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 21.09.2020, 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»

CONTENTS

Original article
https://doi.org/10.21683/1729-2646-2020-20-3-3-14

Predicting Power System Reliability and Outage Duration including Emergency Response

Romney B. Duffey, *Idaho Falls, Idaho, USA*
duffeyrb@gmail.com

Romney B. Duffey

Abstract. Aim. *Enable prediction and planning for large-scale unprecedented power outages of importance for emergency planning and national response actions. Predict outage probability, duration and restoration using a theoretical framework that is applicable globally.* **Methods.** *Data have been collected for power losses and outage duration for a wide range of events in Belgium, Canada, Eire, France, Japan, Sweden, New Zealand and USA. A new theory and correlation is given for the probability of large regional power losses of up to nearly 50,000 MW(e) without additional infrastructure or grid damage. For severe and rare events with damage (major floods, fire, ice storms, hurricanes etc.) the outages are longer and the restoration probability depends on the degree of difficulty that limits access and restoration. The dynamic reliability requirements for emergency back-up power and pumping systems are derived, and demonstrated using the flooding of New Orleans by Hurricane Katrina and of the Fukushima nuclear reactors by a tsunami.* **Conclusions**. *Explicit expressions have been given and validated for the probability and duration for the full range from "normal" large power losses to extended outages due to rare and more severe events with access and repair difficulty.*

Keywords: *Electricity outages, blackouts, restoration probability, resilience, emergency response, theory, disasters.*

For citation: *Romney B. Duffey, Predicting Power System Reliability and Outage Duration including Emergency Response // Dependability. 2020. no. 3. P. 3-14. https://doi.org/10.21683/1729-2646-2020-20-3-3-14*

Received on: *01.06.2020* / **Revised on:** *27.07.2020* / **For printing:** *21.09.2020*

1. Introduction: Electric power loss and restoration

Large electric power outages completely upset modern industrial and urban complexes. Given power losses do occur, we need to know the probability of the loss, size and duration to plan adequate supply margins, deploy back-up generators, undertake emergency response and protect other critical infrastructure [1].

This is not a new topic at all, and has been extensively studied for setting power delivery performance and reliability standards [2] and coping strategies in national emergency plans [3]. But there is a gap in the literature, knowledge and data between the daily routine of providing reliable power delivery and for responding to the unexpected extreme losses due to cataclysmic disasters and extreme natural hazards. In this paper, we have tried to bridge that gap by determining the probabilities for any given MW(e) outage and the subsequent chance of restoration, including using emergency back-up systems for both everyday and extraordinary events.

Overall studies of the day-to-day reliability or dependability of the electric grid are the normal business concern of owners and operators of the power lines and plants and determines how much they are paid. Whole societies are concerned about power restoration delays, especially due to extensive damage and the societal disruption from the impact of rare or record events and natural disasters (e.g. hurricanes, typhoons, floods, tsunamis, and ice storms). It is such major disasters that are of concern for infrastructure fragility, national emergency preparedness and management decisions.

Following all power losses (aka outages or blackouts), the affected power companies, emergency management organizations and government agencies have deployed vast numbers (sometimes many thousands) of staff, repair crews, equipment and procedures to address power recovery, evacuate people and repair damage. Essentially restoration only can proceed "as fast as humanly possible", limited by damage, access and social disruption issues caused by flooding, storms, fires, wind, ice and snow [4], and as stated "the restoration of the grid is generally the same across all hazards" [5].

The probability of any individual loss or outage being restored is actually random, and being observed as outcomes follows the well-known and established laws of statistical physics and mechanics [6,7,8,9]. Our earlier work provided an explicit analysis of the probability and timing of power restoration for very large outages or power losses at the national level [10].

The initial loss and subsequent restoration are *independent* events, being the initial outage fault or failure followed by the repair and recovery process. The dynamic probability, $P(h)_{NR}$, of an outage of any size lasting any duration, h, hours before restoration is then simply given by, where the conventional reliability is simply the complement, $R(h) = 1- P(h)$,

$P(h)_{NR}$ = Probability of initial loss, $P(\text{MW loss})_i$ x Probability of non-restoration, $P(NR)_h$

If emergency power or back-up systems exist or are deployed or activated, we can include the *dependent* probability for continuing loss of all external and other power sources so,

$P(h)_{ELAP}$ = Probability of initial loss, $P(\text{MW loss})_i$ x Probability of non-restoration of any or all power, $P(ELAP)_h$

Hence there are three distinct probabilities to determine for: (1) the initial event outage size based on known or possible power losses for the system; (2) the subsequent recovery or non-restoration of power by some timescale; and (3) the chance of emergency back-up or "black start" systems failing to function and restore power by that time.

To derive these essential elements, the present approach combines human learning and mechanical system reliability theory, correlated to and validated by extensive power loss and restoration data for actual events.

For the initial loss exceedence probability, $P(MW\ loss)_i$, there are outage size data for the entire USA for the period 1984-2000, for losses, Q, between 1 to 40,000MW(e) [11]. A sample of similar plots by sub-region has also been presented and fitted using empirical binomial, Weibull and lognormal distributions [12]. These distributions are of course heavily weighted by the many "normal" or everyday outages, not rare catastrophic events. We also need to predict the low probability "tail" of the distribution where such standard statistical methods are *not* applicable, as clearly evident in their Fig.S-28. Murphy et al [12] also looked to see if outages were linked, and unsurprisingly concluded: "…that the largest correlated failure instances were caused by extreme weather". This observation is precisely what we should expect given the large geographic scale and impact of natural hazards (storms, hurricanes, floods, ice storms and wildfires) on power systems and the consequent universal power restoration characteristics[4]. Large natural hazard events do not respect or recognize human-drawn boundaries or arbitrary grid distribution regions, and cause event-related damage and destruction over wide swathes.

Other national power loss duration data are derived from [13] for large blackouts in France, Sweden and Belgium, being for a range of 28,000, 11,400 and 2,400 MW(e) initial losses, respectively. The outage durations are well correlated by exponential functions derived from learning theory [10].

For the restoration phase, we had previously collected extensive power recovery data for many severe events e.g. storms, ice storms, fires, hurricanes, cyclones and floods, causing outages lasting a maximum of 800 hours over a wide range of urban, regional and international loss scales. The extent of the outage is represented by the number reported by the power distributors of those connections/

customers remaining "without power", so the probability of non-restoration is the fraction of the initial outages that have not been restored. For all outage events, this electric power non-restoration probability, *P(NR),* is well correlated by simple exponential functions, dependent on and grouped by the degree of difficulty as characterized by the extent of infrastructure damage, social disruption and concomitant access issues [4].

We need to design and determine the effectiveness of the emergency systems for limiting damage, restoring the infrastructure, and managing consequences For actual (not hypothetical) major events**,** there are key performance data available during loss of power from: (a) restoration of power in nuclear power plants following loss-of-grid connection but without additional damage ;(b) back-up pumping systems failing to adequately protect the city of New Orleans from flooding by Hurricane Katrina [14]; and (c) the emergency generators and external power repair not cooling and preventing the melting down of the Fukushima nuclear reactors in Japan after an earthquake and tsunami. The data analysis shows the characteristic failure rates that underpin the determination of the probability of extended power loss for these diverse major emergency systems [15].

We will provide the general expressions for the three probabilities based on the facts emerging from the massive losses observed in entire human, designed, operated and controlled power systems.

2. Methods: Assumptions and theoretical development

The first key assumption is that the power losses, outages and

restorations are indeed random, whatever the cause, but all depend on human actions including emergency management decisions . Secondly, because humans learn and think, a systematic trend exists with increasing experience or risk exposure so that, as shown by the data, we should expect larger outage events to have lower probability. Thirdly, the chance of restoration or recovery of any individual initial outage or loss of power depends on the ability and experience gained by emergency managers and crews so also demonstrates a learning trend. Finally, because the probability of any individual outage happening and being restored is actually random, the observed outcome distribution follows the well-known and established laws of statistical physics[6,7,8,9].

After any prior or during any present risk exposure or accumulated experience, ε, the learning hypothesis theory [8] defines the rate of decrease of the observed failure rate, λ(ε), as proportional to the rate, $\frac{d\lambda}{d\varepsilon} \propto \lambda, \frac{d\lambda}{d\varepsilon} = -k\lambda$. For the present case the instantaneous failure rate, λ(ε), is equivalent to the observed rate of change of the number of power loss outages. Solving, this rate is given by,

$$\lambda(\varepsilon) = \lambda_m + (\lambda_0 - \lambda_m)e^{-k\varepsilon}, \quad (1)$$

Here, λ_0 and λ_m are the initial and smallest attainable rates, respectively, and k is the proportionality constant. As usual, the prior probability over some prior risk exposure interval, ε, is,

$$P(\varepsilon) = 1 - e^{-\int \lambda(\varepsilon)\, d\varepsilon} = 1 - e^{-\left(\frac{(\lambda - \lambda_m)}{k}\right)} \quad (2)$$

To evaluate these rates and probabilities, we adopt the simplest approach consistent with the physical situation and model the power loss outcomes as emergent events, without examining the root cause or systemic origins of each and every event, and then test the approximations and results against the data.

2.1. Probability of initial power loss or blackout size

In the past, we have observed portions of an entire power system (a plant, power line, distribution control…) causing initial outages that form some known or assumed distribution of overall loss sizes. The measure of the relative risk exposure or loss experience measure is self-evidently actually directly proportional to the power outage magnitude, ε=f(Q), which we can scale relative to the average outage magnitude, $\overline{Q}$, so $\varepsilon \equiv Q / \overline{Q}$. We may assume for each and every different outage, $\lambda_0 = 1/\varepsilon$, implying individual outage events are independent (which they are in practice); and that the outages are usually nearly completely restored, so we may take, $\lambda_m \ll \lambda \approx \lambda_0 e^{-k\varepsilon}$.

Therefore, from Equations (1) and (2) the probability of any initial power loss or outage, becomes simply the intriguing double exponential,

$$P(\text{MW loss})_i = P(Q)_i = 1 - e^{-\frac{\overline{Q}}{kQ}\left\{1 - e^{-\frac{kQ}{\overline{Q}}}\right\}}. \quad (3)$$

The obvious and sensible limits are:

(a) small outage or loss
$kQ / \overline{Q} \to 0,\ P(Q)_i = 1;$

(b) infinitely large loss
$kQ / \overline{Q} \to \infty,\ P(Q)_i = 0;$

(c) average loss, assuming that k~1,
$Q / \overline{Q} \to 1,\ P(Q)_i = 1 - e^{-\{1 - e^{-1}\}} = 0.74$

2.2. Dynamic probability of outage duration and restoration

We observe that after the initial loss, power is progressively and eventually restored to every individual customer

or connection, where the relevant risk exposure measure is now the elapsed outage time, so ε ≡h, in hours. So the probability of any duration of any individual outage of any initial size at any elapsed time is then simply given by

$$P(h)_{NR} = P(Q)_i \times P(NR)_h. \quad (4)$$

The data for electric power non-restoration probability, $P(NR)_h$, for all outage events are all well correlated by simple exponential functions, dependent on and grouped by the degree of difficulty as characterized by the extent of infrastructure damage, social disruption and concomitant access issues [4] . The instantaneous probability of non-restoration, $P(NR)_h$, of any individual outage in the entire system in any interval is obtained by dividing Equation (1) by the total possible number requiring restoration, being the initial individual outage number count. The general exponential form of the *instantaneous* probability of non-recovery or continuing failure then is [6],

$$P\left(NR\right)_h = P_m + (1 - P_m)e^{-\beta h}, \quad (5)$$

Here, $k \equiv \beta$, and depends on the degree of difficulty for storms, fires, floods and hurricanes, and P_m is due to the few irrecoverable outages Substituting Equations (3) and (5) into (4), and noting $P_m << 1$,

$$P\left(h\right)_{NR} = (1 - e^{-\frac{\overline{Q}}{kQ}\left\{1 - e^{-\frac{kQ}{\overline{Q}}}\right\}})\left(P_m + e^{-\beta h}\right). \quad (6)$$

A good working approximation is, $P_m << e^{-\beta h}$,

$$P\left(h\right)_{NR} \approx (1 - e^{-\frac{\overline{Q}}{kQ}\left\{1 - e^{-\frac{kQ}{\overline{Q}}}\right\}})e^{-\beta h} \quad (7)$$

The limits are again:

(a) small outage or loss, $P\left(h\right)_{NR} \approx e^{-\beta h}$

(b) infinitely large loss, $P\left(h\right)_{NR} \to 0$

(c) average loss with k~1, $P\left(h\right)_{NR} \approx 0,74\ e^{-\beta h}$

2.3. Dynamic probability of extended outage while deploying emergency and "black start" back-up systems

This is an important and more complicated situation, as while overall system restoration is ongoing, emergency back-ups are sometimes deployed locally or grid-wide, being diesel generators, gas turbines or "black start" alternate power plants. Hence, the probability of extended power loss of initial size, Q, depends on the probability, $P(ELAP)_h$, of power not having been already restored by both normal and emergency means, so,

$$P(h)_{ELAP} = P(Q)_i \times P(ELAP)_h. \quad (8)$$

To evaluate, $P(ELAP)_h$, we must combine the non-restoration probability, $P(h)_{NR}$, with the on-going failure to successfully deploy or actuate any or all back-up emergency systems [15,16]. The overall *dependent* probability, $P(ES)$, for any such emergency or back-up system to *not* be successfully deployed or activated is conventionally characterized as exponentially dependent on an overall system average failure rate, λ_{ES} [17].The dynamic probability density of extended failure or loss of all power, $dP(ELAP)_h/dh$, is then the multiplicand of the dynamic probability of the continuing failure of system recovery, $P(NR)_h$, times the probability density, $\frac{dP(ES)}{dh} = \lambda_{ES}\, e^{-\lambda_{ES} h}$, being the changing rate of the probability for unsuccessful emergency restoration [15, 16]. Over the prior elapsed or available restoration time, h, we then have,

$$P\left(ELAP\right)_h = \int_0^h \frac{dP\left(ELAP\right)_h}{dh} dh = \int_0^h P\left(h\right)_{NR} \frac{dP\left(ES\right)}{dt} dh$$

Integrating by parts, and since, $P_m << e^{-\beta h}$,

$$P\left(ELAP\right)_h = \int_0^h \left(e^{-\beta t}\right) \lambda_{ES}\, e^{-\lambda_{ES} h} dh = \left(\frac{\lambda_{ES}}{\beta + \lambda_{ES}}\right)\left[1 - e^{-(\beta + \lambda_{ES})h}\right]. \quad (9)$$

The limits are obvious:

(a) great restoration difficulty, $\beta << \lambda$, $P\left(ELAP\right)_h \approx 1 - e^{-\lambda_{ES} h}$

(b) perfectly reliable backup, $\lambda = 0$, $P\left(ELAP\right)_h = 0$

(c) at very long times, $h \to \infty$,

$$P\left(ELAP\right)_h \to \left(\frac{\lambda_{ES}}{\beta + \lambda_{ES}}\right).$$

Substituting (9) into (8), the extended loss probability is,

$$P(h)_{ELAP} = \left(\frac{\lambda_{ES}}{\beta + \lambda_{ES}}\right)(1 - e^{-\frac{\overline{Q}}{kQ}\left\{1 - e^{-\frac{kQ}{\overline{Q}}}\right\}})\left[1 - e^{-(\beta + \lambda_{ES})h}\right]. \quad (10)$$

Important parameters are the failure rate ratio, $\Psi = \lambda_{ES}/(\beta + \lambda_{ES})$, and the key characteristic time, or e-folding time-scale, $1/(\beta + \lambda_{ES})$. Therefore, for any given initial power loss, Q, the measure of improved resilience, $R_{ES}(Q)$, by successfully utilizing emergency back-up systems is the steadily declining probability ratio, from Equations (7) and (10),

$$R_{ES}(Q) = \frac{P\left(h\right)_{ELAP}}{P\left(h\right)_{NR}} = \Psi\left[1 - e^{-\lambda_{ES} h}\right]. \quad (11)$$

The role of the ratio of the key failure rate parameters is now self-evident, with recovery timing depending on which failure rate dominates. This result can be generalized for deploying any number of independent redundant and/or diverse back up systems with differing failure rates [15].

3. Results: Comparisons and verification with data

To set the parameters and validate the theory of Section 2, we can now sequentially and systematically compare the predictions of Equations (3) (7) and (10) with large-scale loss and restoration data. The events considered all fully include emergency responses, human actions, procedural guidance, specialized repair crews, and management decisions.

3.1. National and regional outage data compared to theory

The original USA outage data from the NERC database for 1984-2000 were shown in [11] as a graph with dots and lines on a log-log plot; but because of the unavailability of the actual data[1], we were forced to hand transcribe using enlarged images. The error incurred is a maximum of about 5% in probability for exceeding a given power loss or outage, $P(Q)_i$, which is sufficient accuracy for the purposes of rare event prediction (see below). For the observed sample of outages, we define the likely mean or probable average outage as,

$$\overline{Q} = \overline{\sum_i P_i\,(Q) \times Q_i}.$$

[1] Our requests were declined for access to and use of the original data files and numbers for the plots in [11,12]. Surprisingly, the actual NERC data for the USA are proprietary (privately owned) so the line drawings are apparently all that are publically or openly accessible.

The data [11] then have an expected average outage of $\overline{Q} = 95\,MBm(\mathrm{e})$. As a basis for correlation, the comparison of the theory to data is shown in Fig.1, obtained by simply adjusting the single parameter, k=2, in Equation (3) so the overall outage distribution shape is reclaimed with,

$$P(Q)_i = 1 - e^{-\frac{\overline{Q}}{2Q}\left\{1 - e^{-\frac{2Q}{\overline{Q}}}\right\}}. \qquad (12)$$

The theoretically-based probability then has a maximum uncertainty of order ±20% compared to the transcribed data, sufficient for present estimating purposes where the predictive larger losses for Q_i > 40,000 MW(e) have a probability of approximately 0.003 or less. The probability, of having an average system outage, $P(\overline{Q})$ = 0.74 compared to the $P(\overline{Q})$ =0.86 observed.

A recent paper presented similar data plots for all eight NERC regions [12] which were fitted using totally empirical distributions. The individual probabilities are naturally one order lower for the largest recorded regional power losses since the average local outage,$\overline{Q}$ and the best-fit k-value change significantly [18].

Furthermore, given this new theory, we can now predict the probability of a total (100%) blackout, being "a catastrophic power outage of a magnitude beyond modern experience" [1]. As an example, for the NPPC-region case, this probability is *P (57,700 MW (e))* = 0.0015, and represent a pure *quantitative* prediction of an unimaginable and not previously experienced outage.

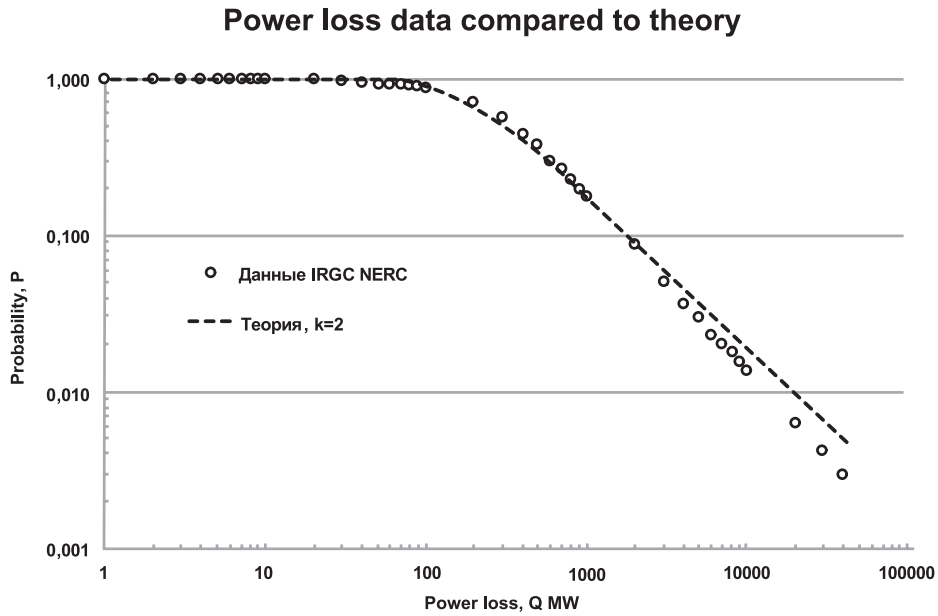


Fig. 1. Comparison of fitted theory to overall probability of any given power loss size (data extracted from [11])

For no major damage, the country-wide losses data were generally caused by overall transmission and distribution failures or overloads, cascading through the system but with no additional physical damage due to flooding, fires or hurricanes etc [13]. The data all follow the Equation (5) exponential learning curve, each with its own e-folding rate of between 0.3-0.8 per hour, and coefficients of determination all of, R^2 =0.9. As shown in Fig.2. the best fit of Equation (5) to the overall pooled data for four events in three countries, with a coefficient of determination, $R^2 = 0.69$, is

$$P(NR) = e^{-0,43h}. \quad (13)$$

It can be seen that even for these massive blackouts, restoration was accomplished in less than 10 hours, despite the factor of ten differences in the Q_i MW(e) size or scale of the initial outage.

The agreement of the trends is sufficiently encouraging to examine comparisons with loss data with additional damage and difficulty as follows.

3.2. Severe events compared to theory

The probability of *local distribution* power system non-recovery is, $P(NR) = n(h)/N_0$, the ratio of the outages remaining, $n(h)$, to the total (initial or maximum) number, N_0, being the complement of the usual reliability, $R(t) = 1-P(NR)$.

Summaries for 17 distinct events are listed in Tab.1. and more details can be found in [4]. They caused very different losses, since on average the size or scale of the overall outage at any time is roughly proportional to the number "without power" or individual outages reported, $n(h)$, so $n(h) \propto Q(h)$. The USA average 24/365 per customer use is about 10,000 kWh, so these events correspond to an initial power loss range of order $8 < Q < 10,000$ MW(e). Therefore, although generally only a fraction of the entire regional distribution system, they can be the entire local electricity grid (as for the Florida Keys) or urban community (as in Queens);

As opposed to traditional plots of the numbers of outages versus time for different events (see e.g. [5]), the present formulation normalizes all the events, and demonstrates it is not solely the number of outages that affects characteristic recovery timescales. The data clearly show groupings between "normal" and "extreme" events restoration, with the "normal" group being faster; and events with more extreme damage and/or access difficulty clearly have much slower restoration and longer durations, by at least a factor of ten to twenty.

As shown by Equation (5), the key issue is the extent of damage, social disruption or access difficulty as reflected in and by the characteristic or e-folding "degree of difficulty"

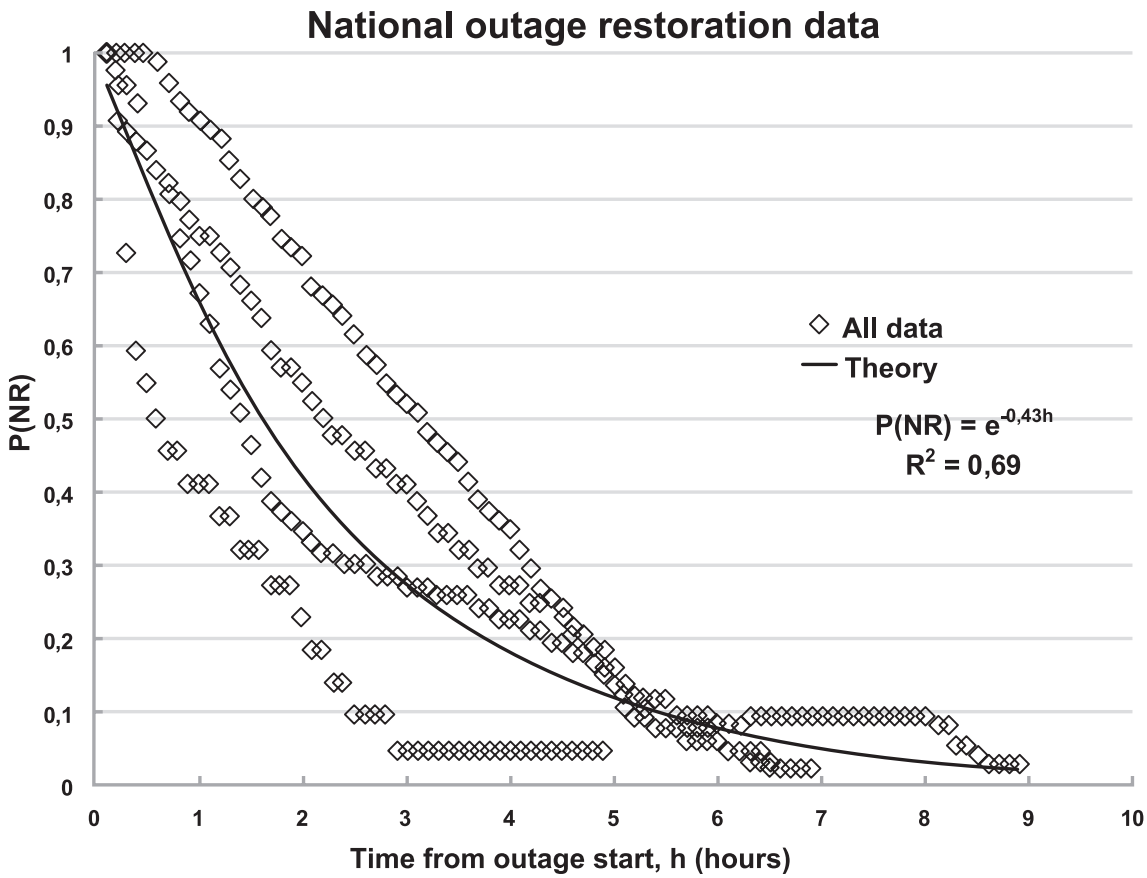


Fig. 2. Overall restoration trends for large scale national power outages

Table 1. Power Outage Data Summary
(Event key: A= Alaska earthquake, B=Baseline; SS=Sandy, E=Storm Emma, F= Florence, G=Cyclone Gita, H=Harvey, HQ= Quebec ice storm, I=Irma, Ma=Matthew, MI= Michael, N=Nate, NH-New Hampshire ice storm, O=Ophelia; Q= Storm Quinn, R=Storm Riley, S=Snowstorm Grayson, T=Storm Toby, W=wildfires)

City and/or region	Data source (event)	Span h	Maximum N_0
Queens, NY	NYPSC/ConEd(B)	88	25,000
New York, NY	ConEd (SS)	336	1,345,000
Florida	FDO (Ma)	240	10,234,174
Houston, TX	CPE (H)	800	109,244
Corpus Christi	AEP (H)	800	201,635
Florida South	FPL (I)	400	1,810,290
Florida NW	Duke-FL (I)	400	1,610,280
Tampa, FL	TECO (I)	400	330,103
Florida Keys	FKEPC/KES(I)	400	60,000
Florida Gulf	Gulf Duke (MI)	320	396,700
Alabama	APC-SCS (N)	60	156,000
N&S Carolina	Duke Energy(F)	190	542,780
Eire, EU	ESB (O)	240	385,000
Eire, EU	ESB (E)	60	127,000
NE, USA	Eversource (S)	50	25,796
NE, USA	Eversource (R)	90	220,378
NE, USA	Eversource (Q)	120	209,706
New Hampshire	NHPS (NH)	312	432,600
New Jersey	Jersey CP&L (T)	37	31,656
Quebec, Canada	HydroQuebec (HQ)	286	1,393,000
Taranaki, NZ	Powerco (G)	160	26,000
Napa, CA	PGE (W)	450	359,000
Ventura, CA	SCE (W)	450	8,400
Anchorage, AK	ChugachMP&L(A)	28	21,713
Totals		5,801	20,061,455

parameter, β per hour. For system design and recovery planning purposes from the actual data we define the loss event categories as (see Fig. 3):

• Type 0: Ordinary, $0.8>\beta>0.3$, due to an effectively instantaneous outage with essentially no additional damage, which we classify as outage restorations that are relatively rapid, taking less than a day with simple equipment replacement, breaker resetting, line/grid repairs, and/or reconnection.

• Type 1: Normal baseline, $\beta \sim 0.2$, when outage numbers quickly peak due to finite but relatively limited additional infrastructure damage. Repairs are still fairly straightforward and all outages are restored over timescales of 20 to about 200 hours.

• Type 2: Delayed, $\beta \sim 0.1$–0.02, progressively reaching peak outages in 20 plus hours, as extensive but repairable damage causes lingering repair timescales of 200–300 hours before almost all outages are restored.

• Type 3: Extended, $\beta \sim 0.01$, with perhaps 50 or more hours before outage numbers peak due to continued damage and significant loss of critical infrastructure causing access difficulty. Restoration repair timescales last for 300–500 hours or more with residual and complex outages lasting even longer.

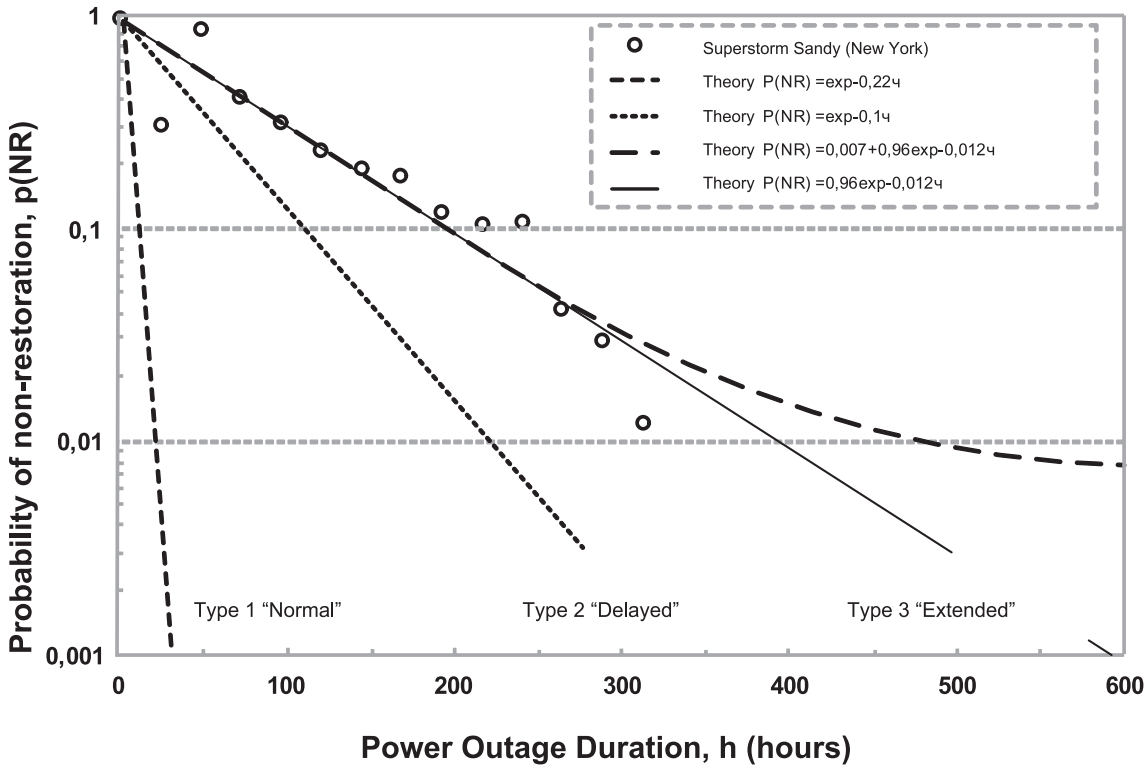


Fig.3. Simplified categories of outage restoration difficulty and timescales.

• Type 4: Extraordinary, β ~ 0.001 or less, for a cataclysmic event with the electric distribution system being essentially completely destroyed and not immediately repairable (e.g. Haiti, Costa Rica, and NAIC "catastrophic outages" [1]).

These categories allow for more refined emergency response and communication, and more realistic restoration planning. This observed variation in the degree of difficulty ($0.01 < \beta < 0.2$) implies an average repair rate spread of 20 simply due to the damage extent. The irreparable fraction data range (the "tail" of the distribution) indicates that the chance of remaining unrestored is small but finite, say $0.003 < P_m < 0.01$,even after several hundred hours. As an example, for every million outages at first, despite achieving over 99% restoration after 600 hours several thousand could still be left without power.

The data for Superstorm Sandy are shown (open circles) purely as an example, because it represents a "long term outage" as specifically defined by FEMA [1, p32]. The exponential form and trends do not change with overall duration.

The US DHS [5] makes the not unreasonable assumption that the restoration curve for power outages or "virtual" damage due to cyber attacks is similar to that for known severe events, like hurricanes and ice storms. By this analogy, cyber attacks causing power outages are postulated to simply increase the restoration timescales and numbers, which we would interpret as reflecting an increased "degree of difficulty" with β reducing further. The publically available data [5, 19] shows a cyber attack caused power outages by disconnecting networks and operator control before being restored after "several hours" .We would now classify this event as a Type 1 "normal" outage, with a *P(NR)* range of "cyber degree of difficulty" $0.1 < \beta < 0.22$, because there was no concomitant or additional access, physical damage, or societal disruption affecting recovery of the power system infrastructure and associated computing/communication networks.

For a hypothetical national catastrophic outage number of 100 million, as shown in Figures 2 and 3, and Equation (7), for some 150,000 the outage duration can be expected to exceed several hundred hours.

3.3 Emergency response data for the Hurricane Katrina and Fukushima nuclear events compared to theory

We validate the method by comparing to cases of successively more severe power outages of national importance and impact, due to the loss of power. The events share the common feature of deploying engineered systems, back-up generators, pumping or cooling systems for which power has to be supplied somehow.

