System Resilience

Lead Author: *John Brtis*, ***Contributing Authors:*** *Scott Jackson, Ken Cureton*

Resilience is a relatively new term in the SE realm, appearing only in the 2006 time frame and becoming popularized in 2010. The recent application of "resilience" to engineered systems has led to confusion over its meaning and a proliferation of alternative definitions. (One expert claims that well over 100 unique definitions of resilience have appeared.) While the details of definitions will continue to be discussed and debated, the information here should provide a working understanding of the meaning and implementation of resilience, sufficient for a system engineer to effectively address it.

□

Contents

Overview

Definition

According to the Oxford English Dictionary on Historical Principles (OED 1973), resilience is “the act of rebounding or springing back.” This definition most directly fits the situation of materials that return to their original shape after deformation. For human-made or engineered systems the definition of resilience can be extended to include the ability to maintain capability in the face of a disruption. The US Department of Homeland Security defines resilience as "ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance." (DHS 2017) Some practitioners define resilience only to include system reactions following an encounter with an adversity, sometimes called the reactive perspective. The INCOSE Resilient Systems Working Group (IRSWG) recommends a definition that includes actions before the encounter with the adversity; this is called the proactive perspective.

The definition recommended by the IRSWG is: resilience is the ability to provide required capability when facing adversity, as depicted in Figure 1.

Error creating thumbnail: File missing

Figure 1. General Depiction of Resilience (Brtis & McEveley 2016, Used with Permission)

Scope of the Means

In applying this definition, one needs to consider the range of means by which resilience is achieved: The means of achieving resilience include avoiding, withstanding, and recovering from adversity. These may also be considered the fundamental objectives of resilience (Brtis and McEvilley 2019). Classically, resilience includes “withstanding” and “recovering” from adversity. For the purpose of engineered systems, “avoiding” adversity is considered a legitimate means of achieving resilience (Jackson and Ferris 2016). Also, it is believed that resilience should consider the system’s ability to “evolve and adapt” to future threats and unknown-unknowns.

Scope of the Adversity

Adversity is any condition that may degrade the desired capability of a system. Ideally, the systems engineer should consider all sources and types of adversity; e.g. from environmental sources, due to normal failure, as well as from opponents, friendlies and neutral parties. Adversity from human sources may be malicious or accidental. Adversities may be expected or not. Adversity may include "unknown unknowns." The techniques for achieving resilience discussed below are applicable to both hostile and non-hostile adversities. Notably, a single incident may be the result of multiple adversities, such as a human error committed in the attempt to recover from another adversity. Finally, it is important to recognize that future risks can cause a detrimental strain on the system in the present. Systems should be designed to be appropriately resilient to emergent risks,

just as they are to known issues.

Taxonomy for Achieving Resilience

A taxonomy containing both the fundamental objectives of resilience and the means to achieve them is valuable. It can help an engineer develop a resilient design. Clemen and Reilly (2001) and Keeney (1992) discuss the importance of distinguishing fundamental objectives from means objectives and their impact on trades and engineering decision making. A three-layer objectives-based taxonomy that provides this distinction is discussed below. It includes: first level, the fundamental objectives of resilience; second level, the means objectives of resilience; and, third level, architecture, design, and operational techniques for achieving resilience. The three layers are related by many-to-many relationships. Most taxonomy content came from Brtis (2016), Jackson and Ferris (2013), and Winsted (2020).

Taxonomy Layer 1: The Fundamental Objectives of Resilience

Fundamental objectives are the first level decomposition of resilience objectives. They establish the scope of resilience. They identify the values pursued by resilience. They represent an extension of the definition of resilience. They are ends in themselves rather than just means to other ends. They should be relatively immutable. Being resilient means achieving three fundamental objectives:

- **Avoid:** eliminate or reduce exposure to stress
- **Withstand:** resist capability degradation when stressed
- **Recover:** replenish lost capability after degradation

These *fundamental* objectives can be achieved by pursuing *means* objectives. Means objectives are not ends in themselves. Their value resides in helping to achieve the three fundamental objectives.

