Resilience assessment as a foundation for systems-of-systems safety evaluation: Application to an economic infrastructure

Aicha Koulou, Norelislam El Hami, Ilyas Ed-Daoui, Abdelkhalak El Hami, Mhamed Itmi, Nabil Hmina, Tomader Mazri

▶ To cite this version:

Aicha Koulou, Norelislam El Hami, Ilyas Ed-Daoui, Abdelkhalak El Hami, Mhamed Itmi, et al.. Resilience assessment as a foundation for systems-of-systems safety evaluation: Application to an economic infrastructure. Safety Science, 2019, 115, pp.446-456. 10.1016/j.ssci.2019.02.030 . hal-02117174

HAL Id: hal-02117174

https://normandie-univ.hal.science/hal-02117174

Submitted on 22 Oct 2021

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.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

Version of Record: https://www.sciencedirect.com/science/article/pii/S0925753518309159
Manuscript_436e91ee1c0956be3ea1dfd8e8515a31

Resilience assessment as a foundation for systems-of-systems safety evaluation: Application to an economic infrastructure

Ilyas Ed-daoui[a,c,*], Abdelkhalak El Hami[a], Mhamed Itmi[b], Nabil Hmina[c], Tomader Mazri[d]

[a]LMN Laboratory, INSA Rouen Normandy, University of Rouen Normandy, France

[b]LITIS Laboratory, INSA Rouen Normandy, University of Rouen Normandy, France

[c]LGS Laboratory, ENSA of Kenitra, Ibn Tofail University, Morocco

[d]ETSE Laboratory, ENSA of Kenitra, Ibn Tofail University, Morocco

*Corresponding author.
Email address: edd.ilyas@gmail.com (Ilyas Ed-daoui)

© 2019 published by Elsevier. This manuscript is made available under the CC BY NC user license
https://creativecommons.org/licenses/by-nc/4.0/

Resilience assessment as a foundation for systems-of-systems safety evaluation: Application to an economic infrastructure

Abstract

In this paper, the authors propose two complementary approaches in an attempt to contribute to systems-of-systems (SoS) safety evaluation through resilience assessment. The first approach is a risk monitoring design, it is conceived to monitor, evaluate and analyze risks that represent destabilizations' catalyzers. The second one is a structural analysis that begins with the estimation of criticality and frailty levels which leads to the calculation of failure impact and susceptibility measures of a component system on/to the SoS performance and process continuity. The combination of these approaches helps to assess SoS resilience through building a futurist, quantitative and anticipative perspective to evaluate the potential risks, their influences and impacts on SoS structure. Accordingly, this embraces a step towards safety forecast, evaluation and enhancement. A case study of a real-based economic infrastructure of a geographic area in France approached as a SoS model, is provided to experiment the proposition. The outcome of the presented approach's application shows that: (1) the use of the risk's monitoring dashboard helps to qualitatively illustrate risks striking the SoS or could possibly affect it in the future; (2) the structural analysis evaluates the impact of a component system's failure on the overall performance and efficiency of the SoS embracing it and vice versa; (3) the proposed approach could be used for anticipative and preventive reasons.

Keywords

Resilience; Risks assessment; Safety; Structural analysis; Systems-of-systems (SoS).

1. Introduction

Systems-of-systems (SoS) have received extensive attention from the scientific community in the past years and numerous definitions were proposed to sire this concept. Some of the potential definitions of SoS are enumerated:

- Jamshidi Mo: "*SoS are large-scale integrated systems which are heterogeneous and independently operable on their own, but are networked together for a common goal*" [7], [13].
- Maier Mark W.: "*SoS are a collection of systems that must have two features: its components must be able to operate independently by the whole system and they do operate independently, being managed at least in part for their own purpose*" [35].
- Department of Defense (USA): "*A SoS is a large-scale composite system, which can realize specific function*" [36].
- Xia Boyuan, Zhao Qingsong, Dou Yajie et al.: "*SoS are special systems, they are composed of systems which can run independently and have their own benefits and values. Once the*

element system is put into the SoS, its independence still exists and the interactions among the systems are frequent" [37].

- Kotov Vadim: "*SoS are large-scale concurrent and distributed systems that are comprised of complex systems*" [38].

They represent a synergy of task-oriented and dedicated systems that pool their resources and capabilities together to create a more complex system which offers more functionalities and performances than simply the sum of the constituent systems.

Correspondingly, SoS engineering is emerging as an attempt to address integrating complex metasystems. However, it is in the embryonic stages of development and lacks consistent focus. Terms such as interoperability, platform integration, systems architecture and information-intensive have emerged to capture the information dimension of this new class of complex systems [4], [11].

Resilience remains difficult to interpret, especially in SoS context, but it is generally defined as the capacity of a system to resist an unpredictable event or a risk and recover. It concerns consequences in case of a risk and inherent uncertainties. In some literature, resilience also represents an important concept to tackle SoS reliability and safety along with survivability and trustworthiness [3], [5], [7], [8], [9], [20], [24], [25], [27], [29], [30]. There is a common belief that safety and resilience concepts are strongly related. This study aims to emphasize the mutual correspondence between the two concepts.

In this work, the authors answer to the demand of safety evaluation through resilience assessment. A risks monitoring dashboard is proposed for risks characterization for monitoring, prevention and anticipation purposes. They understand that it is mandatory to identify, monitor, classify and evaluate risks for a better protection of the system.

A structural approach dedicated to the assessment of SoS architecture is coupled with that. It aims to evaluate component systems failure impact and susceptibility on/to SoS performance and process continuity and vice versa. It represents an extension of the approaches presented in [10].

An application of the theory is done on a real-based economic infrastructure of a geographical area in France approached as a SoS. The economic infrastructure represents the internal facilities of a country that eases business activity, such as communication, transportation, distribution networks and markets. Component systems symbolize enterprises and geographical locations are differentiated by colors to emphasize the regional competitiveness.

The remaining part of the paper is structured as follows:

- Section 2 introduces the related literature
- Section 3 outlines the contribution
- Section 4 and section 5 describe the proposed approaches for resilience assessment
- Section 6 explains the correlation between resilience and safety
- Section 7 presents the application results of the theory on a case study
- The last section summarizes the work and draws conclusions

2. Background

An interdisciplinary discussion has developed concerning how designers can incorporate resilience into the engineering of complex systems in general and especially in SoS.

As authors of [40] state, that there are multitudinous works and publications, from different domains, that attempt to lead the effort behind shedding more light on resilience: Ecological systems [41], Safety engineering [42], critical infrastructures [7], [10], [43], [44], communication networks [45], logistics and transportation networks [46], [47] and organizational resilience [48], [42].

This section gives a brief overview of prominent resilience definitions. Following this overview, relevant frameworks and metrics for assessing resilience are discussed to establish a foundation for the proposed work.

2.1. Resilience definitions

Much of the early work focusing on resilience has been about proposing definitions and common properties of resilient systems. They appear within various scientific fields and are often tailored to specific applications of interest [40].

Therefore, to get a holistic view of resilience, the authors will briefly review insights from various disciplines. Although it is not their intent to provide an in-depth review of such diverse literature, they will refer to some definitions in an attempt to identify those commonalities.

Resilience is defined as a system's ability to continue operations or recover a stable functional state after a major mishap or event and prevent or adapt to changing conditions in order to maintain a system property or properties [49]. However, this definition of resilience can hardly be distinguished from robustness which says that the system can maintain its function within a controlled tolerance under disturbances [50], [32].

Another definition of resilience has been proposed in [51], [52], it is seen as a system's property that can still function to the desired level when the system suffers from a partial damage. A more generalized definition has also been proposed in (Merriam-Webster Online Dictionary) [34]. It is defined as the ability to recover from or adjust easily to misfortune or change.

