ЖУРНАЛ ВКЛЮЧЕН В ПЕРЕЧЕНЬ ВЕДУЩИХ ЖУРНАЛОВ И ИЗДАНИЙ ВЫСШЕЙ АТТЕСТАЦИОННОЙ КОМИССИИ (ВАК)

Надежность
Префикс DOI: 10.21683
ISSN 1729-2646
e-ISSN 2500-3909

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. Пушкарева, 27.

Подписано в печать 08.06.2019
Объем , Тираж 500 экз, Заказ №
Формат 60x90/8, Бумага глянец

Журнал издается ежеквартально с 2001 года,
стоимость одного экземпляра 1045 руб.,
годовой подписки 4180 руб.,
телефон редакции 8 (495) 967-77-05,
e-mail: dependability@bk.ru

Статьи рецензируются.
Статьи опубликованы в авторской редакции.

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

Оригинальная статья
https://doi.org/10.21683/1729-2646-2019-19-4-3-7

Объект в надежности: определение и содержание понятия

Виктор А. Нетес, *Московский технический университет связи и информатики, Российская Федерация, Москва*

Виктор А. Нетес

Резюме. Цель. *Статья продолжает цикл публикаций, исследующих и обсуждающих сущность и определения базовых понятий теории надежности. В ней проведен анализ исходного понятия, являющего предметом рассмотрения в надежности, для которого обычно используется термин «(технический) объект». Именно для него определяется понятие «надежность», и вообще, распространяется вся терминология по надежности в технике. Рассмотрены следующие вопросы: как назвать и определить этот предмет рассмотрения, что он может собой представлять, что может входить в его состав. В частности, обсуждается соотношение между понятиями «объект» и «изделие».* **Методы.** *Прослежена эволюция определений указанного понятия в отечественных и международных терминологических стандартах по надежности за последние 30 лет. Проведен сравнительный анализ других стандартов и федеральных законов, относящихся к объектам различного вида. Рассмотрена возможность применения двух основных способов, позволяющих составить представление о некотором понятии: наглядного (на основе примеров) и дефиниционного (путем последовательного определения одних понятий через другие).* **Результаты и выводы.** *Определение и правильное понимание понятия «объект» имеет большое значение, поскольку от него зависит область применения стандартов по надежности. Объясняется, почему приходится мириться с тем, что определения исходных понятий не могут быть строго формализованы и фактически являются всего лишь пояснениями. Показано, что определения понятия «объект» в действующих отечественном и международном стандартах (ГОСТ 27.002-2015 и IEC 60050-192:2015) имеют неточности. Для их устранения предложены уточненные формулировки примечаний к определению объекта. Первое примечание перечисляет возможные виды объектов: изделия (детали, сборочные единицы, комплексы) и их составные части; здания и сооружения; системы, состоящие из совместно функционирующих изделий и сооружений, и их подсистемы. Второе примечание указывает соотношения между основными составляющими объекта: аппаратными средствами, программным обеспечением и людьми (персоналом), и их возможные комбинации. Обоснована целесообразность рассмотрения виртуальных объектов, играющих важную роль в современных информационных и коммуникационных технологиях и представляющих собой логически выделенные подсистемы в составе систем, на основе которых они создаются. Указаны также недостатки, имеющиеся в определениях различных объектов в ГОСТ 18322-2016.*

Ключевые слова: *надежность, стандартизация, технический объект, определение, виды объектов, составляющие объекта.*

Для цитирования: *Нетес В.А. Объект в надежности: определение и содержание понятия // Надежность. 2019. № 4. С. 3-7. https://doi.org/10.21683/1729-2646-2019-19-4-3-7*

Поступила 09.09.2019 г. / После доработки 18.10.2019 г. / К печати 14.12.2019 г.

Введение

Теория надежности существует уже несколько десятков лет, однако до сих пор ведутся споры вокруг определений ее базовых понятий. В последние годы они обсуждались в ряде статей, предпосылкой к написанию которых сначала стала разработка отечественного и международного терминологических стандартов по надежности (ГОСТ 27.002-2015 и IEC 60050-192:2015), а затем и анализ этих стандартов [1-6 и др.]. В частности, развернулась оживленная дискуссия о том, как определить само понятие «надежность» [2]. На взгляд автора, все это свидетельствует не о кризисе в теории надежности, а о том, что она живет и развивается.

В данной статье анализируется понятие, которое предшествует понятию «надежность», а именно обсуждается, что является предметом рассмотрения в надежности, точнее говоря, надежность чего имеет смысл изучать. Для этого понятия, как правило, используется термин «объект», имеются его определения в стандартах. Однако здесь также нет полной ясности, вокруг этого тоже шло обсуждение. Будут рассмотрены следующие вопросы: как назвать и определить этот предмет рассмотрения, что он может собой представлять, что может входить в его состав. Попутно анализируются замечания, высказанные в [4, 5] в адрес ГОСТ 27.002-2015 «Надежность в технике. Термины и определения» и связанные с рассматриваемой темой.

История вопроса

До 2009 года в основном тексте отечественных терминологических стандартов по надежности отсутствовал термин, соответствующий предмету рассмотрения в надежности. В определениях основных понятий в этом качестве использовался термин «объект», а в справочном приложении, содержащем пояснения к терминам, объяснялось, что терминология по надежности в технике распространяется на любые технические объекты – изделия, сооружения и системы, а также их подсистемы, рассматриваемые с точки зрения надежности на этапах проектирования, производства, испытаний, эксплуатации и ремонта. Далее указывалось, что в качестве подсистем могут рассматриваться сборочные единицы, детали, компоненты или элементы (формулировки из ГОСТ 27.002-89).

В 2009 году взамен ГОСТ 27.002-89 был принят ГОСТ Р 53480-2009, впоследствии получивший обозначение ГОСТ Р 27.002-2009. Он был разработан с учетом основных нормативных положений международного стандарта IEC 60050-191:1990 “International electrotechnical vocabulary – Part 191: Dependability and quality of service” («Международный электротехнический словарь – Часть 191: Надежность и качество услуг»). Здесь стоит отметить, что именно Международная электротехническая комиссия (МЭК, англ. International Electrotechnical Commission, IEC) играет ведущую роль в международной стандартизации надежности [7].

В ГОСТ Р 27.002-2009 появился термин «изделие», имеющий определение: любая функциональная единица, которую можно рассматривать в отдельности. В примечании 1 к нему были приведены примеры изделий: система, подсистема, оборудование, устройство, аппаратура, узел, деталь, элемент. Все основные понятия надежности в этом стандарте определялись применительно к изделию.

При этом в официальном переводе стандарта IEC 60050-191:1990 для соответствующего понятия, выраженного английскими терминами “item” и “entity”, использовался русский эквивалент «объект», которому давалось следующее определение: любая часть, элемент, устройство, подсистема, функциональная единица, аппаратура или система, которые можно рассматривать в отдельности. Таким образом, часть этой формулировки была использована в ГОСТ 27.002-2009 как определение, а другая часть – вошла в примечание к нему.

ГОСТ 27.002-2009 вызвал серьезную критику специалистов, в результате чего вместо него было возобновлено действие ГОСТ 27.002-89 (подробнее эта история описана в [2]). Одним из нововведений, подвергавшихся критике, была замена термина «объект» на «изделие». И дело здесь не только в отходе от ставшей за много лет привычной терминологии. Более серьезным аргументом являлось то, что термин «изделие» уже был стандартизован в системе стандартов ЕСКД. В действовавшем на тот момент ГОСТ 2.101-68 «Единая система конструкторской документации. Виды изделий» говорилось, что изделием называется любой предмет или набор предметов производства, подлежащих изготовлению на предприятии. Таким образом, возникало нежелательное расхождение между определениями одного и того же термина в основополагающих общетехнических стандартах. При этом понимание термина «изделие» в ЕСКД, подразумевающее его изготовление на предприятии, уже, чем у понятия «объект» в надежности. Последнее включает, например, линии, сети и каналы связи, линии электропередачи, трубопроводы и т.п. Все они не являются изделиями в понимании ЕСКД.

В 2015 году взамен стандарта IEC 60050-191:1990 был принят IEC 60050-192:2015 “International electrotechnical vocabulary – Part 192: Dependability” («Международный электротехнический словарь – Часть 192: Надежность»). Общий анализ этого стандарта был дан в [3]. Из двух упомянутых выше английских терминов в нем был оставлен только первый (item), для которого было дано весьма краткое определение: рассматриваемый предмет. В примечании 5 к нему объясняется причина изменения: «Определение объекта в IEC 60050-191:1990 является скорее описанием, а не определением. Новое определение обеспечивает содержательную замену во всем документе. Формулировка прежнего определения образуют новое примечание 1».

В том же году был принят и ГОСТ 27.002-2015. При его разработке ставилась цель, с одной стороны, сохранить преемственность с ГОСТ 27.002-89, а с другой – приблизиться к новому международному стандарту. В результате было принято следующее определение: (технический) объект – предмет рассмотрения, на который распространяется терминология по надежности в технике. Примечание 1 к нему дает список возможных объектов: сборочная единица, деталь, компонент, элемент, устройство, функциональная единица, оборудование, изделие, система, сооружение.

В последующих публикациях были высказаны замечания к этому определению, однако они будут рассмотрены чуть позже. Перед этим уместно будет сделать общетеоретическое отступление, касающееся определений базовых понятий.

Проблема определения исходных понятий

Трудности с определением базовых понятий характерны не только для теории надежности, они носят общий характер. Вот что писал по этому поводу известный математик и лингвист В.А. Успенский: «…Как можно составить представление о том или ином понятии? Есть два основных способа, один из которых мы условно назовем *наглядным*, а другой, столь же условно, – *дефиниционным* (от *лат*. definitio – определение). При наглядном способе понятие усваивается на примерах, при дефиниционном – с помощью определений. <…> …При дефиниционном способе одни понятия определяются через другие, другие – через третьи и т.д. Но ведь мы не

можем продолжать этот процесс бесконечно. А значит, на каких-то … понятиях мы вынуждены остановиться и далее их не определять. Эти понятия, которые уже не имеют определения, называют *неопределяемыми*, или *исходными*. Но если исходные понятия не могут быть определены, …откуда же мы можем знать, что они означают?» [8, с. 309-310, 312-313].

В математике выход из этого тупика дает аксиоматический метод [8, с. 313]. В других областях знаний, не столь строго формализованных, приходится мириться с тем, что определения исходных понятий фактически являются всего лишь пояснениями, подобно тому, как это было со сформулированными Эвклидом определениями базовых понятий геометрии («точка есть то, что не имеет частей», «линия же – длина без ширины» и т.п.) [8, с. 307]. Поэтому в том, что в ГОСТ 27.002-89 и предшествовавших ему стандартах не давалось определение объекта, а лишь пояснение к этому понятию, есть свой смысл.

В самом деле, определения объекта в IEC 60050-192: 2015 и ГОСТ 27.002-2015, строго говоря, таковыми не являются. Поэтому столь важны примеры объектов, приведенные в примечаниях к определениям в этих стандартах, поскольку, как было сказано выше, при наглядном способе понятие усваивается именно на примерах.

Подчас попытки найти выход из описанного тупика приводят к возникновению в определениях порочного круга, при котором некоторое понятие определяется через само себя или понятие А определяется через Б, а Б – через А. Пример подобной ситуаций в стандартах будет приведен ниже. Разумеется, это является серьезным недостатком этих стандартов.

Виды объектов

В [4] справедливо отмечено, что перечень видов объектов, приведенный в примечании 1 к определению объекта в ГОСТ 27.002-2015, не увязан с ГОСТ 2.101-2016 «Единая система конструкторской документации. Виды изделий». Действительно, согласно ГОСТ 2.101-2016, изделие – это предмет или набор предметов производства, подлежащих изготовлению в организации (на предприятии) по конструкторской документации, причем в примечании 1 к этому определению указано, что изделиями могут быть устройства, средства, машины, агрегаты, аппараты, приспособления, оборудование, установки, инструменты, механизмы, системы и др. В ГОСТ 2.101-2016 определяется также составная часть изделия – изделие, выполняющее определенные функции в составе другого изделия, и устанавливаются виды изделий по конструктивно-функциональным характеристикам: деталь, сборочная единица, комплекс и комплект.

Если первые три вида изделий (деталь, сборочная единица, комплекс), безусловно, являются объектами с точки зрения надежности, то комплект вряд стоит считать таковым. В самом деле, комплект – это два и более изделия, не соединенных на предприятии-изготовителе сборочными операциями и представляющих набор изделий, имеющих общее эксплуатационное назначение вспомогательного характера, например: комплект запасных частей, комплект инструмента и принадлежностей, комплект измерительной аппаратуры, комплект упаковочной тары и т.п. (определение из ГОСТ 2.101-2016). Поэтому для комплекта не существует единых требуемых функций, сохранение способности к выполнению которых и характеризует надежность. Конечно, это не исключает возможность отдельно рассматривать надежность входящих в комплект изделий.

Обсуждая понятие «изделие», попутно заметим, что в ГОСТ 2.101-2016 в его определении добавились слова о конструкторской документации, отсутствовавшие в прежней версии этого стандарта 1968 года. При этом ГОСТ 2.001-2013 «Единая система конструкторской документации. Общие положения» определяет конструкторскую документацию как совокупность конструкторских документов, содержащих данные, необходимые для проектирования (разработки), изготовления, контроля, приемки, поставки, эксплуатации, ремонта, модернизации, утилизации изделия. Таким образом, здесь имеет место порочный круг: в определении термина «изделие» присутствует термин «конструкторская документация», а в определении термина «конструкторская документация» – «изделие».

В ГОСТ 27.002-2015 указано, что требования к объекту задаются в документации на этот объект. В [5] это считается недостатком этого стандарта («нечеткость терминологии надежности»), и предлагается, чтобы в этой формулировке фигурировала именно конструкторская документация. Однако такая документация относится только к изделиям, т.е. далеко не ко всем видам объектов. Кстати, и в прежнем ГОСТ 27.002-89 формулировка также не ограничивалась только конструкторской документацией, там говорилось о нормативно-технической и (или) конструкторской (проектной) документации.

Еще одно замечание в [4] касается взаимной увязки ГОСТ 27.002-2015 и ГОСТ 18322-2016 «Система технического обслуживания и ремонта техники. Термины и определения». В каждом из этих стандартов указано, что он применяется совместно с другим. К сожалению, между ними действительно имеются расхождения, в том числе в части понятия «объект». Правда, читая [4], можно подумать, что в ГОСТ 18322-2016 также имеется определение понятия «объект», хотя на самом деле это не так. В этом стандарте определены термины «объект технического обслуживания (ремонта)», «обслуживаемый объект», «необслуживаемый объект», «ремонтопригодный объект», «неремонтопригодный объект». Процитированная же в [4] формулировка «объект представляется в виде единого целого, состоящего из взаимосвязанных частей, объединенных в нем для выполнения общей целевой функции» является только примечанием к указанным терминам. Однако определения всех указанных терминов в ГОСТ 18322-2016 содержат слово «объект». Остается только гадать, что под ним имеется в виду. Возможно, это объект, определенный в

ГОСТ 27.002-2015. В любом случае здесь необходимы были разъяснения.

Далее, термины «обслуживаемый объект», «необслуживаемый объект», «ремонтопригодный объект», «неремонтопригодный объект» имеются в обоих стандартах. При этом определения первых двух из них в ГОСТ 18322-2016 совпадают с определениями этих терминов в ГОСТ 27.002-2015 (хотя отсылка к нему отсутствует), а вторых двух – несколько отличаются от определений в ГОСТ 27.002-2015. Поистине, вслед за авторами [4] хочется воскликнуть: «Чему верить?». При внимательном изучении этих терминов возникают и дальнейшие вопросы. Чем объект технического обслуживания отличается от обслуживаемого объекта, а объект ремонта – от ремонтопригодного объекта?

Следующее замечание в [4] касается увязки ГОСТ 27.002-2015 с Федеральным законом от 30.12.2009 № 384-ФЗ «Технический регламент о безопасности зданий и сооружений». Оно совершенно справедливо, наряду с сооружениями в перечень видов объектов следует включить и здания (непонятно только, почему в [4] они названы составными частями объекта – ведь это самостоятельные виды объектов). В пользу такого дополнения говорят также ГОСТ 27751-2014 «Надежность строительных конструкций и оснований. Основные положения» и ГОСТ Р 58033-2017 «Здания и сооружения. Словарь. Часть 1. Общие термины» (в последнем упоминается надежность).

К объектам относятся также системы, состоящие из изделий и сооружений, совместно выполняющих определенные функции (например, сети связи, электроэнергетические системы, сети газораспределения и т.п.), и их подсистемы. В частности, надежности электроэнергетических систем большое внимание уделяется в Федеральном законе от 26.03.2003 № 35-ФЗ «Об электроэнергетике».

Заметной тенденцией в современных информационных и коммуникационных технологиях является виртуализация. В информационных системах могут использоваться виртуальные вычислительные машины, виртуальные системы хранения данных и т.п. (определения этих и других подобных понятий приведены в ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»). В телекоммуникациях используются виртуальные сети, виртуальные каналы и тракты (в частности, виртуальная частная сеть рассматривается в ГОСТ Р 53729-2009 «Качество услуги «Предоставление виртуальной частной сети (VPN)». Показатели качества»). Сетевая виртуализация считается одной из ключевых технологий перспективных будущих сетей [9]. Для рассмотрения надежности всего этого следует допустить возможность наличия не только физических, но и виртуальных объектов. Они обычно представляют собой логически выделенные подсистемы в составе систем, на основе которых создаются виртуальные объекты.

С учетом всего сказанного, предлагается следующая формулировка примечания 1 к термину «объект»: объектами могут быть изделия (детали, сборочные единицы, комплексы) и их составные части, здания и сооружения, системы, состоящие из изделий и сооружений, совместно выполняющих определенные функции, и их подсистемы.

Что включает в себя объект

Рассмотрим теперь вопрос, что может включаться в состав объекта. В уже упоминавшихся пояснениях в ГОСТ 27.002-89 было сказано, что при необходимости в понятие «объект» могут быть включены информация и ее носители, а также человеческий фактор (например, при рассмотрении надежности системы «машина-оператор»). Эта формулировка представляется не очень удачной, особенно, последняя часть: как фактор может быть включен в объект?

В IEC 60050-191:1990 примечание 1 к термину «объект» гласит: объект может состоять из технических средств, программного обеспечения или их сочетания и может также в частных случаях включать людей. Подобная же формулировка составила примечание 2 к термину «изделие» в ГОСТ Р 27.002-2009. Отметим, что в официальном русском переводе IEC 60050-191:1990 вместо «людей» сказано «технический персонал» (кстати, во французской версии стандарта использован именно термин «персонал» – personnel).

В действующем стандарте IEC 60050-192:2015 в примечании 2 к термину «объект» (item) сказано: объект может состоять из аппаратного обеспечения, программного обеспечения, людей или любой их комбинации (во французской версии по-прежнему использован термин «персонал»). В соответствии с этим в ГОСТ 27.002-2015 примечание 2 к термину «объект» было сформулировано так: объект может включать в себя аппаратные средства, программное обеспечение, персонал или их комбинации. Эта формулировка (в частности, упоминание персонала) в [4] была подвергнута критике.

Проанализируем целесообразность включения в состав объекта наряду с аппаратными средствами программного обеспечения и людей (персонала).

Необходимость учета программного обеспечения при рассмотрении надежности программно-управляемых объектов известна давно. Взаимосвязь между аппаратной и программной составляющими таких объектов четко и убедительно была изложена в [10]: «…Программа работы ЭВМ как самостоятельная субстанция существует только до того момента, как будет введена в запоминающее устройство (ЗУ) машины. Причем до этого момента программа существует не как технический объект (и даже не как составная часть технического объекта), а лишь как документ… Естественно, что в этот период своего существования (до ввода в ЗУ ЭВМ) программа не может самостоятельно функционировать… Следовательно, в этот период программа не обладает и никакими эксплуатационными свойствами технических объектов, в том числе надежностью… <…> Когда же программа введена в память ЭВМ, она перестает быть самостоя-

тельной субстанцией и может рассматриваться только как информация о состоянии определенного множества физических элементов памяти… Теперь уже нельзя указать физической границы между аппаратурой ЭВМ и программой, которая в нее введена и в соответствии с которой машина только и может функционировать… <…> …Одна только аппаратура ЭВМ без какой либо записанной в ЗУ программы также не способна перерабатывать информацию (она может только греться при включенном электропитании, но это не является для ЭВМ «требуемой функцией»), а следовательно, и надежность только элементов этой аппаратуры не может в полной мере характеризовать надежность ЭВМ в целом».

Что касается людей, то необходимость учета человека-оператора при рассмотрении надежности систем «человек-машина» (или «машина-оператор», как сказано в ГОСТ 27.002-89) давно известна. Это отражено, в частности, в ГОСТ 26387-84. «Система «Человек-машина». Термины и определения». Так что, ничего принципиально нового в этом плане ГОСТ 27.002-2015 не вводит.

Вместе с тем, формулировку из IEC 60050-192:2015, допускающую любую комбинацию аппаратного обеспечения, программного обеспечения и людей, и воспроизведенную в несколько смягченном виде в ГОСТ 27.002˙2015, следует признать ошибочной. Например, комбинация только программного обеспечения и людей без аппаратного обеспечения представляется лишенной смысла.

С учетом всего сказанного, предлагается следующая уточненная формулировка примечания 2 к термину «объект»: наряду с аппаратными средствами объект может включать в себя программное обеспечение, необходимое для его функционирования, а для систем «человек-машина» – оперативный персонал.

Заключение

Определение понятия «объект», представляющего собой предмет рассмотрения, на который распространяется терминология по надежности в технике, имеет большое значение, поскольку от него зависит область применения стандартов по надежности. Для его уточнения предлагаются следующие формулировки примечаний к определению этого понятия в ГОСТ 27.002-2015. Примечание 1: объектами могут быть изделия (детали, сборочные единицы, комплексы) и их составные части, здания и сооружения, системы, состоящие из изделий и сооружений, совместно выполняющих определенные функции, и их подсистемы. Примечание 2: наряду с аппаратными средствами объект может включать в себя программное обеспечение, необходимое для его функционирования, а для систем «человек-машина» – оперативный персонал.

Ситуация со стандартизацией научно-технической терминологии вообще, и в области надежности в частности, оставляет желать лучшего, что было показано в [4, 6]. Некоторые предложения, направленные на улучшения ситуации, были высказаны в [6].

Автор обращается с призывом ко всем заинтересованным специалистам высказать свое мнение и дать конструктивные предложения, как по существу затронутых вопросов и предложенных формулировок, так и в части организационных мер по улучшению ситуации.

Библиографический список

1. **Нетес В.А.** Актуальные вопросы стандартизации терминологии в области надежности [Текст] / В.А. Нетес, Ю.И. Тарасьев, В.Л. Шпер // Надежность. – 2014. – № 2. – С. 116-119.

2. **Нетес В.А.** Как нам определить, что такое «надежность» [Текст] / В.А. Нетес, Ю.И. Тарасьев, В.Л. Шпер // Надежность. – 2014. – № 4. – С. 3-14.

3. **Нетес В.А.** Новый международный терминологический стандарт по надежности [Текст] / В.А. Нетес // Надежность. – 2016. – № 3. – С. 54-58.

4. **Ершов Г.А.** Чему верить? О системе стандартов «Надежность в технике» [Текст] / Г.А. Ершов, В.Н. Семериков, Н.В. Семериков // Стандарты и качество. – 2018. – № 8. – С. 14-19.

5. **Похабов Ю.П.** Проблемы надежности и пути их решения при создании уникальных высокоответственных систем [Текст] / Ю.П. Похабов // Надежность. – 2019. – № 1. – С. 10-17.

6. **Нетес В.А.** Как вернуть доверие? О системе стандартов «Надежность в технике» [Текст] / В.А. Нетес // Стандарты и качество. – 2019. – № 2. – С. 19-24.

7. **Богданова Г.А.** МЭК/ТК 56: стандартизация для надежности [Текст] /Г.А. Богданова, В.А. Нетес // Методы менеджмента качества. – 2009. – № 5. – С. 44-47.

8. **Успенский В.А.** Апология математики [Текст]: [сборник статей] / В.А. Успенский. – СПб.: Амфора, ТИД Амфора, 2010. – 554 с.

9. Recommendation ITU-T Y.3011 (01/2012). Framework of network virtualization for future networks [Text].

10. **Резиновский А.Я.** Еще раз о сбоях ЭВМ и так называемой надежности программного обеспечения [Текст] / А.Я. Резиновский // Надежность и контроль качества. – 1988. – № 2. – С. 57-61.

Сведения об авторе

Виктор А. Нетес – доктор технических наук, профессор кафедры «Сети связи и системы коммутации» Московского технического университета связи и информатики, Российская Федерация, Москва, e-mail: v.a.netes@mtuci.ru

Вклад автора в статью

Автор провел анализ определений понятия «технический объект» в отечественных и международных стандартах, выявил присущие им недостатки и предложил уточненные формулировки примечаний к определению объекта, касающиеся возможных видов и основных составляющих объектов.

Оригинальная статья
https://doi.org/10.21683/1729-2646-2019-19-4-8-11

Алгоритм оперативного обнаружения изменения характеристик надежности

Дмитрий С. Репин[1*], Геннадий Ф. Филаретов[2]

[1]Институт информационных технологий Федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий» (ФГАОУ ДПО ЦРГОП и ИТ), Москва, Российская Федерация; [2]Национальный исследовательский университет «Московский энергетический институт (НИУ «МЭИ»), Москва, Российская Федерация.
**r_d_s@inbox.ru*

Дмитрий С. Репин

Геннадий Ф. Филаретов

Резюме. *Целью работы является разработка алгоритма оперативного обнаружения момента изменения характеристик надежности системы, состоящей из совокупности однородных элементов в предположении, что отказы этих элементов происходят в случайные моменты времени, представляют собой пуассоновский поток событий и, следовательно, временны**е** интервалы между ними подчиняются экспоненциальному распределению вероятностей. Предлагается для решения указанной задачи использовать один из классических алгоритмов обнаружения «разладки» дискретного случайного процесса, т.е. спонтанного изменения той или иной его вероятностной характеристики. В качестве такой характеристики выбран параметр экспоненциального распределения θ, однозначно связанный со средним временем между появлениями отказов $T_{ср}$: $\theta = 1/T_{ср}$. Считается, что разладка состоит в скачкообразном изменении параметра θ от исходного стационарного состояния $\theta = \theta_0$ до уровня номинальной (ожидаемой, предельно допустимой, критической) разладки, когда $\theta = \theta_1 > \theta_0$. В работе для целей обнаружения разладки использован алгоритм кумулятивных сумм (АКС или CUSUM-алгоритм) как обладающий определенными оптимальными свойствами и широко применяемый на практике. Для данного алгоритма приведены необходимые расчетные соотношения, описываются его свойства и особенности. Предложена процедура синтеза контролирующего алгоритма с заданными свойствами, в ходе которой по выбранным пользователем значениям желательного среднего интервала между ложными тревогами $\overline{T}_{ЛТ}$, исходному базовому уровню θ_0 и номинальной разладке $\theta_1 > \theta_0$ определяется значение решающей границы H, а также оценивается быстродействие алгоритма путем вычисления среднего времени запаздывания в обнаружении номинальной разладки $\overline{T}_{зап}$ и его эффективность $E_d = \overline{T}_{ЛТ} / \overline{T}_{зап}$ для различных значений d, характеризующих количественно величину разладки: $d=\theta_1/\theta_0$. Для практической реализации процедуры синтеза приводятся найденные методом имитационного моделирования справочные данные, обеспечивающие получение контролирующего алгоритма с требуемыми характеристиками. Отмечается, что представленная в работе процедура синтеза в принципе может быть использована и для случая постепенного (нескачкообразного) изменения параметра θ. Однако при этом останутся неясными статистические свойства контролирующей процедуры, что требует проведения весьма трудоемких дополнительных исследований.*

Ключевые слова: *надежность системы; обнаружение изменения характеристик надежности; обнаружение разладки дискретного случайного процесса; алгоритм кумулятивных сумм; синтез контролирующего алгоритма.*

Для цитирования: *Репин Д.С., Филаретов Г.Ф. Алгоритм оперативного обнаружения изменения характеристик надежности // Надежность. 2019. № 4. С. 8-11. https://doi.org/10.21683/1729-2646-2019-19-4-8-11*

Поступила 17.10.2019 г. / После доработки 16.11.2019 г. / К печати 14.12.2019 г.

Рассматривается задача оперативного обнаружения момента изменения характеристик надежности системы, состоящей из совокупности однородных элементов. Предполагается, что отказы этих элементов происходят в случайные моменты времени $t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots$ и представляют собой пуассоновский поток событий. Как известно [1], в этом случае временны**е** интервалы $\tau_i = t_i - t_{i-1}$ подчиняются экспоненциальному распределению вида

$$f(\tau) = \theta \cdot e^{-\theta\tau}; \theta > 0,\ \tau > 0, \qquad (1)$$

где $\theta = 1/T_{ср}$, $T_{ср}$ – среднее время между появлениями отказов.

Будем считать, что в исходном стационарном состоянии параметр $\theta = \theta_0$. По мере старения (износа) элементов системы этот параметр, очевидно, будет изменяться. Исследование подобных нестационарных ситуаций, несомненно, представляет существенный интерес [2]. В данной работе речь идет об оперативном (в режиме реального времени) обнаружении изменения значений $\theta > \theta_0$, когда такое изменение становится существенным. По своей сути это известная задача обнаружения так называемой «разладки» случайного процесса [3].

В классической постановке задачи о разладке предполагается, что разладка носит скачкообразный характер. Применительно к проблематике надежности, такая постановка мало реальна. Однако ее можно рассматривать как некоторое первое приближение к использованию данного подхода при организации оперативного контроля надежностных характеристик сложных систем.

Известно достаточно много алгоритмов обнаружения разладки [4]. Качество их функционирования может быть описано с помощью ряда *вероятностных* характеристик, таких, как среднее значение интервала между ложными тревогами $\overline{T}_{ЛТ}$, т.е. среднее время между подачами сигналов о наличии разладки, когда в действительности ее нет, и среднее время запаздывания $\overline{T}_{зап}$ в обнаружении номинальной (ожидаемой, предельно допустимой, критической) разладки, когда $\theta = \theta_1 > \theta_0$.

В последнее время наиболее часто используемым в различных практических применениях является *алгоритм кумулятивных сумм* (АКС или CUSUM-алгоритм), предложенный Пейджем еще в 1954 году [5]. Этот алгоритм, как было доказано позднее, обладает определенными оптимальными свойствами в смысле максимизации показателя эффективности алгоритма обнаружения $E = \overline{T}_{ЛТ} / \overline{T}_{зап}$. О популярности данного алгоритма и его больших возможностях наглядно свидетельствуют данные библиометрического анализа [6], зафиксировавшего экспоненциальный рост числа публикаций по данной тематике, начиная с 1964 года, а также примеры различных модификаций исходного варианта CUSUM-алгоритма [7–10].

АКС основан на применении несколько видоизмененного варианта последовательного анализа Вальда, используя в решающей функции, как и там, статистику отношения правдоподобия. В рассматриваемом случае она примет следующий вид:

$$g_i = \max\{0; g_{i-1} + z_i\},\ i = 1, 2, \ldots;\ g = 0, \qquad (2)$$

где

$$z_i = \ln\left[f(\tau_i, \theta_1) / f(\tau_i, \theta_0) \right]. \qquad (3)$$

Нулевое значение в формуле (2) играет роль своего рода поглощающего экрана, не позволяя решающей функции смещаться в область отрицательных значений.

Вычисление решающей функции производится каждый раз в момент поступления сигнала об очередном отказе. Контролирующая процедура продолжается до тех пор, пока на некотором шаге n не будет выполнено неравенство:

$$g_n \geq H, \qquad (4)$$

где H – решающая граница. В этом случае подаётся сигнал о наличии разладки. При этом вполне возможно, что в действительности разладка отсутствует, т.е. имеет место ситуация ложной тревоги.

С учетом (1) соотношение (3) может быть конкретизировано:

$$z_i = \ln(\theta_1/\theta_0) - (\theta_1 - \theta_0)\cdot\tau_i = \ln d - (d-1)\cdot(\tau_i \cdot \theta_0);$$
$$d = \theta_1 / \theta_0. \qquad (4)$$

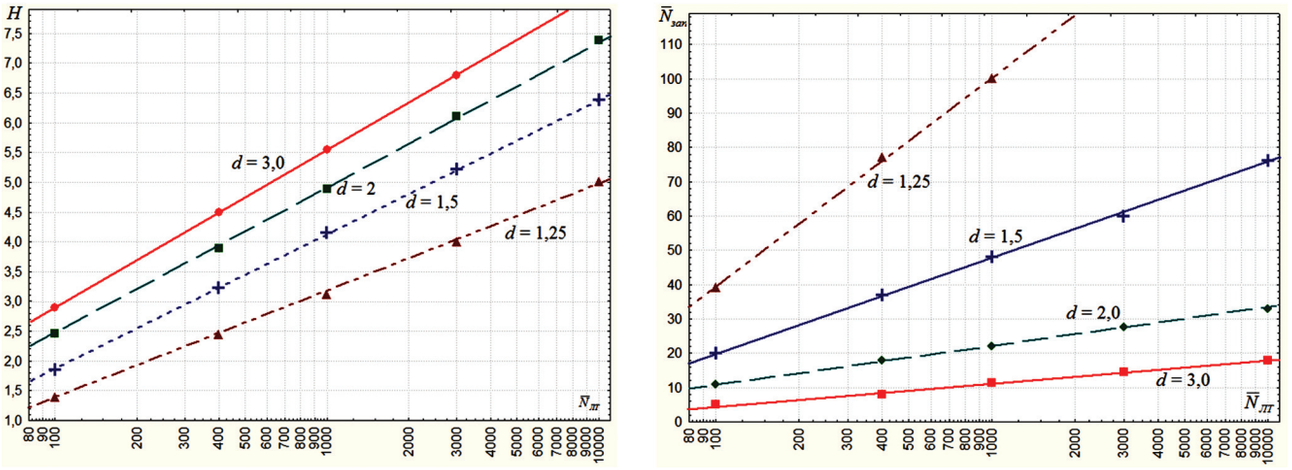
Можно отметить, что математическое ожидание z_i в общем случае равно:

$$M\{z_i\} = \ln d - (d-1)\theta_0 M\{\tau_i\}. \qquad (5)$$

Отсюда следует, что при отсутствии разладки, когда $M\{\tau_i\}=1/\theta_0$, математическое ожидание $M\{z_i\}=\ln d-(d-1)<0$, что препятствует росту значений решающей функции и приводит к достаточно большим средним значениям времени достижения границы H, т.е. достаточно большим значениям $\overline{T}_{ЛТ}$. При номинальной разладке, когда $M\{\tau_i\}=1/\theta_1$, будем иметь $M\{z_i\}=\ln d-(d-1)/d=\ln d-(1-1/d)$. В данном случае $M\{z_i\}>0$, что способствует быстрому возрастанию решающей функции вплоть до порога H, достижение или превышение которого и свидетельствует о наличии разладки.

При практическом использовании алгоритма необходимо предварительно осуществить синтез подходящей контролирующей процедуры. Под синтезом здесь понимается определение решающей границы H по выбранным пользователем значениям $\overline{T}_{ЛТ}$, исходному базовому уровню θ_0 и номинальной разладке $\theta_1 > \theta_0$. Кроме того, при синтезе обычно оценивается быстродействие алгоритма путем вычисления $\overline{T}_{зап}$ и его эффективность E_d для различных значений d.

При проведении таких расчетов необходимо предварительно найти общие соотношения, связывающие перечисленные характеристики. Для их получения использовался метод имитационного моделирования. В ходе моделирования интервалы τ_i рассматривались как значения дискретного временно́го ряда на сетке значений i, в связи с чем и средний интервал между ложными тревогами, и среднее запаздывание определялись как среднее число дискретных отсчетов $\overline{N}_{ЛТ}$ и $\overline{N}_{зап}$ соот-



а) б)

Рисунок 1 – Зависимость решающей границы H (а) и среднего запаздывания $\overline{T}_{зап}$ (б) от $\overline{T}_{ЛТ}$

ветственно; переход из дискретного в реальное время легко может быть осуществлен с помощью очевидных соотношений $\overline{T}_{ЛТ} = \overline{N}_{ЛТ} / \theta_0$ и $\overline{T}_{зап} = \overline{N}_{зап} / \theta_1$.

По результатам моделирования были найдены зависимости границы H от $\overline{N}_{ЛТ}$при различных d из типичного набора d = 1,25; d = 1,5; d = 2,0; d = 3,0, где $d = \theta_1/\theta_0$ и зависимости $\overline{N}_{зап}$ от $\overline{N}_{ЛТ}$. Как оказалось, если рассматривать эти зависимости как функции $\log\overline{N}_{ЛТ}$, то они хорошо аппроксимируются линейными моделями вида: $H=a+b\cdot\log\overline{N}_{ЛТ}$; $\overline{N}_{зап} = c + d\cdot\log\overline{N}_{ЛТ}$. Соответствующие расчетные формулы приведены в табл. 1, а сами эти модели в графической форме отображены на рис. 1 а) и б).

Таблица 1 – Расчетные соотношения для определения решающей границы H и среднего запаздывания $\overline{N}_{зап}$.

d	Формулы для расчета H	Формулы для расчета $\overline{N}_{зап}$
1,25	$H = -2,26 + 1,81\cdot\log\overline{N}_{ЛТ}$	$\overline{N}_{зап} = -83,01 + 61,17\cdot\log\overline{N}_{ЛТ}$
1,5	$H = -2,68 + 2,27\cdot\log\overline{N}_{ЛТ}$	$\overline{N}_{зап} = -35,38 + 27,71\cdot\log\overline{N}_{ЛТ}$
2,0	$H = -2,12 + 2,31\cdot\log\overline{N}_{ЛТ}$	$\overline{N}_{зап} = -10,82 + 10,985\cdot\log\overline{N}_{ЛТ}$
3,0	$H = -2,38 + 2,64\cdot\log\overline{N}_{ЛТ}$	$\overline{N}_{зап} = -8,62 + 6,64\cdot\log\overline{N}_{ЛТ}$

Показатель эффективности контролирующей процедуры E_d может быть рассчитан с помощью соотношения:

$$E(d) = \frac{\overline{T}_{ЛТ}}{\overline{T}_{зап}} = \frac{\overline{N}_{ЛТ} / \theta_0}{\overline{N}_{зап} / \theta_1} = \frac{\overline{N}_{ЛТ}}{\overline{N}_{зап}} \cdot d. \qquad (6)$$

Расчетные значения показателя эффективности E_d для различных d и $\overline{N}_{ЛТ}$ приведены в табл. 2.

Таблица 2 – Расчетные значения показателя эффективности E_d

d	$\overline{N}_{ЛТ}$				
	100	400	1000	3000	10000
1,25	3,2	6,5	12,5	–	–
1,50	7,5	16,2	31,3	75,0	197,4
2,00	18,2	44,4	90,9	165,0	330,0
3,00	60,0	150,0	260,9	620,7	1667,0

Очевидно, что эффективность контролирующей процедуры для наиболее интересных с практической точки зрения вариантов малых значений d и $\overline{N}_{ЛТ}$, к сожалению, относительно невелика.

В заключение можно отметить, что приведенная выше процедура синтеза в принципе может быть использована и для случая постепенного (нескачкообразного) изменения параметра θ. Однако при этом останутся неясными статистические свойства контролирующей процедуры. Их определение с целью получения зависимостей типа представленных в табл. 1, потребует проведения весьма трудоемких дополнительных исследований.

Библиографический список:

1. **Капур К.** Надежность и проектирование систем [Текст] / К. Капур, Л. Ламберсон: Пер. с англ. – М.: Изд-во «Мир», 1980. – 240 с.

2. **Баранов Л.А.** Надежность объектов с нестационарной интенсивностью отказов [Текст] / Л.А. Баранов, Ю.А. Ермолин // Надежность. – 2017. – Том 17. – №4. – С. 3-9.

3. **Бродский Б.Е.** О задаче скорейшего обнаружения момента изменения вероятностных характеристик случайной последовательности [Текст] / Б.Е. Бродский, Б.С. Дарховский // Автоматика и телемеханика. – 1983. – №10. – С. 125-131.

4. **Никифоров И.В.** Последовательное обнаружение изменения свойств временных рядов [Текст] / И.В. Ни-

кифоров. – М.: Наука, 1983. – 200 с.

5. **Page E.S.** Continuous Inspection Schemes [Text] / E.S. Page // Biometrika. – 1954. – Vol. 41. – № 1. – P. 100-115.

6. **Shafid Ahmad.** Bibliometric Analysis of EWMA and CUSUM Control Chart Schemes [Text] / A.Shafid // ITEE Journal. – 2018, April. – Volume 7. – Issue 2. P. 1-11.

7. **Воробейчиков С.Э.** Характеристики процедуры обнаружения разладки процесса авторегрессии с неизвестным распределением помехи [Текст] / С.Э. Воробейчиков, В.В. Конев // Автоматика и телемеханика. – 1992. – № 3. – С. 68-75.

8. **Чернояров О.В.** Обнаружение разладки гауссовского случайного процесса с неизвестной интенсивностью [Текст] / О.В. Чернояров, М.Ф. Рашитов // Материалы Международной научно-технической конференции INTERMATIC–2012, часть 1. – 2012. – № 3. – С. 11-14.

9. **Филаретов Г.Ф.** Последовательный алгоритм обнаружения момента изменения дисперсии временного ряда [Текст] / Г.Ф. Филаретов, А.А. Червова. // Заводская лаборатория. Диагностика материалов. – 2019. – Том 85. – № 3. – С. 75-82.

10. **Сивова Д.Г.** Последовательный алгоритм обнаружения момента изменения характеристик векторных временных рядов [Текст] / Д.Г. Сивова, Г.Ф. Филаретов // Вестник МЭИ. – 2014. – № 2. – С. 63-69.

Сведения об авторах

Дмитрий С. Репин – кандидат технических наук, заместитель директора Института информационных технологий Федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Центр реализации государственной образовательной политики и информационных технологий» (ФГАОУ ДПО ЦРГОП и ИТ), Москва, Российская Федерация, e-mail: r_d_s@inbox.ru; Моб. тел. +7 9166659242.

Геннадий Ф. Филаретов – доктор технических наук, профессор, профессор кафедры управления и информатики Национального исследовательского университета «Московский энергетический институт (НИУ «МЭИ»), Москва, Российская Федерация, e-mail: gefefi@yandex.ru; Моб. тел. +7 9255176319.

Вклад авторов в статью

Дмитрий С. Репин. Разработка программных средств для проведения имитационного эксперимента, его реализация, обработка результатов, получение данных, необходимых для синтеза контролирующего алгоритма.

Геннадий Ф. Филаретов. Обзор и анализ существующего состояния рассматриваемой проблемы, теоретическая составляющая работы.

УДК 519.873, 004.056
Оригинальная статья
Надежность, том 19, №4, 2019 *https://doi.org/10.21683/1729-2646-2019-19-4-12-16*

Дисперсия числа отказов в процессах восстановления

Виталий И. Вайнштейн, *ФГАО ВО «Сибирский федеральный университет», Российская Федерация, 660041, Красноярский край, г. Красноярск, пр. Свободный, 79*

Виталий И. Вайнштейн

Резюме. *Оптимальная организация процесса восстановления имеет важное значение в работе технических, информационно-вычислительных систем, так как возникающие при их работе отказы приводят к значительным негативным последствиям. В работе получена формула дисперсии числа отказов для общего процесса восстановления, которая зависит от функций восстановления (среднего числа отказов) простого и общего процессов восстановления. Также получены формулы дисперсий числа отказов и восстановлений при альтернирующем процессе восстановления, когда наряду со временем работы элемента до отказа учитывается, например, время восстановления. Для экспоненциального распределения при простом и общем процессе восстановления выписаны формулы для дисперсии числа отказов, а также выписано неравенство Чебышева и формула для коэффициента вариации числа отказов для простого процесса восстановления. Представлен алгоритм получения дисперсии в виде рядов для законов распределения наработок, характерных для теории надежности. Разработанный математический аппарат предназначен для применения при постановке и решении различных оптимизационных задач информационной и компьютерной безопасности, а также при эксплуатации технических и информационных систем, программных и программно-аппаратных средств защиты информации, когда возникают отказы, угрозы атак, угрозы безопасности, имеющие случайный характер.*

Ключевые слова: *функция распределения, процесс восстановления, функция восстановления, дисперсия числа отказов, коэффициент вариации.*

Для цитирования: *Вайнштейн В.И. Дисперсия числа отказов в процессах восстановления // Надежность. 2019. №4. С. 12-16. https://doi.org/:10.21683/1729-2646-2019-19-4-12-16*

Поступила 03.09.2019 г. / После доработки 22.10.2019 г. / К печати 14.12.2019 г.

Введение. Постановка задачи. Последовательность неотрицательных, взаимно независимых случайных величин X_i с функциями распределения $F_i(t)$ называется процессом восстановления [1-3]. В теории надежности в процессе восстановления после каждого отказа элемент ремонтируется или заменяется на другой (элемент восстанавливается) и X_i – наработки элемента до отказа после (i–1)-го восстановления, $F_i(t)$ их функции распределения.

В зависимости от структуры последовательности функций распределения $F_i(t)$ имеются различные модели процесса восстановления [1-8].

Так, если все случайные величины X_i имеют одну и туже функцию распределения $F_1(t)$, $F_i(t)=F_1(t)$ имеем простой процесс восстановления. Если $F_i(t)=F_1(t)$, $i\geq 2$ имеем общий процесс восстановления.

Процесс восстановления задает случайную величину $N(t)$ – количество отказов (восстановлений) за время от 0 до t

$$P\left(N\left(t\right)=n\right)=F^{(n)}\left(t\right)-F^{(n+1)}\left(t\right), \qquad (1)$$

$F^{(n)}(t)$ – n-кратная свертка функций распределения $F_i(t)$, i=1,2,…,n

$$F^{(n)}(t)=(F^{(n-1)}*F_n)(t)=\int_0^t F^{(n-1)}(t-x)dF_n(x), F^{(1)}(t)=F_1(t).$$

Важное значение в теоретических и практических задачах теории надежности имеет функция восстановления $H(t)$ – математическое ожидание числа отказов за время от 0 до t в процессе восстановления $H(t)=E(N(t))$

$$H\left(t\right)=\sum_{n=1}^{\infty} nF^{(n)}\left(t\right). \qquad (2)$$

Пусть $HF_1(t)$ – функция восстановления простого процесса, образованного функцией распределения $F_1(t)$, $HF_1F_2(t)$ – функция восстановления общего процесса, образованного первой функцией распределения $F_1(t)$, второй и следующими $F_2(t)$.

Функция восстановления $HF_1(t)$ простого процесса удовлетворяет интегральному уравнению

$$HF_1(t)=F_1(t)+\int_0^t HF_1(t-x)dF_1(x). \qquad (3)$$

Функция восстановления общего процесса восстановления выражается через функцию восстановления простого процесса по формуле

$$HF_1F_2(t)=F_1(t)+\int_0^t HF_2(t-x)dF_1(x).$$

Для простого процесса восстановления формула вычисления дисперсии числа отказов известна [2]

$$D(N(t))=2\int_0^t HF_1(t-x)dHF_1(x)+HF_1(t)-H^2F_1(t). \qquad (4)$$

Цель дальнейшего рассмотрения состоит в получении формулы дисперсии числа отказов при общем процессе восстановления и создание метода ее вычисления для различных законов распределения наработок заменяемых элементов при отказах.

Вычисление дисперсии для общего процесса восстановления. По определению

$$D(N(t))=E(N^2(t))-E^2(N(t))=E(N^2(t))-H^2(t).$$

Таким образом, для вычисления дисперсии наряду с функцией восстановления требуется вычисление $E(N^2(t))$. Приведем вычисление $E(N^2(t))$ [9].

Учитывая (1), (2), получаем

$$E(N^2(t))=\sum_{n=1}^{\infty} n^2P(N(t)=n)=\sum_{n=1}^{\infty} n^2(F^{(n)}(t)-F^{(n+1)}(t))=$$

$$=F_1(t)+\sum_{n=2}^{\infty}(n^2-(n-1)^2)F^{(n)}(t)=F_1(t)+\sum_{n=2}^{\infty}(2n-1)F^{(n)}(t)=$$

$$=-H(t)+2F_1(t)+2\sum_{n=2}^{\infty} nF^{(n)}(t)=-H\left(t\right)+2\sum_{n=1}^{\infty} nF^{(n)}\left(t\right).$$

Таким образом, задача сводится к вычислению для каждой модели процесса восстановления суммы $\sum_{n=1}^{\infty} nF^{(n)}(t)$. В дальнейшем при вычислении этой суммы будет использована формула (2) функции восстановления и определение общего процесса восстановления. Последовательно получаем

$$\sum_{n=1}^{\infty} nF^{(n)}(t)=F_1(t)+2(F_1*F_2)(t)+3(F_1*F_2^{(2)})(t)+\ldots+$$
$$+n(F_1*F_2^{(n-1)})(t)+\ldots=(F_1(t)+(F_1*F_2)(t)+$$
$$+(F_1*F_2^{(2)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+((F_1*F_2)(t)+$$
$$+(F_1*F_2^{(2)})(t)+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+$$
$$+((F_1*F_2^{(2)})(t)+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+$$
$$+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+\ldots+$$
$$+(F_1*F_2^{(n-1)})(t)+(F_1*F_2^{(n)})(t)+\ldots)=$$
$$+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+\ldots+$$
$$6(F_1*F_2^{(n-1)})(t)+(F_1*F_2^{(n)})(t)+\ldots)=(H(t)+$$
$$+(F_1*HF_2)(t)+(F_1*F_2*HF_2)(t)(F_1*F_2*F_2*HF_2)(t)+$$
$$+\ldots+(F_1*(F_2^{(n)}*HF_2)(t)+\ldots)=H(t)+$$
$$+(HF_2*(F_1+(F_1*F_2)(t)+((F_1*F_2*F_2)(t)+\ldots+$$
$$+(F_1*F_2^{(n)})(t)+\ldots))=H\left(t\right)+\left(HF_2*H\right)\left(t\right).$$

Здесь $H(t)=HF_1F_2(t)$. Окончательно

$$D(N(t))=2\int_0^t HF_2(t-x)dHF_1F_2(x)+HF_1F_2(t)-(HF_1F_2\left(t\right))^2. \qquad (5)$$

Пример. Выпишем дисперсии для простого и общего процессов при экспоненциальном распределении наработок

$$F_1(t)=(1-e^{-\alpha_1 t}),\quad F_2(t)=(1-e^{-\alpha_2 t}),\alpha_1\neq\alpha_2.$$

При простом процессе $H(t)=\alpha_1 t$. После интегрирования в (4) $D(N(t))=\alpha_1 t$.

При простом процессе при экспоненциальном распределении наработок дисперсия совпадает с функцией восстановления.

При общем процессе [3]

$$HF_1F_2(t)=\alpha_2 t+(1-\frac{\alpha_2}{\alpha_1})(1-e^{-\alpha_1 t}).$$

После интегрирования в (5)

$$D\left(N(t)\right)=\alpha_2^2t^2+\frac{2\alpha_2\left(\alpha_1-\alpha_2\right)}{\alpha_1}t-$$

$$-\frac{2\alpha_2\left(\alpha_1-\alpha_2\right)}{\alpha_1^2}\left(1-e^{-\alpha_1 t}\right)+HF_1F_2\left(t\right)-H^2F_1F_2\left(t\right).$$

Для многих известных законов распределения, характерных для теории надежности [10], например, экспоненциального, Вейбулла-Гнеденко, Эрланга, нормального, Максвелла, Релея, гамма-распределения и их смесей, функция восстановления получена в явном виде или выписана в виде степенных рядов [2, 3, 11, 12].

В [3, 12] замечено, что указанные функции распределения и их смеси разлагаются в степенные ряды вида

$$F(t)=\sum_{n=0}^{\infty}a_n t^{\beta n+\gamma},\qquad \gamma\geq 0,\ \beta>0. \tag{6}$$

Это дает возможность построения единого алгоритма нахождения функций восстановления простых процессов, образованных функциями распределения вида (6) при условии, если числа β и γ целые, неотрицательные или связаны соотношением $\gamma=l\beta$, l – целое, неотрицательное. В этом случае функции восстановления определяются как решение соответствующего интегрального уравнения (3), если решение искать в виде

$$H(t)=\sum_{n=0}^{\infty}c_n t^{\beta n+\gamma}. \tag{7}$$

Коэффициенты c_n определяются.

По такой схеме в [12] находятся функции восстановления для смесей указанных выше функций распределения за исключением смеси гамма-распределений. При ненатуральных значениях величины γ условие $\gamma=l\beta$, (β=1) не выполняется.

В полученные формулы для вычисления дисперсии входят интегралы $\int_0^t H_1(t-x)dH_2(x)$ от функций восстановления. Пусть в соответствии с (7)

$$H_i(t)=\sum_{n=0}^{\infty}c_{i,n}t^{\beta_i n+\gamma_i},i=1,2.$$

Имеем

$$\int_0^t H_1(t-x)dH_2(x)=$$

$$=\int_0^t(\sum_{n=0}^{\infty}c_{1,n}(t-x)^{\beta_1 n+\gamma_1}\sum_{k=0}^{\infty}c_{2,k}(\beta_2 k+\gamma_2)x^{\beta_2 k+\gamma_2-1})dx=$$

$$=\sum_{k=0}^{\infty}c_{2,k}(\beta_{2,k}+\gamma_2)\sum_{n=0}^{\infty}c_{1,n}\int_0^t(t-x)^{\beta_1 n+\gamma_1}x^{\beta_2,k+\gamma_2-1})dx=$$

$$=\sum_{k=0}^{\infty}c_{2,k}\left(\beta_2+\gamma_2\right)\sum_{n=0}^{\infty}c_{1,n}t^{(\beta_1 n+\beta_2 k+\gamma_1+\gamma_2)}\cdot$$

$$\cdot\frac{\Gamma\left(\beta_1 n+\gamma_1+1\right)\Gamma\left(\beta_2 k+\gamma_2\right)}{\Gamma\left(\beta_1 n+\beta_2 k+\gamma_1+\gamma_2+1\right)}. \tag{8}$$

Здесь учли

$$\int_0^t(t-x)^{\alpha}x^{\beta}dx=t^{\alpha+\beta+1}\frac{\Gamma\left(\alpha+1\right)\Gamma\left(\beta+1\right)}{\Gamma\left(\alpha+\beta+2\right)},$$

$\Gamma(x)=\int_0^{\infty}t^{x-1}e^{-t}dt$ – гамма-функция.

Если $\beta_1=\beta_2=\beta$, то в (8) можно прийти только к одной бесконечной сумме в результате замены $n+k+s$

$$\int_0^t H_1(t-x)dH_2(x)=$$

$$=\sum_{s=0}^{\infty}\frac{t^{\beta s+\gamma_1+\gamma_2}}{\Gamma(\beta s+\gamma_1+\gamma_2+1)}\sum_{n+k=s}c_{1,n}c_{2,k}\Gamma\cdot$$

$$\cdot(\beta n+\gamma_1+1)\Gamma(\beta k+\gamma_2)=$$

$$=\sum_{n=0}^{\infty}\frac{t^{\beta n+\gamma_1+\gamma_2}}{\Gamma(\beta n+\gamma_1+\gamma_2+1)}\sum_{k=0}^{n}c_{2,k}c_{1,n-k}\Gamma\cdot$$

$$\cdot(\beta(n-k)+\gamma_1+1)\Gamma(\beta k+\gamma_2).$$

При определении процесса восстановления предполагалось, что восстановление отказавшего элемента происходит мгновенно. На практике это предположение часто не выполняется. Наряду со временем безотказной работы, не менее важное значение может иметь время простоя, время выяснения причин отказа, время самого восстановления.

Рассмотрим так называемый простой альтернирующий процесс восстановления [2, 3].

Пусть (X_n), (Y_n) – две последовательности неотрицательных, взаимно независимых случайных величин, каждая из которых образует простой процесс восстановления с функциями распределения $F(t)$, $G(t)$ соответственно. Последовательность (X_n, Y_n) называется простым альтернирующим процессом восстановления [2, 3].

Если Y_n – время восстановления элемента после n-го отказа, X_n – время наработки элемента после $(n-1)$-го восстановления (восстановление начинается после первого отказа), то в моменты

$$T_1 = X_1, \quad T_2 = X_1 + Y_1 + X_2, \ldots,$$
$$T_n = X_1 + Y_1 + X_2 + \cdots + Y_{n-1} + X_n, \ldots$$

происходят отказы, а в моменты

$$S_1 = X_1 + Y_1, S_2 = X_1 + Y_1 + X_2 + Y_2, \ldots,$$
$$S_n = X_1 + Y_1 + X_2 + Y_2 + \cdots + X_n + Y_n, \ldots$$

заканчиваются восстановления.

Промежутки между очередными отказами (с учетом времени восстановления) образуют общий процесс восстановления, образованный первой функцией распределения $F(t)$ и второй $(F*G)(t)$. Промежутки между очередными восстановлениями образуют простой процесс восстановления с функцией распределения $(F*G)(t)$ [2, 3].

Среднее число отказов и среднее число восстановлений определяются функциями восстановления $H_0(t) = HF(F*G)(t)$, $H_1(t) = H(F*G)(t)$ соответственно.

Пусть $D_0(t)$ дисперсия числа отказов, $D_1(t)$ дисперсия числа восстановлений. В соответствии с (4, 5) запишем формулы для дисперсий

$$D_0(t) = 2\int_0^t H(F*G)(t-x)dHF(F*G)(x) + H_0(t) - H_0^2(t),$$

$$D_1(t) = 2\int_0^t H(F*G)(t-x)dH(F*G)(x) + H_1(t) - H_1^2(t).$$

Отметим, что знание функции восстановления и дисперсии числа отказов дает возможность решать различные прикладные задачи, связанные с коэффициентом вариации и неравенством Чебышева.

Запишем коэффициент вариации $V(N(t))$ и неравенство Чебышева для процесса восстановления

$$V\left(N(t)\right) = \frac{\sigma\left(N(t)\right)}{H(t)},$$

($\sigma(N(t))$ – среднее квадратическое отклонение)

$$P(|N(t) - H(t)| \geq \int) \leq \frac{D(N(t))}{\int^2}.$$

Рассмотрим простой процесс восстановления при экспоненциальном распределении наработок $F(t)=1-e^{-\alpha t}$. В этом случае $H(t)=\alpha t$, $D(N(t))=\alpha t$ и

$$V\left(N(t)\right) = \frac{1}{\sqrt{\alpha t}}.$$

При увеличении времени эксплуатации коэффициент вариации уменьшается.

Положив $\int = 3\sqrt{D(N(t))}$ и переходя к противоположному событию в неравенстве Чебышева, получаем известную форму неравенства Чебышева, которая для процесса восстановления принимает вид

$$P\left(\left|N(t) - H(t)\right| < 3\sqrt{D\left(N(t)\right)}\right) \geq \frac{8}{9}.$$

Для простого процесса восстановления при экспоненциальном распределении наработок

$$P(|N(t) - \alpha t| < 3\sqrt{\alpha t}) \geq \frac{8}{9}.$$

Заключение. При работе технических и информационных систем, а также программных и программно-аппаратных средств защиты информации происходят отказы, возникают угрозы атак, угрозы безопасности и множество других воздействий, имеющих случайный характер, которые оказывают негативное влияние на их работу. Такие воздействия приводят к процессам восстановления. Число отказов, угроз атак и угроз надежности являются случайными величинами, зависящими от времени и от их функций распределения. Характер изменения этих функций распределения приводит к различным моделям процессов восстановления для которых разработаны методы нахождения математического ожидания (функции восстановления) числа отказов.

В работе для общего и альтернирующего процессов восстановления получена формула для дисперсии, зависящая от функции восстановления двух процессов – простого и общего. Предложен алгоритм вычисления функции восстановления для функций распределения наработок характерных для теории надежности. В качестве примеров получены выражения для дисперсий для простого, общего процесса при экспоненциальном распределении. Для этого случая выписано неравенство Чебышева и коэффициент вариации.

Отметим, что получение формул дисперсии числа отказов для других моделей процессов восстановления представляет самостоятельный интерес.

Наличие формул для среднего и дисперсии числа отказов и рассмотрение в процессе восстановления совместного изменения среднего и дисперсии числа отказов от функций распределения наработок до отказа восстанавливаемых элементов естественным образом приводит к рассмотрению новых оптимизационных задач в процессах восстановления. Например, минимизации дисперсии отказов при ограничении на величину среднего числа отказов во время эксплуатации, приводит к близкой по постановке известной задаче Марковица об оптимальном формировании пакета ценных бумаг [13, 14].

Таким образом, разработанный в работе математический аппарат найдет применение при постановке и решении различных оптимизационных задач информационной и компьютерной безопасности, а также при эксплуатации технических, информационных, социально-экономических, биологических и других систем, в условиях, когда возникновения отказов, имеют случайный характер.

Библиографический список

1. **Боровков А.А.** Теория вероятностей [Текст] / А.А. Боровков. – М.: Либроком, 2009. – 652 с.

2. **Байхельт Ф.** Надежность и техническое обслуживание. Математический подход [Текст]: [пер. с англ.] / Ф. Байхельт, П. Франкен. – М.: Радио и связь, 1988. – 392 с.

3. **Вайнштейн И.И.** Процессы и стратегии восстановления с изменяющимися функциями распределения в теории надежности [Текст] / И.И. Вайнштейн. – Красноярск: СФУ, 2016. – 189 с.

4. **Вайнштейн И.И.** О моделях процессов восстановления в теории надежности [Текст] / И.И. Вайнштейн, В.И. Вайнштейн, Е.А. Вейсов // Вопросы математического анализа: сб. науч. тр. / ред. В. И. Половинкин. ИПЦ КГТУ, Красноярск. – 2003. – Вып. 6. – С. 78-84.

5. **Булинская Е.В.** Асимптотическое поведение некоторых стохастических систем хранения [Текст] / Е.В. Булинская, А.И. Соколова // Современные проблемы математики и механики. – 2015. – С. 37-62.

6. **Анкудинов А.В.** Уравнение восстановления для процессов Кижима-Сумиты [Текст] / А.В. Анкудинов, А.В. Антонов, В.А. Чепурко // Надежность. – 2018. – №18(2). – С. 3-9.

7. **Чумаков И.А.** Некоторые свойства моделей неполного восстановления Кижима [Текст] / И.А. Чумаков, А.В. Антонов, В.А. Чепурко // Надежность. – 2015. – №3(54). – С. 3-15.

8. **Перегуда А.И.** Математическая модель надежности компьютерных сетей [Текст] / А.И. Перегуда, А.А. Перегуда, Д.А. Тимашев // Надежность. – 2013. – №4. – С. 18-43.

9. **Вайнштейн И.И.** Дисперсия числа отказов в моделях процессов восстановления технических и информационных систем. Оптимизационные задачи. [Текст] / И.И. Вайнштейн, В.И. Вайнштейн // Моделирование, оптимизация и информационные технологии. – 2019. – Том 7. – №3.

10. **Литвиненко Р.С.** Практическое применение непрерывных законов распределения в теории надежности технических систем [Текст] / Р.С. Литвиненко, П.П. Павлов, Р.Г. Идиятуллин // Надежность. – 2016. – №16(4). – С. 17-23.

11. **Вайнштейн В.И.** Численное нахождение функции восстановления для одной модели процесса восстановления [Текст] / В.И. Вайнштейн, Е.А. Вейсов, О.О. Шмидт // Вычислительные технологии. – 2005. – №10. – С. 4-9.

12. **Вайнштейн В.И.** Функции восстановления при распределении наработок элементов технических систем как смесь n функций распределения [Текст] / В.И. Вайнштейн // Современные наукоемкие технологии. – 2018. – №6. – С. 44-49.

13. **Markowits Harry M.** Portfolio Selection [Text] / Harry M. Markowits // Journal of Finance. – 1952. – Vol. 7. – №1. – P. 71-91.

14. **Касимов Ю.Ф.** Основы теории оптимального портфеля ценных бумаг [Текст] / Ю.Ф. Касимов. – М: Информационно-издательский дом «Филинъ», 1998. – 144 с.

Сведения об авторе

Виталий И. Вайнштейн – кандидат физико-математических наук, ФГАО ВО «Сибирский федеральный университет», доцент-заведующий НУЛ «Информационная безопасность» кафедры прикладной математики и компьютерной безопасности, Российская Федерация, Красноярский край, г. Красноярск, e-mail: vit037@mail.ru

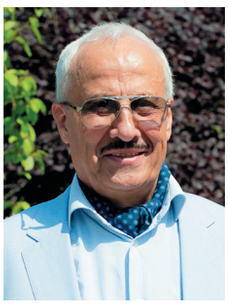
Вклад автора в статью

Получена формула для дисперсии числа отказов общего процесса восстановления и формулы для дисперсий числа отказов и числа восстановлений при альтернирующем процессе восстановления. Предложен алгоритм для нахождения дисперсии числа отказов в виде рядов для законов распределения наработок характерных для теории надежности.

Оригинальная статья
https://doi.org/10.21683/1729-2646-2019-19-4-17-23

Метод нормирования показателей надежности объектов железнодорожного транспорта

Игорь Б. Шубинский[1], Евгений О. Новожилов[1*]
[1]АО «НИИАС», Российская Федерация, Москва
[*]eo.novozhilov@vniias.ru



Игорь Б. Шубинский

Евгений О. Новожилов

Резюме. Цель. *Результаты оценки фактического состояния технической системы (объекта) позволяют принять решение о дальнейшей эксплуатации (продолжение эксплуатации, назначение ремонта, вывод из эксплуатации и замена объекта и т.п.). В условиях ресурсных ограничений актуально выявление наиболее «проблемных» объектов, требующих первоочередного инвестирования. Цель работы состоит в разработке метода нормирования показателей надежности, применение которого направлено на улучшение адресности распределения инвестиций на техническое содержание объектов, что позволяет обеспечить выполнение требований бесперебойности перевозочного процесса в условиях ресурсных ограничений.* **Методы.** *В работе применены методы системного анализа, теории вероятностей, математической статистики, корреляционного анализа. Предложена аппроксимация временного ряда фактических значений показателя надежности трехпараметрическим гамма-распределением на основе функции необеспеченности q(x).* **Результаты.** *В работе рассмотрены критерии выбора объектов инфраструктуры железнодорожного транспорта, требующих повышения надежности для случаев отсутствия и наличия нормируемого показателя надежности. Показано, что при введении нормирования показателей следует учитывать неодинаковые условия эксплуатации объектов в различных структурных подразделениях, что обусловлено различиями в климатических факторах, в оснащенности средствами технического обслуживания и ремонта, в укомплектованности персоналом, в степени износа объектов, в требованиях к их производительности. Проведен анализ условий совмещения требований поставщика и потребителя услуги по установлению нормативного значения показателя надежности. Показана целесообразность установления единственного порогового нормативного значения x показателя надежности, в этом случае нормативное значение x для признака x должно соответствовать требованиям как потребителя услуги, так и ее поставщика. При наличии единственного порогового значения риск $Q = P\{x > x\}$ несоответствия показателя установленным требованиям фактически распределяется между потребителем и поставщиком услуги в соответствии с их соглашением.* **Выводы.** *В статье предложен метод нормирования показателя надежности на основе статистических данных при допущении, что в целом за некоторый период наблюдения этот показатель можно оценить как приемлемый для потребителя услуги. Для выбора и обоснования нормативного значения показателя надежности рассмотрены взаимоотношения поставщика и потребителя услуги, проведен анализ статистики по методу оценки эмпирической обеспеченности ряда исходных данных, а также аппроксимация упорядоченного исходного ряда трехпараметрическим гамма-распределением. Приведен пример установления нормативного значения показателя интенсивности отказов объекта по критерию заданного риска его необеспечения на основе квантилей полученной функции обеспеченности. Показано, что предложенный подход позволяет установить взаимосвязь между задаваемым нормативом и риском его необеспечения через функцию обеспеченности, которая может быть получена на основе существующих статистических данных о надежности объекта за прошедшие периоды. Эта взаимосвязь позволяет гарантировать обеспечение соответствия фактических и нормативных значений показателя с заданным уровнем риска при функционировании объекта в штатном режиме.*

Ключевые слова: *показатель надежности, нормирование надежности; риск поставщика услуги; риск потребителя услуги; функция необеспеченности; трехпараметрическое гамма-распределение; квантиль распределения.*

Для цитирования: *Шубинский И.Б., Новожилов Е.О. Метод нормирования показателей надежности объектов железнодорожного транспорта // Надежность. 2019. № 4. С. 17-23. https://doi.org/10.21683/1729-2646-2019-19-4-17-23*

Поступила 02.10.2019 г. / После доработки 22.11.2019 г. / К печати 14.12.2019 г.

Введение

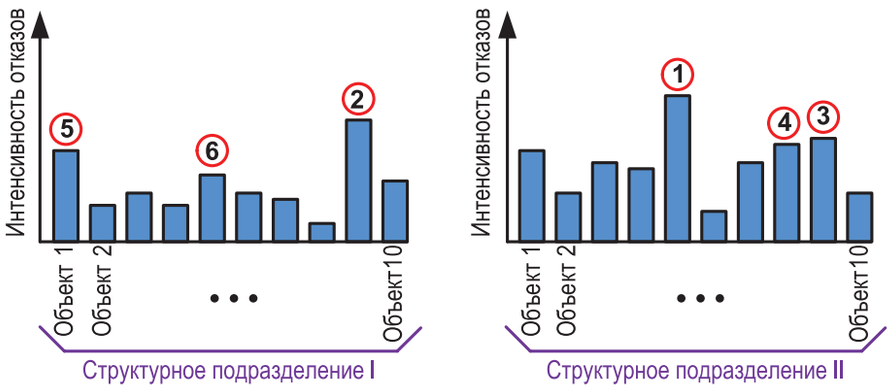
Для любой технической системы одной из важных задач является нормирование показателей надежности (например, допустимых значений показателей готовности, безотказности или ремонтопригодности) [1, 2]. Нормирование надежности – это установление (в технической или иной документации) количественных и качественных требований к надежности. Таким образом, нормирование устанавливает допустимые пределы изменения контролируемой характеристики.

