated by the fact that dependability R can be ensured by various combinations of components R_1, R_2, R_3 . In each particular case the problem of auxiliary optimization can be defined and solved. For instance, that may include finding vector R_1, R_2 , that ensures $R' = R_1$ under minimal cost $C = C_1 + C_2$. The procedure of extremum seeking is set forth in [2, 9] as part of a program that defines the dependence of unit costs $C_{\text{un}} = C_{\Sigma} / N_{\text{req}}$ and standardized unit costs $C_{\text{un}}^s = C_{\text{un}} / C_0$, where $C_0 = C_{10} + C_{20}$ from the required number N_{req} for specific sets of input data [11]. Additionally, calculations can help identify the cost component associated with the compensation of statistical instability of the result as compared to the mathematical expectation

$$\Delta C_{\gamma} = \frac{C_{\Sigma}}{C} \left(\frac{C_{\Sigma}}{N} - \frac{R}{N_{\text{req}}} \right)$$

as well as the cost component associated with assurance of dependability

$$\Delta C_R = 1 - \Delta C_{\gamma} - \frac{C_{\Sigma}}{C_0} (N_{\text{req}} + N^{\text{ed}}).$$

The analysis of the last two formulas allows identifying the range of values of mass product manufacture with various capabilities of using probabilistic requirements as the basis of guaranteeing success [1, 4, 12]. For mass-production items ($N_{\text{req}} > 10^3$) the additional cost of ensuring guaranteed results that compensate for the statistical instability of random phenomena relative to average ones account for several percent of the total cost of program and an insignificant fraction of the total cost of the dependability program. For serial production items ($N_{\text{req}} > 10^2$) the costs associated with the instability compensation account for 10% of the total cost and about 20 % of the cost of the dependability

Let us examine the application field of probabilistic

dependability indicators as the basis for ensuring guarantees depending on the scope of SC application [4, 5, 7]. Let the objective of a one-off program of creation and application of a single-use satellite consist in satisfying the need for N_{req} of such products. The required satellite operation time is specified, probability of no-failure R is used as the product dependability indicator. The dependence between the level of product dependability and the cost as part of the dependability program is known to be $R = R_1 R_2 R_3$, where $R_1 = 1 - (1 - R_{10}) \exp[-\alpha_1 (C_1 - C_{10})]$ is the dependability component, that takes into consideration the effect of components failure subject to redundancy, $R_2 = 1 - (1 - R_{20}) \exp[-\alpha_2 (C_2 - C_{20})]$ is the dependability component that takes into consideration the quality level of manufacture and quality assurance, $R_3 = 1 - (1 - (1 - R_{30}) \exp[-\alpha_3 (N^{\text{ed}} - N^{\text{ed}0})])$ is the dependability component that takes into consideration the quality level of maturity, R_{10}, R_{20}, R_{30} are the initial (minimal) levels of components R_1, R_2, R_3 that correspond to the minimal expenditure $C_{10}, C_{20}, N^{\text{ed}0}$ of resources C_1, C_2 and products N^{ed} spent on the experimental development, $\alpha_1, \alpha_2, \alpha_3$ are the parameters that define the growth rate of components of indicator R as the costs increase.

Possible solutions and strategies take into consideration the fact that achieving the specified objective is possible both through increased expenses on higher level of dependability of each item and through extended scale of products manufacture [14].

As when N SC are manufactured, the number of SC N_S that successfully completed their mission is random, the practically achievable guarantee would be γ , where $\gamma = P\{N_S \geq N_{\text{req}}\}$. Each solution is defined by the vector of components R_1, R_2, R_3 or corresponding costs C_1, C_2, N^{ed} which unambiguously defines level R . For the specified γ and N_{req} subject to known R the number of manufactured SC $N_G = f(N_{\text{req}}, \beta, R)$ can be clearly identified that guarantees successful mission completion. The total costs of program implementation C_{Σ} can be identified using the dependence $C_{\Sigma} = (C_1 + C_2)(N^{\text{ed}} + N_G)$. The rationality (optimality) of the solution that involves the definition of the required level of dependability of the product and allocation of resources to dependability assurance measures consists in the minimization of the total cost of development and manufacture of the required number of SC [11, 15] that guarantees successful operation of $N_S \geq N_{\text{req}}$ products. As the outcome set we will use the sample space. Each sample event ω_i consists in the fact that the use of N SC resulted in exactly $N_S = i$ successes. From the point of view of achieving the set goal the whole outcome set W can be divided into two subsets W_1 and W_2 such that

$$\begin{aligned} A(i=0, 1, \dots, N)(w_i \in W_1) &\leftrightarrow (i \geq N_{\text{req}}); \\ A(i=0, 1, \dots, N)(w_i \in W_2) &\leftrightarrow (i < N_{\text{req}}). \end{aligned}$$

