# System Security

From SEBoK
System Security

---

***Lead Author:*** *Dick Fairley,* ***Contributing Authors:*** *Alice Squires, Keith Willett*

---

https://www.sebokwiki.org/wiki/File:SEBoK_A_Intro_to_SEBoK_Video_Series.mp4
Introduction to System Security (INCOSE Systems Security Working Group 2020; Used with Permission of Keith Willett)

Security engineering is concerned with building systems that remain secure despite malice or error. It focuses on the tools, processes, and methods needed to design and implement complete systems that proactively and reactively mitigate vulnerabilities. Security engineering is a primary discipline used to achieve system assurance.

The term System Security Engineering (SSE) is used to denote this specialty engineering field and the US Department of Defense define it as: "*an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities*" (DODI5200.44, 12).

## Contents



## Overview

Security engineering incorporates a number of cross-disciplinary skills, including cryptography, computer security, tamper-resistant hardware, applied psychology, supply chain management, and

law. Security requirements differ greatly from one system to the next. System security often has many layers built on user authentication, transaction accountability, message secrecy, and fault tolerance. The challenges are protecting the right items rather than the wrong items and protecting the right items but not in the wrong way.

Security engineering is an area of increasing emphasis in the defense domain. Baldwin et al. (2012) provide a survey of the issues and a detailed reference list.

https://www.sebokwiki.org/wiki/File:SEBoK_B_Purpose_for_Security.mp4
Purpose of System Security (INCOSE Systems Security Working Group 2020; Used with Permission of Keith Willett)

The purpose of system security is to help assure system value-delivery while undergoing adversity. The primary objective of System Security Engineering (SSE) is to minimize or contain defense system vulnerabilities to known or postulated security threats and to ensure that developed systems protect against these threats. Engineering principles and practices are applied during all system development phases to identify and reduce these system vulnerabilities to the identified system threats.

The basic premise of SSE is recognition that an initial investment in “engineering out” security vulnerabilities and “designing-in” countermeasures is a long-term benefit and cost saving measure. Further, SSE provides a means to ensure adequate consideration of security requirements, and, when appropriate, that specific security-related designs are incorporated into the overall system design during the engineering development program. Security requirements include: physical; personnel; procedural; emission; transmission; cryptographic; communications; operations; and, computer security.

There may be some variation in the SSE process from program to program, due mainly to the level of design assurance—that is, ensuring that appropriate security controls have been implemented correctly as planned—required of the contractor. These assurance requirements are elicited early in the program (where they can be adequately planned), implemented, and verified in due course of the system development.

The System Security Engineering Management Plan (SSEMP) is a key document to develop for SSE. The SSEMP identifies the planned security tasks for the program and the organizations and individuals responsible for security aspects of the system. The goals of the SSEMP are to ensure that pertinent security issues are raised at the appropriate points in the program, to ensure adequate precautions are taken during design, implementation, test, and fielding, and to ensure that only an acceptable level of risk is incurred when the system is released for fielding. The SSEMP forms the basis for an agreement with SSE representing the developer, the government program office, the certifier, the accreditor, and any additional organizations that have a stake in the security of the system. The SSEMP identifies the major tasks for certification & accreditation (C&A), document preparation, system evaluation, and engineering; identifies the responsible organizations for each task; and presents a schedule for the completion of those tasks.

SSE security planning and risk management planning includes task and event planning associated with establishing statements of work and detailed work plans as well as preparation and negotiation of SSE plans with project stakeholders. For each program, SSE provides the System Security Plan (SSP) or equivalent. An initial system security Concept of Operations (CONOPS) may also be developed. The SSP provides: the initial planning of the proposed SSE work scope; detailed descriptions of SSE activities performed throughout the system development life cycle; the operating conditions of the system; the security requirements; the initial SSE risk assessment (includes risks due to known system vulnerabilities and their potential impacts due to compromise and/or data loss); and, the expected verification approach and validation results.

These plans are submitted with the proposal and updated as required during engineering development. In the case where a formal C&A is contracted and implemented, these plans comply with the government's C&A process, certification responsibilities, and other agreement details, as appropriate. The C&A process is the documented agreement between the customer and contractor on the certification boundary. Upon agreement of the stakeholders, these plans guide SSE activities throughout the system development life cycle.