Even in psychology, a definition of resilience has been proposed. It has been characterized as the positive capacity of individuals to cope with stress and catastrophic events and their level of resistance to future negative events [34]. While in computer networks, resilience has been expressed as the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations [53].

Considering discussions of resilience from a variety of communities, the common aspect of all these definitions is that resilience is defined as a response to unexpected or unforeseen changes and disturbances and the ability to adapt and respond to such changes [7], [34].

2.2. Resilience engineering and assessment

Resilience Engineering is an emerging discipline [53] which aims to enhance an organization's ability to target safety investments proactively in the face of ongoing production and economic pressures [42]. Methods and metrics for quantitatively assessing resilience are also proposed to enable rigorous and traceable comparisons between potential system designs [54]. Several quantitative assessment methods have been proposed in the literature [40]. Authors propose discussions of resilience assessment from related literature.

In [21], a method to characterize the behavior of networked infrastructure for natural hazard events and improve infrastructures resilience is proposed. It includes resilience and interdependency measures. Authors focused their study on the contribution of power delivery systems to post-event infrastructure recovery. The model is a component of a scheme that develops design strategies in order to increase the resilience of infrastructures for extreme natural hazard scenarios.

The goal is to capture the recovery aspects to identify the trends in interconnections in order to assist others who are developing the intricate models and databases required for regional planning and evaluation.

A framework for resilience engineering is proposed in [18]. Authors define resilience from different perspectives and provide a conceptual framework dedicated to analyzing disruptions and present principles for the creation of resilient systems. It includes disruptions, system attributes, methods and metrics. The idea behind such classification is to allow systems engineers to focus on what are the impacted attributes whenever resilience is needed and what methods are appropriate to achieve resilience.

They began by emphasizing that there is a reflex of misattributing systems failure and mishaps occurrence to human error. They also proposed a clarification to the difference between safety, reliability, survivability and resilience. Accordingly, they have emphasized that resilience engineering does not see failure as a breakdown, but, it is viewed as an inability of the system to either absorb perturbations or adapt to changes in real-world conditions.

In [10], an infrastructure resilience-oriented modeling language (IRML) is proposed to facilitate the analysis of operational interdependencies of infrastructure's components, resilience, the ability to withstand risks and recover.

The IRML comes with a set of analysis tools and procedures that investigate structural properties and resilience. Its analysis leads to a screening of structural and dynamic properties that are related to the resilient behavior of a SoS, in order to provide additional insights about possible misbehaviors at a large-scale.

In [31], authors define some principles to enhance enterprise information systems' resilience. They propose an architecture of what they call "resilient enterprise information systems". It is elaborated on a particular identity of resilience which is related to human as it is implicated in its safety and health. Authors see that resilience has roots in biological and ecological systems which leads to derive the proposed five design principles for resilient systems. These design principles are well applicable to enterprise information systems in order to be resilient.

Table 1. Literature positioning towards different aspects siring the concept of resilience

	Risk analysis	Structural analysis	Monitoring	Resilience quantification and measurement	Safety	Reliability	Recovery
Reed et al. [21]		x		x			x
Filippini and Silva [10]		x					x
Zhang and Lin [31]			x			x	
Tran et al. [40]				x			x
Liu et al. [33]		x				x	
Wang et al. [32]				x			

Ed-daoui et al. [7]		**x**		**x**		**x**
This work	**x**	**x**	**x**	**x**	**x**	

Table 1 summarizes the contribution and situates this work with regards to the current literature. As illustrated there is a need for further development in some aspects such as risks management, structural analysis, monitoring, resilience quantification and their influence on SoS safety. The contribution is an answer to this demand.

3. Contribution outline

This section is introductive. Explanations and details regarding each approach are all presented further in the paper. However, the authors outline the essential features of the proposition in order to put the reader in the context.

This work aims to address the assessment of resilience in SoS through two complementary approaches: one dedicated to risks management and the other to structural analysis, as illustrated in Figure 1.

Risks management approach is based on two important steps:

- Risks classification
- Risks monitoring

As a result, the monitoring (aspect) is explicitly included in the risk analysis. While structural analysis approach is based on:

- Dependency network
- Criticality and frailty analysis
- Failure impact and susceptibility calculations

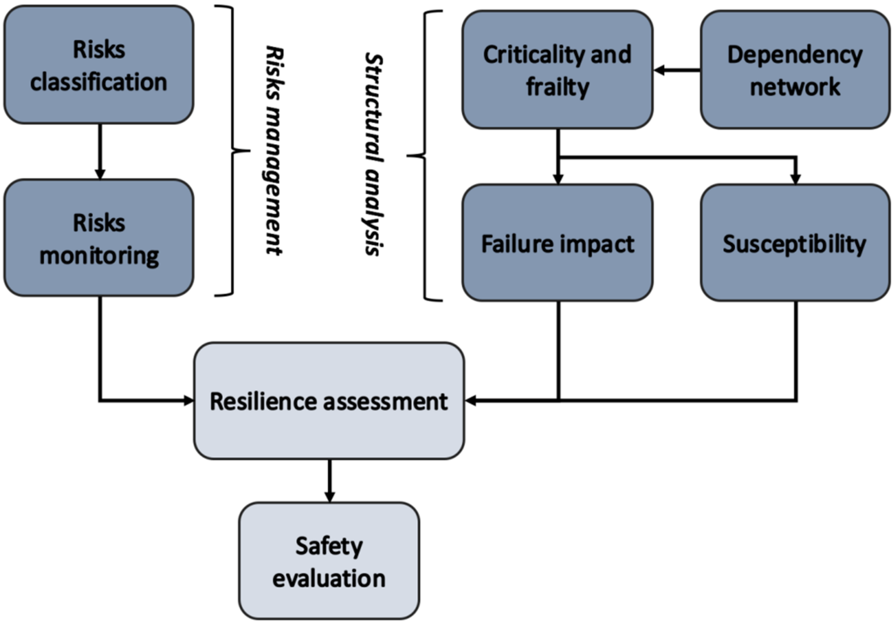


Figure 1. Overview of the contribution

In fact, failure impact and susceptibility metrics are both structural metrics dedicated to the evaluation of a SoS dependence on each one of its component systems and vice versa (in addition to the capability of the SoS to face disturbances). This implies the use of a structural analysis in order to assess and measure resilience.

This paper tackles safety in SoS through risk and resilience analysis with respect to structural models in addition to operational and functional processes amid the SoS. The combination of the approaches (forming the contribution) quantitatively anticipates SoS resilience measurements in the architecting phase. This implicitly embraces a step towards safety evaluation and enhancement as the more the SoS is resilient and capable of performing as expected without failing, the safer it is.

4. Risks management

4.1. Risk model

As SoS have a special architecture with special properties as distribution, heterogeneity, complexity, etc. it is crucial to inspect the potential sources of risks that could disturb the operational and functional return of SoS for resilience assessment purposes.

