# A Framework for Viewing Quality Attributes from the Lens of Loss





***Lead Author:*** *John S. Brtis*

Important but often under-considered areas of systems engineering address potential losses associated with the development and use of systems. These areas fall under the umbrella category of loss-driven systems engineering (LDSE), i.e., the value-adding unification of the systems engineering specialty areas that address the potential losses associated with systems. LDSE can be defined as an overarching systems engineering process which holistically addresses the quality characteristics concerned with loss (such as system resilience, system safety, and system security).

□

## Contents

# Overview

Systems engineering methodologies often focus on the delivery of desired capability. Methodology sources such as the Systems Engineering Handbook (Walden 2015) and ISO/IEC/IEEE 15288 (ISO) provide full lifecycle and fully integrated methodologies that focus on the generation and deployment of a system to deliver capabilities. Those methodologies are largely capability-driven and do not provide detailed fully integrated attention to potential loss. Loss and loss-driven specialty areas are largely treated in isolation. Examples of loss-driven specialty areas include resilience, safety, security, operational risk, environmental protection, quality, and availability. There is commonality and synergy among these specialty areas, which should be addressed by systems engineering. Potential synergies include:

- Shared loss scenarios
- Shared requirements
- Shared modeling and analysis techniques
- Shared architecture and design solutions
- Shared risk management

The expected benefits of applying a unified loss-driven viewpoint in the systems engineering processes include:

- Reducing engineering effort by eliminating redundant efforts among the specialty areas
- Helping to ensure a comprehensive consideration of loss
- Ensuring cohesion and elimination of conflicts among the loss-driven solutions
- Identifying highly effective solutions that address the interests of multiple loss-driven specialty areas
- Providing a holistic viewpoint addressing the multiple perspectives
- Reducing the load of data generated by multiple

specialty areas to a minimal, non-redundant set
- Mutual learning among the loss-driven specialty areas

## Background and Origins

Engineers at the MITRE Corporation explored the commonality of "protecting against loss" in the areas of security, safety, and resilience as part of an effort to improve a sponsor's systems engineering methodologies (Brtis 2020). In parallel, these engineers raised and explored the issue with the INCOSE resilience and security working groups. This led to the realization that these specialty areas had commonalities and synergies with many of the systems engineering specialty areas. The term "loss-driven systems engineering" was coined to identify this area of common interest. These concepts were discussed with the INCOSE Technical Operations Director at the 17th INCOSE International Symposium, and he recommended that the concept be pursued as an INCOSE initiative. An exploratory meeting on LDSE was held at the 18th INCOSE International Symposium. At that meeting participants agreed that this concept should be pursued and decided that as a first step, a special theme issue on loss-driven systems engineering of INCOSE *Insight* magazine should be pursued, to be followed by a section in the SEBoK. That issue of *Insight* was published in December 2021.

## The Basis of Commonality

Systems engineering must address all loss-driven specialty areas in a mutually supportive and optimized manner. The exact definitions and demarcation between the different specialty areas are moot. What matters is meeting all the objectives of the loss-driven areas. Loss-driven areas often have common objectives, common concepts and principles, common requirements, common architectural solutions, common design solutions, common analyses, and common methodologies. Engineers responsible for loss-driven areas can often do a better job if they work collaboratively. This is because they are all interested in the same overarching concern: addressing potential losses associated with the system of interest. An inspection of the Systems Engineering Handbook (Walden 2015) identified specialty engineering areas that shared the concerns of loss-driven systems engineering. Those identified include:

- availability

- environmental impact
- maintainability
- resilience engineering
- reliability
- risk management
- system safety engineering
- system security engineering
- quality management

## Attributes Shared by the Loss-Driven Specialty Areas, a Potential for Unification

The loss-driven specialty areas share attributes that specify the scope of each specialty area. All the loss-driven specialty areas have as attributes:

- the types of assets considered
- the types of loss addressed
- the types of adversity addressed
- the coping strategies considered
- the aspects of the system and its environment under consideration

These attributes define the scope of each specialty area. These scopes differ among the loss-driven specialty areas, but in many cases, they overlap. These loss-driven attributes and the possibility of aggregating their overall values provide a basis for integrating the loss-driven specialty areas, by aggregating the range of values of the parameters and then by addressing their aggregate scopes. Brtis (2020) considers each of these attributes. Figure 1 provides an aggregate summary of the scope of considerations identified for loss-driven attributes. Properly engineering a system requires consideration of the full range of each of the loss-driven attributes.

