

Foundational Concepts in Simulation-Based Resilience Analysis and Design

IEEE Space Mission Challenges for Information Technology - IEEE
Space Computing Conference

**What is Resilience? A Workshop on Resilience, Adaptation, and
Robustness to Design Resilient Space System Architectures**

7/18/2024

Daniel Hulse, Ph.D



About Me



- Received Mechanical Engineering PhD from Oregon State University in 2020
- Dissertation: “A Computational Framework for Resilience-Informed Design”



- Now a researcher at NASA Ames
 - Funded by the System-Wide Safety project in NASA Aeronautics
 - Develop fmdtools resilience simulation library
 - Apply fmdtools to future autonomous aircraft/airspace concepts



What is Resilience?

- This is a question that is **frequently asked** by
 - Skeptics
 - Confused decision-makers
 - Normal people outside the field
- “Many definitions of resilience” in the literature
 - Many literature reviews have aimed to answer this question
 - New papers every year claiming to create a new measure/metric/definition of resilience

Title of this workshop!!!!

What is Resilience? A
Workshop on Resilience,
Adaptation, and Robustness
to Design Resilient Space
System Architectures

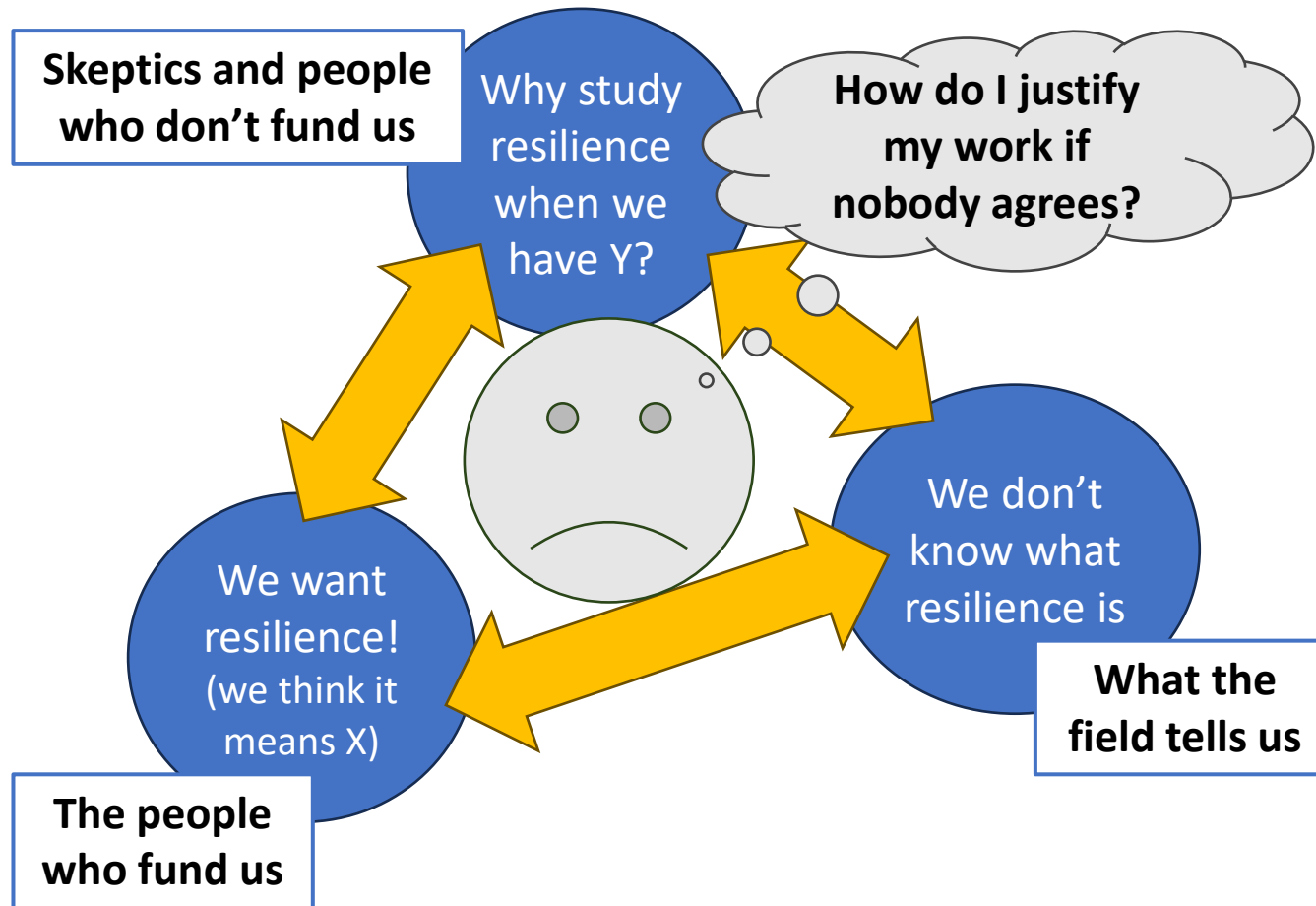
IEEE Space Mission Challenges for Information Technology - IEEE Space Computing Conference

Computer History Museum • Mountain View, CA, USA • 15-19 July 2024

Approved for public release; distribution is unlimited. Public Affairs approval number: AFRL-2024-1108



Do we not know what resilience is?



