



HAL
open science

Methodological resilience assessment of smart cyber infrastructures

Romain Dagnas, Michel Barbeau, Maxime Boutin, Joaquin Garcia-alfaro,
Reda Yaich

► **To cite this version:**

Romain Dagnas, Michel Barbeau, Maxime Boutin, Joaquin Garcia-alfaro, Reda Yaich. Methodological resilience assessment of smart cyber infrastructures. Security and Privacy in Smart Environments. Lecture Notes in Computer Science, 2024, 978-3-031-66707-7. hal-04656303

HAL Id: hal-04656303







<https://hal.science/hal-04656303v1>

Submitted on 22 Jul 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Methodological Resilience Assessment of Smart Cyber Infrastructures

Romain Dagnas¹, Michel Barbeau², Maxime Boutin¹,
Joaquin Garcia-Alfaro³^(✉) , and Reda Yaich¹

¹ Institut de Recherche Technologique SystemX, Palaiseau, France
{romain.dagnas,maxime.boutin,reda.yaich}@irt-systemx.fr

² Carleton University, School of Computer Science, Ottawa, Canada
barbeau@scs.carleton.ca

³ SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France
joaquin.garcia_alfaro@telecom-sudparis.eu

Abstract. The race for digitization created a real need to protect smart infrastructures. Environments are becoming highly connected and automated. Their growing complexity and connectivity make it hard to assure and assess their cyber resilience, i.e., protecting them from cyberattacks, failures, and errors. Traditional strategies for ensuring the cyber resilience of smart infrastructures suffer from a lack of holism. Indeed, since smart infrastructures are often structured in layers, traditional protection methods can lead to conflicting and competing goals. For instance, they may increase the resilience of specific layers at the expense of decreasing the performance of others. This chapter reviews existing methods aiming to address this problem. We focus on two leading methodological assessment families: quantitative and qualitative. The former includes numerical metrics to quantify and assist system-dependent decision-making processes. The latter builds upon symbolic modeling to offer a system-agnostic assessment. The chapter provides an in-depth exploration of quantitative and qualitative methodologies with significant potential to enhance the resilience of layered smart infrastructures. Our exploration covers classical technological aspects (e.g., cascading effects) and socio-technical factors (e.g., human-in-the-loop interaction).

Keywords: Resilience Assessment · Resilience Enhancement · Attack Remediation · Socio-Technical Theory · Cascading Effect · Smart Infrastructure · Cyber-Physical System · Human-in-the-Loop · Security Ceremony · Formal Modeling · Theorem Proving · Hypergraph.

1 Introduction

We live in a constantly changing world. How we conceptualize, design, and build architectures of Cyber-Physical Systems (CPS)s are also changing. We have experienced four industrial revolutions in the last two centuries. The fourth industrial revolution was one of digitization induced by increased competitiveness. To remain competitive, the new generation of systems faces multiple challenges. The

work by Ryalat *et al.* presents the main pillars of Industry 4.0 [35], which are: CPSs, additive manufacturing, automation and industrial robots, simulation, blockchain, augmented reality, big data analysis, cloud computing, Artificial Intelligence (AI), and Internet of Things (IoT). The use of these new technologies aims at enhancing the productivity and reliability of industrial processes. However, there may be a lack of hindsight on these technologies. We may not have a sufficient perception of their potential safety risks.

Motivation. Modern systems consist of multi-layered architectures. Traditional resilience enhancement strategies could help improve the resilience capabilities of one layer but to the detriment of the others. There is a need for holism in resilience mechanisms, especially in smart infrastructures where the high degree of interconnection between its functions increases the risk of cascading effects.

Contributions. The contributions of this chapter are twofold. We discuss existing methodologies to solve the above challenge. We focus on quantitative and qualitative methodologies that could enhance layered smart infrastructures' resilience potential. We review the relevance of the presented methodologies and research challenges related to the resilience enhancement of smart systems.

The chapter is organized as follows. Section 2 presents background on smart infrastructures and preliminaries on the emergence of new technologies and relevant models. Section 3 surveys existing quantitative methodologies, including numeric metrics, to help quantify and assist system-dependent decision-making processes. Section 4 surveys qualitative methodologies, including symbolic modeling and other representative methodologies. Section 5 discusses some directions and trends for further research on the resilience of smart infrastructures. Section 6 concludes the chapter.

2 Smart Infrastructures in a Digitized World

This section presents some preliminary background on smart infrastructures and the new generation of architectures in Industry 4.0. We also provide preliminaries on the emergence of new technologies and representative models used to analyze smart systems and architectures of the future [13].

2.1 Industrial Revolutions

Historically, there have been four industrial revolutions in the last centuries. The first revolution started at the beginning of the 19th century and has led to a major industrial transformation of societies in terms of mechanization. The second revolution started around 1870 with massive technological inventions and industrial advances, fostering the emergence of new energy sources such as electricity, gas, and oil. The third revolution started in the 1970s with the emergence of nuclear energy, the first computers, and the rise of electronics. The fourth revolution is the one of Industry 4.0. However, many people disagree with the arrival

of such a revolution because we do not yet know the magnitude of its impact. The transition to digitization and smart technologies is underway. With the use of highly connected devices in cyberspace, we are becoming aware of new threats and vulnerabilities to which critical systems are subjected. This revolution includes advances in AI, IoT, blockchain, big data, and other technologies that we present in a more detailed way in the next section.

2.2 Emergence of New Technologies and Initiatives

The adjective *smart* describing infrastructures, facilities, and critical systems indicates a high degree of connectivity and digitization in the cyber world. Indeed, the digitization era has led to significant changes in the design of industrial systems’ architecture, such as maritime port infrastructures, supply chain systems, and Industry 4.0. Cyber-physical systems are involved in this transformation because they connect the real and cyber worlds. Figure 1, which has been realized within the Secure Ports of the Future (PFS) project [39], presents new technologies used in smart infrastructures.

The new generation of complex systems comprises the integration of communication technologies for enabling communication between a larger set of connected components (including 5G networks, WiFi, Bluetooth, and GSM to enable connectivity between mobile devices); digitization, involving the use of many connected devices highlights a need to analyze, store and protect these data. These data technologies include IoT and Industrial Internet of Things (IIoT) components, Cloud, Blockchain, Big Data, and also Edge Computing (modern computing paradigm located at the edge of the network, which *allows client data to be processed closer to the data source instead of far-off centralized locations such as huge cloud data centers* [43]) and Fog Computing (located

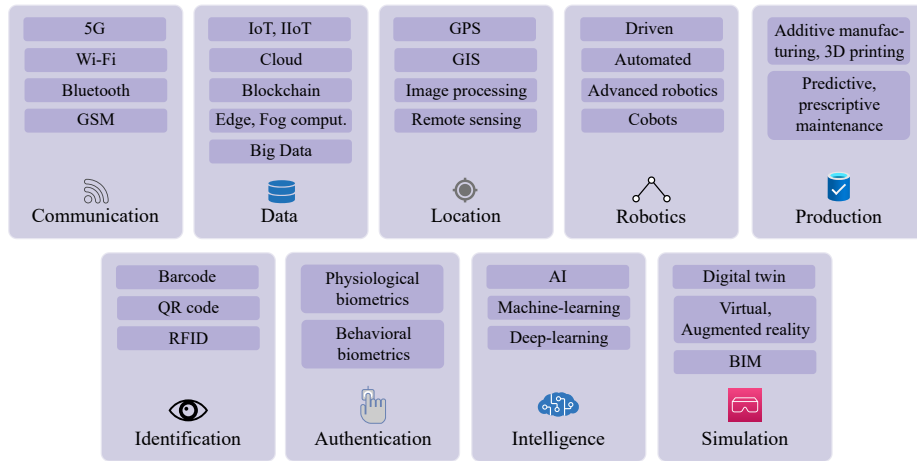


Fig. 1. Technologies used in smart infrastructures.