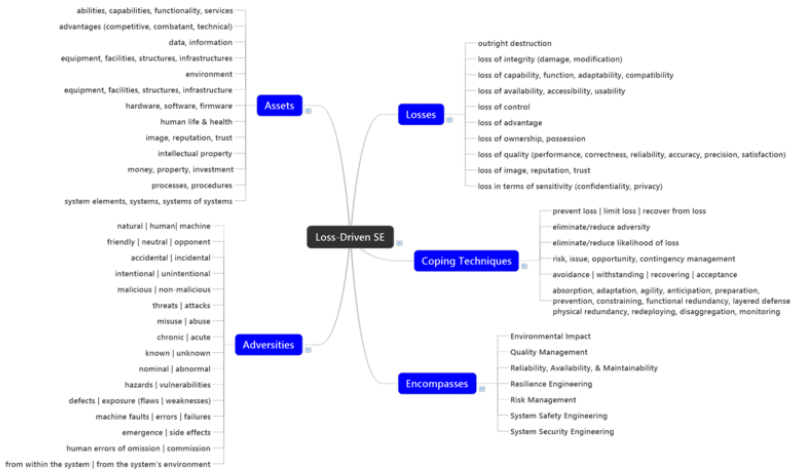


**Figure 1: Attributes and Scope of the Integrated Loss-Driven Systems Engineering Problem Space**

# Core Principles for LDSE

Winstead (2020) investigated the commonality among principles being articulated for individual loss-driven specialty areas. He identified fundamental principles that can be unified across the specialties.

- Candidate principle 1: Systems engineering minimizes hazards.
- Candidate principle 2: Systems engineering seeks to control hazards that cannot be avoided, including assuring transitions from one known acceptable mode or state to another known and acceptable one.
- Candidate principle 3: Systems engineering uses proven and accepted processes, solutions, methods, materials, etc. when the process, etc., achieves the intended trustworthiness.
- Candidate principle 4: The human within the system should be enabled to prevent, minimize, and recover from loss when possible.
- Candidate principle 5: Systems engineering should strive for the simplest solutions.
- Candidate principle 6: Systems engineering produces evolvable systems likely to maintain or improve on loss-driven properties through change.
- Candidate principle 7: Actions should trace to the entity responsible.
- Candidate principle 8: Any critical task should be

possible to perform in more than one way.

Winstead (2020) also considered the systems engineering principles of Watson (2019) and discusses minimal changes needed to make them well-suited for application to loss-driven systems engineering.

## LDSE in the SE Activities

Brtis (2020) found that several the SE practices identified in ISO 15288 and the INCOSE SE Handbook need to be augmented to adequately address the needs of LDSE and recommended specific additions for the following practice areas:

- Business or Mission Analysis Process
- Stakeholder Needs and Requirements Definition Process
- System Requirements Definition Process
- Architecture Definition Process
- Design Definition Process
- Risk Management Process

## LDSE Design Techniques

Winstead (2021) investigates what he calls “loss control” for cyber-physical systems. He investigates loss control independent of any particular systems engineering specialty area. He recommends a set of loss control design principles:

- ***Anomaly Detection*** - Any salient anomaly in the system or in its environment is detected in a timely manner that enables effective response action.
- ***Commensurate Protection*** - The strength and type of protection provided to an element must be commensurate with the most significant adverse effect that results from a failure of that element.
- ***Commensurate Response*** - The design should match the aggressiveness of an engineered response action’s effect to the needed immediacy to control the effects of each loss scenario.
- ***Continuous Protection*** - The protection provided for an element must be effective and uninterrupted during the time that the protection is required.
- ***Defense-in-depth*** - Loss is prevented or minimized

by employing multiple coordinated techniques and strategies.

- ***Distributed Privilege*** - Multiple authorized entities must act in a coordinated manner before an operation on the system is allowed to occur.
- ***Diversity (Dynamicity)*** - The design delivers the required capability through structural, behavioral, data, or control flow variation.
- ***Domain Separation*** - Domains with distinctly different protection needs should be physically or logically separated.
- ***Least Functionality*** - Each element should have the capability to accomplish its required functions, but no more.
- ***Least Persistence*** - System elements and other resources should be available, accessible, and able to fulfill their design intent only for the time they are needed.
- ***Least Privilege*** - Each element should be allocated privileges that are necessary to accomplish its specified functions, but no more.
- ***Least Sharing*** - System resources should be shared among system elements only when necessary, and among as few system elements as possible.
- ***Loss Margins*** - The system is designed to operate in a state space sufficiently distanced below the threshold at which loss occurs.
- ***Mediated Access*** - All access to and operations on system elements are mediated.
- ***Protective Defaults*** - The default configuration of the system provides maximum protection effectiveness.
- ***Protective Failure*** - A failure of a system element should neither result in an unacceptable loss, nor invoke another loss scenario.
- ***Protective Recovery*** - The recovery of a system element should not result in, nor lead to, unacceptable loss.
- ***Redundancy*** - The design delivers the required capability by the replication of functions or elements.