This is a problem!

- How do we sell our work?
- How do we:
 - Solve the problems people want us to solve
 - Back up the claim that this is “resilience”
- How are new researchers supposed to deal with this?
 - Why are so many resilience papers hit-and-run definitions and lit reviews?
 - What other field makes you define basic foundational terms before you can even get started?

Established Risk, Safety, Reliability, Security processes

“Why?”

“Let’s analyze resilience”

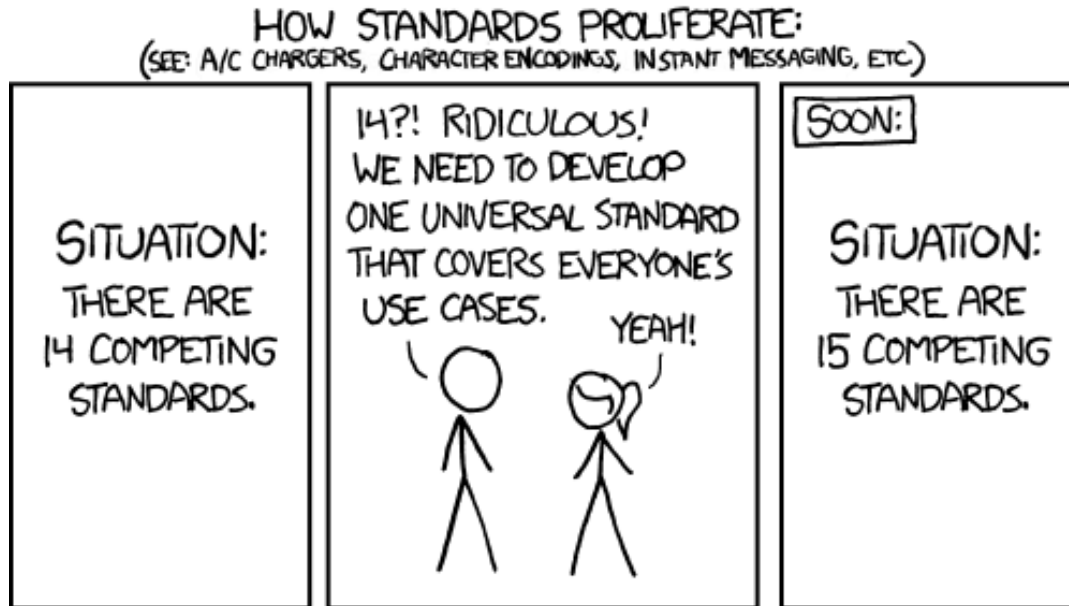


To make this ask easier,
we need to understand:

- how we fit** within existing methods/processes
- our **unique contribution**



Let's define resilience



(hopefully we define resilience generally enough to
escape this dynamic)

Goal of this presentation:

- Define what resilience means in the context of simulation:
 - Very **general framework** for thinking about resilience that unifies important concepts in the field
 - How resilience as a consideration shapes simulation (and vice-versa)
- Convey ideas about what resilience *should* mean (prescriptively) in:
 - Engineering as a whole
 - Systems Engineering
 - Complex Systems
 - Space Missions

source: <https://xkcd.com/927/>

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.



Preexisting notions about resilience

- Resilience as a field-specific property
 - Psychology—ability for people to “bounce back” after turmoil¹
 - Ecology—ability for ecosystems to restore/keep function after disasters²
 - e.g., beavers returning to the Guadalupe river reservoir after being driven out
 - e.g., redwoods sprouting new growth right after a wildfire
 - e.g., food webs re-adjusting to species loss
 - Infrastructure—ability to turn the power back on after it goes out³
- These are all helpful for understanding the concept, but it’s unclear how to adapt outside a given domain
 - What does it then mean for a spacecraft to be resilient?
 - Resilience seems like something that should be **abstract and general enough to apply across domains!**

¹Fletcher and Sarkar (2013) *Psychological Resilience*, doi.org/10.1027/1016-9040/a000124

²CS Holling (1973) *Resilience and stability of ecological systems*, doi.org/10.1017/9781009177856.038

³Vugrin et al. (2017) *Resilience Metrics for the Electric Power System: A Performance-Based Approach*, doi.org/10.2172/1367499



Preexisting notions about resilience

- Resilience as a systems property
 - Resilience as necessary “paradigm shift” away from risk⁴
 - Does resilience capture something that risk doesn’t?
 - What, then, is the relationship between resilience and safety?
 - Resilience as a uniquely socio-technical capability⁵
 - Organizations’ ability to adapt to “make things go right” (Safety-II) as opposed to just “preventing things from going wrong” (Safety-I)