Taxonomy Layer 2: Means Objectives

Next is a set of objectives that are not ends in themselves, but enable achieving the objectives in Layer 1. The definition shown for each objective is specific to

how it is used for resilience and are primarily drawn from references cited elsewhere in this article and from the IRSWG:

- **adaptability/flexibility/agility:** ability to react appropriately and dynamically to a situation to avoid degradation of system capability
- **anticipation:** awareness of the nature of potential adversities their likely consequences, and appropriate responses, prior to the adversity stressing the system
- **complexity management:** leveraging value-added characteristics of complexity, such as emergent behavior, while suppressing their detracting characteristics
- **constrain:** limit the propagation of damage within the system
- **continuity:** endurance of the delivery of required capability, while and after being stressed
- **disaggregation:** dispersing missions, functions, subsystems, or components across multiple systems or sub-systems
- **evolution:** restructuring the system over time to address changes to the adversity of needs
- **graceful degradation:** ability of the system to transition to desirable states when damaged
- **integrity:** quality of being complete and unaltered
- **prepare:** develop and maintain courses of action that address predicted or anticipated adversity
- **prevent:** deter or preclude the realization of strain on the system
- **re-architect:** modify the architecture for improved resilience
- **redeploy:** restructure resources to provide capabilities to recover from degradation of the system
- **robustness:** damage insensitivity or ability of a structure to withstand adverse and unforeseen events or consequences of human errors without being damaged
- **situational awareness:** perception of elements in the environment, and a comprehension of their meaning, and could include a projection of the future status of perceived elements and the risk associated with that status
- **survivability**: ability to avoid or withstand a man-

made hostile environment

- **susceptibility reduction**: reduce the inability to avoid the hostile environment
- **tolerance:**
  - *(damage tolerance):* the ability of a material/structure to resist failure due to the presence of flaws for a specified period of unrepaired usage
  - *(fault tolerance):* the attribute of an item that makes it able to perform a required function in the presence of certain sub-item faults
- **transform:** change aspects of system behavior
- **understand:** develop and maintain useful representations of required system capabilities, how those capabilities are generated, the system environment, and the potential for degradation due to adversity
- **vulnerability reduction**: reduce the harm caused by a hostile environment

Taxonomy Layer 3: Architecture, Design, and Operational Techniques to Achieve Resilience Objectives

Architecture, design, and operational techniques that may achieve resilience objectives include the following. Again, the definition shown for each objective is specific to how it is used for resilience and are primarily drawn from references cited elsewhere in this article and from the IRSWG:

- **absorb:** withstand stress without unacceptable degradation of the system's capability
- **adaptive response:** reacting appropriately and dynamically to the specific situation, to limit consequences and avoid degradation of system capability
- **adversity management:** acting to reduce the number and effectiveness of adversities
- **analytic monitoring and modeling:** gathering, fusing, and analyzing data based on an understanding of the system, to identify vulnerabilities, find indications of potential or actual adverse conditions, identify potential or actual system degradation and

evaluate the efficacy of system countermeasures

- **anomaly detection:** discovering salient irregularities or abnormalities in the system or in its environment in a timely manner that enables effective response action
- **boundary enforcement:** implementing the process, temporal, and spatial limits intended to protect the system
- **buffering:** reducing degradation due to stress through the use of excess capacity
- **coordinated defense:** having multiple, synergistic mechanisms to protect critical functional capability
- **deception:** confusing and thus impeding an adversary
- **defense in depth:** preventing or minimizing loss by employing multiple coordinated mechanisms
- **detection avoidance:** reducing an adversary's awareness of the system
- **distributed privilege:** requiring multiple authorized entities to act in a coordinated manner before a system function is allowed to proceed
- **distribution:** spreading the system’s ability to perform physically or virtually
- **diversification:** use of a heterogeneous set of technologies, data sources, processing locations, equipment locations, supply chains, communications paths, etc., to minimize common vulnerabilities and common mode failures
- **domain separation:** physically or logically isolating items with distinctly different protection needs
- **drift correction:** monitoring the system’s movement toward the boundaries of proper operation and taking corrective action
- **dynamic positioning:** relocation of system functionality or components
- **dynamic representation:** behavior modeling of the system
- **effect tolerance:** the ability to provide capability in spite of the strain on the system
- **error recovery:** automatic detection, control, and correction of an internal erroneous state
- **fail soft:** capable of prioritized, gradual termination of affected functions in the case of a fault or when failure

is imminent

- **fault tolerance:** ability to continue functioning with certain faults present
- **forward recovery:** error recovery in which a system, program, database, or other system resource is restored to a new, not previously occupied state in which it can perform required functions
- **human participation:** including people as part of the system
- **least functionality:** when each element of the system has the ability to accomplish its required functions, but not more
- **least persistence:** when system elements are available, accessible, and able to fulfill their design intent only for the time they are needed
- **least privilege:** when system elements are allocated authorizations that are necessary to accomplish their specified functions, but not more
- **least sharing:** when system resources are accessible by multiple system elements only when necessary, and among as few system elements as possible
- **loose coupling**: minimize the interdependency of elements and thus reduce the potential for propagation of damage
- **loss margins:** designing in excess capability so a partial degradation of capability is acceptable
- **maintainability:** ability to be retained in or restored to a state to perform as required, under given conditions of use and maintenance
- **mediated access:** controlling the ability to access and use system elements
- **modularity:** degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components
- **neutral state:** the condition in which the system and stakeholders can safely take no action while awaiting evaluation of the most appropriate action
- **non-persistence:** retaining information, services, and connectivity or functions for a limited time, thereby reducing an adversary’s opportunity to exploit vulnerabilities and establish a persistent foothold
- **privilege restriction:** restricting authorization assigned to entities by an authority

