LATVIAN JOURNAL OF PHYSICS
AND TECHNICAL SCIENCES
2026, N 4

DOI: 10.2478/lpts-2026-0032

CHALLENGES IN RESILIENCE MODELLING TO SUPPORT SUPPLY CONTINUITY AND RESILIENCE MANAGEMENT DECISION-MAKING

R. Remenyte-Prescott[1], J. Andrews[1], A. Tubis[2],
S. Werbinska – Wojciechowska[2], T. Nowakowski[2],
L. Zemite[3], R. Djakons[3], E. Sousa De Cursi[4], M. Eid[4]

[1]Nottingham University,
Resilience Engineering Research Group, University Park
Nottingham NG7 2RD, UK
[2]Wroclaw University of Science and Technology,
Faculty of Mechanical Engineering,
Department of Technical Systems Maintenance and Operation,
27 Wybrzeże Stanisława Wyspiańskiego, 50-370 Wrocław, POLAND
[3]Riga Nordic University,
1–5 Valērijas Seiles Str., Riga, LV-1019, LATVIA
[4]Accueil INSA ROUEN NORMANDIE,
685 avenue de l'Université
76800 Saint-Étienne-du-Rouvray, FRANCE
*e-mail: mohamed.eid@risklyse.eu

The paper provides an overview of the challenges encountered in resilience mathematical modelling within the context of critical infrastructure (CI) protection, supply continuity, and resilience management decision-making. The paper is intended to contribute to the development of the resilience concept, its fundamental building blocks, and its relevant metrics, specifically suitable for risk engineering and sciences. It underlines the varieties of the concepts of resilience used in some scientific disciplines, such as materials science, ecological sciences, and psychological sciences. The use of the resilience concept is still very varied, especially in supporting the services supply continuity in disaster management contexts. An advanced resilience concept should encompass temporality, stochasticity and measurability. Its constituent should cover normalised specifications of disruptive events, critical infrastructure, hazards, vulnerability, robustness, dependencies, interdependencies,

and recovery mechanisms. Formal models cannot be conceived without such normalised specifications, since formal models are necessary to design smart tools to support rational and effective decision-making in disaster management and critical infrastructure protection.

***Keywords**: Decision-making, disruption, infrastructure, modelling, resilience.*

1. INTRODUCTION

The concept of resilience is increasingly emerging in critical infrastructure (CI) protection and disaster management. However, the present paradigms of resilience still need to be completed and well-settled [1]. Especially, some uses of the term are impertinent, misleading and/or mislead. The concept itself is not a recent one. Many scientific disciplines make frequent use of it. However, the concept of resilience is still fuzzy and loose, especially in risk engineering sciences. Engineers and risk analysts find great difficulties to come up not only with a universal view of resilience but also even with a sectorial view limited to circumstantial engineering applications, needs and/or operational environment.

Developing the concept or concepts of resilience requires the establishment of an R&D framework that can continuously be reviewed and improved. This R&D frame cannot but be conceived on a multidisciplinary basis, as the concept of resilience gained a growing interest because of the growing complexity of the studied systems. The modern systems are more and more smart, distributed, active, proactive, independent, and interdependent. Noting that the most complex systems created by nature are the living beings and their ecosystems, one may conclude that complexity and resilience are related in some way or another.

An exhaustive treatment of the subject of resilience and complexity is beyond the scope of this paper. However, the dialectic resilience-complexity should be present in mind while examining the resilience concepts exploited in psychological sciences and ecological sciences.

This preceding point explains the necessity that classical risk management should integrate in the concept of resilience, as modern systems are increasingly complex. Section 2 presents a brief overview of the proven use of the concept “resilience” in other scientific disciplines to identify any potential generic parcel of knowledge that could help in building up a resilience concept appropriate for risk-engineering disciplines. In Section 3, the features of the resilience concept, models and the corresponding metrics are presented, in a wide generic sense.

