An Overview of the NIST 800-160 System Security Engineering Document

Dr. Ben Calloni, P.E. CISSP, CEH, OCRES

Lockheed Martin Fellow, Software Security

Permission granted to OMG to publish for OMG TC meeting, 12/6/2016

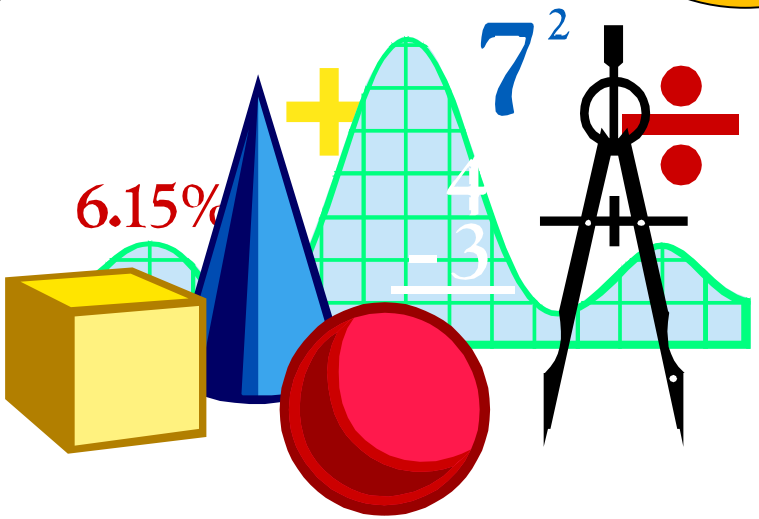
My thanks to Michael McEvilley, MITRE, long time friend, colleague, and co-author of NIST 800-160 for his insights.

Overview

- **Introduction**
- **Security Controls**
  - ***NIST SP800-53***
- **Security Requirements**
  - ***Requirements Engineering***
  - ***IEEE 15288***
- **System Security Engineering**
  - ***NIST 800-160***
- **Concluding Remarks**

Security Baked-In

For system developers, it's all about mathematics, computer science, architecture, and systems engineering—to include systems security engineering



Security should be a by-product of good engineering design and development practices.

Title 44 USC § 3542: Definition

1. **The term "Information Security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—**
   - ***A. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;***
   - ***B. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and***
   - ***C. Availability, which means ensuring timely and reliable access to and use of information.***

Known as the C-I-A Triad!

Title 44 USC § 3542: Definition (cont'd)

2. Further:

a. The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency -

1. the function, operation, or use of which -

I. involves intelligence activities;

II. involves cryptologic activities related to national security;

III. involves command and control of military forces;

IV. involves equipment that is an integral part of a weapon or weapons system; or

V. subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

2. is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

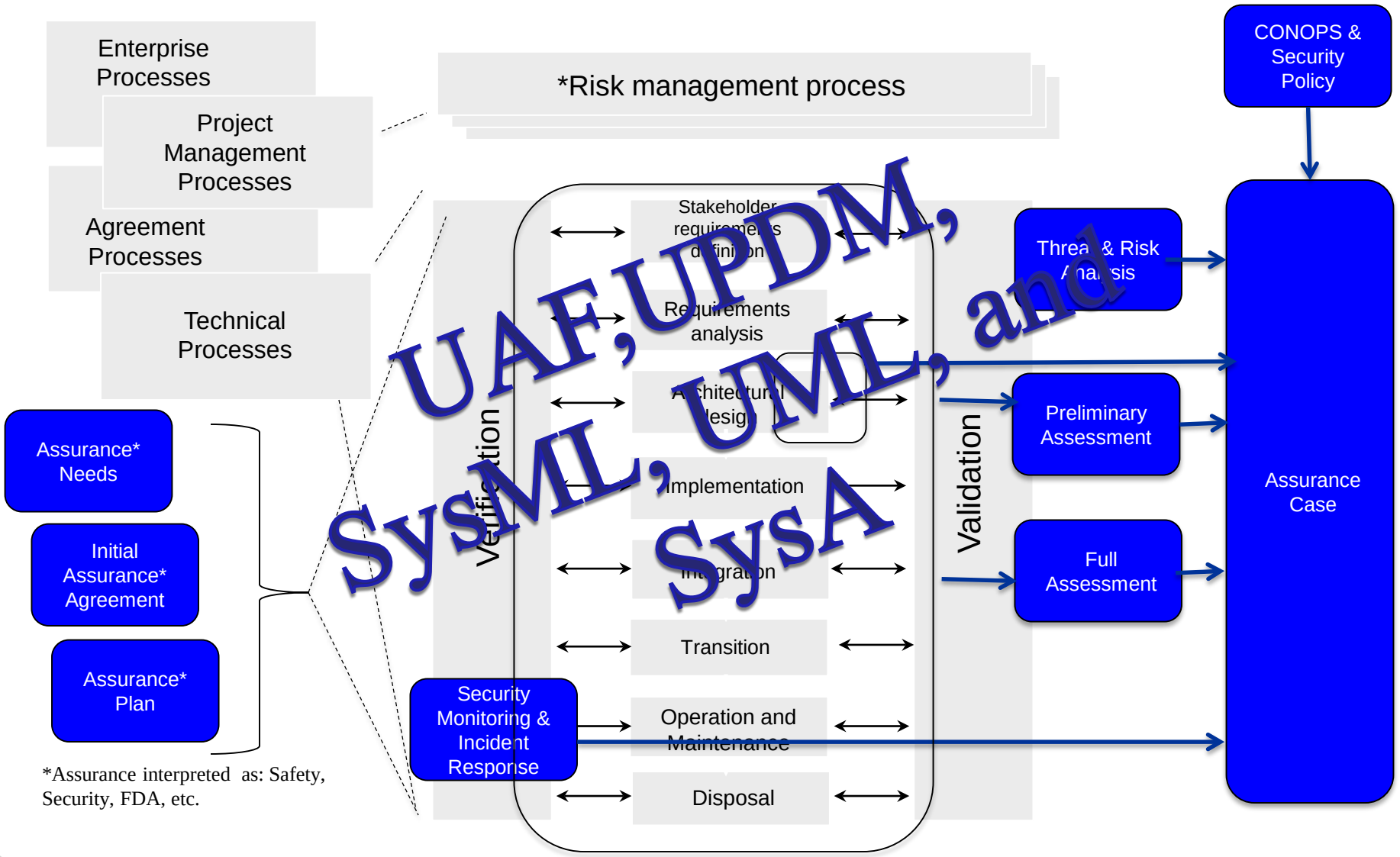
The Problem

- **Personnel at NIST, DHS, OSD observed that NIST SP800-53, "Recommended Security Controls for Federal Information Systems and Organizations" was being treated like a "check list" rather than a basis for "building security in"!**
- **Organizations were not performing due diligence in System Security Engineering to determine the quality / assurance of the controls being developed / utilized.**
- **NIST, NSA/IAD, MITRE authored a new document, NIST 800-160 to include SSE as part of the application of security controls**