- **protection:** mitigation of harm to the value of interest
- **protective defaults:** providing default configurations of the system that provide protection effectiveness
- **protective failure:** ensuring that failure of a system element neither results in an unacceptable loss, nor initiates another loss scenario
- **protective recovery:** ensuring that recovery of a system element does not result in, nor lead to, unacceptable loss
- **realignment:** architectural reconfiguration to improve the system's resilience
- **redundancy, physical & functional:** the existence of more than one means at a given instant of time for performing a required function
- **repairability:** ability to be restored to a specified condition (partial or full functionality)
- **replacement:** change parts of an existing item to regain its functionality
- **restructuring:** dynamically changing the architecture to address the adversity
- **safe state:** providing the ability to transition to a state that does not lead to critical or catastrophic consequences
- **segmentation:** separation (logically or physically) of components to limit the spread of damage
- **shielding:** interposition of material (physical or virtual) that inhibits the adversity's ability to stress the system
- **substantiated integrity**: providing the ability to ensure that system components have not been corrupted
- **substitution:** using new system elements not previously used to provide or restore capability
- **unpredictability:** ability to make changes randomly that confound an opponent's understanding of the system
- **virtualization:** creating a virtual rather than actual version of something, including virtual computer hardware platforms, storage devices, and computer network resources

The means objectives and architectural and design techniques will evolve as the resilience engineering

discipline matures.

The Resilience Process

Implementation of resilience in a system requires the execution of both analytic and holistic processes. In particular, the use of architecting with the associated heuristics is required, as shown in Table 1 below. Inputs are the desired level of resilience and the characteristics of a threat or disruption. Outputs are the characteristics of the system, particularly the architectural characteristics and the nature of the elements (e.g., hardware, software, or humans).

Artifacts depend on the domain of the system. For technological systems, specification and architectural descriptions will result. For enterprise systems, enterprise plans will result.

Both analytic and holistic methods are required, including the techniques of architecting. Analytic methods determine required robustness. Holistic methods determine required adaptability, tolerance, and integrity.

One pitfall to be avoided is to depend on just a single technique to achieve resilience. Resilience benefits from multiple techniques, thus achieving defense in depth.

Resilience should be considered throughout the systems engineering life cycle, but most especially in early life cycle activities that produce resilience requirements. Once resilience requirements are established, they can and should be managed throughout the system life cycle along with all the other requirements in the trade space. Brtis and McEvilley (2019) recommend specific considerations, listed below, to be included in early life cycle activities.

- **Business or Mission Analysis Process**
  - Defining the problem space should include identification of adversities and expectations for performance under those adversities.
  - ConOps, OpsCon, and solution classes should consider the ability to avoid, withstand, and recover from the adversities.
  - Evaluation of alternative solution classes must consider ability to deliver required capabilities under adversity.
- **Stakeholder Needs and Requirements Definition**

Process

- The stakeholder set should include persons who understand potential adversities and stakeholder resilience needs.
- When identifying stakeholder needs, identify expectations for capability under adverse conditions and degraded/alternate, but useful, modes of operation.
- Operational concept scenarios should include resilience scenarios.
- Transforming stakeholder needs into stakeholder requirements includes stakeholder resilience requirements.
- Analysis of stakeholder requirements includes resilience scenarios in the adverse operational environment.

- **System Requirements Definition Process**
  - Resilience should be considered in the identification of requirements.
  - Achieving resilience and other adversity-driven considerations should be addressed holistically.
- **Architecture Definition Process**
  - Selected viewpoints should support the representation of resilience.
  - Resilience requirements can significantly limit and guide the range of acceptable architectures. It is critical that resilience requirements are mature when used for architecture selection.
  - Individuals developing candidate architectures should be familiar with architectural techniques for achieving resilience.
  - Achieving resilience and other adversity-driven considerations should be addressed holistically.
- **Design Definition Process**
  - Individuals developing candidate designs should be familiar with design techniques for achieving resilience.
  - Achieving resilience and the other adversity-driven considerations should be addressed holistically.
- **Risk Management Process**
  - Risk management should be planned to handle risks, issues, and opportunities identified by resilience activities.