In Section 4, the paper focuses on the notions of dependency/interdependency (D/I) and vulnerability. The paper tentatively proposes mathematical models for D/I, vulnerability, and building scenarios composed of n-sequential events. The models for the dependency/ interdependency and vulnerability are purposely illustrative to signal the wide range of possibilities

to envisaged, tested and qualified before applications.

Section 5 treats the metrics concerns and tentatively proposes some to initiate critical thinking about this important theme in resilience engineering. Finally, in Section 6, we conclude by underlining the most marking features and aspects of the challenging concerns, in view of modelling the resilience of the critical infrastructure and vital services supply challenges to support disaster effective management.

2. AN OVERVIEW OF THE RESILIENCE CONCEPT

Historically, the first use of the term "resilience" was in mechanics and material sciences. In mechanics and material sciences, resilience is very well-defined and well-measured. Notably, resilience is defined as "the ability of a material to absorb and release energy within the elastic range" [2]. Two metrics are used to measure resilience, in that sense. The proof resilience is defined as "the maximum elastic energy absorbed by a given body, measured in Joule (J), before it attends its elasticity limit". Secondly, the resilience modulus is defined as "the maximum elastic energy absorbed per unit volume of a given body", [2], [3], measured in Joule per cubic meter (J/m^3), before it attends its elasticity limit.

In material sciences, it is just a matter of restoring the initial state once the stressing state is off. The resilient material should then become "as good as before the stress state". However, there is no concerns about "how long time the stress phase and the recovery phase would take". In material sciences, two different materials are identical from the resilience stand point if their resilience modulus values are identical, even if one can be restored in 10 seconds while the other needs 10 minutes.

This "material resilience" is well defined, the characteristic models exist, and a precisely defined metrics is used. In fact, this is the simplest concept of resilience for the simplest category of systems in sciences. It concerns a piece of matter. In some other fields of science, systems may be more complex.

It is the case in ecological sciences. C. S. Holling [4] has introduced a resilience concept into the ecological sciences in 1973. He writes, "If we are examining a particular device designed by the engineers to perform specific tasks under a rather narrow range of predictable external conditions, we are likely to be more concerned with consistent invariable performance in which slight departures from the performance goal are immediately counteracted. A quantitative view of the behaviour of the system is, therefore, essential. With attention focused upon achieving constancy, the critical events seem to be the amplitude and frequency of oscillations. But if we are dealing with a system profoundly affected by changes external to it, and continually confronted by the unexpected, the constancy of its behaviour becomes less important than the persistence of the relationships. Attention shifts, therefore, to the qualitative and to questions of existence or not." [4]. Holling does clearly focus on the system "being" not on the system "doing/behaviour", in presence of an extreme external aggression (a disaster). Subsequently, qualitative measure receives the highest intention. However, Holling also recognises that if the menace is not

existential then "a quantitative view of the behaviour of the system is, therefore, essential".

Qualitative models can then be built essentially to predict the severity of the existential hazards. Then, one can compare with some referential cataclysmic events such as the extinction of the dinosaurs. Having engineering challenges of today, one may continue arguing differently on Holling's point of view. However, discussing the foundations of this point is out of our scope. We offered this ecological resilience point of view in order to illustrate the multiplicity of the views about resilience. Also, we believe that engineering sciences have much to inspire from ecological and psychological science, as far as the resilience concept is examined.

Regarding the psychological resilience, it switches to societal (community) resilience. It is viewed as a process where communication plays the major role. Researchers distinguish then two kinds of resilience: individual resilience (microscopic) and community resilience (macroscopic). All the basic tools and models used in societal resilience find their roots in the psychological resilience. For example, Hyvärinen J. and Vos M. propose a conceptual framework that can act as a starting point for further investigations on how communication can strengthen community resilience and include citizens in the response network [5]. Their paper contains a very interesting and rich list of references that focus on communication in crises in order to enhance community resilience. However, the concept of societal resilience that they seek to enhance is not defined in the paper. The resilience is then conceived in terms of communication (data flow) between a local microscopic element (the individual) and the macroscopic set of elements (the society). Translating that idea in an engineering figure will match a graph with individual nods and arrows circulating data (information) between the nods.