Показатель надежности – это характеристика, как правило, количественная, одного или нескольких свойств, составляющих надежность технической системы (объекта). Значения показателей надежности могут быть нормативными или фактическими. Они могут определяться расчетными методами, по данным испытаний или экспериментов, по данным эксплуатации или путем экстраполирования. Фактические значения показателей надежности в процессе эксплуатации технической системы получают на основе анализа статистических данных об отказах системы и времени до ее восстановления. Что же касается нормативных значений показателей надежности, то они, как правило, численно задаются при проектировании объекта. Для большинства объектов применяется нормативный вероятностный подход, при котором нормируется и обеспечивается требуемый экономически обоснованный уровень вероятностных показателей надежности, который затем контролируется испытаниями на надежность и поддерживается с помощью системы технического обслуживания при эксплуатации. Исключение составляют критические ответственные объекты с катастрофическими последствиями отказов, отказы которых недопустимы (в данной статье такие объекты не рассматриваются, так как они относятся к сфере функциональной безопасности).

1. Цель нормирования показателей надежности

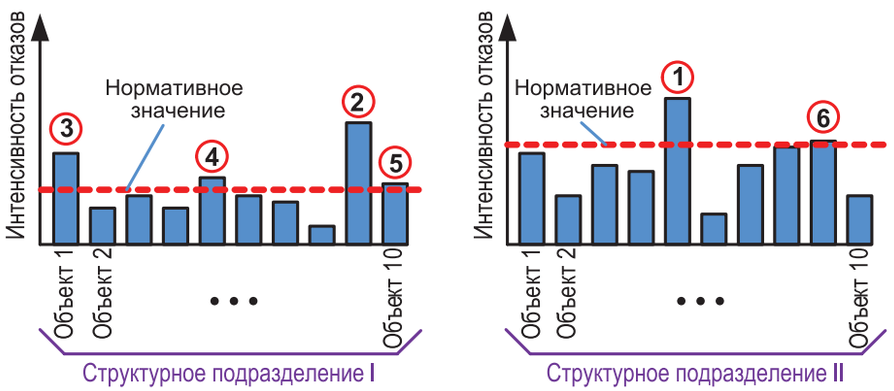
Результаты оценки фактического состояния объекта позволяют принять решение [3] о его дальнейшей эксплуатации (продолжение эксплуатации, назначение ремонта, вывод из эксплуатации и замена объекта и т.п.). В условиях ресурсных ограничений является актуальным выявление наиболее «проблемных» объектов, требующих первоочередного инвестирования.

На рисунке 1 а и 1 б показан пример определения приоритетности объектов инфраструктуры железнодорожного транспорта, требующих повышения надежности, например, путем назначения и проведения ремонта, для двух структурных подразделений, в которых объекты одного вида находятся в различных эксплуатационных условиях. В данном примере мы считаем, что на два



а) б)

Рисунок 1 – Пример определения приоритетности объектов для назначения ремонта (без применения нормирования).



а) б)

Рисунок 2 – Пример определения приоритетности объектов для назначения ремонта (с применением нормирования).

структурных подразделения выделены средства на проведение ремонта 6 объектов.

Рисунок 1 показывает, что на основе фактических значений показателя надежности (например, интенсивности отказов), отражающего текущее состояние объекта в процессе его эксплуатации, можно определить те объекты, которые требуют назначения ремонта в приоритетном порядке, с учетом выделенного финансирования. В этом случае, при отсутствии нормативных значений, объекты выбираются по критерию наихудшего значения показателя.

При введении нормирования показателей следует учитывать неодинаковые условия эксплуатации объектов в различных структурных подразделениях, что обусловлено различиями в климатических факторах, в оснащенности средствами технического обслуживания и ремонта, в укомплектованности персоналом, в степени износа объектов, в требованиях к их производительности (например, при различных размерах движения поездов). В таком случае объекты для назначения ремонта будут выбираться по критерию отклонения показателя в худшую сторону от нормативного значения (рис. 2 а и 2 б).

Очевидно, что при введении нормирования показателей с учетом условий эксплуатации объектов и ряда других факторов деятельности подразделений улучшается адресность распределения инвестиций на техническое содержание объектов, что позволяет обеспечить выполнение требований бесперебойности перевозочного процесса в условиях ресурсных ограничений [4].

2. Интересы потребителя и поставщика услуги

В случае, когда техническая система участвует в процессе предоставления услуг (например, объект железнодорожной инфраструктуры обеспечивает выполнение перевозочного процесса), нормативные значения показателей надежности должны учитывать отношения между поставщиком и потребителем услуги (например, структурным подразделением, отвечающим за функционирование объекта железнодорожной инфраструктуры и структурным подразделением, выполняющим перевозочный процесс).

Следует отметить, что в этой схеме неизбежно существует конфликт интересов потребителя и поставщика услуги. С одной стороны, потребитель заинтересован в том, чтобы отказов объекта, предоставляющего услугу, не было вообще; это позволило бы ему осуществлять свою деятельность с полным отсутствием риска, связанного с отказом объекта (например, риска потери поездо-часов по причине отказа объекта железнодорожной инфраструктуры). С другой стороны, поставщик заинтересован в том, чтобы сократить расходы на предоставление услуги, тем самым увеличив прибыль от своей деятельности; но при сокращении расходов неизбежно возрастание количества отказов объекта. Нормирование показателей надежности объекта в сути своей должно обеспечить компромисс между интересами поставщика, стремящегося обеспечить предоставление услуги в условиях ресурсных ограничений, и интересами потребителя, стремящегося получить услугу с высоким качеством при наименьших затратах.

Рассматриваемая ситуация аналогична той, в которой потребитель принимает у поставщика партию товара и где однозначность взаимного признания качества продукции между поставщиком и потребителем в большинстве случаев регулируется с помощью методов статистического приемного контроля. При этом отношения между поставщиком и потребителем характеризуют приемлемый уровень качества x_α (предельно допустимое значение доли дефектных изделий в партии) и браковочный уровень качества x_β (граница доли дефектных изделий для отнесения партии продукции к браку), где $x_\alpha \le x_\beta$ (рис. 3). Таким образом, область интересов потребителя

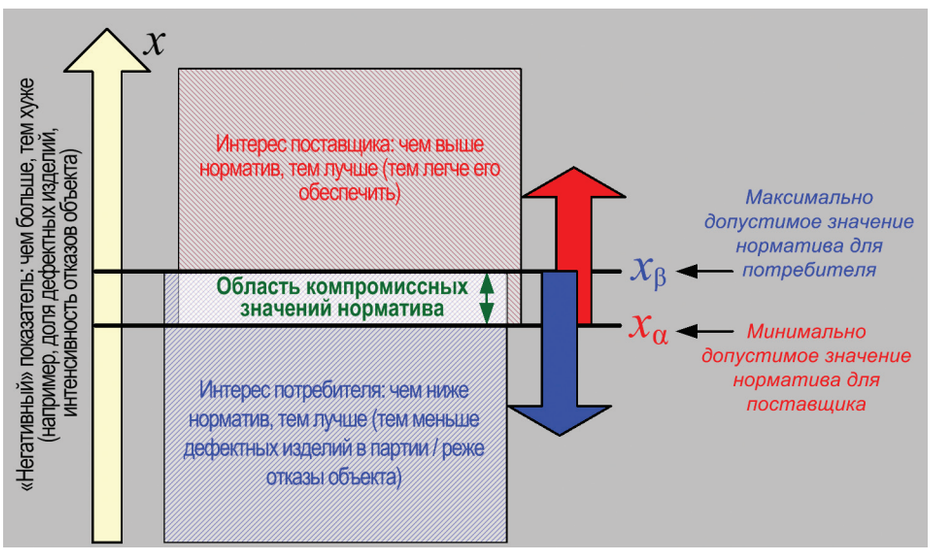


Рисунок 3 – Области интересов потребителя и поставщика услуги.

$x \le x_\beta$, а область интересов поставщика $x > x_\alpha$; очевидно, что эти две области пересекаются, что является необходимым условием для существования компромисса обоих интересов. Область значений признака x ниже x_α является «зоной приемки», выше x_β – «зоной браковки», а между x_α и x_β – «зоной неопределенности».

Отметим, что применение двух точек (x_α, x_β) в качестве пороговых значений является обычной практикой при последовательном выборочном контроле [5], где вывод о годности (или негодности) партии делается на основе доли дефектных изделий в выборке, являющейся частью объема партии. Для этого процесса приемлемый и браковочный уровень качества задают с применением доверительных границ. Вероятность того, что доля дефектных изделий во всей партии составляет не более x_α, когда при контроле выборки был превышен верхний доверительный интервал браковочного уровня, является риском поставщика; напротив, вероятность того, что доля дефектных изделий во всей партии составляет более x_β, когда при контроле выборки был достигнут нижний доверительный интервал приемочного уровня, является риском потребителя.

Из рис. 3 следует, что: поставщик услуги может гарантировать, что фактическое значение x показателя будет находиться выше порогового значения x_α с высокой степенью доверия (вероятностью), например, $P_\alpha = P\{x > x_\alpha\} > 0{,}95$ (риск поставщика $Q_\alpha = 1 - P_\alpha \le 0{,}05$ (ГОСТ Р ИСО 8422-2011. Статистические методы. Последовательные планы выборочного контроля по альтернативному признаку); потребитель услуги ожидает, что фактическое значение x показателя будет не выше порогового значения x_β с высокой степенью доверия (вероятностью), например, $P_\beta = P\{x \le x_\beta\} > 0{,}9$ (риск потребителя $Q_\beta = 1 - P_\beta \le 0{,}1$).

В реальных условиях эксплуатации технической системы задача оценки ее соответствия заданным требованиям надежности чаще всего сводится к сравнению полученного за некоторый интервал наблюдения по статистическим эксплуатационным данным значения фактического показателя надежности с установленным (в технической или другой документации) нормативным значением. В этом случае наличие «зоны неопределенности» будет затруднять оценку, делая ее неоднозначной. Поэтому в технической документации на объект, как правило, задается нормативное значение показателя в виде единственного порогового значения (например: «средняя наработка на отказ с учетом технического обслуживания должна быть не менее 30 000 ч»).

Пусть для показателя надежности объекта по согласованию между потребителем и поставщиком услуги устанавливается единственное пороговое нормативное значение x_η, тогда будем считать, что при $x \le x_\eta$ данный объект соответствует требованиям, а при $x > x_\eta$ – не соответствует. Очевидно (см. рис. 3), что при переходе от двух пороговых уровней к одному целесообразно выполнение условия $x_\alpha < x_\eta \le x_\beta$ (x_η находится в области «компромиссных значений»), в этом случае нормативное значение x_η для признака x удовлетворит требования как потребителя услуги, так и ее поставщика.

При наличии единственного порогового значения риск $Q_\eta = P\{x > x_\eta\}$ несоответствия показателя установленным требованиям фактически распределяется между потребителем и поставщиком услуги в соответствии с их соглашением (например, превышение норматива на одном интервале наблюдения является риском потребителя, а на двух и более следующих подряд интервалах наблюдения – относится на ответственность поставщика).

Одним из путей нормирования показателей надежности, применяемых в мировой практике (в частности, в сфере электроснабжения) является нормирование на основе прошлого опыта (анализа фактических данных о надежности) [5]. Учитывая наличие таких данных на железнодорожном транспорте, будем считать дальнейшей задачей выбор и обоснование значения x_η с применением имеющихся статистических данных о функционировании объекта на протяжении некоторого интервала наблюдения при допущении, что в целом за этот интервал показатели надежности объекта можно оценить как приемлемые для потребителя услуги.

3. Анализ статистических данных и оценка их обеспеченности

Как было отмечено выше, фактические значения показателей надежности являются случайными величинами. Например, для интенсивности отказов объекта (количества отказов в единицу времени) статистика представляет собой временной ряд дискретных значений – например, это последовательность значений количества отказов, произошедших в каждом годовом интервале наблюдения, за несколько лет.

Случайная величина полностью определяется законом распределения, для дискретных величин – это ряд распределения или дискретная функция распределения. Ряд распределения (или дискретная функция распределения) представляет собой таблицу возможных значений случайной величины с соответствующими вероятностями.

Существует очень большое количество различных теоретических законов распределения (равномерный, Бернулли, Коши, Пуассона, нормальный, логнормальный, Гумбеля, Джонсона, 13 кривых распределения Пирсона и др.) [6]. Но на практике часто приходится иметь дело со статистическим материалом весьма ограниченного объема, на основе которого определить конкретный закон распределения для случайной величины не всегда возможно. В таких случаях необходимо описать поведение случайной величины числовыми характеристиками.

При инженерных расчетах и научных исследованиях применяются эмпирические кривые распределения характеристик случайных величин. Основными этапами при построении таких кривых являются ранжирование

исходного временного ряда и оценка его эмпирической обеспеченности. Решение первой из этих задач не представляет сложностей, а второй – требует учитывать, что некоторые формулы для оценки обеспеченности приводят к систематическим погрешностям и дают различные значения случайных погрешностей.

Функция необеспеченности $q(x)$ является аналогом функции распределения $F(x)$ и характеризует вероятность того, что значение аргумента превышает заданное пороговое значение. В работе [7] на основании теоретических исследований и результатов испытаний определена формула, которая дает состоятельные, несмещенные и эффективные значения оценок необеспеченности i-го ($i = 1…n$) члена ранжированной по убыванию дискретной выборки (то есть, вероятностей q_i того, что фактическое значение x превышает значение члена ряда x_i):

$$q_i = P\{x > x_i\} = \frac{i}{n+1}, \quad (1)$$

где n – количество членов ряда.

Рассмотрим алгоритм, включающий ранжирование исходного временного ряда, оценку его эмпирической обеспеченности и аппроксимацию теоретическим законом распределения на примере статистических данных по отказам объектов первичной сети железнодорожной электросвязи за период 2008–2016 гг. (таблица 1, данные предоставлены Центральной станцией связи – филиалом ОАО РЖД).

1) Исходный ряд ранжируется в порядке убывания значений показателя. Вместо годов наблюдения вводятся условные номера членов ранжированного ряда (1, 2, 3, …).

2) Для каждого члена ранжированного ряда по формуле (1) рассчитываются значения q_i функции необеспеченности.

3) Вычисляется математическое ожидание $\overline{x}$ членов ряда.

4) Для каждого члена ранжированного ряда рассчитывается модульный коэффициент, равный отношению значения члена ряда к математическому ожиданию ряда.

В результате получаем таблицу 2.

5) С целью уточнения значений квантилей распределения (q), особенно на уровнях, меньших, чем 0,2, представляющих практический интерес, выполняется аппроксимация ряда модульных коэффициентов таблицы 2 одним из теоретических законов распределения. В качестве примера рассмотрим аппроксимацию трехпараметрическим гамма-распределением [9], которое получило применение, в частности, в гидрологических расчетах [10] и в расчетах ресурса конструкций при случайных потоках нагрузок [11].

С применением модульных коэффициентов k_i из таблицы 2 рассчитываются коэффициент C_v вариации ряда и отношение C_{sv} коэффициента асимметрии ряда к коэффициенту вариации ряда:

$$C_v = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(\frac{x_i}{\overline{x}}-1\right)^2}, \; C_{sv} = \frac{n\sum_{l=1}^{L}\left(\frac{x_i}{\overline{x}}-1\right)^3}{(n-1)(n-2)C_v^4}, \quad (2)$$

при этом если в (2) получено значение $C_v < 0{,}1$, то перед расчетом C_{sv}, а также для дальнейшего применения, принимают $C_v = 0{,}1$ (поскольку для рядов с очень малой вариацией определение квантилей распределения затруднительно). После расчетов значение C_v округляется до кратности 0,1 (0,1; 0,2; 0,3 …), а значение C_{sv} – до кратности 0,5 (0; ±0,5; ±1,0; ±1,5; …) для возможности применения существующих табличных значений функций распределения ввиду того, что их аналитический расчет является очень сложным.

По табличным значениям функций трехпараметрического гамма-распределения [9] для заданной вероятности необеспечения q_i определяется ордината m_i в виде модульного коэффициента (указанные таблицы содержат значения функции распределения для различных значений C_v и наиболее распространенных отношений C_s/C_v).

В рассматриваемом примере для полученных по формулам (2) значений $C_v = 0{,}5$ и $C_{sv} = 0$ имеем ряд значений ординат функции в виде модульных коэффициентов $m_i(p_i)$, включая дополнительные значения на краях функции (таблица 3). Для получения количественных значений y_i интенсивности отказов, которые будут превышены с вероятностью q_i, следует умножить

Таблица 1 – Исходный временной ряд интенсивности отказов объекта

Год наблюдения	2008	2009	2010	2011	2012	2013	2014	2015	2016
Интенсивность отказов, x_i, 1/год	34	37	24	17	12	9	13	43	36

Таблица 2 – Ранжированный временной ряд с оценками обеспеченности и модульными коэффициентами

№ п/п, i	1	2	3	4	5	6	7	8	9
Интенсивность отказов, x_i, 1/год	83	76	37	34	24	14	13	12	9
Мод. к-т, k_i	2,4735	2,2649	1,1026	1,0132	0,7152	0,4172	0,3874	0,3576	0,2682
Необеспеченность, q_i	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9

Таблица 3 – Пример аппроксимированного временного ряда с оценками необеспечения и модульными коэффициентами (C_v = 0,8 и C_{sv} = 1,4)

№ п/п, i	-	-	1	2	3	4	5	6	7	8	9	-	-
q_i	0,01	0,05	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	0,95	0,99
Мод. к-т, m_i	2,01	1,8	1,66	1,47	1,31	1,16	1,01	0,855	0,69	0,511	0,305	0,182	0,055
Интенсивность отказов, y_i, 1/год	50,25	45	41,5	36,75	32,75	29	25,25	21,38	17,25	12,78	7,625	4,55	1,375

модульные коэффициенты m_i на значение $\overline{x}$ математического ожидания ранжированного ряда из таблицы 2 (результаты показаны в таблице 3).

Оценка достоверности аппроксимации выполнялась по коэффициенту линейной корреляции эмпирической $x_i(q_i)$ и подобранной по данному методу $y_i(q_i)$ (для i = 1…9) функций. Получено значение коэффициента линейной корреляции 0,974, оно является близким к 1, что подтверждает близость выбранной функции к исходному ряду с высокой достоверностью.

График эмпирического ряда (точки) и аппроксимирующей функции трехпараметрического гамма-распределения (сплошная линия) показан на рис. 4.

4. Выбор и обоснование нормативного значения показателя

Полученные выше результаты оценки обеспеченности (см. таблицу 3) могут быть применены для определения порогового значения x_η по заданному уровню риска Q_η, установленного по соглашению между поставщиком и потребителем услуги, или же, наоборот, для оценки риска Q_η на основе заданного x_η.

Рассмотрим случай, когда для заданного уровня риска необеспечения нормативного значения (например, Q_η = 0,1) требуется определить нормативное значение x_η показателя надежности (в нашем примере это – интенсивность отказов объекта).

Оценим квантиль функции обеспеченности, который соответствует заданному риску ($q_i = Q_\eta = 0{,}1$). Согласно данным таблицы 3 имеем:

$$y(Q_\eta) = y(q_1 = 0{,}1) = 70{,}8 \approx 71.$$

Следовательно, в качестве нормативного значения показателя можно принять значение интенсивности отказов, равное 71 1/год, которое будет не обеспечено с риском 0,1.

В случае если по соглашению между поставщиком и потребителем услуги установлено нормативное значение показателя надежности, аналогичным путем, на основе полученных результатов оценки обеспеченности (см. таблицу 3) можно определить риск несоответствия показателя установленным требованиям.

В любом случае соглашение между поставщиком услуги и ее потребителем должно предусматривать установление как нормативного значения всех рассматриваемых показателей надежности, так и уровней риска, с которыми

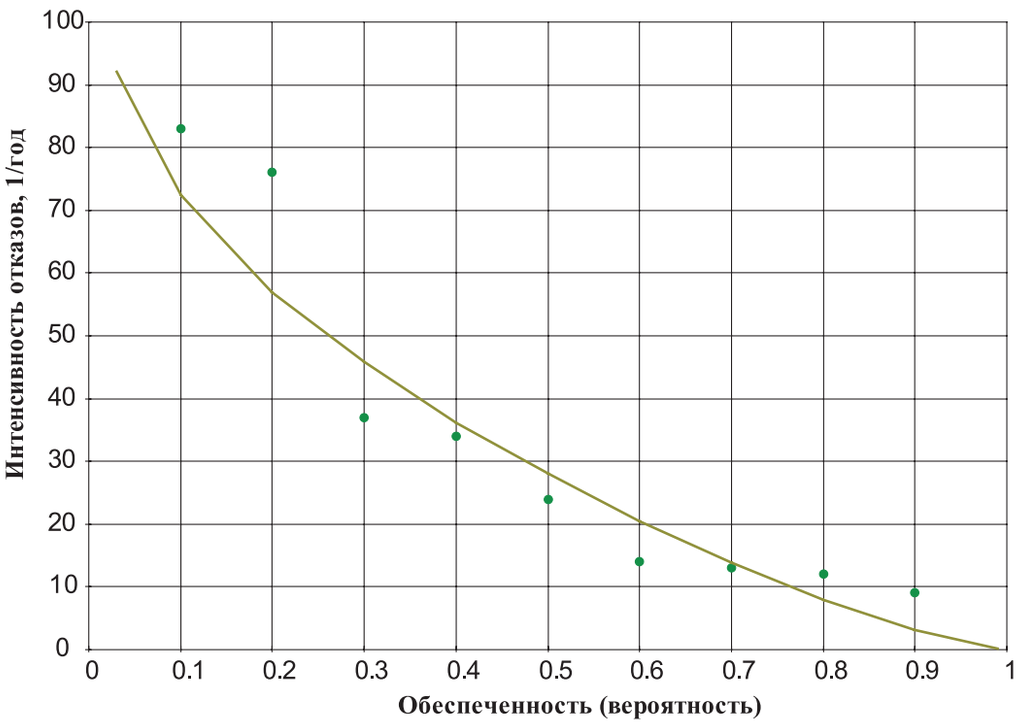


Рисунок 4 – График эмпирического ряда (точки) и аппроксимирующей функции (сплошная линия).

данные нормативные значения могут быть не обеспечены, а также порядок распределения ответственности между поставщиком и потребителем услуги.

Метод, рассмотренный в данной статье, позволяет с применением объективных критериев установить связь между значением нормативного показателя надежности и риском его необеспечения на основе реальных возможностей эксплуатируемых объектов, которые оцениваются по существующим статистическим данным за прошедшие периоды.

Заключение

В данной статье рассмотрен метод нормирования показателя надежности на основе статистических данных при допущении, что в целом за некоторый период наблюдения этот показатель можно оценить как приемлемый для потребителя услуги.

Для выбора и обоснования нормативного значения показателя надежности рассмотрены взаимоотношения поставщика и потребителя услуги, проведен анализ статистики по методу оценки эмпирической обеспеченности ряда исходных данных, а также аппроксимация упорядоченного исходного ряда трехпараметрическим гамма-распределением. Рассмотрен пример установления нормативного значения показателя интенсивности отказов объекта по критерию заданного риска его необеспечения на основе квантилей полученной функции обеспеченности.

Проведенное рассмотрение показало, что предложенный подход позволяет установить взаимосвязь между устанавливаемым нормативом и риском его необеспечения через функцию обеспеченности, которая может быть получена на основе существующих статистических данных о надежности объекта за прошедшие периоды. Эта взаимосвязь позволяет гарантировать обеспечение соответствия фактических и нормативных значений показателя с заданным уровнем риска при функционировании объекта в штатном режиме.

Библиографический список

1. **Долганов А.И.** О назначении уровня надежности [Текст] / А.И. Долганов, А.В. Сахаров // Надежность. – 2018. – Том 18, № 3. – С. 18–21.

2. **Кувашов Ю.А.** Метод оценки технической готовности железнодорожного пути к обеспечению перевозочного процесса [Текст] / Ю.А. Кувашов, Е.О. Новожилов // Надежность. – 2017. – Том 17, № 2. – С. 17–23.

3. **Семенов С.С.** Обзор методов принятия решений при разработке сложных технических систем [Текст] / С.С. Семенов, А.В. Полтавский, В.В. Маклаков и др. // Надежность. – 2014. – № 3. –С. 72-96.

4. **Гапанович В.А.** Система адаптивного управления техническим содержанием инфраструктуры железнодорожного транспорта (проект УРРАН) [Текст] / В.А. Гапанович, И.Б. Шубинский, Е.Н. Розенберг и др. // Надежность. – 2015. – № 2. – С. 4–22.

5. **Руденко Ю.Н.** О подходах к нормированию показателей надежности электроснабжения потребителей [Текст] / Ю.Н. Руденко // Известия Академии наук СССР. Энергетика и транспорт. – 1975. – № 1. – С. 14–23.

6. **Литвиненко Р.С.** Практическое применение непрерывных законов распределения в теории надежности технических систем [Текст] / Р.С. Литвиненко, П.П. Павлов, Р.Г. Идиятуллин // Надежность. – 2016. – Том 16, № 4. – С. 17–23.

7. **Девид Г.** Порядковые статистики [Текст] / Г. Девид. – М.: Наука, 1979. – 336 с.

8. **Вадзинский Р.Н.** Справочник по вероятностным распределениям [Текст] / Р. Н. Вадзинский. – СПб: Наука, 2001. – 295 с., ил. 116.

90. **Сикан А.В.** Методы статистической обработки гидрометеорологической информации [Текст] / А.В. Сикан. – СПб.: РГГМУ, 2007. – 279 стр.

10. **Гусев А.С.** Сопротивление усталости и живучести конструкций при случайных нагрузках [Текст] / А.С. Гусев. – М.: Машиностроение, 1989. – 248 с.: ил.

Сведения об авторах

Игорь Б. Шубинский – доктор технических наук, профессор, заместитель руководителя НТК АО «НИИАС», Москва, Российская Федерация, тел. +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

Евгений О. Новожилов – кандидат технических наук, начальник отдела АО «НИИАС», Москва, Российская Федерация, тел. +7 (495) 967-77-02, e-mail: eo.novozhilov@vniias.ru

Вклад авторов в статью

Шубинский И.Б. Выполнил обзор и анализ существующего состояния рассматриваемой проблемы, определил теоретические составляющие работы, применяемые математические методы.

Новожилов Е.О. Выполнил анализ существующих подходов к нормированию показателей надежности. Предложил алгоритм нормирования показателя надежности, выполнил расчет примера.

УДК 681.5.015:007
Оригинальная статья
Надежность, том 19, №4, 2019 https://doi.org/10.21683/1729-2646-2019-19-4-24-31

Нечеткие когнитивные карты в анализе надежности систем

Александр П. Ротштейн, *Иерусалимский политехнический институт – Махон Лев, Иерусалим, Израиль; Донецкий национальный университет им. В.Стуса, Винница, Украина*

Александр П. Ротштейн

Резюме. Цель. *Начальным этапом моделирования надежности сложной системы является ее структуризация, т.е. разбиение на составные части (блоки, узлы, элементы), для которых известны вероятности отказов. Классическая теория надежности использует понятие структурной функции, которая позволяет ранжировать элементы по важности, что необходимо для оптимального распределения ресурсов, выделенных на обеспечение надежности системы. Для структуризации человеко-машинных систем используется алгоритмическое описание дискретных процессов функционирования, где наличие четких границ между отдельными операциями позволяет собирать статистику о вероятностях ошибок, необходимую для моделирования. Трудности алгоритмизации возникают в человеко-машинных системах с непрерывным характером деятельности человека, где отсутствие четких границ между операциями не позволяет корректно оценивать вероятности их правильного выполнения. Поэтому процесс функционирования приходится рассматривать как единую операцию, правильность выполнения которой зависит от разнородных и взаимосвязанных эргатических, технических, программных, организационных и других факторов. Моделируемая система превращается в «черный ящик» с неизвестной структурой (выход – надежность, входы – влияющие факторы), а традиционная для теории надежности задача ранжирования элементов сводится к задаче ранжирования факторов. Наиболее популярным средством многофакторного моделирования надежности человеко-машинных систем является регрессионный анализ. Он требует большого числа экспериментальных данных и не приспособлен к работе с качественными факторами, измеряемыми экспертно. Удобным средством обработки экспертной информации являются нечеткие правила «если – то». Однако регрессионный анализ и нечеткие правила обладают общим ограничением: они предполагают независимость входных переменных, т.е. влияющих факторов. Этого ограничения лишены нечеткие когнитивные карты – новое средство моделирования, пока не получившее распространения в теории надежности. Цель статьи – привлечь внимание к моделированию надежности с помощью нечетких когнитивных карт.* **Метод.** *На основе теории нечетких когнитивных карт предлагается метод ранжирования факторов, влияющих на надежность системы. В основу метода положена формализация причинно-следственных связей «влияющие факторы – надежность» в виде нечеткой когнитивной карты, т.е. ориентированного графа, вершины которого соответствуют надежности системы и влияющим факторам, а взвешенные дуги отражают силы влияний факторов друг на друга и на надежность системы. Ранг фактора определен как аналог индекса важности элемента по Бирнбауму, который в вероятностной теории надежности вычисляется на основе структурной функции.* **Результаты.** *Предлагаются модели и алгоритмы вычисления индексов важности единичных факторов и их парных эффектов, влияющих на надежность системы, представленной нечеткой когнитивной картой. Метод иллюстрируется на примере надежности и безопасности автомобиля в системе «водитель-автомобиль-дорога» с учетом квалификации водителя, дорожных условий, удельных затрат на эксплуатацию, условий эксплуатации, периодичности технического обслуживания, качества обслуживания и ремонта, качества конструкции автомобиля, качества эксплуатационных материалов и запасных частей, а также условий хранения.* **Выводы.** *Достоинствами метода являются: а) использование доступной экспертной информации без сбора и обработки статистических данных; б) возможность учета любых количественных и качественных факторов, связанных с человеком, техникой, программным обеспечением, качеством обслуживания, условиями эксплуатации и других; в) простота расширения числа учитываемых факторов за счет введения дополнительных вершин и дуг графа когнитивной карты. Возможными объектами применения метода могут быть сложные системы с нечетко определенной структурой, надежность которых сильно зависит от взаимосвязанных факторов, измеряемых экспертно.*

Ключевые слова: *нечеткая когнитивная карта, надежность системы, влияющие факторы, ранжирование факторов, надежность и безопасность автомобиля.*

Для цитирования: *Ротштейн А.П. Нечеткие когнитивные карты в анализе надежности систем // Надежность. 2019. № 4. С. 24-31. https://doi.org/10.21683/1729-2646-2019-19-4-24-31*

Поступила 13.04.2019 г. / После доработки 22.09.2019 г. / К печати 14.12.2019 г.

1. Введение

Успех в решении прикладных задач моделирования в значительной мере определяется выбором математического аппарата. Теория вероятности, лежащая в основе классической теории надежности, плохо приспособлена к формализации экспертных знаний, которые могут быть полезными для принятия решений.

Цель этой статьи – привлечь внимание к моделированию надежности с помощью нечетких когнитивных карт. В ней приводятся основные соотношения этого аппарата и на их основе предлагается метод ранжирования факторов, влияющих на надежность системы. Метод иллюстрируется на примере моделирования надежности и безопасности автомобиля с учетом технических, эргатических, средовых и организационных факторов.

2. Структуризация: от элементов к факторам

Начальным этапом моделирования надежности сложной системы является ее структуризация, т.е. разбиение на составные части (блоки, узлы, элементы), для которых известны вероятности отказов.

Классическая теория надежности [1] использует понятие структурной (логической) функции, которая связывает логическое условие работоспособности системы (1 – нет отказа, 0 – есть отказ) с аналогичными условиями для ее элементов. Переход от структурной функции к вероятностной модели надежности осуществляется по правилам логико-вероятностного исчисления [2]. Структурная функция позволяет ранжировать элементы по важности, что необходимо для оптимального распределения ресурсов, выделенных на обеспечение надежности системы.

Для структуризации человеко-машинных систем используется алгоритмическое описание процессов функционирования [3, 4]. В этом случае исходными данными для расчета надежности являются вероятности правильного выполнения основных, контрольных и диагностических операций. Правила перехода от логико-алгоритмического описания системы на языке алгебры алгоритмов В.М. Глушкова [5] к вероятностным и нечетким моделям надежности предложены в [6, 7].

Алгоритмическое описание является естественным способом формализации систем с дискретными процессами функционирования, например, автоматизированных систем обработки данных и управления, сборочно-монтажного производства и других, где наличие четких границ между отдельным операциями позволяет собирать статистику о вероятностях ошибок, необходимую для моделирования.

Трудности алгоритмизации возникают в человеко-машинных системах с непрерывным характером деятельности человека, где преобладают операции слежения и принятия решений. Примерами служат системы управления на транспорте, в химической и ядерной промышленности и другие системы с повышенной опасностью, где ошибки человека приводят к катастрофическим последствиям.

Отсутствие четких границ между операциями не позволяет корректно оценивать вероятности их правильного выполнения. Поэтому весь процесс функционирования приходится рассматривать как единую операцию, правильность выполнения которой зависит от многих разнородных и взаимосвязанных факторов: эргатических, технических, программных, организационных и других. Моделируемая система представляет собой «черный ящик» с неизвестной структурой: выход – надежность, входы – влияющие факторы. В этом случае традиционная для теории надежности задача ранжирования элементов превращается в задачу ранжирования факторов. В частности, в [8] отмечается, что трудности учета влияющих факторов приводят к невозможности точного прогнозирования вероятности отказа, что вызывает недоверие к расчетам надежности.

Наиболее популярным средством многофакторного моделирования надежности человеко-машинных систем является регрессионный анализ (см. например, [9]). Он требует большого числа экспериментальных данных и не приспособлен к работе с качественными факторами, измеряемыми экспертно. Удобным средством обработки экспертной информации являются нечеткие правила «если – то» [10]. Регрессионный анализ и нечеткие правила обладают общим ограничением: они предполагают независимость входных переменных, т.е. влияющих факторов. Этого ограничения лишены нечеткие когнитивные карты (НКК) [10] – новое средство моделирования, пока не получившее распространения в теории надежности.

Ниже приводятся основные соотношения НКК и на их основе предлагается метод ранжирования факторов, влияющих на надежность и безопасность системы. Для иллюстрации метода используется система «водитель-автомобиль-дорога».

3. Основные понятия и соотношения

3.1. Общие замечания

НКК введены Б. Коско [11] как обобщение бинарных когнитивных карт Р. Аксельрода [12], предназначенных для моделирования динамики причинно-следственных связей в социально-политических системах. НКК представляет собой ориентированный граф со взвешенными дугами, пример которого показан на рис. 1. Вершины графа C_i, называемые *концептами*, соответствуют входным и выходным переменным, которые учитываются в модели. Взвешенные дуги графа отражают *силу влияния* w_{ij} изменения одной переменной C_i на изменение другой C_j.

Термин «когнитивный» говорит о том, что исходными данными для моделирования служат субъективные

мнения эксперта, выраженные словами типа «повышается» или «понижается», например: «повышение C_i приводит к понижению C_j». В бинарных когнитивных картах [12] «повышение» оценивается как «+1», а «понижение» – как «–1».

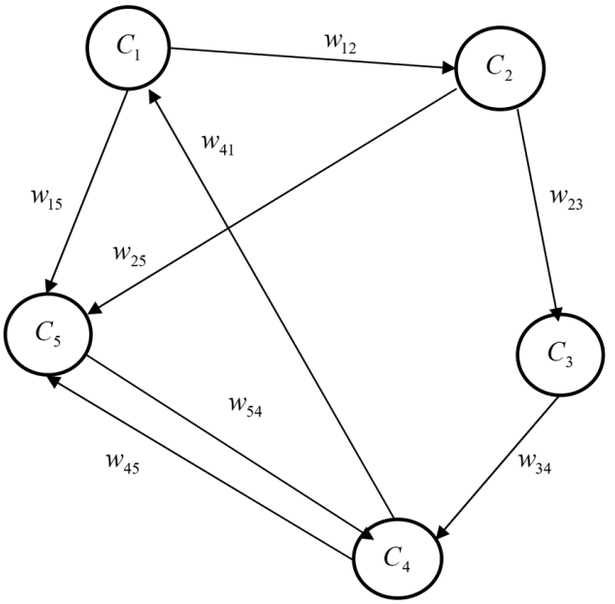


Рисунок 1 – Пример нечеткой когнитивной карты.

Термин «нечеткие» говорит о том, что НКК [11] используют различные уровни «повышения» и «понижения». Они задаются числами из интервалов [0, 1] и [–1, 0], что соответствует термам «слабо», «средне», «сильно» и др. из теории нечетких множеств [10].

С точки зрения теории идентификации [13, 14], которая занимается восстановлением закономерностей по экспериментальным данным, НКК – это аппроксиматор зависимости «входы – выход» с взаимодействующими входами. Как и любой аппроксиматор, например регрессия, нечеткие правила, нейронная сеть и другие, НКК содержит настраиваемые параметры, которые должны оцениваться путем минимизации невязки между модельными и экспериментальными значениями выхода. Если экспериментальные данные «входы – выход» отсутствуют, то качество модели целиком зависит от квалификации эксперта. Искусство моделирования состоит в том, чтобы компенсировать недостающие экспериментальные данные за счет высокого качества экспертных оценок.

Уместно сопоставить НКК и марковские цепи (процессы), привычные специалистам по надежности. Оба вида моделей – это взвешенные ориентированные графы. В основе отличия НКК от марковских моделей надежности лежит принципиальное различие нечеткой логики (причин) и теории вероятности (следствий), показанное на рис. 2: марковские модели отражают динамику вероятностей состояний системы с учетом отказов и восстановлений; НКК моделируют динамику изменения уровней взаимодействующих факторов, которые являются причинами отказов и влияют на вероятность их возникновения.

3.2. Концепты

Пусть $C=\{C_1, C_2, \ldots, C_n\}$ – известное множество концептов, т.е. переменных, используемых в модели. Согласно [11], каждый концепт $C_i \in C$ оценивается величиной $A_i \in [0,1]$, которая определяет уровень концепта и задается экспертно. Для получения величины A_i предлагается следующий способ.

Каждый концепт $C_i \in C$ будем считать лингвистической переменной [10], которая оценивается величиной x_i на универсальном множестве – интервале $\left[\underline{x}_i, \overline{x}_i\right]$, где $\underline{x}_i$ ($\overline{x}_i$) – нижняя (верхняя) граница. Для оценки концепта $C_i \in C$ будем использовать нечеткий терм «перфектность концепта C_i», который обозначается PC_i и представляет собой нечеткое множество

$$PC_i = \int_{\left[\underline{x}_i, \overline{x}_i\right]} \pi\left(x_i\right) / x_i,$$

где $\pi(x_i)$ – функция принадлежности переменной x_i к понятию «перфектность концепта C_i». С помощью этой функции каждой абсолютной оценке $x_i \in \left[\underline{x}_i, \overline{x}_i\right]$ ставится в соответствие число $A_i=\pi(x_i)\in[0,1]$, которое характеризует степень близости значения концепта $C_i \in C$ к некоторому идеалу: 0 – наименьшая перфектность, 1 – наибольшая перфектность. Синонимом понятия «нечеткая перфектность» является терм «нечеткая правильность», для которого функции принадлежности рас-

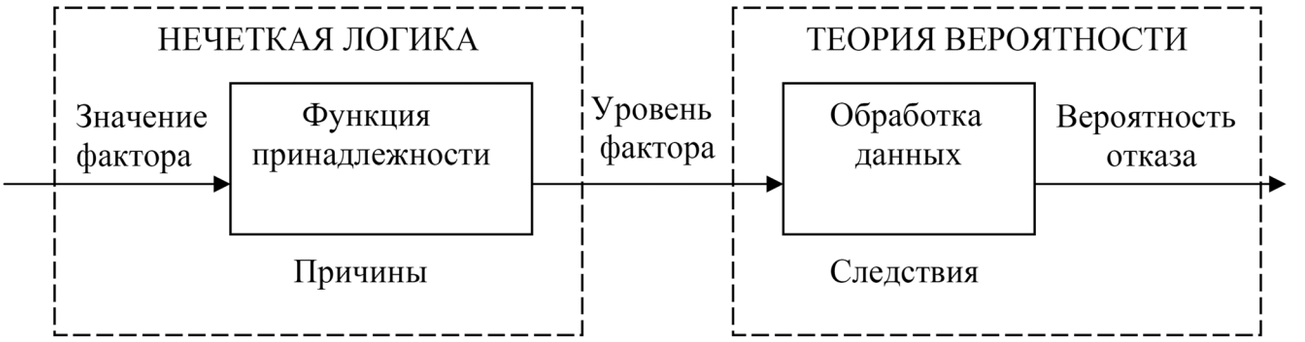
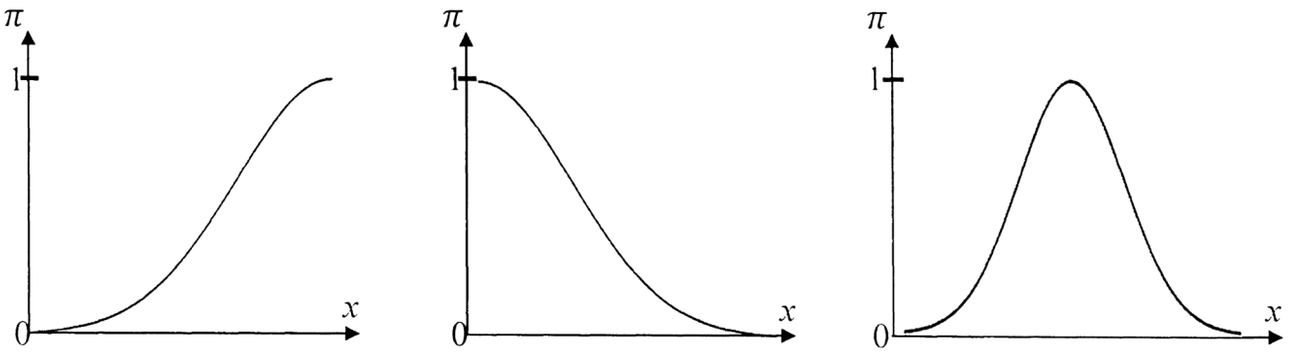


Рисунок 2 – Взаимосвязь теории вероятности и нечеткой логики в оценке надежности.



а) б) в)

Рисунок 3 – Функции принадлежности для нечеткой перфектности.

сматривались в [15]. Варианты нечетких границ между перфектными и неперфектными значениями переменной x показаны на рис. 3, где по мере увеличения значения x происходят следующие переходы:

а) «неперфектно» (0) – «перфектно» (1),

б) «перфектно» (1) – «неперфектно» (0),

в) «неперфектно» (0) – «перфектно» (1) – «неперфектно» (0).

3.3. Связи между концептами

Вес w_{ij} дуги, соединяющей концепты C_i и C_j, указывает на силу влияния C_i на C_j. Пусть концепты C_i и C_j характеризуются переменными x_i и x_j, а в результате эксперимента удается построить зависимость $x_j = \varphi(x_i)$. Тогда вес w_{ij} определяется как производная $w_{ij} = dx_i/dx_j$, которая может быть трех видов (рис. 4):

$w_{ij} > 0$, если повышение (понижение) величины x_i приводит к повышению (понижению) величины x_j (положительное влияние C_i на C_j);

$w_{ij} < 0$, если повышение (понижение) величины x_i приводит к понижению (повышению) величины x_j (отрицательное влияние C_i на C_j);

$w_{ij} = 0$, если значение x_j не зависит от значения x_i (отсутствие влияния C_i на C_j).

Сила влияния (w_{ij}) оценивается экспертно с помощью лингвистических термов и шкалы термометра (табл. 1).

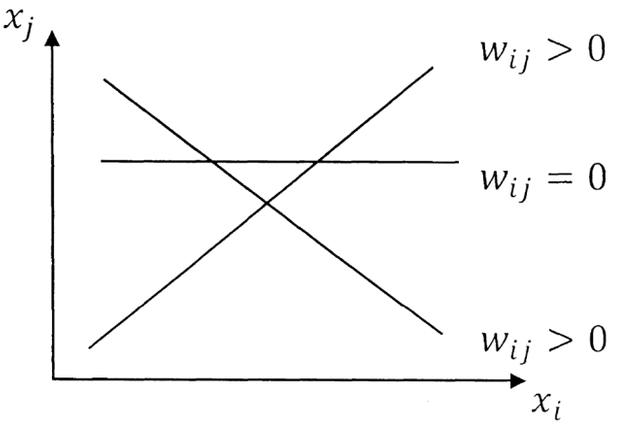


Рисунок 4 – Виды влияний между концептами.

Если учитываются мнения нескольких экспертов, то величина w_{ij} оценивается как взвешенное среднее:

$$w_{ij} = \frac{\alpha_1 w_{ij}^1 + \alpha_2 w_{ij}^2 + \ldots + \alpha_m w_{ij}^m}{\alpha_1 + \alpha_2 + \ldots + \alpha_m},$$

где w_{ij}^p – оценка силы влияния p-м экспертом; α_p – вес p-го эксперта, $p = 1, 2, \ldots, m$; m – количество экспертов.

Для снижения субъективизма экспертных оценок можно воспользоваться методом наименьшего влияния, предложенным в [16].

Таблица 1 – Способы оценки силы влияния.

Шкала термометра	Лингвистические оценки	Количественные значения
	Положительное максимальное	1
	Положительное выше среднего	0,75
	Положительное среднее	0,5
	Положительное ниже среднего	0,25
	Отсутствует	0
	Отрицательное ниже среднего	-0,25
	Отрицательное среднее	-0,5
	Отрицательное выше среднего	-0,75
	Отрицательное максимальное	-1

3.4. Рекуррентные соотношения

Согласно [11, 17], динамика изменения величины концептов в НКК определяется соотношением

$$A_i^{k+1} = f\left(\sum_{\substack{j=1 \\ j\neq i}}^{n} A_j^k w_{ji} + cA_i^k\right), k = 0, 1, 2, \ldots . \qquad (1)$$

где A_i^{k+1} – величина концепта C_i на шаге $k+1$; A_i^k и A_j^k – величины концептов C_i и C_j на шаге k соответственно, w_{ji} – сила влияния концепта C_j на концепт C_i; c – параметр, учитывающий предысторию, т.е. вклад значения концепта на предыдущем шаге, $c \in [0,1]$; f – пороговая функция, благодаря которой величина концепта не превышает единицу.

В этой работе предполагается, что $c = 1$, а в качестве пороговой функции используется положительная часть гиперболического тангенса (рис. 5):

$$f(x) = \begin{cases} \tanh(x) \text{ при } x \geq 0; \\ 0 \text{ при } x < 0, \end{cases} \quad \tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}.$$

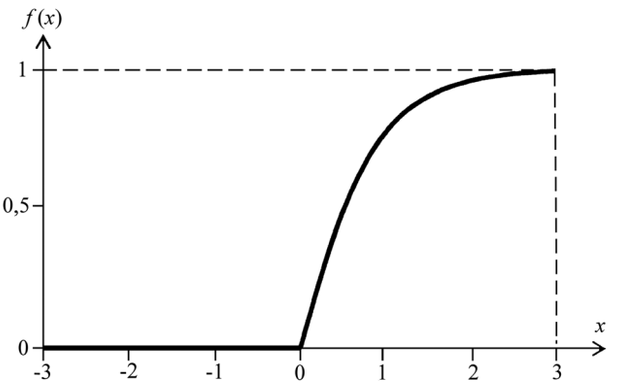


Рисунок 5 – Пороговая функция.

3.5. Матричная модель

Рекуррентное соотношение (1) можно представить в матричной форме

$$A^{k+1} = f\left(A^k W_0 + cA^k\right), k = 0, 1, 2, \ldots, \quad (2)$$

где A^{k+1}, A^k $k = 0, 1, 2, \ldots$ – $(1\times n)$-векторы состояния НКК, элементы которых задают значения концептов на шагах k+1 и k соответственно;

$$W_0 = \begin{bmatrix} 0 & w_{12} & \ldots & w_{1n} \\ w_{21} & 0 & \ldots & w_{2n} \\ . & . & \ldots & . \\ w_{n1} & w_{n2} & \ldots & 0 \end{bmatrix} \quad (3)$$

– $(n\times n)$-матрица сил влияний концептов C_i друг на друга, в которой диагональные элементы равны нулю.

Если вместо матрицы (3) использовать $(n\times n)$-матрицу

$$W = \begin{bmatrix} c & w_{12} & \ldots & w_{1n} \\ w_{21} & c & \ldots & w_{2n} \\ . & . & \ldots & . \\ w_{n1} & w_{n2} & \ldots & c \end{bmatrix}, \quad (4)$$

в которой все элементы по главной диагонали равны параметру $c\in[0,1]$, то соотношение (2) запишем как

$$A^{k+1} = f\left(A^k W\right), k = 0, 1, 2, \ldots, \quad (5)$$

которое напоминает рекуррентное соотношение для марковской цепи, если принять $f(x) = x$. Принципиальное отличие состоит в том, что марковская цепь моделирует динамику изменения вероятностей событий или события, а НКК моделирует динамику уровня причин, т.е. факторов, приводящих к этим состояниям или событиям (см. рис. 2).

Начальное состояние НКК определяется вектором

$$A^0 = \left[A_1^0, A_2^0, \ldots, A_n^0\right], \quad (6)$$

элементы которого отражают значения концептов на шаге $k = 0$. В результате взаимодействия между концептами НКК входит в стационарный режим, который соответствует одному из видов устойчивости [18].

4. Ранжирование концептов

При распределении ресурсов на обеспечение надежности системы используются количественные оценки (ранги) важности ее элементов. В статистической теории надежности наибольшее распространение получил индекс важности элемента по Бирнбауму [1], который определяется на основе функции надежности системы

$$P_S = f_S\left(P_1, \ldots, P_i, \ldots\right), \quad (7)$$

где P_S и P_i – вероятность безотказной работы системы и i-го элемента соответственно.

Первая производная в (7) – индекс важности i-го элемента системы по Бирнбауму, который вычисляется так [1]:

$$I_i = \frac{\partial P_S}{\partial P_i} = P_S\left(P_1, \ldots, P_{i-1}, 1, P_{i+1}, \ldots P_n\right) - P_S\left(P_1, \ldots P_{i-1}, 0, P_{i+1}, \ldots, P_n\right). \quad (8)$$

Вторая производная в (7) – индекс важности совместного влияния i-го и j-го элементов (*joint reliability importace*), введенный в [19, 20].

В нашем случае элементами модели являются входные концепты – факторы, влияющие на выходной уровень надежности системы. Поэтому возникает необходимость вычисления индексов важности концептов НКК.

4.1. Определение индексов важности

Во множестве концептов $C=\{C_1, C_2, \ldots, C_n\}$ будем предполагать следующее:

C_n – выходной концепт, который определяет уровень надежности системы и оценивается числом $A_n\in[0,1]$;

$C_1, C_2, \ldots, C_{n-1}$ – входные концепты, соответствующие взаимосвязанным факторам, которые влияют на уровень надежности системы и оцениваются уровнями $A_i\in[0,1]$, $i = 1, \ldots, n - 1$.

Значение концепта C_n на l-м шаге является функцией от элементов вектора (6), т.е.

$$A_n^l = F\left(A_1^0, A_2^0, \ldots, A_n^0\right). \quad (9)$$

Предполагается, что A_n^l – значение концепта C_n в стационарном режиме, т.е. на таком шаге l, когда A_n^l близко к A_n^{l-1}. Зависимость (9) является аналогом (7), что позволяет перейти к определению рангов концептов на основе производных.

Пусть $I(C_j)$ – индекс важности концепта C_j, а $I(C_j, C_k)$ – индекс совместной важности концептов C_j и C_k. Следуя (8) и [19, 20], определим эти индексы важности так:

$$I\left(C_j\right)=\frac{\partial A_n^l}{\partial A_j}=\frac{F\left(1_j,0\right)-F\left(0\right)}{1-0}=F\left(1_j,0\right), \qquad (10)$$

$$I\left(C_j,C_k\right)=\frac{\partial^2 A_n^l}{\partial A_j \partial A_k}=\frac{F\left(1_j,1_k,0\right)-F\left(0\right)}{\left(1-0\right)\left(1-0\right)}=F\left(1_j,1_k,0\right), \qquad (11)$$

где $F(1_j,0)$ – значение функции (9), когда $A_j^0=1$, а все остальные аргументы равны нулю; $F(0)$ – значение функции (9), когда все аргументы равны нулю (предполагается, что $F(0) = 0$); $F(1_j,1_k,0)$ – значение функции (9), когда $A_j^0=A_k^0=1$, а все остальные аргументы равны нулю.

Замечание. Нулевые значения входных концептов (кроме одного в (10) и двух в (11), равных единице) выбраны для того, чтобы исключить возможность их влияния на выходной концепт за счет транзитивных связей.

4.2. Алгоритм вычисления индексов важности

Шаг 1. Задать начальный вектор (6). Для индекса важности $I(C_j)$ начальный вектор задается как

$$A^0=\left[A_j^0=1, A_i^0=0,\ i=1,2,...,n,\ i\neq j\right], \qquad (12)$$

а для индекса важности $I(C_j, C_k)$ в виде

$$A^0=\left[A_j^0=A_k^0=1, A_i^0=0,\ i=1,2,...,n,\ i\neq j,k\right]. \qquad (13)$$

Шаг 2. Пользуясь рекуррентным соотношением (5) найти вектор состояния НКК

$$A^l=\left[A_1^l, A_2^l,..., A_n^l\right] \qquad (14)$$

в установившемся режиме, т.е. на таком шаге l, при котором $\left|A_i^l-A_i^{l-1}\right|<\varepsilon$, где ε – малое положительное число, $i = 1, 2, \ldots, n$.

Шаг 3. Индексами важности $I(C_j)$ и $I(C_j, C_k)$ считать элементы A_n^l вектора (14), полученные при начальных векторах (12) и (13) соответственно.

5. Пример

5.1. Концепты и влияния

Рассмотрим модель надежности и безопасности автомобиля в системе «водитель-автомобиль-дорога». Нечеткая когнитивная карта системы приведена на рис. 6, где концепты имеют следующее содержание: C_1 – квалификация водителя, C_2 – дорожные условия, C_3 – удельные затраты на эксплуатацию, C_4 – условия эксплуатации, C_5 – периодичность технического обслуживания, C_6 – качество технического обслуживания и ремонта, C_7 – качество конструкции автомобиля, C_8 – качество эксплуатационных материалов и запасных частей, C_9 – условия хранения, C_{10} – надежность и безопасность автомобиля.

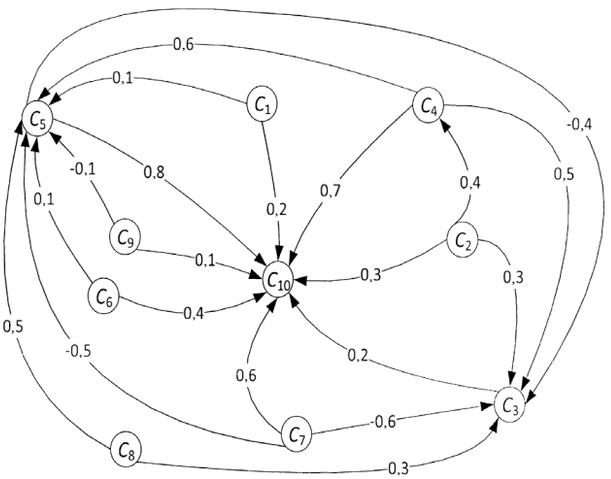


Рисунок 6 – Нечеткая когнитивная карта для оценки надежности и безопасности.

Матрица $\boldsymbol{W}$ (4) экспертными оценками силы влияний, в которой принималось $c = 1$, имеет вид

$$W=\begin{bmatrix}
1 & 0 & 0 & 0 & 0{,}1 & 0 & 0 & 0 & 0 & 0{,}5\\
0 & 1 & 0{,}3 & 0{,}4 & 0 & 0 & 0 & 0 & 0 & 0{,}3\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}2\\
0 & 0 & 0{,}5 & 1 & 0{,}6 & 0 & 0 & 0 & 0 & 0{,}7\\
0 & 0 & -0{,}4 & 0 & 1 & 0 & 0 & 0 & 0 & 0{,}8\\
0 & 0 & 0 & 0 & 0{,}1 & 1 & 0 & 0 & 0 & 0{,}4\\
0 & 0 & -0{,}6 & 0 & -0{,}5 & 0 & 1 & 0 & 0 & 0{,}6\\
0 & 0 & 0{,}3 & 0 & 0{,}5 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & -0{,}1 & 0 & 0 & 0 & 1 & 0{,}1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}.$$

5.2. Индексы важности концептов

Табл. 2 содержит девять пар векторов, связанных с вычислением индексов важности концептов $C_1, \ldots, C_9$. Каждая пара содержит начальный вектор (12) и вектор (14) в установившемся режиме. Последний элемент второго вектора в каждой паре соответствует индексу важности концепта, например $I(C_1) = 0{,}686$. Последний столбец в табл. 2 иллюстрирует пошаговое изменение уровня надежности и безопасности автомобиля (A_{10})

Таблица 2 – Значения концептов в стационарном состоянии для различных начальных векторов.

Шаг	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}
1	1	0	0	0	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3040	0,022	0,000	0,000	0,000	0,187	0,000	0,000	0,000	0,000	0,68579
1	0	1	0	0	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
774	0,000	0,044	0,000	0,365	0,747	0,000	0,000	0,000	0,000	0,94834
1	0	0	1	0	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3717	0,000	0,000	0,020	0,000	0,000	0,000	0,000	0,000	0,000	0,22707
1	0	0	0	1	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3014	0,000	0,000	0,000	0,022	0,335	0,000	0,000	0,000	0,000	0,79115
1	0	0	0	0	1	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
5324	0,000	0,000	0,000	0,000	0,017	0,000	0,000	0,000	0,000	0,33491
1	0	0	0	0	0	1	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3196	0,000	0,000	0,000	0,000	0,186	0,022	0,000	0,000	0,000	0,68912
1	0	0	0	0	0	0	1	0	0	0
…	…	…	…	…	…	…	…	…	…	…
4953	0,000	0,000	0,000	0,000	0,000	0,000	0,017	0,000	0,000	0,30912
1	0	0	0	0	0	0	0	1	0	0
…	…	…	…	…	…	…	…	…	…	…
2742	0,000	0,000	0,000	0,000	0,321	0,000	0,000	0,023	0,000	0,77418
1	0	0	0	0	0	0	0	0	1	0
…	…	…	…	…	…	…	…	…	…	…
3086	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,022	0,18667

Таблица 3 – Индексы важности совместного влияния факторов.

Концепты	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	0,949	0,686	0,801	0,686	0,730	0,335	0,786	0,255
C_2	–	0,948	0,948	0,948	0,950	0,949	0,950	0,948
C_3	–	–	0,791	0,335	0,689	0,309	0,774	0,254
C_4	–	–	–	0,791	0,803	0,703	0,823	0,782
C_5	–	–	–	–	0,689	0,309	0,774	0,187
C_6	–	–	–	–	–	0,356	0,788	0,294
C_7	–	–	–	–	–	–	0,309	0,323
C_8	–	–	–	–	–	–	–	0,763

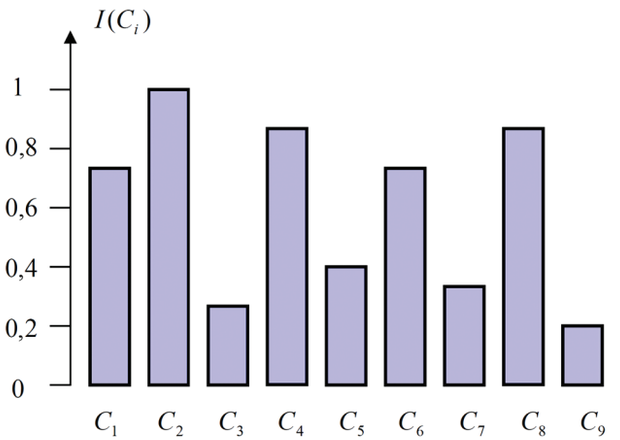


Рисунок 7 – Диаграмма индексов важности факторов.

при активации одного из факторов (A_i, i = 1, …, 9). Диаграмма индексов важности концептов показана на рис. 7. Результаты вычисления индексов важности совместного влияния концептов сведены в табл. 3, например, $I(C_1, C_2) = 0{,}949$.

Следует заметить, что концепт C_7 может быть детализирован с учетом результатов работы [21].

6. Заключение

В этой статье предложен и продемонстрирован на примере человеко-машинной системы метод ранжирования факторов, влияющих на ее надежность. В основу метода положена формализация причинно-следственных связей «влияющие факторы – надежность» в виде нечеткой когнитивной карты, т.е. ориентированного графа,

вершины которого соответствуют надежности системы и влияющим факторам, а взвешенные дуги отражают силы влияний факторов друг на друга и на надежность системы.

Предложенный метод можно рассматривать как аналог ранжирования элементов системы по Бирнбауму в вероятностной теории надежности. Достоинствами метода являются:

• использование доступной экспертной информации без сбора и обработки статистических данных;

• возможность учета любых количественных и качественных факторов, связанных с человеком, техникой, программным обеспечением, качеством обслуживания, условиями эксплуатации и др. В частности, отдельными концептами можно характеризовать различные виды избыточности (структурную, алгоритмическую и др.), которые используются для повышения надежности;

• простота расширения числа учитываемых факторов за счет введения новых вершин и дуг ориентированного графа.

Возможными объектами применения метода могут быть сложные системы с нечетко определенной структурой, надежность которых сильно зависит от взаимосвязанных факторов, измеряемых экспертно.

Библиографический список

1. **Барлоу Р.** Статистическая теория надежности испытания на безотказность [Текст] / Р. Барлоу, Ф. Прошан. – М.: Наука, 1984.

2. **Рябинин И.А.** Надежность и безопасность структурно-сложных систем [Текст] / И.А. Рябинин. – СПб: Изд-во С.-Петерб. ун-та, 2007.

3. **Губинский,А.И.** Эргономическое проектирование судовых систем управления [Текст] / А.И. Губинский, В.Г. Евграфов. – Ленинград: Судостроение, 1977.

4. **Губинский А.И.** Надежность и качество функционирования эргатических систем [Текст] / А.И. Губинский. – Ленинград: Наука, 1982.

5. **Глушков В.М**. Алгебра. Языки. Программирование [Текст] / В.М. Глушков, Г.Е. Цейтлин, Е.Л. Ющенко. – Киев: Наукова Думка, 1978.

6. **Ротштейн А.П.** Вероятностно-алгоритмические модели человеко-машинных систем [Текст] / А.П. Ротштейн // Автоматика. – 1987. – №6. – С. 81-87.

7. **Ротштейн А.П.** Нечеткий анализ надежности алгоритмов деятельности [Текст] / А.П. Ротштейн // Надежность. – 2007. – №2. – С. 3-18.

8. **Barnard A**. Why you cannot predict electronic product reliability [Текст] / A. Barnand. – ARS, Europe: Warsaw, Poland, 2012.

9. **Горяинов А.А.** Анализ влияний факторов на ущерб от происшествий на транспорте с помощью регрессионных моделей [Текст] / А.А. Горяинов, А.М. Замышляев, Е.Н. Платонов // Надежность. – 2013. – №2. – С. 126-144.

10. **Заде Л.** Понятие лингвистической переменной и ее применение к принятию приближенных решений [Текст] / Л. Заде. – М.: Мир, 1976.

11. **Kosko B.** Fuzzy cognitive maps [Text] / B. Kosko // International Journal of Man-Machine Studiens. – 1986. – Vol. 24. – P. 65-75.

12. **Axelrod R.** Structure of Decision: The Cognitive Maps of Political Elites [Text] / R. Axelrod. – Princeton: University Press, 1976.

13. **Цыпкин Я.З.** Основы информационной теории идентификации [Текст] / Я.З. Цыпкин. – М.: Наука, 1984.

14. **Rotshtein A.** Fuzzy Evidence in Identification, Forecasting and Diagnosis [Text] / A. Rotshtein, H. Rakytyanska. – Berlin: Springer, 2012.

15. **Ротштейн А.П.** Выбор условий деятельности человека на основе нечеткой перфектности [Текст] / А.П. Ротштейн // Изв. РАН. Теория и системы управления. – 2018. – № 6. – С. 108-119.

16. **Ротштейн А.П.** Ранжирование элементов системы на основе нечетких отношений: метод нечеткого влияния [Текст] / А.П. Ротштейн // Надежность. – 2015. – № 4. – С. 16-29.

17. **Kosko B.** Neural Network and Fuzzy Systems. Englewood Cliff [Text] / B. Kosko. – N.Y.: Prentice–Hall, 1992.

18. **Бутенин Н.В.** Введение в теорию нелинейных колебаний [Текст] / Н.В. Бутенин, Ю.И. Неймарк, Н.А. Фуфаев. – М.: Наука, 1987.

19. **Hong J.S.** Joint Reliability Importance of two Edges in undirected Network [Text] / J.S. Hong, C.H. Lie // IEEE Transaction on Reliability. – 1993. – Vol. 2. – № 1. – P. 17-23.

20. **Gertsbakh I.** Combinatorial Approach to Computing Component Importance Indexes in Coherent Systems [Text] / I. Gertsbakh, Y. Shpungin // Probability in the Engineering and Information Sciences. Cambridge University Press. – 2012. – Vol. 24(1). – P. 1-10.

21. **Нетес В.А.** Исследование эксплуатационной надежности систем автомобиля LADA KALINA, влияющих на безопасность дорожного движения [Текст] / В.А. Нетес // Надежность. – 2017. – № 4. – С. 31-35.

Сведения об авторе

Александр П. Ротштейн – доктор технических наук, профессор, профессор Иерусалимского политехнического института – Махон Лев, Иерусалим, Израиль; Донецкий национальный университет им. В.Стуса, Винница, Украина, e-mail: rothstei@g.jct.ac.il

Оригинальная статья
https://doi.org/10.21683/1729-2646-2019-19-4-32-44

Решение проблемы аварийности горных машин с использованием Отчета «Тойота» А3

Любиша Папич[1], Ирина В. Гадолина[2*], Милорад Пантелич[3], Неда Папич[4]

[1]Исследовательский центр по управлению качеством и надежностью (DQM), г. Чачак, Сербия. [2]Институт машиноведения им. А.А. Благонравова Российской академии наук, г. Москва, Российская Федерация; [3]Предприятие «Колубара Метал», г. Лазаревац, Сербия. Технический факультет, Крагуевацкий университет, г. Чачак, Сербия; [4]Бакалавр наук по специальности «Промышленная инженерия», студент магистратуры по специальности «Промышленная инженерия». Факультет технических наук, Университет в г. Нови Сад, г. Нови Сад, Сербия
**gadolina@mail.ru*


Любиша Папич


Ирина В. Гадолина


Милорад Пантелич


Неда Папич

Резюме. Целью *статьи явилась демонстрация преимуществ применения отчета «Тойота» А3 как стандартного способа обмена информацией. Необходимо отметить, что в настоящее время метод еще не нашел подобающего распространения. Он заслуживает большего. Показывая на конкретном примере аварии крупной горной машины, каким образом заполняется отчет, авторы статьи надеются, что данная информация поможет внедрить эту систему на других предприятиях. Это, возможно, будет способствовать решению многих вопросов, связанных с промышленным менеджментом. Для предприятий, эксплуатирующих горнодобывающую технику, данный материал будет особенно полезным.* **Метод** *заключается в представления материала на листе бумаги формата А3, который требуется для отражения всей информации, необходимой для решения возникшей проблемы. Почему формат А3? Формат А3 – это максимальный размер листа бумаги, который можно отправить по факсу. До появления персональных компьютеров он был наиболее распространенным средством связи между заводами компании «Тойота Моторс». В рассмотренном примере применения отчета «Тойота» А3, содержатся такие принципиально важные разделы, как обслуживание и безотказность горных машин, информация о проводившихся ранее исследованиях в этом направлении, применение метода «5 почему?» и рассмотрение влияния человеческого фактора. В примере, рассмотренном в статье, в отчете содержится описание обстоятельств аварии экскаватора SRs 1200 24/4 (G2), произошедшей 6 апреля 1995 г. на угольном разрезе «Открытая разработка D» рудного бассейна «Колубара» компании «Электропромышленность Сербии». Отчет также включает оценку последствий и анализ причин аварии.* **Результаты** *заключаются в представлении методологического подхода к решению проблем, краткого формата представления информации, документирования и фиксация сведений, с которыми другие участники рабочего процесса могут ознакомиться; обеспечение возможности составить представление о рабочих процессах и результатами решения проблем. При этом обеспечивается общий язык для общения внутри компании, и создается культура бережливого производства в компании. Отчет А3 – это процесс обучения и основа для будущих изменений в организации производства.* **Выводы.** *Отчет «Тойота» А3 выполняет две основные функции: внесение предложений и ведение отчетности по одобренным мероприятиям согласно указанным предложениям. Он позволит конкретизировать проблему и перейти непосредственно к мероприятиям, направленным на улучшение ситуации. Внедрение отчета в практику взаимодействий отделов внутри предприятий и с предприятиями-поставщиками позволит оперативно и целенаправленно решать вопросы управления. Первоначально разработанный в Японии на предприятиях Тойота, в настоящее время метод находит все большее применение на предприятиях Сербии и других стран.*

Ключевые слова*: авария, решение проблемы, горные машины, угольный разрез, Отчет «Тойота» А3, безотказность и безопасность, Цикл Деминга, «5 Почему?», человеческий фактор, модель «швейцарский сыр», Черный лебедь.*

Для цитирования: *Любиша Папич, И.В. Гадолина, Милорад Пантелич, Неда Папич. Решение проблемы аварийности горных машин с использованием Отчета «Тойота» А3 // Надежность. 2019. № 4. С. 32-44. https://doi.org/10.21683/1729-2646-2019-19-4-32-44*

Поступила 23.05.2019 г. / После доработки 09.11.2019 г. / К печати 14.12.2019 г.

