Educational Competences With Regard to Critical Infrastructure Protection

Jyri Rajamäki[1,2] and Harri Ruoslahti[1, 2]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]University of Jyväskylä, Finland
jyri.rajamäki@laurea.fi
harri.ruoslahti@laurea.fi

Abstract: Current critical infrastructures can be considered cyber-physical systems (CPS). CPS are a subset of sociotechnical systems that provide seamless integration between computational, human and physical elements. The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient: 1) Self-modify/Plan/Prepare, 2) Absorb, 3) Recover, and 4) Adapt and learn. The Network-Centric Warfare doctrine identifies four domains that create shared situational awareness and inform decentralized decision-making: 1) Physical, 2) Information, 3) Cognitive, 4) Social. The research data of our case study is collected from authentic research and development projects (n=16) from three Finnish universities. Results indicate that future competences with regard to CPS are multidisciplinary including many industrial sectors and academic disciplines as well as multiple theories. Designing new curriculums and educational needs with regard to CPS, could benefit from the design science research (DSR) framework from Hevner and Chatterjee (2010). We have exploited the DSR framework for mapping future educational needs with regard to CPS and relevant industrial sectors and academic disciplines should be included. This paper argues that CPS education should, in all cases, cover both the four CPS domains (physical, information, cognitive and social) as well as all event management cycles (plan/prepare, absorb, recover and adapt). Traditional safety and security thinking has been based on the supposition that we can focus our actions in controlling our own systems and to stay inside a “circle of protection”. Thus, multi-stakeholder coordination and cooperation are needed, as no one actor alone can control complex large integrated cyber-physical systems of critical infrastructure. The focus of CPS education should thus also focus on cooperation and information sharing between the different different stakeholders. This is the way to promote more resilient complex systems of systems. Students need frameworks and models that enable resilience management across the entire network to maintain and improve critical functionalities.

Keywords: education, competences, resilience, cyber-physical systems, case study, learning by research and development

1. Introduction

Universities should teach what they research, and vice versa. The research and education field of new innovations, smart cities, critical infrastructures, internet of things and other cyber-physical systems (CPS) is multidisciplinary. Existing empirical research is characterized by a considerable degree of fragmentation among different research programs and different geographic regions in Europe. For example, 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 introduces both threats and opportunities, which are related to societal security, safety and resilience. Thus, we regard the concept to be of high societal importance. The research and education field of resilient cyber-physical systems, related to critical infrastructure, can still be seen to be in its infancy. The topic requires the development of new concepts, approaches and establishing multidisciplinary collaboration between research groups and stakeholders who rarely collaborate with each other. This further underlines the need for a multidisciplinary network to pave the way for future research efforts on resilient CPS. An educational approach, including new programs and tools that support learning both technological and business skills should be opened to students.

In this case study, the main research question is: How can future educational competences with regard to resilient cyber-physical systems be understood? The data for the case study is collected from authentic research and development projects.

The paper is structured as follows: After the introduction, the literature review deals with resilient CPS. Section three covers the major methodologies applied in the study modules as well as the applied research data. Section four presents CPS related research and development projects carried out by students. Section five states cross-case conclusions about the work made by students, and discusses the results. Finally, section five proposes a framework and an overall picture of the future educational competences with regard to CPS.

2. Literature review

CPS, a subset of sociotechnical systems, demonstrate seamless integration between computational, human and physical elements (Broy & Geisberger, 2011) as shown in Figure 1. Interconnections between social and technical subsystems, and encompassing a variety of linear and non-linear relationships, is referred to by the term 'sociotechnical' (Singapore-ETH Centre, 2015). CPS transform the ways in, which we live and interact with things in the physical world. The rate of this transformation is unprecedented in the history of mankind. The technological impacts of CPS and resilience are evident in many fields, including healthcare (Rajamäki & Pirinen, 2017), disaster management (Dahlberg, et al., 2015) and engineering resiliece (Park et al, 2013).

