CRITICAL INFRASTRUCTURES SAFETY AND SECURITY: TRENDS IN THE CONTEXT OF INFORMATION TECHNOLOGY DEVELOPMENT

Societies are becoming more dependent on information technologies (IT), IT-based systems and services. A number of trends represent this dependency. One of the most important relates to problems of safety and security. On the one hand, information technologies provide efficient means of assuring and improving safety of different applications. On the other, these technologies create new deficits in safety and can increase risks of failures, emergencies and crashes. That concerns, first of all, the so-called safety critical, mission critical and business critical systems and infrastructures (or "systems of systems"). Security of IT-systems and infrastructures (cyber security) may be considered as an important attribute of their functional safety. Safety and security of IT-systems and infrastructures have a major impact on the safety and security of critical infrastructures in general.

IT-infrastructures are inherent in critical systems and infrastructures. Nuclear power plants (NPPs) and energy grids, aerospace complexes, national health systems, transport communications, defence systems, and their IT-systems are extremely complex and important objects of research and analysis due to the potentially catastrophic aftermaths of non-tolerable failures and emergencies. Large-scale accidents of NPPs (Three Mile Island, USA, 1979; Chernobyl, USSR, Ukraine, 1986; Fukushima, Japan, 2011), numerous crashes of aerospace systems and airplanes and others accidents provide clear examples.

There is interesting statistics regarding causes of accidents for NPPs and aerospace systems. About 20 percent of accidents and failures in these domains during recent years were caused by failures of computer systems and their components. As critical systems often operate in aggressive and uncertain physical and information environment, engineers and researchers should take into account all possible and 'impossible' influences and intrusions to decrease the risks of failures and emergencies and to guarantee the required level of safety and security. The importance of minimizing risks for different critical systems and infrastructures led to the introduction of new terms and a whole new subject area called *safeware* (term, introduced by Prof. Nancy

Leveson, leading NASA safety expert). The concept of safeware means that the integration of the tasks of analysis and safety assurance as a single complex entity, taking into consideration the hardware, software and human-based components of the target objects. This special engineering venue is described by the term *safeware engineering* (or safety IT-engineering) and may be the answer to challenges in providing safety and security of critical infrastructures.

The CrISS Workshop

The safety IT-engineering was the main theme of the Workshop on Critical Infrastructure Safety and Security (CrISS-DESSERT) that took place in Kirovograd, Ukraine, 11-13 May 2011 (http://www.stc-dessert.com/conf2011/). It was organised by the National Aerospace University "KhAI", Research and Production Corporation RADIY, Taras Shevchenko National University, National Academy of Sciences of Ukraine, Centre for Infrastructure-Oriented Research and Analysis, Poltava National Technical University (Ukraine), the IEEE Ukraine Section and the Centre for Security and Defence Management (Bulgaria).The CrISS-DESSERT'2011 Workshop evolved from the series of international conferences under the title "DEpendable Systems, SERvices & Technologies" (DESSERT).[1]

Among the themes of the series of DESSERT conferences are analysis, modelling, development, testing, verification and validation (V&V), expertise and maintenance of HW&SW components, computer and telecommunication systems and networks, web-services and IT-infrastructures for critical (computer systems for NPPs, aviation, airspace, medicine, transport, power and other systems), business-critical (banking systems, telecommunication networks, e-commerce, e-science, etc.) and commercial applications with rigorous requirements to dependability (reliability, safety, integrity, confidentiality, survivability, maintainability) and resilience.

The CrISS-DESSERT'2011 Workshop examined policies, regulation, assessment, development, integration, V&V, testing and operation of complex computer and communications systems and infrastructures for safety-, mission-, and business-critical applications. This was the first workshop in Eastern Europe dedicated to specific issues in complex problems of safety and security of infrastructures and their components. It approached holistically the issue of infrastructure safety and security. This theme for the Workshop was chosen in order to address:

- Integration, interaction and interdependencies of sets of systems and the ensuing challenges in providing infrastructure safety;

[1] For a detailed account see the series website at www.stc-dessert.com/conf.

- Roles of IT- or computer-based systems—inherent part of each system and the linkage between infrastructures—thus turning distinct infrastructures in a complex system of critical importance; IT systems are used to ensure safety and, on the other hand, introduce vulnerabilities;
- Interdisciplinary research in studying failures in critical systems that are caused, as a rule, by a number of reasons.

The workshop addressed the following specific topics:

- Policies for providing safety and security of critical infrastructures (CrISS);
- Foundations and technologies for safety engineering and management;
- Energy grid safety and security;
- Aviation and space safety and survivability;
- Mathematical methods and techniques for macro-diagnostics and diagnostics of IT-systems and components of critical infrastructures;
- Resilience and intrusion-tolerance of web- and Cloud computing-based business-critical IT-infrastructures;
- Evolving infrastructures and safety management. Self*-systems and infrastructures;
- Formal methods in IT-infrastructure and software development and verification;
- Functional safety of I&C systems for critical infrastructures and Safety Case-oriented techniques;
- Infrastructure aspects for complex electronic component-based systems safety;
- Global aspects of safety and security engineering: education, training, and regulation.

Sixty papers were accepted for presentation at the WS and publication in proceedings. Papers were submitted from eleven countries: Bulgaria, Canada, the Czech Republic, Greece, Iraq, Kingdom of Saudi Arabia, Russia, Syria, Ukraine, United Kingdom, and the United States. The programme included four plenary sessions (ten plenary papers), two general sessions “Safety Engineering and Cyber Security of Safety-Critical Infrastructures” and “Security and Safety of I&C Systems: Paradigms, Requirements, Certification,” and six parallel sessions addressing respectively Infrastructure Safety Analysis: Case-Oriented Techniques and Tools; Critical Software and Systems Development and Verification: Formal Methods-Based Techniques; Computer Systems and Networks Safety and Dependability: Analytical Models and Methods; Safety and Resilience of Critical IT-Infrastructure and I&C Systems: Poli-

cies and Models; Security of Computer Systems, Communications and Mobile Applications: Methods and Tools; and Diagnostics of Critical Systems and Components: Models and Methods.