1. Введение

В основе современного промышленного производства лежат природные ресурсы. Около 70% всех природных ресурсов приходятся на минеральное сырье. Сегодня в мире более триллиона долл. США тратится на сырье (металлические и неметаллические руды, уголь, глина, камень, песок и гравий), которое для многих стран является основными статьями экспорта и импорта.

Во многих странах горнодобывающая промышленность является основой развития и оказывает значительное влияние на национальную экономику в целом. Приведенные ниже данные [1] весьма красноречиво показывают влияние горнодобывающей отрасли на экономику страны (Сербия):

• цены на железо, кокс (каменный уголь) и руду – влияют на 80-90%;

• цены на цветные металлы, руду и электроэнергию – на 90%;

• цены на электроэнергию и уголь – на 60%;

• цена на уголь, стоимость обслуживания горной техники на угольных разрезах – на 35-40% и т.д.

Решение проблем в горнодобывающей промышленности представляет собой, прежде всего, интеллектуальную задачу. Как документировать наиболее важную информацию и решения на каждом этапе проведения работ таким образом, чтобы можно было обмениваться данными внутри коллектива, включать в рабочий процесс новых сотрудников и вносить предлагаемые исправления? Процессы документирования сложных процессов, связанных с решением проблемных ситуаций, часто сопряжены с накоплением большого количества бумажной документации или, учитывая современную специфику, цифровых данных. Компания «Тойота Моторс» со своей стороны отдает предпочтение более простому методу с использованием карандаша, ластика и листа бумаги. Этот метод работы часто называют Отчетом «Тойота» А3. Почему формат А3? Данный формат использовался в «Тойота» изначально, поскольку значительная часть информационного обмена между структурными подразделениями «Тойота» в Японии и ее заводами за рубежом осуществлялась по факсу, а А3 (297 х 420 см) – самый крупный формат, совместимый с соответствующей аппаратурой.

Метод решения проблем с использованием Отчета «Тойота» А3 был разработан для того, чтобы обеспечить максимально четкое описание предлагаемых улучшений. Отчет «Тойота» А3 имеет две основные функции: внесение предложений и ведение отчетности по одобренным мероприятиям согласно указанным предложениям. Суть метода А3 заключается в том, чтобы обеспечить визуализацию предложений на одном листе бумаги формата А3 [2]. Эффективность Отчета «Тойота» А3 обусловлена тем, что он позволяет сводить большие объемы данных в формат, который легко читать и понимать. Это действенное средство оптимизации процессов управления в компаниях, в которых сотрудники выполняют несколько функций, например, на бережливых производствах. Они слишком сильно ограничены во времени, чтобы читать большое количество документов, чтобы понять конкретную проблему или ситуацию.

Преимущества использования Отчета «Тойота» А3 при решении проблем заключаются в следующем:

• методологический подход к решению проблем;

• краткий формат представления информации или ведения отчетности;

• документирование и фиксация сведений, с которыми другие участники рабочего процесса могут ознакомляться; обеспечение возможности ознакомления с процессами управления и результатами решения проблем;

• общий язык для общения внутри компании;

• создание культуры бережливого производства в компании;

• создание основ для будущих изменений.

Как правило, в большинстве компаний информация находится в общем доступе, но логически не структурирована. В результате значительное время затрачивается на разговоры и попытки достичь понимания, наведение порядка, изучение и анализ данных. При этом крайне широко используются портативные компьютеры, а описания методик работы и принципов бережливого производства [3] пылятся на книжных полках, и на то, что их когда-то будут читать, надежды мало. Отчет «Тойота» А3 устроен таким образом, чтобы его не только читали работники, но и использовали в работе, например, при решении некоторых проблем.

2. Обслуживание и безотказность горных машин

Техническое обслуживание многоковшовых экскаваторов при эксплуатации в условиях карьеров непосредственно зависит от реализованной эффективности (безотказности, готовности, ремонтопригодности и безопасности) как на уровне проекта, так и в процессе эксплуатации [4]. Правильно избранная концепция технического обслуживания для систем BWECD (система «экскаватор – ленточный конвейер – откидывание земли») и BWECL (система «экскаватор – ленточный конвейер – погрузка угля»), а также хорошо обученный персонал и высокое качество управления обслуживанием способствуют улучшению финансовых показателей эксплуатации карьеров.

Многоковшовый экскаватор является источником значительного риска, связанного с возможными отказами и авариями, которые представляют эксплуатационную и экологическую опасность. Безотказность многоковшовых экскаваторов, которые проектируются для успешного выполнения целевой функции, определяет продолжительность интервала времени, в течение которого они будут работать без отказов. Изыскания [5], направленные на повышение уровня безотказности и качества управления безотказностью в течение жизненного цикла многоковшовых экскаваторов, имеют своей

целью сформировать систему мер безопасности для экономически эффективной эксплуатации и обеспечения соответствия комплексным нормам экологической и технической безопасности в эксплуатации и в более широком смысле.

Практика разработки угольных месторождений открытым способом показала, что такие системы непрерывного действия как BWECD и BWECL обеспечивают максимальную результативность с технической и экономической точек зрения. Многоковшовые экскаваторы должны обладать высокими показателями безотказности. В этой связи возникает необходимость определения среди прочего количественных показателей безотказности, которые лежат в основе концепции технического обслуживания многоковшового экскаватора [6].

3. Ранее проводившиеся исследования безотказности и безопасности горных машин

В течение последних нескольких десятилетий было проведено множество исследований с целью определения производительности, безотказности и эффективности эксплуатации горных машин в составе систем типа BWECD и BWECL, а также вспомогательных горных машин на карьерах в Сербии [1, 4]. В работах [7, 8, 9] проведен анализ большого объема данных, собранных и обработанных для определения рабочих характеристик горных машин при эксплуатации в условиях карьеров на территории Сербии. Результаты исследований, систематизированных в монографии [5], относятся к полным системам типа BWECD (BWECL). Эти данные показывают число отказов многоковшового экскаватора, самоходного транспортера, ленточного конвейера с резиновой лентой и разгрузочным устройством на карьерах рудного бассейна «Колубара» в г. Лазаревац в Сербии, как показано на рисунке 1.

Как правило, наибольшее время простоя приходится на многоковшовые экскаваторы, хотя на конвейерах с длинными лентами продолжительные простои также могут иметь место. Следующий пример касается одной системы типа BWECD, которая эксплуатируется на карьере «Тамнава» рудного бассейна «Колубара», которая состоит из многоковшового экскаватора SchRs 700, челночной вагонетки, конвейера с тремя резиновыми лентами длиной от 1 тыс. до 1,2 тыс. м и отвалообразователя. Структура времени простоя показывает, что на отказы многоковшового экскаватора приходится 60% простоев, отказы конвейерных лент – 27% простоев, а отказы отвалообразователя – 4% простоев. С другой стороны, струк-

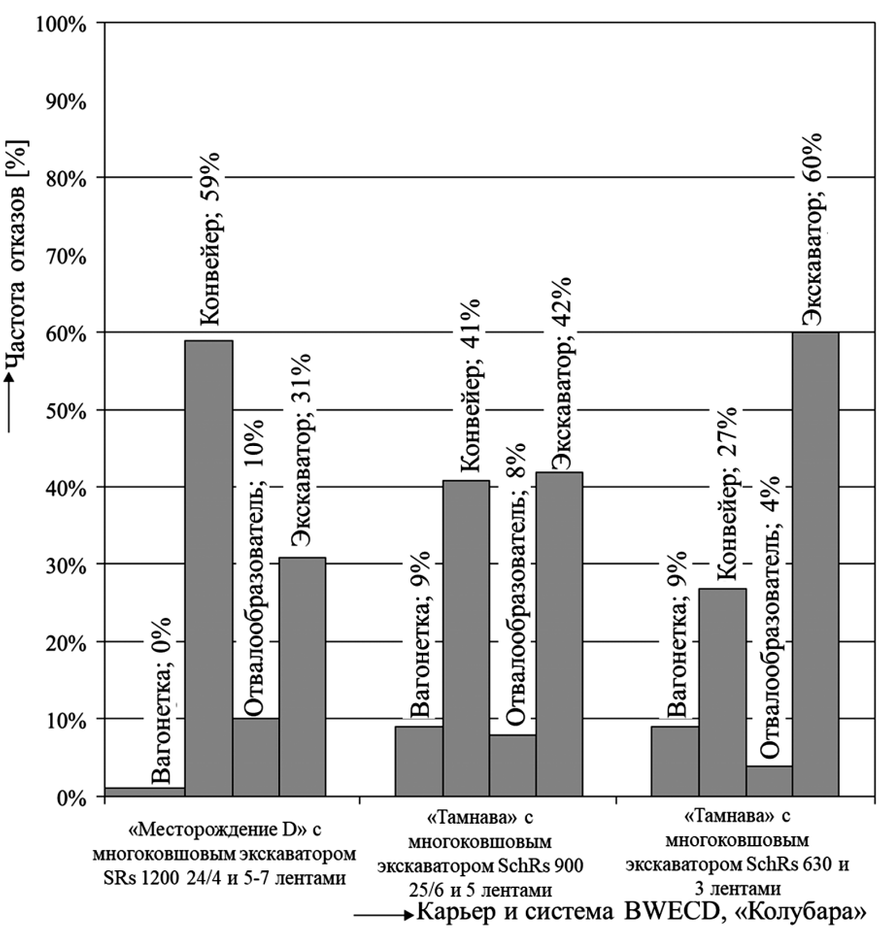


Рисунок 1- Частота отказов для некоторых систем BWECD на карьерах рудного бассейна «Колубара» в г. Лазаревац в Сербии. [5]

тура времени простоя системы типа BWECD на карьере «Тамнава», которая включает в себя многоковшовый экскаватор SchRs 900 25/6 с пятью ленточными конвейерами, показывает, что соотношение отказов экскаватора и конвейерной ленты примерно равно. На карьере «Месторождение D», где система типа BWECD включает в себя многоковшовый экскаватор SRs 1200 24/4, имеющем от 5 до 7 конвейерных лент, на конвейерные ленты в силу их значительной длины приходится почти вдвое большая доля отказов, чем на многоковшовый экскаватор [1].

Приведенные результаты показывают, что поломки системы BWECD были в основном вызваны отказами в многоковшовом экскаваторе (за исключением случаев, когда речь идет о длинных ленточных транспортерах, поскольку их длина обусловлена технологическими условиями). Из этого следует, что увеличение безотказности многоковшового экскаватора приведет к повышению общей безотказности системы BWECD [1].

Многоковшовый экскаватор представляет собой очень сложную техническую систему, состоящую из большого числа объектов (подсистем, узлов, элементов). Каждый объект представляет собой потенциальный источник причины простоя в случайный момент времени и случайной продолжительности. Последствия возникновения отказов на многоковшовых экскаваторах включают в себя снижение производительности экскаватора, которое приводит к снижению экономического эффекта эксплуатации карьера. В связи с этим, рассмотренные в [5] подсистемы экскаватора были классифицированы по приоритетности с точки зрения безотказности. В исследовании рассматривались следующие элементы многоковшового экскаватора:

- подсистема ротора,
- подсистема транспортировки материала на экскаваторе,
- подсистема вращения надстройки,
- подсистема движения экскаватора.

Результаты исследований показали, что наибольшее число поломок на многоковшовых экскаваторах произошло в силу отказа подсистемы ротора (до 51%), что показано на рисунке 2. Повышение безотказности отдельных элементов многоковшового экскаватора позволяет повысить общую безотказность экскаватора. При этом приоритет следует отдавать тем элементам экскаватора, безотказность которых является самой низкой.

Исследования [1, 5] по оценке безотказности многоковшового экскаватора SRs 1200 24/4 (G2) в период с 01.01.2006 по 31.12.2006 проводились с использованием отчетности компании «Электроэнергетика Сербии» по карьерам «Месторождение D» и «Зеоке» рудного бассейна «Колубара». В результате исследований были получены данные о видах, последствиях и причинах отказов, а также сведения о возникновении условий неисправности и простоя. Исследования показали, что наиболее безотказными узлами многоковшового экскаватора SRs 1200 24/4 (G2) являются: механизм подъема стрелы ротора (МПСР) и несущая стальная конструкция (НСК), затем – механизм кругового движения (МКД), механизм транспортировки экскаватора (МТЭ), механизм транспортировки материала (МТМ) и механизм ротора (МР), см. также гистограмму на рисунке 3.

Безотказность и безопасность элементов многоковшового экскаватора не всегда находятся в прямой корреляции. Другими словами, высокой безотказности

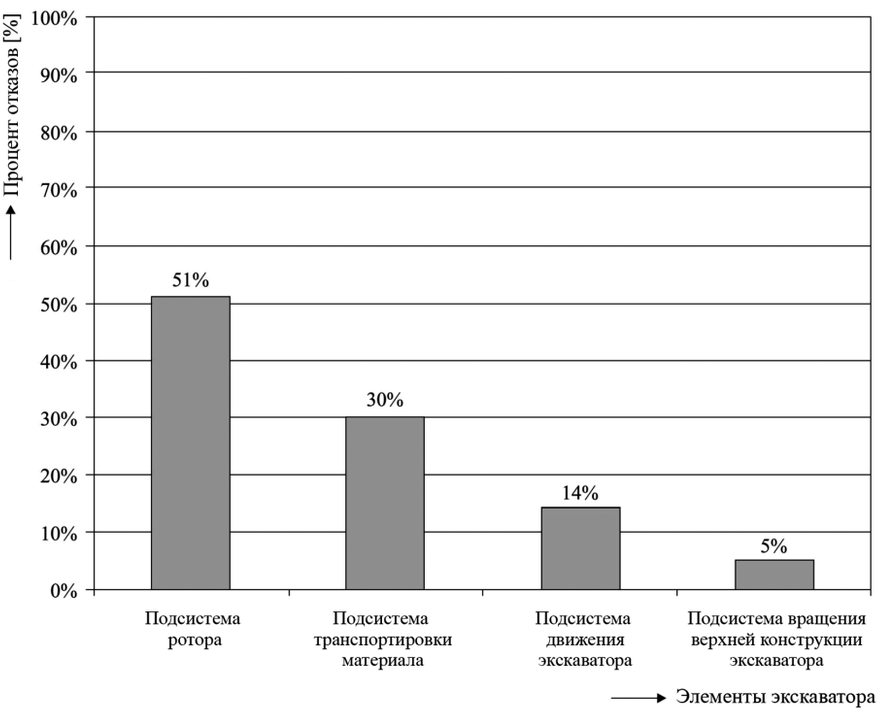


Рисунок 2 – Частота отказов многоковшового экскаватора. [5]

не всегда соответствует низкая критичность работоспособности и наоборот. Критичность отказа элемента многоковшового экскаватора является показателем безопасности функционирования экскаватора. Например, некоторые элементы многоковшового экскаватора могут обладать высокой безотказностью, но, в то же время, низкой безопасностью (т.е. высокой критичностью), что было показано в результате исследования [1, 5]. Это касается следующих узлов и агрегатов: механизм подъема стрелы ротора (МПСР) и несущая стальная конструкция (НСК). На практике это означает, что все виды отказов этих агрегатов происходят редко, но, когда они происходят, это приводит к серьезным последствиям для функционирования многоковшового экскаватора, а значит, и всей системы BWECD. При определении безотказности наряду с длительностью периода времени безотказной работы важную роль играет частота возникновения отказов, при определении безопасности – уровень критичности.

Таким образом, учет последствий отказов, а также своевременное устранение их причин обеспечивает стабильную безопасность многоковшовых экскаваторов.

Коэффициент готовности представляет собой важный комплексный показатель безотказности и ремонтопригодности восстанавливаемых систем, используемый при анализе безотказности и риска. В [10] предложен способ оценки изменчивости коэффициента готовности на основе статистических методов с повторной выборкой. Метод был применен к подсистемам многоковшового экскаватора SRs 1200 24/4 (G2) с использованием статистических данных по отказам, собранных на рудном бассейне «Колубара» в районе г. Лазаревац, Сербия. Использование методов с повторной выборкой, т.е. метода складного ножа и бутстрепа, позволило провести оценку изменчивости коэффициента готовности подсистем экскаватора.

За исключением подсистемы МР безотказность и ремонтопригодность подсистем соответствует требованиям к безотказности сложных технических объектов. Нижний квартиль распределения коэффициента готовности достигает 0,9977 для наиболее ответственной подсистемы МПСР без учета выбросов, что соответствует довольно высокой безотказности даже при том, что оценка интервала проводилась с использованием размножения выборок [10]. Согласно оценке, полученной с использованием разработанного метода [10], 90-процентный доверительный интервал коэффициента готовности системы в целом достигает [0,81; 0,94] со средним значением 0,90.

Недостаточно высокую надежность показывает в ряде случаев система, связанная с копанием породы. Причина кроется в преждевременном износе рабочих частей. Для уточнения инженерной формулы для оценки износа в [11] было проведено уточнение известной ранее формулы с учетом разных режимов эксплуатации. Применение этой формулы поможет спланировать профилактические ремонты и осмотры.

Для анализа отказов экскаватора, как сложной системы, может быть применен метод бэта-фактора [12]. Он является наиболее простым с точки зрения моделирования зависимых отказов и проведения дальнейших расчетов. При этом он не лишен некоторых ограничений. Для сложной системы, которой является экскаватор, обеспечение надежности должно осуществляться с самых ранних стадий жизненного цикла на основе последовательного выполнения определенных конструкторских, технологических и производственных процедур [13]. Отчет «Тойота» А3 может внести некоторую ясность при решении данной проблемы.

4. Авария многоковшового экскаватора SRs 1200 24/4 (G2) 6 апреля 1995 года и ее последствия

Многоковшовый экскаватор SRs 1200 24/4 (G2) был собран и введен в эксплуатацию в 1968 г. на карьере «Месторождение D» рудного бассейна «Колубара» и получил внутреннюю маркировку G2 («Grinding Machine 2», т.е. «Дробилка 2»), рисунок 4.

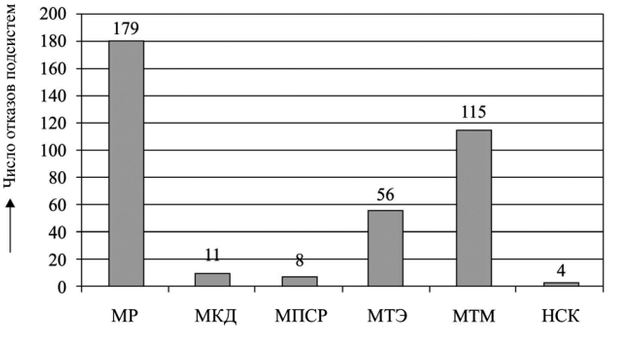


Рисунок 3 – Частота отказов подсистем многоковшового экскаватора SRs 1200 24/4 (G2). [5]

Авария многоковшового экскаватора SRs 1200 24/4 (G2) (рисунок 5) привела к значительному ущербу, в связи с которым было необходимо провести диагностику и оценку отказов, что и было сделано экспертами рудного бассейна «Колубара» и компании «Колубара Метал». Некоторые части поврежденной машины были перевезены на сборочную площадку в г. Зеоке, а некоторые – в металлические мастерские г. Колубары.

Оценка последствий подразумевает анализ прямых и косвенных убытков, которые могут быть вызваны тем или иным исходом (конечным состоянием). Если оценка убытков, связанных с определенным неблагоприятным событием, была произведена в различных единицах измерения, они должны быть сведены в единый ущерб. Кроме того, конечные состояния могут иметь текущий или отложенный эффекты. Так, например, при аварии многоковшового экскаватора SRs 1200 24/4 (G2) на «Месторождении D» рудного бассейна «Колубара» анализ затрат [1] показал наличие двух видов затрат, а именно:

1. Прямые издержки, которые включают:

• проектирование;

• демонтаж поврежденного многоковшового экскаватора;

• транспортировку поврежденного многоковшового экскаватора;

• изготовление и восстановление деталей многоковшового экскаватора (агрегатов, узлов, элементов);

• сборку многоковшового экскаватора;

• ввод в эксплуатацию.

Прямые издержки (расходы) составили 7 500 000,00 Евро.

2. Косвенные издержки ввиду простоя производственных мощностей карьера в период до возобновления работы многоковшового экскаватора в размере 157 000 000,00 Евро.

Данные были получены исходя из издержек от простоя элемента экскаватора (BWECD или BWECL) стоимостью 4500,00 Евро.

Продолжительность неработоспособности:

9 лет х 12 месяцев х 30 дней х 24 часа х 0,45 = 35,000 нормо-часов.

Размер косвенных издержек:

35,000 норм-часов х 4,500 Евро / час = 157 000 000,00 Евро.

Рисунок 4- Вид многоковшового экскаватора SRs 1200 24/4 (G2) до аварии.

5. Анализ причины аварии многоковшового экскаватора SRs 1200 24/4 (G2)

5.1 Применение метода «5 Почему?» для определения основных причин аварий

В основе подхода к определению причин недостаточного качества в компании «Тойота» лежит вопрос «Почему?», заданный пять раз во время обнаружения проблемы. Метод называется «5 Почему?». Если на вопрос «Почему?» удалось ответить пять раз, то основная причина и путь решения проблемы ясны. Анализ основных причин проблем технического обслуживания основан на пятикратном повторении вопроса «Почему?» Данный подход внедрен в систему технического обслуживания компании «Тойота» (Бережливая система технического обслуживания) [14]. Метод «5 Почему?» стремится к детальному исследованию проблем и обстоятельств, которые приводят к основным причинам указанных проблем. Метод «5 Почему?» обычно используется в «Тойота» для поиска источника проблем обслуживания. Он описывает способ мышления, необходимый для достижения уровня, необходимого для предотвращения повторения проблем технического обслуживания. Возможно, это будет не основная причина, но, по крайней мере, на этом уровне корректирующие меры могут предотвратить повторение проблемы. В случае аварии многоковшового экскаватора SRs 1200 24/4 (G2), применение метода «5 Почему?» описывает способ мышления (см. рисунок 6), необходимый для предотвращения повторных аварий.

Рисунок 5- Вид многоковшового экскаватора SRs 1200 24/4 (G2) после аварии 6 апреля 1995 г.

Согласно данным [4], значительная доля всех видов отказов на сложных горных машинах была вызвана человеческим фактором. Они происходили на этапах проектирования, изготовления, контроля качества, сборки, эксплуатации и обслуживания системы с участием сотрудников любого уровня образования, квалификации, компетентности и опыта. Ошибки обслуживающего персонала состоят в неправильном выполнении инструкций по техническому обслуживанию технических систем и вызваны их психофизическим состоянием (усталость, стресс и др.), неправильно организованным рабочим местом по причине отсутствия системы организации труда 5s [15], ошибками в эргономических расчетах, наличием шума на рабочем месте, недостаточной освещенностью рабочего места и др.

В последнее время в Сербии было проведено значительное число исследований с целью выяснения причин

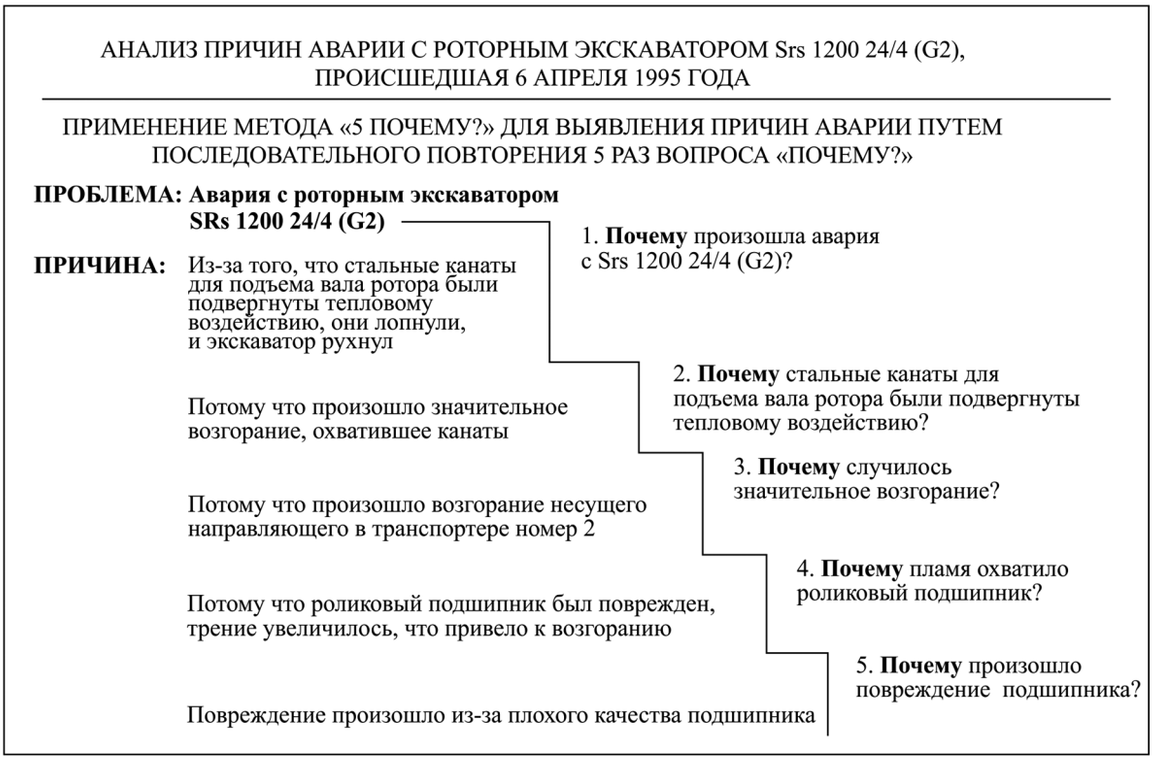


Рисунок 6 – Применение метода «5 Почему?»: Выявление основной причины аварии путем пятикратного повторения вопроса «Почему?».

отказов оборудования, эксплуатируемого на угольных разрезах. Один из отчетов опубликован в работе [5]. Исследования показывают, что ошибки персонала (операторов, специалистов по техническому обслуживанию) играют ключевую роль в возникновении аварий, что подтверждается данными таблицы 1.

Анализ этих данных показывает, что на человеческий фактор приходится 87% причин аварий горной техники. Исходя из этого, на основе рисунка 6 мы можем заключить, что «плохое качество подшипника» опорного ролика также связано с человеческим фактором, т.е. ошибкой персонала при окончательном контроле качества, входном контроле или даже с неверным выбором поставщика подшипников.

5.2 Исследование влияния человеческого фактора на плохое качество подшипника в составе многоковшового экскаватора

Исследование влияния человеческого фактора на возникновение проблемы низкого качества подшипника на многоковшовом экскаваторе SRs 1200 24/4 (G2) проводилось в режиме коллективного обсуждения сотрудниками компании «Колубара Метал». При этом коллектив работал в соответствии со всеми рекомендациями по организации «мозговой атаки» [16]. Основные рекомендации касались состава коллектива, порядка его работы, обязанностей его руководителя. Коллектив вырабатывал идеи относительно причин проблем технического обслуживания, которые требуют решения.

Таблица 1. Процентное распределение причин аварий экскаваторов

Причина аварии	Процентная доля
Плохая подготовка пути движения экскаватора (человеческая ошибка)	27
Ошибка при изготовлении деталей и при сборке экскаватора на угольном разрезе (человеческая ошибка)	22
Ошибка оператора	18
Ошибка специалиста по техническому обслуживанию	13
Усталость материалов, износ оборудования и коррозия	8
Ошибки в проектировании (человеческая ошибка)	7
Прочие факторы	5

В этих исследованиях применялось правило, которое может быть использовано для составления исходной (общей) причинно-следственной диаграммы, и это правило применимо для большинства реальных ситуаций. Правило состоит в том, что почти всегда существует некоторое число категорий возможных причин определенных последствий (нежелательных результатов) процесса. В процессе решения конкретной проблемы,

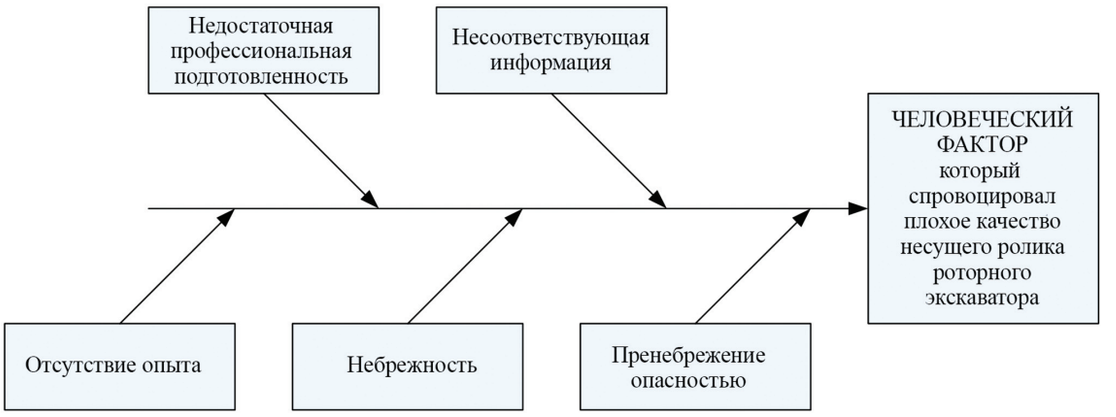


Рисунок 7 – Причины человеческой ошибки. [6]

связанной с аварией многоковшового экскаватора, исследователи установили, от каких факторов (причин) и в какой степени зависит нежелательный результат или последствие: *«Человеческая ошибка, с которой связано низкое качество подшипника опорного ролика на многоковшовом экскаваторе SRs 1200 24/4 (G2)»*.

В исследованиях было, прежде всего, проведено определение и обобщение пяти примеров, как показано на рисунке 7:

- отсутствие подготовки;
- недостоверная информация;
- отсутствие опыта;
- неосторожность;
- пренебрежительное отношение к опасности.

Эта проблема может быть в дальнейшем решена за счет определения причин человеческих ошибок второго и более высоких порядков.

6. Человеческий фактор при моделировании аварий

6.1 Модель типа «швейцарский сыр» причин, вызванных человеческой ошибкой

В большинстве случаев ответственность за аварии и техногенные катастрофы возлагают на отдельные (личные) человеческие ошибки. Но в своей книге «Управление риском организационных аварий» [17] профессор психологии Манчестерского университета Джеймс Ризон подробно исследует вопрос о том, может ли одна человеческая ошибка вызвать аварию, исключая случаи явного саботажа или террористической деятельности. Доказано, что условием возникновения аварии служит целый спектр скрытых и вовремя не обнаруженных ошибок. Культура безопасности и проблемы, которые приводят к указанным ошибкам, обычно, называются «человеческим фактором» [18]. Ведь именно в виду человеческого фактора оператор или специалист по техническому обслуживанию системы принимает неверные решения.

Почему происходят аварии, какие условия их вызывают, какие факторы способствуют их возникновению? Аварии, как правило, происходят не в результате какой-то отдельной ошибки, а являются следствием скрытых, своевременно не выявленных повреждений и отказов, которые накладываются друг на друга и могут привести к ряду нежелательных событий. Следовательно, большинство аварий и инцидентов является следствием целого ряда событий.

Такой атрибут аварии лучше всего описывается моделью «швейцарского сыра», разработанной Джеймсом Ризоном [19] и иллюстрирующей различные виды человеческого «участия» в аварии технических систем. Модель Ризона «швейцарский сыр» объясняет, каким образом люди способствуют нарушению работоспособности сложных и взаимосвязанных технических систем, вызывая, таким образом, аварии.

Если состояние определенной технической системы представить в виде ломтика сыра с отверстиями, то в зависимости от времени проявления виды отказов могут быть следующие:

- скрытые отказы (дефекты);
- активные отказы (дефекты).

Скрытые дефекты (скрытые отказы, скрытые условия, сроки, режимы) представляют собой результат решений или рабочих процессов, который были реализованы задолго до наступления аварии. Эти дефекты и их последствия могут оставаться необнаруженными в течение длительных периодов времени (многих лет). Такие ошибки (виды отказов) обычно происходят на уровне принятия решений и определения правил и положений, либо на уровне оперативного управления, т.е. совершаются лицами, далекими от произошедшей аварии, как во времени, так и в пространстве. Например, решение об объединении обслуживающего персонала двух разных карьеров (двух предприятий) без обучения стандартизированным процедурам обслуживания горных машин представляет собой наглядный пример скрытого дефекта (скрытого отказа).

Активные дефекты (активные отказы, активные ошибки) представляют собой ошибки или нарушения, которые немедленно (без задержки) оказывают неблаго-

приятное воздействие. Такие ошибки обычно совершаются операторами или специалистами по техническому обслуживанию горных машин. Когда оператор или специалист по техническому обслуживанию вместо вращения экскаватора осуществляет подъем его надстройки, являются показательным примером такого рода ошибок (отказов).

7. Теория риска событий типа «Черный лебедь»

7.1 «Черный лебедь. Под знаком непредсказуемости» [19]

Математик и экономист Нассим Николас Талеб в своей книге 2007 года «Черный лебедь. Под знаком непредсказуемости» [19] предложил концепцию «черного лебедя», т.е. неожиданного (непредсказуемого) и значительного (всеобъемлющего) явления, которое существенно меняет ход истории. Эта концепция включает в себя войны, экономические кризисы, появление интернета и т. д. Предсказать их невозможно, но мы должны знать, как с ними жить.

«Черные лебеди» по своей природе непредсказуемы, поскольку подобных событий раньше никогда не происходило. Однако то, как компании и люди, пережившие определенные катастрофические события, справились с их последствиями, изучать можно. Такой анализ мог бы подготовить компанию к разработке стратегии возобновления нормальной работы после чрезвычайных ситуаций (в частности техногенных, например аварий горной техники) в кратчайшие возможные сроки и с минимальными потерями.

Нассим Талеб предложил теорию риска «Черный лебедь», которая рассматривает события, которые трудно предсказать, и редкие события, которые имеют значительные последствия. «Черный лебедь» – метафора, описывающая неожиданные события, влекущие значительные последствиями.

«Если вы всю жизнь видели только белых лебедей, это не значит, что черных лебедей не существует», – пишет Нассим Талеб в своей книге «Черный лебедь. Под знаком непредсказуемости» [19].

7.2 Критерии событий типа «Черный лебедь» и аварий многоковшовых экскаваторов

Авария многоковшового экскаватора SRs 1200 24/4 (G2), которая произошла 6 апреля 1995 года, имеет все указанные характеристики, т. е. удовлетворяет критериям события типа «Черный лебедь». То, что Нассим Талеб называет «Черным лебедем» – это событие, которое имеет три следующие характеристики:

- событие происходит неожиданно;
- событие имеет значительные последствия;
- впоследствии находится разумное объяснение события так, будто оно было ожидаемо.

До аварии 6 апреля 1995 года указанный многоковшовый экскаватор произвел выемку 160 млн. м^3 вскрыши. То, как авария экскаватора отразилась на выработке, видно из цифр годовой отчетности, которые показывают падение с 5 до 7 млн. м^3 вскрыши (рисунок 8).

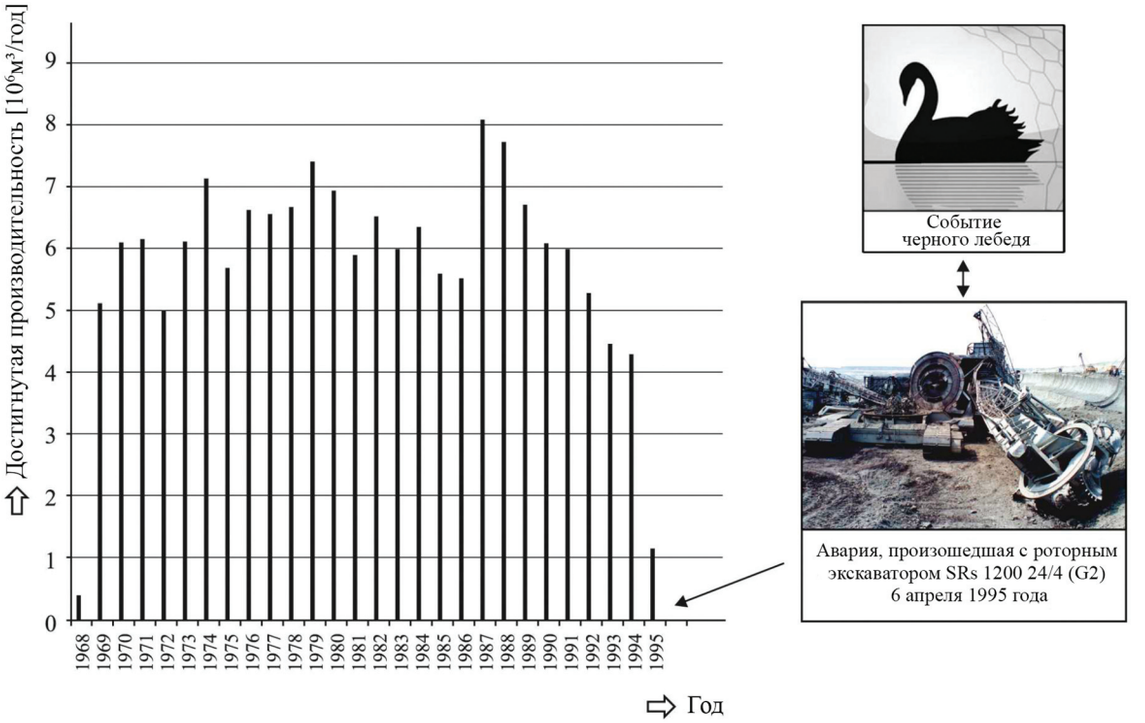


Рисунок 8 – Авария многоковшового экскаватора SRs 1200 24/4 (G2) – типичный «Черный лебедь».

Поскольку такие аварии непредсказуемы, задачей владельца опасного объекта является принятие мер по снижению влияния отрицательных последствий на персонал, население и окружающую среду. В этой связи перед государством стоит цель побудить владельцев соответствующих объектов строго выполнять указания и положения нормативных правовых документов отделами техники безопасности [21].

По мере роста безотказности и сложности технических систем влияние «человеческого» фактора также становится более значительным. Следовательно, важнейшими задачами теории и практики обеспечения безопасности технических систем остается развитие культуры безопасности и создание некарательной производственной среды.

8. Отчет «Тойота» А3 как инструмент решения задач

Составлению Отчетов «Тойота» А3 обучают всех сотрудников компании «Тойота», в первую очередь руководителей низшего звена. Существует универсальный набор состояний и рекомендаций, которые используются при обучении для решения проблем и формирования Отчета «Тойота» А3. Ниже приведены выдержки из данного документа [22].

А. Рекомендации по решению проблем:

• оценивайте ситуацию исходя из фактов;

• отслеживайте (контролируйте, наблюдайте) проблему;

• сосредоточьтесь на одной проблеме (одна проблема на один Отчет «Тойота» А3);

• следите за изменениями в месте появления проблемы;

• детально изучите причину и проанализируйте все факты и данные;

• при необходимости примите временные меры для обнаружения места возникновения проблемы;

• определите основную причину;

• разработайте корректирующие меры, дайте указания и определите сроки выполнения.

Б. Рекомендации по формированию Отчета «Тойота» А3:

• распределите время таким образом, чтобы иметь возможность оценить ситуацию в целом (используйте широкий круг сведений, опирайтесь на факты, а не мнения, учитывайте отдаленные последствия);

• ориентируйтесь на конкретных людей; учитывайте их потребности и понимание ситуации;

• подготавливайте наглядные материалы в соответствии с ценностями и философией компании;

• избегайте использования большого количества слов, отдавайте предпочтение схемам, графикам и другим формам ясного представления информации;

• все слова должны относиться к сфере профессиональной деятельности; используйте точные выражения и избегайте жаргонизмов;

• оценивайте ясность изложения материала; обеспечивает ли оформление отчета четкое понимание изложенной информации?

Интересная аналогия может быть проведена с организацией рабочего пространства на основе принципов «Метода 5S» [15] на заводах «Тойота» при составлении Отчета «Тойота» А3. На бережливом производстве не допускается перегружать рабочее место излишками предметов снабжения, поскольку это влечет за собой убытки [22]. Рациональное использование пространства является залогом создания добавленной стоимости. Присутствие ненужных предметов снижает безопасность, создает беспорядок и мешает обнаруживать отклонения от нормального режима работы. Аналогичным образом при составлении Отчета «Тойота» А3 важно не допускать потерь: лишних слов, пространных объяснений, ненужных схем, которые мешают понять суть изложенного. Таким образом, обеспечивается максимальная эффективность в создании добавленной стоимости. Недостатки документации затрудняют понимание информации и зачастую приводят к тому, что люди теряют из вида ключевой момент.

Отчет «Тойота» А3 и способ его подготовки обеспечивают четкость и оперативность информационного взаимодействия. Использование Отчета «Тойота» А3 способствует положительным изменениям. Так, если использование Отчета «Тойота» А3 приводит к изменениям в стандартах или росту объема имеющихся знаний, то база данных обновляется. Бережливое мышление [23] требует извлечения уроков из решенных задач (а не только исправления сложных ситуаций), и использование Отчета «Тойота» А3 этому способствует.

9. Отчет «Тойота» А3 и цикл Деминга

Стремление компании «Тойота» к экспериментам лежит в основе всех стандартизированных операций и процессов, которые являются частью повседневной работы. Компания «Тойота» преобразовала цикл Деминга (планирование – выполнение – проверка – воздействие), т.е. процесс постоянного совершенствования рабочего процесса, который широко применяется в различных областях хозяйства, в уникальную методологию – Отчет «Тойота» А3. Это отражает культуру «Тойота» [24], где умение решать проблемы считается важнейшим качеством сотрудника, которое формируется с самого начала его карьеры и постоянно совершенствуется в процессе обучения.

Акио Мацубара, бывший исполнительный директор по управлению персоналом, а позже президент Toyoda Gosei North America Corporation говорит [24]:

"Все сотрудники развивают в себе навык решения проблем, который лежит в основе рабочих процессов в компании «Тойота». Философия компании «Тойота» такова: решая проблему, сотрудник вносит свой вклад в реализацию корпоративной политики, ориентированной на удовлетворение потребностей клиентов. Мы говорим

ИНСТРУМЕНТ TOYOTA A3 REPORT

РЕШЕНИЕ ПРОБЛЕМЫ
АВАРИЯ, ПРОИСШЕДШАЯ С ЭКСКАВАТОРОМ Srs 1200 24/4 (G2) 6 АПРЕЛЯ 1995 ГОДА
НА ОТКРЫТОЙ УГОЛЬНОЙ РАЗРАБОТКЕ ПОЛЕ D, КОЛУБАРА, ЭЛЕКТРОЭНЕРГЕТИКА СЕРБИИ

План

ИСХОДНАЯ ИНФОРМАЦИЯ

ВИД ЭКСКАВАТОРА SRs 1200 24/4 (G2)
ПРИ НОРМАЛЬНОЙ ЭКСПЛУАТАЦИИ ДО АВАРИИ

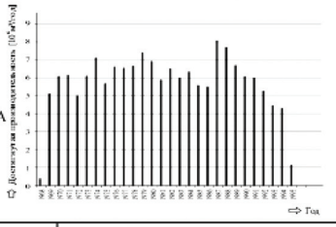
ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ЭКСКАВАТОРА
SRs 1200 24/4 (G2) ДО АВАРИИ

Характеристики	Величина
Теоретическая производительность	3,456м³/ч
Мощность двигателя	400кВт

ОПИСАНИЕ СИТУАЦИИ

ВИД РОТОРНОГО ЭКСКАВАТОРА Srs 1200 24/4 (G2)
ПОСЛЕ АВАРИИ ПРОИСШЕДШЕЙ 6 АПРЕЛЯ 1995 ГОДА

ФАКТИЧЕСКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ ДОБЫЧИ ЭКСКАВАТОРА ПО ГОДАМ С МОМЕНТА ЗАПУСКА В 1968 ГОДУ ДО МОМЕНТА АВАРИИ В 1995 ГОДУ



ЦЕЛЬ

ЦЕЛЬ РЕВИТАЛИЗАЦИИ РОТОРНОГО ЭКСКАВАТОРА Srs 1200 24/4 (G2)

Цель программы ревитализации роторного экскаватора Srs 1200 24/4 (G2), поврежденного в процессе аварии 6 апреля 1995 года: восстановить роторный экскаватор, приведя его в состояние готовности добывать как вскрышные породы, так и уголь

ПРИЧИННО-СЛЕДСТВЕННЫЙ АНАЛИЗ

ПОВРЕЖДЕНИЕ ИЗ-ЗА ПРОИЗОШЕДШЕЙ АВАРИИ РОТОРНОГО ЭКСКАВАТОРА

Прямые потери из-за аварии	Непрямые потери из-за аварии
Создание проекта, разборка, транспортировка экскаватора, производство и восстановление элементов, сборка, запуск в эксплуатацию 7.500.000.00 евро	Потери из-за не выработки пород на поле открытой разработки в процессе ревитализации в течение 9 лет: 157.000.000.00 евро

АНАЛИЗ ПРИЧИН АВАРИИ С РОТОРНЫМ ЭКСКАВАТОРОМ Srs 1200 24/4 (G2), ПРОИСШЕДШАЯ 6 АПРЕЛЯ 1995 ГОДА

ПРИМЕНЕНИЕ МЕТОДА «5 ПОЧЕМУ?» ДЛЯ ВЫЯВЛЕНИЯ ПРИЧИН АВАРИИ ПУТЕМ ПОСЛЕДОВАТЕЛЬНОГО ПОВТОРЕНИЯ 5 РАЗ ВОПРОСА «ПОЧЕМУ?»

ПРОБЛЕМА: Авария с роторным экскаватором SRs 1200 24/4 (G2)

ПРИЧИНА: Из-за того, что стальные канаты для подъема вала ротора были подвергнуты тепловому воздействию, они ослабли, и экскаватор рухнул

1. **Почему произошла авария с Srs 1200 24/4 (G2)?**

Потому что произошло значительное возгорание, охватившее канаты

2. **Почему стальные канаты для подъема вала ротора были подвергнуты тепловому воздействию?**

Потому что произошло возгорание ведущего направляющего в трансформаторе номер 2

3. **Почему случилось значительное возгорание?**

Потому что роликовый подшипник был поврежден, трение увеличилось, что привело к возгоранию

4. **Почему плавился ролликовый подшипник?**

Повреждение произошло из-за плохого качества подшипника

5. **Почему произошло повреждение подшипника?**

Мероприятия, Контроль, Действия

МЕРЫ ПО ПРЕОДОЛЕНИЮ ПРОБЛЕМЫ

ТЕНДЕР НА РЕВИТАЛИЗАЦИЮ РОТОРНОГО ЭКСКАВАТОРА SRs 120024/4 (G2)

С момента ввода в эксплуатацию м 1968 года экскаватор выкопал более 160 миллионов м3 вскрышных пород. Отметив необходимость компенсации этой мощности, нехватка которой еще больше поставила под угрозу производство на карьерном месторождении D электроэнергетики Сербии, было принято решение об открытии международного тендера на активизацию работы роторного экскаватора SRs 1200 24/4 (G2), с помощью льготного кредита от немецкого правительства. Для реализации данного проекта был предоставлен кредит от KFW bank на сумму 7,588,641,00 евро.

РЕВИТАЛИЗАЦИЯ ЭСКАВАТОРА УЧАСТНИКИ

В качестве основного подрядчика на тендере работу по восстановлению роторного экскаватора SRs 1200 24/4 (G2) получила немецкая компания FAM из Магдебурга, которая наняла основных субподрядчиков:
• для механической части, включая интенсивнейшее инженерство, ревитализацию, изготавление и сборку – Компания по обработке металлов Колубары и компания из Vrcoce,
• для проектирования, производства и надзора за монтажом электрических деталей – компания ABB от Cottbus.

ПРОЦЕСС РЕВИТАЛИЗАЦИИ ЭКСКАВАТОРА

Процесс ревитализации экскаватора развивался в двух основных направлениях:
активизация существующего оборудования и строительства, которое было оценено как пригодное для использования, в цехах компании "Колубара металл", изготовление нового оборудования в соответствии с базовым инжинирингом FAM и ABB для электрооборудования.

ПРОЦЕСС СБОРКИ ЭКСКАВАТОРА

Процесс сборки экскаватора имел несколько ключевых этапов:
• установка радиально-осевого подшипника на движущийся станок карусель ,
• вращение платформы;
• подъем и установка столба массой более 801 и при этом использовались 4 подъемника, один из которых имел грузоподъемность 3001,
• поднимающий вал противовеса вместе с электронными контейнерами со встроенным электрооборудованием общей массой более 1101,
• подниматься и ограничивать вала ротора,
• установка 14 ковшей Ротора.
• установка лебедок для подъема вала ротора и опорных канатов,
• оснащение и обеспечение надежности перегрузочного устройства электрооборудования, кабелей и поддерживающей конструкции были встроены на ковшовый экскаватор во время установки.

Около 115 тонн электрического оборудования, проводов и вспомогательных деталей было загружено на роторный экскаватор при его установке.

ПОДТВЕРЖДЕНИЕ ЭФФЕКТА

РЕВИТАЛИЗАЦИЯ РОТОРНОГО ЭКСКАВАТОРА SRs 1200 24/4 (G2) (год 2004)

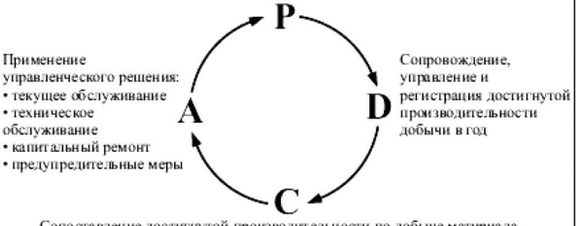
ТЕХНИЧЕСКИЕ ПРЕИМУЩЕСТВА ОТ РЕВИТАЛИЗАЦИИ ЭКСКАВАТОРА
Основные характеристики восстановленного экскаватора SRs 1201 24/4 (G2)

Характеристики экскаватора	Величины
Теоретическая производительность	4100 м³/ч
Мощность ротора	630 кВт
Тройной привод вращательного движения верхней конструкции	
Полностью новая стальная конструкция верхней части	
Впервые в Сербии был применен контейнерный принцип для реализации электрооборудования	
Двигатель настраиваемый по частоте/привод	
Актуальные решения по секции управления	

ФУНКЦИИ УПРАВЛЕНИЯ

ЦИКЛ ДЕМИНГА ПО НЕПРЕРЫВНОМУ УЛУЧШЕНИЮ ПРОЦЕССА ПРОИЗВОДСТВА

Цель: производительность экскаватора 5-10⁶м³/год



Сопоставление достигнутой производительности по добыче матириала с запланированной и внесение предложений по усовершенствованию (корректирующие меры)

Рисунок 9 – Отчет «Тойота» А3 как инструмент решения проблем: Авария многоковшового экскаватора SRs 1200 24/4 (G2), произошедшая 6 апреля 1995 года.

нашим людям, что умение решать проблемы необходимо для достижения успеха в «Тойота»."

Отчет «Тойота» А3 читается сверху вниз, слева направо и используется для решения проблем, обновления сведений и внесения предложений. Отчет «Тойота» А3 построен в соответствии с циклом непрерывного совершенствования Деминга.

10. Отчет «Тойота» А3 о решении проблем в связи с аварией многоковшового экскаватора SRs 1200 24/4 (G2)

10.1 Практическое решение проблемы

Процесс решения проблем, возникших в процессе работы, может быть описан логической последовательностью цикла непрерывного совершенствования Деминга, а Отчет «Тойота» А3 включает в себя следующие семь этапов: исходная информация, текущее состояние, цель, причинно-следственный анализ, корректирующие меры, подтверждение действия, дальнейшие действия. Этот процесс основан на наблюдениях, проведенных в компании «Тойота» и опубликованных в [2].

Окончательный вид Отчета «Тойота» А3 по аварии многоковшового экскаватора SRs 1200 24/4 (G2), произошедшей 6 апреля 1995 года на угольном разрезе «Месторождение D» рудного бассейна «Колубара» компании «Электроэнергетика Сербии», которая ранее была частично проанализирована в [26], показан на рисунке 9.

11. Выводы

Отчет «Тойота» А3 – гибкое средство решения проблем, возникающих в ходе работы – был адаптирован к нуждам эксплуатации горных машин (экскаваторов, транспортеров и др.) на карьерах. Учитывая большой объем имеющихся данных и сведений о таких сложных процессах, как процесс добычи угля и вскрышных работ на карьере, их сбор, возможно, потребует большого количества времени. По этой причине документирование с использованием Отчета «Тойота» А3 имеет большое значение для ускорения коммуникации и сокращения потери времени при работе. Это представляет собой важный шаг в реализации концепции бережливого производства и системы Кайдзен на карьере рудного бассейна «Колубара» в г. Лазаревац компании «Электроэнергетика Сербии».

Отчет «Тойота» А3 имеет потенциальные недостатки, связанные с решением конкретной проблемы аварии многоковшового экскаватора SRs 1200 24/4 (G2). Кажется, что он перегружен информацией и переусложнен. Это нормальная реакция, учитывая сложность документа и то, как много информации (данных) изложено на небольшом листе. Безупречных Отчетов «Тойота» А3 не существует. Каждый раз, когда возникает необходимость в составлении такого отчета, существует способ улучшить его содержание или форму.

Библиографический список

1. **Papic L.** Implementation Methodology for Risk Minimization into Maintenance Process of Production System at Coal Mines, Report of Contract No. 4617 (In Serbian) [Text] / L. Papic, M. Pantelic. – DQM Research Center – Kolubara Metal Company, 2009.

2. **Sobek II Durward K.** Understanding A3 Thinking. A Critical Component of «Toyota»'s PDCA Management System [Text] / K. Sobek II Durward, A. Smalley. – CRC Press, Tailor and Francis Group, 2008.

3. **Krafcik J.F.** Triumph of the Lean Production System [Text] / J.F. Krafcik // Sloan Management Review. – 1988. – Vol. 30. – P. 41-52.

4. **Dhillon B.S.** Mining Equipment Reliability, Maintainability and Safety [Text] / B.S. Dhillon. – Springer, 2008.

5. **Pantelic M.** Maintainability and Safety Engineering of Excavator Units (In Serbian) [Text] / M. Pantelic, L. Papic, J. Aronov. – DQM Research Center, 2011.

6. **Papic L.** Safety Based Maintenance Concept [Text] / L. Papic, J. Aronov, M. Pantelic // International Journal of Reliability, Quality and Safety Engineering. – 2009. – Vol. 16. – № 6. – P. 1-17.

7. **Papic L.** Statistical Safety Analysis of Maintenance Management Process of Excavator Units [Text] / L. Papic, M. Pantelic, J. Aronov // International Journal of Automation and Computing. – 2010. – Vol. 7. – № 2. – P. 146-152.

8. **Papic L.** Maintenance-Oriented Safety Control Charts [Text] / L. Papic, M. Pantelic // International Journal of Systems Assurance Engineering and Management. – 2014. – Vol. 5. – № 2. – P. 149-154.

9. **Papic L.** System Safety Analysis Via Accident Precursors Selection [Text] / L. Papic, M. Pantelic, J. Aronov // Dynamics of Information Systems. Springer Proceedings in Mathematics & Statistics. – 2014. – Vol. 105. – P. 179-204.

10. **Папич Л.** Интервальная оценка коэффициента готовности многоковшового экскаватора на основе бутстреп-моделирования [Текст] / Л. Папич, И.В. Гадолина, Р.И. Зайнетдинов // Проблемы машиностроения и надежности машин. – 2016. – № 6. – С. 55-62.

11. **Гадолина И.В.** Уточнение инженерной методики оценки скорости износа элементов рабочих органов экскаваторов [Текст] / И.В. Гадолина, П.А. Побегайло, Д.Ю. Крицкий и др. // Надежность. – 2019. – Т.19, № 1. – С. 18-23.

12. **Антонов А.В.** Исследование модели учета отказов по общей причине бета-фактора [Текст] / А.В. Антонов, В.А. Чепурко, А.Н. Черняев // Надежность. – 2019. – Т.19, № 2. – С. 9-17.

13. **Похабов Ю.П.** Проблемы надежности и пути их решения при создании уникальных высокоответствен-

ных систем [Текст] / Ю.П. Похабов // Надежность. – 2019. – Т.19, № 1. – С.10-17.

14. **Weigand B.** Lean Maintenance System, Zero Maintenance Time – Full Added Value [Text] / B. Weigand, R. Langmaack, T. Baumgarten. – Lean Management Institut, 2005.

15. **Hirano H.** 5S for Operators: 5 Pilars of the Visual Workplace [Text] / H. Hirano. – New York: Productivity Press, 1996.

16. **Dale B.G.** Managing Quality [Text] / B.G. Dale. – Oxford: Blackwell Publishers Ltd., 1999.

17. **Reason J.** Managing the Risks of Organizational Accidents [Text] / J. Reason. – Manchester: University of Manchester, 1997.

18. **Dhillon B.S.** Safety and Human Error in Engineering Systems [Text] / B.S. Dhillon. – Boca Raton: CRC Press, Taylor and Francis Group, 2013.

19. **Reason J.** Human Error [Text] / J. Reason. – Cambridge: Cambridge University Press, 1990.

20. **Taleb N.N.** The Black Swan: The Impact of the Highly Improbable [Text] / N.N. Taleb. – New York: Random House, 2007.

21. **Aronov J.** Reliability and Safety Management of Engineering Systems Through the Prism of Black Swan Theory [Text] / J. Aronov, L. Papic // System Reliability Management, Solutions and Technologies. – 2018. – P. 103-112.

22. **Morgan J.M.** The «Toyota» Product Development System. Integrating People, Process and Technology [Text] / J.M. Morgan, J.K. Liker. – New York: Productivity Press, 2006.

23. **Womack J.P.** Lean Thinking. Banish Waste and Create Wealth in your Corporation [Text] / J.P. Womack, D.T. Jones. – New York: Free Press, 2003.

24. **Liker J.K.** «Toyota» Culture. The Heart and Soul of the «Тойота» Way [Text] / J.K. Liker, M. Hoseus. – New York: McGraw Hill, 2008.

25. **Osono E.** Extreme «Toyota», Radical Contradictions That Drive Success at the World's Best Manufacturers [Text] / E. Osono, N. Shimizu, H. Takeuchi and others. – New York: John Wiley and Sons Inc., 2008.

26. **Papic L.** A3 Report as an Effective Tool for Excavator Accident Problem Solving (In Serbian) [Text] / L. Papic, M. Pantelic // Proceedings of 21st DQM International Conference on Dependability and Quality Management. – 2018. – P. 3-13.

Сведения об авторах

Любиша Папич – доктор технических наук, профессор, директор Исследовательского центра по управлению качеством и надежностью (DQM), Чачак, Сербия, e-mail: dqmcenter@mts.rs

Ирина В. Гадолина – кандидат технических наук, доцент, старший научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт машиноведения им. А.А. Благонравова Российской академии наук, Москва, Российская Федерация, e-mail: gadolina@mail.ru

Милорад Пантелич – доктор технических наук, директор предприятия «Колубара Метал», г. Лазаревац, Сербия, доцент на Техническом факультете Чачак, Крагуевацкий университет, Сербия**.**

Неда Папич – бакалавр наук по специальности «Промышленная инженерия», студент магистратуры по специальности «Промышленная инженерия»**.** Факультет технических наук, Университет, г. Нови Сад, Сербия.

Вклад авторов в статью

Любиша Папич

Обоснована целесообразность и необходимость применения отчета А3 в задачах управления предприятий, связанных с горнодобывающей промышленностью. На конкретном примере анализа аварии роторного экскаватора продемонстрированы этапы выполнения анализа.

Ирина В. Гадолина

Более детальная проработка информации о текущем состоянии надежности экскаватора, касающаяся вопросов вариабельности коэффициента готовности, построены доверительные интервалы для данной характеристики.

Пантелик Милорад

Осуществлял оперативный контроль за ходом работ по восстановлению экскаватора после аварии. Проводил сбор информации от отказах рабочих органов экскаватора и его подсистем. Организовал предоставление графиков выполнения ремонтных работ.

Папич Неда

Обеспечила представление информации в подобающем для написания статьи виде. Обеспечила дизайн и верстку статьи.

Оригинальная статья
https://doi.org/10.21683/1729-2646-2019-19-4-45-52

Предпосылки для создания цифровой системы управления безопасностью движения

Алексей М. Замышляев, *АО «НИИАС», Российская Федерация, Москва*

Алексей М. Замышляев

Резюме. Цель. *Цифровая трансформация системы управления безопасностью движения в холдинге ОАО «РЖД» предусматривает переход на глобальный уровень взаимодействия с процессами всех подразделений по интегральной оценке риска возможных событий и достижению установленных показателей. Итогом станет интеграция системы управления безопасностью движения с производственными процессами на всех уровнях управления холдинга «РЖД» на основе интегрированной интеллектуальной системы управления процессами и услугами со встроенными функциями оперативного управления безопасностью движения.* **Методы.** *В работе применяется системный анализ существующих подходов и методов обработки структурированных и неструктурированных данных значительных объемов.* **Результаты.** *Проведено рассмотрение стадий развития управления безопасностью движения поездов, а также информационных автоматизированных систем управления, применяемых в целях управления безопасностью движения. Выполнен анализ общих тенденций создания систем сбора и обработки информации. Показана целесообразность внедрения в современные системы управления таких технологий, как Big Data, Data Mining, Data Science. Рассмотрена эффективность применения указанных технологий на примере анализа влияния различных факторов на среднесуточную производительность локомотива, где на первом уровне учитываются такие факторы, как среднесуточный пробег локомотива, средний вес поезда; на втором уровне – участковая скорость, оборот локомотива на станции и др.; на шестом уровне – тип локомотива, его техническое состояние и т.д. Всего учитывается более 50 факторов, влияющих на среднесуточную производительность локомотива. Показано, что с помощью статистических методов факторного анализа и анализа связей в сочетании с другими методами Data Mining, такими, как методы моделирования и прогнозирования, можно выполнить проактивное планирование среднесуточной производительности локомотива. Предложена схема перехода к цифровой системе управления безопасностью движения на основе построения моделей взаимодействия факторов безопасности и надежности всех объектов железнодорожного транспорта на всех уровнях иерархии, а также во взаимосвязи с другими факторами, которые непосредственно не относятся к надежности, однако оказывают влияние на безопасность перевозочного процесса.* **Выводы.** *Основной результат перехода на технологию Big Data состоит в создании динамической модели управления безопасностью движения, в исключении зависимости системы управления от недостатков человеческого фактора и, что особенно важно, в возможности создания в холдинге «РЖД» интегрированной интеллектуальной системы управления процессами и услугами со встроенными функциями оперативного управления безопасностью движения. В результате масштабного развития и внедрения в компании Единой корпоративной платформы (ЕКП) УРРАН реализуется поддержка принятия управленческих решений по обеспечению надежности и безопасности функционирования объектов транспорта на основе оценки рисков. Таким образом, с помощью ЕКП УРРАН заложены основы цифровой трансформации системы управления безопасностью движения в холдинге «РЖД».*

Ключевые слова: *безопасность движения поездов, факторный анализ, автоматизированная система управления, Big Data, Data Mining, человеческий фактор, прогнозирование рисков.*

Для цитирования: *Замышляев А.М. Предпосылки для создания цифровой системы управления безопасностью движения // Надежность. 2019. № 4. С. 45-52. https://doi.org/10.21683/1729-2646-2019-19-4-45-52*

Поступила 25.09.2019 г. / После доработки 30.10.2019 г. / К печати 14.12.2019 г.

Введение

Безопасность движения поездов – одна из главных задач работы холдинга «РЖД» при эксплуатации железной дороги, перевозках пассажиров и грузов. Все организационные и технические мероприятия на железнодорожном транспорте должны отвечать требованиям безопасного и бесперебойного движения поездов. Развитие железных дорог России направлено на повышение интенсивности движения поездов, на увеличение их скорости и массы. При этом увеличивается количество подвижного состава, одновременно курсирующего по железнодорожным путям, значительно усложняется инфраструктура. Это вызывает необходимость повышать требования к качеству и надежности средств обеспечения безопасности движения, а также к профессиональной подготовленности и опыту персонала железных дорог, непосредственно участвующего в реализации движения поездов.

В Политике холдинга «РЖД» в области безопасности движения определены следующие основные цели: минимизация последствий от транспортных происшествий; обеспечение сохранности жизни и здоровья людей; обеспечение сохранности грузов, подвижного состава, объектов инфраструктуры; обеспечение заданного уровня безопасности движения. Широкий спектр задач по обеспечению безопасности движения, с одной стороны, и активное развитие железных дорог России, подвижного состава и инфраструктуры, с другой стороны, вызвали необходимость коренной перестройки существующей системы управления безопасностью движения поездов путем трансформации ее в цифровую платформу управления.

Этапы автоматизации системы управления безопасностью движения

Сегодня в ОАО «РЖД» используется большое количество автоматизированных систем управления (АСУ), созданных в разное время для решения конкретных задач. Часть из них – современные, часть – требует модернизации и актуализации в соответствии с новыми требованиями.

На ранних стадиях развития управление безопасностью движения основывалось на отчетах о результатах ревизорских проверок и технических ревизий железнодорожных станций и депо. Развитие железнодорожного транспорта вызвало необходимость в автоматизации процессов управления безопасностью движения. В 2005 г. была создана Автоматизированная система контроля и анализа выполнения персоналом станций правил безопасности движения и охраны труда (АИС ДНЧ) [1]. Основное назначение системы – организация в службе движения сбора и систематизации информации о результатах ревизорских проверок и технических ревизий железнодорожных станций по безопасности движения и охране труда, их анализ и определение профилактических мероприятий по предотвращению случаев брака в поездной и маневровой работе и случаев производственного травматизма на станциях. Пользователями системы являются работники ДНЧ всех отделений, руководящий состав службы перевозок, аппарат ревизоров безопасности. В системе активно работают 800 пользователей, сформировано более **700 000 актов проверок**, что заложило основу создания неструктурированного хранилища данных по безопасности движения в Компании на примере отдельно взятого хозяйства.

В 2006 г. была создана Автоматизированная система управления безопасностью движения (АС РБ) [2]. Сегодня она выполняет все необходимые функции, обеспечивающие ввод данных, оповещение, классификацию и учет нарушений безопасности движения, контроль выполнения сроков учета, своевременности и качества расследования нарушений безопасности движения, анализ причин и последствий нарушений, формирование сетевой и дорожной отчетности о нарушениях. Эта система имеет более **5000 пользователей**. С ее помощью сформировано **более 40 000 актов технических ревизий и проверок** аппарата ревизоров безопасности.

Комплексная автоматизированная система учета, контроля устранения отказов технических средств холдинга «РЖД» и анализа их надежности (КАСАНТ) внедрена в 2007 году [2, 3, 4]. Эта система явилась принципиально новым инструментом мониторинга состояния объектов инфраструктуры и подвижного состава Компании. Система гарантирует единство порядка учета и расследования случаев отказов технических средств во всех функциональных хозяйствах, на всех железных дорогах ОАО «РЖД», существенно повышает достоверность и оперативность сбора информации за счет «безбумажной» технологии процесса. За последние три года система КАСАНТ позволила поэтапно перейти на единую систему учета и анализа отказов в работе технических средств. Появилась возможность внедрить комплексные методы оценки эффективности эксплуатационной деятельности, как по отраслевым хозяйствам, так и в целом по компании, с использованием единой общесетевой базы данных учета отказов технических средств.

В различные периоды была выполнена интеграция КАСАНТ с автоматизированными системами Компании: ГИД «Урал-ВНИИЖТ» (Система автоматизированного ведения графика движения поездов), АСУ Э (Автоматизированная система управления Трансэнерго), АС КМО (Автоматизированная система ведения актов комиссионных месячных осмотров станций), АСК ПС (Автоматизированная система контроля технического состояния подвижного состава), АСУВОП (Типовая автоматизированная система выдачи и отмены предупреждений), АСУ-П (Автоматизированная система управления путевым хозяйством), АСУ-Ш-2 (Комплексная автоматизированная система управления инфраструктурой хозяйства сигнализации, централизации и блокировки). В последствии осуществлена интеграция с Единой кор-

поративной автоматизированной системой управления инфраструктурой (ЕК АСУИ), которая объединила в себе АСУ инфраструктурного комплекса и осуществляет информационную поддержку бизнес-процессов по текущему содержанию и ремонту.

С помощью системы КАСАНТ обеспечивается работа более **50 000 пользователей**. Ежесуточно фиксируется **1400 оповещений**. Зафиксировано и проанализировано **2 367 747 отказов технических средств.**

В 2011 г. для анализа нарушений технологических процессов персонала железных дорог, приводящих к нарушениям безопасности движения, была разработана и внедрена на сети дорог система КАСАТ – комплексная автоматизированная система учета и анализа случаев технологических нарушений. Представляет собой программно-аппаратный комплекс учета, анализа случаев технологических нарушений в хозяйствах инфраструктуры холдинга «РЖД». С помощью системы КАСАТ обеспечивается работа более 50 000 пользователей. Ежесуточно фиксируется 960 оповещений. Зафиксировано и проанализировано 6 497 274 технологических нарушений.