As the paper is designed within the context of disaster and CI protection management, we will opt for the communication-oriented resilience concept. Therefore, we will rather look in the direction of the psychological resilience. Psychological resilience seeks to understand why some individuals can withstand – or even thrive on – the pressure they experience (traumatic events) in their lives while some others do not [6].

In psychological and behavioural sciences, specialists will rather describe resilience not as a "quality/ability" but as a "process" (exchanging information/data). They may describe resilience as: "as the process of effectively negotiating, adapting to, or managing significant sources of stress or trauma" [7], [8], referred to it as a "dynamic process encompassing positive adaptation within the context of significant adversity". We may also notice from Luthar et al. [8], [9] that this dynamic process has a non-deterministic quality. That means: the dynamic process does not encompass the same adaptive pattern in response to a repetitive action of the same stressing vector on the same individual. The absence of the "deterministic" quality, makes us suppose that it is a "stochastic" process. We would like equally to share G. Windle's view [7] on the use of an "operational definition of resilience". We add then that this operational definition should cover these qualities: distributed operational universe, elasticity, dynamic process, and stochasticity. By elasticity, we refer to the quality of being "as good as before", after exposure to a stressing action. Dynamic

is evidently being time-dependent and evolutive. While "stochastic" refers to the probabilistic inherent characters of the dynamic response of the system under stress.

These are the three qualities that we will be considering when developing resilience models. As for metrics and considering that resilience should be expressed mathematically as a measurable quality, then quantitative measures will receive the highest priority. However, the possibility to develop qualitative relative measures (classes of severity) will always be kept opened. We believe these are the minimum common features for all resilience models describing supply continuity and helping in decision-making in disaster situations.

3. RESILIENCE MODELLING: FEATURES AND CHALLENGES

The previous survey illustrated how developing of resilience concepts is challenging in terms of definition, specification, and measurement in the most advanced and applied scientific disciplines, such as material sciences, ecological sciences, and psychological sciences. These are the disciplines that are mostly advanced in developing and using the concepts of resilience. However, the definitions, the measures and the operational practices are not identical in the three disciplines. Still, we may be able to identify some commonalties and even derive features of an advanced paradigm of resilience. From our stand point, the features to be retained are imbedded in the following definition of the concept: "resilience" describes the process of aggression-disruption-recuperation of a given (complex) system under the action(s) of a disruptive-event (stressing vector).

Visually, the resilience in risk engineering is often represented, as in Fig. 1, as a time-dependent operability function versus time, for a complex system exposed to the action of a disruptive events. If one should compose the story presented schematically in Fig. 1, it would be such as: a complex system was exposed to a disruptive event at t_0. It resisted for within a certain lap of time. Then, the system commences losing gradually its operability. Having joined a critical operability level, the system was decreed "non-operational". The system went through different phases of testing and diagnosis before admission for repair.

Then, the system went through the preparation phase that is characterised by the time interval "Time to Repair". Once after, it went through the second testing, control, and certification phase before being declared operational again. The characteristic time between the two decrees of "non-operational" and "operational" is called "Time to Recover". Then, the system started up to join its nominal operational environment, with a characteristic time interval, "Time to Operate".

In this paper, we identify three major characteristic intervals of time: Time to Fail (TTF), Time to Recover (TTR), and Time to Operate (TTO). We observe equally a secondary characteristic time interval that is the "Time to Repair". Two other major characteristic notions should also be noted in Fig. 1.