The overall, integral and needed emergency system failure rate, λ_{ES}, can be derived from the data for outage restoration in major facilities and with progressively greater difficulty:

(a) The needed failure rate for critical engineered systems without damage is derivable from outage restoration data to avoid core overheating following offsite power

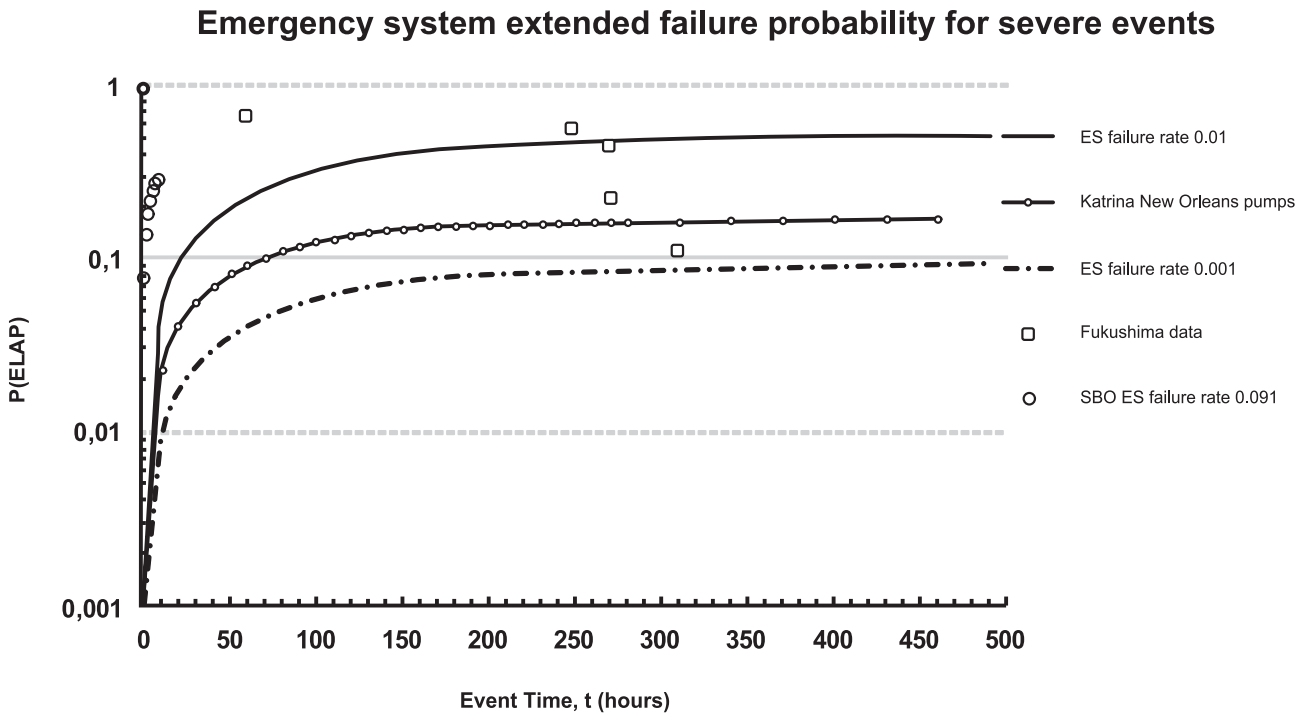


Fig.4. The probability of extended systems failure, $P(ELAP)_h$, for differing emergency system (ES) failure rates, and comparison to data from the Hurricane Katrina and Types 1 and 3 nuclear plant events

loss[1] for multiple US nuclear plants [20]. These restoration events can be considered "normal" or Type 1 with β~0.22 without additional major damage or difficulty, as in minor ice storms, localized fires, and urban outages such as the Queens blackout in New York city [4,15]. In addition, the "Failure probabilities for operator to recover AC power" using emergency batteries and diesel generators (DGRs), $P(ES)_{DGR}$,after the onset of SBO were calculated in [21] for a "representative" large PWR unit. The best fit theoretical line through the nine tabulated points [21, Table 4-13], with elapsed time, h, hours, is, with R^2=0.99,

$$P(ES)_{DGR} = 0.8\ e^{-0.087h} \qquad (14)$$

This result implies an average integral emergency generator failure rate of λ_{DGR}~ 0.09 per hour. Using this rate, the long-term probability of extended outage is $P(ES) \sim \Psi = \lambda/(\beta+\lambda) = 0.09/(0.22+0.09) \sim 0.29$, or nearly 30%..

(b) For analyzing even more demanding conditions, a more severe event was the inundation of New Orleans by Hurricane Katrina in 2005, causing extensive record flooding and infrastructure damage [14]. The failure of emergency flood-prevention systems to successfully deploy and operate to avoid flooding is a known example of a high degree of difficulty in managing the consequences of a major disaster also causing loss of power. The extensive reports show: "The system's performance was compromised by the incompleteness of the system, the inconsistency in levels of protection, and the lack of redundancy" [14, Volume 1]. Several hundred flood prevention pumps were distributed in four regions but many became inoperable, themselves failing due to flooding, power loss and/or forced evacuation [14, Vol VI , Figs 12, 16, 19 and 22].

The *integrated* emergency systems failure rate, λ_{ES} , of the flood prevention systems and of the back-up emergency pumps to operate, was determined from the fractional operating pump data [14, 18]`. The fitted dynamic probability for successful overall emergency pump system operation, $P(ES)_h$,correcting for the running total, for hours, h, after the Katrina event started, was

$$P(ES)_h = 0.8\ e^{-0.003h} \qquad (15)$$

Hence, for these diverse flood prevention and emergency backup systems, the implied time-averaged failure rate is λ_{ES}~0.003 per hour; while at h= 0 hours, there is an initial operating probability of $P(ES)_h$ ~0.8, or approximately 80%. This initial fraction is *identical* to that for the "normal" nuclear plant events (see Equation (14)), and only slightly lower than the US ACE stated availability expectation of 90%. But this high value only exists at the beginning not throughout the event, progressively decreasing (to 20-30 %) over several hundred hours as the developing damage, flooding extent and restoration access issues worsen.

(c) Finally, combined LOSP/LOOP of extensive duration was caused to the nine nuclear reactors at Fukushima by the Great NE Japan offshore earthquake and the result-

[1] In nuclear reactor risk analyses, these event sequences are traditionally termed Station Blackout (SBO) following loss of onsite and/or offsite power (LOSP/LOOP), and the designs include multiple diesel generator and battery back up systems.

ing record tsunami [22,23].The engineered system failures were power line damage and unexpected overtopping of sea walls and flood barriers, resulting in loss of power, disrupted controls, failures of emergency cooling systems, and damage to back-up systems and pumps. Power was not restored in sufficient time to manage or prevent the occurrence of major damage, with highly difficult and demanding conditions including explosions and radiation contamination. Restoration attempts for power and cooling included simultaneous emergency efforts to restore grid power from damaged offsite power lines, provide power onsite, and use whatever back-up, battery, pump, mobile, or other even ad hoc systems that could be deployed.

Using Equation (9) we calculated the actual severe event non-restoration or extended failure probability data for such apparently disparate Type 3 events, with β~0.01 [15]. In Fig. 4, the extended failure data for Fukushima Daiichi Units 1–6 and Daiini Units 1, 3, and 4 is compared with the predicted probability of extended systems failure, $P(ELAP)_h$ for Hurricane Katrina using the actual emergency pump failure rate , λ_{ES} =0.003, as deduced above (see Equation (15)). Also shown are the calculated effects of a wider range of better (λ_{ES}=0.001) or worse (λ_{ES}=0.01) emergency or back up systems failure rates. For comparison, the shorter time-scale Type 1 "normal" nuclear plant SBO results (β=0.22) are shown using the emergency systems failure rate of λ~0.091 that was derived from the published nuclear plant SBO calculations [21].

Discussion

Therefore, we have shown that for all these "extended" Type 3 events or major disasters, the actual emergency systems failure rate range encompassing that actually observed is $0.001<\lambda_{ES}<0.01$ per hour. This range includes different engineered systems, multiple redundant/diverse generators, relevant human and management actions, access and repair difficulty issues, and restoration and procedural processes during emergency recovery and disaster response. The probability of a prolonged or very extended outage has been shown to be non-negligible.

Taking the observed β and λ rate values as typical for any severe event, the critical time, $t^* = 1/(\beta+\lambda)= 1/(0.01+0.003) \sim$ 77 hours, and is dominated by the restoration difficulty; while at very long times, $P\left(ELAP\right)_{h\to\infty} \to \psi = 0,003 / 0,013 \sim 0,23$, or about a 25% chance of extended systems failure or non-recovery even with emergency restoration. Hence, for major events we should expect power and pumping outage durations lasting at least several days, even with multiple backup systems available or externally supplied.

In sections 3.1,3.2 and 3.3 we have been able to inter-compare completely disparate and hitherto apparently unrelated separate outage events, all the way from major losses to recovery and deploying back up and emergency generating systems. The unifying physical mechanism is the link between theoretically–based statistical theory [6,7,8] and the understanding of the importance of human learning behavior [9] on system recovery and required resilience[1,25].

Conclusions

Power generation and distribution systems are part of a nation's critical infrastructure. Power losses or outages are random with a learning trend of declining size with increasing experience or risk exposure, with the largest outages being rare events of low probability. Data have been collected and inter-compared for power losses and outage duration affecting critical infrastructure for a wide range of severe events in Belgium, Canada, Eire, France, Sweden, New Zealand and USA, including Hurricane Katrina flooding New Orleans and the Fukushima reactor meltdowns.

The unifying mechanism is the theoretically–based statistical learning theory combined with the understanding of the importance of human behavior on system recovery and resilience. Using this theory, a new correlation has been obtained for the probability of large regional power losses for outage scales up to nearly 50,000 MW (e) for events without additional infrastructure damage that have been generally fully restored in less than 24 hours.

The theory was extended to more severe events with extended outage durations, including damage due to natural hazards (floods, wildfires, ice storms, tsunamis, hurricanes etc.). The observed variation in recovery timescale of up to more than 600 hours depends on the degree of restoration difficulty. The irreparable fraction (the "tail" of the distribution) indicates that the chance of remaining unrestored is small but finite, even after several hundred hours. For the first time, the impact on restoration probability using emergency systems has also been quantified.

Therefore, explicit expressions have been obtained and validated for both the probability and duration for the full range from "normal" large power loss and to extended outages in rare and more "severe" events with greater access and major repair difficulty. This new formulation enables prediction and planning for large-scale unprecedented outages of interest for emergency planning and national response actions.

Appendix: General equation for rare events

The more general form of this new EVD Equation (3) is, for any variable, x, where the over bar is the relevant or selected average value:

$$P_i\left(x\right) = 1 - e^{-\frac{\bar{x}}{k x}\left\{1 - e^{-\frac{x}{k\,\bar{x}}}\right\}}. \qquad \text{(A1)}$$

There are just two "adjustable" parameters, the average, $\bar{x}$, and the learning constant, k, where both have physical

significance. This equation can be compared to typical arbitrary three-parameter Generalized Extreme Value Distributions (GEVD) quoted elsewhere for power outages [23] and floods [24] of the general form:

$$P_i(x) = 1 - e^{-1+\xi\left(x-\frac{\psi}{\beta}\right)^{-1/\xi}}. \qquad \text{(A2)}$$

For the conventional "named" distributions:

- Gumbell Type 1 $\xi=0$
- Frechet Type 2 $\xi>0$
- Weibull Type 3 $\xi<0$

Ockham's Razor suggests using the simplest. The reader is of course free to adopt whatever best suits the purpose and represents appropriately the physics, available data and logic of the situation.

References

[1] NIAC, 2018, Surviving a catastrophic power outage, President's National Infrastructure Advisory Council, Washington, DC (accessed at www.dhs.gov/national-infrastructure-advisory-council)

[2] NERC, 2020,Reliability Standards for the Bulk Electric Systems of North America, BAL-001-2 Updated June 23 National Electricity Reliability Council, Atlanta , Georgia. (accessed at www.nerc.com/pa/Stand/Reliability Standards Complete Set/RSCompleteSet.pdf)

[3] DHS, 2017, Power Outage Incident Annex (POIA) to the Response and Recovery Federal Interagency Operational Plans, Managing the Cascading Impacts from a Long-Term Power Outage, US Department of Homeland Security, Final, June 2017 (accessed at www.fema.gov/media-library-data/POIA_Final_7 2017v2.508.pdf.)

[4] Duffey, R.B., 2019, Power restoration prediction following extreme events and disasters, Int J Disaster Risk Science, 10(1) pp 134-148, Springer

[5] DHS, 2018, U.S. Department of Homeland Security (DHS), Strengthening the cyber security of Federal networks and critical infrastructure, Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities. August 9. (accessed at www.dhs.gov/sites/default/files/publications/EO13800-electricity-subsector-report.pdf.)

[6] Rushbrooke, G. S., 1949*, Introduction to Statistical Mechanics*, Oxford University Press, London

[7] Greiner et al, 1995, Greiner,W., L.Neise and H. Stocker, 1995, *Thermodynamics and Statistical Mechanics*, Springer , NY, ISBN 0 387 94299

[8] Jaynes, E.T., *Probability Theory: the logic of science*, Cambridge University Press, 2003, ISBN 0 521 59271 2(ed G. L. Bretthorst).

[9] Duffey, R.B. and J.W. Saull, 2008, Managing Risk, J.Wiley and Sons, ISBN 978 0 470 69976 8

[10] Duffey, R.B. and T Ha, 2013, The probability and timing of power system restoration, IEEE Trans Power Systems, 28, pp3-9, Paper # TPWRS-00826-2010, DOI 10: 1109/TPWRS.2012.2203832

[11] IRGC, 2006, Managing and Reducing Social Vulnerabilities From Coupled Critical Infrastructures, White paper #3, Geneva, Switzerland, Figure 5 p28.

[12] Murphy, S, J Apt, J Moura and F Sowell, 2017, Resource adequacy risks to the bulk power system of North America, Applied Energy, 212, pp1360-1376 DOI: 10.1016/j.apenergy.2017.12.097

[13] Kearsley, R., 1987, Restoration in Sweden and experience gained from the blackout of 1983, IEEE Trans. Power Syst., vol. 2, no. 2, pp. 422–428, May .

[14] US ACE (US Army Corps of Engineers),2006, Performance evaluation of the New Orleans and Southeast Louisiana hurricane protection system, Volumes I to VIII, Engineering and Operational Risk and Reliability Analysis, Interagency Performance Evaluation Task Force (all volumes available at US ACE Digital Library usace.contentdm.oclc.org/digital/collection/p266001coll1/id/2844/)

[15] Duffey, R.B.,2019, The Risk of Extended Power Loss and the Probability of Emergency Restoration for Severe Events and Nuclear Accidents, J. Nuc Eng Rad Sci., July, NERS-18-1122, DOI: 10.1115/1.4042970

[16] Barr,J.,Basu, S., Esmaili, H., and Stutzke, M., 2018, Technical Basis for the Containment Protection and Release Reduction Rulemaking for BWRs with Mark I and Mark II containments, U.S. NRC Report NUREG-2206, Washington, DC.

[17] Lewis, E. E., 1994, *Introduction to Reliability Engineering*, John Wiley and Sons, New York, 2nd edition

[18] Duffey, R.B., 2020, Critical Infrastructure: the probability and duration of national and regional power outages, RT&A ,15, 2 (57),pp 62-71

[19] Lee, R M, M J Assante and T Conway, 2016, Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case, E-ISAC Report, Electricity Information Sharing and Analysis Center, Industrial Control Systems, Washington, DC, (accessed at ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)

[20] Eide, S. A., Gentillon, C. D., Wierman, T. E., and Rasmussen, D. M. , 2005, Reevaluation of Station Blackout Risk at Nuclear Power Plants: Analysis of Loss of Offsite Power Events: 1986-2004 , NRC Report No. NUREG-CR6890 Nuclear Regulatory Commission, Washington, DC,

[21] Ma , Z, C Parisis, H Zhang, D Mandelli, C Blakely, J Yu, R Youngblood, and N Andrson, 2018, Plant-Level Scenario-Based Risk Analysis for Enhanced Resilient PWR – SBO and LBLOCA, Report INL/EXT-18-51436, Idaho National Laboratory , US DoE,

[22] TEPCO, 2012, "Fukushima Nuclear Accident Analysis Report," Tokyo Electric Power Company, Tokyo, Japan; and Japanese Government Report to IAEA Ministerial Conference on Nuclear Safety, Vienna, Austria.

[23] ASME, 2012, "Forging a New Safety Construct," American Society of Mechanical Engineers, Presidential Task Force Report, New York, Report

[24] Espinoza, S., M Panteli, P Mancarella, and H Rudnick , 2016, Multi-phase assessment and adaptation of power systems resilience to natural hazards, Electric Power Systems Research, 136, pp 352-361, DOI: 10.1016/j.epsr.2016.03.019

[25] Sandoval, C E., and J. Raynal-Villaseñor ,2008, Trivariate generalized extreme value distribution in flood frequency analysis, Journal Hydrological Sciences, 53:3, 550-567, DOI: 10.1623/hysj.53.3.550

[26] Zio. E.,2016, Challenges in the vulnerability and risk analysis of critical infrastructures, *Reliability Engineering and System Safety*, DOI:10.1016/j.ress.2016.02.009

About the author

Romney B. Duffey, Ph.D, B.Sc., former chair of ASME nuclear division, Idaho Falls, Idaho, USA, e-mail: duffeyrb@gmail.com

The authors' contribution

The author presents the theoretical justification and practical application of the original innovative risk-analysis concept of the structurally complex human-machine systems operation that allows predicting the consequences of the occurrence and impact of the unexpected and emergency situations of different nature on them with acceptable accuracy.

To validate the presented concept, the author collected and compared data on the power loss and outage durations affecting critical infrastructure for a wide range of severe events in Belgium, Canada, Eire, France, Sweden, New Zealand and USA, including Hurricane Katrina flooding New Orleans and the Fukushima reactor meltdowns.

Conflict of interests

The author declares the absence of a conflict of interests.

Methodology of experimental determination of dependability indicators when performing static bending tests of ball valves

Konstantin V. Osintsev[1*], Nikita A. Kuznetsov[2]

[1]South Ural State University, Russian Federation, Chelyabinsk, [2]OOO ChelyabinskSpetsGrazhdanStroy, Russian Federation, Chelyabinsk
[*]osintsev2008@yandex.ru

Konstantin V. Osintsev

Nikita A. Kuznetsov

Abstract. *The quantitative indicators of the dependability characteristics of process equipment, machines and entities include the reliability, maintainability, durability, storability. The* **Aim** *of the research is to develop a methodological framework of experimental determination of dependability indicators when performing static bending tests of ball valves. The aim is to be achieved by solving individual scientific problems, namely the development of the method of static bending testing of ball valves, experimental determination of the destructive test coefficient, analytical calculation of the coefficients of failure, efficiency preservation and product quality. A test stand was developed for experimental determination of the destructive test coefficient. The employed scientific methods of static testing are suggested for the first time ever. The minimal bending test load is the defining value, therefore the experimental work requires a large sample. Additionally, for the ball valve with the lowest endured bending load out of the tested items of the same diameter, it is recommended to use a specially developed methodology to identify such valve as solid-state monolithic units. The conclusions of the conducted experimental and theoretic research are in compliance with the solved research and development objectives. By conducting the experimental research, the authors evaluated the "enhanced" capabilities of ball valves by various manufacturers through comparative analysis of the conducted static bending tests. It is recommended to consider a solid-state monolithic unit along with the operation as part of a pipeline made of a certain material. The destructive test coefficients for the examined ball valves were experimentally determined. Efficiency preservation coefficients were identified that are the basic coefficients of the dependability indicator, that, in turn, is one of the primary dependability characteristics of process equipment, machines and entities.*

Keywords: *ball valve, dependability, static testing.*

For citation: *Osintsev K.V., Kuznetsov N.A. Methodology of experimental determination of dependability indicators when performing static bending tests of ball valves. Dependability 2020; 3: p. 15-20. https://doi.org/10.21683/1729-2646-2020-20-3-15-20*

Received on: *04.04.2020* / **Revised on:** *18.05.2020* / **For printing:** *21.09.2020*

Introduction

Pipeline valves are used in a number of sectors of the economy, for instance, in the oil and gas, chemical, metal, machine-building and energy industries. This paper examines the matters of improving the dependability of valves of heat supply, heating, hot and cold water supply systems. The categories of pipeline valves [1] include isolation, non-return, pressure-relief, distribution and mixing, control, separating and shutoff. The main types of pipeline valves include sliding valves, throttles, tap valves and butterfly valves. This paper examines the ball valves that fall into the category of isolation pipeline valves. The manufacturing process of ball valves is to take into consideration the dependability indicators [2] that will have an effect on faultless operation of industrial pipelines. For instance, the Technical Regulations of the Customs Union introduces the concept of assigned operating life of equipment, upon reaching which the operation of such equipment shall be terminated regardless of its condition [3, 4]. However, the dependability indicators differ from industry to industry and depend on the standard operation model [2].

Relevance of the research topic

The standard operation model, for which dependability indicators are developed, is defined by the specified operating modes of equipment, levels of cooperating factors and loads for each mode, characteristics of the adopted service and repair system [2]. Currently, ball valve manufacturers use various structural materials [5, 6], which, subsequently, involves varied dependability requirements. For instance, each ball valve manufacturer may now designate its product as "reinforced" with no valid reasons, which inconveniences the consumer who is choosing and ordering a ball valve. Thus, it is required to develop a method of testing for classifying valves in terms of the degree of "reinforcement". The method may be based on the existing federal GOST [7], European [8, 9, 10] and Russian industrial [11, 12, 13] standards. The authors suggest developing an additional new standard for static strength testing of ball valves, that would include a classification table (rows) for the purpose of classifying "reinforced" ball valves as a category of its own. The rows are to be made depending on the conventional flow area (nominal dimension) that has no unit of measure and approximately equals the pipeline's diameter. Additionally, the category of "reinforced" ball valves is subdivided into subcategories depending on the range between the test load P_{test} and the maximum load allowed during experimental research $(P_{St})_{\max}$. In other words, it is supposed to distribute the subcategories of "reinforced" ball valves between P_{test} and $(P_{St})_{\max}$ as follows: subcategory "R1" corresponds to load P_{test} + (0.8-1.0)×$[(P_{St})_{\max} - P_{test}]$, subcategory "R2" corresponds to P_{test} + (0.6-0.8)×$[(P_{St})_{\max} - P_{test}]$, subcategory "R3" corresponds to P_{test} + (0.4-0.6)×$[(P_{St})_{\max} - P_{test}]$, subcategory "R4" corresponds to P_{test} + (0.4-0.2)×$[(P_{St})_{\max} - P_{test}]$, subcategory "R5" corresponds to P_{test} + (0.0-0.2)×$[(P_{St})_{\max} - P_{test}]$. As regards the latter case it must be understood that value 0.0×$[(P_{St})_{\max} - P_{test}]$ means none other than the lack of additional reinforcement of a ball valve, and in this case its manufacturer may not claim it is "reinforced". The new standard must also provide basic definitions and take into consideration the effect of external factors on the condition of pipelines, their couplings and valves. The implementation of the new standard is to involve the issue of recommendations and modifications to other industrial standards in terms of dependability rates of pipeline valves.

Procedure and conditions of the research

The authors of the paper have developed an algorithm of static testing of ball valves and individual pipeline sections with valves connected to them. A test stand was created, on which items were tested. A ball valve that complies with the average experimental values and withstands the minimal static load is considered by the authors as a solid-state monolithic unit (SSMU). Upward deviations of this load for other manufacturers' products are used as correction factors. The average values of such coefficients are determined and will be taken as the destructive test coefficient. Out of reference data additional coefficients are selected that are responsible for an entity's dependability. Based on the results of the conducted experimental research, statistical data of ball valve testing is processed, destructive testing coefficients and correction factors (if required) are introduced. The test and reference coefficients form a pool of data that allows calculating the efficiency preservation coefficient C_{ef}.

Goals of the research and problem definition

The Aim of the tests consists in creating a methodological framework of destructive testing as part of static testing of ball valves.

In order to achieve the aim of the research, the following problems are to be solved: definition of the terminology for ball valve dependability indicators; analysis of experimental data based on the results of tests per the authors' method; definition of the most important coefficients and corrections for the standard, recommended as basic efficiency preservation coefficient C_{ef}.

Scientific novelty of the research

As of today, in pipeline valve engineering, there is no conceptual framework for identifying the efficiency preservation coefficient C_{ef} based on experimental data. The method developed by the authors can be extended first to large-diameter ball valves and throttles, and, should the result be satisfactory, be recommended as the foundation for a new dependability standard for pipeline valves. This standard will define the criteria for "reinforced" ball valves reduced to rows, as well as set forth experimental coefficients

that make the efficiency preservation coefficient C_{ef}, such as the destructive test coefficient C_{ds}, etc.

Theoretical part. Dependability of the object of research

According to GOST [14] the primary criterion of dependability is the efficiency preservation coefficient C_{ef} that characterizes the effect of failures of an entity's element on the efficiency of its intended application. At the same time, standards [2, 14] define C_{ef} as recommended, while for each specific case it can be complemented or modified, which depends on the process equipment and industry of application.

The dependability of the object of research is primarily associated with the reliability of its operation. In turn, the reliability of a ball valve is defined by the concept of its "reinforced" capabilities. A well-known method of destructive testing as part of supervision hydraulic testing [9] used in the European Union provides recommendations regarding the test load on ball valves and the formula:

$$P_{test} = 1.5 \times P_{St}, \quad (1)$$

where 1.5 is the coefficient of overpressure relatively to the allowable pressure P_{St} at room temperature. Formula (1) is used for valves designated PN. In case of missing PN data, corrections are introduced.

For the case of static tests, let us use formula (1), but, as the research, among other things, aims to identify the destructive test and correction coefficients, then:

$$P_{test} = K_{\text{THE}} \times (P_{St})_{\min}, \quad (2)$$

where $C_{\text{SSMU}} = 1.5$ is the coefficient of overpressure relatively to the allowable pressure at room temperature for an SSMU, while $(P_{St})_{\min}$ is the average value of the minimal withstood pressure for a ball valve by a manufacturer (SSMU) submitted to the test.

Experimental part

The authors have developed a test stand for the purpose of researching the effect of static bending loads on the strength of ball valves (Fig. 1, general view; Fig. 2, diagram of valve testing; Fig. 3, algorithm of the experiment).

Fig. 1. General view of the destructive testing stand

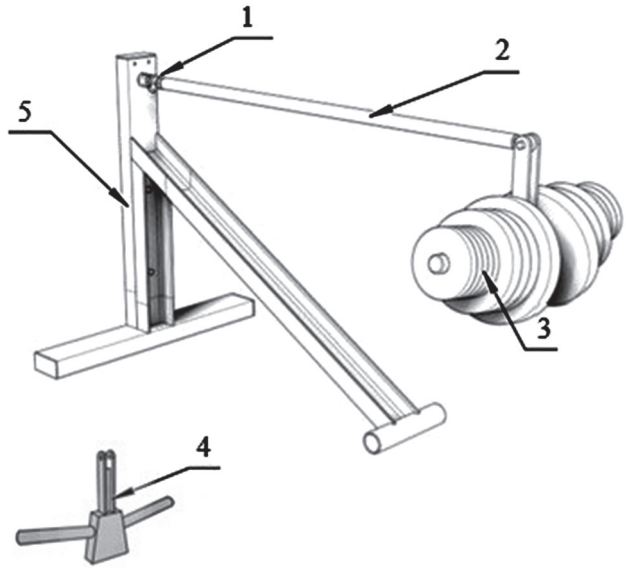


Fig. 2. Diagram of valve testing using the test stand
1 – tested valve; 2 – lever, 4 kg; 3 – weights;
4 – load no. 1, 6 kg; 5 – Stand

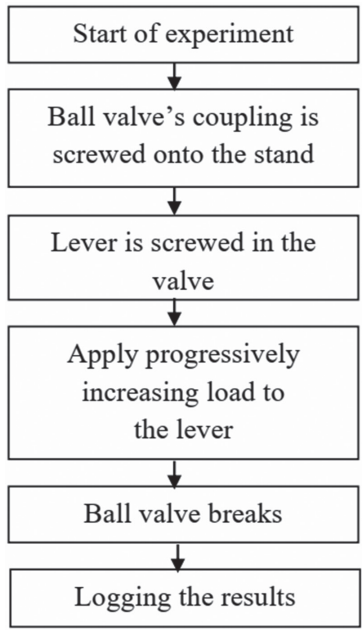


Fig. 3. Algorithm of the experiment.

Similarly, pipelines are tested on the stand.

The algorithms were developed accounting for [12], as well as individual articles and chapters of [13, 14].

The data obtained in the course of the experiment are shown in Table 1.

Let us plot the results summarized in Table 1 in a summary diagram that will also show the static load line.

Using formula (2) we will obtain, given that $(P_{test})_{\min} = 20.5$ kg:

$$P_{test} = C_{\text{SSMU}} \times (P_{test})_{\min} = 1.5 \times 20.5 = 30.75 \text{ kg}. \quad (3)$$

Table 1. Resulting experimental data

	Manufacturer, load, kg		
	1 (China, brass with powder additives)	2 (China, brass)	3 (Russia, brass)
1	19.5	28.5	34.5
2	20.5	28.5	30.0
3	21.5	25.0	33.5
Average	20.5	27.33	32.67

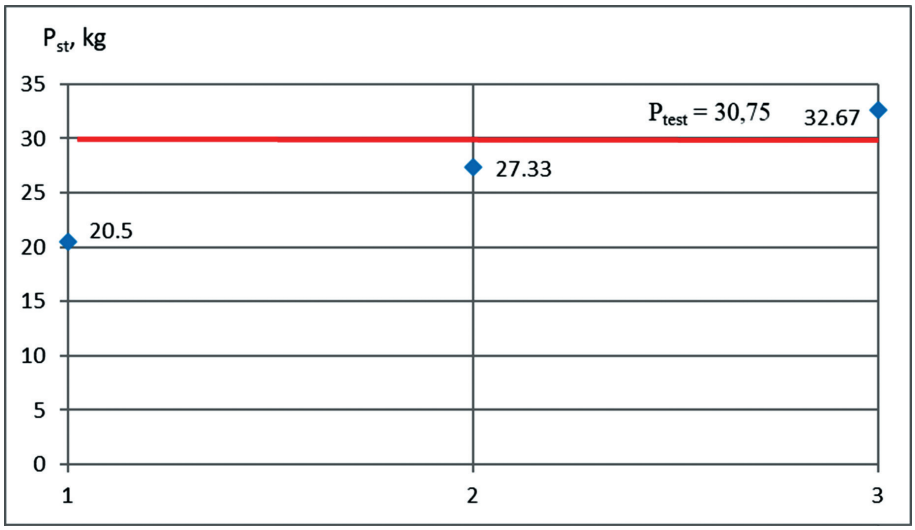


Fig. 4. Summary diagram for identifying the loads on "reinforced" ball valves

In Fig. 4, let us plot the static load line P_{test} = 30.75 kg, according to which we will deduce that ball valves by manufacturer 3 (Russia, brass) can be considered "reinforced" according to the test results.

Visualization of test results

As the result of the experimental activities using the test stand, ball valves by various manufacturers disintegrated under different loads. The test results are visualized in Fig. 5 and 6.

Fig. 5. The results of the conducted dependability tests 1 (China)

Fig. 6. The results of the conducted dependability tests 3 (Russia)

It should be noted that the ball valves get always ruptured in practically the same area.

Destructive testing coefficient

Let us identify the destructive test coefficient that will be used as the primary dependability coefficient:

$$C_{dt} = (P_{St})_i / [C_{SSMU} \times (P_{St})_{min}], \quad (4)$$

where C_{dt} is the destructive testing coefficient, while $(P_{St})_i$ is the average value of the withstood pressure for a ball valve by a manufacturer (i-th manufacturer) submitted to the test.

As the method of static bending tests under development is not standard, the formula of hydroproof testing can only be used as a reference. Given the recommendations regarding the processing of experimental data:

$$P_{test} = (P_{testA} + P_{testB})/2, \quad (5)$$

where P_{testA} is the average value of the test bending load of a ball valve, P_{testB} is the average value of the test bending value of a pipeline.

Thus, generally speaking, a "reinforced" small-diameter ball valve will be deemed as such if it complies with the experimental conditions:

$$P_{test} > C_{SSMU} \times (P_{test})_{min}. \quad (6)$$

Definition of experimental coefficients

According to formula (4), the authors deduced experimental coefficients and summarized them in Table 2.

Table 2. Coefficients obtained during the experiment

C_{dt}		
1 (China, brass with powder additives)	2 (China, brass)	3 (Russia, brass)
0.67	0.89	1.06

According to test data, manufacturer (1) has the lowest dependability coefficient that the authors defined as the destructive test coefficient.

Dependability coefficient according to reference data

According to [2], it is required to introduce correction coefficients for the end product depending on its characteristics:

1. A ball valve is taken as a non-restorable item of a heat supply system, therefore we adopt the failure coefficient $C_f = 0.96$ for all ball valves by various manufacturers.

2. The efficiency preservation coefficient depends on the type of valve. A ball valve for heat supply systems uses process water, therefore $C_{ep} = 0.97$.

3. The quality of manufacture and material will be estimated with the product quality factor C_{pq}. This coefficient will be preliminarily taken as $C_{pq} = 0.99$ for manufacturers (2) and (3) and $C_{pq} = 0.97$ for manufacturer (1).

Efficiency retention factor according to the developed methodology

As the result, using the formula developed by the authors, we will deduce the efficiency preservation coefficient.

$$C_{ef} = C_{dt} \times C_f \times C_{ep} \times C_{pq}, \quad (7)$$

We will obtain data for the efficiency preservation coefficient and summarize them in Table 3.

Table 3. Calculated efficiency retention coefficients

C_{ef}		
1 (China, brass with powder additives)	2 (China, brass)	3 (Russia, brass)
0.61	0.82	0.98

According to Table 3, all coefficients proved to be below 1. Therefore, the authors have correctly chosen the initial experimental conditions.

Recommendations regarding further development of methodological framework

The authors of the paper stress that the developed methodological framework requires additional tests and experimental trials. Thus, the minimal bending test load $(P_{test})_{min}$ is the defining value, therefore the experimental work requires a large sample. Additionally, in this case the authors recommend defining the ball valve with the lowest endured bending load out of the tested items of the same diameter as the SSMU using the method under development.

Conclusions

1. As the result of experimental research the authors evaluated the "enhanced" capabilities of ball valves by various manufacturers through comparative analysis of the conducted static bending tests of the valves.

2. It is recommended to consider an SSMU along with the operation as part of a pipeline made of a certain material. The pipeline is also recommended to submit to static load tests.

3. As the result of conducted experimental research, the ball valve by manufacturer (1) was identified as the SSMU. Given the SSMU, the minimal test load was identified as $(P_{test})_{min} = 20.5$ kg.

4. The destructive test coefficients for the examined ball valves were experimentally determined.

5. Efficiency preservation coefficients were identified, that, according to [2], are the basic coefficients of the reliability indicator, that, in turn, is one of the primary dependability characteristics of process equipment, machines and entities.

References

[1] GOST 24856-2014. Pipeline valves. Terms and definitions. Moscow: Standartinform; 2015. (in Russ.)

[2] GOST 27.003-2016. Industrial product dependability. Contents and general rules for specifying dependability requirements. Moscow: Standartinform; 2018. (in Russ.)

[3] [Technical Regulations of the Customs Union On the safety of equipment operating under excess pressure (TRCU 032/2013) of November 18, 2013]. (in Russ.)

[4] [Technical Regulations of the Customs Union On the safety of machines and equipment (TRCU 010/2011) of October 18, 2011]. (in Russ.)

[5] Ball valves types, construction, applications and advantages. [accessed 01.04.2020]. Available at: http://www.pipingguide.net.

[6] [Ball valves]. [accessed 01.04.2020]. Available at: http://www.chsgs.ru. (in Russ.)

[7] GOST 16504-81. Product test and quality inspection. Moscow: Standartinform; 2011. (in Russ.)

[8] API Standard 598. Valve Inspection and testing; 2004.

[9] BS EN 12266-1: 2012. Industrial valves – Testing of metallic valves. Part 1: Pressure tests, test procedures and acceptance criteria – Mandatory requirements.

