A Qualitative Risk Identification Framework for Cyber-Physical-Social Systems

Sindisiwe Magutshwa
Department of Information Systems
University of Agder
sindisiwe.magutshwa@uia.no

Jaziar Radianti
Department of Information Systems
University of Agder
jaziar.radianti@uia.no

ABSTRACT

As information and communication technologies, real-world physical systems, and people become interconnected in critical infrastructure, attention has shifted to the operations of Cyber-Physical-Social Systems (CPSS). CPSS are progressively integrated in core critical infrastructure organisational processes to achieve a combination of benefits. However, the high degree of integration of technology into human society and mission-critical processes leads to an increase in complexity and introduces novel risks and vulnerabilities. These novel constraints extend beyond what is known from previous cyber-physical and critical infrastructure systems studies and prompt the need for revised risk perception and identification methodologies. This paper aims to develop a novel qualitative risk identification framework that is used in the identification of risk and vulnerability in CPSS ecosystems deployed in critical infrastructure or mission-critical organisational processes. The framework emphasizes interactions between humans and the system making it possible to identify and understand how non-technical risk impacts the CPSS ecosystem.

Keywords

Cyber physical systems, cyber-physical-social systems, social processes, risk, vulnerability, mission-critical.

INTRODUCTION

Advancement in the digitalization of most critical infrastructure (CI) sectors has created ecosystems comprising various critical operations. In the early developments, CI operations integrated cyber and physical elements into their rather complicated background processes, referred to as cyber-physical systems (CPS). CPS combined the capabilities of interacting computational components and networks of physical systems. These combinations are popularly adopted in industrial process control systems, national power grids and smart traffic control (Yilma et al., 2018). The introduction of CPS further complicated CI operations, making them complex two-layer architecture systems that existed in the cyber and physical terrain.

While human actors have always been central to CPS ecosystems, there is a shift in the management of these integrated systems – through the coordination of closely coupled human and machine actors. In such systems, people progressively work closely alongside sensor enabled smart devices, machines, control systems, and robots to complete processes and operations. Personalized healthcare, emergency response, traffic management, transport, and smart manufacturing are examples of sectors where we observe these changes (Dey et al., 2018). The end goal of adopting the smart systems into the foreground of 'social contexts' vary, ranging from introducing new functionalities, to technological advancements leading to efficiency, convenience, personalized service, improved quality of life for users (Wang & Rong, 2009). These smart systems, characterized by the engineered networking of human or social, computational, and physical components are known as Cyber-Physical-Social Systems (CPSS). Human actors are known to be prominent components in the CPS, however, in CPSS environments, they are particularly centralised in the management of CI operations introducing levels of dependence and uncertainty. This necessitates efforts in exploring and understanding how this close coupling of human-machine components may lead to novel risks and system exposure emanating from human behaviour.

Generally, CPSS can be considered a fusion of social systems with cyber-physical systems. Social systems play a prominent role in CPSS, often incorporating interaction with expert and non-expert users. CPSS are popularly embedded into CI sectors such as healthcare, transport, and emergency response., but are also deployed in other application domains, such as a business or organisational setting. Recently, CPSS are incorporated into the critical functions of an organisation such as in decision making, monitoring services, control of organisational processes, and supply chain management. Critical functions are core to achieve the objectives of the organisation. Therefore, any processes that are linked to the delivery of critical functions are 'mission-critical' processes (JTFTI, 2011).

CPSS do present a potential for varying degrees of heightened efficiency, sustainability, and scalability in core organisational processes. For this potential to be realized, customized technological developments, policy, control, and security methods need to be implemented (Frazzon et al., 2013). Unfortunately, due to their complexity and qualitative dissimilarity of the system components (social, physical, and computational), CPSS are widely affected by novel risk, vulnerability, and security threats (Wang & Rong, 2009). CPSS may face security breaches in cases where the people, processes, technology, and other components are compromised. In case of incident, an understanding of the human induced risks, organizational risks and the intertwined nature of the two risks types are important for efficient response to such failures associated with CI and CPSS environments. Questions often arise regarding the nature of the human-organisational relationships that may occur in a CPSS and how they may compound the risk and vulnerabilities that pose a threat to the CPSS.

In CPSS, risk identification is somewhat complicated by the qualitative dissimilarity of the system components, the challenges encountered in CPSS ecosystems are unique. However, existing research related to the risk in CPSS mainly considers CPSS as purely technical systems and provides abstractions from this perspective, focusing on the system architecture layer (Bou-Harb, 2016; Gharib et al., 2017). Therefore, the social system issues such as cognitive behaviour, and human error are often overlooked. Indeed, numerous works examine and propose human risk assessment frameworks (Cacciabue, 2000; Kirwan, 1998a, 1998b), especially in the safety engineering domain, or organizational risk frameworks, especially in the information security management domain (Sebescen & Vitak, 2017; Singh et al., 2014). However, studies that examine the human and organizational-wide risk frameworks in the context of CPSS in CI organisations are still rare. This will be the main contribution of this work.

Hence, the aim of this paper is threefold: First, to provide an overview, of how CPSS are gradually adopted and deployed in an organization´s 'mission-critical´ processes. Second, to understand the potential exposure to novel organization wide and human factor risks and the interactions between these two factors. Third, to propose a qualitative evaluation framework for use in the risk identification process to analyse CPSS ecosystems through the organization-wide risk approach. The ultimate goal is that this framework will fill existing gaps and facilitate the understanding of the CPSS ecosystem dynamics through the decomposition of CPSS into easily identifiable components that are essential from a security risk perspective and how they interact. This framework will serve as an enabler for anticipating and taking comprehensive corrective actions that minimize risk in the social, computational, and physical system layers of the CPSS. This paper is an exploratory attempt to apply the organizational processes into CPSS ecosystems. The research question is: **In what way can a qualitative organizational risk approach to CPSS analysis provide useful insights into CPSS risk assessment approaches?**

The methodological approach of the paper is conceptual, incorporating interrelated literature analyses and drawing further on empirical illustrations. The next section discusses the origins and understanding of CPSS. The 'Previous Studies' section follows where insights from existing works serve as basis for shaping the conceptual reflections in the paper. In later sections, a risk identification framework is developed and applied to empirical illustrations. This is done using secondary data sources through profiling of two cases of CI compromise related to the transportation, and health sectors. The scenarios show the potential and relevance of CPSS usage in mission-critical processes in CI sectors. The rest of the paper is a brief discussion on the Contributions and Limitations of this research work followed by the Conclusion and Future Research Section

ORIGINS, UNDERSTANDING, AND DEFINITION OF CPSS

The origins of CPSS can be traced back to cyber-physical systems (CPS). CPS are 4th industrial revolution smart systems that include the engineered networking of physical and computational components, i.e., information and communication technologies, software, hardware, and data. The physical elements may be any combination of machines, electronic devices, and industrial plants. CPS are characterized as a 'system of systems', often supporting cross domain applications (Lee, 2006; Wang & Rong, 2009).

Typically, CPS harvest data from the environments through use of interconnected devices such as sensors. They bear a potential impact on the physical world due to this connectedness and it is a common cause for concern on their trustworthiness (Gharib et al., 2017; Gunes et al., 2014). As mentioned earlier, CPSS emerges from the further integration of CPS into social systems. In social systems, CPS include interacting individuals that act as a part of the systems and have their own "cognition, preferences, motivation and behaviour" (Zhou et al., 2019). Zhu and Milanović (2020), define CPSS as "a system deployed with emphasis on humans, knowledge, society and culture in addition to cyber and physical space. It connects nature, cyber-space, and society with certain rules". Figure 1 is an illustration of the concept of CPSS seen through a three-layer architecture with two aspects of integration, the cyber-social and cyber-physical.

