# BIG DATA AND INTERNET OF THINGS FOR SAFETY CRITICAL APPLICATIONS: CHALLENGES, METHODOLOGY AND INDUSTRY CASES

*Vyacheslav Kharchenko*

Department of Computer Systems, Networks and Cybersecurity, National Aerospace University KhAI; Centre for Safety Infrastructure Oriented Research and Analysis, Research and Production Company Radiy
v.kharchenko@csn.khai.edu
Ukraine

**Abstract:** The paper discusses some challenges caused by application of Internet of Things (IoT) technologies and Big Data analysis (BDA) in safety critical domains such as Nuclear Power Plants (NPPs), energy grids, health systems and others. Concepts of safety and cyber safety considering security and cyber security attributes for such applications are analysed. The methodological and practical issues of implementing BDA and IoT systems and tools in context of safety and security assessment and assurance are discussed. It's suggested an extended concept of IoT as a (X)Io(Y)Z, where X and Y are adjectives determining main required attribute (X) system and attribute (Y) of generalized thing Z (business, cars, drones, etc). The benefits and limitations of application of BDA and IoT based technologies in safety critical systems are analysed including possibilities of their use for avoiding, monitoring and minimizing consequences of severe accidents. Limitations of BDA application are caused by extensive nature of technologies for collecting and processing big data. Essentially such technologies aren't green, safe and secure and it's required deep analysis of deficits, first of all, cyber security and safety before their usage. The paper describes industrial cases, where IoT and BDA are applied such as Internet of Drones based NPP accident monitoring system, IoT based monitoring and control system, system for prediction of software dependability. The recommendations and limitations of BDA and IoT application in safety critical systems are formulated.

**Key words:** Big Data, Internet of Things, Safety, Cyber Safety, Internet of Drones, Accident Monitoring, Health System, Software Reliability

## 1. INTRODUCTION

### 1.1. Motivation

Information and communication technologies (IT) are, on the one hand, mean of dependability (reliability, availability, safety, security) assurance for systems for critical and commercial domains, and, on the other hand, they are source of vulnerabilities, faults and failures causing new security and safety related challenges and fatal effects for critical infrastructures and business applications.

Influence of modern ITs and IT related paradigms becomes more and more challengeable, first of all, for safety critical systems such as:

- instrumentation and control systems (I&Cs) of nuclear power plants (NPPs),
- on-board and ground control and navigation systems of piloted aerospace and aviation complexes,
- railway signalling and blocking systems,
- automotive systems including vehicle to vehicle, vehicle to infrastructure,
- health monitoring and control systems and so on.

Failures and emergencies of safety critical systems as a rule are caused by several reasons, combination of physical, design and interaction faults and human errors [1,2]. Physical faults are characteristic for hardware, design faults are characteristic for software (and programmable logics), interactive faults are consequences of physical and information intrusions on hardware and software respectively.

To ensure dependability we have to analyze related possibilities and risks at the all levels of a hierarchy "element-component-system-infrastructure" taking into account interaction and interdependency in the vertical and horizontal dimensions [2-4]. Von Neumann's paradigm "reliable systems out of unreliable elements" [5] should be transformed considering challenges caused by application of modern ITs. Paradigm "dependable and safe infrastructure/system/component out of undependable and unsafe (or not enough dependable and safe) systems/components/elements" is becoming more and more important [6].

Besides, concept "IT for safety and security" should be added by "safe and secure IT". New technologies such as Internet of Things (IoT), Big Data (BD) and others can create new positive possibilities and challengeable deficits of cyber security and safety and it's required thorough analysis to search balance of key attributes and to take into account limitations for their application.

### 1.2. Work related analysis

There are lot publications dedicated to aspects of safety and security in context of Big Data (or BD bases analytics – BDA), IoT and other new conceptions and technologies. BDA and IoT are close conceptions, because IoT communications can be called a circulatory system for collection and processing of (big) data. These publications related to BDA/IoT can be divided on three groups:

- publications about BDA/IoT where aspects of safety, security, dependability are not defining and mentioned only [7,8];

- publications describing BDA/IoT based technologies as means to assure safety, security, dependability of critical or non-critical systems [9-11];

- publications that analyse aspects of BDA/IoT safety, security, dependability as a key problem. In this case the challenges and solutions for assessment and assurance of BDA/IoT based systems safety, security, dependability are considered [12-13].

Importance of analysing problems which are crossing of "BD/IoT systems" and "safety, security, dependability attributes" is confirmed by increasing of corresponding references during 2017 (N17) and 2018 (N18) years. Table 1 contains parts related to Internet references on pdf documents concerning fuzzy logic and artificial intelligence (as a close domain to BD and IoT), big data and Internet of Things.

