Towards a Design Theory for Resilient (Sociotechnical, Cyber-Physical, Software-intensive and 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: - Resilience, as a property of a system, must transition from just a buzzword to an operational paradigm for system management, especially under future climate change. Identifying the need for system resilience requires defining the system. Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how sociotechnical, cyber-physical, and systems of systems are conceptualized, built and evaluated. The aim of this paper is to start a development process for a design theory (DT) for resilient systems (DT4RS). With the help of DT4RS, communities are able to develop and operate different information and security technologies, and share knowledge and best practices.

Key-words: - Sociotechnical systems; Cyber-physical systems; Systems of systems, Design theory, Resilience

1 Introduction

Figure 1 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 2a. Current sociotechnical systems are software-intensive systems (SIS) as shown in figure 2b. SIS' future trend is that the software layer (=cyber part) is growing, as illustrated in figure 2c. All SIS are also cyber-physical systems (CPS): human and platform layers form the physical part and the software layer forms the cyber part of the CPS.

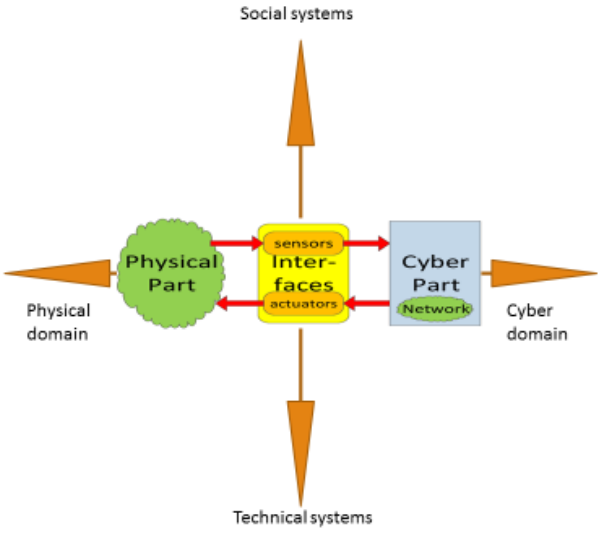

Fig. 1 Variety of sociotechnical cyber-physical system

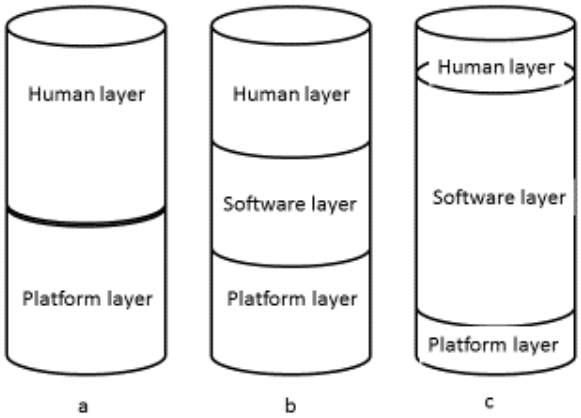

Fig. 2 Software-intensive system trends [1]

According to Jamshidi [2], 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."

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructure lacks the same degree of resilience, typically losing essential

ISBN: 978-1-61804-365-8

functionality following adverse events [3]. Resilient systems are able to minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events [3]. Our society's critical sociotechnical CPS — communication, energy, water, transportation, finance, healthcare— lacks of resilience, typically losing essential functionality following adverse events [3]. Resilience, as a property of a system, must transition from just a buzzword to an operational paradigm for system management. Identifying the need for system resilience requires defining the system. Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how CPS are conceptualized, built and evaluated [1].

Our research goal is to develop an information systems design theory for resilient software-intensive systems (DS4RS) so that communities developing and operating different security technologies can share knowledge and best practices using a common frame of reference. By a sound design theory, the outputs of these communities will combine to create more resilient systems, with fewer vulnerabilities and an improved stakeholder sense of security and welfare.