The three days of the workshop hosted and sponsored by RPC Radiy were full of exciting presentations, fruitful meetings and discussions, opportunities to network with colleagues representing different and complex domains. CrISS-DESSERT'2011 provided opportunities to share experience from the implementation of proposed approaches, methods and tools, research and practical results in support of CrISS and IT-infrastructure programs, new concepts, decision making systems and techniques for safety and security regulation, assessment, management and assurance at different stages of the systems' life cycle.

This volume

The Program Committee of CrISS-DESSERT'2011 and the I&S Editorial Board invited 25 papers for publication in this special issue of *Information & Security*.[2] The papers of this volume are divided in two issues including six themes.

The first theme "Critical Infrastructure Protection Policy and Technologies" is covered by four papers submitted by researchers from Bulgaria, the Czech Republic and Ukraine. The authors look into methods of analytical support to CrISS protection policy and investment decision-making; principles of mitigating and managing the human system risks; critical infrastructures safety management based on technical megastate (a set of states of the systems included in infrastructure); and the state corporate cloud computing-based network for registration of potentially dangerous objects.

The second theme "Critical Infrastructure Interdependencies Analysis" presents novel developments from Ukraine. The challenges under examination in the two papers are how to formalize the power grid influence for nuclear power plant safety assessment and to apply probabilistic approach for establishing an air pollution monitoring network for industrial regions.

The third theme "Critical IT-Infrastructure and Communication Security" features seven papers represented by authors from Greece and Ukraine. Three papers present analytical and technological decisions for support of securing different communication domains: private telephony infrastructure, mesh networking and mobile applications. Two papers cover problems of profiling and assessing assurance requirements to security of IT-infrastructures and nuclear facilities. Methods and techniques for in-

[2] Twenty four papers were submitted according to this journal's requirements.

trusion detection and tolerance using Safety-case tool and diversity approach are proposed by the authors of the last two papers in the section.

The second issue of the volume also covers three themes. The first theme "Critical Infrastructure Safety Risk Analysis and Management" includes three papers from Czech and Ukrainian researchers. The first one systemizes fine exact methods of safety engineering which can be applied in different critical domains. The second paper presents study results and risk assessment of orbital carrier rocket and spacecraft failures and emergencies during last ten years. The final paper in this section describes a methodology and techniques for common cause failures' risk assessment in critical infrastructures.

The second theme "Critical IT-Infrastructure Safety and Dependability" features five papers presented by specialists from Canada, Russia, Ukraine and USA that provide analytical foundation and examples showing how to assess, simulate and assure safety, availability and reliability of IT-infrastructures. The particular focus is on cloud-based infrastructure, aerospace computer-based infrastructure consisting of ground and on-board systems, NPP I&C systems, banking systems. For that authors apply formal methods such as Markov chains.

The final theme "Functional Safety of Critical IT-Infrastructures and Systems" is covered by three papers addressing the methodology of FMECA-based techniques and tools for critical systems safety analysis (FMECA is a technique of failure modes, effects and criticality analysis); the model and implementation of assessment cores for Safety Case methodology and technique; methods of functional safety assurance on different life cycle stages (and a case study for aircraft on-board I&C systems).

The Monitor section introduces the on-going TEMPUS-SAFEGUARD project aiming to facilitate academia-industry interaction in Safety IT-Engineering through a network of innovative centres.

A trend in highlight

John von Neumann formulated the paradigm of "reliable system out of unreliable elements" in the 1950s. The systems in that case were relay contact circuits or primitive digital devices. The basic mechanism of ensuring system reliability relied on standby or voted redundancy (passive fault-tolerance). Later on, in 1960s and 70s, this concept included support of active fault-tolerance. The new paradigm was formulated as "reliable (and fault-tolerant) system out of unreliable components (with a diagnosis and reconfiguration in case of faults)". Systems were complex digital devices, mainframes, computers and computer systems. The components of such systems were chips of small, medium and large integration.

The 1980s and 90s brought the paradigm of “reliable (and fault-tolerant) systems out of unreliable hardware and software components” that reflected the fact that software became a main growth factor of system unreliability. During that period multi-version engineering was developed to provide tolerance to those failures caused by design faults. In the mid 80s a new paradigm was found as “reliable and secure systems out of unreliable and insecure components.” The evolution of the Internet and the development of service-oriented IT systems in the following years led to transforming this paradigm into “dependable systems out of undependable components.” Finally, with regard to emerging technologies of SOA, SaaS and web-services and recent studies of SOA and Internet uncertainty we can speak about “composing dependable service-oriented systems out of web-services with uncertain (not known for sure) dependability”.

In regard to assuring safety and security of critical infrastructures, a new paradigm may be formulated as “safe (and secure) infrastructure out of unsafe and insecure (or insufficiently safe and secure) systems.” Its practical implementation will require development of new methods and technologies, in particular, self-healing and self-evolving systems and CrISS. The main current interests are on self-evolving systems or dynamically evolving systems and CrISS, which are capable of taking into account changes of requirements and environmental characteristics and use internal or external resources to compensate for such changes in real time.

Acknowledgment

On behalf of the participants in the CrISS workshop and authors of this volume I would like to thank Todor Tagarev for his cooperation and support to the workshop organisation, as well as Oleg Illiashenko from the Department of Computer Systems and Networks at the National Aerospace University “KhAI” for collecting the papers for this edition.

Vyacheslav Kharchenko