Cyber physical system security Roadmap

Interreg Aurora: Project WP1

Mike Mekkanen, Tero Vartainen: University of Vaasa Finland
Chen-Wei Yang, Valeriy Vyatkin: Luleå University Sweden

May-2024

Contents

1 Introduction

The roadmap aims to create a wealth of insight and vision of modern critical infrastructures by the coming decade and to produce a development path on cyber-physical system security in critical infrastructures. With an emphasis on Interreg Aurora region, our focus is on digital smart critical infrastructures (CI) such as electricity networks and associated services businesses. Furthermore, there is a strong emphasis on explaining the growing interaction between different CIs operation layers and associated emerging technologies. These interactions and innovative technologies are fostering the expansion and cyberization of the smart energy sector. The roadmap implementation consisted of interviews, starting with background checks, and the final selection of candidates. Development of interview's protocol that consisted of compilation of excitation material (number of questions). In number of interviewed candidates from Interreg Aurora area, active experts in the widely represented industry provided valuable insights and vision for developing the roadmap.

CIs are undergoing a major transformation by interring the digital era through combining the digital and physical worlds. This transformation brings cybersecurity vulnerabilities that need proactive and protective protection to mitigate the impact of different incidents such as failures or cyber-attacks. In this context, the efforts to improve the modern CIs resiliency and reliability will require significant changes in the technology, tools and methods used in the existing CIs networks. Were the obscurity of the transformed CIs, in turn, affects daily life activities, society and economy by providing critical services such as manufacturing, transportation, healthcare delivery, utilities, energy production etc. An exceptionally significant impact on the entire society occurred by the accidental failure or attacks to the CIs in which that may lead to stop or entrapped these critical services provided by the CIs.

The challenges can be tackled with the help of the options that the security and risk management decision-makers must update upgrade existing security management's initiatives to include CPS security and using new technological methods and tools. The development of the CIs business models and regulation enables the efficient and profitable operation of the parties to the entire CIs networks. A reliable resilient and sustainable CI

is achieved through a comprehensive security management initiative that includes CPS security. Achieving the goal requires supporting both the technological development of the CI OT network and the securing of the application of IT network through different parties' cooperation, investments programs for both networks and regulations.

The roadmap for a CI system resiliency developed in the project consists of three principal areas of development, all of which support the security and risk management of CI in an intelligent system and consider crisis preparedness, these areas are:

- CI hardware OT system and networks interfaces
- IT Network Technology System Solutions
- Data, automation, and data management

2 Critical Infrastructure

Modern CIs are transformed to complex Cyber-physical systems, which combine the digital and physical worlds, but also bring cybersecurity vulnerabilities that need proactive protective measures to mitigate the impact of different incidents such as failures or cyber-attacks. Cyber-physical systems bring together two different systems i.e., digital, and physical worlds, eco-system. However, when these systems connect to one another and interact with other CIs systems, the overall attack surface grows significantly. These CIs systems can take many different forms, supporting daily life activities, society, and economy by providing critical services such as manufacturing, transportation, healthcare delivery, utilities [1] etc., as illustrated in Fig 1. These critical roles make them attractive targets for attackers attempting to demand ransomware payments to prevent shutdowns.