Table 1. Resilience Heuristics Based on Means for Achieving Level 2 Objectives

#	Heuristic
1	The system should react appropriately and dynamically to the specific situation to limit consequences, avoid degradation of system capability.
2	System should have the ability to adapt to deliver required capability in unpredictably evolving conditions.
3	System should establish awareness of the nature of potential adversities their likely consequences and appropriate responses prior to the adversity stressing the system.
4	System should limit the propagation of damage within the system.
5	System will maintain the delivery of required capability while and after being stressed.
6	System will disperse missions, functions, subsystems, or components across multiple systems or subsystems.
7	System will restructure itself to address changes to the adversity or needs over time
8	System will have the ability to transition to desirable states after damage
9	System will maintain the quality of being complete and unaltered
10	System will leverage value-added characteristics of complexity and will suppress detracting characteristics following an encounter with an adversity

Resilience Requirements

Brtis and McEvilley (2019) investigated the content and structure needed to specify resilience requirements. Resilience requirements often take the form of a resilience scenario. There can be many such scenario threads in the Conops or OpsCon.

The following information is often part of a resilience requirement:

- operational concept name
- system or system portion of interest
- capability(s) of interest their metric(s) and units
- target value(s); i.e., the required amount of the capability(s)
- system modes of operation during the scenario, e.g., operational, training, exercise, maintenance, and update
- system states expected during the scenario

- adversity(s) being considered, their source, and type
- potential stresses on the system, their metrics, units, and values (Adversities may affect the system either directly or indirectly. Stresses are adversities that directly affect the system.)
- resilience related scenario constraints, e.g., cost, schedule, policies, and regulations
- timeframe and sub-timeframes of interest
- resilience metric, units, determination methods, and resilience metric target; example metrics: expected availability of required capability, maximum allowed degradation, maximum length of degradation, and total delivered capability. There may be multiple resilience targets, e.g., threshold, objective, and "as resilient as practicable." (Resilience metrics are often strains on the system; i.e., the effects of stress on the system.)

Importantly, many of these parameters may vary over the timeframe of the scenario (see Figure 2). Also, a single resilience scenario may involve multiple adversities, which may be involved at multiple times throughout the scenario.

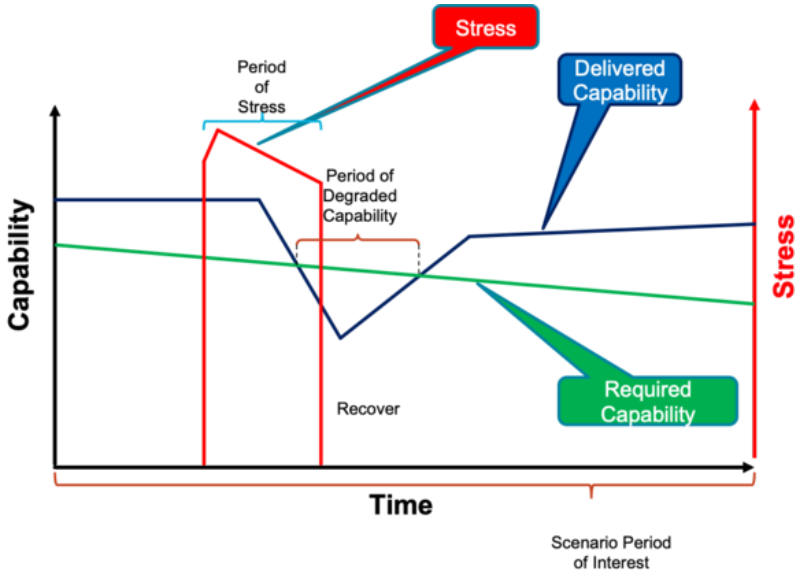

Figure 2. Time-Wise Values of Notional Resilience Scenarios Parameters. (Brtis et al. 2021, Used with Permission)

Representing the complexity of resilience requirements is not straightforward. Brtis, et al. (2021) studied this challenge and recommended three forms for resilience requirements: (1) natural language, (2) entity-relationship diagram (data structure), and (3) an extension to SysML. All contain the same information, but are in forms that meet the needs of different

audiences. An example of a natural language pattern for representing a resilience requirement is:

> The <system, mode(t), state(t)> encountering <adversity(t), source, type>, which imposes <stress(t), metric, units, value(t)> thus affecting delivery of <capability(t), metric, units> during <scenario timeframe, start time, end time, units> and under <scenario constraints>, shall achieve <resilience target(t) (include excluded effects)> for <resilience metric, units, determination method>

Affordable Resilience

"Affordable Resilience" means to achieve an effective balance across life cycle cost and technical attributes of Resilience Engineering. This implies providing required capability when facing adversity in current and changing conditions to satisfy the needs of multiple stakeholders throughout a system's life cycle. Life cycle considerations for affordable resilience should address not only risks and issues associated with known and unknown adversities over time, but also opportunities for gain in known and unknown future environments.