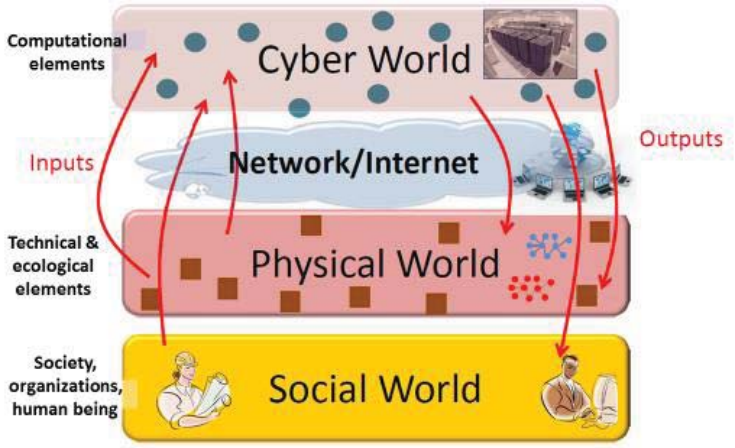

Figure 1: Cyber-physical social systems (modified from Murakami, 2012)

The critical infrastructure of our society, such as energy and water production, transportation, cyber, and communication, typically lack resilience. They may easilily lose essential functionality, if hit by adverse events (Linkov et al, 2014). The National Academy of Sciences (2012) identifies four event management cycles, which a system will need to maintain to be resilient): 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 assets, functions and services availabe to isolate, and while repelling the disruption. 3) Recover: restore availability of all assets, functions and service to their pre-event functionality. 4) Adapt: Use knowledge from the event to alter protocol, configuration of the system, personnel training, or other aspects for better functionality or to become more resilient (National Research Council, 2012). For a self-organising system, The Future Resilience Systems research programme (Singapore-ETH Centre, 2015) named these events (starting from the shock point): 1) absorb, 2) recover, 3) adapt & learn, and 4) self-modify, as shown in Figure 2.

Management strategies for any network of critical infrastructure (e.g., telecommunications, electricity, or transportation) may rely on the functionality other networks. All these networks could be considered being part of an overall system of systems. Thus, resilience can be enhanced by studying and improving the interconnectivity of these relevant networks. Enhancing surrounding social networks is also an important component of societal resilience. (Linkov et al, 2014). According to Amir and Kant (2018) sociotechnical systems, are intentional hybrids of people and technologies, and they involve complex interactions between people, organizations, and technologies. These authors propose that, during times of crisis, resilience of sociotechnical systems, can be understood through 1) informational relations, 2) structures of mutually entangled human organization and material structures, and 3) anticipatory practices.

The Network-Centric Warfare (NCW) doctrine (Alberts, 2002) identifies four domains that create shared situational awareness and inform decentralized decision-making; including: 1) Physical: the physical resources and the capabilities and the design of those resources; 2) Information: all information and information development about the physical domain; 3) Cognitive: how information and physical domains are used to make decisions; and 4) Social nexus: organizational structures and communication for making cognitive decisions. Linkov et al (2013) combined the event management cycles and these NCW domains to create resilience metrics for CPS.

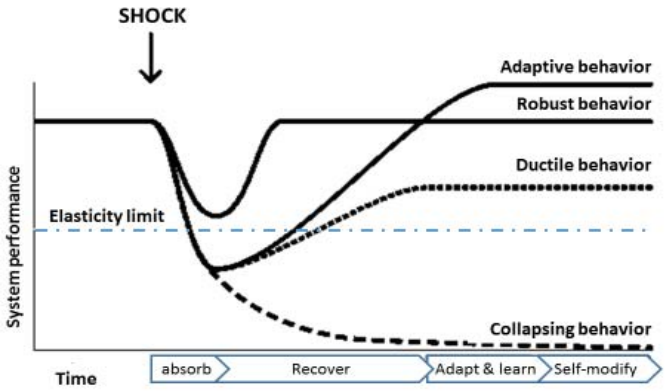

Figure 2: Resilience as response behaviour of a self-organising system to endogenous or exogenous shocks (modified from Singapore-ETH Centre, 2015)

3. Methodology and research data

In this case study, the research setting of the study addresses the following literature: "the case research strategy in studies of information systems" (Benbasat et al, 1987); "building theories from case study research" (Eisenhardt, 1989); "case studies and theory development in the social sciences" (George & Bennett, 2005); "qualitative data analysis" (Miles & Huberman, 1994); "real world research" (Robson, 2001); and "case study research design and methods" (Yin, 2009). Figure 3 presents the research methodology applied in this paper. The research data is collected from authentic research and development projects (n = 16), which wereperformed in three Finnish universities. The data includes e.g. material from bachelor (n = 1), master (n = 53) and PhD level (n=5) students' studies, feedback questionnaire answers from students (n = 53) and feedback from the supervisors (n=3) of R&D projects. All 16 projects studied resilience of cyber-physical systems, and students made the main part of the research work in most projects. In most cases, the target was a critical infrastructure or a function vital to society. The R&D projects cover seven different types of cyber-physical systems, which are shown in Table 1. Table 1 also informs the reference if the study is considered later in this paper or published somewhere else. The next chapter describes some major findings of these projects and lessons learned from them.