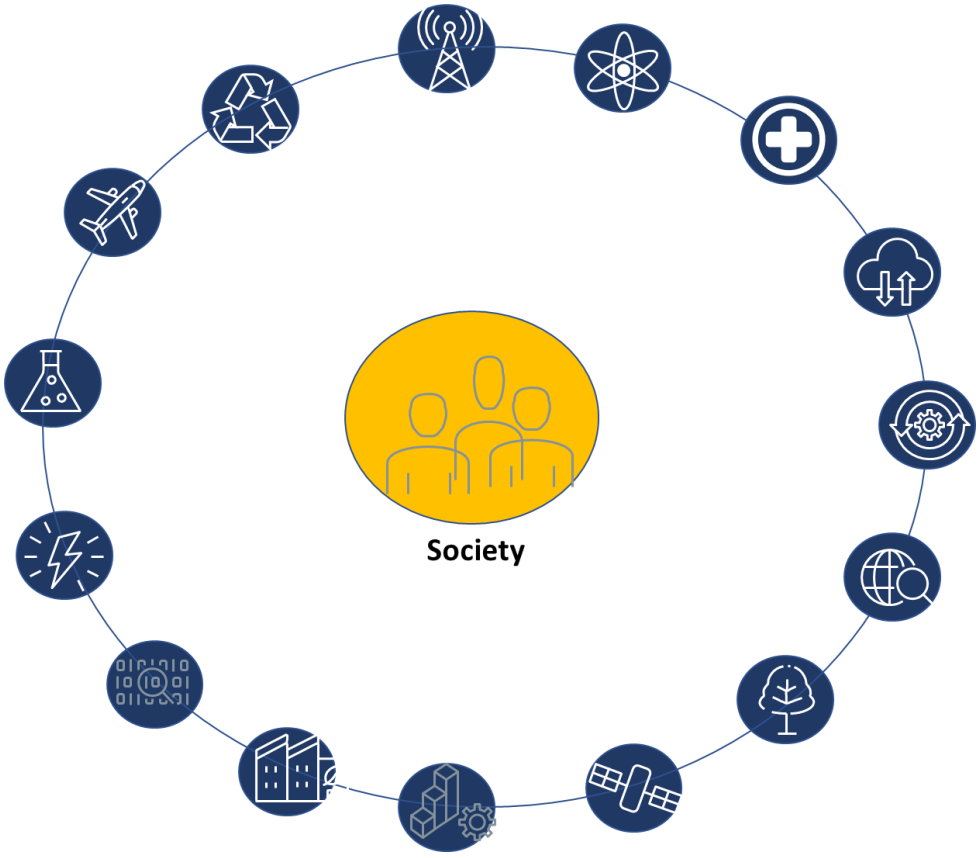

Figure 1: Critical Infrastructure sectors

In this context, security and risk management decision-makers must update existing security management's initiatives to include CPS security. This upgrading security and risk management necessitates more resources and effort, which presents barriers. They should include the CPS risk management and security strategy since existing cybersecurity solutions such as firewalls, antivirus, etc., are no longer sufficient to secure the CIs. Where CIs security, risk managements are extending beyond traditional IT systems and cyber-physical attacks become much more sophisticated and challenging, in which that drawing inspiration from industry leaders' best practices.

Because of the CIs changing landscape, there is a need for a CIs security roadmap with broad focus on (IT and OT) systems. in WP1 we develop a roadmap for critical infrastructures stakeholders, operators, sub-operators, services providers, vendors, prosumers for coming decade, to raise the cyber-physical system CPS security awareness, understand the existing security landscape for CPS, develop security countermeasure, safeguard and improving CIs system resiliency. We focused on Interreg Aurora area.

The roadmap development process starts by developing an interview protocol with a set of questions. The questions are:

- What kind of cyberattacks have you experienced in your organization or in your business line? Please, describe.
- What kind of vulnerabilities are there in your systems or in the systems of your business line?
- What could be the motivations behind the attacks on these systems?
- What kind of damage or harm the attacks could cause?
- What areas of cybersecurity should be developed from your viewpoint and the viewpoint of the whole sector

3 Resilient attributes

Resilience is ‘‘The persistence of service delivery that can justifiably be trusted, when facing changes’’, [2]. Resilience should be the primary strategy for maintaining business continuity. If something goes wrong, which it unconsciously will—a cyberattack, a failure, a storm, a fire, etc.—there will be a way to absorb, recover and deal with the situation as soon as it occurs. Work through it, respond to it, and then, once the incident has been resolved, proceed to update, restart components/sub-systems, possibly adjust, validate, modify your cyber system and engineering responses, take lessons from the past, and resume regular operations. Organizations with high preparation resilience and with a dynamic capabilities' strategy can quickly "self" adjust to internal and external disruptive events such as failure or crisis, guaranteeing a continuous service. To this point in [3] that has defined dependability as the set of qualities that includes availability, reliability, safety, and maintainability. Were because confidentiality, integrity, and availability make up security. It is stated that robustness is an additional quality of reliability. Were as the system's resilient attribute, which enumerates the predefined attributes [3], shown in Fig 2.