*Table 1. Reference statistics*

| **Keywords, pdf** | **Number of Internet references (N17), July 10, 2017** | **Number of Internet references (N18), August 10, 2918** | **N18/ N17** |
|---|---|---|---|
| **fuzzy logic** | 28 000 000 | 50 400 000 | 1.8 |
| fuzzy safety | 2 260 000 | 9 940 000 | 4.5 |
| fuzzy logic security | 2 760 000 | 6 030 000 | 2.2 |
| fuzzy logic dependability | 1 020 000 | 2 670 000 | 2.6 |
| **artificial intelligence** | 46 500 000 | 107 000 000 | 2.3 |
| artificial intelligence safety | 5 150 000 | 21 600 000 | 4.1 |
| artificial intelligence security | 72 000 000 | 83 800 000 | 1.2 |
| artificial intelligence reliability | 8 240 000 | 13 700 000 | 1.7 |
| artificial intelligence dependability | 724 000 | 10 700 000 | 1.5 |
| **big data** | 148 000 000 | 362 000 000 | 2.4 |
| big data reliability | 11 200 000 | 42 900 000 | 3.9 |
| big data safety<br>big data for safety | 17 700 000 | 172 000 000<br>123 000 000 | 9.7<br>7.2 |
| big data security<br>big data for security | 17 700 000 | 215 000 000<br>189 000 000 | 12.8<br>10.6 |
| big data dependability | 154 000 | 428 000 | 2.8 |
| **Internet of Things** | - | 350 000 000 | - |
| Internet of Things reliability | - | 23 800 000 | - |
| Internet of Things safety | - | 116 600 000 | - |
| Internet of Things security | - | 130 700 000 | - |

The following conclusions can be done basing on Table 1:

- number of references "BD/IoT – safety, security,…" has increased by a factor N18/N17 = 1.2-12.8 during 2017-2018 years;

- the most hot topics are “BD safety” and “BD for safety”, “BD security” and BD for security”;
- topics “IoT safety”, “IoT security” have metrics values similar “BD safety” and “BD security” .

Basing on analysis of publications it should conclude that systematic researches of positive possibilities, restrictions and deficits of safety, security and dependability connected with application of BD and IoT are much needed.

### 1.3. The objective and structure

The objective of the paper is to analyse challenges, methodological issues and solutions in area of BDA and IoT application in point of view safety and security. Structure are the following. Sections 2-4 discusses the methodological and practical issues of implementing BDA and IoT systems and tools in context of cyber security and safety assessment and assurance.

Section 2 generalises concepts of safety and cyber safety considering security and cyber security attributes for critical applications. Section 3 discusses the benefits and limitations of application of BDA and IoT based technologies in safety critical systems including possibilities of their use for avoiding, monitoring and minimizing consequences of severe accidents. An extended concept of IoT is suggested and discussed in context of safety and security in Section 4.

Industrial cases such as Internet of Drones based NPP accident monitoring system, IoT based monitoring and control system, system for prediction of software dependability are described in Section 5. Section 6 concludes results and discusses The recommendations and limitations of BDA and IoT application in safety critical systems are formulated.

## 2. SAFETY AND CYBER SAFETY VIA CYBER SECURITY

Safety (Fig.1a) is an attribute defining how IT based (for example I&C) system (via controlled object) influences on environment (other systems and objects with high value of failure and people health or life), decreases risks and consequences of emergencies. On the other side, failures of safety critical I&C can increase these risks, i.e. cause unsafe influence (red arrow) on information or/and physical environment [14]. Security (computer security, cyber security) defines the degree of influence of information or physical environment on system (blue arrow, Fig.1,b). Insecure influence of environment on safety critical system can cause unsafe influence of system on environment (yellow arrow, Fig.1,c).

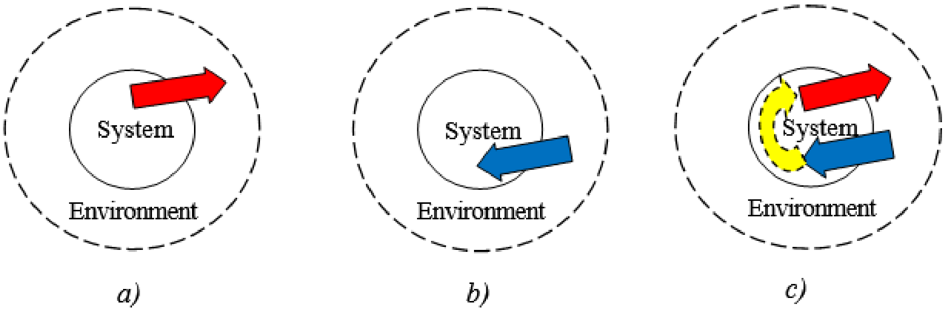


*Fig.1. General models of safety (a), (cyber) security (b) and cyber safety (c)*

In case when transition of system in unsafe state can be caused by attack via open or partially open cyber space a concept "cyber safety" can be used. Other words, if safety of system depends on cyber security (as a part of information security) it's justifiable using of concept "cyber safety" (as a part of safety).

