Clédel *et al. J Surveill Secur Saf* 2020;1:119-39
DOI: 10.20517/jsss.2020.08

Journal of Surveillance, Security and Safety

Review

Open Access

Resilience properties and metrics: how far have we gone?

Thomas Clédel[1], Nora Cuppens[1,2], Frédéric Cuppens[1,2], Romain Dagnas[3]

[1]Department of systems, networks, cybersecurity and digital law, IMT Atlantique, Cesson-Sévigné 35510, France.
[2]Department of IT and software engineering, Polytechnique Montréal, Montréal, QC H3T 1J4, Canada.
[3]Cybersecurity Team, IRT SystemX, Palaiseau 91120, France.

Correspondence to: Prof. Nora Cuppens, Department of IT and software engineering, Polytechnique Montréal, 2500 Chemin de Polytechnique, Montréal, QC H3T 1J4, Canada. E-mail: nora.boulahia-cuppens@polymtl.ca; ORCID: 0000-0001-8792-0413.

How to cite this article: Clédel T, Cuppens N, Cuppens F, Dagnas R. Resilience properties and metrics: how far have we gone?. *J Surveill Secur Saf* 2020;1:119-39. http://dx.doi.org/10.20517/jsss.2020.08

Received: 6 Mar 2020 **First Decision:** 19 May 2020 **Revised:** 31 Aug 2020 **Accepted:** 31 Oct 2020 **Published:** 30 Nov 2020

Academic Editor: Xiaofeng Chen **Copy Editor:** Cai-Hong Wang **Production Editor:** Jing Yu

Abstract

Aim: Resilience is discussed among researchers and practitioners for several decades, but its definition has been questioned even recently and many methods are proposed to evaluate the resilience of systems. This paper presents a review of historic and recent research articles that define and/or propose a way to measure resilience of systems.

Methods: While definitions are classified according to the ideas they focus on, different categories of metrics are described, such as quantitative or qualitative approaches.

Results: This paper points out that many metrics tend to valuate resilience similarly. In fact, they are generally built upon a specific definition. On the other hand metrics can also be really heterogeneous and do not capture the same meaning of system resilience when different definitions of resilience are considered.

Conclusion: This paper aims at gathering and comparing metrics and definitions of resilience in order to determine the origins of the particularities and classify them according to the attributes they take into account.

Keywords: Resilience, metrics/measurement, survey

1. INTRODUCTION

Risk assessment has been the dominant paradigm for system design and management for decades, especially in the case of cyber-physical systems (CPS). These systems are used in critical infrastructures, and a "well-designed risk assessment of CPS will provide an overall view of CPS security status and support efficient allocations of safeguard resources"[1]. Furthermore, "With an understanding of risk, it is then possible for an operator to prioritise the implementation of resilience measures"[2] (additional research results related to this work are available at: http://www.cost-recodis.eu). However, unprecedented adverse events such as natural disasters (the Fukushima Daiichi nuclear accident) or cyber-attacks (StuxNet or BlackEnenergy) have caused unexpected losses. These events have highlighted some weaknesses of well-established models and frameworks. As a consequence, it has recently been accepted by scientific communities and governments that risks threatening critical infrastructure cannot all be identified or prevented and that there is a need for new approaches to mitigate damages. Resilience emerged from this lesson as the logical way to overcome the limitations of previous dominant approaches that are risk assessment and system safety.

While systems were considered safe by design and failures caused by human errors, it is now accepted that mismatches exist between administrative procedures and the ways in which systems actually run. Indeed, normal system performance, resulting from required adjustments, adaptations, and optimizations must be distinguished from normative system performance that is prescribed by rules and regulation[3].

Some studies and audits have been conducted in modern industries and different environments to assess whether resilience was considered during the design and planning phases of industrial processes, and how resilience strategies are applied during the operational phase. Studied environments include nuclear plants[4], electricity distribution[5], chemical plants[6,7], sea fishing[8], oil distribution plants[9], railways[10], *etc*. Carvalho *et al.*[4] introduced a framework for the analysis of micro incidents during nuclear power plant operations. Saurin *et al.*[5] improved a method for assessing health and safety management systems. Azadeh *et al.*[6] presented a new concept of resilience engineering, which includes teamwork, self-organization, redundancy, and fault-tolerance, while Shirali *et al.*[7] identified the challenges that occur in the process of building resilience engineering and its adaptive capacity in a chemical plant. Morel *et al.*[8] focused on "the relationship between resilience and safety, and discusses the choice of strategies for safety-improving interventions, taking into account the system's financial performance and the legal pressure to which it is subjected". Abech *et al.*[9] presented the challenges in order to improve resilience in an oil distribution plant. Hale *et al.*[10] proposed an evaluation, which shows that railways are "examples of poor, or at best mixed, resilience, which can, however, still achieve high levels of safety, at least in certain areas of their operations". Most of these studies conclude that some resilience mechanisms inherently exist in these environments. However, these resilience mechanisms may not always be recognized as such by employees. They demonstrate how people adapt to challenging situations where operational, plannings and procedures are in conflict.

The absence of consensus for a definition of resilience, as well as the abundance of metrics evaluating resilience and the over-dominance of risk assessment and system safety, can explain that resilience is rarely applied and considered as a system design and management paradigm. However, it can be noticed that definitions and metrics are not as heterogeneous since only few criteria are used in the current article to classify them. While some metrics clearly differ from the others and do not evaluate the same "resilience", many definitions and metrics are in fact variations of others. Some of them can be considered as refinements of older metrics or definitions. Occasionally, variations can be justified by a will to produce a domain specific evaluation of resilience.

The goal of this article is not to provide an exhaustive list of articles that deal with resilience. Many articles propose mechanisms, techniques, and technologies to improve resilience of systems but fewer articles provide their own definition and/or metric of resilience, and fewer still provide an original definition or metric. In fact,

many measures and definitions are derived from more original ones, so that those that share a common origin also share many characteristics. The current paper aims at gathering and comparing metrics and definitions of resilience so that common criteria and differentiation criteria emerge from them. This way, categories of metrics and definitions can be defined. To identify pertinent literature, online database searching was performed on databases such as Web of Science and DBLP. Articles were filtered with the keyword "resilience" and a set of other keywords, including "metrics", "measure", evaluation", and "framework". The most relevant were selected on the basis of their titles, abstracts, and whether they applied to the field of engineering. A second step in this research consisted in cross-referencing the sources of the previously selected articles in order to determine the origins of the particularities of their definitions and metrics.

This paper is organized as follows. Section 2 provides a survey of definitions of resilience, from its original definition in ecological system to recent definitions in networks and cyber-physical systems. Definitions are classified according to the ideas they focus on. Because there are many definitions for resilience, the expected attributes of a resilient system can slightly differ from one article to an other. Thus, a description of the various attributes associated with resilience is given in Section 3. Then, a survey of different metrics used to evaluate the resilience of systems is provided in Section 4. Some metrics consist in measuring separately some attributes of resilience and then combining them. Others evaluate resilience without considering what the various capacities that compose resilience, and they measure the impact of harmful events that occurred on a system to assess the level of resilience of this system for these events. All considered metrics are classified according to the attributes they take into account. The results of this classification are summarized in a table at the end of the section. Since resilience is a complex property, it may often be confused with other concepts and system properties. Section 5 provides results of some articles that compare resilience with other properties such as robustness and risk assessment. Section 6 discusses the existing limitations and gaps in the described definitions and metrics. Additionally, it provides the conclusion of this study.

2. RESILIENCE DEFINITIONS

The term "resilience" comes from the Latin word "resilire", which has several interpretations such as "to rebound", to "spring back", or "to withdraw into oneself". Even if the current meaning of "resilience" differs slightly from its Latin origin and despite the diversity of definitions, most of them fit with at least one of these antic meanings. The resilience perspective emerged in the 70s from ecology with the work by Holling[11]. A few years later, the resilience concept began to influence other fields such as anthropology, sociology, or psychology, as described in[12], before it reached engineering sciences and, even more recently, into computer science and information technologies.

The notion of resilience was first developed in some domains such as ecology with the work by Holling[11]. Resilience of a population is defined as a system property where the system behavior is less important than the system persistence. Thus, resilience is distinguished from stability. The author described it as the capacity of a system to move from a stability domain into another one and put the emphasis on "a high capability of absorbing periodic extremes of fluctuations", the maintainability of "flexibility above all else", and a capacity to "restore its ability to respond to subsequent unpredictable environmental changes". Historically, resilience has also been developed in psychology and refers to the ability to recover from trauma and crisis[13] while "childhood resilience is the phenomenon of positive adaptation despite significant life adversities"[14].

