Resilience Management of Critical Cyber-Physical Systems: A Multiple Case Study Analysis

JYRI RAJAMÄKI
Research, Development and Innovations
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND

Abstract: - Modern societies are highly dependent on different critical cyber-physical systems (CPS). The growth of software (= cyber) layer, in size and percentage of the overall system is a future trend. Our society's critical CPS — cyber, energy, water, transportation and communication — lacks of resilience, typically losing essential functionality following adverse events. This multiple case study research analyses five prior research projects from the safety and security field. The target of the paper is to research how resilience management of critical cyber-physical systems can be understood.

Key-words: - Case study; Critical infrastructure; Cyber security; Cyber-physical systems; Information security; Multiple case study analysis; Resilience

1 Introduction

The research field of smart cities, critical infrastructures and other cyber-physical systems (CPS) is a multidisciplinary topic. Existing empirical research is characterized by a considerable degree of fragmentation among different research programs and different geographic regions in Europe. The concept of resilient smart cities offers tremendous potential for innovation and development of new technologies and services. At the same time, the increasing "smartness" of urban environments introduce both threats and opportunities related to societal security, safety and resilience. Thus, we regard the concept to be of high societal importance. The research field of resilient smart cities is still in its infancy. The topic requires the development of new concepts, approaches and establishing multidisciplinary collaboration between research groups and stakeholders that rarely collaborate with each other. This underlines the need for a multidisciplinary network to pave the way for future research efforts on resilient CPS.

The present article is a multiple case study research (MCSR) aimed at the research question formulated in the title: How can resilience management of cyber-physical systems be understood?

2 Research approach

Figure 1 shows how MCSR is applied in this research. The initial step in designing MCSR consists of theory development, and the next steps are case selection and definition of specific measures in the design and data collection process. Each individual case study consists of a whole study, and then conclusions of each case are considered to be the replication by other individual cases. Both the individual case and the multiple-result should be the focus of a summary report. For each individual case, the report should indicate how and why a particular result is demonstrated. Across cases, the report should present the extent of replication logic, including certain and contrasting results [1].

In Figure 1, the dashed-line feedback represents a discovery situation, where one of the cases does not suit the original multiple-case study design. Such a discovery implies a need to reconsider the original theoretical propositions. At this point, redesign should take place before proceeding further, and in this view the replication approach represents a way of generalizing that uses a type of test called falsification or refutation, which is the possibility that a theory or hypothesis may be proven wrong or falsified [2].

3 Theoretical Framework

3.1 Resilience management

According to Linkov et al. [3], resilience, as a property of a system, must transition from just a buzzword to an operational paradigm for system management. Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how CPS are conceptualized, built and evaluated [4]. Currently, a development of a design theory (DT) for resilient CPS is on a way so that communities developing and operating different information and security technologies can share knowledge and best practices using a common frame of reference [5].

The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient [6]: 1) Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack). 2) Absorb: Maintain most critical asset function and service availability while repelling or isolating the disruption. 3) Recover: Restore all asset function and service availability to their pre-event functionality. 4) Adapt: Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient. The Network-Centric Warfare (NCW) doctrine identifies four domains that create shared situational awareness and inform decentralized decision-making [7]: 1) Physical: Physical resources and the capabilities and the design of those resources. 2) Information: Information and information development about the physical domain. 3) Cognitive: Use of the information and physical domains to make decisions. 4) Social: Organization structure and communication for making cognitive decisions. Linkov et al. [8] combined the event management cycles and NCW domains to create resilience metrics for cyber systems. Their approach integrates multiple domains of resilience and system response to threats through integrated resilience metrics; however, study of systems as multi-domain networks is relatively uncommon. Links across domains are likely to affect the network's resilience and should be assessed using network science tools [9].