The concept of CPSS is somewhat new, and therefore in the literature, a variety of terms are used to describe the integration of human aspects into CPS operations. Frazzon et al. (2013), propose "Socio-Cyber-Physical Systems", highlighting the social aspects of CPS and showing how context-dependent behavioural aspects bear impact on the system. Frazzon (2013) further describes that the technological elements are developed to provide support to the human actors in a production network CPS. "Cyber-physical Human System" is found the literature to describe systems of interconnected computers, cyber-physical devices, and people that allow other systems, people and data streams to connect and disconnect. It emphasizes the 'human connection' in the systems (Sowe et al. 2016; Kumar et al. 2017). In another term, "Social Cyber-Physical Systems", are described as complex socio-technical systems in which humans and technical aspects (CPS) are massively intertwined" (Xu et al, 2018).

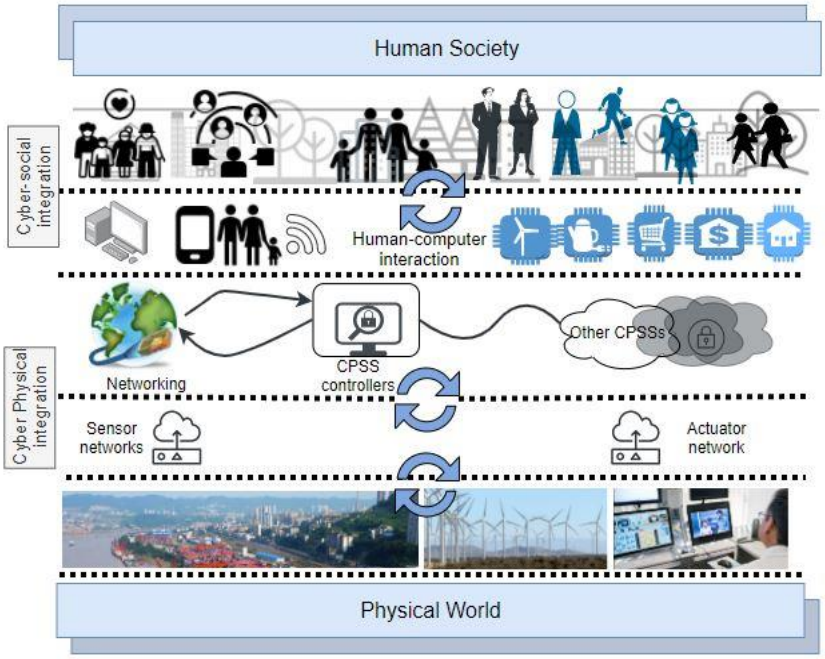


Figure 1: CPSS Architecture (adapted from Zhou, 2019)

The highlighted terms capture notions of CPSS in varying degrees, exploring different paradigms and abstractions of the influence of human aspects such as culture, motivation, and cognitive limitations based on the application domain of the system under study. The essence captured in the reviewed literature is the dependence on equal prominence of both cyber-social and cyber-physical integration elements in the smart environments (Zhou et al., 2019). A common trend across the various application domains is that CPSS require stability, robustness, security, reliability, and efficiency. Additionally, CPSS demand the cognitive interaction of humans with technological and industrial systems in the execution of organizational tasks and processes. This interaction introduces 'human behaviour', a rather complex dynamic aspect compared to the traditionally fully automated domain of CPS. Unlike machines, humans are prone to individuality and may not always follow rules that do not match their logic, needs or capabilities (Yilma et al., 2018). The quality of collaboration, linking the technical, physical, and social prospects determines the overall performance of the system (Frazzon et al., 2013).

The following subsection presents the different CPSS application domains as discussed in the literature. The essence captured in the reviewed literature is the dependence on equal prominence of both cyber-social and cyber-physical integration elements in the smart environments (Zhou et al., 2019).

PREVIOUS STUDIES

This section provides overview of two literatures, first, how CPSS are gradually adopted and deployed in an organization´s 'mission-critical´ processes, and second, on the potential exposure to novel organization-wide and human factor risks and the interactions between these two factors. The first literature selection is based on highly cited publications related to CPSS. It reveals the current discourse, application domains, and deployment of CPSS in engineering, computer science and information systems. The second analyses are based on a set of literature that discusses CPSS risk and threat identification or assessment methodologies from an organisational process viewpoint. It considers the associated risk perception and security recommendations. The aim is to uncover what the prevalent concerns are and potentially considering CPSS as a complex organisational process system in mission-critical

Extant literature on the CPSS paradigm describes it as an interdisciplinary subject area. The methods of investigation and interpretation tend to be aligned to the traditions of the research discipline under which the study is being conducted. This confinement to isolated research areas may be a limitation of sorts in different application fields due to the diversified nature of requirements and outcomes. Given the prominence of the human role, the majority of the studies assume user-centric views, yet in existing traditional design principles for CPSS the human aspect is not factored into the system architecture (Frazzon et al., 2013; Zhou et al., 2019). Much of the literature discussed in the first review reveals a bias to the technical aspects of CPSS, even when the human aspect is acknowledged. However, Frazzon et al. (2013) and Kirwan (1998a) provide compelling argument for research focusing on the 'human influence', highlighting that the efficiency of the resulting network depends on the capability to bridge technical differences and the culture induced behavioural differences among human actors. Given the prominence of the human role, it would be expected that the majority of the studies assume user-centric views, yet in existing traditional design principles for CPSS the human aspect is not factored into the system architecture (Frazzon et al., 2013; Zhou et al., 2019). Much of the literature discussed in the first review reveals a bias to the technical aspects of CPSS, even when the human aspect is acknowledged. However, Frazzon et al. (2013) and Zeng et al. (2020) provide compelling argument for research focusing on the 'human influence', highlighting that the efficiency of the resulting network depends on the capability to bridge technical differences and the culture induced behavioural differences among human actors.

CPSS in CI and Mission-critical Applications

As discussed in the introduction, CPSS has gradually been adopted in CI sectors and as a part of mission-critical organisational processes. *A mission-critical system or process* is "one in which a failure or interruption comes with intolerable operational or human cost. Examples of such costs may be information or research compromise, safety at risk, loss of data, and when critical business function is impacted (Skarin et al., 2018). CPSS is commonly integrated into transportation, energy, and healthcare. In health care, sensors have been deployed for clinical monitoring and rapid response in case of medical emergencies, which can be considered as a mission-critical process in order to deliver continuous health services to the public. Figure 2 shows a CPSS applied in remote patient monitoring, as an illustration of the CPSS in mission-critical application.

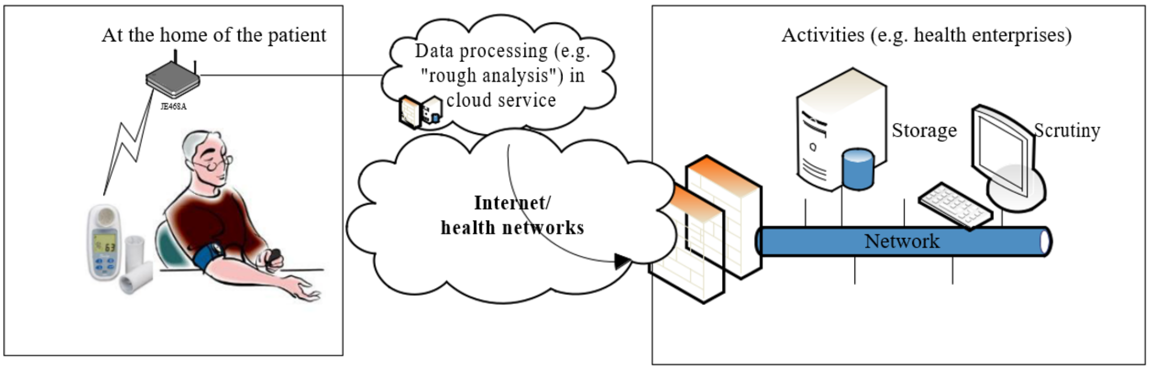

At the home of the patient
Data processing (e.g. "rough analysis") in cloud service
Activities (e.g. health enterprises)
Storage
Scrutiny
Internet/
health networks
Network

Figure 2: CPSS remote patient monitoring via cloud service (normen.no)

Such remote deployment of e-health services can induce more unknown threats and risks, triggered by a combination of vulnerabilities inherited in the technology and infrastructure itself, new ways of using it, and unpredicted behaviors of the patients when exposed to a new electronic service. This example highlights even more, why studies examining various aspects of human-induced risks in the CPSS system are becoming pressing needs, and motivate us to conduct this research.

