NIST SP 800-160

Volume 1, Revision 1

Transitioning to Engineering-based Cybersecurity

Applying Design Principles to Develop Trustworthy Secure Systems

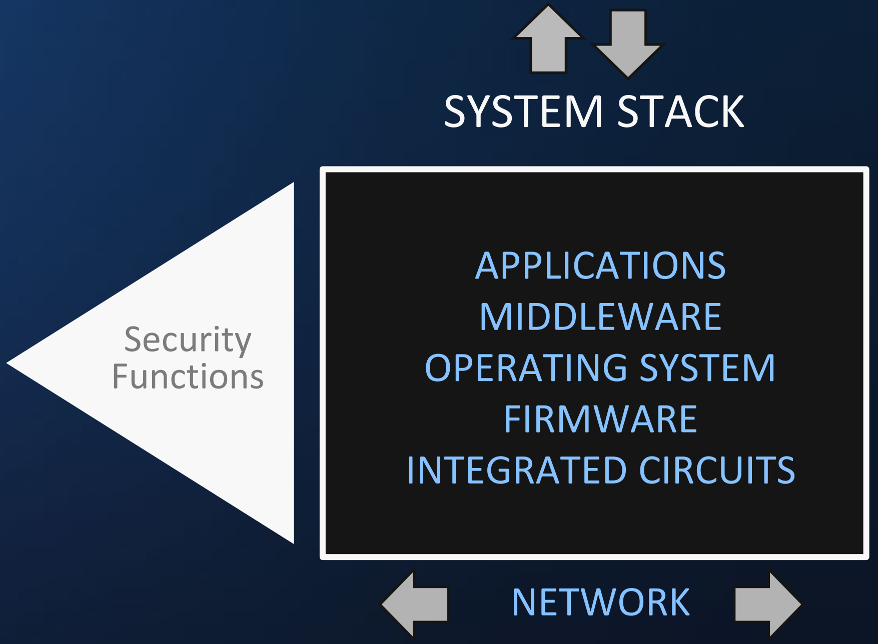
Complexity

Millions, Billions, and Trillions of Everything

The Current Landscape…

Little or no understanding of what’s in the ”black box.”

