

WAEPPSSD Working Group 1 Report

A report on the activities of one of two groups formed during the ACSA Workshop on the Application of Engineering Principles to System Security Design. Prepared for the Working Group by Richard K. McAllister, SPARTA Incorporated

Introduction

The WAEPPSSD met November 6-8, 2002 to “*examine engineering fundamentals, the principles and practice of designing and building secure systems*” (Reference: <http://www.acsac.org/waepssd/index.html>). During this meeting two groups were formed, each with a different approach for examining the state of systems security design and its successes and failures. One group followed the theme that security engineers must stress the application of **proven engineering fundamentals** and sought to identify and document the important principles and practices. The other group was formed with the theme that the security engineers must apply a process of **systems engineering** and sought to identify and document the principles and practices of Information Systems Security Engineering (ISSE). This report presents the activities of the systems engineering group.

The systems engineering process discussed contained phases that were similarly defined by the National Institute of Standards and Technology (NIST)¹ and by the National Security Agency (NSA)²:

NIST Life Cycle Phases	NSA ISSE Activities
Initiation	Discover Needs
Development/Acquisition	Define System Requirements
--	Design System Architecture
--	Develop Detailed Design
Implementation	Implement System
Operation/Maintenance	Assess Effectiveness (of other activities)
Disposal	

The group completed discussions on the (1) Initiation <Discover Needs > and (2) Specification <Define System/Design System Architecture> phases of systems engineering and the security engineering principles involved. The following narrative is based on the notes taken during the group sessions. The author’s expansions and opinions are annotated in brackets [].

¹ NIST Special Publication (SP) 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

² *Information Assurance Technical Framework Version 3.1*, Chapter 3, “The Information Systems Security Engineering (ISSE) Process,” NSA, 2002. <http://www.iatf.net>

Information Systems Engineering Activity

Participants contributed the following comments about information systems engineering:

- The definition of “system” and “components” is recursive such that the components of a system may also be considered systems (as subsystems), etc. A systems engineering process should be applicable [with varying complexity] regardless of the scope of the effort. [One reasonable distinction can be made depending on whether or not the subsystems were specifically designed as part of a greater system. An important problem for the systems engineer is often to bring together components that may never have been combined in a system before].
- [Systems] Security engineering is part of systems engineering³. This points to the view that systems engineering is the general skill and that systems security engineering is a specialty practiced by a systems engineer with additional knowledge and experience. [One view is that there is a difference between engineers and systems engineers and correspondingly between security engineers and systems security engineers. The view maintains that the difference is systems engineers are more capable of designing with intuition and abstraction and by depth of experience are confident that the more detailed design can be accomplished successfully.]
- Interfaces and global impact are critical points. [Bringing components together with a clear knowledge and understanding of the intended and resultant relationships between them is a major skill for the systems engineer. The systems engineer must be aware of not only the local impact of interfacing components but must also consider the global effect on the entire system and its intended functionality.]

Two principles were expressed in conjunction with [all] systems engineering phases:

Engineering Principle: Plan each phase. [This expresses the need for systems engineers to plan and coordinate schedules and resources, and to achieve agreement with the customers.]

Engineering Principle: Use qualified personnel: systems engineer, security engineer. [The systems engineer cannot be an expert in all the needed skills but he must know how and where to acquire the skills needed by the ISSE team.]

The Initiation Phase

This phase is first directed toward developing an in-depth understanding of the information and information management functions that support an organization’s business or mission. The second objective is for the ISSE team to assist the customer in identifying the threats to the information and to decide on the protections and their priorities. Failures during this phase result from poor communications with the customer and from defining requirements based on engineering solutions. This leads to the principles expressed as:

³ See NIST SP 800-27, *Engineering Principles for Information Technology Security, Principle 2*, “Treat security as an integral part of the overall system design.”

Engineering Principle: Identify stakeholders maintain direct dialogue.

Engineering Principle: Keep “solution” out of this phase.

Based on the customer’s perceived threats to information, the ISSE team associates the security services needed to counter the threats. The types and strengths of the security services are based on the customer’s priorities for protection.

The results of these efforts must be documented and agreed to by those in authority within the customer’s organization. The ISSE team thereby acquires the documented security requirements for the mission/business and the definition of the protection to be provided. [These requirements are often referred to as the organizational security policy.] Such a policy should include any assumptions and any known laws, regulations, prior policies, treaties, and agreements with other organizations. It is good practice to identify in such documents who will be responsible for the Certification (security effectiveness) and Accreditation (operational acceptance) of any solutions to the requirements, and any other resources necessary to support, maintain, and enforce the policy. The principles expressed were:

Engineering Principle⁴: Establish written record to get agreement document decisions. Use set of documents of successive refinement or abstraction. Expect revision.

Engineering Principle: Iterate to achieve completeness, consistency, and correctness sufficient to develop solution sets. Accept deviations.

The systems engineering process so far has only discussed information management, information threats, and policies. There is no definition of a solution in the form of systems or security architectures to be analyzed but it is important to begin including those who would evaluate solutions in the understanding of the problem to be solved. For this phase and other phases for similar reasons, the involvement of evaluators is needed. Hence:

Engineering Principle: Submit to independent security engineering analysis at end of each phase.

⁴ See NIST SP 800-27, *Engineering Principles for Information Technology Security, Principle 1*, “Establish a sound security policy as the foundation.”

Development of Specifications Phase

The discussion on the Specifications Phase <Design System Architecture> was preceded by a terminology presentation on “requirements.” Each phase was characterized as placing requirements on lower phases in the hierarchy of a systems engineering process. See Figure 1.