2.1. A system property

Francis and Bekera[15] described resilience as a system property to endure undesired events in order to ensure "the continuity of normal system function". This ability corresponds to three system's capacities: absorptive, adaptive, and restorative capacities. It could be considered that this definition goes against the original concept of resilience given by Holling[11] as the continuity of normal function can be considered as a synonym of system

stability. However, the authors also specified that resilience postulates flexibility in terms of performance, structure and function while these changes are not irreversible or unacceptable.

Resilience is also defined as the maintenance of "state awareness and an accepted level of operational normalcy in response to disturbances"[16]. Operational normalcy corresponds to the maintenance of "stability and integrity of core processes" according to McDonald[17] and resilience was described by Wreathall[18] as the ability to "keep, or recover quickly to, a stable state". These definitions confirm the previous description as resilience focuses on some operational stability even if systems are supposed to "tolerate fluctuations via their structure, design parameters, control structure and control parameters"[19]. A new point highlighted by this definition is the need to collect and fusion data concerning the current state of the system. This knowledge aims at knowing the current date of the system and its environment and is a basis for decisions[18]. Processes to collect, fuse, and prioritize information should be considered when designing resilient systems. Indeed, resilient systems should not be considered as a single technology but as a complex integrated system of systems that ensures coordination among subsystems through communication and sharing of information[20].

2.2. Resilience is related to service delivery

Sterbenz *et al.*[21] considered systems as networks, and their resilience is defined as the ability "to provide and maintain an acceptable level of service in face of various faults and challenges to normal operation". This definition is close to another one given by Laprie[22], where resilience is "the persistence of service delivery that can justifiably be trusted, when facing changes". For both definitions, resilience focuses on service delivery and particularly on avoidance of service failure. System services are the system behavior as it is perceived by its users[23]. They are different from system functions which correspond to the expected result of the system behavior, in other words what the system is intended to do. Delving into a more specific domain of cyber-physical system, Clark and Zonouz[24] defined resilience as the "maintenance of the core [. . .] set of crucial sub-functionalities despite adversarial misbehaviors" and a guarantee of "recovery of the normal operation of the affected sub-functionalities within a predefined cost-limit". Again, this definition reinforces the need to maintain a service delivery above a fixed threshold. If a perturbation leads the system to be under this threshold, then the system is in an unacceptable state and has failed to be resilient.

Power systems are also considered[25], and resilience is defined as the "ability to maintain continuous electricity flow to customers given a certain load prioritization scheme". According to the authors, traditional risk assessment is not the best approach to achieve resilience as resilience concerns "unexpected rare extreme failures" whose likelihood cannot be easily estimated. Thus, this definition completes the previous ones as it focuses on service delivery and underlines that some services are more critical than others and should not be interrupted.

2.3. Events handling

A commonly accepted definition of resilience was given by Vugrin *et al.*[26]. Resilience is described as the ability of a system, for a given disruptive event, to "reduce 'efficiently' both the magnitude and the duration of the deviation from targeted 'system performance' levels". This definition has frequently been used to propose resilience metrics based on system performance such as some metrics detailed in Sections 4.1 and 4.2. This definition and its derived metrics also imply that a system has different levels of resilience to different disruptions and an evaluation of resilience is needed for every specific disruption.

Ayyub's definition of resilience is close to the previous one[27], as resilience is said to be "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions". On the contrary of the previous definition, resilience is not only concerned with the occurrence of disruptions, but is also considered in a pre-disruption phase as a need for preparation and evolution is pointed out by this definition.

Another similar definition was given by Haimes[28] as resilience is "the ability of a system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks". Compared to the previously described definitions, Haimes pointed at the need to estimate the cost of the recovery process.

Another definition of resilience was considered by Mauthe *et al.*[2]. This definition is applied to communication networks: "Resilience of a communication network is its ability to maintain the same level of functionality in the face of internal changes and external disturbances as a result of large-scale natural disasters and corresponding failures, weather-based disruptions, technology-related disasters, and malicious human activities."

However, some definitions do not consider the amplitude of disruptions. Dinh *et al.*[29] defined resilience as "the ability to recover as soon as possible after an unexpected situation". The authors nevertheless pointed out the need to minimize disruptions consequences but only with a view of faster recovery.

Hollnagel[3] defined resilience as "the ability of a system or an organization to react to and recover from disturbances at an early stage, with minimal effect on the dynamic stability." Hale and Heijer's definition describes resilience as "the characteristic of managing the organisation's activities to anticipate and circumvent threats to its existence and primary goals"[30]. Resilience is also "the ability of systems to prevent or adapt to changing conditions in order to maintain (control over) a system property"[31]. On the other hand, Sundström and Hollnagel described resilience as "an organizations ability to adjust successfully to the compounded impact of internal and external events over a significant time period"[32]. Another definition from Wreathall describes resilience as "the ability of an organization (system) to keep, or recover quickly to, a stable state, allowing it to continue operations during and after a major mishap or in the presence of continuous significant stresses"[18].

2.4 Other definitions

Recent work suggests looking at resilience with a different perspective. Thompson[33] considered a system as a set of resources for which particular states are expected, such as ensuring personal safety, preserving confidentiality of a database, etc. Security is the system capacity to maintain expected states of resources. However, security breaches can occur and resilience is defined as "the maintenance of a nominated state of security". This resilience is achieved by detecting, containing, and resolving a security breach. While many approaches only consider resilience of accidental faults, this one seems to focus only on attacks. We provide a classification of resilience definitions in Table 1

3. DESCRIPTION OF RESILIENT SYSTEMS

It is commonly accepted that resilience of a system is supported by three system capacities. These capacities were first described in 1973[11]. Holling compared the resilience of a population with a game "in which the only payoff is to stay in the game". Thus, a resilient population has "a high capability of absorbing periodic extremes of fluctuation", maintains "flexibility above all else", and can "restore its ability to respond to subsequent unpredictable environmental changes". They are known as absorbability, adaptability, and restorability and are considered so central to the notion of resilience that they are frequently used to define resilience[15,34]..

3.1. Absorbability

This capacity is "the degree to which a system can automatically absorb the impacts of systems perturbations and minimize consequences with little effort"[26]. Considering power systems, Arghandeh *et al.*[25] explained that the absorbing potential of a system "depends on the components" design characteristics, the system topology, the control philosophy, and the protection coordination". Indeed, features such as robustness, redundancy, diversity, and defense in-depth enhance the absorbability of a system and provide higher survivability[20]. This capacity is sometimes designed as buffering capacities[35] and corresponds to the maxi-

Table 1. Table of resilience definitions

Reference	Definition orientation				Goal
	Events handling	System stability	Service delivery	Resilience capacities	
Ayyub [27]	✓				Preparation, adaption, resistance, recovery
Dinh *et al.* [29]	✓				Fast post-event recovery
Haimes [28]	✓				Acceptable degradation, time, and costs
Vugrin*et al.* [26]	✓				Reduction of the performance level deviation
Werner [13]	✓				Psychological and social adaptation
Hollnagel [3]	✓				Recover from disturbances at an early stage
Hale and Heijer [30]	✓				Managing activities, anticipation of threats
Leveson *et al.* [31]	✓				Prevent/adapt to maintain a system property
Sundström and Hollnagel [32]	✓				Ability to adjust in a long time period
Wreathall [18]	✓				Continuity of operations during/after a mishap
Mauthe *et al.* [2]	✓				Same level of functionality in case of changes
McDonald [17]		✓			Stability and integrity of core processes
Rieger [16]		✓			State awareness and operational normalcy
Wreathall [18]		✓			Keeping or quick recovery of a stable state
Arghandeh *et al.* [25]			✓		Continuity of electricity flow
Clark and Zonouz [24]			✓		Service delivery and guarantee of recovery
Sterbenz *et al.* [21]			✓		Maintenance of an acceptable level of service
Thompson *et al.* [33]			✓		Maintenance of security state
Francis and Bekera [15]			✓	✓	Continuity of normal service function
Holling [11]				✓	Population survival
Wei and Ji [34]				✓	Incidents handling

mal amplitude of disruptions that can be tolerated. To buffering capacities, Woods specified a need for margin and tolerance assessments that determine how closely and how well a system is currently running near to its performance boundaries.

Moreover, resilience is not directly associated with a capacity to absorb and mitigate incidents [22,36]. However, a need for diversity is specified as it prevent vulnerabilities to become a single point of failure. This diversity manages the vulnerabilities of components to incidents by the use of different components and processes for similar functions, but it should also consider the exposition of components and processes to these incidents with geographic or topological dispersion for example. Dinh *et al.* [29] decomposed absorbability into two complementary properties. The first property is flexibility and can be considered as a synonym of stability in the cited article, as it consists in maintaining the system production variation into a desired range while inputs are changing slightly. The second property is controllability and indicates how easily a system can be brought in a desired state.