Transparency
Traceability
Visibility
Assurance



SYSTEM STACK

Security Functions

APPLICATIONS
MIDDLEWARE
OPERATING SYSTEM
FIRMWARE
INTEGRATED CIRCUITS

NETWORK

Today’s systems…

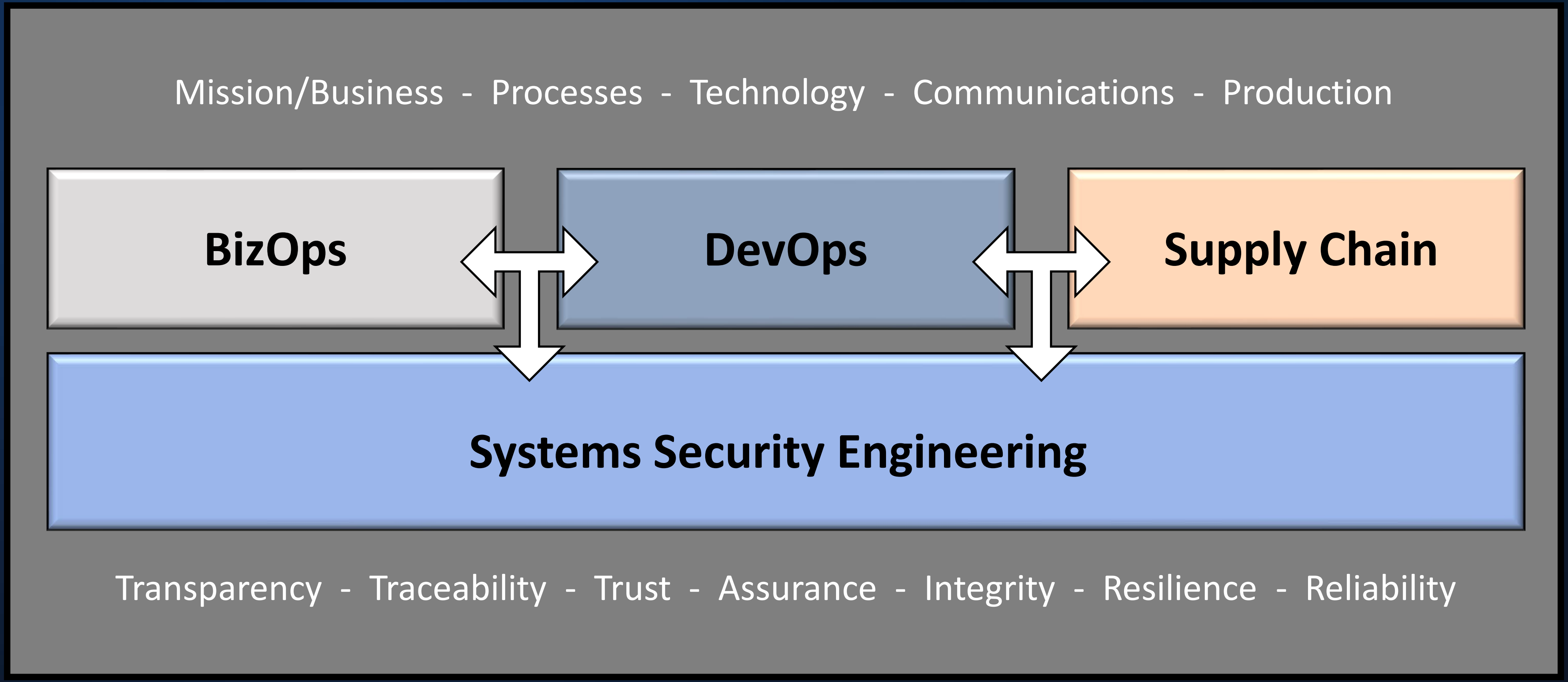
- Present a uniform attack surface
- Rely on a single-dimension protection strategy based on penetration resistance
- Are susceptible to destructive cyber-attacks

“Security is embedded in systems. Rather than two engineering groups designing two systems, one intended to protect the other, systems engineering specifies and designs a single system with security embedded in the system and its components.”

-- *Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts, 2021 INCOSE International Symposium*

The Ecosystem

Framework for Securing Organizational Systems and Assets



Mission/Business - Processes - Technology - Communications - Production

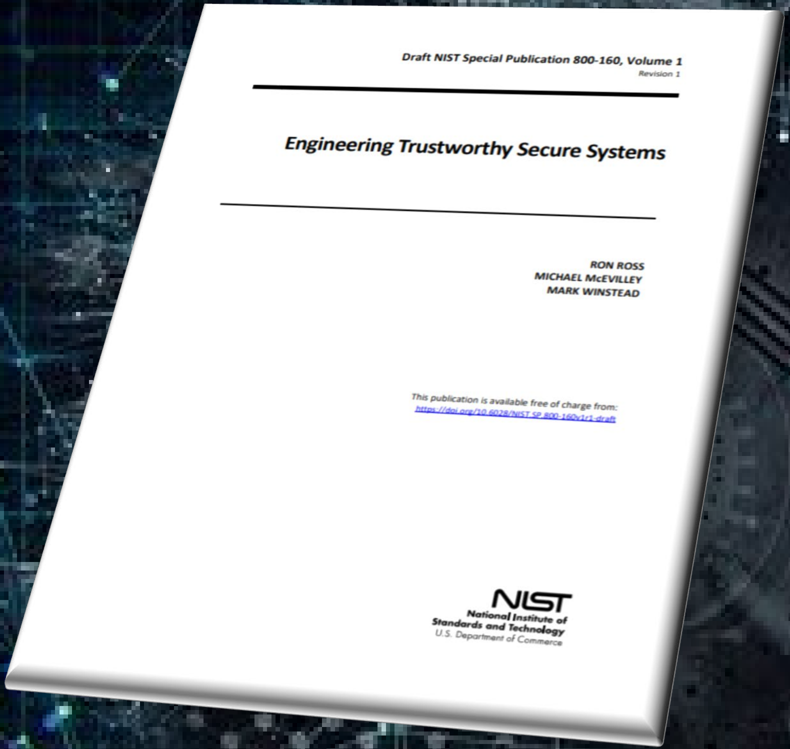
BizOps

DevOps

Supply Chain

Systems Security Engineering

Transparency - Traceability - Trust - Assurance - Integrity - Resilience - Reliability



