FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Design science research towards resilient cyber-physical eHealth systems

Jyri Rajamäki, Rauno Pirinen

Laurea University of Applied Sciences, Espoo, Finland

Jyri Rajamäki, Adjunct Professor, D.Sc., Ph.D., Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, FINLAND. Email: jyri.rajamaki@laurea.fi

Abstract

Most eHealth systems are cyber-physical systems (CPSs) making safety-critical decisions based on information from other systems not known during development. In this design science research, a conceptual resilience governance framework for eHealth CPSs is built utilizing 1) cybersecurity initiatives, standards and frameworks, 2) science of design for software-intensive systems and 3) empowering cyber trust and resilience. According to our study, a resilient CPS consists of two sub-systems: the proper resilient system and the situational awareness system. In a system of CPSs, three networks are composed: platform, software and social network. The resilient platform network is the basis on which information sharing between stakeholders could be created via software layers. However, the trust inside social networks quantifies the pieces of information that will be shared - and with whom. From citizens' point of view, eHealth is wholeness in which requirements of information security hold true. Present procedures emphasize confidentiality at the expense of integrity and availability, and regulations/instructions are used as an excuse not to change even vital information. The mental-picture of cybersecurity should turn from "threat, crime, attack" to "trust" and "resilience". Creating confidence in safe digital future is truly needed in the integration of the digital and physical world's leading to a new digital revolution. The precondition for the exchange of information "trust" must be systematically built at every CPS' level. In health sector, increasingly interconnected social, technical and economic networks create large complex CPSs, and risk assessment of many individual components becomes cost and time prohibitive. When no-one can control all aspects of CPSs, protection-based risk management is not enough to help prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events do occur.

Keywords: eHealth, cyber trust, cyber-physical system, information security, resilience, software-intensive system

Introduction

Cyber-physical systems (CPS) are a subset of sociotechnical systems that provide seamless integration between computational, human and physical elements [1]. Critical eHealth systems (e.g. Health Information systems; Clinical data repositories; Authentication server; Laboratory Information Systems; Radiology Information Systems; Picture Archiving and Communication Systems; Electronic Health Record components; Patient Health Record service; ePrescription service) are CPSs making safety-critical decisions based on information from other systems not known during development. The Forum for Public Safety Communications Europe (http://www.psc-europe.eu) defines safety-critical decision as “a decision that results in either lives being saved or serious injury being avoided.” To achieve the trust of users, measures of safety have to be taken into consideration in accordance with the "privacy by design" approach. This requires secure storage of information and guaranteeing safe exchange of data preventing unauthorized access, loss of data and cyber-attacks.

This research paper comprises four chapters. This introduction is followed by the presentation, in Chapter 2, of the research material and methods applied in this study including discussions about the environment, knowledge base, data collection and data anbalysis of the study. Chapter 3 presents the main results and research contributions that are further discussed in Chapter 4. The last chapter includes also recommendations for further research.

Material and methods

Design science research

The chosen research approach is the design science research framework of Hevner et al. [2,3] as shown in Figure 1.

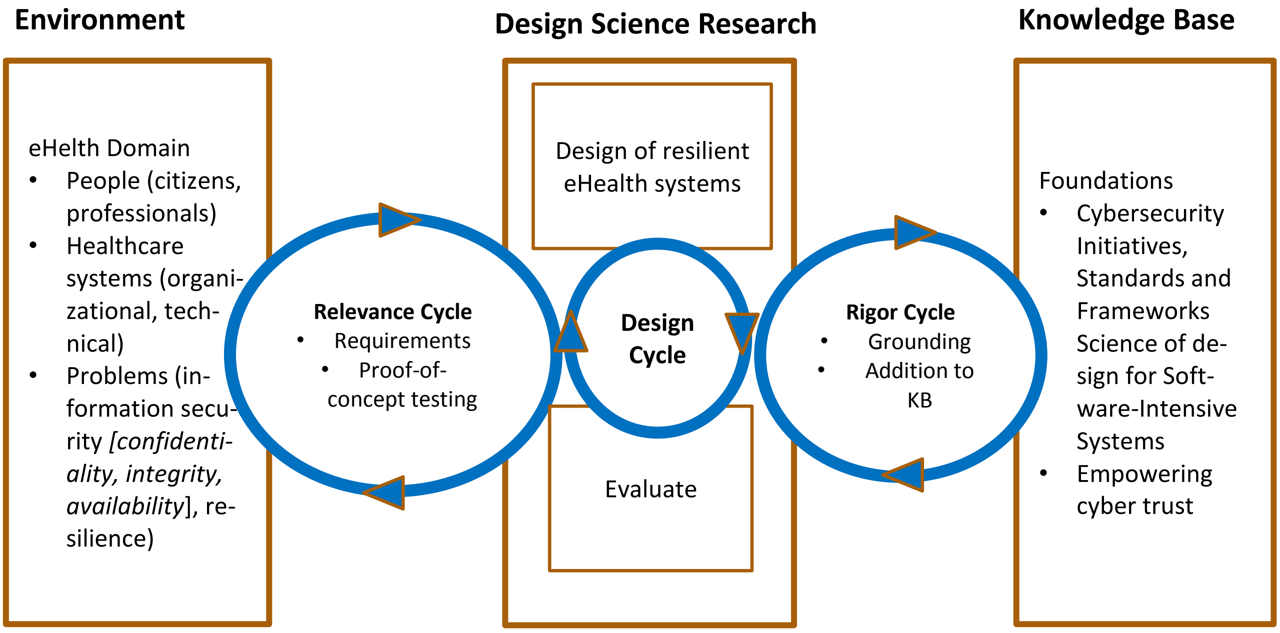
Environment
Design Science Research
Knowledge Base
eHelth Domain
• People (citizens, professionals)
• Healthcare systems (organizational, technical)
• Problems (information security [confidentiality, integrity, availability], resilience)
Design of resilient eHealth systems
Relevance Cycle
• Requirements
• Proof-of-concept testing
Design Cycle
Rigor Cycle
• Grounding
• Addition to KB
Evaluate
Foundations
• Cybersecurity Initiatives, Standards and Frameworks Science of design for Software-Intensive Systems
• Empowering cyber trust

Figure 1. Design science research cycles of this study (modified from [3]).