# Technical Management

## Considerations

The effective coordination and management of LDSE specialty areas – areas that have often operated independently and in isolation of one another – poses a challenge. Jackson (2020) discusses the concept of siloism in the context of LDSE projects and ways to mitigate that effect. Siloism is the unwillingness of members of any team to share information. Failure to mitigate siloism can reduce the effectiveness of the entire team. Jackson recommends mitigating siloism using integrated product teams (IPTs), which utilize organizational structure and rigorous management to encourage sharing of information among specialties. Brtis (2021) suggests that for LDSE the systems engineer should holistically consider:

- the full spectrum of adversities
- the full spectrum of weaknesses, defects, flaws, exposures, hazards, and vulnerabilities
- the full spectrum of assets and losses
- the full spectrum of timeframes of interest
- the full spectrum of coping mechanisms

and further, suggests the systems engineer:

- elicit, analyze, and capture loss-driven requirements as part of the overall stakeholder and system requirements development
- make the loss-driven architectural decisions holistically across the loss-driven specialty areas
- make the loss-driven design decisions holistically across the loss-driven specialty areas
- integrate the management of risks associated with all loss-driven areas

Endler (2021) considers real life integration of loss-driven systems engineering activities into system development activities. Challenges identified include lack of appreciation of the importance of loss-driven systems engineering activities and organizational barriers. He finds that existing systems engineering standards poorly describe loss-driven systems engineering activities and fail to integrate loss-drive activities with traditional engineering activities. He proposes methods to overcome those barriers based on widely accepted standards. He offers an approach to accomplish the needed integration with emphasis on the

need that loss-driven systems engineers participate throughout the system life cycle and be supported by a common understanding of an integrated approach.

# Consequences for Model-Based Systems Engineering

Model-based systems engineering data and models need to be augmented to address the shared attributes of loss-driven systems engineering: assets, losses, adversities, and coping techniques and the common information artifacts identified above. Table 1 identifies some of the additional modeling information (in SysML form) that needs to be captured during the various lifecycle stages to support the effective development and documentation of loss management scenarios and loss management requirements.

**Table 1. Modeling Information and Artifacts During Lifecycle Phases (Brtis 2020)**

| Lifecycle Phase | Artifacts and Information |
|---|---|
| Mission and Stakeholder Needs Analysis | Add adversities to the context diagram as actors<br>• Add loss management scenarios as use cases |
| Stakeholder Requirements | Develop use case interaction diagrams to document the interaction of actors and architectural modules during the loss management scenarios<br>• Develop sequence diagrams to represent the activity flow during loss management scenarios |
| System Requirements | Develop activity diagrams to show the states of the system (and adversities) during loss management scenarios |
| Architecture and System Design | Develop state models of the loss management scenarios<br>• Model events and signals among the architectural nodes |
| System Design | Propose and select loss management design features<br>• Document loss management related object distribution |

# Use Case: Manned Space Rescue Vehicle

Cureton (2020) explores the applicability of LDSE to a

use case, a hypothetical manned space rescue vehicle, via a thought experiment regarding desirable characteristics for achieving resilience, safety, reliability, security, and other loss-driven goals. Various design reference missions are explored for assessment of required loss-driven capabilities in automated flight operations for a hypothetical manned space rescue vehicle.

# Summary

Loss-driven systems engineering offers a valuable unification of loss-driven systems engineering specialty areas. Applying this can integrate currently isolated systems engineering activities, leading to improved system effectiveness and reduced systems engineering costs, while improving the management of potential losses associated with the development and use of systems.

# References

## Works Cited


Cureton, K.L. 2020. “Role of LDSE for a Hypothetical Manned Space Rescue Vehicle.” *INCOSE INSIGHT*, December 19-21.

Brtis, J.S. and M.A. McEvilley. 2019. “Systems Engineering for Resilience,” MITRE Technical Document #190495, The MITRE Corporation. Accessed May 25, 2023. Available at https://www.researchgate.net/publication/334549424_Systems_Engineering_for_Resilience.

Endler, D. 2020. “Integrating Loss-Driven Systems Engineering Activities.” *INCOSE INSIGHT*, December 14-18.

ISO (International Organization for Standardization. 2015. ISO/IEC/IEEE 15288:2015. Systems and software engineering – System life cycle processes. Geneva, CH: ISO.

Jackson, S. 2020. “Loss-Driven Systems Engineering and Siloism.” *INCOSE INSIGHT,* December 32-33.

Watson, Michael D. 2019. "Systems Engineering Principles and Hypotheses." *INCOSE INSIGHT,* May 18-28.

Winstead, M., D. Hild, M. McEvilley, 2021. “Principles of Trustworthy Design of Cyber-Physical Systems.” MITRE Technical Report #210263, The MITRE Corporation, June 2021. Accessed May 25, 2023. Available at https://www.researchgate.net/publication/353934929_Principles_for_Trustworthy_Design_of_Cyber-Physical_Systems_Acknowledgments.

## Primary References

Brtis, J. S. and M. A. McEvilley 2020. “Unifying Loss-Driven Systems Engineering Activities.” *INCOSE INSIGHT*, December 9-13. Accessed May 25, 2023. Available at https://www.researchgate.net/publication/348502815_Unifying_Loss-Driven_Systems_Engineering_Activities.

Walden, D. D., et al. 2015. “Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities.” Fourth Edition. San Diego, US-CA: INCOSE.

Winstead, M. 2020. "An Early Attempt at a Core, Common Set of Loss-Driven Systems Engineering Principles.” *INCOSE INSIGHT*, December 22-26. Accessed May 25, 2023. Available at https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/inst.12316.

## Additional References

None.

---

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

---