[10] BS EN 12266-2: 2002. Industrial valves – Testing of metallic valves. Part 2: Tests, test procedure and acceptance criteria – Supplementary requirements.

[11] [ST TsKBA 008-2014. Pipeline valves. Calculation and assessment of dependability and safety at the stage of design]. Saint Petersburg: Izdatelstvo ZAO NPF TsKBA. (in Russ.)

[12] [ST TsKBA 092-2014. Valves for long-distance pipelines. Design loads caused by pipeline. Methods of calculation and numerical values]. Saint Petersburg: Izdatelstvo ZAO NPF TsKBA. (in Russ.)

[13] [ST TsKBA 008-2014. Pipeline valves. Periodic testing. General requirements]. Saint Petersburg: Izdatelstvo ZAO NPF TsKBA. (in Russ.)

[14] GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

About the authors

Konstantin V. Osintsev, Candidate of Engineering, Head of Department of Industrial Heat Power Engineering, South Ural State University, Russian Federation, 454080, Chelyabinsk, 76 Lenina Ave., e-mail: osintsev2008@yandex.ru.

Nikita A. Kuznetsov, Engineer, OOO ChelyabinskSpetsGrazhdanStroy, Russian Federation, 454010, Chelyabinsk, 47 Yeniseyskaya Str. e-mail: kna@chsgs.ru.

The author's contribution

K.V. Osintsev developed a methodological substantiation of experiments using destruction test stands, suggested using new dependability coefficients and rows of "reinforced" ball valves.N.A. Kuznetsov conducted a research using the destruction test stand, processed the experimental results.

Conflict of interests

The authors declare the absence of a conflict of interests.

Original article
https://doi.org/10.21683/1729-2646-2020-20-3-21-26

Development of an alternative dependability terminology

Nikolay I. Plotnikov, *AviaManager Research and Design Institute of Civil Aviation, Russian Federation, Novosibirsk*
am@aviam.org

Nikolay I. Plotnikov

Abstract. Aim. *This paper contains a brief historical overview of the evolution of the technology dependability theory. The evolution of the concept of dependability reflects the unsolved problem of presentation of the scope and content of concepts in the dependability theory of technical objects. It is proposed to logically elaborate and deduce the terms based on the pseudophysical propositional logic. The paper presents an approach to solving the problem of introduction of the concept of an object's intended use and deduction of alternative basic definitions of dependability. The aim of the paper is to examine the feasibility of applying the modern technology dependability theory to subsequent theoretical developments and practical application of the concept of reliability of organizations, social groups and individuals.* **Methods.** *The problem of the terminology and years-long search for the definitions of dependability consists in the deficiency of the academic development of the subject matter in philological, philosophical and logical terms. Certainly, such research is to be conducted by experts in the appropriate fields of knowledge. Let us make our own contribution as regards the subject matter of this paper. The author suggests a structural approach to terminological research. Essentially, it consists in the following. If identifying the signs of the concept content is complicated, structuring the concept scope may be an option. The structuring is done using universal observation bases: time, space, groups and their combinations: time-space, time-group, space-group. For that purpose, a special terminology is required. The category of "intended use" as an object's property is introduced. The concept of intended use is large in scope, is more abstract than the concept of dependability. Let us note that quality standards were developed under the assumption that the intended use is the compliance of an object's characteristic with the requirements. Russian standards prioritized the dependability concept, where the regulatory descriptions, definitions, such as "the ability to perform the required (specified) functions, (an object's) ability to function", "to function as and when required", "functional dependability", "parametric dependability", "requirements specified in the documentation" are simply generalized by the category of intended use Such descriptions are none other than an indication of the property of an object's intended use. For instance, an object's ability to move in space is a property of the intended use, not dependability. Thus, all the terminological searches in terms of dependability standardization demonstrate an unjustified reduction of the concept of intended use to the concept of dependability. The introduction of the category of intended use solves the problems of terminology in the dependability theory. The author suggests the following definition of intended use. Intended use is the property of an object defined by the natural origin or designed application. Dependability is a set of states as the measure of concordance with the intended use of an object.* **Conclusion**. *The evolution of the concept of technology dependability reflects the unsolved terminological problem in the dependability theory of technical objects. The problem of terminology largely consists in the ambiguous use and confusion of ontological terms. Deduction of such terms based on pseudophysical logic and introduction of the category of object's intended use is the main result of this paper in terms of the introduction of an alternative noncontroversial structure and content of dependability-related terms. The suggested approach is recommended to be used for revision of the existing standards.*

Keywords: *dependability, terminology, ontological terms, property, state, event.*

For citation: *Plotnikov N.I. Development of an alternative dependability terminology. Dependability 2020;3: 21-26. https://doi.org/10.21683/1729-2646-2020-20-3-21-26*

Received on: *25.10.2019* / **Revised on:** *15.05.2020* / **For printing:** *21.09.2020*

1. Introduction

Standard descriptions of dependability were developed for engineering, industrial products, machines and devices. The research of dependability is associated with the theory of life safety and risks. This paper examines the problem of terminology as part of dependability standardization. The aim of the paper is to examine the feasibility of applying the modern technology dependability theory to subsequent theoretical developments and practical application of the concept of reliability of organizations, social groups and individuals.

2. Problem of terminology in the dependability theory of technology

Since the introduction of the term of industrial product dependability and emergence of the first respective documents in the 1950s, there has been an ongoing discussion of the problem of dependability terminology, specificity as regards the specification of the fundamental term of "dependability". The regulatory framework includes Russian and interstate standards: GOST 13377-67; GOST 13.337-75; GOST 27 002-83; GOST 27.002-89; GOST 27.002-2015; GOST R 51901.3-2007 (IEC 60300-2: 2004); GOST ISO 9000-2011; GOST R 27.002-2009. The concept of dependability is examined much wider in standards related to the terminology of quality, risk, safety: GOST 15467-79; GOST R 51901-2002; GOST R 51897-2002; GOST R 51898-2002; GOST 51901.14-2005 (IEC 61025: 1990); GOST R 51901.12-2007; GOST R 53480-2009; GOST R ISO/IEC 31010-2011.

The semantic descriptions of the concept of dependability in the documents can be reduced to the following: "… property of the system to perform the task, … specified functions, … specified indicators within the given ranges, … parameters characterizing the ability to perform the required (specified) functions…" The same is true with the semantic descriptions in the IEC dependability standards: "the ability (of an object) to function as and when required".

The concept of *good state* of a technical device is the initial description that defines the content and scope of the concept of dependability. As machines can operate in a partially faulty state, the definition of [good/faulty state] becomes blurry. The introduction of the term "failure" defines the impossibility to use an engineering product. That caused the definition of dependability through *reliability* and additionally: durability, maintainability, storability. Next, the concept of the *up state* was introduced. GOST R 27.002-2009 defines dependability through *availability*, while GOST 27.002-2015 [3] defines it through *ability*. Thus, the evolution of terminology from 1950 to this day shows roughly the following sequence of replacement of the concept of dependability with other generalized "explicative" concepts:

$$\text{DEPENDABILITY} \cong$$
$$< (\text{good state}) \rightarrow (\text{reliability}) \rightarrow (\text{operability}) \rightarrow (\text{availability}) \rightarrow (\text{ability}) >.$$

A detailed account of the content and historical analysis of the regulatory documents on dependability terminology was presented in [1, 2]. In the author's opinion, the introduction of standard [3] does not resolve the problem of standardization of the dependability terminology. Let us examine the basic definitions in this standard.

Section 3 "Terms and definitions", Item 3.1 "Basic definitions": "3.1.5. **dependability**": The property of an object to maintain in time the ability to perform the required functions in specified modes and conditions of operation, maintenance, storage and transportation. Note 2. Dependability is a composite property that, depending on the intended use and operating condition of the object, may include reliability, maintainability, restorability, durability, storability, availability or certain combinations of such properties". Further in the standard, the above properties are defined. In Item 3.2 "States", the following definitions are introduced: "3.2.1 good state: …, 3.2.2 faulty state: …". In other words, the above properties are also considered as states.

In Item 3.4 "Failures, defects, damage", the terms "failure" and "damage" are defined as *events*, while "defect" is defined as the object's *non-compliance* with the requirements specified in the *documentation*. The "causes of failure are provoked", while the "consequences of a failure are conditioned" in a simultaneous and joint total: *phenomena, processes, events and states*. In Item 3.5.5, restoration is considered both as a process and an event. The standard is full of such cases.

The concept of *dependability*, without any doubt, is abstract, i.e. is a category. That is the main reason of the terminology problem and unchanging need to define dependability through other concepts. To make matters worse, compound words are used, such as reliability, maintainability, durability, restorability, etc., which further complicates the solution of the problem. In logic, the definition of a concept that leads to a term is based on the content (signs), rather than the scope of such concept. If signs are successfully identified, the definition is considered to be strong, quantitative, suitable for object properties calculation. Otherwise the definition comes down to a simple replacement with another concept or several concepts ("dependability is reliability", etc.). In other words, the definition of the term is descriptive, weak and ill-suited for quantitative estimation. In our opinion, identifying the signs of the *content* of the concept of dependability "directly" does not appear to be possible.

The problem of the terminology and years-long search for the definitions of dependability consists in the deficiency of the academic development of the subject matter in the philological, philosophical and logical terms. Certainly, such research is to be conducted by experts in the appropriate fields of knowledge. Let us make our own contribution as regards the subject matter of this paper.

3. Research of the dependability terminology

The philological aspect. The philological examination of the concept of dependability is possible in the lexical and grammatical aspects. The word "dependability" is often searched for in technical literature with no tangible results. Normally, the definition is descriptive and repeats the content set forth in technical documents. Encyclopedias, specialized and explanatory dictionaries enable defining the scope of a concept, but identifying the signs of the content, which is required for term derivation, proves to be unsuccessful.

In the lexical-grammatical aspect, the morphological structure of the word "dependability" consists of the prefix de-, root -pend- and suffix -ability. The lexical-grammatical class of the word *dependability* presents a suffix abstract noun that designates a quality (property) or state of an object, motivated by the adjective *dependable* with the meaning of an abstract sign. "Nouns with a suffix represented with the morpheme -ability with the meaning of "carrier of a sign" designate an abstract state [4, p. 164]; … with the meaning of abstract sign, designate a state with an abstract meaning of a sign, property" [4, p. 177]. It has been theoretically established that nouns are motivated (governed) by adjectives in pairs: "dependability – undependability". Out of this context and the general linguistic definitions, it is impossible to identify, what exactly the noun "dependability" and the adjective "dependable" designate: a property, a state, a sign of an object. Thus, attempted philological research does not bring us closer to the solution.

Analysis of ontological terms in logic. Let us examine how terms, definitions and reducibility of terms are established in logic. Abstract concepts (categories) are also called ontological terms (time, space, beginning, end, cause) that are later specified (defined) with logical terms. The theory of concepts, a sub-discipline of classical logic, has it that the scope and content of categories are the most difficult to define. Furthermore, the most abstract categories such as entity, thing, quality and others are not generalizable at all in terms of scope and their sign cannot be identified in terms of content.

First, the term (object) is specified. Then, the predicate (*sign*) is specified. The term and the predicate are correlated. "The predicate "red" (and the sign corresponding to the "redness") is one-place. The predicate "bigger" (and the size sign "bigger") is two-place. A predicate with the correlation ≥ 2 is n-place. One-place signs are called properties. N-place signs are called relationships [5, p. 61], i.e. assertions with multiplace predicates. Reducing terms to simple ones is the most important problem of logical analysis of scientific knowledge. "Defining a term means establishing its meaning using other terms, whose meaning is already known" [5, p. 228]. Terms are subdivided into initial and derived ones.

D-1. The term t^1 is initial in relation to the term t^2, while t^2 is derivative in relation to t^1 if and only if t^1 is used in the creation (specification of the meaning) of t^2" [5, p. 62].

The creation (introduction) and definition of ontological terms is the most important part of the problem of this paper as regards the terms "property", "state", "event", "situation", "process".

The categories of "property" and "state". There are no definitions of the concepts of "property" and "state" in the technology dependability standards. Meanwhile, the difference between those concepts is not trivial. According to Aristotle, "a *property* (hexis) is the manifestation of a certain activity by that which possesses and what it possesses; such an arrangement towards another, for example, health, is a certain property"…, "a transient property or *state* (pathos) is a property subject to possible changes; various manifestations of such properties and applications" [4, p. 244]. A property is a quality, a state is a quantity.

Examples. (1) A body has the property of weight and can be in the states of movement and rest. (2) The property of water manifests itself in the states of liquid, solid, gaseous (vaporous), crystalline. It can be said that water has a "composite property" and manifests itself in the "sub-properties" of liquid, ice, vapour, snow. However, it is preferable to explain the states.

Thus, in the existing standards, the definition of dependability as a *property* of an object is up to discussion and selection. In our opinion, the concept of dependability is a *state* of an object. That is substantiated below.

The categories of "event" and "process". In [8], the following definitions are introduced:

113-01-04 event: Something that takes place, happens, occurs in a random point in space-time;

113-01-06 process: A time sequence of correlated events.

Those definitions do not satisfy the objectives of this paper, as they are descriptive, weak. In scientific literature, the definitions of the terms under consideration are often missing, are not reduceable to each other or equated to each other. It would be sufficient to note that in D.A. Pospelov's book [Situational management] [9] the concept of "situation" is not defined. According to A.A. Zinoviev, "If X is a statement, then ↓X is a term of event (or state). Events exist or do not exist in a certain given or any situation" [5, p. 166]. Clearly, the terms "event" and "state" are equalized to each other. It is explained that a situation is defined by specifying the following: a) spatial area, b) time, c) event or set of events, d) combination of (a, b, c) is express; or follows from the context. However, out of the above logical construct do not directly follow the definitions of the terms "event", "situation" and others. In our opinion, the definitions can be deduced only using the pseudophysical (pseudological) method.

Deduction of the term of pseudophysical logic. The pseudophysical logic (PL) (term coined by D.A. Pospelov [9]) of the correlation between time, space, causality and their combinations allows deducing the definitions required for subsequent explanation. Let $|O_i|$ be the term, the observed object. Let us represent the following definitions and examples of reality.

D-2. An object's transitions in mapping spaces are called *ascending* if directed towards higher dimensionality: $O_i : s_i\, s_{i+1}, \ldots, s_{i+k}$, $i \in \overline{1,n}$, where n is the number of an object's states.

An example: the moment an aircraft lifts off the runway and starts moving in a three-dimensions space.

D-3. An object's transitions in mapping spaces are called *descending* if directed towards lower dimensionality:, $O_i : s_i\, s_{i-1}, \ldots, s_{i-k}$, $k \in \overline{1,n-1}$ number of transitions.

An example: the moment of an aircraft's landing and transition to movement in a two-dimensional space.

D-4. An object's transitions in mapping spaces are called *symmetrical* if directed either way of the same (higher or lower) dimensionality: $O_i : s_i\, s_{i\pm1}, \ldots, s_{i\pm k}$.

An example: a) moment of the acceleration run at the decision speed; b) the moment at the landing decision point height when the decision is made to land or execute a go-around.

D-5. Object mapping in ascending transitions is called the *involution* of object description data.

D-6. Object mapping in descending transitions is called the *convolution* of object description data.

Defining the terms "event", "situations" is only possible at the convergence of the temporal and spatial logic. A complete derivation of ontological terms is only possible at the convergence of the temporal, spatial and causal logic, which requires additional research.

D-7. A representation of an object in transitions from space to space s_i in the moment in time t_i we call an *event*: $e_i : (t_i s_i\, s_{i\pm1}, \ldots, s_{i\pm k})$, where e_i is the object mapping operator for transition from space to space.

An event, set E, $e_i \in E$ is the association of the PL of relationships between the time and the space $e_i(t_i, s_i)$.

D-8. The set of associations of the PL of relationships between the time and the space we call a situation.

In the above definitions and examples: a situation is a set (beginning of movement and stopping of an object, take-offs and landings, decisions made) of events in ascending, descending, symmetrical transitions.

In [8], there is no definition of the concept of "state". Let us introduce the following definition.

D-9. A **state** is a parameter, set of parameters of an object's properties within the observed time intervals ("113-01-10 time interval): Part of the axis of time limited by two moments" [8]).

In this definition, the concept of state is defined as the **parameter** of *commensuration* of indicators (combined and simultaneous). For instance, the speed of a vehicle is *commensurated* with two indicators: distance and time.

4. Solving the problem of development of the dependability terminology

The structural approach. The author suggests a structural approach to terminological research. The essence of such approach consists in the following. If identifying the signs of the concept *content* is complicated, structuring the concept *scope* may be considered. The structuring is done using universal observation bases: time, space, groups and their combinations: time-space, time-group, space-group [6]. It has been empirically established that the dependability of an object of any nature changes in time in steps, the so-called U-shaped profile: entry (below the norm), normalization, ageing (below the norm). Subsequently, the dependability of any object can be reliably observed (measured, evaluated) according to the U profile. For that purpose, a special terminology is required.

We suggest a strict hierarchic structure of terms. An object has a name. The intended use of an object specifies its property. A property is observed (measured, evaluated) in states or parameters. States are formed by a set of indicators. Indicators are specified based on values. For the purpose of calculating an object's properties, an information unit (IU) is defined with an n-placed five:

{1, assignment $\subseteq$ 2, property $\subseteq$ 3, state (parameter) $\subseteq$ 4, indicator $\subseteq$ 5, value}.

D-10. The IU is single-point if the subset corresponding to the value is single-point and cannot be divided into parts.

D-11. The precision is associated with the value.

Each element of the IU is observed (identified, defined) based on signs. An IU has a hierarchy, does not allow for ambiguous interpretation and arbitrary application of terms. The presented system of terms is a universal model, can be used for calculating the states of objects of any nature. The structure of terms is shown in a diagram in [10, p. 91].

The structural approach also implies the search for and establishment of a more abstract (in relation to the researched one) umbrella term. In our opinion, the category of *intended use* is such a concept. Below is the substantiation.

The category of "intended use" as an object's property. The concept of intended use is large in scope, is more abstract than the concept of dependability. Let us note that the quality standards (ISO) were developed under the assumption of the intended use being the compliance of an object's characteristic with the requirements (GOST ISO 9000-2011: "Quality: the degree of compliance of the sum and the intrinsic characteristics with the requirements").

Russian standards prioritized the dependability concept, where the regulatory descriptions, definitions, such as "the ability to perform the required (specified) functions, (an object's) ability to function", "to function as and when required", "functional dependability", "parametric dependability", "requirements specified in the documentation" are simply generalized by the category of intended use. Such descriptions are none other than an indication of the property of an object's intended use. For instance, an object's *ability* to move in space is a property of intended use, not dependability.

If an automobile "is sitting in traffic" (the example given in [2]), is not intended to also be a helicopter or an airplane like in the 1965 movie Fantomas Unleashed, it is its intended

use per the design, i.e. moving in a two-dimensional space. Therefore, an absolutely dependable automobile will sit in traffic "dependably" and motionlessly.

Thus, all the terminological searches in terms of dependability standardization demonstrate an unjustified reduction of the concept of intended use to the concept of dependability. **The introduction of the category of intended use solves the problems of terminology in the dependability theory.** The author suggests the following definition of intended use.

D-12. Intended use is the property of an object defined by the natural origin or designed application.

The property of natural origin: the intended use of "a pike who lives in the lake is to keep all fish awake".

This definition is introduced for a simple object. The intended use of a complex object may be considered as a combination of property elements. If we adopt the proposed point of view that the concept of intended use is a property, then all the derived concepts are states. In the context of this paper, such states include dependability, safety (security), risk, efficiency, etc.

The problem of alternative terminology in the dependability theory of technology. Given the above, let us present an example (model) of the development of an alternative dependability theory terminology. Only the basic definitions are suggested. This paper does not aim to completely rework the standard.

D-13. Dependability is a set of states as the measure of concordance with the intended use of an object. The alternative definitions are given below (Table 1).

The example of terminology development does not provide for analogous use of terms like "good state". We assume that terms related to events and processes are to be carefully examined in terms of the philological and logical aspects in order to establish clear distinctions. Thus, among other things, instead of the term "defect" the term "breakdown" should probably be used.

5. Conclusion

The evolution of the concept of technology dependability reflects the unsolved terminological problem in the dependability theory of technical objects. The problem of terminology largely consists in the ambiguous use and confusion of ontological terms. Deduction of such terms based on pseudophysical logic and introduction of the category of an object's intended use is the main result of this paper in

Table 1. Example of the development of an alternative terminology in the dependability theory of technology

GOST 27.002-2015	Alternative definitions
3.2 States	States of dependability
3.2.1 good state: The state of an object, in which it complies with all the requirements specified in the respective documentation	**Good state**: a state that complies with the intended use of the object subject to allowable damage.
3.2.2 faulty state: The state of an object, in which it does not comply with at least one of the requirements specified in the respective documentation	**Faulty state**: a state that does not comply with the intended use of the object due to defects.
3.2.3 up state: The state of an object, in which it is able to perform the required function	**Up state**: a state that complies with the intended use of the object.
3.2.4 down state: A state of an object, in which it is unable to perform at least one of the required functions due to reasons depending on it or due to preventive maintenance	**Down state**: a state that does not comply with the intended use of the object.
3.4 Failures, defects, damage	Events of disrupted dependability
3.4.1 failure: An event consisting in the disruption of an object's up state.	**Failure:** an event of disruption of an object's up state.
3.4.2 defect: Each individual non-compliance on an object with the requirements specified in the documentation	**Defect:** an event of disruption of an object's good state.
3.4.3 damage: An event consisting in the disruption of an object's good state under condition of retained up state.	**Damage:** an event of an object's disrupted good state under condition of retained up state.
3.5 Maintenance, restoration and repairs	Dependability restoration processes
3.5.2 Maintenance: A set of organizational actions and technical operations aimed at maintaining the operability (good state) of an object and reducing the probability of its failures in the course of intended use, storage and transportation.	**Maintenance**: the process aimed at maintaining the up and good state of an object.
3.5.5 recovery: A process and event consisting in the transition of an object from the down state into the up state.	**Recovery:** a process aimed at causing the transition of an object from the down state into the up state.
3.5.9 repairs: A set of technical operations and organizational actions aimed at recovering the good or up state of an object and restoration of the operating life of the object or its components.	**Repairs:** a process aimed at causing the transition of an object from the faulty state into the up state.

terms of the introduction of an alternative noncontroversial structure and content of dependability-related terms. The suggested approach is recommended to be used for revision of the existing standards.

References

[1] Netes V.A., Tarasyev Yu.I., Shper V.L. Current issues of terminology standardization in dependability. *Dependability* 2014;2:120-123.

[2] Netes V.A., Tarasyev Yu.I., Shper V.L. How we should define what "dependability" is. *Dependability* 2014;4:15-26.

[3] GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

[4] [Russian grammar]. Moscow: Nauka; 1980. (in Russ.)

[5] Zinoviev A.A. [The logic of science]. Moscow: Mysl; 1971. (in Russ.)

[6] Aristotle. Politics. Metaphysics. Analytics. Moscow: Eksmo; Saint Petersburg: Midgard; 2008.

[7] Klir G. Architecture of Systems Problem Solving. Moscow: Radio i sviaz; 1990.

[8] GOST IEC 60050-113-2015. International Electrotechnical Vocabulary. Part 113. Physics for electrotechnology. Moscow: Standartinform; 2016. (in Russ.)

[9] Pospelov D.A. [Situational management]. Moscow: Nauka; 1986. (in Russ.)

[10] Plotnikov N.I. The bases of human-operator dependability theory]. *Dependability* 2015;2:94-97.

About the author

Nikolay I. Plotnikov, Candidate of Engineering, Director General, AviaManager Research and Design Institute, Russian Federation, Novosibirsk, e-mail: am@aviam.org.

The author's contribution

The author analyzed technology dependability standards. A verbal, lexical-grammatical and logical analysis of the concept of dependability was performed. A new alternative definition of dependability was proposed along with proposals as to the standard's modification.

Conflict of interests

The author declares the absence of a conflict of interests.

European railway operators' experience in managing the dependability and safety of technical assets using advanced digital technologies

Alexey M. Zamyshliaev, *JSC NIIAS, Russian Federation, Moscow*
A.Zamyshlaev@vniias.ru

Alexey M. Zamyshliaev

Abstract. *The Aim of the paper is to analyze and examine the experience of the railway companies of the European Union in designing technical asset management systems based on advanced digital technologies. Railway companies are interested in the development of efficient maintenance and repair strategies that allow increasing the volume of traffic with a high level of safety and reliability using the Big Data produced by diagnostic systems.* **Methods.** *A comparative analysis of the best practices by European railway companies was performed, the employed digital technologies were compared, and the best known and commercially available software solutions for constructing an asset management system were reviewed.* **Findings/ Conclusions.** *Railway companies will have to make a lot of effort in order to not let the vast current expenditures associated with the digitization go to waste, since the deployment of new technology will meet the resistance of the existing system of management and allocation of responsibilities between levels of management within a company. The generic architecture of the European asset management information framework is a highly diverse range of IT solutions, which is a great challenge, as any modification to the operation of the software system requires significant time, managerial and financial resources. In this context, most successful are the companies that have invested in the development of own digital asset management frameworks.*

Keywords: *technical asset management, dependability, safety, risk, railway transportation, railway company infrastructure, maintenance, decision support, digital technology, software, URRAN.*

For citation: *Zamyshliaev A.M. European railway operators' experience in managing the dependability and safety of technical assets using advanced digital technologies. Dependability 2020;3: 27-33. https://doi.org/10.21683/1729-2646-2020-20-3-27-33*

Received on: *11.06.2020* / **Revised on:** *26.06.2020* / **For printing:** *21.09.2020*

1. Introduction

This is especially vital in dynamically changing circumstances of the post-covid world and low oil prices when the established economic relations between countries are being replaced by others due to new societal demands in essential commodities, medicine and equipment and due to market conditions. Nowadays there appear new logistic supply chains and transport routes respectively that have not been used before. In this context we may expect a demand increase for transportation in one direction and a downright cut in other. Such a disproportion can bring a long line of serious problems for railway companies; in particular they have to invest much in renovation and improvement of their infrastructure, to maintain it in good state while supporting a growing volume of transportation. So, railway companies are interested in developing efficient maintenance strategies allowing to increase transportation volumes with a high level of safety and dependability while keeping risks at an acceptable level, based on so called Big Data of diagnostics systems. In order to efficiently manage railway infrastructure and rolling stock, one shall know their current technical state and be able to predict their state in future.

2. State-of-the-art of digitalization of infrastructure maintenance on EU railways

At present there are a lot of talks about the demand for implementation of disrupting (including digital) technologies on railways. Besides obvious benefits, digitalization can bring some serious problems for railway companies. There can be cases when a grade of automation has been wrongly chosen, or wrong parameters have been used for generation of a database of technical assets, or even worse, a company has no objective information about a current real state of technical assets, and available information is just some irrelevant reports produced by quasi-automated systems that are operated in line with the processes described by hired business consultants.

It is also very important to have a clear idea about the size of planned financial expenditures. Advanced technologies of data collection, transfer and analysis in the nearest future can radically change the maintenance rules adopted today on railways and in principle based on a normative approach. Monitoring systems for technical facilities of infrastructure and rolling stock are becoming more available, and they generate huge amounts of data that has been called Big Data, Internet of Things (IoT), Internet of Services (IoS), machine self-learning – all these concepts are actively taking their places in short-term digital strategies of railway development. Today the hot subject of researches is becoming the search for a balance between a rate, process costs, data transfer speed and power consumption of such multisensory systems. As a small example, there is DIANA system [1] developed by infraView for the purpose of diagnostics and analysis of DB infrastructure components. In 2016 over 6500 switches were connected to it, while in 2019 they already amounted to 25 thousands, and in 2020 the system controls 30 thousands of switches. Even today such smart systems begin to generate very huge amounts of data. Their transfer, storage, processing and analysis will become important issues in the years to come. Therefore, there arises a question whether these Big Data are consolidated, analyzed and used by railway companies in the right way. As when using prediction, it is difficult to assess whether various risk levels are acceptable and to take measures that would have seemed too risky before. For instance, one may reduce redundancy and cut the costs of technical maintenance if a decision making person believes it acceptable when a wheel pair achieves a limit state prior to a scheduled repair, though previously he would immediately have sent it for repair. However, while balancing at the level of risks, one should understand that decision makers will also have to balance at the level of responsibility for risk-related decisions made. Therefore, railway companies will have to take a lot of efforts so that the huge investments that they are currently putting into digitalization should not be lost, since the implementation will face opposition from the established system of administration and distribution of responsibility among management levels within a company.

In this context, some positive experience accumulated by the Federal railways of Austria ÖBB can be useful for other railway companies. ÖBB strives to take a lead in implementing ISO 55000 on railway transport and successfully verifies this intention in practice, by getting the ISO 55000 asset management certificate the first among all European railway companies in February 2019 for shifting to track maintenance based on the following principles:

- periodic full renovation of track;
- application of a current maintenance program combining preventive measures and those based on information about a real track state received by regular inspections;
- cancellation of permanent speed restrictions on mainlines;
- rehabilitation of roadbed when necessary on mainlines with dense traffic and at locations of switches.

The company experts have developed a unified network plan of asset management detailed for each technical department.

The ÖBB administration pays a lot of attention to the issues of IT support for the asset management system as a major tool for implementation of this methodology. Thus, from 2013 till 2018 the ÖBB management allocated over 12 mln Euro for the development of an IT platform. As a result of the work, Austrian engineers integrated 360 various databases into one database in order to construct an infrastructure asset management system.

Italian railways RFI became a second European railway company who was certified for their asset management system. This has been the first and the only certification in Italy accredited by Italcertifer through Accredia for physical assets management. The cost of the certification for RFI was over 40000 Euro. As the project manager

Donatella Fochesato said, during the certification procedure 104 processes and 387 sub-processes of the company were described.

The certification is part of a wider strategy aimed at further improvement of network management and generation of an added value for the company as well as for concerned parties.

Irish Rail has invested over 20 mln Euro in constructing an IT system of asset management.

Belgian railways, Infrabel have spent over 10 mln Euro for the development of an IT system for asset management.

General information about EAMS (Enterprise Asset Management System) systems used by some foreign railway companies is given in Table 1.

The generalized architecture of the European asset management IT platform is presented in Fig.1 (authored by Jude Carey, Irish Rail). One can see that it provides rather a diverse spectrum of IT solutions, which project managers in charge of introduction of an asset management in companies admit to be a big problem as making any changes to the platform's software is very time-consuming and requires a lot of financial resources and interactions with an IT department and a software supplier.

Table 1. Examples of EAMS systems at foreign railway companies

Company	Type of EAMS or auxiliary MMS	Year of operation start	Current estimation of satisfaction with applied SW
Irish Rail	Maintenance Management System (IT-tool): SAP PM	Since the beginning of 2000th	There are proposals to improve the functionality, however the high cost of SAP extension prevents the company from including this work in the maintenance contract. Plans are under discussion to transit to IBM Maximo by 2025, though it is complicated to abandon the elaborated solutions, and switching to other IT platform results in a lot of administrative and technical complications
Infrabel, Belgium	SAP	-	-
Network Rail, England	ELLIPSE (supplied by ABB)	2004	No replacement planned, alternatives often proposed, but it would be hard to change the system due to administrative complications, other systems have their own drawback as well
ADIF, Spain	ADIF – proprietary system for tracks and other infrastructure (not for stations)	-	Trying to improve and integrate it with other enterprise systems into a unified management platform
VAYLA, Finland	Raid-e systems (proprietary) RATKO – main data base for railway infrastructure RAIKU – tool for generation of reports about current maintenance (for MMS) RYHTI – tool for planning of infrastructure renovation and refurbishment RAHTI – tool for planning of physical assets	Started at 2016	Still under introduction, early to make conclusions
ÖBB, Austria	Proprietary systems. ARGUS – tool for resources planning MAZE – tool for inspection and harmonization of documents AUER – tool for maintenance invoicing	Since the beginning of 2000th	Systems under permanent improvement. Transit to SAP had been discussed, however it happened too expensive.

Generalized architecture of the European asset management IT platform

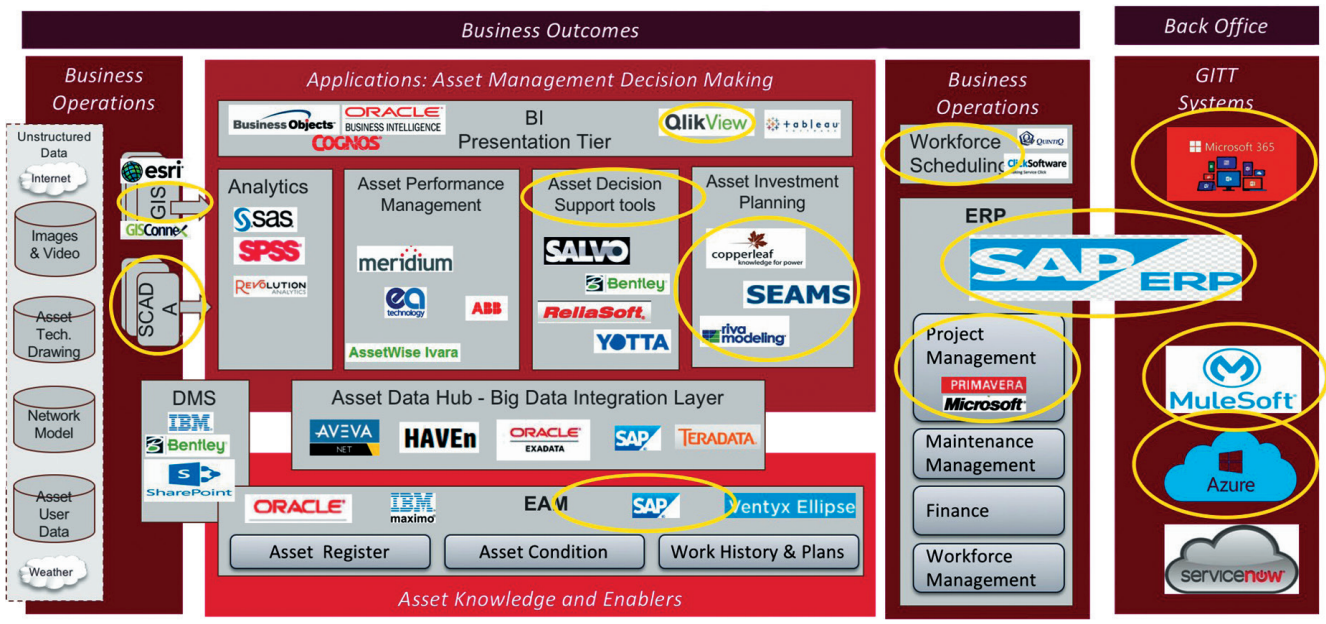


Fig. 1. (authored by Jude Carey, Irish Rail)

3. UIC projects, international interdisciplinary consulting companies' experience and best practices

Assuming the importance of the assessment of expenditures required for maintenance and renovation of a railway network, the International Union of Railways (UIC) as early as 1996 started to collect and analyze respective data within the project Lasting Infrastructure Cost Benchmarking (LISB) [2]. Infrastructure companies from 14 European countries have been participating in the project for over 20 years. The goal of the project is to define levels of railway companies' costs for maintenance and rehabilitation of the current infrastructure as well as to identify factors influencing these costs. It has been found that higher density of a railway network traffic in some cases has resulted in increase of costs for technical maintenance approximately by 5 per cent, and for renovation – by 16 per cent. The LISB project became a starting point for accumulation of statistical data about infrastructure maintenance, collection and analysis of best practices of railways, and exchange of experience among the participants.