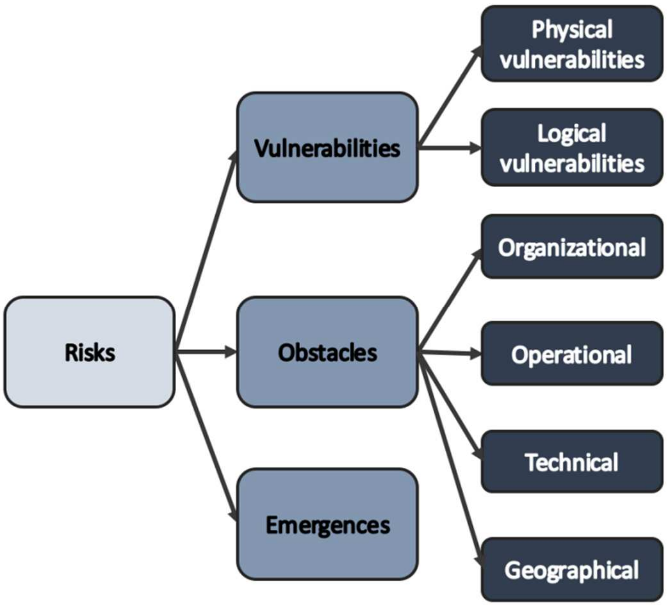


Figure 2. Risks' classification

In this work, the authors consider any barrier that could continuously or in an intermittent manner discommode, interrupt or put an end to an interaction between two (or more) enterprises as a risk. Enterprises are represented as component systems amid the SoS. In Figure 2, SoS risks are classified based on their natures and sources. Here are the main risks classes:

- Vulnerabilities
- Obstacles
- Emergences

Vulnerabilities represent the weaknesses of the system that can be the subject of possible exploitation and consequently put the system at risk. They also can be classified into two categories:

- *Physical vulnerabilities*: linked to the physical architecture of the system, i.e. the entities, the used links, machines and server rooms. An unauthorized access of a malicious person to the infrastructure may lead to titanic problems.
- *Logical vulnerabilities*: related to the software, applications, protocols or procedures that can be exploited by a malicious activity may put the SoS at huge risks.

While obstacles represent the barriers that could possibly disturb, interrupt or intercept the interdependency between interacting systems. A taxonomy of obstacles is proposed, it will be adopted in the proposed approach. Here are the four classes and their definitions:

- *Organizational obstacles*: they concern human, legislative, decisional, financial obstacles, commercial approaches and enterprises' cultures that can discommode the interactions between enterprises.
- *Functional obstacles*: they are related to the incompatibility of procedures, norms and standards to present and communicate information, as well as the methods of work and technical incompatibilities that may perturb the interactions between communicating enterprises.
- *Technical obstacles*: they are related to the technical support of interactions. The authors classify them into two levels: logical and physical. Logical is about the obstacles related to exploited software, programs, etc. and physical is related to the physical architecture supporting the logical solutions.
- *Geographical obstacles*: they represent anything that blocks the pathway between two systems, this can be any natural feature such as mountains or even natural disasters that prevent the interaction from being successful.

Finally, emergence represents a principle in classical systems theory that generally suggests that system properties (patterns, capabilities, structure and behaviors) may be developed from the interaction of system elements [12]. Emergences may represent prominent risks to the SoS if they affect its performance.

Other definitions are proposed to sire the concept of emergence. In [23], emergent behavior is defined as what cannot be expected through analysis. While in [16], emergent behaviors refer to the properties arising from cumulative interactions between systems inside the SoS.

In complex systems, this notion generally includes the following commonly held points [13]:

- Emergent properties exist only at the system level.
- Emergent properties are not held by any of the isolated elements.
- Emergent properties are irreducible. They simply cannot be understood, explained, or inferred from the structure or behavior of constituent elements or their local properties.
- Understanding cause-effect relationships can only be established through retrospective interpretation. This renders traditional reduction-based analytic techniques are incapable of useful predictions of emergent system-level behavior

Figure 2 summarizes the detailed classification of risks. To effectively deal with them, an appreciation of the philosophical, methodological and axiomatic underpinnings is required. The non-governance of the disorder at the very beginning can complicate the restoring of systems' performance after an incident.

4.2. Risks monitoring

The use of the dashboard is an attempt to illustrate, preferably in real-time, qualitative indicators related to risks that are striking the SoS at a given time and in a geographic location or could possibly affect it in the future. The dashboard could be used for both anticipative and preventive reasons. For an optimal exploitation of the dashboard and effective anticipation, it is more advisable to apply it, similarly, on every single dependency and try to anticipate as many scenarios as possible.

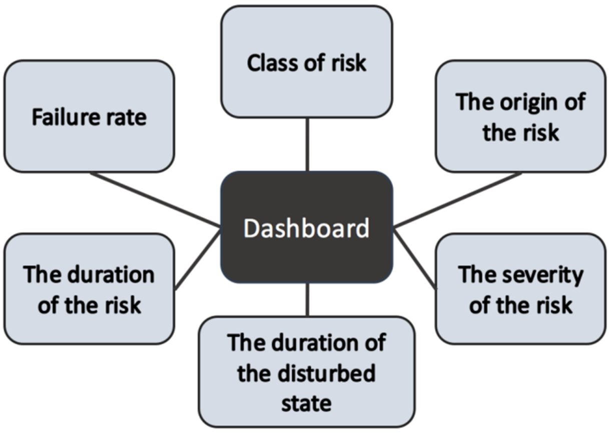
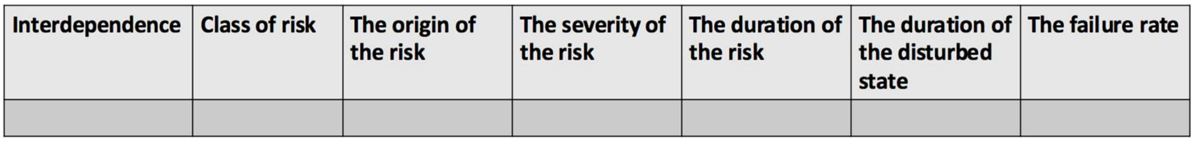


Figure 3. Dashboard for risks' supervision

It is worth noting that the elements included in the dashboard, shown in Figure 3, are not exhaustive. The authors prefer to call them control points, as they are used to determine different risk characteristics and implicitly the state of the SoS at a given time.



Interdependence	Class of risk	The origin of the risk	The severity of the risk	The duration of the risk	The duration of the disturbed state	The failure rate

Figure 4. Example of a dashboard for risks' monitoring

The examined control points may change according to the studied SoS. The idea behind the proposition of the dashboard is not to propose a standard for SoS monitoring but to emphasize the importance of monitoring in such context and suggest an outline of essential features.

Let us examine the key elements included in the dashboard in order to understand their use:

- *The origin of risk*: in order to correctly address a risk, it is crucial to know its origin which also reflects is nature. Besides, knowing where a risk came from helps to understand the risk and elaborate pertinent countermeasures. In fact, there are numerous sources of risks, it could be environmental, human, technical, etc. Accordingly, a risk may be intentional i.e. it could be organized, managed and targeting a vulnerability in the SoS, in this case, the origin may be internal (e.g. coming from component systems users) or external (e.g. as a consequence of an environmental disaster). Or it could be unintentional e.g. as in the case of an environmental risk or a human intervention that led accidentally to a problem.
- *The severity of the risk*: it is very important to know how much the SoS performance has degraded. For this reason, the authors propose a classification of degrees of nuisance according to the degree of the SoS disturbance:
  - It is called 1st degree if it is quick and does not disturb the performance of the SoS.
  - It is called 2nd degree if it remains weak but affects slightly the performance of the SoS for a short period of time before the system returns to its initial state.
  - It is called 3rd degree if it is able to significantly disrupt the performance of the SoS.
  - It is referred to as a 4th degree if it may provoke an interruption to the SoS performance and it becomes difficult for it to return to its initial state.

