Foundational Concepts in Simulation-Based Resilience Analysis and Design

Daniel Hulse
Intelligent Systems Division
NASA Ames Research Center
Moffett Field, California, United States
daniel.e.hulse@nasa.gov

***Abstract*—Resilience is a topic of increasing interest–with ever-present calls from policymakers to increase the resilience of complex systems and infrastructure. However, resilience as a concept can be confusing, because of a lack of a common unified definition and frame of reference. Sometimes it can appear as if resilience analysis is merely duplicating other, more mature fields such as safety, reliability, or risk, while other times it seems as if resilience is providing an "alternative" view with limited rigor. To better understand the resilience concept (and its relation to the broader field of risk management), this paper will present the perspective of simulation-based resilience analysis and design, including some of the foundational precepts and resultant concepts defining the resilience concept. It will further present the motivation for using simulation to understand resilience and highlight some ongoing work and research challenges in this area. From this frame of reference, one can better understand the field of resilience, including how different aspects and definitions of resilience relate to each other, and how resilience relates to broader design considerations and practices.**

***Index Terms*—resilience, modelling and simulation, representation**

I. Introduction and Motivation

There have been increasing calls for increasing and improving the resilience of complex engineered systems and infrastructure. These calls have seen resilience as a means of solving a number of policy problems, such as (but not limited to) (1) better handling and adapting to natural disasters (often related to climate change) [1], (2) encouraging a more agile "learn-as-you-go" approach to handling risks when developing new technologies [2], and/or (3) increasing the adaptiveness of autonomous and complex socio-technical systems to better mitigate hazards that will arise in operations [3].

However, there is often confusion about what is meant by resilience. It is often unclear how resilience fits within (or beside) existing long-standing risk management frameworks like safety and reliability engineering (especially since has been sold as a competitor to these paradigms [4]). From a critic's point of view, resilience may be seen as an (less rigorous, less mature) alternative to these fields [5], or a mere reframing of these fields with no unique contributions of its own. This is further complicated by the many seemingly-conflicting resilience frameworks that have been proposed in the field (see literature reviews: [6] [7], [8]). Thus, there is a need to better understand the definition of resilience and its relationship with the broader fields.

To better provide a conceptual framework to understand the resilience concept, this work will outline some of the basic precepts, concepts, and research questions from the perspective of simulation-based resilience analysis and design. Simulation-based resilience analysis and design is a means of understanding and improving the resilience of a system using quantitative simulations of system behavior [9]. To introduce this area, this presentation will first describe some basic precepts and resultant concepts that define resilience from a modelling and simulation perspective. It will then discuss how modelling and simulation can be used to understand and improve resilience, along with some of the ongoing research questions in the field.

II. Understanding Resilience

Simulating systems resilience first requires a basic conceptual framework of what resilience *is*. Below are some foundational precepts of this conceptual framework, as well as some resultant concepts that may be used to understand the field.

A. Foundational Precept: Resilience can be understood quantitatively.

A major assumption required for understanding resilience in simulation is that it is a quantitative characteristic, meaning it can be expressed in mathematical terms (e.g., numbers, expressions, equations, statistics, etc). This is in contrast to the idea that resilience (as a human/organizational property) should primarily be understood with a qualitative, conceptual or "soft systems" approach.

B. Foundational Precept: Resilience is a dynamical systems property related to the system's response to events.

Considering resilience as a quantitative property, it can then be seen as relating to the behavior of a system after an event

This research is supported by the System-Wide Safety project in the Airspace Operations & Safety program in the NASA Aeronautics Research & Mission Directorate. Any opinions or findings of this work are the responsibility of the authors and do not necessarily reflect the views of sponsors or collaborators.