3.2 Smart cities

Smart Cities is becoming more and more complex, not least with regard to security aspects following a decade of continuous threats to our existing and planned large scale urban built infrastructure. Such infrastructure are critical nodes within the

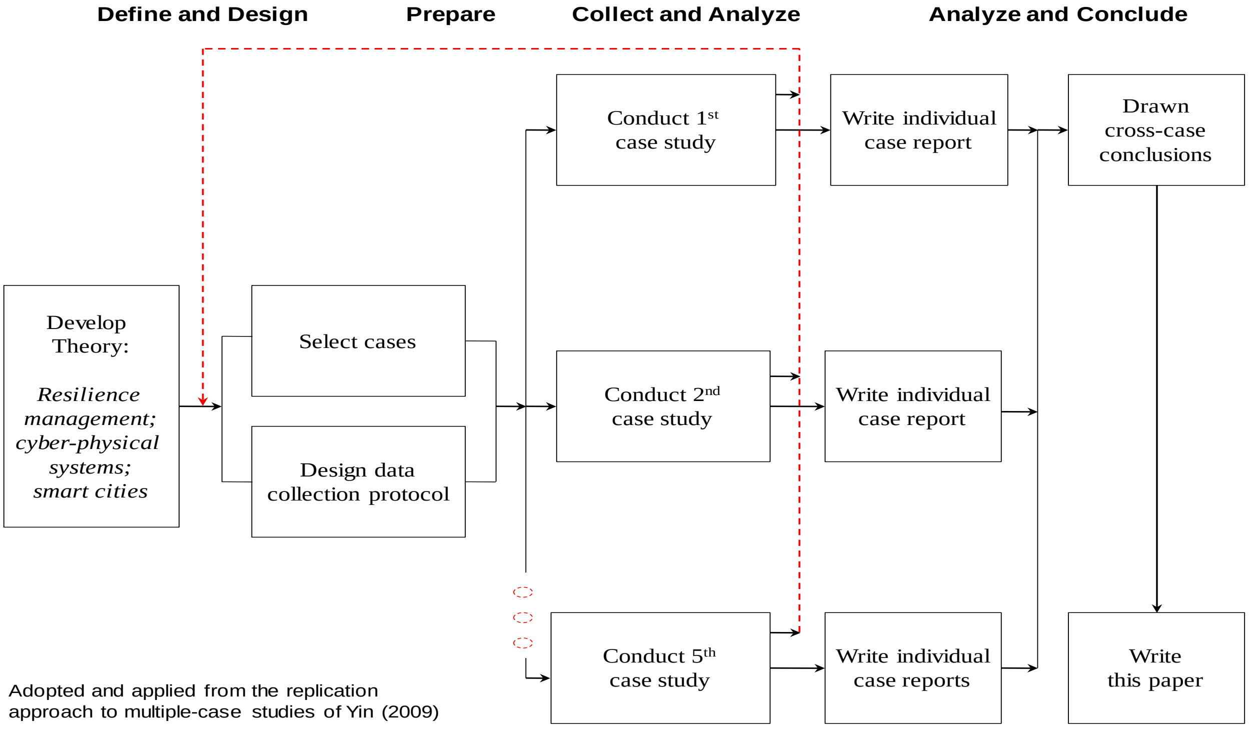
Define and Design
Prepare
Collect and Analyze
Analyze and Conclude
Develop Theory:
Resilience management; cyber-physical systems; smart cities
Select cases
Design data collection protocol
Conduct 1st case study
Conduct 2nd case study
Conduct 5th case study
Write individual case report
Write individual case report
Write individual case reports
Drawn cross-case conclusions
Write this paper
Adopted and applied from the replication approach to multiple-case studies of Yin (2009)

Fig.1 Multiple-case study method of this research

intertwined networks of these urban areas, which include not only physical components, but also integrated hardware and software aspects. To date, a comprehensive and holistic (systematic) approach to improve the resilience and security of large scale urban developments against attacks and disruptions has not been developed thoroughly.

The understating of modern cyber-physical systems' behavior and their dynamics, and the insight into capabilities and risks associated with smart systems integration into modern society can provide an important contribution to European security and safety in the near future.

The system approach provides a number of new opportunities and opens new challenges. It provides a structured interface between social systems and technology research. It allows for the exchange of data and information between humanistic, social, behavioral research, risk management, resilience, and ICT-related research activities and projects. It will facilitate the application of analytical and modelling methods to the complex socio-techno-economic processes related to safety, security, resilience and survivability. The system and system of systems approaches have the potential to provide an interface with experimental research that could benefit from existing European Living labs and test beds. However Smart City research today has been lacking this systems concept and systematic approach, and the connection between basic research and the Living Labs experimental research platforms has not yet been well developed yet.

The humanistic security research related to cultural, societal and behavioral aspects of risk management has until now been carried out mostly in isolation from system and technological research. The potential of the techno-societal system of systems concept as an integrator for societal, technological and economic dimensions of resilience and smart cities research has not yet been exploited at its full capacity.