As Hevner and Chatterjee [3] explains, the Relevance Cycle bridges the contextual environment of the research project with the design science activities. Within eHealth Domain, the Environment includes people (citizens and healthcare professionals), eHealth systems (organizational and technical systems) and different related problems, for example availability, integrity and confidentiality of information in eHealth systems. The Rigor Cycle connects the design science activities with the Knowledge Base of scientific foundations, experience, and expertise that informs the research project [3]. The knowledge base of this study consists of 1) cybersecurity initiatives, standards and frameworks, 2) science of design for software-intensive systems and 3) empowering cyber trust and resilience. The central Design Cycle iterates between the core activities of building and evaluating the design artifacts and processes of the research [3]. The main artifact of this study is the conceptual model for resilient eHealth systems.

eHealth environment

Security Aspects in eHealth: The digital security of information is traditionally expressed in terms of maintaining three characteristics of the information: confidentiality, integrity and availability. In addressing the provision of data security services for information assets, it is necessary to consider the state of the information: is it in storage, in transmission, or in use as being processed. When considering possible aspects to secure digital information, three classes occur: technological solutions; policy-regulation; and practices related to information management; and the frames of education and situational awareness as views of all stakeholders in the security implications of potential activities. The three characteristics of information, the three states of information and three classes of security aspects form the basis of an information security-resilience frame exists, confer [4] and our furthered Figure 2.

Digital security is generally understood as a 'weakest link' problem, so the system cannot be considered secure unless all aspects are dealt with adequately, and with regard to eHealth, many people consider this unlikely to be achieved, hence, the continuing concerns over information privacy [5]. On the other hand, others consider eHealth systems an opportunity to achieve better security and privacy protection than what is available in paper-based systems through additional security functionalities: user authentications and authorizations, the retention of back-up files, user defined storage and retrievals and accountability measures, monitoring and logging access to records, and establishing audit trails and other mechanisms to enable information accountability [5]. However, these require a more comprehensive approach than an attempt to add on technological security measures to an incompletely specified eHealth system.

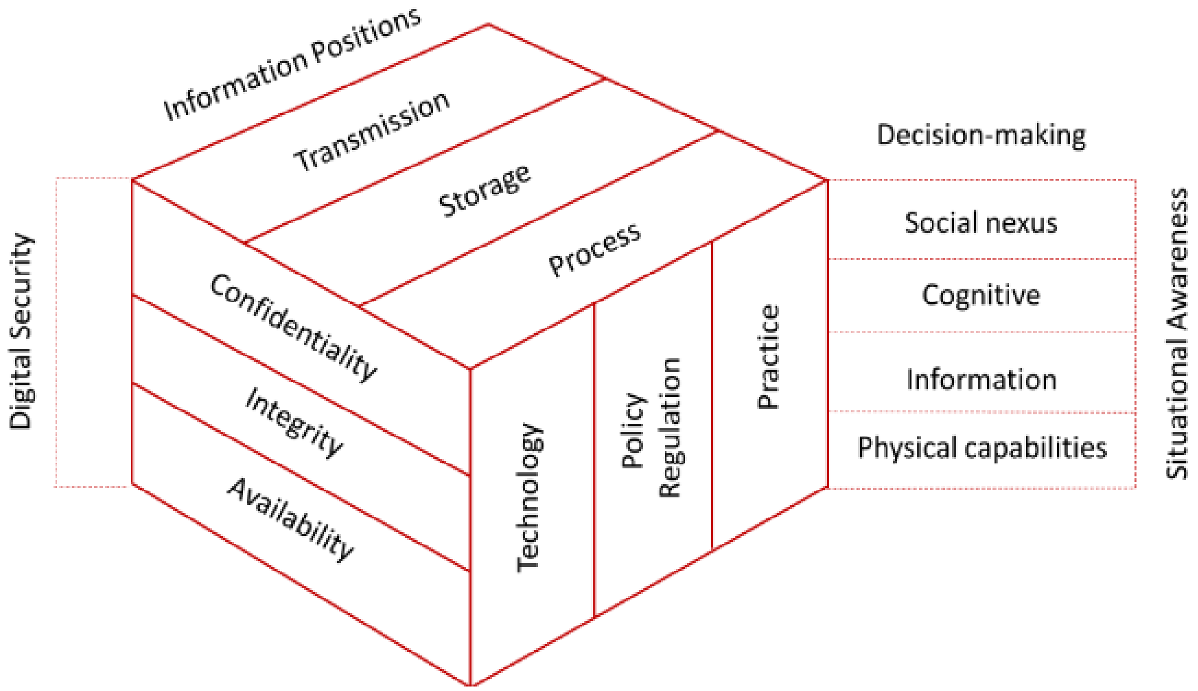

Figure 2. Security aspects for information dimensions (modified from [4]).