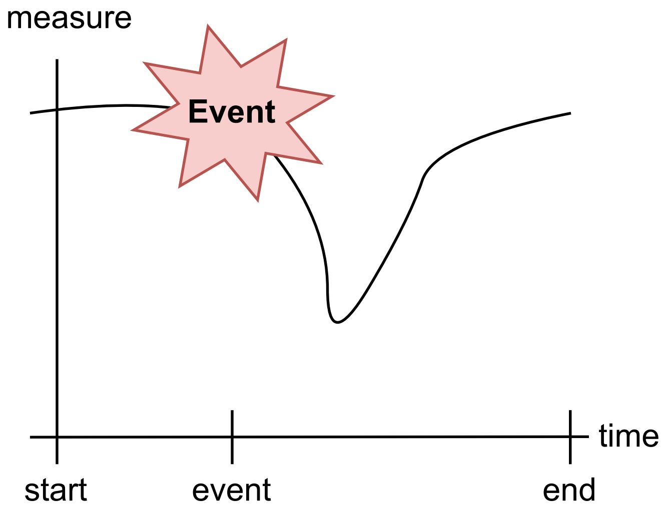

Fig. 1. Resilience Curve Concept

occurs. An event is an occurrence within a particular scenario which may be hazardous, unforeseen, or otherwise important for the purpose of analysis. This behavior may be represented as a curve or function (often called the resilience triangle [10]) of a quantity of interest before, after, and during the event, as shown in Figure 1. This can be called the "resilience curve" and represented using the expression:

$$Re_s = \int_{t_b}^{t_e} r(t, s)dt \quad (1)$$

where s is the scenario including the event, t_b is the beginning of scenario, t_e is the end of the scenario, $r(t, s)$ is the dynamic quantity of interest through the scenario, and Re_s is the resulting resilience metric over the scenario s.

Note that under this definition of resilience, the metric or measure *may be anything of interest*, not a particular performance value (which may be domain-specific). As such, resilience should be understood not as any specific measure (e.g., in the sense that "the resilience of the spacecraft is 7"), but as a framework for considering how measures of interest respond to events (e.g., in the sense that "the system is resilient because the post-event capacity rapidly recovers to its pre-event value in ten minutes").

C. Resultant Concept: Resilience is a means of consideration, of not a competitor to, existing related objectives.

Given the identifying characteristics of resilience being the analysis of event-related dynamical systems properties, it follows that resilience is compatible with existing related fields and considerations. As pointed out by Terje Aven, resilience fits well *within* the framework of risk, as a particular consideration of risk that includes dynamical systems properties [11]. For example, as presented in earlier work [9], *resilience-related losses* (i.e., the value of risk) can be expressed in terms of expected losses using the equation:

$$R = \mathop{\mathbb{E}}_{s \in S} Re_s \quad (2)$$

where R is the risk value, S is the set of uncertain scenarios to consider, and Re_s is a given resilience metric representing a loss (for example, cost or a hazardous outcome occurring). Similarly, resilience can further be considered within existing frameworks of performance and safety as a way of analyzing domain-specific metrics (e.g., speed, capacity, performance, risk of injury) in particular events, rather than devising specialized "resilience metrics" independently.

D. Resultant Concept: Resilience properties can be thought of as inputs and outputs of the resilience curve

Many resilience "definitions" and metrics are compatible with this consideration of resilience and may be categorized as modelling inputs (i.e., assumptions or variables in the equation(s) which output the resilience curve) or outputs (i.e., metrics Re_s). Examples of outputs include recovery time, robustness, while examples of inputs include buffer capacity, intelligence, recovery policy, and situation awareness. The process of improving resilience may further be considered to be changing the various inputs of the resilience curve to improve the resulting output metrics of interest [9].

III. Concepts in the Simulation of Resilience

Given the overall definitions defined in Section II, the use of simulation to assess resilience should be clear. Specifically, the purpose of simulation is to represent the input behaviors to generate the resilience curve and in turn quantify metrics of interest. Using simulation, one may then change different inputs of the simulation to improve the various metrics and thus design a more resilient system.