## System Assurance

NATO AEP-67 (Edition 1), Engineering for System Assurance in NATO Programs, defines system assurance as:

> …the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle… This confidence is achieved by system assurance activities, which include a planned, systematic set of multi-disciplinary activities to achieve the acceptable measures of system assurance and manage the risk of exploitable vulnerabilities. (NATO 2010, 1)

The NATO document is organized based on the life cycle processes in ISO/IEC 15288:2008 and provides process and technology guidance to improve system assurance.

https://www.sebokwiki.org/wiki/File:SEBoK_C_Focus_of_Security.mp4
Focus of Security (INCOSE Systems Security Working Group 2020; Used with Permission of Keith Willett)

One may consider a system with respect to what it is (structure), what it does (function), what it contains (contents), what it uses, (inputs, resources), or where it resides (environment). The focus of security (that which we safeguard) may be structure, state, function, functional exchange (input, output), raw materials (access, supply), fuel/energy to run the system, containing whole (system of systems), or the broader current order (ecosystem). System security focus includes but is not limited to harden, defend, protect, maximize use of renewable resources, minimize use of depletable resources, remain compatible with the current order, and remain viable and relevant.

## Software Assurance

Since most modern systems derive a good portion of their functionality from software, software assurance becomes a primary consideration in systems assurance. The Committee on National Security Systems (CNSS) (2010, 69) defines software assurance as a "level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle and that the software functions in the intended manner."

Goertzel, et. al (2008, 8) point out that "the reason software assurance matters is that so many business activities and critical functions—from national defense to banking to healthcare to telecommunications to aviation to control of hazardous materials—depend on the on the correct, predictable operation of software."

## Hardware Assurance

System hardware assurance is a set of system security engineering activities undertaken to quantify and increase the confidence that electronics function as intended and only as intended throughout their life cycle and to manage identified risks. See System Hardware Assurance for more

information.

## System Description

Robust security design explicitly rather than implicitly defines the protection goals. The Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) partitions robust security into ten domains (Tipton 2006):

1. Information security governance and risk management addresses the framework, principles, policies, and standards that establish the criteria and then assess the effectiveness of information protection. Security risk management contains governance issues, organizational behavior, ethics, and security awareness training.
2. Access control is the procedures and mechanisms that enable system administrators to allow or restrict operation and content of a system. Access control policies determine what processes, resources, and operations users can invoke.
3. Cryptography can be defined as the principles and methods of disguising information to ensure its integrity, confidentiality, and authenticity during communications and while in storage. Type I devices are certified by the US National Security Agency (NSA) for classified information processing. Type 2 devices are certified by NSA for proprietary information processing. Type 3 devices are certified by NSA for general information processing. Type 4 devices are produced by industry or other nations without any formal certification.
4. Physical (environmental) security addresses the actual environment configuration, security procedures, countermeasures, and recovery strategies to protect the equipment and its location. These measures include separate processing facilities, restricted access into those facilities, and sweeps to detect eavesdropping devices.
5. Security architecture and design contains the concepts, processes, principles, and standards used to define, design, and implement secure applications, operating systems, networks, and equipment. The security architecture must integrate various levels of confidentiality, integrity, and availability to ensure effective operations and adherence to governance.
6. Business continuity and disaster recovery planning are the preparations and practices which ensure business survival given events, natural or man-made, which cause a major disruption in normal business operations. Processes and specific action plans must be selected to prudently protect business processes and to ensure timely restoration.
7. Telecommunications and network security are the transmission methods and security measures used to provide integrity, availability, and confidentiality of data during transfer over private and public communication networks.
8. Application development security involves the controls applied to application software in a centralized or distributed environment. Application software includes tools, operating systems, data warehouses, and knowledge systems.
9. Operations security is focused on providing system availability for end users while protecting data processing resources both in centralized data processing centers and in distributed client/server environments.
10. Legal, regulations, investigations, and compliance issues include the investigative measures to determine if an incident has occurred and the processes for responding to such incidents.

One response to the complexity and diversity of security needs and domains that contribute to system security is “defense in depth,” a commonly applied architecture and design approach. Defense in depth implements multiple layers of defense and countermeasures, making maximum use of certified equipment in each layer to facilitate system accreditation.

