Formalization and Evaluation of Non-functional Requirements: Application to Resilience

Behrang Moradi, Nicolas Daclin, Vincent Chapurlat

Formalization and Evaluation of Non-functional Requirements: Application to Resilience

Behrang Moradi, Nicolas Daclin, Vincent Chapurlat

LGI2P, IMT Mines Ales,7, rue Jules Renard 30100 ALES, France
{Behrang.Moradi, Nicolas.Daclin, Vincent.Chapurlat}@mines-ales.fr

Abstract. This paper introduces the development of a method for the specification, formalization and evaluation of resilience. The developed method is based on two working approaches. First, we study and analyze several resilience metrics and indicators as well as the relationship between resilience and other non-functional requirements namely "*-ilities*". Concepts for evaluation are identified and defined. Further, we map out these "*-ilities"* by positioning them according to the dynamic of the resilience represented as a set of zones. A set of indicators to evaluate the resilience and particularly indicators that are associated with these "*-ilities"* to each zone of the resilience has to be selected. The expected benefit of such method is to allow to evaluate resilience in order to master and improve it.

Keywords: System of systems engineering, Resilience, Non-functional property, "*-ilities"*.

1 Introduction

To fulfil its mission adequately, a collaborative system must satisfy functional and non-functional requirements. Among the non-functional requirements a set is called "*-ilities*" [1] and represents "*the desired properties of systems, […] that often manifest themselves after a system has been put to its initial use"* [2]. For instance, let's mention the *Flexibility*, *Robustness*, *Safety*, *Interoperability or Survivability*. Figure 1 presents the network of "*-ilities"* correlations and their relationships as defined in [2]. The work proposed attempts to study and analyze "*-ilities"* as a whole rather than to study an "*-ility*" in isolation and focuses on the resilience assessment. Resilience is an important property because it must be mastered and maximized [3] to effectively cope with disruptive events and maintain acceptable levels of services and performance (*e.g.* loss of an organization in a collaborative network, fire requiring the engagement and collaboration of different organization…). There exist several definitions of resilience. Generally speaking, it is defined as "*the ability of the system to resist, absorb, recover or adapt to disturbances and diminish the consequences as well as to recover quickly and effectively*" [4]. Lastly, resilience is practiced in various application area *e.g.*, critical infrastructure monitoring, security, transport [5], [6], [7].

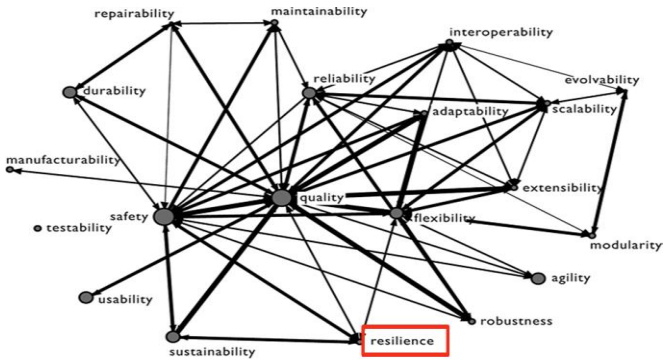

Fig. 1. Correlation network of "*-ilities"* [2]

The research question deals with the evaluation of the resilience. The prevention, preparation and management of negative perturbations for the security and protection of systems have become a major concern. Indeed, a disturbance may lead to heavy loss of performance and affect a system, so that the evaluation resilience can participate to the improvement of a performance of a system. The purpose is to study the resilience with the consideration of its ecosystem that means including the possible relationships with other non-functional requirements. Currently, resilience is evaluated without considering possible impacts coming from other requirements but also possible impacts generated by resilience as well. As a consequence, the targeted objective is to develop a metric to evaluate resilience numerically and sufficiently generic to be practicable to any networked system subject to any type of disruption. The paper is structured as follows. After this brief introduction, the concept of resilience is presented as well as different methods to evaluate it. The next section presents the concepts which act as foundation for the development of our approach to analyze and evaluate resilience. The final section presents the conclusion and the future perspective for this research.