BUILD SECURITY IN

Setting a higher standard for software assurance

Assurance as Part of Systems and Software Engineering - System Lifecycle (ISO 15288:2008)



Questions to address …

- Are security controls and security requirements the same?
- What are “security mechanisms”?
- What are the differences in security controls and engineering requirements?
- Must any differences be preserved?
- How to utilize security controls in a systems engineering environment?

Quantifying the Difference

- Organizational Security Risk Management and Systems Engineering
  - *Organizational Security Risk Management*
    - US Government : NIST SP800-53 “Recommended Security Controls for Federal Information Systems and Organizations”
    - Responsible for life cycle security risk management of the solution
    - Responsible to manage the residual risk in the delivered solution throughout operations, sustainment, and disposal
  - *Systems Engineering*
    - Delivers solutions that contain technical/program risk that is to be managed by the organization responsible for operation, sustainment, and disposal of the solution
    - Manages technical/program risk associated with the solution and informs organizational security risk management processes

Risk Management Framework (RMF)

- **NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach"**
  - ***Applicable to the IT Systems of the Federal Government***
- **CNSSI 1253 "Security Categorization and Control Selection for National Security Systems"**
  - ***Calls out and Tailors the RMF***
  - ***The RMF / Control guidance for National Security Systems***
- **NIST SP800-53**
  - ***Defines and relates security controls, security control baselines, security control overlays***
  - ***Contains a catalog of security and privacy controls***
  - ***Provides a process description for the application of security controls***

Common Basis for All USG Computer Systems!

NIST Special Publication 800-160

Initial Public Draft

Systems Security Engineering

An Integrated Approach to Building Trustworthy Resilient Systems

RON ROSS
JANET CARRIER OREN
MICHAEL McEVILLEY

NIST SP800-160

- Defines systems security engineering as a specialty of systems engineering
- Provides a process description for conducting security-focused engineering activities within the systems engineering technical and non-technical processes
- Is grounded in IEEE 15288 (which aligns with ISO 15288)

NIST SP800-53

- The NIST SP800-53 process description
  - *Focuses on organizational security risk management for information systems and the employment of security controls as risk response/treatment*
- NIST SP 800-53 short comings
  - *Is not written in terms of explicit interaction with systems engineering*
  - *Has no dependency on systems engineering*
  - *Has been applied in the absence of interaction with systems engineering (used as a checklist)*

NIST SP800-160

- Systems Engineering process description
  - *Focuses on engineering security mechanisms/controls for systems that includes but is not limited to risk treatment*
  - *Focuses on requirements as the contractual basis for all design activities, and for all verification and validation activities*
  - *Requires decomposition of requirements to a level that enables implementation*
    - Development, fabrication, reuse, leasing, subscribing
  - *Has no dependency on security controls and is applied successfully in the absence of the use of security controls*

NIST / NSA Objectives for 800-160

- *Reduce duplication of effort*
- *Assign security activities to the "community" most suited*
- *Leverage engineering artifacts (requirements, design, testing) to support organizational information system security risk management*
  - Tailoring of security controls to establish the basis for security control assessment
  - Traceability across the various requirements-based and security-controls based expressions of the system
- *Align security controls with long-standing requirements-engineering based systems engineering activities*

NIST / NSA Objectives for 800-160$_2$

- Increase consistency between
  - *Engineering and (independent) verification and validation activities*
  - *Security control assessment and system authorization*
- Evolve security control assessment towards assurance-driven objectives
  - *Insure security controls are appropriate to their application*
  - *Produce assurance evidence of the control strength*

Requirement and Control

- The terms “requirement” and “control” are not comparable or equivalent

Apples and oranges …
or is it vegetables?

Or worse yet, Minerals?

Compare Definitions

- Requirement (noun):
  - *something that is needed or that must be done*
  - *something that is necessary for something else to happen or be done*

- Control (noun):
  - *the power to make decisions about how something is managed or done*
  - *the ability to direct the actions of someone or something*
  - *an action, method, or law that limits outcomes*
  - *a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system*
  - *a restraint*

The Differences

- **IEEE: Requirement:**
  - ***A condition or capability needed, that must be met, that must be possessed***

- **NIST: Security Control:**
  - ***A safeguard or countermeasure***
    - i.e., a mechanism that serves as a safeguard or countermeasure

Policy, Mechanism, Requirement

- Security Policy:
  - *a statement of what is, and what is not, allowed (Matt Bishop)*
- Security Mechanism:
  - *A method, tool, or procedure for enforcing a security policy (Bishop)*
- Security Requirement:
  - *The Functional and Assurance capability/properties that must be met*

Terminology

- **Requirement: Shall is used to indicate a requirement that is**
  - ***contractually binding,***
  - ***it must be implemented, and***
  - ***its implementation verified. Period!***

  Don't think of "shall" as a word, but rather as an icon that SCREAMS: "This is a requirement." If a statement does not contain the word "shall" it is not a requirement.
- **Facts or Declaration of Purpose: Will is used to indicate a statement of fact.**
  - ***Will statements are not subject to verification.***
    - "The XYZ system will have the timing as defined in an ICD 1234."
    - "This report will contain this data…"

  In a statement of work (SOW) or task order for a vendor or supplier, I use will to communicate something I will do for or provide to the vendor or supplier.
- **Goals, non-mandatory provisions: Should is used to indicate a goal which must be addressed by the design but is not formally verified.**

On Security Controls

- A combination of hardware, software, communication, physical, personnel, and administrative-procedural safeguards is required for comprehensive security.
  - *Security Controls for Computer Systems – Rand Report – February 1970*
  - *Essentially the original "Orange Book" definition of the "Trusted Computing Base (TCB)"*
  - *The principles are found in NIST 800-53*
- Individual "trusted components(controls)" can facilitate security, but…
  - *Providing satisfactory security controls in a computer system is*
    - A system design problem.
    - A systems security engineering responsibility!