  - It is called 5th degree if it can cause a breakdown of the system which makes it impossible for him to regain its initial state
- *The duration of the risk*: represents the duration that took (or may take) a system to resist the risk. As the risk may be instant or slow, the resistance duration also changes according to the risks duration. Authors insist on the fact that this has no relation to the degree of severity of the risk.
- *The duration of the disturbed state*: represents the period where the system leaves its initial state (this depends on the degree of the risk and its duration). In some cases, it may be significantly greater than the duration of the risk, and this may be due to several factors including the degree of risk and the criticality of the systems amid the SoS undergoing this risk. The notion of criticality will be discussed further in this paper.
- *The failure rate:* represents the rate of component systems that failed to return to their initial states after the occurrence of the risk.

$$\text{FR (\%)} = \left(\frac{\text{Number of failed systems}}{\text{Number of component systems}}\right) \times 100 \qquad (1)$$

- *Risk's type*: refers to the class of the risk according to the risk model in the third section.

A major reason why risks may occur and may have predominant consequences is the existence of vulnerabilities. They have existed since the system was implemented. Some of them can be planned from the design stage to be corrected before the system is built, others can be unpredictable and become identifiable only after the SoS has been set up. This triggers the need for frequent maintenance of the system's infrastructure, entities, links, programs and software in order to fix them.

But, why do we need to monitor risks?

First, there are preventive reasons as it is important for engineers and management authorities to have an anticipative and futurist perspective to the SoS behavior, interdependencies' states and overall performance. This helps them to be prepared for eventual risks.

The second reason behind monitoring is a real-time supervision and protection of the SoS. The proposed approach helps to get the real-time state of the performance of the system. In case of a problem, the supervision authority is notified right away. Therefore, some countermeasures to be considered.

The general idea behind the use of a risks monitor is to reduce the response time of the SoS to face a risk as the more the problem is identified earlier the more it is handled efficiently and its consequences are limited.

5. Structural analysis

In this section, an approach based on structural analysis is presented. It aims to evaluate the impact of a component system's failure on overall performance and efficiency of the SoS embracing it and vice versa.

The structural analysis is based on the assessment of functional dependencies between systems. This leads to the evaluation of the criticality and frailty levels of each component system on/to the group it belongs to. Finally, the failure impact and susceptibility of a component system on/to the performance of the whole SoS are deducted.

This gives us an idea about the dependability of the global system on each component system. In addition, this process should be applied, similarly, on every single component system based on the SoS structural architecture in order to be able to locate impactful and frail component systems.

In this section, the structural analysis is detailed via four important steps:

- First is the dependency network elaboration
- Second is the frailty and criticality assessment
- Third one is the failure impact metric
- The last one is the susceptibility metric

5.1. Dependency network

The idea behind dependency analysis is to focus on workflow pathways and directions, as it is illustrated by black arrows in Figure 5. The analysis of dependencies' set emphasizes the functional dependencies relevance. In addition, it identifies clearly the process sequencing by representing functional services to be acquired by systems and dependencies between the systems or between the capabilities by links.

A SoS can be given a topology that accounts for the static representation of its components and the manner they interact and cooperate [7], [8], [9], [10]. The idea is to focus on the component's interface, where data, services and quantities are exchanged through functional relationships, i.e. functional dependencies.

It is important to evaluate the effect of topology and possible systems' performance degradation on the SoS as it helps us implicitly evaluate its resilience and capability to face partial failures and component systems' loss of operability.

5.2. Frailty and criticality analysis

In [7, 10], frailty (or vulnerability, as it is called in the cited reference. The word vulnerability is not used here as it is exploited to express a class of risks) and criticality sets are presented as structural properties that can be analyzed in the dependency network. A system is affected by the systems on which it depends on and it is critical to the systems depending on it. The dependency is related to the workflow pathway between component systems.

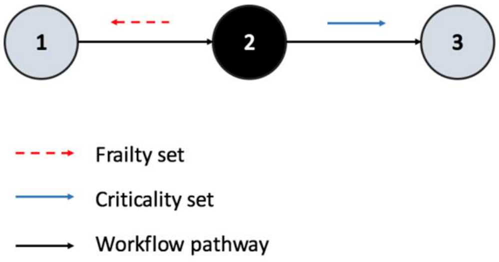


Figure 5. Frailty and criticality positions towards workflow pathway

Figure 5 represents a simple example illustrating three systems. The idea is to locate frailty and criticality sets for system '2' with regards to the workflow pathway. System '2' is critical to system '3' and frail to system '1' at the same time. This depicts the difference between frailty and criticality and their positions towards the SoS workflow pathway. The criticality represents how much the process continuity of the SoS relies on the systems and groups. Practically, it is calculated by using the formula (2).

$$(\forall\, n_i \in G): Criticality\ (n_i) = \frac{Card\big(C(n_i)\big)}{Card(G_j)} \qquad (2)$$

With:

$i \in \{1, 2, \ldots\}$ and $j \in \{1, 2, \ldots\}$

$Card\big(G_j\big)$: the number of component systems forming the group embracing the component system n_i.

$Card\big(C(n_i)\big)$: represents the number of component systems that are directly or indirectly affected by the failure of the system n_i. The component systems should be in the same group as the system n_i.

While the frailty, in SoS context and according to [10], represents how the component system relies on the process continuity. It is calculated by using the formula (3).

$$(\forall\, n_i \in G): Frailty\ (n_i) = \frac{Card\big(F(n_i)\big)}{Card(G_j)} \qquad (3)$$

With:

$i \in \{1, 2, \ldots\}$ and $j \in \{1, 2, \ldots\}$

$Card\big(G_j\big)$: the number of component systems forming the group embracing the component system n_i.

$Card\big(F(n_i)\big)$: represents the number of component systems that affect directly or indirectly the system n_i by their failures.

At this stage, the SoS' groups are supposed to be represented by the set $\{G_1, G_2, \ldots\}$. Moreover, frailty metric values range goes from 0 for not frail at all to 1 for extremely frail. The frailty value may be multiplied by 100 in order to get the criticality rate.

5.3. Failure impact calculation

Failure impact is a structural metric conceived to measure each system's failure impact on the rest of component systems and SoS viability with consideration to the repartition of the SoS into groups. The failure impact value of a system is obtained by multiplying its criticality value (with correspondence to its position towards the process inside the containing group) by the same group's criticality value (corresponding to the process inside the SoS). As it is shown in formula (4).

$$\forall\, \big(n_i, g_j\big) \in G \times F: FI\big(n_{ij}\big) = Criticality_{System}(n_i) \times Criticality_{Group}\big(g_j\big) \quad (4)$$

With:

$i \in 1, 2, \ldots, Card(G)$

$j \in 1, 2, \ldots, Card(F)$

n_i: represents a system inside the group g_j.

g_j: represents a group inside the SoS.

$Card(E_j)$: represents the total number of systems forming the group.

$Card(F)$: the total number of groups forming the SoS.

$Criticality_{System}$ values range goes from 0 for not critical at all to 1 for extremely critical. $Criticality_{Group}$ is equal to 1 in case there is no dependency between groups.

Furthermore, groups criticality values are calculated following the same tactic that has been adopted to calculate each component system's criticality on the rest of component systems within the same group, with consideration of itself. This means that in addition to the groups following the same workflow pathway, the group in question joins to the group's criticality set.

The failure impact metric takes into account all variables taking part of the system's forming. If a system has a high failure impact that means that an important part of the SoS could be affected in case of its deficiency. This means that the infrastructure is not resilient and robust enough to overcome its failure.

5.4. Susceptibility calculation

Contrarily to the failure impact metric, susceptibility is a metric that evaluates component systems fragility to the process continuity, with consideration to the repartition of the SoS in question into groups.