In 2007 the UIC established a special Asset Management Working Group (AMWG) that combined the representatives of 10 European railway companies. Russian experts joined the group in 2016. The key areas of activities of the Group are:

- Research in asset management to promote the development of railways;
- Selection of an asset management strategy for railway enterprises;
- Identification of factors accompanying the optimization of asset management methods;
- Improvement of existing methods of asset management;
- Exchange of advanced experience in the area of asset management in the railway domain;
- Unification of methods and development of common approaches, guidelines and standards for railways to introduce technologies for efficient management and decision making support.

In 2010 the group developed the Guidelines for the Application of Asset Management in Railway Infrastructure Organizations [3], which has since been updated regularly based on the annual work results of the Group. In 2015 a Shortlist of Cost Drivers in Railway Asset Management was issued [4]. Based on the statistical data of the project participants, the document identified the impact of various cost factors (so called cost drivers) on the costs of infrastructure technical maintenance, repair and renovation. It was noted that there are quantitative and qualitative cost drivers. Qualitative cost drivers could not be characterized by quantitative values, so they were presented in the document in a descriptive way. In 2016 the UIC issued the ISO 55001 Guidelines for the Application of Asset Management in Railway. The Russian participation in particular contributed to this international document with the experience accumulated by Russian Railways during the development and application of the Integrated system of dependability, risks, resources at all lifecycle stages, called URRAN for short [5-7]. Special attention in the document was paid to risk management. Compared to any other such documents, this document allows to implement the key principles of asset management: "cost reduction by doing the right job at the right place at the right time, as well as by coordinated activities to achieve the best balance between maintenance, renovation and improvement of the entire asset database".

In 2020 the Group initiated a new project called Asset Management Whole System Decision Making (WiSDoM). The goal of the project is the development of the concept and

respective methods and tools for the common asset management system of decision making (hereinafter "the System") intended to ensure railway asset management. The System concept foresees the integration of the "system of systems" approach used in other industries with existing approaches to asset management and very similar in many aspects to the URRAN methodology. The roadmap of the project provides for the development of the concept of the System implementation for the entire infrastructure, common processes and criteria for decision making, definition of methods and tools ensuring decision making, onsite testing, validation of applied methods and proof of concept. The project is planned to last from January 2021 till December 2023.

Besides the Group's permanent members, there are also representatives of interdisciplinary international consulting companies, research institutions and transport companies of Austria, US, Great Britain, Ireland, France, Netherlands etc who take part in the AMWG regular meetings. Since this market is rather young, let us dwell upon them in more detail.

Oxand [8] was founded in France in 2002 and is a leading consulting company in the area of construction of asset and project management systems. The company's portfolio has over 1500 project references in management of realty, railway infrastructure, power supply and industrial enterprises. The key tool is a proprietary software tool Simeo™ that has in its database the information about over 600 types of assets, analysis of 70000 km of railway infrastructure and over 40 mln m^2 of realty. The system incorporates a decision making support module that uses statistical data about various types of technical assets accumulated for 15 years. The major indicators used for decision making are RAMS parameters.

Systra Solutions [9] is an international engineering and consulting group. It was established by French railways SNCF in France in 1957. It offers its own software solutions for constructing lifecycle models, planning investments, managing risks and safety, optimizing costs as well as constructing a predictive maintenance system based on Big Data.

Assetsman [10] was established in France in 2001 by Dr Celso de Azevedo, the pioneer of introduction of an asset management system in France. The company offers business consulting services, trainings and implementation of an asset management system for industrial enterprises using their own software modules such as AssetsValue, AssetsBudget and AssetsLifetime that cover all issues related to management and decision making support for technical asset management based on RAMS, LCC and risk analysis. For training and workshops the company uses the business game AssetsGame. The company is a member of French Institute of infrastructure asset management (inframi) and provides supporting services for ISO 55001 certification.

COSMOTECH [11], France, founded in 2010. A global supplier (vendor) of Enterprise Digital Twins software and applications for simulation and optimization of corporate operational efficiency. The company has developed a large library of customizable models and templates.

3B infra [12], Austria, founded in 2008, provides business consulting services and system solutions for asset management, including realty, technical maintenance of a customer's infrastructure, costs planning and control using a proprietary integrated system of a railway company's infrastructure and operations management – INFRALIFE. A common software platform allows to take into account the current state of infrastructure, to record costs, to plan repairs and to support decision making based on predictive analytics. It can integrate any existing systems of a customer into its control loop.

ALD [13], Israel, established in 1984. The company is specialized in risk analysis, dependability, fail-safety and FRACAS systems (Failure Reporting Analysis and Corrective Action systems). The company offers the following software solutions:

- FavoWeb, Internet-based version of dynamical FRACAS system, calculation of RAMS parameters, lifecycle cost, analysis of a customer's risks at the level of the whole enterprise. It is capable of integration with any existing databases of a customer;
- RAM Commander – 30 modules replacing a dependability engineer's functionality and automating all his tasks – from prediction of parameters to fault tree analysis at all levels: components, units, systems;
- Safety Commander provides an integrated assessment of fail-safety at the level of a platform (aircraft, ship, train, etc.) by integrating fail-safety parameters at a higher level.

ReliaSoft [14], US, established in 1992. The company provides consulting and training services, licensing, supply of software. ReliaSoft software applications present a wide range of engineering simulation methods and dependability analysis at the stage of a technical item design.

SAP SE [15], Germany, founded in 1972. The company develops automated management systems for such internal corporate processes as accounting, trade, manufacturing, finances, human resources, warehouse management etc. Besides supply of software, the company offers services in its implementation using its own implementation methodology (the initial name was ASAP – Accelerated SAP – and now it is ValueSAP). SAP ERP is the most well-known software product for planning enterprise resources designed by the company. The implementation of the SAP ERP module includes the development and implementation of the following processes:

- Management of reference data;
- Overhauls and current maintenance;
- Annual planning of maintenance;
- Short-term planning;
- Execution of works and accounting of actual costs;
- Technical maintenance management.

ABB [16], Swiss-Swedish Corporation, founded in 1988, works in various industrial segments, however the key activities of the company are power supply engineering and automation technologies combined by a common digital platform ABB Ability™. The enterprise automation software enables the automation of manufacturing management, the

cut of energy consumption and the increase of production rates (operational costs reduction, lifetime extension, dependability and response improvement).

Maximo Asset Management [17] is a software solution by IBM (US) specifically tailored for management of all types of technical assets irrespective of their locations. IBM MAXIMO has 6 interrelated functional units enabling a full cycle of maintenance and management of corporate assets:

- asset management;
- supply management;
- contract management;
- stock management;
- project management;
- service management.

Maximo is a leading solution in the market of EAM systems and intended to increase the efficiency of an enterprise's asset management.

Of course, it is far from a full list of companies and IT products available at the market at present. It is worth noting that there is some general trend in the evolution of the market. The companies that started as developers of RAMS calculation software and only later proceeded to deal with the issues of lifecycle costs, risk assessment and related decision making support systems and methodology represent "the older generation" who have made an evolutionary way from just engineering to development of management tools and search for the most efficient strategy of technical maintenance and repair of infrastructure. The advantages of these representatives are a well-established engineering school and large libraries of technical failures of equipment accumulated for quite a long time. The companies who came into the market at a later stage grew as business consultants in the first place, providing consultations in construction and restructuring of enterprise asset management systems in line with the principles of the ISO 31000 series standards in risk management, the ISO 55000 standards in asset management, while providing services in certification, corporate training, development of business games. The software offered by these companies is rather focused on procedures for description of a customer's business processes, albeit with obligatory application of decision making support indicative markers using RAMS and risk assessment parameters. There is also a third group of companies who appeared around big infrastructure companies and, while providing services in elaboration of an efficient strategy of a customer's infrastructure maintenance, proceeded to maintain a customer's infrastructure by their own as outsourcing companies implementing their solutions in practice. Their advantages are own numerous and well-trained technical staff and availability of a multilayer comprehensive system of a whole enterprise management system using integrated solutions of SCADA systems and integration of a production and operations control loop with accounting systems, that enabling to practically implement principles of cost management and to calculate a lifecycle cost of equipment.

4. Conclusion

The paper analyzed the experience of EU railway companies in construction of a technical asset management systems based on advanced digital technologies. It is found out that a generalized architecture of the European information platform of asset management presents rather a diverse spectrum of IT solutions, which is a big problem, as making any changes to the platform's software is very time-consuming and requires a lot of financial resources. In this context the most successful are the companies who have invested in development of their own digital platform of asset management. To validate this conclusion, best practices of European railway companies were benchmarked, digital technologies used by railway companies were compared, and the most well-known software solutions available in the market for construction of an asset management system were reviewed. A conclusion was made that railway companies will have to take a lot of efforts so that the huge investments that they are currently putting into digitalization should not be lost, since the implementation will face opposition from the established system of administration and distribution of responsibility among management levels within a company.

References

[1] [DIANA, a diagnostic system for turnouts]. *Rail International* 2019;7:73-74. (in Russ.)

[2] Lasting Infrastructure Cost Benchmarking (LISB). 20 years of benchmarking (1996-2015). UIC – Railway Technical Publications (ETF). Paris; 2017. ISBN: 978-2-7461-2643-5.

[3] Guidelines for the Application of Asset Management in Railway Infrastructure Organizations. UIC – Railway Technical Publications (ETF). Paris; 2016. ISBN: 978-2-7461-2521-6.

[4] Key Cost Drivers in Railway Asset Management. UIC – Railway Technical Publications (ETF). Paris; 2016. ISBN:978-2-7461-2482-0.

[5] Zamyshliaev A.M., Shubinsky I.B. [Development of the URRAN project through the construction of a technical asset management system]. *Zheleznodorozhny transport* 2019;12:19-27. (in Russ.)

[6] 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); 15.02.16-18.02.16. IEEE Xplore Digital Library; 244-250.

[7] 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); 15.02.16-18.02.16. IEEE Xplore Digital Library; 481-486.

[8] «Smart Data» for Sustainable Real Estate and Infrastructures Oxand. URL: www.oxand.com (accessed 08.06.2020)

[9] Urban/rail public transport engineering consulting firm (metro, bus, tramway, etc.) – SYSTRA France & international. URL: https://www.systra.com (accessed 08.06.2020).

[10] Assetsman – Asset Management Industriel – Assetsman. URL: https://www.assetsman.com (accessed 08.06.2020).

[11] Cosmo Tech – Enterprise Digital Twin Software Solutions. URL: https://www.cosmotech.com (accessed 08.06.2020).

[12] 3B infra. URL: www.3binfra.at (accessed 08.06.2020).

[13] Reliability Software, Safety and Quality Solutions – ALD Service. URL: https://www.aldservice.com (accessed 08.06.2020).

[14] ReliaSoft – Reliability and Maintainability Analysis – ReliaSoft. URL: https://www.reliasoft.com (accessed 08.06.2020)

[15] SAP Software Solutions Business Applications and Technology. URL: https://www.sap.com (accessed 08.06.2020).

[16] ABB Group. Leading digital technologies for industry. URL: https://new.abb.com/offerings (accessed 08.06.2020).

[17] IBM – Russian Federation. URL: https://www.ibm.com/ru-ru (accessed 08.06.2020).

About the author

Alexey M. Zamyshliaev, Doctor of Engineering, Deputy Director General, JSC NIIAS, 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation, phone: +7 495 967 77 02, e-mail: A.Zamyshlaev@vniias.ru

The author's contribution

The author examined and analyzed the state of the art of development of a technical asset management system for railway companies of the European Union based on advanced digital technologies. It is found out that the European asset management information framework encompasses a lot of various IT solutions and in this case any modification to the operation of the software system requires a lot of expenditures. The author benchmarked the best practices of European railway companies and made a comparative analysis of digital technologies applied in asset management. It is concluded that the difficulties related to the introduction of advanced digital technologies are due to the resistance of the existing system of management and allocation of responsibilities between levels of management within a company.

Conflict of interests

The author declares the absence of a conflict of interests.

Original article
https://doi.org/10.21683/1729-2646-2020-20-3-34-46

On the methods of qualitative estimation of the safety state of structurally complex systems

Alexander V. Bochkov, *Gazprom Gaznadzor, Russian Federation, Moscow*
a.bochkov@gmail.com

Alexander V. Bochkov

Abstract. Aim. *To show a method of overcoming the uncertainty in the requirements for the quality of data in non-standard situations and ways of formalizing the decision-making process aimed at ensuring safe operation of structurally complex systems. The paper proposes a method of axiomatic construction of integrated indicators that describe the properties of a system and its operational environment through the synthesis of the risk function.* **Methods.** *Methods of system analysis of the objective, Russman's methods of the difficulty in achieving the objectives and the Shewhart charts theory.* **Results.** *The author proposed methods of qualitative estimation of two types of safety state, i.e. "better than" (for the purpose of defining a certain target level that characterizes the safety state that is to be ideally achieved) or "not worse than" (for the purpose of defining a certain maximum allowable level that characterizes the safety state, below which it is not allowed to go), that imply certain ranges of deviation from the specified target or, respectively, the minimal allowable levels, within which the safety state evaluated with an integrated index is deemed to be acceptable.* **Conclusions.** *It is shown that, in respect to problems of safety and risk assessment of structurally complex systems, one should not try to work with specific safety-related events only. All such events are characterized by a set of properties and contributing factors with associated characteristics. One should try to identify each property and each characteristic of such property, which would later allow defining proactive and reactive control actions in response to changes in such characteristics and properties. Having worked out a property of a situation or an event, we work out a property of a risk, and it is of no significance in which specific risk this property manifests itself. Combinations of risk properties can be extremely numerous, therefore it is very difficult to predict specific situations. That causes the requirement for a proactive decision support system that ensures high-quality managerial decisions short before a critical event.*

Keywords: *structurally complex system, risk synthesis, safety, management, difficulty in achieving the objective, statistical reasoning.*

For citation: *Bochkov A.V. On the methods of qualitative estimation of the safety state of structurally complex systems. Dependability 2020;3: 34-46. https://doi.org/10.21683/1729-2646-2020-20-3-34-46*

Received on: *16.06.2020* / **Revised on:** *02.07.2020* / **For printing:** *21.09.2020*

Introduction

The problem of optimal decision making in system management under the condition of poor mathematical formulation that is characterized by, first, the uncertainty in the choice of the target function and definition of limitations associated with a large number of heteronymous and contradictory indicators of the possible current and future system state descriptions, and second, the non-standard decision-making situation that consists in the capability to only calculate for each option only the values of individual indicators, lack of knowledge on and difficulty to implement a number of important properties of the objective function, properties of the search domain, etc. In this context, decision-making is in general defined as the process of selection of the best out of all possible solutions. However, in practice, achieving optimal results may be difficult, as decision-makers (DM) and experts often have difficulties making decisions.

Risk analysis is essentially the only way of researching those aspects of safety that cannot be covered by statistics, like, for example, low-probability accidents with high potential consequences [1]. Certainly, risk analysis does not solve all safety problems, but its use is required to compare the consequences caused by various hazards, identify the most important among them, chose the most efficient and cost-effective safety systems, develop accident relief measures, etc. Risk as a dynamic characteristic that depends on the time, assets and information cannot be reduced to "two-dimensional estimates" of probability and damage. Additionally, there is a crucial difference between the stochastic factors that entail decisions in the presence of risk, and indefinite factors that entail decisions under uncertainty. Both cause varied outcomes of managerial actions, but stochastic factors are completely described by available stochastic information (such information is what allows choosing the optimal solution). In respect to uncertain factors such information is not available.

The problem of elimination of uncertainties in the context of safety assessment is of high practical significance and has not been completely resolved yet. Within the scientific community, even the interpretation of the concepts used by various researchers provoke discussions [2].

Many, if not most, methods in statistics use probabilities that comply with the classical Kolmogorov axioms (called "exact", "classical" or "additive" probabilities). However, in the very early publications dedicated to quantitative estimation of uncertainty, among other things, foresight [3], non-additive probabilities [4] and convex sets of probabilities [5] were used. A clear emphasis on exact probabilities developed only after Laplace's works [6], and today many statistics and probability theory researchers are still convinced that additive probabilities are the foundation of the quantitative definition of uncertainty that is rich enough to cope with all types of uncertainty and the information that is generated as part of practical tasks. However, the opinion is becoming commonplace that additive probabilities are too limited and the emerging alternative structures ensure the required flexibility for quantitative estimation of uncertainty, thus also providing new methods of addressing it as part of engineering risk, safety and dependability assessment.

The situation of uncertainty is characterized by the fact that the selection of a specific plan of actions may lead to any result out of a certain set of variants, but the probability of the effect of random factors is unknown. Normally, two cases are distinguished: in the first case, the probabilities are unknown due to the lack of required statistical information, while in the second case the situation is not statistical and objective probabilities are out of the question (the situation is the so-called "perfect" uncertainty). The "perfect" uncertainty is the most common, as decisions (specificity strategic ones) are normally taken under unique conditions. Decisions taken under uncertainty are strongly associated with risk.

Engineers usually addressed uncertainty using safety factors, requiring that the actual load capacity of a structure is above the design load by a certain coefficient. Nevertheless, the approach involving the safety factor does not provide any information on the actual time to failure and thus is not completely satisfactory. As a better analytical description of uncertainties was preferable, engineering evaluations were incorporated in the probabilistic basis since the 1950s in the innovative works of Freudenthal, Bolotin and others. This approach implied that each parameter of a model is considered as a random value, and instead of absolute safety the probability of failure is considered. Such probabilistic approach causes an explosive growth of the number of parameters: each physical parameter now has a probability distribution that, in turn, is described by distribution parameters (such as the average value, standard deviation, excess, etc.), not to speak of the description of correlations between variables. Unfortunately, that requires much more information than usually available. Thus, in practice, distribution parameters must be partially defined through normative assumptions, e.g. by simply limiting the type of distribution by the type that is common to technical literature, or naively presuming independence, if information on correlations is unavailable. In other words, it is required to introduce artificial information, that cannot be confirmed by available data.

The pursuance of uncertainty models that reflect the actual level of available information lead to the search for alternative models within the engineering community: probabilistic models were considered to be an excessively rigid concept, while engineering practice had sufficiently clearly shown that interval estimation of uncertainty is superior to pointwise estimation.

What is the solution? We must migrate towards risk synthesis in system management and conceptual design of management systems. Probability is not an additive value. The addition of the products of probability and damage only works for small probabilities. This matter was, for

example, discussed in previous articles [7, 8]. The key idea expressed in those publications is that risk assessment shall be performed on the assumption of unachievable "ideal". As consequence, the development program (project, model) must include a description of such ideal in reference to all factors and threats. Solving this problem requires developing the structure of the management system that would reflect the correlations between such elements, threats, risks and vulnerabilities. By definition, the problem of such system's structure synthesis comes down to the definition of the set of correlations over the set of its elements.

In terms of perception, for instance, where the field of consciousness can be easily analyzed experimentally, it has been concluded that the so-called "elements" are always products of dissociation or extraction out of a whole within an initial set and no special correlation can be identified without the initial identification of the characteristic structural properties of the set. Eventually, that will lead to the realization of the requirement for a truly functional monitoring system that, in general, implies solving four interdependent problems [9, 10]:

– observation that consists in the acquisition and distribution of information, processing and delivery to users (this is the integration function and allows building a database for the purpose of analysis, estimation and prediction of the state of the monitoring object and its development);

– analysis and assessment involve the analysis of the collected information, identification of causal relationships, comparison of the adopted indicators with the specified standard ones;

– prediction that is associated with the feasibility to use high-quality monitoring information for the purpose of reliable representation of the general future development pattern of the observed phenomenon, object or system and thus scientifically substantiated development of short and long-term plans for the transformation and management of certain processes;

– supervision that consists in constant monitoring of the obtained results and their comparison with the input data, as well as organization and follow-up of the planned measures and tasks.

The inclusion of the analytical component into the monitoring system is justified and reasonable. Additionally, analysis is the most significant element of monitoring, since monitoring is not only about recording facts, mirror-image presentation of the occurring processes, but also analytics, assessment that enables conclusions and suggestions, predictions, planning, development scenario preparation, etc. The prognostic component is the basic one of the supervision, planning and management functions. If we imagine management as the transmission of information flows from one management entity to another, then management is the process of conditioning of the behaviour of the controlled object and ensuring its stable operation under risk and uncertainty by organizing internal and external information flows, as well as methods of its retrieval, processing and distribution that allow developing, selecting and implementing rational managerial decisions. In the context of limited flows of information on the state of the controlled object or the extreme scarcity of the safety-specific features of situation description, qualitative estimation may find widespread application.

1. On the qualitative assessments

There are two types of qualitative estimation of process safety: **"better than"** (for the purpose of defining a certain target level that characterizes the safety state that is to be ideally achieved) or **"not worse than"** (for the purpose of defining a certain maximum allowable level that characterizes the safety state, below which it is not allowed to go). Both estimates imply certain **ranges of deviation from the specified target or, respectively, the minimal allowable level**, within which the process safety state evaluated with an integrated index is deemed to be acceptable.

The advantage of qualitative estimation consists in the simplicity of application and use of a lesser amount of information, simplicity of perception and interpretation by the DM. Global experience shows that the application of qualitative methods of estimation often produces a higher number of safety recommendations than the quantitative method. Such methods have a number of characteristic features. Normally, qualitative indicators are expressed in points or ranks that are numbers, but such numbers cannot be subject to basic mathematical operations, they do not comply with general mathematical rules, i.e. if one of the indicators is assigned the rank of "1", while another is assigned the rank of "2", that does not mean that the former evaluates the hazard twice lower than the latter. In order to obtain an aggregate qualitative estimate of safety, logical rules and procedures are normally used.

2. On the assessment scale

For the purpose of indicator estimation, adequate numerical or ordinal scales must be developed. Indicator scoring, for instance, can be done using the nonlinear, nonuniform scale that has shown its efficiency as part of a number of practical tasks [11-13].

It is constructed on the basis of the knowledge of the range of values received by the indicators, i.e. the knowledge of the minimum x_{min} and maximum x_{max} estimates. It is adopted that the value 1 equals to x_{min}, while the value 9 equals to x_{max}, respectively (Fig. 1).

The average estimate 5 is to correspond with such value of indicator x_5 that meets the condition: relation x_{max}/x_5 is equal to x_5/x_{min}. Having solved equation $(x_{max}/x_5) = (x_5/x_{min})$ we deduce that x_5 is equal to the geometric mean of x_{min}, x_{max}. Value x_3 is defined similarly as $\sqrt{x_3 x_{min}}$; $x_5 = \sqrt{x_{max} x_{min}}$; $x_7 = \sqrt{x_5 x_{max}}$, respectively. Then, x_2 is the average compound $\sqrt{x_{min} x_3}$; $x_4 = \sqrt{x_3 x_5}$; $x_6 = \sqrt{x_4 x_7}$; $x_8 = \sqrt{x_7 x_9}$ and x_{min}, x_2, x_3,…, x_8, x_{max} are average values that correspond to 1, 2, 3, ..., 9 points.

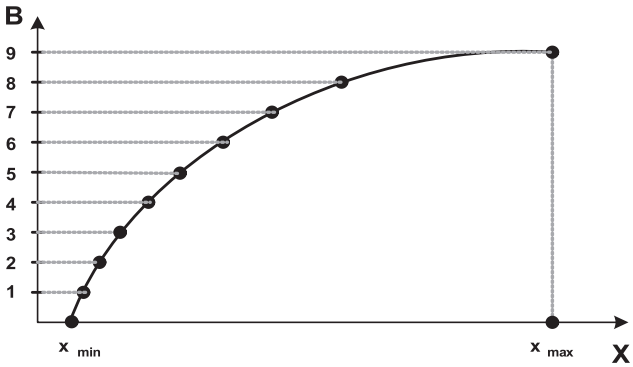


Fig. 1. Nonlinear, nonuniform scale of indicator estimation

The limit separating the values that correspond to one and two points is calculated as $\sqrt{x_{\min} x_2}$. Then, the limits between two and three points are defined as $\sqrt{x_2 x_3}$, etc. Finally, the limits between the eight-point and nine-point estimates are calculated as $\sqrt{x_8 x_{\max}}$. If there is no available information on an indicator, when transforming into point-based estimate, it is assigned the value of 5. The maximum and minimum values of features, relative to which the scale is calculated, are selected out of all data on the ranked objects of a certain object of evaluation.

For a random set of objects $\{O_j\}$ with dimension x_j, designating A the minimal out of all values x_j, and B the maximum value of all x_j, we have that in order to build a scale with K steps it is required to calculate K–1 values (i=1, ..., K–1). For instance, for K=9: $\tilde{x}_i = A \cdot \left(\frac{B}{A}\right)^{\frac{1}{2K-2}} \cdot \left(\frac{B}{A}\right)^{\frac{2(i-1)}{2K-2}}$ and, respectively:

$$\tilde{x}_1 = A \cdot \left(\frac{B}{A}\right)^{\frac{1}{16}};\ \tilde{x}_2 = A \cdot \left(\frac{B}{A}\right)^{\frac{3}{16}};\ \tilde{x}_3 = A \cdot \left(\frac{B}{A}\right)^{\frac{5}{16}};$$

$$\tilde{x}_4 = A \cdot \left(\frac{B}{A}\right)^{\frac{7}{16}};\ \tilde{x}_5 = A \cdot \left(\frac{B}{A}\right)^{\frac{9}{16}};\ \tilde{x}_6 = A \cdot \left(\frac{B}{A}\right)^{\frac{11}{16}};$$

$$\tilde{x}_7 = A \cdot \left(\frac{B}{A}\right)^{\frac{13}{16}};\ \tilde{x}_8 = A \cdot \left(\frac{B}{A}\right)^{\frac{15}{16}};$$

Next, all $x_j < \tilde{x}_1$ will be estimated as 1 point, all $\tilde{x}_i \le x_j < \tilde{x}_{2+1}$ $(i = 2,\ldots,K-1)$ will be rated i points and, finally, all $x_j \ge \tilde{x}_{K-1}$ will be rated (Fig. 2) $\tilde{x}_1$, maximum of K points.

Fig. 2. Table for conversion of actual object description parameter values into points

3. On the whole (minimally allowable) level

The target or, respectively, minimum safety status can be defined in two ways:

- statistically (based on the processing of a priori information on the changes of an indicator value that evaluates the safety status over a period of at least 5 years);

- expertly (based on consolidated opinions of safety experts on the allowable values of the appropriate indicators).

For instance, according to 116-FZ, industrial safety is the state of protection of the vital interests of individuals and the society against accidents in hazardous industrial facilities and their consequences. Considering "accidents in hazardous industrial facilities and their consequences" as the result of realization of the threats to "vital interests of individuals and the society", the concept of "**safety**" – regardless of the application field – can be considered as the **acknowledged by individuals and the society allowable level of hazard to their vital interests**. That concept was defined in GOST R ISO 31000-2010 Risk management. Principles and guidelines as "risk": **risk is the effect of uncertainty on the objectives**.

If the objective of safety consists in achieving a subjective feeling of safety from hazards associated with any industrial activity that is sufficient to individuals and the society, then the measures aimed at achieving such objective are to reduce the effect (possible damage, losses) and uncertainty (of information, place, time) of an acknowledged hazard on safety.

Acknowledging the allowable level of hazard involves using the risk assessment procedure that is essentially the only possible way of researching those aspects of safety that cannot be answered by statistics, e.g. low-probability accidents with significant potential consequences, so-called Black Swan events (a term referring to events subjectively evaluated as impossible and, as consequence, not considered), etc. The irreplaceability of the approach based on the assessment of the risk associated with the existing options for the development of safety management systems is due to the fast-changing nature of the respective process, and therefore the corresponding data that describe the states of the system and its environment, that leads to a situation when models based on large amounts of statistical information soon become obsolete and do not reflect the reality. Given the above, the migration from point-wise assessment of the state of safety management system to interval integral estimates is inevitable.

4. On the integrated index

As an integral estimate of process safety, it is suggested using comprehensive target metric that is a convolution (weighted sum) of local safety indicators of the form [14]:

$$F = \sum_{v=1}^{h} \lambda_v \mathrm{F}_v\left(\alpha^i\right),\ F = \prod_{v=1}^{h} \mathrm{F}_v\left(\alpha^i\right)^{\beta_v} \qquad (1)$$

where $\alpha^i \in D$; λ_v and β_v are the weight numbers obtained using certain additional assumptions on the operation of the model α^i; such numbers depend on the achieved particular indicators $F_v\left(\alpha^i\right)$; D is the allowable set of estimates.

The matter of selection of the type of convolution requires additional research. The initial premise of the convolution-

based methods is that each individual alternative can be evaluated numerically. However, as each alternative depends on many variables, the problem of finding the best alternative becomes complicated, because points in a multidimensional space cannot be ordered naturally.

Hypothetically, we can imagine a case when one of the alternatives has the highest values of all compared criteria and, subsequently, is the best. However, in practice, such cases almost never occur. One of the most common and simple methods of comparing multicriteria alternatives consists in reducing a multicriteria problem to a unicriterial problem, i.e. replacing a vector argument function with a scalar function.

In specialized literature, this operation was named convolution calculation (construction of supercriterion, integrated indicator) that is the numerical measure that allows comparing it with the measures of the alternatives.

The following methods are currently the most commonly used:

- weighted summation;
- additive convolution;
- multiplicative convolution.

Weighted summation is based on the calculation of the mathematical average. A set of coefficients is to meet the normalization requirement, non-compliance with which makes the scales of individual criteria and, subsequently, the final estimates of the alternatives, incomparable. The only advantage of the weighted summation is the computational efficiency, while the shortcomings come down to the following: the computational result is the absolute values of criteria, which does not allow comparing heterogeneous criteria (e.g. cost, distance, weight); criteria values are not adjusted to the [0; 1] range of the absolute scale, which allows using only the properties of the "weaker" interval scale; the average, as an estimate of an alternative, does not contain the criterion's share of its maximum value, which does not allow comparing estimates obtained in different scales. The introduction of utility has an axiomatic substantiation in the form of the R. Keeney theorem, according to which the unicriterial utility may be either additive, or multiplicative [15].

Additive convolution. The characteristic property of the additive convolution is that it gives maximum estimates to those alternatives that have higher numbers of criteria whose values are close to maximum (given equal average values for all alternatives). If the direction of optimization changes, the priorities are reversed. The use of additive convolution instead of weighted summation has the following advantages: the convolution transforms absolute values into relative ones, which allows comparing heterogeneous qualities; the convolution reduces the criteria values to the range of [0; 1] of the absolute scale, which enables all permitted algebraic operations; specifying the criterion's share of its maximum value allows comparing estimates obtained in different scales.

Multiplicative convolution. The characteristic property of the multiplicative convolution is that it favours those alternatives that have a more even distribution on the absolute scale of criteria given equal average values for all alternatives. The advantages of the multiplicative convolution are similar to those of the additive convolution.

5. On the partial indices

The structure of indicators depends on the controlled object and regular availability of data on the values that describe the object and its environment in its features and characteristics. An example of such structure is the conventional structure of particular indicators of the process safety procedure of subsidiary operating companies and organizations (Fig. 3).

5.1. **Indicator of the quality of process safety of subsidiary operating companies and organizations** (F_{PS})

The generalized estimate of the state of process safety characterizes the overall level of the company's process safety accounting for the number, frequency, eliminability and severity of the inconsistencies.

5.2. **Indicator of the safety of subsidiary operating companies and organizations personnel** (F_{OT})

5.2.1. The **LTIF indicator**, the lost time injury frequency, i.e. the specific losses in manpower, cases of loss of productivity (including fatalities, as well as temporary and permanent incapacitation (disability) per 1 mil ppl/h of work. This number of cases of lost time incidents (LTI) taken relative to the total work hours in a business unit or company (WH) over a certain period of time (normally, a year) and normalized to 1 mil ppl/h. It characterizes the total work hours lost as the result of injuries.

5.2.2. The **TRCF indicator**, total recordable case frequency, i.e. the number of all recorded cases (TRC) taken relative to the total work hours (WH) and normalized to 1 mil ppl/h. It reflects the workplace injury situation in a timely and comprehensive manner.

5.3. **Indicator of subsidiary operating companies and organizations stability** (F_s)

5.3.1. **Process safety indicator** (Saf)

5.3.1.1. Number of accidents in the facility over five years.

5.3.1.2. Number of 1-st group incidents in the facility over five years.

5.3.1.3. Number of 2-nd group incidents in the facility over five years.

5.3.1.4. Integrity indicator (integral score of operability) calculated using the methods currently adopted in the industry. The indicator is calculated based on the logical and probabilistic evaluation of an object's probability of no-failure, significance of its engineering elements in term of their failure's effect on the operability, total technology-related risk of possible accidents.

