2019 Annual INCOSE Western States Regional Conference (WSRC)

Systems Security Engineering

Mehrdad Sharbaf, Ph.D.

Adjunct Professor CSUDH

Chair CLAS IEEE Computer Society Chapter

Objective

- Understand System Security Engineering processes in the development of systems.
- Evaluate the security design of systems using security engineering processes and principles.
- Develop system designs that embed security functions and provide adequate protection to system functions.
- Analyze system security risk within the context of system operations and organizational risk tolerance.
- Understand NIST SP800-160 System Security Engineering Framework, and Engineering secure systems with ISO 26702, ISO 21827 and 27001

Agenda

- Problem related to information security
- What is system engineering?
- What is system security engineering?
- System Security Engineering Processes
- Design For Security
- Security risk assessment and management
- The Systems Security Engineering Capability Maturity Model (ISO 21827)
- NIST SP800-160 System Security Engineering Framework
- System Security Engineering Assistant Tools

Problem related to information security

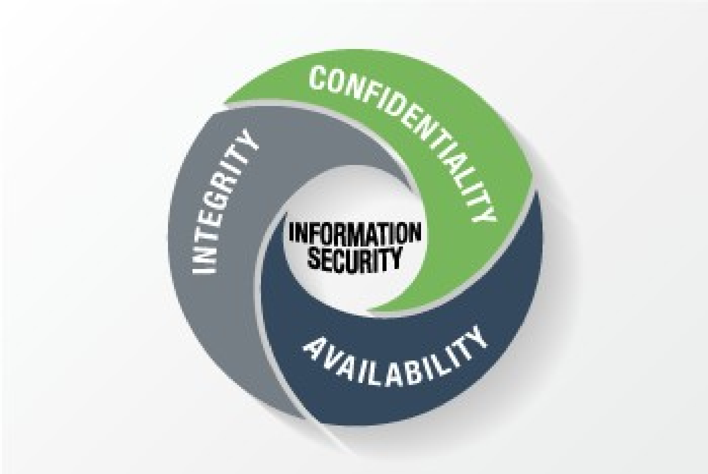
- How does management establish and track an information security program when:
- Current system security strategies are inadequate, and it lacks proper security engineering implementation within organization
- That impacts the organization costly, and systems fail to be certified and accredited. As systems have grown more complex and adversaries in cyberspace continue to successfully exploit numerous vulnerabilities, the need for improved secure system engineering has become acute.
- Risks are real
- Risks are nearly infinite
- The information environment is highly dynamic
- Resources are finite

Introduction to Information Security

- The protection of information and its critical elements, including systems, software, and hardware that use, store, and transmit that information
- Necessary tools: risk management, policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

Security Goals

- Confidentiality
  - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.



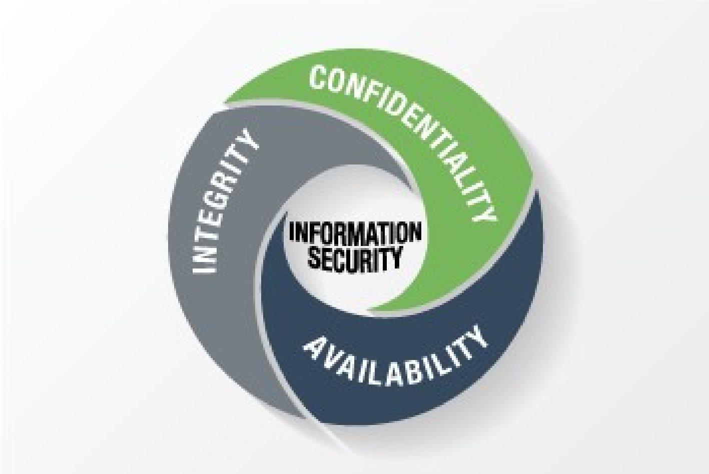
Security Goals

- Integrity
  - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.

CONFIDENTIALITY
INTEGRITY
INFORMATION SECURITY
AVAILABILITY

Security Goals

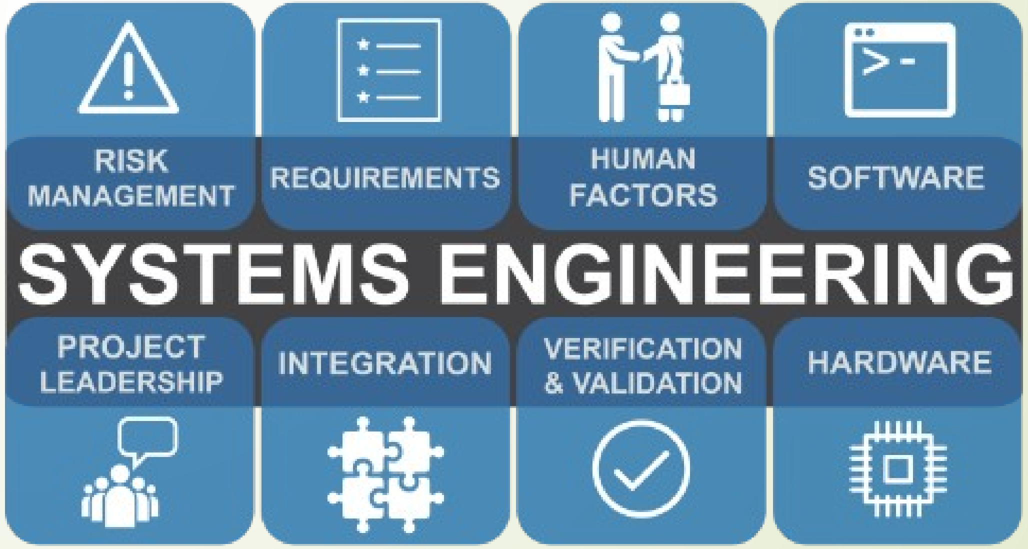
- Availability
  - Availability means that people who are authorized to use information are not prevented from doing so



System Engineering

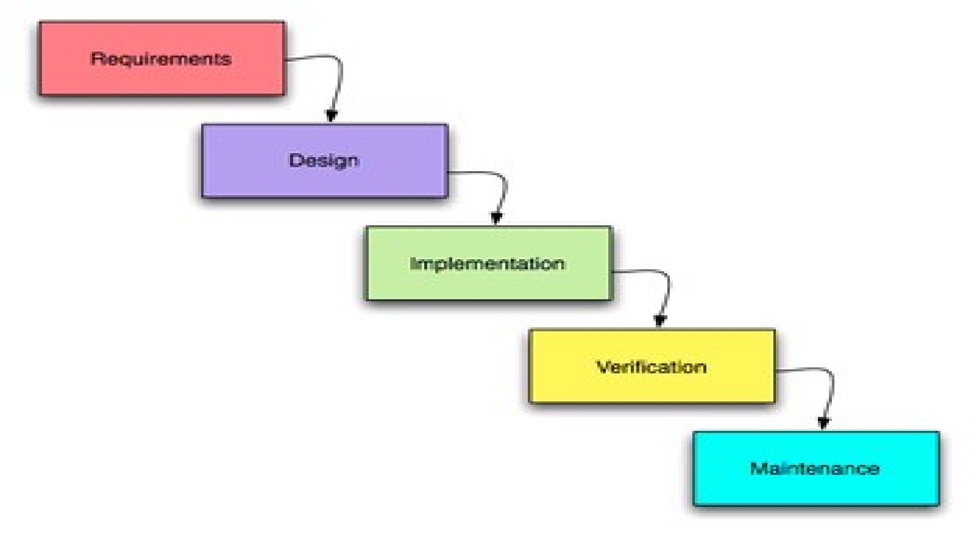
- Systems Engineering (SE) is the engineering discipline that focuses on integrating all the key elements of a system into one overall system and managing it throughout its lifecycle.
- “Systems engineering is an interdisciplinary engineering management process that evolves and verifies an integrated, life-cycle balanced set of system solutions that satisfy customer needs.” (DoD).
- Systems Engineering integrates all the disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation. Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs(INCOS).