These definitions don’t solve our problem

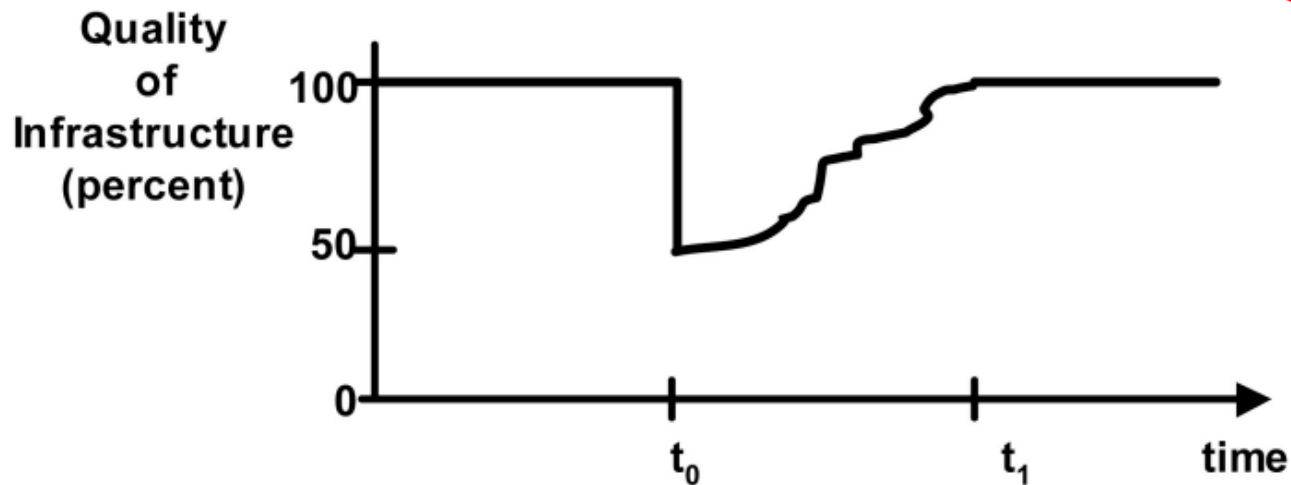
- Risk has a precise mathematical definition. If resilience and risk are incompatible, that implies a lack of rigor and perhaps an invalid formalism
- The idea of resilience as solely an organizational/human property seems incompatible with the idea of:
 - Resilient autonomous systems
 - Resilient parts (e.g., springs)
 - Other domain-specific notions of resilience

⁴Linkov et al. (2013) *Changing the resilience paradigm* doi.org/10.1038/nclimate2227

⁵Hollnagel et al (2006) *Resilience Engineering: Concepts and Precepts* doi.org/10.1201/9781315605685



Preexisting notions about resilience



- Resilience “triangle”⁶
- Metrics about resilience triangle
 - Robustness ($100 - Q_0$)
 - Rapidity ($t_1 - t_0$)
 - etc.

- This definition is clarifying, but perhaps lacks some generality
 - Is it really a triangle?
 - What if there is no recovery?
- Lack of clarity on metrics
 - Often scaled—is this really something we can use for decision-making?
 - **Can we really point to a single number as “the resilience” and move on?**
 - Especially when people keep coming up with new ones!

⁶Bruneau et al. (2003) *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities* doi.org/10.1193/1.162349



What does resilience mean in the context of simulation?