5.3.2. **Unplanned losses indicator** (insurance) LACE, loss of average capital employed, a dimensionless parameter (measured in %) defined as the ratio of the size of unplanned losses with allowance for insurance to the average capital employed [16]:

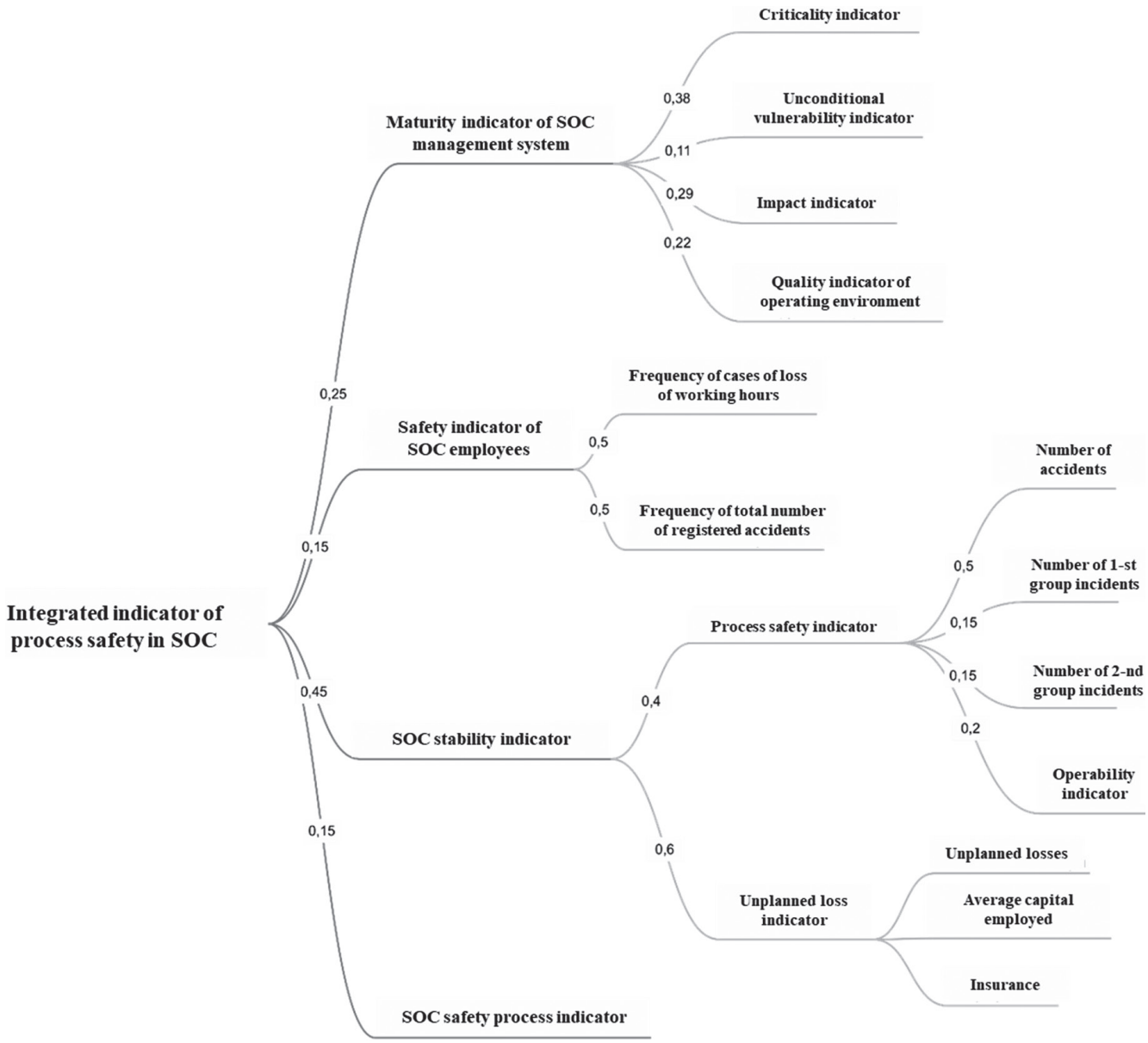


Figure 3. Structure of particular indicators of the process safety procedure of subsidiary operating companies and organizations (tentative example)

$$LACE = \frac{(1-M)\cdot UPL}{ACE},$$

where *UPL* is the unplanned losses (including the total money equivalent of material losses, human resource and financial losses, including compensation for losses from business interruption, compensation of damage to legal entities and property of citizens, compensations for environmental damage) that, through lower-level indicators is associated with industrial risk indicators: individual risk; social risk; economic risk; *M* is the indicator of unplanned losses insurance; *ACE* is the average capital employed.

As the "basis" of *LACE* calculation, the average employed capital is to be used (similarly to the definition of the first-level target indicator), the return on capital employed. In the Russian practice, operating costs are normally used as the "basis".

5.4. **Indicator of the maturity of the process safety management system of subsidiary operating companies and organizations' facilities evaluated based on a metric opposite of the risk of insufficient supervision** (F_{RIM})

The risk of insufficient supervision is a composite indicator that characterizes the hazard of a supervisory authority missing an object (business unit), that may potentially be affected by nonconformances and accidents. The risk of insufficient supervision defines the rank (place) of a subsidiary's business unit in the listing of supervised objects. The risk of insufficient supervision is calculated for various businesses (natural resources producers, gas transmission providers, processing companies, underground gas storage facilities, etc.) according to the same procedure [17].

The management system maturity indicator is defined as the value opposite of the weighted sum of the four indicators of risk of insufficient supervision (rated in points):

$$F_{RIM} = 1 - \sum_{i=1}^{4} \lambda_i F_i,$$

where λ_i is the weight indicator of the respective scale in units of the correction scale that are defined expertly;

supervision object criticality indicator (F_1) evaluates the specificity of the ranked subsidiary's business unit in terms of the aims of supervision (this indicator is used in calculations and is closely associated with the incident rate and inefficient gas utilization). It is calculated through the convolution of standardized description features of a business unit of the ranked type with appropriate weights;

indicator of unconditional "vulnerability" of the supervised object (F_2) evaluates the risk of imposition of sanctions by public supervisory bodies and the risk of undesirable consequences as the result of failure to eliminate the violations identified by corporate supervision. It is calculated through the convolution of standardized description features of a business unit of the ranked type with appropriate weights;

the indicator (coefficient) of the "effect" of the supervised object (F_3) for gas transmission (distribution) facilities is calculated using a flow-oriented model and statistical data on the structure of gas consumption in Russia's regions and characterizes the importance of performance by the object of a unit of commodity transport operation. For objects that are not gas transmission (distribution) facilities the value of this indicator is adopted as national-average;

the indicator (coefficient) of the "quality of the environment", in which the supervised object operates (F_4), a dimensionless value that is calculated based on fitted statistical data on the characteristics of subsidiaries in relation to their spatial location; for each territory, on account of geographical factors, specificity of the operating structure, sociocultural, ethnic, corruption-related and other differences, unique calculation models must be developed that would largely rely on subjective estimates by experts familiar with such specificity (the primary source of information for the calculation of the environment "quality" indicator of a ranked object is the Regiony Rossii. Sotsialno-ekonomicheskie pokazateli (Regions of Russia. Socioeconomic indicators) yearbook.

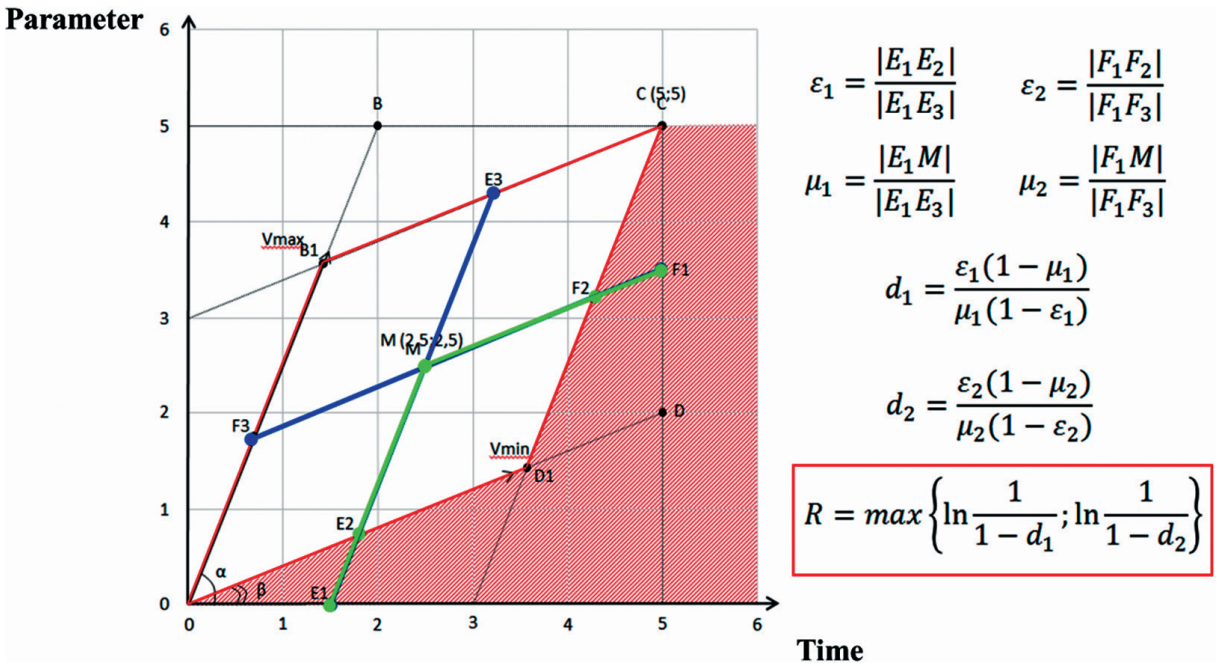
The weights of indicators shown in Fig. 3 as an example can be obtained by means of expert evaluation (e.g., Saaty's pairwise comparison). Detailed descriptions of the method can be found in literature [18].

6. On the methods of qualitative estimation

In order to obtain a qualitative estimate "better than", it is suggested using I. Russman's method [19-21] (estimation of the difficulty in achieving the target indicator value), while in order to obtain a qualitative estimate "not worse than", it is suggested to use Shewhart charts [22-24] (estimation of random and special causes of indicator value variation).

6.1. Estimation of the difficulty in achieving the target indicator value

The method is applicable if there is a specified (required) value of the integrated indicator, whose quantitative expression is the value in point C (Fig. 4). Information is available that allows evaluating the minimum and



$$\varepsilon_1 = \frac{|E_1E_2|}{|E_1E_3|} \qquad \varepsilon_2 = \frac{|F_1F_2|}{|F_1F_3|}$$

$$\mu_1 = \frac{|E_1M|}{|E_1E_3|} \qquad \mu_2 = \frac{|F_1M|}{|F_1F_3|}$$

$$d_1 = \frac{\varepsilon_1(1-\mu_1)}{\mu_1(1-\varepsilon_1)}$$

$$d_2 = \frac{\varepsilon_2(1-\mu_2)}{\mu_2(1-\varepsilon_2)}$$

$$R = max\left\{\ln\frac{1}{1-d_1}; \ln\frac{1}{1-d_2}\right\}$$

Fig. 4. Russman's basic calculation formulas

maximum rate of change of the indicator over the previous observation periods.

If, over time, the integrated indicator falls within the dashed area (Fig. 4), achieving the target within the specified time will become impossible, therefore this area becomes forbidden and proximity to it should be considered as potential mission failure and, consequently, unsatisfactory assessment of the process safety.

For the purpose of qualitative estimation of process safety of subsidiary operating companies and organizations, let us define the difficulty in achieving the specified target indicator values as the hazard of non-achievement of the specified target value of the integrated safety indicator. The difficulty consists in the variable value that is a function relative to the current position of the indicator: it grows as the indicator value approaches certain allowable limits, upon crossing which achieving the target value is practically impossible.

Under the adopted assumption the difficulty qualitatively characterizes the probability of non-achievement of the target. Graphically, this probability is taken as the ratio between the length of the segment of possible velocities to the length of the segment of allowable velocities (maintaining which the target indicator value can be achieved within the given time).

The **"better than" estimation criteria** of process safety of subsidiary operating companies and organizations impose limitations on the rate of change of the integrated indicator, namely:

Criterion 1. *The rate of change of the integrated indicator of process safety of subsidiary operating companies and organizations cannot be lower than the minimum rate over the whole preceding measurement interval.*

Criterion 2. *The rate of change of the integrated indicator of process safety of subsidiary operating companies and organizations cannot be negative.*

In case those two conditions (criteria) are met, the state of process safety of subsidiary operating companies and organizations is recognized as satisfactory, as under any current indicator value there remains a nonzero probability of the specified target value being reached. The method allows ranking subsidiary operating companies and organizations depending on the quantitative estimation of the integrated indicator.

Let us illustrate the practical application of Russman's method using the example of conventional integrated indicator dynamics analysis. The value of indicator Ψ^k over the current year, when the estimation is performed, and the preceding year are shown in Table 1.

The rate of change of the indicator value is calculated according to formula $V = \frac{\Psi^k_{t+1}}{\Psi^k_t}$, whereby $V_{\max} = 1,8500$ and $V_{\min} = 0,6507$. Respectively, the rate vector inclination angles to the speed to the axis of X are equal to 61.60 and 330. Let the value 0.96 be defined as the target value of indicator

Table 1.

No.	Performance target values		Rate of change of performance target
	Ψ^k_t	Ψ^k_{t+1}	
1	0.950	0.940	1.0106
2	0.954	0.960	0.9938
3	0.950	0.910	1.0440
4	0.960	0.850	1.1294
5	0.980	0.982	0.9980
6	0.965	0.980	0.9847
7	0.982	0.930	1.0559
8	0.940	0.840	1.1190
9	0.968	0.974	0.9938
10	0.985	0.940	1.0479
11	0.991	0.990	1.0010
12	0.650	0.999	0.6507
13	0.999	0.890	1.1225
14	0.920	0.840	1.0952
15	0.925	0.500	1.8500

Ψ^k after t+2 years from the starting moment of evaluation. The current average value Ψ^k is equal to 0.941. Let us now assume that a year later, in the year t+1, one of the companies obtained the value of integrated indicator Ψ^k equal to 0.946. The situation is illustrated in Fig. 5.

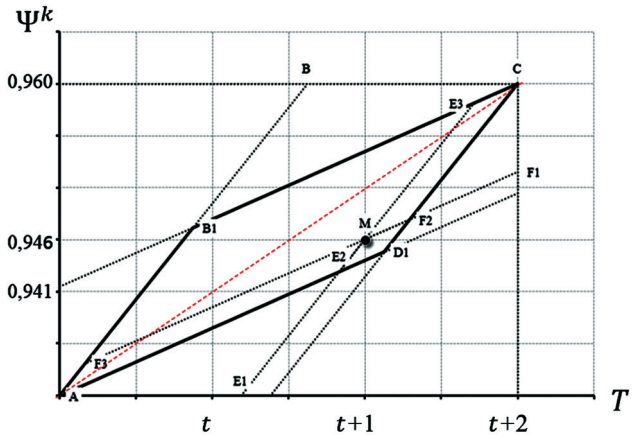


Fig. 5. Example of calculation. Critical system state

For this situation, in accordance with Russman's method, we have:

$$\varepsilon_1 = \frac{|E_1E_2|}{|E_1E_3|} = 0,4247;\ \varepsilon_2 = \frac{|F_1F_2|}{|F_1F_3|} = 0,2499;$$

$$\mu_1 = \frac{|E_1M|}{|E_1E_3|} = 0,5338;\quad \mu_2 = \frac{|F_1M|}{|F_1F_3|} = 0,3528;$$

$$d_1 = \frac{\varepsilon_1(1-\mu_1)}{\mu_1(1-\varepsilon_1)} = 0,6448;\ d_2 = \frac{\varepsilon_2(1-\mu_2)}{\mu_2(1-\varepsilon_2)} = 0,6110,$$

and, consequently,

$$R_{t+1} = \max\left\{\ln\frac{1}{1-d_1};\ln\frac{1}{1-d_2}\right\} \cong 1.$$

The value $R_{t+1} \cong 1$ show that if the indicator's rate of change remains the same, in a year the target value will not be able to be achieved. It can be seen (Fig. 5) that point M that denotes the current position of the indicator was approaching the hazardous limits AD_1C, beyond which there was a high probability of loss of control and non-fulfillment of mission. The current situation requires attention and corrective measures. For comparison, let us examine the integrated indicator estimate for another company that the same year t+2 achieved a higher estimate (Fig. 6).

For this situation, respectively:

$$\varepsilon_1 = \frac{|E_1E_2|}{|E_1E_3|} = 0,3633;\ \varepsilon_2 = \frac{|F_1F_2|}{|F_1F_3|} = 0,1205;$$

$$\mu_1 = \frac{|E_1M|}{|E_1E_3|} = 0,7878;\quad \mu_2 = \frac{|F_1M|}{|F_1F_3|} = 0,4137;$$

$$d_1 = \frac{\varepsilon_1(1-\mu_1)}{\mu_1(1-\varepsilon_1)} = 0,1537;\ d_2 = \frac{\varepsilon_2(1-\mu_2)}{\mu_2(1-\varepsilon_2)} = 0,1942;$$

$$R_{t+1} = \max\left\{\ln\frac{1}{1-d_1};\ln\frac{1}{1-d_2}\right\} = 0,2159.$$

The value R_{t+1}=0.2159 under this scenario (again, it is assumed that the indicator's rate of change remained the same) shows that if the parameter's rate of change remains as before, in a year the target value will well be able to be achieved. The risk is not high, the point that characterizes the location of the indicator is practically on the optimal trajectory.

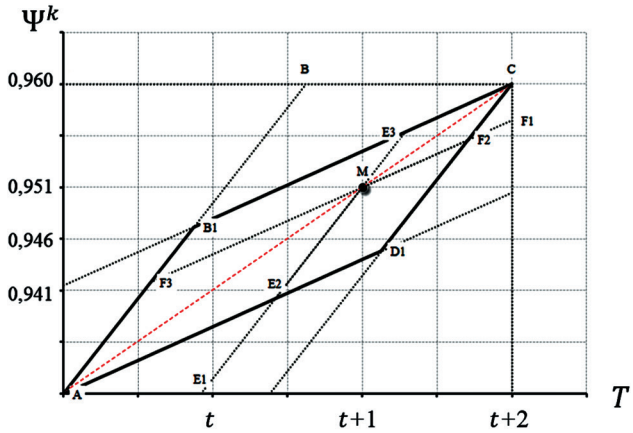


Fig. 6. Example of calculation. Controllable system state

Both values of the integrated indicator meet the above criteria and in both subsidiary operating companies the state of process safety is satisfactory. However, compared to the target value of the safety indicator, the second company shows qualitatively better results.

6.2. Estimation of random and special causes of indicator variations

A control chart is a graphical tool for decision making regarding the stability or predictability of any process, which defines the methods of managing such processes.

The control chart theory distinguishes two types of variability. The first type is random variability caused by "common" or "random" causes. It is due to a wide range of permanent causes, whose identification at the moment is complicated or economically unviable, and among which none is dominant. However, as a whole, the sum of all such causes creates something that can be considered systemic variability of a process. Preventing or reducing the effect of common causes requires managerial decisions aimed primarily at modifying the system. The second type of variability consists in the effect of such causes that are not inherent to the process, do not belong to the system and can be identified and eliminated, at least in theory. Such causes of variability are conventionally called "special". Those include insufficient material homogeneity, tool breakdown, personnel error, non-performance of procedures, etc.

As long as a process is affected by special causes of variability, it, according to the definition suggested by Shewhart, is unstable, or uncontrollable.

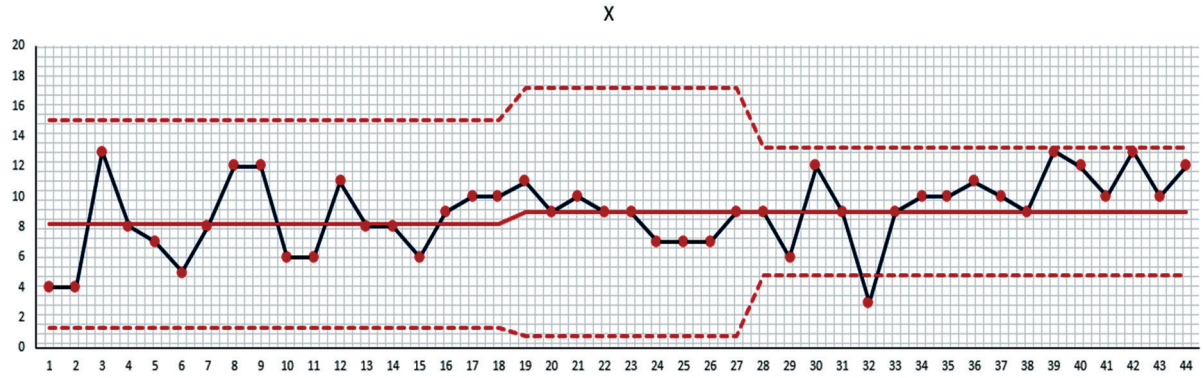


Fig. 7. Chart of outliers of the conventional integrated index of process safety of subsidiary operating companies and organizations

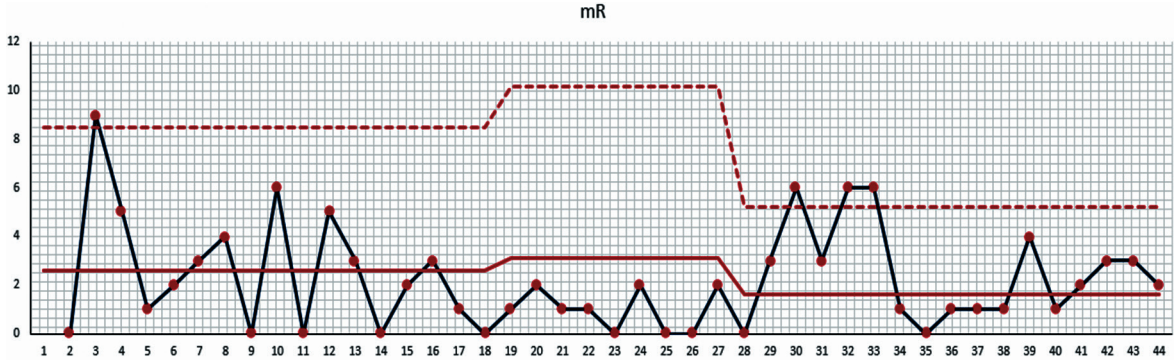


Fig. 8. Chart of value ranges of the conventional integrated index of process safety of subsidiary operating companies and organizations

Therefore, the purpose of control charts is to identify whether a process is stable. If not, the main task is to stabilize the process, which requires finding the root causes of intervention in the system and eliminate them. If the process involves only common causes of variability, it is in the statistically controllable state.

One must bear in mind that the boundaries of Shewhart's control charts are calculated based on data on the process itself, are not associated with tolerances and are not lines of certain probabilities. Constructing a Shewhart's control chart requires data obtained from the process with certain time intervals using samples (data subsets). Time intervals may be defined by either time, or be associated with the moment a certain number of supervised items has been checked. Normally, each sample consists of same-type supervised items with the same supervised quality indicators. All samples (subsets) in most cases have the same size. For each sample (subset) one or more statistical characteristics are defined, such as the total number of inconsistencies, share of inconsistent products, arithmetic mean value, range of sample, etc.

A Shewhart's control chart has a center line (CL), Fig. 7, 8.

For the purpose of studying the process and estimating whether the process is statistically controllable, the center line is the arithmetic mean value of the examined data. For the purpose of process management, the center line is the target value of the quality characteristic of products defined in the specifications. A Shewhart's control chart also has two statistically defined control limits that are usually symmetrical in relation to the center line and are the upper control limit (UCL) and lower control limit (LCL). Control limits are 3σ above and below the center line (± 3σ), where σ is the standard deviation of random variations of the used statistical characteristic (statistic) in the entire assembly. The variability within samples (subsets) is the measure of such random variations and does not include the value of between-groups variance.

The center line and the regulation boundaries reflect the laws of variation of the supervised characteristic under normal process realization, i.e. in the absence of special causes. The ordinate of the center line corresponds to the statistical estimate of the position, and the control limits correspond to the highest and the lowest limits of the intrinsic variability interval. In terms of the quantitative indicator, charts reflect the variability of quality both in terms of dispersion and position.

Therefore, in terms of the quantitative indicator, control charts should be analyzed in pairs, one chart for dispersion and one for position. The pair of the chart X and mR is the most commonly used (Fig. 7, 8). X is the average value of a small subset (measure of position), mR is the range of values within each subset (measure of dispersion).

An example of indicators of special causes appearing in a chart (points that require a closer attention and additional research in order to identify the causes of such deviations):

- points above the UCL or below the LCL;
- a long series of points (7 and more) above or below the CL;
- ascending or descending long series of points (trend);
- other manifestations of "non-randomness":

a) significantly more than 2/3 of points are situated within the middle third of the area between the UCL and the LCL (concentrated around the CL);

b) significantly less than 2/3 of the points are situated around the CL;

c) obvious trends within short series;

d) repeating differences in the results within individual samples (e.g., the first is always higher than the rest).

For the purpose of defining control limits, Shewhart chose the number 3 for other (not normal) types of distribution as well. That was done in order to keep from considering and calculating exact probabilities, as for other distributions under number 3 such probabilities are close to one as well. Therefore, for the range and reject charts, limits with the distance of ±3σ are also used instead of exact probabilistic limits, which simplifies the understanding and interpretation of such control charts. In this context, the calculation of control limits is "approximate", qualitative in its nature.

The **"not worse than" estimation criterion** of process safety of subsidiary operating companies and organizations imposes limitations on the variations (deviations) of the integrated indicator from the average value:

Criterion. *Deviations from the average value of the integrated indicator are not to exceed three standard deviations (± 3σ).*

The probability of control limits violation is very low (0.3%). Therefore, the emergence of a point outside the control limits (onset of a rare event) should be considered as the effect of non-random (special) causes on the process.

The use of control charts involves two types of possible errors: the errors of the first and second kind.

An error of the first kind occurs when the process is a statistically controllable (stable) state, and the point crosses the control limits accidentally. As the result, an incorrect decision is taken implying that the process has gone beyond the stable, i.e. statistically controllable state, and an attempt is made to find and eliminate the cause of a non-existent problem. The probability of such error is 0.3%, or three cases per thousand (0.003). In case an error of the first kind occurs, no special cause of stability disruption will be found, as the process is in fact in a statistically controllable state. The fact of the point going beyond a control limit in such case shows the onset of a rare random event.

An error of the second kind occurs when the examined process goes beyond the statistically controllable state, but all points of the control chart are within the control limits.

7. On the construction of supercriterion

In case the two above approaches are employed simultaneously, the state of safety may yield varying estimates.

It becomes necessary to develop an integrated supercriterion $F = F\left(F_1(\alpha),\ldots,F_k(\alpha)\right)$ for the purpose of selecting the optimal estimate over the allowable set. As it was shown above, the most usable integrated criteria are formulas (1) (see [14]).

If we introduce designation $\lambda_v F_v = F_v^{'}$ into (1), the first of the above estimates becomes the sum of the values of local criteria, and if we substitute $F_v^{\beta_v} = F_v^{''}$, the second integral estimate becomes the product of the local criteria taken as dimensionless value-based numbers. In both cases integrated criterion F can be constructed through repetitive use of a binary associative and communicative operation and is an integer analytical function of local criteria $F_v, v = 1,\ldots,k$. As it was shown by Russman, the class of such operations is sufficiently narrow and there are only three (accurate to constant parameters) binary operations that meet the condition of commutativity, associativity and integral analyticity. They are defined by the following three functions: a) c; b) $F_1 + F_2 + c$; c) $a\left(F_1 + F_2\right) + bF_1F_2 + \frac{a(a-1)}{b}; a,b,c - const, b \neq 0.$

He also showed (see [14]) that the third of the estimates provided by the theorem (under certain values of the coefficients that are part of it) is to be used for the purpose of obtaining the integrated criterion of quality, provided there is interaction between subsystems and criterial limitations F_v^{**} of the ranges of variation of local estimates.

Convolution of difficulties for k criteria

$$d = 1 - \prod_{v=1}^{k}\left(1 - d_v\right).$$

Russman notes that other types of convolution can be used that meet the conditions of commutativity, associativity, but are not integral analytical functions. He cites the example of the convolution of type $F = \max(F_1, F_2)$ that is exactly like that. Such convolutions are often used when the quality of the whole system is defined by the performance of its weakest subsystem.

Conclusion

As the final observation, let us note that the main conclusion of the above arguments and reasonings consists in the obvious idea: you should not try to operate with specific security events only. All such events are characterized by a set of properties and contributing factors with associated characteristics. One should try to identify each property and each characteristic of such property, which would later allow defining proactive and reactive control actions in response to changes in such characteristics and properties. Thus, having worked out a property of a situation or an event, we work out a property of a risk, and it is of no significance in which specific risk this property will manifests itself. Combinations of risk properties can be extremely numerous; therefore, it is very difficult to predict specific situations. That causes the requirement for a proactive decision support system that ensures qualitative DM support short before a critical event. Along with that, it is completely unimportant what cataclysm triggers such critical event. What matters is that it will be feasible to clearly identify what level of a property's characteristic is critical for a company (project, facility) and

what the company (project manager, operator) should do in order to put off this critical level.

The probability is not to be subject to subjective assessment. At the exact moment when subjective probability estimates come into use, an objective concept of an impossible event (like Nasim Taleb's Black Swan) is substituted with a subjective one. In the subjective understanding, a Black Swan can be any unusual or even ordinary event. It is important to draw a clear line.

The application of the most efficient security management methods is inseparable from an active use of the external and internal information space, whose state is defined by a special type of resource allocation, the information resources.

The concept of a control systems' information resources provision comprises a set of methods and procedures of information process management within production systems that allow selecting and using a required IT solution for the purpose of acquiring information on the manufacturing situation.

Consequently, the following management problems are identified:

– problem of objective definition, i.e. the required state or behaviour of the system;

– problem of stabilization, i.e. maintaining the system in the current state in the presence of disturbing effects;

– problem of task performance, i.e. taking the system into the required state, when the values of the controlled variables vary according to known deterministic laws;

– problem of supervision, i.e. ensuring the required system behaviour, when the laws of variation of the controlled variables are unknown or not constant;

– problem of optimization, i.e. retention or bringing the system into a state with extreme characteristic values under the given conditions and limitations.

One might say that security should be researched using the methods common to cybernetics that use the information approach to the research of managerial processes that involves identifying and examining, within the test objects, various types of information flows, methods of their processing, analysis, transformation, transmission procedures, etc. Under this approach, management is very broadly understood as the process of conditioning of a goal-oriented system behaviour through controlling information action by a person or a device.

References

[1] Bochkov A.V. Safonov V.S. Special analysis and assessment of risk indicators for rare events in regard to dangerous industrial facilities. *Vesti Gazovoy Nauki* 2020;1(42):84-95. (in Russ.)

[2] Kolesnikov E.Yu. A topic of uncertainty in the publications of the journal "Issues of Risk analysis". *Issues of Risk Analysis* 2019;16(3):78-93. (In Russ.) DOI:10.32686/1812-5220-2019-16-3-78-93.

[3] Huygens C. (1657). De calcul dans les jeux de hazard. Oeitvr. Comply t. 14. La Haye; 1920.

[4] Bernoulli J. Ars conjectandi, opus posthumum. Accedit Tractatus de seriebus infinitis, et epistola gallicé scripta de ludo pilae reticularis. Basel: Thurneysen Brothers; 1713.

[5] Boole G. An Investigation of the laws of thought on which are founded the mathematical theories of logic and probabilities. New York: Dover; 1957.

[6] Laplace P.S. Le Systeme du Monde. Leningrad: Nauka; 1982.

[7] Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. *Dependability* 2019;4:53-64. DOI:10.21683/1729-2646-2019-19-4-53-64.

[8] Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. *Dependability* 2020;1:57-67. DOI:10.21683/1729-2646-2019-19-4-53-64.

[9] Bochkov A.V., Ponomarenko D.V. [Methodological foundations of monitoring and prediction of process safety in PAO Gazprom]. *Gas Industry Magazine*. 2017;3(749):20-30. (in Russ.)

[10] Ponomarenko D.V., Lesnykh V.V., Bochkov A.V. Modern approach to monitoring of industrial safety for hazardous production facilities. *Issues of Risk Analysis* 2018;15(1):6-17. (In Russ.)

[11] Bochkov A. Ram M., Davim J., editors. Hazard and Risk Assessment and Mitigation for Objects of Critical Infrastructure. Diagnostic Techniques in Industrial Engineering. Management and Industrial Engineering. Springer, Cham; 2017. DOI:10.1007/978-3-319-65497-3_3.

[12] Bochkov A., Zhigirev N. 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; 121-154.

[13] Bochkov A., Lesnykh V., Lukyanchikov M. Problem of Creation of Integrated Index of Assessment of Production Safety Condition at Hazardous Production Facilities. In: Beer M., Zio E., editors. Proceedings of the 29th European Safety and Reliability Conference. Research Publishing, Singapore; 2019; 1643-1650. DOI:10.3850/978-981-11-2724-3 0077-cd.

[14] Artobolevsky I.I. [On some methods of selection of integral criteria of quality in respect to optimal design of machines]. *Proceedings of the Academy of Sciences of the USSR* 1978;2:3-10. (in Russ.)

[15] Keeney R.L., Raiffa H. Decisions with multiple objectives: preferences and value tradeoffs. Moscow: Radio i sviaz; 1981.

[16] Barsukov A.N., Bykov A.A., Lesnykh V.V. [Development of a system of indicators of emergency situations and crises]. [Industrial and environmental safety of gas industry facilities: Collection of studies]. Moscow: VNIIGAZ LLC;2008:76–86. (in Russ.)

[17] Lukianchikov M.I. et al. [On the specificity of application of the risk-oriented approach as part of some types of inspection and oversight activities in Gazprom]. *Gas Industry Magazine* 2020;1(107):21-27. (in Russ.)

[18] Saaty T.L. Decision making with dependence and feedback: The analytic network process. Moscow: Izdatelstvo LKI; 2008.

[19] Gayday A.A., Russman I.B. [Continuous supervision of the process of meeting a goal]. *UBS* 2004;7:106-113. (in Russ.)

[20] Berkolayko M.Z., Dolgikh Yu.V., Ivanova K.G. [Difficulties in the sense of I.B. Russman and dependability estimation of control]. Proceedings of Voronezh State University. Series: Systems analysis and information technologies. 2008;2:7-9. (in Russ.)

[21] Berkolayko M.Z., Dolgikh Yu.V. [Application of the difficulties apparatus to dependability estimation of organizational systems management]. Proceedings of the X International Research and Practice Conference System Analysis in the Design and Management. Saint Petersburg. 2006. 126-144. (in Russ.)

[22] Cowden D. Statistical Methods in Quality Control. Moscow: Gosudarstvennoe izdatelstvo fiziko-matematicheskoy literatury; 1961.

[23] Adler Yu., Shper V. [Practical guidelines for statistical process control]. Moscow: Alpina Publisher; 2019. (in Russ.)

[24] GOST R 50779.42-99 (ISO 8258-91) Statistical methods. Shewhart control charts. Moscow: IPK Izdatelstvo standartov; 2002. (in Russ.)

About the author

Alexander V. Bochkov, Doctor of Engineering, Head of Unit for Analysis and Ranking of Controlled Facilities, Administration, Gazprom Gaznadzor, Russian Federation, Moscow, e-mail: a.bochkov@gmail.com.

The author's contribution

Within the scope of the unified concept of the system for monitoring the safety state of structurally complex systems and facilities the author has generalized the methods of qualitative estimation of the safety state of two types, i.e. "better than" (for the purpose of defining a certain target level that characterizes the safety state that is to be ideally achieved) or "not worse than" (for the purpose of defining a certain maximum allowable level that characterizes the safety state, below which it is not allowed to go), that imply certain ranges of deviation from the specified target or, respectively, the minimal allowable levels, within which the safety status evaluated with an integrated index is deemed to be acceptable.

Conflict of interests

The author declares the absence of a conflict of interests.