Systems Security Engineering as System Engineering Requirements

- Security mechanisms provide a capability aka. protection
- The capability need for a security mechanism, once ascertained, is specified by security requirements.
- A security mechanism must satisfy its allocated security requirements and behave in a manner that achieves the security policy behavioral intent.
- A NIST security controls(mechanism), must be expressed in terms of security requirements

Primary Types of Requirements

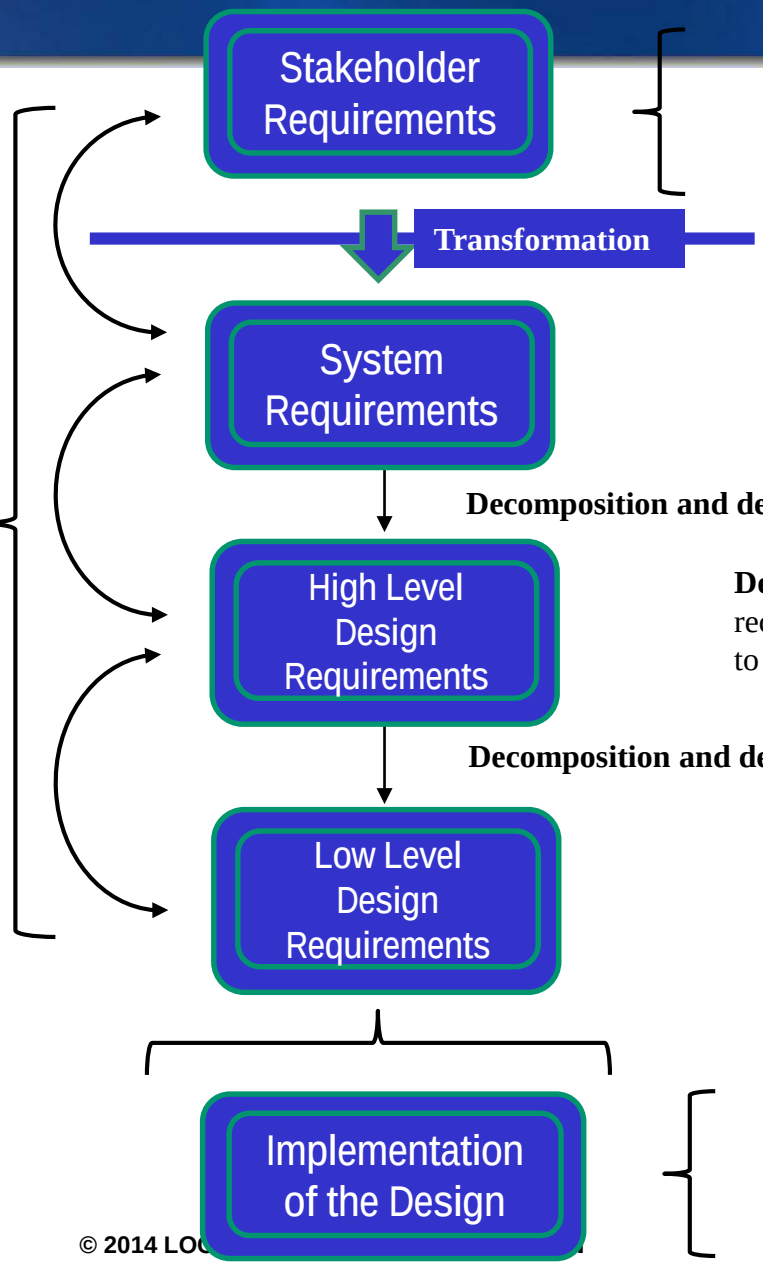
- Stakeholder Requirements (Design independent)
  - *Describe the needs, wants, desires, expectations and perceived constraints of identified stakeholders.*
    - Needs and requirements imposed by society
    - Constraints imposed by an acquiring organization
- System Requirements (Design dependent)
  - *Describe the representation of a future system that will meet stakeholder requirements*
    - Does not imply any specific implementation.
    - Includes the criteria/basis for measurement to determine acceptance by the stakeholder.

Design Independence and Design Dependence are similar concepts to the OMG's Modeling specifications: Platform Independent Model (PIM) / Platform Specific Model (PSM), Or Common Criteria Protection Profiles and Security Targets

Engineering Requirements Relationships

Traceability demonstrates that all requirements have a ***basis for their existence***.

Note: *Not shown is the traceability of stakeholder requirements back to the statement of needs*



Validation demonstrates that the implementation satisfies the ***stakeholder requirements***.
"Did we build the right thing?"

Decomposition and derivation recursively refines design requirements to ***enable implementation***.

Verification demonstrates that the implementation satisfies the ***design requirements***.
"Did we build it right?"