In general, unsafe behaviour of system can be caused by [14,15]:

- hardware anomalies (physical faults, manufacture design and physical faults, vulnerabilities of hardware components attacked by intruders);
- software anomalies (design faults tolerated by changing data environment, for example, by restart; design faults which have to be eliminated by changing of software code; faults caused by software ageing and vulnerabilities of software components attacked by intruders);
- FPGA anomalies similar hardware physical faults and software design faults, and two types of hardware and software vulnerabilities;
- system anomalies (configuration and system vulnerabilities).

Cyber safety is very important methodological concept safety critical systems which perform in cyber space and can be attacked by intruders.

## 3. BIG DATA FOR SAFETY AND SECURITY CRITICAL DOMAINS

### 3.1. Possibilities and risks of application of BDA for critical domains

Data can be collected in such systems by use of different sensors, storages and other sources of information [16]. Table 2 shows possibilities and risks of BDA application in critical domains.

*Table 2. Possibilities and risks of application of BDA for critical domains*

| **Criticality types** | **Domains** | **How (where) are BD made available?** | **Why can BD be applied?** | **Risks BDA application** |
|---|---|---|---|---|
| Safety critical | Nuclear Instrumentation and Control | By sensors and I&C storage | To optimize maintenance | Safety (via security) risk |

| | | | | |
|---|---|---|---|---|
| | (NPP I&C) | | | |
| | Aviation on-board systems | By sensors and OBS storage | To support decision making | Safety (via security) risk,<br>Real time mode |
| | Airport flight control systems (AFC) | By sensors and AFC storage | To support decision making | Safety (via security) risk,<br>Real time mode |
| | Health (control) systems | By patient e-record database analysis | To support decision making | Safety (via security) risk,<br>Real time mode |
| Security/ Data critical | Health (monitoring, storage) systems | By patient e-record database analysis | To support decision making | Security (privacy) risk |
| | Banking (access) | Banking database and other data analysis | To minimize risk of access | Security (privacy) risk |
| Mission critical | Space (unpiloted) | Data storages (Internet) | To minimize risks and optimize results | Security risk |
| | Big R&D project | Data storages (Internet) | To get the best results | Security (money loss) risk |
| Business critical | Banking (charges) | Banking database and other data analysis | To minimize risk | Security (money loss) risk |
| | E-commerce | Banking database and other data analysis | To optimize services | Security (money loss) risk |

BDA is used to achieve the following objectives:

- to minimize risks or avoid potentially dangerous situations;
- to support decision making in pre-accident and post-accident cases;
- to optimize services and maintenance of complex systems (similar NPP I&C systems) and so on.

Main risks of BDA application are caused by two reasons:

- increasing of data capacity and additional possibilities to get unauthorized access to information;
- necessity of real time processing of huge data capacity to make decision or support decision making in time.

### 3.2. Reasons of accidences and application of BDA

Main reasons of accidents are complexity of projects and design anomalies, human errors and environment factors. Severe accidents are occurred if such reasons overlap in time. It confirmed by results of analysis of accident reasons for different severe emergencies beginning of crash of the biggest Swedish ship Vasa in 1668 to Fukushima accident (Table 3).

More detailed description of accident reasons has been presented in [17]. Two questions and aspects of analysis are most interesting:

- are these accidents Black Swan? [18] Expert assessment of the accidents with priority Yes/No is shown in Table 3;
- could BDA used to help to predict and avoid these accidents? BDA could be used to support decision making for recovery after NPP accidents.

*Table 3. Reasons of accidences and application of BDA*

| **Accidents, years** | **Countries** | **Complexity issue** | **Design anomalies** | **Human factors/ errors** | **Environment** | **Is it Black Swan?** | **Could BDA help?** |
|---|---|---|---|---|---|---|---|
| Vasa, 1668 | Sweden | Yes/No | Yes | Yes (politics, overloading) | Yes (strong wind) | No/Yes | No/Yes |
| Titanic, 1912 | UK | Yes | Yes | Yes (business) | Yes (iceberg) | Yes/No | No/Yes |
| Three Mile Island, 1979 | USA | No | Yes | Yes (violations of rules and errors) | No | Yes/No | Yes, for recovery |
| Challenger, 1986 | USA | No | Yes | Yes (business, prestige) | Yes (wind) | No/Yes | No |
| Chernobyl, 1986 | Ukraine | No | Yes | Yes (violations of rules) | No | Yes/No | Yes, for recovery |
| Fukushima, 2011 | Japan | No | Yes | Yes (imperfect management during recovery) | Yes (tsunami) | Yes/No | Yes, for recovery |

### 3.3. Application of BDA: pro and contra

Preliminary conclusions of application of BDA for safety critical systems are the following.