2 Design Theory Development

Designing security for software-intensive systems is challenging since the technologies that make up these systems, e.g., operating systems, databases, networks, and the world-wide web, have traditionally used different models for security. Furthermore, the communities that develop these technologies do not systematically learn from each other's best practices in designing for security [4].

In the operating system community, the necessity to distinguish the level of privilege required to run code from that required to read a file or access other resources is well-known. Also, before any code is run on a system, the originator of the code should be authenticated and authorized or acknowledged as trusted by the user [4]. These design principles and security mechanisms have been expressed more than three decades ago. On the other hand, the database development and operations communities still allow Structured Query Language injection attacks to cause significant damage to businesses and consumers (e.g., reputation damage, financial loss, identity theft, etc.) by not properly observing these design principles. The development, networking, and operations communities have made similar mistakes. Examples are routing advertisements as parameters to code that modify critical shared resources – routing tables on the Internet – service providers have frequently allowed information that is transported over the Internet to be misrouted and delivered to a hacker's network or machine. However, all informed security communities understand that security benefits from following an appropriate design process in the context of a system lifecycle [4].

Gregor and Jones [5] define six core components of design theory and two additional components that are shown in Table I. Next section of this paper proposes our design theory for resilient software-intensive systems with regard to the six core components.

3 Proposed Elements of Design Theory for Resilient Systems

3.1 The Purpose and Scope

The main purpose for designing resilient systems is how to return privacy and trust in digital world and to gain a global competitive edge in security-related business, such as critical infrastructures. The purpose, with regard to security, is to know what is going on and what will happen in the network(s), and to be aware of the current level of security in the network(s), how to design or build-in security and resiliency to a networked environment, and to define trade-offs for security and privacy levels versus system's usability. The overall aim is to mitigate cyber security risks, which in its turn supports the business continuity and operations of the whole society.

3.2 Constructs

3.2.1 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 run-time situational awareness and a priori risk analysis.

3.2.2 Situational Awareness

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.

ISBN: 978-1-61804-365-8

Table I. Eight components of an Information System Design Theory

Component	Description
Core components	
Purpose and scope (the causa finalis)	"What the system is for," the set of meta-requirements or goals that specifies the type of artifact to which the theory applies and in conjunction also defines the scope, or boundaries, of the theory.
Constructs (the causa materialis)	Representations of the entities of interest in the theory.
Principle of form and function (the causa formalis)	The abstract "blueprint" or architecture that describes an IS artifact, either product or method/intervention.
Artifact mutability	The changes in state of the artifact anticipated in the theory, that is, what degree of artifact change is encompassed by the theory.
Testable propositions	Truth statements about the design theory.
Justificatory knowledge	The underlying knowledge or theory from the natural or social or design sciences that gives a basis and explanation for the design (kernel theories).
Additional components	
Principles of implementation (the causa efficiens)	A description of processes for implementing the theory (either product or method) in specific contexts.
Expository instantion	A physical implementation of the artifact that can assist in representing the theory both as an expository device and for purposes of testing.

The most important enablers of situational awareness are observations, analysis, visualization, and cyber-policy of the government.

3.2.3 Security Technology

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.

3.2.4 Security Management and Governance

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 [6].

3.3 Principles of Form and Function

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 3 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 4. 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.

The design principles towards trust-building includes:

1. Proactive – design for security. A proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries.

2. Self-healing – utilizing the toolbox. Novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing.

3. Public awareness – increase trust. Enable seamless cyber security integration to every-day life. By efficiently utilizing tools and methods, stakeholders can co-operate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public awareness and understanding will move towards accepting cyber security as a natural element of a connected world.