- Functional Baseline: basis for contracting and controlling the system design.
- Allocated Baseline: performance requirements for each configuration item of the system
- Product Baseline: detailed design specification for system elements

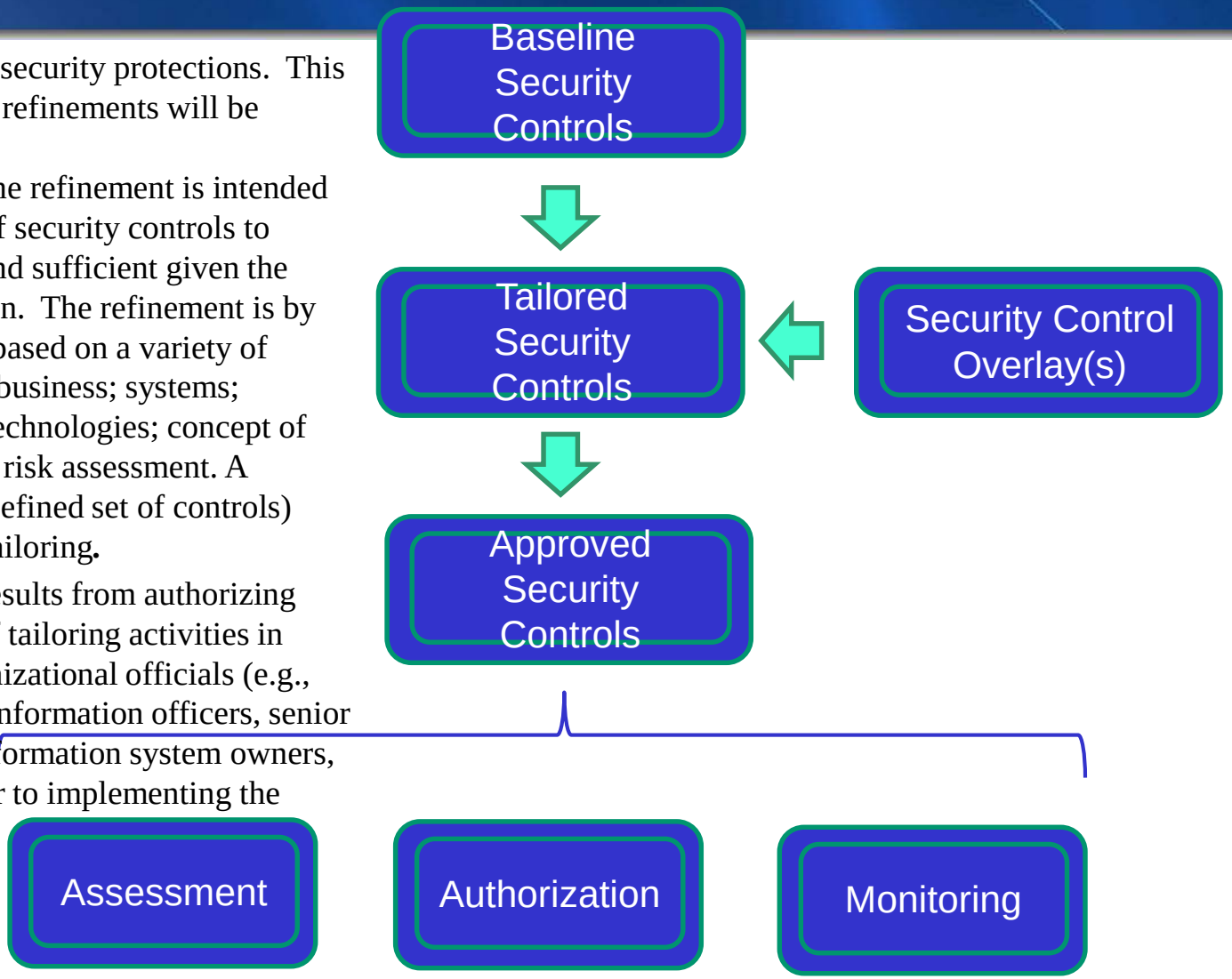
Source: IEEE 15288-2008

Security Controls Relationships

Initial statement of the *desired* security protections. This is the ***starting point*** from which refinements will be made..

Tailored Security Controls. The refinement is intended to modify the initial statement of security controls to ensure that they are necessary and sufficient given the specific needs of the organization. The refinement is by ***tailoring***. The tailoring may be based on a variety of factors that include the mission/business; systems; processes and methods; use of technologies; concept of operation; the environment; and risk assessment. A security controls ***overlay*** (a predefined set of controls) may be used as an input to the tailoring**.**

Approved Security Controls results from authorizing officials approving the results of tailoring activities in coordination with selected organizational officials (e.g., risk executive [function], chief information officers, senior information security officers, information system owners, common control providers) prior to implementing the security controls.



