A deterministic approach for systems-of-systems resilience quantification

Ilyas Ed-daoui*
LMN Laboratory, INSA Rouen Normandy,
University of Rouen Normandy,
685 University Av.,
76800 Saint-Etienne-du-Rouvray, France
and
LGS Laboratory, ENSA of Kenitra,
Ibn ToFAIL University,
BP 242, University Av., Kenitra 14 000, Morocco
Email: edd.ilyas@gmail.com
*Corresponding author

Mhamed Itmi
LITIS Laboratory, INSA Rouen Normandy,
University of Rouen Normandy,
685 University Av.,
76800 Saint-Etienne-du-Rouvray, France
Email: mhamed.itmi@insa-rouen.fr

Abdelkhalak El Hami
LMN Laboratory, INSA Rouen Normandy,
University of Rouen Normandy,
685 University Av.,
76800 Saint-Etienne-du-Rouvray, France
Email: abdelkhalak.elhami@insa-rouen.fr

Nabil Hmina
LGS Laboratory, ENSA of Kenitra,
Ibn ToFAIL University,
BP 242, University Av., Kenitra 14 000, Morocco
Email: hmina@univ-ibntofail.ac.ma

Tomader Mazri
ETSE Laboratory, ENSA of Kenitra,
Ibn ToFAIL University,
BP 242, University Av., Kenitra 14 000, Morocco
Email: tomader20@gmail.com

Copyright © 2018 Inderscience Enterprises Ltd.
A deterministic approach for systems-of-systems resilience quantification

Abstract: With recent advances in systems-of-systems, reliability analysis becomes a very challenging research topic. One of the most pressing issues is to figure out a plan to handle resilience. On this basis, we propose, in this paper, a structural deterministic approach to quantitatively measure systems resilience. This approach is based on a three-step method. First, evaluate the functional dependencies between groups by considering a system-of-systems as a large-scale interconnected network of systems distributed into interdependent groups. This leads us to better understand the overall connections and process continuity. Next, analyse how much the global architecture of the system-of-systems depends on every group. Last, estimate its structural resilience by measuring the impact of each system’s failure on the other systems forming the global system and building the process. Two case studies are provided to experiment our approach. The results are cross-compared and evaluated.

Keywords: critical infrastructures; criticality; failure impact; reliability; resilience; systems-of-systems.


Biographical notes: Ilyas Ed-daoui is currently a PhD student in the LGS Laboratory in the ENSA-Kenitra of Morocco. He is in international cotutelle of thesis with LMN Laboratory at INSA-Rouen of France. His thesis title is: ‘The reliability of systems-of-systems’. He is also the author and co-author of a book and a number of papers published in international journals and conferences. He obtained his Master’s in Information Systems Security at the ENSA-Kenitra of Morocco and Bachelor of Mathematics and Informatics at the Mohammed V University.

Mhamed Itmi earned his PhD in Probability Theory and Statistics in 1980 and second PhD in Computer Science in 1989. He received his Habilitation Diploma to supervise research (HDR) in 2006 with the focus on the modelling and simulation of distributed discrete event systems. He managed different logistics and transportation research projects and supervised several PhD theses. He also is the author and co-author of more than 100 papers published in international journals and conferences. His research presently focuses on autonomous systems. He is an Associate Professor at the INSA-Rouen, France.

Abdelkhalak El Hami is a Full Professor at INSA Rouen, Normandy France, as well as the Deputy Director of LMN and Director of Mechanical Engineers. His research activities include reliability-optimisation systems. He has supervised 38 PhD theses. He also is the author and co-author of more than a 20 books and more than 550 papers published in international journals and conferences. He received his Doctorate in Engineering Sciences from the University of Franche-Comté in France in 1992. He received his Habilitation Diploma to supervise research (HDR) in 2000. He is the Editor-in-Chief of three sets of international books: ISTE, Wiley and Elsevier.

Nabil Hmina earned his PhD in Engineering Sciences in University and Central School of Nantes, 1994. He is a Full Professor, the Director of the National School of Applied Sciences of Kenitra since 2011, Vice-President for Academic Affairs and Information Technology of the University Ibn Tofail, 2005–2011 and Director of Laboratory of Systems Engineering since 2012. He is a partner and coordinator of several European projects, organiser, Chairman.
and a member of program committees and scientific boards of several international and national conferences in the field of computer security, optimisation, embedded systems, and renewable energy. He supervised several PhD theses. He also is the author and co-author of several books and a number of papers published in notorious journals and international conferences.