Draft NIST Special Publication 800-160, Volume 1
Revision 1

Engineering Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
MARK WINSTEAD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v1r1-draft

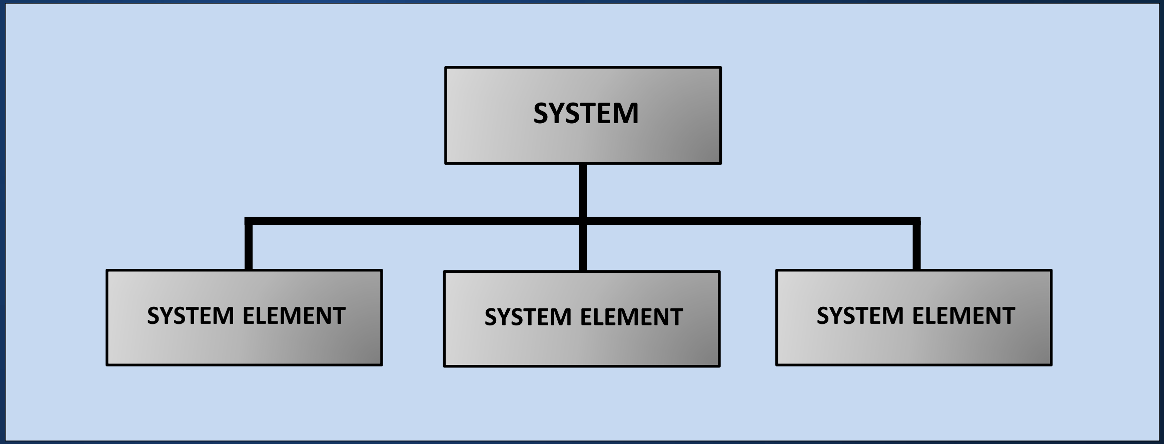
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Multidimensional Protection Strategy

- Penetration-resistant architecture
- Damage-limiting operations
- Designs to achieve trustworthy secure systems

