System Security

Lead Author: Mark Winstead, ***Contributing Authors:*** Terri Chan and Keith Willett

---

Security is freedom from those conditions that may lead to loss of assets (anything of value) with undesired consequences (Ross, Winstead, & McEvilley 2022). Systems Security specifically is concerned with systems delivering capability (an asset) with intended and only intended behaviors and outcomes (no unacceptable consequences such as loss of asset integrity) in contested operational environments (cyberspace or physical).

Restated, Systems Security is about engineering for intended and authorized system behavior and outcomes despite anticipated and unanticipated adversity, conditions that may cause loss (e.g., threats, attacks, hazards, disruptions, exposures). (McEvilley & Winstead 2022)

Note: This is a completely new article inserted in SEBoK 2.9, replacing the previous version by Richard Fairley, Alice Squires, and Keith Willett which originally appeared in SEBoK 1.0 and was periodically updated through SEBoK 2.8.

☐

Contents

Overview

Secure systems ideally have three essential characteristics (Ross, Winstead, & McEvilley 2022):

- Enable required system capability delivery despite intentional and unintentional forms of adversity.
- Enforce constraints to ensure only the desired behaviors and outcomes associated with the required capability are realized while realizing the first characteristic.
- Enforce constraints based on a set of rules defining the only authorized interactions and operations allowed to occur while satisfying the second characteristic.

Desired behaviors and outcomes are those reflecting the delivery of the desired system capabilities and features without experiencing loss with undesired consequences, such as loss of information privacy.

While these characteristics are to be achieved to the extent practicable, gaps will occur between the ideal and what can be dependably achieved. A system should be as secure as reasonably practical (ASARP) while meeting minimum stakeholder expectations for security and optimized among other performance objectives and constraints, informed by the principle of commensurate trustworthiness – trustworthy to a level commensurate with the most significant adverse effect resulting from loss or failure. (Hild, McEvilley, & Winstead 2021)

Secure systems ideally have three essential

characteristics (Ross, Winstead, & McEvilley 2022):

- Enable required system capability delivery despite intentional and unintentional forms of adversity.
- Enforce constraints to ensure only the desired behaviors and outcomes associated with the required capability are realized while realizing the first characteristic.
- Enforce constraints based on a set of rules defining the only authorized interactions and operations allowed to occur while satisfying the second characteristic.

Desired behaviors and outcomes are those reflecting delivery of the desired system capabilities and features without experiencing loss with undesired consequences, such as loss of information privacy.

While these characteristics are to be achieved to the extent practicable, gaps will occur between the ideal and what can be dependably achieved. A system should be as secure as reasonably practical (ASARP) while meeting minimum stakeholder expectations for security and optimized among other performance objectives and constraints, informed by the principle of commensurate trustworthiness – trustworthy to a level commensurate with the most significant adverse effect resulting from loss or failure. (Hild, McEvilley, & Winstead 2021)

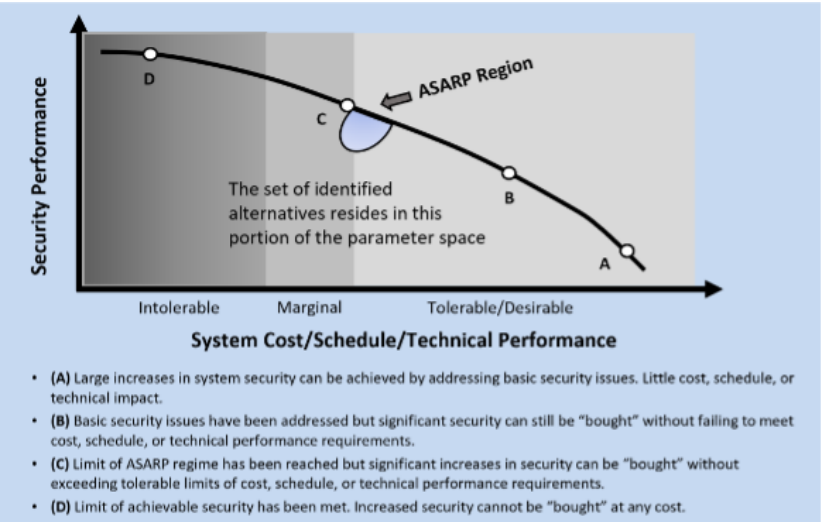

Figure 1. System Security and Cost/Schedule/other Performance (Ross, Winstead, & McEvilley, 2022 - Public Domain)

To understand the optimization of security among other performance objectives, stakeholders need to be aligned and respectful of each other's needs. As loss and loss effects or consequences are easily understood, a collaborative understanding of loss tolerances provides a

means to alignment as well as forms a basis for metrics across the system lifecycle. (Dove, et al. 2023)

Why Security?