In this context the probability of event $w_i \leftrightarrow \{N_Y = i\}$

Introduction

The stages of design, starting from the development of the technical specifications for a system to the delivery of significance within the overall problem of ensuring dependability of spacecraft (SC). An important activity that governs the relationships among all the parties involved in the SC development is the substantiation of the dependability program (DP) of a product as a whole, its components and element, as well as the development and approval of the procedure of dependability requirements confirmation at all stages of development [1-4]. For that purpose, DP models, standard DP and dependability confirmation models (procedures) are used. After the selection of all project, architectural, design and process engineering solutions before the final formalization of a project by the company's dependability service jointly with the developing units, the design outputs are evaluated in terms of dependability and the adopted solutions are adjusted [5-8].

SC is a complex multicomponent system that includes both hardware and software components [9-12]. Consequently, their operation involves real-time supervision of their characteristics and state analysis. Dependability is one of the primary characteristics of a technical system [3]. According to the Russian national standard, dependability is understood as the property of an item to maintain in time and within the set limits the values of all parameters that characterize the ability to perform the required functions in specified modes and conditions of operation, maintenance, repairs, storage and transportation [4]. Due to the complexity of SC structure (and, subsequently, complex nature of relations among the individual components), the process of obtaining the numerical values of dependability indicators becomes more complicated as well [5-8].

The methodological aspects and objectives of the problem

A number of methods and measures are used for prevention and detection of failures related to the design, manufacture and operation, as well as protection of system elements from their consequences. If preliminary studies of system efficiency determine the required quantity and level of guaranteed mission completion, the minimal required level of product dependability can be clearly determined by estimating and minimizing the total cost of development and application, i.e. program execution as a whole [6, 7]. Development of a limited use system (tens of items). In this case all components of the total cost must be taken into consideration: costs of system development, manufacture and operation of the whole fleet of products that ensures mission completion not less than N_{req} times (required number of products) with the guarantee not lower than γ_{req} [9-12]. Specifying system and components dependability requirements involves:

- making a list of dependability indicators,

- definition of dependability norms (specification of the required quantitative values of dependability indicators of the system components),
 - definition of confidence probability or mean square deviation norms, that must be observed while confirming the standard values of system dependability indicators by the time the state tests are complete,
 - specification of managerial and technical requirements for dependability per system elements,
 - definition of the procedure of confirmation of dependability requirements per design stages of system components.
- In the general formulation, the dependability norms definition is as follows [8, 9, 13].
- Let SC consist of N elements integrated with a certain structure and performing certain functions. The following are known [9, 10, 14]: type of joint density of SC element failures $(\tau_i, i = 1, N)$, required value (or a series of values) of the system dependability indicator P_i functions of relations between dependability and considered factors $\phi_i, i = 1, N, \Phi_v, v = 1, S$, $i = 1, L$; distribution function of faultless operation time of components $F_i = P_i \{f(\tau_i)\}$, $i = 1, N$; objective function (functional) $g = g\{P_i, i = 1, N\}$, where P_i is the pointwise value of the dependability estimate of the i -th element, Φ_v is the considered v -th factor, S is the number of factors under consideration, L is the number of functions of relations.
- It is required to find such values of elements' dependability that optimize the objective function g [1, 9].
- If it is required to design a SC with minimal cost or mass, the cost or mass $g = C, C = C\{P_i, i = 1, N\}$, or $g = M$ are chosen as the objective function, $M = M\{P_i, i = 1, N\}$. The solution involves finding vector $P = \{P_1, P_2, \dots, P_N\}$ that minimizes C or M , i.e. $C(P) = \min C(P); P = \{P_1, P_2, \dots, P_N\}$, or $M(P) = \min M(P); P = \{P_1, P_2, \dots, P_N\}$. If the task consists in maximizing function $\Phi(P)$ under the given cost (or mass) limitations, then $\Phi = \Phi\{P_i, i = 1, N\}$. Vector P is found that maximizes $\Phi(P)$, i.e. $\Phi(P) = \max \Phi(P)$ if $C(P) \leq C_0$ or $\Phi(P) = \max \Phi(P)$ if $M(P) \leq M_0$. Norm definition often takes into consideration not only system dependability requirements, but safety requirements as well. Then, the problem is solved using the safety function as function $\Phi(P)$, i.e. $B = \Phi(P)$, then condition $B = \Phi(P) \geq P_B$. Is verified. If it is fulfilled, the problem is solved, if not, the solution continues starting from vector $P = P_B$, i.e. vector that satisfies the solution at the first stage.