Current Cybersecurity Challenges in eHealth: In 2015, The European Union Agency for Network and Information Security (ENISA) published their study “Security and Resilience in eHealth” [6] that focus on eHealth information systems and infrastructures as well as on the relevant assets that are considered critical both for the society and the relevant stakeholder groups. This study can be seen as a description of the state of the art how EU member states perceive cybersecurity in their health systems, which are the specific approaches they follow, and which are the measures they take to protect these systems.

According to the ENISA, the most important cybersecurity challenges in eHealth infrastructures and systems are: 1) systems availability; 2) lack of interoperability; 3) access control and authentication; 4) data integrity; 5) network security; 6) security expertise and awareness; 7) data loss; 8) standardization, compliance and trust; 9) cross-border incidents; and 10) incidents management [6].

Knowledge base

Existing Cybersecurity Initiatives, Standards and Frameworks: The Internet and the broader concept of 'cyber world' that includes not only the computers and data and information networks but also the complete and comprehensive system of human existence in those networks [7], has provided businesses with new opportunities for competitive advantage against competitors and a new vector for further economic growth. At the same time concerns about the security of cyber world have also grown exponentially as criminals are continuously looking to exploit this new environment for their own economic benefit. Increasingly, a priority concern in this regard is associated with the potentially sensitive, classified and personal information that is stored and processed by organizations - often related to their supply chain, customers and employees. One commonly used tool to take control and to protect information in cyber world is an information security management system (ISMS). ISMSs are designed to maximize business continuity and minimize risk, defining the policies, procedures and governance needed to secure organizations sensitive data and protect against the risk of cybersecurity breaches. ISMSs typically aim to cover the full spectrum of businesses knowledge assets, from data and technology to employee behavior and business culture.

Standards such as ISO/IEC 27001 provide internationally recognized and accredited specifications for the creation of an ISMS. Such accreditation goes some way to providing customers, partners and other members of the supply chain that their data, systems and employee practices are secured and governed to meet a baseline of information security requirements. In certain sectors appropriate ISO/IEC certification is required to initiate business relationships whilst also meeting basic security audit requirements. Such compliance is a mandatory precondition for companies. However, there is a growing sense of urgency for multidisciplinary, flexible and adoptable cybersecurity frameworks that go beyond the baseline set by these standards, and make provisions for conditions that arise as a result of the rapidly changing cyber threat landscape and the new and evolving risks that emerge as a result.

While security audits and certifications have been increasingly used in both the public and private sectors, they are often based on generic models and are not wholly applicable and interoperable across all organizations and sectors. These audits primarily address the technological aspects of cybersecurity, i.e. compliance with security requirements. While cybersecurity/cybercrime metrics and statistics are available in a variety of data types, the economic value, especially in the long term, of these metrics is often missing or hard to evaluate (as in the case of reputation loss). In addition, the available metrics and consistency of overall cybersecurity terminology is not always clear. Lack of common definitions and methodologies leaves open the possibility of misinterpretation and thus can result in big differences when assessing the economic implications of cybersecurity incidents. It also creates a challenge for government bodies when devising cybersecurity policies providing due to the availability of many contrasting methodologies and a shortage of reliable data.

The cybersecurity challenges: On the one hand, we have asynchronous cybersecurity practices, many standards and frameworks to cope with while on the other hand, nation-states, online criminals, organized hacktivists, insider threats and hackers with malafide intentions to deal with. The Center for Cyber Safety and Education's global information security workforce study conducted in year 2015 confirms that globally we are not only loosing but also backpedaling against aforementioned threats and risks at cyber world [8]. One of the key reasons of rapidly increasing breaches denoted to "attack surface" [9] (the set of ways in which an adversary can attack the system) in addition to increasing vulnerabilities, number of internet users, and number of users accessing online resources. How do organizations conduct and practice their cybersecurity to protect against dramatic attack surfaces? And most importantly, how do they allocate limited cybersecurity resources in defense? Most organizations advices to adopt more systematic approaches using standards, framework, audits and best practices. However, ENISA's recent study [6] also confirms that there are gaps in existing systematic approaches of cybersecurity.

Taking into account the results of existing projects looking at defining priority research areas associated with cybercrime and information security, such as COURAGE, CAMINO and CyberROAD [10,11] it is clear that the actual, tangible, cost of cybercrime is really not yet known. The availability of reliable data is essential for policy-making and revenue allocation from the top (governments) downwards (individual stakeholders) in order to meet the challenges of the future as well as those we face currently. With factors such as traditionally low levels of reporting and the challenges associated with quantifying the medium and long terms of costs of cybersecurity breaches all contributing to the aforementioned challenges, there is clearly no single 'catch-all' solution address these gaps.

Science of Design for Software-Intensive Systems: Theory of complex systems traces its roots to the 60s when Herbert A. Simon wrote his book "Science of the Artificial" [12]. Fulfillment of purpose involves the relationship between the artifact, its environment and a purpose or goal. Alternatively, it can be viewed as the interaction of an inner environment (internal mechanism), an outer environment (conditions for goal attainment) and the interface between the two. According to Hevner and Chatterjee [3], the real nature of the artifact is the interface. Both the inner and outer environments are abstracted away. The science of artificial complex systems should focus on the interface, the same way design focuses on the "functioning." A general theory of complex systems must refer to a theory of hierarchy, and the near-decomposability property simplifies both the behavior of a complex system and its description [3].

Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how software-intensive systems (SIS) are conceptualized, built and evaluated. Manual methods of software and systems engineering must be replaced by computational automation that will transform the field into a true scientific and engineering discipline [3]. They also argue that the vision of design science for SIS must achieve the following essential objectives: 1) Intellectual amplification: Research must extend the human capabilities (cognitive and social) of designers to imagine and realize large-scale, complex software-intensive systems; 2) Span of control: Research must revolutionize techniques for the management and control of complex software-intensive systems through development, operations, and adaptation; 3) Value generation: Research must create value and have broad impacts for human society via the science and engineering of complex software-intensive systems and technologies [3].