Search, transmission, collection, processing of big data can be applied:

- to improve maintenance and avoid failures including techniques of predictive analytics [19];

- to predict and minimize risks of emergencies;
- to support decision making and decrease resources/costs for recovery accidents and so on.

However, collecting and processing of huge data capacity can be

- useless, if required information and knowledge haven't been got;
- unsafe/insecure, if additional vulnerabilities resulted from increased capacity of data have been used for attacks and intrusions and cause obtaining secret/private information, fatal failures or accidents;
- energy-intensive, because BDA increases number of sensors, traffic intensity, additional storage and so on.

Implementation of BDA technologies can be a reason of extensive development as:

- the probabilistic/deterministic methods and techniques based on "small" data can provide more "fast" processing and receiving of information;
- "slow" traditional methods of processing of "big" data can be more effective;
- BDA based on artificial intelligence, Deep Learning requires big data to start application. Such situation is similar to "snowball effect" and can be called a rule "big data requires more big data";
- big data can be more unsafe/insecure than "small" data for safety critical (non-critical) systems.

Partial question is the following: what is better more complex (for example, semi-Markov's) model with inaccurate parameters calculated by use of big/"small" data or more simple (Markov's) model with accurate parameters calculated by use of "small"/big data?

## 4. CONCEPT EXTENDING AND LIMITATIONS OF INTERNET OF THINGS APPLICATION

To analyse IoT and IoT based systems safety and security issues definition of Internet of Things has to be specified. There are a lot of definitions [20]. In simplified view they are formulated by the following ways:

IoT is a new technology…

IoT is a mix/joining of existed technologies…

IoT is a new idea joining of known and modern technologies…

The conclusion to be drawn that IoT is a paradigm of joining and parametrization of a few technologies such as sensors, embedded and programmable devices, communications and cloud services).

IoT can be presented in general as

IoT → (X)Io(Y)Z ,

where (X) is an adjective determining main required attribute such as

X = {Dependable, Safe, Secure,…; Industrial,…};

I = Internet or Web; Web of Things (WoT) is known as well as IoT;

(Y) is an adjective determining actual attribute of things (Z), Y = {Dependable, Safe, Secure,…; Important, Intelligent,…};

Z = {Alphabet: A (Aqua,...), B (Business,...), C (Cars,...), D (Drones,...), ...}.

Considering that application of IoT is accompanied by increasing of nodes and communications, increasing of transmitted data and, hence, increasing of threats, vulnerabilities, potential attacks and failures which can cause emergencies the following expressions, that are not strong mathematical formulas, describe these circumstances:

IoT = IoT (Internet of Things = Internet of Threats),

IoE = IoE (Internet of Everything = Internet of Emergencies).

According with [21] one of the ten main trends of IT development during next five years will be problem of IoT security and safety. Through 2022, half of all security budgets for IoT will go to fault remediation, recalls and safety failures rather than protection.

Hence, Von Neumann paradigm can be formulated for IoT application by following way: safe/secure IoT based systems or computing out of unsafe (or not enough safe)/ insecure (or not enough secure) nodes and communications. There are a few separate options of this expression depending on characteristics of nodes, communications and cloud resources.

## 5. INDUSTRY CASES

Three industrial cases are described in this section. First and second cases are based on Internet of Things technologies, third one is a supporting technique allowing to specify parameters for modeling.

### 5.1. Internet of drones based post NPP accidence monitoring system

A general structure and underlying principles for creating an IoT based multi-version post-severe NPP accident monitoring system is shown on the Fig.2 [22]. The system consists of an Internet of Things (IoT S) subsystem, a single wired communication subsystem (Wire S), light and wireless communication subsystems (Li-Fi S and Wi-Fi S) and three drone-based wireless subsystems (Drones, DF1, DF2). Drone fleet communicate with private cloud using IoT (DoT S1-S3 and IoT S). Thus sensors subsystems, drone fleet and private cloud form Internet of Drones (IoD) system for accident monitoring with multi-version sensor and communication sybsystems.

System dependability has to be assessed taking into account three issues: reliability, security and survivability.

