Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Resilience by Design Fault Model Design Tools

Resilience-By-Design with fmdtools

Resilience, the ability of a system to dynamically mitigate hazardous events as they arise, is an important consideration for a wide range of complex engineered systems across domains. While engineering resilience has traditionally been seen as property of infrastructure (e.g., [1]), the resilience perspective is increasingly having relevance to a wide range of technologies. In aviation, for example, resilience is considered an aspect of human pilots to proactively prevent and perform contingency management actions to recover from hazardous flight events [2], which is becoming increasingly important to replicate in the implementation of autonomous and partially autonomous flight systems [3]. Cases like this especially increase the importance of incorporating resilience in the design of the system prior to implementation, so that new technologies will fulfill the public's high expectations of safety and dependability and not pose undue risks on society.

The fmdtools (Fault Model Design Tools) library[1] was developed to enable the consideration of resilience in the design process [4]. To enable this, it provides modelling constructs to represent a system's structure and (both nominal and hazardous) behavior, methods to simulate the dynamic effects of hazardous scenarios over time, and visual and statistical methods to analyze and thus improve resilience. As a python-based library, fmdtools is widely adaptable across domains to a wide range of use-cases including power systems, drones, and autonomous rovers, as well as system-of-systems and infrastructure use-cases like aerial firefighting [5] and airport taxiways [6].

The development of fmdtools features and capabilities for resilience analysis have been well-documented in the literature, including:

- Representation of human-oriented, automation-oriented, and general systems of systems resilience properties, including task execution [7], performance degradation [8], and distributed situation awareness [6].
- Support for trade assessment and optimization via model parameterization [9]
- Ability to construct and sample large spaces of hazardous scenarios [10]

In the future, it is the goal of the fmdtools developers to make these capabilities more accessible to a wider range of users, through the development of an integrated graphical user interface.

Bibliography

[1] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace and D. Von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra,* pp. 733-752, 2003.

[1] Available at: https://github.com/nasa/fmdtools

[2] J. B. Holbrook, M. J. Stewart, B. E. Smith, L. J. Pinzel, B. L. Matthews, I. Avrekh, C. T. Cardoza, O. C. Ammann, V. Adduru and C. H. Null, "Human performance contributions to safety in commercial aviation," NASA, Hampton, Virginia, 2019.

[3] National Academies of Sciences, Engineering, and Medicine, "Advancing Aerial Mobility: A National Blueprint," The National Academies Press, Washington, DC, 2020.

[4] D. Hulse, H. Walsh, A. Dong, C. Hoyle, I. Tumer, C. Kulkarni and K. Goebel, "fmdtools: A fault propagation toolkit for resilience assessment in early design," *International Journal of Prognostics and Health Management,* 2021.

[5] S. R. Adrade and D. E. Hulse, "Evaluation and Improvement of System-of-Systems Resilience in a Simulation of Wildfire Emergency Response," *IEEE Systems,* vol. 17, no. 2, pp. 1877 - 1888, 2022.

[6] L. Irshad and D. Hulse, "Modeling Distributed Situation Awareness in Resilience-Based Design of Complex Engineered Systems," *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference,* vol. 87295, p. V002T02A050, August 2023.

[7] L. Irshad, D. Hulse, H. O. Demirel, I. Y. Tumer and D. C. Jensen, "Quantifying the Combined Effects of Human Errors and Component Failures," *ASME Journal of Mechanical Design,* p. 101703, 2021.

[8] D. Hulse and L. Irshad, "Using Degradation Modeling to Identify Fragile Operational Conditions in Human- and Component-driven Resilience Assessment," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, Portsmouth, VA, 2022.

[9] D. Hulse and C. Hoyle, "Understanding Resilience Optimization Architectures: Alignment and Coupling in Multilevel Decomposition Strategies," *ASME Journal of Mechanical Design,* p. 111704, 2022.

[10] D. Hulse and L. Irshad, "Synthetic Fault Mode Generation for Resilience Analysis and Failure Mechanism Discovery," *ASME Journal of Mechanical Design,* p. 031707, 2023.