2 Resilience Definition and Evaluation

2.1 Definition

There are numerous definitions of resilience. Let's mention the following ones:

- "*the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions*" [8]*;*
- "*the ability to anticipate, prepare for, respond to, adapt to disruptions and to mitigate the consequences as well as to recover in timely and efficient manner including preservation restoration of services*" [9];

They all suggest that resilient systems are able to manage disastrous situation due to several capacities requested throughout the classical phases of the disaster management lifecycle: **Anticipation** (***Preparation***, ***Prevention***), **Response** (***Absorption***, ***Adaptation***) and **Recovery** (Figure 2).

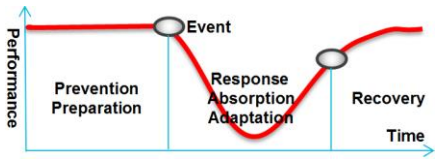

Fig. 2. The classical resilience dynamic

Anticipation (***Prevention*** and ***Preparedness***) aims at identifying and minimizing the risks of the occurrence of an event. This zone concerns also the preparation to face up an event [10]. ***Response*** (***Absorption*** and ***Adaptation***) expresses the absorptive capability (**robustness**), *i.e.,* the ability to reduce the negative impacts caused by disruptive events and minimize consequences with less efforts [3], [4]. The adaptive capability (**adaptability**) refers to the ability to adapt to disruptive events through self-organization (**flexibility**, **interoperability**) to minimize consequences and it can be enhanced by using emergency systems. ***Recovery*** is defined as a return to a qualified acceptable condition. The restorative capability refers to the ability of the system to rapidly be repaired (**maintainability, repairability**) and return to a, as much as possible, normal and a reliable functioning mode that meets the requirements for an acceptable and desirable level of quality of service and expected control [3]. The study and synthesis of different definitions shows that the authors believe resilience is characterized by zones such as Anticipation, Recovery and Response; each author considers more or less zones in their study (*e.g.* for [19] resilience is a problem of response and recovery) (Figure 3). As part of resilience assessment, we consider the three areas of dynamic of resilience, as defined by [20].

Anticipation	Response	Recovery	Reference
✓	✓	✓	*[20]*
✗	✓	✓	*[19]*
✗	✓	✓	*[11]*
✗	✓	✓	*[5]*
✗	✓	✓	*[21]*
✗	✗	✓	*[15]*

Fig. 3. Resilience dynamic

2.2 Resilience Metric

Resilience can be assessed in different ways. It can be evaluated by measuring the performance or loss of performance of a system before and after the disruptive event, the potential loss of functionality, the loss of quality of service, the effectiveness of the security barriers, as well as the activities recovery. Numerous works related to the

evaluation of the resilience are provided in the literature *e.g.* [13] [15] [5] and [16] that evaluates resilience with different points of view. [13] proposes a metric of resilience that can be associated in two types such as the *focus* attribute parameters, which usually consist of indices based on subjective assessments and the *indicators* built on databases, which quantify the system attributes that contribute to resilience. The performance-based methods, which measure the consequences of system disturbances and the impact that system attributes have on mitigating these consequences. [5] states the measurement of resilience is a function of the 3 capacities (absorption, adaptation and recovery) as well as recovery time, through the measurement of the performance and its evolution. The method is based on a resilience analysis framework and a metric for measuring resilience. The analysis framework consists of system identification, resilience objective setting, vulnerability analysis, and stakeholder engagement. Lastly, [16] provides a quantitative measure of resilience in the face of multiple disaster-related events. It extends the concepts of the resilience triangle and predictive resilience in disaster by considering the trade-offs between several criteria. Its work is based on sudden disasters and the initial impact of each event as well as the recovery time of the system before the next event. In this work (Figure 4), robustness is used to increase the resilience so that it recovers its performance and returns to an acceptable state. Thus, there is a link between resilience and robustness.