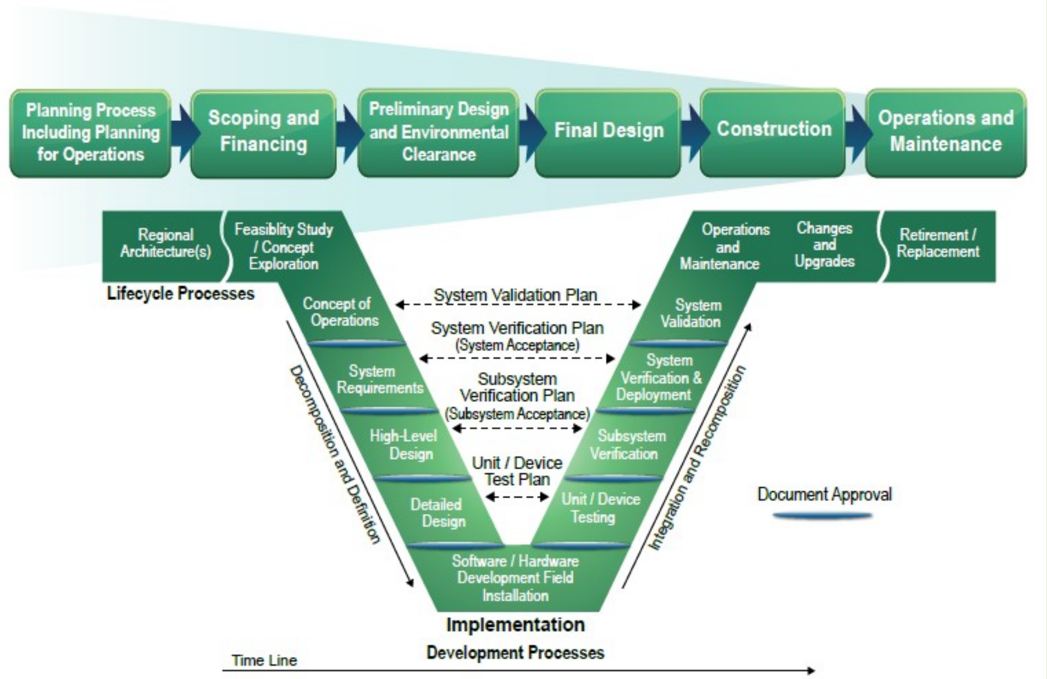
System Engineering



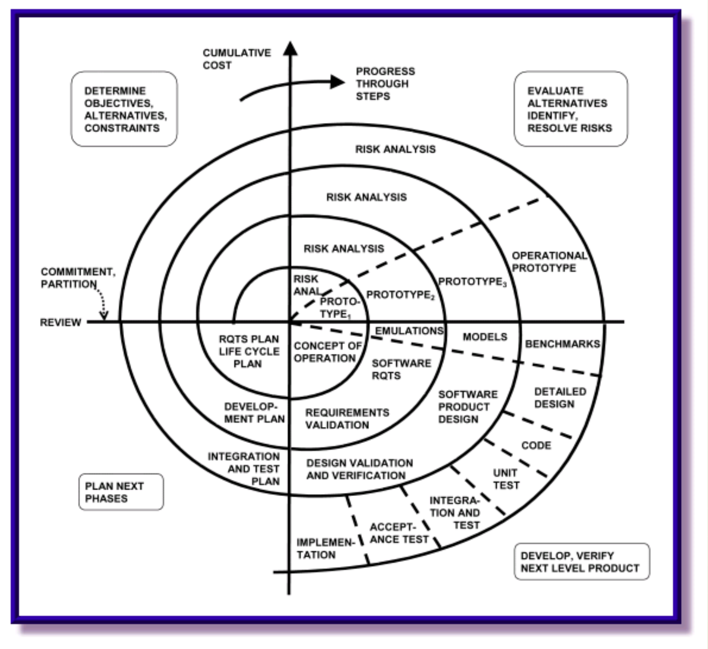
Definition of a “system”

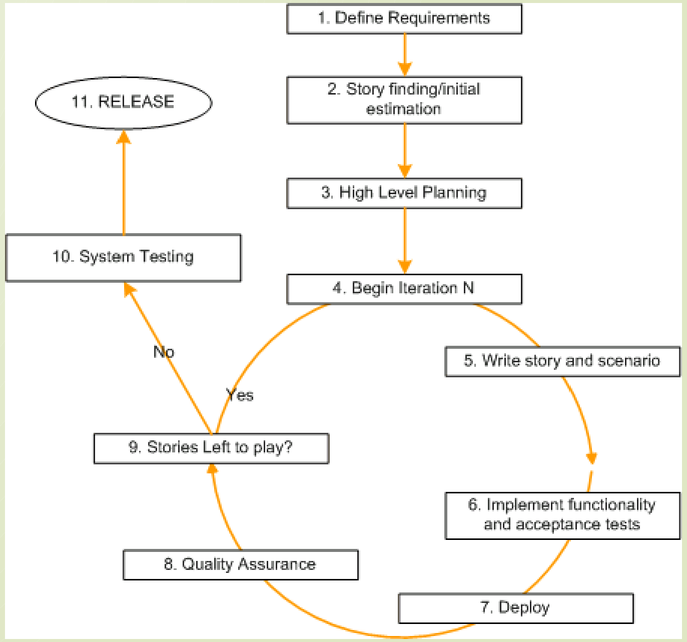
> “**System design** is the process or art of defining the hardware and software architecture, components, modules, interfaces, and data for a computer system to satisfy specified requirements.”




Planning Process Including Planning for Operations
Scoping and Financing
Preliminary Design and Environmental Clearance
Final Design
Construction
Operations and Maintenance
Regional Architecture(s)
Feasiblity Study / Concept Exploration
Lifecycle Processes
Concept of Operations
System Requirements
High-Level Design
Detailed Design
Software / Hardware Development Field Installation
Implementation
Development Processes
Time Line
Decomposition and Definition
Integration and Recomposition
System Validation Plan
System Verification Plan (System Acceptance)
Subsystem Verification Plan (Subsystem Acceptance)
Unit / Device Test Plan
Operations and Maintenance
Changes and Upgrades
Retirement / Replacement
System Validation
System Verification & Deployment
Subsystem Verification
Unit / Device Testing
Document Approval

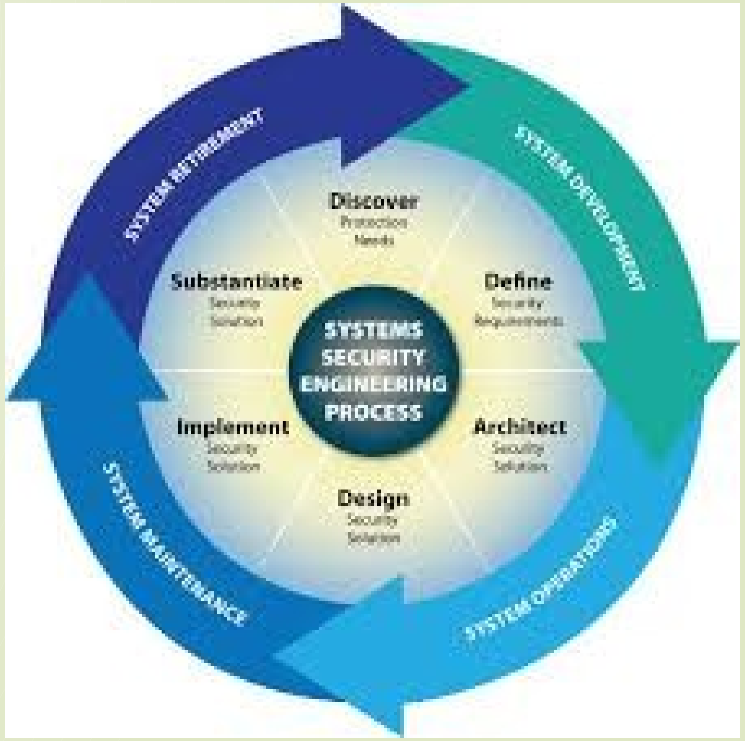
Some examples of System and software development models





Systems Security Engineering

- Description: The concept of Systems Security Engineering is to serve the organization to ensure that the security requirements of systems are met under advanced adversarial attack.
- System Security Engineering (SSE) is an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities [DoD 5200.44].



Systems Security Engineering

- The focus of the Systems Security Engineering discipline is:
  - tools,
  - processes, and
  - methods
- needed to
  - design,
  - implement, and
  - test
- complete systems, and to adapt existing systems as their environment evolves.

Process Models

- **Secure Process**
  - Set of activities performed to develop, maintain, and deliver a secure software solution
  - Activities could be concurrent or iterative
- **Process model**
  - provides a reference set of best practices that can be used for both
    - process improvement and process assessment.
  - defines the characteristics of processes
  - usually has an architecture or a structure

System Development Life Cycle (SDLC)

- A survey of existing processes, process models, and standards seems to identify the following four SDLC focus areas for secure system development
  - Security Engineering Activities
  - Security Assurance
  - Security Organizational and Project Management Activities
  - Security Risk Identification and Management Activities

SDLC

- Security Engineering Activities
  - activities needed to engineer a secure solution.

    security requirements elicitation and definition,

    secure design based on design principles for security,

    use of static analysis tools,

    reviews and inspections, security testing, etc..
- Security Assurance Activities

  verification, validation, expert review,

  artifact review, and evaluations.

SDLC

- Security Organizational and Project Management Activities
  - Organizational management
    - organizational policies, senior management sponsorship and oversight, establishing organizational roles, ….
  - Project management
    - project planning and tracking,
    - resource allocation and usage
- Security Risk Identification and Management Activities
  - Cost-based Risk analysis
  - Risk mitigation ..