Tomader Mazri received her HDR degree in Networks and Telecommunication from Ibn Tolaf University, PhD in Microelectronics and Telecommunication from Sidi Mohamed Ben Abdellah University and INPT of Rabat, Master’s in Microelectronics and Telecommunication Systems, and Bachelor’s in Telecommunication from the Cadi Ayyad University. She is currently a Professor at the National School of Applied Sciences of Kenitra, a permanent member of Electrical and Telecommunications Engineering Laboratory, author and co-author of 20 articles journals, 30 articles in international conferences, a chapter and three books. Her major research interests are on microwave systems for mobile and radar, smart antennas and mobile network security.

1 Introduction

Research on critical infrastructures is crucial for the security and safety of modern societies and their assets. There are some existing initiatives, precisely in Department of Homeland Security (2003) and European Council (2008), giving emphasis to the development of technical support to policymaking, and analysis tools for the assessment of critical infrastructures. These tools privilege a systemic view of the overall infrastructure, so systems may recognise and trade-off, by themselves, the different and conflicting objectives (Hémon and Robert, 2014).

The word infrastructure is not conceived as a unique static entity, but it is rather the aggregation of components which adjust their interrelationships in accordance with changes in the operation scenario (Carlock and Lane, 2006).

In recent literature, infrastructures are classified as a special instance of systems-of-systems of which they possess a number of distinctive features such as operational and managerial independence, geographical distribution, emergent behaviour and evolutionary development (Sousa-Poza et al., 2008; Jamshidi, 2008; Eusgeld et al., 2011; Kotov, 1997; Nguyen et al., 2016; Polinpinhino and Keating, 2015).

To sire the broad scope of systems-of-systems is a tremendous challenge. They are super systems comprised of several heterogeneous systems which themselves were not conceived to cooperate (Keating et al., 2003; Konur et al., 2006; Boardman and Sauser, 2006; Walewski, 2016; Valerdi et al., 2008). They operate autonomously but in mutual interaction so as to achieve a common goal (Katina and Hester, 2013; Jamshidi, 2008). Whereas, the inherent and growing need for the exploitation of such systems, as well as the rapidly increasing cost incurred by loss of operation as a consequence of failures, stimulate some serious reliability concerns.

Nowadays, we expect of a system-of-systems more than just to be functional and free from failures and defects in the implementation phase but also to enhance its reliability level, to preserve the same performance, to complete the required functions and most importantly to anticipate as many defects as possible in the architecting phase (Aggarwal, 1993; Han et al., 2012; Xia et al., 2016).
In fact, there are numerous perspectives to tackle reliability in the context of systems-of-systems (Cardon and Itmi, 2016; Ed-daoui et al., 2016). A recent one is related to the relationship with the concept of resilience (Laprie et al., 2004; Zio, 2009). The latter is defined as the ability of systems to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time, and composite costs, and risks.

Resilience is about the consequences in the case of disturbances and associated uncertainties, and it reflects the ability of the system to withstand them and recover (Aven, 2011; Sherrieb et al., 2010). We say that a system is resilient if it can face disturbances and gets back to normal performance within an acceptable duration (Aven, 2011; Uday and Marais, 2014; Tran et al., 2016; Norris et al., 2008).

In our work, we try to respond to the stimulated concerns related to reliability by the growing need for the exploitation of systems-of-systems. We propose a deterministic approach to quantify systems’ resilience via a structural analysis of the architecture of systems-of-systems. We evaluate the functional dependencies between groups. Then we analyse how much process continuity depends on every system, by studying the criticality level of each system. After that, we estimate the failure impact of each system in order to evaluate the structural resilience of the whole system-of-systems.

The estimation of the failure impact of each system helps to anticipate, from a quantitative perspective, the resilience measurements of the system-of-systems. This includes implicitly the reliability evaluation and analysis.

The idea of conceiving such a metric is actually simple. We need a methodology to measure each system’s failure impact on the rest of the system and working process in order to be cognizant of the rate of the possibility of system’s survivability after each system’s failure. This is our perspective to handle resilience of systems-of-systems.