Figure 3 illustrates the three layers of SIS: 1) the platform layer, 2) the software layer and 3) the human (social) layer, and the two critical interfaces between these layers. Also, concepts of the software layer are shown on the right side of the figure. According to Hevner and Chatterjee [3], the software layer is a makeup of software code, information and control within the context of an application domain. They continue that "the overlaps among these three concepts support varying methods and techniques of understanding and building the software layer of systems. For example, software architectures define structures for integrating the concept of code, information, and control for a particular application domain system."

SIS design entails many important decisions, such as the design and allocation of system behaviors (e.g., functions, actions) and system qualities (e.g., performance, security, reliability) to the different layers [3]. A particular system activity could be realized in hardware (platform), via, for example, a service call (software), by human behavior (human) or by some combination of activities across all three layers, and a performance requirement (e.g., response time) for an SIS transaction could be divided and allocated as performance requirements in each of the layers [3]. Nearly all future SIS will be connected to environmental resources and other systems via network connections, and these connections lead to complex systems-of-systems architectures to provide behaviors and qualities [3]. There will be identifiable networks across all three SIS layers: physical networks support the transmission of digital and analog data among system platforms, software networks provide the middleware layers and protocols that transform the transmitted data into information that is shared among the information processing systems, and social networks provide a means of interaction and community among the human participants of the complex system [13].

Empowering Cyber Trust and Resilience: International standardization organizations' recent study [14] on public-private partnership for cybersecurity identified three main cybersecurity challenges by 2020: 1) Cybersecurity governance framework 2) Common understanding and scope of cybersecurity 3) Re-establishing and assuring cyber-trust. Cybersecurity governance framework, with the focus on mapping existing best practices, increases harmonization of European cybersecurity initiatives and also reduces fragmented practices of cybersecurity solutions by validating with cybersecurity metrics, indicators and certifications. Common understanding and scope of cybersecurity can map and validate cybersecurity processes considering social and economic perspective. The goal should be to measure and increase effectiveness of cybersecurity program through implementation, effectiveness and impact. The framework would establish a common understanding through validated best practices that matches with cybersecurity standards and framework. However, lack of trust is the main cybersecurity challenge – not technology or processes [15]. The aim of re-establishing and assuring cyber-trust is that cybersecurity should be seen as a key enabler for the development and maintenance of trust in the digital world [16]. It is important to complement the currently dominating "cybersecurity as

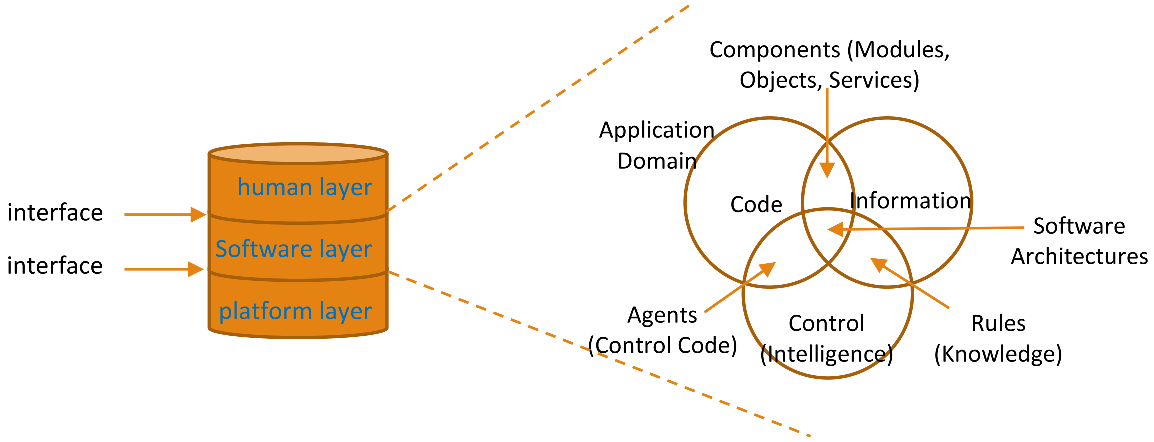

Figure 3. Software-intensive systems (Modified from [3]).

a barrier” perspective by emphasizing the role of “cybersecurity as an enabler” of interoperability, new interactions and services - and recognizing that trust is a positive driver for growth. Therefore, we must create methods and structures that enhance trust by mapping current and beyond state-of-the-art cybersecurity practices, then creates measurement practices with cybersecurity metrics and finally adding social and economic dimension creating and validating cybersecurity cost-benefit framework.

Increasingly interconnected social, technical and economic networks create large complex systems, and risk assessment of many individual components becomes cost and time prohibitive, or even impossible [17]. No-one can control the wholeness and our outlook should move to coordination and co-operation. The uncertainties associated with the vulnerabilities of these systems challenges our ability to understand and manage them. Risk assessment and risk management are no longer sufficient to focus on increasing risks in the modern cyber-physical world having non-foreseeable and non-calculable stress situations. To address these challenges, risk assessment should be used where possible to help prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events do occur [17].

The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient [18]: *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 [19] identifies four domains that create shared situational awareness and inform decentralized decision-making; including: *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; and *4) Social nexus:* Organization structure and communication for making cognitive decisions. Linkov et al. [20] 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 resiliency and should be assessed using network science tools [21].