The malfunctioning of the cyber elements (e.g., wearable health sensors) may lead to remote therapy disruption or even loss of life. In transport, vehicle-to-vehicle, and car-to-road communications to ensure safer automatic driving have become prevalent. They are mission-critical, because any malfunctioning sensors leas to a lack of situational awareness of road traffic, possibly leading to accidents. In energy, electricity grids and smart devices have been mounted on the grids to monitor power distribution, acquiring customer data and power consumption.

These are among mission-critical processes in electricity sectors. Of interest across the respective application domains revealed in literature is the "new relationships between physical and cyber components that entail new architectural models" (Dey 2018, Zhou 2019). Basically, a certain level of reliability, predictability and safety are required for the use of CPSS in CI sectors. Most discussions centre around the dynamic, decentralised, and changing ecosystem that CPSS create. The systems are repeatedly identified as complex socio-technical environments. It is argued that due to these CI sector applications, CPSS have acquired additional characteristics over ordinary CPS such as the awareness of users in social contexts. CPSS also possess an adaptability towards 'optimal collaboration' and accomplish the high levels of dependability (Dey et al., 2018; Frazzon et al., 2013).

The major challenges of CPSS are mainly related to security, safety, and reliability of the systems. It is repeatedly mentioned that to attain these goals and fully understand the CPSS ecosystem, improvements need to be made to computing abstractions, software development and physical processes. Further, research models need to be developed to reflect the revised properties of interest in CPSS (Bou-Harb, 2016; Dey et al., 2018; Gharib et al., 2017). Authors engage the system architecture (Yilma et al., 2018), application contexts, and resource management. Surprisingly, even though CPSS ecosystems are repeatedly identified as a part of critical function, little mention is made of the possibility to analyse CPSS from a process-oriented view, with a focus on mission-critical processes (Bou-Harb, 2016).

Risk Identification Perspectives, Frameworks, and Guidelines for CPSS

There are widely used and accepted risk management guidelines such as ISO 31000, IEC 31010, and NIST frameworks that outline suitable approaches to the different risk-related activities in CI and organisations. The NIST framework for improving CI cybersecurity (2018), emphasizes that there is no 'one size fits all' approach to managing cybersecurity risk in CI. There is need to customise practices described in a framework to reflect the unique needs of any CI operations. This implies that any framework should be flexible, and easily modifiable to suit different environments. The NIST framework provides a systematic approach to the identification, assessment, and management of security risk in CI. The framework also serves as a basis for novel security approaches, providing a basis for improved risk activities. In the case of CPSS in CI processes, the arrangement and organisation the elements are significant to risk related activities. A perspective of the system that reveals all the relationships for ensuring a comprehensive risk assessment outcome, with wide risk management approach can be seen in Figure 3, which stratifies the risk management process of any organisation into three tiers.

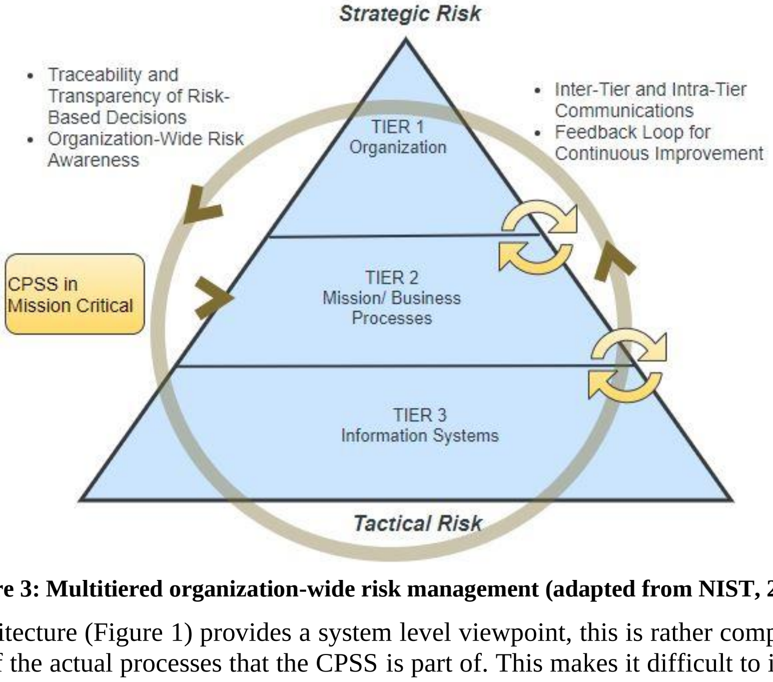

Strategic Risk
• Traceability and Transparency of Risk-Based Decisions
• Organization-Wide Risk Awareness
• Inter-Tier and Intra-Tier Communications
• Feedback Loop for Continuous Improvement
TIER 1
Organization
CPSS in Mission Critical
TIER 2
Mission/ Business Processes
TIER 3
Information Systems
Tactical Risk

Figure 3: Multitiered organization-wide risk management (adapted from NIST, 2011)

While the layered architecture (Figure 1) provides a system level viewpoint, this is rather complex and provides no conceptualisation of the actual processes that the CPSS is part of. This makes it difficult to identify the novel risk or vulnerability posed through the implementation of the CPSS within the organisation or CI. A possibly simpler viewpoint is proposed in the multi-tiered organisation-risk related activities are applied across all three tiers making it possible to identify strategic and tactical risk, overlaps and dependencies. Of particular interest to this paper is Tier 2. The description of the interconnection that exists between the mission/business process and the underlying technology that is implemented to execute the processes (JTFTI, 2011). The translation of a CPSS ecosystem within this framework would provide a process level view that enables the identification of novel risk and vulnerability.

Research Gaps and Potential Contributions

Yoneda et al. (2015), propose the Risk Breakdown Structure (RBS) approach for use in the extraction and analysis of risk for CPS in 'office' environments. The emphasis of the work is on information and physical security. Notably, to begin with, in the risk extraction phase, 'risk factors' are identified and classified into either 'physical threats' or 'information security threats. Identified risks such as virus infection, spoofing, and illegal copying are weighted and classified based on a quantitative scale that they refer to as the 'risk matrix method'. Based on the matrix, control measures such as regular anti-virus updates, secure authentication systems and illegal copy check tools are then determined. This is a quantitative evaluation method, and the approach captures the essence of system performance which is ideal for CPS environments. However, the initial RBS classification of possible risk only into two streams – physical and information security, only makes it partially applicable to CPSS, focusing on the physical and cyber aspects of the system. Singh and Jain (2018) suggest purely technical measures by looking at vulnerabilities in hardware, software, technical, network, platform, and management vulnerabilities. Risk is interpreted as the various types of attacks that can be made to the network. This is once again a quantitative approach with a strong weight towards the cyber and physical components of the operational environment.

The prior sections highlight the prevalent use of CPSS in critical sectors such as personalized health care and emergency management lead to an increase in cyberattacks on CPSS. While cybersecurity continues to focus on the cyber and physical tiers of the systems the risk has evolved and this is no longer enough to protect the systems (Zhou et al., 2019). Different techniques have been used to introduce human actors in CPS. The use of smart devices and the tight coupling to their users has led to the possibility of 'human sensors', instances where humans are the primary source of information for the system. The need for revised methodology that factors in the social aspects of the CPS has also been highlighted in several studies (Lee, 2006; Zeng et al., 2020; Zhou et al., 2019). The revision of the risk and vulnerability identification process as a preliminary step to wider revisions in the risk-related activities of operations would lead to a balanced, comprehensive process. The risk identification process is used to establish other risk-based activities such as assessment, response, and monitoring. It is the identification of the "assumptions, constraints, risk tolerances and priorities/trade-offs", and establishes effective communications and feedback loops for continuous improvement in the risk-related activities of an organisation. The identification and appropriate classification of human induced risk in a CPSS is a key component to the development of comprehensive risk decision making, ensuring that all three layers (cyber, physical, social) are factored in.