The development and integration of artificial intelligence based smart ICT systems into city management and the daily life of the urban population has the potential to considerably improve the security of citizens and society generally. It presents huge potential for innovation. At the same time smart ICT systems present serious challenges and risks for society and citizens if applied inappropriately. A better understanding of complex techno-social urban systems will provide an insight into the underlying systemic processes involved. This will improve our ability to model and reduce these risks. Smart Cities research can benefit from the latest developments in Internet of Things (IoT), Big Data, Cloud Computing, Cloud Services, Social Media and Social Networks. Interoperability at all levels presents a serious challenge today. Standardization activities for Smart Cities have not yet been started by the leading standardization bodies in Europe - ETSI and CENELEC.

4 Empirical Cases

This section briefly describes the five empirical cases that belong to this multiple case study analysis. The individual case report were published earlier, but this section summarizes their main research results with regard to this MCSR.

4.1 Case I: The RIESCA Project

The RIESCA – Rescuing of Intelligence and Electronic Security Core Applications – project was a Finnish national research project with 13 partners that lasted 42 months (01/10/2007 – 31/03/2010). It developed information security management techniques that can be used to ensure the proper functioning of critical systems in all circumstances. Particular attention was paid to the situation of moving from normality to a crisis situation and recovering from the crisis to a normal state. The other aim was to develop different security management and communication systems for critical events, including mass events, high-level political meetings and crisis situations and to assess methods for evaluating their functionality.

The RIESCA project developed a) usability analysis of critical functionalities, b) improvement of a process dealing with critical activities, c) a reliability framework, d) an audit framework, e) Corporate Governance survey, and f) implemented a survey tool all of which can be used to ensure the proper functioning of critical systems under all circumstances.

The research partners of the project were the University of Oulu, University of Eastern Finland, and Laurea University of Applied Sciences. The main funder was Tekes – the Finnish Funding Agency for Innovation. Other participating organizations were dealing with critical infrastructure, either directly or indirectly. Organizational distribution was balanced act, three of them were on public sector, three of them represented small and medium sized organizations

(SME), and three of them fall into industrial category. The international research partners were Georgia State University/J. Mack College of Business/Department of Computer Information Systems; USA; University of Arizona, USA; and The Central Information Technology Services Department (ZID) of the University of Innsbruck, Austria.

During the project, researchers and university students, as research colleagues in co-operation with other RIESCA project researchers, analysed existing standards and methods, and evaluated their applicability for the evaluation and development of critical systems and events. One target of the project was to create a process that could evaluate and develop security management for critical infrastructures. This was done by making as much use of existing methods and standards as possible. The pilot projects concerning these methods were mostly carried out with organizations that took part in the project. The whole process was supplemented by solutions that were developed during the project.

RIESCA had societal impacts; it implicated national and international discussions in the field of critical infrastructure protection. RIESCA aligned with the key concepts regarding the 1st EU-US Expert Meeting on Critical Infrastructure Protection (CIP). Furthermore, RIESCA partially contributed on the improvement of the national authorities' communities' network (TUVE). RIESCA aided in creation of public-private-partnerships (PPP) between the participators and external partners. RIESCA increased networking with international actors, regarding the Infragard system, which was presented to Finnish actors. RIESCA raised discussions on privacy of citizens, as there was lot of discussions about privacy versus traceability of person. RIESCA raised awareness of the weaknesses of different networks with regard to dependability of networks. Furthermore, participators of RIESCA actively collaborated to different security related standards and frameworks, such as the national "Vahti" group work and ISO/IEC standards.

With regard to this paper, RIESCA's main lesson to be learnt is that all critical infrastructures are software-intensive socio-technical systems, as shown in figure 2. There has been a gigantic shift from a hardware product based economy to one based on software and services [4]. This has also been the fact with regard to critical infrastructures. From every indication, the growth of the software layer, in size and percentage of the overall systems, will be the future trend.