Given the definition of resilience in Equation (1), the resilience curve may be understood as an ordinary differential equation (or system of equations) representing behavior over time. While simple time-based ordinary differential equations may be solved analytically, this becomes untenable for most real-world systems, where there are complex switching behaviors (i.e., modes), events/scenarios, and interactions between different behaviors and systems, motivating the use of discrete-time (or discrete-event) simulation [12]. Further consideration of resilience requires an approach taylored to the domain under study, along with the analysis questions of interest, as explained below.

A. Resilience may be simulated differently, depending on the goals of analysis.

Since there is not one "resilience" metric or treatment, there is furthermore not a single universal simulation approach for analyzing system resilience. Instead, simulations are adapted to the considerations relevant to the particular analysis concept. For example, an important aspect of simulation set-up is the scenarios under consideration, which may vary depending on the research question [13] in the following ways:

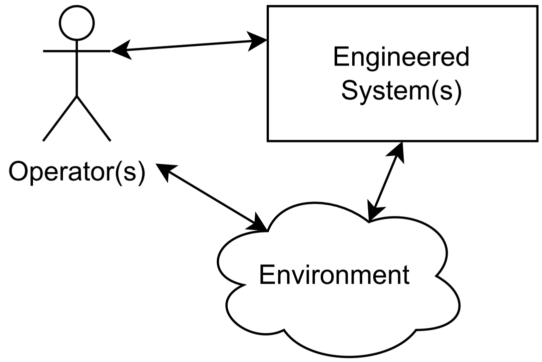

Fig. 2. Prototypical Resilience Simulation Setup

- The number of events to simulate may vary, depending on if the goal is to understand the system's response to a single event, a type of event, the worst-case event, or the set of events envisioned to occur.
- If the goal is to improve resilience, the response of the system will be evaluated over a number of different input parameters (e.g., buffer, capacity, response policy).
- The length and time-scale of the resilience to consider may vary, depending on the scope of consideration. For example, one may be interested in the system response in the immediate aftermath of an event or the long-range repair and reconfiguration of the system

These are all important considerations for developing an overall simulation approach. In particular, the desire to model a large amount of longer-running simulations increases the computational time required for evaluation, which can be important to manage when improving system resilience.

B. The needs of resilience analysis push the boundaries of existing simulation approaches

While modelling and simulation has significant potential to inform the assessment of resilience, the representation of the behavior of interest in a simulation is often a difficult task. Systems where resilience is most relevant and desirable often have a significant amount of behavioral complexity, such as (1) complex human and algorithmic behaviors such as perception, reasoning, and acting (see: [14]) (2) stochastic and potentially unknown environmental behaviors (e.g., events) and (3) non-trivial interactions between behaviors (e.g., component couplings, multi-agent behaviors [15], etc). These are represented in Figure 2, and each present major challenges in terms of representation, because unlike "typical" engineered systems (e.g., springs, engines, etc.) they do not map neatly to an existing, definitive physical laws.

This does not mean simulation is not useful. In fact, simulation brings a number of advantages to the analysis, including conceptual rigor, the ability "test" concepts without taking on real-world risk, and the ability to apply advanced methodologies for identifying hazardous events which could not have been identified otherwise [16]. Often, challenges may be revealed by simulating a system which would not have been envisioned prior to implementation otherwise, because there would otherwise not be a chance to integrate the components and test different behaviors. Nevertheless, how to fully represent the resilience of complex engineered systems remains an active research question with many problems to solve.

IV. Conclusions

This paper outlined a basic conceptual overview of resilience from the perspective of modelling and simulation. Resilience analysis is the consideration of a system's dynamic mitigation of hazardous events, which may support overall design activities like risk reduction, safety assurance, and performance improvement. Modelling and simulation support the assessment of resilience by providing a means of quantifying resilience curves (and their resulting metrics) from input assumptions. While these concepts are relatively straightforward, the implementation of them reveals a number of challenges for modelling and simulation techniques–including how to best represent intelligent systems and their interactions within a complex environment. This is an active area of study that could have transformative impacts on how the community understands the diverse considerations defining the concept of resilience.