This paper is organised as follows:

- We introduce the reliability of systems-of-systems and, then we present explicitly our adopted methodology (Section 2).
- We give the syntax and semantics of our approach dedicated to the quantitative estimation of resilience. We also illustrate our method on the first case study (Section 3).
- We apply our approach on the second case study in order to see how our metric will behave. The results of both examples are evaluated and cross-compared (Section 4).

## 2 A literary comparison of related methodologies

The resilience of systems-of-systems is a relatively new field of study that has emerged in the 21st century and, as such, its literature is fragmented. Thus, in order to undertake a discussion of the systems-of-systems and resilience, it is first necessary to survey the existing works addressed to assess these concepts.

One is the infrastructure resilience-oriented modelling language (IRML) (Filippini and Silva, 2015) which is designed to facilitate the analysis of operational interdependencies of infrastructure’s components, resilience, the ability to withstand disturbances and recover.
This approach has three major objectives. First is to model infrastructure interdependencies; second is to support a resilience-oriented analysis, and the third one is to provide results for thorough preliminary assessments of criticality and vulnerability to support decision-making.

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 behaviour of a system-of-systems, in order to provide additional insights about possible misbehaviours at a large-scale.

Same authors propose a modelling framework for resilience analysis in Filippini and Silva (2014). The paper represents a methodology of resilience analysis of systems-of-systems. A conceptual representation of the infrastructure, based on the functional relationships among its components, is given and then analysed with respect to structural and dynamic properties of the system under study.

Functional dependencies among components (e.g., producer-consumer, controller-controlled) are the modelling focus and are represented by a dependency network, which is analysed with respect to its structural and dynamic properties.

The structural analysis focuses on functional dependencies among components. The dynamic analysis copes with the network response to a disturbance, which is done by a conditional analysis that returns a pre-screening of the proneness of the network to develop.

The previously presented works are complementary and propose perspectives to assess the systems-of-systems’ resilience, the consideration of the infrastructure’s architecture in the evaluation of resilience, as well as the structural analysis.

However, the criticality, by definition in Filippini and Silva (2014) which represents the direct and indirect dependency for each system on the rest of systems, does not consider the possible existence of groups within the system-of-systems.

In other words, it considers only one infrastructure for the whole system-of-systems. This perspective is limitative, as the system-of-systems in question could embrace a composition of various infrastructures called groups (in this paper, the term ‘group’ stands for a combination of systems active in a given economic sector) with all their properties and constraints. This emerges the need for a metric considering the heterogeneity of the global infrastructure of systems-of-systems.

Another framework dedicated to the evaluation of systems-of-systems was proposed in Bukowski (2016). The proposed theoretical models and examples are based on the methodology of service engineering and are closely related to the idea of resilient enterprise as well as to the concept of disruption-tolerate operation.

A collective concept describing the time-related operating quality of a system is also proposed in the same paper. It is called dependability. It represents the ability to avoid disruptions that are more frequent and more severe in consequences.

The proposed framework adopts a service continuity oriented approach in order to quantitatively assess the systems-of-systems dependability. Three proposed perspectives to embrace systems’ dependability are proposed, which are availability related probabilistic approach, availability and credibility related probabilistic deterministic approach and risk related approach.

The availability related probabilistic approach has three influencing factors of availability defined as following:
A deterministic approach for systems-of-systems resilience quantification

- Reliability performance: is the ability of an item to perform a required function under given conditions for a given time interval.

- Maintainability performance: is the ability of an item under given conditions of use, to be retained in or restored to a state in which it can perform a required function when maintenance is performed under given conditions and using stated procedures and resources.

- Maintenance support performance: is the ability of maintenance organisation, under given conditions to provide upon demand, the resources required to maintain an item, under a given maintenance policy.

The availability and credibility related probabilistic approach, dependability owns two components:

- Availability: as probabilistic component, its performance measures can be created with support of statistical tools.

- Credibility: it is defined as the extent to which a system is able to recognise and signal the state of the system and to withstand incorrect inputs or unauthorised access.

- The deterministic property consists of two other components:

- Integrity: the assurance provided by a system that the task will be performed correctly unless notice is given any state of the system, which could lead to the contrary.