Needs of Simulation – Basic Precepts

$\times \div + - = \Sigma \int 0 1 2 3 4 5 6 7 8 9$

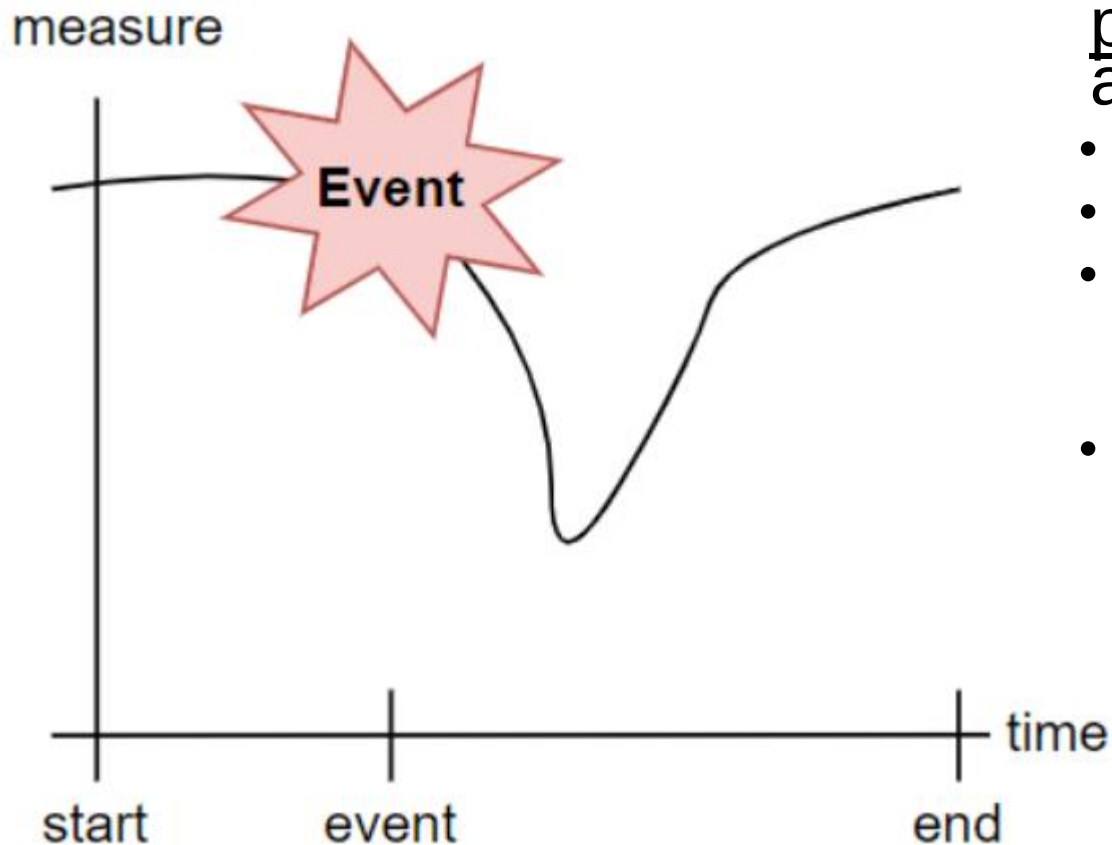
1. Resilience is a quantitative property

- Simulation demands numbers!
- This sacrifices the “soft systems” notion of resilience which may be helpful for thinking and conceptualization but resists quantification
 - We may consider this an input



Needs of Simulation – Basic Precepts

Resilience Curve Notion



2. Resilience is a dynamical systems property characterizing the **response** to an **event**

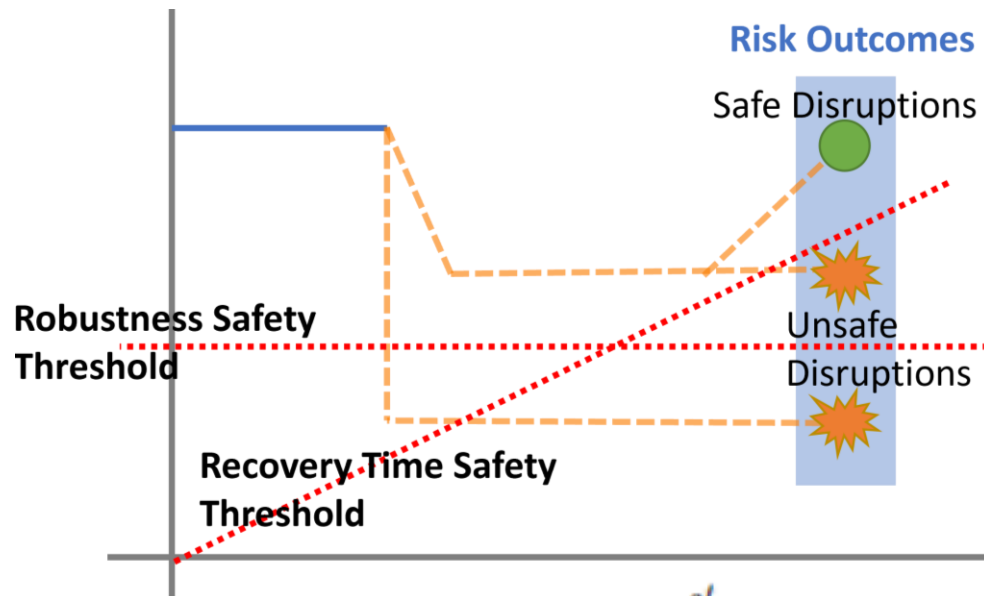
- **Event:** State of affairs
- **Response:** Behavior over time
- Illustrated via the “resilience curve”
 - Generalization of “resilience triangle”
 - Represents arbitrary response profiles
- Quantified via integrals or integral functions

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

- $r(t, s)$ – response curve for a measure of interest
- t_e —scenario end time
- t_b —scenario beginning time
- Re_s —resilience metric
 - Generalized, more abstract definition



Resutant ideas



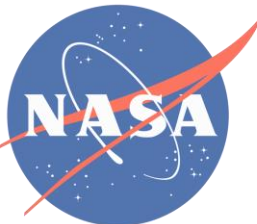
Resilience measure: $Re_s = \int_{t_h}^{t_e} r(t, s) dt$