Capability Maturity Models (CMM)

- CMM
  - Provides reference model of mature practices
  - Helps identify the potential areas of improvement
  - Provides goal-level definition for and key attributes for specific processes
  - Systems Security Engineering Capability Maturity Model (SSE-CMM)
    - Specifically to develop secure systems

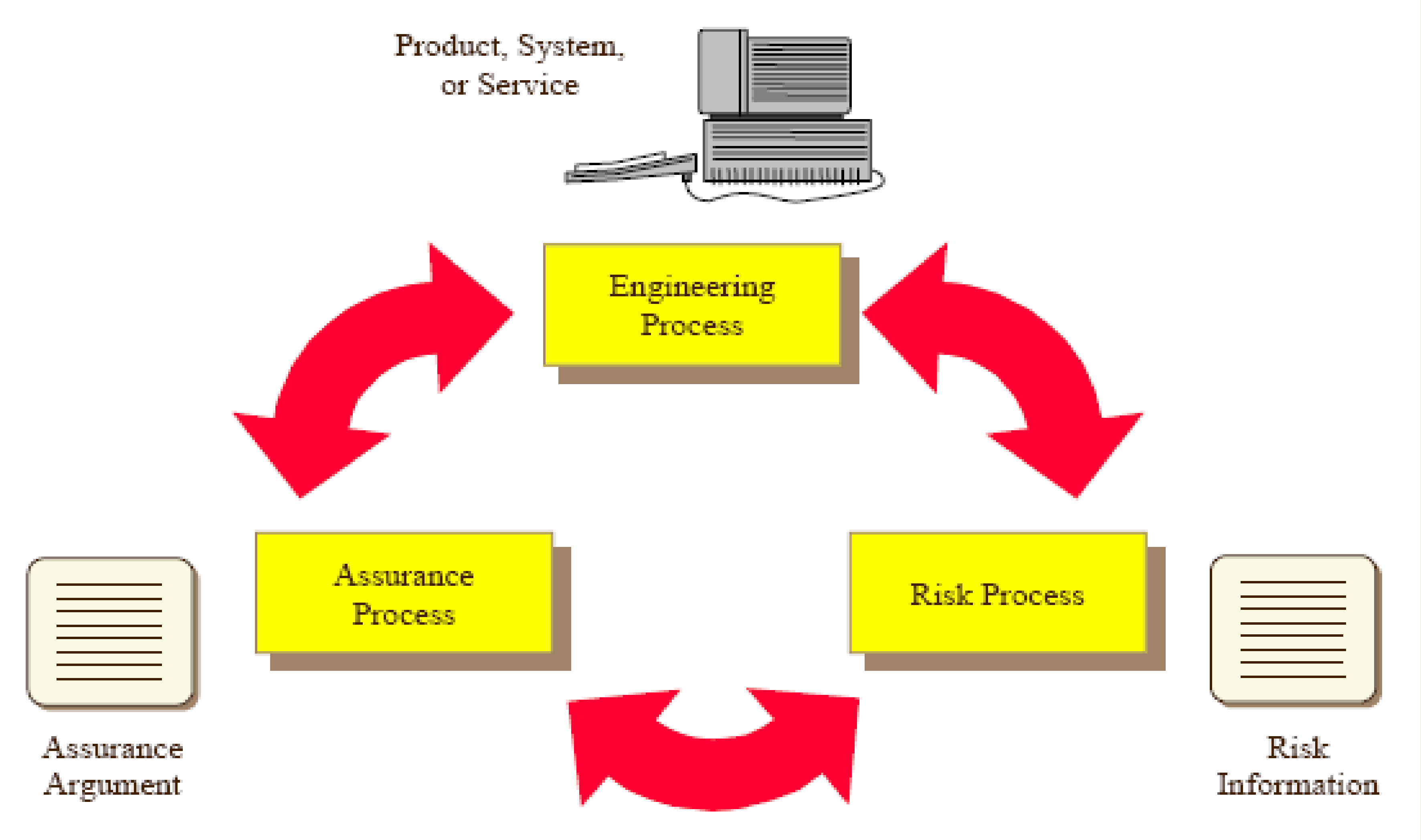
Systems Security Engineering CMM

- The SSE-CMM
  - To improve and assess the security engineering capability of an organization
- provides a comprehensive framework for
  - evaluating security engineering practices against the generally accepted security engineering principles.
- provides a way to
  - measure and improve performance in the application of security engineering principles.

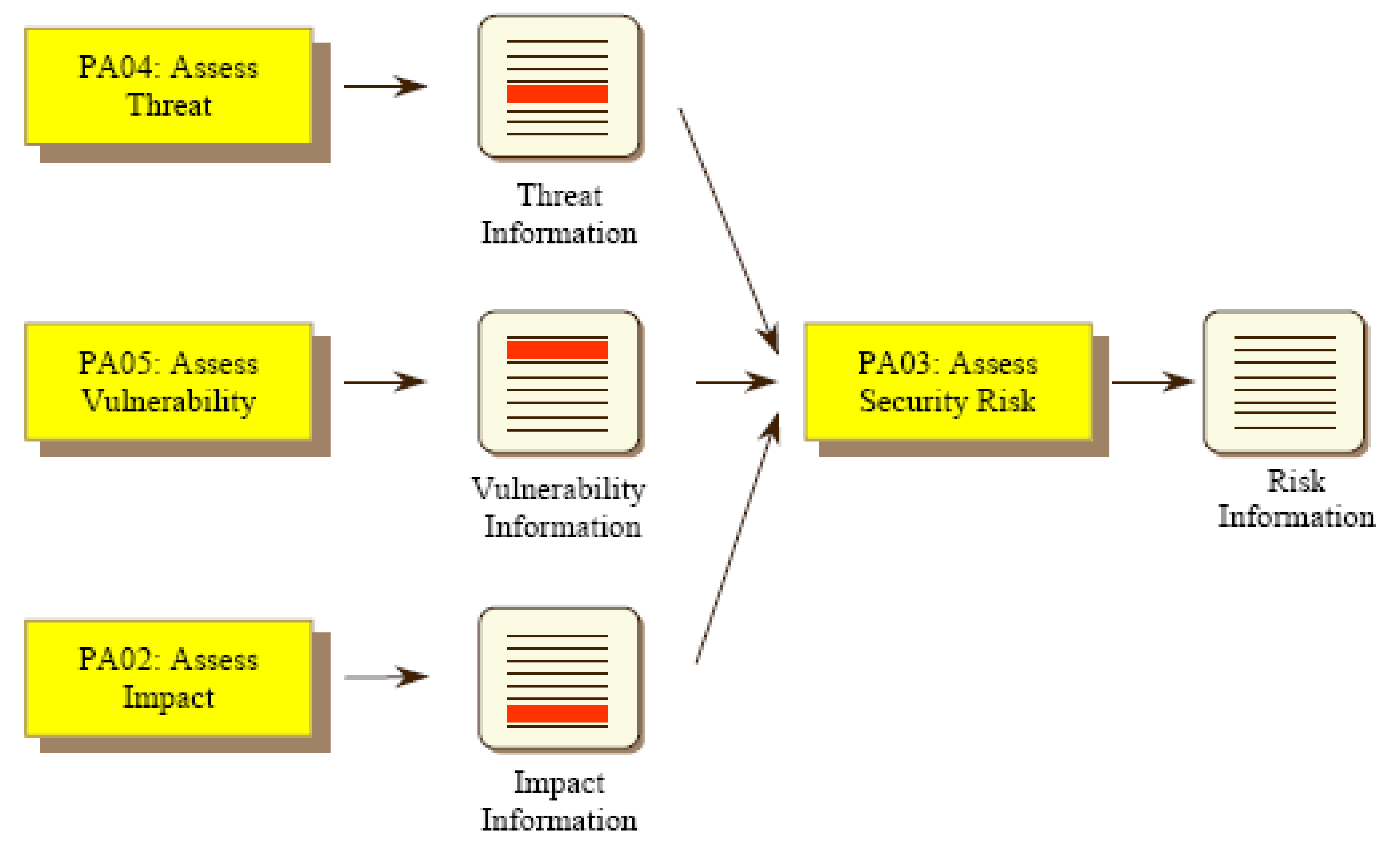
SSE-CMM

- Purpose for SSE-CMM
  - To fill the lack of a comprehensive framework for evaluating security engineering practices against the principles
- The SSE-CMM also
  - describes the essential characteristics of an organization’s security engineering processes.
    - The SSE-CMM is now ISO/IEC 21827 standard