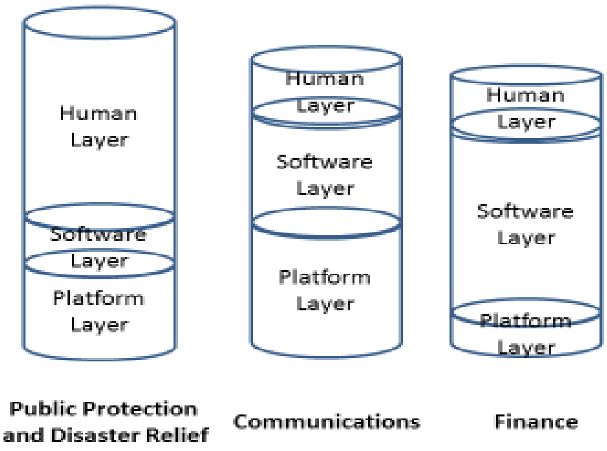

Fig.2 Critical infrastructures as software-intensive socio-technical systems

4.2 Case II: The MACICO Project

The MACICO – Multi-Agency Cooperation In Cross-border Operations – project (01/12/2012 – 31/12/2014) addresses the interactions and research and development of security organizations and cross-border processes. The shared MACICO processes operates usually in dedicated networks and using of own systems and services, but which in some critical missions could directly and indirectly benefit by respective sharing of external activities, distribution of mission critical information, and sharing of information systems or information intensive infrastructure. In a short-term scenario, MACICO project was addressed to the needs for improved systems, tools and equipment for radio communication in cross-border operations and during operations which were taking place on the territory of other member states as critical over border situations. In a long-term perspective, MACICO encompassed the interoperability issues of European countries and for formulation of transition from currently deployed legacy networks into the future broad band networks.

With regard to this paper, MACICO's main lesson to be learnt is that interoperability should be built on all levels (users, service providers, services, technologies), as shown in figure 3. Trust is the main issues within cross-organizational cooperation.

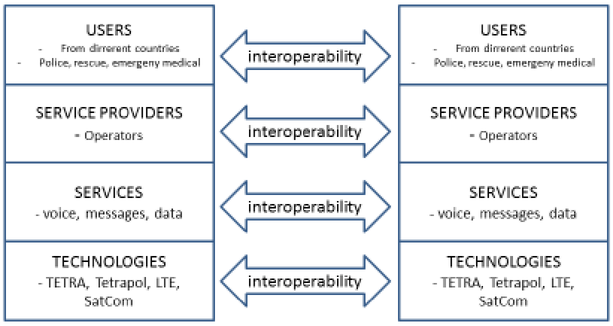

Fig.3 Layers of interoperability

4.3 Case III: The AIRBEAM Project

The AIRBEAM (http://airbeam.eu/) - AIRBorne information for Emergency situation Awareness and Monitoring - (March, 2011 to February, 2015) is a Seventh Framework Programme (FP7) project related to crisis management. The goal is to develop a multi-platform approach to situational awareness for crisis management, especially utilizing Unmanned Aerial Vehicles (UAVs), aerostatic platforms and satellites. In addition to Airbus, the AIRBEAM Consortium includes 22 partners, including some of the largest high-tech companies in Europe. The role of Laurea is as the coordinator of Work Package 1 of AIRBEAM, which focuses on studying potential concepts of use and specifying end-user requirements. This work is in close collaboration with end-user organizations.

Situational Awareness is the main prerequisite towards cyber security. Without situational awareness, it is impossible to systematically prevent, identify, and protect the system from the cyber incidents and if, for example, a cyber-attack happens, to recover from the attack. Situational awareness involves being aware of what is happening around your system to understand how information, events, and how your own actions affect the goals and objectives, both now and in the near future. It also enables to select effective and efficient countermeasures, and thus, to protect the system from varying threats and attacks.

Figure 4 illustrates that a situational awareness (SA) system itself is a cyber-physical system, cyber SA being a subset of it. Situational awareness is a prerequisite for a cyber-physical system to be resilient.

4.4 Case IV: The HARMONISE Project

The general aim of HARMONISE - A Holistic Approach to Resilience and Systematic Actions to Make Large Scale Built Infrastructure Secure - is to develop a comprehensive, multi-faceted, yet mutually reinforcing concept for the enhanced security, resilience and sustainability of urban infrastructure and development. HARMONISE will result in resilience enhancement methods for large scale urban built infrastructure. It will see the development of a concept to improve the security and resilience of this infrastructure, encompassing the design and planning phases of such projects (and thereby leading to robust built infrastructure invulnerable to natural/man-made disasters). HARMONISE will improve the design and planning of urban areas, thereby increasing their security and resilience to new threats.