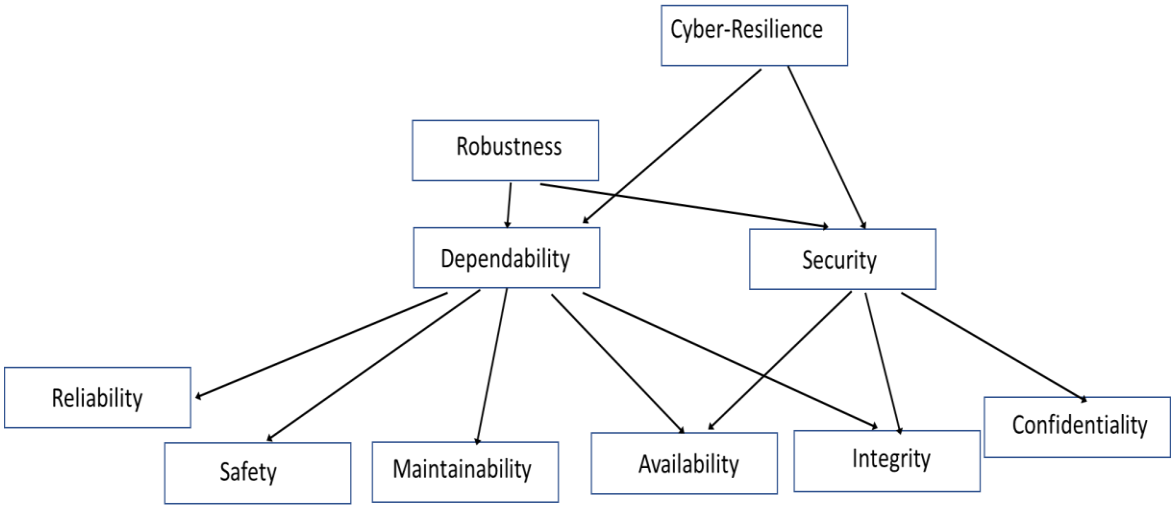

Figure 2: Resilient Attribute, Cyber resilience include all kind of fault plus cyber attacks

4 National Institute of Standards and Technology NIST framework

NIST provides the first edition of the guidelines for organizations to adopt to mitigate risks and build organizational resilience in 2014. This Framework consists of five key functions that represent the overall strategic point view of managing cybersecurity risk as illustrated in Fig 3.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 3: NIST Framework [4]

The Framework five key functions are as follows; *Identify*: Gain the organizational knowledge necessary to control the risk of cybersecurity to assets, capabilities, data, and systems. *Protect*: Create and put into place the necessary counter measures to guarantee the provision of essential infrastructure services. *Detect*: develop a mechanism to detect and carry out the necessary actions to determine when a cybersecurity event oc-

curs. *Respond*: Develop and execute the necessary actions based on protective and proactive measures to respond to a cybersecurity event that has been detected. *Recover*: Develop and execute out the necessary actions to maintain resilience strategies and isolate/restore any services or capabilities (dynamic capabilities) that were hampered by a cybersecurity incident, learn from the past event, and prevent it from occurrence in future.

5 Towards the Roadmap

The evolving complexity and interdependencies among different CI systems and services necessitates the need for efficient security and resilience. These services are essential to national security, business continuity, and public safety to continue and be reliable. To this context, protection and safeguarding these services is essential. Thus, there are several factors are arising for effective CPS security and resilience need to be addressed and understood, as follows;

- Understanding and built-in knowledge of the CI assets and their security posture in which that allows to effectively evaluate, identify and prioritize the required optimization steps.
- Understanding of CI operation and define their risk vectors, security counter-measures metrics
- Methods and tools for evaluating conditions of security in real time as well as analytically to assist in risk management decision-making
- CI operators must establish self-assessment and autonomous correction operations applying assigned tools and procedures.
- Real-time security state monitoring tools that link to the self-assessment and autonomous operation activates for self-healing actions, while allowing the operators to override them, if necessary
- Cyber environments would benefit from additional knowledge gained from threats that have been identified and resolved to prevent recurrences in future.
- Modelling and simulation tools for system and threat modeling in real-time to test and assess the holistic CI monitoring, detecting and protection systems.
- critical infrastructure subsectors could likewise profit from real-time monitoring and protection due their coherent interdependences
- Additionally, promoting awareness, fostering a security culture, and providing ongoing professional training should receive special focus.