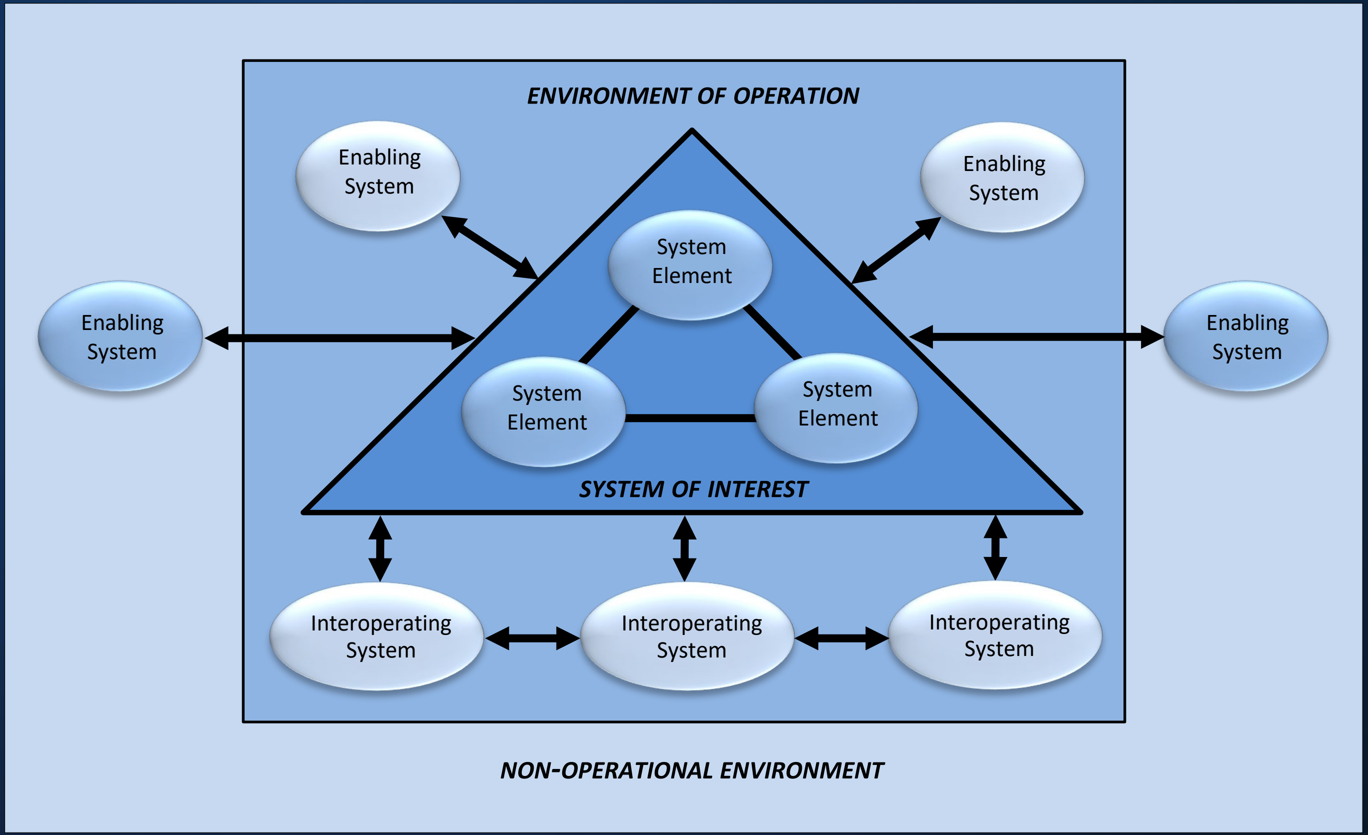
https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/draft

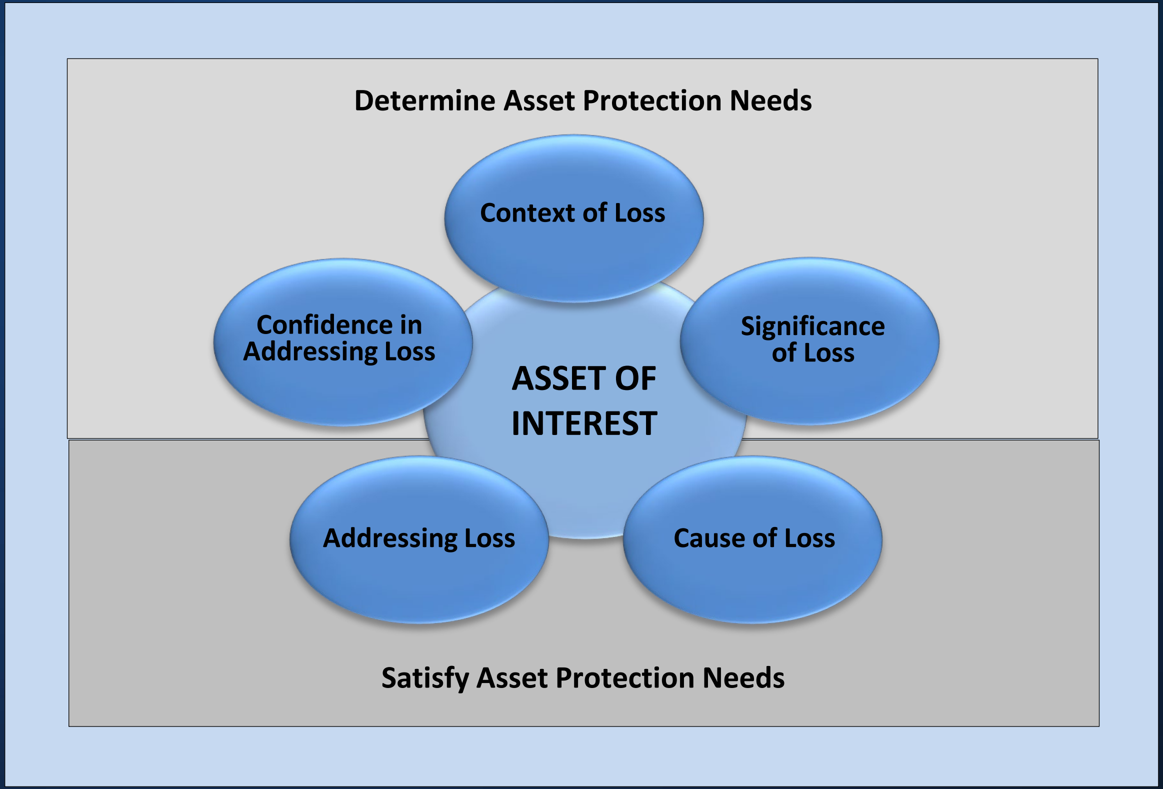
What is a System?