 Original article
https://doi.org/10.21683/1729-2646-2020-20-3-47-52

A study of the society's attitude to the introduction of unmanned passenger transportation

Marina V. Korabliova[1]*, Larisa I. Rogavichene[1]
[1]*ITMO University, Russian Federation, Saint Petersburg*
**korablevamary@yandex.ru*

Marina V. Korabliova

Larisa I. Rogavichene

Abstract. Aim. *Obtaining initial data regarding the attitude of the Saint Petersburg residents to the emergence of unmanned vehicles in public transportation, identifying possible barriers and advantages, people's readiness to start using innovative vehicles.* **Methods.** *The research uses the methods of statistical analysis, polling, mathematical analysis. The paper presents the method of the research and makes hypotheses that it is to confirm or refute.* **Results.** *The paper highlights the correlation between the attitude of the surveyed to unmanned passenger transportation and how often they use public transportation. The authors identify the advantages and disadvantages of deployment of urban unmanned transportation based on the poll results.* **Conclusion**. *The paper highlights the city residents' attitude to the introduction of unmanned transportation. The results of a survey of Saint Petersburg residents aimed at revealing their fears and readiness to use unmanned urban public transportation. Those surveyed prefer not to be the first who try the innovative transport, and intend to wait for the practical experience and other people's opinion. Most importantly, people are worried about faults in the system and in its communication both with passengers and other road users. Legal issues and software vulnerability to potential cyberattacks are mentioned as well. In terms of advantages the surveyed noted that the presence of unmanned vehicles will improve the observance of traffic regulations, reduce congestion and the risk of traffic accidents.*

Keywords: *unmanned vehicle, innovation, urban passenger transportation, infrastructure.*

For citation: *Korabliova M.V., Rogavichene L.I. A study of the society's attitude to the introduction of unmanned passenger transportation. Dependability 2020;3: 47-52. https://doi.org/10.21683/1729-2646-2020-20-3-47-52*

Received on: *25.05.2020* / **Revised on:** *26.06.2020* / **For printing:** *21.09.2020*

Introduction

Today, unlike a few years ago, unmanned vehicles do not seem to be a thing of fantasy. In many countries around the world, including Russia, unmanned vehicles are undergoing tests [1, 2, 3]. For instance, on November 26, 2018 the Russian Prime Minister Dmitry Medvedev signed the resolution on unmanned vehicle testing on public roads. According to the document, the experiment will be held from December 1, 2018 through March 1, 2022 in Moscow and the Republic of Tatarstan [4].

According to the Concept of development of the passenger transportation system in Saint Petersburg [5], on a week day in Saint Petersburg 6830 ths rides (100%) are made, out of which 4980 ths (73%) using public transportation and 1850 ths (27%) using automobiles. Thus, despite the growing vehicle-to-population ratio, public transportation caters for 73% of the demand for passenger transportation, remaining the key element of Saint Petersburg's transportation system.

According to the World Health Organization (WHO) [6], over 3 ths persons are killed and 100 ths are seriously injured in traffic every year worldwide.

The Russian traffic accident statistics [7] show that 2019 proved to be a better year for motorists than the previous one. Thus, in 2018, 168099 accidents were registered. In 2019, this figure dropped by 2.2% to 164358.

The General Administration for Traffic Safety statistics [7] show that over 80% of traffic accidents in Russia were caused by drivers.

In Saint Petersburg 5529 accidents happened that were caused by traffic violations [7], in other words, due to the human factor.

The relevance of the research consists in the fact that the use of unmanned transportation will allow reducing the number of traffic accidents caused by the human factor. However, due to various concerns and fears, not all city residents are prepared to see unmanned public passenger transportation (UPPT) in the streets. As there is no prior research providing insight into the attitude of the people of Saint Petersburg to unmanned transportation as an alternative to conventional buses, trolleybuses and streetcars, it was decided to conduct an online poll in order to identify and analyze the existing hindrances to the transition to unmanned transportation.

The key aim of the poll was to obtain initial data regarding the attitude of the Saint Petersburg residents to the emergence of unmanned vehicles in public transportation, identify possible barriers and advantages, people's readiness to start using innovative vehicles.

The big city was the object of research. The topic of research was the attitude of the Saint Petersburg residents to the introduction of UPPT.

Before the beginning of the polling process, the following hypotheses were made:

1) males are more prepared to the deployment of UPPT than females;

2) people aged under 30 are better disposed to the application of innovative technology than respondents from other age groups, as well as better informed on the developments in unmanned transportation;

3) the primary problems associated with the application of unmanned transportation would be people's distrust of the safety of unmanned transportation, the system itself and possible faults, electronic systems failure; inability of the technology to correctly react to traffic incidents;

4) it is assumed that among the advantages of the introduction of UPPT the respondents would, above all, note the potential improvement of road safety, reduction of the number of traffic accidents, observance of traffic regulations by the road users.

Method of research

The following method is proposed for the research:

1. Target audience definition.
2. Sample definition.
3. Surveying with the use of a predefined questionnaire with open and closed questions.
4. Processing of the results and conclusions.

1. Target audience definition.

The target audience of the survey was residents of Saint Petersburg [8] aged 18 or older with no other limitations. The entire assembly is 4460446 persons, the total number of Saint Petersburg residents aged 18 or older as of 2019.

2. Sample definition.

It was required to poll 384 residents of Saint Petersburg in order to obtain specific results. The required sample size was calculated under the assumption of confidence probability of 95% and confidence range (error) of 5%.

Remote polling was conducted in January and February 2020.

3. The research.

The polling questionnaire consisted of three blocks: title, general and main.

The title block introduced the respondents to UPPT, indicated the goals of the research, outlooks of the results application, as well as informed that the polling was anonymous and the results were confidential.

The general block was intended for obtaining general information on the respondents. It contained questions regarding the respondents' gender (male or female), age group with three possible options: up to 30, from 31 to 59, 60 and older, frequency of use of public transportation and awareness of the developments in UPPT.

The main block included a number of rating questions aimed at identifying the public opinion on the subject matter of the research. In this block, the respondents were expected to evaluate their agreement with statements that reflect the presumed difficulties that the deployment of UPPT may cause. The agreement or disagreement was to be expressed on a Likert scale [9] of 5 items, where the leftmost, "Strongly disagree", corresponded to the numerical value 1, while the rightmost, "Strongly agree",

corresponded to the numerical value 5. Besides the Likert scale this block included open questions intended for the collection of information on people's concerns regarding the introduction of innovative public transportation and what advantages they expect. Along with questions about the expected barriers, the research participants were asked about their general disposition towards the introduction of UPPT, also using a Likert scale of 5 items, where 1 indicated "Strongly negative", while 5 indicated "Strongly positive".

4. Processing of the results and conclusions.

The poll produced 472 responses. Upon filtration, removal of incomplete and redundant information, 411 valid responses of unique people were collected, 197 (47.93%) males and 214 (52.07%) females.

Based on the resulting data, a "portrait" of an average respondent was drawn.

Out of those surveyed 126 persons practically never use public transportation on a daily basis. 75 people use public transportation 2 or 3 times a week, while 102 persons use public transportation 4 or 5 days a week. 108 respondents use public transportation every day. That is shown in Fig. 1.

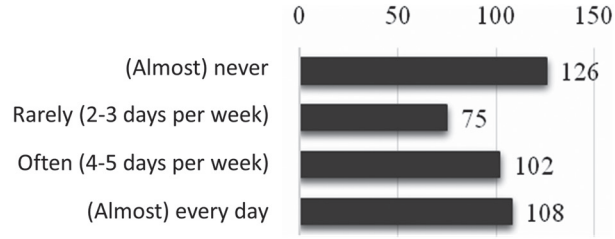


Fig. 1. Frequency of the respondents' rides in public transportation

The responses to the question regarding the awareness of unmanned public transportation are shown in Figure 2.

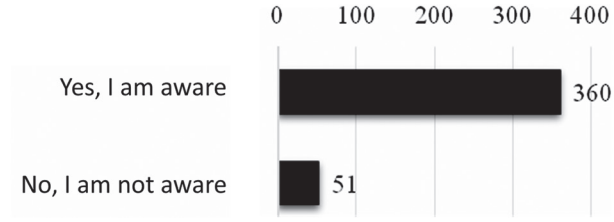


Fig. 2. The respondents' awareness of unmanned vehicles

As can be seen from Figure 2, only 12% of the respondents did not know about the developments in unmanned transportation. Out of the 51 persons who never heard of the developments in unmanned public transportation 63% (32 people) are 60 years of age or older. This correlation is shown in Fig. 3.

As can be seen from Fig. 3, people aged under 30 are best informed of innovative developments (214 people), while people 60 years of age or older are less aware of those. Their number was only 10. 136 people aged 31 to 59 are aware of the developments and only 8 persons are not. 11 people aged under 30 stated that they were also not aware of unmanned vehicles.

As the results, for each question of the main block with a Likert scale, the average value was calculated both for the total number of those surveyed, and for each individual group. The obtained values can be considered as the rating of the attitude of a certain group of city residents to UPPT.

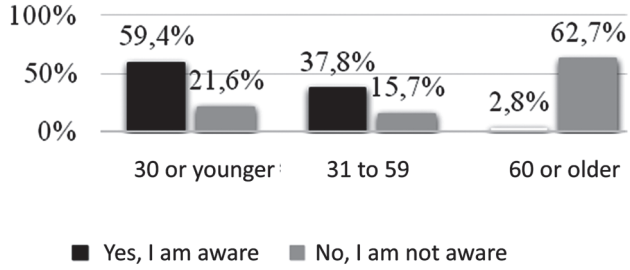


Fig. 3. Correlation of people's awareness of the developments in unmanned transportation and age

The results of the research allow concluding that the respondents are generally well disposed towards unmanned vehicles. Thus, the average score for all those surveyed is 3.95 points.

Surveyed females have a more positive attitude to unmanned transportation. Their average estimate is 3.58 points. Males are more skeptical about innovations and their average estimate is 3.47. This gender-based distribution of the attitude to innovations is shown in Fig. 4.

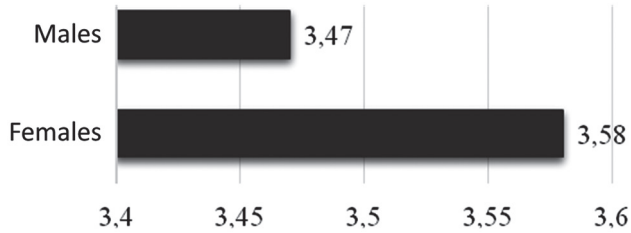


Fig. 4. Correlation between the attitude to unmanned vehicles and gender

It can be assumed that males are more skeptical about unmanned transportation because driving is their hobby. Besides, careless driving is often the case. The introduction of unmanned vehicles implies, strict observance of traffic regulations, as an artificial system is not yet trained

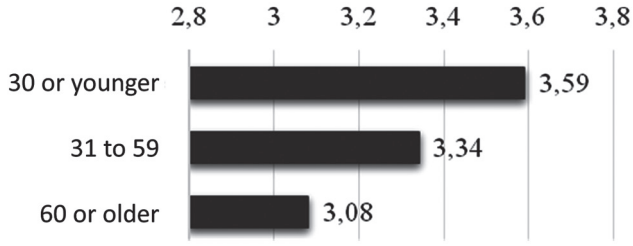


Fig. 5. Correlation between the attitude to the deployment of unmanned vehicles and age

to react to unexpected traffic situations, including a human-controlled vehicle suddenly changing lanes may confuse an autonomous vehicle.

Out of the received responses it can be concluded that the older the respondents are, the more skeptical they are about the idea of deploying UPPT in Saint Petersburg. The obtained rating of age groups' attitude to the potential deployment of unmanned vehicles is shown in Fig. 5.

Young people from the first age group are more open to innovations that respondents from the third group. They are more open to new technology, in particular in transportation. Practice showed that people aged under 30 more actively use modern alternative means of transportation (e.g. mono-wheels, electric scooters, etc.) to get around the city.

Fig. 6 shows the correlation between the attitude to the replacement of conventional with unmanned transportation and the frequency of rides.

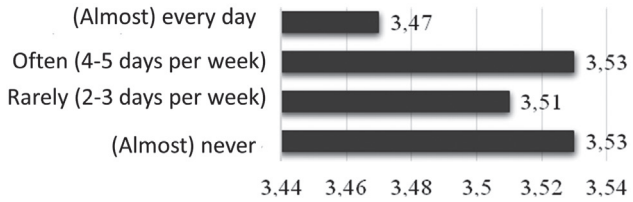


Fig. 6. Correlation between the attitude to the replacement of conventional with unmanned transportation and the frequency of rides

The average estimate made by people who use public transportation almost every day is 3.47 points. The numbers of people who often use public transportation (4 or 5 days a week) and those who never use it proved to be equal (3.53). That implies that the respondents who have a personal vehicle or do not use public transportation for other reasons have an equally good opinion regarding UPPT as those who frequently use public transportation.

As the survey showed (Fig. 6), people's attitude to the replacement of conventional public transportation with UPPT practically does not depend on the frequency of use. The ratings in this section are close to the average value of 3.5.

A significant difference in the ratings was obtained in groups formed on the basis of the awareness of the developments in unmanned transportation, which can be seen in Fig. 7.

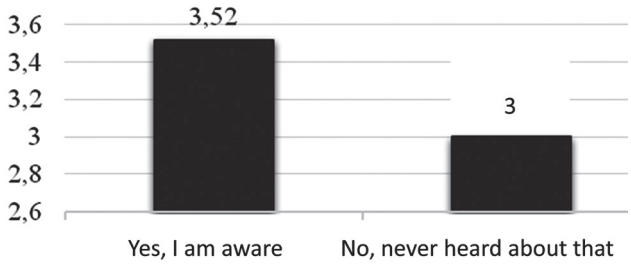


Fig. 7. Correlation between the attitude to unmanned vehicles and the awareness

The survey showed that most respondents are aware of the current developments in unmanned transportation. That should not be a surprise, as Saint Petersburg often hosts exhibitions, forums and conferences dedicated to unmanned transportation.

Among people's main worries due to the deployment of unmanned vehicles we can identify:

– initial surprise of drivers and pedestrians at the emergence of unmanned transportation. For instance, people might start taking videos on their smartphones and get distracted from the road and driving;

– video cameras and lidars collecting mud from the vehicles ahead;

– loss of communication with the dispatcher in an emergency situation (a passenger feeling sick, vehicle malfunction, short circuit);

– excessive vigilance by the unmanned vehicle in nighttime, in fog, bad weather;

– possible software faults;

– the infrastructure not being prepared for the deployment of UPPT.

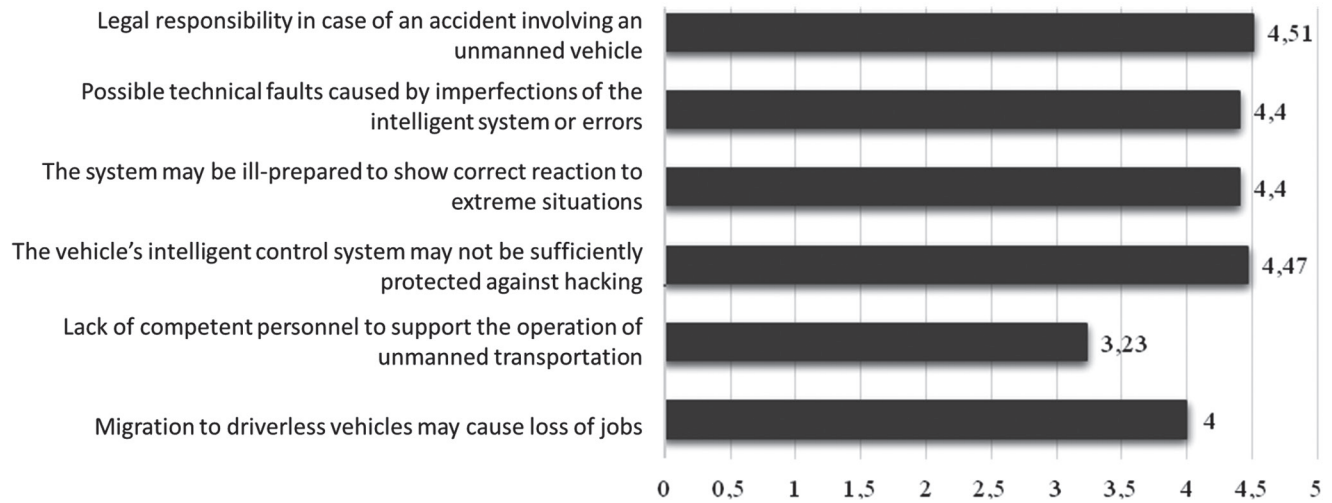


Fig. 8. Level of agreement with the identified obstacles

Among the advantages, the respondents noted the traffic safety, reduction of the number of traffic jams, reduction of the risk of traffic accident and improved observance of road regulations, elimination of routine driving operations, emergence of new professions.

However, for those advantages to materialize, the city residents must realize that an unmanned vehicle is a programmed machine that operates in accordance with specified algorithms and rules, therefore it is necessary to avoid emergencies by observing the road regulations.

According to the obtained results, those surveyed are seriously concerned about the above problems associated with the deployment of UPPT. Practically all such issues were rated on the average above three, while 5 problems out of 6 had the average score of 4 and higher. That can be well seen in Fig. 8.

The main causes of concerns are the legal matters, non-availability of a regulatory framework that would strictly define the scope of responsibility of the parties involved in an incident. Of practically equal concern are the consequences of cyberattacks on the control systems of unmanned vehicles. The respondents were least worried about possible loss of jobs in transportation, as well as shortage of well-trained and qualified staff that would ensure stable, safe and efficient operation of UPPT.

Conclusion

While automotive manufacturers, the press and the academia universally agree that unmanned vehicles will usher in the next age of transportation worldwide, this research identified, evaluated and ranked major concerns of future passengers regarding the quite radical innovations.

Females have a more positive attitude to the introduction of UPPT (their average assessment is 3.58), rather than males (average assessment 3.47).

The conducted research showed that if a person has doubts about the safety of a technology or its advantages, he/she usually refrains from using it.

Regarding the hypotheses made at the beginning of the paper, it can be noted that not all of them were confirmed. Thus, for instance, the first assumption that males are better disposed to the presence of innovative technology on roads proved to be false. It should be noted that only 5% of those surveyed expressed an overtly negative attitude to unmanned vehicles.

The second hypothesis proved to be correct. Young people of Saint Petersburg aged under 30 are more open to unmanned transportation. That may be due to the fact that the young generation is more and more dependent on gadgets and more familiar with modern technologies, and would want to personally try out things like unmanned passenger transportation. However, it was noted that the older the respondents are, the more skeptical they are about the idea of deploying of UPPT.

The third and fourth hypotheses were also confirmed by the research. Less than a half of those surveyed (30.4%) stated that they wanted to be the first to use UPPT. Those were 125 persons. Most respondents (214 persons, or 52.1%) intend to wait for other users' experience and start using it themselves only knowing it is safe. 17.5% of respondents (72 persons) would never use UPPT.

The survey also identified a number of problems, the most important of which are the legal aspect and lacking regulatory framework, possible cyberattacks, uncertainty of unmanned vehicles' reaction to emergency situations.

References

[1] Korobeev A.I., Chuchaev A.I. [Unmanned vehicles: new challenges to public security]. *Lex Russica* 2019;2(147):9-26 [accessed 10.03.2019]. Available at: https://cyberleninka.ru/article/n/bespilotnye-transportnye-sredstva-novye-vyzovy-obschestvennoy-bezopasnosti. DOI: 10.17803/1729-5920.2019.147.2.009-028. (in Russ.)

[2] Pokusaev O.N. et al. [On world market of autonomous (driverless) cars]. Modern Information Technologies and IT-Education 2018;3:737-747 [accessed 11/03/2019]. Available at: https://cyberleninka.ru/article/n/mirovoy-rynok-avtonomnyh-bespilotnyh-avtomobiley. DOI: 10.25559/SITITO.14.201803.737-747 (in Russ.)

[3] Brom A.E., Belonosov K.Yu. The issue of autonomous vehicle introduction into economic environment. Bulletin of the Moscow Region State University 2018;1:23-32. [accessed 12.04.2019]. Available at: https://cyberleninka.ru/article/v/issledovanie-problem-vnedreniya-bespilotnyh-avtomobiley-v-ekonomicheskuyu-sredu. DOI: 10.18384/2310-6646-2018-1-23-32. (in Russ.)

[4] [On the experimental operation of unmanned vehicles on public roads]. (accessed 12.04.2019). Available at: http://government.ru/news/34837/. (in Russ.)

[5] [Resolution of January 23, 2008 no. 44 On the concept of development of the passenger transportation system in Saint Petersburg, including the subway and other rapid transit for the period up to 2020]. [Tekhekspert: an electronic fund of regulatory and legal documents] [accessed 25.01.2020]. Available at: http://docs.cntd.ru/document/8467872. (in Russ.)

[6] [Traffic accidents statistics in Russia and abroad]. [accessed 28.10.2019]. Available at: https://tass.ru/info/3233185. (in Russ.)

[7] [General Administration for Traffic Safety. Indicators of the status of road traffic safety]. [accessed: 10.10.2019]. Available at: http://stat.gibdd.ru/. (in Russ.)

[8] [Saint Petersburg and Leningrad Oblast Office of the Federal State Statistics Service (PETROSTAT). Age and gender composition of the population of Saint Petersburg as of January 1, 2019. Statistical bulletin no. VS – 140/1148 of 20.12.2019]. Saint Petersburg; 2019. (in Russ.)

[9] Dubina I.N. [Mathematical foundations of empirical socioeconomic research. A study guide]. Altai State University Publishing; 2006. (in Russ.)

About the authors

Marina V. Korabliova, Master of technological management and innovation, ITMO University, 11/2 Chaikovskogo Str., room 1-S, 191187 Saint Petersburg, Russian Federation, korablevamary@yandex.ru

Larisa I. Rogavichene, Associate Professor, Candidate of Economics, Ordinary Senior Lecturer, Faculty of Technological Management and Innovation, ITMO University, 11/2 Chaikovskogo Str., room 1-S, 191187 Saint Petersburg, Russian Federation, rogavichene@itmo.ru

The authors' contribution

Korabliova M.V. analyzed the state of the art of the problem under consideration. She made the research questionnaire and conducted a research of the Saint Petersburg residents' attitude to the introduction of unmanned transportation. Processing of the obtained results.

Rogavichene L.I. drafted the plan and hypothesis of the research, as well as its questionnaire. She conducted a research of the Saint Petersburg residents' attitude to the introduction of unmanned transportation. Processing of the obtained results.

Conflict of interests

The authors declare the absence of a conflict of interests.

Cyberthreat risk identification based on constructing entity-event ontologies from publicly available texts

Michael K. Ridley, *MAI, Russian Federation, Moscow*
mr@kalabi.ru

Michael K. Ridley

Abstract. Aim. *Out of the currently used methods of ensuring cyber security the most productive ones are traffic analysis, malware detection, denial of unauthorized access to internal networks, incident analysis and other methods of corporate perimeter protection. The efficiency of such methods however depends on the timeliness and quality of threat data. The Aim of the paper is to study the ways of improving the cyber threat awareness and capabilities to analyze texts in open sources for the purpose of cyberattack prediction, identification and monitoring of new threats, detection of zero-day vulnerabilities before they are made public and leaks are discovered.* **Methods.** *Publicly available knowledge on cyber security is acquired through continuous collection of data from the Internet (including fragments of its non-indexed part and specialized sources) and other public data networks (including a large number of specialized resources and sites in the TOR network). The collected texts in various languages are analyzed using methods of natural language processing for the purpose of extracting entities and events that are then grouped into canonical entities and events, and all of that information is used for continuous updating of a subject-matter event-entity ontology. It includes general forms of entities and events required for the context and specialized forms of events and entities for purposes of cyber security (technical identifiers, attack vectors, attack surfaces, hashes, identifiers, etc.) Such ontology can function as a knowledge base and be used for structured queries by cyber security analysts.* **Results.** *The proposed method and the system based upon it can be used for analyzing computer security information, monitoring, detection of zero-day vulnerabilities before they are made public and leaks are discovered. The information retrieved by the system can be used as highly informative features in statistical models. The latter served as the basis for a classifier that defines the risk of exploits for a specific vulnerability, as well as an IP address scoring system that can be used for automatic blocking. Additionally, a method was developed for risk-based ranking of events and entities associated with cyber threats that allows identifying – within the abundance of available information – the entities and events that require special attention, as well as taking timely and appropriate preventive measures.* **Conclusion**. *The proposed method is of direct practical value as regards the problems of analytics, risk-based ranking and monitoring of cyber threats, and can be used for the analysis of large volumes of text-based information and creation of informative features for improving the quality of machine learning models used in computer security.*

Keywords: *cybersecurity, railway infrastructure security, knowledge extraction, semantic web, ontology, natural language processing.*

For citation: *Ridley M.K. Cyberthreat risk identification based on constructing entity-event ontologies from publicly available texts. Dependability 2020;3: 53-60. https://doi.org/10.21683/1729-2646-2020-20-3-53-60*

Received on: *23.06.2020* / **Revised on:** *18.07.2020* / **For printing:** *21.09.2020*

Introduction

Over the last decade, cybercrime made a quantum leap and became a highly competitive market. In 2016, its direct damage to the global economy amounted to 3 billion dollars, while in 2020 this figure was as high as 6 billion dollars. The sum is growing along with the rate of digitization: the higher the number of automated systems, the more there are ways of disrupting the activities of a business. For instance, during six weeks of its operation, a little-known German project HoneyTrain that simulated railway infrastructure management systems was exposed to 2.3 million attacks [1].

Attacks against railway infrastructure are often aimed at client services. For instance, in May 2018, a DDoS attack (a distributed attack for the purpose of causing a denial of service) prevented the passengers of the Danish State Railways (DSB) from buying tickets both online and from fixed terminals. Attacks against control systems happen more rarely, but they are more hazardous. For instance, in October 2017, the Swedish transportation system temporarily lost the ability to monitor the location of the railway rolling stock and geoinformation services. Additionally, attacks against SCADA (supervisory control and data acquisition) systems happen as well. Among the examples are the Stuxnet infection of a uranium-manufacturing facility in Iran or attack against a nuclear power plant in Kansas, US.

JSC RZD is making active efforts in terms of cyber security of railway infrastructure. For instance, 2016 saw the beginning of a joint project by JSC RZD, Positive Technologies and JSC NIIAS[1] that examined the EBILock 950 interlocking system that, through object controllers, controls such trackside devices as level crossings, track circuits and point machines.

Importantly, JSC RZD employs versatile technology. The sixteen railways operated by JSC RZD use different types of equipment and protocols. At the top level, about 100 automated management systems are used, while at the bottom (local) level tens of thousands computer-based traffic management systems of almost 70 different types are in operation [2].

Currently, the focus is on ensuring protection and repelling known attacks. For instance, the above project resulted in the deployment of the Positive Technologies Industrial Security Incident Manager. That was of course the right thing to do, as in 2018 alone the number of components of process control systems available online grew 1.5 times, as well as the number of vulnerabilities that can be used remotely without privileged access.

Nevertheless, perimeter defense and traffic analysis are not sufficient. The system must insure real-time notification of new vulnerabilities, cyberattacks occurring worldwide (including planned ones), hacktivist activities, attacks against other systems of similar class, etc. Such monitoring is on the list of important recommendations for railway infrastructure facilities [3]. For example, it allows reacting to a vulnerability identified in a used software solution a week before its official publication.

As it is known, open sources often report information on vulnerabilities and exploits before they are featured in the common databases, the CVE (Common Vulnerabilities and Exposures) and NVD (National Vulnerability Database), whereby the time gap may be as long as several months [4]. Such information appears in open source software issue trackers, on Twitter, subject-matter blogs, Q&A services for software designers like StackOverflow, e-mails, hacker forums and trading sites in anonymous networks. For the purpose of efficient monitoring, computer security analysts need methods of automatic retrieval of information from texts in public networks, including some unindexed segments of the Internet and anonymous networks like TOR. Thus, the monitoring will allow not only identifying new threats and cyber security risks, but analyzing and scoring threats in a more complete and systematic way.

Monitoring such source is a way of automatically tracking zero-day vulnerabilities that are especially hazardous and often remain unnoticed in network traffic analysis. Such vulnerabilities include those, for which there are no developed or published protection mechanisms, which allows intruders to freely use them until the fix is published, as well as interferes with the protective features' efforts to detect the attempts to exploit them. That is also an efficient tool for real-time search for information leaks similar to the one that occurred in June 2019, when hundreds of thousands of documents from JSC RZD's corporate resources were stolen[2]. As intruders often look for ways to monetize the stolen assets, they place announcement in special sites, where the leak will be discovered several minutes after the publication.

Construction of entity-event ontologies for applied knowledge bases

One of the methods of conceptualization of text-based information is the construction of an ontology based on the described facts. Such ontologies include domain concepts, their relations and their attributes. They are extracted in accordance with the meta-ontology (top-level ontology that describes a specific ontology) using computer linguistics tools, Hearst pattern-type and regular expression matching rules, statistical models.

Automatic ontology construction is most often used for creating universal ontologies that are based on linguistic categories of the type hyponym/hyperonym and meronym/holonym, IS-A, INSTANCE-OF and other relationships. That is relevant in the context of many problems related to artificial intelligence, but not the problems associated with the representation and collection of applied knowledge.

For the purpose of knowledge acquisition, it is more practical to use self-extending entity-event ontologies. The author has previously developed an analytics system that extracts texts from sources, analyses them, builds an ontol-

[1] Source: https://bit.ly/2YkAQ4N

[2] Source: https://www.kommersant.ru/doc/4252728

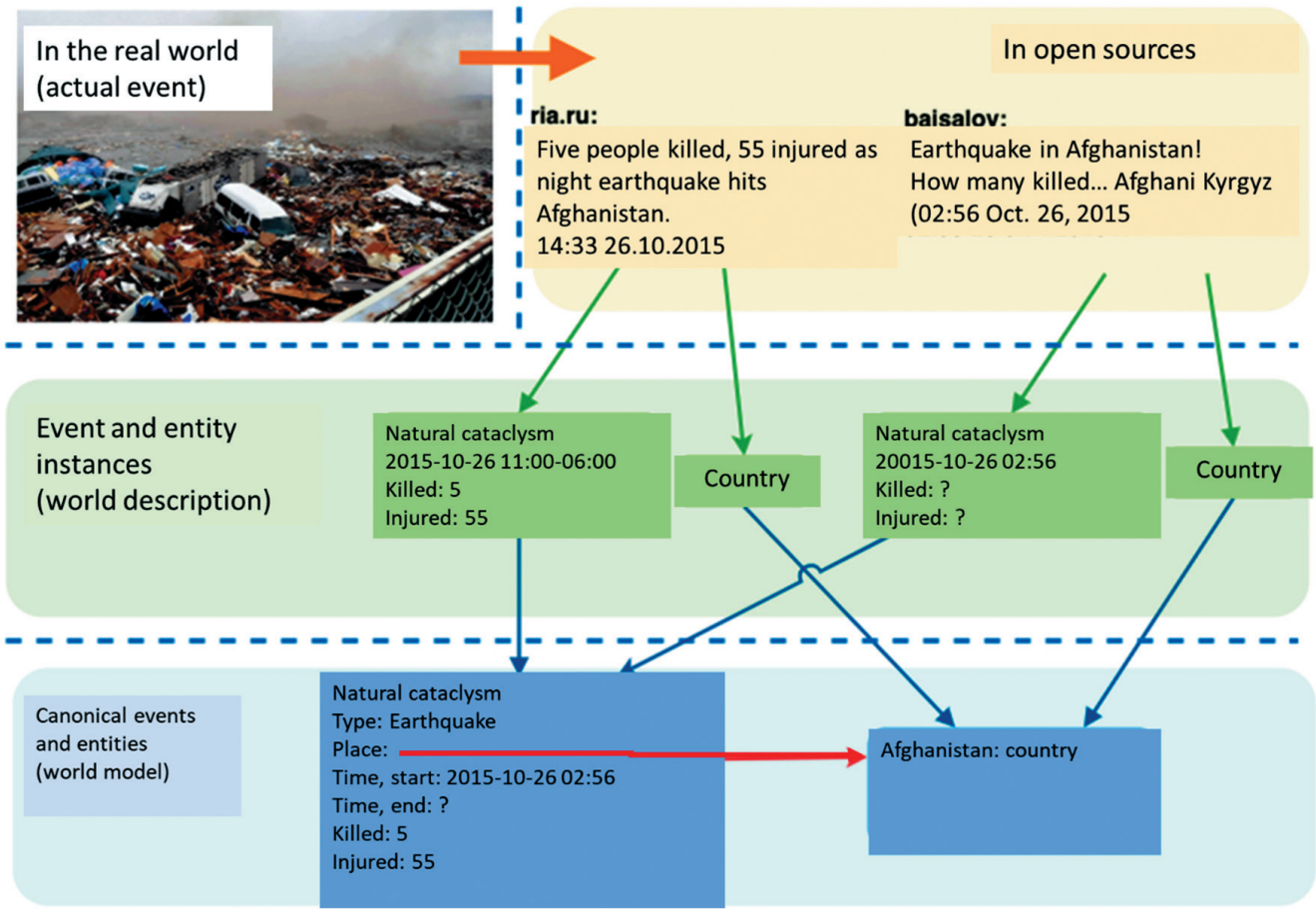


Fig. 1. An example of description of real phenomena through canonical events and their mentions

ogy and provides it to the user as a knowledge base [5]. The system was developed for news and political applications, as well as for commercial aviation [6]. One of the aims of this paper is to adapt the system for the purpose of analyzing and monitoring cyber threats.

The approach involving entity-event ontologies implies that the world is modeled by means of separating documents from their contents, i.e. the canonical entities and events that correspond to real people, technologies, companies, meetings, business transactions, attacks and political events. Each canonical entity and each canonical event may be associated with a number of instances that relate the mentions of canonical objects in texts with the time, place and other contextual information, as illustrated in Fig. 1. Such ontology allows for structured queries to the knowledge base. One can find out the technical identifiers associated with an attack, obtain the list of sources that referred to an attack, get to know the types of systems that can be attacked using a specific exploit, who and where is selling a specific set of exploits and other matters that come down to attribute-based filtering.