between the Cloud and the Edge, it is based on *locating certain resources and transactions closer to the edge of a network* [43]). Smart systems also integrate various location technologies to find merchandise and external or internal human employees during sensitive missions. Robotic technologies in handling or transportation systems are also a part of smart systems. In the industrial field, predictive maintenance algorithms are used to anticipate malfunctions. Recently, prescriptive algorithms have been created to provide not only the failure date of a component but also prescription recommendations to optimize a component's lifetime. Identification technologies such as barcodes, Radio Frequency Identification (RFID), and QR codes are used in smart infrastructures to obtain a detailed information sheet about products involved in the supply chain. In such smart infrastructures, there is a need to improve the authentication processes. Organizations use physiological and behavioral biometrics to guarantee an accurate and secure authentication process. Many machine-learning and deep-learning strategies are used to identify patterns in data and make appropriate decisions. Virtual, augmented reality and digital twins are also part of Industry 4.0. These advanced simulation techniques allow us to anticipate the exploitation of vulnerabilities by an adversary and analyze security scenarios in specific environmental constraints.

These new technologies and infrastructures must remain competitive and respond to society's challenges while remaining high-performance. For this reason, these new systems are building their activities on smart initiatives that use future technologies, such as blockchain, AI, Machine Learning (ML), IoT, IIoT, virtual reality, and digital twins. However, these technologies are not the only innovations that bring critical infrastructures into the 4.0 era. Environmental problems such as global warming and increasing pollution will anchor future systems in environmental protection approaches. Some initiatives are *eco-friendly* and aim to reduce the environmental impact of systems in terms of pollution, noise pollution, and so on. Other initiatives aim to encourage using renewable energies such as wind, hydro, geothermal, and even hydrogen. The systems of the future are also intended to be anchored in participatory democracy strategies, involving citizens living near industrial facilities in new land use and other projects.

In Wavestone's report dedicated to smart ports [38], Sinibaldi has presented three main families of smart solutions. They include ecological solutions, which are related to the use of renewable energies and focused on protecting the environment from the impact of facilities; economic solutions associated with the supporting functions, the core business, and the open innovation strategies of a company; and participatory which includes solutions involving citizen in new projects.

We have analyzed the evolutionary trends of the ten smartest ports in the world. Figure 2 [39] presents the results of our analysis. We can see that in maritime port infrastructures, the emphasis is put on support functions (orange) and core business-related smart solutions (brown). Indeed, these solutions aim to enhance the port's competitiveness and facilitate operations and missions. We also see that most of the smartest ports apply environment-related solutions

to reduce noise nuisance and air pollution and use automated vehicles. These diversified initiatives show that there's a shift in the way we design the architectures of the future and modernize existing ones. Industry 4.0 systems must be anchored in a world where environmental protection and the use of renewable energies are becoming a real issue.

3 Quantitative Methodologies

Quantifying the resilience of complex cyber-physical systems is a vital research axis of growing interest. Quantifying approaches aim to design complex systems considered resilient-by-design and assist designers in improving and upgrading existing infrastructures to bring resilience capacities. This section reviews relevant existing methodologies to quantify and help system-dependent decision-making processes.

Quantitative deterministic metrics are built upon intrinsic properties of a system such as performance, mission delivery, reliability, and accuracy. These metrics provide either a numerical estimation of resilience based on certain properties or a numerical score of different parameters that compose resilience. Metric-based strategies involve numerical indicators that build upon certain system properties. As resilience is highly related to performance, many metrics are used to quantify a system's ability to complete a certain mission, deliver a specific rendering, or remain secure during an adversarial event. Linkov and Kott present two different families of strategies for assessing the resilience of systems, which are metrics-based and model-based [23]. Clédel *et al.* [11] present methodologies for measuring resilience capacities. These approaches are twofold:

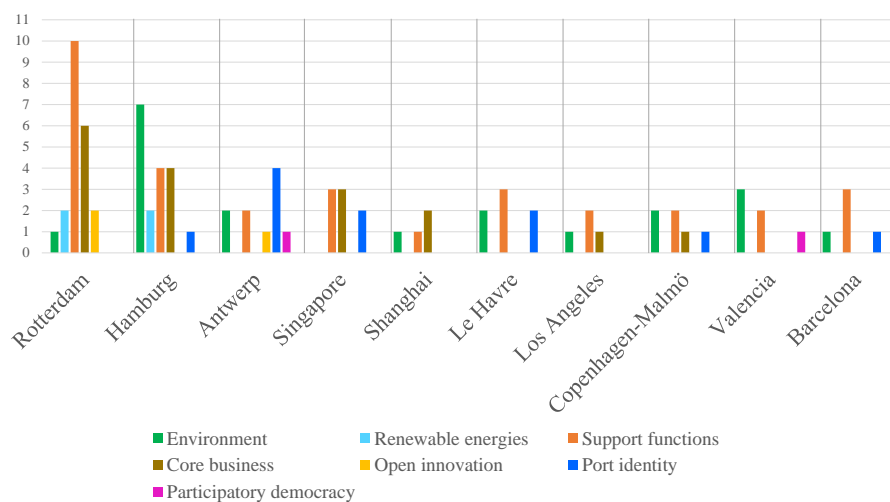


Fig. 2. Number of smart initiatives per smart port.

(i) quantitative deterministic, which involves indicators to analyze performance losses of a system facing known disruptive events; (ii) quantitative probabilistic, based on uncertainties. Thus, stochastic aspects are added to resilience assessment. Another way to classify metrics is by their empirical or analytic nature. They are discussed further in the following.



Fig. 3. Ottawa O-Train transit system.

Date	Duration (Minutes)
04-10-2019	124
21-10-2019	116
22-10-2019	138
23-10-2019	115
01-11-2019	191

Fig. 4. Disruptions (Data source: [16]).

3.1 Empirical Metrics

Empirical metrics rely on data collected by observing cyber-physical systems during a time interval. Their use in resilience analysis of cyber-physical systems has been highlighted by Lewis [25].

We review some empirical metrics using sample data collected during the operation of the Ottawa O-Train transit system, Figures 3 and 4. The table lists disruptions exceeding 100 minutes that occurred in October and November 2019. For this example, the disruption time threshold is 100 minutes. During that two-month observation period (T_0), five (N) disruptions exceeded 100 minutes. The average monthly occurrences is:

$$N_m = N/T_0, \text{ i.e., } 2.5. \quad (1)$$

A probability of exceedance model can be constructed using this parameter to predict the future. The probability of exceedance is defined as:

$$P = 1 - e^{-N_m T_p} \quad (2)$$

Where T_p is the prediction period.