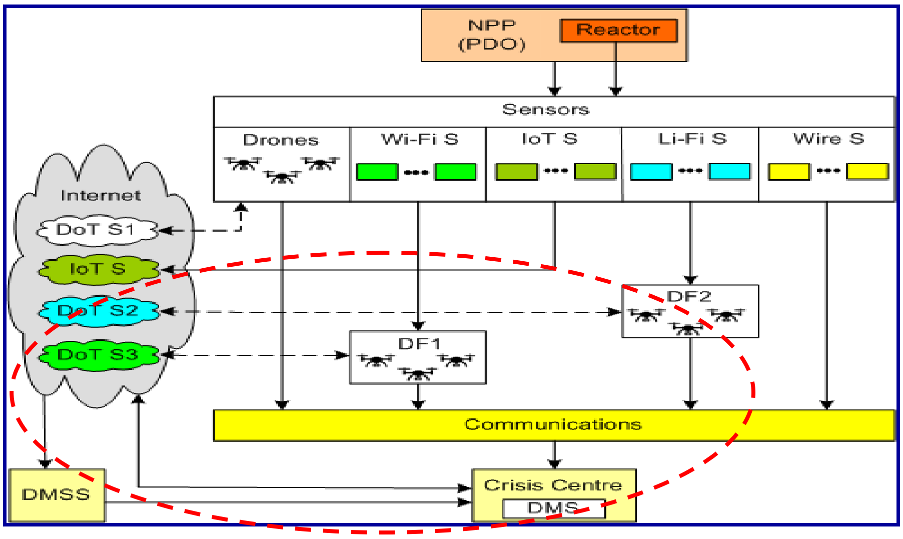


*Fig.2. Internet of Drones based system for monitoring of severe NPP accident*

Reliability block diagrams (RBD) for the system and its subsystems are based on considerations of different variants of sensor, communication and decision making subsystems [15,23]. The probability of failure-free operation can be estimated and researched considering subsystem failure rates and various system configurations depending on strategy and procedures of drone fleet application [24].

Security assessment is based on vulnerability analysis of IoD subsystem and simulation of attacks on component and system vulnerabilities [25]. Survivability models are described in [26].

### 5.2. Internet of mobile devices based health systems

Other case is a healthcare IoT system (Fig.3) [27]. The system has unified structure and is designed to monitor and help to patients with diseases such as diabetics. The system components are a device with a reader, cloud, healthcare provider and communication channel.

Networked healthcare devices sense electrical, thermal, chemical, and other signals from the patient’s body and inform about the physical and mental state. Such devices and system as a whole are safety critical because a human's life depends on its performance.

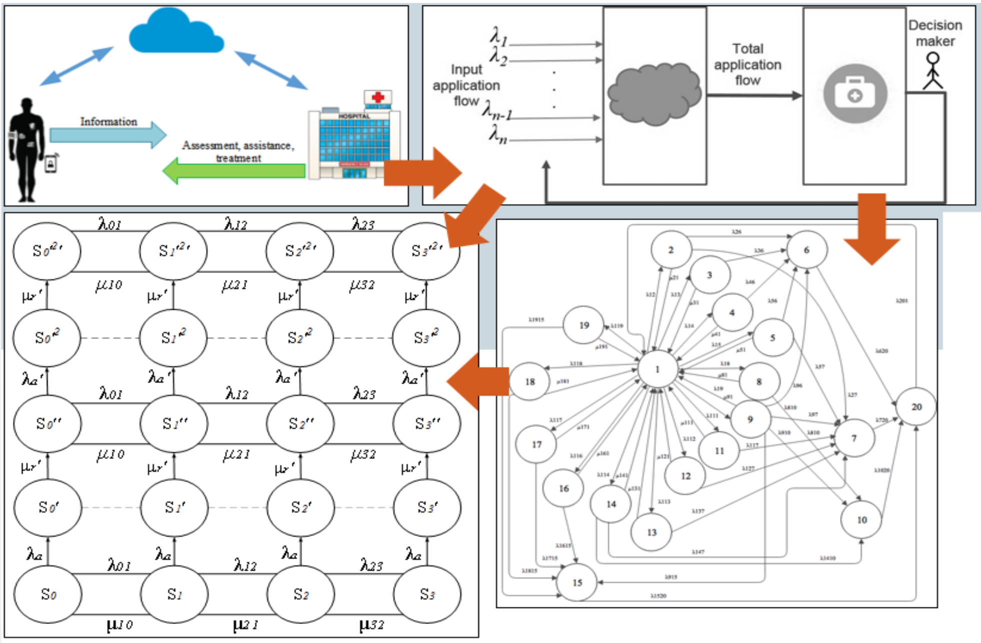

Information
Assessment, assistance, treatment
HOSPITAL
Input application flow
$\lambda_1$
$\lambda_2$
$\lambda_{n-1}$
$\lambda_n$
Total application flow
Decision maker
$\lambda_{01}$ $\lambda_{12}$ $\lambda_{23}$
$\mu_{10}$ $\mu_{21}$ $\mu_{32}$
$\mu_r'$
$\lambda_a'$
$\lambda_a$
$S_0^{r2}{}'$ $S_1^{r2}{}'$ $S_2^{r2}{}'$ $S_3^{r2}{}'$
$S_0^{r2}$ $S_1^{r2}$ $S_2^{r2}$ $S_3^{r2}$
$S_0''$ $S_1''$ $S_2''$ $S_3''$
$S_0'$ $S_1'$ $S_2'$ $S_3'$
$S_0$ $S_1$ $S_2$ $S_3$
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