# Discipline Management

https://www.sebokwiki.org/wiki/File:SEBoK_D_Sec_Principles.mp4
Fundamental Security Principles (INCOSE Systems Security Working Group 2020; Used with Permission of Keith Willett)

Discipline management includes the following fundamental security principles (Willettt 2008) with informal descriptions. There are many formal definitions that take on different nuances depending on context; e.g., government-based, international standards, or particular legislation.

| Principle | Description (Positive) | Description (Negative) |
|---|---|---|
| Confidentiality | Ensure only authorized disclosure | Safeguard against unauthorized disclosure |
| Integrity | Ensure only authorized modification | Safeguard against unauthorized modification |
| Availability | Ensure ready for use | Safeguard against denial of service |
| Possession | Ensure physical possession | Safeguard against loss or theft; minimize damage resulting from loss or theft |
| Utility | Ensure *fit for purpose*, or *ready for use* | Safeguard against loss of purpose |
| Authenticity | Ensure system conforms to reality or acts upon information that conforms to reality | Safeguard against deception |
| Privacy | Ensure the right to be unobserved and the right to be forgotten | Safeguard against unwanted observation and persistence of personal details (e.g., photos) |
| Non-Repudiation | Ensure non-deniability | Safeguard against anonymity in performing actions |
| Authorized Use | Ensure only authorized use of services | Safeguard against misuse of cost-incurring (resource expending) activity |

# Security Domains

https://www.sebokwiki.org/wiki/File:SEBoK_E_Security_Domains.mp4
Security Domains (INCOSE Systems Security Working Group 2020; Used with Permission of Keith Willett)

There are many security domains, each of which may have distinct or overlapping disciplines. Some security domains for consideration:

- Orchestration Space guides workflow execution
- Workflow Space fulfills the organizational mission
- Organizational Efficacy is the capacity to fulfill mission
- Safeguards preserve organizational efficacy
- Desired Security Posture is an intentionally assumed position to define applicable safeguards
- Risk Posture is an intentionally assumed position to drive desired security posture
- Mission Risk Tolerance helps define risk posture

- Tolerance for workflow disruption drives mission risk tolerance
- Marketplace Dynamics (ecosystem dynamics) drive mission priorities
- Mission Priorities are non-static and influence mission risk tolerance
- Vulnerability Space contains weaknesses within orchestration and workflow
- Vulnerabilities influence risk posture
- Threat Space contains potential disruptions to workflow
- Compliance Space partially address the threat space
- Compliance drivers influence risk posture
- Continuous Monitoring provides snapshots of current security posture
- Gap Analysis provides difference between desired and current security posture
- Corrective Action provides gap closure within resource constraints
- Resource Constraints: people (skills, knowledge), budget, technology, etc.

A change in any one domain has cascading effects on the other domains. In this sense, they have causal loop or dynamic feedbacks resulting in infinite cycles. An emerging goal is to identify, understand, and act upon domain states and interactions within cyber-relevant time (Herring and Willettt 2014).

**Web-based Resource**

A good online resource for system and software assurance is the US Department of Homeland Security's Build Security In web site (DHS 2010), which provides resources for best practices, knowledge, and tools for engineering secure systems.

# References

## Works Cited


Baldwin, K., J. Miller, P. Popick, and J. Goodnight. 2012. *The United States Department of Defense Revitalization of System Security Engineering Through Program Protection.* Proceedings of the 2012 IEEE Systems Conference, 19-22 March 2012, Vancouver, BC, Canada. Accessed 28 August 2012 at http://www.acq.osd.mil/se/docs/IEEE-SSE-Paper-02152012-Bkmarks.pdf.

CNSS. 2010. *National Information Assurance Glossary", Committee on National Security Systems Instruction (CNSSI) no. 4009". Fort Meade, MD, USA: The Committee on National Security Systems.*

DHS. 2010. *Build Security In.* Washington, DC, USA: US Department of Homeland Security (DHS). Accessed September 11, 2011. Available: https://buildsecurityin.us-cert.gov.

DODI5200.44, United States Department of Defense, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*, Department of Defense Instruction Number 5200.44, November 2012, Accessed 3 November 2014 at Defense Technical Information Center http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf.

Goertzel, K., et al. 2008. *Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance.* Washington, DC, USA: Data and Analysis Center for Software (DACS)/US Department of Homeland Security (DHS).

NATO. 2010. *Engineering for System Assurance in NATO programs.* Washington, DC, USA: NATO Standardization Agency. DoD 5220.22M-NISPOM-NATO-AEP-67.