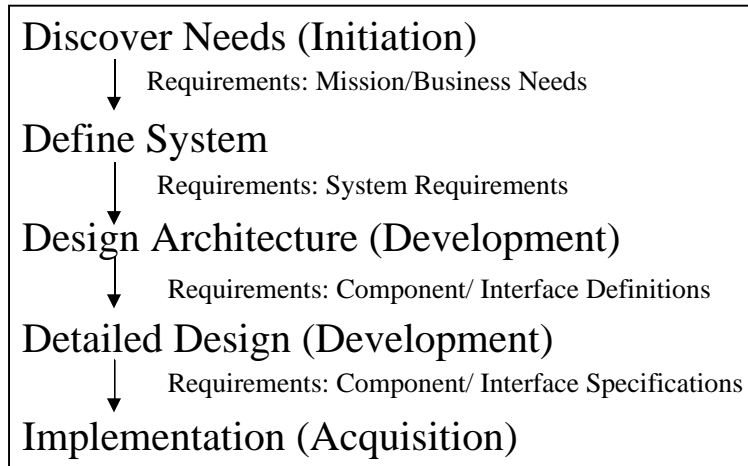


Figure 1. Systems Engineering Process Hierarchy

Requirements have different names and are more detailed (less abstract) in lower phases. [Objections usually arise here to top-down design. There is nothing in the hierarchy that imposes order but only a normal flow of requirements. Where the systems engineer begins the process predetermines the expected quality of the results, and each phase can be visited at any time with the associated cost and schedule impacts]. An important principle was discussed in this context:

Engineering Principle⁵: Do not change requirements because you find you can or can't do something. Identify unsatisfied requirements.

The importance of this principle is that while requirements may have varying priorities, they should never be deleted. They should be documented as not having been met. The loss of a requirement means there will be no trace should technological advances make the solution possible. They should also be retained as a requirements base for new technology. [The push to delete requirements is an artifact of contracting where a vendor doesn't want to be penalized for not meeting the terms of the contract. The systems engineer has the opportunity to discuss requirements at each phase and to document, with customer agreement, any discontinuance of a requirement trace.] A minority opinion was expressed in the group:

Minority Opinion: Modify mission or requirements. Redefine scope. [Previous comments apply.]

⁵ See NIST SP 800-27, *Engineering Principles for Information Technology Security*, Principle 6, “Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.”

No new principles were identified but all of the principles of the Initiation phase are similarly applicable to this and all other phases of the process.

- **Plan each phase.**
- **Use qualified personnel: systems engineer, security engineer.**
- **Identify stakeholders and maintain direct dialogue.**
- **Keep “solution” out of this phase [requirements, not solutions, drive lower phases].**
- **Establish written record to get agreement document decisions. Use set of documents of successive refinement or abstraction. Expect revision.**
- **Iterate to achieve completeness, consistency, and correctness sufficient to develop solution sets. Accept deviations.**
- **Submit to independent security engineering analysis at end of each phase.**

Although not recorded as a principle, the concept that systems security engineering was an integral part of systems engineering was restated several times.

The remaining discussion of this phase included a series of steps in accomplishing the system (security) architecture:

- Define one or more solution sets [each with different allocations to existing and to-be-developed target systems].
- Allocate (security) requirements to (new and existing) solution set components.
- Identify (security) requirements allocated to “target” systems [security requirements are mainly the required security services located where needed].
- Avoid negative security impact on pre-existing environment.
- Develop series of documents as refinement and increased specificity.
- Develop architecture(s) expressing alternative solution set(s).
- Provide recommendations to management. [with associated security trade-offs].
- Develop system specifications from system requirements.
- Allocate functions to subsystems [types of security mechanisms].
- Perform dependency analysis [estimate the effectiveness of combined mechanisms in providing the required system security services].

Separation-of Concerns Principle: Bart De Win, from Belgium, took the opportunity to explain his paper⁶ contribution on this [design approach] principle. It argues that despite the prevalent notion that security is a pervasive problem, it is possible to design [at least software] systems by creating security objects that focus the security responsibilities to serve the whole system. [See his paper for a much better description.]

⁶ [On the importance of the separation-of-concerns principle in secure software engineering](#)

De Win, Bart; [Piessens, Frank](#); Joosen, Wouter; and Verhanneman, Tine. Katholieke Universiteit Leuven,

Are These Principles?

The group expressed some behaviors that were not clearly principles but at least good practices:

- Follow good design principles.
- Focus on the weakest link.
- Keep it simple (KISS).
- Do good engineering. Avoid fads.
- Expect threats to change. Design for change.

Program Management Considerations

Throughout the discussions the group expressed several practices, some of which have associated principles:

- Security engineering must interact with project management.
- Contracting alternatives may affect outcome.
- [Plan].
- [Track] resources.
- [Consider] alternatives.
- [Control] requirements creep.

Summary

The group was led to derive principles from an exploration of an ISSE process. The original position of the group leader around whom the group was formed was that the problem was not engineering fundamentals but a failure to apply systems engineering. Several **[systems] engineering principles** were put forth that are presented as applicable to each of the phases of the process. The group leader and author of this report has added clarifying explanations and personal views.

[The group leader's paper⁷ somewhat guided the discussion and it provides some guidance on what is needed for the future: EDUCATION. As for the WAEPPSSD, I recommend future participation by practicing NSA ISSEs. I don't feel that there has been a serious breakdown in engineering as a discipline but there is a need for a massive infusion of ISSE into the business. The WAEPPSSD can lead in that effort.]

Richard K. McAllister
SPARTA Incorporated
Columbia, MD
rncall@sparta.com
410-381-9400 x231

⁷ *Information Systems Security Engineering: The Need for Education*, McAllister, Richard K., Sparta Inc.