- An arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. Systems can be physical or conceptual, or a combination of both. [ISO/IEEE 15288] [INCOSE]

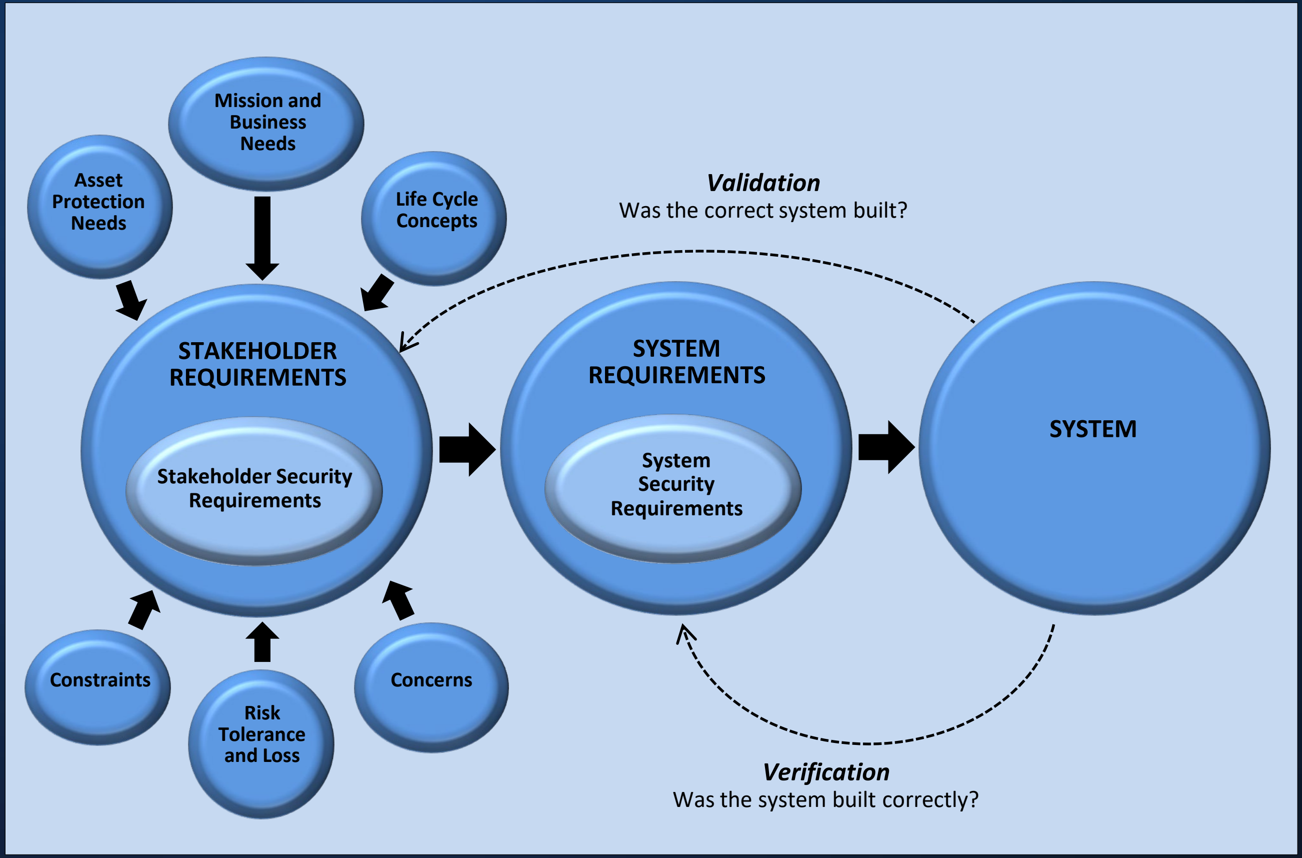
System of Systems




Determine Asset Protection Needs
Context of Loss