3.2. Adaptability

Adaptability [26], also known as flexibility [35], is "the degree to which the system is capable of self-reorganization for recovery of system performance" and is described as "the ability to replace component or input with another" or the "system's ability to restructure itself" to face changes and external pressures. While this description could be associated with diversity, which is more commonly interpreted as part of absorbability, adaptability is also concerned with changing the system structure, policies, and priorities to mitigate the impact of a disruption.

Some works refer to adaptability as evolvability [22,36]. It represents the ability of a system to "accommodate changes" by upgrading itself with new functions or technologies during design and implementation phases or by dynamically adjusting its behavior or its architecture to face operational faults and attacks. Moreover, in [30], the authors affirmed that resilience has to be continuously kept up-to-date as it can disappear or be ineffective against specific threats.

One possible adaptive mechanism is the use of safe mode controls. It consists in using simple but extremely reliable systems that prevent critical failures [20]. Safe mode depends on few input sources such as Earth's

magnet field is used to control spacecraft stability[37], and the used sensors are reliable and redundant enough so that the safe mode system is considered "fail safe". By definition, safe mode is designed to limit the impact of a perturbation but not to mitigate it. It ensures a minimal system function.

3.3. Recoverability

Recoverability is determined by internal and external entities and their capacity to easily restore the system to its original state or a better one. It consists in dynamic mechanisms such as repairing or replacing damaged components, reinitializing components to a proper state, etc. While adaptability can alter the system structure to preserve or restore system performance, recoverability aims at "returning a system to near its original structure"[26]. Moreover, adaptive changes are in general temporary, whereas restorative changes are expected to be as permanent as possible.

3.4. Other capacities and descriptions

While the works[22,36] described absorbability (with diversity) and adaptability (evolvability) as resilience capacities, restorability is not considered. In place of it, it is claimed that a resilient system has "assessability" and usability. Assessability is the ability to verify and evaluate if a system behaves properly and if the quality of service is delivered. This verification and evaluation can be performed during design and pre-deployment phases but should also be an ongoing process as systems are supposed to evolve. Usability describes how ergonomic user interfaces are. It consists in measuring how easy it is to learn basic tasks, memorize them, and avoid errors; how quickly tasks can be performed; and how pleasant the interface is to use. Usability is needed as systems are more and more complex and errors can lead to critical failures.

Some works[29,34] describe a resilient system as one that can anticipate and handle unexpected events. They describe capacities that such systems have: security (minimization of the incidence of undesirable events), mitigation/minimization capacity, and recovery ability. This description of resilience differs from the others for two reasons. Firstly, security is taken into account while resilience is generally considered only when an incident occurs, in other words, after security has failed. The second reason is the absence of adaptability amongst resilience capacities, even if the authors of both articles gave an example of minimization capacity that could be interpreted as adaptability. Indeed, minimization capacity includes an ability to detect disruptions and faults as soon as possible and to enable mitigation measures.

Resilience has been decomposed into three capacities[33]. First, a system must recognize and identify security breaches, which is a detection ability. A second capacity, containment, is the ability of a system to absorb and limit the impact of security breaches. The third capacity is resolution and consists in eradicating security breaches and restoring the system. Even if those capacities are not explicitly the three traditional ones, they are not unrelated. Recoverability is included in the resolution capacity. Detection and containment capacities have the same objectives as absorbability and adaptability: to maintain an acceptable level of service while facing and eradicating the security breaches. Although the authors did not describe how a system could face a security breach when detected, they pointed out that two resilience mechanisms come into play: survivability and impact limitation.

4.HOW TO MEASURE RESILIENCE

4.1 Quantitative deterministic

The articles described in this section use different measures for system performances or about some characteristics of an undesired event to build a metric of resilience. While most of these metrics provide a resilience value for a system, others consist in providing a score for different factors that compose resilience. They are denoted semi-quantitative approaches. The provided scores give clues concerning the resilience of a system but do not precisely result in a measure of it.

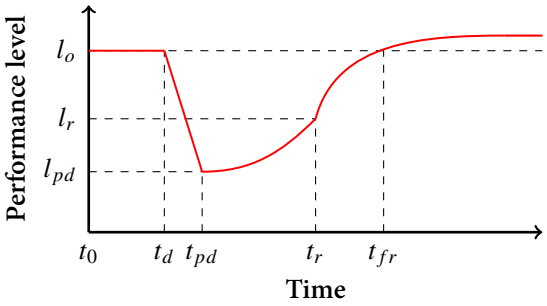

Figure 1. Performance level during the handling of a disruption (fault or attack).

Accidents and incidents cannot be considered as an absolute and direct indicator of system resilience [4]. External factors such as disturbances and attacks are not intrinsic properties of system resilience and their involvement in resilience metrics can be argued [38]. However, clues and markers of resilience can be provided by the analysis of the system dynamics and the interplay of its subsystems during the occurrence of these events.

With this in mind, several metrics evaluate resilience from the actual level of performance of a system during the occurrence of an unexpected event. Level performance can be used to illustrate different business cases [39] such as production capacity, quality, waste, cost, etc. The less performance is affected, the more resilient the system is. These metrics are event specific, which means that an event (fault or attack), or a set of events, is determined and the system resilience to this event is evaluated. It implies that resilience of a system should be evaluated for every known event or set of events that can occur in the system. This kind of metric is illustrated in Figure 1. Four times are generally considered. (1) t_d corresponds to the occurrence of a disruption. Before t_d, the system works at its original performance level l_o. (2) Despite absorption and adaptation mechanisms, the performance level is degraded by the disruption and reaches its lowest level l_{pd}. This moment is called the post-disruption time, t_{pd}. (3) Resilient mechanisms allow the system to partially recover until the disruption is resolved at time t_r. (4) Recovery mechanisms come into play and the system returns to its original level performance. The system has fully recovered from the disruption at t_{fr} but evolving capacities can allow the system to improve its performance after that.

The authors of [26,34] evaluated the performance loss due to a disruption as the integral of the difference between the original level and the actual level of performance on the interval $[t_d, t_{rf}]$. For the sake of comparison, Gholami *et al.* [40] proposed to use a per-unitized metric such that resilience is a ratio bounded in the range $[0, 1]$. Ayyub [27] proposed something similar but the expected performance level of the system is not constant over time; it decreases with aging effects. As a consequence, the older a system is before a disruption, the less resilient it is, as described below. Let $\mathcal{P}$ and $\mathcal{P}_{exp}$ be the time-dependent functions that correspond to the actual and expected performance levels of the system, respectively:

- Performance loss [34]:

$$\mathcal{P}_{loss} = \int_{t_d}^{t_{fr}} \left(l_o - \mathcal{P}\left(t\right)\right)\, dt \tag{1}$$

- Resilience ratio [40]:

$$\mathcal{R}_r = \mathcal{P}_{loss} \Big/ \int_{t_d}^{t_{fr}} l_o\, dt \tag{2}$$

[27]:

$$\mathcal{R}_r = \frac{td + F.\left(t_{pd} - t_d\right) + R.\left(t_{fr} - t_{pd}\right)}{t_{fr}} \tag{3}$$

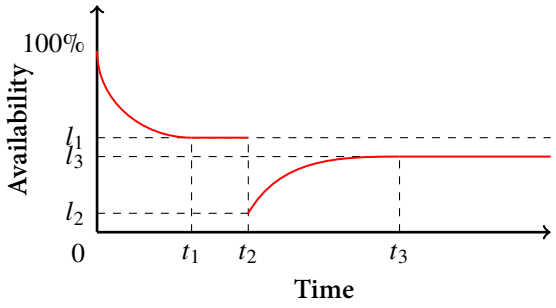

Figure 2. Availability of a system before, during, and after a shock[38].

with the failure profile

$$F = \int_{t_{pd}}^{t_d} \mathcal{P}(t)\ dt \Big/ \int_{t_{pd}}^{t_d} \mathcal{P}_{exp}(t)\ dt \tag{4}$$

and the recovery profile

$$R = \int_{t_{fr}}^{t_{pd}} \mathcal{P}(t)\ dt \Big/ \int_{t_{fr}}^{t_{pd}} \mathcal{P}_{exp}(t)\ dt \tag{5}$$

To this performance loss, called systemic impact[26], the authors added a recovery cost. This recovery cost corresponds to resources expended in recovery efforts, and, once combined with the performance loss, it gives the total loss due to a determined disruption, called recovery-dependent resilience[26].

