Resilient Sociotechnical, Cyber-Physical, Software-Intensive Systems of Systems

JYRI RAJAMÄKI
Research, Development and Innovations
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
Jyri.Rajamaki@laurea.fi http://www.laurea.fi

Abstract: - Our society's critical infrastructures (CI) — energy, water, transportation, communication, critical information infrastructure — lacks of resilience, typically losing essential functionality following adverse events. In the future, the number of climatic extremes may intensify or become more frequent, and building resilience becomes the optimal course of action for large complex systems. CI are cyber-physical systems (CPS) increasingly using open networks for operation. The vulnerabilities of the software deployed in the new control system infrastructure will expose the control system to many potential risks and threats from attackers. CPS have become a major area for research and development. However, all CPS are also sociotechnical systems (STS), and for successful integration with society, the sociotechnical dimension of CPS should be addressed. The target of this paper is to research how resilience management of critical systems can be understood. The study indicates that situational awareness, continuous learning and the sociotechnical dimension of CPS are prerequisites for any CI to become resilient.

Keywords: Cyber security, Critical infrastructure, Critical infrastructure protection, Resilience, Sociotechnical system, Cyber-Physical system, Software-Intensive System, System of systems

1 Introduction

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructures, such as communication, energy, water, transportation, finance and healthcare systems, lack the same degree of resilience, typically losing essential functionality following adverse events [1].

Figure 1 presents our society's critical infrastructures and functions vital to society [2]. Critical infrastructures are key state assets that will provide the functions vital to society. Safety deals with the risks arising from the system and potentially impacting the environment, whereas security is concerned with the risks originating from the environment and potentially impacting the system [3]. Security analysis provides what should be protected and which threaten the assets. The risk of execution of threats is determined in the security analysis; risk is the probability that the threat has become. According to Czech safety analysis, fundamental threats to critical infrastructure are: 1) natural disasters, 2) technological accidents, 3) cyber-attacks, 4) criminal activities, and 5) terrorist attacks [4].

Critical infrastructures and functions vital to society all are cyber-physical systems (CPS) which are increasingly using open networks for operation. However, all CPS are also sociotechnical systems (STS), and for successful integration with society, the

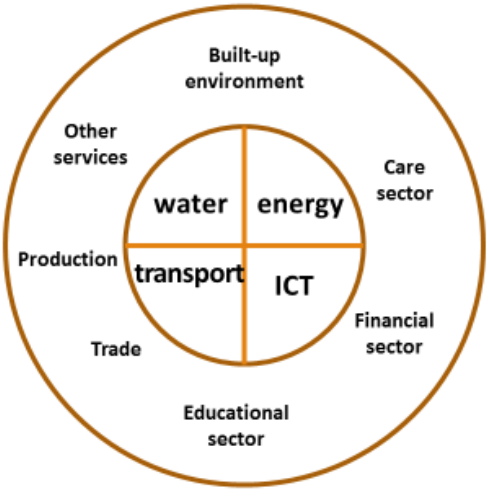

Fig. 1 Critical infrastructures and functions vital to society [2]

sociotechnical dimension of CPS should be addressed.

The structure of the remainder of the paper: Section 2 gives a literature review with regard to sociotechnical cyber-physical systems (CPS) and their cyber security issues. Section 3 presents the "methodology" of this paper; design theory development. Section 4 describes the proposed elements of the design theory for resilient systems. Section 5 discusses about the usefulness of the solution and concludes the paper.

2 Sociotechnical Cyber-Physical Systems

The Networking and Information Technology Research and Development (NITRD) Program is the U.S.' primary source of federally funded work on advanced information technologies (IT) in computing, networking, and software. Their definition for Cyber-Physical Systems is:

> *"Cyber Physical Systems (CPS) are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications. In CPS systems, the joint behavior of the "cyber" and "physical" elements of the system is critical - computing, control, sensing and networking can be deeply integrated into every component, and the actions of components and systems must be safe and interoperable."*

Figure 2 shows the evolution of CPS. Figure 3 presents the domain of sociotechnical cyber-physical systems. Past sociotechnical systems were physical systems, including only the human layer and the platform layer, as shown in figure 4a. Current sociotechnical systems are software-intensive systems (SIS) [6] as shown in figure 4b. SIS' future