Risk measure: $R = \mathbb{E}_{s \in S} Re_s$

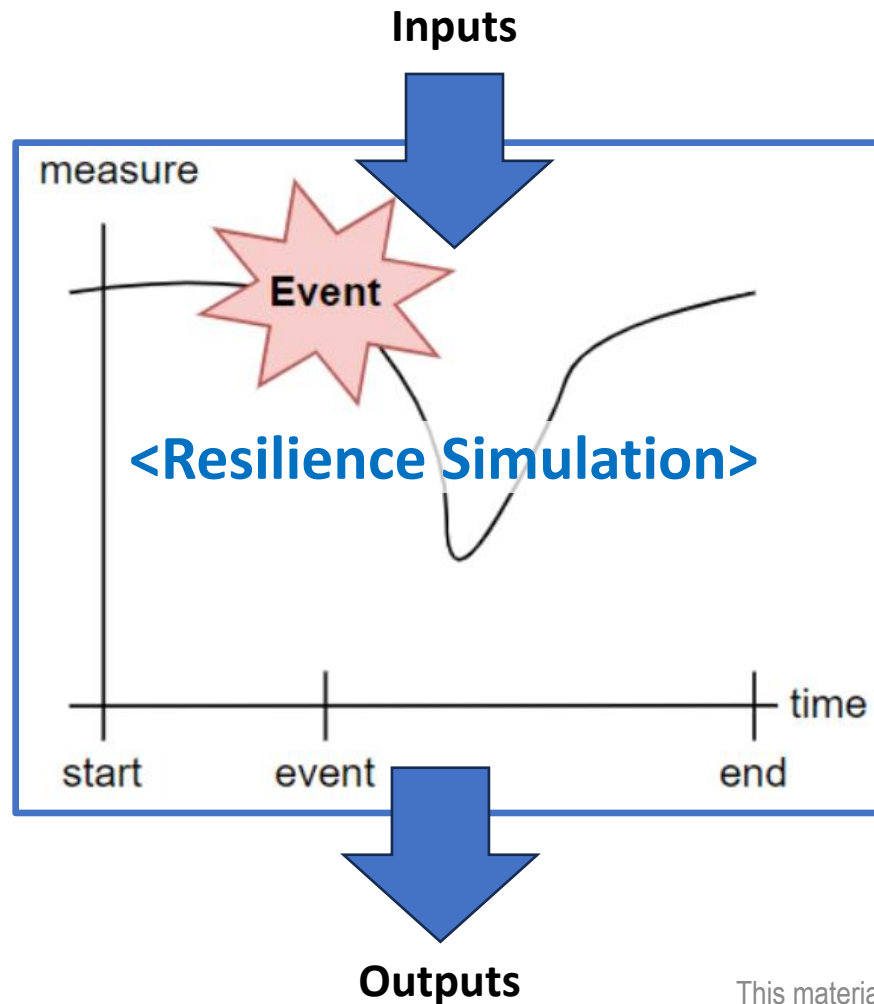
3. Resilience is a means of consideration, not an objective unto itself

- Resilience analysis doesn't prescribe measures of interest to consider, it provides ways of considering them
- **Risk and Resilience (and Safety) are compatible points of view⁷**
 - Provided Re_s is the represents a **value function** (e.g., losses in a scenario), risk is the expectation of this function over the set of scenarios
 - Safety represents constraint(s) on risk functions and can be considered with resilience methods

⁷Aven. (2021) *On Some Foundational Issues Concerning the Relationship Between Risk and Resilience*,



Resultant ideas



4. Resilience properties can be thought of as inputs and outputs of the resilience curve (i.e., the simulation)

- Outputs:

- Recovery time
- Robustness
- Risk and Safety
- Availability
- ...etc.

measures of resilience
i.e., metrics

- Inputs:

- Redundancy
- Buffer characteristics
- Active mitigation features
- Situation awareness
- ...etc.

resilience characteristics
i.e., variables



What does this mean for resilience simulation?

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.



How do we simulate resilience?

How simulate resilience depends on our **goals**

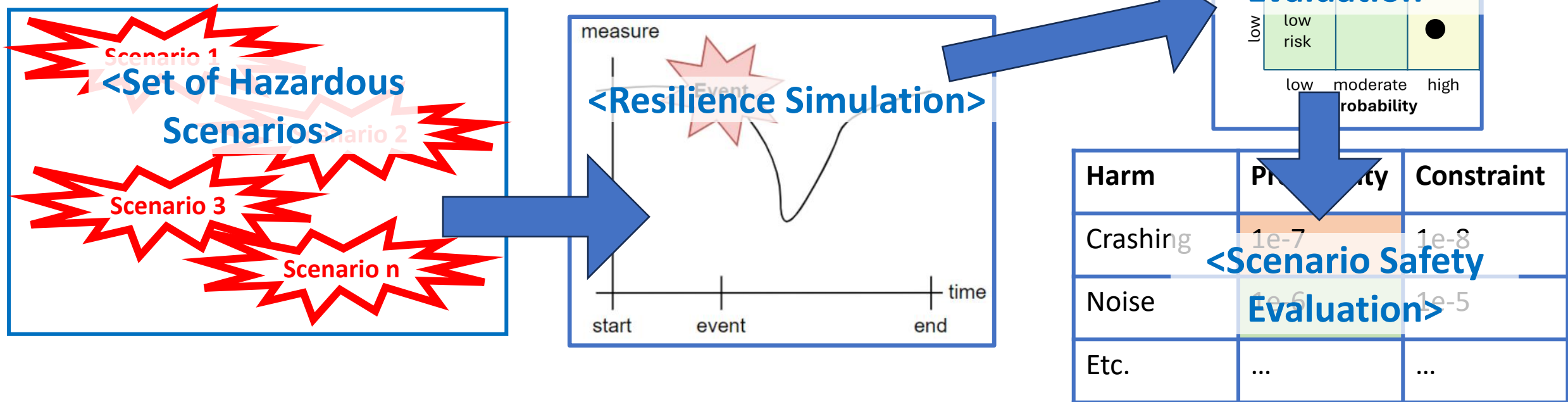
- There is **no single number that is “the resilience”**
- There is also no **single way to evaluate** metrics of interest