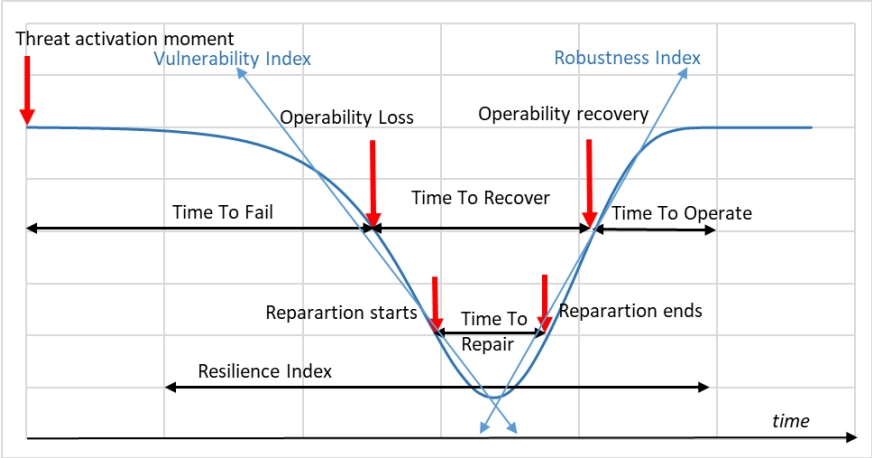

Fig. 1. A schematic representation of the operability vs time of a complex system exposed to the action of a disruptive event.

- The Vulnerability Index: it is represented by the descending slope that describes the operability loss rate (an average value).
- The Robustness Index: it is represented by the ascending slope that describes the operability growth rate (an average value).

The four characteristic time intervals and the two additional notions, all identified above, represent the most challenging aspects in developing resilience models. These aspects should also be completed by carrying on some taxonomy activities in parallel, e.g., see [10]. In the context of this paper, we use the term "process" to cover the two features, temporality and randomness. The following features of the resilience concept are listed below: descriptive process of disruption-recuperation (elasticity), dynamic (temporality), and stochastic (randomness/probabilistic models and metrics).

4. MODELLING D/I AND VULNERABILITY

A disaster is declared once the continuity of supply of a vital service (or many vital services) is potentially or effectively menaced. Each vital service supply is dependent on the operability of a set of well-identified CIs and/or processes. These CIs and processes may to some extend be dependent and interdependent. The dependency/interdependency propagates the loss of operability from one CI to another and may even amplify it through some interdependency-loops.

4.1. D/I

The D/I between CIs may be described in two disjoint ways: either through the operability loss rate or operability loss probability. As for the work reported here,

we are proposing to describe D/I through the operability loss rate, as described in [11]–[13], after some revision. We use a 1st-order approximating model to describe the D/I such as:

$$\hat{\lambda}_i = \lambda_i \left[\prod_{\substack{j=1 \\ j \neq i}}^{N} (1 + \varepsilon_{ij}) \right], \quad (1)$$

where

ε_{ij} – the dependency strain factor, describing the dependency of the i^{th} critical infrastructure on the j^{th} critical infrastructure, facing a given disruptive event;

λ_i – the operability loss rate of the i^{th} critical infrastructure, in the absence of the dependencies, facing the same disruptive events;

$\hat{\lambda}_i$ – the overall operability loss rate of the i^{th} critical infrastructure, considering the interdependencies between different critical infrastructures (N infrastructures), facing the same disruptive events.

Obviously, one may propose more elaborated models. However, we recall that this is not the scope of the present paper. That main focus here is to illustrate the possibility of developing dependency/interdependency models rather than to propose a validated model. The development of validated and proved independency models is obviously an open critical challenge. We admit four classes of D/I models as described by Rinaldi et al. in [14], such as: physical, cyber, geographical and logical.

However, we partially admit Rinaldi et al.'s definition of "interdependency" as: a "bidirectional relationship between two infrastructures". The "bidirectional" interdependency is only one mode that we admit and we classify it as a "1st-order interdependency mode". Then, we identify other modes of higher orders of interdependency. It is the case with the following monodirectional dependencies: an infrastructure A impacts (partially or fully) B, B impacts (partially or fully) C and C impacts (partially or fully) A.

Whatever the class of the dependency, we would like also to consider the temporal dimension. That means that the propagation of the "loss of operability" from CI to the others takes time. Generally, the propagation is not instantaneous. This "propagation time" depends on the "loss of operability" mode and the concerned couples involved in the propagation.

The dependence between a set of CIs can then be described through the dependency strain matrix ε_{ij} that describes the dependence of the i^{th} the j^{th} infrastructure. We note that ε_{ij} is generally not symmetric.