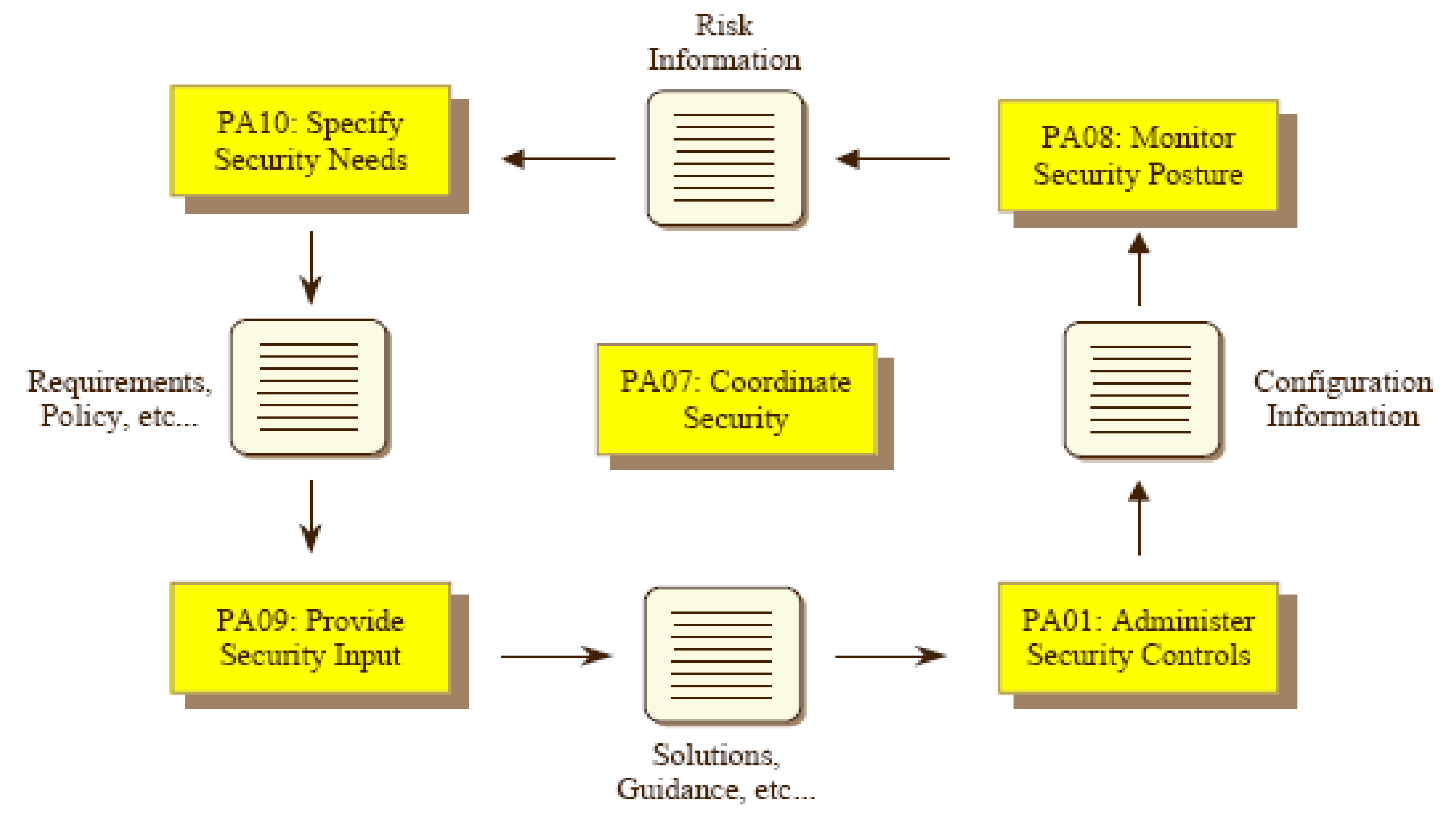
Security Engineering Process



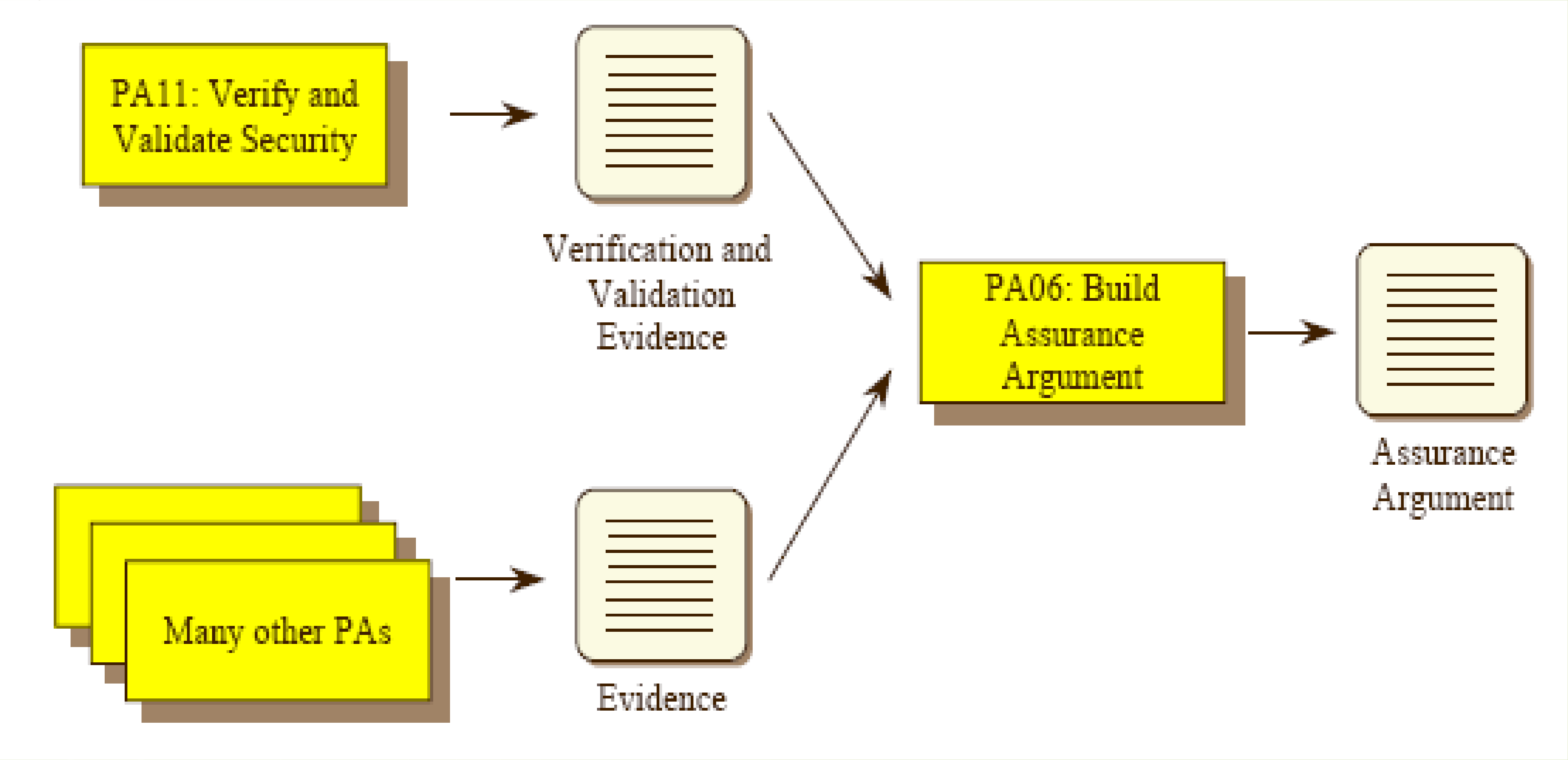
Security Risk Process



Security is part of Engineering

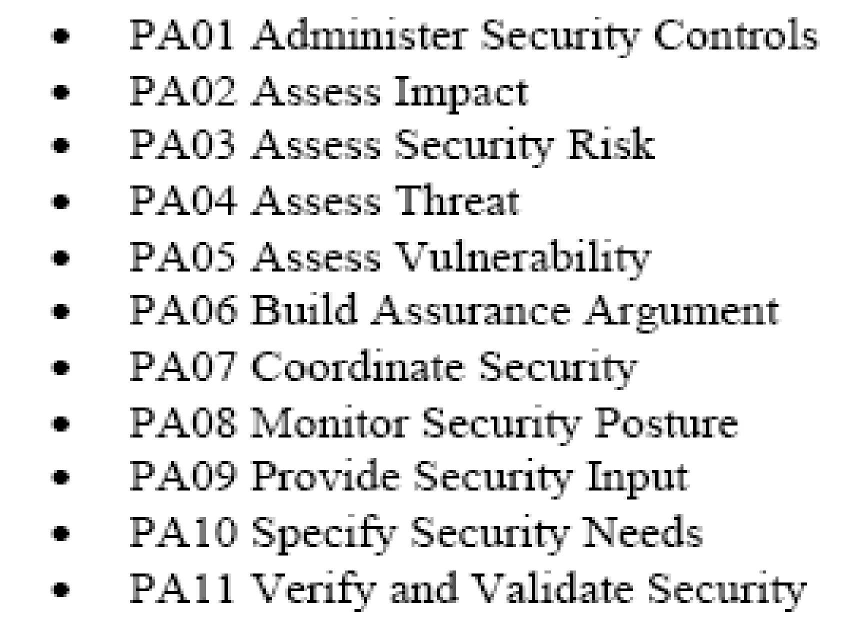

Risk Information
PA10: Specify Security Needs
PA08: Monitor Security Posture
Requirements, Policy, etc...
PA07: Coordinate Security
Configuration Information
PA09: Provide Security Input
PA01: Administer Security Controls
Solutions, Guidance, etc...