Instead, we have **techniques** that we adapt to our problem, e.g.:

- **To quantify risk**, we need to simulate over a number of hazardous scenarios
- **To evaluate designs**, we need to simulate the response over different parameters
- **To evaluate long and short-term effects**, we may vary the timescale of simulation
- **To evaluate different types of properties** (human, environmental, mechanical, systems-of-systems etc.), we may change the scope and modelled behaviors included in the model
- ...etc.



Example: Resilience in a Risk Framework



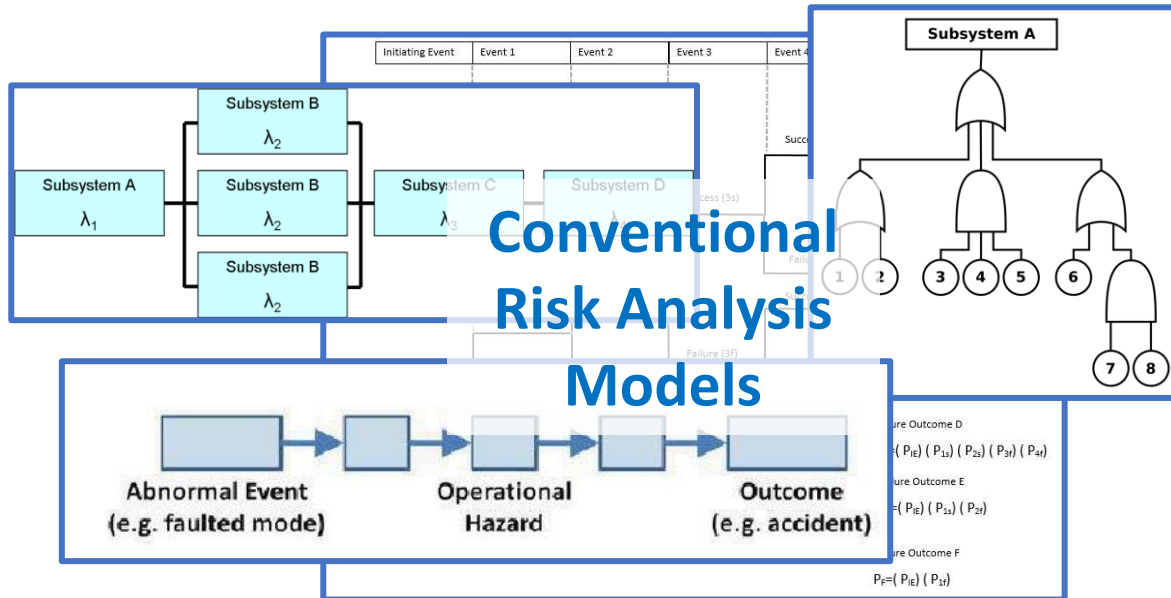
- Evaluating risk changes how we simulate (scenarios etc.)
- **This is still resilience** because we are still **modelling dynamic responses**
 - We've just wrapped it in a risk/safety framework

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

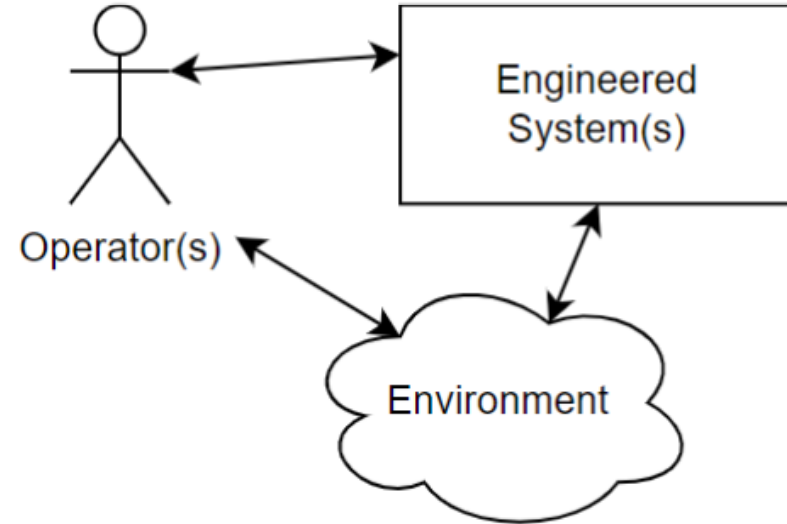
If resilience is just a part of risk/safety, what's the point?