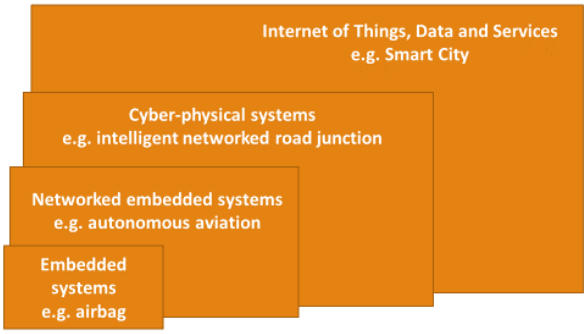

Fig. 2 Evolution of cyber-physical systems [5]

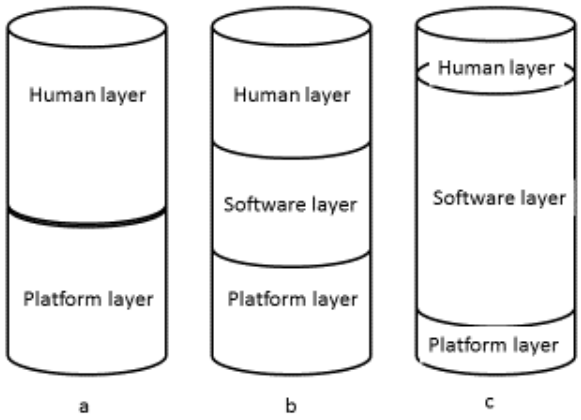

Fig. 4 Software-intensive system trends [6]

trend is that the software layer (=cyber part) is growing, as illustrated in figure 4c. All SIS are also cyber-physical systems (CPS) where the human and platform layers form the physical part and the software layer forms the cyber part of the cyber-physical system [7].

When individual CPS (e.g. autonomous vehicles) communicate independently in a larger system (the traffic system) and interact with other systems (people, other vehicles, sensors in roads, GPS systems, traffic lights), a system of systems is automatically created. According to Jamshidi [8], systems of systems (SoS) means "a SoS is an integration of a finite number of constituent systems which are independent and operable, and which are networked together for a period of time to achieve a certain higher goal." In a system of CPS, the individual system communicates not only with its

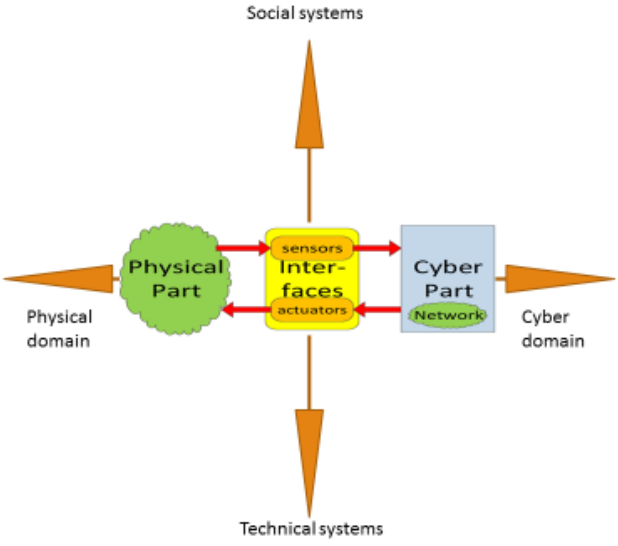

Fig. 3 Variety of sociotechnical cyber-physical system [7]