Assurance


PA11: Verify and Validate Security
Verification and Validation Evidence
Many other PAs
Evidence
PA06: Build Assurance Argument
Assurance Argument

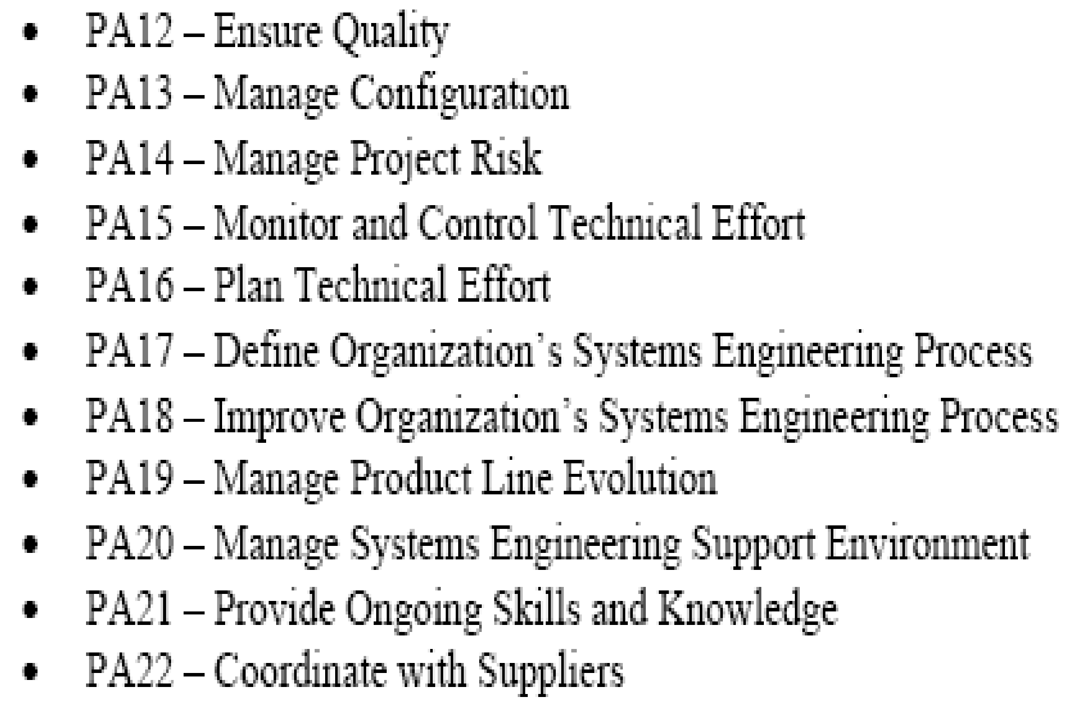
Process Areas

Process Areas related to Security Engineering process areas



- PA01 Administer Security Controls
- PA02 Assess Impact
- PA03 Assess Security Risk
- PA04 Assess Threat
- PA05 Assess Vulnerability
- PA06 Build Assurance Argument
- PA07 Coordinate Security
- PA08 Monitor Security Posture
- PA09 Provide Security Input
- PA10 Specify Security Needs
- PA11 Verify and Validate Security

Process Areas related to project and Organizational practices



- PA12 – Ensure Quality
- PA13 – Manage Configuration
- PA14 – Manage Project Risk
- PA15 – Monitor and Control Technical Effort
- PA16 – Plan Technical Effort
- PA17 – Define Organization's Systems Engineering Process
- PA18 – Improve Organization's Systems Engineering Process
- PA19 – Manage Product Line Evolution
- PA20 – Manage Systems Engineering Support Environment
- PA21 – Provide Ongoing Skills and Knowledge
- PA22 – Coordinate with Suppliers

Design for security

- Architectural design - how do architectural design decisions affect the security of a system?
- Good practice - what is accepted good practice when designing secure systems?
- Design for deployment - what support should be designed into a system to avoid the introduction of vulnerabilities when a system is deployed for use?

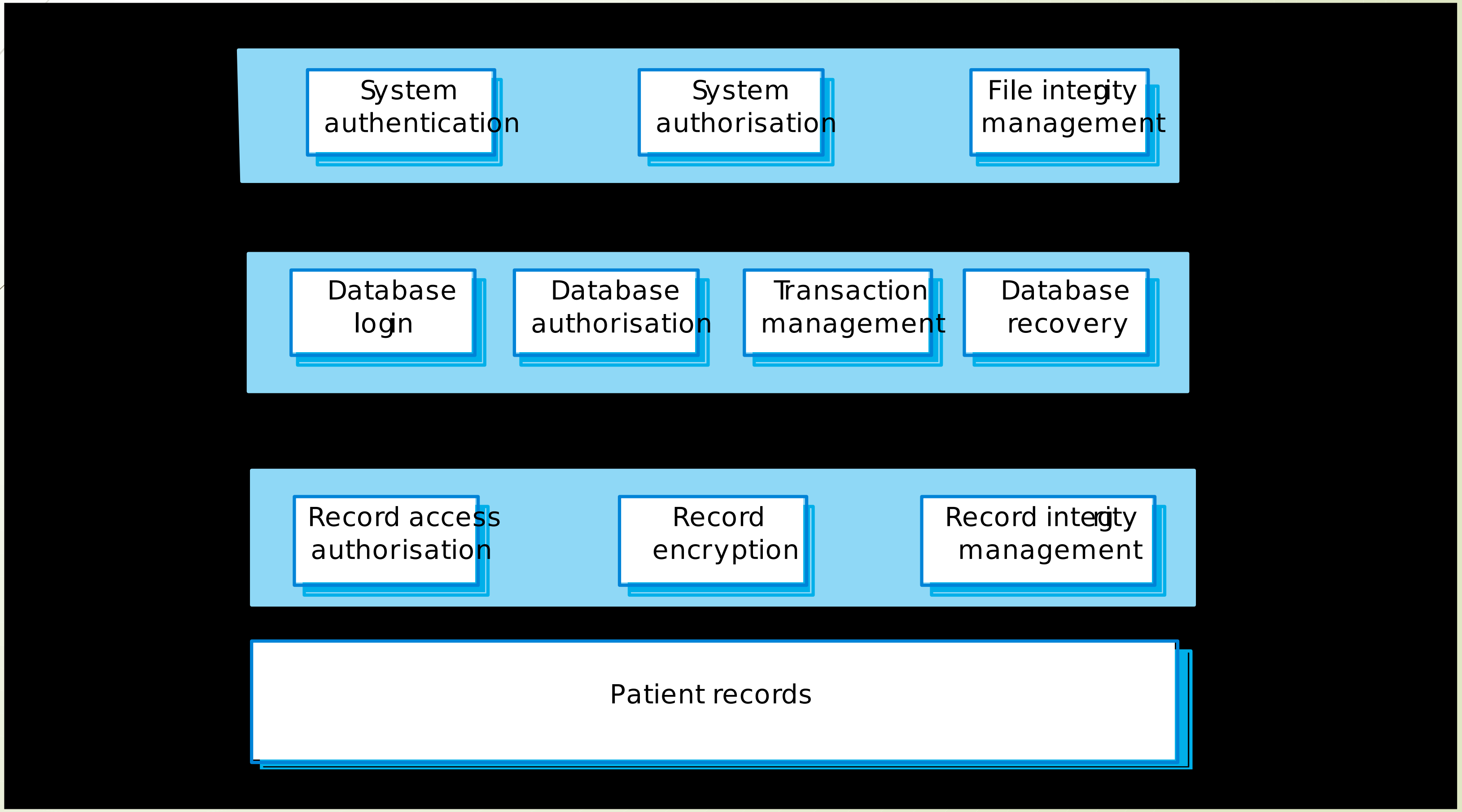
Architectural design

- Protection
  - How should the system be organized so that critical assets can be protected against external attack?
- Distribution
  - How should system assets be distributed so that the effects of a successful attack are minimized?
- Potentially conflicting
  - If assets are distributed, then they are more expensive to protect.

Protection

- Platform-level protection
- Application-level protection
- Record-level protection

Layered protection



System authentication

System authorisation

File integrity management

Database login

Database authorisation

Transaction management

Database recovery

Record access authorisation

Record encryption

Record integrity management

Patient records

Design guidelines

- Design guidelines encapsulate good practice in secure systems design
- Design guidelines serve two purposes:
  - They raise awareness of security issues in a software engineering team.
  - They can be used as the basis of a review checklist that is applied during the system validation process.

Design guidelines 1

- Base security decisions on an explicit security policy
- Avoid a single point of failure
- Fail securely
- Balance security and usability
- Be aware of the possibilities of social engineering

Design guidelines 2

- Use redundancy and diversity to reduce risk
- Validate all inputs
- Compartmentalize your assets
- Design for deployment
- Design for recoverability

Survivability strategies

- Resistance
  - Avoiding problems by building capabilities into the system to resist attacks
- Recognition
  - Detecting problems by building capabilities into the system to detect attacks and failures and assess the resultant damage
- Recovery
  - Tolerating problems by building capabilities into the system to deliver services whilst under attack