Security, one of 10 acknowledged areas of growing stakeholder expectations in INCOSE's Systems Engineering Vision 2035, is recognized as needed to become a foundational perspective for system design. (INCOSE 2021) This growing expectation is motivated by increasing cyberspace-based attacks as evidenced by reports such as Security Magazine's report for computers with Internet access, an attack occurred every 39 seconds in 2017 and has increased since (Security 2017) by observations from the conflict in Ukraine (Carnegie Endowment for International Peace 2023) including attacks on civilian targets such as critical infrastructure, and many well-publicized exploited vulnerable systems. (Agile IT 2023)

Scope

Adversity, conditions that can cause a loss of assets (e.g., threats, attacks, vulnerabilities, hazards, disruptions, and exposures), occurs throughout the system lifecycle. Such conditions are internal and external to the system, with internal conditions often the result of faults and defects (e.g., missing requirements, implementation errors). Consequently, system security's scope matches systems engineering's scope, and every systems engineering process and activity has security considerations. (Ross, Winstead, & McEvilley 2022)

"Unless security is [engineered] into a system from its inception, there is little chance that it can be made secure by retrofit". (Anderson 1972) Consequently, security must be a foundational perspective from concept exploration.

Assets

An asset is an item of value to a stakeholder. Ross, Winstead, & McEvilley (2022) identified broad asset classes, summarized in Table 1.

Table 1. Common Asset Classes (Ross, Winstead, and McEvilley, 2022 - Public Domain)

Class	Description	Loss Protection Criteria

Material Resources and Infrastructure	Includes • physical property (e.g., buildings, facilities, equipment) • physical resources (e.g., water, fuel). • basic physical and organizational structures and facilities (i.e., infrastructure) needed for an activity or the operation of an enterprise or society. An infrastructure commonly comprised of assets, such as a nation's national airspace infrastructure, which includes the nation's airports	*Material resources* are protected from loss if they are not stolen, damaged, or destroyed or are able to function or be used as intended, as needed, and when needed. *Infrastructure* is protected from loss if it meets performance expectations while delivering only the authorized and intended capability and producing only the authorized and intended outcomes
System Capability	The set of capabilities and services provided by a system	*System capability* is protected from loss when it meets its performance expectations while delivering only the authorized and intended capability and producing only the authorized and intended outcomes.
Human Resources	Personnel who are part of the system and personnel affected by the system	*Human resources* are protected from loss if they are not injured, suffer illness, or killed.
Intellectual Property	Trade secrets, recipes, technology, and other items that constitute an advantage over competitors	*Intellectual property* is protected from loss if it is not stolen, corrupted, destroyed, copied, substituted in an unauthorized manner, or reverse-engineered in an unauthorized manner.

Data and Information	Includes all types of data and information and all encodings and representations of data and information	*Data and information* are protected from loss due to unauthorized alteration, exfiltration, infiltration, and destruction.
Derivative Non-Tangible	Includes image, reputation, and trust. Such assets are affected by the success or failure to protect other assets	*Non-tangible assets* are protected from loss by ensuring the adequate protection of assets in the other classes.

Systems Thinking

Systems thinking is the practice of thinking holistically about systems: relating systems behaviors and concepts to principles based on patterns. It is flexible, conceptual, and strategic in nature: hence generally adapted in systems architecture work. Systems thinking focuses not on immediate cause and effect, but also examines the dynamics of a system to identify secondary effects on behaviors and choices. (Goodman 2018)

Security, especially cybersecurity, has suffered from being treated as a tactics problem, focusing on threat defense and incident response. Security has also become a forensics exercise, steeped in root cause analysis, to add to the known threat defense. Systems thinking realizes the greater objective is assuring a systems' ability to produce the capability (functions and services) that users depend on the system for and contributing to business and mission needs and produce that capability in an acceptable manner (i.e., no harm to stakeholder assets). The need is to focus less on efforts to defend against adversarial action beyond the control of the systems engineer and more on assuring the system performs and protects stakeholder assets, controlling the system from effects of loss, to include avoiding vulnerability that leads to loss when practical. (Young & Leveson 2013) Systems thinking brings security back into the conceptual, design, and implementation of systems capabilities.