We equally note that ε_{ij} is always positive in order to guarantee the "coherency" of the system-of-systems. The "coherency" condition requires that the "loss of operability" of a CI cannot improve the global operability of the set of the concerned CIs, and the "growth of operability" of a CI cannot degrade the global operability of the set of the concerned CIs. Vulnerability can also be conceived as a dependency relation between a critical infrastructure and a disruptive event so that one may use the same logical structure describing the dependency/interdependency.

4.2. Vulnerability

The CIs vulnerability to disruptive events may be described in two disjoint ways, as mentioned above: either through the operability loss rate or operability loss probability. CIs loss of operability is also dependent on the type of the disruptive events. We can also affirm the CIs are differently vulnerable to different disruptive events.

As far as our work reported here is con-

cerned, we propose to describe vulnerability through the operability loss rate. As it is fully described in [10], [11], the authors use a 1st-order approximating model to describe the D/I as follows:

$$\hat{\lambda}_i = \lambda_i\left[\prod_{j=1}^{L}(1+\nu_{ij})\right], \quad (2)$$

where

ν_{ij} – the vulnerability strain factor of the j^{th} disruptive event on the i^{th} critical infrastructure;

λ_i – the operability loss rate of the i^{th} critical infrastructure, facing the j^{th} disruptive event;

$\hat{\lambda}_i$ – the overall operability loss rate of the i^{th} critical infrastructure, facing multi-disruptive events (L disruptive events).

As vulnerability impacts failure and repair, strain matric ν_{ij} describes the vulnerability i^{th} of the CI to the j^{th} disruptive event. The element ν_{ij} can only be

- positive ($\nu_{ij} \in [0,1]$) if λ_i is a failure rate, or
- negative ($\nu_{ij} \in [-1,0]$) if λ_i is a repair rate.

That is to describe two classes of events. The first class contains the events where occurrence rates increase under stress. This is to say failure rates cannot be worst during the active phase of a disruptive event, i.e., failure rates increase. The second class contains those where occurrence rates decrease under stress. This is to say repair rates cannot be worst during the active phase of a disruptive event, i.e., repair rates decrease. Both situations are functionally identical and guarantee the coherence of the system-of-systems, as explained in the preceding section.

4.3. Scenario Modelling

In the scope of crisis/disaster management activities, experts determine the significant (plausible) scenarios. Significant scenarios result from the combination of the actions of some disruptive events and the (partial or full) loss of operability of a set of impacted CIs and processes. Very often, the occurrence order of the preceding events determines a specific scenario associated to a specific set of hazardous outcomes that may be more or less of different probability distribution and severity.

Accordingly, an effective disaster management process should consider the plausible set of well-identified scenarios of events. The occurrence probability $P_n(t)$ of a given scenario of n-ordered events can then be described by the following model:

$$P_n(t) = \int_{t=0}^{T}\rho_1(\xi_1)d\xi_1\int_{t=\xi_1}^{T}\rho_2(\xi_2)d\xi_2\ldots\int_{t=\xi_{n-2}}^{T}\rho_{n-1}(\xi_{n-1})d\xi_1\int_{t=\xi_{n-1}}^{T}\rho_n(\xi_n)d\xi_n. \quad (3)$$

Equation (3) may equally be rewritten in the following form:

$$\frac{d}{dt}P_n(t) = \rho_{n-1}(t)P_{n-1}(t), \quad (3)$$

where $P_n(t)$ is the probability distribution function of the events in the specified order.

If the ordered events follow a Poisson's stochastic process, an analytical solution exists [15]. It is obvious that each scenario of events leads to a well-defined set of hazardous outcomes. However, the same well-identified set of hazardous outcomes may be the result of different possible scenarios. The mapping of all the sets related to the plausible scenarios and the set of potential outcomes is not bijective.

4.4. Required Data

The proposed approach requires three distinguished types of datasets:

- The CI unstressed (nominal) loss of operability probability distribution function;
- The vulnerability strain factors describing the vulnerability of a given CI to a set of well-defined disruptive events;
- The dependency strain factors describing the directional dependency between the concerned CIs.