While general risk identification has been suggested in different frameworks, there is very little information on how CPS or CPSS human induced security risks should be assessed. In the areas of CIs, twenty tools and frameworks have been identified targeting various users ranging from operators, asset managers, CI operators to policy makers (Giannopoulos et al., 2012). Typically, an additional step is required before identifying risk source, i.e., identifying CI assets. There is a need for adaptations of previous frameworks to address the organization wide CPSS risk identification processes and highlight the prominent role of human actors and how this leads to novel risk. In short, the authors observe the following gaps in the literature:

- Research on the security of the cyber and physical layers of CPSS has a bias to the technical components (Kumar et al 2020). In fact, the nature of risk has evolved in current systems. Thus, methodological changes that provide more holistic approaches to human-induced risk related activities of CPSS are required.
- Some authors, e.g., Yoneda et al. (2015), Singh and Jain (2018) propose different risk management approaches for CPS that operate in 'social settings. However, the suggested methodologies are quantitative, have a technical bias in the risk identification processes. The exploration of risks emanating from human activity would require primarily qualitative approaches.
- Majority of the proposed risk frameworks emphasize the identification of vulnerabilities and risk at a system level. They lack emphasis on the notion of interdependencies and the possibility of cascading effect/ risk.
- Existing works provided rarely consider CI operations from an organisational process-oriented perspective, and as a result provide limited insight into why research is now obliged to consider human actors as essential components in the management of critical infrastructure.

Hence, the proposed framework is intended to fill the highlighted gaps. The novelty in this work is to offer a customizable qualitative risk identification approach in CPSS ecosystems that provides the possibility of understanding the relationship among the social, cyber, and physical layers of a given CPSS. We propose and inclusive and balanced perspective using the multi-tiered organisation wide risk management approach. This is important to tailor the technical and non-technical aspects within mission-critical processes.

METHODOLOGY

To address our research goals, we used a combination of qualitative research techniques. For the first and second research goal, a literature analysis was conducted. This was done to support the previously mentioned problem statement and clarify how CPSS has evolved and come to use in critical infrastructure organisations. This was a non-exhaustive literature search targeting studies that focus on specifically CPSS or CPS in CI organisations. We selected recent, highly cited publications that identify the prevailing understanding of CPSS to reveal the degree to which it has been adopted and deployed in mission-critical organisation processes. The literature search also targeted studies that focus on the perception of security risk in CPS and CPSS, specifically risk identification and assessment methodologies. The activities and findings related to these two goals are detailed under 'Previous Works: Problem Statement and Potential Contributions' sections of this paper.

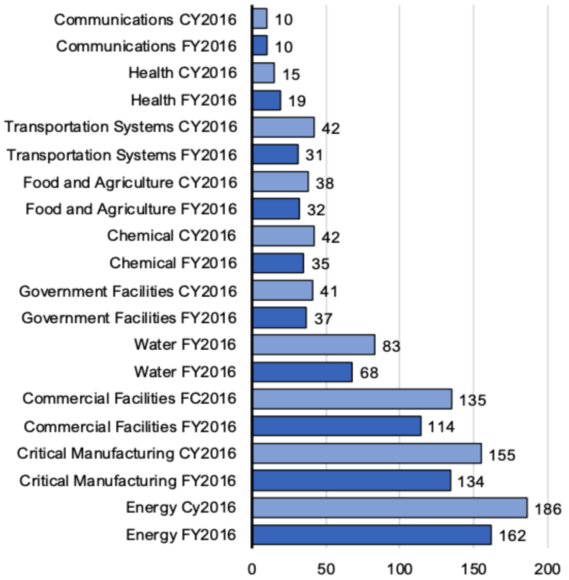


Figure 4: Vulnerabilities found in CI sectors 2016, with occurrences > 10

(Adapted from: ICS CERT Report, NCIC 2016)

To achieve the third research goal, the development of the so-called Qualitative Risk identification framework (Q-ID), the authors reviewed several models uncovered in the literature analyses that have been used by scholars to identify the risks and vulnerabilities in the CI and CPS systems and refined them to cover the various notions of risk in the CPSS, as a part of the mission-critical business processes (TIER2 as seen in Figure 3).

Furthermore, a qualitative evaluation is done to validate the proposed framework and demonstrate it can be applied satisfactorily to identify the novel risk and vulnerabilities of CPSS in mission-critical organisational processes. This is done through the identification of practical application scenarios and empirical illustrations, which have been selected, where the significance is supported through data. Over the years, CIs have been attractive targets for disempowering an organization or even a country. Figure 4 shows the vulnerabilities reported based on attacks occurred in Industrial Control System (ICS) in Fiscal Year (FY) and Calendar Year (CY) 2016, (NCCIC, 2016) as registered by the US ICS-CERT (Industrial Control System Computer Emergency Response Team), which is the core of cyber infrastructure. The statistical data shows that the vulnerabilities have been reported at least ten CI sectors, which include the transport and health sectors. Hence, we selected these two sectors for illustrating the applicability of Q-ID Framework, as two emerging sectors that recently are prompted by the prevalent use of CPS systems and sensor technologies for clinical management in the healthcare sector. The authors find this an interesting case of CPSS, that may provide greater insight due to the high degree of integration of the CPSS into human society (see Figure 1). ENISA Threat Landscape report on Main incidents in the EU and Worldwide has included Health Care attack as one of five the most targeted sectors (ENISA, 2020).

In brief, these two sectors - transport, and health are selected for further analysis and show the applicability of the risk identification framework from CPSS in mission-critical lens. The following section discusses the proposed framework, providing a justification for this qualitative risk identification framework and highlighting aspects in which the organisation-wide risk management approach leads to useful insights in CPSS risk analysis methodology.