Technical attributes for affordable resilience include potential treatment of technical risks, reliability, robustness, flexibility, adaptability, tolerance, and integrity, as well as the ability to prepare for and avoid, withstand, and recover from adversity. This may require balancing the time value of funding vs. the time value of resilience in order to achieve affordable resilience as shown in Figure 3.

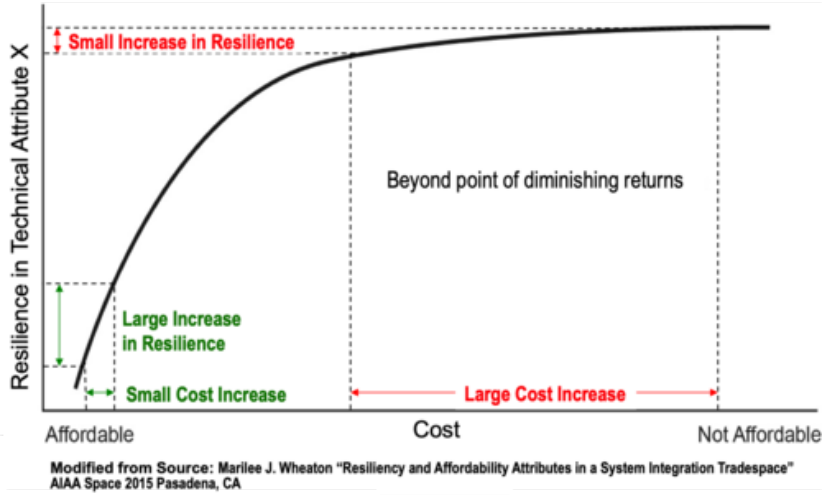

Figure 3. Resilience versus Cost. (Wheaton 2015, Used with Permission)

Once the affordable levels of resilience are determined for each key technical attribute, the affordable levels across those attributes can be prioritized via standard techniques, such as Multi-attribute Utility Theory (MAUT) (Keeney and Raiffa 1993) and Analytical Hierarchy Process (AHP). (Saaty 2009)

The priority of affordable resilience attributes for systems is typically domain-dependent; for example:

- Public transportation systems may emphasize safety as well as meeting regulatory requirements and mitigating liability risks, with spending spread out in time to match current and future budgets
- Electronic funds transfer systems may emphasize cyber security, with whatever funding is required to meet regulatory requirements and liability risks
- Unmanned space exploration systems may emphasize survivability to withstand previously-unknown environments, usually with specified (and often limited) near-term funding constraints
- Electrical power grids may emphasize safety, reliability, and meeting regulatory requirements together with adaptability to change in the balance of power generation and storage technologies with shifts in power distribution and usage
- Medical capacity for disasters may emphasize rapid adaptability to major incidents, with affordable levels of planning, preparation, response, and recovery to meet public health demands. This emphasis must balance potential liability and concurrent accomplishment of key emergency medical practices,

such as triage and “first do no harm”.

Discipline Relationships

Resilience has commonality and synergy with a number of other quality areas. Examples include availability, environmental impact, survivability, maintainability, reliability, operational risk management, safety, security and, quality. This group of quality areas is referred to as loss-driven systems engineering (LDSE) because they all focus on potential losses involved in the development and use of systems. These areas frequently share the assets considered, losses considered, adversities considered, requirements, and architectural, design and process techniques. It is imperative that these areas work closely with one another and share information and decision-making in order to achieve a holistic approach. The concept of pursuing loss-driven systems engineering, its expected benefits, and the means by which it can be pursued are addressed extensively in an edition of *INCOSE Insight* (2020).

Discipline Standards

Two standards stand out for insight on resilience:

- ASISI (2009) is a standard pertaining to the resilience of organizational systems.
- NIST 800-160 (Ross, R. et al. 2018) considers the resilience of physical systems.

Personnel Considerations

People are important components of systems for which resilience is desired. This aspect is reflected in the human in the loop technique identified by Jackson and Ferris (2013). Decisions made by people are at the discretion of the people in real time. Apollo 11 described by Eyles (2009) is a good example.

Organizational Resilience

Because organizational systems and cyber-physical systems differ significantly, it is not surprising that resilience is addressed differently in each. It is important that those pursuing organizational resilience and cyber-physical resilience learn and benefit by understanding the alternate perspective. Organizations as systems and systems of systems typically view resilience in terms of

managing continuity of its operations, including through emergencies, incidents, and other adverse events, with a host of processes whose required capability is focused on ensuring the organization's core functions can withstand disruptions, interruptions, and adversities. ISO 22301 addresses requirements for security and resilience in business continuity management systems. It is an international standard that provides requirements appropriate to the amount and type of impact that the organization may or may not accept following a disruption.