Figure 5(a) plots the exceedance probability for a 100 minute disruption or longer versus time (in months). The random variable is time. For this example, the probability is one for three months and longer. In such a case, the metric to minimize is the probability of a disruption. Another interesting number that can be derived is the *mean recurrence interval*, which corresponds to the ratio:

$$T_x = 1/N_m \quad (3)$$

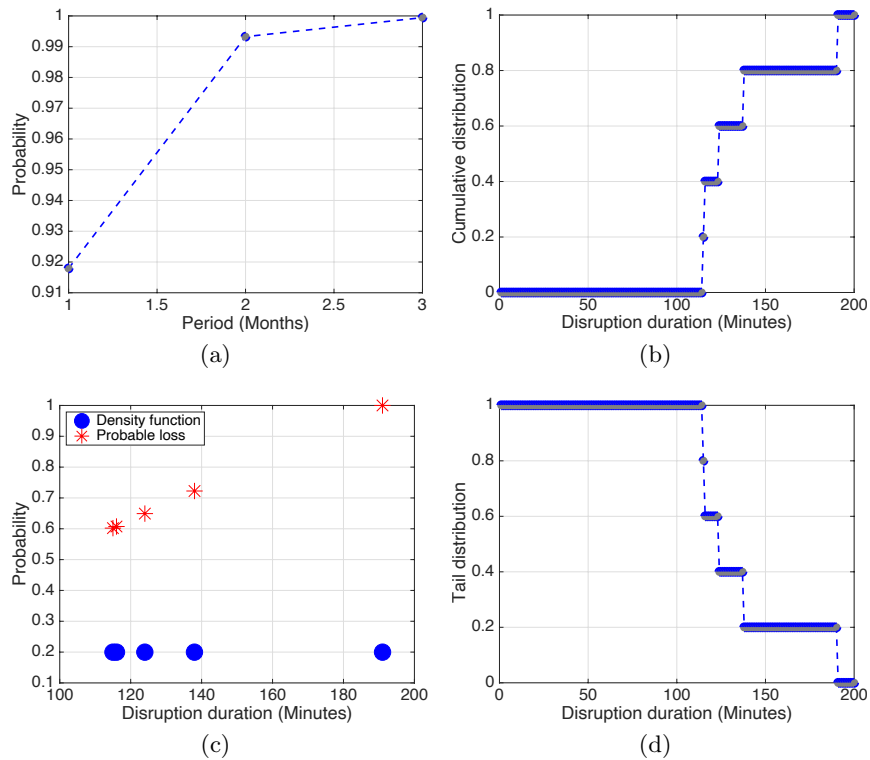


Fig. 5. Example of empirical metrics usage associated to sample data collected during the operation of the Ottawa O-Train transit system. (a) 100-minute disruption exceedance. (b) Cumulative distribution. (c) Density function and probable loss. (d) Tail distribution.

In this example, it is 0.4 month. It roughly means that a 100-minute disruption can be expected biweekly. The data can be examined from several different perspectives. Figure 5(b) plots the cumulative duration of a disruption versus the duration of a disruption (minutes). In this case, the random variable X is the disruption duration. The diagram plots

$$F(x) = Pr[X \leq x], \text{ for } x = 1, 2, \dots, 200 \text{ minutes.} \quad (4)$$

When a disruption occurs, the plot indicates the probability that it is at least that time for every possible duration. The $F(x)$ derivative yields the probability density function of X , that is, $f(x)$. The product $xf(x)$ is interpreted as the probable loss, Figure 5(c). This probable loss has a maximum. The ratio $xf(x)$ over the maximum indicates resilience. The complementary of $F(x)$ is:

$$F(\bar{x}) = Pr[X > x] = 1 - F(x) \quad (5)$$

It is interpreted as the tail distribution, Figure 5(d). When alternatives are available, resilience-wise, a thin tail distribution is preferable to a fat tail distribution. The examples presented in this section are built using a small data set. Ideally, analyses should be built on large sets of data. Such data sets may not be available for new systems. In such cases, analytic metrics discussed in the upcoming section can be used.

Quantitative probabilistic metrics include stochastic strategies. Some uncertainties exist in such metrics. The probability considered in resilience evaluation includes the stochasticity of the occurrence of an adversarial event. In such quantitative probabilistic approaches, there exist event-specific metrics. For such metrics, the resilience of a system facing a specific event is considered. Certain approaches claim that resilience can be quantified only once a threat scenario is established [11,18]. This approach is called event-specific.

3.2 Analytic Metrics

Analytic approaches rely on mathematical or logical reasoning to predict cyber-physical systems' resilience. Analytic metrics may be considered in a graph modeling framework. Graph modeling is a rigorous framework that captures entities and relationships between them [21]. In contrast to classical databases, the emphasis is on the relationships and how entities interact. They are particularly well adapted for answering queries involving several relationships chained together. Graphs are well-suited for capturing the design aspect of complex cyber-physical systems. For example, functionality can be defined as the percentage of functioning graph nodes. Links from node to node can capture cascading effects due to fault propagation.

The issue of cascading effects is of paramount importance. Indeed, smart infrastructures are, due to their complexity, more prone to the damaging consequences of cascading effects, i.e., their functions, components, and sub-systems have high link densities between elements of the systems, which increase the risk.

A cascading attack describes an adversarial event during which an adversary attacks a specific point of an infrastructure, gains access to another system, and compromises it due to their connectivity. According to this definition, a cascading effect corresponds to a domino effect through interconnected systems with severe and unexpected consequences.

For cyber-physical system modeling, graph nodes may correspond to system components, such as pumps and valves. Links represent connections between components, such as conduits. The interconnections can be specified with an adjacency matrix where rows and columns correspond to components. *Spectral radius* has been considered to characterize the resilience of a cyber-physical system modeled as a graph. The spectral radius is the largest eigenvalue of the adjacency matrix [40]. When there are nodes that tend to play the roles of centers, the spectral radius reflects their number of connections to other neighbor nodes. It is indicative of the potential for fault propagation through cascading effects. A graph can also be analyzed to highlight the presence of *blocking nodes* versus the number of links. Removing a blocking node partitions the graph, breaking connections from one partition to another. Resilience-wise, a low blocking nodes-number of links ratio is preferable.

Wang *et al.* [42] studied six different graph spectral metrics and highlighted that their interpretation regarding resilience may be contradictory. In a recent paper [14], we investigated the use of the spectral radius and (k, ℓ) -resilience to evaluate the resilience of a water treatment system [2,3]. We arrived at similar conclusions.

3.3 Multi-Layered Frameworks

Frameworks, such as the Industrial Internet Reference Architecture (IIRA) [26] and Reference Architectural Model Industrie 4.0 (RAMI 4.0) [19], are dedicated to helping model architectures of the Industry 4.0 as multi-layered architectures. Figure 6 represents the RAMI 4.0 framework.

The RAMI 4.0 framework works with a 3-D model by representing an architecture with the following layers: asset, integration, communication, information, functional, and business. The two other axes are the *life cycle value stream* and *hierarchy levels*. RAMI 4.0 is made to ensure that all the participants involved have a common understanding of a specific system.