Consequently, the need is to focus on a system's trustworthiness rather than singularly focus on risk. (Dove, et al. 2021) Quality evidence such as that generated by verification and validation activities feed assurance arguments that merit trustworthiness, providing a basis for trust by stakeholders. Without such

assurance, security functionality is a form of veneer security (Saydjari 2018), providing an unmerited sense of trustworthiness.

Loss

Loss, the experience of having an asset taken away or destroyed or the failure to keep or to continue to have an asset in a desired state or form (Ross, Winstead, & McEvilley 2022), provides language understood by all stakeholders (Dove, et al. 2023). Stakeholder concern is typically the effects of loss caused by adversity, not the adversity itself, and their priorities driven by consequences (e.g., impact to mission). Their needs and requirements can thus be expressed in terms of loss, loss scenarios, loss tolerance, and acceptable loss.

Addressing loss must consider loss results from combinations of adverse events or conditions that cause or lead to unacceptable ramifications, consequences, or impacts. Due to uncertainty (including uncertainty about adversity), guaranteeing a loss will not occur is not possible. The focus must be on controlling loss effects, including cascading or ripple events; e.g., the effect causes additional losses to occur. (Ross, Winstead, & McEvilley 2022)

Loss control objectives frame addressing loss. Loss can be addressed by use of historically-informed practices (known good things to do) and assessing specific loss scenarios for opportunities to address conditions and the potential loss itself.

Table 2. Los Control Objectives (Ross, Winstead, and McEvilley, 2022 - Public Domain)

Loss Control Objective	Discussion

Prevent the Loss from Occurring	*Loss is avoided. Despite the presence of adversity: • ◦ The system provides only the intended behavior and produces only the intended outcomes. ◦ Desired properties of the system and assets are retained. • Achieved by combinations of: ◦ Preventing or removing the event or events that cause the loss ◦ Preventing or removing the condition or conditions that allow the loss to occur ◦ Not suffering an adverse effect despite the events or conditions (e.g., fault tolerance)
Limit the Extent of Loss	*Loss can or has occurred. The loss effect extent is to be limited. • Achieved by combinations of: ◦ Limiting dispersion (e.g., propagation, ripple, or cascading effects) ◦ Limiting duration (e.g., milliseconds, minutes, days) ◦ Limiting capacity (e.g., diminished service or capability) ◦ Limiting volume (e.g., bits or bytes of data/information) • Decisions to limit loss extent may require prioritizing what constitutes acceptable loss across a set of losses (i.e., limiting the loss of one asset requires accepting loss of some other asset). • Loss recovery and loss delay are two means to limit loss: ◦ Loss Recovery: Action is taken by the system or enabled by the system to recover (or allow the recovery of) some or all its ability to function and to recover assets used by the system. Asset restoration can limit the dispersion, duration, capacity, or volume of the loss. ◦ Loss Delay: The loss event is avoided until the adverse effect is lessened or when a delay enables a more robust response or quicker recovery.

Loss Scenarios

Loss scenarios describe the events and conditions that lead to unacceptable outcomes. These scenarios do not necessarily lead back to “root causes” in each case, but must capture the internal system (e.g., system states, internal faults) and the external environmental conditions (e.g., loss of power, presence of malicious

insider threat) that may lead to a loss, including unauthorized system use (e.g., loss of control). See Figure 2.