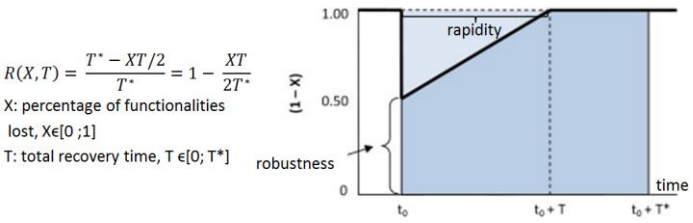

Fig. 4. The predicted resilience triangle as a proportion of T* [16]

These works show three approaches to assess resilience (Figure 5). Let's note that [16] highlights the link between resilience and another "-*ility*" (robustness in the Zone2-response). Its measurement shows the importance of considering the link between "-ilities" since the more the robustness, the more the resilience can be efficient. However, each metric treats the resilience in isolation, *i.e.*, they do not consider the possible relationship with other "-*ilities*". In this sense, stakeholders don't have any information about the possible impact of the resilience onto other "-*ilities*" and *vice versa*. Thus, the ecosystem of "-*ilities"* and their relationship can be used and study to evaluate a given "-*ility*", here, the resilience.

Reference	Ecosystem of '-ilities'	Method/ approach	Zone
[5]		Resilience factor	Response, Recovery
[15]		Potential losses	Recovery
[16]	(Robustness)	Loss of features	Response, Recovery

Fig. 5. Synthesis of different resilience assessment methods

3 Research Work Proposal

The assessment of resilience relies on defining and analyzing the set of "*-ilities", i.e.,* the analysis and formalization of the relationship between resilience and other "*-ilities"* (Figure 6). In this hypothesis, we focus on the analysis of the resilience and its environment and highlight the various components to consider to evaluate resilience. The four components considered are (in red and numbered on Figure 6):

1. The influence. It identifies which "*-ilities"* influence resilience. Some influences are currently identified. However, as claimed in [2], some might exist but are not yet identified. In order to assess resilience based on all elements, it is necessary to identify any dependence between resilience and other "*-ilities*".

2. The orientation. It means to define if the influence is unidirectional (ex. quality → resilience) or bidirectional (ex. quality ↔ resilience). This orientation must be considered "from" resilience "to" another "*-ilities"* as well as "from" another "*-ilities"* to resilience.

3. Dependence. It defines the intensity of the variation between two *"-ilities"*. For instance a high variation (positive or negative) of an "*-ility*" leading to a high variation (positive or negative) of the impacted "*-ility*" expresses a high dependence.

4. The propagation. The chain represents a relation "starting from" the resilience and returning to the resilience via another "*-ilities"* (resilience → safety → sustainability). In this work we consider and limit a chain to a path with 3 "*-ilities"*.

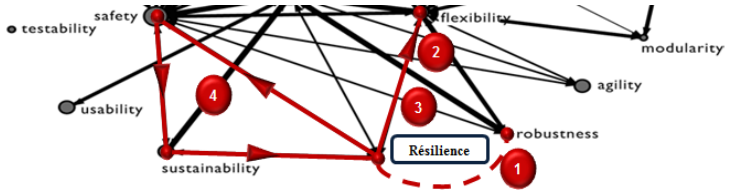

Fig. 6. Partial correlation network of "*-ilities"* including components for evaluation.

In this hypothesis, we present the "*-ilities"* that have links with the resilience and thus we analyze their relations based on the four components (influence, orientation, dependence, and propagation). Figure 7 shows the set of "*-ilities"* in relation with the resilience. Some links stem from [2], and some are added following the study of the "*-ilities"* and their possible relationships. For instance, interoperability is linked with resilience, since it enables a collaborative system to collaborate coherently to achieve the desired operational effect, so the relationship with resilience – *e.g.* to mitigate crisis situation - is needed and important. Adaptability is an "*-ility*" expected in the dynamic of resilience (response zone – ability to adapt), so it has a direct link to resilience, which helps to minimize a negative impact. Then a given link must be characterized by the four components defining a relation. For instance, the sustainability influences (component 1 – influence) the resilience that means a variation of sustainability leads a variation of the resilience. Then, the direction (component 2 - orientation) of this influence is directed from sustainability to resilience, because sustainability allows the system to withstand shocks (Zone 2 –