Confidence in Addressing Loss
Significance of Loss
ASSET OF INTEREST
Addressing Loss
Cause of Loss
Satisfy Asset Protection Needs

Security Engineering Focuses on Asset Loss

Requirements Engineering



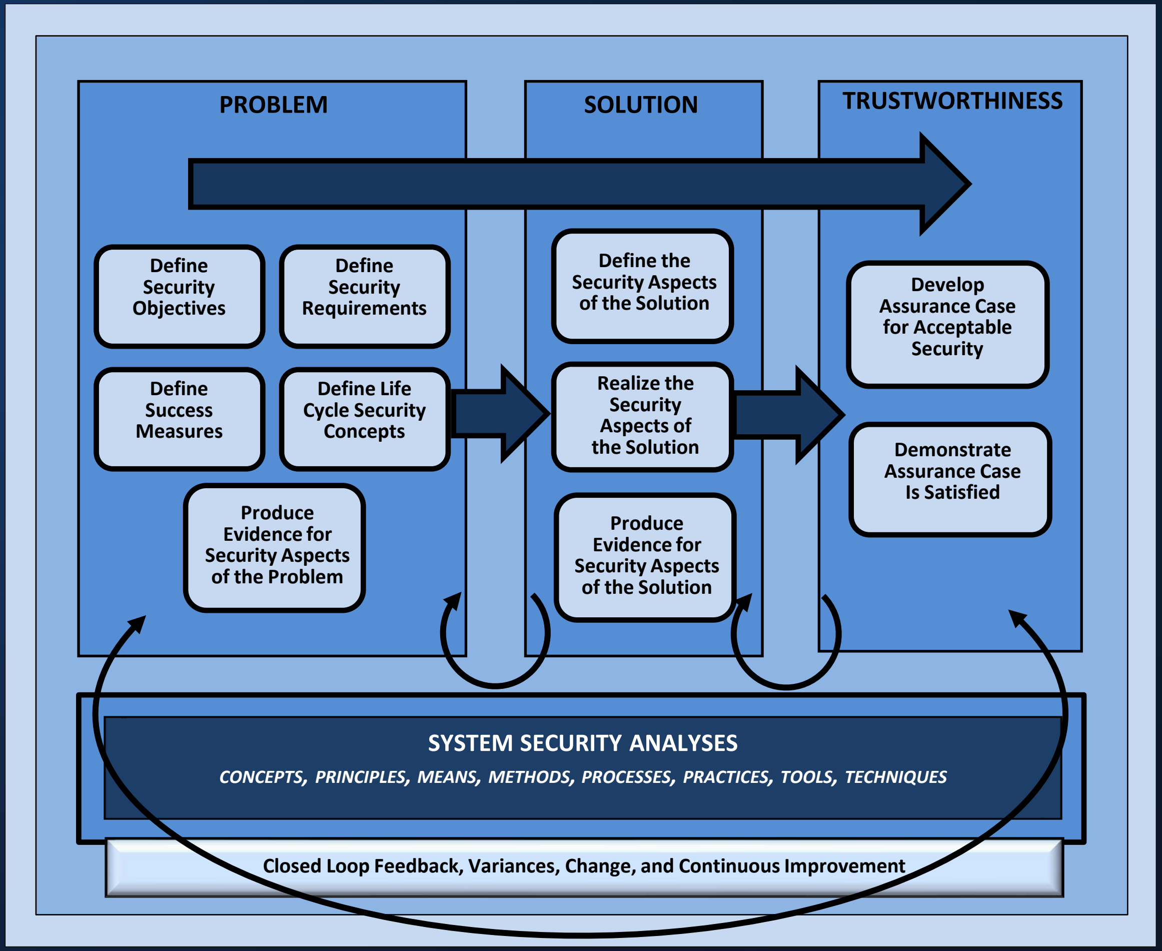
Validation
Was the correct system built?