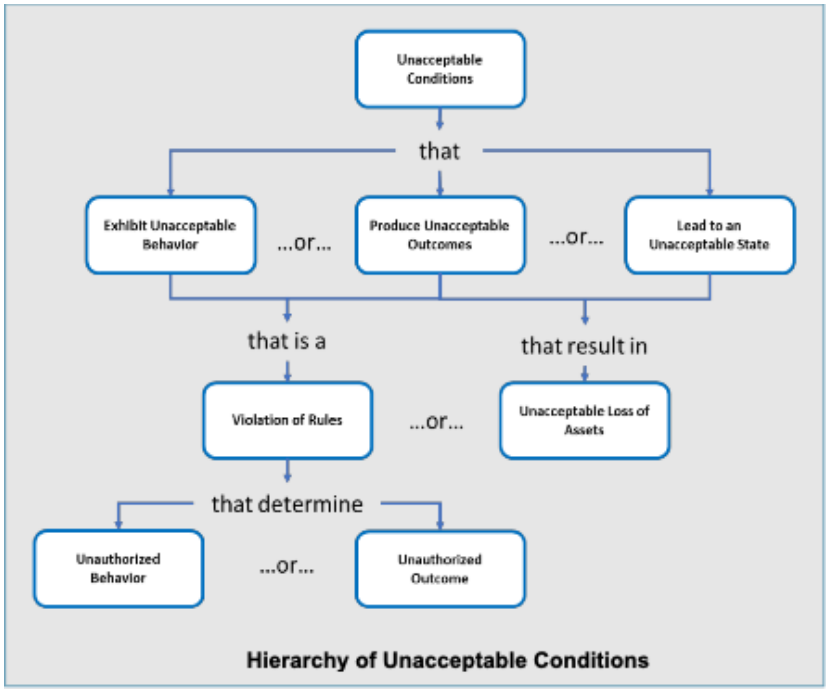

Figure 2. Hierarchy of Unacceptable Conditions (OUSD(R&E) 2022 - Public Domain)

Loss scenarios may be analyzed to inform requirements definition and derivation and analyze design alternatives, as well as inform tailoring of historically-informed practice usage.

Enterprise Relationships

Most systems are part of a larger system of systems or enterprises. Adversity often comes through or from these connected systems.

Systems engineering must balance a system's self-protection capability with opportunities for mutual collaborative protection (Dove, et al. 2021) with trustworthy systems within an enterprise. Enterprises may have dedicated systems for protection, often within network operations and security centers (NOSCs). (Knerler, Parker, & Zimmerman 2022) Systems may also collaborate by sharing situational awareness, with one system alerting others of suspicious activity that may indicate malicious actions others may experience.

Discipline Relationships

Systems Security has commonality and synergy with

many other disciplines, such as safety; quality management; reliability, availability, and maintenance (RAM); survivability; operational risk management; and resilience. Overlapping concerns exist with assets, losses, and adversities considered; requirements; and various engineering processes and analyses similarities and opportunities; e.g., System Theoretic Process Analysis, or STPA (Young & Leveson 2013). Some considerations for pursuing these commonalities and synergies were explored in Brtis (2020).

Personnel Considerations

Systems security engineering is a sub-discipline of systems engineering, defined in Ross, Winstead, & McEvilley (2022) as a transdisciplinary and integrative approach to enable the successful secure realization, use, and retirement of engineered systems using systems, security, and other principles and concepts, as well as scientific, technological, and management methods. Systems security engineers are part of the systems engineering teams.

But as security is demonstrated in a system's behaviors and outcomes, systems engineering responsibility, the systems engineer is ultimately responsible for a system's security. (Thomas 2013) However, reflecting the maxim "Security is everyone's job", all engineering disciplines have security responsibilities (Dove, et al. 2021), not just the systems engineer and various specialists in areas like supply chain assurance, hardware assurance, software assurance, cybersecurity, and physical security.

Security in the Future of Systems Engineering

The INCOSE SE Vision 2035 sets an aim that security "will be as foundational a perspective in systems design as system performance and safety are today". (INCOSE 2021) To that end and other aims for security within the Vision, the INCOSE Systems Security Engineering Working Group has set objectives and roadmap concepts (Dove 2022).

Roadmap Concept	General Needs to Fill
Security Proficiency in the Systems Engineering Team	System security and its evolution effectively enabled by systems engineering activity.

Education and Competency Development	Education at all levels focused on security of cyber-physical systems.
Stakeholder Alignment	Common security vision and knowledge among all stakeholders.
Loss-Driven Engineering	Standard metrics and abstractions relevant to all system lifecycle phases.
Architectural Agility	Readily composable and re-composable security with feature variants.
Operational Agility	Ability for cyber-relevant response to attack and potential threat; resilience in security system.
Capability-Based Security Engineering	Top-down approach to security starting with desired results/value.
Security as a Functional Requirement	Systems engineering responsibility for the security of systems.
Modeled Trustworthiness	Reinvigorate formal modeling of system trust as a core aspect of system security engineering; address issues of scale with model-based tools and automation.
Security Orchestration	Tightly coupled coordinated system defense in cyber-relevant time.
Collaborative Mutual Protection	Augmented detection and mitigation of known and unknown attacks with components collaborating for mutual protection.