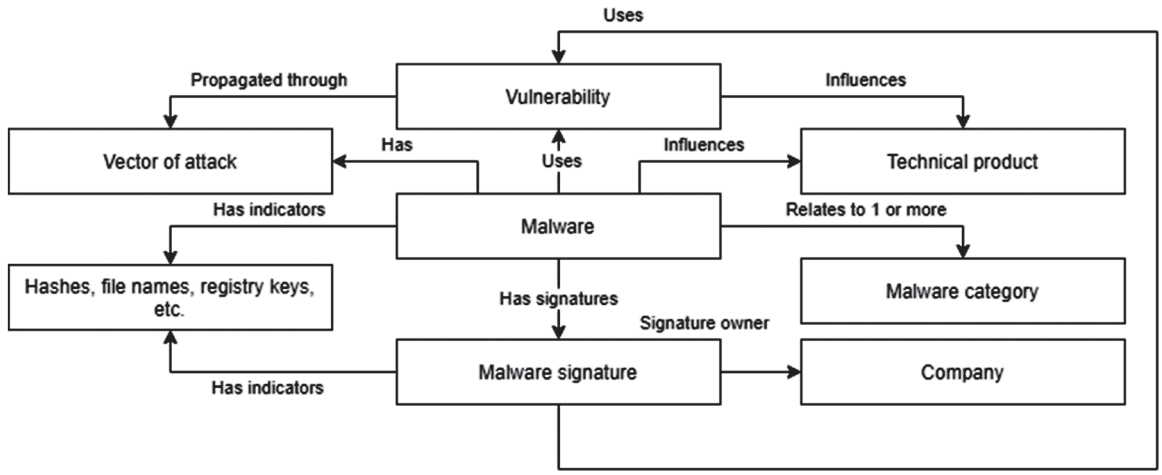


Fig. 2. A fragment of a meta-ontology of cyber security entities

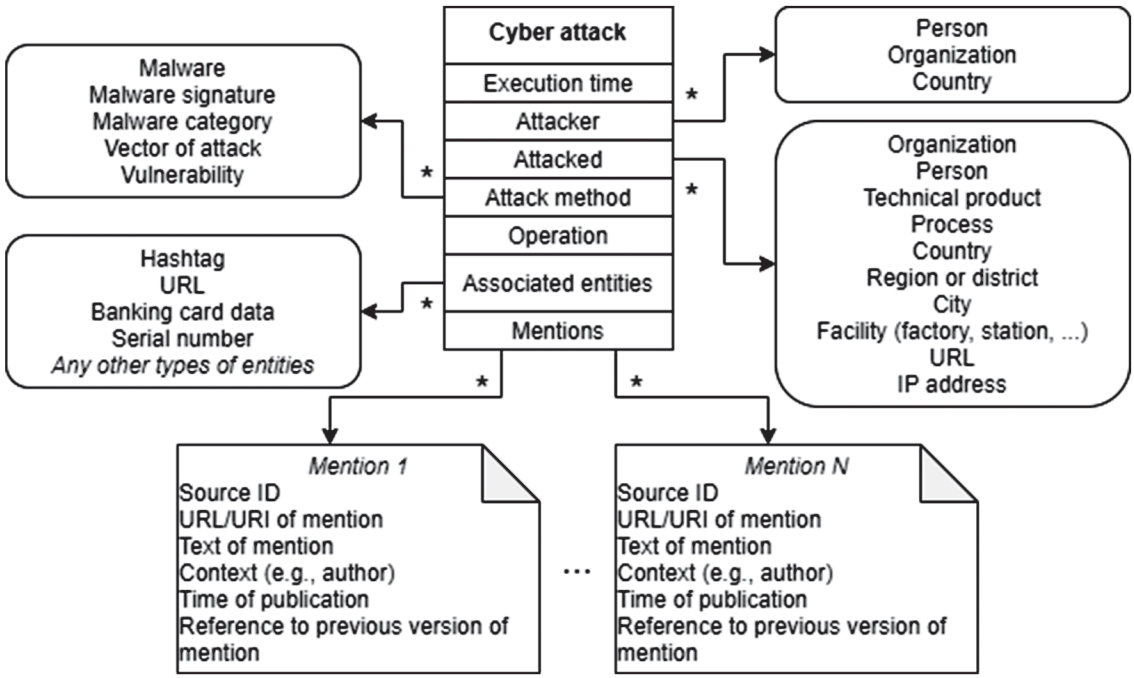


Fig. 3. Event scheme of type "Cyber attack"

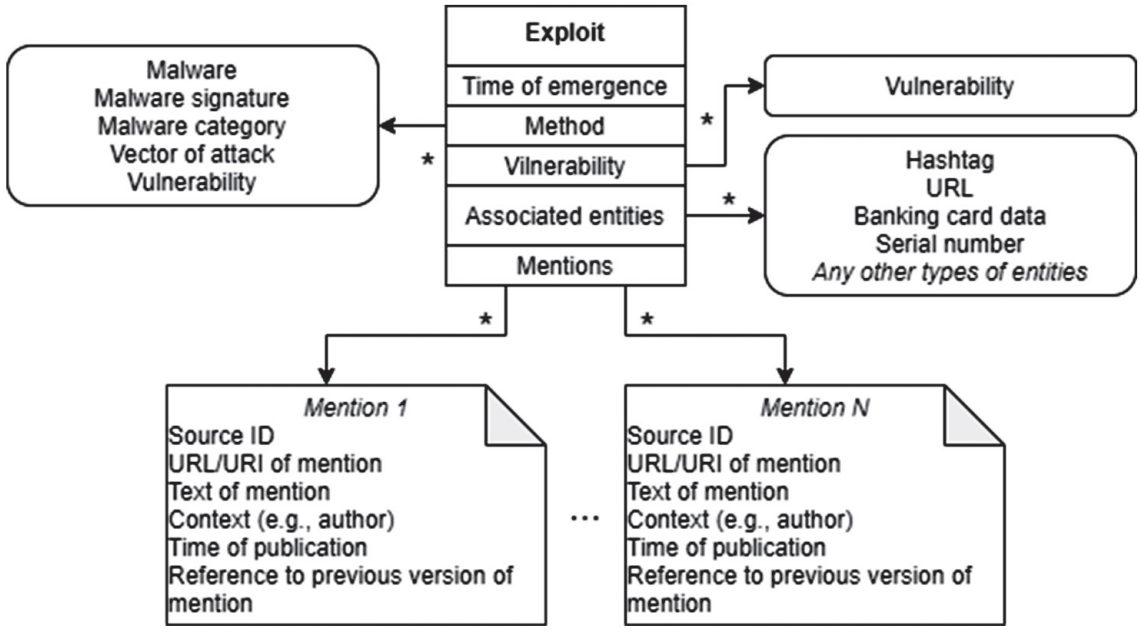


Fig. 4. Event scheme of type "Exploit"

The meta-ontology that supports the continuous updating of the entity-event ontology based on text references was completed to suit the needs of cyber security. The cyber security ontology for critical infrastructure was used as the foundation. It was revised to be made compatible with events and entities [7]. In terms of entities, the meta-ontology is illustrated in Fig. 2, in terms of events, it is shown in Fig. 3 and 4.

Implementation of text analysis for construction of entity-event ontologies

Out of various natural language texts it is required to extract information on entities (individuals, organizations, card numbers, mailing addresses, hashes, IP addresses, software signatures, file names, etc.) and events (company mergers, political protests, cyberattacks, bankruptcies, etc.).

The system uses five ready-made natural language processing tools (Table 1) and a set of own tools for exotic entities (hashes, serial numbers, vulnerability codes, code fragments, etc.). The developed extraction tools use regular expression rules or the conditional random field (CRF) method, whose specificity consists in the absence of necessity to model the probabilistic dependencies between the observable variables and the problem of marker shift unlike in a maximum-entropy Markov model.

Table 1. Employed ready-made computational linguistics tools

StanfordNLP	Tomita parser	OpenCalais	OpenNLP	Rosette EX
Supported languages				
English, German, Spanish, Chinese	Any, defined by dictionaries and grammars	English	European languages	55 languages (including Russian, Arabic and Chinese)
Primary interfaces				
API, JAVA and Python libraries, web interface	Console-based application, API	API, web interface	JAVA library	API, web interface
The best developed branch of functionality (used in the system)				
Entity extraction using statistical algorithms and neural networks	Generation of grammar and entity extraction using dictionaries	Entity and event extraction based on the news ontology	Entity extraction using statistical algorithms and neural networks	Entity, fact extraction, coreference resolution
Output methods recommended by the developer				
JSON, XML, CoNLL, graphic	Output format is defined by the grammar	RDF, XML, graphic	XML	RDF, XML, graphic

The extracted entities and facts are compared and resolved according to the ontology in order to specify their meaning and resolve the coreference. Ontologies of structured relationships between entities are used for managing the process of filtering and as the gazetteer for improving the extraction process.

Having acquired a set of filtered entities, the module responsible for proposition extraction associates the entities with the events mentioned in the document. The events are assigned fragments of text out of the document that provide the best possible short description, while also ensuring summarization. For each fragment, the sentiment is analyzed.

Next, the facts are submitted to temporal analysis. Cultural and regional categories are extracted from a document in order to take into consideration the hemisphere, first day of the week and date format. The events may be either past or anticipated. The future events are either planned (election

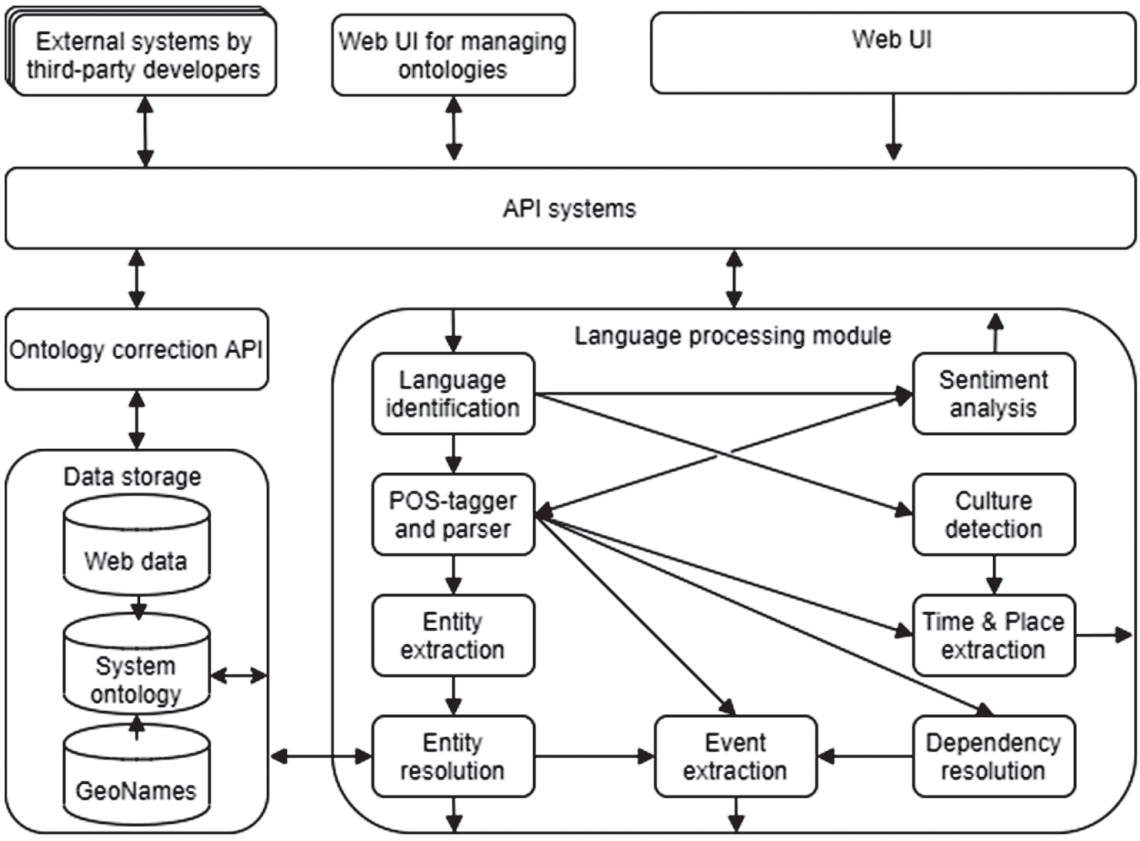


Fig. 5. Top-level architecture of the language data analysis subsystem

days), or speculative (assumption of when a rally should be called). For instance, that enables anticipating actions of hacktivists like Anonymous and release of patches by software manufacturers.

The events are marked with the type, time interval, involved entities, their roles (which attributes of an event they are assigned to), sentiment and source. The layout of the architecture of the language data processing subsystem is shown in Fig. 5. It is an independent system integrated with the main system that is examined in the following section of the paper.

Architecture and implementation of the ontology-based data collection and analysis system

Figure 6 shows the top-level system architecture.

The collection subsystem is responsible for the acquisition of text-based data from the Internet. As the input, it receives a list of predefined and configured resources and regularly retrieves data from them. The system outputs a flow of unstructured texts with the indication of the time of collection, context and source.

The input of the *language data processing subsystem* consists of cleaned texts from the collection subsystem. The subsystem outputs a list of snippets (fragments of text) marked-out in XML with the entities, events, time and place stamps highlighted. This is the only language-dependent place within the system. Providing support for a new language requires the development of a new module within the subsystem, while the system as a whole operates with either "raw" texts, or language-independent facts.

The input of the *storage subsystem* consists of marked-up snippets that it processes, upon which the extracted facts are stored. It also receives requests from external systems. The fact storage is accessed through an application program interface (API) in the JSON format in accordance with the REST API principles. The subsystem outputs ontology slices (sets of facts, events and entities, as well as their metrics of importance type) corresponding to the API request.

The fact storage is viewed and modified by the modules of the *data integration subsystem* that enrich and refine the data. This subsystem attenuates improbable events and amplifies the high-profile events, simultaneously enriching them with additional structure and forming canonical events and entities.

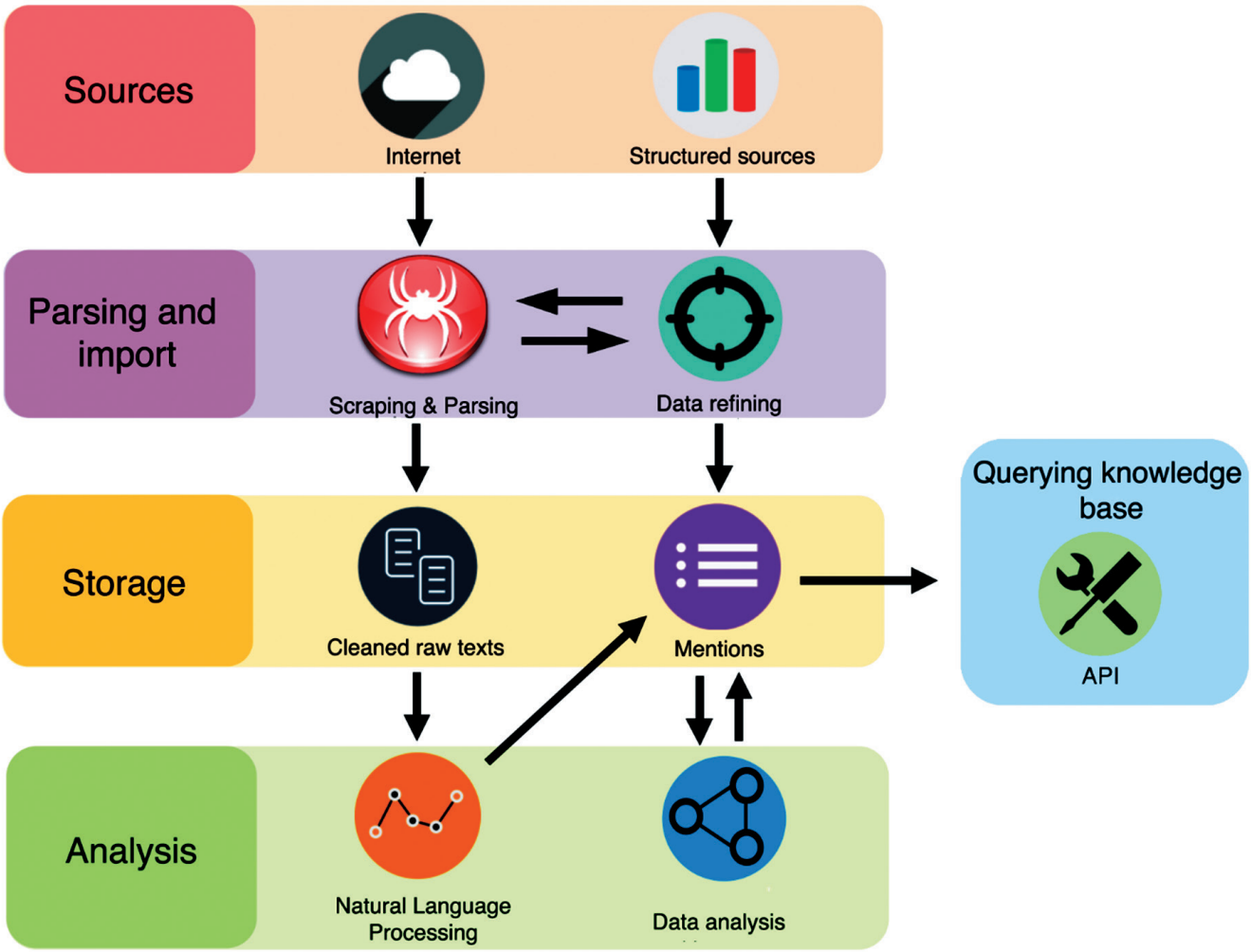


Fig. 6. Top-level operating diagram of the system

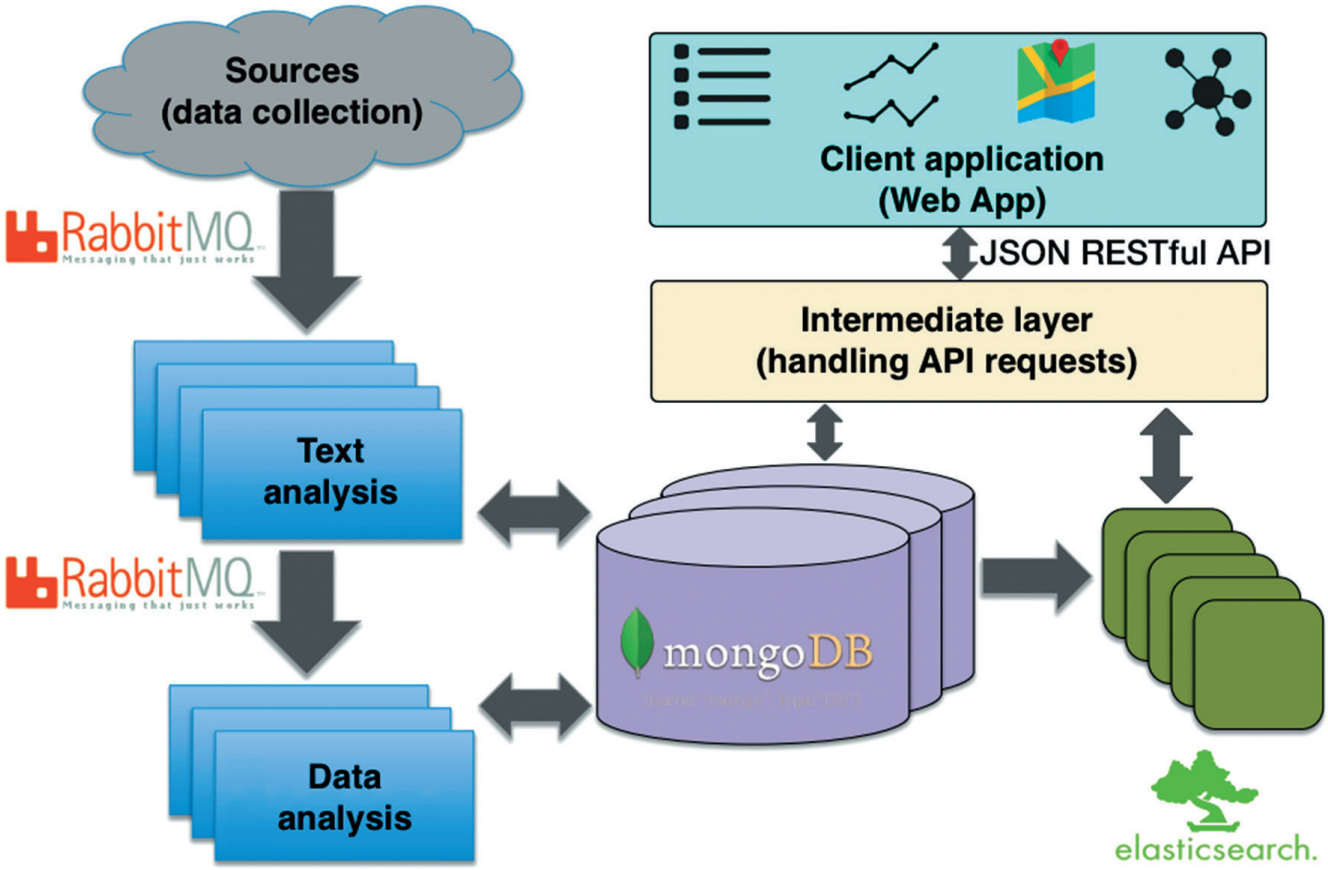


Fig. 7. Technical architecture of the system in terms of data flow

The system is distributed and has a microservice architecture (Fig. 7). The components communicate using RabbitMQ message queues generating about 4000 messages a second. The knowledge base is stored in a MongoDB NoSQL storage (9 shards with read and write roles), while for the snippets, the ElasticSearch full-text search system is used (7 shards). Metadata for a hundred documents take 1 Mb on average.

Results of the method's application as part of applied problems

Monitoring and cyber security analytics, prediction.

The generated entity-event ontologies are directly used for predicting hacktivist attacks, detecting zero-day vulnerabilities and searching for leaks. Another direct use is the analysis of computer security information: what entities and through what are associated with a set of exploits, what methods a specific group uses, what industries are currently threatened, etc.

Early detection of zero-day vulnerabilities.

It has been identified that 77% of vulnerabilities out of the list of CVE (Common Vulnerabilities and Exposures) in Linux were known before they were made public as zero-day vulnerabilities, while the average delay between the first mention and the date of official publishing is 19 days. Additionally, all the vulnerabilities featured in CVE could be found on Twitter [8].

Creation of highly informative features for machine learning.

The obtained and continuously updated knowledge base of cyber security facts can be used for creating highly-informative features in machine learning models as shown in the following problem.

Definition of the risk of an exploit for a vulnerability.

Using supervised training based on support vector machines, a classifier has been obtained that, for each specific vulnerability, predicts whether an exploit will be created with the accuracy of 0.79 and completeness of 0.80. A balanced learning sample included 7000 examples of vulnerabilities. The classifier predicts the risk of a specific vulnerability being exploited and suits the purposes of prioritization of activities aimed at developing countermeasures, emergency isolation of vulnerable systems in case of high risk, etc.

IP address scoring

IP address scoring allows cyber security analysts making decisions regarding further analysis, and, in high alert situations, automatically blocking IP addresses in order to complicate access by the attackers. Importantly, the cybercrime market is commoditized and provides botnets and specialized infrastructure for attacks for rent. Therefore, in practice, blocking high-risk IP addresses is quite efficient, especially against DoS attacks aimed at causing the denial of service by systems.

Risk-based ranking of cyber security events and entities.

The risk of an entity or event is calculated based on the reference dynamics, presence of significant targets and diversity of a language in the mentions. All features

are calculated using the moving average for the estimated entity, as the mentions often occur in "spikes" (day-night, week day-week end, etc.). The level of criticality for entities is based on the number of references to events of cyberattacks/exploits occurring today or within the next month and including the entity. The overall scope of references of a certain entity does not affect the level of criticality: small spikes and anomalies have a more significant effect, as in cyber security not the known status, but deviations from it are what matters.

The linguistic diversity in the references is evaluated based on the repetitiveness of the descriptive vocabulary. Descriptions in different languages are deemed to be different. Such metrics allow distinguishing events that cause real discussions (sign that the event directly affects someone's interests) and allows avoiding over-evaluation, which occurs in many social networking monitoring systems due to repetitions.

Conclusion

The paper showed that the use of entity-event ontologies in cyber security is of practical value. Additionally, it can be a significant component or an auxiliary mechanism as part of other methods.

Another finding is the high informativeness of features based on retrieved information when it is used in machine learning models, which allows improving the quality of such models used in cyber security for the purpose of identifying anomalies, extrapolation and prediction, classification and clusterization, search for patterns and associations.

The theoretical result consists in the feasibility to preprocess corpora that enables the use of classical quantitative and categorical methods with regard to texts by means of information acquisition.

Further research should cover the applicability of the method for the analysis of logs (including within borders), correspondence (search for leaks), social networks monitoring, analysis of cyber security documents.

References

[1] Kühner H., Seider D. Security Engineering für den Schienenverkehr. *Eisenbahn Ingenieur Kompendium* 2018:245-264.

[2] Makarov B.A. Topicality of cybersecurity on railway transport. *Railway Equipment Journal* 2015;3(31):10-15.

[3] Kiseliova E.M. [Railways as an object of cyber security]. www.eduherald.ru; 2018 [accessed 15.06.2020]. Available at: http://www.eduherald.ru/ru/article/view?id=19179. (in Russ.)

[4] McNeil N., Bridges R.A., Iannacone M.D., Czejdo B., Perez N., Goodall J.R. Pace: Pattern accurate computationally efficient bootstrapping for timely discovery of cyber-security concepts. 12th International Conference on Machine Learning and Applications 2013;2:60-65.

[5] Kuzmina N.M., Ridley M.K. About automatic construction in information systems of civil aviation ontology of the subject field on the corps of texts. *Scientific Bulletin of The State Scientific Research Institute of Civil Aviation* 2018;21:122-131. (in Russ.)

[6] Kuzmina N.M., Ridley M.K. Architecture of ontology construction and semantic search system. *Scientific Bulletin of the State Scientific Research Institute of Civil Aviation* 2019;28:103-113. (in Russ.)

[7] Bergner S., Lechner U. Cybersecurity ontology for critical infrastructures. Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management 2017;2:80-85.

[8] Trabelsi S., Plate H., Abida A., Aoun M., Zouaoui A., Missaoui C., Gharbi S., Ayari A. Mining social networks for software vulnerabilities monitoring. 7th International Conference on New Technologies, Mobility and Security (NTMS) 2015:1-7. DOI:10.1109/NTMS.2015.7266506.

About the authors

Michael K. Ridley, post-graduate student, Moscow Aviation Institute (National Research University), Russian Federation, Moscow, e-mail: mr@kalabi.ru

The author's contribution

The author has analyzed the subject area, suggested a method of acquisition of information from open sources using entity-event ontologies. An analytics system previously developed by the author for the purpose of acquisition and storage of entity-event ontologies was improved and adapted to the needs of cyber security. Five application problems were solved, i.e. monitoring and analytics in cyber security, early detection of zero-day vulnerabilities, identification of the risk of a vulnerability's exploit, IP address scoring, risk-based event and entity ranking in cyber security).

Conflict of interests

The author declares the absence of a conflict of interests.

Original article
Dependability, vol. 20 no. 3, 2020 https://doi.org/10.21683/1729-2646-2020-20-3-61-67

Methods of quantitative estimation and reduction of uncertainty of the accidental risk in fire explosive facilities

Evgeny Yu. Kolesnikov, *Volga State University of Technology, Russian Federation, Yoshkar-Ola*
e.konik@list.ru

Evgeny Yu. Kolesnikov

Abstract. *Currently, ensuring the industrial safety of hazardous industrial facilities involves – along with conventional oversight – the risk-oriented approach that is significantly more flexible. The procedure of quantitative estimation of an accidental risk for hazardous industrial facilities is essentially one of the procedures of conformity assessment, as it includes the comparison of the risk indicators obtained by means of calculation (or expert assessment) with their standard values. The* **Aim** *of the paper is to define the problem of uncertainty that is associated with all the stages of quantitative estimation of an accidental risk, make a brief historical account, analyze its types and sources, describe the approaches employed as part of quantitative estimation of this uncertainty. Currently, it is accepted to identify the terminological, parametric and model types of uncertainty, whose examples are provided in the paper. Analysis shows that a fourth – computational – type should be added, whose contribution in many cases may be considerable. It is shown that, due to a number of circumstances, scalar numbers that are normally used for defining parameter values of the physical-mathematical models of failure processes are in reality mere indicators of the ranges of their value variation. Currently, uncertainties in the values of accidental risk parameters are accounted for using probabilistic and deterministic approaches, as well as fuzzy numbers.* **Methods.** *For the purpose of quantitative estimation of uncertainty, the paper employs the method of interval analysis. In the most general case, without using the hypothesis on the behaviour of a parameter value within the range of its possible variation, the parametric uncertainty can be defined with an interval number. In that case, all the required calculations are performed using interval methods. The natural (naive) version of interval analysis has a serious drawback that consists in an unjustified increase of the width of the interval number deduced by means of interval calculations, if one or more input parameters of the model enter into the calculation formula more than once, or the input parameters are functionally interdependent. Modern interval analysis employs methods allowing to alleviate this effect. They are briefly described in this paper. It is shown that if statistical information is available on the behaviour of parameter values within their variation intervals, the results of interval calculations of the accidental risk indicators can be significantly improved. The suggested method of reducing the computational uncertainty of quantitative estimation of the accidental risk in the interval setting is illustrated with a numerical example of risk indicator calculation for the "fireball" accident scenario. The paper sets forth the results of interval calculation of an individual accidental risk for an explosion and fire hazardous facility "reservoir with a flammable liquid" in three ways: a) naive; b) accounting for the effect of parameter correlation; c) additionally, accounting for available statistical information.* **Conclusions.** *Interval methods allow not only taking into consideration the presence of uncertainty in the accidental risk parameters, but evaluating it quantitatively. There are efficient methods of alleviating the negative*

Keywords: *industrial safety, accidental risk, parametric uncertainty, interval methods of calculation, minimization of computational uncertainty.*

For citation: *Kolesnikov E.Yu. Methods of quantitative estimation and reduction of uncertainty of the accidental risk in fire explosive facilities. Dependability 2020;3: 61-67. https://doi.org/10.21683/1729-2646-2020-20-3-61-67*

Received on: *16.06.2020* / **Revised on:** *04.07.2020* / **For printing:** *21.09.2020*

Introduction

Large-scale transportation of hazardous substances, including flammable ones, in hazardous industrial facilities (HIF) is fraught with uncontrolled emissions and leaks that may cause explosions and fires, toxic damage to people and pollution of large territories. Explosions may also occur within industrial equipment, if the process parameters exceed the safe limits.

Over the last two decades in Russia, along with the conventional, supervisory approach to industrial safety, an alternative method has been used that is based on the analysis and quantitative estimation of an accidental risk (QER). The risk-oriented approach is much more flexible, innovation-friendly as compared to the conventional method. It does not restrict specific engineering solutions. Instead of regulating many parameters of the design and process, it only requires a number of target indicators (individual, social risk of an accident) to be within the standard values [1].

The procedure of HIF QER is essentially one of the procedures of conformity assessment, as it includes the comparison of the risk indicators obtained by means of calculation (or expert assessment) with their standard values.

The QER methodology originated and developed almost simultaneously in the Old (in the chemical industry) and New World (in the nuclear industry and astronautics). As early as at the first stage of the application of the risk analysis methodology it became apparent that many parameters of the problem (e.g. the properties of a hazardous facility and its environment) in reality vary, change within certain ranges. In order to take such variations into account, initially the quantitative estimations of risk were performed according to the most conservative scenario, whereas the quantity of a hazardous substance involved in an accident is the highest, the weather conditions and location of the target facilities within the affected area are the least favourable.

However, with time, the conservative approach was abandoned, as the probability of a simultaneous combination of all marginal conditions is too low. As an alternative, it was suggested to use "average" parameter values for accident risk assessment. In our opinion, this approach is also unsatisfactory, because it: a) creates a dangerous illusion of "accurate" assessment of the risk indicators; b) does not allow evaluating the actual range an indicator value varies (or may be) within. Such changes of a parameter value are conventionally called and quantitatively estimated with its uncertainty (parametric).

Types of uncertainty of the results of quantitative risk assessment

Uncertainty is associated with all stages of the QER procedure, just like any mathematic simulation. The causes, part objective, part subjective, are analyzed in [2]. For the purpose of quantitative estimation of uncertainty (QEU) of accidental risk and adoption of measures for its reduction, it is important to classify the uncertainty by origin. Conventionally, the terminological, parametric and model types of uncertainty are distinguished. To that should be added the computational uncertainty caused by the specificity of the computational methods used in the course of simulation.

The *terminological uncertainty* is due not only to the ambiguous definitions of the used terms and concepts in the QER guidelines, but also their different interpretation by experts. The latter is due to the differences in the mindsets of the people, their basic education, standards and stereotypes of the professional environment. It should be noted that the terminological uncertainties (ambiguous interpretation of a term, concept, parameter), along with the obvious qualitative, has a clear quantitative aspect. That can be seen using the example of the parameter "length of flame" L (pool fire, flare). Most QER guidelines do not provide a clear and unambiguous interpretation of this parameter, which is fraught with serious differences:

a) L, average height (length) of the flame, m [3];

b) L_f, length of truncated cone (flare), m [3];

c) L, visible length of flame, m [4].

Meanwhile, the meaning of this parameter is not as obvious as it seems. The situation is similar to the case with the parameter of "fireball diameter" D_F. The matter is that the concepts of "visible" length of flame ("visible" ball diameter) and the concept of "size of the area efficiently radiating heat" should be distinguished. According to CPR-14E [3], in case of pool fire, the value L defined using those two methods may differ up to three times! Only the AIChE CCPS Guidelines [4] clearly define the average length of the flame. Meanwhile, this parameter affects the magnitude of the adverse factors of an accident, i.e. the rate of the heat flow against the target facility I, kW/m^2.

The *parametric uncertainty* means that the parameter value of a model (problem) cannot be assigned a precise (point-wise, scalar) value. That is due to the fact that the parameter value:

a) either objectively varies, like the air temperature and windspeed (if the HIF is situated in the open), or the quantity of the hazardous substance inside a piece of equipment at the moment of accident, etc. that are not exactly known;

b) or is adopted as the result of measurements that are inevitably associated with measurement uncertainty;

c) or is quoted in reference literature in the form of an interval;

d) or, due to the scarcity of available information, was adopted by means of expert methods, etc.

The parametric uncertainty due to the first two circumstances is called aleatoric; its nature is objective. By contrast, uncertainty caused by c) and d) is subjective; it is called epistemic. Objective uncertainty cannot be eliminated in principles, while epistemic uncertainty can be reduced, and that should be done, when possible.

Model uncertainty occurs in the course of QER (but not only), if used for describing the nature of any physical-

mathematical, mathematical, simulation and other models. It is obvious that, as any model simplifies, coarsens the simulated object or process, it has a limited applicability, because the simulation results will always differ from the reality. That is a fact simply because, within the scientific paradigm, experience is chosen as the main criterion of a theory's validity, while due to the presence of measurement uncertainty (error, as it used to be called) the calculation data obtained through the most advanced model will never exactly match the experimental data. Currently, HIF QER uses several alternative models that describe the progress of accident scenarios, development of the adverse factors of an accident, probability of damage to target facilities. It suffices to name at least the models recommended in [3–6], although the authoritative three-volume monograph [7] features dozens of such models. It was many times demonstrated that the variation in the results of quantitative estimation of risk obtained using various models may be as high as three or more orders of magnitude.

There are at least two methods of minimizing the model uncertainty while performing QER:

1) conventional for the USSR and now Russia, under which a certain model is adopted as reference and assigned as normative, the only allowed while performing QER;

2) development of the most adequate model, experimentally verified with a clearly defined application.

The existence of *computational uncertainty* is due to the approximate methods of solving model equations. Analytic solutions of model equations are now an exotic thing. Solutions are obtained using modern application software. However, even if all model parameters are set accurately, the use of floating-point numbers in the computer code, inevitably implying rounding, truncation of terms of series, interruption of the iterative computational process, etc., cause the uncertainty of approximate calculations. Another source of computational uncertainty that is due to the specificity of interval calculations will be examined below.

Conventional mathematic simulation operates on pointwise, scalar parameter values (both input and of model parameters). The calculation results are also normally represented in the form of a scalar number. Given the above circumstances, the result of mathematic simulation is always an interval. Naturally, the HIF QER procedure as part of the risk-oriented approach is not an exception. However, it is obvious that such scalar values of risk indicators are in reality just markers of the intervals, within which their value can vary in reality.