NIST Systems Security Engineering Initiative

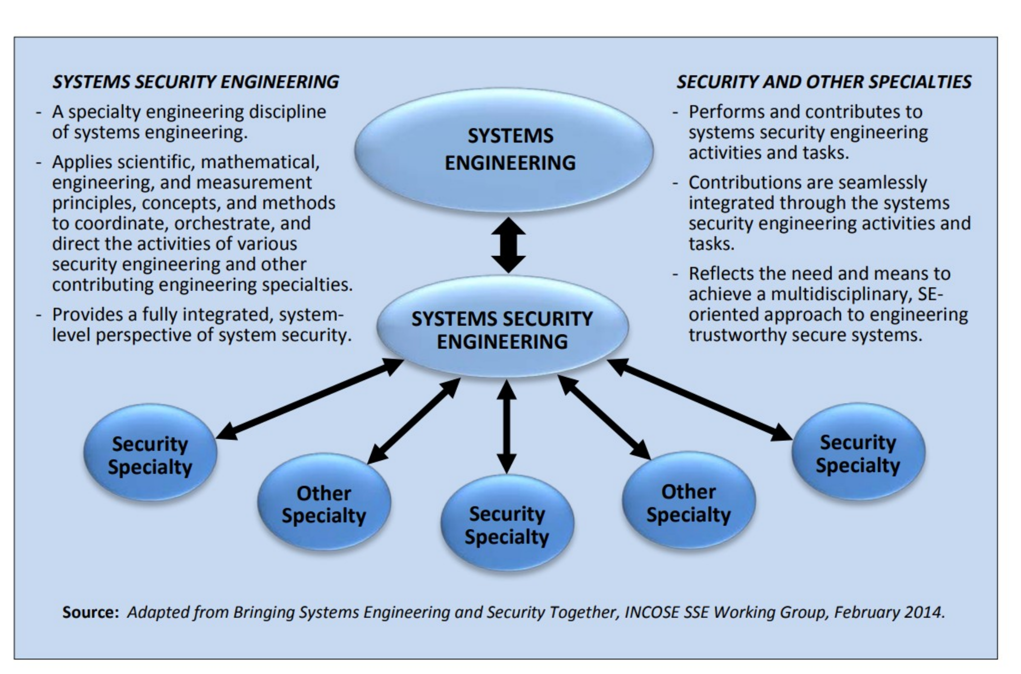
- NIST Special Publication 800-160 is the flagship publication in a series of planned systems security engineering publications.
- The series of 800-160 publications will include several important systems security engineering topics, for example: hardware security and assurance; software security and assurance; and system resiliency.
- Each topic will be addressed in the context of the system life cycle processes contained in ISO/IEC/IEEE 15288 and the security related activities and tasks that are described in SP 800-160.

NIST-Systems Security Engineering

- Systems security engineering, as an integral part of systems engineering, helps to ensure that the appropriate security principles, concepts, methods, and practices are applied during the system life cycle to achieve stakeholder objectives for the protection of assets—across all forms of adversity characterized as disruptions, hazards, and threats.
- It also helps to reduce system defects that can lead to security vulnerability and as a result, reduces the susceptibility of the system to adversity

NIST-Systems Security Engineering

- Systems security engineering leverages many security specialties and focus areas that contribute to systems security engineering activities and tasks. These security specialties and focus areas include, for example: computer security; communications security; transmission security; antitamper protection; electronic emissions security; physical security; information, software, and hardware assurance; and technology specialties such as biome



SYSTEMS SECURITY ENGINEERING

- A specialty engineering discipline of systems engineering.
- Applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering and other contributing engineering specialties.
- Provides a fully integrated, system-level perspective of system security.

SECURITY AND OTHER SPECIALTIES

- Performs and contributes to systems security engineering activities and tasks.
- Contributions are seamlessly integrated through the systems security engineering activities and tasks.
- Reflects the need and means to achieve a multidisciplinary, SE-oriented approach to engineering trustworthy secure systems.

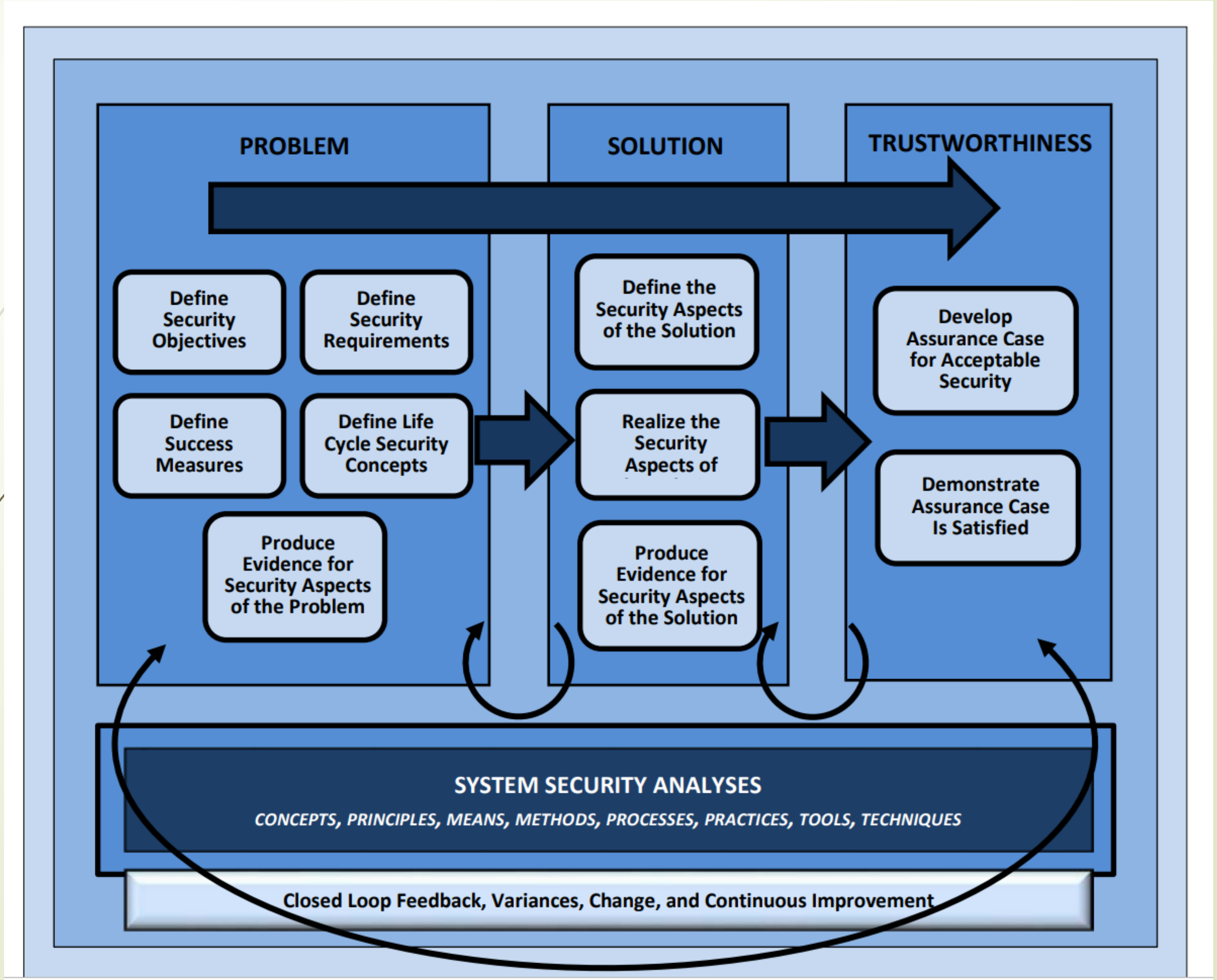
Source: *Adapted from Bringing Systems Engineering and Security Together, INCOSE SSE Working Group, February 2014.*

NIST-Role of Systems Security Engineering

- Engineering the security functions that provide system security capability
- Engineering the security-driven constraints for all system functions; and
- Engineering and advising for the protection of data, information, technology, methods, and assets associated with the system throughout its life cycle.
- These roles require a systems security engineering presence in all systems engineering activities in order to establish a multidisciplinary security and specialty approach to engineering—resulting in sustainably trustworthy secure systems throughout the system life cycle.

NIST-SYSTEMS SECURITY ENGINEERING FRAMEWORK

- The systems security engineering framework emphasizes an integrated, holistic security perspective across all stages of the system life cycle and is applied to satisfy the milestone objectives of each life cycle stage.
- The figure provides an overview of the systems security engineering framework and its key components.
- The framework defines three contexts within which the systems security engineering activities are conducted. These are the problem context, the solution context, and the trustworthiness context. Establishing the three contexts helps to ensure that the engineering of a system is driven by a sufficiently complete understanding of the problem articulated in a set of stakeholder security objectives that reflect protection needs and security concerns



PROBLEM

Define Security Objectives

Define Security Requirements

Define Success Measures

Define Life Cycle Security Concepts

Produce Evidence for Security Aspects of the Problem

SOLUTION

Define the Security Aspects of the Solution

Realize the Security Aspects of

Produce Evidence for Security Aspects of the Solution

TRUSTWORTHINESS

Develop Assurance Case for Acceptable Security

Demonstrate Assurance Case Is Satisfied

SYSTEM SECURITY ANALYSES

CONCEPTS, PRINCIPLES, MEANS, METHODS, PROCESSES, PRACTICES, TOOLS, TECHNIQUES

Closed Loop Feedback, Variances, Change, and Continuous Improvement

The Problem Context

- The problem context defines the basis for an acceptably and adequately secure system given the stakeholder’s mission, capability, performance needs and concerns; the constraints imposed by stakeholder concerns related to cost, schedule, risk and loss tolerance; and other constraints associated with life cycle concepts for the system
- The problem context includes:
- Determining life cycle security concepts
- Defining security objectives;
- Defining security requirements; and
- Determining measures of success.

