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 which 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 (RSWG) recommends a definition that includes actions before the encounter with the adversity; this is called the proactive perspective.

The definition recommended by the RSWG is: resilience is the ability to provide required capability when facing adversity.

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.

Taxonomy for Achieving Resilience

Achieving resilience can be facilitated by considering a taxonomy of its objectives and techniques. A useful three-layer, objectives-based taxonomy 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 items in the three layers relate by many-to-many relationships. The aggregation of work on resilience taxonomies by (Brtis 2016) and (Jackson and Ferris 2013) is:

Taxonomy Layer 1: The Intrinsic Value of Resilience

There are three objectives that reveal the intrinsic value of resilience:

- Avoid adversity
- Withstand adversity
- Recover from adversity

Taxonomy Layer 2: Means Objectives that are not Ends in Themselves

Table 1 shows a set of objectives that are not as fundamental as those in Layer 1, but enable achieving Layer 1's objectives:

Table 1. Means Objectives

• adaptability/flexibility	• agility	• anticipation
• constraint	• continuity	• disaggregation
• evolution	• graceful degradation	• integrity
• preparation	• prevention	• re-architecting
• redeployment	• robustness	• situational awareness
• tolerance	• transformation	• understanding

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

The engineering techniques in Table 2 support achieving resilience objectives.

Table 2. Architecture, Design, and Operational Techniques to Achieve Resilience Objectives

• absorption	• adaptive response	• analytic monitoring and modeling
• boundary enforcement	• buffering	• complexity avoidance
• coordinated defense	• deception	• defense in depth
• detection avoidance	• distribution	• diversification
• drift correction	• dynamic positioning	• dynamic representation
• effect tolerance	• human participation	• internode interaction and interfaces
• least privilege	• loose coupling	• modularity
• neutral state or safe state	• non-persistence	• physical & functional redundancy
• privilege restriction	• proliferation	• protection
• realignment	• reconfiguring	• reparability
• replacement	• restructuring	• segmentation

• substantiated integrity	• substitution	• threat suppression
• unpredictability	• virtualization	

Definitions of these terms are available in Brtis (2016) and Jackson and Ferris (2013). The list of means objectives and architectural and design techniques will evolve as the resilience domain 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. 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, including the techniques of architecting, are required. Analytic methods determine required robustness. Holistic methods determine required adaptability, tolerance, and integrity.

One pitfall is to depend on just a single technique to achieving resilience. The technique of defense in depth suggests that multiple techniques may be required to achieve resilience.

While resilience should be considered throughout the systems engineering life cycle, it is critical that resilience be considered in the early life cycle activities that lead to the development of resilience requirements. Once resilience requirements are established, they can and should be managed along with all of the other requirements in the trade space throughout the system life cycle. 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.

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
- 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"

Importantly, many of these parameters may vary over the timeframe of the scenario (see Figure 1). Also, a

single resilience scenario may involve multiple adversities, which may be involved at multiple times throughout the scenario.

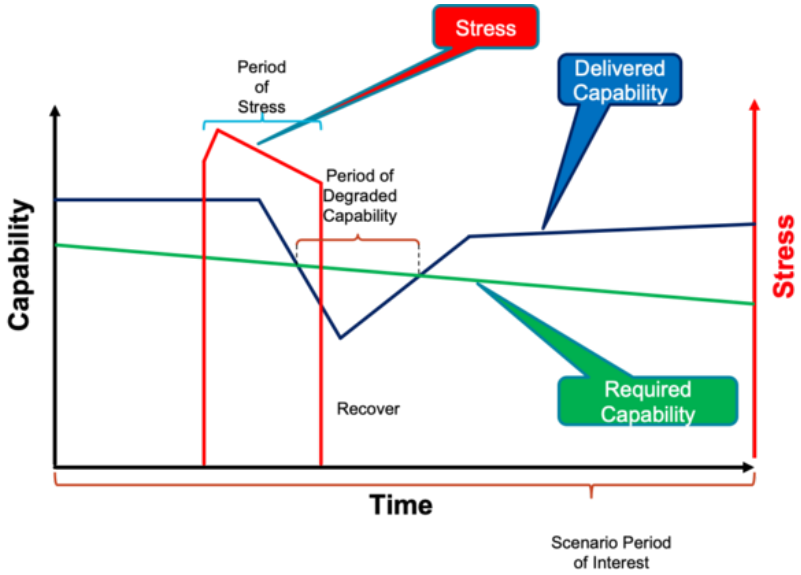

Figure 1. Time-Wise Values of Notional Resilience Scenarios Parameters. (Brtis et al. 2021, Used with Permission)

Representing the complexity of resilience requirements is not straight forward. Brtis, et al. (2021) studied this challenge and recommend patterns for resilience requirements. They recommend patterns in three forms to address the needs of different audiences: (1) natural language, (2) entity-relationship diagram (date structure), and (3) an extension to SysML. 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 as required 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 seeking 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 often requires balancing the time value of funding vs. the time value of resilience in order to achieve affordable resilience as shown in Figure 2.

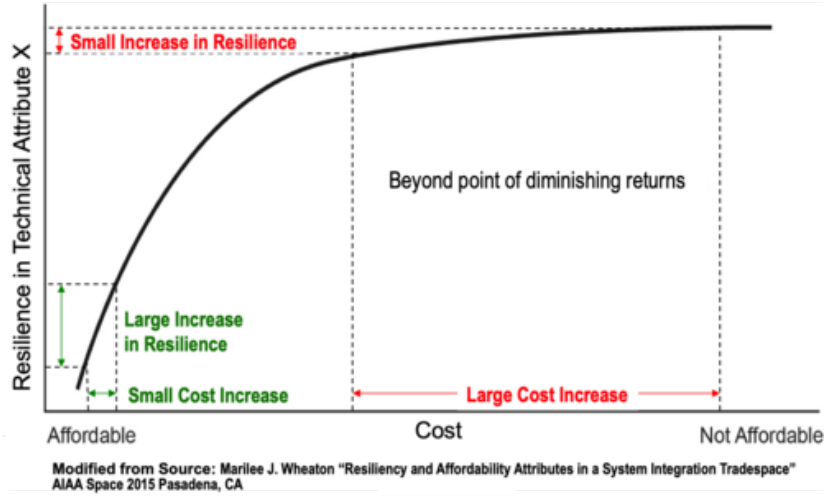

Figure 2. Resilience versus Cost. (Wheaton 2015, Used with Permission)

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 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

Humans 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 the humans are at the discretion of the humans in real time. Apollo 11 described by Eyles (2009) is a good example.

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: 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.

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: 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/

Hitchins, D. 2009. "What are the General Principles Applicable to Systems?" *INCOSE Insight.* 12(4): 59-6359-63. Accessed April 2, 2021. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/inst.200912459

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: 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: https://www.academia.edu/34079700/Proactive_and_Reactive_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.K. and H. Raiffa. 1993. *Decisions with Multiple Objectives.* Cambridge University Press.

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 Univeristy 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: 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.

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.

Primary References

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

Jackson, S., & Ferris, T. (2013). "Resilience Principles for Engineered Systems." *Systems Engineering*, 16(2): 152-164.

Jackson, S., S.C. Cook, and T. Ferris, T. "Towards a Method to Describe Resilience to Assist in System Specification." Proceedings of the INCOSE International Symposium.

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: https://9-11commission.gov/report//

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: https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

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: 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: https://onlinelibrary.wiley.com/doi/10.1002/inst.12003

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 Organisational Accidents.* Aldershot, UK: Ashgate Publishing Limited.

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

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. 2.6, released 20 May 2022