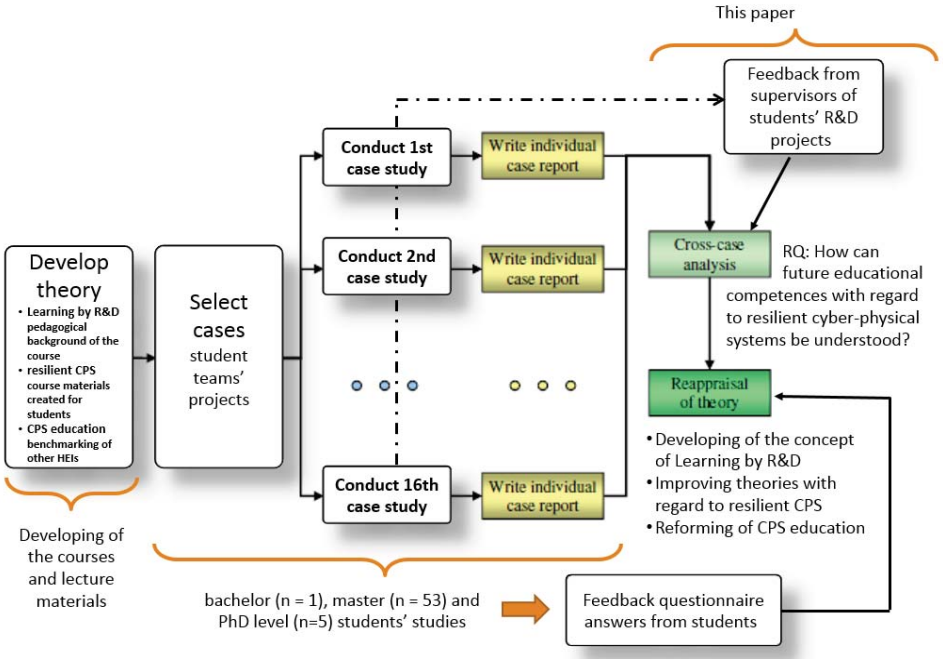

Figure 3: Research methodoly applied within this paper (modified from Yin, 2009)

Table 1: Relevent fields of critical infrastructure industry

Critical infrastructure	Reference
1. Energy supply: Regional Eeectricity generation company Finnish electricity grid syste Smart grid	(Pöyhönen et al, 2018)
2. Communication and information sharing environments: Finnish telecommunications system TUVE - State security communications network CISE - Information sharing systems on the Maritime Domain KRIVAT - Information Sharing Network between Critical Infrastructure Companies	 Section 4.1 Section 4.2
3. Air transportation: Smart airport Airplane Aviation cyber security Air-traffic control	
4. Road transportation: Smart cars Tesla pilot	
5. Finance: Verifone sales connector	 (Rajamäki, 2018)
6. Food supply: Finnish food supply system as a CPS	 Section 4.3
7. Living: Smart homes	

4. Descriptions and lessons learned from student R&D projects

4.1 CISE - information sharing systems on the maritime domain

While the plan/prepare phase creates a basis for the ability to absorb and recover from a disruptive incident, the adapt phase creates a feedback loop to enhance future plan/prepare phases. In this way the process becomes cyclical. This principle is also known in Business Continuity Planning literature (Woodman, 2007), (Savage, 2002). Ruoslahti and Tikanmäki (2017) raise the issue that technical systems, such as the Common Information Sharing Environment (CISE) initiative by the European Union, need structured and shared frameworks of content to base their human processes of operation on. In this example the physical are the information and communications system components, the information are objects and phenomenon, which are shared, the cognitive are the common principles in which way they are shared, and the social the organizational structures of the CISE network, and all its participating authorities and the shared communication between them.