Source: NIST SP800-53 rev4

Key Differences

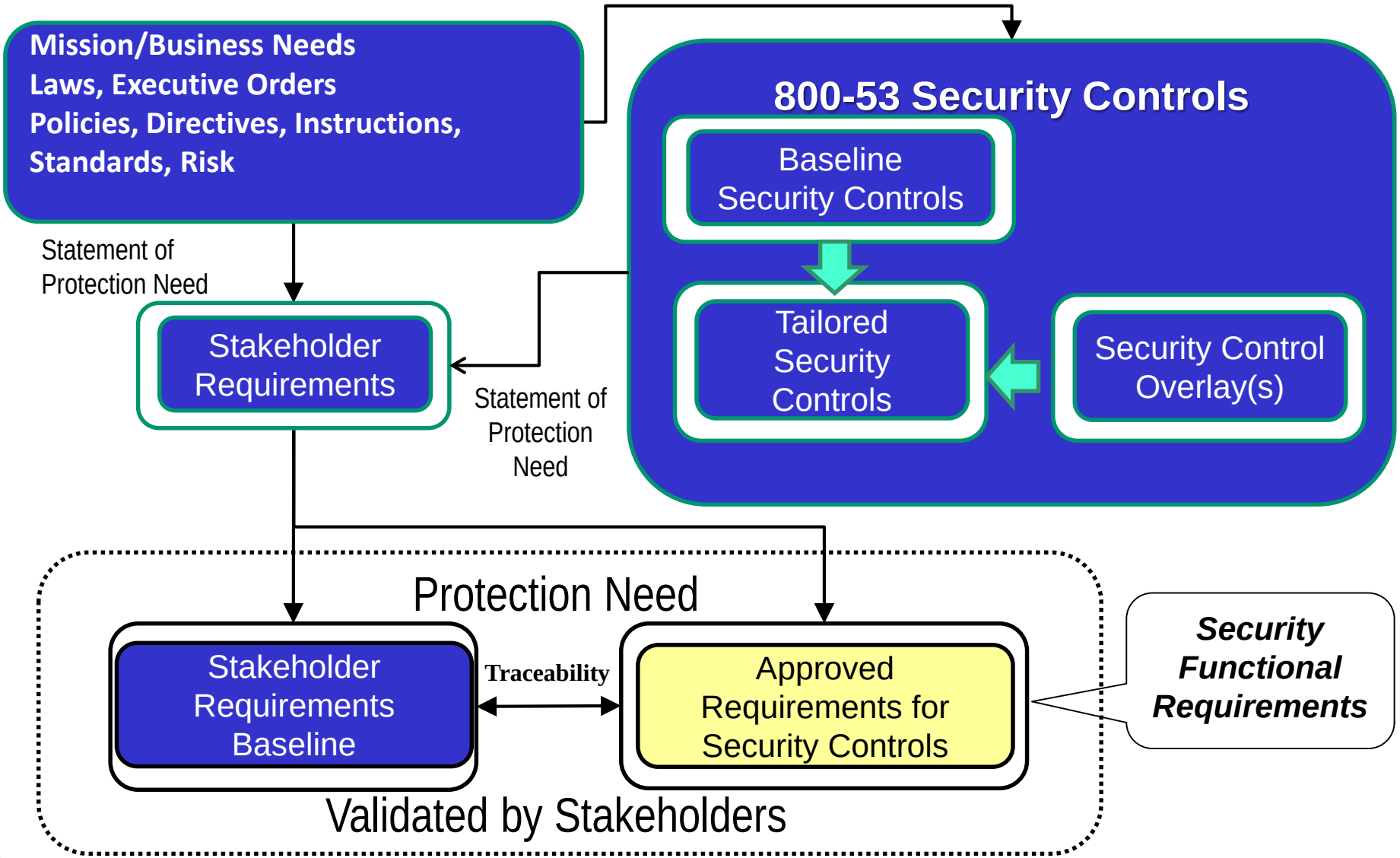
Controls	Requirements
• No distinction between design-independent and design-dependent views	• Distinct design-independent and design-dependent views
• No levels of design abstraction	• Multiple levels of design abstraction
• Configuration control?	• Each requirement type and abstraction maintained under configuration control
• Traceability?	• End-to-end traceability

MERGING 800-53 WITH SYSTEMS SECURITY ENGINEERING (NIST SP800-160)

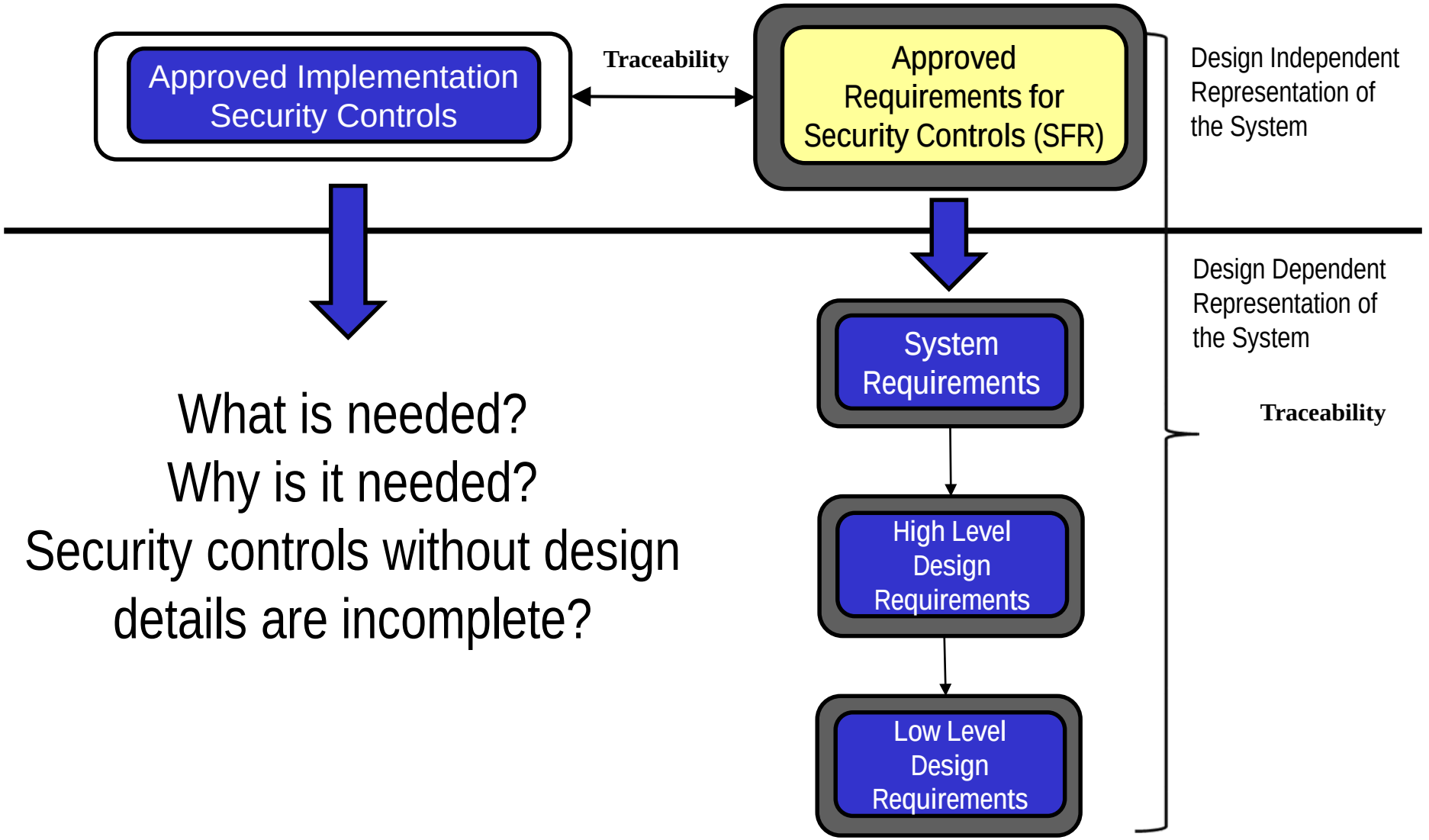
Assumptions … Ground Rules

- **Leverage requirements engineering**
  - ***Distinguish the two types of requirements***
    - design independent, stakeholder requirements
    - design dependent, system requirements, high level requirements, low level requirements
  - ***Multiple baseline views***
  - ***Traceability***

Design Independent Viewpoint



Design Dependent View



TRUSTWORTHINESS

Trustworthiness

- The measure of confidence to which an information system can be expected to preserve the *confidentiality*, *integrity*, and *availability* of the information being processed, stored, or transmitted across a full range of threats.