We have applied RAMI 4.0 to a water treatment system architecture. Figure 8 presents the obtained model divided according to the RAMI 4.0 layers [44]. Indeed, the asset layer is dedicated to physical components such as sensors and actuators. The integration layer makes a transition between the physical and cyber-world. It deals with easy information processing. The communication layer provides communication elements between the integration and information layers. The information layer is related to all the information about materials manufactured in an industry or, in our case, information related to the water treatment process. The functional layer deals with system control and processing rules. The business layer integrates business strategies or business models used

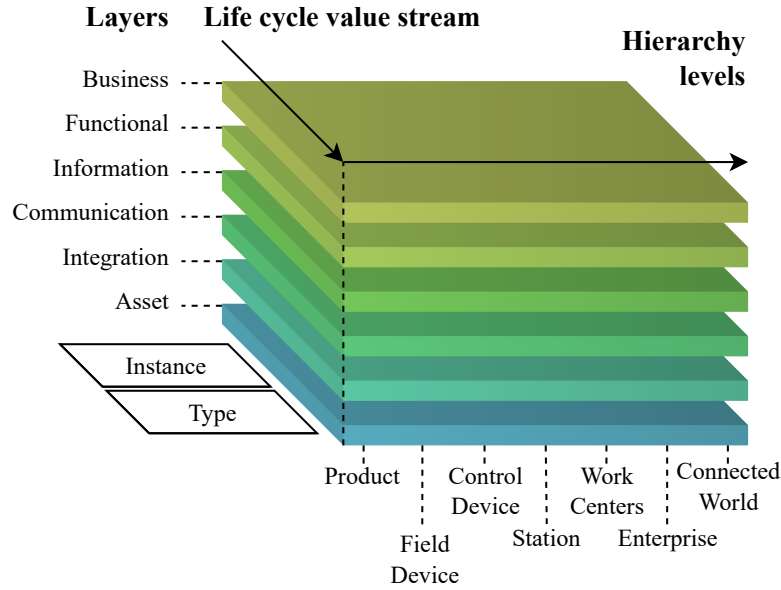


Fig. 6. RAMI 4.0 model.

during the life cycle of a system. In the case of a water treatment system controlled by a state and healthcare agencies, business models can be summarized as initiatives to launch inter-sectoral water swaps, for example, [34].

We must highlight that the RAMI 4.0 model combines the vital elements of Industry 4.0 in a layered model. Such a structure is useful to systematically organize and flourish the technologies used in Industry 4.0.

3.4 Knowledge Graphs

The knowledge graph concept gained interest in various areas, especially cyber security. Indeed, knowledge graphs can structure and process high volumes of data generated from cyberspace. Using ontology-based knowledge representations, they capture information's complexity and heterogeneous nature [37,45].

The knowledge graph presented in Figure 7 represents the Secure Water Treatment System (SWaT) [12]. It is a CPS test bed reproducing the behavior of an actual water treatment station in Singapore. SWaT consists of six sub-functions: (1) pumping phase; (2) chemical dosing phase; (3) Ultrafiltration (UF) phase, which works by alternating filtration and backwash cycles to clean the UF membrane until a manual cleaning is required; (4) ultraviolet treatment and dechlorination phase; (5) reverse osmosis phase; (6) final stage and backwash sending flow for the membrane of the UF unit in the third phase. Each of the six sub-functions is controlled by a Programmable-Logic Controller (PLC),

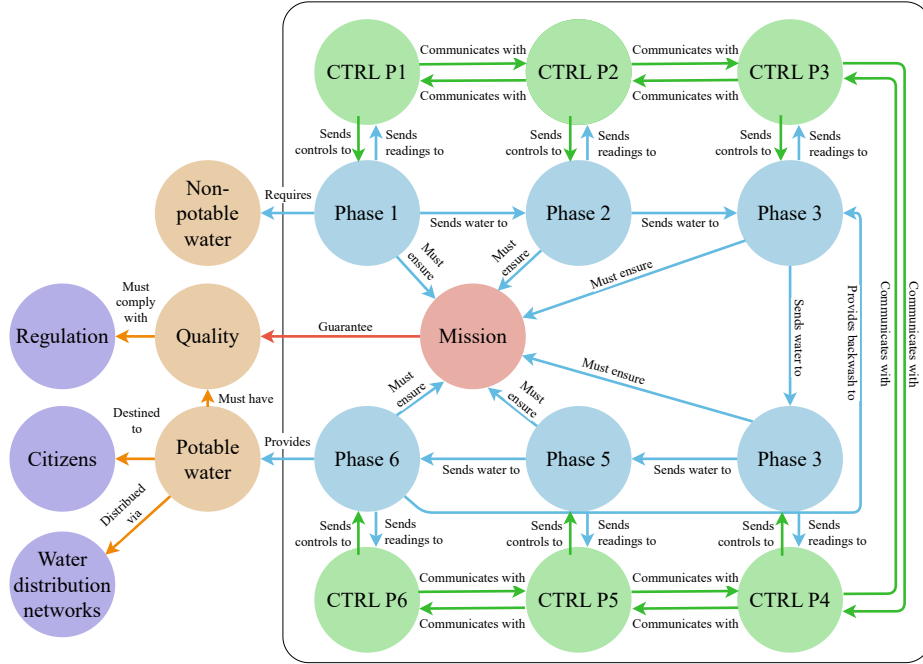


Fig. 7. Knowledge graph of a water treatment system.

and each of these PLCs communicate with each other during the water treatment process. The nodes and links related to the system are put into a dark square. Other entities are considered outside the scope of the system. Indeed, the system requires non-potable water from the groundwater or rivers. At the level of the last stage, the system produces potable water sent through water distribution networks to residential areas. The produced water must also comply with the regulations established by organizations responsible for implementing health policy.

3.5 Summary

We have presented multiple approaches for resilience assessment purposes. Given the wide variety of approaches in the literature to quantify the resilience of CPSs, we refer the reader to the surveys [1,7,11] for further details on existing resilience techniques.

We must highlight that the knowledge graph and multi-layer approaches presented in Sections 3.3 and 3.4 are considered quantitative because the metrics applied to such models for resilience assessment purposes yield a quantitative estimation of the resilience.

Some of the techniques we presented are based on mathematical indicators, while others use probabilistic reasoning, graph representations, or disrupting

events analysis. The main takeaway is that due to their new intrinsic structures, resilience applied to smart infrastructures must be considered with a new look. Indeed, the new principles of Industry 4.0 can be summarized as follows:

- More widespread Internet availability.
- Devices become smart and connected to the cyber-space.
- New services and functions are involved.
- All parties involved in business processes, in the manufacturing and process industry, are mutually connected.
- Information from suppliers, customers, and within organizations are connected and transparently available for the stakeholders.
- The production is managed autonomously by machines.
- There are transitions between companies and sectors.

The Industry 4.0 principles aim to connect the stakeholders involved in a system and allow data to be shared. Some of the metrics presented previously help model such smart architectures. Knowledge graphs allow the modeling of several entities, e.g., physical or conceptual. Representing the links between these entities enables us to consider a system holistically, i.e., within its environment.

4 Qualitative Methodologies

We review qualitative methodologies, such as symbolic modeling methodologies and alternative solutions that can be used for resilience assessment purposes. Symbolic modeling can help to examine architectures from a holistic point of view. However, these methodologies may be undated or inaccurate for quantitative assessment.

4.1 Symbolic Modeling Methodologies

We discuss how symbolic modeling can contribute to resilience evaluation. It is an interesting approach because it complements the spectral radius and (k, ℓ) -resilience metrics, focusing on system structure [2,3]. Loss scenarios, a symbolic approach, consider threats from the environment and control structures (physical controller or human employee) interacting with a system. However, due to abstraction and several assumptions about the examined system and its environment, obtaining results perfectly reflecting reality is challenging.