response). The force (component 3 – dependence) is defined such as the high increase of sustainability leads to a high increase of the resilience. Lastly, the propagation (component 4 – propagation) represents the chain - limited to three path - starting from the sustainability *via* the resilience. In this example the chain is characterized by the path sustainability – resilience – safety (with a last feedback to sustainability). Figure 8 summarizes the relation between resilience and sustainability in agreements with the four items of the first hypothesis. In this end, each relationship between resilience and other "*-ilities"* (which impact resilience) have to be identified and formalized. In the same way, the components, such as dependence and propagation, must formally established to allow the evaluation of the resilience (*e.g.* quantification or qualification of dependence and definition of effect in the propagation chain).

Fig. 7. Network of correlation of "*-ilities"* and resilience

Based on these first components presented, we will define resilience indicator that will measure and manage the capacity of a collaborative system to recover from an event. The indicator considers the capacity to cope with the consequences of disturbances. In addition, the indicator explains the impact of anticipation, response and recovery activities that could be taken after the disruption to reach the acceptable level of service (performance).

Influence	Orientation	Dependence	Propagation
Resilience-Sustainability	S → R	Strong	

Fig. 8. Characterization of the relation between resilience and sustainability

Moreover, the resilience dynamic must be considered. Indeed, the aim is to know the level of resilience for each zone to implement adapted solution to improve resilience. To this purpose, "*-ilities"* and their influences are mapped in each zone (*e.g.* flexibility can be expected during the prevention, Figure.9). This positioning is relative to the analysis of resilience and "*-ilities"* that have identified links in each area. The objective is to get a resilience indicator for each zone. In the end, the aggregation of each indicator will provide an evaluation of the resilience. Thus, each "*-ilities"* related to resilience is analyzed to be re-located precisely on the corresponding phase of resilience. This analysis is mainly related to the study of the intrinsic characteristics and their understanding of a given "*-ility*" with regards to characteristics expected during a given phase of the resilience. It is to note that a given "*-ility*" can cover several phases of resilience life-cycle. For instance,

robustness is interpreted as a measure of performance change. It is positioned in anticipation zone, because the effect of robustness allows the system to increase the readiness to deal with disruptive events. It is also positioned in the response zone, which makes it possible to absorb the negative effects of a disturbing event and increase the level of resilience of the system. Adaptability is the ability of a system to change to perform its basic work in uncertain or changing environments. Thus, adaptability is positioned in the response zone (figure 9), by minimizing the negative impact by protection against shocks. As last example, flexibility can be defined as the ability of a system to comply with its core mission that is not included in the definition of system requirements in disrupted or changing environments. This can be conceptualized as minimizing the consequences with less effort [18]. Thus, the flexibility is positioned on response and recovery zones. Figure 9 shows the mapping of the "*-ilities"* with the different resilience zones (*e.g.* flexibility is positioned in zone 2, zone 3 and robustness in zone 1, zone 2, zone 3). Mapping makes possible to establish the resilience indicators associated with these "*-ilities"* and for each zone. These indicators ultimately enable the level of resilience to be accurately identified and assessed, so aggregation of all these indicators will provide an assessment of the overall resilience.