Babiceanu and Seker[41] evaluated separately the loss of performance in three phases: degradation of performance from t_d to t_{pd}, balanced degradation from t_{pd} to t_r, and recovery of performance from t_r to t_{rf}. The evaluation is the same as the previous one: the integral of the difference between the original level and the actual level of performance over a period.

The resilience of a system to an event is evaluated by a resilience factor that is the product of three elements[15]: a degradation ratio l_{pd}/l_o, a partial recovery ratio l_r/l_o, and a speed factor t_r/t_δ. t_δ corresponds to the maximum acceptable value for t_r and $t_r > t_\delta$ implies that the system cannot recover from the disruption.

Cai *et al.*[38] used system availability instead of performance level. They defined availability as the ability to be in a state of performing a function if required external resources are provided. This approach is similar to the previously described ones in[15,26,41] and is depicted in Figure 2. The system begins at 100% of availability and then progressively reaches a stable level l_1 at time t_1. Then, n shocks impact the system at time t_2 and availability falls from l_1 to l_2. Resilience mechanisms handle these shocks such that availability reaches a post-shock steady state l_3 at time t_3. Thus, resilience is measured as the product of availability before and after shocks:

$$\text{(resilience)}^{[38]} : \mathcal{R} = \frac{l_1}{n \ln(t_1)} \sum_{i=1}^{n} \frac{l_3^i . l_2^i}{\ln\left(t_3^i - t_2^i\right)} \tag{6}$$

The authors claimed that the natural logarithm function is used to balance the availability and the recovery process of the system.

Sterbenz *et al.* proposed another approach to evaluate network resilience[42]. A system is composed of several layers: physical, link, topology, network path, end-to-end transport, and application. Each layer is represented

at a given time t by an operational state that consists in a $l \times m$ matrix of l operational metrics and m possible values, and a service state that consists in another $l \times m$ matrix of l service parameters and m possible values. Layers are overlapping such that the service state of a layer at time t becomes the operational state of the layer above at time $t + 1$. According to this model, the system resilience is evaluated at the boundary between two layers as the transition trajectory to move from the state of a layer to the state of the layer above.

Clark and Sonouz[24] used a linear time-invariant model to represent a system and its adversarial impacts. They considered a set of safe states and a basin of attraction that is a set of states allowing the system to return to a safe state under certain conditions. From these definitions, a system is considered resilient to an adversarial event as long as it remains in a safe state or in a state included in a basin of attraction. Since attackers can either physically attack the system or compromise input signals or inject false data, impacts of an attack are modeled as modified input and state matrices. Once a system and an attack are modeled, it can be determined if the system is resilient to this attack. Nonetheless, resilience can be evaluated as the amplitude of adversarial event that must impact the system to pull it out of safe states and basins of attraction. This idea of an attraction basin can be found in the original article of Holling[11], as described in Section 4.2.

4.1.1. Semi-quantitative approach

Shirali *et al.*[43] used six previously described resilient factors[18]: management commitment, reporting culture, learning culture, awareness, preparedness, and flexibility. Employees of an industry are divided into several groups corresponding to process units and are given a questionnaire. After gathering the questionnaires, a score from one to five is given for each resilient factor and for each group of employees. From these scores, managers can identify weaknesses in some resilient factors for some specific groups of employees. Despite this, interconnections between the six resilient factors or between groups of employees are not considered in this approach.

4.2.Quantitative probabilistic

Probabilistic approaches relate resilience with uncertainties and thus they add a stochastic component to the resilience evaluation. For several of them, denoted as event specific, this is the resilience of a system to a determined event that is evaluated. Generally, the probabilities considered in a resilience evaluation come from the stochasticity of occurrence of undesired events.

Originally, Holling did not provide metrics and methods to evaluate resilience in his article about resilience and stability of ecological systems[11]. According to Holling, resilience is only concerned with populations extinctions and resilience is the ability of a population to move from a stable population state to another one. Thus two parameters must be considered to evaluate resilience: the probability that an incident moves the population outside a stable state and the distance between stable states that determines how harmful the incident must be to lead to extinction. However, Holling explained that such measures require an immense amount of knowledge about the system.

4.2.1. Event Specific

Haimes claimed that resilience of a system can be determined only once a threat scenario is determined[28,44]: "the question 'What is the resilience of cyberinfrastructure X ?' is unanswerable". According to other articles, resilience can be evaluated only once all possible undesired events are determined[34]. For example, in addition to a quantitative deterministic evaluation of resilience, Babiceanu and Seker[41] provided two probabilistic metrics. The first extra metric is the probability of occurrence of a disruptive event that is the product of three other probabilities, the probability of a system to be vulnerable, the probability to be attacked, and the conditional probability of security to be bypassed (the attack is successful). The second extra metric is the probability of the system to recover from this event. It depends on the availability of a resilience solution for

this event, the conditional probability of this solution to be activated and the conditional probability of the system to recover once resilience mechanisms are engaged.

Once all undesired events are determined, resilience of a system is the sum, for all these events, of the probability of occurrence of each event multiplied by a resilience factor [15]. The resilience factor is system specific and event specific, as described in Section 4.1. For this metric, resilience factors are weighted with a fragility function that corresponds to a probability function of system failure. This fragility function is also event specific. On top of that, probabilities of the occurrence of events is combined with an entropy factor that represents the uncertainty of these probability distributions.

Thompson *et al.* [33] presented resilience as the maintenance of a security level and resilience is achieved in three steps: detection, containment, and resolution. According to this description, a metric based on these three capacities is proposed [45]. For a determined security breach, a probability is assigned to each of these capacities and represents the probability that the breach is detected, contained, or resolved. The authors argued that three events can lead to the restoration of the expected security state: (1) the breach is detected, then contained, and finally resolved; (2) the breach is detected and resolved without containment; and (3) the breach is resolved without detection or containment. As these events are independent, resilience is the probability that one of these events occurs.

Dynamic Bayesian networks are used [46] to represent a system. The resilience of a system to a disruption is expressed as the joint probability of the occurrence of the disruption and of the three resilient capacities: the probability to absorb, adapt to, and recover from the disruption. The authors described a nuclear plant, Fukushima Daiichi, as a set of eleven components such as Process Control System, Cooling System, Sea Wall, etc. These components contribute to at least one of the three resilience capacities, and the contribution of a component to one capacity is represented by a failure probability. Thus, 1–3 failure probabilities can be associated to each component. Nevertheless, as components can be involved in more than one resilient capacity, the three resilient capacities are not independent and Bayesian Networks are used to model these dependencies. The result of the application of this model is the time-dependent probability function of the resilience of a system to a determined disruption.

4.3. Fuzzy models

Fuzzy sets are a generalization of conventional set theory that were introduced by Zadeh [47] as a mathematical as well as natural way to deal with problems in which the source of imprecision is the absence of sharply defined criteria. They play an important role in human thinking such as determining if someone is tall or if something belongs to the class of animals. For example, while dogs are clearly classified as animals, it is more ambiguous concerning bacteria, plankton, etc. The articles given in this section use fuzzy sets and membership functions to build metrics for resilience.

According to Francis and Bekera [15], resilience is a designed and engineered property of a system. Moreover, Muller [48] proposed to separately evaluate system architectures through attributes such as redundancy, adaptivity, robustness, etc, for which numerous metrics already exist. To accommodate differences amongst metrics, system architectures are thus represented with fuzzy membership functions associated with evaluated resilience attributes. Using these membership functions, resilience attributes are combined using fuzzy rules to obtain a measure of resilience from a resilience membership function. An example of fuzzy rule is:

IF *adaptability* is *moderate* AND *robustness* is *high* THEN *resilience* is *high*

To evaluate organizational resilience, Aleksic *et al.* [49] proposed to consider a system as a network of processes. Processes have many resilience potentials, divided into three categories: (1) internal factors such as quality, human factors, or planning strategies; (2) external factors that are external capacities and capabilities; and (3)

enabling resilience factors such as detection and emergency response. These potentials are represented by fuzzy attributes and are given a value defined within [0, 1]. Uncertainties' attributes, such as the relative importance of resilience potentials for a specific process, are also considered and are given a similar value. Then, values assigned to all these fuzzy attributes, resilience potentials, and uncertainties are combined using membership functions to produce an estimation of the system resilience .

Azadeh *et al.*[50] used nine resilient factors/potentials contributing to a complex system resilience. While six of them were described[18] and used by Shirali *et al.*[43] in a semi-quantitative metric, the authors added three factors: teamwork, redundancy, and fault-tolerance. Because these nine factors depend on each other, fuzzy cognitive maps are used to represent their interconnections and evaluate their contribution to system resilience. Following Aleksic *et al.*[49], membership functions are associated with each factor in order to evaluate the system resilience.