The unstressed loss of operability characteristics is, in principle, available for most of the critical infrastructures and their internal components and subsystems. These data are effectively embedded in the daily operational histograms of each CI. It is also the outcome of the reliability assessments relative to these CIs in a nominal operational phase. However, these data have a sectorial nature: energy, gas, transport, and health.

Many embedded disruption data exist in databases such as insurance companies' databases: Energy Losses Database of WTW [16], Marsh's Energy Database [17], and Sigma database of Swiss Re [18]. Sectorial CI disruptions are also embedded in accident databases such as: Worldwide Offshore Accident Databank (WOAD) of DNV, the Energy-Related Severe Accident Database (ENSAD) of PSI, and the OECD Databases for Chemicals and Biosafety [19], [20]. A good collection of data on man-made accidents is referenced by ANL in [21]. However, there are many other private databases used by national industries that map and monitor the operations of the nation's systems of electric grids, ICT networks, processing plants, gas pipelines, etc. Most of this information is proprietary.

Regarding vulnerability of CIs to disruptive events, some databases exist. However, it is not exactly in the suitable form to be directly exploited by the proposed approach. As in the previous paragraph, many data are embedded in some databases, such as EM-DAT of the International Emergency Disasters Database of the Centre for Research on the Epidemiology of Disasters (CRED), NatCat: Natural Catastrophes Service (Munich Re). However, as far as we can assert, there is no a specific vulnerability database. We believe this is mainly due to:

- the loose concept of vulnerability;
- the proliferation of vulnerability models and indices, with no convergence towards a standard set of models or even of conceptual definitions.

One may also add that the vulnerability is a local quality. For example, the vulnerability of two identical buildings to the same quake would be so different if the soil is rocky or sandy. The vulnerability of a structure/procedure/organisation to a given disruptive event integrates all the elements of its ecosystem. This seems to be true whatever the definition of the vulnerability is.

As for the dependency data required for models' development purpose, they are not available in the required form, as well. Several R&D programs are conducted in order to develop dependency databases. In Argonne National Laboratory (ANL), a team is developing data collection tools and

models [21] in order to allow for a more detailed analysis of critical infrastructure dependencies and interdependencies.

In academia, data collection and analyses start to address physical, cyber, and geographic dependencies and initiate the anticipation and visualisation of first-order cascading failures [22]. However, most of the existing tools and models operate in silos and have little interaction with complementary tools and models. Understanding logical dependencies and escalating failures is obviously a complex task.

We may then conclude that only disruption data exist for CIs. Althoug, it is not always explicitly available, it is always embedded in the operational histograms of the CI. Still, the required data should allow working out both the strain dependency matrix and the strain vulnerability matrix .

We admit how challenging the issue of the adequate data and data sources is. Developing data models and collecting data require long-term continuous efforts, generous resources, and adequate standards underlays.

4.5. Resilience Representation

The key feature in the resilience concept compared to that of risk is the ability to tolerate undesirable events. With risk, an effort is focused on preventing undesired events, in resilience while avoidance is still a feature, other processes are considered to control the event's impact.

Waiting for a close-to-real global modelling of resilience, topological representation may be of great use in presenting resilience global dynamic by sector of application.

This is shown in Fig. 2 [23], which characterises the impact of the disruptive event on a public transport system performance. This representation is consistent with that shown in Fig. 1 of the paper which is more schematic. It includes the resilience phases of absorbing, adapting to and recovering from the disruption. Resilience measures can be calculated using the area under this resilience profile.