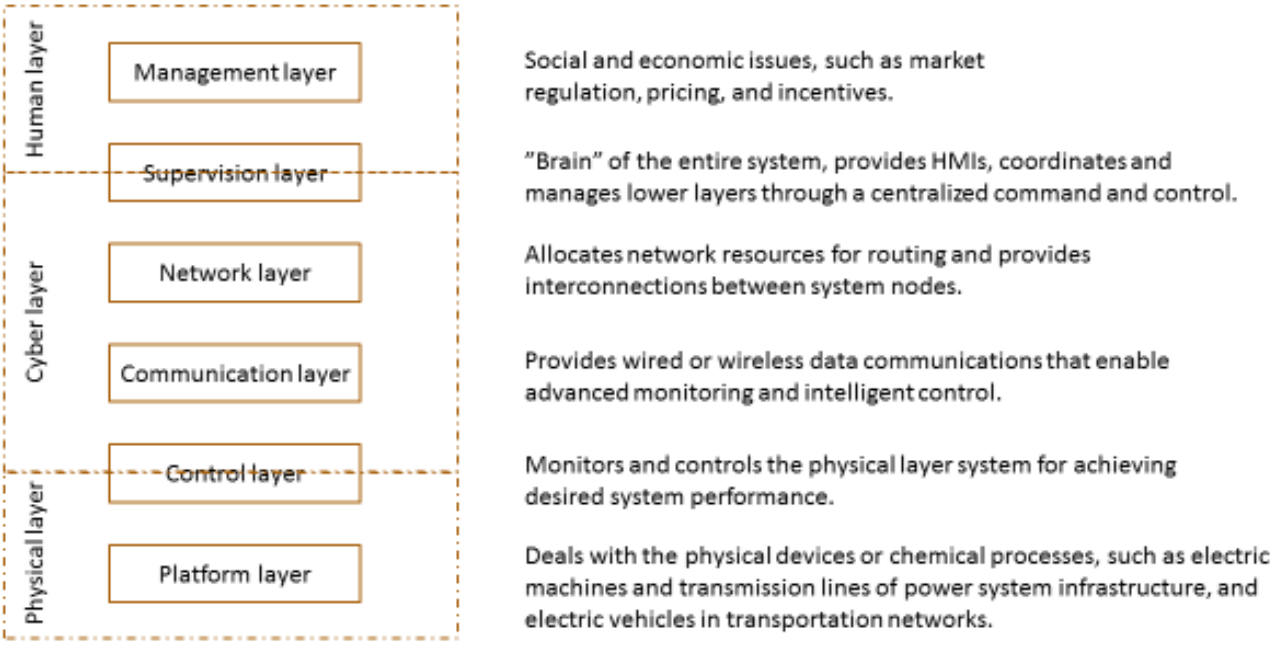

Fig. 5 Hierarchical structure of cyber-physical control systems [19]

own components, but also with technical and social systems in its environment.

3 Cyber Attacks to CPS

The last few years have seen the publication of numerous research papers that analyze cyber vulnerabilities in CPS, see [9], [10], [11], [12], [13], [14], [15], [16] and [17]. Figure 4 identifies the control loop components that can be impacted by cyber attacks, including measurements, actuator signals, controllers and reference signals [18]. Han et al. [18] introduce a framework for understanding cyber attacks and the related risks to CPS that consists of two elements, a three-layered (Physical layer, Control layer, and Cyber layer) logical model and reference architecture for CPS, and a meta-model of CPS attacks that is referred to as the CPS kill-chain.

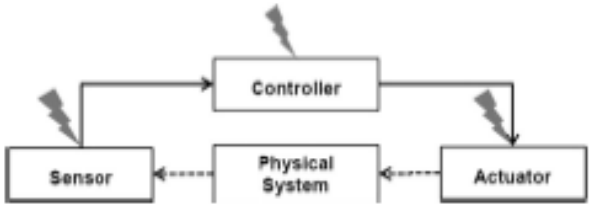

Fig. 4 Cyber-physical system attacks

Zhu and Basar [19] introduce a cross-layer approach for designing resilient control systems for CPS. Their approach integrates physical control systems with cyberinfrastructure and divides the cyber-physical control system into six layers: physical, control, communication, network, supervisory, and management, as shown in figure 5. To manage the increasing complexity of CPS, it is essential that control designs exploit the hierarchical nature of such systems [19], [20].

4 Resilient Systems

Resilience means that a system or infrastructure is able to adapt to changing conditions. In the case of information security, resilience is based on integrating two parallel subtasks: (1) run-time situation awareness and (2) a priori risk analysis. On the other hand, resilience itself is a twofold topic: (1) the system has to be robust against attacks, i.e., the attack is prevented in its first phase, and (2) the system has to be able to return to a safe state after the attack. Healing requires that utilized data and system operation can be restored as soon as possible. Therefore, healing processes have to be trained and tested.

4.1 Situational Awareness: Prerequisite of Cyber Security

Situational Awareness involves being aware of what is happening around one to understand how information, events, and one's own actions affect the goals and objectives, both now and in the near future. The most important enablers of situational awareness are observations, analysis, visualization, and cyber-policy of the government.

The overall target of cyber security is that all systems and infrastructures are resilient. Situation Awareness is the main prerequisite towards cyber security. Without situation 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. Situation 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.

Situational awareness is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resiliency focuses. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, are needed. This requires information exchange between different stakeholders. And always, when dealing with information exchange, the main question is "trust".

4.2 Security Technologies: Tools of Cyber Security

Security technologies include all technical means towards cyber security, such as secure system architectures, protocols and implementation, as well as tools and platforms for secure system development and deployment.

Security technologies include all technical means towards cyber security, such as secure system architectures, protocols and implementation, as well as tools and platforms for secure system development and deployment. Security technologies are needed for fulfilling the recognized security requirements, and for building resilient infrastructures and systems with dependable hardware and software that can also meet future security challenges.