Modeling threat scenarios in propositional logic leads to obtaining the truth assignment of axioms that validate them. For example, consider the following scenario: *The RAW_WATER_TANK is full. CTRL-P1 does not produce the Start Pump Control Action because CTRL-P1 incorrectly believes that the tank is not full.* This flawed condition occurs when there is a delay between the data coming from the level sensors of the tank, a wrong conversion of data units from the sensors, or readings are not received from the level sensor. This may be due, for instance, to a sensor failure or a conflict between the sensor readings and the conversion tool used to adapt to the global data units.

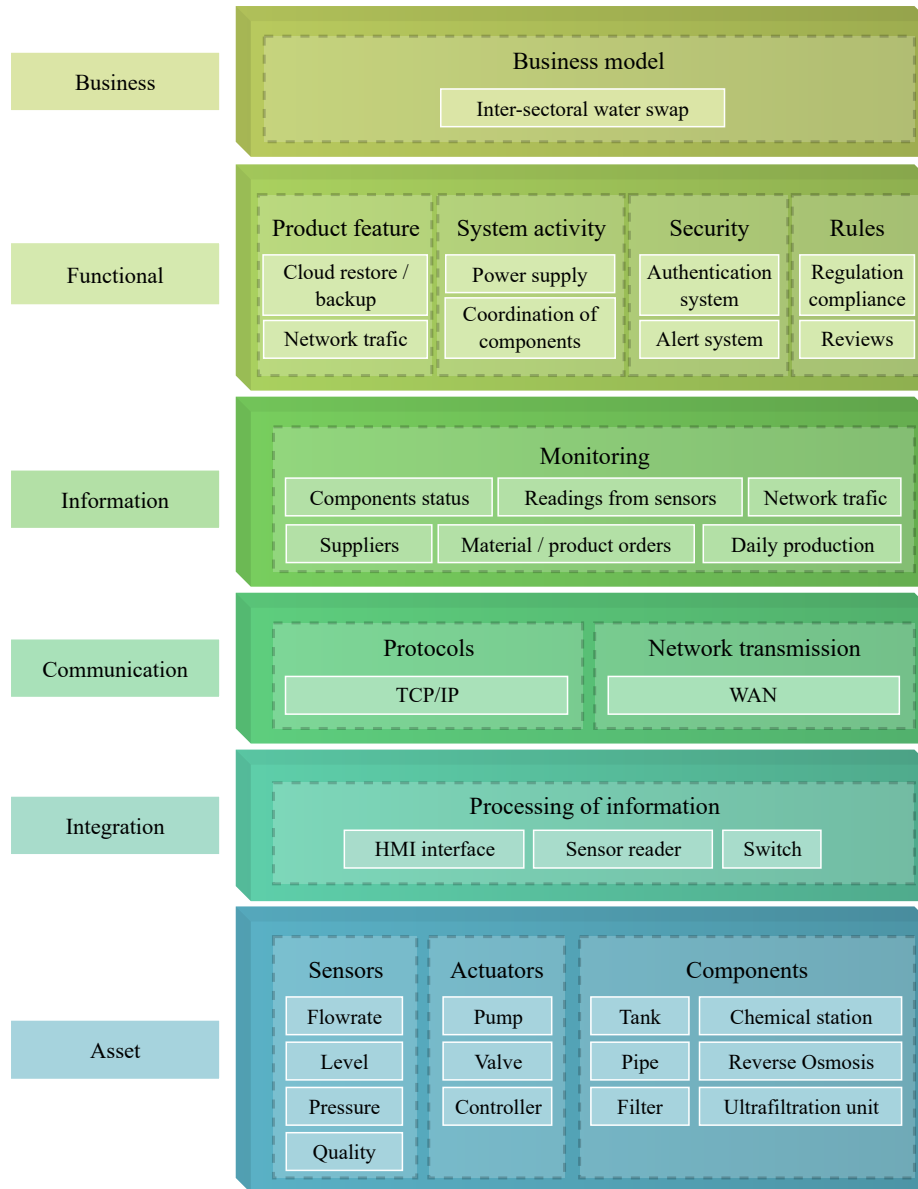


Fig. 8. RAMI 4.0 model of a water treatment system.

In this scenario, we distinguish between error, failure, and fault. According to ISO/IEC/IEEE 24765:2017, an error can be an erroneous system state or a difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. A failure is the non-performance or inability of a component (or a system) to perform its intended function. A fault is a defect in a hardware device or component that causes errors. In the scenario, it is implied that the fault *conflict between readings* causes the error *a wrong conversion of data unit from the sensors*, which in the end causes the failure *Start Pump Control Action is not produced*. This scenario can be translated into the following formula $((FAULT.OCCURED) \leftrightarrow (ERROR.OCCURED)) \wedge FULL.WATER.TANK$. The result of such a formula is either a loss or not. However, we could change the previous formula if we consider that an error can happen without fault. Furthermore, this level of abstraction makes it impossible to know which kind of loss occurs, such as loss of life, loss of regulatory conformity, or loss of customer satisfaction.

As we can see, propositional modeling has limitations due to its abstraction and distance from reality. However, it remains an interesting research axis to consider. Axiom combinations highlight dangerous combinations of events that were not anticipated by risk assessment methodologies.

4.2 Security Ceremonies and the Human Factor

Security ceremonies, introduced by Ellison [15], have been initially applied to network and security protocols to encompass everything considered out-of-band, such as humans. Ceremonies are a way to emphasize the need to include humans and their behavior in analyses. This is in response to the fact that, as Ellison [15] noted: *It is common for computer professionals to disparage human users as the source of all the flaws that make an excellently designed product malfunction*. This concept can be applied to any cyber-physical system that interacts with human users, variously called *socio-technical systems* [17,41], *socio-technical physical systems* [24], or *cyber-socio-technical system* [32]. As some other authors noted [5,30,33], there is a need to meld cyber security with social sciences. However, both the security ceremony analysis and security analysis of socio-technical systems are disciplines that are still in their early stages. The interdisciplinary combination of cyber resilience analysis and quantification of socio-technical systems is also an emergent field. The complexity of CPSs from an architecture and an operating point of view makes it challenging to quantify and assess cyber resilience. Many indicators, such as performance indicators and robustness, could be used to conduct resilience assessments. However, the abstraction problem remains a significant challenge in considering accurate resilience strategies. These aspects are related to CPSs architectures. Still, from our point of view, the human factor must also be considered in cyber resilience assessment and enhancement applied to complex systems. As such, cyber resilience analysis of CPSs needs to be regarded as a socio-technical challenge. However, the formal analysis requires clarifying the ceremony's structure to build a ceremony model.