Resilient organizations require resilient employees. Coutu (2002) explores three characteristics of resilient organizations and resilient people: (1) they accept the harsh realities facing them, (2) they find meaning in terrible times, and (3) they are creative under pressure, making do with whatever's at hand.

Hamel & Valikangas (2003) explore means of achieving *strategic resilience*, i.e., "the ability to dynamically reinvent business models and strategies as circumstances change...and to change before the need becomes desperately obvious". An organization with this capability constantly remakes its future rather than defending its past.

Lee, Vargo, and Seville (2013) developed metrics and tools for measuring organizational resilience based on three dimensions: (1) the level of organizational situational awareness, (2) management of organizational vulnerabilities, and (3) organizational adaptive capacity. These three items seem to be well accepted and appear in some form in many papers.

Preparing for the unknown is a recurring challenge of resilience. Organizations must frequently deal with adversities that were previously unknown or unknowable. Scoblic, *et. al*. (2020) describes techniques for developing *strategic foresight*. He recommends adopting the practice of scenario planning, where multiple adverse futures are envisioned, countermeasures are developed, and coping strategies that appear most frequently are deemed "robust" and candidates for action. This process also trains personnel to better deal with emerging adversity.

Metrics

Uday and Marais (2015) performed a survey of resilience metrics. Those identified include:

- Time duration of failure
- Time duration of recovery
- Ratio of performance recovery to performance loss
- A function of speed of recovery
- Performance before and after the disruption and recovery actions
- System importance measures

Jackson (2016) developed a metric to evaluate various systems in four domains: aviation, fire protection, rail, and power distribution, for the principles that were lacking in ten different case studies. The principles are from the set identified by Jackson and Ferris (2013) and are represented in the form of a histogram plotting principles against frequency of omission. The data in these gaps were taken from case studies in which the lack of principles was inferred from recommendations by domain experts in the various cases cited.

Brtis (2016) surveyed and evaluated a number of potential resilience metrics and identified the following:

- Maximum outage period
- Maximum brownout period
- Maximum outage depth
- Expected value of capability: the probability-weighted average of capability delivered
- Threat resiliency; i.e. the time integrated ratio of the capability provided divided by the minimum needed capability
- Expected availability of required capability; i.e. the likelihood that for a given adverse environment the required capability level will be available
- Resilience levels; i.e. the ability to provide required capability in a hierarchy of increasingly difficult adversity
- Cost to the opponent
- Cost-benefit to the opponent
- Resource resiliency; i.e. the degradation of capability that occurs as successive contributing assets are lost

Brtis found that multiple metrics may be required, depending on the situation. However, if one had to select a single most effective metric for reflecting the meaning of resilience, Brtis proposed that it would be "the expected availability of the required capability."

Expected availability of the required capability is the probability-weighted sum of the availability summed across the scenarios under consideration. In its most basic form, this metric can be represented mathematically as:

$R = \sum_{1}^n\Bigl(\frac{P_i}{T}\int_{0}^{T} Cr(t)_i,{dt}\Bigr)$

where,

R = Resilience of the required capability (Cr);

n = the number of exhaustive and mutually exclusive adversity scenarios within a context (n can equal 1);

P_i = the probability of adversity scenario i;

$Cr(t)_i$ = time wise availability of the required capability during scenario i: 0 if below the required level, 1 if at or above the required value. Where circumstances dictate this may take on a more complex, non-binary function of time;

T = length of the time of interest.

References

Works Cited

Adams, K. M., P.T. Hester, J.M. Bradley, T.J. Meyers, and C.B. Keating. 2014. "Systems Theory as the Foundation for Understanding Systems." *Systems Engineering,* 17(1):112-123.

ASISl. 2009. Organizational Resilience: Security, Preparedness, and Continuity Management Systems--Requirements With Guidance for Use. Alexandria, VA, USA: ASIS International.

Billings, C. 1997. *Aviation Automation: The Search for Human-Centered Approach.* Mahwah, NJ: Lawrence Erlbaum Associates.

Boehm, B. 2013. *Tradespace and Affordability – Phase 2 Final Technical Report.* December 31 2013, Stevens Institute of Technology Systems Engineering Research Center, SERC-2013-TR-039-2. Accessed April 2, 2021. Available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a608178.pdf.

Browning, T.R. 2014. "A Quantitative Framework for Managing Project Value, Risk, and Opportunity." *IEEE Transactions on Engineering Management.* 61(4): 583-598, Nov. 2014. doi: 10.1109/TEM.2014.2326986.

Brtis, J.S. 2016. *How to Think About Resilience in a DoD Context: A MITRE Recommendation.* MITRE Corporation, Colorado Springs, CO. MTR 160138, PR 16-20151,

Brtis, J.S. and M.A. McEvilley. 2019. *Systems Engineering for Resilience.* The MITRE Corporation. MP 190495. Accessed April 2, 2021. Available at https://www.researchgate.net/publication/334549424_Systems_Engineering_for_Resilience.