CISE can thus, be seen as a platform of active participation and open collaboration between authorities (Ruoslahti & Tikanmäki, 2017). Active stakeholder participation requires common aims. An important foundation for open cooperation is openly shared information, which in turn requires collaborative co-creative processes and information sharing. Thus, the value networks, which aim at co-creation, need stakeholder participation, which in turn needs active facilitation, and relevant tools and platforms to foster open collaboration and information sharing sharing (Ruoslahti, 2018).

There are many frameworks of collaboration to bring together the many dispersed authorities on the different European maritime fields. They all have needs to exchange information directly within and with each other. Maritime Situational Awareness is constantly shared between these participating parties. This benefits maritime safety, rescue, assistance, environmental protection, security, and law enforcement, while providing resilience in shared actions. Continuity of operations are enhanced when different authorities have the capability and interoperability to supplement and, when needed fill in for each other (Tikanmäki & Ruoslahti, 2017; Ruoslahti & Hyttinen, 2016).

There has been work done in several EU-wide (PERSEUS, CoopP, EUCISE2020, and MARISA, and national (such as FINCISE) projects on information sharing on the maritime domain, which, the authors argue, should be continued and elaborated. These projects show the importance of sharing information both cross-sector and

nationally between different authorities; and cross-border between authorities from different EU member states; and also with cooperative third country authorities. Anomaly detection, classification, threat assessment, to alert operators are key to classify the threats, evaluate their seriousness, and predict possible impacts, and to gain a Common Operational Picture between all these different contributors (Ruoslahti & Tikanmäki, 2017).

When we dare to add more complexity, to what is now just network collaboration, we may find the potential of reaching deeper forms of co-creation (Ruoslahti & Tikanmäki, 2017), and faster innovation. In this case substantially faster detection, assessment, planning, and response are reached for increased system resilience on all four levels physical, information, cognitive, and social. It can be argued that increased collaboration will affect the depth of planning, the abilities to absorb and recover, as well as the ability to adapt, or learn together.

4.2 KRIVAT - information sharing network between critical infrastructure companies

The KRIVAT service of the State Security Networks Group Finland is an example of an information sharing and cooperation framework, which is specifically designed for the management of disturbances and continuity of critical infrastructure operations. It thus, exists to specifically enhance the preparedness of critical infrastructure. KRIVAT is a framework for action and its main purpose is to supplement the existing preparedness and disturbance management activities of critical infrastructure operators during major disturbances. It responds to a recognized need for clearer communications structures and better situation awareness between organizations for disturbance management (Koski, 2015).

Once any one threat meets vulnerability and has the capability to cause a consequence, it may be considered a risk (Linkov et al, 2014). Crisis management enables an organization to sustain and resume operations, minimizing financial losses to stakeholders, and leading to learning on how to better manage future incidents (Pearson & Clair, 1998). The KRIVAT concept involves organizations from various sectors to, when encountering disturbances or crisis, take needed actions together. Thus, critical infrastructure operators and their support organizations have a shared system for real-time information exchange between these organizations when incidents occur.

KRIVAT works to reduce damage caused by major disturbances, first by aiding in the planning and preparation for disturbances, and second by speeding up recovery processes when these disturbances do occur. KRIVAT also brings enhanced coordination of resources between organizations, increases information sharing, and provides better situational awareness. Shared situational awareness, interoperability, open communication, and shared crisis management add to preparedness and, thus to the overall resilience of participating critical infrastructure operators.

Under normal conditions, the organizations in the KRIVAT network may compete with one another on the marketplace. Therefore it is not natural for them to exchange operational information between them. However, facilitating open information sharing is key to the KRIVAT community. This is why all KRIVAT member organizations sign an agreement of mutual aid. This agreement has rules for both information exchange between the organizations and for the treatment of information. To make information exchange as clear as possible, a traffic light protocol is used to classify non-public information. This is to identify optimal levels of interoperability between organizations, because unclear communication responsibilities cause problems.

Successful crisis management efforts enable an organization to first sustain and then resume its operations, to minimize losses, and to adapt to manage future incidents (Linkov et al, 2013). Effective response to disturbances, and collaboration during them depend heavily on shared situation awareness. Exercises were found to be useful in activating users to share, train, and keep active. KRIVAT and its systems remain mostly unused between disturbances. Thus training exercises help users remember KRIVAT as their preferred option to respond to a live crisis. Where time is of the essence, falling back on possible old routines may not be as efficient a timely and innovative response.