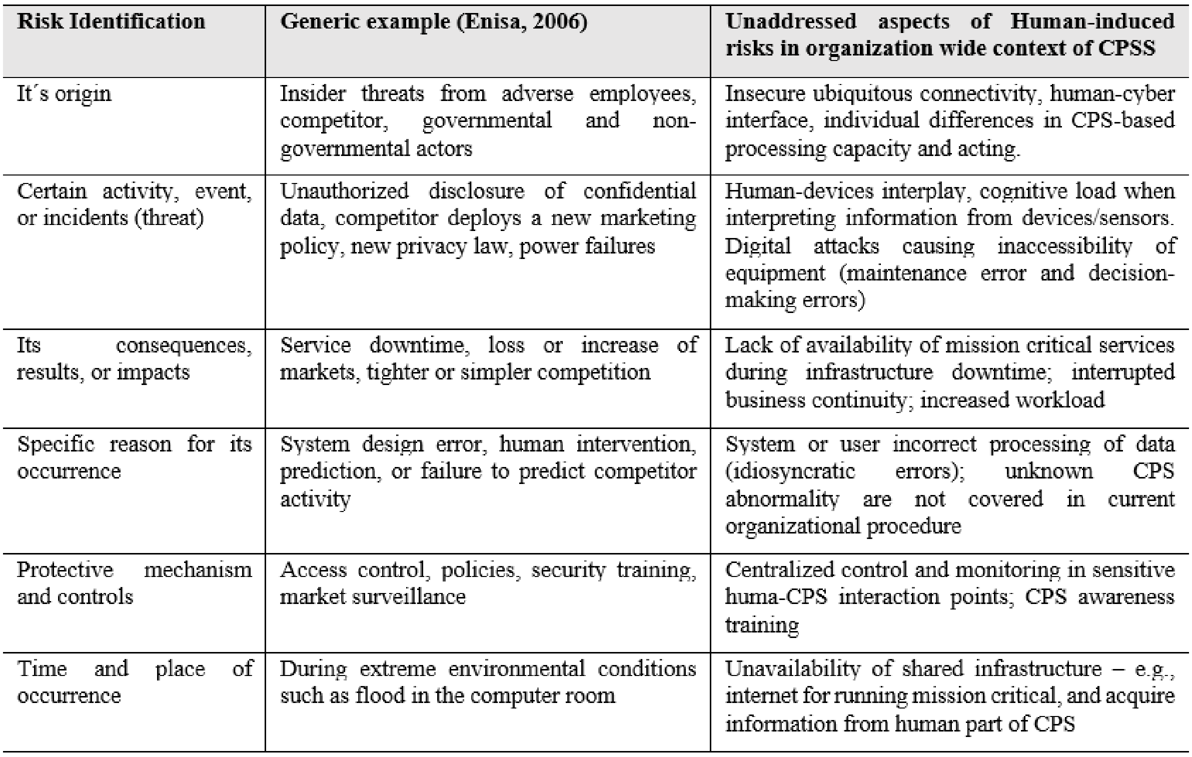
RESULTS: PROPOSED FRAMEWORK

Prior sections in this paper discuss how CPSS has a layered architecture comprising of various components, which are at times interdependent. We have also discussed how this key attribute of CPSS generates novel risk and vulnerability that highlight the need for revised methodology to facilitate the interoperability and manage the emerging effects of these changing ecosystems (Dey et al 2018). Various frameworks to identify risks or vulnerabilities in CPSS or CPS environments have also been discussed. Many of the studies emphasize the cyber components or physical components, and rarely investigate the social components, or consider CPSS deployed in CI organisations for mission-critical processes. There is a gap between existing risk identification and assessment methodologies and the current trends in CPSS ecosystems. The proposed framework considers CPSS to be an organisational process, that is deployed at various levels of an organisation to collectively achieve a particular aim or objective. The framework emphasizes the existence of relationships among the composite actors, assets, and stresses how the dynamics that exist among these elements may result in dependencies. This may lead to novel risk and vulnerability. This logic coincides with context-driven risk assessment approaches such as the OCTAVE method that motivates for identifying risk relative to business goals and key business assets (ENISA, 2006; Tweneboah-Koduah & Buchanan, 2018).

Prior sections in this paper discuss how CPSS has a layered architecture comprising of various components, which are at times interdependent. We have also discussed how this key attribute of CPSS generates novel risk and vulnerability that highlight the need for revised methodology to facilitate the interoperability and manage the emerging effects of these changing ecosystems (Dey et al 2018). Various frameworks to identify risks or vulnerabilities in CPSS or CPS environments have also been discussed. Many of the studies emphasize the cyber components or physical components, and rarely investigate the social components, or consider CPSS deployed in CI organisations for mission-critical processes.

The proposed framework considers multiple existing frameworks, and the primary objective of the proposed framework is to further contribute to and optimize the existing frameworks. Beyond the identified frameworks in the Previous Studies Section adopted by the researchers, there are numerous frameworks and standards for risk assessment such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (Octave) method, ISO standards such as ISO 27005 for information systems, ISO 31010 for IT Governance, and ISO 31000 for organizational wide (ENISA, 2006; Tweneboah-Koduah & Buchanan, 2018). Risk identification is a part of overall risk assessment process. Risk identification methodology can be done in several ways, including looking at the checklist, records, experience data and records. (ENISA, 2006) suggests that identification of risks can be related or characterized by the following steps outlined in Table 1, which is mostly focus on "cyber" domain. On the right column, we point out unaddressed issues when using this framework for organizational-wide context.

Table 1: Risk identification Methodology and examples of unaddressed aspects of organizational-wide context of CPSS



Risk Identification	Generic example (Enisa, 2006)	Unaddressed aspects of Human-induced risks in organization wide context of CPSS
It´s origin	Insider threats from adverse employees, competitor, governmental and non-governmental actors	Insecure ubiquitous connectivity, human-cyber interface, individual differences in CPS-based processing capacity and acting.
Certain activity, event, or incidents (threat)	Unauthorized disclosure of confidential data, competitor deploys a new marketing policy, new privacy law, power failures	Human-devices interplay, cognitive load when interpreting information from devices/sensors. Digital attacks causing inaccessibility of equipment (maintenance error and decision-making errors)
Its consequences, results, or impacts	Service downtime, loss or increase of markets, tighter or simpler competition	Lack of availability of mission critical services during infrastructure downtime; interrupted business continuity; increased workload
Specific reason for its occurrence	System design error, human intervention, prediction, or failure to predict competitor activity	System or user incorrect processing of data (idiosyncratic errors); unknown CPS abnormality are not covered in current organizational procedure
Protective mechanism and controls	Access control, policies, security training, market surveillance	Centralized control and monitoring in sensitive huma-CPS interaction points; CPS awareness training
Time and place of occurrence	During extreme environmental conditions such as flood in the computer room	Unavailability of shared infrastructure – e.g., internet for running mission critical, and acquire information from human part of CPS

CI organisations such as health, transport, energy, and water are known to be targets for malicious actors and face frequent cyber and physical attacks (Haque et al., 2014). The identification of technical and non-technical risks in mission-critical organisational processes is a prerequisite step to the assessment, and management of risks. The enhancement of existing frameworks, the novel components of the qualitative risk identification framework are:

Integration of the organisation-wide risk management model: The translation of the CPSS architecture into the organisation-wide risk management model is a means of attaining a greater level of visibility of the key processes and actors that comprise the system in the different tiers from an organisational perspective. This viewpoint provides an understanding of the security risks within the CPSS from each of the different layers – physical, cyber, and social. This approach allows for a smooth engagement of non-technical risks such as human behaviour during risk identification and may show how they are connected to or impact IT control gaps and vulnerability findings in the technical components of the system.

Identification and Classification of cross-functional risk from the organisational environment: in the qualitative risk identification framework the risk is understood to be cross-functional. Cross-functional risks are of a tactical and strategic nature (see Figure 3), this means they can present as technical risks – e.g., software, system complexity or non-technical risks – e.g., legal, environmental, or cognitive behaviour. People in the CPSS ecosystem work on different organizational processes that collectively generate a combination of strategic and tactical risks that affect the security and overall organisation objectives. The risk identification in the proposed framework comprises of a process tracing and risk mapping exercise. Unlike traditional risk identification frameworks, the proposed framework goes a step further in classifying the identified risk from the preceding step into human and technology induced risks. This approach provides improved appreciation for security or organisational objectives that are impacted by cross-functional risk or process-based vulnerability. An additional benefit of this exercise is the identification of mission-critical processes and the organisational resources (people or technology) that are tightly associated or linked to them.

Emphasis on the interaction between human and system alongside associated human risk in CPSS: the cyber-social integrations and human computer interactions highlighted earlier in Figure 1 give rise to novel vulnerabilities and threats. Among these being susceptibility to human error and the entailing risk. Examples of such human error are action execution errors, diagnostic/ decision making errors, and errors of commission (Kirwan, 1998a). The proposed framework provides a series of process tracing steps that make it possible to identify and understand how non-technical 'human risk' can affect the system.

A Qualitative Risk Identification Process Framework

The proposed framework is a useful addition to the risk assessment methodology of an organisation, preceding the actual risk assessment procedure. It is helpful for the identification, understanding, and communication of risk and vulnerability in a CPSS ecosystem, benefitting strategic risk identification mission-critical process researchers in an organisational or CI setting. Use of this framework provides clarity on the operational context, resources connected to critical function, and oversight on possible security risks. The framework considers CPSS as a multi-layer, organisation-wide system, this coincides with existing organisational risk methodologies that emphasize the need for equal tactical and strategic risk assessment. Figure 4 is a flow chart, outlining the objectives of each of the steps that are later incorporated into the proposed framework.