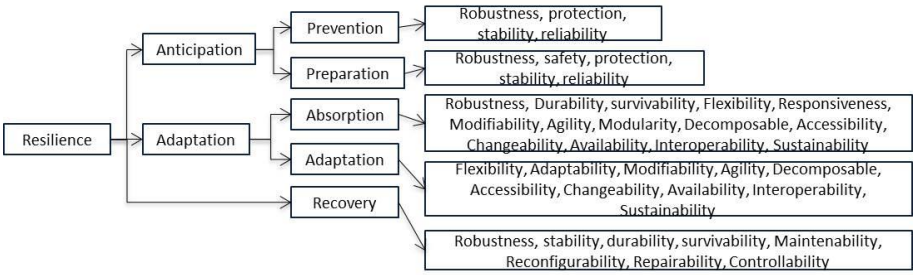

Fig. 9. Resilience Dynamic and "*-ilities"* mapping

4 Conclusion

The here presented work aims, in the end, to evaluate the resilience relying on the dynamic of the resilience and on its study as an "*-ilities"* belonging to an ecosystem of "*-ilities"*. The purpose is to support a collective of actors - for instance involved in a collaborative network - to manage their resilience based on the knowledge of its level and to improve it. First, several resilience metrics are studied and analyzed as well as the relationship between resilience and other "*-ilities"*. Then, the components that defines the relationship between "*-ilities"* are defined and "*-ilities*" linked to the resilience are mapped by positioning them according to its dynamic. Future work is related to the formalization of the components of relationship to get metric and to evaluate the resilience.

References

1. ISO/TC 184/SC 5. *Advanced automation technologies and their applications — Part 1 : Framework for enterprise interoperability*. (2011).
2. De Weck, O. L., Ross, A. M. & Rhodes, D. H. Investigating Relationships and Semantic Sets amongst System Lifecycle Properties (Ilities). *Third Int. Eng. Syst. Symp. CESUN 2012, Delft Univ. Technol. 18-20 June 2012*.
3. Chin, K. S., Yau, P. E. E. E., Wah, S. I. M. K. & Khiang, P. C. FRAMEWORK FOR MANAGING SYSTEM-OF-SYSTEMS ILITIES. 56–65 (2013).
4. Haimes, Y. Y. On the Definition of Resilience in Systems. *Risk Anal.*(2009).
5. Francis, R. & Bekera, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering* (2014).
6. Berkeley Iii, A. R. & Wallace, M. National Infrastructure Advisory Council A Framework for Establishing Critical Infrastructure Resilience Goals Final Report and Recommendations by the Council. (2010).
7. Andrews, Z., Bryans, J., Payne, R. & Kristensen, K. Fault Modelling in System-of-Systems Contracts, (2014).
8. Hollnagel, E. Resilience engineering in practice: A guidebook. (2013).
9. Cutter, S. L. *et al.* Disaster Resilience: A National Imperative. 25–29 (2013).
10. UNESCO. Disaster Planning: prevention, response, recovery. (2017).
11. Nan, C. & Sansavini, G. A quantitative method for assessing resilience of interdependent infrastructures. *Reliab. Eng. Syst. Saf.* (2017).
12. Francis, R. & Bekera, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. **121,** 90–103 (2014).
13. Henry, D. & Emmanuel Ramirez-Marquez, J. Generic metrics and quantitative approaches for system resilience as a function of time. *Reliab. Eng. Syst. Saf.* **99,** 114–122 (2012).
14. Zobel, C. W. Representing perceived tradeoffs in defining disaster resilience. *Decis. Support Syst.* **50,** 394–403 (2011).
15. Henry, D. & Emmanuel Ramirez-Marquez, J. Generic metrics and quantitative approaches for system resilience as a function of time. (2012).
16. Zobel, C. W. Comparative Visualization of Predicted Disaster Resilience. *Seventh Int. ISCRAM Conf.* 1–6 (2010).
17. Fricke, E. & Schulz, A. P. Design for changeability (DfC): Principles to enable changes in systems throughout their entire lifecycle. *Syst. Eng.*(2005).
18. Bordoloi, S. K., Cooper, W. W. & Matsuo, H. Flexibility, adaptability, and efficiency in manufacturing systems. *Prod. Oper. Manag.* (1999).
19. Nogal, M., O'Connor, A., Caulfield, B. & Martinez-Pastor, B. Resilience of traffic networks: From perturbation to recovery via a dynamic restricted equilibrium model. *Reliab. Eng. Syst. Saf.* **156,** 84–96 (2016).
20. Cox, A., Prager, F. & Rose, A. Transportation security and the role of resilience: A foundation for operational metrics. *Transp. Policy* (2011).
21. Filippone, E., Gargiulo, F., Errico, A., Di, V. & Pascarella, D. Resilience management problem in ATM systems as a shortest path problem. (2016).