Tipton, H.F. (ed.). 2006. *Official (ISC)2 guide to the CISSP CBK,* 1st ed. Boston, MA, USA: Auerbach Publications.

## Primary References

Anderson, R.J. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems,* 2nd Ed. New York, NY, USA: John Wiley & Sons. Accessed October 24, 2014 at http://www.cl.cam.ac.uk/~rja14/book.html

DAU. 2012. "Defense Acquisition Guidebook (DAG): Chapter 13 -- Program Protection." Ft. Belvoir, VA, USA: Defense Acquisition University (DAU)/U.S. Department of Defense (DoD). November 8, 2012. Accessed October 24, 2014 at https://dag.dau.mil/

ISO. 2008. "Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)," Second Edition. Geneva, Switzerland: International Organization for Standardization (ISO), ISO/IEC 21827:2008.

ISO/IEC. 2013. "Information technology — Security techniques — Information security management systems — Requirements," Second Edition. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2013.

Kissel, R., K. Stine, M. Scholl, H. Rossman, J. Fahlsing, J. Gulick. 2008. "Security Considerations in the System Development Life Cycle," Revision 2. Gaithersburg, MD. National Institute of Standard and Technology (NIST), NIST 800-64 Revision 2:2008. Accessed October 24, 2014 at the Computer Security Resource Center [1]

Ross, R., J.C. Oren, M. McEvilley. 2014. "Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems." Gaithersburg, MD. National Institute of Standard and Technology (NIST) Special Publication (SP), NIST SP 800-160:2014 (Initial Public Draft). Accessed October 24, 2014 at the Computer Security Resource Center http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

## Additional References

Allen, Julia; Barnum, Sean; Ellison, Robert; McGraw, Gary; and Mead, Nancy. 2008. *Software security engineering: a guide for project managers.* New York, NY, USA: Addison Wesley Professional.

ISO. 2005. *Information technology -- Security techniques -- Code of practice for information security management.* Geneva, Switzerland: International Organization for Standardization (ISO). ISO/IEC 27002:2005.

Jurjens, J. 2005. "Sound Methods and effective tools for model-based security engineering with UML." *Proceedings of the 2005 International Conference on Software Engineering.* Munich, GE: ICSE, 15-21 May.

MITRE. 2012. "Systems Engineering for Mission Assurance." In *Systems Engineering Guide.* Accessed 19 June 2012 at MITRE http://www.mitre.org/work/systems_engineering/guide/enterprise_engineering/se_for_mission_assurance/.

NIST SP 800-160. *Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems*. National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-160. Accessed October 24, 2014 at the Computer Security Resource Center http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf.

## Videos

- https://www.sebokwiki.org/wiki/File:Arch_the_Future_of_Security.mp4Architecture for the Future of Society. By Keith Willett. Used with Permission. Uploaded 17 May 2021.
- https://www.sebokwiki.org/wiki/File:SEBoK_F_Security_Concepts_Part_1.mp4SEBoK F Security

Concepts Part 1. By Keith Willett. Used with Permission. Uploaded 17 May 2021.
- https://www.sebokwiki.org/wiki/File:SEBoK_F_Security_Concepts_Part_2.mp4SEBoK F Security Concepts Part 2. By Keith Willett. Used with Permission. Uploaded 17 May 2021.
- https://www.sebokwiki.org/wiki/File:SEBoK_L_Sys_Think_Security.mp4SEBoK L Systems Thinking and Security. By Keith Willett. Used with Permission. Uploaded 17 May 2021.
- https://www.sebokwiki.org/wiki/File:SEBoK_N_Sec_Ops_Workflow.mp4SEBoK N Security Operations Workflow. By Keith Willett. Used with Permission. Uploaded 17 May 2021.
- https://www.sebokwiki.org/wiki/File:SEBoK_O1_LDSE_Intro.mp4SEBoK O1 LDSE Intro. By Keith Willett. Used with Permission. Uploaded 17 May 2021.
- https://www.sebokwiki.org/wiki/File:SEBoK_O2_ODSE_Intro.mp4SEBoK O2 OSDE Intro. By Keith Willett. Used with Permission. Uploaded 17 May 2021.

---

< Previous Article | Parent Article | Next Article (Part 7) >
**SEBoK v. 2.4, released 19 May 2021**