*Fig. 3. Modeling of IoT based health system*

To assess safety a few techniques are applied [28]:

- failure/attack trees to identify security problems of the IoT infrastructure;

- a few models of healthcare IoT system based on the queueing theory considering dynamics of requests and publishing of vulnerabilities;

- multi-fragmental Markovian chains with fragments described by availability model of devices.

The models describe streams of the requests, hardware and software faults, attacks on vulnerabilities and procedure of recovery by restart and eliminating of one or more vulnerabilities.

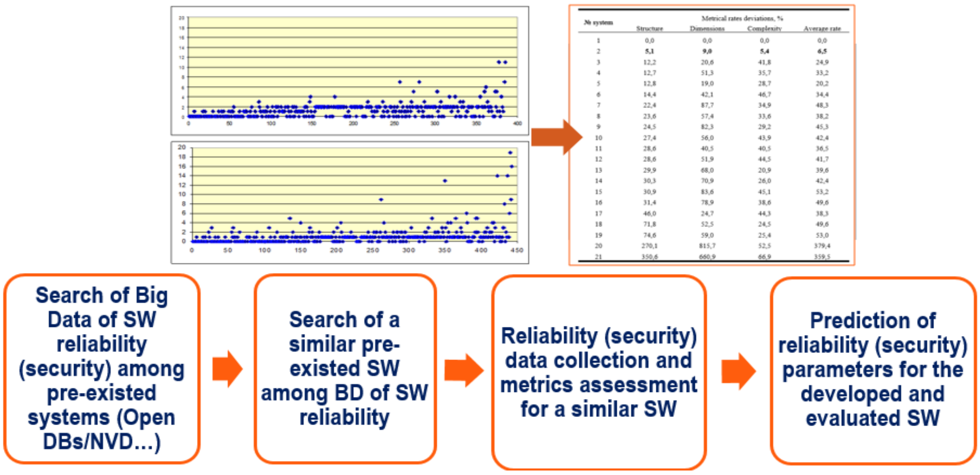
### 5.3. BDA based prediction of software (SW) reliability and security

To assess safety and security of mentioned and other industrial systems it's required to parametrize developed models. Most complex task is parametrization of software reliability and security. Usually information to evaluate software failure rates is not enough in frame of a company that develops and maintains a system [29]. The methodology of software system reliability and security prediction can based on processing information about software with similar attributes and metrics, which is extracted from BD storages and vulnerability databases [30]. The technique to search of similar programs uses [31]:

- metrics of complexity and structure software, metrics of program language similarity. The metrics assess group and average deviation rates describing the software system similarity;

- software agent tool to search, collect and process data.

The stage of SW reliability and security prediction and screenshots are shown on Fig. 4.



| № system | Metrical rates deviations, % | | | |
|---|---|---|---|---|
| | Structure | Dimensions | Complexity | Average rate |
| 1 | 0,0 | 0,0 | 0,0 | 0,0 |
| 2 | **5,1** | **9,0** | **5,4** | **6,5** |
| 3 | 12,2 | 20,6 | 41,8 | 24,9 |
| 4 | 12,7 | 51,3 | 35,7 | 33,2 |
| 5 | 12,8 | 19,0 | 28,7 | 20,2 |
| 6 | 14,4 | 42,1 | 46,7 | 34,4 |
| 7 | 22,4 | 87,7 | 34,9 | 48,3 |
| 8 | 23,6 | 57,4 | 33,6 | 38,2 |
| 9 | 24,5 | 82,3 | 29,2 | 45,3 |
| 10 | 27,4 | 56,0 | 43,9 | 42,4 |
| 11 | 28,6 | 40,5 | 40,5 | 36,5 |
| 12 | 28,6 | 51,9 | 44,5 | 41,7 |
| 13 | 29,9 | 68,0 | 20,9 | 39,6 |
| 14 | 30,3 | 70,9 | 26,0 | 42,4 |
| 15 | 30,9 | 83,6 | 45,1 | 53,2 |
| 16 | 31,4 | 78,9 | 38,6 | 49,6 |
| 17 | 46,0 | 24,7 | 44,3 | 38,3 |
| 18 | 71,8 | 52,5 | 24,5 | 49,6 |
| 19 | 74,6 | 59,0 | 25,4 | 53,0 |
| 20 | 270,1 | 815,7 | 52,5 | 379,4 |
| 21 | 350,6 | 660,9 | 66,9 | 359,5 |

Search of Big Data of SW reliability (security) among pre-existed systems (Open DBs/NVD...)