Verification
Was the system built correctly?

Systems Security Engineering

Characteristics

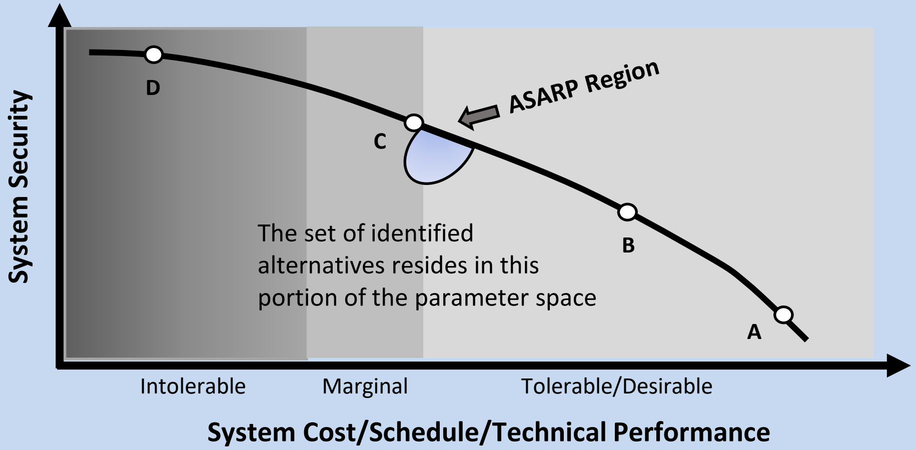
- Disciplined and structured development process
- Integrates security into the system life cycle
- Applied to all elements in the system stack
- Can be tailored and implemented in agile development processes
- Provides needed traceability of requirements and transparency into development processes leading to greater trust in systems and system elements


PROBLEM
SOLUTION
TRUSTWORTHINESS
Define Security Objectives
Define Security Requirements
Define Success Measures
Define Life Cycle Security Concepts
Produce Evidence for Security Aspects of the Problem
Define the Security Aspects of the Solution
Realize the Security Aspects of the Solution
Produce Evidence for Security Aspects of the Solution
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

No system can provide *absolute* security due to the limits of human certainty, the uncertainty that exists in the life cycle of every system, and the constraints of cost, schedule, performance, feasibility, and practicality.

As such, trade-offs made routinely across contradictory, competing, and conflicting needs and constraints are optimized to achieve *adequate* security, which reflects a decision made by stakeholders.

Adequate Security



A: Large increases in system security can be achieved by addressing basic security issues. Little cost, schedule, or technical impact.

B: Basic security issues have been addressed but significant security can still be “bought” without failing to meet cost, schedule, or technical performance requirements.

C: Limit of ASARP regime has been reached but significant increases in security can be “bought” without exceeding tolerable limits of cost, schedule, or technical performance requirements.

D: Limit of achievable security has been met. Increased security cannot be “bought” at any cost.

Adapted from NASA.