Brtis, J.S., M.A. McEvilley, and M.J. Pennock. 2021. "Resilience Requirements Patterns." *Proceedings of the INCOSE International Symposium,* July 17-21, 2021.

Checkland, P. 1999. *Systems Thinking, Systems Practice*. New York, NY: John Wiley & Sons.

Clemen, Robert T. and T. Reilly. 2001. *Making Hard Decisions, with DecisionTools.* Duxbury Press, Pacific Grove, CA.

Coutu, Diane L., "How Resilience Works". Harvard Business Review 80(5):46-50, 2002.

Cureton, Ken. 2023. *About Resilience Engineering in (and of) Digital Engineering*. Presented to the Defense Acquisition University, February 23, 2023. Accessed October 2, 2023. Available at https://media.dau.edu/media/t/1_xfmk3vyh.

DHS. 2017. *Instruction Manual 262-12-001-01 DHS Lexicon Terms and Definitions 2017 Edition – Revision 2.* US Department of Homeland Security. Accessed April 2, 2021. Available at https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf.

Eyles, D. 2009. "1202 Computer Error Almost Aborted Lunar Landing." Massachusetts Institute of Technology, MIT News. Accessed April 2, 2021. Available http://njnnetwork.com/2009/07/1202-computer-error-almost-aborted-lunar-landing/.

Hamel, G. and L. Valikangas. 2003. "The Quest for Resilience," *Harvard Business Review*, 81(9):52-63.

Hitchins, D. 2009. "What are the General Principles

Applicable to Systems?" *INCOSE Insight.* 12(4):59-6359-63. Accessed April 2, 2021. Available athttps://onlinelibrary.wiley.com/doi/abs/10.1002/inst.20 0912459.

Hollnagel, E., D. Woods, and N. Leveson (eds). 2006. *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate Publishing Limited.

INCOSE. 2015. *Systems Engineering Handbook, a Guide for System Life Cycle Processes and Activities*. New York, NY, USA: John Wiley & Sons.

INCOSE. 2020. "Special Feature: Loss-Driven Systems Engineering," *INCOSE Insight.* 23(4): 7-33. Accessed May 7, 2021. Available at https://onlinelibrary.wiley.com/toc/21564868/2020/23/4.

Jackson, S. and T. Ferris. 2013. "Resilience Principles for Engineered Systems." *Systems Engineering*. 16(2):152-164. doi:10.1002/sys.21228.

Jackson, S. and T. Ferris. 2016. Proactive and Reactive Resilience: A Comparison of Perspectives. Accessed April 2, 2021. Available at https://www.academia.edu/34079700/Proactive_and_Rea ctive_Resilience_A_Comparison_of_Perspectives.

Jackson, W.S. 2016. Evaluation of Resilience Principles for Engineered Systems. Unpublished PhD, University of South Australia, Adelaide, Australia.

Keeney, R.L. 1992. *Value-Focused Thinking, a Path to Creative Decision-making*, Harvard University Press Cambridge, Massachusetts.

Keeney, R.L. and H. Raiffa. 1993. *Decisions with Multiple Objectives.* Cambridge University Press.

Lee, A.V., J. Vargo, and E. Seville. 2013. "Developing a tool to measure and compare organizations' resilience". *Natural Hazards Review*, 14(1):29-41.

Madni, A. and S. Jackson. 2009. "Towards a conceptual framework for resilience engineering." *IEEE Systems Journal.* 3(2):181-191.

Neches, R. and A.M. Madni. 2013. "Towards affordably adaptable and effective systems". *Systems Engineering*, 16: 224-234. doi:10.1002/sys.21234.

OED. 1973. The Shorter Oxford English Dictionary on Historical Principles. edited by C. T. Onions. Oxford: Oxford University Press. Original edition, 1933.

Ross, R., M. McEvilley, J. Oren 2018. "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems." National Institute of Standards and Technology (NIST). SP 800-160 Vol. 1. Accessed April 2, 2021. Available at https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final.

Saaty, T.L. 2009. *Mathematical Principles of Decision Making.* Pittsburgh, PA, USA: RWS Publications.

Scoblic, J.P., A. Ignatius, D. Kessler, "Emerging from the Crisis," *Harvard Business Review*, July, 2020.

Sillitto, H.G. and D. Dori. 2017. "Defining 'System': A Comprehensive Approach." *Proceedings of the INCOSE International Symposium* 2017, Adelaide, Australia.

Uday, P. and K. Morais. 2015. Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges. *Systems Engineering.* 18(5):491-510.

Warfield, J.N. 2008. "A Challenge for Systems Engineers: To Evolve Toward Systems Science." *INCOSE Insight.* 11(1).