Methods of specific implementation

In the process of creation of space technology products that have no analogs and prototypes, instead of strict standard values of dependability indicators, algorithms and methods of specification and norm definition of quantitative dependability requirements are developed that take into consideration the characteristic aspects of application of a SC and its element [15, 16], as well as the actual limitations.

Method of dependability assessment of spacecraft in design and engineering studies

Vladimir Ya. Gecha, A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control and Electromechanical Systems, Russian Federation, Moscow
Ruslan N. Barbul, A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control and Electromechanical Systems, Russian Federation, Moscow
Nikolay I. Sidniayev, Bauman Moscow State Technical University, Russian Federation, Moscow
Yulia I. Butenko, Bauman Moscow State Technical University, Russian Federation, Moscow



Vladimir Ya. Gecha



Ruslan N. Barbul



Nikolay I. Sidniayev



Yulia I. Butenko

Abstract. The paper examines the matters of operational dependability of space systems (SS), efficiency of complex systems, use of redundancy in spacecraft (SC) design. It presents methods of predicting the dependability of designed devices, design of devices with desired dependability and comparison of dependability of various SS. For that purpose, the authors set forth the fundamentals of the dependability theory for SS design, methods of collection and processing of data of equipment dependability based on the results of operation and special dependability tests. Methods, mathematical models are developed, the equipment architecture at the stage of design and manufacture is analyzed. The paper also cites the design ratios for various tested types of redundancy, lifetime extension of SC units based on the residual operating life estimation method. The existing methods of dependability analysis are classified and examined. The authors outline the problems of ambiguity of information of the input data in case of classical computing. The effect of nominal deviations of the external effects, irregularity of the failure rate, non-linear nature of the effect of external factors on the dependability are examined. The paper also takes a look at the way the external factors affect the dependability and the degree to which such factors are taken into consideration in the existing methods. It is noted that the qualitative, technical and organizational (design and software) requirements for dependability in the technical specifications for each stage of elements and SS development, shall be observed and confirmed at the respective stage of activities. The paper presents the methods of estimation of technical item operating life with the focus on those based on the physical premises of operating life depletion. Attention is drawn to the importance of the economic aspect in the research dedicated to SS lifetime extension.

Keywords: dependability, methods, operating life, design, spacecraft, operating life assessment.

For citation: GechayYa, Barbul RN, Sidniayev NI, ButenkoYul. Method of dependability assessment of spacecraft in design and engineering studies. Dependability 2019;2: 3-8. DOI: 10.21683/1729-2646-2019-19-2-3-8

CONTENTS

<i>Structural dependability. Theory and practice</i>	
Gecha V.Ya., Barbul R.N., Sidniyev N.I., Butenko Yu.I. Method of dependability assessment of spacecraft in design and engineering studies.....	3
Antonov A.V., Chepurko V.A., Cherniaev A.N. Study of the beta-factor model application for common cause failure modeling	9
Mikhailov V.S. Estimation of the gamma-percentile life for the binomial test plan.....	18
<i>Functional dependability. Theory and practice</i>	
Ivanov A.I., Kuprianov E.N., Tureev S.V. Neural network integration of classical statistical tests for processing small samples of biometrics data	22
Rozenberg E.N., Korovin A.S., Penkova N.G. Model of efficiency assessment of diagnostic tools of onboard equipment	28
<i>Functional safety and survivability. Theory and practice</i>	
Baranov L.A., Kulba V.V., Shelkov A.B., Somov D.S. Indicator-based approach to safety management of railway infrastructure facilities.....	33
Efimov V.V. On the matter of the terminology of aeronautical structures survivability	42
<i>Risk management. Theory and practice</i>	
Popov V.G., Sukhov F.I., Bolandova Yu.K. Economic assessment of the accidental risk of natural emergencies to train traffic.....	48
Gnedenko Forum	54

EDITORIAL BOARD

Editor-in-Chief

Igor B. Shubinsky, PhD, D.Sc in Engineering, Professor, Expert of the Research Board under the Security Council of the Russian Federation, Director General CJSC IBTrans (Moscow, Russia)

Deputy Editor-in-Chief

Schäbe Hendrik, Dr. rer. nat. habil., Chief Expert on Reliability, Operational Availability, Maintainability and Safety, TÜV Rheinland InterTraffic (Cologne, Germany)

Deputy Editor-in-Chief

Mikhail A. Yastrebenetsky, PhD, D.Sc in Engineering, Professor, Head of Department, State Scientific and Technical Center for Nuclear and Radiation Safety, National Academy of Sciences of Ukraine (Kharkiv, Ukraine)