- Security: the assurance provided by a system that any incorrect input or unauthorised access is denied

Finally, the dependability, as an integrative concept, consists of three parts:

1 Dependability attributes:
   - availability
   - reliability
   - safety
   - confidentiality
   - integrity
   - maintainability

2 Dependability means:
   - fault prevention
   - fault tolerance
   - fault removal
   - fault forecasting
3 Dependability threats:
- faults
- errors
- failures.

Two models dedicated to the evaluation of the dependability of systems-of-systems, are also developed:
- The static model: can be created as a fuzzy logic-oriented advisory expert system and it is useful at the design stage of systems-of-systems or in situations when insufficient data obstruct the estimation of the statistical measures.
- The dynamic model: is based on the risk oriented approach and can be useful both at the design stage and for the management of the systems-of-systems.

The limitation of this approach is that the proposed models for siring the concept of dependability are probabilistic and stochastic and possess some inherent randomness, which means that the same dependency network and initial conditions may lead to different (random) resilience measures. Thus, the evaluation of the resilience of systems-of-systems via this perspective may be evasive.

In Katina and Hester (2013), resiliency along with interdependency, dependency, and risk sculpt a comprehensive four tuple of criticality factors, in an attempt to create a generalisable method for prioritising critical infrastructures. This method contributes to the ranking and prioritisation of infrastructures.

Each criticality factor owns miscellaneous and distinct mechanism for measurement:
- Level of resiliency is measured via system defensive properties (deterrence, detection, delay, response).
- Level of interdependency is measured via infrastructure system connectedness (external relationships).
- Level of dependency is measured via usability (economic performance, effects, magnitude of failure, cost to repair).
- Level of infrastructure risk is measured by traditional risk approaches (probability of occurrence and consequences) it can be extended to include threat, vulnerability and intent.

The concept of resiliency, espoused by authors in Katina and Hester (2013), refers to system defensive characteristics (for instance: detection, time to recovery, etc.), system defensive properties (including physical barriers), maintenance capability to resist attacks, susceptibility, capacity, time to repair, availability of warning systems, and critical time.

An application of this approach in the context of smart grids is in Katina et al. (2016). Authors extend the set of criticality’s factors proposed in Katina and Hester (2013) to also comprise probability and consequence in a new perspective baptised criticality-based approach (CBA). Each category measurement involves a set of properties that could be used in design, analysis, and evolution of smart grids. The development of countermeasures for issues associated with performance is also considered.
However, the limitation of the authors’ definition to resilience is that it lacks the consideration of the architecture of the infrastructure. The latter is captured by the factor of interdependency.

This means that an alteration of the infrastructure has no consequence on the resilience, which is absurd because the concept of resilience, by definition, reflects the ability of systems to withstand a major disruption within acceptable degradation parameters, to recover within acceptable conditions and about the consequences in the case of disturbances and associated uncertainties. This makes it strictly inherent to infrastructure.

In this context, we propose on the basis of structural analysis, a metric for the quantitative measurement of resilience. Following this method, we will be able to measure the system’s resilience in the architecting phase. This implicitly embraces the reliability status of the architecture by anticipating the failure impact of the existing systems of the architecture.

Figure 1  A taxonomy of criticality factors proposed in Katina and Hester (2013) (see online version for colours)

3 Resilience of systems-of-systems as an object of investigation

3.1 General overview

In this section, we project our analysis and approach on two case studies (see Figure 2 and Figure 7). We consider the economic infrastructure of a region as the global system-of-systems, economic sectors as groups and companies as systems. Dependencies’ arrows represent both process direction and relations between enterprises.

We hint by economic infrastructure the internal facilities of a country that ease business activity, such as communication, transportation, distribution networks and markets.
Before we commence the explanation of the proposed approach, we opine that it is crucial to clarify some concepts used in our explanation. Let us start with failures. Failures represent the abortion, suspension or alteration of an operation of a business activity (which in our context refers to communication, transportation, distribution or any other activity within an economic infrastructure) between at least two systems.

These failures could be due to two categories of disturbances:

- **Internal disturbances**: which are abnormalities inside the systems or the global system-of-systems.
- **External disturbances**: which are abnormalities due to external basis as politics.

