Proceedings of the International Conference on
Information Technologies (InfoTech-2018)
20-21 September 2018, Bulgaria

BIG DATA AND INTERNET OF THINGS FOR CRITICAL DOMAINS: CHALLENGES AND SOLUTIONS

PLENARY REPORT SUMMARY

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

Introduction. Information, communication and electronic technologies (IT) are, on the one hand, mean of dependability (reliability, availability, safety, security) assurance for sophisticated systems for critical and commercial domains, and, on the other hand, they are source of threats, vulnerabilities, faults and failures causing new security and safety deficits 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 nuclear power plants (Instrumentation and Control systems of NPPs), piloted aerospace complexes, aviation and railway systems (on-board control and navigation systems, vehicle to vehicle, vehicle to infrastructure and so on), 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]. 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.

Von Neumann's paradigm (VNP) "reliable systems out of unreliable elements" 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. Besides, concept "IT for safety and security" should be added by "safe and secure IT".

Goals. The paper discusses some challenges caused by application of Internet of Things (IoT) technologies and Big Data analysis (BDA) in critical domains such as Nuclear Power Plants (NPPs) and energy grids, health systems and systems for prediction of software dependability. The methodological and practical issues of implementing BDA and IoT systems and tools are analysed in context of cyber security and safety assessment and assurance.

Extending of IoT. Several problems related to IoT and IoT based systems are analysed. First question is: what does IoT mean? There are a lot of definitions. 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…

In our opinion IoT is a paradigm of joining and parametrization of a few technologies (embedded decisions/ sensors and programmable devices, communications and cloud services).

IoT paradigm can be presented in general as

(X)Io(Y)Z ,

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

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

I = Internet (BTW: Web of Things is known as well → WoT)

(Y) is an adjective determining actual attribute of things *(Z)*

X = {Dependable, Safe, Secure,…; Important, Intelligent,…},

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

The following "formulas" are discussed:

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

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

Case studies. Three industrial cases are described and discussed.

Case 1. Internet of drones based post NPP accidence monitoring system. A general structure and underlying principles for creating an Internet of Drone-based multi-version post-severe NPP accident monitoring system is described. The proposed design consists of an IoT subsystem, a single wired subsystem and three drone-based wireless subsystems. Reliability block diagrams (RBD) for the system and its subsystems are built based on considerations of different variants of sensor, communication and decision making systems. On the basis of RBDs, reliability models of the system and their subsystems are analysed. The probability of failure-

free operation that depends upon various system configurations and on the use of multiple redundant Wi-Fi communicating drones is obtained and discussed.

Case 2. Internet of mobile devices based health systems. A healthcare IoT infrastructure with a brief description of each component is presented. These components are a device with a reader, cloud, healthcare provider and a communication channel. Networked healthcare devices sense electrical, thermal, chemical, and other signals from the patient's body. They directly sense and collect biomedical signals, that is, information about the physical and mental state of health. Such devices are safety critical because a human's life depends on its performance. The application of failure / attack trees to identify security problems of the IoT infrastructure is considered. An example of a fault tree for the IoT system is given. This case presents a few models of healthcare IoT system based on the queueing theory and multi-fragmental Markovian chains. The models describe streams of the requests, hardware and software faults, attacks on vulnerabilities and procedure of recovery by restart and eliminating of one and / or two vulnerabilities.

Case 3. BDA based prediction of software (SW) reliability and security. Implementation of the methodology of SW reliability and security prediction is based on processing information about software with similar attributes and metrics, which is extracted from Big Data storages. The technique to search of similar programs is discussed. The similarity principle is based on complexity and structure SWS metrics and metrics of program language similarity. The formulas for metrics calculation of group and average deviation rates describing the SWS similarity. Software Agent for Search of Similar programs and data processing (ASS) is analysed. Case study related to search programs with the same complexity metrics in data storage is described.

Conclusions. For Internet of Things (IoT) systems Von Neumann's paradigm should be specified as "a secure IoT out of unsecure nodes, communications and clouds". BDA can be used as a powerful tool for trustworthy assessment of safety and security. Industrial cases which have been analysed illustrate possibilities how IoT and BDA can be used to assure safety and security for critical systems and infrastructures. Besides, they show how can be tolerated challenges of inaccurate assessment of high availability assessment.