Рассмотренные системы в определенной мере обеспечивают автоматизацию процессов управления безопасностью движения. Они позволяет проводить анализ состояния отдельных объектов железнодорожного транспорта. Однако с точки зрения оценки процессов, данные не структурированы. Кроме того, в этих системах разрозненные собственные классификаторы, они работают с различной периодичностью съема информации и, что особенно важно, данные, с которыми они оперируют, имеют различный уровень детализации и различные форматы. К этому следует добавить немаловажное обстоятельство необходимости взаимодействия систем управления безопасностью с большим количеством других транспортных автоматизированных систем (АС), в числе которых 33 системы учета и 8 систем планирования. Все это свидетельствует о необходимости при управлении безопасностью движения обрабатывать громадные массивы разрозненных неструктурированных данных. Классический путь решения задачи – агрегирование данных (например, по опасным событиям, по показателям интенсивности отказов, по ущербам и др.), а также анализ свойств управляемой системы. Этот путь позволяет в некоторой мере выполнять проактивное планирование: выявлять непосредственные причины нежелательных событий и планировать точечные мероприятия, контролировать достижение целевых значений. Однако при управлении безопасностью на железнодорожном транспорте имеет место одних только наименований **данных более 250,** а сами массивы данных оцениваются числами на уровне **миллионов терабайтов**. В этих условиях даже агрегирование данных не дает желаемого эффекта – необходимо переходить к созданию цифровой системы управления безопасностью движения.

Развитие систем сбора и обработки информации о фактических состояниях инфраструктуры и подвижного состава

В различных областях человеческой деятельности имеют место общие тенденции создания систем сбора и обработки информации. В XIX веке наши предшественники извлекали полезную для управления информацию посредством личных наблюдений, ручных измерений, хранили ее в рукописных книгах. Во времена паровозов управленческие решения принимались на основе нескольких мегабайт информации (рисунок 1).

В XX веке появились не только новые вычислительные машины, но и информационные системы, автоматизированные рабочие места. К натурным осмотрам и личному контролю присоединились автоматические

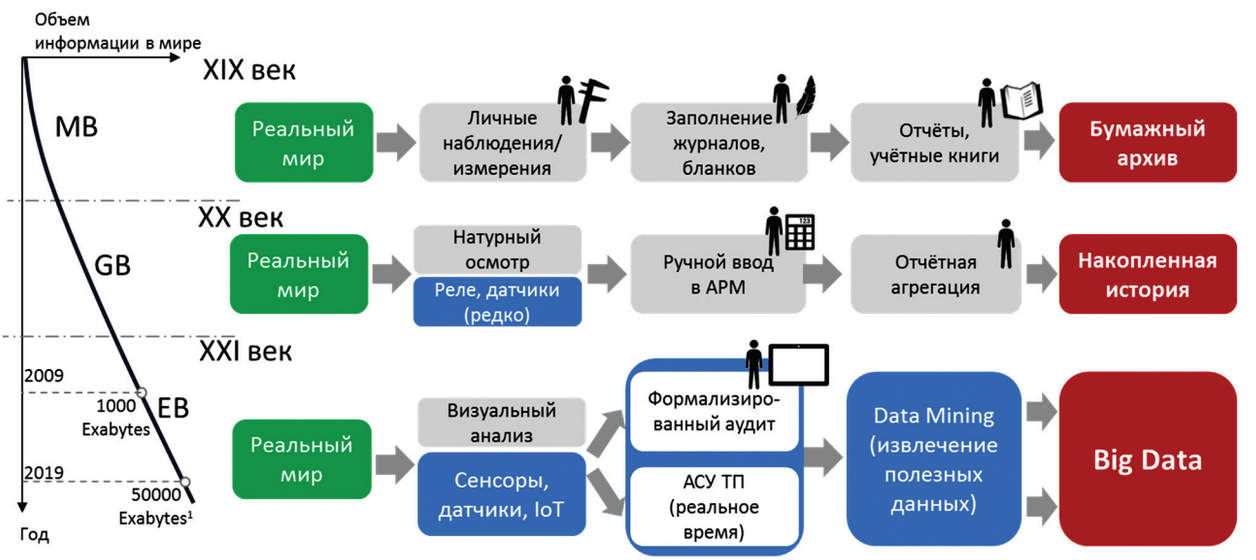


Рисунок 1 – Этапы развития систем сбора и обработки информации.

системы сбора данных, основанные на датчиках, реле. Речь шла уже о гигабайтах информации, которая собиралась, хранилась, анализировалась и использовалась для построения прогнозов. XXI век охарактеризовался взрывным развитием технологий. И сейчас мы говорим об экзабайтах (10^9 гигабайтов) информации. Именно возможность сбора и контроля такого огромного количества данных позволяет использовать современные технологии. Скорости движения, доступные в настоящее время, значительно превосходят способности человеческой реакции. Естественным образом роль человека в системах сбора такого количества данных постепенно уменьшается. Все больше информации о реальном мире собирают сенсоры, диагностические комплексы, появляются технологии взаимодействия искусственных объектов между собой без участия человека.

Большое количество накопленной, а главное, ежедневно получаемой информации не может не изменить наше отношение к ней. Для обеспечения безопасности и надежности перевозочных процессов требуется решать задачи прогнозирования рисков, автоматизации принятия решений. То есть, такие задачи, которые ранее считались прерогативой человека. Теперь уже большая часть этих задач перераспределяется на компьютерную обработку.

Структурированные и неструктурированные данные огромных объемов и значительного многообразия, эффективно обрабатываемые программными средствами, принято называть **Big Data.** Эта технология хранения и обработки «больших данных» альтернативна традиционным технологиям управления базами данных. В качестве определяющих характеристик для больших данных традиционно выделяют «три V»: объем (англ. *volume*, в смысле величины физического объема), скорость (*velocity* в смыслах как скорости прироста, так и необходимости высокоскоростной обработки и получения результатов), многообразие (*variety*, в смысле возможности одновременной обработки различных типов структурированных и полуструктурированных данных) в дальнейшем возникли различные вариации и интерпретации этих признаков.

Не все собранные данные могут быть полезными, поэтому сегодня мы говорим об интеллектуальном подходе к анализу данных, который принято называть **Data Mining** – собирательное название, используемое для обозначения совокупности методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности. Основу методов Data Mining составляют всевозможные методы классификации, моделирования и прогнозирования, основанные на применении деревьев решений, искусственных нейронных сетей, генетических алгоритмов, эволюционного программирования, ассоциативной памяти, нечеткой логики. К методам Data Mining нередко относят *статистические методы* (дескриптивный анализ, корреляционный и регрессионный анализ, факторный анализ, дисперсионный анализ, компонентный анализ, дискриминантный анализ, анализ временных рядов, анализ выживаемости, анализ связей).

Данные – накапливаемые, вновь получаемые, исторические являются основой для перехода на цифровую модель управления процессами на железнодорожном транспорте. В настоящее время в холдинге «РЖД» эта основа создана. Задачей создания цифровой платформы на центральном уровне корпоративного управления ОАО «РЖД» является развитие и внедрение модели комплексной информатизации на основе систем управления, объединенных в единую корпоративную платформу УРРАН (ЕКП УРРАН). Это совокупность нормативно-методологического обеспечения и программно-аппаратных средств, предназначенных для управления объектами инфраструктуры, подвижным составом и технологическими процессами с целью обеспечения гарантированной безопасности и надежности перевозочного процесса в холдинге РЖД [5]. Эта система уже применяется в хозяйствах пути, связи, в Трансэнерго и позволяет проводить автоматическую оценку рисков связанных как с отказами технических средств, так и с нарушениями безопасности движения [6]. Накапливаемая в ней информация позволяет говорить о реальности построения ее и связанных с ней систем КАСАНТ, АС РБ, КАСАТ, КАСКОР, ЕК АСУ И и т. д. на основе технологии Big Data. При этом один из наиболее проблемных вопросов – это структурирование данных. Большое количество неструктурированной информации – это характерная особенность современных многофункциональных АС. По данным международных аудиторов информационных систем [7] до 90% получаемой информации является неструктурированной. Поэтому переход на технологию Big Data необходимо осуществлять на научной основе **Data Science**. При построении моделей интеллектуального анализа данных до 80% времени всего проекта тратится на обработку первоначальных данных, разработку моделей исследований, анализ базовой статистики, разработки моделей регулярных расчетов. Для этого необходимы менеджеры, ставящие стратегические цели анализа, инженеры, понимающие бизнес, ученые, разрабатывающие математические модели. И только после того, как интеллектуальная модель анализа данных будет построена (включая взаимосвязи между всеми системами, участниками, факторами) наступает время технологий Big Data и программных решений.

В связи с очевидностью затрат на построение цифровой системы управления безопасностью и надежностью движения возникает вопрос целесообразности приложения таких усилий. Анализ опыта построения таких систем для промышленных предприятий показывает эффективность подобных работ. Так, проект «когнитивный геолог Газпром» [8] позволил сократить время на разработки проекта с 2 лет до 2 месяцев. Также этот проект показал, что 30% исходных данных, использован-

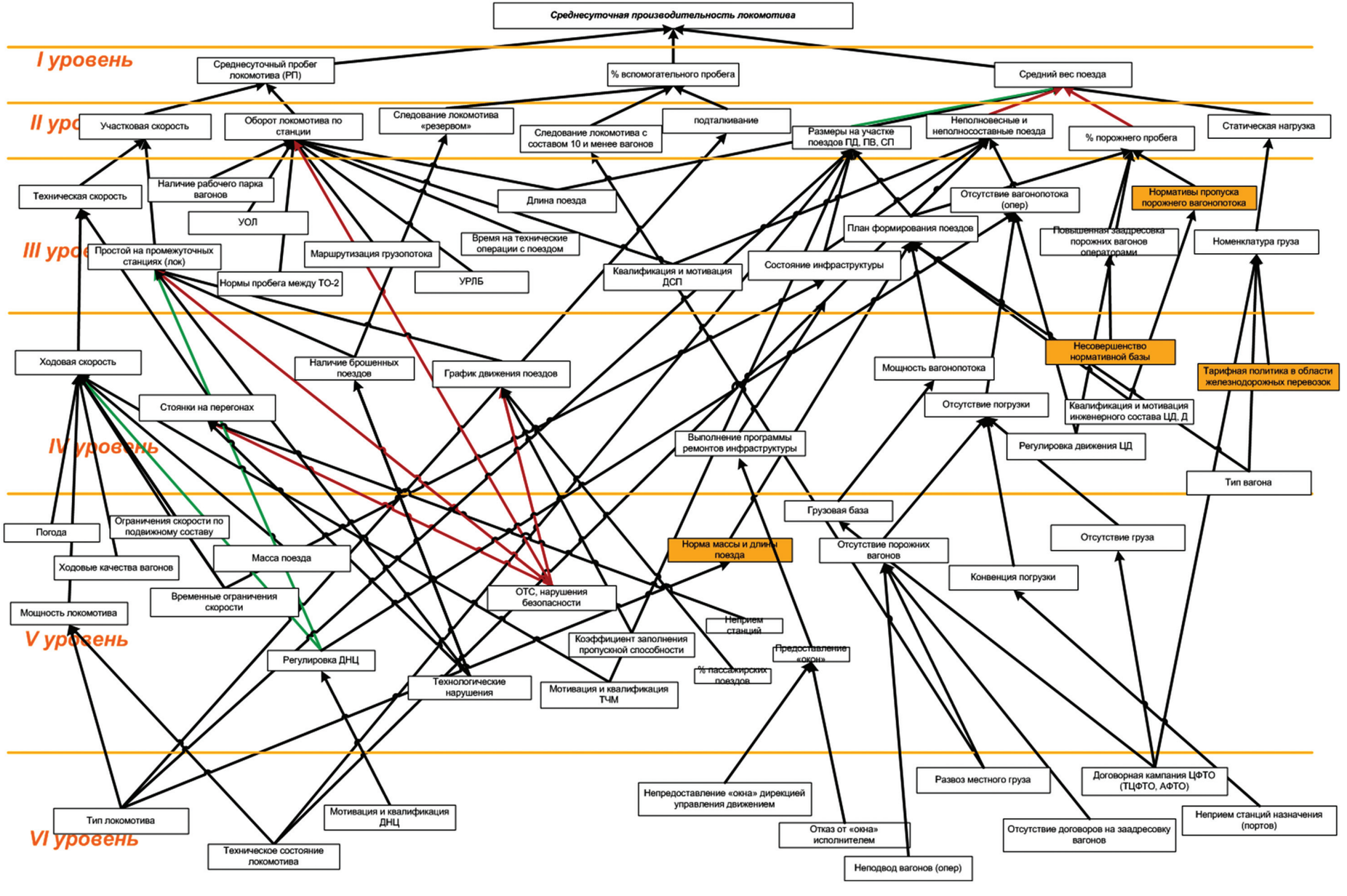


Рисунок 2 – Иерархическая структура влияния факторов на среднесуточную производительность локомотива.

ных раннее, не были полезными. На железнодорожном транспорте Швеции технология Big Data применяется для управления линейными активами, в частности для принятия решения о техническом обслуживании инфраструктуры и подвижного состава [9].

Многофакторный анализ рисков безопасности движения

В основе управления большими данными лежит понимание бизнеса. Применительно к железнодорожному транспорту это означает понимание процессов обеспечения безопасности и надежности перевозочного процесса. В настоящее время в холдинге «РЖД» действует 85 нормативно-методических документов в области безопасности движения и надежности. С помощью АС оценивается безопасность и надежность элементов, железнодорожных систем и технологических процессов. Это настоящее. В будущем ожидается, что современные технологии имитационного моделирования, прогноза рисков позволят осуществлять мониторинг недопустимых состояний, управлять активами на основе принципа ALARP [10, 11], встроить функции безопасности в технологические процессы. Первым шагом движения в такое будущее является разработка структурной схемы управления рисками в области безопасности движения. Эта схема должна включать в себя *методики оценки рисков* безопасности движения (с учетом выбора мер снижения воздействия факторов рисков и сценариев упреждающих воздействий), *методики факторного анализа* (взаимозависимости между факторами и рисками), *реестры источников информации* о состоянии факторов, *реестры факторов*, обусловливающих риски, *реестры рисков* хозяйств, *реестр общекорпоративных рисков* холдинга «РЖД» и их классификационных признаков.

Несомненным преимуществом современных интеллектуальных машинных методов перед классическими методами, является возможность работать с многомерными данными, то есть, рассматривать объект с учетом всех возможных признаков и факторов. Методы позволяют устанавливать взаимосвязи показателей в многомерном пространстве, что для человека крайне затруднительно с точки зрения временных ресурсов. Машинные (как правило, интеллектуальные) методы практически исключают вероятность допущения ошибки при расчете.

На рисунке 2 показана иерархическая шестиуровневая структура влияния факторов на такой показатель как среднесуточная производительность локомотива. На первом уровне учитываются такие факторы, как среднесуточный пробег локомотива, средний вес поезда. На втором уровне – участковая скорость, оборот локомотива на станции и др. На шестом уровне – тип локомотива, его техническое состояние и т. д. Всего учитывается более 50 факторов, влияющих на среднесуточную производительность локомотива. Для расчета должны быть приведены статистические данные по каждому фактору. Затем с помощью статистических методов факторного анализа и анализа связей в сочетании с другими методами Data Mining, такими, как методы моделирования и прогнозирования, можно выполнить проактивное планирование среднесуточной производительности локомотива.

Осуществление многофакторного анализа рисков с использованием методов анализа больших данных и машинного обучения позволит осуществлять динамическую оценку рисков хозяйств, выявлять аномалии в значениях показателей в режиме реального времени и предсказывать вероятность возникновения опасного события.

Переход к цифровой системе управления безопасностью движения

В настоящее время с учетом внедрения ЕКП УРРАН и связанных с ней систем (КАСАНТ, АС РБ, КАСАТ, КАСКОР, ЕК АСУ И, АСУ Т и др.) управление безопасностью движения состоит в текущей оценке и прогнозировании безопасности и надежности элементов и устройств железнодорожной техники (автономно по каждому хозяйству), отдельно систем (например, парк локомотивов, контактная сеть, мосты и т. д.), затем технологических процессов (управление движением, техническое обслуживание и ремонт и др.). Эти операции агрегированы на уровне устройств, систем, процессов и разделены по хозяйствам. Безопасность обеспечения услуги по пассажирским и грузовым перевозкам основывается на решениях ревизорского аппарата по полученной постфактум статистической и в реальном времени информации от автоматизированных систем (рисунок 3). Эти решения во многом зависят от человеческого фактора, поскольку поступающие данные в большинстве своем не взаимосвязаны – ни горизонтально по хозяйствам, ни вертикально по элементам, системам, процессам. Вследствие этого отсутствует объемная цельная картина по текущему состоянию безопасности и надежности инфраструктуры и подвижного состава.

Переход к цифровой системе управления безопасностью движения должен осуществляться путем построения моделей взаимодействия факторов безопасности и надежности всех объектов железнодорожного транспорта на всех уровнях иерархии, а также во взаимосвязи с другими факторами, которые непосредственно не относятся к надежности, однако оказывают влияние на безопасность перевозочного процесса. К таким факторам относятся, например, класс линии, участковая скорость, вес поезда, плановые и внеплановые окна для технического обслуживания и ремонта пути, состояние балласта, состояние мостов и многие другие факторы. Большое количество факторов и исключительно большое многообразие связей между ними могут быть формали-

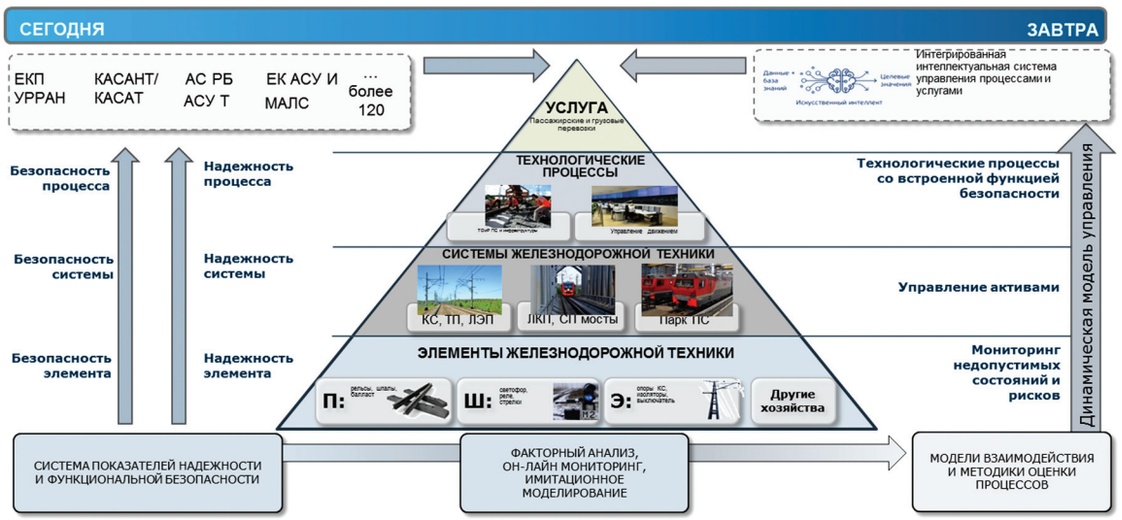


Рисунок 3 – Переход к цифровой интеллектуальной системе управления безопасностью.

зованы и сохранены с помощью указанной современной технологии Big Data. Это позволит в реальном масштабе времени осуществлять комплексный мониторинг недопустимых состояний и рисков. В основе мониторинга следует использовать разработанную в рамках системы УРРАН методологию управления техническими, социальными и техногенными рисками объектов транспорта [12, 13]. Это позволит с учетом результатов комплексной оценки рисков управлять техническими активами холдинга «РЖД» и формировать технологические процессы со встроенной функцией безопасности.

Заключение

Основной результат перехода на технологию Big Data состоит в создании динамической модели управления безопасностью движения, в исключении зависимости системы управления от недостатков человеческого фактора и, что особенно важно, в возможности создания в холдинге «РЖД» интегрированной интеллектуальной системы управления процессами и услугами со встроенными функциями оперативного управления безопасностью движения. Цель цифровой трансформации системы управления безопасностью движения в холдинге ОАО «РЖД» заключается в переходе на глобальный уровень взаимодействия с процессами всех подразделений по интегральной оценке риска возможных событий и достижению установленных показателей. Практическое внедрение этого подхода будет реализовано на основе технологий больших данных (Big Data) и искусственного интеллекта, систем диагностики с использованием Интернета вещей, цифровизации процессов производства и ремонта подвижного состава и инфраструктуры и др. Итогом станет интеграция системы управления безопасностью движения с производственными процессами на всех уровнях управления холдинга «РЖД» в соответствии с тремя принципами цифрового бизнеса: *Полная согласованность*, *Бизнес в режиме онлайн* и *Управление сервисами*. Для функционального направления «Безопасность движения» это означает анализ актуальных данных о состоянии сети и подвижного состава, онлайн-контроль состояния ценных и опасных грузов, осуществляемый путем сбора информации с датчиков, потоковый анализ данных об актуальном техническом состоянии подвижного состава и локомотивов с оценкой рисков эксплуатации, формированием оперативных предупреждений и выработкой рекомендаций по дальнейшему использованию и ремонтам с минимизацией рисков.

В результате масштабного развития и внедрения в компании Единой корпоративной платформы (ЕКП) УРРАН реализуется поддержка принятия управленческих решений по обеспечению надежности и безопасности функционирования объектов транспорта на основе оценки рисков. Так, с помощью разработанной и внедренной в 2018 г. ЕКП УРРАН Э (подсистема «Э» хозяйства электрификации и электроснабжения), реализована комплексная работа более 1 000 пользователей. При этом по объектам Трансэнерго введено более 4,3 млн. контрольно-оценочных карт. В этом же году проведена разработка и внедрение в постоянную эксплуатацию ЕКП УРРАН С, которая позволяет в связевом комплексе оперативно рассчитывать ключевые показатели надежности и безопасности и оценивать риски. Функциональное развитие ЕКП УРРАН П в путевом комплексе позволило начиная с 2019 г. повысить объективность оценки деятельности структурных подразделений комплекса и объективность задания нормируемых показателей надежности. Разработка и внедрение в комплексе автоматики и телемеханики ЕКП УРРАН Ш и в локомотивном комплексе ЕКП УРРАН Т уже с 2019 г. создаст необходимые условия для повышения эффективности их технического содержания на основе управления ресурсами и рисками.

Таким образом, с помощью ЕКП УРРАН заложены основы цифровой трансформации системы управления безопасностью движения в холдинге «РЖД».

Библиографический список

1. **Розенберг И.Н.** Автоматизированная информационная система ревизора движения [Текст] / И.Н. Розенберг, М.А. Аветикян, А.М. Замышляев // Железнодорожный транспорт. – 2004. – № 7. – С. 46-48.

2. **Замышляев А.М.** Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте [Текст] / А.М. Замышляев. – М.: Надежность, 2013. – 143 с.

3. **Розенберг Е.Н.** Система КАСАНТ: задачи, возможности, перспективы развития [Текст] / Е.Н. Розенберг, И.Н. Розенберг, А.М. Замышляев и др. // Железнодорожный транспорт. – 2008. – № 9. – С. 6-9.

4. **Замышляев А.М.** Система КАСАНТ: второй этап внедрения [Текст] / А.М. Замышляев, Г.Б. Прошин, А.А. Горелик // Автоматика, связь, информатика. – 2009. – № 7. – С. 9-13.

5. **Гапанович В.А.** Математическое и информационное обеспечение системы УРРАН [Текст] / В.А. Гапанович, И.Б. Шубинский, А.М. Замышляев // Надежность. – 2013. – № 1. – С. 3-11.

6. **Гапанович В.А.** Метод оценки рисков системы из разнотипных элементов [Текст] / В.А. Гапанович, И.Б. Шубинский, А.М. Замышляев // Надежность. – 2016. – № 2. – С. 49-53.

7. **Rizzatti R.** Digital Data Storage is Undergoing Mind-Boggling Growth [Электронный ресурс] / Dr. Lauro Rizzatti, Verification Consultant // URL: https://www.eetimes.com// Подробнее: https://www.eetimes.com/author.asp?section_id=36&doc_id=1330462 (Дата обращения: 31.10.2018 г.).

8. **Макевнин Б.** Цифровая нефть. Большие данные как один из ключевых инструментов цифровой трансформации [Текст] / Б. Макевнин, А. Столяров // Сибирская нефть. – 2017. – № 9/146.

9. **Thaduri A.** Railway assets: A potential domain for big data analytics [Text] / Adithya Thaduri, Diego Galar, Uday Kumar; Lulea University of Technology, Lulea, Sweden. // Procedia Computer Science. – 2015. – Volume 53. – P. 457-467.

10. **Гапанович В.А.** Построение и использование матриц рисков в системе управления рисками на железнодорожном транспорте [Текст] / В.А. Гапанович, И.Б. Шубинский, А.М. Замышляев // Надежность. – 2011. – № 4. – С. 56-68.

11. **Zamyshlyaev A.** Adaptive Management System of Dependability and Safety of Railway Infrastructure [Text] / A. Zamyshlyaev, I. Shubinsky // Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO). Be'er-Sheva, Israel, 15.02.16-18.02.16, IEEE Xplore Digital Library. – P. 244-250.

12. **Shubinsky I.** Risk management system on the Railway Transport [Text] / I. Shubinsky, A. Zamyshlyaev // Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO). Be'er-Sheva, Israel, 15.02.16-18.02.16, IEEE Xplore Digital Library. – P. 481-486.

13. **Шубинский И.Б.** Основные научные и практические результаты разработки системы УРРАН [Текст] / И.Б. Шубинский, А.М. Замышляев // Надежность. – 2012. – № 3. – С. 3-12.

Сведения об авторе

Алексей М. Замышляев – доктор технических наук, заместитель Генерального директора АО «НИИАС», Москва, Российская Федерация, тел. +7 (495) 967-77-02, e-mail: A.Zamyshlaev@vniias.ru

Вклад автора в статью

Автор проанализировал этапы автоматизации системы управления безопасностью движения, установил, что в настоящее время при управлении безопасностью движения необходимо обрабатывать громадные массивы разрозненных неструктурированных данных и предложил создание четырехуровневой (элементы, системы, процессы, услуги) цифровой интеллектуальной системы управления безопасностью, включающими управление безопасностью, надежностью, техническими активами и технологическими процессами.

УДК 004.413.4:614.8.026.1
Оригинальная статья
Надежность, том 19, №4, 2019 https://doi.org/10.21683/1729-2646-2019-19-4-53-64

О природе рисков в управлении безопасностью структурно сложных систем

Александр В. Бочков, *ООО «Газпром газнадзор», Российская Федерация, Москва*

Александр В. Бочков

Резюме. Цель. *В общем случае риск-ориентированный подход охватывает как вероятностные методы моделирования аварийных процессов и событий, так и детерминистские методы. Использование вероятностных и детерминированных оценок заняло значительное место в исследованиях по повышению безопасности и по совершенствованию эксплуатационных процедур. Однако опыт использования сугубо вероятностного анализа (по сути – однокритериального инструмента) показал, что этот подход охватывает не все необходимые аспекты обеспечения безопасности. Цель статьи – ввести определения (уточнения) самих понятий «анализ» и «синтез», применительно к рискам при исследовании вопросов обеспечения безопасности структурно сложных систем (ССС) и построении систем мониторинга опасностей и угроз их устойчивому развитию.* **Метод.** *В статье с позиций системологии рассматривается методология анализа и синтеза рисков как инструмента создания современных систем мониторинга угроз безопасности функционирования ССС. Приведено сравнение основных концепций управления рисками в ССС, принятыми в настоящее время и показана необходимость их творческого развития. Приведен вид функционала риска, позволяющего определять решение в области обеспечения безопасности величиной математического ожидания потерь с учетом соответствующих поправок.* **Результат.** *Введено понятие «синтез рисков» как единого с анализом инструмента познания, учитывающего существующие связи между элементами исследуемых ССС с точки зрения всей системы как целого. Сформулированы принципы составления полного набора данных, необходимых для принятия решений.* **Вывод.** *Предложенный подход формирует предпосылки к разработке метода синтеза рисков и предполагает создание перспективных экспертно-аналитических систем поддержки принятия решений о безопасности ССС как систем многофункциональных и многоуровневых, предназначенных как для фиксации и анализа каждого конкретного случая (события), так и для прогнозирования тенденций и формирования профилактических мероприятий в случае их необходимости.*

Ключевые слова: *структурно-сложная система, объекты критически важной инфраструктуры, риск, синтез, анализ, безопасность, управление.*

Для цитирования: *Бочков А.В. О природе рисков в управлении безопасностью структурно сложных систем // Надежность. 2019. № 4. С. 53-64. https://doi.org/:10.21683/1729-2646-2019-19-4-53-64*

Поступила 26.08.2019 г. / После доработки 23.10.2019 г. / К печати: 14.12.2019 г.

...Большинство ученых работников стремятся узнать устройство, состав и содержание своего предмета, разлагая его на части. Они пытаются понять, как части соединяются в целое. Иногда это напоминает желание разобрать часы, чтобы понять, что такое время...

Аксенов Г.П. [1]

Введение

Вопросам анализа и оценки рисков посвящено много работ, причем их число стремительно растет в последние годы. Рисунок 1 наглядно демонстрирует рост частоты появления (в количестве на 1 млн слов в год) в англоязычных публикациях слова «риск» с момента его первого упоминания в 1661 году до настоящего времени.

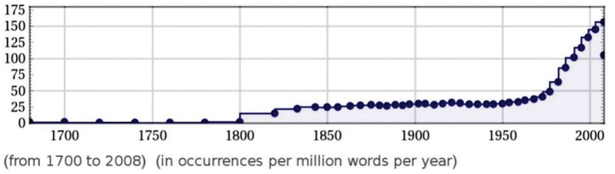


Рисунок 1 – Частота упоминания слова «риск» [2]

Отчасти это связано с общей «модой» на исследования в этой области, отчасти – это ответ на вызовы времени, когда создание человеком большого числа взаимно пересекающихся и частично интегрированных друг в друга систем разного назначения существенно поколебало общую устойчивость развития общества, породило трудно прогнозируемые опасности и угрозы. Появилось даже целое направление в системной инженерии, занимающееся инженерией систем, отдельные части которых могут существовать автономно, были разработаны независимо друг от друга, и тем самым представляют собой полноценную целевую систему. Риск часто выступает как осознанная угроза, следствием чего и является повышенный интерес к нему исследователей. Однако их усилия нередко очень наглядно иллюстрируют слова Г.П. Аксенова, биографа В.И. Вернадского, вынесенные в эпиграф.

В этой связи первостепенную актуальность приобретает задача определения (уточнения) самих понятий «анализ» и «синтез» применительно к рискам. Анализ и синтез – не два разных пути и способа познания, а являются противоположностями одного познающего сознания, разделимыми лишь в абстракции. А. Казеннов [3], например, показывает, что основанием этого единства является их происхождение из практического анализа и из исследования вообще. «…родовым словом для определения анализа, – пишет он, – является не «разделение» (в том числе – мысленное) предмета, а «исследование». А специфическим отличием определения является «различение частей целого и их соотношения друг с другом посредством этого целого». Не расчленение, а различение… Нужно только найти момент тождества «части» и целого, одной части и других «частей».

В то же время отождествление различенных частей друг с другом объединяет предметы (в данном случае – части) в нечто одно, в целое. Но это уже синтез. А определение анализа следует сформулировать так: анализ есть исследование, различающее части предмета и соотносящее их с целым и друг с другом посредством этого целого. Целое в анализе является исходным, опосредствующим все движение исследования. Части же, как правило, выделены уже до данного исследования – предшествующими практическими и теоретическими исследованиями: аналитическими и синтетическими познаниями… синтез: это исследование, рассматривающее соотношение различенных частей предмета и их целого посредством сущности (существенной части) целого. Нахождение такой сущности или существенной части и есть фундаментальное научное открытие, которое проливает новый свет на все предшествующие понятия, выражающие сущность предмета. Она перестраивает всю систему понятий и, соответственно, всю теорию».

При оценке рисков такой подход к их изучению представляется наиболее конструктивным. Особенно важно это при исследовании системы систем и связанной с ней т.н. проблемы критической инфраструктуры, часто обсуждаемой в последние годы [4-9]. Суть этой проблемы заключается в том, что почти во всех важнейших секторах экономики существуют системы, элементы которых настолько далеко разнесены в пространстве (иногда эти системы относят также к классу территориально-распределенных), что экономически практически невозможно полностью защитить все объекты даже какого-либо одного сектора, не говоря уже обо всех секторах системы. Главными вопросами и проблемой лица, принимающего решения (ЛПР) в области обеспечения безопасности функционирования подобных систем является вопрос оценки угроз и рисков, значимых для системы в целом и для ее элементов и определение приоритетности защиты элементов и объектов критической инфраструктуры с учетом ограниченных, как правило, ресурсов, имеющихся в его распоряжении.

Помимо огромных размеров, многие сектора настолько сложны, что технологически и экономически невозможно предвидеть, и просчитать все непредвиденные последствия любого инцидента, независимо от того, был ли инцидент вызван последствиями злонамеренных действий людей, или явился следствием природных бедствий. Как правило, крайне трудно предсказать последствия малых возмущений в одной части критической инфраструктуры для других ее участков. Например, все коммуникации в сети интернет в Южной Африке были полностью прекращены вследствие падения башен-близнецов в результате террористической атаки на США 9 сентября 2001 г., а относительно незначительные неисправности в электрической полезной мощности First Energy в Огайо (США) ускорили блэкаут в августе 2003 года, затронувший 50 миллионов человек за тысячи километров от источника проблемы [10-12].

По сути, существующая инфраструктура уязвима просто потому, что она содержит так много очень тесно взаимосвязанных между собой компонентов, что для большинства технических консультантов, аналитиков и ЛПР, определяющих политику ее безопасности, это становится неразрешимой задачей.

Понятие структурной сложности, как и понятие системы вообще, до сих пор не нашло однозначного определения. Вместе с тем современные требования к построению систем обеспечения безопасности и эффективности их функционирования были и остаются достаточно высокими. Как следствие, возникают задачи выбора приоритетных объектов оснащения из их генеральной совокупности и оптимального распределения имеющихся в распоряжении владельца системы (собственника, государства) финансовых и материальных ресурсов на их защиту. О понятии оптимальности в приложении к задачам синтеза риска мы поговорим позже. Прежде всего, необходимо разобраться с понятием риска, его онтологией. Измерять можно только то, что четко определено, хотя А. Эйнштейн утверждал, что «мир понятие не количественное, а качественное».

Люди избавились бы от половины своих неприятностей, если бы договорились о значении слов…

Рене Декарт

1. О природе риска и подходах к обеспечению безопасности

Риск – это понятие, возникающее на стыке понятий надежности и безопасности. Сама по себе техника, производственные системы не рискуют. Рискует всегда человек. Надежность – свойство технического объекта безотказно функционировать непрерывно со 100% уровнем эффективности. При анализе надежности главный критерий – критерий отказа, который делит все на «да» (работоспособное состояние) и «нет» (неработоспособное состояние). Надежность зависит, если можно так выразиться, от внутренних свойств и характеристик объекта (качества изготовления, его наработки на отказ, технологических особенностей, требований к эксплуатации и т.п.). Безопасность – свойство того же объекта выполнять свои функции без нанесения ущерба обслуживающему персоналу, окружающей среде и пр. Безопасность зависит уже от свойств внешних (окружающая среда, угрозы, квалификация персонала). Кроме того, безопасность – это одновременно и ощущение, и состояние. Состояние безопасности определяется развитием соответствующих технологий, а оценивается с помощью математических методов моделирования; оно основано на анализе и оценке рисков и эффективности различных мер, средств и механизмов защиты. Ощущение безопасности – это психологические реакции человека на угрозы и риски, и психологическое же восприятие достаточности мер защиты; то, что называется уровнем приемлемого риска (т.е., от каких угроз человек готов не защищаться, какие ущербы для него являются допустимыми). В том смысле, что ощущение безопасности может субъективно меняться, можно согласиться с высказыванием американского криптографа, писателя и специалиста по компьютерной безопасности Брюса Шнайдера: «Безопасность – это процесс, а не результат». Но это совсем не означает, что у процесса обеспечения безопасности нет цели. Цель обеспечения безопасности – достигнуть такого состояния защищенности человека и окружающей среды, которое соответствует его субъективному ощущению опасности (т.е., приемлемому уровню риска). Для достижения этой цели применяют т.н. «риск-ориентированный подход».

Риск появляется как оценка опасности для человека, выполняющего работу с помощью технических устройств. Поскольку и при рассмотрении надежности, и при рассмотрении безопасности есть скрытые дефекты и неопределенности места и времени возникновения отказов и опасностей, риск часто трактуют как влияние неопределенностей на достижение поставленных человеком-оператором целей деятельности. Конкретика возникает, когда рассматривается конкретный механизм (объект, промышленное предприятие, корпорация и т.п.), который человек использует для реализации целей деятельности в определенной среде (которая, в свою очередь, характеризуется наличием угроз, природными особенностями, наличием конкурентов, имеющих свои цели и т.п.)

В живых системах, например, неустойчивость используется целесообразно – это одна из самых важных движущих сил эволюции. Можно сказать, что высокая адаптивность живых организмов является следствием их неустойчивости. Известный сторонник «управляемой неустойчивости» Насим Талеб, также неоднократно подчеркивал, что многоуровневая избыточность – главное свойство естественных (живых) систем, управляющее риском [13]. Как и в живых системах, неустойчивые процессы в системах обеспечения безопасности – залог их адаптивности к изменяющимся угрозам и опасностям.

С некоторой оговоркой можно сказать, что риск служит наилучшей мерой для количественного описания опасности. Это понятие широко используется в современной литературе и часто подразумевает совершенно различный смысл. В наиболее общем случае риск характеризуется: вероятностью возникновения неблагоприятного воздействия, вероятностью того, что возникает неблагоприятное воздействие именно данного типа и вероятностью того, что данный тип воздействия вызывает определенную величину отклонений состояния субъекта воздействия от его динамического равновесия. То есть, риск – векторная величина, которая может описывать опасности разного вида и куда все его значения, приведенные выше, входят составными частями. Так как основные вопросы, обсуждаемые ниже, так или иначе связаны с обеспечением безопасности промышленных объектов, то там, где это не оговорено особо, под термином «риск» мы будем понимать риск техногенного или, более конкретно, промышленного происхождения.

Первым приближением, в вопросах, связанных с обеспечением безопасности, чаще всего является требование достижения пренебрежимо малого или «нулевого» риска, связанного с той или иной, как правило, производственной, деятельностью. Поэтому системы безопасности, которые создавались и использовались в промышленности, чаще всего являлись инженерными решениями, направленными на выполнения требования абсолютной безопасности. Основной принцип, используемый для создания этих систем – т.н. принцип **ALAPA** (As Low As Practicable Achievable). Согласно этому принципу, необходимо повышать промышленную безопасность любыми средствами и независимо от достигнутого уровня, если это технически осуществимо. Иными словами, согласно ALAPA необходимо создавать технические меры безопасности, которые предотвращали бы аварийные ситуации, т.е. сводили на нет саму возможность возникновения и развития аварии. Усложнение технологий привело к тому, что часто просто немыслимо предугадать все возможные сценарии развития аварии и, соответственно, предусмотреть инженерные и организационные решения для их предотвращения, что лишний раз показали аварии в Чернобыле и Фукусиме. Все это потребовало принципиально нового подхода в решении задач обеспечения безопасности. В последнее три десятилетия этим вопросам было посвящено значительное количество работ, которые убедительно подтвердили уже ставшее аксиоматическим утверждение о том, что достижение абсолютной безопасности невозможно.

Философия риска, основанная на концепции абсолютной безопасности, с необходимостью пришла к концепции приемлемого риска. Концепция приемлемого риска потребовала отказа от принципа ALAPA и прохода к новому принципу **ALARA** (As Low As Reasonable Achievable). Согласно ALARA, необходимо достижение определенного уровня безопасности, который должен определяться исходя из социальных и экономических условий развития общества. Для аварий, риск от которых выше приемлемого, необходимо использовать инженерные решения для их предотвращения и ослабления последствий, а для тех аварий, риск от которых меньше, только меры по ослаблению последствий. Реализация этого принципа, например, для атомной энергетики нашла отражение в соответствующих положениях по обеспечению безопасности. Для ССС также вводится понятие приемлемого (предельно допустимого) риска как риска, уровень которого допустим и обоснован исходя из экономических и социальных соображений. Хотя полноценных методик определения приемлемого риска для опасных промышленных объектов ССС до настоящего времени нет, можно сказать, что в настоящее время решение задач безопасности сводится к тому, чтобы на основании определенных критериев ответить на вопрос о том, какими средствами и до какого уровня необходимо снижать риск в той или ивой области производственной деятельности, чтобы безопасность как человека, так и окружающей среды была оптимальной.

Анализ риска является единственной возможностью исследовать те вопросы безопасности, на которые не может быть получен ответ из статистики, как, например, аварии с малой вероятностью реализации, но с большими потенциальными последствиями. Конечно, анализ риска не является решением всех задач обеспечения безопасности, однако только используя его, можно сравнить риски от различных источников опасности, выделить наиболее существенные из них, выбрать наиболее эффективные и экономичные системы по увеличению безопасности, разработать мероприятия по снижению последствий аварий и т.д.

В зарубежной печати наряду с понятием «анализ риска» (Risk Analysis) иногда пользуются методом **PRA** (Probabilistic Risk Analysis, вероятностная оценка риска), утвержденным NRC (Nuclear Regulatory Commission, Комиссия по ядерному регулированию США). Принципиального различия между ними нет, хотя считается, что PRA преимущественно нацелен на анализ аварий с низкой вероятностью, однако при помощи PRA часто исследуются события и с широким спектром вероятности возникновения. В отечественной литературе такого разделения не существует.

В настоящее время процедуру анализа риска можно условно разделить на две основные составные части и несколько промежуточных, каждая из которых характеризуется своими проблемами и использует присущие ей методы и модели: оценка и управление. Важно при этом помнить, что вопросы анализа риска нельзя рассматривать отдельно от игровой постановки. Риск, как динамическая характеристика, зависящая от времени, средств и информации, сведена к «двумерным оценкам» вероятности и ущерба.

Забыто, что прежде всего существует принципиальное различие между стохастическими факторами, приводящими к принятию решения в условиях риска, и неопределенными факторами, приводящими к принятию решения в условиях неопределенности. И те, и другие приводят к разбросу возможных исходов результатов управления.

Но стохастические факторы полностью описываются известной стохастической информацией, эта информация и позволяет выбрать лучшее в среднем решение. Но основные формулы в анализе риска (АР) извращены, упрощены, забыта их принадлежность к теории игр. Причин этому несколько. Слово риск стало «модным», в итоге специалисты «ухватились за термин» не понимая, откуда он происходит, какие аксиомы в этот термин «положены». В итоге экономисты, страховщики, экологи, и другие много лет плодят ложные научные результаты исходя из ложных ими придуманных определений. Иногда («ложь» на «ложь» дает «истину») получают приемлемые результаты. Но это, как правило, касается только статических и стационарных случаев (где работает теория «надежности»), но никак не динамических случаев. Для ряда приложений нужно было, чтобы формула была «попроще», чтоб ее понимали развивающиеся страны, вступающие, например, в МАГАТЭ. В итоге риск как динамическая характеристика, зависящая от времени, средств и информации, свелась к двумерным снимкам фотографий, в которых присутствует только вероятности

и ущерб. Дело было отдано «войскам гражданской обороны» (ныне МЧС), не имеющим тогда соответствующего научного «потенциала» и выступающим как «заказчики» НИР. Наиболее влиятельные Министерства (Минсредмаш, МинОбщемаш), в общем, имели собственные представления о риске, которые в целом значительно отличались друг от друга. На формирование мнения, что задачи анализа риска разрешимы за счет «статистики» наблюдаемых явлений, подавляющее влияние оказали западные ученые (TNO из Нидерландов другие). Влияние было настолько сильным, что в современном анализе рисков были оставлены «теория прочности» и «теория надежности». Но были задавлены на корню исследования по «теории живучести», «теории гомеостазиса», адаптивные теории, включая «теорию выбора решений», «теорию перспективной активности», «теорию рефлексий», «теорию самоорганизующихся систем».

Применительно к неопределенным факторам подобная информация отсутствует. В общем случае неопределенность может быть вызвана либо противодействием разумного противника (более сложный случай – связанный с рефлексиями противника (террористическая угроза)), либо недостаточной осведомленностью об условиях, в которых осуществляется выбор решения.

Выбор решений при наличии недостаточной осведомленности относительно условий, в которых осуществляется выбор, принято называть «играми с природой». В терминах «игры с природой» задача принятия решений может быть сформулирована следующим образом. Пусть лицо, принимающее решение, может выбрать один из M возможных вариантов своих решений: $X_1, X_2, \ldots, X_M$ и пусть относительно условий, в которых будут реализованы возможные варианты, можно сделать N предположений: $Y_1, Y_2, \ldots, Y_N$. Оценки каждого варианта решения в каждых условиях (X_m, Y_n), где $m = 1 \ldots M$, $n = 1 \ldots N$, известны и заданы в виде матрицы выигрышей лица, принимающего решения: $A=A(X_m, Y_n)=\|A_{mn}\|$.

Предположим вначале, что априорная информация о вероятностях возникновения той или иной ситуации Y_n отсутствует. Теория статистических решений предлагает несколько критериев оптимальности выбора решений. Выбор того или иного критерия неформализуем, он осуществляется ЛПР субъективно, исходя из его опыта, интуиции и т.п. Рассмотрим эти критерии.

Критерий Лапласа. Поскольку вероятности возникновения той или иной ситуации Y_n неизвестны, будем их все считать равновероятными. Тогда для каждой строки матрицы выигрышей подсчитывается среднее арифметическое значение оценок. Оптимальному решению будет соответствовать такое решение, которому соответствует максимальное значение этого среднего арифметического, т.е.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\frac{1}{N}\sum_{n=1}^{N} A_{mn}\right).$$

Критерий Вальда. В каждой строчке матрицы выбираем минимальную оценку. Оптимальному решению соответствует такое решение, которому соответствует максимум этого минимума, т.е.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\min_{1 \le n \le N}\left(A_{mn}\right)\right).$$

Этот критерий очень осторожен. Он ориентирован на наихудшие условия, только среди которых и отыскивается наилучший и теперь уже гарантированный результат.

Критерий Сэвиджа. В каждом столбце матрицы находится максимальная оценка $\overline{A}_n = \max_{1 \le m \le M}\left(A_m\right)$ и составляется новая матрица, элементы которой определяются соотношением $R_{mn} = \overline{A}_n - A_{mn}$. Это размер сожалений, что при стратегии Y_n сделан не оптимальный выбор X_m.

Величину R_{mn} называют риском, под которым понимают разность между максимальным выигрышем, который имел бы место, если бы было достоверно известно, что наступит самая выгодная ситуация $\overline{Y}_n$ для лица, принимающего решения, и реальным выигрышем при выборе решения X_m в условиях Y_n.

Эта новая матрица называется матрицей рисков. Далее из матрицы рисков выбирают такое решение, при котором величина риска принимает наименьшее значение в самой неблагоприятной ситуации, т.е. $\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\max_{1 \le n \le N}\left(R_{mn}\right)\right)$.

Сущность этого критерия заключается в минимизации риска. Как и критерий Вальда, критерий Сэвиджа очень осторожен. Они различаются разным пониманием худшей ситуации: в первом случае – это минимальный выигрыш, во втором – максимальная потеря выигрыша по сравнению с тем, чего можно было бы достичь в данных условиях.

Критерий Гурвица. Вводится некоторый коэффициент α, называемый «коэффициентом оптимизма», $0<\alpha<1$. В каждой строке матрицы выигрышей находится самая большая оценка $\max_{1 \le n \le N}\left(A_{mn}\right)$ и самая маленькая $\min_{1 \le n \le N}\left(A_{mn}\right)$.

Они умножаются соответственно на α и $(1-\alpha)$ и затем вычисляется их сумма. Оптимальному решению будет соответствовать такое решение, которому соответствует максимум этой суммы, т.е.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\alpha \times \max_{1 \le n \le N}\left(A_{mn}\right) + (1-\alpha) \times \min_{1 \le n \le N}\left(A_{mn}\right)\right).$$

При (α=0) критерий Гурвица трансформируется в критерий Вальда. Это случай крайнего «пессимизма». При (α=1) (случай крайнего «оптимизма») человек, принимающий решение, рассчитывает на то, что ему будет сопутствовать самая благоприятная ситуации. «Коэффициент оптимизма» α назначается субъективно, исходя из опыта, интуиции и т.п. Чем более опасна ситуация, тем более осторожным должен быть подход к выбору решения и тем меньшее значение присваивается коэффициенту α.

Важно, что к анализу рисков этот критерий не имеет отношения. Разве только к субъективному восприятию «случайных» и «добровольных» рисков.

Как же считать риски?

Из вышесказанного следует, что оценка риска возможна только при наличии альтернатив выбора. Если существует всего один единственный вариант выбора, то риск автоматически равен нулю и разброс платежей является лишь характеристикой неуправляемой природной среды. Впрочем, надо заметить, альтернатива всегда присутствует в виде отказа принимать решение.

В каких-то случаях отказ принимать какое-то решение может давать оптимум по столбцам и тогда появятся не нулевые риски в вариантах за счет выбора неправильного решения. Например, выгодно не играть в казино, чем играть, придерживаясь какой-то стратегии. Напротив, в шахматах есть смысл играть даже в случае единственного (вынужденного) хода. Например, когда противник объявляет «шах», закрыться нечем, а отступление возможно только на единственную клетку – риск также нулевой, поскольку отказ играть – автоматическое поражение.

Наличие оценок вероятностей $\sum_{n=1}^{N} p_n = 1$ для описания состояния природной среды $p_1 = p(Y_1)$, $p_2 = p(Y_2)$, …, $p_N = p(Y_N)$ позволяет отказаться от выбора самого неблагоприятно случая при использовании критерия Сэвиджа, и записать искомое решение в виде:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{N} p_n \times \left(\max_{1 \le n \le N}\left(A_{mn}\right) - A_{mn}\right)\right),$$

что является более правильной формулой.

Для случая, когда для любой пары (X_m, Y_n) платеж определяется только размером потерь $A_{mn}=B–C_{mn}$ имеем:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

Для случая, когда уровень потерь при оптимальном варианте для условий Y_1, Y_2, …, Y_N не зависит от n и равен $\overline{C}$, тогда:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B - \overline{C} + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

Только в этом случае решение действительно будет определяться величиной математического ожидания потерь. Но с поправкой на B и $\overline{C}$. Неучет этих поправок содержится во множестве работ. Обычно принимают B и $\overline{C}$ равными нулю. Например, в экологии улучшать «воздух» ничего не стоит (не приносит прибыли), и если никто не заболел, то оптимальный ущерб принимается за 0.

К тем же оценкам приводит Критерий Байеса:

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times A_{mn}\right) =$$

$$= \left(B = 0; \overline{C} = 0\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

В целом, проблема обеспечения безопасности и анализа рисков объектов ССС в условиях изменения состава и интенсивности угроз устойчивому развитию отрасли не теряет своей актуальности на протяжении длительного времени. Требования безопасности, установленные для объектов высокой и средней категории опасности, порой высоки, и существенно повышают возможности собственников объектов. Как следствие, возникает вопрос ранжирования объектов внутри заданных категорий для определения очередности оснащения объектов требуемыми средствами защиты. Для этого необходимо задать критерий, относительно которого будет определяться важность (и, соответственно, порядковый номер) того или иного объекта в ранжированном перечне.

Используемые методы ранжирования объектов основаны на математическом моделировании, экспертных оценках, теории принятия решений и интервальном оценивании. В той или иной мере они учитывают интересы организаций, эксплуатирующих эти объекты, государственных надзорных органов, страховых компаний. Вместе с тем, имеющиеся на сегодняшний день методы ранжирования (например, ранжирование объектов по защищенности от ЧС на железнодорожном транспорте, ранжирование объектов опасных производственных систем газораспределения и др.) не учитывают особенности структурной связности объектов ранжирования и важности работы конкретного объекта для смежных систем и подсистем.

Задача ранжирования объектов ССС является типовой задачей теории измерения некоторых сложных синтетических свойств объектов. Формально решение задачи сводится к построению некоторой функции ценности, полезности, связывающей измеряемое свойство с более простыми измеряемыми в натуральных величинах ресурсными показателями (факторами). Функция ценности используется как для решения задач выбора некоторого наилучшего варианта из множества альтернатив, так и для решения более композиционных задач, типа задачи формирования портфеля заказов на выполнение работ при ограничениях на ресурсы (объемы финансирования создания или модификации объектов). Факторы, через которые строятся ранги, часто измеряются не в количественных, а в качественных шкалах, поэтому требуется использование методов экспертных оценок и экспертных технологий для построения зависимостей между полезностью и первичными ресурсными факторами. В связи с развитием компьютерной техники появилась возможность оценивания объектов, факторы описания которых задаются с погрешностью, что требует разработки специфического аппарата статистической обработки первичных данных и использования инструментария нечеткой логики. Существенной чертой решения задач ранжирования является

адаптивный характер процедур принятия решений выбора оптимальных вариантов, при которых для построения окончательной формулы функции ранжирования требуется проведение нескольких циклов согласования экспериментальных данных и экспертных предпочтений.

В данном контексте оценка риска является тем этапом, на котором определяются неблагоприятные последствия, связанные с той или иной производственной деятельностью. И прежде необходимо идентифицировать источники опасности, для чего нужно определить границы исследуемой системы. Другими словами, необходимо знать, какие источники включать в рассмотрение, а какие нет при оценке риска в регионе или от конкретной исследуемой системы. Жестких правил здесь нет и быть не может. Однако на сегодняшний день существует ряд разработанных положений, которые должны быть учтены при исследовании вопросов безопасности. Наиболее полно сформулированные положения по определению границ исследуемых региональных или крупных промышленных систем можно найти в разных источниках. Международные организации отмечают тот факт, что при оценке риска даже от одной конкретной технологии в различных странах в большинстве случаев получают различные значения. Поэтому для облегчения сбора и обработки данных должен быть принят единый набор терминов и положений для описания энергетических и промышленных систем и их основных компонент [14].

2. Замечания о категории риска

Основными моментами в оценке риска является подробное описание источника опасности и определение связанного с ним возможного ущерба. Существуют различные модели источников опасности, которые позволяют определить вероятность того или иного развития аварии и определить соответствующую мощность выброса опасных веществ в окружающую среду. В зависимости от типа источника выделяют три категории риска.

Обычный риск связан с нормальной работой предприятия. В условия нормальной работы включаются и аварии с незначительным ущербом, которые происходят довольно часто. Эта категория риска характеризуется вероятностью реализации равной или близкой к единице. В большинстве случаев обычный риск либо является неотъемлемой частью самого производственного процесса, либо легко контролируется. Источники такого риска обычно описываются мощностью выброса или утечки в окружающую среду, связанные с нормальной работой либо с каким-то происшествием. Оценка мощности выброса или утечки для работающих предприятий может быть произведена на основании измерений либо результатов опыта работы аналогичных предприятий.

Другие две категории риска связаны с авариями на производстве, при транспортировке или хранении опасных веществ. Под аварией при этом понимается событие с низкой вероятностью осуществления (например, менее одного за все время жизни предприятия), но со значительными или даже катастрофическими последствиями. При анализе аварийных ситуаций обычно рассматриваются возможные сценарии развития аварии. При этом должны быть учтены такие факторы, как тип инициирующего события, количество имеющегося опасного вещества, эффективность аварийных систем безопасности и многие другие. Обычно существует большое число возможных сценариев развития аварии и поэтому в оценке риска необходимо определить весь спектр возможных сценариев и их вероятности. Величины вероятности могут при этом изменяться от 10^{-6} до 10^{-8} событий в год. Более редкие события настолько трудно оценить, что считают, что они практически невероятны.

Периодический риск связан с теми авариями, которые довольно часто повторяются, но вызывают ограниченный ущерб, куда могут входить даже человеческие жертвы. Это вовсе не означает, что такие аварии являются планируемыми. Они, конечно, нежелательны, и для предотвращения их создаются и используются системы безопасности. Однако несмотря на эти меры, такие аварии могут происходить, и риск, связанный с ними, имеет довольно широкий диапазон значений в зависимости от типа производственной деятельности. Причиной таких аварий является обычно нарушение технологического процесса, неверное использование оборудования и ошибки персонала. Для оценки риска этой категории частота аварий и другие необходимые параметры оцениваются при помощи стандартных статистических методов на основе имеющихся данных.

Гипотетический риск связан с авариями, которые, как считается, могут происходить с очень малой вероятностью, но приводить к очень большим последствиям. Для такого класса аварий характерно отсутствие либо недостаточное количество статистических данных. Однако из-за их огромного потенциального ущерба невозможно просто ждать, пока наберется достаточный практический опыт. Поэтому в этих случаях производят анализ гипотетических аварий с целью определения вероятности реализации этой аварии и оценки возможных ее последствий. Обычно недостаток статистических данных относится к поведению крупной промышленной или энергетической системы в целом. Поэтому такой анализ проводится либо при помощи экспертной оценки, либо методом «деревьев событий», где вероятность гипотетической аварии может быть предсказана на основе возможных неисправностей или отказов в работе отдельных узлов или механизмов, по которым имеются соответствующие статистические данные.

Следует помнить о том, что для оценки риска нет необходимости использовать чрезмерно усложненные модели из-за больших неопределенностей и осреднений, возникающих при расчете. Кстати, нахождение величины неопределенности и диапазона возможных значений риска является еще одной составной характеристикой риска вообще. Так, по мнению различных экспертов, неопределенность в оценке риска от аварий на промышленных предприятиях может составлять один и даже достигать двух порядков величины. Это связано с недостатком базы знаний по широкому кругу технических, экологических и социальных факторов, которые необходимо учитывать в

анализе риска. Есть даже заключения, основанные на анализе точности и неопределенности при определении риска, что модели переноса, позволяющие получить значение концентрации опасного вещества в исследуемом месте с точностью 10% (максимум 20%) вполне приемлемы.

3. Замечания о системе мониторинга

Таким образом, устойчивое функционирование и развитие любой ССС зависит от влияния большого числа внешних и внутренних факторов, в том числе факторов негативного воздействия. Для мониторинга и оценки этих факторов и принятия решений, направленных на снижения негативных последствий их проявления, повсеместно внедряются т.н. системы сбалансированных показателей (Balanced Scorecard), ключевых показателей эффективности (КПЭ) (количественно характеризующих факторы рисков, которым подвержена система) из числа которых выбираются стратегические целевые показатели (СЦП), количественно отражающие стратегические цели функционирования системы и представляющие собой базовые экономические и производственные показатели, которые характеризуют эффективность ее развития (опосредовано их недостижение характеризует уровень существующих угроз и степень их реализации в рассматриваемый промежуток времени).

На основе этих показателей строятся системы мониторинга угроз и рисков, позволяющие собирать данные об изменениях и проводить анализ эффективности функционирования системы по нескольким сотням показателей в организационном, продуктовом, географическом и других разрезах на суточном, квартальном и годовом горизонте планирования. Считается, что результаты анализа позволяют осуществлять «управление по отклонениям», акцентируя внимание на проблемных областях каждого объекта управления посредством «светофорной» индикации. Однако по мере накопления данных возникает проблема интерпретации сигналов этих сотен «светофорных индикаторов». Не очевидно, что считать «хорошим» или «плохим» сигналом в целом для системы, если, например, половина из индикаторов «горит» зеленым цветом, а половина «красным». Как квалифицировать ситуацию, если «зеленых» индикаторов немного больше, чем «красных» и т.п. Неочевидна также связь анализируемых индикаторов с показателями высокого уровня (СЦП) и степени их влияния на достижение целевых значений СЦП, утвержденных руководством компании. Возникает так называемый эффект «больших данных», когда аналитики не успевают обработать накапливающуюся информацию, а стандартные статистические методы просто перестают работать.

Кроме того, система мониторинга угроз и рисков, построенная на основе анализа трендов изменения показателей, не способна предсказывать кризисы и ситуации с негативной динамикой. Такие события редки и протекают, как правило, при различном прогнозном фоне, а в случае анализа рядов исторических данных редких событий имеют место дискретные динамические вероятностные процессы.

Целью анализа ССС как объекта прогнозирования в области обеспечения безопасности функционирования и устойчивости развития является построение такой прогностической модели динамики ситуаций, возникающих при ее функционировании, которая позволит с помощью вычислительных экспериментов и подбора приемлемых параметров уменьшать степень неопределенности дат событий и их масштаба, то есть, получать прогнозную информацию об объекте прогнозирования за счет выявления скрытых закономерностей, которые указывают либо на изменения состояния объекта, либо на закономерности изменений параметров внешней среды, существенно влияющей на его функционирование (так называемые законы изменчивости «прогнозного фона»).

Из-за дискретной природы кризисных ситуаций использование аппарата анализа данных, основанного на классических законах больших чисел, некорректно. Сходимость по вероятности в реальности практически никогда не наблюдается, за исключением статистики, накопленной в системах массового обслуживания. Панель индикаторов, реализованная в виде «светофора», построенного на основе использования дисперсии как основного показателя, может в течение всего года указывать на нормальное состояние, когда на самом деле система переходит в область предкризисных значений.

Кроме того, при официально декларируемой иерархической системе показателей, как правило, отсутствует однозначная функциональная связь и взаимное влияние показателей нижнего и верхнего уровня.

Как следствие, необходим корректный первичный анализ многолетней статистики, и уже на основе этого анализа можно дать заключение – возможна ли разработка адекватного исследуемой задаче инструмента прогнозирования и какая доля случайности дат возникновения неблагоприятных ситуаций и их масштабов может быть с его помощью устранена. Также очевидно, что, поскольку истинные законы распределения анализируемых случайных процессов и, главное, факторы их определяющие, будут непрерывно корректироваться (любая высокотехнологичная система, изменяется быстрее, чем накапливается адекватная статистика), необходимо использовать критерии, «свободные от распределений». В частности, например, в качестве критериев достижения прогностической цели следует взять не величины отклонений модельных и реальных данных, а критерии, используемые в методах классификации и распознавания образов. Например, в качестве измерения точности прогноза можно использовать величины ошибок предсказания первого и второго родов для различных классов и типов ситуаций, причем, если удастся, в зависимости от классов физического объекта и в зависимости от значения параметров прогнозного фона. Второе обстоятельство очень важно, поскольку, например, некорректно складывать статистику аварийности различных времен года, так как в различные сезоны технологические процессы протекают по-разному.

Надежное выполнение системой своих функций характеризуется сохранением некоторых заданных характери-

стик (отражаемых в соответствующих значениях СЦП и КПЭ) в установленных пределах. На практике полностью избежать отклонений невозможно, однако необходимо стремиться к минимизации отклонений текущего состояния от некоторого заданного идеала – цели, заданной, например, в виде значений СЦП первого уровня.

Мера угрозы недостижения заданных значений СЦП первого уровня (по сути, мы снова говорим о риске), рассматривается в данном случае как переменная величина, представляющая собой функцию относительно текущего положения системы: она увеличивается при приближении оцениваемой ситуации к некоторой допустимой границе, после достижения которой система не может выполнить свои обязательства и достичь соответствующих заданных целевых значений СЦП первого уровня.

Общая математическая постановка обсуждаемой задачи: пусть задано множество признаков текущей ситуации X (например, текущих значений КПЭ, факторов риска и т.п.), множество допустимых реализаций ситуаций Y (например, текущее значение СЦП первого уровня больше (или меньше) предыдущего и т.п.), и существует целевая функция y^*: $X \to Y$, значения которой $y_i = y^*(x_i)$ известны только на конечном подмножестве объектов $\{x_1,\ldots,x_l\} \subset X$ (например, соответствующие текущему значению СЦП первого уровня значения КПЭ). Пары «объект-ответ» (x_i, y_i) – прецеденты. Совокупность пар $X_l = \sum_{i=1}^{l} x_i, y_i = 1$ составит обучающую выборку. Требуется по выборке X_l восстановить зависимость y^*, то есть, построить решающую функцию $A: X \to Y$, которая приближала бы целевую функцию $y^*(x)$, причем не только на объектах обучающей выборки, но и на всем множестве X. Поскольку при этом решающая функция A должна допускать эффективную компьютерную реализацию, возможно называть ее также алгоритмом.

Условно существует два класса объектов, с которыми приходится сталкиваться специалистам в области автоматизации управления: «простые» и «сложные». «Простыми» являются объекты, точные математические модели которых, например, в виде системы алгебраических уравнений или модели линейного программирования, при учете всех необходимых количественных факторов, влияющих на поведение объекта, пригодны для реализации на ЭВМ выбранного класса и вполне адекватны объекту. «Сложные» объекты управления имеют следующие главные отличительные особенности: не все цели выбора управляющих решений и условия, влияющие на этот выбор, могут быть выражены в виде количественных соотношений; отсутствует, либо является неприемлемо сложным, формализованное описание объекта управления; значительная часть информации, необходимая для математического описания объекта, существует в форме представлений и пожеланий специалистов-экспертов и т.п. Построение точных математических моделей «сложных» объектов, пригодных для реализации и эксплуатации на современных ЭВМ, либо затруднительно, либо часто вообще невозможно.

Но это не означает, что задача не имеет решения. В общем случае возможных направлений поиска может быть два. Первое – попытаться применить нетрадиционный математический аппарат для построения модели, учитывающей все особенности объекта и пригодной для реализации. Второе – строить не модель объекта, а модель управления объектом (т.е., моделируется не сам объект, а человек-оператор в процессе управления объектом). По своей сути алгоритм в этом случае связан с построением поля структуры данных и анализом его эффектов, включая и уточнение самой структуры. В любых данных одновременно присутствует и порядок, и беспорядок. Поскольку исключающее ИЛИ «построить» трудно, возможна реализация идеи построения решающих правил (далее – решатель) на монотонных функциях, задающих сетевой порядок [15, 16].

Геометрический смысл решателя достаточно прост: необходимо так подобрать признаки, сохраняя свойства частного порядка, чтобы объекты на подмножестве признаков разделились. Это – классическая задача дискретной математики о нахождении логической функции, и решается она десятками различных способов, в основе которых лежит метод разложения любой логической функции в суперпозицию более простых функций. Методы решения с оптимизацией при всех успехах эвристической математики, как правило, приводят к большому перебору вариантов, что не гарантирует оптимальность найденных решений. Методы построения оптимальных (содержащих меньше переменных, или с непересекающимися сомножителями в логических суммах) формул для частично заданных логических функций имеют алгоритмы комбинаторной сложности с экспоненциальным ростом затрат вычислительных ресурсов от размеров решаемых таблиц (как по количеству переменных, так и по количеству обучающих объектов).

4. Принципы составления полного набора данных

Исходя из вербального определения «рискованное действие – это дело, затеянное на удачу в надежде на успех», собственно, вытекает идеология оценок, анализа и управления рисками. Что в данном определении присутствует? Первое – наличие, как минимум, двух исходов – «успешный», на который имеется надежда, и «неуспешный», при котором затеянное не свершается или свершается в меньшем масштабе. В тех редких случаях, когда имеется только два исхода, рисковая ситуация описывается платежной матрицей (табл. 1).

Таблица 1 – Платежная матрица

	Успешный исход	Неуспешный исход
Выгода (платеж за действие)	X_0	X_1
Мера возможности реализации	p_0	$p_1=1-p_0$

Недополученная выгода (X_0–X_1) называется, как правило, ущербом, а величина математического ожидания недополученной прибыли – риском R:

$$R = p_0\left(X_0 - X_0\right) + p_1\left(X_0 - X_1\right) = p_1\left(X_0 - X_1\right). \quad (1)$$

В случае, когда возможна угроза реализации неуспешных исходов с различными ущербами (X_0–X_n), риск исчисляется по формуле:

$$R = \sum_{n=1}^{N} p_n\left(X_0 - X_n\right). \quad (2)$$

Формула (2) может быть корректно применима для текущей оценки рискового действия только в тех случаях, когда это действие «обратимо», то есть, когда имеется возможность повторить это действие достаточно большое число раз для того, чтобы обеспечить сходимость «по вероятности».

При анализе слабо формализуемых угроз такая ситуация не наблюдается.

Во-первых, как правило, исследователям ничего не известно о возможности или невозможности появления «новых» сценариев с неуспешными исходами, кроме тех, что внесены в анализируемую платежную матрицу (табл. 1). Поэтому, хотя и должно выполняться классическое условие $\left(p_0 + \sum_{n=1}^{N} p_n = 1\right)$, но величины $p_n(n=0, \ldots, N)$ – это не вероятности (probability (вероятность) – апостериорные вероятности, подсчитанные частоты), а возможности (likelihood (правдоподобие) – априорные вероятности, предполагаемые пропорции реализации исходов).

Во-вторых, приходится считать, что различных сценариев слишком много, и каждый из них имеет пренебрежительно малую вероятность реализации. Собственно, в жизненном процессе реализуется только один единственный сценарий – тот, который реализуется в реальности. Поэтому неуспешные исходы должны группироваться в классы. Первая процедура при разбиении исходов на классы осуществляется по признаку эквивалентности ущербов, что опять-таки неправильно с позиций классической теории вероятностей: величины оценок возможностей $p_g(g=0, \ldots, G)$, где индекс g указывает на группу исходов, зависят от субъективного восприятия ущерба (значимости ущерба). В результате анализируется распределение «псевдовероятностей» по шкале исследователя, а не по шкале природы явления.

В-третьих, часто решение о вступлении в рискованное действие реализуется лишь один раз, поэтому сомнительно использовать вероятностные имитационные инструменты анализа типа метода Монте-Карло.

В-четвертых, часто приходится решать задачу выбора рискованного действия из множества альтернативных вариантов, чтобы исключить риски неприемлемого уровня. Оценочная функция, соответствующая случаю недопущения ущерба ниже теоретически возможного, предполагает, что от действий, для которых существует хотя бы один сценарий $\tilde{n}$, при котором ущерб $\left(X_0 - X_{\tilde{n}}\right)$ превышает заданный уровень, надо отказаться. Оценочная функция, соответствующая политике «крайней осторожности», строится на основе минимаксного критерия.

Для оценки угроз такой критерий, впрочем, трудно признать пригодным для использования – редкие сценарии с большими ущербами отменили бы любую деятельность кроме «безнаказанной». Поэтому на практике приходится «сглаживать» ситуацию, что делается несколькими путями.