- Trustworthy information systems are systems that are believed to be *capable* of operating within defined levels of risk despite—
  - *Environmental disruptions.*
  - *Human errors.*
  - *Component faults, errors, failures.*
  - *Purposeful attacks.*

People place “trust” in a system when dependability is demonstrably acceptable!

Factors in Determining Trustworthiness

- Security Functionality (Protection Capability)
  - *Security features, functions, mechanisms, services, procedures, of the system*
- Employment of Security Functionality (Policy Enforcement)
  - *Organization security policy, automated security policy, policy-based processes and procedures, policy-based configuration*
- Security Assurance (Verification and Validation)
  - *Measure of confidence about security functionality*
    - implemented correctly
    - operating as intended
    - producing the desired outcome
    - susceptible to threats (vulnerability)

Verifying Functionality …

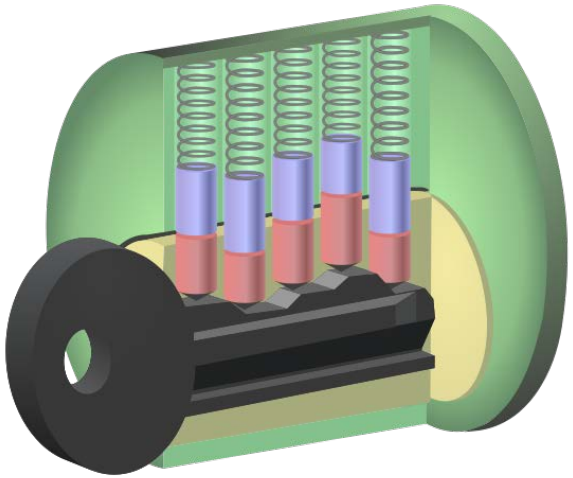
… and Obtaining Assurance

FUNCTIONALITY

What is the behavior to be confirmed?

Is the behavior that is confirmed good enough – does it provide sufficient assurance?

ASSURANCE



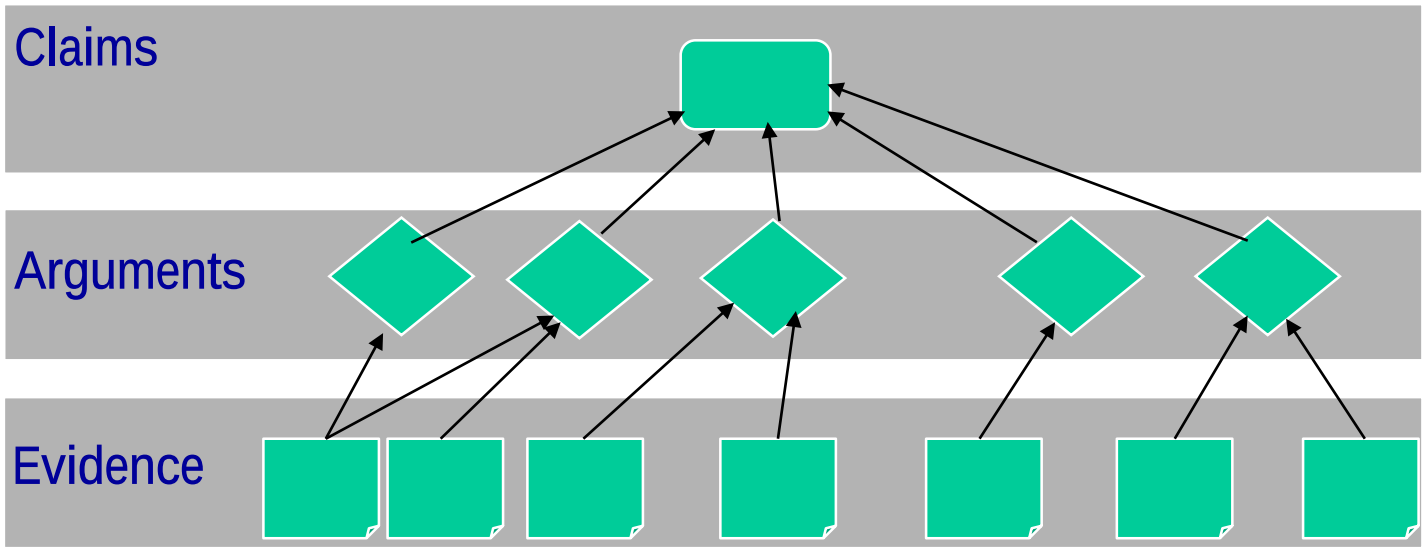
What amount of assurance is necessary to accept the functionality?
And what is necessary that can be known ONLY from assessing the design and the mechanism?

Dimensions of Assurance

- Satisfactory design requirements
- Sufficiency of Design
- Achieves desired outcomes
- Absence of unspecified and emergent behavior
- Security policy enforcement
- Residual vulnerability and susceptibility to threat
- Absence of known/identified vulnerabilities
- Ability to resist, withstand, and recover from attack, fault, error, failure, and misuse
- … and many others …

Assurance and Evidence

- **Assurance is best grounded in relevant and credible evidence used to substantiate a claim**
  - ***"the system is acceptably secure"***
- **An *assurance case* relate claims and evidence**
  - ***Via structured argumentation and argument patterns***
  - ***Automated via assurance case tools***
    - see OMG Structured Assurance Case Metamodel specification / tools



INTEGRATING RMF SECURITY CONTROLS AND SSE

Secure System Design Principles and Practices

Architectural Design

- Reduced Complexity
- Modularity and Layering
- Defense-in-Depth
- Least Common Mechanism
- Minimized Sharing
- Secure System Evolution