The susceptibility of a component system inside a SoS is obtained by the multiplication of its frailty (with correspondence to its position towards the process inside the containing group) by the frailty value of the same group (corresponding to the process inside the SoS). As it is shown in formula (5).

$$\forall\ (n_i, g_j) \in G\ \times\ F: S(n_{ij}) =\ Frailty_{System}(n_i)\ \times\ Frailty_{Group}(g_j) \quad (5)$$

With:

$i \in 1, 2, \dots, Card(G)$

$j \in 1, 2, \dots, Card(F)$

n_i: represents a system inside the group g_j.

g_j: represents a group inside the SoS.

$Card(E_j)$: represents the total number of systems forming the group.

$Card(F)$: the total number of groups forming the SoS.

$Frailty_{System}$ values range goes from 0 for not frail at all, which means that the component system is independent inside its group and does not receive any workflow from any component system, to 1 for extremely frail, which means that the component system receives flaw from all systems inside the same group. $Frailty_{Group}$ is equal to 1 in case there is no dependency between groups.

Correspondingly, the calculation of the frailty of each group on the rest of groups within the SoS is done following the same tactic that has been adopted to calculate the criticality of each group on the rest of groups within the same SoS, with consideration of itself. This means that in addition to the groups following the same workflow pathway, the group in question joins the group's frailty set.

Failure impact and susceptibility metrics are both structural metrics dedicated to the evaluation of a SoS dependence on each one of its component systems and vice versa. This implies the evaluation of SoS resilience and capability to overcome disturbances.

6. The correlation between resilience and safety

One the founding principles of safety science is the need to take a systems approach to understand how an organization or a composition of components succeeds and sometimes fails in managing increasingly complex systems in more highly pressured contexts [58]. A systems approach to safety in complex systems requires a shift in how to study, model and measure operational processes [42], [53], [59], [60], [61], [62], [63], [64], [65].

In safety science literature, resilience represents the ability of a system to "adjust its functioning prior to, during, or following changes and disturbances, so that it can continue to perform as required after a disruption or a major mishap, and in the presence of continuous stresses" [56], [57], [61], [62]. The introduction of the concept of resilience in safety science has contributed to shifting focus from including strength to tackle functional recovery and survivability [53], [57]. The same goes for the relationship between reliability and resilience, as one of the recent definitions of reliability is related to resilience [3], [7], [55].

In this study, the authors tackle safety in SoS through risks and resilience analysis with respect to structural models in addition to operational and functional processes of the SoS. Risks analysis addresses menaces that could possibly affect component systems. While the structural analysis anticipates the impact of these menaces on the architecture of the SoS and implicitly on the process continuity. These approaches are effective manners to anticipate risks, their influence and impact on the SoS. The combination of both approaches quantitatively anticipates resilience measurements of SoS in the architecting phase. This implicitly embraces a step towards safety evaluation and enhancement.

Accordingly, the authors insinuate by process continuity the resumption of the performance of systems, groups and the SoS after the occurrence of a disturbance. The correlation between the concept of process continuity and the proposed metrics is that the anticipation of the impact of a risk, based on a structural analysis, can help to foresee its impact on the performance on SoS and the process continuity after recovery.

Safety and resilience concepts are two strongly related notions. This study aims to emphasize the mutual correspondence between the two concepts. Resilience evaluation and assessment implies the implicit evaluation and assessment of the safety. See Figure 1 that represents an overview of the proposed model which also explains the correspondence between resilience and safety.

With this in mind, when a reorganization of a SoS architecture is triggered by an application of the proposed combination of approaches, it assesses the SoS structure and evaluates its capability to survive and keep performing as expected during and after the disturbance(s). Therefore, this implicitly concerns the safety enhancement as the more it is resilient and capable of performing as expected without failing, the safer it is. Another theory is that resilience assessment through this proposition contributes to the quantitative anticipation of the degree of safety of the SoS.

7. Case study

In this section, a projection of the analysis and approach is done on a case study (see Figure 6). An economic infrastructure of an area in France is represented by the global SoS. Geographical locations are differentiated by colors in order to emphasize territorial region and regional competitiveness. They form three groups of fourteen enterprises presented as component systems. Dependencies' arrows represent both production lines and relations between enterprises.

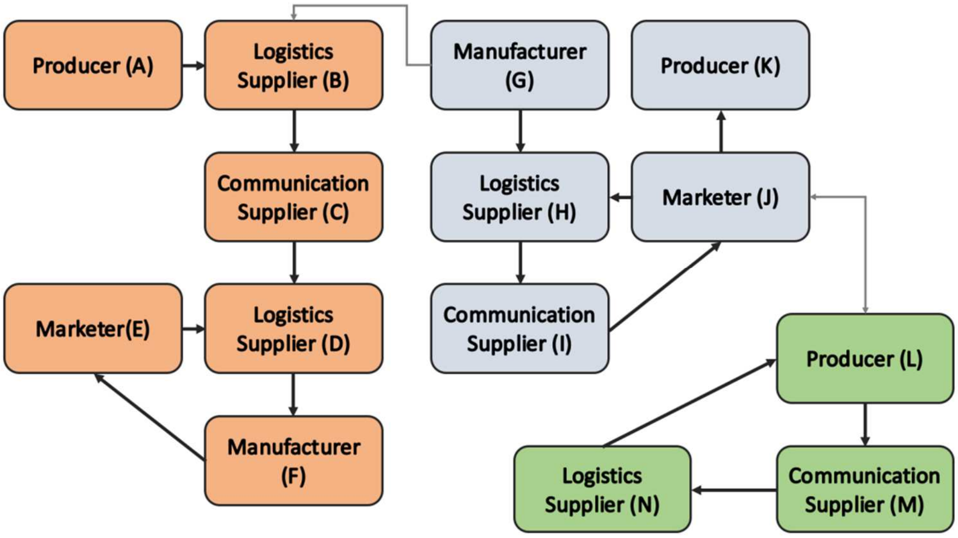


Figure 6. Dependency network of the studied SoS

In fact, economic infrastructure refers to the internal facilities of a country that ease business activity, such as communication, transportation, distribution networks and markets.

A SoS can be given a topology that accounts for the static representation of its components and the manner they can interact and cooperate [7], [10]. The idea is to focus on the component's interface, where data, services and quantities are exchanged through functional relationships, i.e. functional dependencies.

7.1. Risk's monitoring application

In practical terms, each aspect of organizational, functional, technical and geographical barriers is evaluated by virtue of the taxonomy presented in section 4. Therefore, if an interdependency has a barrier or an obstacle that prevents the interaction from being successful it should be mentioned on the dashboard, represented by Table 2, as the latter embraces all information about the obstacles hindering the SoS viability in order to effectively address them.

The authors aim to evaluate the interdependencies between enterprises that are considered as component systems within the studied SoS through risks' classification. They note that this case study is based on a real case and the information within Table 2 is based on real information.

Table 2. Illustration of the risks' monitoring dashboard for the studied case

Interdependence	Class of risk	The origin of the risk	The severity of the risk	The duration of the risk	The duration of the disturbed state	The failure rate
B to C	Logical Vulnerability	Application in System B	4th degree	From the beginning of the interdependence	Unpredictable	Undefined
F to G	Functional and technical	Procedures, standards and technological	2nd degree	Every time the interdep-endence is being	Every time the interdep-endence becomes	

		incompatibility		operational	operational	Undefined
M to N	Logical Vulnerability	Application in System B	4th degree	From the beginning of the interdepend-dence	Unpredictable	Undefined
J to K	Organizational	Financial	1st degree	Every time the interdep-endence is being operational	Every time the interdep-endence becomes operational	Undefined
H to I	Organizational and Technical	Financial, and technological	2nd degree	Every time the interdep-endence is being operational	Every time the interdep-endence becomes operational	Undefined
J to L	Technical	Technological incompatibility	2rd degree	Every time the interdep-endence is being operational	Every time the interdep-endence becomes operational	Undefined
C to D	Functional	Human resources organization	1st degree	Every time the interdep-endence is being operational	Every time the interdep-endence becomes operational	Undefined

7.2. Frailty and criticality calculations

Figure 7 illustrates frailty and criticality values distribution across the studied SoS. It is evident that component systems ‘D’, ‘E’, ‘F’ and ‘K’ are “weaker” than the others as their frailty values are around 0.8 which means that they are affected by the failure of more than 80 % of their groups.