The process continuity refers to the resumption of the performance of systems, groups and the global system-of-systems after the occurrence of the disturbance. The correlation between the concept of process continuity and the proposed metric is that the anticipation of the impact of a failure, based on a structural analysis, can help to foresee its impact on the performance on systems-of-systems and the process continuity after recovery.

### 3.2 Structural analysis

The aim of the structural analysis step is to analyse the functional dependencies between systems and groups, then to measure the criticality level, in order to deduct the related failure impact rate. This process should be applied, similarly, on every single system based on the system’s structural architecture.

#### 3.2.1 Functional dependencies analysis

Generally, the purpose of the dependency analysis is to focus on data pathways. The functional dependency scheme analysis represents the overall representation of all the relevant functional dependencies. In our work, we target the adoption of this technique because we see that 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.

In fact, the dependency network analysis technique has been applied first to operational networks based on the functional dependency network analysis (FDNA) (Guariniello and DeLaurentis, 2013). This method is used to evaluate the effect of topology and possible degraded functioning of one or more systems on the operability of each system in the network. Therefore, the resilience of systems-of-systems can be evaluated in terms of capability to reduce the loss of operability when single systems are affected by partial failures.

We represent in Figure 2 our case study that includes three groups, since it is not uncommon for systems-of-systems to overcome infrastructural circumferences. Each one of these groups is composed of several systems put in different geographical locations and following different schemes to interact.

As we mentioned at the beginning of this section, the system-of-systems, illustrated in Figure 2, refers to the economic infrastructure of a region, groups stand for economic sectors and systems symbolise companies. The dependencies’ arrows represent relations between enterprises and process direction.
3.2.2 Systems’ criticality analysis

Another important step in the structural analysis is the criticality measurement. The latter is very helpful in calculating our proposed metric. In other words, we need to calculate the criticality of every system in order to be able to deduct the related values of our metric.

The criticality, in a system-of-systems context, represents how much the process continuity relies on the systems and groups. Practically, it is calculated by using the formula below.

Let $E$ be the set of all the systems forming the group $r$ with $E = \{n_1, n_2, \ldots, n_{\text{Card}(E)}\}$. Then:

$$\forall n_i \in E: \text{Criticality}(n_i) = \frac{\text{Card}(C(n_i / \text{r}))}{\text{Card}(E)}$$ (1)

With:

$$i \in \{1, 2, ..., \text{Card}(E)\}$$

where

- $n_i$: represents a system from the evaluated group $r$.
- $\text{Card}(E)$: the total number of systems forming the group $r$.
- $\text{Card}(C(n_i / \text{r}))$: represents the number of systems inside the group that are directly or indirectly affected by the failure of the system $n_i$. 

At this stage, we suppose that the systems of the set $E$ are in a group $r$. Moreover, the criticality metric values range goes from 0 for not critical at all to 1 for very critical. We multiply the criticality value by 100 in order to get the criticality rate.

Figure 3 illustrates the variation of criticality values across all existing systems. It is obvious that there are systems that seem to be tremendously important and critical inside the group, particularly ‘A’ for the first group, ‘G’ for the second and ‘L’ for the third, these systems have a high criticality values reaching more than 0.7 which means more than 70% of the group may not be able to work correctly in case these systems fail.

Figure 3 The criticality of all systems synthesised by groups

Now, the question is: If a system has a criticality value inside a group, is that criticality value remains the same towards all the system-of-systems?

Let us analyse, for a second, the studied examples. The global system-of-systems, which represents the economic infrastructure of a region, contains three groups representing three different economic sectors. Similarly, each group comprises several systems illustrating companies.

Moreover, the criticality of a system represents the degree of reliance of the group on the system in question. So the question, in this context, opens a discussion whether the criticality of a system inside a group remains the same inside the global system-of-systems, or it, actually, changes.

The answer of this question will lead us to our proposed metric, which will be introduced in the following.

3.3 The failure impact metric

Before we answer the question asked in the previous section, which emphasises the need to evaluate the importance and criticality levels of each system to the studied system-of-systems and not only in their restricted group, we illustrate, in Figure 4, the criticality distribution of each group within the system-of-systems.
The calculation of the criticality level of each group on the rest of groups within the system-of-systems is done following the same tactic that we adopted to calculate the criticality of each system on the rest of systems within the same group.