Первый – оценивать ущербы и риски, занимая «уравновешенную» позицию. Предполагается, что на практике реализуются варианты между точками зрения крайнего оптимизма (только успех, а другого не может быть) и крайнего пессимизма (прикладываются максимальные усилия на предотвращение и/или смягчение ущербов от угрозы, но все равно реализуется наихудший из возможных сценариев реализации угрозы).

Второй – угадать и корректировать пропорции, в которых ожидаются возможные реализации сценариев угроз, для этого необходимо «периодически» оценивать текущее состояние, тенденции изменения и прогнозируемые состояния угроз. То есть, речь идет о построении адаптивной схемы корректировки платежных матриц.

Это разделение крайне важно, так как различные источники информации имеют различную специфику воздействия на оценки рискованных действий.

Так, например, «компетентные источники» могут уточнять текущее состояние – вплоть до внесения новых альтернатив реализаций угроз (столбцов платежных матриц). Но отслеживание динамики состояния угроз для них не является основным видом деятельности. Научно-технологические источники достаточно уверенно могут дать предельные характеристики прогнозируемых величин (скажем, даты промышленного освоения той или иной технологии).

А вот оценки тенденций, оценки скоростей нарастания или ослабления угроз можно получать только путем анализа показателей внештатных и кризисных ситуаций.

Основанием для создания мониторинговых модулей могут служить многочисленные факты, указывающие на то, что, прежде чем сформируется угроза большого масштаба (например, крупного землетрясения), этому предшествует серия угроз меньшего масштаба (учащающиеся мелкие толчки).

Экспертно-аналитическая система должна быть многофункциональной и многоуровневой системой, предназначенной как для фиксации и анализа каждого конкретного случая (события), так и для прогнозирования тенденций и формирования профилактических мероприятий, если таковы ожидаются. Ожидание тех ситуаций, которые требуют действий, типично для служб пожарной охраны, МЧС, скорой медицинской помощи. В случае же слабо формализуемых угроз стационарного характера негативных событий нет «по определению», поэтому об этих угрозах система узнает из компетентных источников, сообщающих об этих угрозах в дополнение к их основной деятельности, либо из СМИ, когда об угрозе говорят все, «кому не лень». Между «компетентными источниками» и «общедоступными СМИ» имеется ши-

рокий спектр источников информации типа «материалы выставок и конференций», публикации научных изданий и специалистов, местная пресса (заведомо более близкая к субъектам и объектам угроз) и т.п.

Все источники информации, таким образом, выстраиваются в некоторую двумерную шкалу. Первое измерение отражает комплиментарность источника информации: «свой», «приближенный», «нейтральный», аффилированный с конкурентами, «недружественный». Второе измерение отражает уровень специализации (компетентности) источника информации. Например, к мнению специалиста (узкоспециализированного журнала) в его области естественно относиться с большим доверием, но с меньшим доверием в более широкой области, поскольку такой источник, «очевидно», будет переоценивать факты и результаты из своей области, и принижать значимость фактов и результатов из смежных областей, рассматривая их в качестве конкурентов. Оценивая ту или иную информацию, поступающую от источника по соответствию реальности (на потоке ретроспективных данных), мы можем сформировать отношение к источнику как к некоторому инструменту измерения, классификации, распознавания той или иной ситуации.

Большое разнообразие альтернативных источников информации требует проведения их сравнительного анализа и, по возможности, отбора и оптимизации задолго до того, как принять решение об использовании их в практической работе системы обеспечения безопасности.

Для этого необходим ответ на ключевой вопрос, а именно: по каким критериям оценивать источники, чтобы обеспечить сравнимость результатов их использования? В качестве технических критериев качества источников можно использовать показатели полноты и точности [17, 18].

Коэффициент полноты *ComplMcl* метода классификации *Mcl* равен доле правильно классифицированных объектов класса C из тестирующей выборки $\{X\}^{\in C \Rightarrow \in C}$ к полному количеству объектов класса C, находящихся в ней $\{X\}^{\in C}$:

$$ComplMcl = \frac{\{X\}^{\in C \Rightarrow \in C}}{\{X\}^{\in C}}. \quad (3)$$

Коэффициент точности *ExactMcl* метода классификации *Mcl* равен доле правильно классифицированных объектов класса C из тестирующей выборки $\{X\}^{\in C \Rightarrow \in C}$ к полному количеству объектов этой выборки, которые были классифицированы как принадлежащие классу C:

$$ExactMcl = \frac{\left|\{X\}^{\in C \Rightarrow \in C}\right|}{\left(\left|\{X\}^{\in C \Rightarrow \in C}\right| + \left|\{X\}^{\in C}\right|\right)}. \quad (4)$$

Коэффициент полноты связан с ошибками первого рода – неправильной классификацией объектов, принадлежащих классу C. Коэффициент точности корреспондируется с ошибками второго рода – классификациями ложных объектов как принадлежащих классу C.

Хороший метод классификации должен допускать меньше ошибок, то есть, иметь большие значения *ComplMcl* и *ExactMcl*. Однако 100% результат достигается лишь на специально подготовленных «эталонных» массивах данных. На практике же редко наблюдается одновременное превышение величинами *ComplMcl* и *ExactMcl* значения 70% [19, 20].

Повышение надежности оценок для формирования обучающих выборок требует наличия объясняющих компонент, что вытекает из аналитического характера деятельности.

В практике мы фактически наблюдаем два типа оценок:

• оценки собственно экспертов-источников;

• оценки, рассчитываемые из близости размещения текстов, поступающих от источников, по близким рабочим местам.

То есть, окончательную оценку качества источников требуется проводить по «конечному результату». В качестве интегральных критериев доверия к источнику информации предлагаются следующие показатели:

• среднее время наработки критического количества ошибок источника;

• среднее время наработки критического соотношения ошибок первого и второго рода, совершенных на базе данных источника.

Заключение

Таким образом, в части задачи построения системы мониторинга безопасности и прогнозирования рисков ССС следует рассматривать возможность одновременного использования двух базовых показателей ее развития: рисков развития (в качестве которых могут использоваться количественные показатели, определяющие неблагоприятное сочетание вероятностей возникновения опасных процессов и их последствий – ущербов – в экономическом и научно-технологическом развитии компании на заданном прогнозном отрезке времени) и эффективности комплексных мероприятий в процессе развития (количественный показатель, определяющий повышение стратегически важных уровней экономического и научно-технического развития компании на прогнозном отрезке времени за счет формирования и проведения корпоративной политики по базовым приоритетным направлениям, методам, критериям и системам реализации прогнозов с учетом стратегических рисков развития).

Для адекватной оценки текущего состояния системы необходимо иметь:

• полную систему индикаторов состояния системы и внешней (конкурентной) среды (описание позиции);

• генератор конечного обозримого количества возможных сценариев развития системы (ходы «своих» «фигур», «нейтральные» ходы «природы» и антагонистические ходы «фигур» «противника»);

• функцию оценки состояния (выигрыш – улучшение позиции – ухудшение позиции – проигрыш).

При этом, не дожидаясь наступления «проигрыша» (при ухудшении оценки текущего состояния, или же когда конкуренты предпринимают нерассмотренные ранее ходы), необходимо искать новые сценарии развития, поскольку

все рассмотренные ранее варианты приводят к проигрышу или вероятность благоприятных последствий чрезвычайно мала. Вследствие того, что в развитии любой системы присутствуют активные противники (конкуренты), частично управляемые внутренние факторы (техногенная и антропогенная аварийность) или неуправляемые факторы (природные бедствия и катастрофы) все сценарии носят вероятностный характер. Поэтому даже при плавном изменении состояния системы (в котором невозможно получить крупный проигрыш в короткое время) необходимо учитывать фактор накопления случайностей и разрабатывать индикаторы оценки близости исследуемой системы к границам потери устойчивости развития.

Библиографический список

1. **Аксенов Г.П.** Вернадский [Текст] / Г.П. Аксенов. – М.: Молодая гвардия, 2015. – 526[2] с.: ил. – (Жизнь замечательных людей).

2. По материалам: Word frequency history based on a Google Books sample of one million books in English; Michel, J.-B., Y. K. Shen, A. P. Aiden, A. Veres, M. K. Gray, The Google Books Team, J. P. Pickett, D. Hoiberg, D. Clancy, P. Norvig, J. Orwant, S. Pinker, M. A. Nowak, and E. L. Aiden. «Quantitative Analysis of Culture Using Millions of Digitized Books» Science 331 (2011).

3. **Казеннов А.С.** К пониманию единства анализа и синтеза [Электронный ресурс] / А.С. Казеннов. – URL: http://www.smyrnyh.com/?page_id=686. – Дата доступа: 18.08.2019.

4. Critical Infrastructure Security. Assessment, Prevention, Detection, Response [Text] / Edited By: F. Flammini (2012). // WIT Transactions on State-of-the-art in Science and Engineering (ISBN 978-1-84564-562-5). – 2012. – Volume 54. – 325 p.

5. National Infrastructure Protection Plan [Text]. – U.S. Department of Homeland Security, 2009. – 100 p. – (Available at www.DHS.gov).

6. National Strategy for the Physical Protection of Critical Infrastructure and Key Assets [Text]. – U.S. Department of Homeland Security, 2003. – (Available at www.DHS.gov).

7. **Dudenhoeffer D.D.** CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis [Text] / D.D. Dudenhoeffer, M.R. Permann, M. Manic: In L.F. Perronc, F.P. Wieland, J. Liu, B.G. Lawson, D.M. Nicol & R.M. Fujimoto (Eds) // Proceedings of the 2006 Winter Simulation Conference. – Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2006. – P. 478-485.

8. **Perrow C.** Normal Accidents [Text]. – Princeton University Press, Princeton, NJ, 1999. – 450 p.

9. **Ramo J.C.** The Age of the Unthinkable [Text]. – Little, Brown & Company, New York, NY, 2009. – 280 p.

10. National Research Council, The Internet Under Crisis Conditions: Learning from September II. National Academics Press. – Washington, DC, 2003. – (Available at www.nap.edu).

11. August 14th Blackout: Causes and Recommendations. – U.S.-Canada Power System Outage Task Force, April 2004. – P. 12. – (Available at https://reports.energy.gov).

12. **Рябинин И.А.** Надежность и безопасность структурно-сложных систем [Текст] / И.А. Рябинин. – СПб.: Изд-во С.-Петерб. Ун-та, 2007. – 276 с.

13. **Taleb N.N.** Antifragile: Things That Gain from Disorder (Incerto) [Text] / N.N. Taleb // Series: Incerto (Book 3). – Random House Trade Paperbacks: Reprint edition (January 28, 2014). – 544 p.

14. **Радаев Н.Н.** Методические аспекты задания требования, оценки и обеспечения защищенности объектов газовой отрасли от противоправных действий [Текст] / Н.Н. Радаев, В.В. Лесных, А.В. Бочков: Монография. – М.: ООО «ВНИИГАЗ», 2009. – 164 с.

15. **Bochkov A.V.** Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty [Text] / A.V. Bochkov, N.N. Zhigirev : In: Ram M., Davim J. (eds) // Advanced Mathematical Techniques in Engineering Science. Series: Science, Technology and Management. – 2018. – May, 17. – P. 121-154.

16. **Бочков А.В.** Использование метода опорных векторов для поиска скрытых закономерностей в задачах классификации ситуаций, описываемых оцененными вопросниками [Текст] / А.В. Бочков, Н.Н. Жигирев // Proceedings 8th DQM International Conference Life Circle Engineering and Management ICDQM-2017. – 2017. – June 29-30. – P. 43-71.

17. **Корнеев В.В.** Интеллектуальная обработка данных [Текст] / В.В. Корнеев, А.Ф. Гареев и др. – М.: Нолидж, 1999.

18. **Salton G.** Automatic Text Processing [Text] / G.Salton. – Addison-Wesley Publishing Company, Inc., Reading, MA, 1989.

19. **Гареев А.Ф.** Решение проблемы размерности словаря при использовании вероятностной нейронной сети для задач информационного поиска [Текст] / А.Ф. Гареев // Нейрокомпьютеры: разработка, применение. – 2000. – №1. – С. 60-63.

20. Global Trends 2015: A Dialogue About the Future With Nongovernment Experts [Электронный ресурс] / This paper was approved for publication by the National Foreign Intelligence Board under the authority of the Director of Central Intelligence. Prepared under the direction of the National Intelligence Council. NIC 2000-02, December 2000. – URL:http://infowar.net/ cia/publications/globaltrends2015/ http://www.futurebrief.com /globaltrend2015.pdf.

Сведения об авторе

Александр В. Бочков – кандидат технических наук, заместитель начальника отдела анализа и ранжирования объектов контроля Администрации ООО "Газпром газнадзор" (Москва, Россия). e-mail: a.bochkov@gmail.com

Вклад автора в статью

Автор выполнил сравнение основных концепций управления рисками и показал необходимость их творческого развития. Предложен вид функционала риска, позволяющего определять решение в области обеспечения безопасности величиной математического ожидания потерь с учётом некоторых поправок. Автором введено понятие «синтез рисков» и сформулированы предпосылки к разработке соответствующего метода.

Gnedenko e-Forum
International Group on Reliability

http://www.gnedenko.net

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.

ТРЕБОВАНИЯ РЕДАКЦИИ ПО ОФОРМЛЕНИЮ СТАТЕЙ В ЖУРНАЛАХ ИЗДАТЕЛЬСКОЙ ГРУППЫ IDT PUBLISHERS

Письмо от организации, где работает автор(ы), либо лично от автора(ов) с предложением о публикации статьи направляется в редакцию журнала по адресу: 109029, г. Москва, ул.Нижегородская, д. 27, стр.1, офис 209, ООО «ЖУРНАЛ «НАДЕЖНОСТЬ» или по адресу e-mail: dependability@bk.ru (в отсканированном виде).

К письму прилагается в электронном виде (на CD или по приведенному выше E-mail) текст статьи с аннотацией и ключевыми словами, информацией об авторах, с пристатейным библиографическим списком, предоставляется с одним комплектом рисунков

Внимание! Названия статьи, ФИО авторов, аннотация и ключевые слова обязательно представляются в соответствии с требованиями ВАК на русском и английском языках. Аннотация не менее 350 слов.

Информация о каждом авторе должна содержать следующие стандартные сведения:

- **Фамилия, имя, отчество;**
- **Ученая степень, ученое звание, почетное звание;**
- **Членство в общественных союзах и т.д.;**
- **Место работы, должность;**
- **Перечень и номера журналов IDT Publishers, в которых ранее публиковались статьи автора;**
- **Сведения для контактов;**
- **Фотографии всех авторов статьи.**

Текст необходимо набирать в редакторе Word 97-2003 шрифтом № 12; текст не форматируется. Абзацы организуются путем нажатия клавиши Enter. Текст статьи набирается через полтора интервала на странице формата А4; слева должно быть поле 2 см; страницы нумеруются, «красная строка» обязательна.

Все буквенные обозначения, приведенные на рисунках, необходимо пояснять в основном или подрисуночном тексте. Недопустимы отличия в обозначениях на рисунках и в тексте. Нумеровать следует только те формулы и уравнения, на которые есть ссылка в тексте.

Непосредственно в тексте набираются простые формулы (например, m^2; n^2t, $C = 1 + DDF - A_2$), греческие буквы и символы, например, β, © — шрифтом Symbol. То, что невозможно набрать непосредственно в текстовом редакторе, — с использованием редактора формул Microsoft Equation (входящего в комплект поставки Microsoft Office) или редактора формул Mathtype.

Не допускается представление текста, в котором формулы представлены в виде изображения. Фотографии и рисунки к статьям предоставляются отдельными файлами с расширением TIF, или EPS или JPEG с разрешением не менее 300 dpi .

Список использованной литературы составляется в порядке цитирования и дается в конце статьи. Ссылки на литературу в тексте отмечаются порядковыми цифрами в квадратных скобках.

Вниманию авторов, публикующихся в журналах IDT Publishers.

Представленная информация о каждом авторе помимо журнала будет размещаться на сайте techizdat.ru в разделе “Авторы” на отдельной интернет-странице.

Авторам также предоставляется возможность при публикации своих статей направить в редакцию свою электронную фотографию и дополнительные материалы для размещения их на этой индивидуальной Интернет-визитке. По своему усмотрению автор может рассказать более подробно о себе, об интересных примерах и историях решения технических проблем, о современных задачах – в соответствии с тематикой соответствующего журнала – и т.п. Желательный объем этого материала – не более 1000 знаков с пробелами.

ПОДПИСКА НА ЖУРНАЛ «НАДЕЖНОСТЬ»

Подписаться на журнал можно:

- Через агентство «Роспечать» – индекс 81733;
- По каталогу «Пресса России» агентства «Книга-Сервис» – индекс 11804;
- Через редакцию на любой срок
  тел.: 8 (495) 967-77-05
  e-mail: dependability@bk.ru

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: dependability@bk.ru
ИНН 7709868505 КПП 770901001
р/с 40702810100430000017, ПАО «УРАЛСИБ БАНК» г. Москва
к/с 30101810100000000787

Адрес доставки:

Кому:_____

Куда:_____

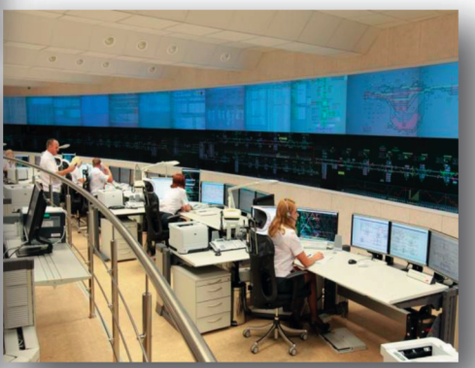
_____

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

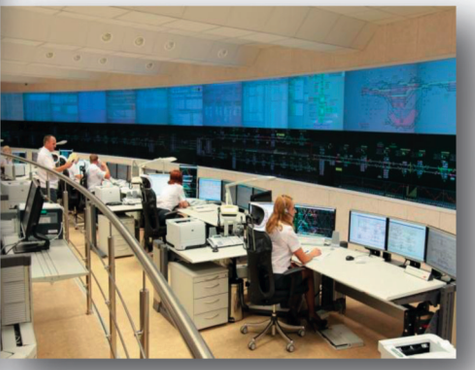
Основные направления деятельности

- •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
FOR INFORMATION TECHNOLOGY, SIGNALLING AND TELECOMMUNICATIONS
ON RAILWAY TRANSPORT (JSC NIIAS)



JSC NIIAS 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:

transportation

- ❑ efficiency,
- ❑ 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.vniias.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: dependability@bk.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.

REQUIREMENTS OF EDITION ON EXECUTION OF PAPERS IN JOURNALS OF PUBLISHING GROUP OF IDT PUBLISHERS

A letter from the organisation where the author (s) works or from the author (s) personally with the paper offered for publication should be sent to the de facto editorial office address: 109029, Moscow, Str. Nizhegorodskaya, 27, Building 1, office 209, LLC "JOURNAL DEPENDABILITY" or e-mail: dependability@bk.ru (in scanned form).
The letter should be attached to a paper text containing the summary and keywords, information on authors, bibliographic list, and one complete set of figures. All listed items are to be presented in an electronic form (on CD or via the e-mail address provided above).
Attention! Titles of papers, names of authors, summary and keywords must be presented, in Russian and English languages, according to the requirements of the Higher Attestation Commission. The information on each author should contain the following standard data:
- Surname, name, patronymic;
- Scientific degree, academic status, honorary title;
- Membership of relevant public unions, etc.;
- Place of employment, position;
- The list and numbers of Journals of IDT Publishers in which papers of the author have been previously published;
- Contact information.

Texts should be presented in Word 97-2003 format in a 12-point typeface; the text should not be formatted. Paragraphs should be arranged by pressing the "return" key. The text of the paper should be double-spaced on pages of A4; on the left there should be a margin of 2 cm; pages should be numbered, the «first line indent» is obligatory.
All alphabetical designations represented in figures should be explained in the body text or in a legend. Inconsistencies between designations in figures and in the text are inadmissible. Numbering should only be applied to those formulas and equations that are referred to in the text.
Simple formulas appearing directly in the text (for example, m^2, n^2t, $c = 1 + DDF - A_2$), and the Greek letters and symbols, for example, β, © may be typed using the Symbol font. When it is not possible to type directly in the text editor, use the "Microsoft Equation" formula editor (available with the complete installation of Microsoft Office) or the "Mathtype" formula-editing program. Representation of formulae in the text in the form of images is not admissible. Photos and figures for papers should be provided in individual files with extension TIF, EPS or JPG with a resolution of not less than 300 dpi. The list of literature referred to in the paper (bibliography) is presented according to order of citation and provided at the end of paper. References to the literature in the text are marked by serial numerals in square brackets.

To authors that are published in journals of "IDT Publishers".
In addition to the journal, information on each author will be presented at the techizdat.ru site in the «Authors» section on the individual web page.
Authors of papers for publication have the opportunity to send an electronic photo and additional material to appear on this individualised Internet-business card. At their own discretion, authors can present more details about themselves, interesting examples and stories of solutions to technical problems, about contemporary problems according to subjects of corresponding journal, etc. This material should not exceed 1000 characters including spaces.

SUBSCRIPTION TO THE JOURNAL «DEPENDABILITY»

It is possible to subscribe to the journal:

- Through the agency «Rospechat»
  – for the first half of the year: an index 81733;

- Under the catalogue "Press of Russia" of the agency «Books-services»:
  – for half a year: an index 11804;

- Through the editorial office:
  – for any time-frame
  tel.: +7 (495) 967-77-05; e-mail: dependability@bk.ru

Gnedenko e-Forum

International Group on Reliability

http://www.gnedenko.net

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.

in data mining as part of classification of questionnaire-described situations]. Proceedings of the 8th DQM International Conference Life Circle Engineering and Management ICDQM-2017; 2017 [in Russian].

[17] Korenev VV, Gareev AF et al. Intellektualnaya obrabotka dannykh [Intelligent data processing]. Moscow: Nolidzh; 1999 [in Russian].

[18] Salton G. Automatic Text Processing. Reading (Massachusetts, USA): Addison-Wesley Publishing Company, Inc.; 1989.

[19] Gareev AF. Reshenie problemy razmernosti slovarya pri ispolzovanii veroyatnostnoy neyronnoy seti dlya zadach informatsionnogo poiska [Solution to the problem of directory size in the context of application of probabilistic neural networks in information search]. Neyrokompyutery: razrabotka, primenenie 2000;1:60-63 [in Russian].

[20] Global Trends 2015: A Dialogue About the Future With Nongovernment Experts. This paper was approved for publication by the National Foreign Intelligence Board under the authority of the Director of Central Intelligence. Prepared under the direction of the National Intelligence Council. NIC 2000-02; December 2000, http://infowar.net/cia/publications/globaltrends2015/ <http://www.futurebrief.com /globaltrend2015.pdf>.

About the author

Alexander V. Bochkov, Candidate of Engineering, Deputy Head of Unit for Analysis and Ranking of Controlled Facilities, Gazprom Gaznadzor, Russian Federation, Moscow, e-mail: a.bochkov@gmail.com

The author's contribution

The author has compared the primary concepts of risk management and shown it is to be developed and improved. A type of risk functional is proposed that allows defining a safety solution with the value of mathematical expectation of losses, subject to corrections. The author introduces the concept of "risk synthesis" and sets forth the prerequisites for the development of the corresponding method.

Conclusion

Therefore, for the purpose of the construction of a safety monitoring and risk prediction system of SCS, we should consider the possibility of simultaneous application of two basic indicators: risks of development (in this capacity we can use quantitative indicators that identify unfavorable combination of probabilities of occurrence of dangerous processes and their consequences (harms) in the economic and scientific development of a company at the specified forecasted period of time) and efficiency of comprehensive measures in the development process (quantitative indicator that determines the increase of strategic levels of economic and scientific development of a company at the forecasted period of time owing to the development and implementation of corporate policy on basic priority directions, methods, criteria and systems of prediction implementation taking into account the strategic risks of development).

For the appropriate assessment of the current status of a system, it is necessary to have:

• Complete system of indicators of the status of the system and environment (competitive environment) (description of the position);

• Generator of the finite possible number of scenarios of the system development (moves of "your own figures", "neutral" moves of "nature" and "antagonistic" moves of "competitor's figures");

• Functions of status assessment (win – improvement of the position – deterioration of the position – lose).

At the same time, without waiting for "lose" happening (in the case of the deterioration of the assessment of the current state, or competitors take moves not forecasted before), it is necessary to search for new development scenarios, since all the previously reviewed options result in loss or the probability of favorable consequences is extremely small. Since in the development of any system there are active opponents (competitors), partially controlled internal factors (technological and human accidents) or uncontrolled factors (natural disasters and accidents), all scenarios have a probabilistic nature. Therefore, even with a smooth change of the system's status (in which it is impossible to result in a huge loss in a short time), it is necessary to take into account the factor of accumulation of accidents and to develop the indicators for assessing the proximity of a tested system to the limits of the loss of sustainable development.

References

[1] Aksyonov GP. Vernadsky. Moscow: Molodaya gvardia; 2015 [in Russian].

[2] Michel J-B, Shen YK, Aiden AP, Veres A, Gray MK, The Google Books Team, Pickett JP, Hoiberg D, Clancy D, Norvig P, Orwant J, Pinker S, Nowak MA, Aiden EL. Word frequency history based on a Google Books sample of one million books in English. Quantitative Analysis of Culture Using Millions of Digitized Books. Science 2011;331.

[3] Kuznetsov AS. K ponimaniyu edinstva analiza i sinteza [Towards the understanding of the unity of analysis and synthesis], <http://www.smyrnyh.com/?page_id=686>; 2019 [accessed 18.08.2019] [in Russian].

[4] Flammini F, editor. Critical Infrastructure Security. Assessment, Prevention, Detection, Response. WIT Transactions on State-of-the-art in Science and Engineering 2012;54. ISBN 978-1-84564-562-5.

[5] National Infrastructure Protection Plan. U.S. Department of Homeland Security; 2009, <

[6] National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. U.S. Department of Homeland Security; 2003, <.

[7] Dudenhoeffer DD, Permann MR, Manic M. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In: Perronc LF, Wieland FP, Liu J, Lawson BG, Nicol DM, Fujimoto RM, editors. Proceedings of the 2006 Winter Simulation Conference. Piscataway (New Jersey, USA): Institute of Electrical and Electronics Engineers; 2006. p. 478-485.

[8] Perrow C. Normal Accidents. Princeton (New Jersey, USA): Princeton University Press; 1999.

[9] Ramo JC. The Age of the Unthinkable. New York: Little, Brown & Company; 2009.

[10] National Research Council, The Internet Under Crisis Conditions: Learning from September 11. Washington, DC: National Academics Press; 2003, <

[11] August 14th Blackout: Causes and Recommendations. U.S.-Canada Power System Outage Task Force; 2004, <https://reports.energy.gov>.

[12] Riabinin IA. Nadezhnost i bezopasnost strukturnoslozhnykh sistem [Dependability and safety of structurally complex systems]. Saint Petersburg: Saint Petersburg University Publishing; 2007 [in Russian].

[13] Taleb NN. Antifragile: Things That Gain from Disorder. Random House Trade Paperbacks: Reprint edition; 2014.

[14] Radaiev NN, Lesnykh VV, Bochkov AV**.** Metodicheskie aspekty zadaniya trebovaniya, otsenki i obespecheniya zashchishchennosti obektov gazovoy otrasli ot protivopravnykh deystviy. Monogrfia [Methodology aspects of requirements specification, assessment and assurance of gas facilities protection against unlawful activities. A monograph]. Moscow: VNIIGAZ; 2009 [in Russian].

[15] Bochkov AV, Zhigirev NN. Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty. In: Ram M, Davim J, editors. Advanced Mathematical Techniques in Engineering Science. Series: Science, Technology and Management 2018; May 17, p. 121-154.

[16] Bochkov AV, Zhigirev NN. Ispolzovanie metoda opornykh vektorov dlya poiska skrytykh zakonomernostey v zadachakh klassifikatsii situatsiy, opisyvaemykh otsenennymi voprosnikami [Use of the method of reference vectors

rent state, trends and predicted threats. This means the construction of an adaptive scheme for correction of payoff matrices.

This distinction is extremely important, since different sources of information have different specifics of impact on risk assessment.

For example, "sources of expertise" can update the current state up to introduction of new alternatives for implementing threats (columns of payoff matrices). However, control of dynamics in the state of threats is not their main activity. Science and technology sources can correctly produce limiting characteristics of predicted values (dates of industrial application of some technology).

On the contrary, estimations of trends, rate of increase or diminution of threats can be obtained by analyzing of indicators of emergency and crisis situations.

The basis for the creation of monitoring modules can be numerous facts indicating that before a large-scale threat (for example, a large earthquake) is formed, there are series of smaller-scale threats (increasing small tremors).

An expert analytical system should be a multifunctional and multilevel system intended for registration and analysis of each specific case (event) as well as for prediction of trends and generation of preventive activities if any. The expectation of those situations that require actions is typical for fire services, the Ministry of Emergency Situations, emergency medical services. In case of poorly formalizable threats of permanent character, there are no negative events "by definition"; therefore, the system gets information on these threats from competent sources who inform about these threats in addition to their main activities or from generally available media sources when everybody talks about a threat. There are a wide range of sources like exhibition and conference proceedings, scientific publication, local press (which is closer to the subjects and objects of threats) etc. between competent sources and generally available media sources.

Thereby, all information sources form some two-dimensional scale. The first dimension reflects complementarity of the information source: "reliable", "approximate", "neutral", affiliated with competitors, "unfriendly". The second dimension reflects the specialization (competence) level of information source. For example, it is natural to have a greater confidence for the opinion of a specialist (highly specialized magazine) and to have a less confidence for the opinion of specialists in a wide professional sphere because such a source will "obviously" overestimate facts and results in their sphere, and downplay the importance of facts and results obtained from neighboring spheres considering them as competitors. Evaluating different information obtained from a source in terms of its relation to reality (on the stream of retrospective data), we can form an attitude to the source as some tool for measuring, classifying, identifying a particular situation.

A great variety of alternative information sources requires a comparative analysis of them and, if possible, their selection and optimization long before taking a decision to use them in the practical work of a safety ensuring system.

This requires an answer to the following key question: what criteria should be applied to assess information sources in order to ensure comparability of the results of their application? The indicators of information completeness and accuracy can be applied as technical criteria of sources' quality [17, 18].

Completeness coefficient *ComplMcl* of the classification method *Mcl* is equal to the share of correctly classified objects of *C* class from a test sample $\{X\}^{\in C \Rightarrow \in C}$ to the full number of objects of *C* class with $\{X\}^{\in C}$:

$$ComplMcl = \frac{\{X\}^{\in C \Rightarrow \in C}}{\{X\}^{\in C}}. \quad (3)$$

Accuracy coefficient *ExactMcl* of the classification method *Mcl* is equal to the share of correctly classified objects of *C* class from a test sample $\{X\}^{\in C \Rightarrow \in C}$ to the full number of objects of this sample, which were classified as belonging to the *C* class:

$$ExactMcl = \frac{\left|\{X\}^{\in C \Rightarrow \in C}\right|}{\left(\left|\{X\}^{\in C \Rightarrow \in C}\right| + \left|\{X\}^{\in C}\right|\right)}. \quad (4)$$

Completeness coefficient is associated with the mistakes of the first kind – an incorrect classification of objects belonging to *C* class. Accuracy coefficient corresponds to the mistakes of the second kind, i.e. with classifications of false objects as belonging to the *C* class.

The good classification method should allow fewer mistakes, i.e. has great values of *ComplMcl* and *ExactMcl*. However, the 100% result is achieved with the specified prepared "reference" data array. In practice, both *ComplMcl* and *ExactMcl* values seldom exceed 70% [19, 20].

Improving the reliability of estimates for the preparation of training samples requires explanatory components, which follows from the analytical nature of the activity.

In practice, we in fact observe two types of estimates:

• Estimates of experts (sources);

• Estimates calculated according to the similarity of text publications, which are acquired from the experts in similar professions.

That is, a final estimate of the sources' quality should be carried out according to the "final result". The following indicators are proposed as integral criteria of trust to the information source:

• Mean time to a critical number of mistakes in the source;

• Mean time to a critical ratio of mistakes of the first and second types made on the basis of the data source.

Table 1. Payoff matrix

	Success	Unsuccess
Profit (payment for action)	X_0	X_1
Feasibility measure	p_0	$p_1=1-p_0$

on a subset of attributes would be divided. This is a classical task of discrete mathematics on finding a logical function, and this task is solved in dozens of different ways, which are based on the method of decomposing any logical function into a superposition of simpler functions. With all successes of the heuristic mathematics, solution methods with optimization lead to a large enumeration of options, which does not guarantee the optimality of the solutions found. Methods of construction of optimum formulas (containing fewer variables, or with nonoverlapping multipliers in logical sums) for partially defined logical functions have combinatorial complexity algorithms with an exponential increase in the consumption of computing resources in line with the size of tables to be solved (both in the number of variables and in the number of training objects).

4. Principles for compiling a complete dataset

Based on the verbal definition of "risk action is an action for luck with the hope of success", the ideology of risk assessment, analysis and management follows. What does this definition include? The first is the presence of at least two outcomes: "successful", for which there is hope, and "unsuccessful", where the expected does not happen or happens on a smaller scale. In those rare cases, when there are only two outcomes, the risk situation is described as a payoff matrix (Table 1).

Lost profit (X_0–X_1) is usually called harm, and the mathematical expectation of lost profit is called risk R:

$$R = p_0 (X_0 - X_0) + p_1 (X_0 - X_1) = p_1 (X_0 - X_1). \quad (1)$$

In the case when there is a threat of implementation of unsuccessful outcomes with different harms (X_0–X_n), the risk is calculated in accordance with the following formula:

$$R = \sum_{n=1}^{N} p_n (X_0 - X_n). \quad (2)$$

Formula (2) can be correctly applied for the current assessment of the risk action in those cases when this action is "reversible", i.e. when there is a possibility to repeat this action several times in order to ensure convergence "in probability".

When analyzing poorly formalizable threats, this situation is not observed.

First, as a rule, researchers do not know anything about the possibility or impossibility of the appearance of "new" scenarios with unsuccessful outcomes, except for those that are included in the analyzed payoff matrix (Table 1). Therefore, although the standard condition $\left(p_0 + \sum_{n=1}^{N} p_n = 1 \right)$ should be fulfilled, the values p_n(n=0, …, N) are not probabilities (probability is posterior probabilities, calculated frequencies), but the possibilities (likelihood is priory probabilities, estimated proportions of outcomes).

Second, one must assume that there are too many different scenarios, and each of them has a negligibly small probability of implementation. In fact, only one scenario is realized in a life process, the one that is realized in real life. Therefore, unsuccessful outcomes should be grouped in classes. The first procedure when dividing the outcomes into classes is carried out on the basis of harm equivalence, which is incorrect in the context of the classical theory of probability: the values of the probability estimates, where the index g indicates a group of outcomes, depend on the subjective perception of harm (significance of harm). As a result, the distribution of "pseudoprobabilities" is analyzed on the researcher scale, not on the scale of the nature of a phenomenon.

Third, the decision on risk action is often implemented only once, so it is disputable to use probabilistic simulation analysis tools such as the Monte Carlo method.

Fourth, one must often solve the problem of choosing a risk action from many alternative options in order to exclude risks of an unacceptable level. An evaluation function, corresponding to the case of avoiding harm below the theoretically possible, suggests that actions for which there is at least one scenario, in which the harm $(X_0 - X_{\tilde{n}})$ exceeds the specified level, must be abandoned. An evaluation function corresponding to the "extreme care" policy is formed on the basis of minimax criterion.

To assess threats, however, such a criterion is hard to consider suitable for application; rare scenarios with great harm would cancel any activity except "unpunished". Therefore, in practice the situation must be "smoothed", and there are several ways to do this.

The first one is to assess harms and risks while taking a "balanced" position. It is assumed that in practice variants between extreme optimism (only success, there is no other way) and extreme pessimism (maximum efforts to prevent and/or smooth the harm are made but anyway the worst possible scenario for the threat is realized) take place.

The second one is to guess and correct proportions, in which possible threat scenarios are expected; for this purpose, it is necessary to assess "periodically" the cur-

detection of hidden regularities, which indicate changes of an object's state or the regularities of changes in the parameters of the external environment significantly influencing its functioning (the so-called laws of variability of "forecast background").

Due to the discrete nature of crisis situations, the application of data analysis apparatus based on classical laws of large numbers, is incorrect. Probability convergence is practically not observed in reality, except for the statistics accumulated in systems of mass service. The indicators panel realized in the form of "traffic light" constructed with the help of application of dispersion as the main indicator can indicate the normal state during the whole year when in fact the system passes in the area of pre-crisis values.

Besides, there is, as a rule, no univocal functional connection and mutual influence of indicators of lower and upper levels for an officially declared hierarchical system of indicators.

As a consequence, it is necessary to have a correct primary analysis of a long-term statistics, and only based on this analysis it can be concluded whether it is possible to develop a predicting instrument corresponding to a research problem and what share of randomness of dates in occurrence of unfavorable situations and their scale can be eliminated with its help. It is also obvious that as true laws of distribution of analyzed random processes and their determinants will be continuously corrected (any hi-tech system changes faster than adequate statistics are collected), it is necessary to use criteria "free from distributions". In particular, for example, as criteria of achievement of predictive purpose we should take not deviation values of model and real data, but the criteria used in classification and pattern recognition methods. For example, as measurement of prediction precision we can use the prediction error values of the first and second types for different classes and types of situations, depending on classes of a physical object and parameter values of the forecast background, if possible. The second circumstance is very important as, for example, it is incorrect to sum up accident statistics of different seasons, since during different seasons technological processes function differently.

The reliable execution of its functions by a system is characterized by retaining some specified characteristics (reflected in the corresponding STI and KPI values) in set limits. In practice, it is not possible to completely avoid deviations, but it is necessary to aim at minimizing deviations of the current state from some specified ideal – the target set, for example, in the form of STI values of the first level.

The threat of non-achievement of STI set values of the first level (in fact, we again speak about the risk) is considered in this case as a variable value, which is a function to the current state of the system: it increases with the assessed situation approaching to some permissible limit after reaching which the system cannot fulfill its obligations and reach respective STI set values of the first level.

General mathematical statement of a task in question: let there be a set of signs of the current situation X (for example, current KPI values, risk factors etc.), the set of admissible realization of Y situations (for example, the current STI value of the first level is higher (or less) than the previous one etc.), and let there be the target function $y^*: X \to Y$, whose values $y_i = y^*(x_i)$ are known only on the finale subset of objects $\{x_1,\ldots,x_l\} \subset X$ (for example, the KPI values that correspond to the current STI state of the first level). Pairs "object-answer" x_i, y_i are precedents. A set of pairs $X_l = \sum_{i=1}^{l} x_i, y_i = 1$ will make a training sample. It is required based on the sample X_l to recover y^* dependence, i.e. to construct a function $A: X \to Y$, which would approach a target function $y^*(x)$, and not only on objects of a training sample, but also on the whole set X. As a decisive function A should allow for a effective computer realization, it is possible to call it an algorithm.

Conditionally, there are two object classes faced by experts in the field of management automation: "simple" and "complicated". "Simple" ones are objects, whose precise mathematic models, for example, in the form of algebraic equations or linear programming models with all necessary quantitative factors that influence the object's behavior considered, are suitable for implementation on computers of a specific class and are quite adequate to the object. "Complicated" objects have the following distinctive features: not all purposes of the choice of decisions and conditions influencing this choice can be expressed as quantitative ratios; formalized description of a control object is absent or is unacceptably difficult; a significant part of information necessary for the mathematical description of an object is in the form of the ideas and proposals of experts etc. The construction of the exact mathematic models of the "complicated" objects suitable for implementation on modern computers is either difficult or often completely impossible.

But it does not mean that the task has no decision. In general, there are two possible ways of search. The first one is to try to apply a nontraditional mathematical tool for the creation of the model considering all object's features and suitable for implementation. The second one is to construct not an object's model, but an object control model (i.e. not an object itself is simulated but a human operator in the process of controlling an object). In its essence, the algorithm in this case is associated with the construction of a data structure field and the analysis of its effects, including the improvement of the structure itself. All data are structured and unstructured at the same time. As excluding OR is difficult to "construct", it is possible to realize the idea of the construction of solving rules (hereinafter is a solver) on the monotone function defining network order [15, 16].

The geometric significance of a solver is rather simple: it is necessary to select attributes in such a way, while keeping the characteristics of a specific order, that objects

the type of an initiating event, the amount of hazardous substance, the effectiveness of emergency safety systems and many others should be taken into account. Usually there are a large number of possible scenarios for the development of an accident. Therefore, the entire spectrum of possible scenarios and their probabilities should be determined when assessing the risk. The probability values can vary from 10^{-6} to 10^{-8} events per year. Rarer events are so difficult to evaluate that they are considered almost incredible.

Periodic risk is associated with those accidents, which are often repeated, but cause limited damage that may include human casualties. This does not mean that such accidents are planned. They are, of course, undesirable, and safety systems are created and used to prevent them. However, despite these measures, such accidents can occur, and the risk associated with them has a fairly wide range of values depending on the type of production activity. The cause of such accidents is usually a violation of the procedure, improper use of equipment and human error. To assess the risk of this category, accident frequency and other necessary parameters are estimated using standard statistical methods based on available data.

Hypothetical risk is associated with accidents, which are believed to occur with a very low probability but have very severe consequences. This class of accidents is characterized by the absence or insufficient amount of statistical data. But because of the enormous potential damage, it is impossible to just wait until enough practical experience is gained. Therefore, an analysis of hypothetical accidents is carried out in order to determine the probability of this accident and assess its possible consequences. Typically, a lack of statistics refers to the behavior of a large industrial or energy system as a whole. Therefore, such an analysis is carried out either by means of an expert assessment, or by the "event tree" method, where the probability of a hypothetical accident can be predicted based on possible malfunctions or failures in the operation of individual nodes or mechanisms, for which relevant statistics are available.

It should be remembered that there is no need to use overly complicated models for risk assessment due to many uncertainties and averagings that arise in the calculation. By the way, finding the degree of uncertainty and the range of possible risk values is another composite characteristic of risk in general. Thus, according to various experts, the uncertainty in assessing the risk of accidents at industrial enterprises can be one or even reach two orders of magnitude. This is due to the lack of knowledge on a wide range of technical, environmental and social factors that must be considered in risk analysis. There are even opinions, which are based on the analysis of accuracy and uncertainty in risk assessment, that translation models that allow for obtaining the concentration of a hazardous substance in the study area with an accuracy of 10% (maximum 20%) are quite acceptable.

3. Comments on a monitoring system

Thereby, the stable functioning and development of any SCS are subject to the influence of many external and internal factors including negative impact factors. To monitor and assess these factors and make a decision aimed at reducing negative effects of their manifestations, the so-called systems of balanced scorecard and key performance indicators (KPI) (quantitatively characterizing the risk factors to which the system is exposed) are widely implemented. From these indicators one chooses strategic targeted indicators (STI) that quantitatively reflect strategic goals of the system's functioning and represent basic economic and production indicators, which characterize the effectiveness of its development (if they are not achieved, it indirectly characterizes the level of existing threats and degree of their implementation in the considered period of time).

Based on these indicators, one constructs threats and risks monitoring systems that allow collecting data on changes as well as analyze the effectiveness of the system for several hundred indicators in organizational, product, geographical and other sections on daily, quarterly and annual planning horizons. It is believed that the results of the analysis allow for "deviation control", focusing on the problem areas of each control object through a "traffic light" indication. However, as collected data is growing bigger, there arises a problem related to interpretation of signals of these hundreds of "traffic light indicators". It is not obvious what signal should be considered as "good" or "bad" for the system in general if, for example, half of the indicators are "green", and half are "red". The question is how to qualify the situation if there are a little more of "green" indicators than of "red" etc. One cannot also say that there is an obvious connection of the analyzed indicators with the high-level indicators (STI) and the degree of their influence on the achievement of STI target values approved by the company management. There arises the so-called "Big Data" effect, when analysts cannot manage to process the collected information, and standard statistical methods are just not coping.

Besides, based on the analysis of trend in indicators changes, a system of threats and risk monitoring is not capable to predict crises and situations with negative dynamics. Such events are rare and as a rule take place at various forecast backgrounds, and in case of the analysis of historical datasets of rare events there are discrete dynamic probabilistic processes in place.

The purpose of analysis of SCS as an object for forecasting in the field of operation safety and development sustainability is the creation of such a predictive model of situations dynamics arising out of its functioning that will allow reducing the degree of uncertainty of events dates and their scale by means of computing experiments and selection of acceptable parameters, i.e. obtaining predictive information on the forecast object owing to

Only in this case the solution will really be determined by the value of the mathematical expectation of losses. But adjusted for B and $\overline{C}$. In many works these corrections are not taken into account. Usually B and $\overline{C}$ are considered equal to zero. For example, in ecology, improving the "air" costs nothing (does not bring profit), and if no one is sick, then the optimal damage is taken as 0.

Bayes criterion leads to the same estimates:

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M} \left(\sum_{n=1}^{M} p_n \times A_{mn} \right) =$$

$$= \left(B = 0; \overline{C} = 0\right) = \min_{1 \le m \le M} \left(\sum_{n=1}^{M} p_n \times C_{mn} \right).$$

In general, the problem of safety insurance and risk analysis of SCS facilities in the face of changes in the composition and intensity of threats to the sustainable development of the industry remains relevant. Safety requirements established for objects of high and medium hazard categories are sometimes rather high and significantly surpass the capabilities of property owners. As a result, the question of ranking the objects within the given categories to determine the sequence of equipping them with the required protective means arises. In order to do that, it is necessary to set a criterion to determine the importance (and the serial number accordingly) of an object in the ranked list against it.

The methods used to rank objects are based on mathematical modeling, expert assessment, decision making theory, and interval estimation. To some degree, they take into account the interests of organizations operating these facilities, state supervisory authorities, and insurance companies. At the same time, the ranking methods available today (for example, ranking objects by protection against emergencies in railway transport, ranking objects of hazardous gas distribution production systems, etc.) do not take into account the structural connectivity of the ranked objects and the importance of a particular object operation for related systems and subsystems .

Ranking SCS objects is a typical task for the theory of measurement of some complex synthetic properties of objects. Technically, the solution of the problem is reduced to the construction of a value (utility) function linking the measured property with simpler resource indicators (factors) measured in physical quantities. The value function is used both to solve the problems of choosing some best option from a variety of alternatives, and to solve more composite problems, such as the task of forming a portfolio of orders for work with limited resources (funding for creating or modifying objects). The factors through which the ranks are built are often measured not in quantitative but in qualitative scales, therefore, the use of expert assessment methods and expert technologies is required to build dependencies between utility and primary resource factors. Due to the development of computer technology, it is now possible to evaluate objects whose description factors are specified with an error, which requires the development of a specific apparatus for the statistical processing of primary data and the use of fuzzy logic tools. An essential feature of ranking problems is the adaptive nature of decision-making procedures for selecting optimal options, in which several cycles of experimental data and expert preferences coordination are required to construct the final formula for the ranking function.

In this context, risk assessment is the stage at which the negative effects associated with a particular production activity are determined. And first the dander sources should be identified. In order to do that, the boundaries of the investigated system should be determined. In other words, when assessing risk in a region or of a particular system, one should choose which sources to be considered. There are no strict rules here, and there cannot be. However, today there are a number of developed provisions that should be taken into account when studying safety issues. The most comprehensive provisions for determining the boundaries of the studied regional or large industrial systems can be found in various sources. International organizations note that there are normally different values of risk assessments in different countries even when assessing one particular technology. Therefore, to facilitate data collection and processing, a single set of terms and provisions should be adopted to describe energy and industrial systems and their main components [14].

2. Comments on risk categories

The basic moments in risk assessment are the detailed description of a hazard and the definition of harm related to it. There are various models of hazard sources that allow identifying a probability of this or that scenario of an accident's development and defining the amount of dangerous emissions into the environment. Depending on the type of a source, three types of risk are identified.

Usual risk is related to normal operations of an enterprise. The conditions of normal operations include accidents with low harm that occur rather often. This category of risk is characterized by an occurrence probability equal or close to entity. In most cases usual risk is integral part of production process itself or easily controlled. The sources of such a risk are described by the amount of emissions or dissipations into the environment caused by normal operations or some accident. Assessment of emission or dissipation level for functioning enterprises can be made on the basis of measurements or the results of operational experience of analogous enterprises.

The other two risk categories are related to industrial accidents during transportation or storage of hazardous substances. An accident is understood as an event with a low probability of occurrence (for example, less than one for the entire life of an enterprise), but with significant or even catastrophic consequences. When analyzing emergencies, possible scenarios for the development of an accident are usually considered. Then factors such as

Assume that a priori information about the probabilities of a particular situation Y_n is absent. The theory of statistical decisions offers several criteria for optimizing the choice. The choice of the criterion cannot be formalized, it is carried out by the decision maker subjectively, based on their experience, intuition, etc. Let us consider these criteria.

Laplace criterion. Since the probabilities of occurrence of some situation Y_n are unknown, all situations will be considered equally probable. Then, for each row of the gains matrix, the arithmetic mean value of the estimates is calculated. The optimal solution is the solution with the maximum value of this arithmetic mean, i.e.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\frac{1}{N}\sum_{n=1}^{N} A_{mn}\right).$$

Wald criterion. In each row of the matrix, the minimum estimate is selected. The optimal solution is the solution with the maximum of this minimum, i.e.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\min_{1 \le n \le N}\left(A_{mn}\right)\right).$$

This criterion is very cautious. It focuses on the worst conditions, among which the best and now guaranteed result is only found.

Savage criterion. In each column of the matrix the maximum estimate $\overline{A}_n = \max_{1 \le m \le M}\left(A_m\right)$ is found, and a new matrix is compiled, the elements of which are determined by the relation $R_{mn} = \overline{A}_n - A_{mn}$. This is the amount of regret that the optimal choice X_m was not made in the strategy Y_n.

The value R_{mn} is called the risk, meaning the difference between the maximum gain, that would take place if it were reliably known that the most favorable for the decision-maker situation $\overline{Y}_n$ would occur, and the real gain when choosing X_m under condition Y_n.

This new matrix is called the risk matrix. Then a solution with the risk that has the lowest value in the most unfavorable situation, i.e. $\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\max_{1 \le n \le N}\left(R_{mn}\right)\right)$, is chosen from the risk matrix.

The point of this criterion is to minimize risk. Like the Wald criterion, the Savage criterion is very cautious. They differ in their understanding of the worst situation: in the first case, it is the minimum gain, in the second, the maximum loss of the gain compared to what could have been achieved under the given conditions.

Hurwitz criterion. A certain coefficient α is introduced, named the "optimism coefficient",. In each row of the gains matrix the largest estimate $\max_{1 \le n \le N}\left(A_{mn}\right)$ and the smallest estimate $\min_{1 \le n \le N}\left(A_{mn}\right)$ are found.

They are multiplied by α and $(1-\alpha)$, respectively, and then their sum is calculated. The optimal solution is the solution with the maximum of this amount, i.e.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\alpha \times \max_{1 \le n \le N}\left(A_{mn}\right) + (1-\alpha) \times \min_{1 \le n \le N}\left(A_{mn}\right)\right).$$

For (α=0) the Hurwitz criterion is transformed into the Wald criterion. This is a case of extreme "pessimism". For (α=1) (a case of extreme "optimism"), the decision maker expects the most favorable situation. The "optimism coefficient" α is assigned subjectively based on experience, intuition, etc. The more dangerous the situation, the more cautious the approach to choosing a solution should be and the lesser value is assigned to the coefficient α.

It is important to note that this criterion is not relevant to risk analysis, only to the subjective perception of "random" and "voluntary" risks.

Then how is the risk calculated?

It follows from the above that risk assessment is only possible if there are alternatives to choose. If there is only one single option, then the risk is automatically equal to zero and the spread of gains is just a characteristic of an uncontrolled natural environment. However, it should be noted that the alternative is always present in the form of a refusal to make a decision.

In some cases, with the refusal to make a decision an optimum for the columns may appear, then there will be non-zero risks in the options due to the choice of a wrong decision. For example, it is more profitable not to play in a casino than to play, aligning to some strategy. On the contrary, in chess it makes sense to play even in the case of a single (forced) move. For example, when the opponent declares a "check", there is no way to interpose, and retreat is only possible on a single square, then the risk is also equal to zero, since refusing to play means automatic defeat.

Probability estimates $\sum_{n=1} p_n = 1$ describing the state of the environment $p_1 = p\left(Y_1\right)$, $p_2 = p\left(Y_2\right)$, …, $p_N = p(Y_N)$ allow preventing choosing the most unfavorable case when using the Savage criterion, and the desired solution takes the form:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{N} p_n \times \left(\max_{1 \le n \le N}\left(A_{mn}\right) - A_{mn}\right)\right),$$

which is a more correct formula.

For the case when the gain is determined only by the loss amount A_{mn}=B–C_{mn} for any pair (X_m, Y_n):

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

For the case when the loss level at the optimal option for the conditions Y_1, Y_2, …, Y_N does not depend on n and is equal to $\overline{C}$:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B - \overline{C} + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

Over the past three decades, a significant number of works have been devoted to these issues, which convincingly confirmed the already axiomatic notion that achieving absolute safety is impossible.

The risk philosophy based on the concept of absolute safety inevitably came to the concept of acceptable risk. The concept of acceptable risk required the abandonment of the ALAPA principle and the adoption of a new ALARA principle (As Low As Reasonably Achievable). According to ALARA, the required level of safety is determined based on the social and economic conditions of the society development. For accidents with a risk higher than acceptable, it is necessary to use engineering solutions to prevent and mitigate the consequences, and for accidents with a risk less than acceptable, only mitigating measures are needed. In the nuclear energy sector, for example, this principle is reflected in the relevant safety provisions. For SCS, the concept of acceptable (maximum allowable) risk is introduced meaning the level of risk which is acceptable and justified on the basis of economic and social considerations. To this date there are still no full-fledged methods for determining the acceptable risk for hazardous industrial facilities of the SCS. It can be said that at present, the safety problems are resolved by deciding by what means and to what level the risk should be reduced to reach the optimal safety level of both humans and the environment, based on certain criteria.

Risk analysis is the only way to investigate those safety issues that cannot be answered by statistics, such as low probability accidents with severe potential consequences. Naturally, risk analysis is not a solution to all safety tasks, but it is the only way to compare risks from various sources of danger, identify the most significant of them, choose the most effective and cost-effective systems to increase safety, develop measures to mitigate consequences, etc.

In foreign literature, along with the concept of "risk analysis" (Risk Analysis), they use the PRA method (Probabilistic Risk Analysis) established by the NRC (Nuclear Regulatory Commission). There is no fundamental difference between them, although PRA is believed to be mainly aimed at analyzing low probability accidents. However, PRA is frequently used to analyze the events with a wide range of probability of occurrence. There is no such distinction in Russian literature.

Currently, the risk analysis procedure can be divided into two main components and several intermediate parts, each with its own problems and inherent methods and models: assessment and management. It is important to bear in mind that risk analysis issues cannot be considered separately from the game setting. Risk as a dynamic characteristic dependent on time, means and information is reduced to "two-dimensional estimates" of probability and damage.

It is forgotten that, first of all, there is a fundamental difference between stochastic factors leading to decision making under conditions of risk, and uncertain factors leading to decision making under conditions of uncertainty. Both lead to a scatter of possible outcomes of management results.

But stochastic factors are completely described by known stochastic information, which allows for deciding on the optimal solution. Nonetheless, basic formulas in risk analysis (RA) are distorted and simplified, their association with game theory is forgotten. There are several reasons for this. The word risk has become "trendy", as a result, specialists "seized on the term" without understanding where it comes from, what axioms are "behind" this term. As a result, for many years economists, insurers, ecologists, and others have been producing false scientific results based on false definitions they invented. Sometimes ("false" multiplied by "false" results in "true") acceptable results are obtained. But this usually only applies to static and stationary cases (where the "reliability" theory applies), but not to dynamic cases. For a number of applications, it was required that a formula was "simpler", so that it could be understood by developing countries that joined the IAEA, for example. As a result, the risk as a dynamic characteristic, depending on time, means and information, was reduced to two-dimensional snapshots in which only probabilities and damage are present. The case was given to the "civil defense forces" (now the Ministry of Emergency Situations), which did not have the corresponding scientific "potential" at the time and was acting as the "customer" of research work. The most influential Ministries (Ministry of Medium Machine-Building Industry, Ministry of General Machine-Building Industry) had their own general ideas of risk, which normally differed significantly from each other. The establishment of the opinion that risk analysis can be conducted through "statistics" of the observed phenomena was overwhelmingly influenced by Western scientists (Netherlands Organisation for Applied Scientific Research and others). The influence was so strong that the "strength theory" and "reliability theory" were left in the modern risk analysis. But research on the "survivability theory", "homeostasis theory", adaptive theories, including "decision making theory", "perspective activity theory", "reflections theory", and "the theory of self-organizing systems" were nipped in the bud.

For uncertain factors, such information is not available. In the general case, the uncertainty can be caused either by the counteractions of an intelligent opponent (a more complicated case is related to the opponent's reflections (terrorist threat)), or lack of knowledge of the conditions under which the decision is made.

Decision making with the insufficient knowledge of the conditions in which the choice is made is called "games with nature". In terms of "games with nature," the decision-making problem can be formulated as follows. Let the decision maker choose one of the M possible options: $X_1, X_2, \ldots, X_M$ and let N assumptions be made regarding the conditions under which the possible options will be implemented: $Y_1, Y_2, \ldots, Y_N$ The estimates of each solution in each condition (X_m, Y_n), where $m = 1 \ldots M$, $n = 1 \ldots N$, are known and given in the form of a gains matrix for the decision maker: $A=A(X_m, Y_n)=|A_{mn}|$.

functioning have been and still are quite high. As a result, there are tasks of choosing priority equipment facilities from their total population and the optimal distribution of financial and material resources available to the system owner (proprietor, state) for their protection. The notion of optimality regarding risk synthesis will be discussed later. First, it is necessary to deal with the notion of risk, its ontology. You can only measure what is clearly defined, although A. Einstein argued that "the world is not a quantitative concept, but a qualitative one".

People would get rid of half of their problems if they could agree on the meaning of words…

René Descartes

1. On the nature of risk and safety approaches

Risk is a notion arising at the boundary of dependability and safety. The technology itself and the production systems do not take risk. It is a man who always takes risk. Dependability is the ability of a technical object to function continuously and fail-safely with 100% level of efficiency. When analyzing dependability, the main criterion is the failure criterion, which divides everything into "yes" (operational state) and "no" (non-operational state). Dependability depends, so to speak, on the internal properties and characteristics of an object (quality, time to failure, technological features, operation requirements, etc.). Safety is the ability of the same object to perform its functions without causing damage to maintenance personnel, the environment, etc. Safety depends on the external properties (environment, threats, personnel qualification). Moreover, safety is both a sense and a state. The safety status is determined by the development of appropriate technologies and is evaluated using mathematical modeling methods; it is based on the analysis and assessment of risks and the effectiveness of various measures, means and mechanisms of protection. A sense of safety is a person's psychological reaction to threats and risks, and the psychological perception of the adequacy of protective measures; what is known as the level of acceptable risk (i.e. from what threats a person is ready not to defend themselves, what damages are acceptable to them). In the meaning that the sense of security can subjectively change, one can agree with the statement of Bruce Schneider, an American cryptographer, writer and computer security specialist: "Security is a process, not a product". But this does not mean that the safety process has no purpose. The purpose of safety is to achieve a state of safety of man and environment that corresponds to their subjective sense of danger (i.e. an acceptable level of risk). To achieve this goal, the so-called "risk-oriented approach" is used.

Risk occurs as a hazard assessment for a person performing work using technical devices. Since there are latent defects and uncertainties in the place and time of failure and hazard occurrence both in dependability and safety assessment, risk is often interpreted as the effect of uncertainties on the achievement of the goals set by a human operator. Specifics occur when a specific mechanism (an object, an industrial enterprise, a corporation, etc.) used by man person uses to realize the goals of an activity in a certain environment (which, in turn, is characterized by the presence of threats, environmental features, and the presence of competitors with their own goals, etc.) is considered.

In living systems, for example, instability is used practically: it is one of the most important driving forces of evolution. One can say that the high adaptability of living organisms is a consequence of their instability. A well-known advocate of "controlled instability" Nassim Taleb also repeatedly emphasized that multilevel redundancy is the main property of natural (living) systems that controls risk [13]. Just like in living systems, unstable processes in safety systems are key to their adaptability to changing threats and dangers.

With some reserve, risk can be considered as the best measure to quantify a hazard. This concept is widely used in modern literature and often implies completely different meanings. In the most general case, risk is characterized by the probability of a negative effect, the probability that a negative effect of a particular type occurs, and the probability that this type of effect causes a certain amount of deviation of the state of an effected subject from its dynamic balance. In other words, risk is a vector variable that can describe different types of hazards with all its values given above being its constituent parts. Since the main issues discussed below are one way or another related to ensuring the safety of industrial facilities, the term "risk" shall mean the risk of anthropogenic or, more specifically, industrial origin, unless otherwise specified.

The first approximation in issues related to ensuring safety is very often the requirement to achieve a negligibly small or "zero" risk associated with some (generally) production activities. Therefore, the safety systems that were created and used in industries were often engineering solutions aimed at fulfilling the requirements of absolute safety. The basic principle in creating these systems is the so-called ALAPA principle (As Low As Practicably Achievable). According to this principle, the industrial safety should be increased by any means and regardless of the level achieved, if it is technically feasible. In other words, according to ALAPA, one should construct technical safety measures that would prevent emergency situations, i.e. eliminate the very possibility of the occurrence and development of an accident. The complication of technologies has led to the fact that it is often simply impossible to predict all scenarios of an accident development and, therefore, to provide engineering and organizational solutions to prevent them, that being once again shown by the accidents in Chernobyl and Fukushima. All that required a fundamentally new approach to solving safety problems.

…Most scientists strive to learn the structure, composition and content of their subject, decomposing it into parts. They try to understand how parts make up a whole. Sometimes it resembles the desire to take a watch apart to understand what the time is.

Aksyonov G.P. [1]

Introduction

Risk analysis and risk assessment are the focus of many researches, whose number has been growing rapidly lately. Figure 1 shows the increase in the frequency of the word "risk" occurrence (per million words per year) in English-language publications from the moment it was first mentioned in 1661 till present.

Figure 1. Frequency of occurrence of the word "risk" [2]

This is partly due to the general "trend" for research in this area, but partly it is a response to the challenges of the time when a large number of mutually overlapping and partially integrated systems of different purposes made by man significantly has shaken the general sustainability of social development and has given rise to dangers and threats that are hard to predict. A whole new direction in systems engineering has even appeared that deals with the engineering of systems, whose individual parts can exist independently, were developed independently, and thus are a complete target system. Risk is often a conscious threat, and therefore being the focus of researchers' increased interest. However, their efforts are often very clearly illustrated by the words of G.P. Aksyonov, biographer of V.I. Vernadsky, cited in the epigraph.

In this regard, it is especially relevant to introduce (update) the very concepts of "analysis" and "synthesis" as applied to risks. Analysis and synthesis are not two different ways of cognition, but are opposites of one cognizing consciousness, separable only in abstraction. For example, A. Kazennov [3] shows that the basis of this unity is their origin from practical analysis and from research in general. "... the generic word for analysis," he writes, "is not "decomposition" (including mental decomposition) of a subject, but "research". And a specific difference of a definition is "distinguishing parts of the whole and their relationship to each other through this whole." Not decomposition, but distinction... It is only necessary to find the point of identity of the "part" and the whole, one part and the other "parts".

At the same time, the identification of different parts with each other unites objects (in this case, parts) into a whole. And that is already synthesis. While analysis should be defined as follows: analysis is a study that distinguishes parts of an object and correlates them with the whole and with each other through this whole. The whole in the analysis is the initial thing, mediating the whole course of research. In general parts are already distinguished before this study by previous practical and theoretical studies: analytical and synthetic cognition... synthesis is a study that considers the ratio of different parts of an object and their whole through the essence (essential part) of the whole. Finding such an essence or an essential part is a fundamental scientific discovery that sheds new light on all previous concepts expressing the essence of an object. It reorganizes the whole system of concepts and, accordingly, the whole theory".

This approach seems to be the most constructive for risk assessment. This is especially important when studying a system of systems and the so-called critical infrastructure problem related to that and often discussed in recent years [4-9]. The problem is that almost in all of the most important economy's sectors there are systems with such spatially distributed elements (sometimes these systems are also classified as geographically distributed) that it is practically impossible in practical terms to fully protect all objects of one particular sector, not to mention all the sectors of a system. The main issues and problems of a decision maker (DM) in the field of ensuring the safe functioning of such systems are the issues related to assessing threats and risks that are significant for the system as a whole and for its elements and prioritizing the protection of critical infrastructure elements and objects, taking into account usually limited resources at his disposal.

Besides large sizes, many sectors are so complex that it is technologically and economically impossible to predict and calculate all the consequences of any incident, regardless of whether the incident is caused by the malicious actions of people or is the result of natural disasters. Generally, it is extremely difficult to predict the consequences of small disturbances in one part of the critical infrastructure for its other sections. For example, all Internet communications in South Africa were completely terminated due to the fall of the twin towers as a result of the terrorist attack on the United States on September 11, 2001. And the relatively minor malfunctions in First Energy's electric payload in Ohio (USA) accelerated blackout in August 2003, affecting 50 million people thousands of kilometers away from the source of the problem [10-12].

In fact, the existing infrastructure is vulnerable simply because it contains so many very closely interconnected components that for most technical consultants, analysts and decision makers who determine its safety policy, this becomes an impossible task.

The notion of structural complexity, as well as the notion of a system in general, has not yet been unambiguously defined. At the same time, modern requirements for the construction of safety systems and the effectiveness of their

Original article
https://doi.org/10.21683/1729-2646-2019-19-4-53-64

On the nature of risk in the safety management of structurally complex systems

Alexander V. Bochkov, *Gazprom Gaznadzor Ltd, Russian Federation, Moscow*

Alexander V. Bochkov

Abstract. Aim. *In the general case, a risk-oriented approach encompasses probabilistic methods of emergency processes and events simulation as well as deterministic methods. The use of probabilistic and deterministic estimations has been the focus of research aiming to improve safety and operational procedures. However, the experience of using probabilistic analysis only (essentially, one-criterium tool) has shown that this approach does not encompass all the required aspects of safety. The aim of the paper is to introduce (update) the definitions of the very concepts of "analysis" and "synthesis" as regards the risks for the purpose of research of safety of structurally complex systems (SCS) and design of systems for monitoring hazards and threats to their stable development thereof.* **Method.** *The paper examines – from the point of view of systems science – the method of analysis and synthesis of risks as a development tool of advanced systems for monitoring SCS safety threats. The paper compares the primary current concepts of risk management in SCS and has shown that they should be developed and improved. A type of risk functionality is proposed that allows defining a safety solution by the value of mathematical expectation of losses, with appropriate corrections taken into account.* **Result.** *The concept of "risks synthesis" is introduced as a scientific tool integrated with analysis that takes into consideration the existing connections between the elements of considered SCS in terms of a whole system in its entirety. Principles are formulated for the collection of comprehensive sets of data required for decision-making.* **Conclusion.** *The proposed approach paves the way for the development of the method of risks synthesis and suggests the development of advanced expert systems to support decision-making regarding the safety of SCS as multifunctional and multilevel systems intended for both recording and analysis of each individual case (event), and prediction of trends and preparation of prevention measures as necessary.*

Keywords: *structurally complex system, critical infrastructure facilities, risk, synthesis, analysis, safety, management.*

For citation: *Bochkov AV. On the nature of risk in the safety management of structurally complex systems. Dependability 2019; 4: 53-64. https://doi.org/10.21683/1729-2646-2019-19-4-53-64*

Received on 26.08.2019 / Revised on 23.10.2019 / For printing 14.12.2019

About the author

Alexey M. Zamyshliaev, Doctor of Engineering, Deputy Director General, JSC NIIAS, Moscow, Russian Federation, phone: +7 495 967 77 02, e-mail: A.Zamyshlaev@vniias.ru.

The author's contribution

Zamyshliaev AM has analyzed the stages of automation of the traffic safety management system, established that currently traffic safety management involves processing massive amounts of scattered raw data and suggested developing a four-level (elements, systems, processes, services) digital intelligent safety management system, including safety, dependability, assets and process management.

JSC RZD of an integrated intelligent process and service management system that enables real-time traffic safety management. The digital transformation of the traffic safety management system in JSC RZD consists in the top-level integration with the operating processes of all business units in terms of integral assessment of the risk of possible events and achievement of specified indicators. The developed solutions will be deployed using the Big Data and artificial intelligence, IoT-based diagnostics systems, digitization of rolling stock and infrastructure assets manufacture and maintenance, etc. The result will be the integration of the traffic safety management system with the process of all levels of JSC RZD's management in accordance with the three principles of digital business: *Complete coordination*, *Online business* and *Service management*. In the case of the Traffic Safety functional area, that means the analysis of real-time data on the status of the network and rolling stock, online supervision of valuable or dangerous freight by means of collection of sensor data, analysis of data flow regarding the current status of rolling stock and locomotives with assessment of operation, risks, generation or real-time warnings and recommendations for further use and maintenance with minimal risks.

An extensive development and deployment within the company of the URRAN Single Corporate Platform enabled executive decision support as regards risk-based functional dependability and safety of transportation facilities. Thus, the SCP URRAN E (subsystem E responsible for the electrification and power supply) developed and deployed in 2018 enabled comprehensive operations involving over 1 000 users. Over 4.3 mil score cards have so far been filed per Transenergo facilities. Earlier this year, SCP URRAN S was developed and put into revenue operation. It enables real-time calculation of key indicators of dependability and safety, as well as risk assessment within the telecommunications facilities. The functional development of SCP URRAN P in the track service since 2019 allowed improving the reliability of assessment of the activities of the service's business units and objectivity of assignment of standardized dependability indicators. The development and deployment of SCP URRAN Sh in the signalling service and SCP URRAN T in the locomotive service will – as early as 2019 – enable higher efficiency of maintenance through resource and risk management.