Security technologies enable technical protection of infrastructures, platforms, devices, services, and data. The technical protection starts with secure user identification and authorization that are necessary features in most secure infrastructures, platforms, devices and services. Fortunately, well-known technologies exist for their implementation. Typically, processes and data objects are associated with an owner, represented in the computer system by a user account, who sets the access rights for others. A global trend is to increase the use of cloud service technology when providing critical services. Data go into a cloud and will not come back to end-users' devices. Also, government data has already gone to a cloud, and in the future more and more government data will migrate to cloud servers and services. Partnerships between cloud service providers and security solution providers are becoming more common. We will see the emergence of cloud service-specific-solution providers as well. Identity management and encryption will be the most important cloud security services to be offered. These services will be eventually offered for small to medium-sized businesses as well. We will also see emergence of cloud security standards. Challenges are that quite often cloud service providers believe that security is just an end user issue and firewall means security. Therefore, currently, we do not have proper cloud security standards and we lack awareness of a true understanding of comprehensive cloud security.

Security technologies are needed also then if something has happened. For example, forensics can lead to the sources of the attack/mistake and provide information for legal and other ramifications of the issue. Forensics also facilitates the analysis of the causes of the incident, which in turn, makes it possible to learn and avoid similar attacks in the future.

4.3 Security Management and Governance: The "Brain" of Cyber Security

Security management and governance covers the human and organizational aspects of information security. Its focus areas include: (1) Security policy development and implementation, and (2) Information security investment, incentives, and trade-offs. Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve

confidentiality, integrity and availability of the organization's information assets that do preserve [21].

The well-known fact of live is that people are the rock-bottom of cyber security. Security management and governance, "the brain and Intelligence of cyber security" takes care the human and organizational aspects of cyber security.

Security policy is currently the main element used to communicate secure work practices to employees and ICT stakeholders. It is a declaration of the significance of security in the business of the organization in question. Additionally, the security policy defines the organization's policies and practices for personnel collaboration. However, people still often fail to comply with security policies, exposing the organization to various risks. One challenge is to promote methods and techniques that can support the development of comprehensible security policies in the emerging ICT paradigms, e.g., cloud computing and multiple devices. Developing of policies that can defeat the main reasons driving non-compliance, such as a habit, is challenging.

ISMS provides controls to protect organizations' most fundamental asset, information. Many organizations apply audits and certification for their ISMS to convince their stakeholders that security of organization is properly managed and meets regulatory security requirements [22]. An information security audit is an audit on the level of information security in an organization. Security aware customers may require ISMS certification before business relationship is established. Unfortunately, ISMS standards are not perfect and they possess potential problems. Usually guidelines are developed using generic or universal models that may not be applicable for all organizations. Guidelines based to common, traditional practices take into consideration differences of the organizations and organization specific security requirements [23].

4 Discussion and Conclusions

Trustworthy and secure technologies and platforms are a basis to build on. As the security risks continue to increase with cybercrime and other unauthorized access, the security solutions and management of IT security need systematic design and constant development. Figure 6 shows the new systematic approaches towards resilient software-intensive systems. Both the resilient system and the situation awareness system are SISs. Security technologies are applied in and between their platform and software layers. Trust management is the main tool in and between human layers.

Software-intensive systems consist of three layers: the platform layer, the software layer and the human layer. Every cyber-secure system consists of two SISs: the proper resilient system, and the situational awareness system that is the main prerequisite towards cyber security. A complex SIS is a system of software-intensive sub-systems, which platform layers compose a physical network, software layers compose a software network and human layers compose a social network, as shown in figure 7. Cyber security should be systematically built up at all layers and networks. The resilient physical network (composed by blue arrows in figure 4) is the basis on which the information sharing between different stakeholders could be created via software layers (green arrows). However, the trust inside social networks (red arrows) quantifies the pieces of information that will be shared, - and with whom.