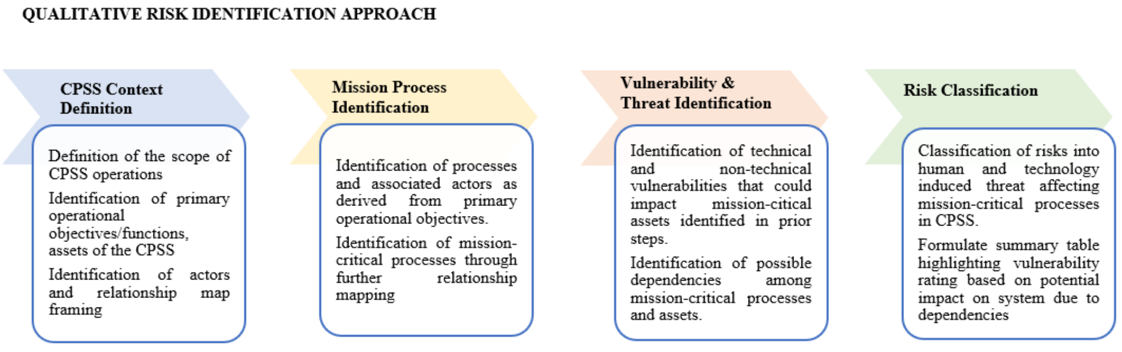

QUALITATIVE RISK IDENTIFICATION APPROACH
CPSS Context Definition
Definition of the scope of CPSS operations
Identification of primary operational objectives/functions, assets of the CPSS
Identification of actors and relationship map framing
Mission Process Identification
Identification of processes and associated actors as derived from primary operational objectives.
Identification of mission-critical processes through further relationship mapping
Vulnerability & Threat Identification
Identification of technical and non-technical vulnerabilities that could impact mission-citical assets identified in prior steps.
Identification of possible dependencies among mission-critical processes and assets.
Risk Classification
Classification of risks into human and technology induced threat affecting mission-critical processes in CPSS.
Formulate summary table highlighting vulnerability rating based on potential impact on system due to dependencies

Figure 5: Analysis of CPSS and derivation of Qualitative Risk Identification Approach

Modelling Concepts for use in Relationship Mapping

An aspect of the proposed Q-ID approach is the relationship mapping exercise carried out alongside other activities in steps 1 -3 of Figure 5. The relationship map informs the risk classification activity in step 4. The relationship map includes select modelling concepts that are necessary to illustrate, understand, and express security risk in qualitative terms. An overview of the concepts used in the proposed framework is discussed below.

Actors: an actor within the CPSS is a representation of humans that exist within the ecosystem in their respective roles. Actors are a part of the system operations and they are integrated into the system loop. Every actor that exists within the CPSS ecosystem has a purpose, for instance – data acquisition, information retrieval, user feedback or general action (Zhou et al., 2019). Actors are also linked to goals, the operational objectives, and functions of a CI organisation; they carry out tasks that lead to their goal achievement and the CPSS's operational objectives.

Goals: goals are the overall activities associated with an actor that support and are derived from a selection of the CI's operational functions. Goals are generally reflected in the outcome of the processes in which an actor participates. An example of goals in a CPSS may be tasks/processes that relate to confidentiality, integrity, and availability of patient data in healthcare service. The goals are linked to and determined by the information security objectives of the CPSS operation.

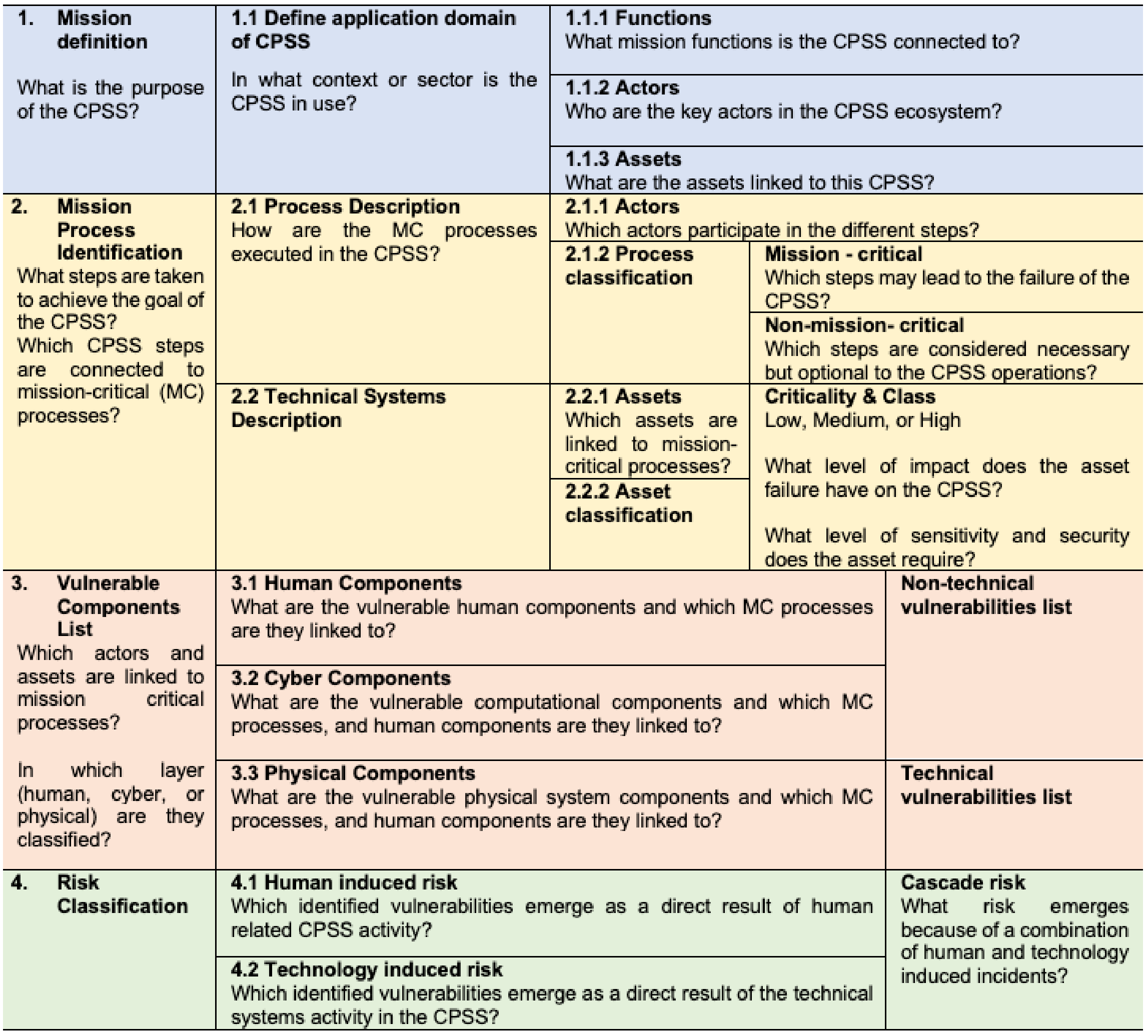
Risks: risk as discussed in QID is perceived to be the possibility of the occurrence of undesired outcomes due to unintended incidents or events. Risk poses a threat in various forms towards the attainment of a CI's operational objectives. Risk in the proposed framework is classified under security as technical and non-technical. The risk identification is based on qualitative methods, combining process tracing and relationship mapping exercises. This will facilitate the identification of mission-critical processes, the risks and vulnerabilities that threaten them.

Assets: in QID, assets are understood to be tangible entities that are necessary and of value to the CPSS operational objectives. The identification of key assets and the relationship they share with actors and processes in the CPSS is an important part of the risk identification activity. An asset is described using two main features in the framework, criticality, and class. **Class** is the determination of sensitivity of an asset and the level of security required to protect it. **Criticality** is defined as a 'measure of the consequences associated with the degradation or loss of an asset. Criticality is ranked on a low, medium, or high scale and this ranking determines an asset's value to the CPSS operational objectives and mission.

Threats and Vulnerabilities: vulnerabilities are the potential weaknesses that exist within the CPSS operations that make it susceptible to external threats. In the framework, threats and vulnerabilities are then connected to assets, actors, and mission-critical processes that they are connected to.

Dependencies: threats affecting one component of the CPSS can propagate through the system, eventually affecting multiple parts of the CPSS (Wu et al., 2015b). A key consideration to understand the risks and vulnerabilities of a CPSS is through the examination of how the connections among computational, physical, and social dimensions interact in the system.