Roadmap for Cyber physical system security

From the interviews and the aforementioned sections the roadmap is developed for coming decade. This roadmap aims to produce a wealth of insight and wild clear development path for critical infrastructures stakeholders and decision-makers to improve CIs resiliency. This task will be achieved by requiring of supporting both the technological development of the CI OT network and the securing of the application of IT network. In which that may also require different party's cooperation, investments programs for both networks and updating policies, regulations and define responsibilities. The roadmap development is also follow the NIST recommendation frame work, as illustrated in Fig 4.

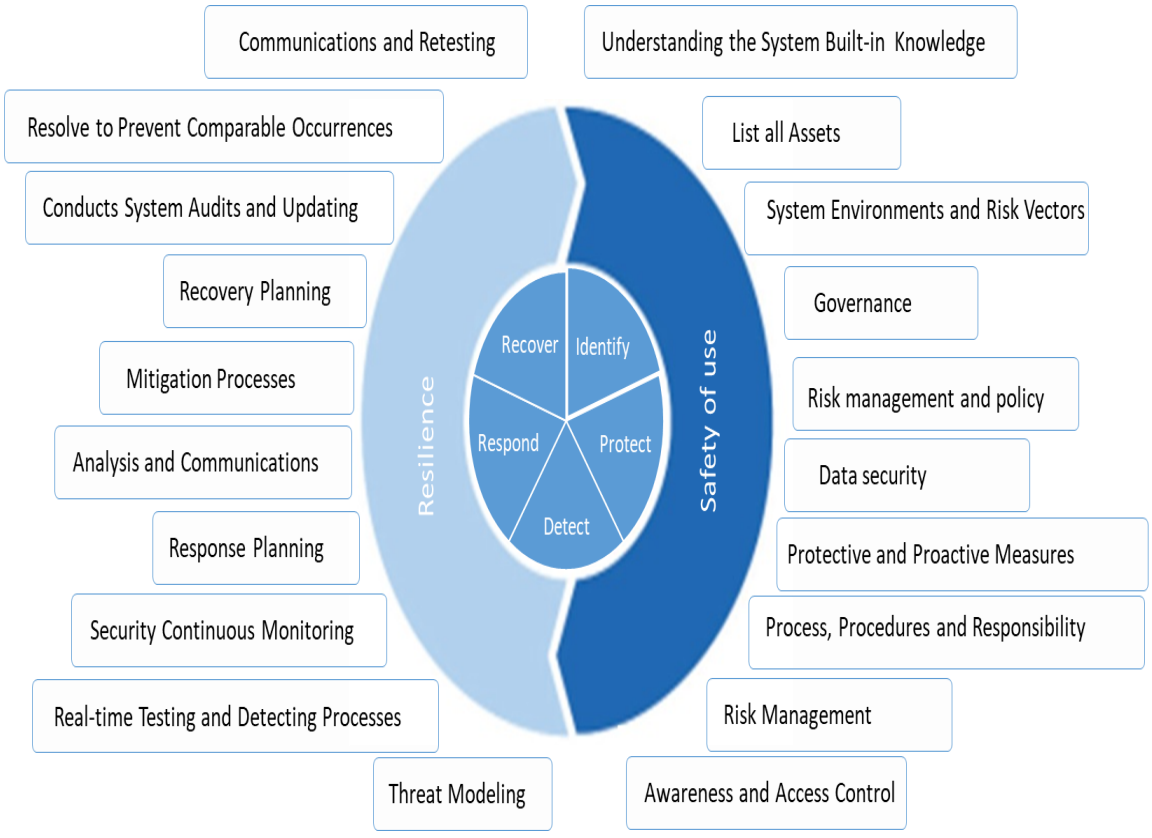

Figure 4: Roadmap for Cyber physical system security

References

[1] https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure

[2] J.-C. Laprie, ‘‘From dependability to resilience,’ in Proc. 38th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN), Jun. 2008, pp. G8–G9.

[3] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, ‘‘Basic concepts and taxonomy of dependable and secure computing,’’ IEEE Trans Dependable Secure Compute., vol.1, no. 1, pp. 11–33, Jan./Mar. 2004

[4] NIST Framework, available [Online], https://www.nist.gov/