4.3 Finnish food supply system as a CPS

The food supply chain ranges from agriculture and other primary production, through refining to distributing foods, and it is one of the most important basic functions of society, as it secures food for all its citizens. Its aim is to secure that the entire population, can in all conditions, get sufficient nourishment that corresponds to

normal conditions. The national agricultural production is the central foundation of the food supply. Attempts to increase crop farming should be made, production of high energy crops, e.g. corn. increased, and domestic animal production refocused. For example, pig, poultry and fur farming should be reduced, because they feed on suitable human foods, such as corn, potato and fish.

Legistlation and national regulations instruct general principles for preparedness, and any alterations to normal operations and irregular actions are based on government decisions, which in turn are based on objectives for the security of supply. These decisions define that adequate food supplies be secured under all circumstances. Maintaining certainty of an adequate food supply is a vital function of society.

During unusual conditions, the production equipment capacity of standard times are supplemented by different reserve supplies of foods, and by available production equipment. There are also intervention warehouses, which are controlled by the European Union.

The food supply chain is very vulnerable and dependent on other critical infrastructures, such as energy, transportation, finance and communications. To nourish the population during unusual conditions, the entire food supply must be examined to prepare the logistic chains that are needed during disturbances. Two main objectives are first, to secure adequate agricultural production and second, to make sure that food industry has sufficient refining capacity. Functional distribution systems for food from industry, through trade and up to the consumer must be examined andhe operations of retail and group eating food distribution networks secured.

Information systems direct the physical devices, which food production is based on. One example is the tractor manufacturing company John Deere. They tried to prevent independent maintenance of farm machines manufactured by them and closed the software that controls their machines. This resulted in hackering tools being marketed to the field of agriculture (Koebler, 2017).

The food safety system in Finland is systematically prepared against different threats, and considered to be at a high level internationally. Both the safety of foods and informing consumers are regulated and supervised by both national authorities and the actors responsible for the production. Some challenges in the future will be climate change and risks brought by population development. Possible shortcomings may be, among others, the loss of clean drinking water and any intentional endangering of food safety.

5. Cross-case analysis and discussion

5.1 Environment and industrial sectors

Event management cycles (self-modify/plan/prepare, absorb, recover and adapt&learn) should be taken into account in relation to CPS, which are composed from cyber, technical, social and ecological systems. Known best practices of CPS and historical experiences from the critical infrastrucure sectors (communications, energy supply, food supply, finance, etc.) affect the design and maintainance of resilient CPS. According to the student case studies, most CPS are very complex and interconnected. Thus, the characteristics and experiences from many different industry sectors should be considered simultaneously.

Complexity within networks may be greatest in multi-stakeholder co-creation, where stakeholder roles are fluid and constantly changing. Co-creation networks aiming at value, knowledge, and innovation, require active stakeholder participation, which is best achieved through common aims that promise benefits for every concerned stakeholder. Open collaboration should benefit the aims of each innovation network stakeholder. Innovation projects and open innovation environments, such as CISE and KRIVAT, are examples of CPS frameworks that facilitate communication and interaction between network stakeholders. CPS in critical infrastructure and vital fuctions, and related education, should take this into account the fluidity of stakeholder roles and their need for common goals in designing facilitation activities (Ruoslahti, 2018).

One example is that so far there are no scientific methods available that could precisely predict major weather phenomena, such as the long-term evolution and spatial distribution of tropical cyclones, atmospheric blockages or extratropical storm surges; nor are the impacts on society's infrastructure in any way quantified (Linkov et al, 2014). Because of these unknowns, building resilience becomes the optimal course of action for large cyber-physical systems that manage society's critical infrastructure and vital functions.

5.2 Knowledge base and academic disciplines

The theoretical perspectives of critical infrastructure related CPS include socio-technical systems (STS) theory, which is based on insights derived from a multitude of fields ranging from human-machine interaction, risk management, history of technology, philosophy of technology, science and technology studies and systems engineering. The physical domain of CPS means technology-focused social-ecological systems; resilience domains (physical, information, cognitive and social) as well as all event management cycles (plan/prepare, absorb, recover and adapt).