3.4 Artifact Mutability

From every indication, the growth of the software layer, in size and percentage of the overall systems, will be the future trend [1]. The role of software will become dominant in nearly all complex systems. Thus, research and development in SIS must actively address the challenges of using software as the primary building material in future complex systems [1]. According to Hevner and Chatterjee [1], in the future world of pervasive computing and ubiquitous cyber-physical devices, it will be essential that IT artifacts and the integrated systems containing these artifacts be reliable, adaptable, and sustainable. Design for SIS should draw its foundations from multiple research disciplines and paradigms in order to effectively address a wide range of system challenges. According to Hevner and Chatterjee [1], the most important intellectual drivers of future science of design in SIS research will be dealing with complexity, composition and control. Hanseth and Lyytinen [7] adopt the viewpoint of designers: how to 'cultivate' an installed base and promote its dynamic growth by proposing design rules for information infrastructure (II) bootstrapping and adaptive growth. Within their design rules, the II

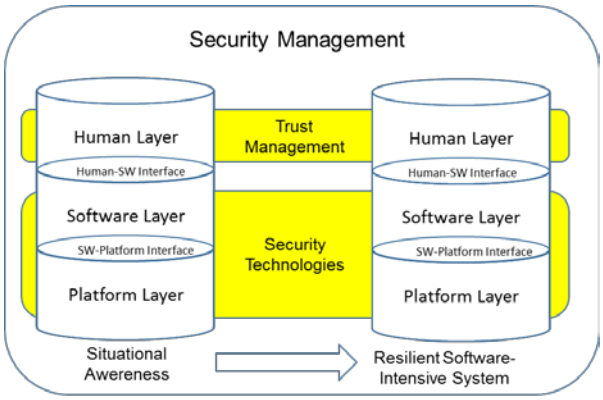

Fig.3 Systematic approach towards resilient software-intensive systems

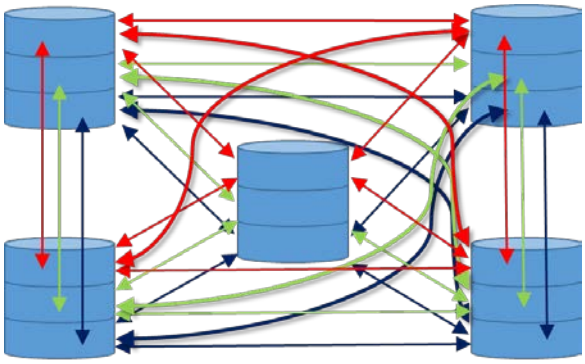

Fig.4 Software-intensive system of systems

designers would have to prefer continuous, local innovation to increase chaos and to apply simple designs and crude abstractions. According to Hanseth and Lyytinen [7], this change is not likely, as design communities are often locked into institutional patterns that reinforce design styles assuming vertical control and complete specifications.

3.5 Testable propositions

This section present the truth statements of DT4RS.

3.5.1 Resilience

The overall target of cyber security is that all systems and infrastructures are resilient. 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.

ISBN: 978-1-61804-365-8

3.5.2 Situational Awareness

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”.

3.5.2 Security technology

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.

3.5.3 Security management and governance

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 [8]. 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 [9].

3.6 Justified Knowledge

The approach proposed is derived from the science of critical infrastructures, cyber trust/trust building, and complex software-intensive systems presented.

4 Discussion and Conclusions

The choice properties and design aspects described in this study are a proposed start to a design theory for resilient SISs. The next future work is to cover the additional components of ISDT presented in Table I.

References

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

[2] Jamshidi, M., Systems of Systems Engineering: principle and applications, CRC Press, 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] L. Waguespack, D. Yates and W. Schiano, "Towards a Design Theory for Trustworthy Information Systems," 47th Hawaii International Conference on System Sciences (HICSS), pp. 3707-3716, 2014.

[5] S. Gregor and D. Jones, "The anatomy of a design theory," Journal of the Association for Information Systems, vol. 8, pp. 312-335, 2007.

[6] 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.

[7] O. Hanseth and K. Lyytinen, "Design theory for dynamic complexity in information infrastructures: the case of building internet," J. Inf. Technol, vol. 25, pp. 1-19, 2010.

[8] J. S. Broderick, "ISMS, security standards and security regulations," Information Security Technical Report, vol. 11, pp. 26-31, 2006.

[9] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," Information & Management, vol. 46, pp. 267-270, 2009.