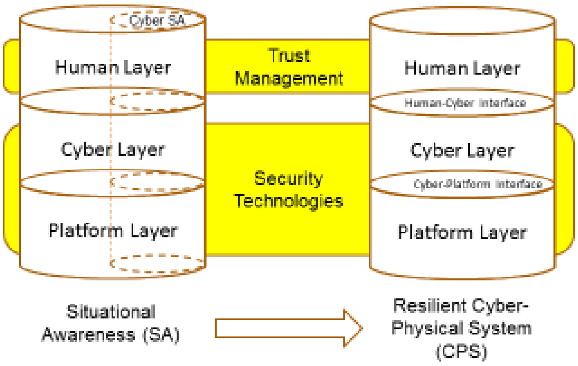

Fig.4 Situational awareness as a prerequisite for resilience

Specifically HARMONISE seeks to deliver: a) A holistic and interactive online HARMONISE Platform; b) A suite of innovative tools (toolkit hosted within the HARMONISE platform) for decision support; c) Greater understanding and awareness of urban security and resilience vis-a-vis dissemination activities; and, d) Commercialization and employment opportunities among emerging new markets in this field. The HARMONISE concept will be applied across a number of European cities through the use of case studies for validation and refinement.

Recent international work in urban resilience has charted a number of commonalities in how different jurisdictions adopt, and then enhance, their resilience over time in a series of ‘waves’. These accounts highlight how resilience has, over time, become more local, proactive and embedded within the everyday practices of built environment professionals, as shown in figure 5.

4.5 Case V: The INACHUS Project

The INACHUS FP7 project aims to achieve a significant time reduction related to Urban Search

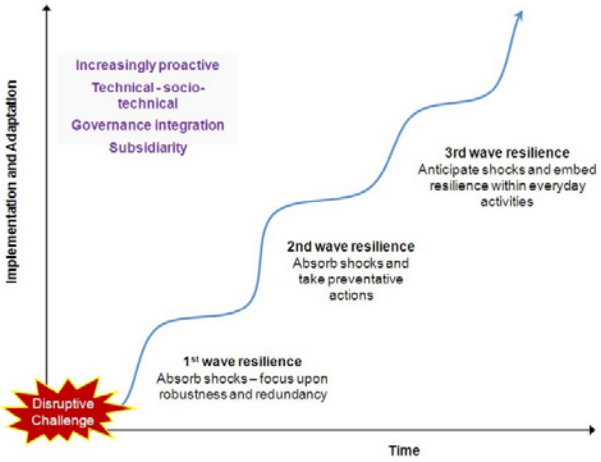
Implementation and Adaptation
Increasingly proactive
Technical - socio-technical
Governance integration
Subsidiarity
3rd wave resilience
Anticipate shocks and embed resilience within everyday activities
2nd wave resilience
Absorb shocks and take preventative actions
1st wave resilience
Absorb shocks – focus upon robustness and redundancy
Disruptive Challenge
Time

Fig. 5 An evolving resilience process

and Rescue (USaR) phase by providing wide-area situation awareness solutions for improved detection and localisation of the trapped victims assisted by simulation tools for predicting structural failures and a holistic decision support mechanism incorporating operational procedures and resources of relevant actors. The INACHUS objectives are:

1. Development of simulation tools for estimating the number and locations of survival spaces created after a structural collapse.

2. Development of Decision and Planning Components for Advanced Casualty and Damage Estimation performing structural damage analysis based on input coming from: i) 3-D airborne and ground-based laser-scanning, ii) images and iii) Structural Health Monitoring sensors.

3. Integration of existing and novel sensors as well as advanced “electronic nose” based on off-the-shelf sensors for accurate localization and detection of alive trapped humans.

4. INACHUS will advance the state of the art by developing a robust snake robot mechanism.

5. Interconnection between the developed devices providing an integrated architecture on a network-centric scheme to interconnect all needed sensors and actors via advanced and secure communication links, able to decrease time of reaction and drastically increase the efficiency of the relevant actors.

6. Enhanced data fusion and analysis techniques to improve USaR operations with respect to response time and situational awareness.

7. System Integration of all the above software and hardware subcomponents (INACHUS platform).

8. Contribution to standards/best practices and guidelines for the USaR operations through strong user presence.

9. Consideration of Societal Impact, Legal and Ethical issues of the proposed solution feeding the technical solutions and guidelines of its use.