Table 2: Proposed qualitative risk identification (Q-ID) framework for CPSS



1. Mission definition What is the purpose of the CPSS?	**1.1 Define application domain of CPSS** In what context or sector is the CPSS in use?	**1.1.1 Functions** What mission functions is the CPSS connected to?	
		1.1.2 Actors Who are the key actors in the CPSS ecosystem?	
		1.1.3 Assets What are the assets linked to this CPSS?	
2. Mission Process Identification What steps are taken to achieve the goal of the CPSS? Which CPSS steps are connected to mission-critical (MC) processes?	**2.1 Process Description** How are the MC processes executed in the CPSS?	**2.1.1 Actors** Which actors participate in the different steps?	
		2.1.2 Process classification	**Mission - critical** Which steps may lead to the failure of the CPSS?
			Non-mission- critical Which steps are considered necessary but optional to the CPSS operations?
	2.2 Technical Systems Description	**2.2.1 Assets** Which assets are linked to mission-critical processes?	**Criticality & Class** Low, Medium, or High What level of impact does the asset failure have on the CPSS? What level of sensitivity and security does the asset require?
		2.2.2 Asset classification	
3. Vulnerable Components List Which actors and assets are linked to mission critical processes? In which layer (human, cyber, or physical) are they classified?	**3.1 Human Components** What are the vulnerable human components and which MC processes are they linked to?		**Non-technical vulnerabilities list**
	3.2 Cyber Components What are the vulnerable computational components and which MC processes, and human components are they linked to?		
	3.3 Physical Components What are the vulnerable physical system components and which MC processes, and human components are they linked to?		**Technical vulnerabilities list**
4. Risk Classification	**4.1 Human induced risk** Which identified vulnerabilities emerge as a direct result of human related CPSS activity?		**Cascade risk** What risk emerges because of a combination of human and technology induced incidents?
	4.2 Technology induced risk Which identified vulnerabilities emerge as a direct result of the technical systems activity in the CPSS?		

The identification and classification of risk and vulnerability in CPSS, is a complex, system-wide activity. It requires the analysis of risk "from a strategic to a tactical level, ensuring risk-based decision making is integrated into every aspect of the organization". The identification of risk in a CPSS is a first step before the implementation of controls and 'manage' the risk levels—which are beyond the scope of this work. Table 2 shows the proposed QID framework that considers the CPSS in mission-critical aspect. The colours in Table 1 correspond to Figure 5.

The aim of the mapping exercise is to reveal underlying connections and dependencies among the processes, assets, and actors. This step is helpful in the highlighting of the possibility of cascading risk. Cascading risk is an emergent behaviour of CPSS emanating from the multi-layer integrations in the systems (Wu et al., 2015a). The applicability of QID in CPSS mission-critical is discussed in empirical illustrations in the next section.

Q-ID FRAMEWORK EVALUATION

Rigour demands the evaluation of Q-ID framework as a demonstration to highlight how it facilitates CPSS risk identification in CPSS. The context definition of a CPSS is determined by the physical process in which it is embedded. We consider empirical illustrations highlighting CPSS linked to transport, and health.

Transport Infrastructure – Connected Vehicles

Vehicle manufacturers such as Audi, Mercedes Benz, and Tesla are examples of companies that are at the forefront of intelligent transport innovation. Vehicles come with a suite of on-board drive assist systems, with services such as lane control, emergency assist, and multi-collision brake assist. In this example, t*he vehicle and occupants are the CPSS*. The physical process that we will be analyzing is the emergency assist systems such as (Figure 6). This is considered a mission-critical process because the safety of human lives is at stake.

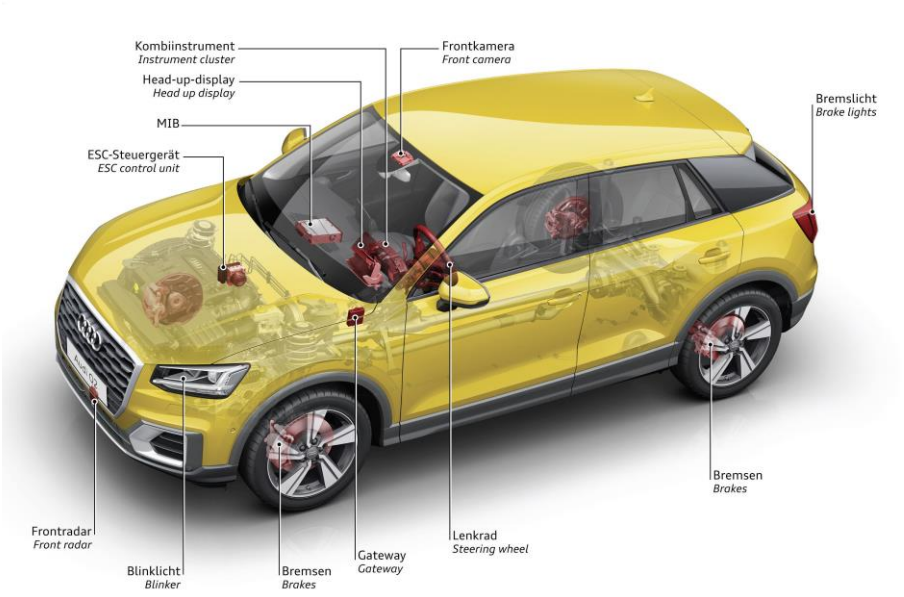


Figure 6: vehicle emergency assist sensor distribution (source Audi AG)

In Q-ID (**steps 1- 1.1.3**) the CPSS (Emergency-assist) delivers its goals (driver safety) in a series of planned steps (processes). Each step incorporating essential components, e.g. an actor (driver and passengers), asset (sensors, brakes, vehicle computer box) leading to successful delivery of a mission-critical process. Various emergency-assist related information is collected through use of intelligent sensors strategically placed in the vehicle (Figure 6) to achieve the CPSS goals. A series of processes follows (Q-ID **steps 2 – 2.1**). Based on the sensor data, emergency assist detects, within system limits when the driver is inactive. Should the driver be incapacitated, the system assumes control of the vehicle and automatically brake to a standstill in its own lane. Emergency assist is achieved through monitoring of the steering wheel movements and lane assist systems. When the driver appears unresponsive, the system, repeatedly prompts the driver, using a series of visual and audio cues and brake jolts (first brake jolt is at 80km/hour). The hazard lights are also activated to alert fellow motorists. The driver may deactivate the system by moving the steering wheel, disabling lane assist or cruise control, or pressing the brake, or accelerator pedals. Should the driver remain unresponsive following prompting, Emergency-assist brings the vehicle to a standstill and the parking brake is engaged. There are instances where the vehicle goes a step further and makes a call to emergency responders, providing vehicle location details through onboard GPS.

In the Q-ID (**steps 2.1.2 – 2.2.2**), the described processes would all be classified as 'mission-critical' - they have a direct influence on the overall safety of the driver. However, in the asset classification, the technical assets that participate in the process would be ranked differently on the criticality and class rankings, for instance, the car brakes would have a high criticality and class rating when compared to the brake lights. Interestingly, in Q-ID step 3 there is a duality to the vehicle driver, interpreted as an actor prior to an incident, and then a CPSS vulnerability in the case of incapacitation. This is due to the lack of predictability that emerges when something is wrong with the driver, yet they still convince the system otherwise. **In step 4**, it is shown that emergency-assist may be unable to complete its goal (driver safety) if the driver, moved the steering wheel or brake pedal (physical asset) or was otherwise intoxicated while operating the vehicle. The framework reveals a dependence between the cognitive state of the driver and emergency-assist that emerges as a 'human-induced risk', which leads to cascade risk such as road traffic accidents and fatality.

Health Infrastructure – Remote Patient Monitoring

The use of digital solutions in the health sector is an emerging trend. Various sensors and digital tools are used to capture biomedical and clinical data from patients living at home, allowing remote monitoring of chronic health conditions (see Figure 2). Digital health technologies have been integrated into and applied to processes such as contact tracing, clinical management, and infection screening. In this case, we analyze the use of a remote clinical monitoring application (see Figure 2) where data is uploaded to a cloud service from the patient, and the service includes the preprocessing of data in the cloud service.