The theoretical background of the cyber domain of CPS can be derived from the science of design for software-intensive systems (Hevner & Chatterjee, 2010) including software design theories (building artifacts, evaluating artifacts, artifact behaviors, artifact qualities, representations, utility theories), dynamic system theories (control theories, emergent behaviors, emergent qualities, adaptive design theories, real-time systems), socio-economic theories (human cognitive abilities, social and group behaviors, human-computer interaction, economic theories, market forces), and domain theories (laws, rules and constraints of the application domain), as well as a multi-actor communication approach (engagement of many very diverse actors, who may have very diverse aims), and co-creation of knowledge and innovation.

5.3 Pedagogy

CPS covers nearly all industrial sectors and academic disciplines. Thus, the history and focus of the discipline in question, together with the best practices of relevant industrial sectors, should be taken into account, when designing new curriculums and educational needs with regard to CPS in critical infrastructure. Learning together increases the speed and ability to adapt, and it may even facilitate the creation of innovations. Increased interaction and collaboration between the stakeholders of critical infrastructure can result in deeper more encompassing planning. This in turn can enhance a system's and a system of system's ability to absorb and recover. Thus, learning to understand collaboration frameworks, modes of co-creation, such as the co-creation cycle (Ruoslahti, 2018), help leaders of tomorrow add resilience to their businesses and the whole of society.

Our case study indicates that future competences with regard to CPS are multidisciplinary. Many industrial sectors and theories from multiple academic disciplines can be included in academic research, applied development, and education. The design science research (DSR) framework (Hevner & Chatterjee, 2010) can be applied to designing new curriculums and educational needs with regard to CPS. Figure 4 summaries the research findings of this paper. It demonstrates how the DSR framework was applied to map future CPS related educational needs. These became demonstrated in the research projects of this case study.

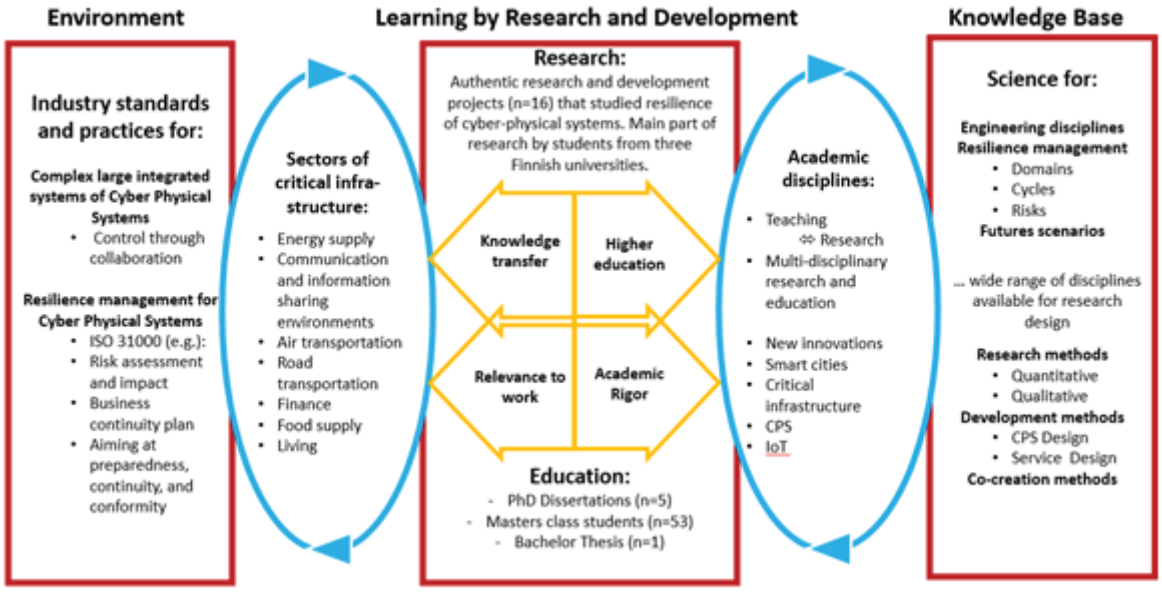

Figure 4: Future educational competencies applied from case studies on cyber-physical systems

Open and clear information exchange between the network of organizations reponsible for critical infrastructure with CPS is key in handling crisis and recovering from disturbances. Knowledge of communication theory and

practical skills, and modes of promoting interoperability between organizations should be a focus in the higher education programs that aim to address resilience. In addition, understanding how to build and maintain shared situational awareness is important to be included. It is needed to effectively respond to disturbances and collaborate effectively.