Why resilience?



Prototypical Resilience Model

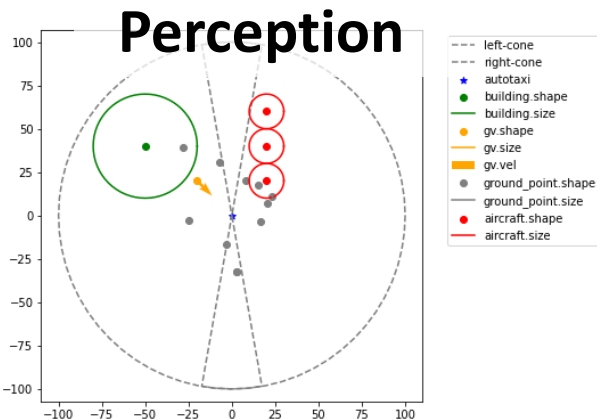
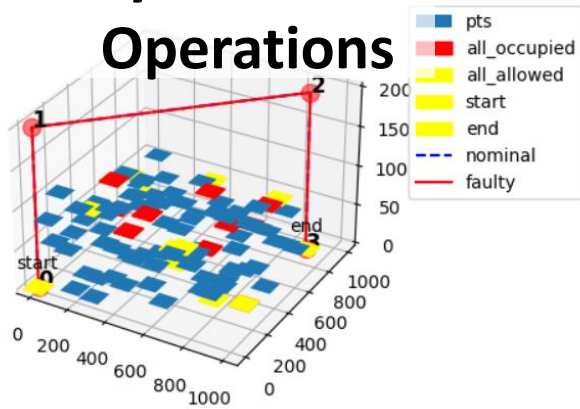


- Resilience techniques **push the boundaries** of risk/safety approaches to consider dynamic behavioral interactions, e.g., between the **operator**, **engineered system**, and **environment**
- Traditionally, these haven't been considered⁸

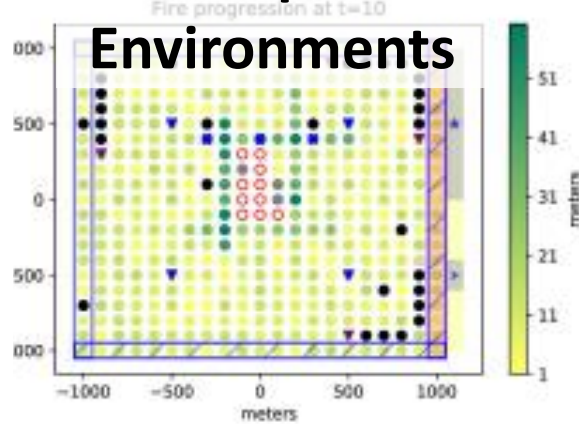
⁸Leveson. (2021) *Introduction to STAMP*. <https://www.youtube.com/watch?v=ptmjAbacMk>

Implications for Simulation

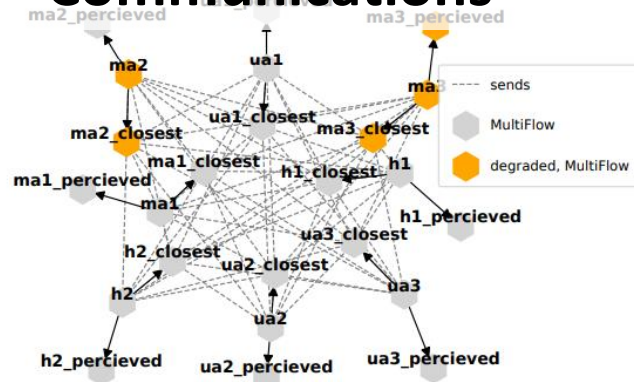
Dynamics of Operations



Complex Environments



Communications



- Resilience as a framework helps us understand the effects of **complex interactions** and **behaviors** in hazardous scenarios
- This is a **difficult simulation challenge** because it requires:
 - Representing cyber-physical behaviors that aren't often modelled
 - Integration between “low level” parts and “high-level” SoS
 - Characterizing off-nominal behaviors
 - (This has been the motivation for developing fmdtools)