Remote patient monitoring is primarily designed to allow patients to gain some independence while they continue to receive a reasonable level of care. Such applications generate a considerable amount of data, the possibility of loss of this sensitive data makes this a *mission-critical process*. In this example, the patient and all the infrastructure (see Figure 2) are the CPSS. In Q-ID (**steps 1 – 1.1.3**) a selection of biosensors (e.g., pulse-oximeter), are used to deliver a customised medical care plan (goal). The CPSS generates a lot of data – input, historic, and output data. When a patient (actor 1) makes a reading, input data is initially transmitted through a Wi-Fi connection to a cloud-based server, for pre-processing by clinicians (actors 2). They provide advice and feedback to the patient based on this data. Eventually, historic data is transferred via the internet or a secure health network into private storage. In Q-ID steps **2.1.2 – 2.2.2**, there are two main mission-critical processes that are identified – harvesting of patient data and the secure data transmission while ensuring its integrity. The criticality and class ranking for e.g., stable Wi-Fi connectivity and the biosensors is high within the patient monitoring process, and less so for secure data transmission.

In step 3, relationships between the actors (patients, clinicians), assets (e.g., biosensors, secure networks) and these processes are revealed. While the biosensors are seemingly passive, they require Wi-Fi connectivity to complete the CPSS goals. This connectivity has a direct impact on the patient privacy and data security in the cloud service and the wider network. While use of an identifiable Wi-Fi network allows flexibility and mobility for the patient, an unintended consequence is the 'surveillance' effect of such a system. This can compromise patient privacy that may carry safety, legal, or ethical implications. Further, should the patient opt to connect through an insecure network, this may compromise not only their individual data but that of other patients. The interpretation of the available information obtained from the CPSS/ sensors etc. further emphasizes the human-device interplay, highlighting how cognitive load could influence the overall quality of care the patient receives. **In step 4,** with further operational details, it is possible to deduce which aspects of the mission-critical processes are dependent on cognitive traits. Leading to an understanding of how a lapse in judgement by the patient or the clinician could compromise the CPSS ecosystem.

CONCLUSION & FUTURE RESEARCH

This paper is an exploratory attempt to apply the 'organisation-wide risk assessment methodology' to CPSS ecosystems in critical infrastructure sector applications. CPSS is understood to be a collective of resources, technological capabilities, and organisational processes. This understanding can be a starting point for further studies. The recommended alternative approach highlights the novel dynamics that are introduced through the integration of complex critical infrastructure systems into human society. The methodological approach is mainly conceptual incorporating empirical illustrations and the main contribution of this research work is a qualitative risk identification framework for CPSS analysis. The Q-ID framework serves as a building block for future research in the CPSS domain. However, the research results presented here require further elaboration, analysis and competing views. Further empirical and design-oriented studies are required to give deeper evaluations and go beyond the limited insights provided by the identified empirical illustrations.

REFERENCES

Bou-Harb, E. (2016). *A Brief Survey of Security Approaches for Cyber-Physical Systems.* Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus.

Cacciabue, P. (2000). Human Factors Impact on Risk Analysis of Complex Systems. *Journal of Hazardous materials, 71*(1-3), 101-116.

Dey, N., Ashour, A. S., Shi, F., Fong, S. J., & Tavares, J. M. R. (2018). Medical Cyber-Physical Systems: A Survey. *Journal of medical systems, 42*(4), 74.

ENISA. (2006). *Users' Guide: How to Raise Information Security Awareness*. European Union Agency for Cybersecurity (ENISA).

ENISA. (2020). *Enisa Threat Landscape 2020: Main Incidents in the Eu and Worldwide*. European Union Agency for Cybersecurity (ENISA).

Frazzon, E. M., Hartmann, J., Makuschewitz, T., & Scholz-Reiter, B. (2013). Towards Socio-Cyber-Physical Systems in Production Networks. *Procedia Cirp, 7*(2013), 49-54.

Gharib, M., Lollini, P., & Bondavalli, A. (2017). *Towards an Approach for Analyzing Trust in Cyber-Physical-Social Systems.* Proceedings of the 12th System of Systems Engineering Conference (SoSE), Hawaii, USA.

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. *JRC Technical Notes*.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A Survey on Concepts, Applications, and Challenges in

Cyber-Physical Systems. *KSII Transactions on Internet & Information Systems, 8*(12).

Haque, S. A., Aziz, S. M., & Rahman, M. (2014). Review of Cyber-Physical System in Healthcare. *international journal of distributed sensor networks, 10*(4), 217415.

JTFTI. (2011). *Sp 800-39. Managing Information Security Risk: Organization, Mission, and Information System View*. Retrieved from

Kirwan, B. (1998a). Human Error Identification Techniques for Risk Assessment of High Risk Systems—Part 1: Review and Evaluation of Techniques. *Applied ergonomics, 29*(3), 157-177.

Kirwan, B. (1998b). Human Error Identification Techniques for Risk Assessment of High Risk Systems—Part 2: Towards a Framework Approach. *Applied ergonomics, 29*(5), 299-318.

Lee, E. A. (2006). *Cyber-Physical Systems-Are Computing Foundations Adequate.* Proceedings of the NSF workshop on cyber-physical systems: research motivation, techniques and roadmap, Austin, Texas, USA.

NCCIC. (2016). *Ics-Cert Annual Vulnerability Coordination Report Industrial Control Systems Cyber Emergency Response Team 2016*. Retrieved from USA:

Sebescen, N., & Vitak, J. (2017). Securing the Human: Employee Security Vulnerability Risk in Organizational Settings. *Journal of the Association for Information Science and Technology, 68*(9), 2237-2247.

Singh, A., & Jain, A. (2018). *Study of Cyber Attacks on Cyber-Physical System.* Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), Jaipur, India.

Singh, A. N., Gupta, M., & Ojha, A. (2014). Identifying Factors of "Organizational Information Security Management". *Journal of Enterprise Information Management*.

Skarin, P., Tärneberg, W., Årzen, K.-E., & Kihl, M. (2018). *Towards Mission-Critical Control at the Edge and over 5g.* Proceedings of the 2018 IEEE International Conference on Edge Computing (EDGE), San Fransisco, USA.

Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *The Computer Journal, 61*(9), 1389-1406.

Wang, J.-W., & Rong, L.-L. (2009). Cascade-Based Attack Vulnerability on the Us Power Grid. *Safety science, 47*(10), 1332-1336.

Wu, W., Kang, R., & Li, Z. (2015a). *Risk Assessment Method for Cyber Security of Cyber Physical Systems.* Proceedings of the 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, China.

Wu, W., Kang, R., & Li, Z. (2015b). *Risk Assessment Method for Cybersecurity of Cyber-Physical Systems Based on Inter-Dependency of Vulnerabilities.* Proceedings of the 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore.

Yilma, B. A., Naudet, Y., & Panetto, H. (2018). *Introduction to Personalisation in Cyber-Physical-Social Systems.* Proceedings of the OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", Rhodes, Greece.

Yoneda, S., Tanimoto, S., Konosu, T., Sato, H., & Kanai, A. (2015). *Risk Assessment in Cyber-Physical System in Office Environment.* Proceedings of the 18th International Conference on Network-Based Information Systems, Taipeh, Taiwan.

Zeng, J., Yang, L. T., Lin, M., Ning, H., & Ma, J. (2020). A Survey: Cyber-Physical-Social Systems and Their System-Level Design Methodology. *Future Generation Computer Systems, 105*, 1028-1042.

Zhou, Y., Yu, F. R., Chen, J., & Kuo, Y. (2019). Cyber-Physical-Social Systems: A State-of-the-Art Survey, Challenges and Opportunities. *IEEE Communications Surveys & Tutorials, 22*(1), 389-425.

Zhu, W., & Milanović, J. V. (2020). Assessment of the Robustness of Cyber-Physical Systems Using Small-Worldness of Weighted Complex Networks. *International Journal of Electrical Power & Energy Systems, 125*, 106486.