Thus, SCP URRAN sets the stage for the digital transformation of the traffic safety management system in the Russian Railways.

References

[1] Rozenberg IN, Avetikian MA, Zamyshlyaev AM**.** Avtomatizirovannaya informatsionnaya sistema revizora dvizheniya [Traffic supervisor's automated information management system]. Zheleznodorozhny transport 2004;7:46-48 [in Russian].

[2] Zamyshliaev AM. Prikladnye informatsionnye sistemy upravleniya nadezhnostyu, bezopasnostyu, riskami i resursami na zheleznodorozhnom transporte [Applied information systems for management of dependability, safety, risks and resources in railway transportation]. Moscow: Nadiozhnost; 2013 [in Russian].

[3] Rozenberg EN, Rozenberg IN, Zamyshliaev AM et al. Sistema KASANT: zadachi, vozmozhnosti, perspektivy razvitiya [KASANT system: tasks, capabilities, prospects of development]. Zheleznodorozhny transport 2008;9:6-9 [in Russian].

[4] Zamyshliaev AM, Proshin GB, Gorelik AA. Sistema KASANT: vtoroy etap vnedreniya [KASANT system: the second stage of deployment]. Avtomatika, sviaz, informatika 2009;7:9-13 [in Russian].

[5] Gapanovich VA, Shubinsky IB, Zamyshlyaev AM. Mathematical and information support of the URRAN system. Dependability 2012;3:12-19.

[6] Gapanovich VA, Shubinsky IB, Zamyshliaev AM. Risk assessment of a system with diverse elements. Dependability 2016;16(2):49-53.

[7] Rizzatti R. Digital Data Storage is Undergoing Mind-Boggling Growth. <https://www.eetimes.com/author.asp?section_id=36&doc_id=1330462>, [accessed 31.10.2018].

[8] Makevnin B, Stoliarov A. Tsifrovaya neft. Bolshie dannye kak odin iz klyuchevykh instrumentov tsifrovoy transformatsii [Digital oil. Big data as one of the key tools of digital transformation]. Sibirskaya neft 2017;9(146):10-15.

[9] Thaduri A, Galar D, Kumar U. Railway assets: A potential domain for big data analytics. Lulea (Sweden): Lulea University of Technology. Procedia Computer Science 2015;53:457-467.

[10] Gapanovich VA, Shubinsky IB, Zamyshliaev AM. Postroenie i ispolzovanie matrits riskov v sisteme upravleniya riskami na zheleznodorozhnom transporte [Design and application of risk matrices as part of risk management systems in railway transportation]. Dependability 2011;4:56-68 [in Russian].

[11] Zamyshlyaev A, Shubinsky I. Adaptive Management System of Dependability and Safety of Railway Infrastructure. Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO). Be'er-Sheva (Israel): IEEE Xplore Digital Library; 2016. p. 244-250.

[12] Shubinsky I, Zamyshlyaev A. Risk management system on the Railway Transport. Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO). Be'er-Sheva (Israel): IEEE Xplore Digital Library; 2016. p. 481-486.

[13] Shubinsky IB, Zamyshlyaev AM. Osnovnye nauchnye i prakticheskie rezultaty razrabotki sistemy URRAN [Primary scientific findings and practical effects of the URRAN system development]. Dependability 2012;3:3-12 [in Russian].

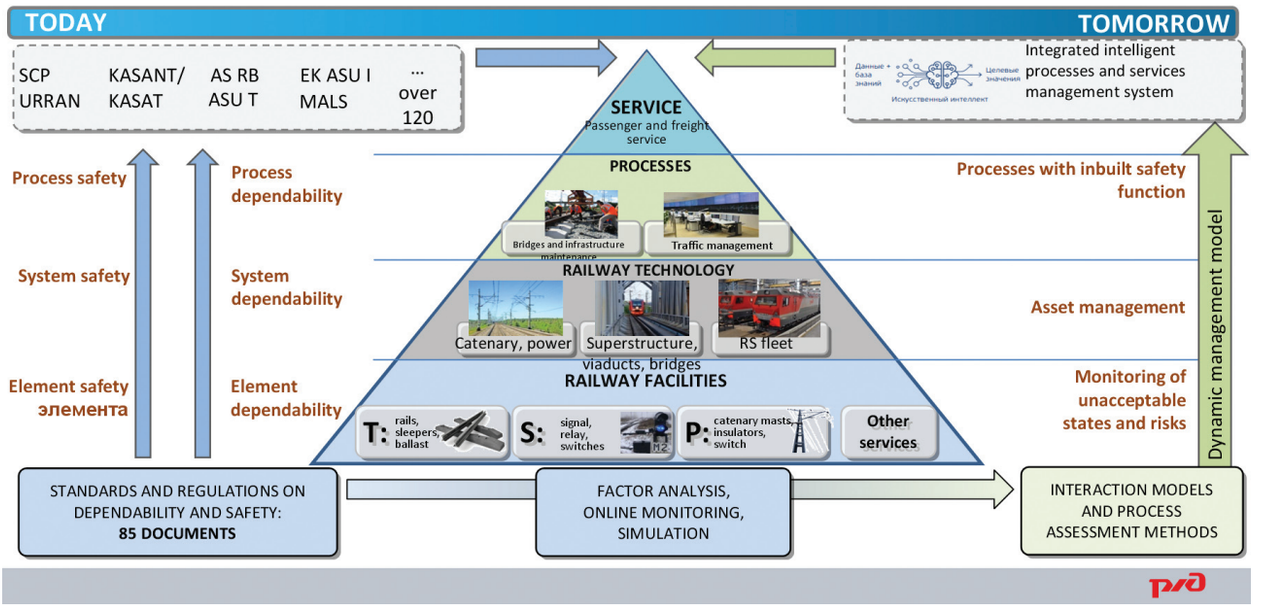


Figure 3. Migration towards a digital intelligent safety management system

Figure 2 shows the six-level hierarchical structure of various factors' contribution to such indicator as average daily performance of a locomotive. At the first level such factors as the locomotive's average daily run, average trainload are taken into consideration. At the second level the service speed, locomotive turnaround in station, etc. are taken into consideration. At the sixth level the locomotive type, its technical state, etc. are taken into consideration. In total, the effects of over 50 factors affecting the average daily performance of a locomotive are taken into consideration. Calculations require statistical data for each factor. Then, using statistical methods of factor analysis and link analysis combined with such other methods of Data Mining as methods of simulation and prediction, the average daily performance of a locomotive can be planned proactively.

Multifactor risk analysis using Big Data analytics and machine learning will enable dynamic risk assessment in railway services, identification of abnormal values in real time and prediction of the probability of hazardous events.

Migration toward the digital traffic safety management system

Currently, given the ongoing deployment of SCP URRAN and associated systems (KASANT, AS RB, KASAT, KASKOR, EK ASU I, ASU T, etc.), traffic safety management consists in current estimation and prediction of the safety and dependability of elements and devices of railway technology (individually for each service), systems separately (e.g. locomotive fleet, catenary, bridges, etc.), then processes (traffic management, service and repair, etc.). Those operations are aggregated at the level of devices, systems, processes and classified by service. The safety of passenger and freight services is based upon the decisions of auditors made according to post-audit statistical and real-time information supplied by automated systems (Figure 3). Such decisions largely depend on the human factor, as the received data mostly are not interrelated neither horizontally service-to-service, not vertically per elements, systems and processes. Due to that there is no comprehensive image of the current status of safety and dependability of infrastructure and rolling stock.

The migration towards a digital traffic safety management system must be based on models of interaction of safety and dependability factors of all railway facilities at all railway levels of hierarchy, as well as in association with other factors that are not directly associated with dependability, yet affect the safety of the transportation process. Such factors include, for instance, line class, service speed, trainload, scheduled and unscheduled track maintenance possessions, condition of ballast, condition of bridges and many more. The large number of factors and exceptional diversity of connections can be formalized and saved with the help of Big Data technology. That will enable real-time comprehensive monitoring of unacceptable states and risks. The monitoring procedure should be based on the methods of management of technical, social and industrial risks of transportation facilities developed as part of the URRAN system [12, 13]. That will allow using comprehensive risk assessment while managing the technical assets of JSC RZD and designing business processes that incorporate the safety function.

Conclusion

The primary benefit of migration towards Big Data consists in the development of a dynamic model of traffic safety, elimination of the human factor in control systems. Most importantly, it enables the creation within

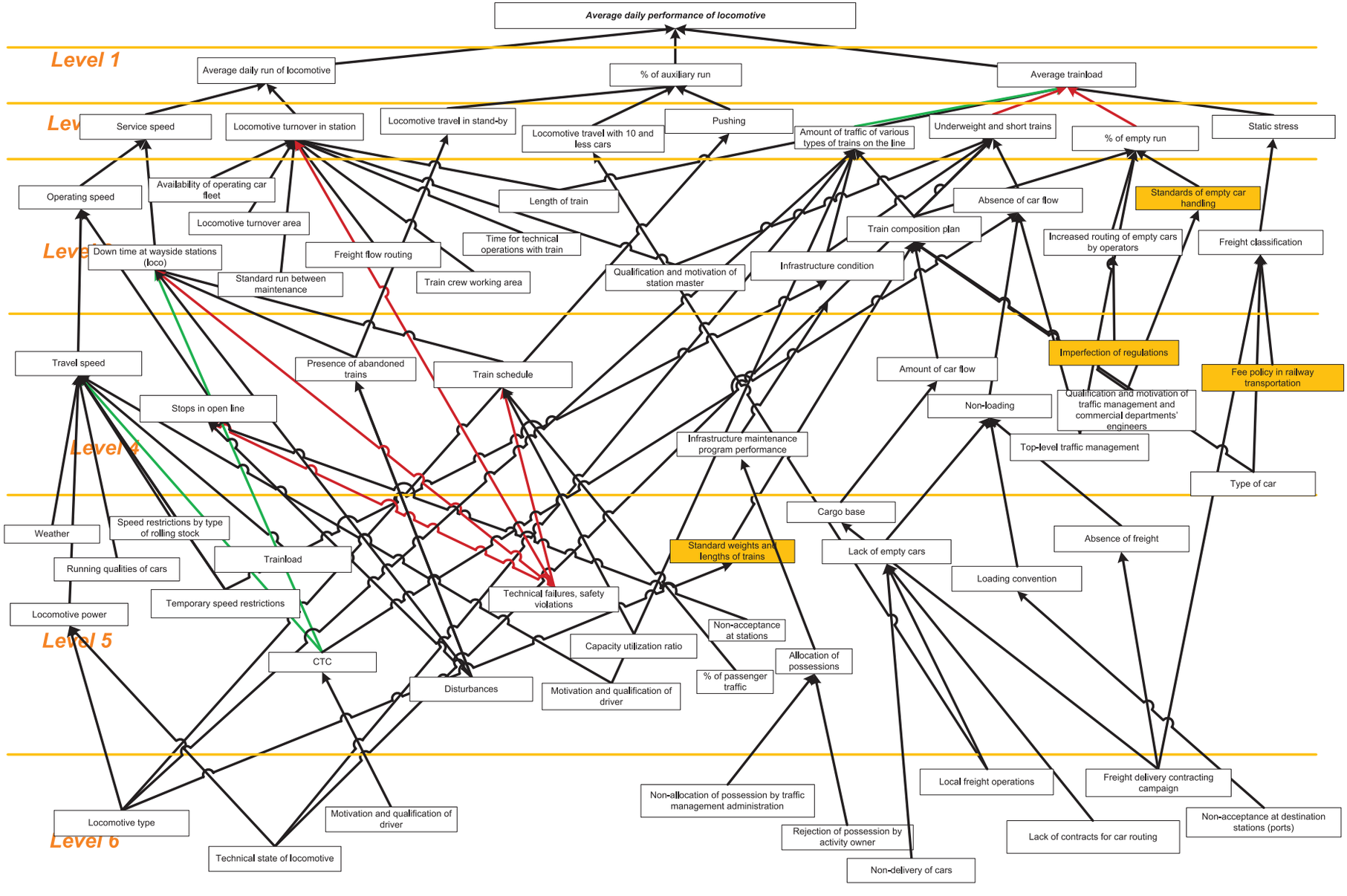


Figure 2. Hierarchical structure of factors' effect on the average daily performance of a locomotive

Big Data. This technology of storage and processing of Big Data is an alternative to the conventional database management technology. The defining characteristics of Big Data are the "three Vs": volume in terms of the physical volume, velocity in terms of the speed of growth, and the requirement for high-speed processing and acquisition of results), variety in terms of the capability to simultaneously process various types of structured and semistructured data). Subsequently, some variants and interpretations of the above characteristics came into being.

Not all collected data are useful, that is why today we discuss intelligent approaches to data analysis commonly known as **Data Mining**, a collective name that denotes a set of methods of discovering within data previously unknown, non-trivial, useful and practical interpretations of knowledge required for decision-making in various human activities. Data Mining is based on various methods of classification, simulation and prediction that use decision trees, artificial neural networks, genetic algorithms, evolutionary programming, associative memory, fuzzy logic. According to some experts, methods of Data Mining include the statistical methods (descriptive analysis, correlation and regression analysis, factor analysis, variance analysis, component analysis, discriminatory analysis, time series analysis, survival analysis, link analysis).

Data, whether collected, newly obtained or historical, are at the foundation of the migration towards the digital model of process management in railway transportation. Within JSC RZD, such foundation has been created. The aim of the activities associated with the creation of a top-level digital corporate management platform in JSC RZD consists in the development and deployment of the comprehensive automation model based on control systems integrated within the URRAN Single Corporate Platform (SCP URRAN). That is a set of regulatory and guidance documents, hardware and software systems intended for managing infrastructure facilities, rolling stock and manufacturing processes aimed at assuring guaranteed safety and dependability of the transportation processes performed by JSC RZD [5]. The system is already in use in the track, communications and power supply services and enables automatic assessment of the risks associated with both technical facility failures and traffic safety violations [6]. The analysis of the information it is collecting gives reason to believe that the system, along with the associated solutions, such as KASANT, AS RB, KASAT, KASKOR, EK ASU I, etc., can be designed on the basis of Big Data technology. Data structuring is one of the biggest problems. Large amounts of unstructured information are a typical feature of today's multifunctional AMS. According to international information systems auditors [7], up to 90% of the information we obtain is unstructured. Therefore, the migration towards Big Data must be executed using the foundations of **Data Science**. Up to 80% of time of data mining model generation is spent processing primary data, developing research models, analyzing basic statistics, developing regular calculation models. That requires managers who set goals of strategic analysis, engineers who understand business processes, scientists who develop mathematical models. And only after the data mining model is complete (including connections among all systems, users, factors), Big Data technologies and software solutions set in.

Due to the obvious costs associated with the creation of a digital traffic safety and reliability management system the question arises, whether such efforts are justified. The experience with the creation of similar systems for various industries demonstrates the productivity of such activities. Thus, Gazprom's Cognitive Geologist project [8] enabled the reduction of project development time from 2 years to 2 months. The project also showed that 30% of previously used initial data did not prove to be later useful. In Sweden, Big Data technology is used for managing trackside assets, in particular as part of decision-making regarding infrastructure and rolling stock [9].

Multifactor risk analysis of traffic safety

Big Data management is based on the understanding of business processes. In the context of railway transportation that involves understanding the processes of ensuring safety and reliability of the transportation process. Currently, JSC RZD employs 85 guidelines and regulations in the area of traffic safety and reliability. AMS are used in safety and dependability assessment of elements, railway systems and processes. That is the present. In the future, it is expected that advanced technologies of simulation, risk prediction will allow monitoring unacceptable states, manage assets using the ALARP principle [10, 11], integrating the safety function into business processes. The first step towards such future would be the development of a structure diagram of traffic safety risk management. Such diagram must include *methods of traffic safety risk assessment* (subject to the chosen measures of reduction of the effects of risk factors and prevention scenarios), *methods of factor analysis* (interrelations between factors and risks), *registers of the sources of information* on factor statuses, *registers of factors* that affect risks, service-specific *registers of risks*, *register of corporate risks* of JSC RZD and their classification attributes.

Certainly, the advantage of today's advanced computer-based methods over the conventional ones consists in the capability to handle multivariate data, i.e. consider an object subject to all possible attributes and factors. The methods allow establishing interrelations between indicators in a multidimensional space, which is extremely difficult due to time constraints. Computer-based (normally, intelligent) methods practically eliminate the possibility of calculation errors.

The above systems to some extent automate the process of traffic safety management. They enable condition analysis of individual railway facilities. However, in terms of assessment of processes, the data is not structured. Additionally, the systems have proprietary classifiers, they have different information acquisition periods, most importantly, the data they operate have different levels of detail and formats. There is also quite an important fact that safety management systems must be coordinated with many other automated systems of the transportation industry, including 33 recording systems and 8 planning systems. That indicates that the process of traffic safety management involves processing enormous amounts of raw data. The classical solution is data aggregation (for instance, per hazardous events, indicators of failure rate, damage, etc.), as well as analysis of the properties of the managed system. That, to some extent, enables proactive planning: identification of the direct causes of undesired events and planning targeted measures, confirming the achievement of target values. However, in safety management of railway transportation there are over **250 data names** alone, while the sizes of data arrays are evaluated at **millions of terabytes**. In this context, even aggregated data does not provide the desired effect. A digital traffic safety management system must be created.

Development of systems for collection and processing of information on the actual state of infrastructure and rolling stock

Various areas of human activity share the same trends of collection and processing of information. In the XIX centuryб our predecessors obtained management-specific information by means of personal observations, manual measurements, stored it in script books. In the era of steam engines, executive decisions were made on the basis of several megabytes of information (Figure 1).

In the XX century, new computer systems, information systems and automated workstations emerged. Field inspections were complemented with automatic systems for data collection that were based on sensors, relays. The amount of processed information was gigabytes. It was collected, stored, analyzed and used for purposes of forecasting. The beginning of XXI century was marked by explosive technological developments. Now we are talking about exabytes (10^9 gigabytes) of information. The capability of collecting and controlling such enormous amounts of data enables the application of modern technology. Currently available speeds are far beyond human response time. Naturally, the role of people in the operation of systems intended for collection of such amounts of data is progressively declining. An ever-increasing amount of information on the real world is collected with the use of sensors, diagnostic systems, technologies that enable interaction of artificial objects with no human involvement.

A large amount of collected and, most importantly, constantly increasing information inevitably changes our perception of it. Ensuring the safety and reliability of transportation processes relies on the prediction of risks, automation of the decision-making process. In other words, we are talking about tasks that used to be the prerogative of people. Now, most of such tasks are assigned to computer-based systems.

Structured and unstructured data in great amounts and considerably diverse, that are efficiently processed with the use of software tools, are conventionally known as

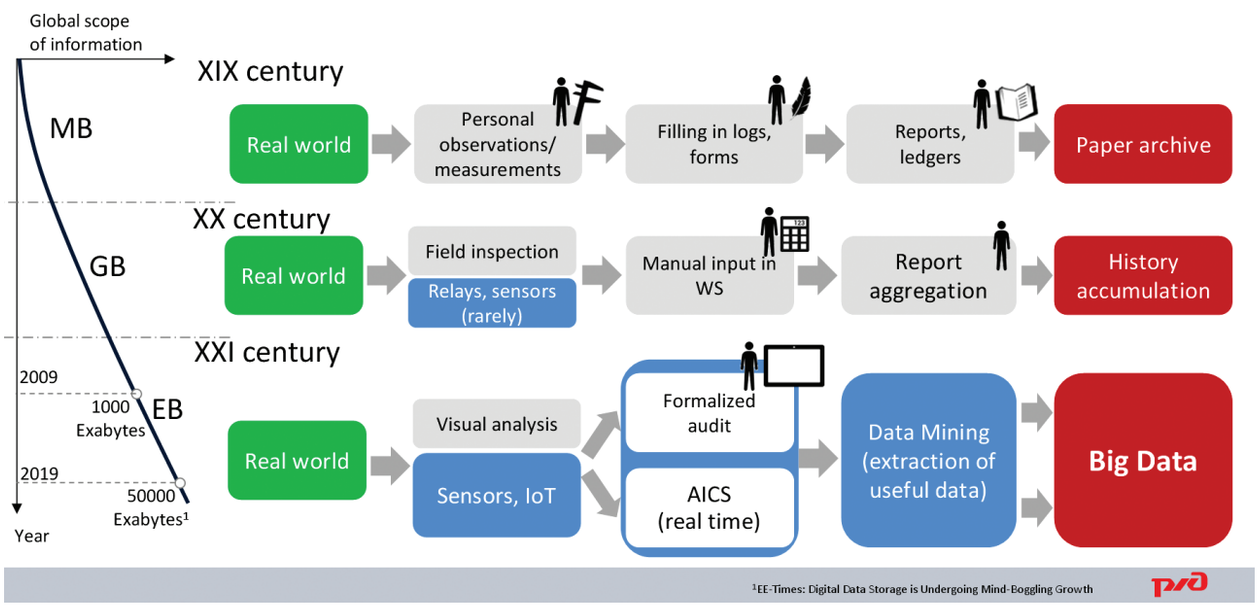


Figure 1. Stages of development of data collection and processing systems

Introduction

Train traffic safety is one of the key concerns of JSC RZD in the context of operation of the railway system, passenger and freight traffic. All the organizational and technical measures in railway transportation must comply with the requirements of safety and faultless train traffic**.** The development of Russia's railways is aimed at increasing the rate, speed and freight capacity of train traffic. That involves a higher number of vehicles simultaneously operating on railway tracks, as well as significantly more complex infrastructure. Due to that, stricter requirements must be specified for the quality and dependability of traffic safety facilities, as well as the professional qualifications and experience of railway personnel directly involved in traffic management.

JSC RZD's traffic safety policy defines the following main goals: minimization of the consequences of transportation incidents; protection of human life and health; assurance of safety of cargo, rolling stock, infrastructure facilities; assurance of a set level of traffic safety. The wide range of traffic safety tasks, on the one hand, and rapid development Russia's railways, rolling stock and infrastructure, on the other hand, require a major rearrangement of the existing traffic safety management system through its transformation into a digital management platform.

Stages of automation of a traffic safety management system

Today, JSC RZD uses a significant number of automated management systems (AMS) developed in various periods for the purpose of solving specific tasks. Some of them are modern, some require upgrading and updating in accordance with new requirements.

At the early stages, traffic safety management was based on railway stations and depots inspection reports. The development of railway transportation required the automation of traffic safety management. In 2005, the Automated System for Supervision and Analysis of Application of Traffic and Workplace Safety Rules by Station Personnel (AIS DNCh) [1] was created. The system's main purpose consists in organizing – within the train service – of collection and classification of information on the results of inspections of railway stations as regards traffic and work safety, its analysis and definition of preventive measures aimed at eliminating faults in the train and shunting operations, as well as cases of workplace injury in stations. The system's users include safety supervisors of all divisions, management of the commercial service, safety office employees. The system has 800 active users, over **700 000 inspection reports** have been prepared so far. They formed the basis of the corporate non-structured safety data storage using the example of a specific service.

In 2006, the Automated Traffic Safety Management System (AS RB) was created [2]. Today, it performs all the required functions that ensure data input, warning, classification and recording of traffic safety violations, supervision of the observance of the terms or registration, timeliness and quality of investigation of traffic safety violations, analysis of the causes and consequences of violations, generation of network-level and division-level violation reporting documentation. The system has over **5000 users**. It has so far generated **over 40 000 technical inspection reports** by safety inspectors.

The Integrated Automated Systems for Recording, Supervision of Elimination of Failures of Technical Facilities and Dependability Analysis (KASANT) was deployed within JSC RZD in 2007 [2, 3, 4]. The system is a radically new tool for the Company's infrastructure facility and rolling stock condition monitoring. It guarantees a single procedure of registration and investigation of technical facility failures in all operational services, in all divisions of JSC RZD, significantly increases the reliability and speed of data collection through a "paperless" process. Over the last three years, KASANT enabled a staged migration towards a single system for registration and analysis of technical facility failures. It became possible to implement comprehensive method of estimation of operational efficiency, both for specific services, and for the whole company, using a single network-wide database of technical facility failures.

At different moments in time, KASANT was integrated with the Company's following automated systems: GID Ural-VNIIZhT (System for Automated Train Traffic Scheduling), ASU E (Transenergo Automated Management System), AS KMO (Automated System for Documentation of Monthly Commission Inspections of Stations), ASK PS (Automated System for Rolling Stock Technical State Supervision), ASUVOP (Standard Automated System for Issue and Cancellation of Warnings), ASU-P (Automated Systems for Track Facilities Management), ASU-Sh-2 (Integrated Automated System for Signalling, Interlocking and Block Infrastructure Management). Later, the above were integrated with the Single Corporate Automated Infrastructure Management System (EK ASUI) that encompassed the AMSs of the infrastructure services and now provides information support of maintenance and repair process.

KASANT has over **50 000 users**. The daily number of registered warnings is **1400**. **2 367 747 technical facility failures** have so far been detected and analyzed**.**

In 2011, KASAT, or the Integrated Automated System for Recording and Analysis of Process Violations, was developed and deployed for the purpose of analyzing cases of process violations by railway personnel causing traffic safety disturbances. It is a hardware and software system for recording, analysis of cases of process violations in infrastructure facilities of JSC RZD. KASAT has over 50 000 users. The daily number of registered warnings is 960. So far 6 497 274 process violations have been detected and analyzed.

Original article
https://doi.org/10.21683/1729-2646-2019-19-4-45-52

Premises of the creation of a digital traffic safety management system

Alexey M. Zamyshliaev, *JSC NIIAS, Russian Federation, Moscow*

Alexey M. Zamyshliaev

Abstract. Aim. *The digital transformation of the traffic safety management system in JSC RZD involves top-level integration with the operating processes of all business units in terms of integral assessment of the risk of possible events and achievement of specified indicators. The result will be the merger of the traffic safety management system with the processes of all levels of the company's management enabled by an integrated intelligent system for managing processes and services whose functionality includes real-time traffic safety management.* **Methods.** *The paper uses system analysis of existing approaches and methods of processing of large quantities of structured and unstructered data.* **Results.** *The paper examines the development stages of train traffic safety management, as well as automated information and control systems that enable traffic safety management. General trends in the creation of systems for collection and processing of information are analyzed. The applicability of such technologies as Big Data, Data Mining, Data Science as part of advanced control systems is shown. The paper examines the performance of the above technologies by analyzing the effect of various factors on the average daily performance of a locomotive, where, at the first level, such factors as average daily run of a locomotive, average trainload are taken into consideration; at the second level, the focus is on the service speed, locomotive turnover at station, etc.; at the sixth level, the focus is on the type of locomotive, its technical state, etc. It is shown that statistical methods of factor analysis and link analysis combined with such other methods of Data Mining as methods of simulation and prediction, the average daily performance of a locomotive can be planned proactively. The author proposes a procedure of migration towards a digital traffic safety management system that would be based on models of interaction of safety and dependability factors of all railway facilities at all railway levels of hierarchy, as well as in association with other factors that have no direct relation to dependability, yet affect the safety of the transportation process.* **Conclusions.** *The primary benefit of migration towards Big Data consists in the development of a dynamic model of traffic safety, the elimination of human factor in control systems. Most importantly, it enables the creation within the Russian Railways company (JSC RZD) of an integrated intelligent process and service management system that enables real-time traffic safety management. An extensive process of development and deployment within the company of the URRAN Single Corporate Platform (SCP) enabled executive decision support as regards risk-based functional dependability and safety of transportation facilities. Thus, the URRAN SCP sets the stage for the digital transformation of the traffic safety management system in JSC RZD.*

Keyword: *train traffic safety, factor analysis, automated control system, Big Data, Data Mining, human factor, risk prediction.*

For citation: *Zamyshliaev AM. Premises of the creation of a digital traffic safety management system. Dependability 2019;4: 45-52 p. https://doi.org/10.21683/1729-2646-2019-19-4-45-52*

Received on 25.09.2019 / Revised on 30.10.2019 / For printing 14.12.2019

[24] Liker J. K., Hoseus M.: Toyota Culture. The Heart and Soul of the Toyota Way, McGraw Hill, New York, 2008, 592 p.

[25] Osono E., Shimizu N., Takeuchi H., Dorton J.K.: Extreme Toyota, Radical Contradictions That Drive Success at the World's Best Manufacturers, John Wiley and Sons Inc., New York, 2008, 288 p.

[26] Papic L., Pantelic M.: A3 Report as an Effective Tool for Excavator Accident Problem Solving (In Serbian), Proceedings of 21st DQM International Conference on Dependability and Quality Management, ICDQM-2018, Prijevor, Serbia, 2018, pp. 3-13.

About the authors

Ljubiša Papić, DR.SC in Engineering, Professor, Director, Research Center of Dependability and Quality Management (DQM), Čačak, Serbia, e-mail: dqmcenter@mts.rs

Irina V. Gadolina, Candidate of Engineering, Associate Professor, Senior Researcher, Federal State Publicly Funded Scientific Establishment Mechanical Engineering Research Institute of the Russian Academy of Sciences, Moscow, Russia, e-mail: gadolina@mail.ru

Milorad Pantelić, Doctor of Engineering, Director, Enterprise Kolubara Metal, Lazarevac, Serbia, Associate Professor, Faculty of Technical Sciences, University of Kragujevac, Čačak, Serbia

Neda Papić, BSc in Industrial Engineering, MSc student in Industrial Engineering. Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia

The authors' contribution

Ljubiša Papić substantiated the expediency and requirement for the application of the Toyota A3 Report in enterprise operations management in the mining industry. Using a specific example of bucket-wheel excavator failure, the stages of analysis are shown.

Irina V. Gadolina performed a more detailed analysis of the information on the current dependability status of the excavator in terms of the variability of the availability factor, built confidence intervals of this characteristic.

Milorad Pantelić oversaw the recovery operation after the excavator accident. He collected the information on the failure of the excavator implements and its subsystems. He also ensured the delivery of the repair operations schedules.

Neda Papić ensured the presentation of information in a publishable from. She was also responsible for the design and composition of the paper.

11. Conclusions

The Toyota A3 Report, as a flexible mean for solving problems, occurred during work, was adjusted for terms of mining machines operation (excavators, transporters, depositors etc.) on open-pit mines. Considering the situation that there is a large number of available data and information about processes that are highly complexed, such as the process of coal and overburden exploitation on open-pit mine, there is a possible consumption of a large amount of time for their finding. Because of that, the way of documenting in the form of the Toyota A3 Report has a great significance for speeding up communication and removing a loss of time in work processes. That represents an important step at implementing Lean production and Kaizen concept on the open-pit mine in Mining Basin Kolubara, Lazarevac, Electric-power Industry of Republic of Serbia

There are potential shortcomings in the Toyota A3 Report which relate to solving a particular problem of bucket-wheel excavator SRs 1200 24/4 (G2) accident. It seems that it is overloaded with information and complicated. That is a normal reaction considering such a complex document because there is a great volume of information (data) concentrated on a small place. The immaculate Toyota A3 Reports do not exist. Every time when there is a need for making such a report – there is a way to improve its content or form.

References

[1] Papic L., Pantelic M.: Implementation Methodology for Risk Minimization into Maintenance Process of Production System at Coal Mines, Report of Contract No. 4617 (In Serbian), DQM Research Center – Kolubara Metal Company, Prijevor – Vreoci, Serbia, 2009, 468 p.

[2] Sobek II Durward K., Smalley A.: Understanding A3 Thinking. A Critical Component of "Toyota"'s PDCA Management System, CRC Press, Tailor and Francis Group, New York, 2008, 173 p.

[3] Krafcik J. F.: Triumph of the Lean Production System, Sloan Management Review, Vol. 30, No.1, 1988, pp. 41-52.

[4] Dhillon B. S.: Mining Equipment Reliability, Maintainability and Safety, Springer, London, 2008, 211 p.

[5] Pantelic M., Papic L., Aronov J.: Maintainability and Safety Engineering of Excavator Units (In Serbian), The Library DQM Monographs Quality and Reliability in Practice, Monograph No. 5, DQM Research Center, Prijevor, Serbia, 2011, 289 p.

[6] Papic L., Aronov J., Pantelic M.: Safety Based Maintenance Concept, International Journal of Reliability, Quality and Safety Engineering, Vol. 16, No. 6, 2009, pp. 1-17.

[7] Papic L., Pantelic M., Aronov J., Verma A. K.: Statistical Safety Analysis of Maintenance Management Process of Excavator Units, International Journal of Automation and Computing, 7(2), 2010, pp. 146-152.

[8] Papic L., Pantelic M.: Maintenance-Oriented Safety Control Charts, International Journal of Systems Assurance Engineering and Management, 5(2), 2014, pp. 149-154.

[9] Papic L., Pantelic M., Aronov J.: System Safety Analysis Via Accident Precursors Selection, In: Dynamics of Information Systems, Computational and Mathematical Challenges, Springer Proceedings in Mathematics and Statistics, Volume 105, Springer International Publishing Switzerland, 2014, pp. 179-204.

[10] Papich L., Gadolina I., Zainetdinov R.: Interval Estimation of the Availability Factor of the Bucket-Wheel Excavator Based on Bootstrap Modeling, Journal of Machinery Manufacture and Reliability, Vol. 45, No. 6, 2016, pp.531-537. // Папич Л., Гадолина И.В., Зайнетдинов Р.И.: Интервальная оценка коэффициента готовности роторного экскаватора на основе бутстреп-моделирования, Проблемы машиностроения и надёжности машин, № 6, 2016, с. 55-62.

[11] Gadolina IV, Pobegaylo PA, Kritsky DYu, Papic L. Refinement of the engineering practice of evaluation of the wear rate of excavator implement components. Dependability 2019;1:18-23.

[12] Antonov AV, Chepurko VA, Cherniaev AN. Research of the beta-factor model of accounting for common cause failures. Dependability 2019;2:9-17.

[13] Pokhabov YuP. Problems of dependability and possible solutions in the context of unique highly vital systems design. Dependability 2019;19(1):10-17.

[14] Weigand B., Langmaack R., Baumgarten T.: Lean Maintenance System, Zero Maintenance Time – Full Added Value, Lean Management Institute, Aachen, 2005, 165 p.

[15] Hirano H.: 5S for Operators: 5 Pilars of the Visual Workplace, Productivity Press, New York, 1996, 160 p.

[16] Dale B. G.: Managing Quality, Blackwell Publishers Ltd., Oxford, 1999, 495 p.

[17] Reason J.: Managing the Risks of Organizational Accidents, University of Manchester, 1997, 266 p.

[18] Dhillon B.S.: Safety and Human Error in Engineering Systems, CRC Press, Taylor and Francis Group, Boca Raton, 2013, 260 p.

[19] Reason J.: Human Error, Cambridge University Press, Cambridge, 1990, 302 p.

[20] Taleb N.N.: The Black Swan, The Impact of the Highly Improbable, Random House, New York, 2007, 369 p.

[21] Aronov J., Papic L.: Reliability and Safety Management of Engineering Systems Through the Prism of Black Swan Theory, In: System Reliability Management, Solutions and Technologies, CRC Press, Taylor and Francis Group, Boca Raton, 2018, pp. 103-112.

[22] Morgan J.M., Liker J.K.: The Toyota Product Development System. Integrating People, Process and Technology, Productivity Press, New York, 2006, 440 p.

[23] Womack J. P., Jones D. T.: Lean Thinking. Banish Waste and Create Wealth in your Corporation, Free Press, New York, 2003, 396p.

are used during training for solving problems and for shaping The Toyota A3 Report. Here we give some parts of this review [19].

A. Recommendations for solving problems:

• evaluate the situation relying on facts,

• follow (monitor, observe) the problem,

• concentrate on one problem (one Toyota A3 Report – one problem),

• watch deviations where the problem appears,

• study in detail the cause and analyze all the facts and data,

• if necessary, take temporary measures to locate the problem,

• detect (determine) the main cause,

• develop corrective measures, give tasks and determine deadlines for their realization.

B. Recommendations for shaping The Toyota A3 Report:

• distribute the time so the situation can be evaluated entirely (use a wide range of information, rely on the facts and not on opinions, take into consideration longterm effect),

• orientate towards concrete listeners; Take into consideration their needs and level of understanding of the situation,

• coordinate showing material with values of the company and its philosophy,

• avoid using a lot of words, use more schemes, graphics and other ways of clear information representation,

• every word should be from the field of work; Express yourself precisely and avoid slang terms,

• evaluate the clarity of material presentation; Does shaping of report helps to the understanding of its content?

An interesting analogy could be drawn between organizing a space, based on principles of the «5S Method» [12], in the Toyota factories while making The Toyota A3 Report. In a Lean Enterprise, it is unacceptable to overload space with a surplus of supplies because they represent – loses [19]. Rational usage of space is proof of making an effective additional value. Unnecessary material decreases safety, makes mess and disturbes discovering of standard deviation. On a similar way, shaping The Toyota A3 Report it is important not to allow losses: redundant words, extensive explanations, unnecessary schemes, which disturbs an essence to be seen. In that way, maximal effectiveness of adding the value is provided. The loss in documents blurs the basic idea and often leads to people losing the key moment from their sight.

The Toyota A3 Report and the way of their preparation make communication clear and operational, besides, The Toyota A3 Reports contribute to continual development. So, if making of The Toyota A3 Report brought to standards change or to increase of knowledge circumference – the database is renewed. The Lean Thinking [20] requires learning a lesson from solving problems (not only repairing of a complicated situation) and The Toyota A3 Report helps to such training.

9. The Toyota A3 Report and PDCA cycle

Aspiration of Toyota towards experiments lies in the base of all the standardized operations and processes which represent the part of everyday work. The Toyota company converted the cycle «Plan – Do – Check – Act» (PDCA) i.e. process of continual work improvement which is widely applied in different areas of business, into unique methodology «The Toyota A3 Report». It reflects the culture of Toyota [21] where the ability to solve problems is considered to be the most important quality of an employee which is formed from the beginning of his career and is continuously improving in the training process.

Akio Matsubara, former executive director for personnel management and now the president of Toyota Gosei North America Corporation sais [22]:

«In the first ten years of a person working in the Toyota company, we repeat multiple times a three-phase cycle of training which develops the ability and skill of solving problems in a man. The entire personnel develops inside itself a skill of problem overcoming which represents the basic approach in the Toyota working. The philosophy of the Toyota company implies: overcoming the problem, the employee is giving a contribution to the realization of cooperative politics, focused on satisfying the customer demands. We advise our people that the skill of overcoming the problem is necessary for achieving success in Toyota».

The Toyota A3 Report is read from top to down, from left to right and is used for solving problems, updating states and suggestions. The Toyota A3 Report follows the methodology of the Deming cycle of continuous improvement PDCA.

10. The Toyota A3 Report about solving problems of «Bucket-wheel excavator SRs 1200 24/4 (G2) accident»

10.1 Practical solving of the problem

The process of solving problems occurred during work can be described by the logical course that follows the Deming cycle of continuous improvement PDCA, and the Toyota A3 Report contains the following seven sections (steps): initial information, current state, goal, cause-consequence analysis, corrective measures, confirmation of effect, following actions. This process is defined on the basis of observations conducted in Toyota Company and published in the book [2].

The final look of The Toyota A3 Report about solving problem of an accident on bucket-wheel excavator SRs 1200 24/4 (G2) which happened on April 6th in 1995 on open-pit mine Field D, MB Kolubara, Electric Power Industry of Serbia, which was previously partially analyzed in the paper [23], is shown in Figure 9.

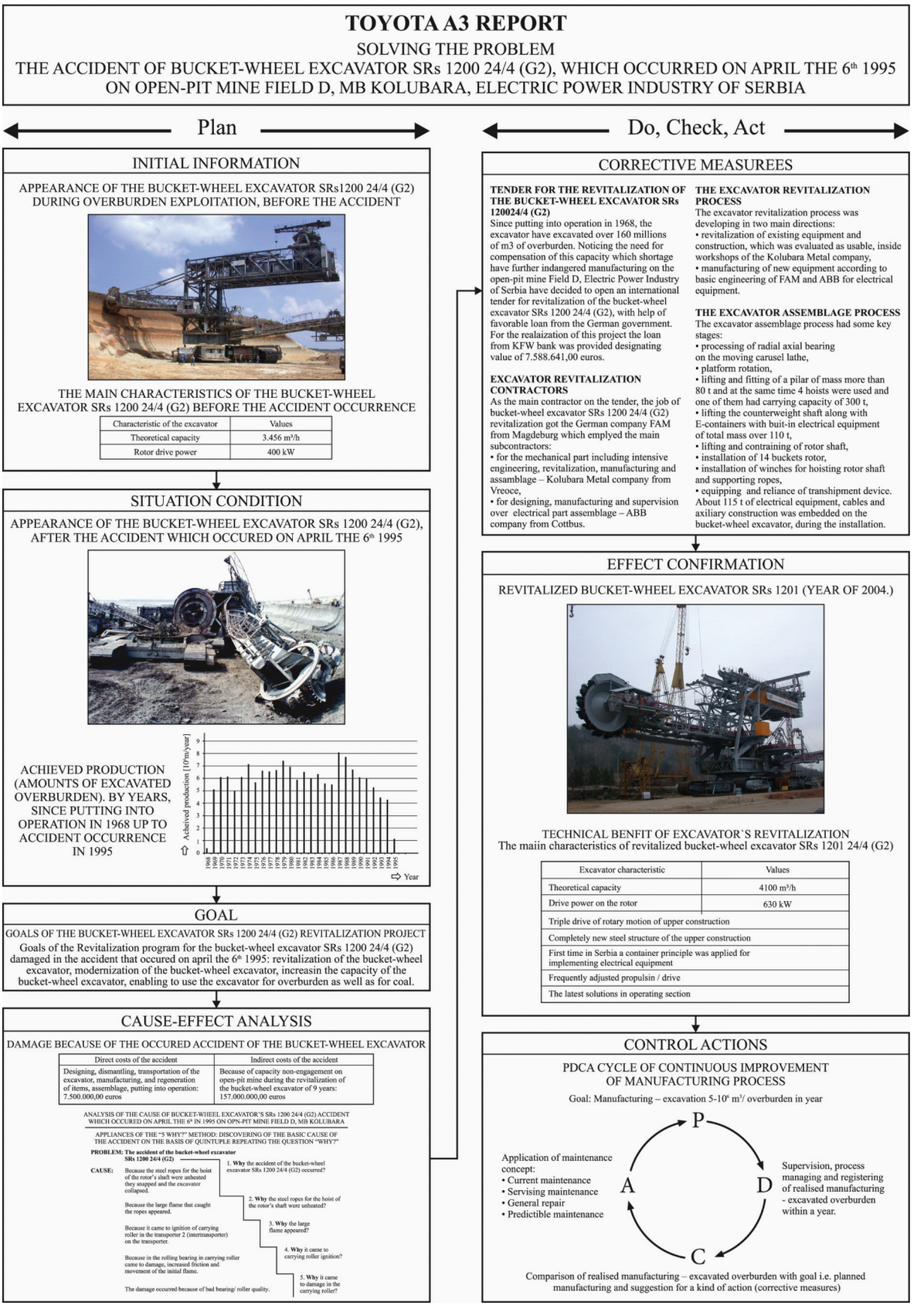


Figure 9 – The Toyota A3 Report view for the problem solving: «The accident of bucket-wheel excavator SRs 1200 24/4 (G2), which occured on April the 6th 1995».

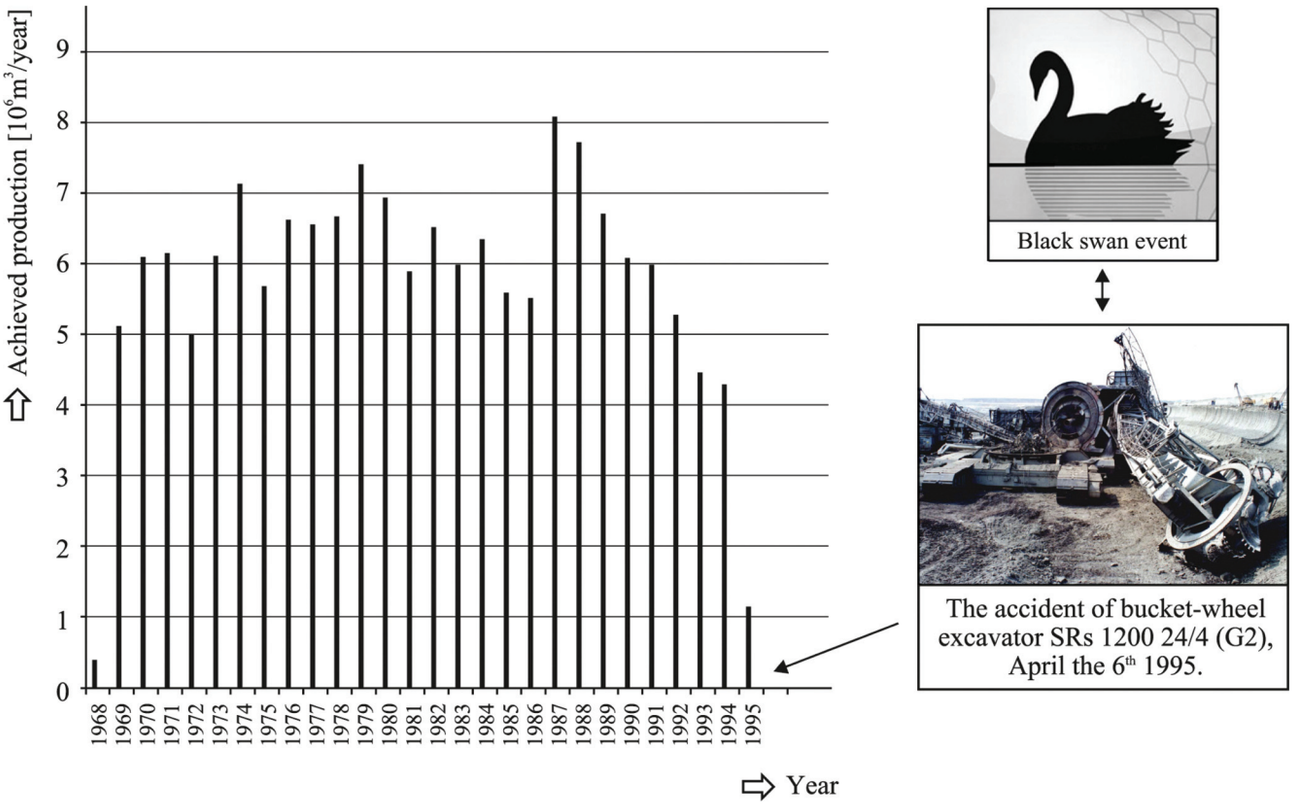


Figure 8 – The accident of bucket-wheel excavator SRs 1200 24/4 (G2) – typically «Black Swan» event.

It is impossible to predict them but we should know how to live with them.

By its character «Black Swans» couldn't be predicted because of similar events haven't ever happened before. However, it is possible to study how companies and people who have survived some disasters coped with their consequences. Such an analysis could help the company to be prepared for strategy making that help them stand on their feet after extraordinary disasters (technical disasters such as mining machines accidents) as soon as possible and with minimal damage.

Nassim Taleb has suggested the risk theory «Black Swan» which considers events that are hard to predict and rare events which have significant consequences. «Black Swan» is a metaphor which describes surprising events with great consequences.

«If you have seen only the white swans your entire life, that doesn't mean that black swans do not exist».

- writes Nassim Taleb in his book «The Black Swan, The Impact of the Highly Improbable» [17].

7.2 Criteria for «Black Swan» events and bucket-wheel excavator accidents

The accident of bucket-wheel excavator SRs 1200 24/4 (G2) which happened on April the 6th in 1995. has all the characteristics i.e. satisfies the criteria of «Black Swan» events. That what Nassim Taleb calls «Black Swan» – that is an event which has a following three characteristics:

- the event is unexpected,
- the event causes great consequences,
- after the occurrence, retroactively, the event has a reasonable explanation as if the event has been expected.

Until the accident that happened on April 6th in 1995, this bucket-wheel excavator has excavated over 160 million m^3 of overburden. How large emptiness was made due to the failure of this excavator could be seen by the production in years that moved from 5 to 7 million m^3 of overburden (Figure 8).

Since those accidents could not be predicted, the task of the owner of dangerous objects is to assure decrease of its negative impact on the personnel, population and environment. In that regard, the task of this country is to compel the owners of such objects to strictly carry out directions, regulations and directives of normative documents in safety department [18].

As far as engineering systems reliability and their complexity increases, the «human factor» part increaes as well. Therefore, safety culture education, making of non-punishment manufacturing environment stays the most important task of theory and practice for engineering systems safety.

8. Toyota A3 Report as a problem-solving tool

Making The Toyota A3 Report is teaching every employee in Toyota, first of all, their direct supervisors. There is a universal review of states and recommendations which

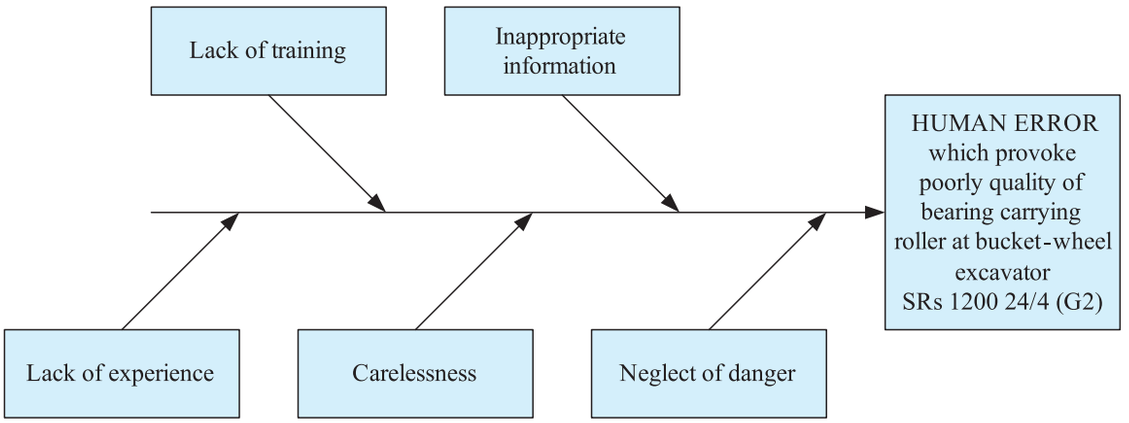


Figure 7 – Causes of the human error [6].

This problem could be further solved in a qualitative way by determining the cause of the second and higher degree of human errors.

6. Human factor in modeling of accident occurrence

6.1 The «Swiss cheese» model of human errors' causes

More often the responsibility for accidents and technical disasters are attributed to individual (personal) human errors. But in his book «Managing the Risk of Organizational Accidents» [14] psychology professor James Reason from the University of Manchester, in detail studies a problem whether one human error can cause the accident if we don't take into account cases of obvious sabotage or terrorist activities. It is proven that the entire array of hidden and undiscovered on time errors leads to an accident. Safety culture and problems which cause this array of errors, as usual, are called «human factor» [15]. After all, exactly the human factor forces the operator or maintainer of the engineering system to make wrong decisions.

Why there are accidents happening, which conditions are causing them, which factors contribute to their occurrence? Accidents, as a rule, occur not as a result of some individual error but they are a consequence of hidden, undiscovered on time damages and failure kinds that are cumulating on each other and could bring to an unwanted array of events. Hence, the largest number of accidents and unfortunate incidents are a consequence of an array of events.

That kind of accident attribute is described the best by the «Swiss cheese» model, which was developed by James Reason [16] and which illustrates various kinds of human «contribution» to engineering systems' accidents. Reason's «Swiss cheese» model explains what way people contribute to working ability disturbance of complex and mutually connected engineering systems, which leads to accidents.

If the state of a certain engineering system is shown in the shape of a slice of cheese with holes, in that case, and depending on the time of manifesting the kinds could be classified into two:

- hidden failure kinds (hidden defects),
- active failure kinds (active defects).

Hidden defects (hidden kinds of failures, hidden conditions, terms, regimes) represent the result of a decision or procedures of work which has been performed long before the accident (occurrence). These defects and their consequences can stay undetected for a long period of time (for many years). Such errors (failure kinds) usually occur on the decision making level and determining rules and regulations or on the level of operating management i.e. persons further from an occurred accident, as in time as well in space. For example, a decision about merging maintenance personnel from two different open-pit mines (two enterprises) without training that personnel for standardized procedures for maintaining the mining machines represents a clear example of hidden defect (hidden kind of failure).

Active defects (active kinds of failure, active errors) represent mistakes or disturbances which immediately (without delay) have an unfavorable effect. Such errors are usually made by operators or maintainers of mining machines. Actions of operators or maintainers which moves the lever for lifting the upper excavator's construction instead of moving the lever for excavator's rotation sets an explicit example for this kind of error (failure).

7. «The Black Swan» event risk theory

7.1 «The Black Swan, The Impact of the Highly Improbable» [16]

Mathematician and economist Nassim Nicholas Taleb, in his book «The Black Swan, The Impact of the Highly Improbable» [17] from 2007, has proposed a concept of «Black Swans» – unexpected (unpredictable) and significant (comprehensive) phenomenon that essentially change the course of history. That concept includes wars, economic crisis, internet appearance etc.

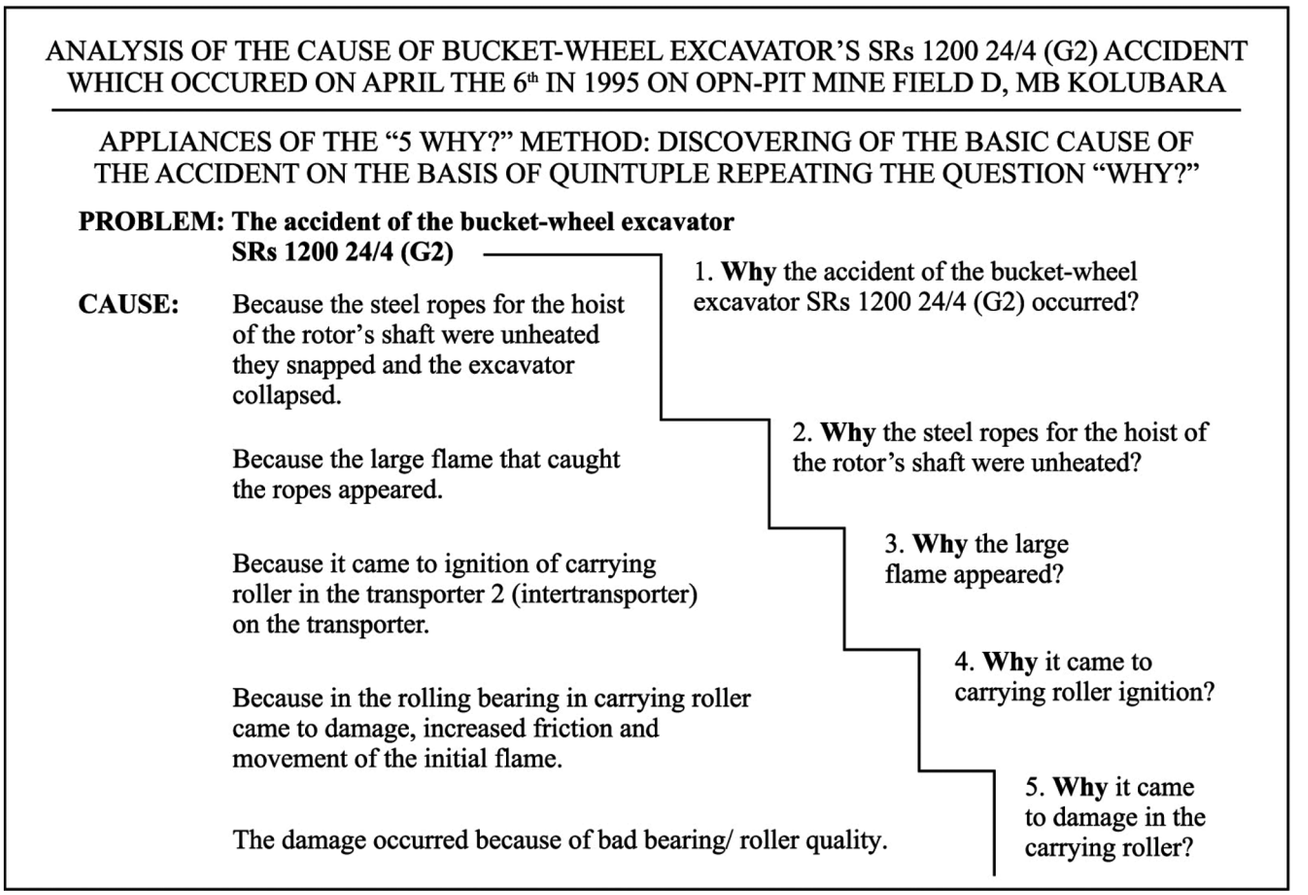


Figure 6 – Application of the «5 Why» method: Discovering of the basic cause of the accident on the basis of quintuple the question «Why».

5.2 Investigation of human errors causes at the bad bearings quality occurrence on the bucket-wheel excavator

Investigation of human errors at the bad bearings quality occurrence on the bucket-wheel excavator SRs 1200 24/4 (G2) was performed through the teamwork in Brainstorming method mode in the Kolubara Metal company. Thereat, the team acted according to all the recommendations for the Brainstorming organization [13]. The main of the recommendations were related to: team composition, the way of operating within the team, the team leader role. The team generated ideas about causes of maintenance problems which demands a solution.

Table 1. Accident share of excavators accidents causes

Cause of accident	Accident share [%]
Inadequate prepared pathway for the excavator (human error)	27
Error in parts manufacturing and excavator assembly at open-pit coal mine (human error)	22
Operator's error	18
Maintainer's error	13
Fatigue of materials, wear of equipment and corrosion processes	8
Inadequate design (human error)	7
Other miscellaneous factors	5

In these investigations, a certain rule that is suitable for composing of the initial (general) causal diagram was applied, and that rule is applicable for most of the real situations. The rule consists of that that there is almost always a certain number of categories of possible causes for some consequences (unwanted results) of the process. Solving a particular problem of bucket-wheel excavator's accident, investigations discovered from which factors (causes) and to what extent unwanted result or consequence depends on:

«Human error which provoke poorly quality of bearing carrying roller at bucket-wheel excavator SRs 1200 24/4 (G2)».

Investigations have at first determined and abstracted five samples in terms as shown in Figure 7:

- lack of training,
- inadequate information,
- lack of experience,
- carelessness,
- negligence of the danger.

Figure 4 – Look of bucket-wheel excavator SRs 1200 24/4 (G2) before the accident appearance.

Figure 5 – Look of bucket-wheel excavator SRs 1200 24/4 (G2), after the accident which occured on April the 6th 1995.

The worth of direct costs (expenses) is: 7.500.00,00 EUR.

2. Indirect expenses, because of non-engagement of capacities on the open-pit mine during the period of bucket-wheel excavator revitalization, amount to 157.000.000,00 EUR.

This data was obtained on the basis of the price of 4.500,00 EUR of excavator's items down-time within the system (BWECD or BWECL).

Time of break duration:

9 years x 12 months x 30 days x 24 hours x 0,45 = 35.000 norm-hours

The worth of indirect costs is:

35.000 norm-hours x 4.500 EUR/hour = 157.000.000,00 EUR.

5. Analysis of bucket-wheel excavator's SRs 1200 24/4 (G2) accident cause

5.1 The «5 Why?» method application for determination of basic accident causes

The basis of the approach to the determination of quality problem causes in the Toyota company consists of asking the question «Why?» for five times during discovering the problem, which is labeled as «5 Why?». If there is the answer to the question «Why?» five times, then the basic cause and the way for its solution will be clear. The analysis of the basic maintenance problem causes based on quintuple repeating the question «Why?» is implemented into the maintenance system of the Toyota company (Lean Maintenance System) [11]. The «5 Why?» method is committed to a detailed investigation of problems and culture that lead to the basic causes of these problems. The «5 Why?» method is usually used in the Toyota for searching for the source of the maintenance problem. It describes the way of thinking needed to reach the level necessary for preventing reoccurrence of maintenance problems. This doesn't have to be the basic cause, but at least on this level, the corrective measures could be appropriate to prevent the return of the problem. In case of accident of the bucket-wheel excavator SRs 1200 24/4 (G2), the application of «5 Why?» method describes the way of thinking necessary to prevent reoccurrence of the accident, in terms shown in Figure 6.

According to data published into book [4], a significant percentage portion of every kind of failures on complex mining machines was caused by human error. They happen in the stages of designing, manufacturing, control, assemblage, exploitation and system maintenance, and also in the stage of operating, to any level of education, qualification, competence, and personnel experience. Errors of maintenance personnel consist of wrongly executing engineering system's maintenance manuals and they depend on their psychophysical state (fatigue, stress etc.), wrongly organized workplace due to the absence of a 5S system for workplaces managing [12], error in ergonomic calculations, the presence of noise on the workplace, not sufficient brightness on the workplace etc.

In the past period in Serbia, many investigations have been performed on account of determinating accidents' causes of mining mechanization on the open-pit mines for coal excavation. One such report from the investigation was published in [5]. Investigations show that errors of the personnel (operators, maintainers) play an essential role in accidents occurrence, which is confirmed by data from Table 1.

Analysis of this data shows that human errors in 87% of cases represent accidents' causes on the mining machines. Based on this, from Figure 6, we can conclude that «Bad bearing quality» in carrying roller is as well a human error i.e. personnel error in the final control, in the entry control, or even in the poorly made decision about bearings supplier choice.

Transportation Mechanism (ETM), Material Transportation Mechanism (MTM), and Material Excavating Mechanism (MEM), see histogram on Figure 3.

Reliability and safety of bucket-wheel excavator items don't always have to be in positive correlation. In other words, for high reliability, there's not always a low criticality to comply with and vice versa. Criticality of bucket-wheel excavator item's failure kind is an indicator which characterizes the safety of excavator functioning. For example, some items of bucket-wheel excavator could have a high reliability but at the same time a low safety as well (i.e. high criticality), which investigations have shown [1,5]. Here, this is the case with building groups (items): Mechanism For the Hoist of the Rotor's Arrow (MFHRA) and Supporting Steel Structure (SSS). That practically means that all kinds of failures of this building group occur rarely, but when they occur it causes serious consequences for bucket-wheel excavator functioning, and that means the entire BWECD system as well. In determining reliability, along with the length of time period UP TIME, a frequency of failure occurrence plays its part as well as the level of criticality for safety determining.

Therefore, taking into consideration the consequences of potential failure kinds, as well as in due time removing their causes, enables incensement of bucket-wheel excavators safety.

The availability factor is an important complex index of reliability and maintainability of the restorable systems used in the problems of reliability and risk analysis. The method of estimating the variability of the availability factor has been developed in the paper [10] based on the statistical methods with the generation of the repeated samples (resampling). The subsystems of the bucket-wheel excavator SRs 1200 24/4 (G2) using the statistical data on the failures collected in Mining Basin Kolubara, Lazarevac, Serbia, have been used as the object of applying the method. The use of the resampling methods, i.e., the jackknife and bootstrap methods, permitted one to estimate the variability of the availability factor of the excavator subsystems.

Except for the MEM subsystem, the reliability and maintainability of the subsystems corresponds to the requirements to the reliability of the complex technical objects. The lower quartile of the scattering of the availability factor reaches 0,9977 for the most responsible subsystem MFHRA without taking into account the outliers, which corresponds to a rather high reliability event considering the range estimated using bootstrap [10]. The 90% confidence interval for the availability factor for the total system reaches [0,81; 0,94] according to the estimate based on the developed method with the median 0,90.

The digging system in some cases does not demonstrate sufficient dependability. That is caused by premature wear of the implements. In [11] the engineering formula for wear assessment was refined based on the previously known formula subject to various modes of operation. The application of this formula will help schedule preventive maintenance and inspections.

The beta factor method [12] can be used for the analysis of the failures of excavators as complex systems. It is the most simple in terms of simulation of dependent failures and further calculations. However, it has limitations of its own. For a complex system, such as an excavator, dependability must be ensured from the earliest life cycle stages through consecutive execution of specific design, process-related and manufacturing procedures [13]. The Toyota A3 Report can put some clarity into this matter.

4. Accident of bucket-wheel excavator SRs 1200 24/4 (G2) which happened on April 6th 1995 and its consequences

Bucket-wheel excavator SRs 1200 24/4 (G2) that has been assembled and put into operation in 1968 on the open-pit mine Field D, MB Kolubara, and was given internal mark G2 («Grinding Machine 2»), Figure 4.

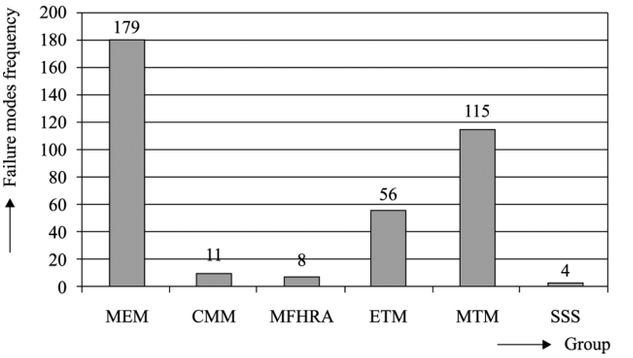


Figure 3 – Failure modes frequency of groups for bucket-wheel excavator SRs 1200 24/4 (G2) [5].

The accident of bucket-wheel excavator SRs 1200 24/4 (G2), Figure 5, has brought to great damages that had to be failure diagnosed and assessed, which was done by MB Kolubara and Kolubara Metal experts. Certain parts of the damaged machine have been transported on the assembly site in Zeoke, and some in Kolubara Metal Workshops.

The assessment of consequences is in connection with the analysis of direct and indirect damages, which can occur at a certain outcome (end state). If damages have been calculated in different units of measurement, as a result of a certain outcome, they should be reduced to one coequal damage. Besides, the end states can have a current or delayed effect. For example, during bucket-wheel excavator's SRs 1200 24/4 (G2) accident on the Field D, MB Kolubara open-pit mine, the cost analysis [1] has shown the existence of two kinds of expenses, as follows:

1. Direct expenses which include:
   - designing,
   - a dismantling of damaged bucket-wheel excavator,
   - transportation of damaged bucket-wheel excavator,
   - manufacturing and recovering of bucket-wheel excavator's items (assemblies, subassemblies, elements),
   - an assemblage of the bucket-wheel excavator,
   - putting into operation.

currence on bucket-wheel excavators (except when there are long conveyor belt systems in question, because the length of transport cannot be influenced due to technological conditions), which leads to conclusion that with rotary excavator reliability increase to the fullest extent, the entire BWECD system reliability could be increased as well [1].

Bucket-wheel excavator (rotary excavator) is a very complex engineering system which consists of a larger number of items (subsystems, assemblies, elements). Every item represents a potential source of DOWN TIME condition, accidental by the moment of occurrence and by the time of duration. Consequences of failure occurrence on rotary excavators (bucket-wheel excavators) are productivity reduction, i.e. excavator's capacity reduction, which reflects on a reduction of open-pit mine economic effects. For those reasons, in terms of given investigations [5] the excavator's items were ranked according to priority from the aspect of reliability. Subjects of the investigation were the following items of bucket-wheel excavator (rotary excavator):

- subsystem for material excavation,
- subsystem for transportation of material on the excavator,
- subsystem for rotation of the upper construction of the excavator,
- subsystem for excavator motion.

Results of these investigations have shown that the largest number of breaks on bucket-wheel excavators occurred because of material excavating subsystem failure (up to 51%), which is shown in Figure 2. Increasing the reliability of certain items of bucket-wheel excavator is possible to increase a total excavator's reliability. Thereat, the priority should be given to those items of the excavator which reliability is the lowest.