Challenges

The challenging problems for system security are numerous. Some of this is a result of neglecting the addressing of security early in the system life cycle as recognized by the Systems Engineering Vision call for security to be a foundational perspective – as Carl Landwehr wrote “This whole economic boom in [security] seems largely to be a consequence of poor engineering” (Landwehr 2015).

For example, system of systems engineering security faces challenges in part to not knowing or trusting the component systems which may not have been engineered with security in mind, or at least did not consider documenting the evidence that informs trustworthiness. Another system of systems challenge comes as formerly isolated cyber-physical systems (CPSs) are increasingly connected to form larger system of systems, negating assumptions impacting security if security was considered at all. Additionally, legacy CPSs

were not built thinking of the need to update the software; i.e. use sustainable security (Rosser 2023)), which creates a challenge in upgrading software to reflect revised assumptions and security models for the CPS in question.

Another challenge comes with the advancing use of Artificial Intelligence (AI). Any new technology presents security challenges until its usage matures, but AI introduces complexity and decreases predictability (INCOSE 2021). Managing complexity and uncertainty is necessary for security (Ross, Winstead, & McEvilley 2022), and AI increasing of both compounds the problem space for systems engineering security.

References

Works Cited

Agile IT. n.d.. The Top 10 Biggest Cyberattacks of 2022. Accessed September 15, 2023. Available at https://www.agileit.com/news/biggest-cyberattacks-2022/.

Anderson, J. 1972. Computer Security Technology Planning Study, Technical Report ESD-TR-73-51. October 1, 1972. Hanscom AFB: Air Force Electronic Systems Division. Accessed September 15, 2023. Available at https://apps.dtic.mil/sti/citations/AD0758206.

Brtis, J. (ed). 2020. Loss-Driven Systems Engineering. INCOSE Insight, 23(4):7-8. Wiley. Accessed September 15, 2023. Available at https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/inst.12312.

Carnegie Endowment for International Peace. n.d.. Cyber Conflict in the Russia-Ukraine War. Accessed September 15, 2023. Available at https://carnegieendowment.org/programs/technology/cyberconflictintherussiaukrainewar/.

Dove, R. 2022. “Setting Current Context for Security in the Future of Systems Engineering”. INCOSE Insight, 25(2):8-10.

Dove, R., K. Willett, T. McDermott, H. Dunlap, H, D.P. MacNamara, and C. Ocker. 2021. “Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts”. Proceedings of the 31st

INCOSE International Symposium, July 17-22. Virtual only,

Dove, R., M. Winstead, H. Dunlap, M. Hause, A. Scalco, A. Scalco, A. Williams, and B. Wilson. 2023. “Democratizing Systems Security”. Proceedings of the 33rd INCOSE International Symposium. July 15-20. Honolulu, Hawaii: Wiley.

Goodman, M. 2018. Systems Thinking: What, Why, When, Where, and How? Accessed September 15, 2023. Available at https://thesystemsthinker.com/systems-thinking-what-why-when-where-and-how/

Hild, D., M. McEvilley, and M. Winstead. 2021. Principles for Trustworthy Design of Cyber-Physical Systems. MITRE Technical Report, MTR210263.

INCOSE. 2021. INCOSE Systems Engineering Vision 2035. Accessed September 15, 2023. Available at https://www.incose.org/about-systems-engineering/se-vision-2035

Knerler, K., I. Parker, and C. Zimmerman. 2022. 11 Strategies of a World-Class Cybersecurity Operations Center (2nd ed.). McLean, VA: MITRE. Accessed September 15, 2023. Available at https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Landwehr, C. 2015. “We Need a Building Code for Building Code”. Communcations of the ACM, 58(2):24-26. Accessed September 15, 2023. Available at doi:https://doi.org/10.1145/2700341

McEvilley, M., and M. Winstead. 2022. “Functionally Interpreting Security”. INCOSE Insight, 25(2):15-17. Wiley. Accessed September 15, 2023. Available at https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/inst.12380

OUSD(R&E). 2022. Security and Resilience Interpretation 1.0. Prepared by MITRE. Accessed September 2023. Available at https://www.crws-bok.org/asset/83a0d3528e6e27272a52b7e2c3758facc16773fd