Data collection

The data collection of this study is cumulative and systematically used for a qualitative analysis for model design, where (n) indicates an instance of data collection used for this analysis between January 2008 and March 2017. The data collection is comprised according to the results descriptions by Finnish Academia including eighteen (n=18) cumulative data categories followed: 1) scientific publication (n=52) according to publication forum classification; 2) number of open data collections (n=2) facilitated and licensed data collections used; 3) collective creation of international publication (n=72) articles; 4) data of international researcher exchange; 5) integration of education (n=6) study units related (n=3) theses and (n=3) dissertations; 6) data of European Commission’s funded research projects (n=4) and data of national programme of Ministry (n=1) and data of new proposal (n=1) for H2020; 7) presentations and audiences with (n=56) stakeholders; 8) data of (n=4) workshops and (n=6) seminars, creation of (n=4) events for research and development; 9) participation to public audiences, such as in a parliament and participation to statements (n=1); 10) publication in (n=6) newspapers and general descriptions according to publication forum classifications; 11) invited (n=3) presentations; 12) indicators of social media: Twitter, LinkedIn, Facebook and (n=3) homepages; 13) support of public events for international, national, and regional audiences; and data of economic indicators, such as 14) investigations, 15) patents, 16) licenses, 17) spin-offs, and 18) start-ups.

The data collection category (6 above) namely programmes, projects and proposals for qualitative analysis included followed: The data collection of Finnish National Architecture for Digital Services Programme (KAPA) by Ministry of Finance. The three (n=3) European Commission funded research projects: epSOS deliverables, EU_CISE_2020 and MARISA; and data collection of H2020 proposal namely SecSOS.

Programme [National Architecture for Digital Services: KAPA] by Finnish Ministry of Finance [140:00/2013] addresses to design of compatible infrastructure facilitating information transfer between organisations and services. This programme involves creating a national data exchange layer, the shared service views required by citizens, companies and authorities, a new national e-identification model and national solutions for the administration of roles and authorisations for organisations and individuals. The expected contribution followed: 1) to simplify and facilitate transactions by citizens, companies and organisations with the authorities and to improve security 2) to promote openness in public administration and to improve the quality of public services 3) to enable cost-efficiency in online services 4) to improve shared use of information and the compatibility of information systems 5) to promote corporate opportunities for leveraging public administration databases and services 6) to support the national economy by making public administration more efficient and by creating new business opportunities in the private sector.

Project [epSOS deliverables] Open eHealth Initiative for a European Large Scale Pilot of Patient Summary and Electronic Prescription [Project ID 22499; funded under Competitiveness and Innovation Framework Programme by EC; between July 2008 and June 2014] intended to design of a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. The epSOS project contributed to seamless healthcare to European citizens. Key goals were to improve the quality and safety of healthcare for citizens when travelling to another European country. It concentrated on developing a practical eHealth mechanisms and information systems infrastructure that enables secure access to patient health information among different European healthcare systems. The deliverables of epSOS shares data collection and proposal of design setting for contribution to patient safety by reducing the frequency of medical errors and by providing quick access to documentation as well as by increasing accessibility of ones prescribed medicine also abroad. For this research of cyber-emergency design: documentation as one category of gathered research data provides the medical personnel perspective with life-saving information; hence, this data collection was used for analysis of models for progress of more resilient cyber-physical eHealth systems and related pre-operational validation setting.

Project [EU_CISE_2020] European Union’s Information Sharing Environment [Project ID 608385; Funded under FP7-SECURITY] addresses steps forward along the accomplishment of the European roadmap for Common Information Sharing and Distributed Systems and Services Environment. The project attains the widest possible experimental environment of innovative and collaborative services and processes between European maritime institutions and takes as reference a broad spectrum of factors in the field of European Integrated Maritime Surveillance, arising from the European legal framework, as well as from studies, pilots, and related R&D projects. The timeframe of EU_CISE_2020 is between 01/06/2014 and 01/06/2018. Here, the EU_CISE_2020 data collection is facilitated for research and development of data sharing models and increasing resilience in cyber-physical eHealth systems and its related pre-operational validation.

Project [MARISA] Maritime Integrated Surveillance Awareness [Project ID 740698; Funded under H2020] is our new current H2020 project, timeframe between April 2017 and September 2019. The overarching goal of this project is to provide the security communities operating at sea with a data fusion toolkit, which provides a suite of methods, techniques and software modules to correlate and fuse various heterogeneous and homogeneous data and information from different sources, including Internet and social networks, with the aim to improve information exchange, situational awareness, decision-making, reaction capabilities and resilience. The expected solution will provide mechanisms to get insights from any big data source, perform analysis of a variety of data based on geographical and spatial representation, use techniques to search for typical and new patterns that identify possible connections between events, explore predictive analysis models to represent the effect of relationships of observed object at sea. Enterprise and ad-hoc reporting and Maritime Services, within the CISE context furthers users-centring and operational systems in their daily activities, as well as presentation tools for navigating and visualizing results of data fusion processing. Our assumption is that large amount of MARISA results as data fusion capabilities would be reflected in the eHealth domain.

Proposal [SecSOS] Digital Security for European Health Care Data and Open Services on a Systemic Level [Proposal ID 727643; Call H2020-DS-SC1-2016] addressed to design of healthcare services as critical infrastructures (CI) which should be protected from all types of threats, including cybersecurity attacks. Real information security can increasingly be based on the openness and transparency of the security solution and the secrecy of its encryption keys. The research scope of SecSOS was in development of externally auditable open-source security solutions that are needed in order to ensure the privacy and integrity of eHealth data and gain the validity and trust of the customers. Based on technological, integration and system readiness level (SRL) metrics, design of SecSOS addressed to new security readiness level (SecRL) metrics that would support the development of European operational standards for secure cross-border data exchange and patient privacy protection. Based on these metrics and prior open-source solutions (such as the OpenNCP suite), SecSOS proposal addressed to realization of both portable and server-based secure node platforms and components that enable the secure sharing and exchange of eHealth related data among countries and end users. Based upon the critical information infrastructure protection point of view, the SecSOS cyber resilience governance data collection included an approach to combating cyber threats, ensuring the viability of critical cyber assets and services, and items for building cyber trust.