Clédel *et al.*[51] provided a framework to compare the resilience potential of different systems or configurations of the same system. The described model and metric cannot be used to determine if a system is resilient to a specific threat but it is used to determine if a system has more resilience potential than another one. A system is represented as a network of components. Components are service users of their previous components in the network and service providers of their next components. Services are represented through a partially ordered set of attributes, called data dimensions. Components inputs are fuzzy values associated with some dimensions. A value assigned to a dimension corresponds to the likelihood of this dimension to be externally consistent[52,53]. The article shows how these fuzzy values can be aggregated and manipulated so that components output fuzzy values associated with a set of data dimensions. Resilience is evaluated as follows: some nodes are the system client and their input values are fuzzy values for some expected dimensions. These expected dimensions correspond to services expected to be provided by the system, and their corresponding values are the likelihood for these services to be provided.

4.4. Frameworks

Some articles do not provide metrics or methods to evaluate the current resilience of a system. In place, they propose methodologies, guidelines, and good practices that are to be followed to design, maintain, and enhance the resilience of a system.

A framework for resilience, based on PAR risk assessment model[54] was proposed by Arghandeh *et al.*[25]. They claimed that, contrary to a risk assessment framework, the temporal dimension of disturbances and response time of remedies are to be considered in a resilience framework. Moreover, probabilities of occurrence of disturbance are not crucial except if the system has not yet recovered from a previous disturbance. A resilient system life cycle consists in three steps: (1) system identification, which is the establishment of network topology, physical characteristics, system behaviors, etc. (2) vulnerability analysis, which is basically an ongoing risk analysis taking into consideration the temporal aspect of the disruptions; and (3) resilience operations, which define new settings to improve recovery and absorbing potentials of the system. Once these changes have been made, a new identification phase begins.

Linkov *et al.*[55,56] provided a 4×4 matrix of resilience metrics. Each cell of the matrix corresponds to one of the four stages of event management cycle and one of the four system domains. Domains are different system layers: physical, information, cognitive, and social, and the stages correspond to one pre-event phase (Prepare) and three event handling phases (Absorb, Recover, and Adapt). Instead of providing a metric for resilience, the authors proposed to use cells of the matrix as guidelines to build metrics that, once combined, allow measuring the overall system resilience.

Table 2. Table of resilience evaluations.

Reference	Metrics					Frameworks
	Event specific	Quantitative probabilistic	Quantitative deterministic	Fuzzy	Adversary	
Abimbola and Khan [46]	✓	✓				
Thompson *et al.* [45]	✓	✓			✓	
Babiceanu and Seker [41]	✓	✓	✓			
Francis and Bekera [15]	✓	✓	✓			
Ayyub [27]	✓		✓			
Cai *et al.* [38]	✓		✓			
Gholami *et al.* [40]	✓		✓			
Rieger [39]	✓		✓			
Vugrin *et al.* [26]	✓		✓			
Wei and Ji [34]	✓		✓			
Clark and Sonouz [24]	✓		✓		✓	
Sterbenz *et al.* [42]	✓		✓		✓	✓
Holling [11]		✓				
Shirali *et al.* [43]			✓			
Azadeh *et al.* [50]				✓		
Aleksic *et al.* [49]				✓	✓	
Clédel *et al.* [51]				✓	✓	
Muller [48]				✓	✓	
Linkov *et al.* [55,56]						✓
Sterbenz *et al.* [21]					✓	✓
Mauthe *et al.* [2]					✓	
Van Mieghem *et al.* [64]						✓

The *ResiliNets* strategy [21] is an architectural framework intended to enhance resilience of networks. This framework is based on four axioms: (1) faults are inevitable; (2) normal operation has to be understood; (3) adverse events have to be expected and prepared for; and (4) responses to adverse events are required. According to these axioms, the *ResiliNets* strategy consists in two active phases. The first phase is composed of four steps that are defending, detecting, remediating, and recovering from challenges and attacks, while the second phase enables long-term evolution of the system through diagnostic of the root cause of the fault/attack and refinement of the system behavior to improve the first phase mechanisms and thus to increase the system resilience.

4.5. Adversarial events

Most contemporary control systems have been designed according to conventional model paradigms that are system safety and risk assessment. Originally, these approaches only consider unexpected but accidental events such as human errors or natural disasters. However, the emergence of cyber-physical systems and the accessibility from the Internet of legacy equipment, reliable but not secured, imply that faults resulting from the cyber-environment must be considered. However, only a few approaches presented in this article are able to take these threats into consideration. Indeed, adversarial impacts are explicitly represented in the linear time-invariant model that corresponds to a system [24]. According to Thompson *et al.* [45], resilience only concerns the handling of security breaches. As a consequence, this concept of resilience implies the management of adversarial events. Other approaches (see, e.g., [42,48,49,51]) do not represent events that could impact a system but focus on system's capacities and potentials that are available to handle events. This way, the specific case of adversarial events can be considered without having to explicitly represent them. The counterpart is the inefficiency of such approaches to assess the resilience of a system for a given perturbation. A classification of resilience evaluations is provided in Table 2.

5. RESILIENCE COMPARED WITH OTHER NOTIONS

The term "resilience" is frequently used as a synonym of fault-tolerance [57], adaptive systems [58,59], self-healing [60,61], *etc.* However, resilience is a design paradigm for large scale and complex systems that encompass cybersecurity, physical security, economic efficiency, and dynamic stability [39]. Wei and Ji [34] con-

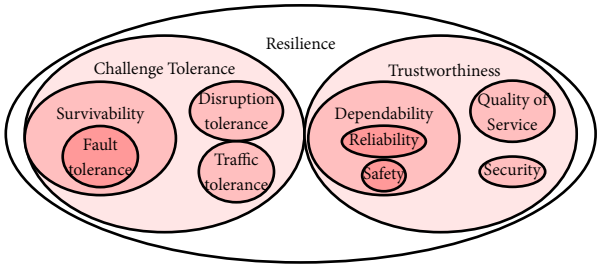

Figure 3. Disciplines of resilience from [21].

sidered resilience as a super-set of numerous properties such as robustness, adaptiveness, survivability, and fault-tolerance. Numerous disciplines contribute to the resilience of a system, but they have been developed independently in different engineering domains [21]. Interconnections between these disciplines are shown in Figure 3 and the Table 2.

5.1. Risk assessment

McDonald [17] described resilience as a capacity to anticipate and manage risk efficiently. However, resilience is clearly distinguished from risk assessment [15,18]. While risk assessment determines potential undesired events, their causal factors and negative consequences, and how to mitigate the exposure of the system to those events, resilience focuses on the system abilities to face undesired events and does not put the emphasis on the events themselves. In the domain of engineered system, safety and resilience are distinct but linked. According to Francis and Bekera [15], resilience aims to compensate poor system design in the case of unanticipated events. As a consequence, resilience can be seen as an addition to safety since it brings the "ability to anticipate, circumvent and recover rapidly from events that threaten safety". Comforting this distinction, the risk assessment goal is situation awareness and diagnostics while "resilience is about the mitigation of unexpected rare extreme failures" [25] that can necessitate extreme remedial actions such as partial or temporary outages in order to ensure the availability of critical services. Resilience is "essential when risk is incomputable" and is characterized "by surprise, complexity, urgency and the necessity of adaptation" [55]. Moreover, historic data of such rare events are out-of-date, uncertain, and biased, and it is not always pertinent to compare them with more recent events [18]. Thus, resilience approaches are complementary to, but distinct from risk analysis approaches, or from risk-aware approaches [62].

On top of that, faults resulting from the cyber-environment and intelligent adversary are generally not considered while critical infrastructure are increasingly connected and cyber-physical systems become the norm [39].

5.2. Robustness

Robustness, as described by Sterbenz *et al.* [21], is a system property that corresponds to the behavior of a system in face of challenges. It bridges the gap between the trustworthiness of a system, which consists in its dependability, security, and quality of service, and the challenge tolerance of the system, which corresponds to the system tolerance to faults, disruptions, intrusion, etc. While resilience and robustness are similar according to Sterbenz *et al.*, other authors make a clear distinction between these two notions.

According to Arghandeh *et al.* [25], "robustness is the ability of a system to cope with a given set of disturbances and maintain its functionality". Thus, robustness is centralized on stability and the handling specific threats, whereas resilience is concerned with flexibility and unbounded perturbations. In other words, resilience tolerates a degradation of performance as it is the ability to recover an original level of performance after a disruption, but, by definition, robustness does not tolerate degradation of performance [56]. The authors of [34,63] compared robustness and resilience: the former is related to consequences and uncertainties given a fixed harmful event while the latter is related to consequences and associated uncertainties but without con-

sidering a specific threat or considering all possible threats. In other words, uncertainties and amplitudes of events are quantified and bounded in robustness discipline and a robust solution can be found according to these quantities. On the other hand, resilience discipline cannot consider these quantities—uncertainties and amplitudes—as harmful events are unknown.