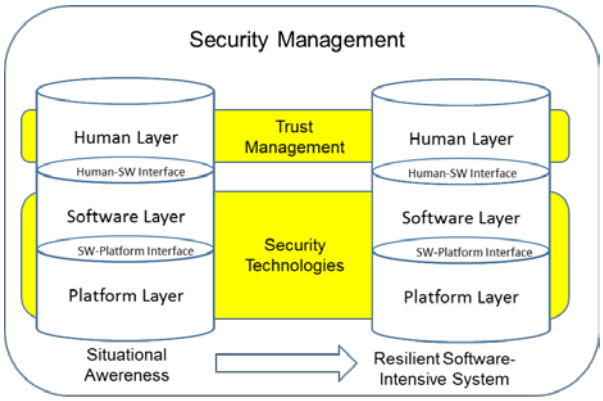

Fig.6 Systematic approach towards resilient software-intensive systems

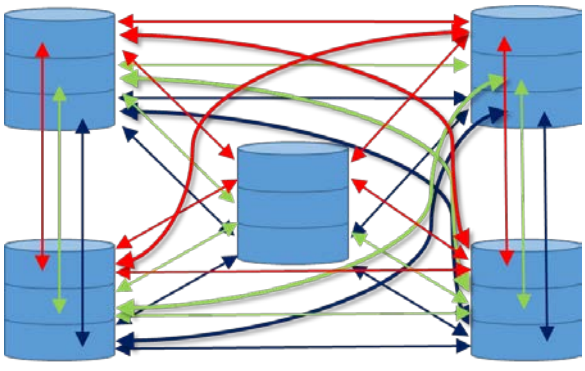

Fig.7 Software-intensive system of systems

References

[1] 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.

[2] P. Bosch, "RESIN: Resilient Cities and Infrastructures," *European CIIP Newsletter*, vol. 9, no. 3, pp. 15-16, 2015.

[3] M. Sveda, "Dependability in Cyber-Physical Systems Network Applications," in *Latest Trends in Circuits, Systems, Signal Processing and Automatic Control*, Salerno, 2014.

[4] L. Lukas and M. Hromada, "Management of protection of Czech Republic critical infrastructure elements," in *Proceedings of the 13th WSEAS international conference on Automatic control, modelling & simulatio*, 2011.

[5] H. S. Ariane Hellinger, *Cyber-Physical Systems. Driving force for innovation in mobility, health, energy and production*, 2011.

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

[7] J. Rajamäki, "Towards a Design Theory for Resilient (Sociotechnical, Cyber-Physical, Software-intensive and Systems of) Systems," in *Recent Advances in Information Science*, Barcelona, 2016.

[8] M. Jamshidi, *Systems of Systems Engineering: principle and applications*, CRC Press, 2009.

[9] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," Sept. 2010. [Online]. Available: http://www.computerworld.com/s/article/print/9185419. [Accessed 18 March 2016].

[10] S. Greengard, "The new face of war," *Commun. ACM*, vol. 53, no. 12, pp. 20-22, 2010.

[11] B. Krebs, "Cyber incident blamed for nuclear power plant shutdown," Washington Post, June 2008. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html. [Accessed 18 March 2016].

[12] S. Gorman, "Electricity grid in U.S. penetrated by spies," Wall Str. J., April 2009. [Online]. Available: http://online.wsj.com/article/SB123914805204099085.html. [Accessed 18 March 2016].

[13] A. Cardenas, S. Amin and S. Sastry, "Securecontrol:Towards survivablecyber-physicalsystems," in *Proceedings oftheTwenty-Eighth International Conferenceon Distributed Computing Systems Workshops*, 2008.

[14] Y. Liu, P. Ning and M. Reiter, " False data injection attacks against state estimation in electric power grids," in *Proceedings of the Sixteenth ACM Conference on Computer and Communications Security*, 2009.

[15] C. Li, A. Raghunathan and N. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proceedings of the Thirteenth IEEE International Conference on e-Health Networking Applications and Services*, 2011.

[16] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in *The Black Hat Technical Security Conference USA*, 2011.

[17] D. Shepard, J. Bhattiand and T. Humphreys, "Dronehack: Spoofing attack demonstration on a civilian unmanned aerial vehicle," *GPS World*, 1 August 2012.

[18] A. Hahn, R. Thomas, I. Lozano and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *Internal Journal of Critical Infrastructure Protection*, vol. 11, pp. 39-50, 2015.

[19] Q. Zhu and T. Basar, "Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems: Games-in-Games Principle for Optimal Cross-Layer Resilient Control

Systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46-65, 2015.
[20] M. Ilic, "From hierarchical to open access electric power systems," *Proc. IEEE*, vol. 95, no. 5, pp. 1060-1084, 2007.
[21] W. Lee and S. Jang, "A study on information security management system model for small and medium enterprises," *Recent Advances in E-Activities, Information Security and Privacy*, pp. 84-87, 2009.
[22] J. S. Broderick, "ISMS, security standards and security regulations," *Information Security Technical Report*, vol. 11, pp. 26-31, 2006.
[23] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management*, vol. 46, pp. 267-270, 2009.