10. Several field tests will be arranged targeting a variety of post-disaster situations aiming at demonstrating the capabilities of the developed INACHUS platform.

11. Development of training package and extensive training courses will be carried out for the first responders.

With regard to this paper, INACHUS’ main lesson to be learnt is that all critical cyber-physical systems have interdependences, but their internal event management cycles could be in different phase, as shown in figure 6. This should be considered when shaping overall situational awareness.

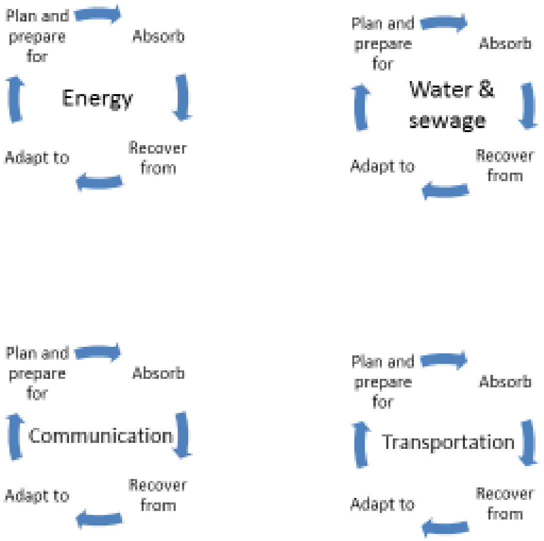

Fig. 6 Event management cycles of critical infrastructes

5 Cross-case Conclusions

Developing resilience management of critical cyber-physical systems requires a deep understanding of their characteristics and the interdependencies it engenders at all levels (from macro to micro). Building on clearly-defined terms to allow coherent interdisciplinary work, the challenge is then to understand the consequences of techno-social interactions. Maintaining the advantages of the smart city environment without compromising security, resilience, safety and privacy represents a challenge requiring broad input and deep understanding, especially in the areas of analysis and modelling. The challenge in these areas is to bring together cross-disciplinary teams for developing new and combining existing techniques, in order to provide a coherent framework to support implementation

There has been a gap between basic research on security and technology and the applied experimentally-driven research and open and social innovation carried out by Living Labs across Europe. The potential of Living Lab as a validation, information collection and cooperation platform in security and systems research has not been fully exploited. At the same time the extensive network of Urban Living Labs in Europe offers big potential for developments and cooperation on these topics.

Smart city concept is an example of a cyber-physical system. There has been a lack of knowledge and awareness among city management and regional authorities about system concepts, tools and new opportunities provided by advanced ICT. It is therefore important to stimulate dialog with them and encourage their participation in the network of scientific communities. Involvement of citizens in research through participation in Living Lab activities will help the authorities introduce services that will better serve their communities in multiple societal security domains.

The future aim should be to build a multidisciplinary community of researchers, authorities, industry and Living Labs to develop a scientific foundation and platform for partnership in system research and a federated Living Lab environment for Secure Smart Cities. It will create a network of research experts and groups to consolidate the multidisciplinary expertise necessary to tackle this complex area of high societal importance.

References

[1] R. K. Yin, *Case Study Research Design and Methods*, Thousand Oaks: Sage Publications, 2009.

[2] K. Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge*, London: Routledge Classics, 2009.

[3] I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs and T. Thiel-Clemen, “Changing the resilience paradigm,” *Nature Climat Change*, vol. 4, pp. 407-409, 2014.

[4] A. Hevner and S. Chatterjee, *Design Science Research in Information Systems*, Springer, 2010.

[5] J. Rajamäki and R. Pirinen, “Critical infrastructure protection: Towards a design theory for resilient software-intensive systems” *European Intelligence and Security Informatics Conference (EISIC)*, 2015.

[6] *Disaster resilience: a national imperative*, National Academy of Sciences, 2012.

[7] D. Alberts, Information age transformation, getting to a 21st century military. DOD Command and Control Research Program, 2002.

[8] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen and J. Kott, “Resilience metrics for cyber systems,” *Environ Syst Decis*, 2013.

[9] T. Abdelzaher and A. Kott, *Resiliency and Robustness of Complex Systems and Networks. Adaptive, Dynamic and Resilient Systems*, Florida: Auerbach Publications, 2013.