Executive Editor

Aleksey M. Zamyshliaev, PhD, D.Sc in Engineering, Deputy Director General, JSC NIAS (Moscow, Russia)

Technical Editor

Evgeny O. Novozhilov, PhD, Head of System Analysis Department, JSC NIAS (Moscow, Russia)

Chairman of Editorial Board

Igor N. Rozenberg, PhD, D.Sc in Engineering, Professor, Director General, JSC NIAS (Moscow, Russia)

Cochairman of Editorial Board

Nikolay A. Makhutov, PhD, D.Sc in Engineering, Professor, corresponding member of the Russian Academy of Sciences, Chief Researcher, Mechanical Engineering Research Institute of the Russian Academy of Sciences, Chairman of the Working Group under the President of RAS on Risk Analysis and Safety (Moscow, Russia)

EDITORIAL COUNCIL

Zoran Z. Avramovic, PhD, Professor, Faculty of Transport and Traffic Engineering, University of Belgrade (Belgrade, Serbia)
Leonid A. Baranov, PhD, D.Sc in Engineering, Professor, Head of Information Management and Security Department, Russian University of Transport (MIIT) (Moscow, Russia)
Alexander V. Bochkov, PhD, Deputy Head of Division for Analysis and Ranking of Monitored Facilities, Analytic Center, Gazprom Gaznadzor, Moscow, Russia

THE JOURNAL PROMOTER:

“Journal “Reliability” Ltd
It is registered in the Russian Ministry of Press, Broadcasting and Mass Communications.
Registration certificate III 77-9782, September, 11, 2001.
Official organ of the Russian Academy of Reliability

Publisher of the journal
LLC Journal “Dependability”
Director
Dubrovskaya A.Z.
The address: 109029, Moscow,
Str. Nizhegorodskaya, 27,
Building 1, office 209
Ltd Journal “Dependability”
www.dependability.ru
Printed by JSC “Regional printing house,
Printing place” 432049, Ulyanovsk,

Pushkarev str., 27. Circulation: 500 copies.
Printing order
Papers are reviewed. Signed print
Volume , Format 60x90/8, Paper gloss
Papers are reviewed.
The opinion of members of the editorial board may not coincide with the point of view of authors’ publications. The reprint of materials is granted only with the written permission of the editorial board. Manuscripts are not returned.

Konstantin A. Bochkov, D.Sc in Engineering, Professor, Chief Research Officer and Head of Technology Safety and EMC Research Laboratory, Belarusian State University of Transport (Gomel, Belarus)

Valentin A. Gapanovich, PhD, President, Association of Railway Technology Manufacturers (Moscow, Russia)

Viktor A. Kashtanov, PhD, M.Sc (Physics and Mathematics), Professor of Moscow Institute of Applied Mathematics,

National Research University “Higher School of Economics” (Moscow, Russia)

(Moscow, Russia)

Sergey M. Klimov, PhD, D.Sc in Engineering, Professor, Head of Department, 4th Central Research and Design Institute of the Ministry of Defence of Russia (Moscow, Russia)

Yury N. Kofanov, PhD, D.Sc. in Engineering, Professor of Moscow Institute of Electronics and Mathematics, National Research University “Higher School of Economics” (Moscow, Russia)

Achutha Krishnamoorthy, PhD, M.Sc. (Mathematics), Professor Emeritus, Department of Mathematics, University of Science and Technology (Cochin, India)

Eduard K. Letsky, PhD, D.Sc in Engineering, Professor, Head of Chair, Automated Control Systems, Russian University of Transport (MIIT) (Moscow, Russia)

Viktor A. Netes, PhD, D.Sc in Engineering, Professor, Moscow Technical University of Communication and Informatics (MTUCI) (Moscow, Russia)

Ljubiša Papić, PhD, D.Sc in Engineering, Professor, Director, Research Center of Dependability and Quality Management (DQM) (Prijevor, Serbia)

Roman A. Polyak, M.Sc (Physics and Mathematics), Professor, Visiting Professor, Faculty of Mathematics, Technion – Israel Institute of Technology (Haifa, Israel)

Boris V. Sokolov, PhD, D.Sc in Engineering, Professor, Deputy Director for Academic Affairs, Saint Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) (Saint Petersburg, Russia)

Lev V. Utkin, PhD, D.Sc in Engineering, Professor, Telematics Department, Peter the Great St. Petersburg Polytechnic University (Saint Petersburg, Russia)

Evgeny V. Yurkevich, PhD, D.Sc in Engineering, Professor, Chief Researcher, Laboratory of Technical Diagnostics and Fault Tolerance, ICS RAS (Moscow, Russia)