As it is illustrated in Figure 4, the second group is the most critical one among the three, and it seems very logic because if we return to Figure 2 illustrating the functional dependencies of the studied system-of-systems, we intuitively deduct that the first and the third groups depend on the second to relate them, hence its importance and criticality.

**Figure 4** Groups’ criticality values distribution

After developing the dependency scheme and analysing the criticality of systems and groups, it is time to introduce our proposed metric which is called ‘the failure impact’. We define it as a structural metric conceived to quantitatively measure the system-of-systems resilience by measuring the impact of each system’s failure on the rest of systems forming the global system, with the consideration of the repartition of systems into groups.

To obtain the failure impact value of a system, we multiply its criticality value corresponding to its position towards the process inside the containing group by the criticality value of the same group corresponding to the process inside the system-of-systems, as shown in formula (2).

Let $E_j$ be the set of all the systems of each group $r_j$ within $F$ which represents the set of all groups forming the studied system-of-systems. With $E_j = \{n_1, n_2, \ldots, n_{\text{Card}(E_j)}\}$.

Then:

$$\forall (n_i, r_j) \in E_j \times F : FI(n_i) = \text{Criticality}_{\text{system}}(n_i) \times \text{Criticality}_{\text{Group}}(r_j)$$

(2)

With:

$$i \in \{1, 2, \ldots, \text{Card}(E_j)\}$$

$$i \in \{1, 2, \ldots, \text{Card}(F)\}$$
Criticality_{system} values range goes from 0 for not critical at all to 1 for very critical. Criticality_{Group} is equal to 1 in case there is no dependency between groups.

where:

- \( n_{ij} \): represents a system inside the group.
- \( r_{j} \): represents a group inside the system-of-systems.
- \( Card_{(ij)} \): the total number of systems forming the group
- \( Card_{(F)} \): the total number of groups forming the system-of-systems.
- \( Criticality_{system}(n_{ij}) \): refers to the criticality of the system inside the group.
- \( Criticality_{Group}(r_{j}) \): refers to the criticality of the group inside the system-of-systems.

We can obtain the ‘failure impact rate’ by simply multiplying the failure impact by 100.

Figure 5 illustrates the distribution of the failure impact of each system in the system-of-systems. It depends on two different metrics: the criticality of the system inside the group and the criticality of the groups themselves inside the system-of-systems.

Eventually, as an answer to the question asked in the previous section, where we wondered if a criticality value of a system inside a group, remains the same towards the system-of-systems. it turns out that a highly critical system inside the group does not imply that it is highly critical for the global system-of-systems unless the group embracing the system is highly critical.

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

So, in order to have a high failure impact, a system should be critical inside a critical group. As an illustration, the system ‘G’ has been the most impactful system inside the studied system-of-systems.

**Figure 5** Systems’ failure impact rates distribution for the first case study
The failure impact metric contributes in the anticipation of the resilience measurement by locating, in the architecting phase, the impactful systems and predicting their impacts on the system-of-systems. This location can be followed by the reorganisation of the architecture of the system-of-systems in order to demean the impact of systems on the process continuity and the overall performance of the global system-of-systems.

**Figure 6** Criticality and failure impact rates distribution and divergence for the first case study
Besides, when a system has a high failure impact that means that an important part of the system-of-systems could be affected in case of its deficiency. This means that the infrastructure is not resilient and robust enough to handle potential failures. Thus, the failure of one of the systems may provoke important disturbances to the performance of the system-of-systems and process continuity, which can be settled by the organisation of the infrastructure.

3.4 The failure impact vs. criticality analysis

In our study case, we work on systems-of-systems where network topologies have tendency to be variant and most of the time distributed into several groups. In spite of defining the criticality metric as how much a system depends directly on each system, it does not consider the topology’s arrangement into separated groups in addition to the process continuity and dependencies between groups. In fact, it only considers the system-of-systems as a unit.

Consequently, it does not measure the system as it really is because when the global system is distributed into groups, we should consider dependencies between systems and groups before starting any calculation.

Correspondingly, we see that the criticality metric can be used in order to evaluate some cases. However, it is far from being efficient because it alters the real systems architecting model by removing borders, simplifying the architecture without considering many properties that could possibly change the resilience-related expectations based on the criticality metric in real cases.