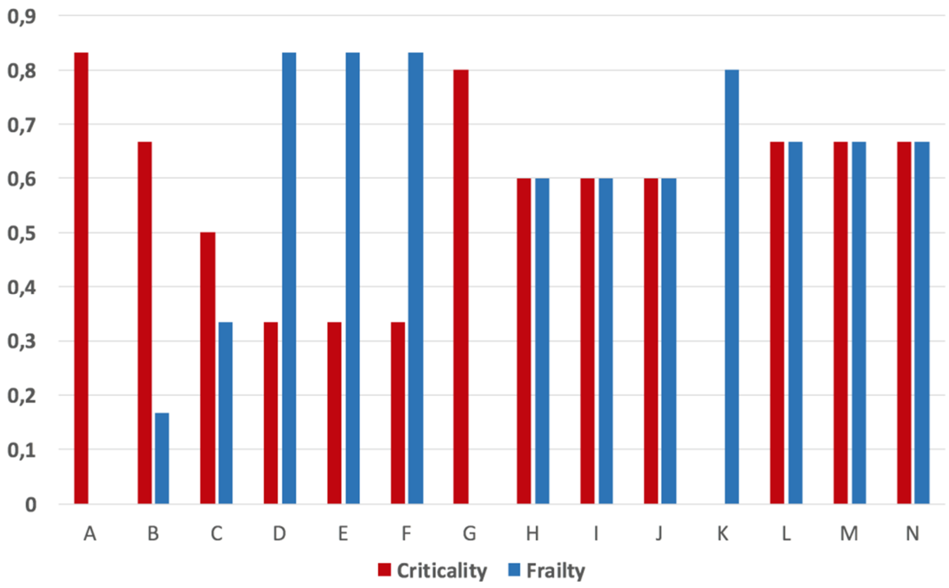


Figure 7. Frailty and criticality values distribution of all component systems

Accordingly, 'A' and 'G' are the most critical component systems in their groups by reaching around 0.8 in criticality values, which means that more than 80 % of each single group is affected by their failures.

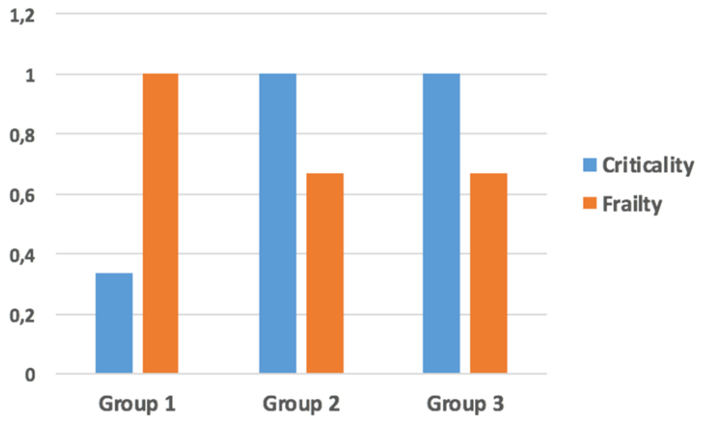


Figure 8. Groups criticality and frailty values distribution

The calculation of the criticality and frailty levels of each group on the rest of groups within the SoS is done as presented previously. In Figure 8, second and third groups are the most critical one among the three. While, the first group is the frailest group among the others.

This seems logical because if we return to Figure 6 illustrating the functional dependencies of the SoS, we intuitively deduct that the first group represents the end of the workflow pathway between groups within the studied SoS, hence its frailty. In addition, since both second and third groups represent simultaneously the start of the workflow pathway, they are equally critical to the first group and implicitly to the global system.

7.3. Failure impact and susceptibility calculations

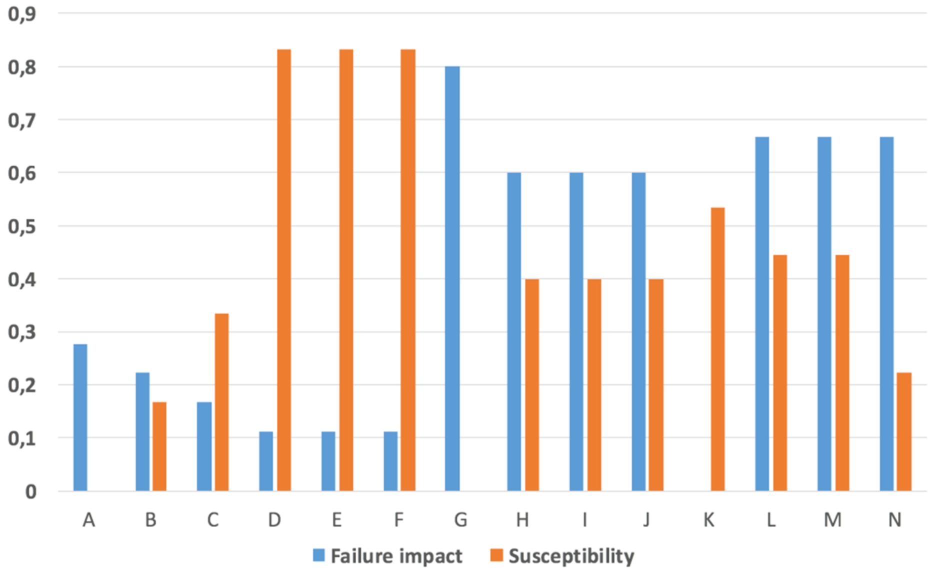


Figure 9. The distribution of failure impact and susceptibility values of all component systems

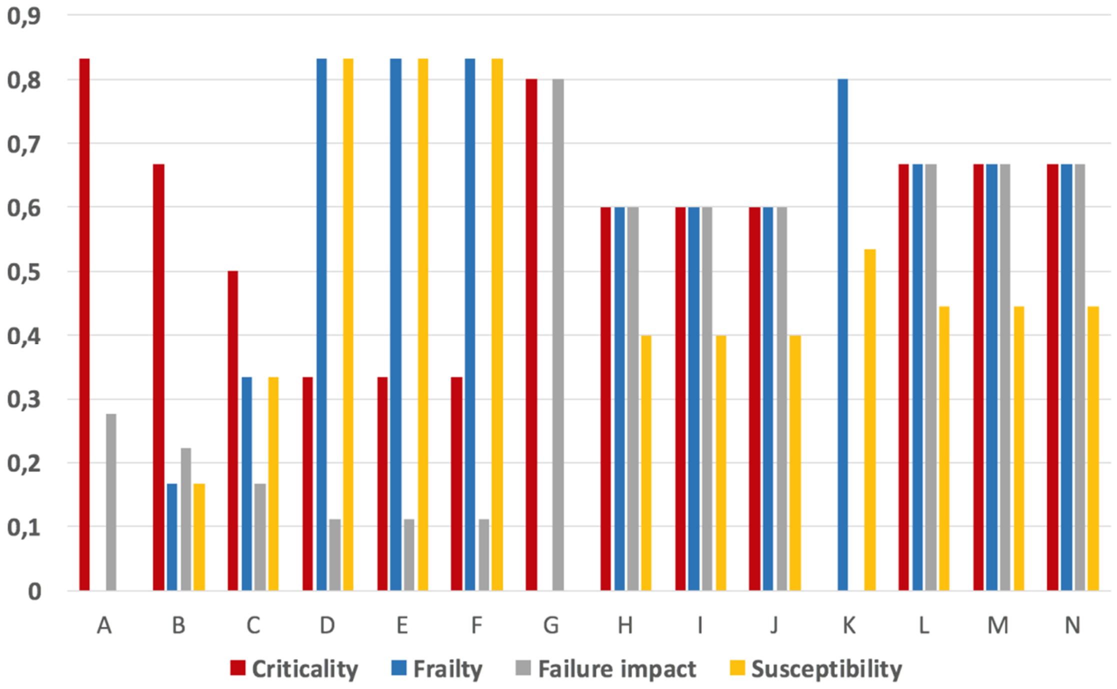


Figure 10. A comparative illustration of criticality, frailty, failure impact and susceptibility values of all component systems