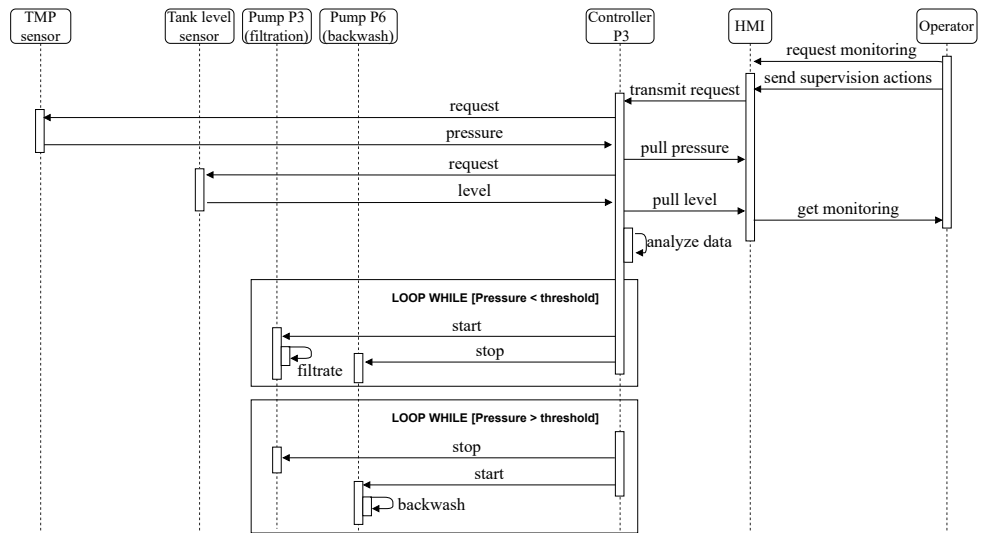
The model defined in [4] spans several socio-technical layers, ranging from a computer network to society.

In the literature, Bella *et al.* [6] use Tamarin to present a distributed and interacting threat model related to humans involved in security ceremonies. Radke *et al.* [33] investigated security flaws in three security ceremonies, named HTTP, EMV, and Opera Mini. In their work [9], Carlos *et al.* present a dynamic threat model for a dynamic analysis of the corresponding ceremonies. Johansen and Jøsang [22] follow a different approach and present a model based on user-interaction information obtained by sociologists to model human actions as a probabilistic process. Martina and Carlos [27] proposed an extended abstract that formalizes human-cognitive processes in security ceremonies for protocol verification. From the resilience perspective, Haring *et al.* [20] explore the resilience quantification of socio-technical CPSs.

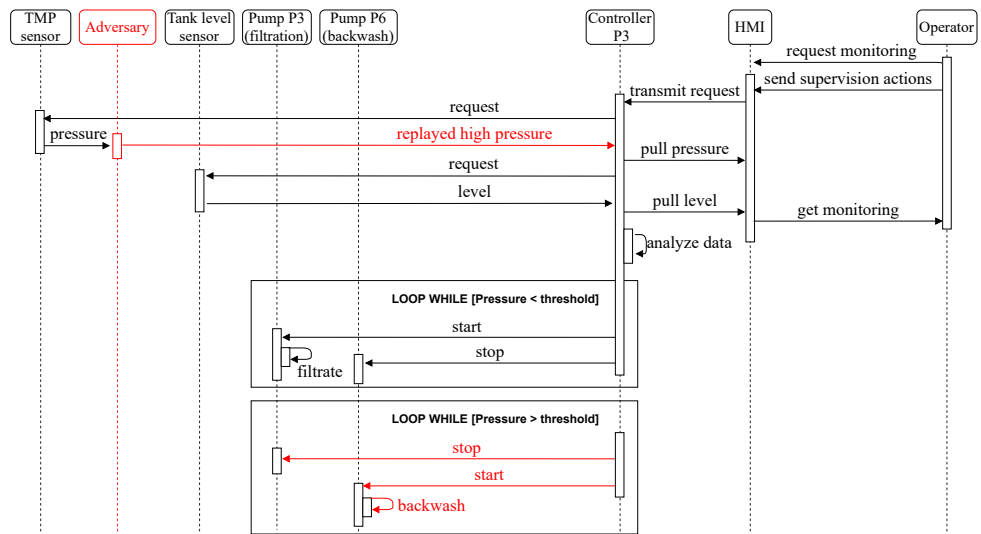
We consider the SWaT system presented with more details in Section 3.4. The Figure 9 shows two exchange diagrams of the third phase of SWaT dedicated to the UF process, namely normal operating (Fig 9(a)) and facing a replay-adversary (Fig 9(b)). Seven roles have been identified, namely: *Operator* (the human supervisor having access to the monitoring system of the plant); *IHM* (the human-machine interface itself); *Controller P3* (the controller assigned to the UF phase of SWaT); *Pump P6* (the backwash pump involved after a filtration cycle); *Pump P3* (the pump sending water through the UF membrane during a filtration cycle); *Tank level* (the ultrasonic level sensor of the feed tank); *TMP* (the Transmembrane Pressure (TMP) sensor of the UF unit); plus an additional role dedicated to the replay-adversary in the diagram presented in Fig 9(b).

The SWaT test bed has been studied and exposed to many different attacks to analyze its behavior under constraints. An example of a powerful attack perpetrated against the system is the one compromising the readings sent by the TMP sensor (located on the UF membrane, in the third sub-function) to the corresponding controller [29]. Indeed, this pressure sensor, measuring the cake layer formation pressure on the membrane, tells the controller to switch from a filtration cycle to a backwash cycle. The study has shown that an adversary attempting to compromise the readings made by the sensor and sent to the controller by increasing the measured pressure values could put the system in a perpetual backwash cycle, interrupting the production of purified water. The attack is impactful, leading to different kinds of losses such as financial loss (due to the production lack of clean water), reputation loss (due to the impact on the mission of the system), loss or damage to the material of the system (a membrane submitted of a high-pressure backwash during too much time could be degraded), and loss of mission and loss of customer satisfaction (due to the incapacity to clean the water).

According to the literature, an adversary attempting to perpetrate such an attack can do so in four different ways: (i) man-in-the-middle attack: the adversary must intercept the legitimate traffic through the network, then send corrupted data to the intended destination, i.e., the controller; (ii) replay attack (a kind of man-in-the-middle attack): the adversary must eavesdrop on the net-



(a) Exchange diagram of the ultrafiltration phase of SWaT in normal condition.



(b) Exchange diagram of the ultrafiltration phase of SWaT facing a replay attack.

Fig. 9. Exchange diagrams of the ultrafiltration phase of SWaT [12].

work, mimic legitimate data and replay it to the controller; (iii) jamming attack: the adversary must know the transmission power and modulation scheme of the communicating parties; and (iv) hardware Trojan attack: it requires modification of an Integrated Circuit (IC).

4.3 Summary

We have presented several approaches that consider qualitative resilience assessment. Other approaches are described in [11], including methodologies based on events handling, fuzzy rules, frameworks, and guidelines.

The approaches that we have presented are based on symbolic modeling, which offers interesting research axes, such as the theorem-proving strategies applied to the top layers of a multi-layered architecture, associated with model-checking strategies applied to the lower levels, which are dedicated to the physical, and component views of a given system. It is important to note that symbolic modeling methodologies could be complex to apply to models. However, some approaches such as the one applied by Sempreboni *et al.* [36] are interesting to consider due to their ability to capture unexpected human actions.

5 Further Research Directions

Through the previous sections, we reviewed various techniques and methodologies for resilience assessment and enhancement purposes. A new comparison between these approaches is presented in Table 1. To go beyond this comparison, we must highlight that choosing an appropriate resilience enhancement strategy depends on the system. Indeed, symbolic methodologies based on model-checking and theorem proving are suitable to conduct a resilience analysis of an IC component. On the other hand, multi-layer modeling and knowledge graphs are suitable for complex systems such as maritime ports or water treatment stations involving various families of components or many stakeholders. Graph models are adapted to network architectures or smart-grid systems.