Conclusion: What Resilience Means

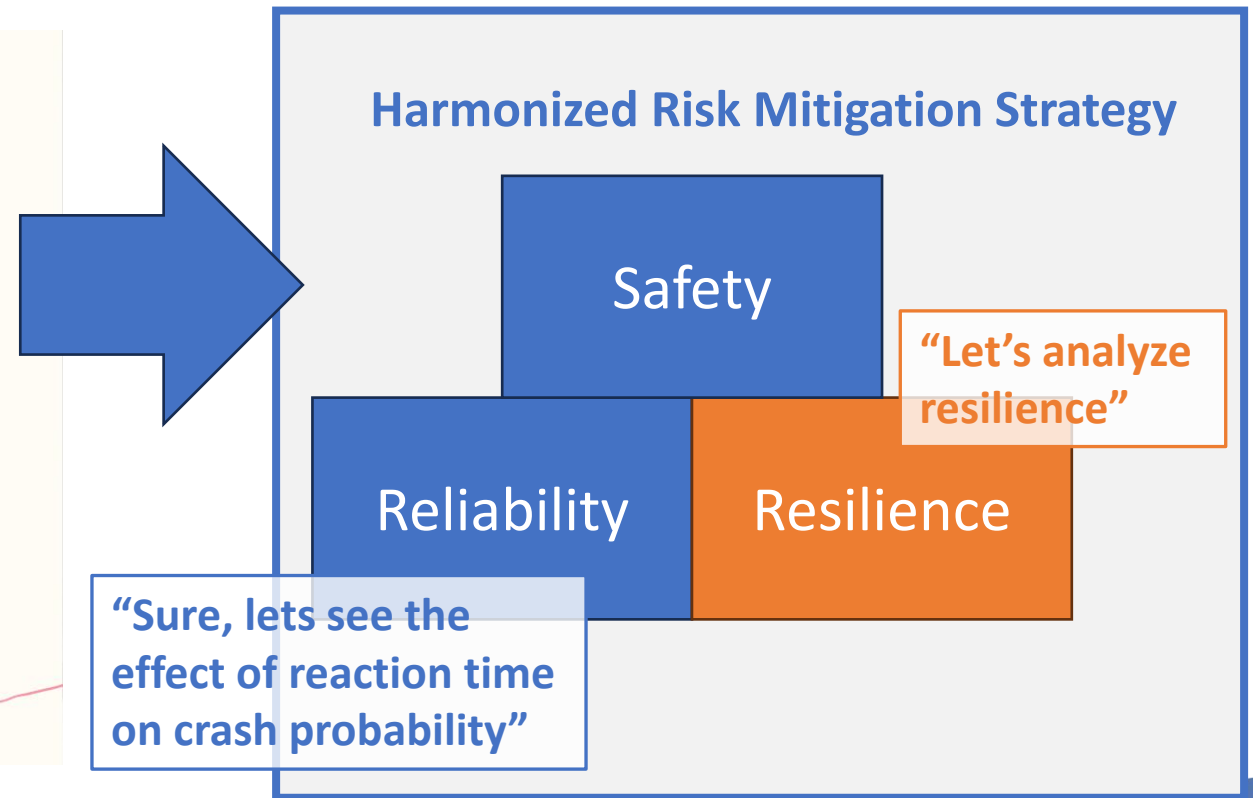
- **Resilience analysis** is a **means of considering** the dynamics of a system's response to hazardous scenarios
- **Resilience analysis** informs Risk, Safety, Economics, etc. because it:
 - helps us **evaluate harms** in a particular scenario
 - helps us **evaluate mitigation strategies** (controls, recovery, etc.)
 - helps us **understand human, environmental, and systems-of-systems considerations** not typically considered in risk models
- Simulation is conducive for resilience analysis, because
 - It lets us represent/play out the dynamics
 - It lets us evaluate large numbers of scenarios for risk/trades analysis



Resilience as a **competitor** to existing methods



Resilience as a **complement** to existing methods



Questions, Comments, Discussion

Links

- Email: daniel.e.hulse@nasa.gov
- Google Scholar: https://scholar.google.com/citations?user=fa1S_74AAAAJ&hl=en
- ResearchGate: <https://www.researchgate.net/profile/Daniel-Hulse-4>
- GitHub: <https://github.com/hulsed>
- fmdtools: <https://github.com/nasa/fmdtools>

Sources

- ¹Fletcher and Sarkar (2013) *Psychological Resilience*, doi.org/10.1027/1016-9040/a000124
- ²CS Holling (1973) *Resilience and stability of ecological systems*, doi.org/10.1017/9781009177856.038
- ³Vugrin et al. (2017) *Resilience Metrics for the Electric Power System: A Performance-Based Approach*, doi.org/10.2172/1367499
- ⁴Linkov et al. (2013) *Changing the resilience paradigm*, doi.org/10.1038/nclimate2227
- ⁵Hollnagel et al (2006) *Resilience Engineering: Concepts and Precepts* doi.org/10.1201/9781315605685
- ⁶Bruneau et al. (2003) *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities* doi.org/10.1193/1.162349
- ⁷Aven. (2021) *On Some Foundational Issues Concerning the Relationship Between Risk and Resilience*, doi.org/10.1111/risa.13848
- ⁸Leveson. (2021) *Introduction to STAMP*, https://www.youtube.com/watch?v=_ptmjAbacMk