Contrariwise, our proposed metric takes into account all variables taking part of the system’s forming, and it is conceived to be able to quantify systems-of-systems resilience in a more efficient and realistic manner.

Figure 6 illustrates the contrast between criticality and failure impact metrics. It depicts that a highly critical system does not necessarily have a high failure impact on the system-of-systems and global process continuity. However, the variation of both metrics’ values are related.

4 Second case study presentation and cross-comparison of failure impact values

In this section, we discuss the final step towards evaluating our metric. We apply our metric on a second example resulting from adding a dependency between two groups in the first case study, in order to observe how the metric’s values will change in these new conditions.

We add dependencies between first and third groups. We also separate equally the economic activities between the three groups. Then we evaluate the variation of the ‘failure impact’ rates of all systems.

As a result of failure impact calculations, illustrated in Figure 8, the architecture of the second case study decreases considerably the criticality value of the second group compared to the first one’s architecture. Accordingly, failure impact values of systems of the second group also cutback. Consequently, the most impactful system is no longer the system ‘G’: it is the system ‘A’.
5 The prevalent correlation between emergence controllability and the resilience of systems-of-systems

In the context of systems-of-systems, the emergence’s concept has always been related to unpredictable and unexpected behaviours of systems (Gharajedaghi, 2006). There are numerous proposed definitions to sire this concept.

In Ryan (2006), emergent behaviour is defined as what cannot be expected through analysis. In Kuras (2007), emergent behaviours refer to the properties arising from cumulative interactions between systems inside the system-of-systems.

Besides, what is in common between all the definitions is that emergence occurs when we try to give up control and let the system govern itself as much as possible (Johnson, 2001).
In order to make this self-governance reliable, the emergences must be noticed and controlled, even if the emergent phenomena or even the possibility of emergent phenomena cannot be identified by simulations (Abbott, 2007) and can only be explained after it is recognised, studied and analysed (Ludeman and Erlandson, 2004).

The emergence controllability, for organisations managing systems-of-systems and seeking a reliable performance of the latter, can be effectuated following the two steps below. These steps are inspired by Jamshidi (2008).

The first step is to anticipate the maximum of problems that could face the organisation while managing the system-of-systems. The second step is to conceive a strategy adapted to the context and to the anticipated emergent behaviours, in order to become more successful or at least remain viable.

The emergence controllability has a complementary role to the proposed metric. They both collaborate to estimate the impact of the anticipated problems on the performance of the system-of-systems. This helps the organisation adopting the system-of-systems develop pertinent strategies for recovery or to keep the performance of the system-of-systems intact.

6 Conclusions

In this paper, we presented an approach dedicated to reliability analysis and resilience quantification of systems-of-systems’ architectures through structural analysis. It starts with functional dependencies analysis. Next, it estimates the dependency of the process continuity on every system, thanks to the criticality of each system. Then, it estimates the failure impact of each system in order to evaluate the structural resilience of the whole system-of-systems.

The failure impact metric contributes in the anticipation of the resilience measurement by locating, in the architecting phase, the impactful systems and predicting their impacts on the system-of-systems. This location can be followed by the reorganisation of the architecture of the system-of-systems in order to demean the impact of systems on the process continuity and the overall performance of the global system-of-systems.

The motivation of such a metric is to measure each system’s failure impact on the rest of the system-of-systems and the overall working process. This leads to the estimation of the system’s survivability after each system’s failure.

Besides, it helps the organisation of the architecture by locating systems with high failure impact in order to reorganise the infrastructure so that the system-of-systems overcomes their failures and maintain the continuity of the performance.

Furthermore, it has potential to be extended to a proactive methodology for failure impact calculation and impactful system’s location as the architecture of studied system-of-systems changes by dynamic integration of new systems and removal of existing ones. As it is common for systems-of-systems to be heterogeneous and to support the integration and the removal of systems in parallel with keeping the same performance.

Our work in progress is to address regions’ competitiveness logistics through this perspective.
Acknowledgements

This research is supported by the European Union (EU) with the European Regional Development Fund (ERDF) and Normandy Region.

References


A deterministic approach for systems-of-systems resilience quantification