Data analysis

In this study, the design science research approach was used [3], and the research setting of study addresses the following literature for analysis: "qualitative data analysis" [22]; "real world research" [23]. In this analysis, the qualitative analysis followed replication logic, and the selected data samples served in a manner similar to multiple experiments, with similar results. A literal replication or contrasting results in a theoretical replication predicted explicitly at the outset of the investigation [24]; and "case study research" [25]. The analysis used herein brings an understanding of a complex issue and object, and can extend experience or add strength to what is already known through previous research and reviewed literature for building, improving and testing of research and development models for cyber-physical systems in domain of eHealth systems Here, the study emphasize a detailed contextual analysis of a limited number of events or conditions and their relationships when the relevant behavior is not manipulated and the role of the researcher is that of an "objective outsider," as [26] positioned.

Results

In overall, study revealed that eHealth is the high-value growing field that is fast expanding as it is motivated by information and communication systems support to vary health vacancies and doctors can expressively improve the quality of the entire health care by improving the excellence of care with often lowered economical extents. Information systems can help older peoples residing at their home by means of data fusion systems comprised health care sensors, agents, actuators, and vary number of emergent technologies. Then, the terms resilience and adaption are imperative in order to provide guarantees about robust and as well safe implementation of systems, especially in focused viewpoints of unpredictable situations (situational awareness) and activities.

In this environment, all resilient CPSs consist of two sub-systems: the proper resilient system and the situational awareness system that is the main prerequisite towards cybersecurity. In a system of CPSs, three networks are composed: platform, software and social network. Trust should be systematically built up at all layers. The resilient platform network is the basis on which the information sharing between different stakeholders could be created via software layers. However, the trust inside social networks quantifies the pieces of information that will be shared - and with whom.

The cyber resilience governance framework and design aspects for eHealth are based on recent settings of sociotechnical, cyber-physical, software-intensive and systems of systems in references [27,28]. The continuum of a design theory for resilient CPS can be a useful method for communities to share knowledge and best practices utilizing a common frame of reference, design and resilience aspects, cf. [28] and [18] and Figure 4.

According to this study, the term “resilience” in cyber domain would address to that a system is able to adapt to changing conditions based on run-time situational awareness, and a priori risk analysis when possible. Situational awareness (can be a software-intensive system itself) involves being aware of what is happening 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. Security technologies include all technical means towards cybersecurity, such as secure system architectures, protocols and implementation, as well as tools and platforms for secure system development and deployment.

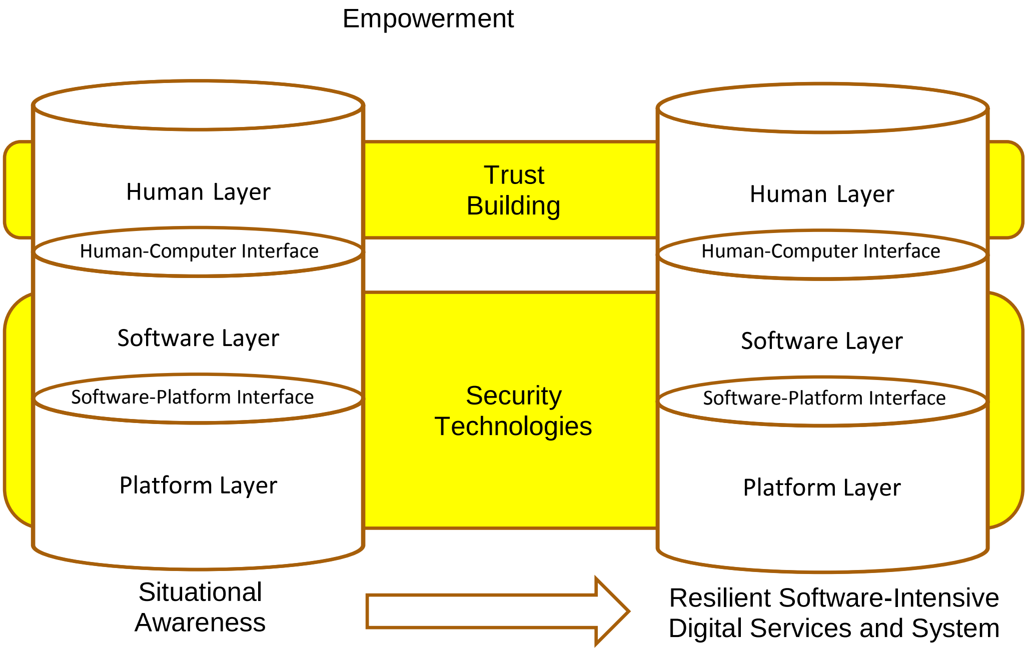

Figure 4. Conceptual resilience governance framework for eHealth CPSs.

Security management and governance covers the human, organizational and cognitive aspects of information security. Its focus areas include: Security policy development and implementation, and information security investment, incentives, and trade-offs. Information security management system (ISMS) focuses on 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. Cognitive aspects run around the framework; all technical and human components should learn from prior events and incidents, see [15,16,27,28].