Another definition of robustness is used for networks. The network robustness is defined[64] as: "A measure of the network's response to perturbations or challenges (such as failures or external attacks) imposed on the network". Van Mieghem *et al.* introduced a mathematical value in the interval [0,1], called the R-Value, which is proposed to give a computation of the robustness value of a network.

5.3. Control theory

Several mathematical models, such as differential equations or state-space representation, can be used to model cyber-physical systems[65]. It is well known that, from a differential equation, which models the relation between the inputs and the outputs of a system, we can obtain a state–space representation:

$$x(t+1) = Ax(t) + Bu(t) \tag{7}$$

$$y(t) = Cx(t) + Du(t) \tag{8}$$

In Equation (7), x is a state vector. u and y are, respectively, the input and output vectors. A, B, C, and D are four matrices, respectively, named: state, input, output, and feedthrough matrices. In Equation (8), the output vector y contains the measurements of several sensors. By incorporating and diversifying the sensors to a system, we have more observability. This observability is very useful, especially for the attack detection.

Another important notion is the controllability, which can be defined as follows: our ability to bring a system into a desired state. In fact, incorporating a controller into a cyber-physical system is a way to improve the controllability. The controller uses the outputs of the system to generate the input signal(s). A CPS is a plant which communicates with the physical and the virtual world[66]. To be protected, the design of a CPS aims at controllability and observability. Designing CPS by incorporating physical elements which give controllability and observability can be considered as a way to improve the resilience.

5.4. Other notions

Wei and Ji compared resilience and adaptivity[34]. However, they considered adaptivity limited, as it only concerns mitigation mechanisms that control algorithm parameters, while resilience is open to a larger range of mechanisms. Particularly, adaptivity, as well as fault-tolerance and robustness, does not address the restorability of a system.

Fault-tolerance is the ability of a system to tolerate faults in order to avoid service failures. Sterbenz *et al.*[21] claimed that fault-tolerance is a subset of survivability which considers multiple correlated failures while fault-tolerance does not. It relies on redundancy and is one of the oldest resilience discipline. Moreover, fault-tolerance does not address intelligent adversaries and thus is not sufficient to provide resilience[34].

Morel *et al.*[8] claimed that there is a link between safety and performance levels: any increase in safety is to the detriment of performance. However, resilience lies in this link, and, by tolerating a variation across time of the expected performance level, it is possible to increase the safety level when needed. Resilience is depicted as the gain of safety when performance level is opened to variation.

De Florio[67] considered resilience as "a system's ability to retain certain characteristics of interest", in order to maintain the system identity. This article also introduces elasticity, a complementary notion to resilience, which

considers the system's abilities to change "with respect to its surroundings". Thus, by taking into account these two notions, a new notion, called anti-fragility, can be developed. Anti-fragility encompasses both resilience and elasticity.

6. CONCLUSION

6.1. Gaps and limitations

Most definitions and metrics described in this paper have one thing in common: they derive from risk analysis. According to risk analysis, possible threats can be identified, evaluated, and, even if they are uncertain, their probabilities of occurrence can be estimated. Thereby, resilience is calculated from the results of this risk analysis. Nonetheless, if one tries to assess the resilience of critical infrastructures nowadays, cyber-physical systems and their specific vulnerabilities must be considered. Adversary models must be studied as threats are not only accidental but also come from cyber-criminals, disgruntled employees, and terrorism[68]. These threats from malicious origin are difficult to evaluate. Their probabilities of occurrence are unknown because of the varied nature of the attackers and because of a lack of historical data. Besides, their consequences on the targeted system are hardly predictable.

In addition, several definitions and metrics delegate the evaluation of resilience to an evaluation of service delivery or to an evaluation of system performance. Some articles describe resilience in domain specific terms and provide accurate metrics that match the chosen definition. For example, network resilience is not only concerned with network connectivity[59,69] but also focuses on latency and route stability[58]. However, more generic approaches do not always clearly describe what are system services and system performance. Only a few models (see, e.g.,[51]) provide a framework that makes the description of system services possible.

Another noteworthy remark is the usefulness of the binary assessment of the resilience of a system. It is still critical to predict the behavior of a system when it is challenged by a determined event. This assessment makes it possible to determine if the system is resilient to this event. However, this kind of approach could be less pertinent if the threat is not well defined: its probability of occurrence is vague, its detection is uncertain, and its dynamic behavior, as well as the system response to this threat, are unclear. The authors of[48–51] suggested that assessing the resilience potential of a system could be more relevant than determining whether a system is resilient. Fuzzy logic is used by all four groups to describe this potential for resilience, but other approaches may be considered to assess resilience in a non-binary way.

6.2. Concluding remarks

Many definitions and metrics of resilience are addressed in this paper, from the original definition given by Holling about the resilience in ecological system to more recent and less domain specific ones. Definitions are classified according to their focus: Is resilience defined as the expected behavior when facing attacks and failures or as the combination of systems capacities that allow the mitigation of unexpected events? In addition to the intrinsic system characteristics, is resilience also specific to a determined perturbation? Some of these questions can be used again to classify metrics for resilience. Some metrics are event specific, which implies that resilience of a system must be evaluated separately for every threat or that resilience of a system is the sum of its resilience values for determined threats. Others do not consider possible events and evaluate resilience only from internal characteristics and properties of a system. While the results produced by some metrics determine a timely dependent likelihood of a system to be resilient, others give a resilient score or provide guidelines that ensure the maintenance and the enhancement of system resilience.

To conclude, resilience is compared to some other concepts or paradigms, such as robustness and risk assessment. While it is agreed that resilience is distinct from risk assessment and can be implemented and studied as a complement for traditional design and management approaches, the distinction with other notions is

Table 3. Glossary : Resilience definitions

Notion	Ref.	Title
Origins	[13]	The children of Kauai A longitudinal study from the prenatal period to age ten
	[11]	Resilience and Stability of Ecological Systems
	[14]	Resilience and Vulnerability Adaptation in the Context of Childhood Adversities
	[12]	Resilience: The emergence of a perspective for social-ecological systems analyses
A system property	[11]	Resilience and Stability of Ecological Systems
	[19]	Designing resilient engineered systems
	[16]	Resilient control systems: Next generation design research
	[15]	A metric and frameworks for resilience analysis of engineered and infrastructure systems
	[20]	Resilient control for critical infrastructures and systems
	[17]	Organisational resilience and industrial risk
	[18]	Properties of resilient organizations: an initial view
Service delivery	[23]	Basic concepts and taxonomy of dependable and secure computing
	[22]	From dependability to resilience
	[21]	Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines
	[25]	On the definition of cyber-physical resilience in power systems
	[24]	Cyber-Physical Resilience: Definition and Assessment Metric
Events handling	[28]	On the Definition of Resilience in Systems
	[26]	A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane
	[29]	Resilience engineering of industrial processes: Principles and contributing factors
	[27]	Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making
	[2]	Disaster-Resilient Communication Networks: Principles and Best Practices
Other definitions	[33]	A proposed resilience framework

Table 4. Glossary : Resilience properties

Notion	Ref.	Title
Absorbability	[36]	Resilience for the Scalability of Dependability
	[22]	From dependability to resilience
	[26]	A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane
	[29]	Resilience engineering of industrial processes: Principles and contributing factors
	[20]	Resilient control for critical infrastructures and systems
	[25]	On the definition of cyber-physical resilience in power systems
	[35]	Essential characteristics of resilience
Adaptability	[36]	Resilience for the Scalability of Dependability
	[37]	Validation of innovative state estimation and control techniques
	[22]	From dependability to resilience
	[26]	A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane
	[20]	Resilient control for critical infrastructures and systems
	[30]	Defining resilience
	[35]	Essential characteristics of resilience
Recoverability	[26]	A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane
Other capacities, descriptions	[36]	Resilience for the Scalability of Dependability
	[22]	From dependability to resilience
	[34]	Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights
	[21]	Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines
	[29]	Resilience engineering of industrial processes: Principles and contributing factors
	[33]	A proposed resilience framework

not always trivial. For example, even if some authors do not differentiate robustness and resilience in theory, the fact that these notions had originally been developed in independent scientific domains and in different communities produces a difference of usage in practice.