Some of the approaches presented provide answers to specific questions. Indeed, dealing with the resilience quantification of complex systems in the context of Industry 4.0 implies using models and frameworks adapted to complex architectures. In this context, as covered in Section 3.3, multi-layered models are attractive for two reasons. They can represent an architecture consisting of an overlay of layers that captures how the components, functions, and sub-systems work together and communicate. Such a multi-layered representation constitutes a foundation for introducing resilience strategies at each system level. The main challenge is to make each layer resilient without detrimental effects on the others.

Particular attention must also be paid to the interpretation attributed to metrics. Indeed, it has been established that the results obtained for a given metric could have several interpretations. These interpretations may be contradictory [14,25]. An example is the spectral radius applied to graph models. This

Table 1. Comparison of the presented approaches.

Approach	Scope	Limitations
Empirical	Based on the study of testbed and real system data.	Does not consider the constraints of real environments.
Analytical	Mathematical modeling for predicting a system's behavior.	Difficult to apply to complex systems.
Multi-layer	Infrastructures involving stakeholders or architectural levels.	Requires a level of abstraction to build all the layers.
Knowledge graph	Complex systems with complex interactions, difficult to model.	The way the graph is built impact the assessment results.
Symbolic	Model-checking and theorem-proving analysis.	Difficult to apply to complex systems. Difficult to use.
Ceremonies	Include the human factor and how complex relationships impact a system.	Requires a well-understanding of the way a system operates.

notion of graph models related to analytic metrics has been discussed in Section 3.2. On the one hand, a value increase from one design to another of the same system represented as graphs could reflect higher resilience. This is due to the increase in the density of links between two states, reflecting a lower risk of unreachable states in case of a node deletion, e.g., a component failure. On the other hand, a value increase can also be interpreted as lower resilience because a higher density of links between the states reflects a higher risk of producing cascading effects due to an attack. Two possible interpretations do not mean that a metric is useless for quantifying the resilience of a system. The spectral radius illustrates very well the fact that there is a delicate balance between increasing the resilience potential and mitigating the increase in the security risk [14].

Another research axis concerns the human factor in modeling and resilience assessment strategies, as covered in Section 4.2. It is well-known that many incidents are due to human factors. Ceremonies, which consider a system from a holistic point of view, can help evaluate the human factor. The underlying problem is the unpredictability of human actions. Risk analysis can help anticipate the wrong or dangerous actions that human people can perpetrate, but an accurate knowledge of the system is necessary. This problem is related to the prediction of cascading effects on complex systems. We have shown an example of an exchange diagram in Section 4.1 that can be used to predict the adversary's actions. However, there is a lack of tools to accurately quantify the impact of the human factor on resilience strategies.

What we know about resilience assessment strategies is that they are based on simulation. These simulation models can be applied to data provided by test beds, as covered in Section 3.1. We must highlight an intrinsic limitation in the data obtained with test beds. In a resilience assessment context, test bed-generated data do not capture the stress present in live scenarios, i.e., the actual operating conditions and characteristics of a specific environment. These particular features cannot be imagined or anticipated with test beds because they do not operate in a real environment. Thus, metrics applied to test bed data may yield erroneous or inaccurate results. Using live scenarios and stochastic engineering (e.g., use of chaos monkeys [28]) can address the limitations of test beds.

This notion of environment is also related to knowledge graphs, as discussed in Section 3.4. Indeed, knowledge graphs allow us to consider a higher diversity of entities than traditional graphs, such as abstract entities, e.g., missions, regulations, and stakeholders involved in the life cycle of a system. In our past research [14], we used traditional graphs mapped to square adjacency matrices to model physical and logical links between the components of a use case, a water treatment system. However, this model only considers physical elements such as controllers, valves, pumps, and sensors. The knowledge graph that we have presented in Section 3.4 shows the potential of the model in comparison to traditional graphs. With this supplementary knowledge, the anticipation of cascading effects is more accurate.

Advances in these research axes are essential to implement the resilience principles in smart infrastructures. However, we must note that the resilience concept can conflict with other objectives. Similar to the cyber security principle that was not taken into account by all organizations during the last decades, the resilience concept is not sufficiently valued and considered. This can be explained by the fact that increasing the resilience potential of an architecture is related to augmenting the diversity of the controllability and observability aspects [14]. This augmentation has a cost. Several organizations are not prepared to spend money to increase the resilience potential of their systems. Resilience also increases the complexity of an architecture. It is known that adding more components connected to the cyber world increases the attack surface. Increasing the complexity also increases the risk of cascading effects due to the high density of links between each component or function of a system.

In our opinion, accepting resilience is highly related to regulation. Indeed, a common basis must be established to ensure that resilience principles have been officially analyzed and proven to be of paramount importance to organizations. The Cyber Resilience Act [8,10] is an initiative that works on three guarantees: (i) providing harmonized rules when products or software including a digital component are brought to market; (ii) providing a cyber security requirements framework for the governance of the planning, design, and development and the maintenance of such products. Obligations must also be met at each stage of the value chain; (iii) providing a duty of care for the whole lifecycle of these products. Other initiatives, such as the General Data Protection Regulation (GDPR)

[31], which deals with data protection across the European Union, highlight the importance of regulations across several countries. These initiatives are very important to know which entity, organization, state or country is responsible in case of a problem with the conformity of products to resilience principles.

6 Conclusion

As the main conclusion, we can state that considering and applying resilience principles are based on several pillars. The first pillar is understanding the systems to be considered and acquiring sufficient knowledge about their behavior and missions to model them accurately. The second pillar is layered modeling for complex systems because the physical and cyber views depend on other levels, such as the mission, stakeholders, and business processes. The third pillar is the need to consider systems holistically, which involves threats from everywhere. The more we understand an architecture, the more we can avoid cascading effects with damaging consequences. In the context of such a holistic view, knowledge graphs have an exciting potential. They allow the modeling of various entities, their relationships, and structures. The absence of international regulations indicates that work remains to ensure that resilience principles are understood, accepted, and applied.

Acknowledgments — Authors acknowledge support from the European Commission (Horizon Europe projects DYNAMO and AI4CCAM, under grant agreements 101069601 and 101076911), the French Government (PFS project, under the “France 2030” program) and the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

1. AlHidaifi, S.M., Asghar, M.R., Ansari, I.S.: A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Comput. Surv.* (feb 2024). <https://doi.org/10.1145/3649218>, just Accepted
2. Barbeau, M., Cuppens, F., Cuppens, N., Dagnas, R., Garcia-Alfaro, J.: Metrics to enhance the resilience of cyber-physical systems. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 1167–1172 (2020). <https://doi.org/10.1109/TrustCom50675.2020.00156>
3. Barbeau, M., Cuppens, F., Cuppens, N., Dagnas, R., Garcia-Alfaro, J.: Resilience estimation of cyber-physical systems via quantitative metrics. *IEEE Access* **9**, 46462–46475 (2021). <https://doi.org/10.1109/ACCESS.2021.3066108>
4. Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) *Information Security and Privacy Research*. pp. 273–286. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
5. Bella, G., Curzon, P., Lenzini, G.: Service security and privacy as a socio-technical problem. *Journal of Computer Security* **23**(5), 563–585 (2015)