Models such as Learning by R&D (Pirinen, 2011; Pirinen, 2017)) or Learning by Developing (Laurea University of Applied Sciences, 2011), (Hyttinen et al, 2017) can be adopted to integrate learning and R&D related to critical infrastructure and cyber-physical systems. The structure of the Learning by R&D model, for example, is easy to adapt and renew, when change or turbulence occurs. It can develop from within or produce interactions, adaptions, resilience and innovations.

6. Conclusions

When designing CPS education, relevant industrial sectors and academic disciplines should be selected and focused on so that they complement eachother (see Figure 4). In any case CPS education should cover all resilience domains (physical, information, cognitive and social) as well as all event management cycles (plan/prepare, absorb, recover and adapt).

Academic knowledge bases are a good place to begin, when designing research or education related to resilience of critical infrastucture. Many academic disciplines can be applied. Some important disciplines are engineering, resilience management, and future scenarios. The field of critical infrastructure is especially one that should focus on resilience and continuity of operations. Disruptions in operations affect many and in some cases the entire society. Thus securing the operations of critical infrastructure operators – be they public or private – is cruical for the functioning of society.

Some industrial fields that are critical to society are energy supply, communication and information sharing environments, air transportation, road transportation, finance, food supply, and living. All these fields of industry are increasingly CPS in nature. The fields of critical infrastructure use resilience practices and business continuty planning, such as ISO 31000:2018, standards that guide their planning and preparedness. Risk assessment, business impact analysis, and business continuity planning are commonly used by these industries.

Teaching and research should find a clear tie between knowledge base and R&D needs. Knowledge base provides the theory and methods on which to ground applied R&D activities. These activities serve to provide a context for practical learning. Including stakeholders from the environment using co-creative methods provides genuine user input and relevance to work.

When integrating learning with Research and Development three roles were identified: 1) who integrates learning development objectives with research and development activities (responsible teacher), 2) who integrates teaching with research and development activities (teacher preparing lecture materials), and who integrates learning with research and development activities (student).

Complience with the requirements set by the different critical infrastrucure industrial secors and need to provide a baseline for resilience of CPS, and related systems of systems. The focus of security actions have traditionally been to control one's own system, improving its protection, staying inside a circle of protection, because safety and security thinking has been based on the supposition that we can prevent risks and are able to prevent "bad touch". However, no one alone is able to fully control complex large integrated cyber-physical systems; coordination and cooperation are needed, and these need to be tought in higher education.

The focus of CPS education should shift from controlling and securing one's own data to collaboration and information sharing between the different stakeholders. This way more resilient complex systems of systems can be promoted. Existing safety and risk management knowledge-base should be complemented by developing frameworks and models that enable network-wide resilience management to maintain and improve critical functionalities.

References

Alberts, D. (2002) *Information age transformation, getting to a 21st century military*, Defense Technical Information Center, Fort Belvoir.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987) "The case research strategy in studies of information systems", *MIS Quarterly*, Vol 11, No. 3, pp 369–386.

Broy, M. and Geisberger, E. (2011) *Cyber-physical systems, driving force for innovation in mobility, health, energy and production*, Acatech: The National Academy Of Science and Engineering, Munich.

Dahlberg, R., Johannessen-Henry, C., Raju, E. and Tulsiani, S. (2015) "Resilience in disaster research: Three versions", *Civil Engineering and Environmental Systems*, pp 44–54.

Eisenhardt, K. (1989) "Building theories from case study research", *Academy of Management Review*, Vol 14, pp 532–550.

George, L. and Bennett, A. (2005) *Case studies and theory development in the social sciences*, MIT Press, Massachusetts.

Hevner, A. and Chatterjee, S. (2010) *Design research in information systems: theory and practice,* Springer Science and Business Media, New York.

Hyttinen, K., Ruoslahti, H. and Jokela, J. (2017) "Model for Effective Integration between Research, Work Life and Higher Education in International Security Studies", *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, Vol 3, pp 299–306.