References

[1] Committee on Hazard Mitigation and Resilience Applied Research Topics, Policy and Global Affairs, and National Academies of Sciences, Engineering, and Medicine, Resilience for Compounding and Cascading Events. Washington, D.C.: National Academies Press, 2022. Accessed: Apr. 17, 2024. [Online]. Available: https://nap.nationalacademies.org/catalog/26659/resilience-for-compounding-and-cascading-events

[2] E. National Academies of Sciences, Advancing Aerial Mobility: A National Blueprint. 2020. Available: https://nap.nationalacademies.org/catalog/25646/advancing-aerial-mobility-a-national-blueprint

[3] J. Hay, P. Craven, B. Merrel, P. Williams, and G. Wusk, "Resiliency in Future Cislunar Space Architectures," ntrs.nasa.gov, Dec. 2022, Accessed: Apr. 17, 2024. [Online]. Available: https://ntrs.nasa.gov/citations/20220018492

[4] I. Linkov et al., "Changing the resilience paradigm," Nature Climate Change, vol. 4, no. 6, pp. 407–409, Jun. 2014, doi: https://doi.org/10.1038/nclimate2227.

[5] A. Clark-Ginsberg, "What's the Difference between Reliability and Resilience?," in ICSJWG Quarterly Newsletter, Mar. 2015. Available: https://doi.org/10.13140/RG.2.2.20571.46885

[6] L. Shen, B. Cassottana, H. R. Heinimann, and L. C. Tang, "Large-scale systems resilience: A survey and unifying framework," Quality and Reliability Engineering International, vol. 36, no. 4, pp. 1386–1401, Jun. 2020, doi: https://doi.org/10.1002/qre.2634.

[7] N. Yodo and P. Wang, "Engineering Resilience Quantification and System Design Implications: A Literature Survey," Journal of Mechanical Design, vol. 138, no. 11, Sep. 2016, doi: https://doi.org/10.1115/1.4034223.

[8] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," Reliability Engineering & System Safety, vol. 145, pp. 47–61, Jan. 2016, doi: https://doi.org/10.1016/j.ress.2015.08.006.

[9] D. E. Hulse, "A Computational Framework for Resilience-Informed Design," Ph.D Disseration, Oregon State University.

[10] M. Bruneau et al., "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," Earthquake Spectra, vol. 19, no. 4, pp. 733–752, Nov. 2003, doi: https://doi.org/10.1193/1.1623497.

[11] T. Aven, "On Some Foundational Issues Concerning the Relationship Between Risk and Resilience," Risk Analysis, Oct. 2021, doi: https://doi.org/10.1111/risa.13848.

[12] H. Sayama, "Introduction to the Modeling and Analysis of Complex Systems," Open Textbook Library, 2015. https://open.umn.edu/opentextbooks/textbooks/233

[13] "Intro to resilience modeling, simulation, and visualization in Python with fmdtools. — fmdtools 2.0-rc-2 documentation," nasa.github.io. https://nasa.github.io/fmdtools/docs/Intro_to_fmdtools.html (accessed Apr. 17, 2024).

[14] L. Irshad and D. Hulse, "Can Resilience Assessments Inform Early Design Human Factors Decision-making?," IFAC-PapersOnLine, vol. 55, no. 29, pp. 61–66, 2022, doi: https://doi.org/10.1016/j.ifacol.2022.10.232.

[15] L. Irshad and D. Hulse, "Modeling Distributed Situation Awareness in Resilience-Based Design of Complex Engineered Systems ," in Proceedings of the ASME 2023 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. , ASME, 2024, p. V002T02A050. Accessed: Apr. 17, 2024. [Online]. Available: https://doi.org/10.1115/DETC2023-116689

[16] D. Hulse and L. Irshad, "Synthetic Fault Mode Generation for Resilience Analysis and Failure Mechanism Discovery," Journal of mechanical design, vol. 145, no. 3, Dec. 2022, doi: https://doi.org/10.1115/1.4056320.