6. Bella, G., Giustolisi, R., Schürmann, C.: Modelling human threats in security ceremonies. *Journal of Computer Security* **30**(3), 411–433 (2022)
7. Berger, C., Eichhammer, P., Reiser, H.P., Domaschka, J., Hauck, F.J., Habiger, G.: A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms. *ACM Comput. Surv.* **54**(7) (sep 2021). <https://doi.org/10.1145/3462513>
8. Car, P., De Luca, S.: EU Cyber resilience act. EPRS, European Parliament (2022)
9. Carlos, M.C., Martina, J.E., Price, G., Custódio, R.F.: An updated threat model for security ceremonies. In: *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. p. 1836–1843. SAC '13, Association for Computing Machinery, New York, NY, USA (2013). <https://doi.org/10.1145/2480362.2480705>
10. Chiara, P.G.: The Cyber Resilience Act: the EU commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review* **3**(2), 255–272 (2022)
11. Clédél, T., Boulahia Cuppens, N., Cuppens, F., Dagnas, R.: Resilience properties and metrics: how far have we gone? *Journal of Surveillance, Security and Safety* **1**(2), 119–139 (2020)
12. iTrust (Center for Research in Cyber Security): Secure Water Treatment (SWaT Testbed). Tech. rep., SUTD (Singapore University of Technology and Design) (July 2021), version 4.4
13. Dagnas, R., Arabi, W., Yaich, R.: PFS L1.2 Étude prospective, description des métiers du port et navire du futur et architectures associées. Tech. rep., IRT SystemX (2023)
14. Dagnas, R., Barbeau, M., Boutin, M., Garcia-Alfaro, J., Yaich, R.: Exploring the quantitative resilience analysis of cyber-physical systems. In: *2023 IFIP Networking Conference (IFIP Networking)*. pp. 1–6 (2023). <https://doi.org/10.23919/IFIPNetworking57963.2023.10186355>
15. Ellison, C.: Ceremony design and analysis. *Cryptology EPrint Archive* (2007)
16. Foote, A.: Woe-train: Ottawa’s LRT troubles, by the numbers. CBC (2019)
17. Giustolisi, R.: Free rides in denmark: lessons from improperly generated mobile transport tickets. In: *Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017, Proceedings 22*. pp. 159–174. Springer (2017)
18. Haimes, Y.Y.: On the definition of resilience in systems. *Risk Analysis: An International Journal* **29**(4), 498–501 (2009)
19. Hankel, M., Rexroth, B.: The reference architectural model industrie 4.0 (rami 4.0). *Zvei* **2**(2), 4–9 (2015)
20. Häring, I., Ebenhöch, S., Stolz, A.: Quantifying resilience for resilience engineering of socio technical systems. *European Journal for Security Research* **1**, 21–58 (2016)
21. Hutson, G., Jackson, M.: *Graph Data Modeling in Python: A practical guide to curating, analyzing, and modeling data with graphs*. Packt Publishing (2023)
22. Johansen, C., Jøsang, A.: Probabilistic modelling of humans in security ceremonies. In: Garcia-Alfaro, J., Herrera-Joancomartí, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F., Suri, N. (eds.) *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. pp. 277–292. Springer International Publishing, Cham (2015)
23. Kott, A., Linkov, I.: *Cyber Resilience of Systems and Networks*. Springer Publishing Company, Incorporated, 1st edn. (2018)
24. Lenzini, G., Mauw, S., Ouchani, S.: Security analysis of socio-technical physical systems. *Computers & electrical engineering* **47**, 258–274 (2015)
25. Lewis, T.G.: The many faces of resilience. *Communications of the ACM* **66**(1), 56–61 (2022)

26. Lin, S.W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., Torenbeek, R., Duggal, D., Martin, R., Bleakley, G., et al.: Industrial internet reference architecture. Industrial Internet Consortium (IIC), Tech. Rep (2015)
27. Martina, J.E., Carlos, M.C.: Why should we analyse security ceremonies. Proc. of CryptoForma (2010)
28. Martinez, A.G.: Chaos monkeys: Obscene fortune and random failure in Silicon Valley. Harper Business (2016)
29. Mathur, A.P., Tippenhauer, N.O.: SWaT: a water treatment testbed for research and training on ICS security. In: 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater). pp. 31–36 (2016). <https://doi.org/10.1109/CySWater.2016.7469060>
30. Nowak, V., Ullrich, J., Weippl, E.: Cybersecurity is more than a technological matter—towards considering critical infrastructures as socio-technical systems. Applied Cybersecurity & Internet Governance **1** (2023)
31. Parliament, E., Council, E.: General data protection regulation. official Journal of the European Union **59**, 294 (2016)
32. Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A., Villani, M.L.: Wax: An integrated conceptual framework for the analysis of cyber-socio-technical systems. Safety science **136**, 105142 (2021)
33. Radke, K., Boyd, C., Gonzalez Nieto, J., Brereton, M.: Ceremony analysis: Strengths and weaknesses. In: Camenisch, J., Fischer-Hübner, S., Murayama, Y., Portmann, A., Rieder, C. (eds.) Future Challenges in Security and Privacy for Academia and Industry. pp. 104–115. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
34. Rao, K., Hanjra, M.A., Drechsel, P., Danso, G.: Business models and economic approaches supporting water reuse. Wastewater: Economic asset in an urbanizing world pp. 195–216 (2015)
35. Ryalat, M., ElMoaqet, H., AlFaouri, M.: Design of a smart factory based on cyber-physical systems and internet of things towards industry 4.0. Applied Sciences **13**(4), 2156 (2023)
36. Sempredoni, D., Viganò, L.: X-men: A mutation-based approach for the formal analysis of security ceremonies. In: 2020 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 87–104 (2020). <https://doi.org/10.1109/EuroSP48549.2020.00014>
37. Sikos, L.F.: Cybersecurity knowledge graphs. Knowledge and Information Systems pp. 1–21 (2023)
38. Sinibaldi, T.: Les Smart Ports, Radar International des Solutions Smart Appliquées aux Ports de Commerce. Wavestone (2019)
39. SystemX, I.: PFS: Secure Ports of the Future. IRT SystemX Website (2023)
40. Van Mieghem, P., Omic, J., Kooij, R.: Virus spread in networks. IEEE/ACM Transactions On Networking **17**(1), 1–14 (2008)
41. Viganò, L.: Formal methods for socio-technical security: (formal and automated analysis of security ceremonies). In: Coordination Models and Languages: 24th IFIP WG 6.1 International Conference, COORDINATION 2022, Held as Part of the 17th International Federated Conference on Distributed Computing Techniques, DisCoTec 2022, Lucca, Italy, June 13–17, 2022, Proceedings. pp. 3–14. Springer (2022)
42. Wang, X., Feng, L., Kooij, R.E., Marzo, J.L.: Inconsistencies among spectral robustness metrics. In: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. pp. 119–136. Springer (2018)

43. Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., Kong, J., Jue, J.P.: All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture* **98**, 289–330 (2019). <https://doi.org/https://doi.org/10.1016/j.sysarc.2019.02.009>
44. Zahee, M.A.: RAMI 4.0 (part 1): Smart Electronic Industry 4.0 Architecture Layers. DZone (2017)
45. Zhang, K., Liu, J.: Review on the application of knowledge graph in cyber security assessment. *IOP Conference Series: Materials Science and Engineering* **768**(5), 052103 (mar 2020). <https://doi.org/10.1088/1757-899X/768/5/052103>