Koebler, J. (2017) "Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware", [online], Motherboard, https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware.

Koski, E. (2015) "Building Organisational Interoperability and Situation Awareness for Crisis Management – The KRIVAT Framework", [online], Theseus, https://www.theseus.fi/handle/10024/101656.

Laurea University of Applied Sciences (2011) "Learning by Developing. LbD Guide", [online] https://www.laurea.fi/en/document/Documents/LbD_Guide_04102011_ENG.pdf.

Lave, J. and Wenger, E. (2009) *Situated learning: Legitimate peripheral participation,* University Press, Cambridge.

Linkov, I. et al (2014) "Changing the resilience paradigm", *Nature Climate Change*, Vol 4, pp 407–409.

Linkov, I. et al (2013) "Resilience metrics for cyber systems", *Environment Systems and Decisions*, Vol 33, No. 4, pp 471–476.

Miles, M. and Huberman, A. (1994) *Qualitative data analysis: an expanded sourcebook*. Sage Publications, Thousand Oaks.

Murakami, K. J. (2012) "CPSS (Cyber-physical-social systems) initiative - Beyond CPS (Cyber-physical systems) for a better future", [online], Grid Consortium Japan, http://www.jpgrid.org/event/2011/ws34_murakami.pdf.

National Research Council (2012) *Disaster Resilience: A National Imperative,* The National Academies Press, Washington, DC.

Park, J. et al (2013) "Integrating risk and resilience approaches to catastrophe management in engineering systems" *Risk Analysis*, Vol 33, No. 3, pp 356–267.

Pearson, C. and Clair, J. (1998) "Reframing Crisis Management" *Academy of Management Review*, Vol 23, No. 1, pp 59–76.

Pirinen, R. (2011) "Externally Funded Research and Development Projects in Perspective of Learning", *International Journal of Engineering Pedagogy*, Vol 3, pp 27–36.

Pirinen, R. (2017) "Resilient Learning: Towards Integration of Strategic Research Programmes", *International Journal of Engineering Pedagogy*, Vol 7, No. 2, pp 94–108.

Pöyhönen, J., Nuojua, V., Lehto, M. and Rajamäki, J. (2018) "Application of Cyber Resilience Review to an Electricity Company", *ECCWS 2018*, Academic Conferences and Publishing International Limited, Sonning Common, [In Press].

Rajamäki, J. (2018) "Industry-University Collaboration on IoT Cyber Security Education. Academic Course: 'Resilience of Internet of Things and Cyber-Physical Systems'", *IEEE Global Engineering Education Conference (EDUCON)*, [In Press].

Rajamäki, J. and Pirinen, R. (2017) Design science research towards resilient cyber-physical eHealth systems. *Finnish Journal of eHealth and eWelfare*, Vol 9, No. 2–3, pp 203–216.

Robson, C. (2001) *Real world research*, Blackwell Publishing, Oxford.

Ruoslahti, H. (2018) "Co-creation of Knowledge for Innovation and Multi-Stakeholder Participation of End Users: A Structured Literature Review", European Public Relations Education and Research Association (EUPRERA), [In Press].

Ruoslahti, H. and Hyttinen, K. (2016) "A Co-created Network Community for Knowledge and Innovations – Promoting Safety and Security in the Arctic", *Proceedings of the 23rd International Public Relations Research Symposium BledCom,* Faculty of Social Sciences, Ljubljana, pp 100–106.

Ruoslahti, H. and Tikanmäki, I. (2017) "End-Users Co-create Shared Information for a More Complete Real-time Maritime Picture". *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, Vol 3, pp 267–274.

Savage, M. (2002) "Business continuity planning", *Work Study*, Vol 51, No. 5, pp 254–261.

Singapore-ETH Centre (2015) "Future Resilient Systems", [Online], https://www.ethz.ch/content/dam/ethz/special-interest/dual/frs-dam/documents/FRS-Booklet.pdf.

Tikanmäki, I. and Ruoslahti, H. (2017) "Increasing Cooperation between the European Maritime Domain Authorities", *International Journal of Environmental Science*, Vol 2, pp 392–399.

Woodman, P. (2007) *Business Continuity Management,* Chartered Management Institute, London.

Yin, R. (2009) *Case study research design and methods*. Sage Publications, Thousand Oaks.