Table 5. Glossary : Metrics for resilience

Notion	Ref.	Title
Quantitative deter.	[11]	Resilience and Stability of Ecological Systems
	[4]	Micro incident analysis framework to assess safety and resilience in the operation of safe critical systems: A case study in a nuclear power plant
	[34]	Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights
	[26]	A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane
	[42]	Modelling and analysis of network resilience
	[15]	A metric and frameworks for resilience analysis of engineered and infrastructure systems
	[39]	Resilient control systems Practical metrics basis for defining mission impact
	[27]	Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making
	[38]	Availability-based engineering resilience metric and its corresponding evaluation methodology
	[40]	Toward a Consensus on the Definition and Taxonomy of Power System Resilience
	[24]	Cyber-Physical Resilience: Definition and Assessment Metric
	[41]	Cyber resilience protection for industrial internet of things: A software-defined networking approach
Semi-quantitative		A new method for quantitative assessment of resilience engineering by PCA and NT approach:
	[43]	A case study in a process industry
	[18]	Properties of resilient organizations: an initial view
Quantative prob.	[11]	Resilience and Stability of Ecological Systems
Event specific	[44]	On the Complex Definition of Risk: A Systems-Based Approach
	[28]	On the Definition of Resilience in Systems
	[34]	Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights
	[42]	Modelling and Analysis of Network Resilience
	[15]	A metric and frameworks for resilience analysis of engineered and infrastructure systems
	[33]	A proposed resilience framework
	[45]	A New Resilience Taxonomy
	[41]	Cyber resilience protection for industrial internet of things: A software-defined networking approach
	[46]	Resilience modeling of engineering systems using dynamic objectoriented Bayesian network approach
Fuzzy models	[47]	Fuzzy sets
	[52]	A Comparison of Commercial and Military Computer Security Policies
	[53]	Automated support for external consistency
	[48]	Fuzzy Architecture Assessment for Critical Infrastructure Resilience
	[49]	An assessment of organizational resilience potential in SMEs of the process industry, a fuzzy approach
		A new method for quantitative assessment of resilience engineering by PCA and NT approach
	[43]	A case study in a process industry
	[15]	A metric and frameworks for resilience analysis of engineered and infrastructure systems
		Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps
	[50]	A petrochemical plant
	[18]	Properties of resilient organizations: an initial view
	[51]	Towards the Evaluation of End-to-End Resilience Through External Consistency
Frameworks	[54]	At Risk: Natural Hazards, People's Vulnerability and Disasters
		Resilience and survivability in communication networks:
	[21]	Strategies, principles, and survey of disciplines
	[64]	A Framework for Computing Topological Network Robustness
	[42]	Modelling and Analysis of Network Resilience
	[55]	Measurable Resilience for Actionable Policy
	[56]	Resilience metrics for cyber systems
	[25]	On the definition of cyber-physical resilience in power systems
	[2]	Disaster-Resilient Communication Networks: Principles and Best Practices
Adversarial events		Resilience and survivability in communication networks:
	[21]	Strategies, principles, and survey of disciplines
	[42]	Modelling and analysis of network resilience
	[48]	Fuzzy Architecture Assessment for Critical Infrastructure Resilience
	[49]	An assessment of organizational resilience potential in SMEs of the process industry, a fuzzy approach
	[45]	A New Resilience Taxonomy
	[2]	Disaster-Resilient Communication Networks: Principles and Best Practices
	[51]	Towards the Evaluation of End-to-End Resilience Through External Consistency
	[24]	Cyber-Physical Resilience: Definition and Assessment Metric

Designing resilient systems is a challenge, especially in the case of CPS used in critical infrastructures. As described in Section 5, intrinsic properties of a CPS can be used to include, for example, physical components, making the system resilient by design. These components can be considered as protective layers for the CPS. One of the actual challenges consists in improving a CPS resilience by diversifying its incorporated hardware, or software components.

To provide an overall view of the main notions included in this paper, we refer the reader to the three glossaries, respectively, related to: resilience definitions [Table 3], resilience properties [Table 4], and resilience metrics [Table 5]. Based on the observations made, and on the classifications of the existing definitions, properties, and metrics, there are several topics that can be addressed in future works.

DECLARATIONS

Authors' contributions

Wrote and review the article: Clédel T, Cuppens N, Cuppens F,Dagnas R.
Each author contributed equally to the paper.

Availability of data and materials

Not applicable.

Financial support and sponsorship

This work was supported by the Cyber CNI Chair of Institute Mines-Télécom which is held by IMT Atlantique and supported by Airbus Defence and Space, Amossys, BNP Parisbas, EDF, Nokia and the Regional Council of Brittany; it has been acknowledged by the French Centre of Excellence in Cybersecurity.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

REFERENCES

1. Peng Y, Lu T, Liu J, Gao Y, Guo X, Xie F. Cyber-physical System Risk Assessment, 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013,Oct. 16-18, Beijing, China. IEEE, 2013. pp. 442-7.
2. Mauthe A, Hutchison D, Çetinkaya EK, et al. Disaster-resilient communication networks: Principles and best practices, 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), 2013 Oct. 16-18, Halmstad, Sweden. IEEE, 2016. pp. 1-10.
3. Hollnagel E. Resilience: The challenge of the unstable. In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 9-17.
4. Carvalho P V R, dos Santos I L, Gomes J O, Borges M R S. Micro incident analysis framework to assess safety and resilience in the operation of safe critical systems: A case study in a nuclear power plant. *J Loss Prevent Proc* 2008;21:277–86.
5. Saurin T A, Carim Júnior G C. Evaluation and improvement of a method for assessing HSMS from the resilience engineering perspective: A case study of an electricity distributor. *Saf Sci* 2011;49:355–68.
6. Azadeh A, Salehi V, Ashjari B, Saberi M. Performance evaluation of integrated resilience engineering factors by data envelopment analysis: The case of a petrochemical plant. *Proc Saf Environ Protec* 2014;92:231–41.
7. Shirali G H A, Motamedzade M, Mohammadfam I, Ebrahimipour V, Moghimbeigi A. Challenges in building resilience engineering (RE) and adaptive capacity: A field study in a chemical plant. *Process Saf Environ* 2012;90:83–90.
8. Morel G, Amalberti R, Chauvin C. How good micro/macro ergonomics may improve resilience, but not necessarily safety. *Saf Sci* 2009;47:285–94.
9. Abech M P, Berg G A, Delis M G, Guimaraes L B M, Woods D D, editors. Analyzing Resilience of an Oil Distribution Plant. Proceedings of the 2006 IEEE Systems and Information Engineering Design Symposium; 2006 April 28-28; Charlottesville, VA, USA. IEEE; 2007.
10. Hale A, Heijer T. Is resilience really necessary? The case of railways. In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 125-48
11. Holling C S. Resilience and Stability of Ecological Systems. *Annu Rev Ecol Syst* 1973;4:1–23.