Trustworthiness

- Trusted Components
- Hierarchical Trust
- Hierarchical Protection
- Minimized Security Elements
- Least Privilege
- Separation of Privilege
- Self-Reliant Trustworthiness
- Secure Distributed Composition
- Trusted Communication Channels

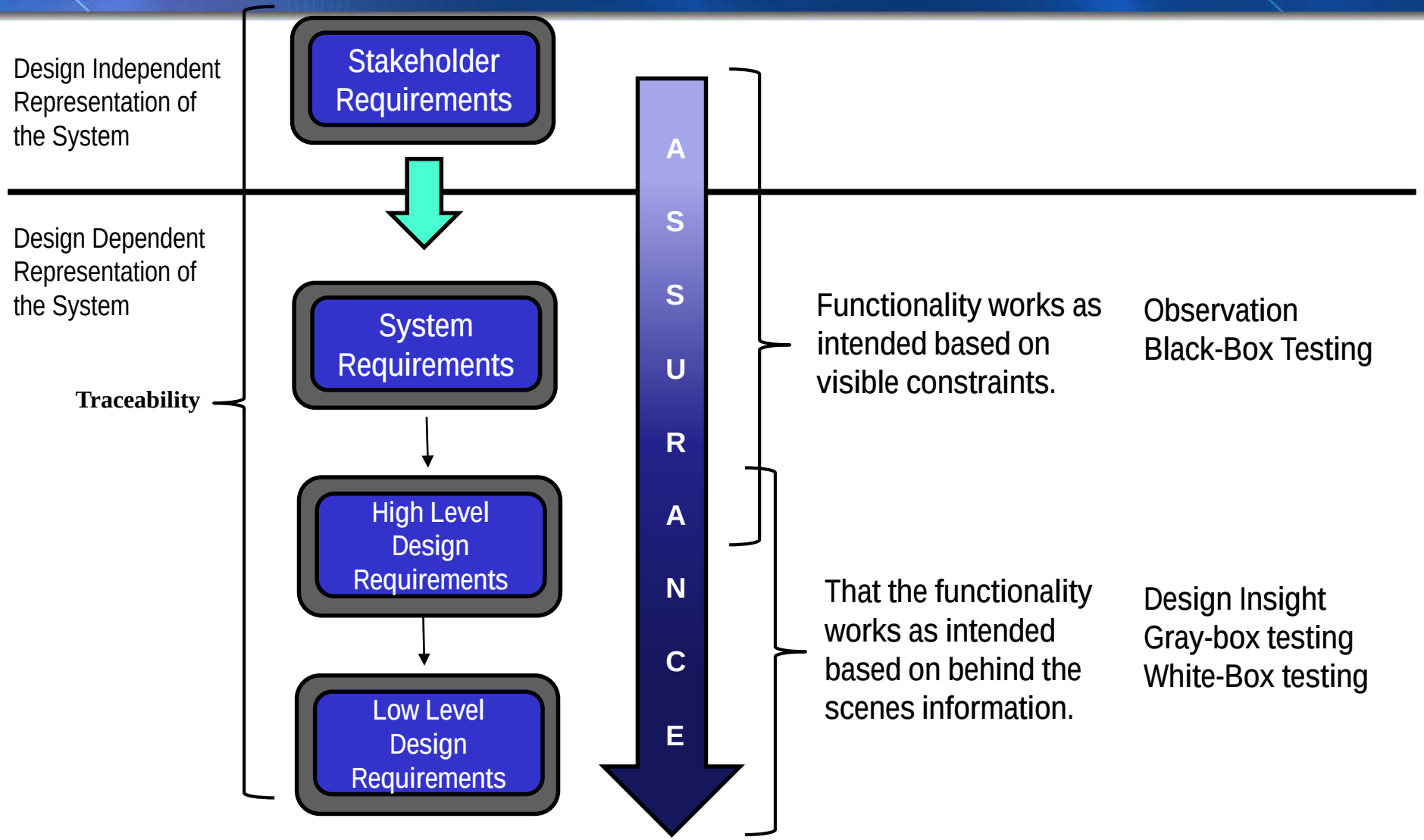
Function and Behavior

- Continuous Protection
- Complete Mediation
- Secure Metadata Management
- Self-Analysis
- Secure Defaults
- Secure Failure and Recovery