Search of a similar pre-existed SW among BD of SW reliability

Reliability (security) data collection and metrics assessment for a similar SW

Prediction of reliability (security) parameters for the developed and evaluated SW

*Fig. 4. Principle and stage of BDA for software reliability and security prediction and assessment*

## 6. CONCLUSIONS

### 6.1. Discussion

New technologies create new possibilities for people and society, but bring new deficits of cyber security and safety. This conclusion concerns fully of technologies of Big Data Analysis and Internet of Thing. Concept of cyber safety is important attribute for these and other technologies applied in critical domains.

BDA can be used as a powerful tool for trustworthy assessment of safety and security. Industrial cases illustrate possibilities how IoT and BDA can be used to assure safety and security for critical systems and infrastructures. Besides, big data analysis techniques can tolerate challenges of inaccurate assessment of high availability systems assessment.

BDA makes it possible to improve maintenance and minimize risks of (fatal or prefatal) failures, support decision making and decrease resources/costs for recovery.

Limitations of BDA application are caused by extensive nature of technologies for collecting and processing big data. There are several challenges for BDA application in critical domains.

Some closure of safety critical domains causes restriction of multi-domain application of BDA. There is a problem “BD are not such big as they could be”; for example, diversity application results and CCF statistics are not enough available for each other [32].

Verification of BDA based techniques application. Independent verification and validation is a strong requirement to safety critical systems creation process in nuclear and other domains with high value of failure.

BD based technologies are used for power saved/green applications. However, BDA requires more and more resources. Hence, BDA has to become greener itself. It is required to search of a balance between traditional "small" data based methods and BDA.

### 6.2. Future research

There is common challenge for BDA and IoT: the more data and the more IoT nodes and communications – the less security (confidentiality) and safety of systems. For IoT and IoT systems Von Neumann's paradigm should be specified and implemented as "a secure IoT out of unsecure nodes, communications and clouds".

Hence, important direction of future research is search of balance between "BDA and IoT for system security and safety" and assurance of "security and safety of BDA and IoT based systems" considering features of developed and operated systems, physical and cyber environment.

## REFERENCES

[1] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Transactions on Dependable and Secure Computing, Volume 1, No 1, Pp.1-23, 2004.

[2] M. Yastrebenetsky, V. Kharchenko (editors), Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, IGI Global, USA, 472p, 2016.

[3] Hristo Hristov, Wang Bo, "Safety Critical Computer Systems: Failure Independence and Software Diversity Effects on Reliability of Dual Channel Structures", Information Technologies and Control, Volume 12, No2, Pp.9-18, 2015.

[4] https://pdfs.semanticscholar.org/5acb/243d3a7e679148a211ff8ddc78593c05eb42.pdf , Bernhard Schneidhofer, Stephen Wolthusen, "A case study in Critical Infrastructure Interdependency", 2015.

[5] J. von Neumann, "Lectures on probabilistic logics and the synthesis of reliable organisms from unreliable components", The Institute for Advanced Study Princeton, N. J. at the California Institute of Technology, 1952.

[6] V. Kharchenko, A. Gorbenko, "Evolution of von Neumann's paradigm: Dependable and green computing", Proceedings of the Conference East-West Design & Test Symposium, 2013.

[7] Albert Y. Zomaya, Sherif Sakr (editors), Handbook of Big Data Technologies Springer International Publishing AG, 890 p., 2017.

[8] Wolfgang Karl Härdle, Henry Horng-Shing Lu, Xiaotong Shen (editors), Handbook of Big Data Analytics, Seria Springer Handbooks of Computational Statistics, Springer International Publishing, 538p., 2018.

[9] H.J. Parkinson, G. Bamford, "The Potential for Using Big Data Analytics to Predict Safety Risks by Analysing Rail Accidents", Proceedings of the Third International Conference on Railway Technology: Research, Development and

[10] Maintenance, 2016.

[11] Raghav Toshniwal, Kanishka Ghosh Dastidar, Asoke Nath, "Big Data Security Issues and Challenges", International Journal of Innovative Research in Advanced Engineering, Volume 2, No2, Pp.15-20, 2015.

[12] Geoff Walter, Keith Bowers, New Concept for a Big Data Safety Strategy, Campbell Institute, 24p., 2018.

[13] Zahid Alam, Hiral Patel, “Security and Privacy Issues of Big Data in IoT based Healthcare System using Cloud Computing”, International Journal on Recent and Innovation Trends in Computing and Communication Volume 5, No6, Pp.26-30, 2017.