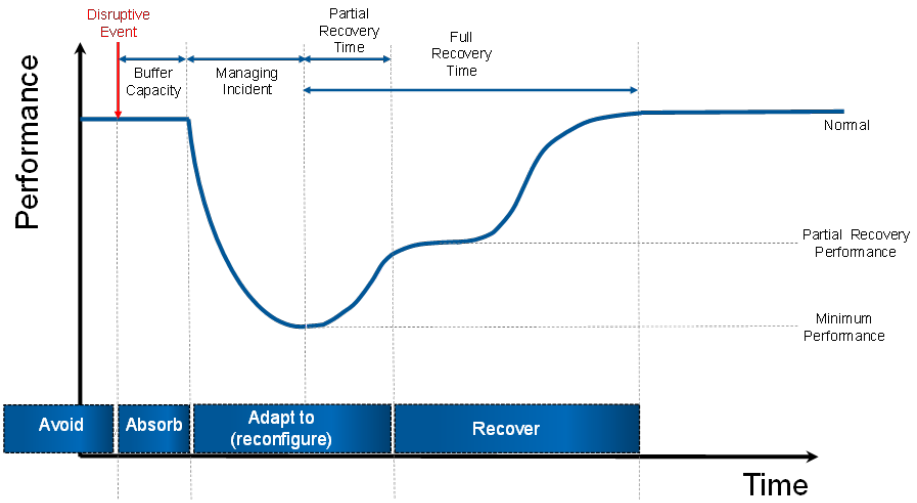

Fig. 2. Representing the resilience profile [23].

The profile is an excellent visual tool for communicating the resilience concept. It also demonstrates why resilience is so difficult to exploit in modelling. Usually, the disruptive event can occur in a number of ways, each way can be defined by parameters that specify its magnitude and dynamics (e.g., a leak will have the amount of material released together with a release rate). Different magnitudes may elicit different activities performed in the resilience phases. Thus, in the case of a leak, whether it is above or below a specified threshold may produce different sets of responses to absorb, adapt to or recover from. Within each action performed for the resilience phases, further parameters will define the effort and speed of the response. All of these variables affect the dynamics of the resulting profile. A full resilience assessment requires the execution of a large number of computationally expensive, detailed models.

For outcomes following the disruptive event where the event is controlled and the system functionality is fully restored, the profile is relevant. If the failure is catastrophic and leads to the destruction of the system, decisions are required regarding how such situations should be included, since the time needed to rebuild the system and restore full performance will dominate and distort the analysis results.

The complexity of the process is clear. Risk modelling is essentially the same as the first phase of the resilience concept – the avoidance phase – and this phase alone is usually challenging. The issues outlined help explain why, to date, there is not an accepted resilience modelling framework that, like risk analysis, has been adopted across the different industrial sectors.

5. CONCLUSION

This paper has intended to share a deep insight in the challenges facing the development of mathematical models for resilience in view of supporting decision-making in CI resilience assessment and disaster management. The insight covers:

- the definition of the concept “resilience” and relevant notions;
- the identification of its features, characteristic parameters, and major indices;
- an illustrative proposal of mathematical models of resilience evaluation and associated metrics
- a note regarding needs to carry on some taxonomy activities in relation to resilience and relevant metrics.

We have observed that the concept of resilience is still not clearly defined in risk engineering compared to other advanced disciplines, such as in ecological science and behavioural psychology. The paper has provided an overview to stimulate innovative thinking and conceptualisation in resilience engineering. Finally, the overview has enabled us to identify some generic features of resilience that seem universal, including descriptive relationship framing aggression-recuperation process, dynamic, and stochastic features.

ACKNOWLEDGEMENT

This work has been the outcome of many seminars organised by ESReDA over the past 15 years and of many other free exchanges within ESReDA's experts and ESReDA stimulating environment. No names to mention as they are so many, with similar expertise but different skills.