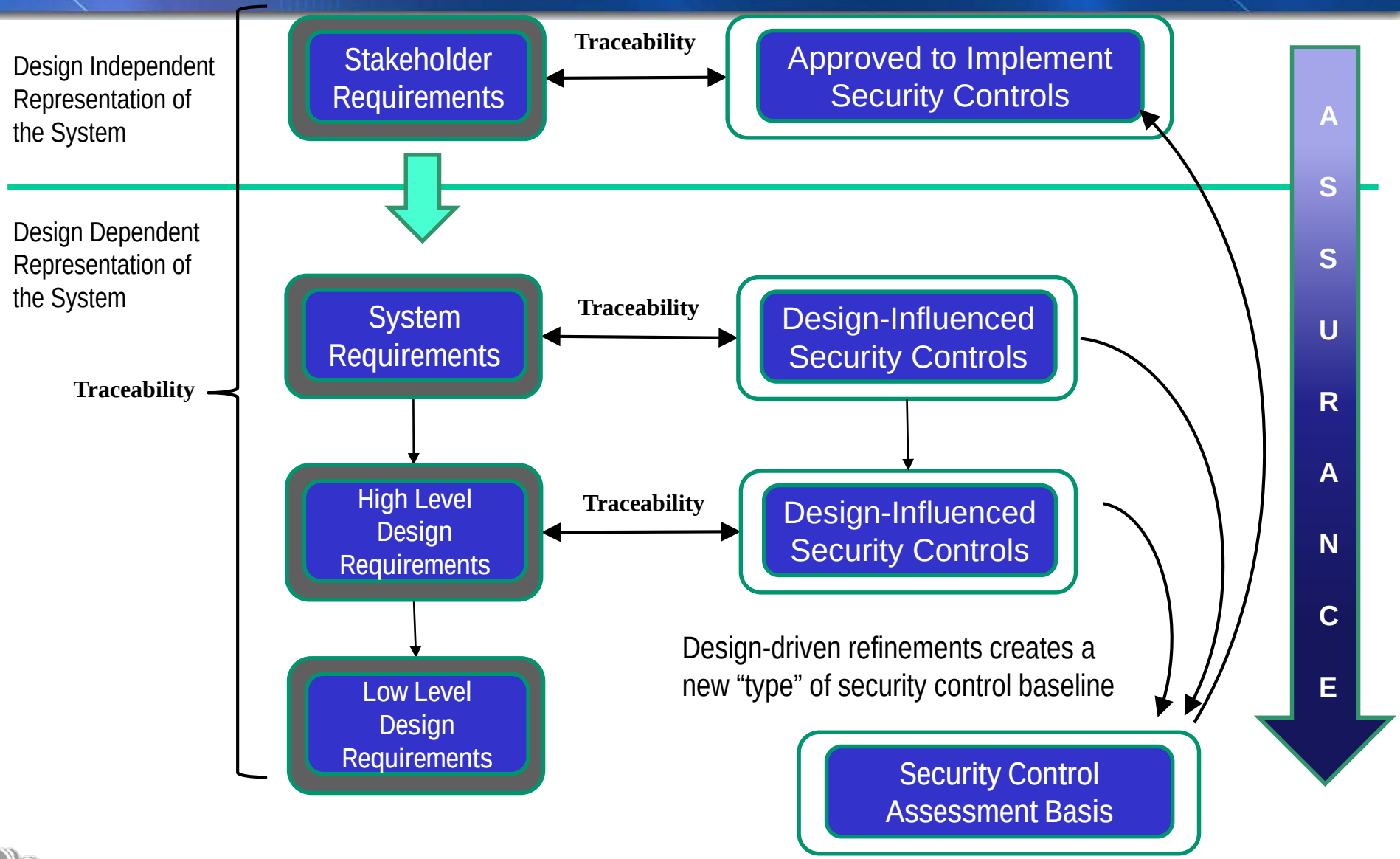
Life Cycle

- Design for Security
- Repeatable, Documented Procedures
- Procedural Rigor
- Secure System Modification
- Sufficient Documentation
- Sufficient Evidence Base

Design Dependent View w/ Assurance



Integrating Security Controls with Systems Engineering Proposed Model



Design Dependent View: New Model Key Relationships

- Stakeholder requirements trace to the equivalent statement of Approved to Implement Security Controls
- The Security Control Assessment Basis is used to perform security control assessment
- The details captured in the Security Control Assessment Basis matches the level at which Security Control Assessment will be conducted, and no more.
- The level of detail is commensurate to the assurance to be demonstrated and the evidence required to provide a compelling argument to authorization stakeholders.

Example: Common Criteria EAL 1-4

Design Dependent View: New Model Benefits

- Security controls representation and decomposition parallels the engineering requirements
- Full traceability exists
  - *Separately within requirements and controls*
  - *Between corresponding views of requirements and controls*
- Facilitates security control assessment tied to assurance goals
- Provides added-value in the absence of systems engineering
  - *Does not break current NIST 800-53 model*

SYSTEMS SECURITY ENGINEERING (NIST SP 800-160)

Integrated Systems and Security Engineering

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

Grounded in foundational systems theory to build systems able to withstand the modern day threat environment!

Strategy

- Align to IEEE Std 15288-2008 (ISO/IEC 15288) to facilitate communication across historically separated communities
  - *Systems and Software Engineering – System Life Cycle Processes*

System Security Engineering

- Applies scientific, mathematics, and engineering principles and methods to deliver trustworthy security protection capability that
  - satisfies stakeholder needs;
  - presents residual risk deemed acceptable and manageable to stakeholders, and;
  - is seamlessly integrated into the delivered system.
- Leverages multiple security specialties and integrates across the contributions of those specialties
- Provides security relevant perspective, enhancements, additions, and contributions to systems engineering process activities, tasks, and outcomes

Systems Security Engineering

… a specialty discipline of Systems Engineering

Systems Engineering [excerpts from INCOSE definition/elaboration]	**Systems Security Engineering** [adaptation of the INCOSE definition/elaboration]
ensures stakeholder needs are satisfied in a high quality, trustworthy, cost efficient, risk tolerant, and schedule-compliant manner throughout a system's entire life cycle	ensures stakeholder *protection needs* are satisfied in a high quality, trustworthy, cost efficient, risk tolerant, and schedule-compliant manner throughout a system's entire life cycle
delivers solutions and the technical information necessary to support stakeholders' life cycle risk management processes and to support solutions throughout its life cycle	delivers *trustworthy* solutions and the *security* technical information necessary to support stakeholders' life cycle *security* risk management processes and to *securely* support solutions throughout its life cycle
leverages a variety of specialty engineering disciplines and serves as the integrating mechanism for the technical and technical-management efforts	leverages a variety of specialty *security* engineering disciplines and serves as the integrating mechanism for the *security* technical and technical-management efforts

IEEE 15288 System Life Cycle Processes

Agreement Processes	Organization Project-Enabling Processes	Project Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Project Portfolio Management • Human Resource Management • Quality Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement	• Stakeholder Requirements Definition • Requirements Analysis • Architectural Design • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

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

"Software Assurance: The Necessary Evil of Safety/Security Critical Systems"

- **Concluded with Unified Requirements**
  - ***Product Functional Requirements***
    - Specify the thing(s) the system is being built to do!
    - These Requirements define the capabilities to be implemented
  - ***Security / Safety Functional Requirements***
    - The functions which enforce the security policy or safety critical requirements
  - ***Security / Safety Assurance Requirements.***
    - Define and document how well ALL Functional Requirements are implemented (a level of confidence)

The End Goal SSE and SE!

Build the Right Thing …,

Build It Right …,

and then Continuously Monitor

Accepted Safety Process vs. Current Enterprise IA Process

Imagine if COTS Aviation Safety were treated with the same attitude as current “security practices” in Enterprise Information Assurance Architectures!!!

Disclaimer: Photo edited with flames for emphasis of slide context!

Questions.