Interval presentation of the parametric uncertainty

The active Guidelines for the quantitative estimation of the risk of accident in HIF [8] recommend assessing the uncertainty of the obtained risk indicators, yet do not indicate how to do that. Meanwhile, as it is known, there are a number of methods of solving the problem: a) using fuzzy numbers; b) in the probabilistic setting; c) using interval numbers.

In our opinion, the latter appears to be the most universal, as it does not require hypothesizing about the behaviour of a parameter value within the variation range [2], which is required for both the probabilistic description of uncertainty, and the use of fuzzy numbers. It should be understood that the probabilistic description of a value means it has the probability distribution function (in the differential or interval form). The latter is only possible if there is an entire assembly of objects of the given type, a statistical stability, when any sample parameters tend to the theoretical probabilistic values in case of infinite increase of the sample size.

In respect to real HIF, identifying sets of elements that could be made an entire assembly is unlikely. Manufactured by different companies, having different histories of load and maintenance, even such simple elements as a latch, in practice have significantly varied properties. Therefore, for instance, the hypothesis of normal distribution of strength with specified average and standard deviation, requires serious substantiation.

It is much more reliable to specify the same value with an interval number (interval). The latter will mean that the parameter value is within the specified limits. No assertions are made regarding its distribution within the range.

Defining parameter values of mathematical models with intervals complies with their nature, given the uncertainty. Today, interval analysis (the branch of mathematics that operates on interval numbers) is widely used and allows performing all calculations required for QER and deducing risk indicators in interval form.

A vast majority of mathematical models used in the active Guidelines for quantitative estimation of accidental risk are analytical (parametric). Therefore, calculating risk indicators implies finding the range of values of the objective function, or external assessment of the range of values in the interval setting.

Performing QER in the interval setting perfectly fits the purpose of QEU, as the width of the obtained interval numbers constitutes a direct quantitative estimation of their uncertainty. In practice, the situation is simplified by the fact that at this point there are commercially available special software products that support interval calculations. One of such programs is INTLAB toolbox developed by Professor S.M. Rump of the Institute for Reliable Computing, Hamburg University of Technology. INTLAB is an interval application of MATLAB that allows performing calculations with interval numbers.

Another obvious advantage of the interval expression of parametric uncertainty is the capability to simultaneously account for uncertainties of various types:

a) measurement, conventionally expressed as the average ± measurement uncertainty (± measurement error, as it used to be called);

b) epistemic, expressed in the form of intervals;

c) stochastic (if there is a probability distribution function) defined by a confidence interval.

Negative characteristics of the interval methods and ways of their minimization

As it is known from experience, if risk indicators are calculated using natural (previously known as naive) interval methods, without taking special measures in order to reduce the calculation uncertainty, the result may constitute interval values of very significant width, which deprives the operation of any practical value.

Let us note that over the last few decades Russian and foreign experts have been actively furthering interval analysis (see, for instance, [9–11]). It has been shown that it helps solve some complex mathematical problems better that by using classical mathematical methods. Problems inherent to interval analysis alone have been identified and researched:

a) disproportionate widening of calculation results in cases when the parameters of the calculation expression enter into it more than once;

b) similar widening of the result in a situation when such parameters are associated with a functional relationship.

For the purpose of minimizing the above negative effects, several methods have been developed: Ramon Moore's interval splitting, branch-and-bound, global optimization, etc.

Method of reducing uncertainty of the target risk metrics in the interval setting using information on the distribution of parameter values

In a situation when reliable, statistically stable information is available on the distribution of parameter values within the variation intervals, the uncertainty of the risk metrics can be significantly reduced. That can be done following on from the standard method of the EMERCOM of Russia [6], according to which the magnitude of the individual risk R, year^{-1} for an employee within the facility is identified according to formula

$$R = \sum_{i=1}^{I} q_{im} P(i), \qquad (1)$$

where $P(i)$ is the magnitude of the potential risk in the i-th area of the facility's territory, year^{-1};

q_{im} is the probability of the employee's presence in the i-th area of the facility's territory.

We will apply this idea not only to the location of personnel within a HIF's territory, but other parameters of the problem as well. Let us assume that the considered HIF has reliable statistical data, according to which:

1) P_1 of the time (unit fractions) personnel are at the distance X_1 away from the center of the considered production unit (PU), while the remaining time P_2 they are at the distance X_2;

2) the mass m_0 of hazardous substance in the PU, kg: a) during P_m01 of the time (unit fractions) $m_{01} \in \left[\underline{m_{01}}; \overline{m_{01}}\right]$; b) P_m02 of the time $m_{02} \in \left[\underline{m_{02}}; \overline{m_{02}}\right]$ and c) P_m03 of the time $m_{03} \in \left[\underline{m_{03}}; \overline{m_{03}}\right]$;

3) based on the available meteorological information, the discrete density of the distribution probability of free air can be recovered, which can be illustrated with a specific example. According to SP 131.13330.2012 [12], the average monthly free air temperature t_a in the area of a certain HIF, °C is: I, -12.1; II, -11.4; III, -4.6; IV, -4.7; V, 12.0; VI, 16.5; VII, 18.6; VIII, 16.1; IX, 10.3; X, 3.4; XI, -3.7; XII, -9.4. By introducing the designation $T_a = t_a + 273.15$, K, we have $T_a \in [261.05; 291.75]$ K. By rounding-off external interval boundaries to whole numbers, we will obtain $T_a \in [261; 292]$ K.

Let us use MATLAB to approximate the yearly variation of the temperature [13] with a sixth-degree polynomial and present the results in Fig. 1.

Then, let us split the temperature range T_a into 31 subintervals with the width of 1 K and calculate the frequencies n_j of the temperature being within such intervals ($j = 1, 2, \ldots 31$). As a discrete valuation of the probability P_{Tj} of temperature distribution within the range [261; 292] K let us adopt the values $P_{Tj} = n_j/31$ (it is obvious that the normalization requirement $\sum_{j=1}^{31} P_{Tj} = 1$ is met).

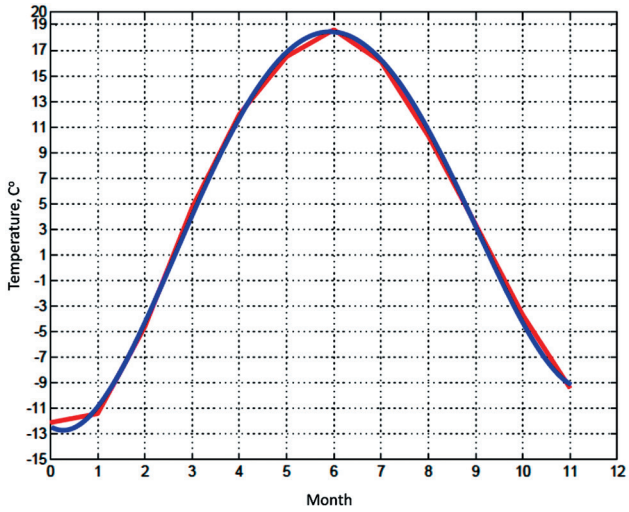


Fig. 1. Annual variation of free air temperature:
— per SP 131.13330.2012;
— polynomial approximation

Further, let us calculate the target risk metrics (e.g., individual risk R_{ijk}) for all combinations of parameter subintervals ($i = 1, 2$, distance between the personnel and the epicenter of the accident at the moment of its occurrence; $j = 1, 2, \ldots 31$, free air temperature; $k = 1, 2, 3$, quantity of the hazardous substance in the PU).

The considered parameters X_i, T_j and m_{0k} as independent random values, target metric (individual risk R_{ind}) of the examined production unit using formula

$$R_{ind} = \sum_{i=1}^{2} \sum_{j=1}^{31} \sum_{k=1}^{3} R_{ijk} P_{Xi} P_{Tj} P_{m_{0k}}. \qquad (2)$$

The calculation of individual accidental risk performed using this method and INTLAB has shown that the suggested technique allows significantly reducing its uncertainty (interval width).

Example of individual accidental risk estimation using the suggested method for the fireball scenario

Let us examine another example of application of the suggested method. As it is known, one of the scenarios of accidents affecting reservoirs containing a flammable substance in liquid, is the BLEVE-type explosion. Such scenario, as accident statistics show (see, for instance, [14]), may occur in situations, when a spherical or horizontal cylindrical reservoir with a flammable substance (LHCG, HIL) is within the body of fire. If the heat inflow from the outside is so high, that the vapour jets outflowing though the open valves of the reservoir are unable to prevent the pressure buildup in its steam space, at some point in time the shell of the reservoir will rupture. A cloud of overrich mixture will be released into the environment that will immediately catch fire on the outside and start floating up in the atmosphere releasing a powerful heat flow. Phenomenologically, a "fireball" (FB) is a glowing cloud of a varying shape, whose temperature and emission power are constant both in time, and in terms of the surface area. However, in the engineering practice, FB are normally imitated with a glowing sphere, that has a constant surface radiant heat intensity and floats up in the atmosphere under the action of the force of buoyancy.

As the target indicator of the risk of such accident scenario, let us consider the individual accidental risk, the probability of lethal injury to personnel by downward heat flow. The AIChE CCPS QER Guidelines [4] suggest calculating FB parameters (diameter D_{FB}, height of the center H_{FB} and glow duration t_{FB}) using empirical dependences that are power relations: $D_{FB} = 5.8 \cdot m_0^{1/3}$; $H_{FB} = 0.75 \cdot D_{FB}$, where m_0 is the initial mass of the flammable substance in the reservoir, kg. The FB model has an interesting feature [4]. In it, the calculation formula for the parameter t_{FB} depends on the value of m_0:

a) if $m_0 < 30\,000$ kg $t_{FB} = 0.45 m_0^{0.33}$, (3)

b) if $m_0 < 30\,000$ kg $t_{FB} = 2.6 m_0^{0.166}$. (4)

For the radiant emittance E_f, the FB caused by BLEVE, in the opinion of AIChE CCPS, the $E_f \in [200; 350]$ kW/m^2 is typical.

In the FB approximation with a point emitter, the heat flow I, kW/m^2 hitting the target facility, can, according to [4], be calculated as follows:

$$I = E_f \tau_a \left(R_{FB} - \frac{D_{FB}}{2} \right) F_q, \quad (5)$$

where R_{FB} is the distance from the center of the FB to the target facility, m;

$\tau_a(X)$ is the transparence of the free air to the infrared flux;

F_q is the geometric visibility factor for a vertical surface (e.g., a standing person).

As the atmospheric absorption of the thermal emission is primarily ensured by vapour molecules, the AIChE CCPS recommends estimating τ_a with the help of the Pietersen and Huerta correlation

$$\tau_a(X) = 2,02 (P_W X)^{-0,09}, \quad (6)$$

where P_W is the partial pressure of vapour, PA;

X is the distance travelled by the beam, m.

For the purpose of calculating P_W under known relative humidity R_H, % and air temperature T_a, K, Mudan and Croce suggested a simple correlation that is true in respect to the range $10^4 < P_W \cdot X < 10^5$ H/m:

$$P_W = 1013,25 R_H \exp\left(14,4114 - \frac{5328}{T_в}\right). \quad (7)$$

Let us specify the relative air humidity in the area of the HIF with the interval $R_H \in [50, 85]$ %.

According to [4], for distances X that exceed the FB radius, F_q is calculated according to formula

$$F_q = \frac{X \left(\frac{D_{FB}}{2} \right)^2}{\left(X^2 + H_{FB}^2 \right)^{3/2}}, \quad (8)$$

that, subject to the formula $H_{FB} = 0.75\ D_{FB}$ is easily modified into:

$$F_q = \frac{4\beta_X}{9\left(1 + \beta_X^2\right)^{3/2}}, \quad (9)$$

where $\beta_X = \frac{X}{H_{FB}}$ – is a dimensionless distance.

The probability of human injury caused by thermal radiation P_{inj} in the course of QER is evaluated using the so-called probit-function Pr. This approach, first suggested by Finney, is suitable for describing the facility's response to the effect of any factor of accidental nature, if this effect is normally distributed [4]. The dependence $P_{inj}(\Pr)$ can be expressed with a standard error function:

$$P_{inj}(\Pr) = 0,5\left[1 + erf\left(\frac{\Pr - 5}{\sqrt{2}}\right)\right]. \quad (10)$$

Guidelines [4] recommend calculating the function Pr of lethal human injury caused by heat flow using formula:

$$\Pr = -14,9 + 2,56 \cdot \ln\left(\frac{t_{exp} \cdot I^{4/3}}{10^4}\right), \quad (11)$$

where t_{exp} is the duration of exposure, s (in case of FB $t_{exp} = t_{FB}$);

I is the intensity of the FB heat flow affecting a person, W/m^2.

It is obvious that, if the density of the incident heat flow I is expressed in kW/m^2,

$$\Pr = -14,9 + 2,56 \cdot \ln\left(t_{exp} \cdot I^{4/3}\right), \quad (12)$$

Table. Results of individual accidental risk estimation in interval setting by three methods

Parameter value	Interval estimation method		
	"Naive"	accounting for the effect of parameter correlation	additionally, accounting for available statistical information
Value of individual accidental risk, year^{-1}	$[0.0; 0.56]\times10^{-4}$	$[0.0001; 0.54]\times10^{-4}$	$[0.0034; 0.4]\times10^{-4}$

Let us evaluate in the interval setting the individual accidental risk of injury to personnel of a certain conventional HIF caused by FB heat flow:

$$R_{inj} = P_{inj} \cdot P_{av}, \quad (13)$$

where P_{av} is the probability of realization of this accident scenario, year^{-1}.

Let us assume that in the present case FB appears after the explosion of an RGS-100 (steel horizontal reservoir) situated in its territory and containing isopropyl alcohol that was affected by fire. Let the probability P_{av} be evaluated with the value $P_{av} \in [3.8; 5.7]\times10^{-5}$ year^{-1}.

Let us further assume that:

- according to reliable statistical data:

a) HIF personnel within the lethal area of the accident: 1) during 25% of the time ($P_x1 = 0.25$) is at the distance of $X_1 \in [70; 80]$ m from the reservoir, while during the remaining time ($P_x2 = 0.75$) they are at the distance of $X_2 \in [80; 100]$ m;

b) mass m_0 of isopropyl alcohol in the reservoir: a) during 20% of the time ($P_m01 = 0.2$) $m_{01} \in [30\,000; 40\,000]$ kg; b) during 50% of the time ($P_m02 = 0.5$) $m_{02} \in [40\,000; 50\,000]$ kg, and c) during 30% of the time ($P_m03 = 0,3$) $m_{03} \in [50\,000; 60\,000]$ kg;

- the average monthly free air temperature in the HIF area is the same as the values cited in the previous section.

We will perform interval calculation of the individual accidental risk R_{ind} of the considered accident scenario for HIF personnel using INTLAB by three methods: a) naive; b) with alleviation of the parameter correlation of the model using the simplest Moore method; c) accounting for available statistical information (by formula (2). Let us present the findings in the summary table.

An analysis of the table shows that the suggested methods allow significantly improving the results of interval calculations (narrowing the intervals) by reducing the computational uncertainty.

Along with those described in this paper, there are other methods (affine arithmetic, global optimization) that allow efficiently mitigating unjustified widening of the interval calculation results.

Conclusion

Interval methods of accidental risk calculation allow not only taking into consideration the uncertainty inherent to the problem's parameters, but use it, which provides for quantitative evaluation of the problem's target indicators. As the result of calculations in the interval setting, the risk indicators are also presented in intervals, which is perfectly natural and adequate in the context of emergency safety of hazardous technical facilities.

At the same time, calculation in the natural (naive) version of interval analysis due to its specificity can be associated with significant disproportional growth of the width of the calculation result interval. As of today, there are efficient methods of finding the ranges of values of interval-valued functions enabling results free of parasite widenings.

The paper presents the results of interval calculations of the individual accidental risk of one of the simple emergency scenarios in three ways: a) the natural method; b) with reduction of the cohesiveness of model parameters; c) with the use of the available reliable information on the behaviour of a number of the problem's parameters within their intervals. It is shown that the second and, specificity, the third methods allow significantly reducing the width of the interval of the target accidental risk value.

References

[1] Kolesnikov E.Yu., Teliakov E.Sh. [On the role of the risk analysis methodology in managing fire and industrial safety]. *Herald of Kazan Technological University* 2015;18(1):285. (In Russ.)

[2] Kolesnikov E.Yu. Quantitative estimation of the uncertainty of fire risk. Emergency scenario Flammable liquid spill fire. *Issues of Risk Analysis* 2014;11(4):52. (in Russ.)

[3] CPR-14E Methods for the calculation of Physical Effects, 3-rd ed. The Hague; 2005.

[4] Guidelines for chemical process quantitative risk analysis, 2-nd ed. AIChE/CCPS; 2000.

[5] World Bank technical paper number 55. Techniques for Assessing Industrial Hazards. A Manual. Washington D.C.; 1988.

[6] [Method of identification of estimated values of fire risk at industrial facilities. Approved by order of the EMERCOM of Russia of 10.07.2009 no. 404 as per the order of the EMERCOM or Russia of 14.12.2010 no. 649 "On amendments to order of the EMERCOM of Russia of 10.07.2009 no. 404"]. (in Russ.)

[7] Lee's Loss Prevention in the Process Industries. Vol. 1–3. 3-rd ed. Elsevier; 2005.

[8] [Safety handbook. Methodological framework of the analysis of hazards and emergency risk assessment in hazardous industrial facilities]. Approved by Federal Service for Ecological, Technological and Nuclear Supervision 11.04.2016. Ser. 27. Issue 16. Moscow: ZAO NTTs PB; 2016]. (in Russ.)

[9] Moore R.E., Kearfott R.B., Cloud M.J. Introduction to interval analysis. Philadelphia; 2009.

[10] Shary S.P. [Finite-dimensional interval analysis]. Novosibirsk: XYZ; 2019 [accessed 10.01.2020]. Available at: http://www.nsc.ru/interval. (in Russ.)

[11] Hansen E., Walster G.W. Global optimization using interval analysis. Izhevsk: NITs Regulyarnaya i khaoticheskaya dinamika. Institut kompyuternykh issledovaniy; 2012. (in Russ.)

[12] [SP 131.13330.2012 Building climatology]. (in Russ.)

[13] Zverev A.S., Kiriukhin B.V., Kondratiev K.Ya. et al. Tverskoy P.N., editor. [A course in meteorology (atmospheric physics). A study guide]. Leningrad: Gidrometeoizdat; 1951. (in Russ.)

[14] Prugh R.W. Quantitative Evaluation of Fireball Hazards. Process Safety Progress 1994;13(2):83.

About the author

Evgeny Yu. Kolesnikov, Candidate of Physics and Mathematics, Associate Professor, Senior Lecturer in Life Safety, Volga State University of Technology, Russian Federation, 424000, Yoshkar-Ola, 3 Lenina Sq., e-mail: e.konik@list.ru

The author's contribution

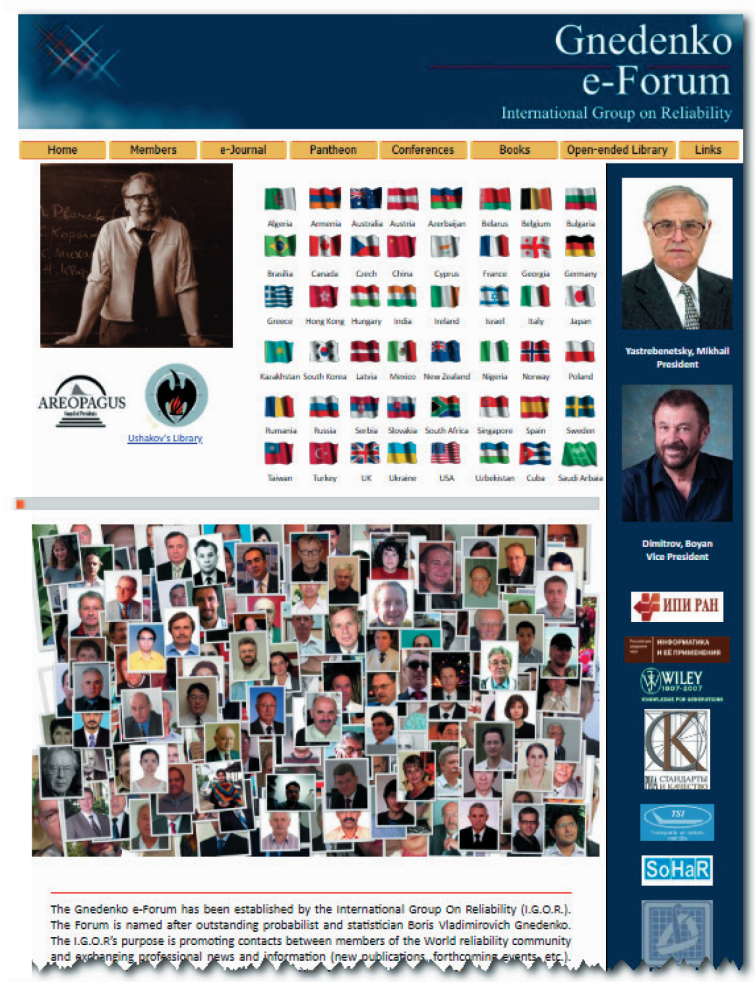
Kolesnikov E.Yu. is the sole author of the paper. Its idea belongs to the author, all calculations were performed by the author without anyone else's involvement.

Conflict of interests

The author declares the absence of a conflict of interests.

GNEDENKO FORUM

INTERNATIONAL GROUP ON RELIABILITY



The Gnedenko Forum was founded in 2004 by an unofficial international group of experts in the dependability theory for the purpose of professional support of researches from all over the world who are interested in studying and developing the scientific, technical and other aspects of the dependability theory, risk analysis and safety in the theoretical and practical domains.

The Forum exists on the Internet as a non-for-profit organization. It aims to involve into joint discussion and communication technical experts interested in developing the dependability theory, safety and risk analysis regardless of their home country and membership in whichever organization.

The Forum acts as an impartial and neutral entity that delivers scientific information to the press and public as regards the matters of safety, risk analysis and dependability of complex technical systems. It publishes reviews, technical documents, technical reports and research essays for the purpose of dissemination of knowledge and information.

The Forum is named after Boris V. Gnedenko, an outstanding Soviet mathematician, expert in the probability theory and its applications, member of the Ukrainian Academy of Sciences. The Forum is the platform for distribution of information on educational grants, academic and professional positions related to dependability, safety and risk analysis all over the world.

Currently, the Forum has 500 members from 47 countries.

Since January 2006, the Forum has been publishing its quarterly journal, Reliability: Theory & Applications (www.gnedenko.net/RTA). The Journal is registered in the Library of Congress (ISSN 1932-2321) and publishes articles, reviews, memories, information and literature references regarding the theory and application of dependability, survivability, maintenance, risk analysis and management methods.

Since 2000, the Journal is indexed in Scopus.

Membership in the Gnedenko Forum does not imply any obligations. It is only required to send your photograph and a brief professional biography (resume) to a.bochkov@gmail.com.
Templates can be found at http://www.gnedenko.net/personalities.htm.

www.gnedenko.net

DEPENDABILITY JOURNAL ARTICLE SUBMISSION GUIDELINES

Article formatting requirements

Articles must be submitted to the editorial office in electronic form as a Microsoft Office Word file (*.doc or *.docx extension). The text must be in black, on a A4 sheet with the following margins: 2 cm for the left, top and bottom margins; 1.5 or 2 cm for the right margin. An article cannot be shorter than 5 pages and longer than 12 pages (can be extended upon agreement with the editorial office). The article is to include the structural elements described below.

Structure of the article

The following structural elements must be separated with an *empty line*. Examples of how they must look in the text are shown *in blue*.

1) Title of the article

The title of the article is given in the English language.

Presentation: The title must be in 12-point Times New Roman, with 1.5 line spacing, fully justified, with no indentation on the left. The font face must be bold. The title is not followed by a full stop.

An example:

Improving the dependability of electronic components

2) Author(s)' name.

This structural element for each author includes:

In English: second name and first name as "First name, Second name" (John Johnson).

Presentation: The authors' names must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be bold. The authors' names are separated with a comma. The line is not followed by a full stop.

An example:

John Johnson[1], Karen Smith[2*]

3) The author(s)' place of employment

The authors' place of employment is given in English. Before the place of employment, the superscripted number of the respective reference to the author's name is written.

Presentation: The reference to the place of employment must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal. Each place of employment is written in a new line. The lines are not followed by a full stop.

An example:

[1] Moscow State University, Russian Federation, Moscow

[2] Saint Petersburg Institute of Heat Power Engineering, Russian Federation, Saint Petersburg

4) The e-mail address of the author responsible for maintaining correspondence with the editorial office

Presentation: The address must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal, all symbols must be lower-case. Before the address reference, symbol * is written. The title is not followed by a full stop.

An example:

*johnson_j@aaa.net

5) Abstract of the article

This structural element includes a structured summary of the article with the minimal size of 350 words and maximum size of 400 words. The abstract is given in the English language. The abstract must include (preferably explicitly) the following sections: Aim; Methods; Results/Findings; Conclusions. The abstract of the article should not include newly introduced terms, abbreviations (unless universally accepted), references to literature.

Presentation: The abstract must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal, except "**Abstract**", "**Aim**", "**Methods**", "**Conclusions**", that (along with the full stop) must be in bold. The text of the abstract must not be paragraphed (written in a single paragraph).

An example:

Abstract. Aim.Proposing an approach … taking into consideration the current methods. **Methods.** The paper uses methods of mathematical analysis,…, probability theory. **Results.** The following findings were obtained using the proposed method … **Conclusion**. The approach proposed in the paper allows…

6) Keywords

5 to 7 words associated with the paper's subject matter must be listed. It is advisable that the keywords complimented the abstract and title of the article. The keywords are written in English.

Presentation: The text must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal, except "**Keywords:**" that (along with the colon) must be in bold. The text must not be paragraphed (written in a single paragraph). The text must be followed by a full stop.

An example:

Keywords: dependability, functional safety, technical systems, risk management, operational efficiency.

7) Text of the article

It is recommended to structure the text of the article in the following sections: Introduction, Overview of the sources, Methods, Results, Discussion, Conclusions. Figures and tables are included in the text of the article (the figures must be "In line with text", not "behind text" or "in front of text"; not "With Text Wrapping").

Presentation:

The titles of the sections must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be bold. The titles of the sections (except the Introduction and Conclusions) may be numbered in Arabic figures with a full stop after the number of a section. The number with a full stop must be separated from the title with a no-break space (Ctrl+Shift+Spacebar).

The text of the sections must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with a 1.25-cm indent. The font face must be normal. The text of the sections must be paragraphed. There must be no indent in the paragraph that follows a formula and contain notes to such formula, e.g.:

where *n* is the number of products.

An example:

1. State of the art of improving the dependability of electronic components

An analysis of Russian and foreign literature on the topic of this study has shown that …

Figures (photographs, screenshots) must be of good quality, suitable for printing. The resolution must be at least 300 dpi. If a figure is a diagram, drawing, etc. it should be inserted into the text in editable form (Microsoft Visio). All figures must be captioned. Figures are numbered in Arabic figures in the order of their appearance in the text. If a text has one figure, it is not numbered. References to figures must be written as follows: "Fig. 3. shows that …" or "It is shown that … (see. Fig. 3.)." The abbreviation "Fig." and number of the figure (if any) are always separated with a no-break space (Ctrl+Shift+Spacebar). The caption must include the counting number of the figure and its title. It must be placed a line below the figure and center justified:

Fig. 2. Description of vital process

Captions are not followed by a full stop. *With center justification there must be no indent!* All designations shown in figures must be explained in the main text or the captions. The designations in the text and the figure must be identical (including the differences between the upright and oblique fonts). *In case of difficulties with in-text figure formatting, the authors must – at the editorial office's request – provide such figures in a graphics format (files with the* *.tiff, *.png, *.gif, *.jpg, *.eps extensions).

The tables must be of good quality, suitable for printing. The tables must be editable (not scanned or in image format). All tables must be titled. Tables are numbered in Arabic figures in the order of their appearance in the text. If a text has one table, it is not numbered. References to tables must be written as follows: "Tab. 3. shows that …" or "It is shown that … (see. tab. 3.)." The abbreviation "tab." and number of the table (if any) must be always separated with a no-break space (Ctrl+Shift+Spacebar). The title of a table must include the counting number and its title. It is placed a line above the table with center justification:

Table 2. Description of vital process

The title of a table is not followed by a full stop. *With center justification there must be no indent!* All designations featured in tables must be explained in the main text. The designations in the text and tables must be identical (including the differences between the upright and oblique fonts).

Mathematical notations in the text must be written in capital and lower-case letters of the Latin and Greek alphabets. Latin symbols must always be oblique, except function designators, such as sin, cos, max, min, etc., that must be written in an upright font. Greek symbols must always be written in an upright font. The font size of the main text and mathematical notations (including formulas) must be identical; in Microsoft Word upper and lower indices are scaled automatically.

Formulas may de added directly into the text, for instance:

Let $y = a \cdot x + b$, then…,

or written in a separate line with center justification, e.g.:

$$y = a \cdot x + b.$$

In formulas both in the text, and in separate lines, the punctuation must be according to the normal rules, i.e. if a formula concludes a sentence, it is followed by a full stop; if the sentence continues after a formula, it is followed by a comma (or no punctuation mark). In order to separate formulas from the text, it is recommended to set the spacing for the formula line 6 points before and 6 points after). If a formula is referenced in the text of an article, such formula must be written in a separate line with the number of the formula written by the right edge in round brackets, for instance:

$$y = a \cdot x + b. \quad (1)$$

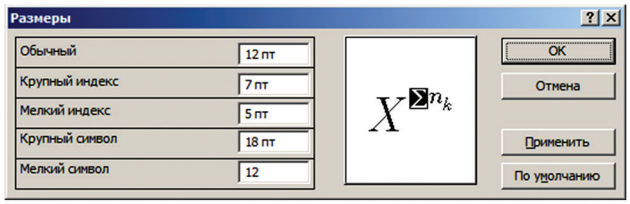
If a formula is written in a separate line and has a number, such line must be right justified, and the formula and its number must be tab-separated; tab position (in cm) is to be chosen in such a way as to place the formula roughly at the center. Formulas that are referenced in the text must be numbered in Arabic figures in the order of their appearance in the text.

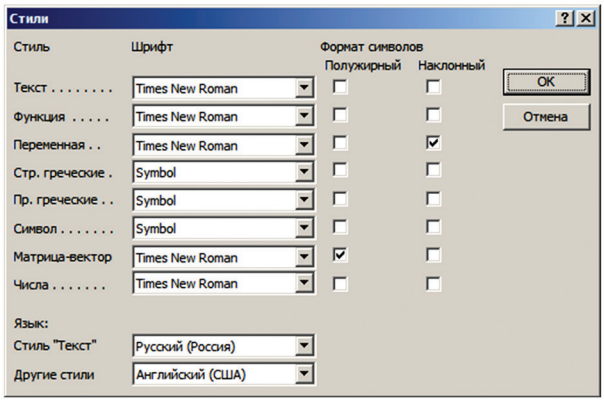
Simple formulas should be written without using formula editors (in MS Word, Latin should be used, as well as the "Insert" menu + "Special Characters", if Greek letters and mathematical operators are required), while observing the required slope for Latin symbols, for example:

$$\Omega = a + b \cdot 0.$$

If a formula is written without using a formula editor, letters and +, –, = signs must be separated with no-break spaces (Ctrl+Shift+Spacebar).

Complex formulas must be written using a formula editor. In order to avoid problems when editing and formatting formulas it is highly recommended to use Microsoft Equation 3.0 or MathType 6.x. In order to ensure correct formula input (symbol size, slope, etc.), below are given the recommended editor settings.





When writing formulas in an editor, if brackets are required, those from the formula editor should be used and not typed on the keyboard (to ensure correct bracket height depending on the formula contents), for example (Equation 3.0):

$$Z = \frac{a \cdot \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{m} y_i \right)}{n+m}. \quad (2)$$

Footnotes in the text are numbered with Arabic figures, placed page by page. Footnotes may include: references to anonymous sources on the Internet, textbooks, study guides, standards, information from websites, statistic reports, publications in newspapers, magazines, autoabstracts, dissertations (if the articles published as the result of thesis research cannot be quoted), the author's comments.

References to bibliographic sources are written in the text in square brackets, and the sources are listed in the order of citation (end references). The page number is given within the brackets, separated with a comma and a space, after the source number: [6, p. 8].

8) Acknowledgements

This section contains the mentions of all sources of funds for the study, as well as acknowledgements to people who took part in the article preparation, but are not among the authors. Participation in the article preparation implies: recommendations regarding improvements to the study, provision of premises for research, institutional supervision, financial support, individual analytical operations, provision of reagents/patients/animals/other materials for the study.

Presentation:

The information must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

9) References

The References must include only peer-reviewed sources (articles from academic journals and monographs) mentioned in the text of the article. It is not advised to references autoabstracts, dissertations, textbooks, study guides, standards, information from websites, statistic reports, publications in newspapers, websites and social media. If such information must be referred to, the source should be quoted in a footnote.

The description of a source should include its DOI, if it can be found (for foreign sources, that is possible in 95% of cases).

References to articles that have been accepted, but not yet published must be marked "in press"; the authors must obtain a written permission in order to reference such documents and confirmation that they have been accepted for publication. Information from unpublished sources must be marked "unpublished data/documents"; the authors also must obtain a written permission to use such materials.

References to journal articles must contain the year of publication, volume and issue, page numbers.

The description of each source must mention all of its authors.

The references, imprint must be verified according to the journals' or publishers' official websites.

Presentation:

References must be written in accordance with the Vancouver system.

The references must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with a 1.25-cm indent on the left. The font face must be normal. Each entry must be numbered in Arabic figures with a full stop after the number. The number with a full stop must be separated from the entry with a no-break space (Ctrl+Shift+Spacebar).

10) About the authors

Full second name, first name (in English); complete mailing address (including the postal code, city and country); complete name of the place of employment, position; academic degree, academic title, honorary degrees; membership in public associations, organizations, unions, etc.; official name of the organization in English; e-mail address; list and numbers of journals with the author's previous publications; the authors' photographs for publication in the journal.

Presentation:

The information must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

11) The authors' contribution

Detailed information as to each author's contribution to the article. For example: Author A analyzed literature on the topic of the paper, author B has developed a model of real-life facility operation, performed example calculation, etc. Even if the article has only one author, his/her contribution must be specified.

Presentation:

The information must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

12) Conflict of interests

A conflict of interests is a situation when people have conflicting and competing interests that may affect editorial decisions. Conflicts of interests may be potential or conscious, as well as actually existing. The objectivity may be affected by personal, political, financial, scientific or religious factors.

The author must notify the editorial office on an existing or a potential conflict of interests by including the corresponding information into the article.

If there is no conflict of interests, the author must also make it known. An example of wording: "The author declares the absence of a conflict of interests".

Presentation:

The text must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

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.

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