Wheaton, M.J. and A.M. Madni. 2015. "Resiliency and Affordability Attributes in a System Integration Tradespace", Proceedings of AIAA SPACE 2015 Conference and Exposition, 31 Aug-2 Sep 2015, Pasadena California. Accessed April 30, 2021. Available at: https://doi.org/10.2514/6.2015-4434.

Winstead, M. 2020. "An Early Attempt at a Core, Common Set of Loss-Driven Systems Engineering Principles." INCOSE *INSIGHT*, December 22-26.

Winstead, M., D. Hild, and M. McEvilley. 2021. "Principles of Trustworthy Design of Cyber-Physical Systems." MITRE Technical Report #210263, The MITRE Corporation, June 2021. Available: https://www.mitre.org/publications/technical-papers.

Primary References

Hollnagel, E., D.D. Woods, and N. Leveson (Eds.). 2006. *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate Publishing Limited.

Jackson, S. and T. Ferris. 2013. "Resilience Principles for Engineered Systems." *Systems Engineering*,

16(2):152-164.

Jackson, S., S.C. Cook, and T. Ferris. 2015. "Towards a Method to Describe Resilience to Assist in System Specification." *Proceedings of the INCOSE International Symposium*. Accessed May 25, 2023. Available at https://www.researchgate.net/publication/277718256_Towards_a_Method_to_Describe_Resilience_to_Assist_System_Specification.

Jackson, S. 2016. Principles for Resilient Design - A Guide for Understanding and Implementation. Accessed April 30, 2021. Available at https://www.irgc.org/irgc-resource-guide-on-resilience.

Madni, A. and S. Jackson. 2009. "Towards a conceptual framework for resilience engineering." *IEEE Systems Journal.* 3(2):181-191.

Additional References

9/11 Commission. 2004. 9/11 Commission Report. National Commission on Terrorist Attacks on the United States. Accessed April 2, 2021. Available at https://9-11commission.gov/report/.

Ball, R. E. (2003). *The Fundamentals of Aircraft Combat Survivability Analysis and Design*. 2nd edition. AIAA (American Institute of Aeronautics & Astronautics) Education series. (August 1, 2003)

Billings, C. 1997. *Aviation Automation: The Search for Human-Centered Approach*. Mahwah, NJ: Lawrence Erlbaum Associates.

Bodeau, D. K and R. Graubart. 2011. *Cyber Resiliency Engineering Framework.* The MITRE Corporation. MITRE Technical Report #110237.

Bodeu, D. K. and R. Graubart. 2012. Cyber Resiliency Engineering Framework. The MITRE Corporation. Accessed April 2, 2021. Available at https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework.

DoD. 1985. *MIL-HDBK-268(AS) Survivability Enhancement, Aircraft Conventional Weapon Threats, Design and Evaluation Guidelines.* US Navy, Naval Air Systems Command.

Henry, D. and E. Ramirez-Marquez. 2016. "On the Impacts of Power Outages during Hurricane Sandy – A

Resilience Based Analysis." *Systems Engineering.*19(1): 59-75. Accessed April 2, 2021. Available at https://onlinelibrary.wiley.com/doi/10.1002/sys.21338.

Jackson, S., S.C. Cook, and T. Ferris. 2015. A Generic State-Machine Model of System Resilience. *INCOSE Insight.* 18(1):1 4-18. Accessed April 2, 2021. Available at https://onlinelibrary.wiley.com/doi/10.1002/inst.12003. Accessed on April 2, 2021.

Leveson, N. 1995. Safeware: System Safety and Computers. Reading, Massachusetts: Addison Wesley.

Pariès, J. 2011. "Lessons from the Hudson." in *Resilience Engineering in Practice: A Guidebook*, edited by E. Hollnagel, J. Pariès, D.D. Woods and J. Wreathhall, 9-27. Farnham, Surrey: Ashgate Publishing Limited.

Perrow, C. 1999. *Normal Accidents: Living With High Risk Technologies.* Princeton, NJ: Princeton University Press.

Reason, J. 1997. *Managing the Risks of Organizational Accidents.* Aldershot, UK: Ashgate Publishing Limited.

Rechtin, E. 1991. *Systems Architecting: Creating and Building Complex Systems*. Englewood Cliffs, NJ: CRC Press.

Schwarz, C.R. and H. Drake. 2001. *Aerospace Systems Survivability Handbook Series. Volume 4: Survivability Engineering.* Joint Technical Coordinating Group on Aircraft Survivability, Arlington, VA.

US-Canada Power System Outage Task Force. 2004. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Washington-Ottawa.

< Previous Article | Parent Article | Next Article >
SEBoK v. 2.10, released 06 May 2024