Investigations [1,5] for reliability assessment of the bucket-wheel excavator SRs 1200 24/4 (G2), in the time period from 1.1.2006. to 31.12.2006. have been based on Dispatch Report of Electric Power Industry of Serbia, MB Kolubara, open-pit mines Field D, Zeoke. Investigations have given the data about kinds, consequences, and causes of failure, as well as data about UP TIME and DOWN TIME condition occurrence. These investigations have shown that the most reliable groups of bucket-wheel excavator SRs 1200 24/4 (G2) building are: Mechanism For the Hoist of the Rotor's Arrow (MFHRA) and Supporting Steel Structure (SSS), followed by Circular Motion Mechanism (CMM), Excavator

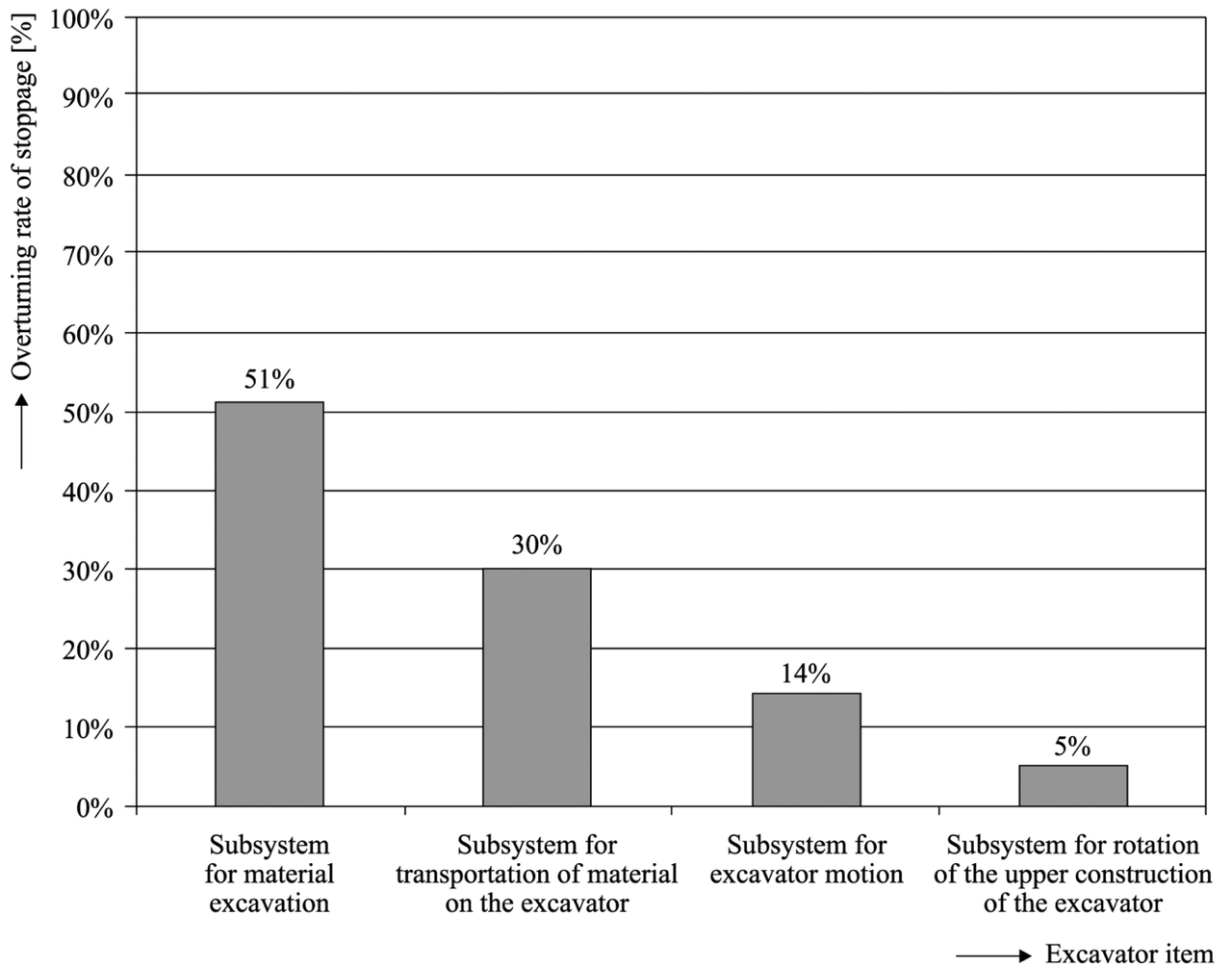


Figure 2 – Overturning rate of break with bucket-wheel excavator [5].

3. Previous reliability and safety investigations of mining machines

During the last few decades, there have been plenty of investigations with the purpose to determine productivity, reliability, and effectiveness in the stage of mining machines exploitation within the BWECD and BWECL systems and auxiliary mining machinery on open-pit mines in Serbia [1,4]. A large number of data, which substantiated for concluding about mining machines behavior during the exploitation in open-pit mines, has been collected, processed, and published and analyzed in the papers [7,8,9]. Results of investigations that are systematized within the monograph [5] refer to entire BWECD (BWECL) system. These results give the amount of breaks that was caused by the bucket-wheel excavator, self-propelled transporter (bandwagon), belt conveyor with rubber band and disposer, within open-pit mines Mining Basin Kolubara, Lazarevac, Serbia, as shown in Figure 1.

Generally, the largest number of DOWN TIMES occurs on the bucket-wheel excavator, although on conveyors with long belts DOWN TIME can be long-lasting. The following example is given for one BWECD system on open-pit mine Tamnava within MB Kolubara, which consists of rotary excavator SchRs 700, bandwagon, three conveyor belts with the rubber band that is 1.000 to 1.200 meters long and overburden disposer. Down-time structure shows that failures on the bucket-wheel excavator have caused 60% of down-times, failures of conveyor belts have caused 27% of down-times, bandwagon failure caused 9% and disposer failure has caused 4% of down-times. On the other hand, down-time structure of BWECD system on open-pit mine Tamnava, which consists of rotary i.e. bucket-wheel excavator SchRs 900 25/6 with five belt conveyors, shows that the percentage of excavator's failure and conveyor belt's failure is approximately the same. On the open-pit mine Field D, where BWECD system operates with rotary i.e. bucket-wheel excavator SRs 1200 24/4, with approximately 5 to 7 conveyor belts, the conveyor belts (because of their length) have almost double the share in failures then rotary excavators [1].

From given results of research we can perceive that breaks of BWECD system have mostly been caused by failure oc-

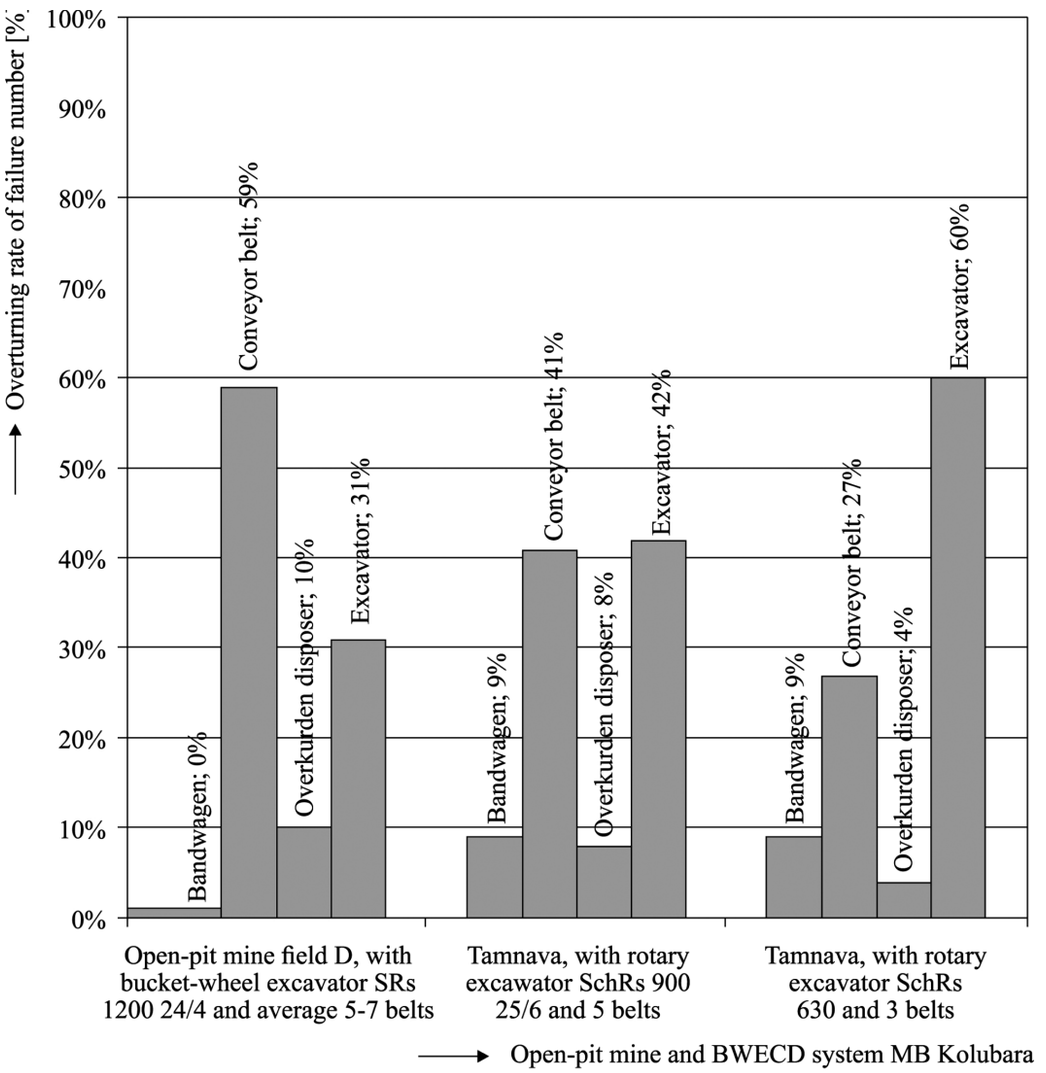


Figure 1- Overturning rate of failure number with certain BWECD systems at open-pit mines MB Kolubara, Lazarevac, Serbia [5].

1. Introduction

The basis of contemporary industrial manufacturing is made of natural recourses. Approximately 70% of natural recourses make mineral raw materials. In the world, today over 1.000 milliard dollars are spent on raw materials (metallic ore, non-metallic ore, coal, clay, stone, sand, and gravel), which for many countries represent the main good of export and import.

As an economic branch, mining in many countries represents the basis of development and has a great impact on their total economy. The fact of how much the mining economy impacts the economy of the country is illustrated the best by the following data [1]:

• the price of iron, the price of coke (stone coal) and ore participates with 80-90 [%],

• the price of non-ferrous metals, price of ore and electric power participates with 90%,

• the price of electric power, coal participates with 60%,

• the price of coal, maintenance of mining machinery on open-pit mine participates with 35-40 [%], etc.

Solving problems in the mining industry, before all, represents the ability to think. How to document the most important information and decisions in every stage, so that would be possible to exchange data with associates, include them into the working process and import corrections considering their opinion? When it comes to documenting a complex process of solving problems, piles of papers or, considering a contemporary situation, online data basis are given. However, Toyota Motor Company gives priority to the more simplified approach which requires a pen, an eraser and a piece of paper. Often, that method of work is called The Toyota A3 Report. Why the A3 format? The very format has been used in Toyota since the beginning because the significant portion of information exchange between organizational items of Toyota in Japan and its factories abroad has been carried out by fax and A3 format (297cm x 420cm) is the largest one that can be sent by facsimile.

The Toyota A3 Report method for problem-solving has been developed in order to present improvement description in a cleanly manner. The Toyota A3 Report has two main functions: proposition making and manner of reporting on approved actions given in the proposition. The idea of A3 method is to enable the visualization of proposed ideas on one A3 format piece of paper [2]. The Toyota A3 Report is an effective method because it decreases large amounts of data into a format that is easy to read and understand. That is a useful tool for work rationalization within companies in which employees perform multiple functions, for example in Lean companies, so they have very little time for reading a large number of documents to understand a particular problem or actual situation.

Advantages of using The Toyota A3 Report for solving problems are:

• methodological approach for solving problems,

• concise format for representation or for reporting to other persons,

• documenting and leaving a trace which other persons can follow and for others to understand procedures and results of solving problems,

• the common language in communication within a company,

• creating the Lean culture within a company,

• setting a basis for future changes.

In most companies, as a rule, information is made accessible but unconnected, without a clear logic. As a result, a large portion of time is spent on conversations and attempts for understanding, bringing into order, researching and analyzing data. Thereat, there is endless usage of laptop computers, but descriptions of work methodologies and principles of Lean production [3] lie on bookshelves, without a great hope that they are going to be read. The Toyota A3 Report is shaped not only to be read by the employees but to be worked upon, for example – to solve certain problems!

2. Maintenance and reliability of mining machines

Maintenance of bucket-wheel excavators on open-pit mines is directly in function of accomplishing acquired effectiveness (reliability, availability, maintainability, and safety), both on their design level as well as during their exploitation [4]. Well-chosen maintenance conception for BWECD system (Bucket-Wheel Excavator – Conveyor – Disposer System) and for BWECL system (Bucket-Wheel Excavator – Conveyor – Loader System), with well-trained personnel and maintenance management quality, impacts improvement of financial results on open-pit mines.

Bucket-wheel excavator carries a great potential risk from possible failures and accidents occurrence that is dangerous for the operative and wider environment. Reliability of bucket-wheel excavators, designed for successfully performing the objective function, determines the duration of the time interval in which they will operate without failure. Investigations [5] referred on increasing of reliability level and reliability management during a life cycle of bucket-wheel excavators have a goal to define safety precautions system of economic exploitation and achievement of complex regulations in connection with environmental protection and safety, both of operational as well as of more extensive environment.

Open-pit coal exploitation practice has proven that systems of continuous operating mode, such as BWECD and BWECL, provide maximal technological and economical results. Bucket-wheel excavators are required to have a high level of the task performing reliability. That indicates the necessity to determine the reliability quantity characteristics, among other issues, in order to adopt an adequate bucket-wheel excavator maintenance concept [6].

Original article
Dependability, vol. 19 no. 4, 2019 https://doi.org/10.21683/1729-2646-2019-19-4-32-44

Mining machines accident problem solving via the Toyota A3 Report

Ljubiša Papić[1], Irina V. Gadolina[2*], Milorad Pantelić[3], Neda Papić[4]

[1]Research Center of Dependability and Quality Management (DQM), Čačak, Serbia, [2]Mechanical Engineering Research Institute of the Russian Academy of Sciences, Moscow, Russian Federation; [3]Enterprise Kolubara Metal, Lazarevac, Serbia, Faculty of Technical Sciences, University of Kragujevac, Čačak, Serbia; [4]BSc in Industrial Engineering, MSc student in Industrial Engineering, Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia
**gadolina@mail.ru*


Ljubiša Papić


Irina V. Gadolina


Milorad Pantelić


Neda Papić

Abstract. *The Aim of the paper is to show the advantages associated with the application of the Toyota A3 Report as a standard method of information exchange. It must be noted that as of today this method has not found widespread application. It deserves better. Using specific examples of accidents involving mining machines, the authors show how a Report is completed hoping that this information will help in the adoption of this system in other enterprises. That may contribute to the solution of many problems of industrial management. This paper will be most useful for operators of mining machines. The* **Method** *consists in presenting material on an A3 sheet of paper, that is required in order to set forth all the information needed to solve a problem. Why the A3 format? A3 is the maximum size of a sheet of paper that can be faxed. Before the emergence of personal computers it was the most common tool of communication between Toyota Motor factories. The above example of application of the Toyota A3 Report contains such crucial sections as maintenance and reliability of mining machines, information on prior research, application of the "5 Why?" method and consideration of the human factor. In the example given in the paper, the report describes the circumstances of the accident involving the SRs 1200 24/4 (G2) excavator, that occurred on April 6, 1995 in the open-pit mine Field D, mining basin Kolubara by the Electric Power Industry of Serbia. The report also includes an estimate of the consequences and analysis of the causes of the accident. The* **Findings** *include the methodological approach to the solution of problems, brief format of information presentation, documentation and registration, so that other people involved in the process can review it; assuring the persons involved can form an idea of the operating procedures and outcome of problem resolution. A common language is provided for communication within the company along with a culture of Lean production. The A3 Report is a training process and foundation for future changes in the manufacturing process management.* **Conclusions.** *The Toyota A3 Report has two primary functions: submission of proposals and reporting on the approved measures per the submitted proposals. It allows strictly defining the problem and proceeding to the measures aimed at improving the situation. The practical application of the Report as part of communication within the company and with suppliers will enable quick and targeted solution of managerial problems. Initially developed in Japan within the Toyota company, the method currently finds wider application in Serbian enterprises and elsewhere.*

Keywords: *Accident, Problem solving, Mining machines, Open-pit coal mine, The Toyota A3 Report, Reliability and safety, PDCA, 5 Why?, Human factor, Swiss cheese model, Black swan event.*

For citation: *Papić L, Gadolina IV, Pantelić M, Papić N. Mining machines accident problem solving via the Toyota A3 Report. Dependability 2019; 4: 32-44.p. https://doi.org/10.21683/1729-2646-2019-19-4-32-44*

Received on 23.05.2019 / Revised on 09.11.2019 / For printing 14.12.2019

[3] Gubinsky A.I., Yevgrafov V.G. Ergonomicheskoe proektirovanie sudovykh sistem upravleniya [Ergonomic design of ship control systems]. Leningrad: Sudostroenie; 1977 [in Russian].

[4] Gubinsky A.I. Nadezhnost i kachestvo funktsionirovaniya ergaticheskikh sistem [Dependability and operational quality of man-machine systems]. Leningrad: Nauka; 1982 [in Russian]

[5] Glushkov V.M., Tseitlin G.E., Yushchenko E.L. Algebra. Yazyki. Programmirovanie [Algebra. Languages. Programming]. Kiev: Naukova Dumka; 1978.

[6] Rotshtein A.P. Veroyatnostno-algoritmicheskie modeli cheloveko-mashinnykh sistem [Probabilistic algorithmic models of man-machine systems]. Avtomatika 1987;6:81-87 [in Russian].

[7] Rotshtein A.P. Nechetkiy analiz nadezhnosti algoritmov deyatelnosti [Fuzzy analysis of the reliability of activity algorithm]. Dependability 2007;2:3-18 [in Russian].

[8] Barnard A. Why you cannot predict electronic product reliability. ARS, Europe: Warsaw, Poland; 2012.

[9] Goryainov A.V., Zamyshliaev A.M., Platonov E.N. Analysis of the influence of factors on damage caused by transport accidents using regression models. Dependability 2013;2:136-144.

[10] Zadeh L. Ponyatie lingvisticheskoy peremennoy i ee primenenie k prinyatiyu priblizhennykh resheniy [The concept of linguistic variable and its application to approximate reasoning]. Moscow: Mir; 1976 [in Russian].

[11] Kosko B. Fuzzy cognitive maps. International Journal of Man-Machine Studies 1986;24:65-75.

[12] Axelrod R. Structure of Decision: The Cognitive Maps of Political Elites. Princeton: University Press; 1976.

[13] Tsypkin Ya.Z. Osnovy informatsionnoy teorii identifikatsii [Foundations of the information theory of identification]. Moscow: Nauka; 1984 [in Russian].

[14] Rotshtein A., Rakytyanska H. Fuzzy evidence in identification, forecasting and diagnosis. Berlin: Springer; 2012.

[15] Rotshtein A.P. Vybor usloviy deyatelnosti cheloveka na osnove nechetkoy perfektnosti [Selection of human working conditions based on fuzzy correctness]. Proceedings of the Russian Academy of Sciences. Control science and systems 2018;6:108-119 [in Russian].

[16] Rotshtein A.P. Ranking of system elements on the basis of fuzzy relations: the least influence method. Dependability 2015;(4):23-29.

[17] Kosko B. Neural Network and Fuzzy Systems. Englewood Cliff. New York: Prentice-Hall; 1992.

[18] Butenin N.V., Neymark Yu.I., Fufaev N.A. Vvedenie v teoriyu nelineynykh kolebaniy [Introduction to the theory of nonlinear oscillations]. Moscow: Nauka; 1987 [in Russian].

[19] Hong J.S., Lie C.H. Joint reliability importance of two edges in undirected network. IEEE Transaction on Reliability 1993;2(1):17-23.

[20] Gertsbakh I., Shpungin Y. Combinatorial Approach to Computing Component Importance Indexes in Coherent Systems. Cambridge University Press: Probability in the Engineering and Information Sciences 2012;24(1):1-10.

[21] Denisov I.V., Smirnov A.A. Research of the operational dependability of the Lada Kalina vehicle systems affecting traffic safety. Dependability 2017;4:31-35.

About the author

Alexander P. Rotshtein, Doctor of Engineering, Professor, Professor of the Jerusalem College of Technology – Machon Lev, Jerusalem, Israel, e-mail: rothstei@g.jct.ac.il

qualification, C_2 is the road conditions, C_3 is the unit costs of operation, C_4 is the operating conditions, C_5 is the frequency of maintenance operations, C_6 is the quality of service and repair, C_7 is the quality of automobile's design, C_8 is the quality of operational materials and spare parts, C_9 is the storage conditions, C_{10} is the dependability and safety of the automobile.

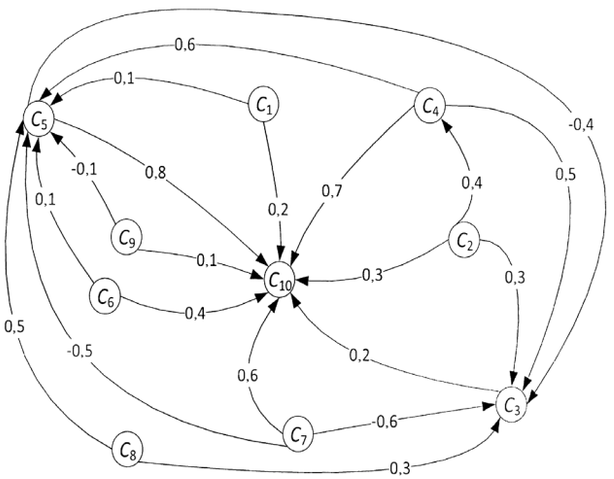


Figure 6 – Fuzzy cognitive map for dependability and safety estimation.

Matrix $\boldsymbol{W}$ (4) with expert estimates of the magnitude of effect, that assumes that $c = 1$, is as follows

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 & 0,1 & 0 & 0 & 0 & 0 & 0,5 \\ 0 & 1 & 0,3 & 0,4 & 0 & 0 & 0 & 0 & 0 & 0,3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0,2 \\ 0 & 0 & 0,5 & 1 & 0,6 & 0 & 0 & 0 & 0 & 0,7 \\ 0 & 0 & -0,4 & 0 & 1 & 0 & 0 & 0 & 0 & 0,8 \\ 0 & 0 & 0 & 0 & 0,1 & 1 & 0 & 0 & 0 & 0,4 \\ 0 & 0 & -0,6 & 0 & -0,5 & 0 & 1 & 0 & 0 & 0,6 \\ 0 & 0 & 0,3 & 0 & 0,5 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -0,1 & 0 & 0 & 0 & 1 & 0,1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

5.2. Importance indices of concepts

Table 2 contains nine pairs of vectors associated with the calculation of the importance indices of concepts $C_1, \ldots, C_9$. Each pair contains the initial vector (12) and vector (14) in steady-state operating conditions. The last element of the second vector in each pair corresponds to the importance index of the concept, i.e. $I(C_1) = 0.686$. The last column in Table 2 shows the step-by-step change of the level of dependability and safety of an automobile (A_{10}) in case of activation of one of the factors (A_i, $i = 1, \ldots, 9$). The diagram of the importance indices of concepts is shown in Figure 7. The results of calculation of the importance indices of the combined effect of concepts are shown in Table 3, i.e. $I(C_1, C_2) = 0.949$.

It should be noted that concept C_7 can be detailed subjects to the conclusions of [21].

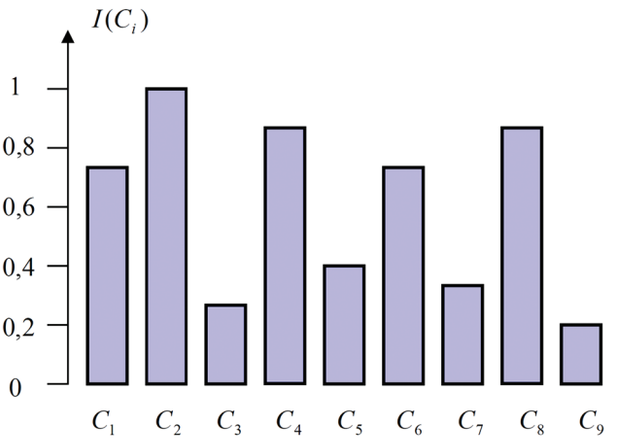


Figure 7 – Diagram of importance indices of factors.

6. Conclusion

The paper proposes and demonstrates with an example of a man-machine system a method of ranking of factors that affect its dependability. The method is based on the formalization of causal relationships between the contributing factors and the dependability in the form of a fuzzy cognitive map, i.e. directed graph, whose nodes correspond to the system dependability and contributing factors, while the weighted edges indicate the magnitude of the factors' effect on each other and the system's dependability.

The proposed method may be regarded as an equivalent to Birnbaum's ranking of system components in the probabilistic dependability theory. The advantages of the method include:

• use of available expert information with no collection and processing of statistical data;

• capability to take into consideration any qualitative and qualitative factors associated with people, technology, software, quality of service, operating conditions, etc.; In particular, individual concepts can characterize various types of redundancy (structural, algorithmic, etc.), that are used to improve dependability;

• easily scalable number of considered factors through the introduction of new nodes and edges of a directed graph.

The method can be applied to complex systems with fuzzy structures, whose dependability strongly depends on interrelated factors that are measured by means of expert methods.

References

[1] Barlow R., Proschan F. Statistical theory of reliability and life testing. Moscow: Nauka; 1984.

[2] Riabinin I.A. Nadezhnost' i bezopasnost' strukturno-slozhnykh sistem [Dependability and safety of structurally complex systems]. Saint Petersburg: Saint Petersburg University Publishing; 2007 [in Russian].

4.2. Algorithm of importance index calculation

Step 1. Specifying the initial vector (6). For importance index $I(C_j)$, the initial vector is specified as follows

$$A^0 = \left[A_j^0 = 1, A_i^0 = 0,\ i = 1, 2, ..., n,\ i \neq j \right], \quad (12)$$

while for importance index $I(C_j, C_k)$ it is specified as

$$A^0 = \left[A_j^0 = A_k^0 = 1, A_i^0 = 0,\ i = 1, 2, ..., n,\ i \neq j, k \right]. \quad (13)$$

Step 2. Using recurrence equation (5), finding the FCM state vector

$$A^l = \left[A_1^l, A_2^l, ..., A_n^l \right] \quad (14)$$

in steady-state operating conditions, i.e. at such step l, whereas $\left| A_i^l - A_i^{l-1} \right| < \varepsilon$, where ε is a small positive number, $i = 1, 2, \ldots, n$.

Step 3. Elements A_n^l of vector (14) obtained under initial vectors (12) and (13) respectively shall be considered to be importance indices $I(C_j)$ and $I(C_j, C_k)$.

5. An example

5.1. Concepts and effects

Let us examine the automobile dependability and safety model in the "driver-automobile-road" system. The fuzzy cognitive map of the system is shown in Fig. 6, where the concepts have the following contents: C_1 is the driver's

Table 2. Values of concepts in steady state for various initial vectors.

Step	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}
1	1	0	0	0	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3040	0,022	0,000	0,000	0,000	0,187	0,000	0,000	0,000	0,000	0,68579
1	0	1	0	0	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
774	0,000	0,044	0,000	0,365	0,747	0,000	0,000	0,000	0,000	0,94834
1	0	0	1	0	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3717	0,000	0,000	0,020	0,000	0,000	0,000	0,000	0,000	0,000	0,22707
1	0	0	0	1	0	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3014	0,000	0,000	0,000	0,022	0,335	0,000	0,000	0,000	0,000	0,79115
1	0	0	0	0	1	0	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
5324	0,000	0,000	0,000	0,000	0,017	0,000	0,000	0,000	0,000	0,33491
1	0	0	0	0	0	1	0	0	0	0
…	…	…	…	…	…	…	…	…	…	…
3196	0,000	0,000	0,000	0,000	0,186	0,022	0,000	0,000	0,000	0,68912
1	0	0	0	0	0	0	1	0	0	0
…	…	…	…	…	…	…	…	…	…	…
4953	0,000	0,000	0,000	0,000	0,000	0,000	0,017	0,000	0,000	0,30912
1	0	0	0	0	0	0	0	1	0	0
…	…	…	…	…	…	…	…	…	…	…
2742	0,000	0,000	0,000	0,000	0,321	0,000	0,000	0,023	0,000	0,77418
1	0	0	0	0	0	0	0	0	1	0
…	…	…	…	…	…	…	…	…	…	…
3086	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,022	0,18667

Table 3. Importance indices of combined effect of factors.

Concepts	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	0,949	0,686	0,801	0,686	0,730	0,335	0,786	0,255
C_2	–	0,948	0,948	0,948	0,950	0,949	0,950	0,948
C_3	–	–	0,791	0,335	0,689	0,309	0,774	0,254
C_4	–	–	–	0,791	0,803	0,703	0,823	0,782
C_5	–	–	–	–	0,689	0,309	0,774	0,187
C_6	–	–	–	–	–	0,356	0,788	0,294
C_7	–	–	–	–	–	–	0,309	0,323
C_8	–	–	–	–	–	–	–	0,763

$$A^{k+1} = f\left(A^k W_0 + cA^k\right), k = 0, 1, 2, \ldots, \quad (2)$$

where A^{k+1}, A^k $k = 0, 1, 2, \ldots$ are $(1\times n)$ state vectors of FCM, whose elements define the values of concept at steps k+1 and k respectively;

$$W_0 = \begin{bmatrix} 0 & w_{12} & \ldots & w_{1n} \\ w_{21} & 0 & \ldots & w_{2n} \\ . & . & \ldots & . \\ w_{n1} & w_{n2} & \ldots & 0 \end{bmatrix} \quad (3)$$

is the $(n\times n)$ matrix of the magnitude of mutual effects of concepts C_i, in which diagonal elements are equal to zero.

If instead of matrix (3) an $(n\times n)$ matrix is used,

$$W = \begin{bmatrix} c & w_{12} & \ldots & w_{1n} \\ w_{21} & c & \ldots & w_{2n} \\ . & . & \ldots & . \\ w_{n1} & w_{n2} & \ldots & c \end{bmatrix}, \quad (4)$$

in which all elements on the main diagonal are equal to parameter $c\in[0,1]$, then we will write formula (2) as

$$A^{k+1} = f\left(A^k W\right), k = 0, 1, 2, \ldots, \quad (5)$$

that is similar to the recurrence equation for a Markovian chain, if we take $f(x) = x$. The fundamental difference consists in the fact that a Markovian chain simulates the dynamics of event probability variation, while FCM simulates the dynamics of the level of causes, i.e. factors that lead to such states or events (see Fig. 2).

The initial state of an FCM is defined by vector

$$A^0 = \left[A_1^0, A_2^0, \ldots, A_n^0\right], \quad (6)$$

whose elements reflect the values of concepts at step $k = 0$. As the result of interaction between concepts FCM enters the steady mode, that corresponds with one of the types of stability [18].

4. Ranking of concepts

The allocation of system dependability resources is based on quantitative estimates (ranks) of its elements' importance. In the statistical dependability theory, Birnbaum's importance index of an element is the most widely used [1]. It is defined based on the system's dependability function

$$P_S = f_S\left(P_1, \ldots, P_i, \ldots\right), \quad (7)$$

where P_S and P_i are the system's probability of no-failure and its i-the element respectively.

The first derivative in (7) is the importance index of the system's i-th element according to Birnbaum, that is calculated as follows [1]:

$$I_i = \frac{\partial P_S}{\partial P_i} = P_S\left(P_1, \ldots, P_{i-1}, 1, P_{i+1}, \ldots P_n\right) - P_S\left(P_1, \ldots P_{i-1}, 0, P_{i+1}, \ldots, P_n\right). \quad (8)$$

The second derivative in (7) is the importance index of the joint effect of the i-th and j-th elements (*joint reliability importance*), that was introduced in [19, 20].

In our case the elements of the model include the input concepts, i.e. the factors that affect the output level of system dependability. That explains the requirement to calculate the importance indices of FCM concepts.

4.1. Definition of importance indices

In the set of concepts $C=\{C_1, C_2, \ldots, C_n\}$ we will assume the following:

C_n is the output concept that defines the level of system dependability and is estimated with number $A_n\in[0,1]$;

$C_1, C_2, \ldots, C_{n-1}$ are the input concepts that correspond with the interconnected factors affecting system dependability and estimated by levels $A_i\in[0,1]$, $i = 1, \ldots, n-1$.

The value of concept C_n at the l-th step is the function of the elements of vector (6), i.e.

$$A_n^l = F\left(A_1^0, A_2^0, \ldots, A_n^0\right). \quad (9)$$

It is assumed that A_n^l is the value of concept C_n in the steady state, i.e. at such step l, when A_n^l is close to A_n^{l-1}. Formula (9) is equivalent to (7), which allows proceeding to the definition of concept ranks based on derivatives.

Let $I(C_j)$ be the importance index of concept C_j, while $I(C_j,C_k)$ be the index of combined importance of concepts C_j and C_k. Following (8) and [19, 20], let us identify such importance indices as:

$$I\left(C_j\right) = \frac{\partial A_n^l}{\partial A_j} = \frac{F\left(1_j, 0\right) - F\left(0\right)}{1-0} = F\left(1_j, 0\right), \quad (10)$$

$$I\left(C_j, C_k\right) = \frac{\partial^2 A_n^l}{\partial A_j \partial A_k} = \frac{F\left(1_j, 1_k, 0\right) - F\left(0\right)}{\left(1-0\right)\left(1-0\right)} = F\left(1_j, 1_k, 0\right), \quad (11)$$

where $F(1_j,0)$ is the value of function (9), when $A_j^0 = 1$ are equal to zero; $F(0)$ is the value of function (9), when all arguments are equal to zero (it is assumed that $F(0) = 0$); $F(1_j,1_k,0)$ is the value of function (9), when $A_j^0 = A_k^0 = 1$, while all the other arguments are equal to zero.

Note. The zero values of input concepts (except one in (10) and two in (11) that are equal to one) are selected in order to eliminate the possibility of them having an effect on the output concept through transitive connections.

number $A_i=\pi(x_i)\in[0,1]$, that characterizes the proximity of the value of concept $C_i\in C$ to a certain ideal: 0 is the lowest perfection, 1 is the highest perfection. "Fuzzy perfection" is synonymous with "fuzzy correctness", for which the membership functions were considered in [15]. Possible fuzzy boundaries between perfect and non-perfect values of variable x are shown in Fig. 3, where, as the value of x grows, the following transitions take place:

a) "non-perfect" (1) – "perfect" (0),

b) "perfect" (1) – "non-perfect" (0),

c) "non-perfect" (0) – "perfect" (1) – "non-perfect" (0).

3.3. Associations between concepts

The weight w_{ij} of the edge that connects concepts C_i and C_j indicates the magnitude of the effect of C_i on C_j. Let concepts C_i and C_j be characterized by variables x_i and x_j, while – as the result of the experiment – dependence $x_j = \varphi(x_i)$ was achieved. Then, the weight w_{ij} is defined as the derivative $w_{ij} = dx_i/dx_j$ that can have three forms (Fig. 4):

$w_{ij} > 0$, if the increase (decrease) of value x_i causes the increase (decrease) of value x_j (positive effect of C_i on C_j);

$w_{ij} > 0$ if the increase (decrease) of value x_i causes the decrease (increase) of value x_j (negative effect of C_i on C_j);

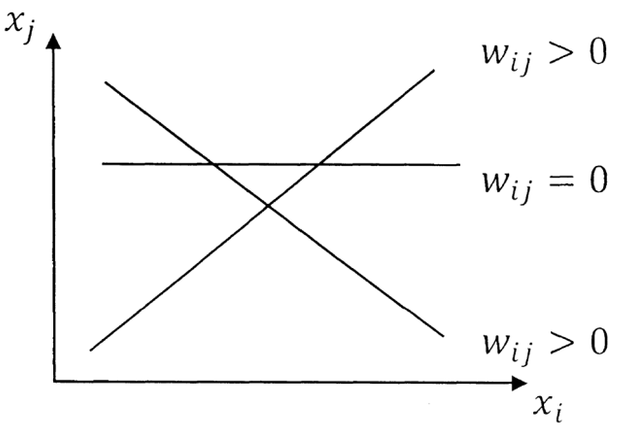


Figure 4 – Types of effects between concepts.

Table 1. Methods of estimating the magnitude of an effect.

Thermometer scale	Linguistic estimations	Quantitative estimations
	Positive maximum	1
	Positive above average	0,75
	Positive average	0,5
	Positive under average	0,25
	Not available	0
	Negative under average	-0,25
	Negative average	-0,5
	Negative above average	-0,75
	Negative maximum	-1

$w_{ij} = 0$ if value x_j does not depend on value x_i (no effect C_i on C_j).

The magnitude of effect (w_{ij}) is estimated expertly by means of linguistic terms and thermometer scale (Table 1). If several expert opinions are taken into consideration, the value w_{ij} is estimated as the weighted average:

$$w_{ij} = \frac{\alpha_1 w_{ij}^1 + \alpha_2 w_{ij}^2 + \ldots + \alpha_m w_{ij}^m}{\alpha_1 + \alpha_2 + \ldots + \alpha_m},$$

where w_{ij}^p is the estimate of the magnitude of the effect of the p-th expert; α_p is the weight of the p-th expert, $p = 1, 2, \ldots, m$; m is the number of experts.

In order to reduce the subjectivity of expert estimates, the method of the least effect proposed in [16] can be used.

3.4. Recurrence equations

According to [11, 17], the dynamics of concept values variation in FCM are defined by formula

$$A_i^{k+1} = f\left(\sum_{\substack{j=1 \\ j\neq i}}^{n} A_j^k w_{ji} + cA_i^k\right), k = 0, 1, 2, \ldots . \qquad (1)$$

where A_i^{k+1} is the value of concept C_i at step $k+1$; A_i^k and A_j^k is the value of concept C_i and C_j at step k respectively, w_{ji} is the magnitude of the effect of concept C_j on concept C_i; c is the parameter that takes into consideration the history, i.e. the contribution of the concept's value at the preceding step, $c\in[0,1]$; f is the threshold function, due to which the value of the concept does not exceed one.

In this paper, it is assumed that $c = 1$, while for the threshold function is used the positive part of the hyperbolic tangent (Fig. 5):

$$f(x) = \begin{cases} \tanh(x) \text{ при } x \geq 0; \\ 0 \text{ при } x < 0, \end{cases} \qquad \tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}.$$

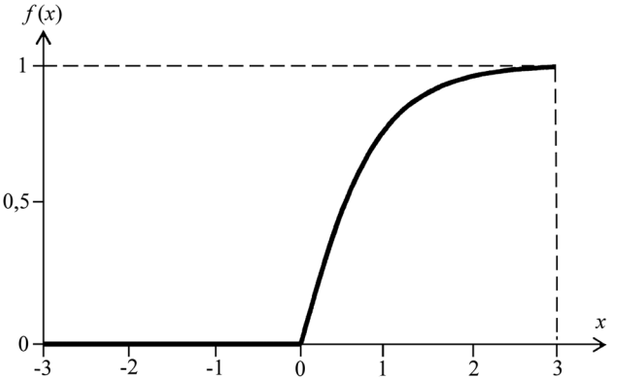


Figure 5 – Threshold function.

3.5. Matrix model

The recurrence equation (1) can be represented in matrix form

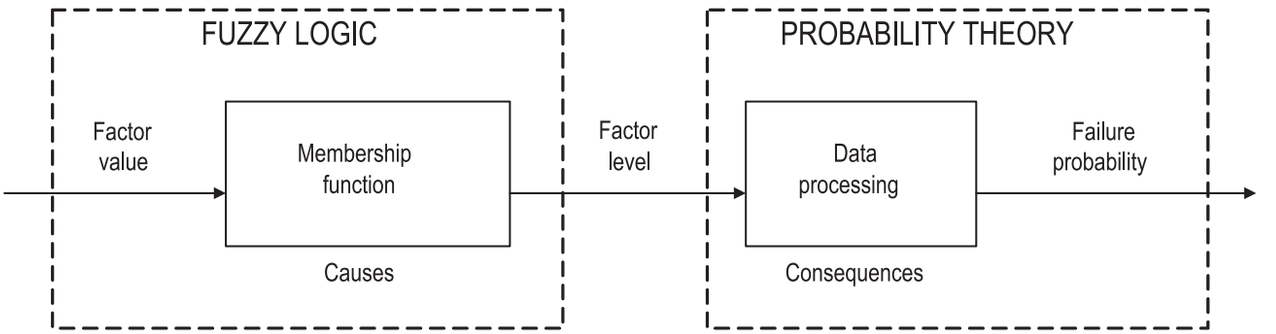


Figure 2 – Interrelation between the probability theory and fuzzy logic in dependability estimation.

in sociopolitical systems. FCM is a directed graph with weighted edges, of which an example is shown in Fig. 1. Graph nodes C_i called *concepts* correspond to the input and output variables that are taken into consideration in the model. Weighted edges of the graph reflect the *magnitude of the effect* w_{ij} of the changes of one variable C_i on the changes of another variable C_j.

The term "cognitive" implies, that the initial data for simulation consists of subjective opinions of an expert expressed as, e.g. "increases" or "decreases", for instance: "increasing C_i causes the decrease of C_j". In binary cognitive maps [12], an "increase" is estimated as "+1", while a "decrease" is estimated as "–1".

The term "fuzzy" implies that FCM [11] use various levels of "increase" and "decrease". They are defined by numbers from the intervals [0, 1] and [–1, 0], which corresponds to the terms "weak", "average", "strong", etc. from the fuzzy set theory [10].

From the point of view of the identification theory [13, 14] that involves restoring patterns based on experimental data, FCM is an approximator of the "inputs/outputs" dependence with interrelated outputs. As any approximator, e.g. regression, fuzzy rules, neural network, etc., FCM contains configurable parameters that are to be estimated through minimization of the disparity between the model and experimental output values. If the experimental data "inputs-outputs" is not available, the quality of the whole model depends on the expert's qualification. The art of simulation consists in compensating for the missing experimental data through high quality of expert estimates.

It would be relevant comparing FCM and Markovian chains (processes) familiar to the dependability experts. Both types of models are weighted directed graphs. The basic difference between FCM and Markovian dependability models consists in the fundamental difference between the fuzzy logic (causes) and probability theory (effects) shown in Fig. 2: the Markovian models reflect the dynamics of system state probabilities accounting for failures and restorations; FCM simulate the level dynamics of interrelated factors that cause failures and affect their probability.

3.2. Concepts

Let $C=\{C_1, C_2, \ldots, C_n\}$ be a known set of concepts, i.e. variables used in the model. According to [11], each concept $C_i \in C$ is evaluated with value $A_i \in [0,1]$, that defines the level of the concept and is based on expert opinion. Value A_i is to be obtained as follows.

We will assume each concept $C_i \in C$ to be a linguistic variable [10], that is estimated with value x_i on a universal set, i.e. interval $\left[\underline{x}_i, \overline{x}_i\right]$, where $\underline{x}_i$ ($\overline{x}_i$) is the lower (upper) boundary. We will estimate concept $C_i \in C$ with the use of the fuzzy terms "perfection of concept C_i", that is denoted as PC_i and is a fuzzy set

$$PC_i = \int_{\left[\underline{x}_i, \overline{x}_i\right]} \pi\left(x_i\right)/x_i,$$

where $\pi(x_i)$ is the membership function of variable x_i in the notion of "perfection of concept C_i". Using this function, each absolute estimate $x_i \in \left[\underline{x}_i, \overline{x}_i\right]$ is associated with

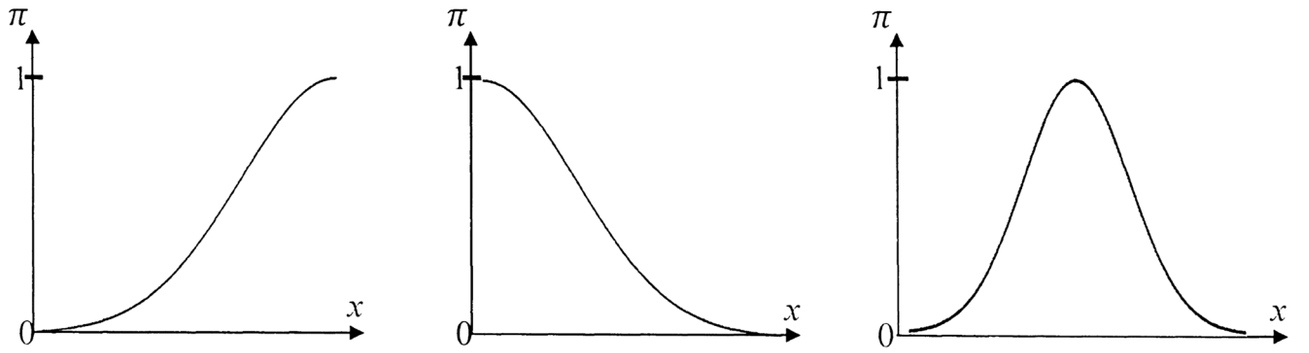


Figure 3 – Membership functions for fuzzy perfection.

1. Introduction

Successful simulation in the context of application tasks is largely defined by the choice of mathematics. The probability theory, that is at the foundation of the classic dependability theory, is poorly adapted to formalizing expert knowledge, that may prove to be useful as part of the decision-making process.

The Aim of the paper is to raise awareness of dependability simulation with fuzzy cognitive maps. It sets forth the primary formulas of the above and further proposes the method of ranking of factors that affect system dependability. The method is illustrated using the example of simulation of dependability and safety of automobiles subject to technical, human-machine system-related, environmental and managerial factors.

2. Structuring: from elements to factors

Dependability simulation of a complex system starts with its structuring, i.e. partitioning into components (blocks, units, elements), for which probabilities of failure are known.

The classical dependability theory [1] uses the concept of structural (logical) function that associates the logical condition of system operability (1, no failure, 0, failure) with the respective conditions for its elements. The transition from the structure function to the probabilistic dependability model is performed according to the rules of probabilistic logic calculation [2]. The structural function allows ranking elements by their importance, which is required for optimal distribution of the resources allocated to ensuring system dependability.

Man-machine systems are structured using the algorithmic description of the operating processes [3, 4]. In this case, the given data for dependability calculation is the probabilities of correct performance of basic, check and diagnostic operations. The rules of transition from logical algorithmic description of a system in the language of algorithmic algebra by V.M. Glushkov [5] to probabilistic and fuzzy dependability models are suggested in [6, 7].

Algorithmic description is a natural method of formalization of systems with discrete processes of operation, e.g. automated data processing and control systems, assembly lines, etc., where the presence of clear boundaries between individual operations allows collecting statistical data on the probabilities of errors that is required for modeling.

Algorithmization is complicated in case of man-machine systems with continuous human activity that is dominated by operations of supervision and decision-making. Examples include control systems of the transportation, chemical and nuclear industries and other high-risk systems, where human errors cause catastrophic consequences.

The absence of clear boundaries between operations prevents a correct estimation of the probability of their correct performance. For that reason the process of operation has to be considered as a single operation, whose correct performance depends on heterogeneous and interconnected human-machine system-related, technical, software-specific, managerial and other factors. The simulated system is a "black box" with unknown structure: output is dependability, inputs are contributing factors. In this case, the conventional problem of the dependability theory – the ranking of elements – becomes a problem of factor ranking. For instance, in [8] it is noted, that the difficulty of taking into account the contributing factors makes it impossible to accurately predict the probability of failure, which undermines the confidence in the dependability calculations.

Regression analysis is the most popular means of multifactor dependability simulation of man-machine systems (see e.g. [9]). It requires a large quantity of experimental data and is not compatible with qualitative factors that are measured by expert methods. The "if – then" fuzzy rules are a convenient tool for expert information processing [10]. Regression analysis and fuzzy rules have a common limitation: they require independent input variables, i.e. contributing factors. Fuzzy cognitive maps (FCM) [10] do not have this restriction. They are a new simulation tool that is not yet widely used in the dependability theory.

Set forth below are the primary FCM formulas and proposed method of ranking the factors that affect system dependability and safety. The method is illustrated with the "driver-automobile-road" system.

3. Primary concepts and formulas

3.1. General observations

FCM were introduced by B. Kosko [11] as a generalization of R. Axelrod's binary cognitive maps [12], intended for simulating the dynamics of the causal relationships

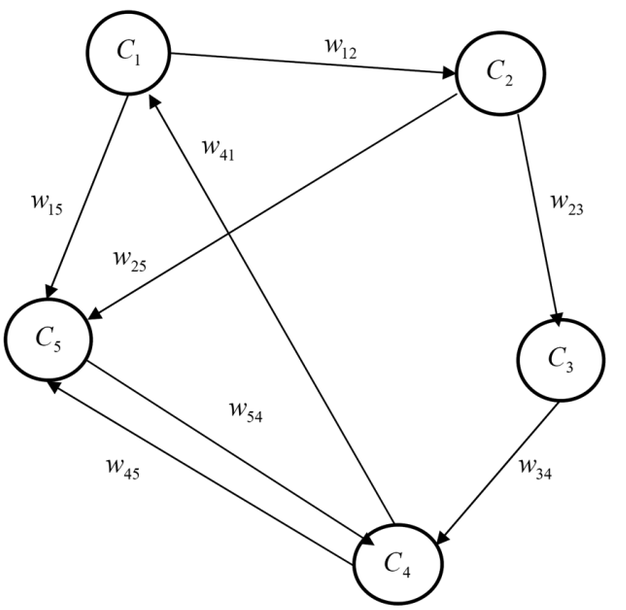


Figure 1 – An example of a fuzzy cognitive map.

Original article
Dependability, vol. 19 no. 4, 2019 https://doi.org/10.21683/1729-2646-2019-19-4-24-31

Fuzzy cognitive maps in the dependability analysis of systems

Alexander P. Rotshtein, *Jerusalem College of Technology – Machon Lev, Jerusalem, Israel; Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine*

Alexander P. Rotshtein

Abstract. Aim. *Dependability simulation of a complex system starts with its structuring, i.e. partitioning into components (blocks, units, elements), for which probabilities of failure are known. The classical dependability theory uses the concept of structural function that allows ranking elements by their importance, which is required for optimal distribution of the resources allocated to ensuring system dependability. Man-machine systems are structured using an algorithmic description of discrete processes of operation, where the presence of clear boundaries between individual operations allows collecting statistical data on the probabilities of error that is required for modeling. Algorithmization is complicated in case of man-machine systems with continuous human activity, where the absence of clear boundaries between operations prevents the correct assessment of the probability of their correct performance. For that reason, the process of operation has to be considered as a single operation, whose correct performance depends on heterogeneous and interconnected human-machine system-related, technical, software-specific, managerial and other factors. The simulated system becomes a "black box" with unknown structure (output is dependability, inputs are contributing factors), while the problem of element ranking typical to the dependability theory comes down to the problem of factor ranking. Regression analysis is one of the most popular means of multifactor dependability simulation of man-machine systems. It requires a large quantity of experimental data and is not compatible with qualitative factors that are measured by expert methods. The "if – then" fuzzy rule is a convenient tool for expert information processing. However, regression analysis and fuzzy rules have a common limitation: they require independent input variables, i.e. contributing factors. Fuzzy cognitive maps do not have this restriction. They are a new simulation tool that is not yet widely used in the dependability theory. The Aim of the paper is to raise awareness of dependability simulation with fuzzy cognitive maps.* **Method.** *It is proposed – based on the theory of fuzzy cognitive maps – to rank factors that affect system dependability. The method is based on the formalization of causal relationships between the contributing factors and the dependability in the form of a fuzzy cognitive map, i.e. directed graph, whose node correspond to the system's dependability and contributing factors, while the weighted edges indicate the magnitude of the factors' effect on each other and the system's dependability. The rank of a factor is defined as an equivalent of the element's importance index per Birnbaum, which, in the probabilistic dependability theory is calculated based on the structure function.* **Results.** *Models and algorithms are proposed for calculation of the importance indexes of single factors and respective effects that affect system dependability represented with a fuzzy cognitive map. The method is exemplified by the dependability and safety of an automobile in the "driver-automobile-road" system subject to the driver's qualification, traffic situation, unit costs of operation, operating conditions, maintenance scheduling, quality of maintenance and repair, quality of automobile design, quality of operational materials and spare parts, as well as storage conditions.* **Conclusions.** *The advantages of the method include: a) use of available expert information with no collection and processing statistical data; b) capability to take into account any quantitative and qualitative factors associated with people, technology, software, quality of service, operating conditions, etc.; c) ease of expansion of the number of considered factors through the introduction of additional nodes and edges of the cognitive map graph. The method can be applied to complex systems with fuzzy structures, whose dependability strongly depends on interrelated factors that are measured by means of expert methods.*

Keywords: *fuzzy cognitive map, system dependability, contributing factors, factor ranking, dependability and safety of automobiles.*

For citation: *Rotshtein AP. Fuzzy cognitive maps in the dependability analysis of systems. Dependability 2019; 4: 24-31 p. https://doi.org/10.21683/1729-2646-2019-19-4-24-31*

Received on 13.04.2019 / Revised on 22.09.2019 / For printing 14.12.2019

[2] Kuvashov YA, Novozhilov EO. Method of evaluation of the railway track's availability for traffic operations. Dependability 2017;17(2):17-23.

[3] Semenov SS, Poltavsky AV, Maklakov VV, Krianev AV. Overview of decision-making techniques used in the development of complex engineering systems. Dependability 2014;3:85-96.

[4] Gapanovich VA, Shubinsky IB, Rozenberg EN, Zamyshlyaev AM. System of adaptive management of railway transport infrastructure technical maintenance (URRAN project). Dependability 2015;2:14-22.

[5] Rudenko YuN**.** O podkhodakh k normirovaniyu pokazateley nadezhnosti elektrosnabzheniya potrebiteley [On the approaches to the standardization of the dependability indicators of electric power supply to consumers]. Proceedings of the Academy of Sciences of the USSR. Energy and transportation 1975;1:14-23 [in Russian].

[6] Litvinenko RS, Pavlov PP, Idiyatullin RG. Practical application of continuous distribution laws in the theory of reliability of technical systems. Dependability 2016;16(4):17-23.

[7] David H. Order statistics. Moscow: Nauka; 1979.

[8] Vadzinsky RN. Spravochnik po veroyatnostnym raspredeleniyam [Handbook of probability distribution]. Saint Petersburg: Nauka; 2001 [in Russian].

[9] Sikan AV. Metody statisticheskoy obrabotki gidrometeorologicheskoy informatsii [Methods of statistical processing of hydrometeorological information]. Saint Petersburg: RSHU; 2007 [in Russian].

[10] Gusev AS. Soprotivlenie ustalosti i zhivuchesti konstruktsiy pri sluchaynykh nagruzkakh [Fatigue strength and survivability of structures under random load]. Moscow: Mashinostroenie; 1989 [in Russian].

About the authors

Igor B. Shubinsky, Doctor of Engineering, Professor, Deputy Director of Integrated Research and Development Unit, JSC NIIAS, Moscow, Russian Federation, phone: +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

Evgeny O. Novozhilov, Candidate of Engineering, Head of Unit, JSC NIIAS, Moscow, Russian Federation, phone: +7 495 967 77 02, e-mail: eo.novozhilov@vniias.ru

The authors' contribution

Igor B. Shubinsky reviewed and analyzed the state of the art of the problem under consideration, defined the theoretical aspects of the paper, applied mathematical methods.

Evgeny O. Novozhilov analyzed the existing approaches to the normalization of dependability indicators. He proposed an algorithm of dependability indicators normalization, performed an example calculation.

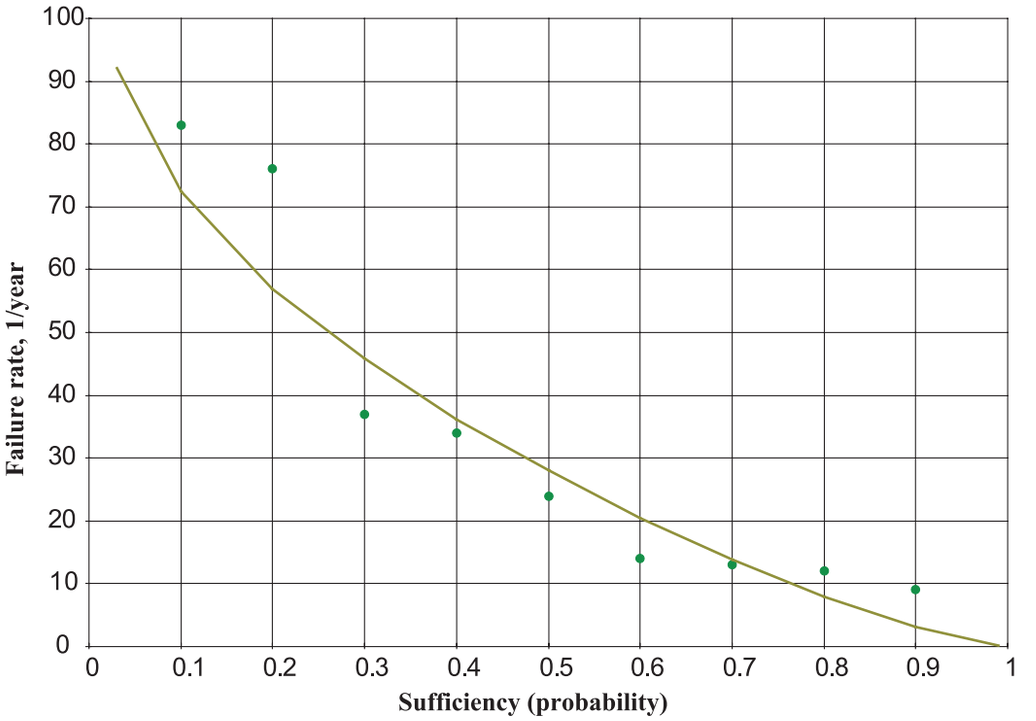


Figure 4. Graph of an empirical series (points) and approximation function (solid line).

4. Choice and justification of a normative indicator value

The results of sufficiency estimation obtained above (see Table 3) can be applied for defining a threshold value x_η for a specified level of risk Q_η agreed between a supplier and a user of a service or vice versa for estimating risk Q_η based on a specified value x_η.

Let us consider a case when for a specified risk level of noncompliance with a normative value (for example, $Q_\eta = 0.1$) we have to define a normative value x_η of a dependability indicator (in our case it is a facility's failure rate).

Let us estimate the quantile of a sufficiency function that corresponds to a specified risk ($q_i = Q_\eta = 0.1$). According to the data of Table 3 we have:

$$y(Q_\eta) = y(q_1 = 0.1) = 70.8 \approx 71.$$

Therefore, as an indicator's normative value we can take a failure rate equal to 71 1/year, which will be not ensured with a risk of 0.1.

In case if by agreement between a supplier and a user of a service there is a specified normative value of dependability, in a similar way based on the obtained results of sufficiency estimation (see Table 3) one can define risk of noncompliance of an indicator with specified requirements.

In any case an agreement between a supplier and a user of a service shall foresee both the specification of a normative value of all dependability indicators in question and the specification of risk levels for nonfulfillment of these normative values as well as the procedure of splitting of responsibility between a supplier and a user of a service.

The method considered in the paper allows defining a relation between a value of a dependability normative indicator and a risk of its nonfulfillment by objective criteria based on factual capabilities of operated facilities that are estimated as per existing statistical data for the past periods.

Conclusions

The paper has considered a method of normalization of a dependability indicator based on statistical data assuming that in general this indicator may be evaluated for a certain period of observance as acceptable for a service user.

For to choose and justify the normalized value of a dependability indicator, the authors have studied the relations between a service supplier and a service user, have analyzed statistics using the method of estimation of empirical sufficiency of a raw data series as well as approximation of an ordered initial series by a three-parameter gamma distribution. The paper provides an example of normalizing a value of a facility failure rate indicator as per the criterion of a specified risk of its violation based on the quantiles of an obtained function of sufficiency.

The research has demonstrated that the proposed approach allows establishing a correlation between a normalized value and a risk of its violation via a function of sufficiency, which can be obtained on the basis of existing statistical data on a facility's dependability for the past periods. This correlation makes it possible to guarantee the ensuring of compliance of factual and normalized indicator values with a specified risk level for a facility working in normal mode.

References

[1] Dolganov AI, Sakharov AV. On the assignment of dependability level. Dependability 2018;18(3):18-21.

Table 1. Initial time series of a facility's failure rate

Observance year	2008	2009	2010	2011	2012	2013	2014	2015	2016
Failure rate, x_i, 1/year	34	37	24	17	12	9	13	43	36

Table 2. Ranked time series with scarcity estimates and modulus coefficients

Item No., i	1	2	3	4	5	6	7	8	9
Failure rate, x_i, 1/year	83	76	37	34	24	14	13	12	9
Mod. coeff., k_i	2.4735	2.2649	1.1026	1.0132	0.7152	0.4172	0.3874	0.3576	0.2682
Scarcity, q_i	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9

Table 3. Example of an approximated time series with scarcity estimates and modulus coefficients (C_v = 0.8 и C_{sv} = 1.4)

Item No., i	-	-	1	2	3	4	5	6	7	8	9	-	-
q_i	0.01	0.05	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95	0.99
Mod. coeff., m_i	2.01	1.8	1.66	1.47	1.31	1.16	1.01	0.855	0.69	0.511	0.305	0.182	0.055
Failure rate, y_i, 1/year	50.25	45	41.5	36.75	32.75	29	25.25	21.38	17.25	12.78	7.625	4.55	1.375

Let us consider the algorithm comprising the ranking of an initial time series, the estimation of its empirical sufficiency and the approximation by a theoretical distribution law using the statistical data on failures of primary railway telecommunications network facilities for the years of 2008–2016 (Table 1, the data submitted by the Central telecommunications station – JSC RZD branch).

1) An initial series is ranked in order of descending of an indicator's values. Instead of observance years we introduce conditional numbers of a ranked series' members (1, 2, 3, …).

2) For each member of a ranked series we calculate values q_i of scarcity function using formula (1).

3) Then we calculate mathematical expectation $\overline{x}$ of series members.

4) For each member of a ranked series we calculate a modulus coefficient equal to a relation of a series member's value to a series' mathematical expectation.

As a result, we have Table 2.

5) For refinement of values of distribution quantiles (q), especially at levels lower than 0.2, that are of practical interest, we make approximation of a series (Table 2) using one of the theoretical distribution laws. As an example, let us consider approximation by a three-parameter gamma distribution [8] that has been in particular applied in hydrological calculations [9], calculations of construction resources for random flows of loads [10] and calculations of structures' service life under random load flows [11].

Using modulus coefficients k_i from Table 2 we calculate the coefficient C_v of series variation and relation C_{sv} of a series' asymmetry coefficient to a series' variation coefficient:

$$C_v = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(\frac{x_i}{\overline{x}}-1\right)^2}, \; C_{sv} = \frac{n\sum_{l=1}^{L}\left(\frac{x_i}{\overline{x}}-1\right)^3}{(n-1)(n-2)C_v^4}, \quad (2)$$

Where if in (2) we obtain the value $C_v < 0.1$, then before calculating C_{sv}, as well as for further usage, we assume that $C_v = 0.1$ (as for series with a very small variation it is complicated to define distribution quantiles). After calculation the value C_v is approximated to multiplicity 0.1 (0.1; 0.2; 0.3 …), while the value C_{sv} is approximated to multiplicity 0.5 (0; ±0.5; ±1.0; ±1.5; …) to allow the application of existing table distribution function values since their analytical calculation is very complicated.

Using table values of three-parameter gamma distribution functions [9] for a specified scarcity probability q_i, we define the ordinate m_i in form of a modulus coefficient (the mentioned tables contain values of a distribution functions for various values C_v and most widely-spread relations C_s / C_v).

In the example in question for values $C_v = 0.5$ and $C_{sv} = 0$ obtained using formulas (2), we have a series of values of function ordinates as modulus coefficients $m_i(p_i)$, including additional values at the boundaries of a function (Table 3). In order to obtain quantitative values y_i of failure rate that will be exceeded with the probability q_i, we should multiply modulus coefficients m_i by the value $\overline{x}$ of mathematical expectation of a ranked series from Table 2 (the results are summarized in Table 3).

The estimation of approximation reliability was made using a coefficient of an empirical linear correlation $x_i(q_i)$ and a function chosen as per this method $y_i(q_i)$ (for i = 1…9). We obtained the value of a linear correlation coefficient as 0.974, which is close to 1, thus confirming the closeness of the chosen function to the initial series with a high reliability.

Fig. 4 present a graph of an empirical series (points) and an approximating function of a three-parameter gamma distribution (solid line).

is "unacceptance region", and that between x_α and x_β is "uncertainty region".

Note that the application of two points (x_α, x_β) as threshold values is a general practice for a sequential selective test [5], where a conclusion on usability (or non-usability) of a batch is made on the basis of a defective items share in a selection that is a part of a batch volume. For this process, acceptable and unacceptable levels are set using confident intervals. A probability that a share of defective items in the whole batch is not larger than x_α, when an upper confident interval of an unacceptable level is exceeded for a selection test, is a supplier's risk; vice versa, a probability that a share of defective items in the whole batch is larger than x_β, when a lower confident interval of an acceptable level is reached for a selection test, is a user's risk.

From Fig. 3 it follows that a service supplier can guarantee that the factual value x of an indicator will be above the threshold value x_α with a high degree of confidence (probability), for example, $P_\alpha = P\{x > x_\alpha\} > 0.95$ (supplier's risk $Q_\alpha = 1 - P_\alpha \le 0.05$ (GOST R ISO 8422-2011. Statistical methods. Sequential plans of selective tests as per alternative attribute); a service user expects that the factual value x of an indicator will not be higher than the threshold value x_β with a high degree of confidence (probability), for example, $P_\beta = P\{x \le x_\beta\} > 0.9$ (user's risk $Q_\beta = 1 - P_\beta \le 0.1$).

Under the real conditions of a technical system's operation, the task of evaluating its compliance with specified requirements of dependability is often brought down to comparison of the value of a factual dependability indicator obtained for some period of observance of statistical operational data with a normative value specified in technical or other documentation. In this case the presence of "uncertainty region" will complicate estimation making it ambiguous. That's why technical documentation for a facility generally contains a normative value of an indicator in form of a single threshold value (for example, "mean time to failure shall be not lower than 30 000 h, maintenance inclusive).

Let a single threshold value normative value x_η be specified for a facility dependability indicator by agreement between a user and a supplier, then we will assume that for $x \le x_\eta$ this facility complies with the requirements, and for $x > x_\eta$ it does not. It is obvious (see Fig. 3) that when transiting from two threshold levels to one it is reasonable to comply with the condition $x_\alpha < x_\eta \le x_\beta$ (x_η belongs to the area of "compromise values"), in which case the normative value x_η for the attribute x satisfies to the requirements of both a service user and a service supplier.

In the case of a single threshold value, the risk $Q_\eta = P\{x > x_\eta\}$ of noncompliance of an indicator with specified requirements is in fact split between a user and a supplier of a service according to their agreement (for example, th exceedance of a normative value at one interval of observance is a user's risk, while at two or more consecutive intervals of observance it is the responsibility of a supplier).

One of the ways of normalizing dependability indicators used in the global practice (in particular, in the power supply field) is the normalization based on past experience (analysis of factual data on dependability) [5]. Given the availability of such data on railway transport, we will consider a further task as a choice and justification of the value x_η using existing statistical data on the operation of a facility during some interval of observance, assuming that in general these indicators of a facility's dependability may be evaluated for this interval of observance as acceptable for a service user.

3. Analysis of statistical data and evaluation of their sufficiency

As it was noted earlier, the factual values of dependability indicators are random values. For example, for a facility's failure rate (number of failures per time unit) the statistics presents a time series of discrete values – for instance, this is a sequence of failure rate values per each annual interval of observance for several years.

A random value is fully defined by a distribution law, for discrete values this is a distribution series or a discrete distribution function. A distribution series (a discrete distribution function) presents a table of possible values of a random size with respective probabilities.

There are a great number of various theoretical laws of distribution (uniform, Bernoulli, Cauchy, Poisson, normal, lognormal, Gumbel, Jonson, 13 Pearson's curved distributions etc.) [6]. However, in practice one often deals with statistical material of rather a limited volume, and it is not always possible to identify a concrete distribution law for a random value based on this volume. In such cases it is necessary to describe the behaviour of a random value by numeric characteristics.

For engineering calculations and scientific researches one uses empirical curved distributions of random values characteristics. When constructing such curves, major stages are ranking of an initial time series and estimation of its empirical sufficiency. Solving the first of these tasks presents no difficulties, whereas for the second it is necessary to take into account that some formulas for estimation of sufficiency lead to systematic errors and give different values of random errors.

Scarcity function $q(x)$ is an analog of distribution function $F(x)$ and characterizes a probability that the value of an argument exceeds a specified threshold value. [7] based on theoretical researches and results of testing defined a formula, which gives efficient, nonbiased and effective values of scarcity estimates of the i-th ($i = 1 \ldots n$) member of a discrete sample ranked in descending order (i.e., of probabilities q_i that the factual value x exceeds the value of x_i series member):

$$q_i = P\{x > x_i\} = \frac{i}{n+1}, \quad (1)$$

Where n is a number of series members.

resource limits, it is vital to identify most "problematic" facilities that require primary investments.

Figures 1 a and 1 b show an example of determination of priority levels of railway infrastructure facilities requiring the enhancement of dependability – for example, by assignment and execution of repair – for two enterprise units, where facilities of one type are under different operation conditions. In this example we assume that in these two enterprise units there are funds reserved for repair of 6 facilities.

Figure 1 shows that based on factual values of a dependability indicator (for example, a failure rate), that reflects the current state of the facility in operation, we can identify those facilities that require repair assignment as a priority with the size of an allocated investment taken into account. In this case, if normative values are not available, facilities are chosen by the criterion of the worst indicator value.

When introducing normalization of indicators one should take into account non-similar maintenance conditions for facilities in different enterprise units, which are determined by differences in climatic factors, technical capabilities for maintenance and repair, staffing levels, grades of tear and wear of facilities, requirements for their productivity (for example, with different sizes of train traffic). In this case facilities will be chosen for repair assignment by the criterion of an indicator's deviation to the worse side from a normative value (Fig. 2 a и 2 b).

Obviously, introduction of normative indicators considering operation conditions and other factors of enterprise units' activities improves targeted investment allocation for maintenance of facilities, which allows fulfilling the requirement of uninterruptible transportation under the conditions of resource scarcity [4].

2. User and supplier interests

In case when a technical system is involved in providing services (for example, a railway infrastructure facility ensures transportation process execution), normative values of dependability indicators shall consider relations between a supplier and a user of a service (for example, an enterprise unit in charge of the functioning of a railway infrastructure facility and an enterprise unit executing transportation process).

It is worth to note that this scheme presents an inevitable conflict between the interests of a user and a supplier of a service. From the one hand, a user is interested that there would not be any failures of a facility providing a service at all; this would allow him to execute his activities with no risk related to a facility failure (for example, a risk of train hours loss due to the failure of a railway infrastructure facility). From the other hand, a supplier is interested in reducing the costs of a service, thus increasing the operating profit, but a reduction of costs inevitably causes increased failure rates. Normalization of a facility's dependability indicators shall in essence ensure a compromise between the interests of a supplier who seeks to provide a service under the conditions of resource limits and the interests of a user who seeks to have a service of high quality with the lowest expenditures.