REFERENCES

1. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., … & Thiel-Clemen, T. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407–409. https://doi.org/10.1038/nclimate2227
2. Gere, J. M. (2004). Mechanics of materials (6th ed.). Brooks/Cole–Thomson Learning.
3. Goodno, B. J., & Gere, J. M. (2018). Mechanics of materials (9th ed.). Cengage Learning.
4. Holling, C. S. (1973). Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4, 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245
5. Hyvärinen, J., & Vos, M. (2015). Developing a conceptual framework for investigating communication supporting community resilience. Societies, 5(3), 583–597. https://doi.org/10.3390/soc5030583
6. Fletcher, D., & Sarkar, M. (2013). Psychological resilience: A review and critique of definitions, concepts, and theory. European Psychologist, 18(1), 12–23. https://doi.org/10.1027/1016-9040/a000124
7. Windle, G. (2011). What is resilience? A review and concept analysis. Reviews in Clinical Gerontology, 21(2), 152–169. https://doi.org/10.1017/S0959259810000420
8. Luthar, S. S., & Cicchetti, D. (2000). The construct of resilience: Implications for interventions and social policies. Development and Psychopathology, 12(4), 857–885. https://doi.org/10.1017/S0954579400004156
9. Luthar, S. S., Cicchetti, D., & Becker, B. (2000). The construct of resilience: A critical evaluation and guidelines for future work. Child Development, 71(3), 543–562. https://doi.org/10.1111/1467-8624.00164
10. Schoene, D. W. R. (2022, November 10). The difference between hazard, risk and threat. LinkedIn. Available at: https://www.linkedin.com/pulse/difference-between-hazard-risk-threat-david-schoene/
11. Eid, M., Hakkarainen, T., Kling, T., Souza de Cursi, E., & El-Hami, A. (2016). Critical infrastructure preparedness: Cascading of disruptions considering vulnerability and dependency. Journal of Polish Safety and Reliability Association, 7(1), 61–66. Available at: https://bibliotekanauki.pl/articles/2069144.pdf
12. Eid, M., El-Hami, A., & Souza de Cursi, E. (2018). Proposal of a R&D frame to develop resilience models for services supply continuity in view of crisis situations. Journal of Polish Safety and Reliability Association, 9(3), 21–30. Available at: https://bibliotekanauki.pl/articles/2068753
13. Eid, M., El-Hami, A., Souza de Cursi, E., Kołowrocki, K., Kuligowska, E., & Soszyńska-Budny, J. (2015). Critical infrastructures protection (CIP): Coupled modelling for threats and resilience. Journal of Polish Safety and Reliability Association, 6(1), 85–94. Available at: https://bibliotekanauki.pl/articles/2069190
14. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11–25. https://doi.org/10.1109/37.969131

15. Eid, M. (2011). A general analytical solution for the occurrence probability of a sequence of ordered events following Poisson stochastic processes. Reliability: Theory & Applications, 2(21), 21–32. Available at: https://www.gnedenko.net/Journal/2011/022011/RTA_2_2011-02.pdf
16. Willis Towers Watson. (2016). Willis Towers Watson energy loss database [Data set]. https://www.willis.com/Documents/Publications/Industries/Energy/2155_energy%20_loss_database.pdf
17. Marsh. (2023). Energy & power. Available at: https://www.marsh.com/uk/industries/energy-power.html
18. Swiss Re Institute. (2018). Natural catastrophes and man-made disasters in 2017: A year of record-breaking losses (Sigma No. 1/2018). https://www.swissre.com/library/editors-pick/sigma_1_2018_en.html
19. Organisation for Economic Co-operation and Development. (n.d.). Chemical safety and biosafety. Available at: http://www.oecd.org/env/ehs/directoriesanddatabasesforchemicalsandbiosafety.htm
20. Mihailidou, E. K., Antoniadis, K. D., & Assael, M. J. (2012). The 319 major industrial accidents since 1917. International Review of Chemical Engineering, 4(6), 529–540. Available at: https://pdfs.semanticscholar.org/23a3/09d1767f6e0531668ae43dee5a2a10c52ee8.pdf
21. Petit, F., Verner, D., Brannegan, D., Buehring, W. A., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J., & Peerenboom, J. (2015). Analysis of critical infrastructure dependencies and interdependencies (Report No. ANL/GSS-15/4). Argonne National Laboratory. https://doi.org/10.2172/1184636
22. Pietrucha-Urbanik, K., Tchórzewska-Cieślak, B., & Eid, M. (2018). Cascading failure analysis in order to assess the resilience of a water supply system. Journal of Polish Safety and Reliability Association, 9(3). Available at: https://bibliotekanauki.pl/articles/2068731
23. Andrews, A. (2026). Resilience representation & issues. Private Communication.