Digital service driven progress brings opportunities across many sectors but also vulnerabilities to cyber-physical systems and related digital services. In the target scale of European-Global healthcare, there is a need for eHealth information nexus being one example of a safety-critical decision based networked system on cross-border secure and safe information exchange and common eHealth information sharing democracy and digital citizen's empowerment. In order to achieve the trust of users, measures of safety and security should be taken into consideration in line with the aspects of privacy by design and citizens' digital empowerment.

Discussion

From citizens' point of view, eHealth is wholeness in which sectors of information security (availability/confidentiality/integrity) hold true. Present procedures emphasize confidentiality at the expense of integrity and availability, and regulations/instructions are used as an excuse not to change even vital information. The mental-picture of cybersecurity should turn from "threat, crime, attack" to "trust". Creating confidence in safe digital future is truly needed in the integration of the digital and physical world's leading to a new digital revolution. The precondition for the exchange of information "trust" must be systematically built at every CPS' level (platform, software, people).

This research paper presents the conceptual resilience governance framework and design aspects for resilient cyber-physical eHealth systems (see figure 4). The digitalization and new better services require cooperation. The safety and security thinking has been based on to suppose that we are safe and we are able to prevent "bad touch", and the focus of actions has been the control of own systems, the improvement of the protection and staying inside the protection. However, nobody is able to control complex large integrated cyber-physical systems, but on the other hand, coordination and cooperation are needed. In eHealth, this means that the focus is moved from the control and securing of health information towards utilizing of eHealth to promote health, as shown in figure 5. A metaphor for not sharing health information for privacy protection risks is to forbid all people from outdoor activities at wintertime because a risk of slip. On the other hand, we have an urgent need to complement the existing knowledge-base of safety and risk management by developing frameworks and models enabling network-wide resilience management that strives for maintaining and improving critical functionalities.

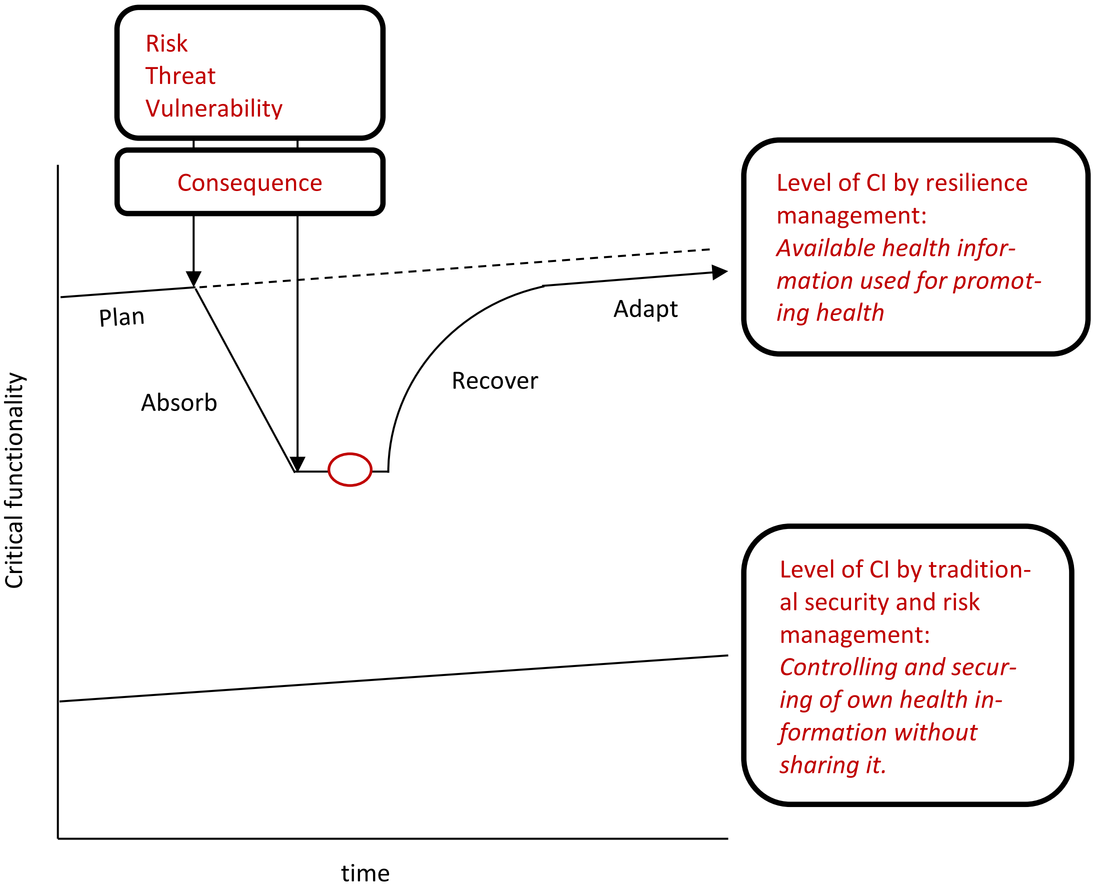
Risk
Threat
Vulnerability
Consequence
Level of CI by resilience management:
Available health information used for promoting health
Plan
Absorb
Recover
Adapt
Critical functionality
Level of CI by traditional security and risk management:
Controlling and securing of own health information without sharing it.
time

Figure 5. Resilience management of eHealth: Tool for promoting health.

Further research is needed for comprehensive mapping of existing cybersecurity initiatives, standards and frameworks across both the public and private sectors including transdisciplinary considerations. The aim should be to identify cybersecurity initiatives, standards and frameworks activities by investigating work that has already begun or been completed. The objective of the future study could be to identify areas with the best practices of effective cybersecurity solutions and matching with the capabilities of standardization and certifications.