The situation in question is similar to the situation when a user receives a product batch from a supplier and where the unambiguity of mutual acknowledgment of a product's quality by a supplier and a user is in most cases regulated by methods of statistical acceptance tests. And the relations between a supplier and a user characterize an acceptable level of quality x_α (the maximum acceptable value of defective items share in a batch) and an unacceptable quality level x_β (the boundary of defective items share for attributing a batch as defective), where $x_\alpha \le x_\beta$ (Fig. 3). Therefore, the area of a user's interests is $x \le x_\beta$, and the area of a supplier's interests is $x > x_\alpha$; it is obvious that the two areas cross each other that being a prerequisite condition for the existence of compromise between both interests. The area of an attribute value x under x_α is "acceptance region", that above x_β

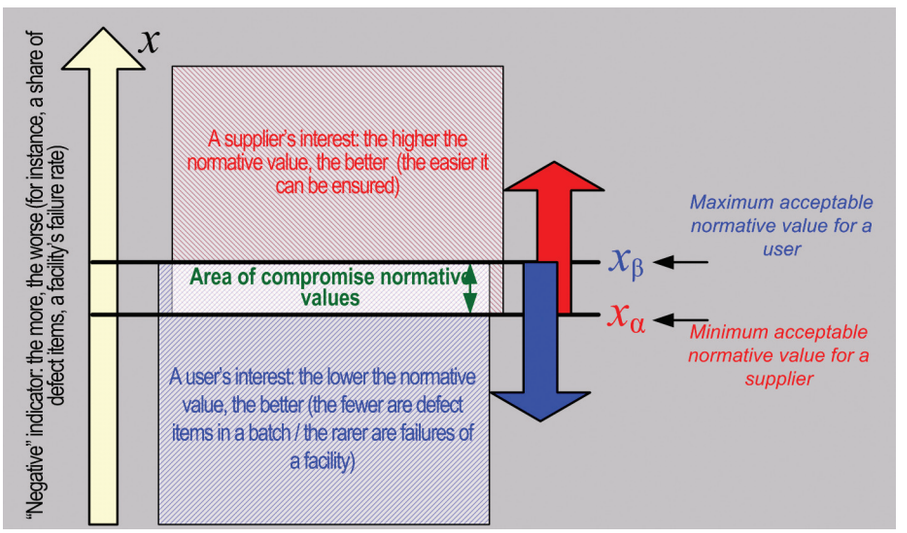


Figure 3. Areas of a service user's and a service supplier's interests.

Introduction

For any technical system one of the important tasks is the normalization of dependability indicators (for example, acceptable value of availability, reliability and maintainability) [1, 2]. Dependability normalization is the specification (in technical or other documentation) of quantitative or qualitative requirements for dependability. Therefore, normalization sets acceptable limits for changes of a controlled characteristic.

A dependability indicator is a characteristic (as a rule, quantitative) of one or several properties comprising the dependability of a technical system (facility). The values of dependability indicators can be normative or factual. They can be determined by calculation methods, on the basis of maintenance data or by extrapolation. Factual values of dependability indicators during the process of operation of a technical system are obtained based on the analysis of statistical data on a system's failures and time to its recovery.

As far as normative values of dependability indicators, they are as a rule specified in a quantitative way at the design stage of a facility. For most facilities one applies a normalization probabilistic approach when one normalizes and ensures a required economically justified level of probabilistic dependability indicators that is afterwards controlled by dependability tests and kept by a maintenance system. The exclusion is safety critical facilities with catastrophic failure consequences, whose failures are not acceptable (this paper doesn't consider such facilities since they belong to the field of functional safety).

1. The goal of normalization of dependability indicators

The results of evaluation of a technical facility's factual state allow making a decision [3] on a further life (operation continuation, maintenance assignment, decommissioning and a facility's replacement etc.). Under the conditions of

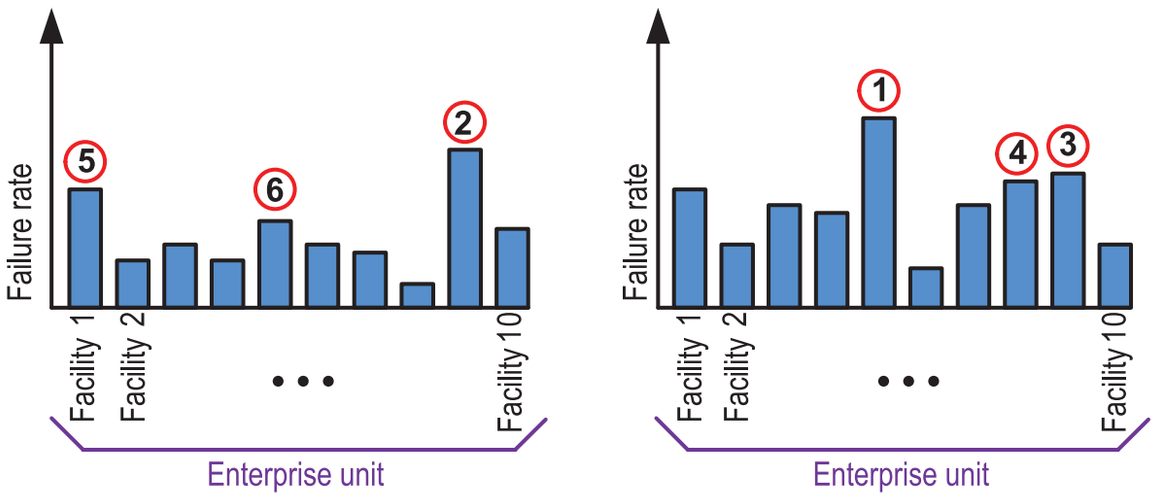


Figure 1. Example of determination of facilities' order of priority for repair assignment (without normalization).

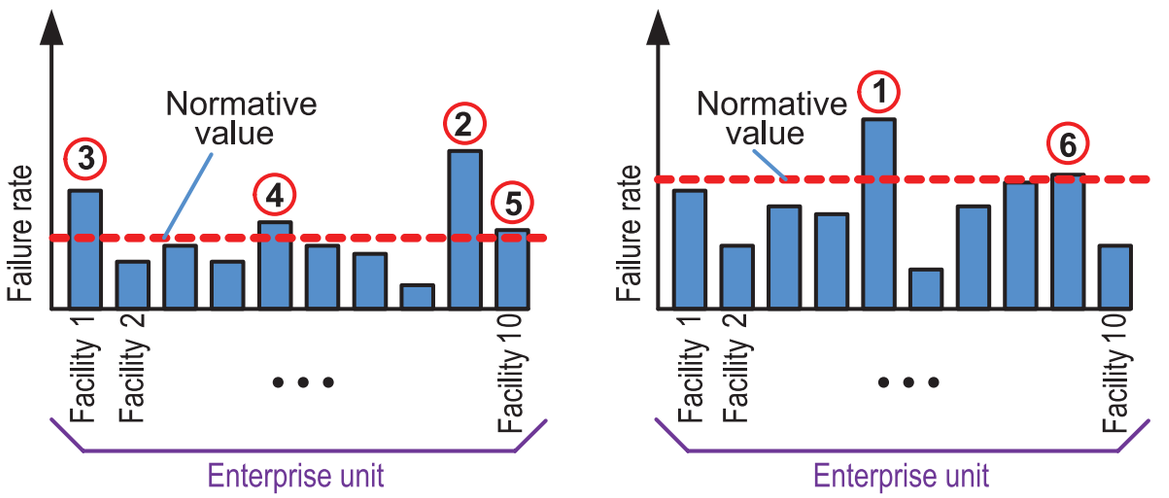
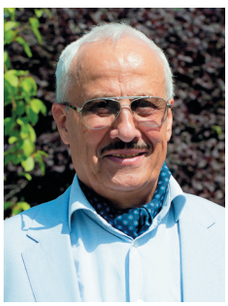


Figure 2. Example of determination of facilities' order of priority for repair assignment (with normalization).

Original article
https://doi.org/10.21683/1729-2646-2019-19-4-17-23

Method of normalization of dependability indicators of railway transport facilities

Igor B. Shubinsky[1], **Evgeny O. Novozhilov**[1*]
[1]*JSC NIIAS, Russian Federation, Moscow*
[*]*eo.novozhilov@vniias.ru*


Igor B. Shubinsky


Evgeny O. Novozhilov

Abstract. Aim. *The results of evaluation of a technical system's (facility's) factual state allow making a decision on a further life (operation continuation, maintenance assignment, decommissioning and a facility's replacement etc.). Under the conditions of resource limits, it is vital to identify most "problematic" facilities that require primary investments. The aim of the research is to develop a method of normalization of dependability indicators whose application is intended to improve targeted investment allocation for maintenance of facilities, which allows fulfilling the requirement of uninterruptible transportation under the conditions of resource scarcity.* **Methods.** *The research uses methods of system analysis, probability theory, mathematical statistics, and correlation analysis. It proposes approximation of a time series of factual values related to a dependability indicator by a three-parameter gamma distribution based on a scarcity function q(x).* **Findings.** *The research has considered the criteria of choice of railway transport facilities requiring the enhancement of dependability for the cases of unavailability and availability of a normalized dependability indicator. It has been shown that if introducing normalization of indicators one should take into account non-similar maintenance conditions for facilities in different enterprise units, which are determined by differences in climatic factors, technical capabilities for maintenance and repair, staffing levels, grades of tear and wear of facilities, requirements for their productivity. The research has analyzed the conditions of association of a service supplier's and user's requirements for normalization of a dependability indicator value. It has been demonstrated that it is reasonable to establish a single threshold normalized value x of a dependability indicator, in which case a normalized value x for the attribute x shall comply with the requirements of a service user as well as a service supplier. In the case of a single threshold value, the risk $Q = P\{x > x\}$ of noncompliance of an indicator with the specified requirements is in fact split between a service user and a service supplier according to their agreement.* **Conclusions.** *The paper proposes a method of normalization of a dependability indicator based on statistical data assuming that in general this indicator may be evaluated for a certain period of observance as acceptable for a service user. For to choose and justify the normalized value of a dependability indicator, the authors have studied the relations between a service supplier and a service user, have analyzed statistics using the method of estimation of empirical sufficiency of a raw data series as well as approximation of an ordered initial series by a three-parameter gamma distribution. The paper provides an example of normalizing a value of a facility failure rate indicator as per the criterion of a specified risk of its violation based on the quantiles of an obtained function of sufficiency. It has been shown that the proposed approach allows establishing a correlation between a normalized value and a risk of its violation via a function of sufficiency, which can be obtained on the basis of existing statistical data on a facility's dependability for the past periods. This correlation makes it possible to guarantee the ensuring of compliance of factual and normalized indicator values with a specified risk level for a facility working in normal mode.*

Keywords: *dependability indicator, dependability normalization, service supplier's risk, service user's risk, scarcity function, three-parameter gamma distribution, distribution quantile.*

For citation: *Shubinsky IB, Novozhilov EO. Method of normalization of dependability indicators of railway transport facilities // Dependability 2019;4; 17-23 p. https://doi.org/10.21683/1729-2646-2019-17-23.*

Received on 02.10.2019 / Revised on 22.11.2019 / For printing 14.12.2019

nadezhnosti [Processes and strategies of restoration with ramp distribution functions in the dependability theory]. Krasnoyarsk: SFU; 2016 [in Russian].

[4] Vaynshteyn II, Vaynshteyn VI, Veysov EA. O modelyakh protsessov vosstanovleniya v teorii nadezhnosti [On the models of restoration processes in the dependability theory]. In: Polovinkin VI, editor. Voprosy matematicheskogo analiza: sb. nauch. tr. Vyp. 6 [Matters of mathematical analysis: a collection of research papers. Vol. 6]. Krasnoyarsk: IPTs KGTU; 2003 [in Russian].https://elibrary.ru/author_items.asp?refid=535409857&fam=%D0%92%D0%B0%D0%B9%D0%BD%D1%88%D1%82%D0%B5%D0%B9%D0%BD&init=%D0%98+%D0%98https://elibrary.ru/author_items.asp?refid=535409857&fam=%D0%92%D0%B0%D0%B9%D0%BD%D1%88%D1%82%D0%B5%D0%B9%D0%BD&init=%D0%92+%D0%98 https://elibrary.ru/author_items.asp?refid=535409857&fam=%D0%92%D0%B5%D0%B9%D1%81%D0%BE%D0%B2&init=%D0%95+%D0%90

[5] Bulinskaya EV, Sokolova AI. Asimptoticheskoe povedenie nekotorykh stokhasticheskikh sistem khraneniya [Asymptotic behaviour of some stochastic storage systems]. Sovremennye problemy matematiki i mekhaniki; 2015. p. 37-62 [in Russian]. https://elibrary.ru/author_items.asp?refid=376420328&fam=%D0%91%D1%83%D0%BB%D0%B8%D0%BD%D1%81%D0%BA%D0%B0%D1%8F&init=%D0%95+%D0%92 https://elibrary.ru/author_items.asp?refid=376420328&fam=%D0%A1%D0%BE%D0%BA%D0%BE%D0%BB%D0%BE%D0%B2%D0%B0&init=%D0%90+%D0%98

[6] Ankudinov AV, Antonov AV, Chepurko VA. Renewal equation for Kijima-Sumita processes. Dependability 2018;18(2):3-9.

[7] Chumakov IA, Antonov AV, Chepurko VA. On some properties of Kijima incomplete restoration models. Dependability 2015;3(54):10-15.

[8] Pereguda AI, Pereguda AA, Timashev DA. The mathematical model of computer networks' reliability. Dependability 2013;(4):31-43.

[9] Vaynshteyn II, Vaynshteyn VI. Dispersiya chisla otkazov v modelyakh protsessov vosstanovleniya tekhnicheskikh i informatsionnykh sistem. Optimizatsionnye zadachi [Dispersion of failure numbers in restoration process models of technical and information technology systems]. Modeling, optimization and information technology 2019; 7(3) [in Russian].

[10] Litvinenko RS, Pavlov PP, Idiyatullin RG. Practical application of continuous distribution laws in the theory of reliability of technical systems. Dependability 2016;16(4):17-23.

[11] Vaynshteyn VI, Veysov EA, Shmidt OO. Chislennoe nakhozhdenie funktsii vosstanovleniya dlya odnoy modeli protsessa vosstanovleniya [Numerical method of finding the restoration function for one restoration process model]. Novosibirsk: Vychislitelnye tekhnologii 2005;10:4-9 [in Russian].https://elibrary.ru/author_items.asp?refid=535409856&fam=%D0%92%D0%B0%D0%B9%D0%BD%D1%88%D1%82%D0%B5%D0%B9%D0%BD&init=%D0%92+%D0%98https://elibrary.ru/author_items.asp?refid=535409856&fam=%D0%92%D0%B5%D0%B9%D1%81%D0%BE%D0%B2&init=%D0%95+%D0%90https://elibrary.ru/author_items.asp?refid=535409856&fam=%D0%A8%D0%BC%D0%B8%D0%B4%D1%82&init=%D0%9E+%D0%9E https://elibrary.ru/contents.asp?titleid=8610

[12] Vaynshteyn VI. Recovery functions of elements of technical systems which operation time distribution is a mixture of n functions distributions. Modern High Technologies 2018;6:44-49 [in Russian].https://elibrary.ru/item.asp?id=35197333https://elibrary.ru/author_items.asp?refid=535409856&fam=%D0%92%D0%B0%D0%B9%D0%BD%D1%88%D1%82%D0%B5%D0%B9%D0%BD&init=%D0%92+%D0%98

[13] Markowitz HM. Portfolio Selection. Journal of Finance 1952;7(1):71-91.

[14] Kasimov YuF. Osnovy teorii optimalnogo portfelya tsennykh bumag [Fundamentals of the theory of an optimal investment portfolio]. Moscow: Filin; 1998 [in Russian].

About the author

Vitaly I. Vaynshteyn, Candidate of Physics and Mathematics, Siberian Federal University, Associate Professor, Head of Laboratory for Information Security, Department of Applied Mathematics and Computer Security, Russian Federation, Krasnoyarsk Krai, Krasnoyarsk, e-mail: vit037@mail.ru

The author's contribution

The paper sets forth a formula for the dispersion of the number of failures of the general restoration process and formula for the dispersion of the number of failures and number of restorations under an alternating restoration process. An algorithm for obtaining the dispersion of the number of failures in the form of series for the laws of operation time distribution common to the dependability theory.

failures occur, while at moments

$$S_1 = X_1 + Y_1, S_2 = X_1 + Y_1 + X_2 + Y_2, \ldots,$$
$$S_n = X_1 + Y_1 + X_2 + Y_2 + \cdots + X_n + Y_n, \ldots$$

restorations end.

The times between failures (accounting for the restoration time) form the general restoration process that is defined by the first $F(t)$ and second $(F*G)(t)$ distribution functions. The times between restorations form a simple restoration process with distribution function $(F*G)(t)$ [2, 3].

The average number of failures and average number of restorations are defined by the restoration functions $H_0(t) = HF(F*G)(t)$, $H_1(t) = H(F*G)(t)$ respectively.

Let $D_0(t)$ be the failure number dispersion, and $D_1(t)$ be the restoration number dispersion. In accordance with (4, 5), let us write the formulas for dispersions

$$D_0(t) = 2\int_0^t H(F*G)(t-x)dHF(F*G)(x) + H_0(t) - H_0^2(t),$$

$$D_1(t) = 2\int_0^t H(F*G)(t-x)dH(F*G)(x) + H_1(t) - H_1^2(t).$$

Let us note that the value of the restoration function and dispersion of the number of failures enables the solution of various practical problems involving variation coefficients and Chebyshev inequality.

Let us write the variation coefficient $V(N(t))$ and Chebyshev inequality for the restoration process

$$V\left(N\left(t\right)\right) = \frac{\sigma\left(N\left(t\right)\right)}{H\left(t\right)},$$

($\sigma(N(t))$ is the mean square deviation)

$$P(|N(t) - H(t)| \geq \int) \leq \frac{D(N(t))}{\int^2}.$$

Let us examine the simple restoration process under exponential distribution of operation times $F(t)=1-e^{-\alpha t}$. In this case $H(t)=\alpha t$, $D(N(t))=\alpha t$ and

$$V\left(N\left(t\right)\right) = \frac{1}{\sqrt{\alpha t}}.$$

As the time of operation increases, the variation coefficient decreases.

Taking $\int = 3\sqrt{D(N(t))}$ and transitioning to the contrary event in the Chebyshev inequality, we obtain a well-known form of the Chebyshev inequality, that in the case of the restoration process becomes

$$P\left(\left|N\left(t\right) - H\left(t\right)\right| < 3\sqrt{D\left(N\left(t\right)\right)}\right) \geq \frac{8}{9}.$$

For a simple restoration process under exponential distribution of operation times

$$P(|N(t) - \alpha t| < 3\sqrt{\alpha t}) \geq \frac{8}{9}.$$

Conclusion. The operation of technical and information systems, as well as information security software and firmware is associated with failures, threats of attack, safety threats and many other effects, random in their nature, that negatively affect their operation. Such effects cause restoration processes. The number of failures, threats of attack and safety threats are random values that depend on the time and their distribution functions. The variation patterns of such distribution functions cause the variety in the models of restoration process, for which methods have been developed for finding the mathematical expectation (restoration function) of the failure number.

For the general and alternating restoration processes the paper obtained the formula of dispersion that depends on the restoration function of two processes, the simple and the general. It also suggests an algorithm for calculating the restoration function for operation time distribution functions common to the dependability theory. As an example, dispersion expressions were obtained for the simple, general process under an exponential distribution. For that case, a Chebyshev inequality and variation coefficient were written.

Let us note that obtaining the failure number dispersion formulas for other models of restoration process is of interest as well.

The availability of formulas for the average and dispersion of the failure number, as well as accounting for the joint variation of the average and dispersion of the failure number in the process of restoration from the times to failure distribution functions of restorable elements naturally entails the consideration of new optimization problems in restoration processes. For instance, minimization of the failure dispersion under a restricted value of the average failure number in operation leads to a problem that in terms of its definition is similar to the Markowitz problem of optimal investment portfolio [13, 14].

Thus, the mathematics developed in this paper will find their application in the definition and solution of various optimization problems of information and computer security, as well as in the operation of technical, information, socio-economic, biological and other systems when the occurrence of failures is random.

References

[1] Borovkov AA. Teoriya veroyatnostey [Probability theory]. Moscow: Librokom; 2009 [in Russian].https://elibrary.ru/author_items.asp?refid=376420326&fam=%D0%91%D0%BE%D1%80%D0%BE%D0%B2%D0%BA%D0%BE%D0%B2&init=%D0%90+%D0%90

[2] Beichelt F, Franken P. Reliability and Maintenance. Mathematical Methods. Moscow: Radio i sviaz; 1988.

[3] Vaynshteyn II. Protsessy i strategii vosstanovleniya s izmenyayushchimisya funktsiyami raspredeleniya v teorii

An example. Let us write the dispersions for the simple and general processes under an exponential distribution of operation times

$$F_1(t)=(1-e^{-\alpha_1 t}),\quad F_2(t)=(1-e^{-\alpha_2 t}),\alpha_1\neq\alpha_2.$$

Under a simple process, $H(t)=\alpha_1 t$. Upon integration in (4), $D(N(t))=\alpha_1 t$

Under a simple process and exponential distribution of operation times the dispersion matches the restoration function.

Under a general process [3].

$$HF_1F_2(t)=\alpha_2 t+(1-\frac{\alpha_2}{\alpha_1})(1-e^{-\alpha_1 t}).$$

Upon integration in (5),

$$D\left(N(t)\right)=\alpha_2^2 t^2+\frac{2\alpha_2\left(\alpha_1-\alpha_2\right)}{\alpha_1}t-$$

$$-\frac{2\alpha_2\left(\alpha_1-\alpha_2\right)}{\alpha_1^2}\left(1-e^{-\alpha_1 t}\right)+HF_1F_2(t)-H^2F_1F_2(t).$$

For many know distribution laws that are common to the dependability theory [10], for instance, exponential, Weibull-Gnedenko, Erlang, normal, Maxwell, Raileigh, gamma and their combinations, the restoration function is obtained in an explicit form or expressed as power series [2, 3, 11, 12].

In [3, 12], it is noted that the above distribution functions and their combinations are expanded into power series as follows

$$F(t)=\sum_{n=0}^{\infty}a_n t^{\beta n+\gamma},\qquad \gamma\geq 0,\ \beta>0. \tag{6}$$

That enables the development of a single algorithm for finding the restoration function of simple processes formed by the distribution function of type (6), provided that numbers β and γ are whole, non-negative or related as $\gamma=l\beta$, l is whole, non-negative. In this case, the restoration function is defined as the solution of the corresponding integral equation (3), if the solution is sought in the following form:

$$H(t)=\sum_{n=0}^{\infty}c_n t^{\beta n+\gamma}. \tag{7}$$

Coefficients c_n are identified.

In [12], in a similar way restoration functions are found for combinations of the above distribution functions, except for the combination of gamma distributions. Under non-natural values of γ, the condition $\gamma=l\beta$, ($\beta=1$) is not fulfilled.

The obtained formulas include integrals $\int_0^t H_1(t-x)dH_2(x)$ of restoration functions for the purpose of dispersion calculation. Let in accordance with (7)

$$H_i(t)=\sum_{n=0}^{\infty}c_{i,n}t^{\beta_i n+\gamma_i},i=1,2.$$

We have

$$\int_0^t H_1(t-x)dH_2(x)=$$

$$=\int_0^t\Big(\sum_{n=0}^{\infty}c_{1,n}(t-x)^{\beta_1 n+\gamma_1}\sum_{k=0}^{\infty}c_{2,k}(\beta_2 k+\gamma_2)x^{\beta_2 k+\gamma_2-1}\Big)dx=$$

$$=\sum_{k=0}^{\infty}c_{2,k}(\beta_{2,k}+\gamma_2)\sum_{n=0}^{\infty}c_{1,n}\int_0^t(t-x)^{\beta_1 n+\gamma_1}x^{\beta_2,k+\gamma_2-1}\Big)dx=$$

$$=\sum_{k=0}^{\infty}c_{2,k}\left(\beta_2+\gamma_2\right)\sum_{n=0}^{\infty}c_{1,n}t^{(\beta_1 n+\beta_2 k+\gamma_1+\gamma_2)}\cdot$$

$$\cdot\frac{\Gamma\left(\beta_1 n+\gamma_1+1\right)\Gamma\left(\beta_2 k+\gamma_2\right)}{\Gamma\left(\beta_1 n+\beta_2 k+\gamma_1+\gamma_2+1\right)}. \tag{8}$$

The following was taken into consideration:

$$\int_0^t(t-x)^{\alpha}x^{\beta}dx=t^{\alpha+\beta+1}\frac{\Gamma\left(\alpha+1\right)\Gamma\left(\beta+1\right)}{\Gamma\left(\alpha+\beta+2\right)},$$

$\Gamma(x)=\int_0^{\infty}t^{x-1}e^{-t}dt$ is a gamma function.

If $\beta_1=\beta_2=\beta$, then (8) can only arrive to a single infinite sum by replacing $n+k+s$

$$\int_0^t H_1(t-x)dH_2(x)=$$

$$=\sum_{s=0}^{\infty}\frac{t^{\beta s+\gamma_1+\gamma_2}}{\Gamma(\beta s+\gamma_1+\gamma_2+1)}\sum_{n+k=s}c_{1,n}c_{2,k}\Gamma\cdot$$

$$\cdot(\beta n+\gamma_1+1)\Gamma(\beta k+\gamma_2)=$$

$$=\sum_{n=0}^{\infty}\frac{t^{\beta n+\gamma_1+\gamma_2}}{\Gamma(\beta n+\gamma_1+\gamma_2+1)}\sum_{k=0}^{n}c_{2,k}c_{1,n-k}\Gamma\cdot$$

$$\cdot(\beta(n-k)+\gamma_1+1)\Gamma(\beta k+\gamma_2).$$

The definition of the restoration process assumed that the restoration of a failed element happens instantaneously. In practice, this assumption is often false. Along with the time of no-failure, of significant potential importance is the down time, cause of failure identification time and restoration time itself.

Let us examine the so-called simple alternating restoration process [2, 3].

Let (X_n), (Y_n) be two sequences of non-negative, mutually independent, random values each of which forms a simple restoration process with distribution functions $F(t)$, $G(t)$ respectively. Sequence (X_n, Y_n) is called simple alternating restoration process [2, 3].

If Y_n is the time of an element's restoration after the n-th failure, X_n is the element's operation time after the $(n-1)$-th restoration (restoration begins after the first failure), then at moments

$$T_1=X_1,\quad T_2=X_1+Y_1+X_2,\ldots,$$
$$T_n=X_1+Y_1+X_2+\cdots+Y_{n-1}+X_n,\ldots$$

Introduction. Problem definition. A sequence of non-negative, mutually independent, random values X_i with distribution functions $F_i(t)$ is called a restoration process [1-3]. In the reliability theory, in the process of restoration after each failure an element is repaired or replaced (with a restoration element) and X_i is the element's times to failure after the (i–1)-th restoration, $F_i(t)$ is their distribution function.

Depending on the structure of the sequence of distribution functions $F_i(t)$ there are various models of the restoration process [1-8].

Thus, if all random values X_i have the same distribution function $F_1(t)$, $F_i(t)=F_1(t)$, we have a simple restoration process. If $F_i(t)=F_1(t)$, $i\geq 2$, we have a general restoration process.

The restoration process defines the random value $N(t)$, i.e. the number of failures (restorations) over the time from 0 to t

$$P\left(N\left(t\right)=n\right)=F^{(n)}\left(t\right)-F^{(n+1)}\left(t\right), \quad (1)$$

$F^{(n)}(t)$ is the n-fold comparison of distribution functions $F_i(t)$, i=1,2,…,n

$$F^{(n)}(t)=(F^{(n-1)}*F_n)(t)=\int_0^t F^{(n-1)}(t-x)dF_n(x), F^{(1)}(t)=F_1(t).$$

Of significant importance as regards the theoretical and practical problems of the dependability theory is the restoration function $H(t)$, i.e. the mathematical expectation of the number of failures over the time from 0 to t in the process of restoration $H(t)=E(N(t))$

$$H\left(t\right)=\sum_{n=1}^{\infty} nF^{(n)}\left(t\right). \quad (2)$$

Let $HF_1(t)$ be the restoration function of a simple process shaped by the distribution function $F_1(t)$, $HF_1F_2(t)$ be the restoration function of the general process shaped by the first distribution function $F_1(t)$, as well as the second and the subsequent $F_2(t)$.

The restoration function $HF_1(t)$ of a simple process satisfies the integral equation

$$HF_1(t)=F_1(t)+\int_0^t HF_1(t-x)dF_1(x). \quad (3)$$

The restoration function of a general restoration process is expressed through the restoration function of a simple process using formula

$$HF_1F_2(t)=F_1(t)+\int_0^t HF_2(t-x)dF_1(x).$$

For a simple restoration process, the formula for calculating the failure number dispersion is known [2]

$$D(N(t))=2\int_0^t HF_1(t-x)dHF_1(x)+HF_1(t)-H^2F_1(t). \quad (4)$$

Further study aims to obtain the formula for the failure number dispersion under a general restoration process and development of the method of its calculation for various distribution laws for the operation times of replaced failed elements.

Calculation of dispersion for general restoration processes.

By definition

$$D(N(t))=E(N^2(t))-E^2(N(t))=E(N^2(t))-H^2(t).$$

Thus, in order to calculate the dispersion, along with the restoration function $E(N^2(t))$ must be calculated. Let us examine the calculation of $E(N^2(t))$ [9].

Considering (1), (2) we obtain

$$E(N^2(t))=\sum_{n=1}^{\infty} n^2P(N(t)=n)=\sum_{n=1}^{\infty} n^2(F^{(n)}(t)-F^{(n+1)}(t))=$$
$$=F_1(t)+\sum_{n=2}^{\infty}(n^2-(n-1)^2)F^{(n)}(t)=F_1(t)+\sum_{n=2}^{\infty}(2n-1)F^{(n)}(t)=$$
$$=-H(t)+2F_1(t)+2\sum_{n=2}^{\infty} nF^{(n)}(t)=-H\left(t\right)+2\sum_{n=1}^{\infty} nF^{(n)}\left(t\right).$$

Thus, the problem comes down to calculating the sum $\sum_{n=1}^{\infty} nF^{(n)}(t)$ for each model of the restoration process. Further, this sum will be calculated using restoration function formula (2) and definition of the general restoration process. Successively, we obtain

$$\sum_{n=1}^{\infty} nF^{(n)}(t)=F_1(t)+2(F_1*F_2)(t)+3(F_1*F_2^{(2)})(t)+\ldots+$$
$$+n(F_1*F_2^{(n-1)})(t)+\ldots=(F_1(t)+(F_1*F_2)(t)+$$
$$+(F_1*F_2^{(2)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+((F_1*F_2)(t)+$$
$$+(F_1*F_2^{(2)})(t)+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+$$
$$+((F_1*F_2^{(2)})(t)+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+$$
$$+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+\ldots+$$
$$+(F_1*F_2^{(n-1)})(t)+(F_1*F_2^{(n)})(t)+\ldots)=$$
$$+(F_1*F_2^{(3)})(t)+\ldots+(F_1*F_2^{(n-1)})(t)+\ldots)+\ldots+$$
$$6(F_1*F_2^{(n-1)})(t)+(F_1*F_2^{(n)})(t)+\ldots)=(H(t)+$$
$$+(F_1*HF_2)(t)+(F_1*F_2*HF_2)(t)(F_1*F_2*F_2*HF_2)(t)+$$
$$+\ldots+(F_1*(F_2^{(n)}*HF_2)(t)+\ldots)=H(t)+$$
$$+(HF_2*(F_1+(F_1*F_2)(t)+((F_1*F_2*F_2)(t)+\ldots+$$
$$+(F_1*F_2^{(n)})(t)+\ldots))=H\left(t\right)+\left(HF_2*H\right)(t).$$

Here $H(t)=HF_1F_2(t)$. Finally,

$$D(N(t))=2\int_0^t HF_2(t-x)dHF_1F_2(x)+HF_1F_2(t)-(HF_1F_2\left(t\right))^2. \quad (5)$$

Dispersion of the number of failures in restoration processes

Vitaly I. Vaynshteyn, *Siberian Federal University, Russian Federation, 660041, Krasnoyarsk Krai, Krasnoyarsk, 79 pr. Svobodny*

Vitaly I. Vaynshteyn

Abstract. *Optimal organization of the restoration process is of significant importance in the operation of technical, information and computer systems, since failures occurring during their operation lead to substantial negative consequences. In this paper, a formula for the variance of the number of failures is obtained for the general restoration process, which depends on the restoration functions (average number of failures) of the simple and general restoration processes. Also obtained are the formulas for the variances of the number of failures and restorations during the alternating restoration process, when along with the element's time to failure, for example, the restoration time is taken into account. For an exponential distribution with a simple and general restoration process, formulas are written for the variance of the number of failures, as well as the Chebyshev inequality and the formula for the coefficient of variation of the number of failures for a simple restoration process. The paper presents an algorithm for obtaining dispersion in the form of series for the operation time distribution laws common to the dependability theory. The developed mathematics are intended for the definition and solution of various optimization problems of information and computer security, as well as in the operation of technical and information systems, software and formware information protection facilities affected by random failures, threats of attacks and security threats.*

Keywords: *distribution function, restoration process, restoration function, failure number dispersion, variation coefficient.*

For citation: *Vaynshteyn VI. Dispersion of the number of failures in restoration processes. Dependability 2019; 4: 12-16 p. https://doi.org/10.21683/1729-2646-2019-19-4-12-16.*

Received on 03.09.2019 / Revised on 22.10.2019 / For printing 14.12.2019

[9] Filaretov G.F., Chervova A.A. Posledovatelnyy algoritm obnaruzheniya momenta izmeneniya dispersii vremennogo ryada [Sequential algorithm of detection of the moment of change in the temporal series dispersion]. Zavodskaya laboratoriya. Diagnostika materialov 2019;85(3):75-82.

[10] Sivova D.G., Filaretov G.F. Posledovatelnyy algoritm obnaruzheniya momenta izmeneniya kharakteristik vektornykh vremennykh ryadov [Sequential algorithm of detection of the moment of change in a vector temporal sequence characteristics]. Vestnik MEI 2014;2:63-69 [in Russian].

About the authors

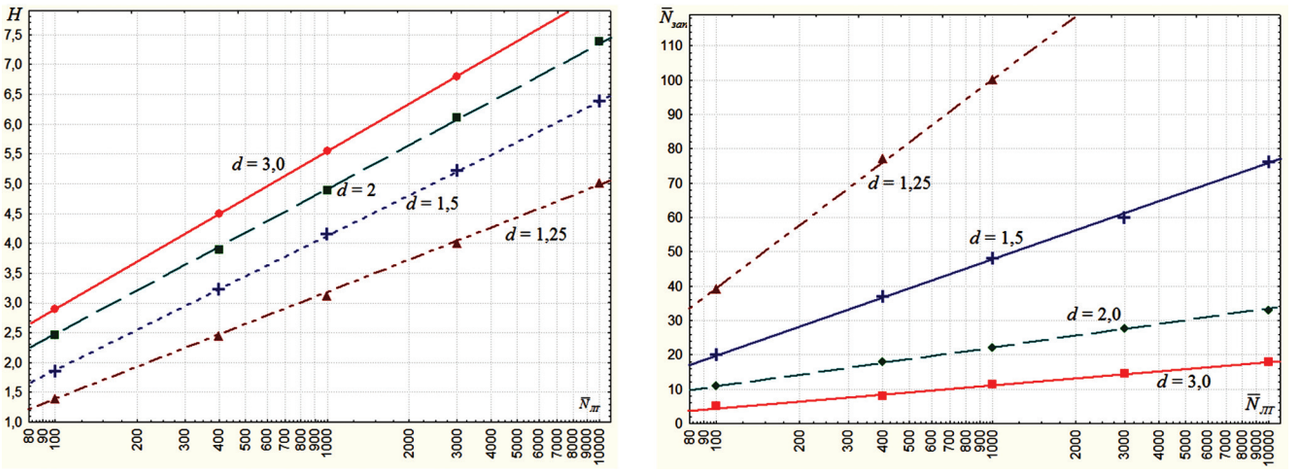
Dmitry S. Repin, Candidate of Engineering, Deputy Director, Institute of Information Technology, Federal State Autonomous Educational Institution for Further Vocational Education Center for Implementation of the National Educational Policy and Information Technology, Moscow, Russian Federation, e-mail: r_d_s@inbox.ru; Mobile: +7 9166659242.

Gennady F. Filaretov, Doctor of Engineering, Professor, Professor of the Department of Control and Computer Science, National Research University Moscow Power Engineering Institute (MPEI), Moscow, Russian Federation, e-mail: gefefi@yandex.ru; Mobile: +7 9255176319.

The authors' contribution

Filaretov G.F. Review and analysis of the state of the art of the problem, theoretical aspect of the paper.

Repin D.S. Development of software tools for the simulation experiment, its performance, processing of the results, acquisition of data required for the synthesis of the control algorithm.



a) b)

Figure 1. The dependence of the decision boundary H (a) and average lag $\overline{N}_{\text{lag}}$ (b) on $\overline{N}_{\text{FA}}$

the simulation, intervals τ_i were considered as values of a discrete time series on value grid i, therefore both the mean time between false alarms and the mean lag were defined as the average number of samples $\overline{N}_{\text{FA}}$ and $\overline{N}_{\text{lag}}$ respectively; the transition from discrete to real time can be easily performed using obvious formulas $\overline{T}_{\text{FA}} = \overline{N}_{\text{FA}} / \theta_0$ and $\overline{T}_{\text{lag}} = \overline{N}_{lag} / \theta_1$.

The simulation helped find the dependences of boundary H from $\overline{N}_{\text{FA}}$ under various d from the typical set d = 1.25; d = 1.5; d = 2.0; d = 3.0, where $d = \theta_1/\theta_0$ and dependences $\overline{N}_{\text{lag}}$ on $\overline{N}_{\text{FA}}$. As it turned out, if such dependences are considered as the function $\log \overline{N}_{\text{FA}}$, they are closely approximated by linear models as follows: $H = a + b \cdot \log \overline{N}_{\text{FA}}$; $\overline{N}_{\text{lag}} = c + d \cdot \log \overline{N}_{\text{FA}}$. The corresponding calculation formulas are shown in Table 1, while the models themselves in graph form are shown in Figures 1 a) and b).

The efficiency indicator E_d of the control procedure can be calculated using the following formula:

$$E(d) = \frac{\overline{T}_{\text{FA}}}{\overline{T}_{\text{lag}}} = \frac{\overline{N}_{\text{FA}} / \theta_0}{\overline{N}_{\text{lag}} / \theta_1} = \frac{\overline{N}_{\text{FA}}}{\overline{N}_{\text{lag}}} \cdot d \qquad (6)$$

Expected values of efficiency indicator E_{d} for various d and $\overline{N}_{\text{FA}}$ are shown in Table 2.

Table 2. Expected values of efficiency indicator Ed

d	$\overline{N}_{\text{FA}}$				
	100	400	1000	3000	10000
1.25	3.2	6.5	12.5	–	–
1.50	7.5	16.2	31.3	75.0	197.4
2.00	18.2	44.4	90.9	165.0	330.0
3.00	60.0	150.0	260.9	620.7	1667.0

It is obvious that, unfortunately, the efficiency of the control procedure for the most practically interesting small values of d and $\overline{N}_{\text{FA}}$ is relatively low.

In conclusion, it can be noted that the above synthesis procedure, in principle, can also be used for cases of gradual (continuous) change of parameter θ. However, the statistical properties of the control procedure will remain unclear. Their definition for the purpose of obtaining the dependences similar to those shown in Table 1 requires quite intensive additional research.

References

[1] Kapur K., Lamberson L. Reliability in engineering design. Moscow: Mir; 1980.

[2] Baranov L.A., Yermolin Yu.A. Dependability of objects with nonstationary failure rate. Dependability 2017;4:3-9.

[3] Brodsky B.E., Darkhovsky B.S. O zadache skoreyshego obnaruzheniya momenta izmeneniya veroyatnostnykh kharakteristik sluchaynoy posledovatelnosti [On the problem of prompt detection of the moment of change of probabilistic characteristics of a random sequence]. Avtomatika i telemekhanika 1983;10:125131 [in Russian].

[4] Nikiforov I.V. Posledovatelnoe obnaruzhenie izmeneniya svoystv vremennykh ryadov [Sequential detection of temporal series property changes]. Moscow: Nauka; 1983 [in Russian].

[5] Page E.S. Continuous inspection schemes. Biometrika 1954;41(1):100-115.

[6] Shafid A. Bibliometric Analysis of EWMA and CUSUM Control Chart Schemes. ITEE Journal 2018;7(2):1-11.

[7] Vorobeychikov S.E., Konev V.V. Kharakteristiki protsedury obnaruzheniya razladki protsessa avtoregressii s neizvestnym raspredeleniem pomekhi [Characteristics of the procedure of detection of imbalance in an autoregression process with unknown noise distribution]. Avtomatika i telemekhanika 1992;3:68-75.

[8] Chernoyarov O.V., Rashitov M.F. Obnaruzhenie razladki gaussovskogo sluchaynogo protsessa s neizvestnoy intensivnostyu. Chast 1 [Detection of imbalance in a Gaussian random process with unknown intensity. Part 1]. In: Proceedings of the international science and technology conference INTERMATIC 2012;3:11-14 [in Russian].

The paper examines the problem of prompt detection of the moment of dependability characteristics variation in a system that consists of a set of homogeneous elements. It is assumed that failures of such elements occur at random moments in time $t_1, t_2, \ldots, t_i\text{-}1, t_i, t_{i+}1, \ldots$ and are a Poisson event flow. As it is known [1], in this case time intervals $\tau_i = t_i - t_i\text{-}1$ follow the exponential distribution of the form

$$f(\tau) = \theta \cdot e^{-\theta\tau}; \theta > 0,\ \tau > 0, \quad (1)$$

where $\theta = 1/T_{mn}$, T_{mn} is the mean time between failures.

Let us assume that in the initial steady state parameter $\theta = \theta_0$. As system elements age (wear out), this parameter will obviously change. The research of such non-steady situations is certainly of significant interest [2]. This paper deals with prompt (real-time) detection of variations of value $\theta > \theta_0$, when such variations become significant. Essentially, this is a well-known problem of detection of the so-called "imbalance" of random processes [3].

According to the classical imbalance problem definition, it is assumed that such imbalance is discontinuous in its nature. In the context of dependability, this definition is hardly realistic. However, it can be considered as a tentative application of this approach in the context of real-time supervision of dependability characteristics of complex systems.

There are quite many known algorithms of imbalance detection [4]. The quality of their operation can be described with a set of such *probabilistic* characteristics as the average value of the time between false alarms $\overline{T}_{FA}$, i.e. the mean time between warnings of imbalance in the absence of such, and mean lag $\overline{T}_{lag}$ in the detection of minimal (expected, maximum allowable, critical) imbalance, when $\theta = \theta_1 > \theta_0$.

As of late, the *cumulative sum algorithm* (CUSUM) proposed by Page back in 1954 [5] has been the most commonly applied. This algorithm, as it was later shown, has certain optimality properties in terms of maximization of the efficiency indicator of detection algorithm $E = \overline{T}_{FA} / \overline{T}_{lag}$. The popularity and considerable capabilities of the algorithm are demonstrated by the bibliometric analysis [6] that shows an exponential growth of the number of associated publications since 1964, as well as examples of various modifications of the original CUSUM algorithm [7-10].

CUSUM is based on a slightly modified sequential Wald analysis. In both cases the likelihood ratio statistic is used in the decision function. In the present case it will take the following form:

$$g_i = \max\{0; g_{i-1} + z_i\},\ i = 1, 2, \ldots;\ g = 0, \quad (2)$$

where

$$z_i = \ln\left[f(\tau_i, \theta_1) / f(\tau_i, \theta_0) \right]. \quad (3)$$

The zero value in formula (2) acts as a sort of an absorbing barrier by not allowing decision function to shift towards the area of negative values.

The decision functions are calculated each time a failure signal arrives. The control procedure lasts until, at a certain step *n,* the following inequality is fulfilled:

$$g_n \geq H, \quad (4)$$

where H is the decision boundary. In this case an imbalance warning is issued. In reality though, there might be no imbalance, i.e. there is a situation of false alarm.

Subject to (1), formula (3) can be specified:

$$z_i = \ln(\theta_1/\theta_0) - (\theta_1 - \theta_0) \cdot \tau_i = \ln d - (d-1) \cdot (\tau_i \cdot \theta_0);$$
$$d = \theta_1 / \theta_0. \quad (4)$$

Let us note that the mathematical expectation z_i is in the general case equal to:

$$M\{z_i\} = \ln d - (d-1)\theta_0 M\{\tau_i\}. \quad (5)$$

That means that, if there is no imbalance, when $M\{\tau_i\}=1/\theta_0$, the mathematical expectation $M\{z_i\}=\ln d-(d-1)<0$, which impedes the growth of the value of the decision function and results in sufficiently high average values of the time of hitting boundary H, i.e. sufficiently high values of $\overline{T}_{FA}$. Under nominal imbalance, when $M\{\tau_i\}=1/\theta_1$, we will have $M\{z_i\}=\ln d-(d-1)/d=\ln d-(1-1/d)$. In this case $M\{z_i\}>0$, which causes a quick increase of the decision function up to the threshold H, the attainment or crossing of which is the indication of imbalance.

A practical application of the algorithm would require an appropriate control procedure to be synthesized. Synthesis is understood as the definition of the decision boundary H based on user-selected values of $\overline{T}_{FA}$, initial base level θ_0 and nominal imbalance $\theta_1 > \theta_0$. Additionally, synthesis normally involves the estimation of the algorithm's speed of action through the calculation of $\overline{T}_{lag}$ and its efficiency E_d for various values of d.

Such calculation must be preceded by finding the general formulas that associate the above characteristic with each other. They are obtained using simulation. In the course of

Table 1. Estimated formulas for the definition of the decision boundary *H* and average lag $\overline{N}_{lag}$.

d	Formula for calculating H	Formula for calculating $\overline{N}_{lag}$
1.25	$H = -2.26 + 1.81 \cdot \log \overline{N}_{FA}$	$\overline{N}_{lag} = -83.01 + 61.17 \cdot \log \overline{N}_{FA}$
1.5	$H = -2.68 + 2.27 \cdot \log \overline{N}_{FA}$	$\overline{N}_{lag} = -35.38 + 27.71 \cdot \log \overline{N}_{FA}$
2.0	$H = -2.12 + 2.31 \cdot \log \overline{N}_{FA}$	$\overline{N}_{lag} = -10.82 + 10.985 \cdot \log \overline{N}_{FA}$
3.0	$H = -2.38 + 2.64 \cdot \log \overline{N}_{FA}$	$\overline{N}_{lag} = -8.62 + 6.64 \cdot \log \overline{N}_{FA}$

Original article
https://doi.org/10.21683/1729-2646-2019-19-4-8-11

Algorithm of prompt detection of dependability characteristics variation

Dmitry S. Repin[1*], Gennady F. Filaretov[2]

[1]Institute of Information Technology, Federal State Autonomous Educational Institution for Further Vocational Education Center for Implementation of the National Educational Policy and Information Technology, Moscow, Russian Federation;
[2]National Research University Moscow Power Engineering Institute (MPEI), Moscow, Russian Federation
[*]r_d_s@inbox.ru


Dmitry S. Repin


Gennady F. Filaretov

Abstract. *The Aim of the paper is to develop an algorithm of prompt detection of the moment of dependability characteristics variation in a system that consists of a set of homogeneous elements, assuming that failures of such elements occur at random moments in time, are a Poisson flow of events and, consequently, the time intervals between them are an exponential probability distribution. In order to solve the problem, it is suggested using one of the classical algorithms of detection of "imbalance" of a discrete random process, i.e. spontaneous change of one of its probabilistic characteristics. As such a characteristic, the exponential distribution parameter* θ *was chosen, that is uniquely associated with the mean time between failures* T_{mn}: $\theta = 1/T_{mn}$. *It is believed that the imbalance consists in the discontinuous variation of parameter* θ *from the initial steady state* $\theta = \theta_0$ *to the level of minimal (expected, maximum allowable, critical) imbalance, when* $\theta = \theta_1 > \theta_0$. *In this paper, the imbalance is detected using the cumulative sum algorithm (CUSUM) as it has certain optimal properties and is widely used in practice. For this algorithm, the required design ratios, descriptions of its properties and features are provided. The paper proposes a procedure for synthesizing the control algorithm with desired properties, in the course of which, based on the user-selected values of desired mean time between false alarms* $\overline{T}_{\text{FA}}$, *initial basic level* θ_0 *and nominal imbalance* $\theta_1 > \theta_0$, *the value of decision boundary H is identified, the speed of algorithm action is estimated trough the calculation of the average lag in the detection of nominal imbalance* $\overline{T}_{lag}$, *along with its efficiency* $E_d = \overline{T}_{\text{FA}} / \overline{T}_{\text{lag}}$ *for various values of d, that quantitatively characterize the value of imbalance:* $d=\theta_1/\theta_0$. *For the purpose of practical implementation of the synthesis procedure, the paper cites reference data, that was obtained by means of simulation and that ensures the development of the control algorithm with required characteristics. It is noted that the presented synthesis procedure can, in principle, also be used for cases of gradual (continuous) change of parameter* θ. *However, the statistical properties of the control procedure will remain unclear as they require sufficiently intense additional research.*

Keywords: *system dependability; detection of dependability characteristics variation; detection of discrete random process imbalance; cumulative sum algorithm; control algorithm synthesis.*

For citation: *Repin DS, Filaretov GF. Algorithm of prompt detection of dependability characteristics variation. Dependability 2019; 4: 8-11 p. https://doi.org/10.21683/1729-2646-2019-19-4-8-11*

Received on 17.10.2019 / Revised on: 16.11.2019 / For printing 14.12.2019

strict form, in GOST 27.002–2015, is an error. For instance, a combination of only software and people without hardware appears to be meaningless.

Given the above, we propose the following improved wording of note 2 to the term "item": along with hardware components, an item may include software required for its operation, and operational personnel in the case of human-machine systems.

Conclusion

The definition of the concept of "item" that is the subject matter referred to by the terms and definitions of dependability in engineering is of great significance, as it affects the application field of dependability standards. For the purpose of its specification, the following refined notes are proposed to its definition in GOST 27.002–2015. Note 1: items may include products (parts, assembly units, complexes) and their components, buildings and structures, systems consisting of jointly functioning products and structures, and their subsystems. Note 2: along with hardware components, an item may include software required for its operation, and operational personnel in the case of human-machine systems.

The current situation in the standardization of scientific and technical terminology in general, and in the area of dependability in particular, leaves much to be desired, which was shown in [4, 6]. Some proposals aiming to improve the situation were expressed in [6].

The author calls upon all the interested experts to share their opinion and put forward proposals both regarding the essence of the matters at hand and the proposed corrections, as well as in terms of organizational measures aimed at improving the situation.

References

[1] Netes VA, Tarasyev YuI, Shper VL. Current issues of terminology standardization in dependability. Dependability 2014;2:120-123.

[2] Netes VA, Tarasyev YuI, Shper VL. How we should define what "dependability" is. Dependability 2014;4:15-26.

[3] Netes VA. New international standard for dependability. Dependability 2016;3:54-58.

[4] Yershov GA, Semerikov VN, Semerikov NV. Chemu verit? O sisteme standartov «Nadezhnost v tekhnike» [What to believe? On the system of standards "Dependability in technics"]. Standarty i kachestvo 2018;8:14-19 [in Russian].

[5] Pokhabov YuP. Problems of dependability and possible solutions in the context of unique highly vital systems design. Dependability 2019;19(1):10-17.

[6] Netes VA. Kak vernut doverie? O sisteme standartov «Nadezhnost v tekhnike» [How to regain trust? About the system of standards "Dependability in technics"]. Standarty i kachestvo 2019;2:19-24 [in Russian].

[7] Bogdanova GA, Netes VA. MEK/TK 56: standartizatsiya dlya nadezhnosti [IEC/TC 56: standardization for dependability]. Metody menedzhmenta kachestva 2009;5:44-47 [in Russian].

[8] Uspensky VA. Apologiya matematiki [Apology of mathematics]. Saint Petersburg: Amfora; 2010 [in Russian].

[9] Recommendation ITU-T Y.3011 (01/2012). Framework of network virtualization for future networks.

[10] Rezinovsky AYa. Eshche raz o sboyakh EVM i tak nazyvaemoy nadezhnosti programmnogo obespecheniya [Back to the matter of computer interruptions and the so-called software dependability]. Nadezhnost i kontrol kachestva 1988;2:57-61 [in Russian].

About the author

Victor A. Netes, Doctor of Engineering, Professor of the Department of Telecommunication Networks and Switching Systems, Moscow Technical University of Communication and Informatics, Russian Federation, Moscow, e-mail: v.a.netes@mtuci.ru

The author's contribution

The author analyzed the definitions of the concept of "item" in the Russian and international standards, identified their shortcomings and proposed improved wordings of notes to the definitions of item as regards the possible types and primary components thereof.

first two of them in GOST 18322–2016 match the definition of such terms in GOST 27.002–2015 (though with no reference thereto), while those of the last two are slightly different from those given in GOST 27.002–2015. Indeed, one would want following the authors of [4] and exclaim: "What to believe?" Upon a careful examination of the above terms, further questions arise. What is the difference between a maintenance item and a maintainable item, and between a repair item and a repairable item?

The next observation in [4] is about the harmonization of GOST 27.002–2015 with the Federal Law of December 30, 2009 no. 384-FZ *Technical Regulations on the Safety of Buildings and Structures*. It is perfectly justified. Along with structures, the list of types of items should include buildings (though it is still unclear why in [4] they are referred to as components of items, as they are an individual type of item). The feasibility of such addition is further supported by GOST 27751–2014 *Reliability for constructions and foundations. General principles* and GOST R 58033–2017 *Buildings and civil engineering works. Vocabulary. Part 1. General terms* (the latter mentions dependability).

The list of items also includes systems consisting of products and structures, that jointly perform certain functions (for instance, communications networks, electric power systems, gas distribution networks, etc.) and their subsystems. In particular, dependability of electric power systems is extensively covered in the Federal Law of March 26, 2003 no. 35-FZ *On the electric power industry*.

Virtualization is an important trend in today's information and communication technologies. Information systems can use virtual computers, virtual data storage systems, etc. (the definitions of those and other similar concepts are given in GOST R 56938–2016 *Information protection. Information security with virtualization technology. General*). In telecommunications, virtual networks, virtual channels and paths are used (for instance, virtual private networks are considered in GOST R 53729–2009 *Quality of service "allocation of the Virtual Private Network". Quality indices*). Network virtualization is considered as one of the key technologies of future networks [9]. While examining their dependability, we should allow for the existence of not only physical, but virtual items as well. Normally, they are logically distinct subsystems within systems that serve as foundations for virtual items.

Given the above, the following wording of note 1 to the term "item" is proposed: items may include products (parts, assembly units, complexes) and their components, buildings and structures, systems consisting of jointly functioning products and structures, and their subsystems.

What an item includes

Now, let us consider the question as to what can be included in an item. The above mentioned notes to GOST 27.002–89 stated that, if required, the concept of "item" can include information and its media, as well as the human factor (for instance, when considering the dependability of operator-machine systems). This wording does not appear to be very good, especially the last part: how can a factor be included into an item?

In IEC 60050-191:1990, note 1 to the term "item" states that an item may consist of hardware, software or their combinations and in particular cases may include people. A similar wording makes note 2 to the term "entity" in GOST R 27.002–2009. Let us note that in the official Russian translation of IEC 60050-191:1990 the word "people" was replaced with "technical personnel" (by the way, the French version of the standard uses the term "personnel").

In the current standards IEC 60050-192:2015, in note 2 to the term "item" it is stated, that an item may consist of hardware, software, people or any combinations thereof (the French version, again, uses the word "personnel"). Accordingly, in GOST 27.002–2015, note 2 to the term "item" states that an item may include hardware, software, personnel or their combinations. This wording (in particular, the reference to personnel) was criticized in [4].

Let us analyze, whether software and people (personnel) should be included in an item along with hardware.

It is well known that software must be taken into consideration while examining the dependability of program-controlled items. The interrelation between the hardware and software components of such items was clearly and convincingly shown in [10]: "…As a separate entity, computer software only exists up until the moment it is entered into the memory device (MD) of a machine. Up until that moment the software exists not as a technical item (and not even as a component of a technical item), but as a document… Naturally, during that period of its existence (to the moment of entering into a computer's MD) a piece of software cannot operate on its own… Subsequently, during that period the program does not have any operating properties of a technical item, including dependability… <…> After the program's entering into a computer's memory, it stops being a separate entity and can be considered only as information on the state of a certain set of physical memory units… Now, it is impossible to pinpoint the boundary between the computer's hardware and its software, that has been entered and according to which the machine can only operate… <…> …Computer hardware alone with no software installed in the MD is also incapable of processing information (it can only get hot, when the power is on, but that is not the "required function" of a computer), and subsequently, the dependability of those hardware elements alone cannot fully characterize the dependability of an entire computer".

As to people, it has also long been known that human operators must be taken into consideration in the context of dependability of human-machine (or operator-machine as in GOST 27.002–89) systems. That, for instance, is reflected in GOST 26387–84 *Man-machine system. Terms and definitions*. Thus, GOST 27.002–2015 does not introduce anything radically new in this regard.

However, we should admit that the wording from IEC 60050-192:2015 allowing for any combination of hardware, software and people, that was, though in a less

cian and linguist V.A. Uspensky wrote the following: "… How can one get an idea of a certain concept? There are two primary ways, one of which we will conventionally call *illustrative* , while the other we will equally conventionally call *definitional* (from lat. definitio, meaning definition). Under the illustrative method, a concept is acquired using examples, under the definitional method, it is acquired using definitions. <…> …Under the definitional method, some concepts are defined through others, others through still others, etc. But this process cannot continue indefinitely. That means that we must stop at certain … concepts and not define them any further. Such concepts, that do not have definitions, are called *indefinable* , or *original*. But if original concepts cannot be defined, …how can we know, what they mean?" [8, p. 309–310, 312–313].

In mathematics, the axiomatic method provides a way out [8, p. 313]. In other fields of knowledge, that are not as strictly formalized, we have to put up with a situation, when the definitions of original concepts are mere explanations, much like the Euclid's definitions of the basic concepts of geometry ("a point is that which has no part", "a line as breadthless length", etc.) [8, p. 307]. Therefore, the fact that GOST 27.002–89 and preceding standards did not define, but rather just explained an item, makes some sense.

Indeed, strictly speaking, the definitions of item in IEC 60050-192:2015 and GOST 27.002–2015, are not really definitions. That explains the importance of the examples of items given in the notes to the definitions in such standards, because, as previously mentioned, under the illustrative method, a concept is acquired with the use of examples specifically.

Sometimes, attempts of finding a way out of the above difficulty cause a vicious circle in the definitions, whereas a concept is defined through itself or concept A is defined through B, while B is defined through A. An example of such situation in standards will be provided below. Naturally, that represents a serious shortcoming in such standards.

Types of items

In [4] it is justly noted, that the list of the types of items given in note 1 to the definition of item in GOST 27.002–2015 is not coordinated with GOST 2.101–2016 *Unified system for design documentation. Types of products*. Indeed, according to GOST 2.101–2016, a product is an article or set of articles , that are to be manufactured by an organization (enterprise) in accordance with design documentation. Moreover, in note 1 to that definition it is stated, that products may include devices, facilities, machines, units, instruments, appliances, equipment, installations, tools, mechanisms, systems, etc. GOST 2.101–2016 also defines a product component as a product that performs certain functions as part of another product, and specified the types of products in terms of structural and functional characteristics: part, assembly unit, complex and set (kit).

If the first three types of products (part, assembly unit, complex) are certainly items in terms of dependability, a set should not be considered as such. Indeed, a set is two and more products, that were not put together at the manufacturing enterprise by means of assembly operations, and are a number of products that share the same operational purpose that is auxiliary in its nature, e.g.: a set of spare parts, a set of tools and accessories, a set of instruments, a set of package, etc. (definition according to GOST 2.101–2016). Therefore, for a set there are no common required functions, whose maintained performance characterizes dependability. Certainly, that does not rule out the possibility of individual consideration of the dependability of the products in a set.

While examining the concept of "product" let us simultaneously note that in GOST 2.101–2016 its definition is complemented with a reference to design documentation that was absent in the previous version of the standard published in 1968. At the same time, GOST 2.001–2013 *Unified system for design documentation. General principles* defines design documentation as a set of design documents, that contain data required for the design (development), manufacture, supervision, acceptance, delivery, operation, repair, upgrade, disposal of a product. Thus, there is a vicious circle: the definition of "product" refers to "design documentation", while the definition of "design documentation" refers to "product".

In GOST 27.002–2015, it is stated, that the requirements for an item are specified in the documentation for such item. In [5], that is cited among the shortcomings of that standard ("fuzziness of dependability terminology"). It is also proposed to refer to design documentation specifically. However, such documentation is associated only with products, i.e. by far not all types of items. Besides, in GOST 27.002–89 the wording also was not limited to design documentation only. It referred to regulatory and technical and/or design (project) documentation.

Another observation in [4] is about the harmonization of GOST 27.002–2015 and GOST 18322–2016 *Maintenance and repair system of engineering. Terms and definitions*. Each of those standards states that they are applied jointly with the other. Unfortunately, there are indeed some discrepancies between them, which include the interpretation of "item". Although, reading [4] one can think that in GOST 18322–2016 there also is a definition of "item", while in reality that is not so. This standard defines the terms "maintenance (repair) item", "maintainable item", "non-maintainable item", "repairable item", "non-repairable item". The wording cited in [4] "an item is a whole that consists of interconnected parts integrated within it for the purpose of performing a common target function" is just a note to the specified terms. However, the definitions of all the above terms in GOST 18322–2016 contain the word item (in Russian "*ob'yekt*" – "object"). We can only guess what exactly that means. Probably, that is the item defined in GOST 27.002–2015. In any case, an explanation was supposed to be provided.

Then, the terms "maintainable item", "non-maintainable item", "repairable item", "non-repairable item" are present in both standards. At the same time, the definitions of the

Introduction

The dependability theory has existed for several dozen years, however its basic definition are still debatable. Over the last few years, they were examined in a number of papers motivated by the development of the Russian and international dependability terminology standards (GOST 27.002–2015 and IEC 60050-192:2015) and the subsequent analysis of such standards [1–6, etc.]. For instance, an animated discussion of how to define the very concept of "dependability" took place in [2]. In the author's opinion, all of that indicates that the dependability theory is alive and well, rather than in the middle of a crisis.

This paper analyzes the concept that precedes the concept of "dependability". More specifically, it discusses the subject matter of dependability, i.e. the dependability of what should be studied. This concept is normally expressed with the term "item". It is defined in a number of standards. However, there is no perfect clarity in this aspect either and discussions also took place. The following issues will be considered: how to name and define this subject of consideration, what it can be, what its constituents can be. Simultaneously, the observations expressed in [4, 5] regarding GOST 27.002–2015 *Dependability in technics. Terms and definitions*, that are associated with the topics of this paper, are analyzed as well.

Background

Up until 2009, the main text of Russian dependability terminology standards lacked a term that would correspond to the subject matter of dependability. The basic definitions use the term "item", while in the informative annex, that contains terminology notes, it is explained that the terminology of dependability in engineering covers all technical items, i.e. products, structures and systems, as well as their subsystems considered in terms of dependability at the stages of design, manufacture, testing, operation and maintenance. Further, it was indicated that subsystems may include assembly units, parts, components and elements (wordings per GOST 27.002–89).

In 2009, instead of GOST 27.002–89, GOST R 53480–2009 was adopted that was later designated GOST R 27.002–2009. It was developed taking into account the primary regulations of international standard IEC 60050-191:1990 *International electrotechnical vocabulary – Part 191: Dependability and quality of service*. Let us note that the International Electrotechnical Commission is instrumental in the international standardization of dependability [7].

GOST R 27.002–2009 uses the term "product" that is defined as any functional unit that can be considered individually. Note 1 thereto mentions examples of such entities: system, subsystem, equipment, device, apparatus , module , component, element. All primary concepts of dependability in that standard were defined in the context of product.

The official Russian translation of IEC 60050-191:1990 gived the single Russian equivalent *"ob'yekt"* (item, literally "object") for the two English terms "item" and "entity", which were treated then as synonyms. An item (entity) was defined as any part, component, device, subsystem, functional unit, equipment or system that can be individually considered. Thus, a part of that wording was used in GOST 27.002–2009 as the definition, while another part was featured in the note thereto.

GOST 27.002–2009 was heavily criticized by experts, as the result of which the validity of GOST 27.002–89 was resumed (that matter was described in detail in [2]). One of the novelties that were criticized was the replacement of the term "item" with the term "product". There is more to that than the deviation from the terminology everyone got used to over the years. A stronger point consisted in the fact that the term "product" had already been standardized as part of the Russian Unified System for Design Documentation (USDD). The then-active GOST 2.101–68 *Unified system for design documentation. Types of products* stated that a product is any article or set of articles , that are to be manufactured at an enterprise. Thus, an undesirable discrepancy arose between the definitions of the same term in baseline technical standards. At the same time, the understanding of the term "product" in USDD that assumes the manufacture at an enterprise is narrower than the concept of "item" in dependability. The latter, for instance, includes communication lines, networks and channels, power transmission lines, pipelines etc. All of them are not products according to USDD.

In 2015, IEC 60050-191:1990 was replaced by IEC 60050-192:2015 *International electrotechnical vocabulary – Part 192: Dependability*. A general analysis of that standard was done in [3]. Out of the above-mentioned English terms it retained only the first one (item) that was defined simply as a subject being considered. Note 5 thereto explains the reasons for the modification: "The definition of item in IEC 60050-191:1990 is a description rather than a definition. The new definition provides meaningful substitution throughout this document. The words of the former definition form new note 1".

The same year, GOST 27.002–2015 was adopted. Its development aimed, on the one hand, to maintain the continuity with GOST 27.002–89, and, on the other hand, to approximate the new international standard. As the result, the following definition was adopted: item is the subject of consideration covered by the terminology of dependability in engineering. Note 1 thereto cites a list of possible items: assembly unit, part, component, element, device, functional unit, equipment, product, system, structure.

Subsequent publications made remarks regarding this definition, however, they will be considered later. First, a general theoretical observation should be made regarding the definition of basic concepts.

The problem of basic concepts definition

The difficulties associated with the definition of basic concepts are common not only to the dependability theory; they are general in their nature. The well-known mathemati-

Original article
https://doi.org/10.21683/1729-2646-2019-19-4-3-7

Item in dependability: definition and content of the concept

Victor A. Netes, *Moscow Technical University of Communication and Informatics, Russian Federation, Moscow*

Victor A. Netes

Abstract. Aim. *The paper continues the series of publications that investigate and discuss the essence and definitions of the basic concepts of the dependability theory. It analyzes the basic concept, which is the subject of consideration in dependability, for which the term "item" is usually used. The concept of "dependability" is defined for it, and in general all the terminology of dependability applies to it. The following issues are considered: how to name and define this subject of consideration, what it can be, what can be its constituents. In particular, the relationship between the concepts of "item" and "product" is discussed.* **Methods.** *The evolution of definitions of this concept in the Russian and international terminological standards in dependability over the past 30 years is traced. A comparative analysis of other standards and federal laws relating to items of different types is carried out. The viability of two main ways of getting an idea of a concept is considered: illustrative (based on examples) and definitional (by means of sequential definition of some concepts through others).* **Findings and conclusions.** *The definition and correct understanding of the concept of "item" is of great importance, as it affects the scope of dependability standards. It is explained why it is necessary to accept that the definitions of the basic concepts cannot be rigorously formalized and are in fact only explanations. It is shown that the definitions of the item in the existing Russian and international standards (GOST 27.002–2015 and IEC 60050-192:2015) have inaccuracies. To eliminate them, improved notes to the definition of an item are proposed. The first note lists the possible types of items: products (parts, assembly units, complexes) and their components; buildings and structures; systems consisting of jointly functioning products and structures and their subsystems. The second note indicates the relationship between the main constituents of the item: hardware, software and people (personnel), and their possible combinations. The paper provides reasons for considering virtual items that play an important role in today's information and telecommunication technologies and are logically isolated subsystems within the systems that they are part of. Besides that, it points out the deficiencies in the definitions of various items in GOST 18322–2016.*

Keywords: *dependability, standardization, item, definition, types of items, constituents of an item.*

For citation: *Netes V.A. Item in dependability: definition and content of the concept. Dependability 2019;4: 3-7 p. https://doi.org/10.21683/1729-2646-2019-19-4-3-7.*

Received on 09.09.2019 / Revised on 18.10.2019 / For printing 14.12.2019

CONTENTS

THE JOURNAL IS INCLUDED IN THE LIST OF THE LEADING JOURNALS AND EDITIONS OF THE HIGHER ATTESTATION COMMISSION (VAK)

Dependability,
DOI:10.21683
ISSN 1729-2646
e-ISSN 2500-3909

THE JOURNAL PROMOTER:
"Journal "Reliability" Ltd

It is registered in the Russian Ministry of Press, Broadcasting and Mass Communications. Registration certificate ПИ 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

The Journal is published quarterly since 2001.
The price of a single copy is 1045 Rubles, an annual subscription costs 4180 Rubles.
Phone: +7 (495) 967 77 05.
E-mail: dependability@bk.ru.

Papers are reviewed.
Papers are published in author's edition.

THE JOURNAL IS PUBLISHED WITH THE PARTICIPATION AND SUPPORT OF THE JOINT-STOCK COMPANY «RESEARCH AND DESIGN INSTITUTE OF INFORMATISATION, AUTOMATION AND COMMUNICATION ON RAILWAY TRANSPORT» (JSC «NIIAS») AND LLC PUBLISHING HOUSE «TECHNOLOGY»