Figure 9 illustrates the distribution of failure impact and susceptibility values of each system in the SoS. As explained earlier, failure impact depends on two different metrics: the criticality of component systems inside groups and the groups' criticality to the SoS. While susceptibility depends on the frailty of component systems inside groups and the groups' frailty to the SoS.

Figure 10 illustrates the contrast between criticality, frailty, failure impact and susceptibility metrics. It demonstrates through the studied SoS that a highly critical component system does not necessarily have a high failure impact on the SoS and global process continuity. The same thing goes for frailty and susceptibility.

And by highly critical, the authors mean that the element in question, whether it is a system or a group, is impactful more than the other elements.

7.4. Towards safer economic infrastructure

Practically, there are numerous manners to address safety issues through the results generated from the combination of both risks management and structural analysis approaches. In this case study, it is supposed that the SoS is already established. Thus, a structural enhancement is triggered in order to assure SoS safety. Accordingly, the authors propose some measures in order to enhance the SoS safety, therefore, the economic infrastructure's safety.

Some measures can be triggered by the results generated from the risk's monitoring dashboard, which evaluates the interdependencies between enterprises (approached as component systems). For example, we can address risks by their severity order (from the most influential to the least).

An alternative to address SoS safety is proposed by failure impact results, which locate and classify impactful component systems on SoS safety and process continuity. For example, we can address dependencies linking component systems by respecting their failure impact order (from the most influential to the least).

Another alternative is proposed by susceptibility calculations which locate frail component systems. For example, we can address issues related to dependencies linking component systems by respecting their susceptibility order (from the most influenced to the least).

Moreover, a more balanced option lays in equilibrating between approaches results and avoiding prioritization between them instead of merely depending on one approach. Other aspects could be considered for pertinent safety enhancement, for instance: (political, strategic, natural, etc.) environment embracing the economic infrastructure, expectations from it, the process amid the SoS, etc.

The authors believe that the proposed approaches can be useful at the conceptual level (SoS architects could use these approaches in order to conceive a well-balanced and safe SoS) and after the construction of the SoS (as engineers could use the presented approaches in order to enhance structural SoS safety).

Epilogue

In this work, the authors responded to the concerns related to SoS safety through resilience assessment by managing risks and analyzing the structural architecture of SoS. They proposed an approach to anticipate risks, their influences and impacts, which contributes to the quantitative anticipation of SoS resilience and safety. This implicitly embraces a step towards safety evaluation and enhancement. It is authors' belief that safety and resilience concepts are two strongly related notions. This study aims to emphasize the mutual correspondence between the two concepts.

An application of the theory is effectuated on a real-based economic infrastructure of a geographic area in France approached as SoS approach. The economic infrastructure represents the internal facilities of a country that eases business activities, such as communication, transportation, distribution networks and markets.

As a perspective, the authors believe that this work can be extended to cover this limitation. Furthermore, a proactive approach for SoS resilience assessment while integrating new systems and removing existing ones could also be a judicious perspective; since it is common for SoS to be heterogeneous and to support systems integration and segregation while maintaining the performance.

In addition, the automatization of the reorganization process is also an important perspective as the current proposal requires the existence of a management authority for the evaluation and the rearrangement of the SoS architecture.

Acknowledgements

This research is supported by the European Union (EU) with the European Regional Development Fund (ERDF) and the Regional Council of Normandie.

References

[1] Abbott, R. (2007, January). Emergence and Systems Engineering: Putting Complex Systems to Work. In Symposium on Complex Systems Engineering, RAND Corporation, Santa Monica, CA (pp. 11-12).

[2] Aven, T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Analysis, 31(4), 515-522.

[3] Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, 1(1), 11-33.

[4] Bone, M. A., Cloutier, R., Korfiatis, P., & Carrigy, A. (2010, June). System architecture: Complexities role in architecture entropy. In System of Systems Engineering (SoSE), 2010 5th International Conference on (pp. 1-6). IEEE.

[5] Bukowski, L. (2016). System of systems dependability–Theoretical models and applications examples. Reliability Engineering & System Safety, 151, 76-92.

[6] Dahmann, J., Lane, J. A., Rebovich, G., & Lowry, R. (2010, June). Systems of systems test and evaluation challenges. In System of Systems Engineering (SoSE), 2010 5th International Conference on (pp. 1-6). IEEE.

[7] Ed-daoui, I., Itmi, M., Hami, A. E., Hmina, N., & Mazri, T. (2018). A deterministic approach for systems-of-systems resilience quantification. International Journal of Critical Infrastructures, 14(1), 80-99.

[8] Ed-daoui, I., Mazri, T., & Hmina, N. (2016). Security Enhancement Architectural Model for IMS based Networks. Indian Journal of Science and Technology, 9(46).

[9] I. Ed-daoui, T. Mazri, and N. Hmina. Towards Reliable IMS-based Networks. LAP LAMBERT Academic Publishing, 2017.

[10] Filippini, R., & Silva, A. (2014). A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. Reliability Engineering & System Safety, 125, 82-91.

[11] Griendling, K., & Mavris, D. (2010, June). An architecture-based approach to identifying system-of-systems alternatives. In System of Systems Engineering (SoSE), 2010 5th International Conference on (pp. 1-6). IEEE.

[12] Hitchins, D. K. (2003). Advanced systems thinking, engineering, and management. Artech House.

[13] Jamshidi, M. O. (2008). System of systems engineering-New challenges for the 21st century. IEEE Aerospace and Electronic Systems Magazine, 23(5), 4-19.

[14] Johnson, S. (2002). Emergence: The connected lives of ants, brains, cities, and software. Simon and Schuster.

[15] Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., ... & Rabadi, G. (2003). System of systems engineering. Engineering Management Journal, 15(3), 36-45.

[16] M. L. Kuras. Complex-system engineering. In Symposium on Complex Systems Engineering, RAND Corporation, 2007.

[17] K. Ludeman and E. Erlandson. Coaching the alpha male. Harvard Business Review, (5), 2004.

[18] Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. IEEE Systems Journal, 3(2), 181-191.

[19] Mansouri, M., Sauser, B., & Boardman, J. (2009, March). Applications of systems thinking for resilience study in maritime transportation system of systems. In Systems Conference, 2009 3rd Annual IEEE (pp. 211-217). IEEE.

[20] Mansouri, M., Sauser, B., & Boardman, J. (2009, March). Applications of systems thinking for resilience study in maritime transportation system of systems. In Systems Conference, 2009 3rd Annual IEEE (pp. 211-217). IEEE.