The mapping will be further quantified as below:

1) Investigating and identifying the best cybersecurity initiative, standard and framework considering transdisciplinary approach. The mapping will be done in accordance with previous recommendations by CEN-CENELEC Focus Group on Cybersecurity (CSCG) considering beyond current state of the art.

2) Further studying the effectiveness and value of identified cybersecurity solutions and verifying with work already completed or ongoing across the Europe. The focus will be on protection effectiveness, compliance assurance and economic impact on a cross-sectoral basis.

3) Finally, the selection of standard and framework considering cross analysis and identification of existing effective practices. This will be a primary recommendation for creating cybersecurity metrics, indicators and cost-benefit framework during CEA project.

The goal of further research should be to increase harmonization of European cybersecurity initiatives and also reduce fragmented practices of cybersecurity solutions by validating with cybersecurity metrics, indicators and certifications.

References

[1] National Academy of Science and Engineering (DE), editor. Cyber-physical systems: driving force for innovations in mobility, health, energy and production. acatech POSITION PAPER, 2011 Dec. 44 p.

[2] Hevner A, March S, Park J, Ram S. Design science research in information systems. MIS Quarterly 2004 28(1):75-105.

[3] Hevner A, Chatterjee, S. Design research in information systems: theory and practice. New York: Springer Science and Business Media; 2010. 320 p. https://doi.org/10.1007/978-1-4419-5653-8

[4] National Training Standard for Information Systems Security (INFOSEC) Professionals. NSTISSI; 1994.

[5] Sahama T, Simpson L, Lane B. Security and Privacy in eHealth: Is it possible? In Proceedings of the 15th IEEE International Conference on e-Health Networking, Applications & Services (Healthcom). IEEE Conference Publications; 2013. p. 249-253.

[6] Liveri D, Sarri A, Skouloudi C. Security and Resilience in eHealth: Security Challenges and Risks. European Union Agency For Network And Information Security; 2015. 48 p.

[7] Kuusisto T, Kuusisto, R. Cyber world as a social system. In: Lehto M, Neittaanmäki P, editors. Cyber security: analytics, technology and automation. Springer International Publishing Switzerland; 2015. p. 31-43. https://doi.org/10.1007/978-3-319-18302-2_2

[8] Ranke M, Carleton J. The Professionals' Perspective: Cyber Security in the DACH Region. Frost & Sullivan; 2015. 10 p.

[9] Wing P, Manadhata J. An attack surface metric. IEEE Transactions on Software Engineering 2011;37(3):371-386. https://doi.org/10.1109/TSE.2010.60

[10] Akhgar B, Brewster B, editors. Combatting cybercrime and cyberterrorism: challenges, trends and priorities. Springer; 2016.

[11] Armin J, Thompson B, Ariu D, Giacinto G, Roli F, Kijewski P. 2020 cybercrime economic costs: No measure no solution, In Proceedings of the 10th IEEE international conference on availability, reliability and security (ARES). IEEE Conference Publications; 2015. p. 701-710. https://doi.org/10.1109/ares.2015.56

[12] Simon H. The science of the artificial. Cambridge: MIT Press; 1978.

[13] Fiadeiro JL. Designing for software's social complexity. IEEE Computer 2007;40(1):34-39. https://doi.org/10.1109/MC.2007.16

[14] CEN and CENELEC response to the EC Public Consultation on the contractual public-private partnership and possible accompanying measures. CEN and CENELEC; 2016.

[15] Rajamäki J, Knuuttila J. Cyber security and trust: tools for multi-agency cooperation between public authorities. In Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2015). SCITEPRESS; 2015. p. 397-404. https://doi.org/10.5220/0005628803970404

[16] Rajamäki J. Cyber security, trust-building, and trust-management: as tools for multi-agency cooperation within the functions vital to society. In: Clark R, Hakim S, editors. Cyber-physical security: protecting critical infrastructure. Springer; 2016. p. 233-249.

[17] Linkov I, Bridges T, Creutzig F, et al. Changing the resilience paradigm. Nature Climat Change 2014;4(6):407-409.
https://doi.org/10.1038/nclimate2227

[18] Disaster resilience: a national imperative. National Academy of Sciences (US); 2012.

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

[20] Linkov I, Eisenberg D, Plourde K, et al. Resilience metrics for cyber systems. Environment Systems and Decisions 2013;33(4):471-476. https://doi.org/10.1007/s10669-013-9485-y

[21] Abdelzaher T, Kott A. Resiliency and robustness of complex systems and networks. Adaptive, Dynamic and Resilient Systems 2013;67:67-86.

[22] Corbin J, Strauss A. Basics of qualitative research: techniques and procedures for developing grounded theory. 3 ed. Los Angeles: Sage Publications; 2008.

[23] Robson C. Real world research. 2 ed. Oxford: Blackwell Publishing; 2001.

[24] Miles M, Huberman A. Qualitative data analysis: an expanded sourcebook. Thousand Oaks: Sage Publications; 1994.

[25] Yin R. Case study research design and methods. 4th ed. Thousand Oaks: Saga Publications; 2009.

[26] Herr K, Anderson G. The action research dissertation: a guide for students and faculty. Thousand Oaks: Sage Publications; 2005. https://doi.org/10.4135/9781452226644

[27] Rajamäki J. Towards a design theory for resilient (sociotechnical, cyber-physical, software-intensive and systems of) systems. In: Zhuang X. Recent advances in information science. WSEAS Press; 2016. p. 29-34.

[28] Rajamäki J, Pirinen R. Critical infrastructure protection: towards a design theory for resilient software-intensive systems. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC). IEEE Conference Publications; 2015. p. 184.