The Solution Context

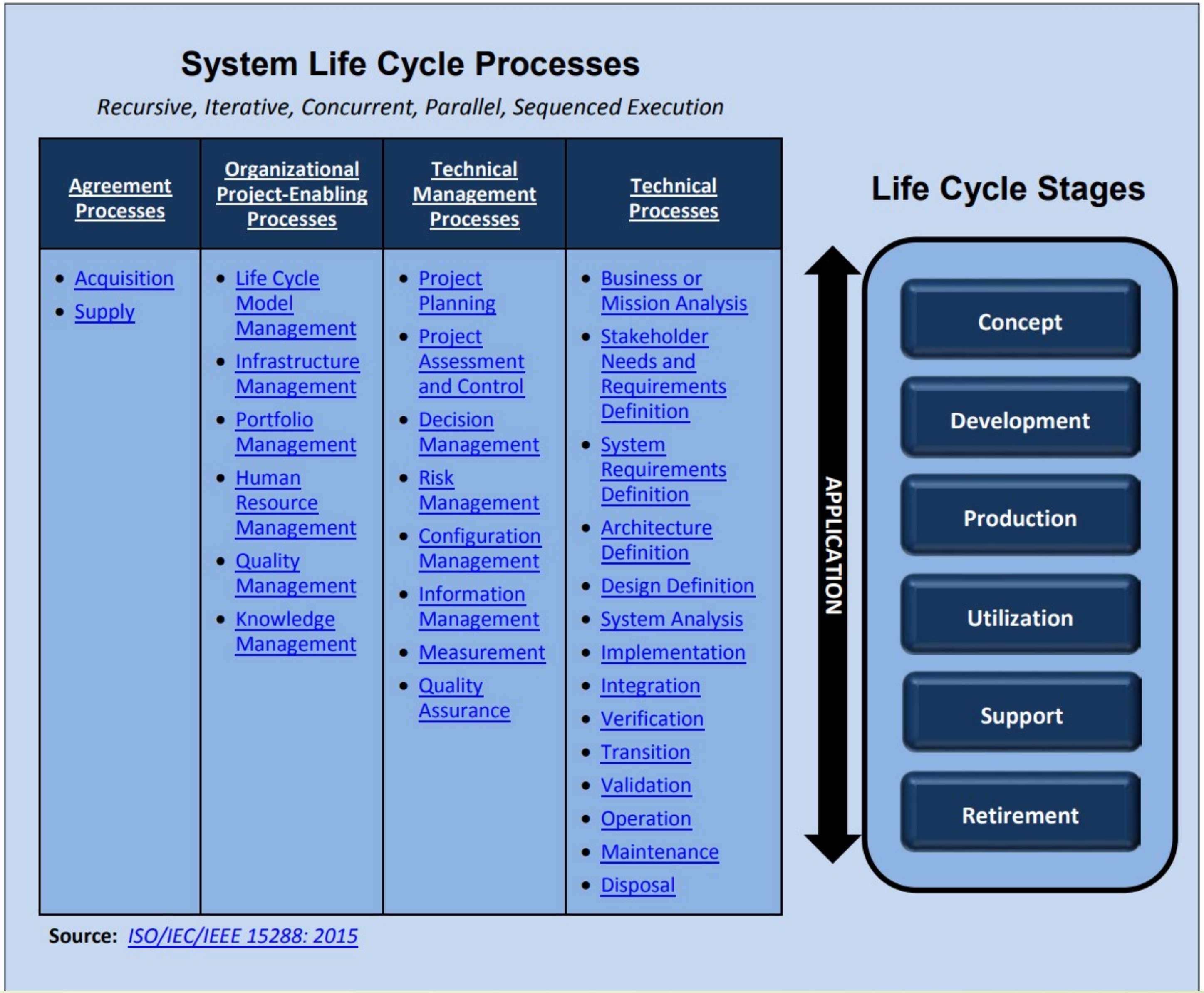
- The solution context transforms the stakeholder security requirements into design requirements for the system; addresses all security architecture, design, and related aspects necessary to realize a system that satisfies those requirements; and produces sufficient evidence to demonstrate that those requirements have been satisfied.
- The system security protection strategy is consistent with the overall concept of secure function. The concept of secure function, defined during the problem context, constitutes a strategy for a proactive and reactive protection capability throughout the system life cycle.
- The Solution Context includes:
- Defining the security aspects of the solution
- Realizing the security aspects of the solution; and
- Producing evidence for the security aspects of the solution.

The Trustworthiness Context

- The trustworthiness context is a decision-making context that provides an evidence-based demonstration, through reasoning, that the system-of-interest is deemed trustworthy based upon a set of claims derived from security objectives.
- The trustworthiness context consists of:
- Developing and maintaining the assurance case; and
- Demonstrating that the assurance case is satisfied.

SYSTEM LIFE CYCLE PROCESSES SYSTEM SECURITY IN SYSTEM LIFE CYCLE PROCESSES

- It describes the security considerations and contributions to system life cycle processes to produce the security outcomes that are necessary to achieve trustworthy secure systems.
- The security considerations and contributions are provided as systems security engineering activities and tasks and they are aligned with and developed as security extensions to the system life cycle processes in ISO/IEC/IEEE 15288, Systems and software engineering – System life cycle processes.



System Life Cycle Processes

Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organizational Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Life Cycle Stages

APPLICATION

- Concept
- Development
- Production
- Utilization
- Support
- Retirement

Source: *ISO/IEC/IEEE 15288: 2015*

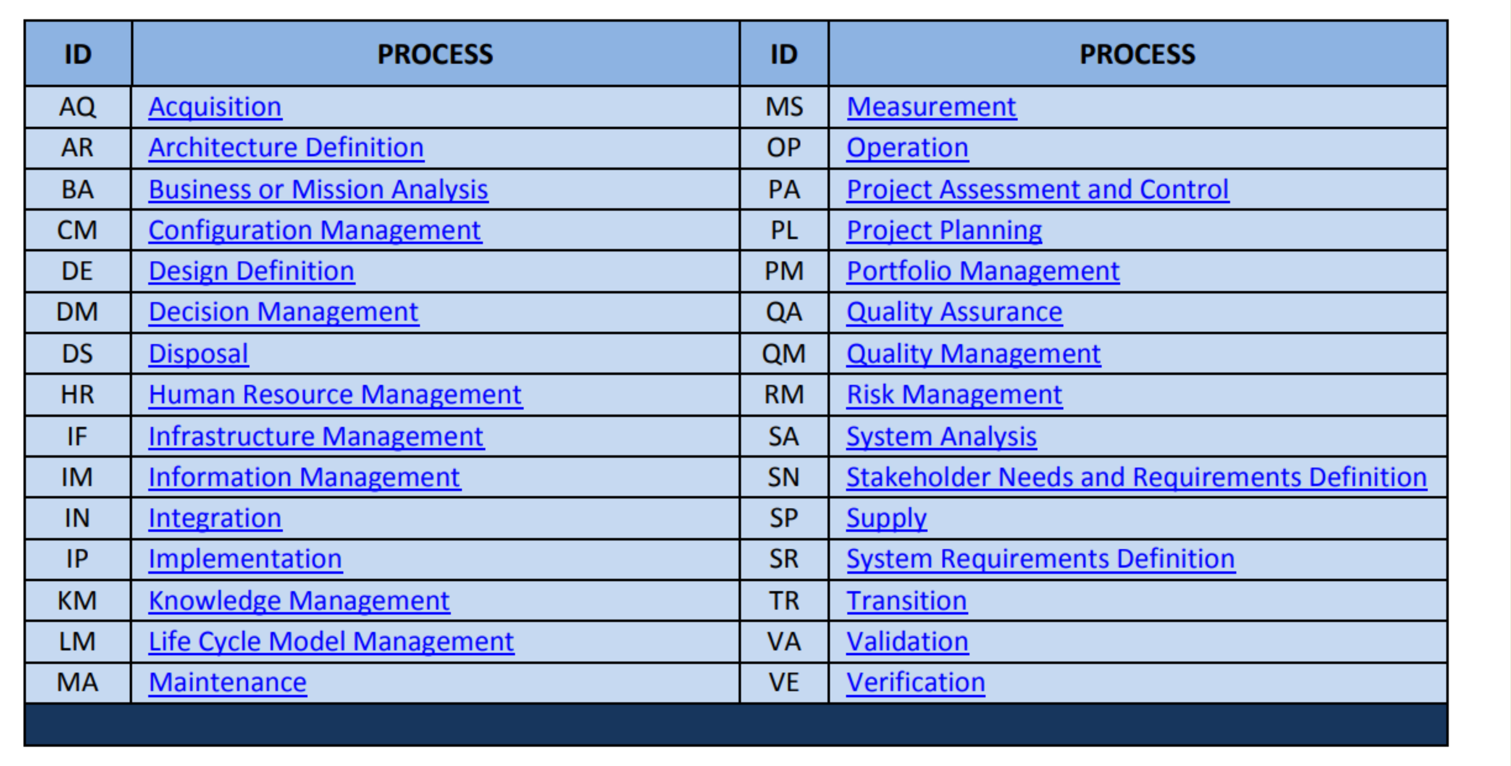
SSE contributes to all SE life cycle processes – with emphasis on the Technical Processes

SECURITY IN SYSTEM LIFE CYCLE PROCESSES

- Each of the system life cycle processes contains a set of system security activities and tasks that produce a set of security-oriented outcomes.
- These outcomes combine to deliver a system and a corresponding body of evidence that serves as the basis to substantiate the security and the trustworthiness of the system.
- Each life cycle process description has the following format:
- Purpose: The purpose section identifies the primary goals and objectives of the process and provides a summary of the security-focused activities conducted during the process.
- Outcomes: The outcomes section describes the security-focused outcomes achieved by the completion of the process and the data generated by the process.
- Activities and Tasks: The activities and tasks section provides a description of the security oriented work performed during the process including the security-focused enhancements to the activities and tasks.