[14] http://cra.org/ccc/resources/ccc-led-whitepapers/, Fu K., Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., Zorn B., Safety, “Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things”, 2017.

[15] Kishor S. Trivedi, Andrea Bobbio, Reliability and Availability Engineering, Cambridge Book Press, 703p., 2017.

[16] V. Kharchenko, “Diversity for Safety and Security of Embedded and Cyber Physical Systems: Fundamentals Review and Industrial Cases”, Proceedings of 15th Biennial Baltic Electronics Conference, 2016.

[17] V. Kharchenko, “Critical Computing and Big Data: Challenges and Solutions”, Proceedings of 2nd IEEE Conference Data Stream Mining and Processing, 2018.

[18] V. Kharchenko, “Big Data and Internet of Things for Safety Critical Domains: Challenges and Solutions”, Proceedings of the International Conference on Information Technologies, 2018.

[19] Diego Galar, “Data Science in Industry and Transport: The black swan effect and the swan song desire”, Proceedings of 4th Annual Conf. on Computational Science and Computational Intelligence, 2017.

[20] Balar Khalid, Naji Abdelwahab “Big Data and Predictive Analytics: Application in Public Health Field”, International Journal of Computer Science and Information Technology and Security, Volume 6, No5, Pp.1-6, 2016.

[21] https://www.i-scoop.eu/internet-of-things/, Nitsawan Katerattanakul, I-SCOOP, “What is the Internet of Things? Internet of Things definitions”, 2016.

[22] https://www.gartner.com/events/emea/barcelona-symposium#!strategic-predictions/, Gartner, 2018.

[23] V. Kharchenko, A. Sachenko, V, Kochan, H. Fesenko, M Yanovsky, N. Yastrebenetsky, “NPP post-accident monitoring system based on unmanned aircraft vehicle: concept, design principles”, Nuclear and Radiation Safety, No1(73), Pp.24-29, 2017.

[24] V. Kharchenko, A. Sachenko, V, Kochan, H. Fesenko, ”Reliability and survivability models of integrated drone-based systems for post emergency monitoring of NPPs”, Proceedings of the International Conference on Information and Digital Technologies, 2016.

[25] V. Kharchenko, V. Torianyk, “Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment”, Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, 2018.

[26] H. Fesenko. V. Kharchenko, N. Bardis, “An approach to the drone fleet survivability assessment based on a combinatorial model”, Proceedings of the AIP Conference, 2018.

[27] A. Strielkina, D. Uzun, V. Kharchenko, “Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities”, Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, 2018.

[28] A. Strielkina, D. Uzun, V. Kharchenko, “Modelling of healthcare IoT using the queueing theory”, Proceedings of 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2017.

[29] S. Yaremchuk, V. Kharchenko, “Big data and similarity-based software reliability assessment: The technique and applied tools”, Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, 2018.

[30] V. Kharchenko, S. Yaremchuk, “Technology Oriented assessment of software reliability: Big Data based search of similar programs”, Proceedings of the 13th International Conference on ICT in Education, research and industrial applications, 2017.

[31] S. Yaremchuk, V. Kharchenko, A. Gorbenko, "Search of Similar Programs Using Code Metrics and Big Data-Based Assessment of Software Reliability,. In: Alani M., Tawfik H., Saeed M., Anya O. (editors), Applications of Big Data Analytics. Springer, 2018.

[32] V. Kharchenko, A. Siora, V. Sklyar, A. Volkoviy, V. Bezsaliy, "Multi-diversity versus common cause failures: FPGA-based multi-version NPP I&C systems", Proceedings of the 7th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, 2010.

## *Information about the author:*

**Vyacheslav Kharchenko** is Professor, Doctor of Science on Engineering, honored inventor of Ukraine. head of the Department of Computer Systems and Networks, National Aerospace University KhAI, head of the Centre for Safety Infrastructure-Oriented Research and Analysis, RPC Radiy. He is acting as invited speaker and visiting professor of a lot of international conferences and universities (UK, USA, Germany, Poland, Slovakia, Estonia, etc). Author of 40 monographs and textbooks published in USA, UK, Switzerland, Ukraine, 760 inventions and 226 chapters, journal and proceeding papers indexed in Scopus, Web of Science. Founder and GC of international conference DESSERT (Dependable Systems, Services and Technologies, since 2006) and 5 International WSs. National coordinator and team leader of 8 EU funded projects, including projects on dependable computing, nuclear safety, green IT, cyber security and resilient systems, verification and validation, Internet of Things for human and industry domains. Editor and author of multi-volume monography on Green IT Engineering published by Springer in 2017-2019. Supervisor of 45 PhD and Dr.Sc defended thesis. Research interests include dependable and green computing, software reliability and qaulity, cyber safety, big data and IoT for critical domains.

**Manuscript received on 15 October 2018**