[21] Reed, D. A., Kapur, K. C., & Christie, R. D. (2009). Methodology for assessing the resilience of networked infrastructure. IEEE Systems Journal, 3(2), 174-180.

[22] Ruiz-Martin, C., López-Paredes, A., & Wainer, G. (2018, January). What we know and do not know about organizational resilience. In International Journal of Production Management and Engineering (Vol. 6, No. 1, pp. 11-28). Universitat Politècnica de València.

[23] Ryan. A. Personal Communication. 2006.

[24] Saleh, J. H., & Marais, K. (2006). Highlights from the early (and pre-) history of reliability engineering. Reliability engineering & system safety, 91(2), 249-256.

[25] Sherrieb, K., Norris, F. H., & Galea, S. (2010). Measuring capacities for community resilience. Social indicators research, 99(2), 227-247.

[26] Tannahill, B. K., & Jamshidi, M. (2014). System of Systems and Big Data analytics–Bridging the gap. Computers & Electrical Engineering, 40(1), 2-15.

[27] Tran, H. T., Domerçant, J. C., & Mavris, D. N. (2016). A Network-based Cost Comparison of Resilient and Robust System-of-Systems. Procedia Computer Science, 95, 126-133.

[28] Uday, P., & Marais, K. B. (2014). Resilience-based system importance measures for system-of-systems. Procedia Computer Science, 28, 257-264.

[29] Verny J., Itmi M., El Hami A., Cardon A., Couturier L. & Abdulrab H. (2012). A sustainable multidisciplinary approach to building regional competitiveness. In the Symposium on security and safety of Complex Systems.

[30] Yaghlane, A. B., & Azaiez, M. N. (2017). Systems under attack-survivability rather than reliability: Concept, results, and applications. European Journal of Operational Research, 258(3), 1156-1164.

[31] Zhang, W. J., & Lin, Y. (2010). On the principle of design of resilient systems–application to enterprise information systems. Enterprise Information Systems, 4(2), 99-110.

[32] Wang, J. W., Gao, F., & Ip, W. H. (2010). Measurement of resilience and its application to enterprise information systems. Enterprise Information Systems, 4(2), 215-223.

[33] Liu, D., Deters, R., & Zhang, W. J. (2010). Architectural design for resilience. Enterprise Information Systems, 4(2), 137-152.

[34] Erol, O., Sauser, B. J., & Mansouri, M. (2010). A framework for investigation into extended enterprise resilience. Enterprise Information Systems, 4(2), 111-136.

[35] Maier, M. W. (1998). Architecting principles for systems-of-systems. Systems Engineering: The Journal of the International Council on Systems Engineering, 1(4), 267-284.

[36] Department of Defense, System of Systems Engineering in Defense, Acquisition Guidebook, Washington (2004).

[37] Xia, B., Zhao, Q., Dou, Y., & Zhan, C. (2016, July). Robust system portfolio modeling and solving in complex system of systems construction. In Control Conference (CCC), 2016 35th Chinese (pp. 9573-9577). IEEE.

[38] Kotov, V. (1997). Systems of systems as communicating structures (Vol. 119). Hewlett Packard Laboratories.

[39] Ed-daoui13, I., El Hami, A., Itmi, M., Hmina, N., & Mazri, T. (2018). Unstructured Peer-to-Peer Systems: Towards Swift Routing. International Journal of Engineering & Technology, 7(2.3), 33-36.

[40] Tran, H. T., Balchanos, M., Domerçant, J. C., & Mavris, D. N. (2017). A framework for the quantitative assessment of performance-based system resilience. Reliability Engineering & System Safety, 158, 73-84.

[41] Holling, C. S. (1973). Resilience and stability of ecological systems. Annual review of ecology and systematics, 4(1), 1-23.

[42] Woods, D. (2006, October). Engineering organizational resilience to enhance safety: A progress report on the emerging field of resilience engineering. In Proceedings of the human factors and ergonomics society annual meeting (Vol. 50, No. 19, pp. 2237-2241). Sage CA: Los Angeles, CA: Sage Publications.

[43] Turnquist, M., & Vugrin, E. (2013). Design for resilience in infrastructure distribution networks. Environment Systems & Decisions, 33(1), 104-120.

[44] Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational models of infrastructure resilience. Risk Analysis, 35(4), 562-586.

[45] Sterbenz, J. P., Çetinkaya, E. K., Hameed, M. A., Jabbar, A., Qian, S., & Rohrer, J. P. (2013). Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation. Telecommunication systems, 52(2), 705-736.

[46] Ip, W. H., & Wang, D. (2011). Resilience and friability of transportation networks: evaluation, analysis and optimization. IEEE Systems Journal, 5(2), 189-198.

[47] Zhao, K., Kumar, A., Harrison, T. P., & Yen, J. (2011). Analyzing the resilience of complex supply network topologies against random and targeted disruptions. IEEE Systems Journal, 5(1), 28-39.

[48] Mendonça, D., & Wallace, W. A. (2015). Factors underlying organizational resilience: The case of electric power restoration in New York City after 11 September 2001. Reliability Engineering & System Safety, 141, 83-91.

[49] Leveson, N., Dulac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., & Barrett, B. (2006). Engineering resilience into safety-critical systems. In Resilience engineering: Concepts and precepts (pp. 95-123). Ashgate, Surrey.

[50] Zang, C., Friswell, M. I., & Mottershead, J. E. (2005). A review of robust optimal design and its application in dynamics. Computers & structures, 83(4-5), 315-326.

[51] Zhang, W.J. (2007). Is resilience the destiny for safety management paradigm? Presentation at the Northeastern University of China.

[52] Zhang, W.J. (2008). Resilience engineering [online]. Presented at a seminar at Chinese Natural Science Foundation. Available from: http://homepage.usask.ca/*wjz485/Other%20 Publication.htm [Accessed 3 November 2009].

[53] Hollnagel, E., Woods, D. D., & Leveson, N. (2007). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd..

[54] Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., ... & Scrimshaw, S. C. (2013). Disaster resilience: A national imperative. Environment: Science and Policy for Sustainable Development, 55(2), 25-29.

[55] Birolini, A. (2017). Reliability engineering: theory and practice. Springer.

[56] Hollnagel, E. (2016). The four cornerstones of resilience engineering. In Resilience Engineering Perspectives, Volume 2 (pp. 139-156). CRC Press.

[57] Cedergren, A., Johansson, J., & Hassel, H. (2017). Challenges to critical infrastructure resilience in an institutionally fragmented setting. Safety Science.

[58] Reason, J. (2016). Managing the risks of organizational accidents. Routledge.

[59] Zhang, C., Kong, J. J., & Simonovic, S. P. (2018). Restoration resource allocation model for enhancing resilience of interdependent infrastructure systems. Safety Science, 102, 169-177.

[60] Tran, H. T., Balchanos, M., Domerçant, J. C., & Mavris, D. N. (2017). A framework for the quantitative assessment of performance-based system resilience. Reliability Engineering & System Safety, 158, 73-84.

[61] Cedergren, A., Johansson, J., & Hassel, H. (2017). Challenges to critical infrastructure resilience in an institutionally fragmented setting. Safety Science.

[62] Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. Safety Science, 102, 79-100.

[63] Stroeve, S. H., & Everdij, M. H. (2017). Agent-based modelling and mental simulation for resilience engineering in air transport. Safety science, 93, 29-49.

[64] Harvey, C., & Stanton, N. A. (2014). Safety in System-of-Systems: Ten key challenges. Safety science, 70, 358-366.

[65] Alexander, R., & Kelly, T. (2013). Supporting systems of systems hazard analysis using multi-agent simulation. Safety science, 51(1), 302-318.