PROCESS NAMES AND DESIGNATORS

- The following naming convention is established for the system life cycle processes. Each process is identified by a two-character designation (e.g., BA is the official designation for the Business or Mission Analysis process). The Table provides a listing of the system life cycle processes and their associated two-character designators.



ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

SYSTEMS SECURITY ENGINEERING KEY POINTS

- Systems that possess
- resilient,
- trustworthy,
- system-level protections
- sufficient to enable achievement of mission/business objectives
- within performance parameters and risk tolerance

Analysis Classes

Static analysis examines the system without executing it and can be applied to design representations, source code, binaries, and bytecode. Tools include attack modeling, source code analyzers, obfuscated code detection, bytecode or binary disassembly, human review/inspection, origin analysis, digital signature verification, configuration checking, permission manifest analysis, development/sustainment version control, deliberate obfuscation, rebuild and compare, and formal methods.

Dynamic analysis examines the system execution, giving it specific inputs and examining results and/or outputs. Tools and techniques include network scanner, network sniffer, network vulnerability scanner, host-based vulnerability scanner, fuzz tester, framework-based fuzzer, negative testing, digital forensics, intrusion detection systems/intrusion prevention systems, automated monitored execution, forced path execution, firewall, man-in-the middle attack tool, debugger, and fault injection.

Hybrid analysis applies to the tight integration of static and dynamic analysis approaches.

Reference: SOAR

Analysis Tools

- Use a combination of tools.
- Static analysis and dynamic analysis are complementary
- Origin analysis should be used whenever third-party components are present.
- Use interactive security testing and hybrid tools if needed to get the most coverage.

Tools, Tools, Tools

ASTaaS

FindBugs

AFIC

IST

MAST

Regshot

ACAS

LSK 5.0

CodeSonar

Fortify

MONIT

SrvMan

Checkmarx

DriverMax

Gendarme

SIGVERIF

Starter

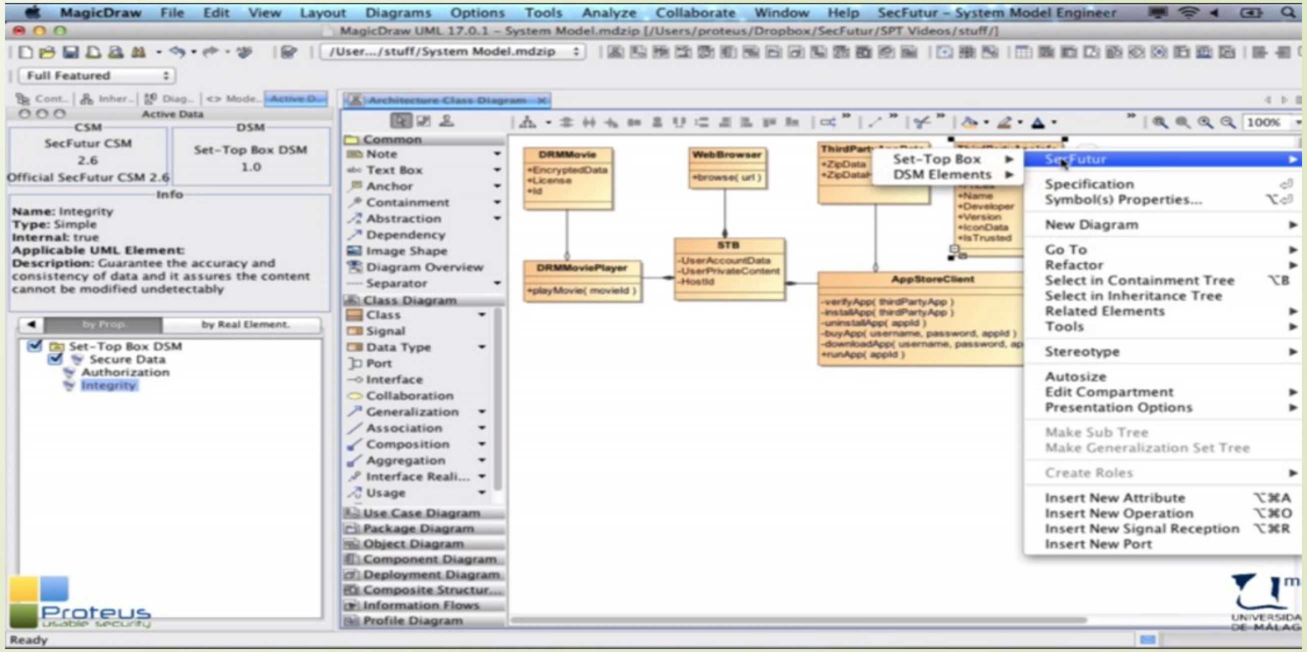
TRIPWIRE

FCIV

Coverity

System Security Engineering Assistant Tool

- System Security Engineering Assistant (S2EA) is a modelling tool that supports system engineers to adopt and deploy security mechanisms proactively by-design. S2EA follows a UML model-based paradigm and establishes a controlled and supervised modelling framework to support system engineers to create their system architectures and to integrate appropriate security mechanisms into them while ensuring design integrity.
- System Security Engineering Assistant (i85693.wixsite.com)



MagicDraw File Edit View Layout Diagrams Options Tools Analyze Collaborate Window Help SecFutur – System Model Engineer
MagicDraw UML 17.0.1 – System Model.mdzip [/Users/proteus/Dropbox/SecFutur/SPT Videos/stuff/]
/User..../stuff/System Model.mdzip
Full Featured
Cont.. Inher.. Diag.. <> Mode.. Active D..
Active Data
CSM
SecFutur CSM
2.6
Official SecFutur CSM 2.6
DSM
Set-Top Box DSM
1.0
Info

Name: Integrity
Type: Simple
Internal: true
Applicable UML Element:
Description: Guarantee the accuracy and consistency of data and it assures the content cannot be modified undetectably

Tools

- **Top 10 Vulnerability Scanners**
- http://sectools.org/tag/vuln-scanners/
- **Top 10 Web Vulnerability Scanners**
- http://sectools.org/tag/web-scanners/
- **Top 15 Security/Hacking Tools & Utilities**
- http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/
- **Top 125 Network Security Tools**
- http://sectools.org/
- More Information about Tools, please visit my blog
- http://Msharbaf.wordpress.com

References

- [ISO/IEC 21827] International Organization for Standardization/International Electrotechnical Commission/Institute Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model, 2008
- [ISO/IEC/IEEE 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, Systems and software engineering — Systems life cycle processes, May 2015.
- [ISO/IEC 15026-3] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15026-3:2015, Systems and software engineering -- Systems and software assurance -- Part 3: System integrity levels, November 2015.
- [ISO/IEC 27001] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements, September 2013.
- Federal Information Security Modernization Act of 2014, (P.L. 113- 283, Title II), December 18, 2014.
- Department of Defense (DoD) Directive 8140.01, Cyberspace Workforce Management, August 2015.
- Committee on National Security Systems Instruction (CNSSI) No. 4009, Committee on National Security Systems (CNSS) Glossary, April 2015.
- System Engineering Handbook—A Guide for System Engineering Life Cycle Processes and Activities, International Council On Systems Engineering TP-2003-002-04, 4th Edition, July 2015.
- A. Madni and S. Jackson, Towards a Conceptual Framework for Resilience Engineering, IEEE Systems Journal, Vol. 3, No. 2, June 2009.
- NIST-[SP-800-160], Vol. 2, R. Ross, R. Graubart, D. Bodeau, R. McQuaid, *Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems*, vol. 2, 2018.
- NIST-[SP 800-160], Vol. 1,R. Ross, R. Michael Mcevilley, Janet Carrier Oren, *Systems security engineering,* vol. 1, 2016
- NIST-[SP 800-37] National Institute of Standards and Technology Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (updated June 5, 2014).
- [SP 800-53A] National Institute of Standards and Technology Special Publication (SP) 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, December 2014 (updated December 18, 2014).
- M. McEvilley, Towards a Notional Framework for Systems Security Engineering, The MITRE Corporation, NDIA 18th Annual Systems Engineering Conference, October 2015.
- R. Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, Publisher: John Wiley & Sons, 2008.
- Carol C. Woody and Nancy R. Mead, Cyber Security Engineering: A Practical Approach for Systems and Software Assurance, publisher Addison-Wesley, 2017
- Stuart Jacobs, Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, publisher IEEE Press/Wiley, 2016
- Daniel Mellado a, Carlos Blanco b, Luis E. Sánchez c, Eduardo Fernández-Medina, A systematic review of security requirements engineering, Elsevier, Computer Standards & Interfaces 32(4):153-165 · June 2010.
- Ian Alston , Simon Campbell, *Selex Galileo Ltd,* A Systems Engineering Approach For Security System Design, IEEE 2010 International Conference on Emerging Security Technologies.
- Jennier L. Bayuk, Systems Security Engineering, IEEE Security & Privacy Journal, March/April 2011, pp. 72-74, vol. 9.