12. Folke C. Resilience: The emergence of a perspective for social–ecological systems analyses. *Glob Environ Change* 2006;16:253–67.
13. Werner E E, Bierman J M, French F E. The children of Kauai: A longitudinal study from the prenatal period to age ten. Honolulu: University of Hawaii Press; 1971.
14. Luthar S S, editor. Resilience and Vulnerability: Adaptation in the Context of Childhood Adversities. Cambridge: Cambridge University Press; 2003. [DOI: 10.1017/CBO9780511615788]
15. Francis R, Bekera B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab Eng Syst Safe* 2014;121:90–103.
16. Rieger C G, Gertman D I, McQueen M A, editors. Resilient control systems: Next generation design research. Proceedings of the 2009 2nd Conference on Human System Interactions; 2009 May 21-23; Catania, Italy. IEEE; 2009.
17. McDonald N. Organisational resilience and industrial risk. In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 155–80.
18. Wreathall J. Properties of resilient organizations: an initial view. In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 275–85.
19. Mitchell S M, Mannan M S, O'Connor M K. Designing resilient engineered systems. *Chem Eng Prog* 2006;102:39–15.
20. Yang Y, Syndor R. Resilient control for critical infrastructures and systems. NRC 2014. Available from: https://www.researchgate.net/profile/Yaguang_Yang/publication/283091635_Resilient_control_for_critical_infrastructures_and_systems/links/562a9ec108ae518e347f74e1/Resilient-control-for-critical-infrastructures-and-systems. [Last accessed on 04-10-2020]
21. Sterbenz J P G, Hutchison D, Çetinkaya E K, et al. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Com Net* 2010;54:1245–65.
22. Laprie J C. From dependability to resilience. Available from: https://www.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_laprie.pdf.. [Last accessed on 04-10-2020]
23. Avizienis A, Laprie J C, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE T Depend Secure* 2004;1:11-33.
24. Clark A, Zonouz S. Cyber-Physical Resilience: Definition and Assessment Metric. *IEEE T Smart Grid* 2019;10:1671-84.
25. Arghandeh R, von Meier A, Mehrmanesh L, Mili L. On the definition of cyber-physical resilience in power systems. *Renew Sust Energ Rev* 2016;58:1060–9.
26. Vugrin E D, Warren D E, Ehlen M A. A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Proc Safety Prog* 2011;30:280-90.
27. Ayyub B M. Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making. *Risk Anal* 2014;34:340-55.
28. Haimes Y Y. On the Definition of Resilience in Systems. *Risk Anal* 2009;29:498-501.
29. Dinh L T, Pasman H, Gao X, Mannan M S. Resilience engineering of industrial processes: Principles and contributing factors. *J Loss Prevent Proce Indus* 2012;25:233-41.
30. Hale A, Heijer T. Defining resilience. In: Hollnagel E,Woods D, LevesonN, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 35–40.
31. Leveson N, Dulac N, Zipkin D, Cutcher-Gershenfeld J, Carroll J, Barrett B. Engineering resilience into safety-critical systems. In: Hollnagel E,Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 95–123.
32. Sundström G, Hollnagel E. Learning how to create resilience in business systems. In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 235–52.
33. Thompson M A, Ryan M J, McLucas A C, editors. A proposed resilience framework. Proceedings of the Systems Engineering and Test and Evaluation (SETE) Conference; 2014 April; Canberra, AS. 2002. Available from: https://www.researchgate.net/profile/Mike_Ryan7/publication/274660820_A_Proposed_Resilience_Framework/links/5524ff4c0cf22e181e73b971.pdf. [Last accessed on 04-10-2020]
34. Wei D, Ji K, editors. Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. Proceedings of the 2010 3rd International Symposium on Resilient Control Systems; 2010 Aug 10-12; Idaho Falls, ID, USA. IEEE; 2010.
35. Woods D D. Essential characteristics of resilience. In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: Concepts and precepts, 1st ed. Aldershot: Ashgate; 2006. pp. 21–34.
36. Laprie J-C, editor. Resilience for the Scalability of Dependability. Proceedings of the 4th IEEE International Symposium on Network Computing and Applications; 2005 July 27-29; Cambridge, MA, USA. IEEE; 2006.
37. de Lafontaine J, Côté J, Kron A, Vuilleumier P, Santandrea S, van den Braembussche P, editors. Validation of innovative state estimation and control techniques on PROBA-2. Proceedings of the 6th International ESA Conference on Guidance, Navigation and Control Systems. 2005 Oct 17-20; Loutraki, Greece. ESA SP-606; 2006. Available from: http://adsabs.harvard.edu/full/2006ESASP.606E..23D. [Last accessed on 04-10-2020]
38. Cai B, Xie M, Liu Y, Liu Y, Feng Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. *Reliability Engineering & System Safety* 2018;172:216-24.
39. Rieger C G, editor. Resilient control systems Practical metrics basis for defining mission impact. Proceedings of the 2014 7th International Symposium onResilient Control Systems (ISRCS); 2014Aug 19-21; Denver, CO, USA. IEEE; 2014.
40. Gholami A, Shekari T, Amirioun MH, Aminifar F, Amini MH, Sargolzaei A. Toward a Consensus on the Definition and Taxonomy of Power System Resilience. *IEEE Access* 2018;6:32035-53.
41. Babiceanu R F, Seker R. Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry* 2019;104:47-58.

42. Sterbenz J P G, Çetinkaya E K, Hameed M A, Jabbar A, Rohrer J P, editors. Modelling and analysis of network resilience. Proceedings of the 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011); 2011 Jan 4-8; Bangalore, India. IEEE; 2011.
43. Shirali G A, Mohammadfam I, Ebrahimipour V. A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. *Reliability Engineering & System Safety* 2013;119:88-94.
44. Haimes Y Y. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Anal* 2009;29:1647-54.
45. Thompson M A, Ryan M J, Slay J, McLucas A C. A New Resilience Taxonomy. *INCOSE International Symposium* 2016;26:1318-30.
46. Abimbola M, Khan F. Resilience modeling of engineering systems using dynamic object-oriented Bayesian network approach. *Computers & Industrial Engineering* 2019;130:108-18.
47. Zadeh L A. Fuzzy Sets. *Information and Control* 1965;8:338-53.
48. Muller G. Fuzzy Architecture Assessment for Critical Infrastructure Resilience. *Procedia Computer Science* 2012;12:367-72.
49. Aleksić Al, Stefanović M, Arsovski S, Tadić D. An assessment of organizational resilience potential in SMEs of the process industry, a fuzzy approach. *J Loss Prevent Proce Industr* 2013;26:1238-45.
50. Azadeh A, Salehi V, Arvan M, Dolatkhah M. Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. *Saf Sci* 2014;68:99-107.
51. Clédel T, Foley S N, Cuppens N, Cuppens F, Kermarrec Y, et al. Towards the Evaluation of End-to-End Resilience Through External Consistency. In: Castiglione A, Pop F, Ficco M, Palmieri F, editors. Proceedings of the 10th International Symposium on Cyberspace and Security (CSS); 2018 Oct 29-31; Amalfi, Italy. Springer; 2018. pp. 99-114.
52. Clark D D, Wilson D R. A Comparison of Commercial and Military Computer Security Policies. Proceedings of the 1987 IEEE Symposium on Security and Privacy; 1987 April 27-29; Oakland, CA, USA. IEEE; 2014.
53. Williams J G, Padula L J L. Automated support for external consistency. Proceedings of the [1993] Proceedings Computer Security Foundations Workshop VI; 1993 June 15-17; Franconia, NH, USA. IEEE; 2002.
54. Wisner B, Blaikie P M, Cannon T, Davis I. At Risk: Natural Hazards, People's Vulnerability and Disasters. 2nd ed. London: Routledge; 2004. Available from: https://books.google.fr/books?id=566bdm7T5VEC. [Last accessed on 04-10-2020]
55. Linkov I, Eisenberg DA, Bates ME, et al. Measurable Resilience for Actionable Policy. *Environ Sci Technol* 2013;47:10108-10110.
56. Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A. Resilience metrics for cyber systems. *Environ Syst Decis* 2013;33:471-6.
57. Stoller S D, Liu Y A. Algorithm Diversity for Resilient Systems. In: Foley SN, editor. Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy; 2019 Jul 15-17; Charleston, SC, USA. Springer; 2019. pp. 359-378.
58. Andersen D, Balakrishnan H, Kaashoek F, Morris R. Resilient Overlay Networks. *Sigcomm Comput Commun Rev* 2002;32:66-66.
59. Costa da Fontoura L. Reinforcing the resilience of complex networks. *Phys Rev E* 2004;69:066127.
60. Sousa P, Neves N F, Verissimo P, editors. How resilient are distributed f fault/intrusion-tolerant systems?. Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05); 2005 June 28 - Jul 1; Yokohama, Japan. IEEE; 2005.
61. Lucia W, Sinopoli B, Franze G, editors. A set-theoretic approach for secure and resilient control of Cyber-Physical Systems subject to false data injection attacks. Proceedings of the 2016 Science of Security for Cyber-Physical Systems Workshop (SOSCYPS); 2016 April 11-11; Vienna, Austria. IEEE; 2016.
62. Kanoun W, Cuppens-Boulahia N, Cuppens F, Dubus S, editors. Risk-aware Framework for Activating and Deactivating Policy-based Response Risk-aware framework for activating and deactivating policy-based response. Proceedings of the 2010 Fourth International Conference on Network and System Security; 2010 Sept 1-3; Melbourne, VIC, Australia. IEEE; 2010.
63. Aven T. On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Anal* 2011;31:515-522.
64. Van Mieghem P, Doerr C, Wang H, Hernandez J M, Hutchison D, et al. A framework for computing topological network robustness. Delft University of Technology, Report 20101218, 2010.
65. Baheti R, Gill H. Cyber-physical systems. *The Impact of Control Technology* 2011;12:161-166.
66. Lee E A, editor. Cyber-physical systems-are computing foundations adequate. Proceedings of the Position paper for NSF Workshop on Cyber-physical Systems: Research Motivation, Techniques and Roadmap; 2006 Oct 16-17; Austin, TX, USA.
67. De Florio V. Antifragility = Elasticity + Resilience + Machine Learning: Models and Algorithms for Open System Fidelity. *Procedia Comput Sci* 2014;32:834-41.
68. Cardenas AA, Amin S, Sinopoli B, et al. Challenges for Securing Cyber Physical Systems. 1st Workshop CyberPhys. *Syst Security* 2009;5:1.
69. Hayel Y, Quanyan Z, editors. Resilient and secure network design for cyber attack-induced cascading link failures in critical infrastructures. Proceedings of the 2015 49th Annual Conference on Information Sciences and Systems (CISS); 2015 Mar 18-20; Baltimore, MD, USA. IEEE; 2015.