Ross, R., M. Winstead, M., M. McEvilley. 2022. Engineering Trustworthy Secure Systems. NIST SP 800-160 Volume 1 Revision 1. Gaithersburg, MD: NIST. Accessed September 15, 2023. Available at

https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

Rosser, L.A. 2023. “Applying Agility for Sustainable Security”. INCOSE Insight, 26(2):45-52. Wiley. Accessed September 15, 2023. Available at https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/inst.12445

Saydjari, O.S. (ed.). 2018. Engineering Trustworthy Systems: Get Cybersecurity Design Right the First Time. New York: McGraw Hill. Accessed September 15, 2023. Available at https://www.amazon.com/Engineering-Trustworthy-Systems-Cybersecurity-Design/dp/1260118177

Security. 2017. Hackers Attack Every 39 Seconds. Accessed September 15, 2023. Available at https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

Thomas, J.A. 2013. “Critical System Behaviors of The Future”. INCOSE Insight, 16(2):3-5. Wiley.

Young, W. and N. Leveson. 2013. “Systems Thinking for Safety and Security”. Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13), pp. 31-35. Accessed September 15, 2023. Available at https://dspace.mit.edu/handle/1721.1/96965

Primary References

Anderson, R. 2020. Security Engineering: A Guide to Building Dependable Distributed Systems (3rd Edition). Wiley. Accessed September 15, 2023. Available at https://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/1119642787

Neumann P. 2004. Principled Assuredly Trustworthy Composable Architectures, CDRL A001 Final Report, SRI International, Menlo Park, CA. Accessed September 15, 2023. Available at https://ieeexplore.ieee.org/document/1335465

Ross, R., M. Winstead, M., and M. McEvilley. 2022. Engineering Trustworthy Secure Systems. NIST SP 800-160 Volume 1 Revision 1. Gaithersburg, MD: NIST. Accessed September 15, 2023. Available at https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

Additional References

Avizienis A., J. Laprie, B. Randell. and C. Landwehr C. “Basic Concepts and Taxonomy of Dependable and Secure Computing”. IEEE Transactions on Dependable and Secure Computing 1(1):11-33. Accessed September 15, 2023. Available at http://www.csl.sri.com/users/neumann/chats4.pdf

DoD. 1983. DoD Standard 5200.28-STD Trusted Computer System Evaluation Criteria. Accessed September 15, 2023. Available at http://www.csl.sri.com/users/neumann/chats4.pdf

National Security Agency. 2002. Information Assurance Technical Framework (IATF), Release 3.1. Accessed September 15, 2023. Available at https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA606355.xhtml

Schroeder M.D., D.D. Clark, and J.H. Saltzer. 1977. “The Multics Kernel Design Project”. Proceedings of Sixth ACM Symposium on Operating Systems Principles. Accessed September 15, 2023. Available at https://dl.acm.org/doi/pdf/10.1145/800214.806546

Videos

Keith Willett previously authored a series of videos that explain aspects of systems security. They are not referenced in the above article, but remain quite relevant and interesting viewing.

https://sebokwiki.org/wiki/File:Arch_the_Future_of_Security.mp4

Architecture for the Future of Society. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

https://sebokwiki.org/wiki/File:SEBoK_F_Security_Concepts_Part_1.mp4

SEBoK F Security Concepts Part 1. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

https://sebokwiki.org/wiki/File:SEBoK_F_Security_Concepts_Part_2.mp4

SEBoK F Security Concepts Part 2. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

https://sebokwiki.org/wiki/File:SEBoK_L_Sys_Think_Security.mp4

SEBoK L Systems Thinking and Security. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

https://sebokwiki.org/wiki/File:SEBoK_N_Sec_Ops_Workflow.mp4

SEBoK N Security Operations Workflow. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

https://sebokwiki.org/wiki/File:SEBoK_O1_LDSE_Intro.mp4

SEBoK O1 LDSE Intro. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

https://sebokwiki.org/wiki/File:SEBoK_O2_ODSE_Intro.mp4

SEBoK O2 OSDE Intro. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

< Previous Article | Parent Article | Next Article (Part 7) >

SEBoK v. 2.11, released 25 November 2024

This page was last edited on 24 November 2024, at 18:57.