As secure as reasonably practicable…

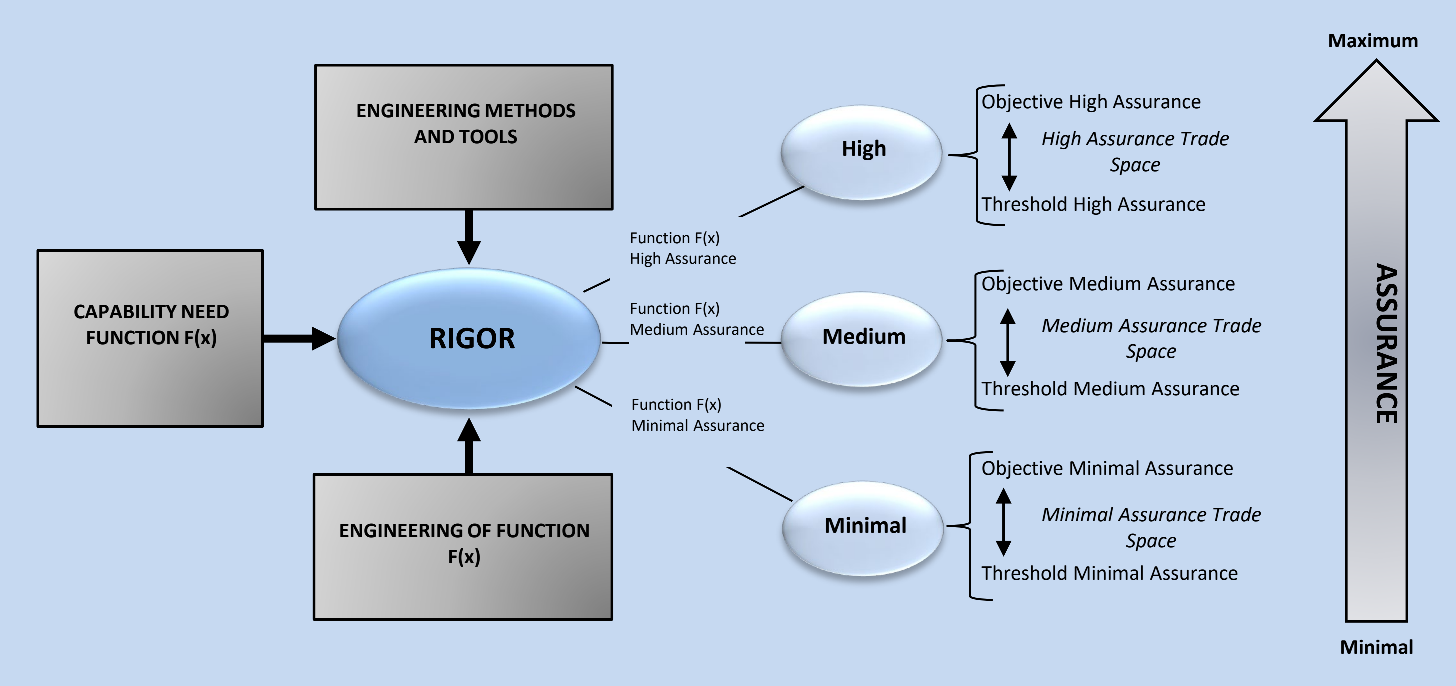
Assurance Case

An *assurance case* is a reasoned, auditable artifact that is created to support the contention that a top-level claim is satisfied.

An assurance case contains:

- One or more claims about properties
- Arguments that logically link the evidence and any assumptions
- A body of evidence
- Justification of the choice of a top-level claim and the method of reasoning

Assurance and Rigor



ENGINEERING METHODS AND TOOLS
CAPABILITY NEED FUNCTION F(x)
RIGOR
ENGINEERING OF FUNCTION F(x)
Function F(x) High Assurance
Function F(x) Medium Assurance
Function F(x) Minimal Assurance
High
Medium
Minimal
Objective High Assurance
High Assurance Trade Space
Threshold High Assurance
Objective Medium Assurance
Medium Assurance Trade Space
Threshold Medium Assurance
Objective Minimal Assurance
Minimal Assurance Trade Space
Threshold Minimal Assurance
Maximum
ASSURANCE
Minimal

Key Issues for Building Trustworthy Secure Systems

Systems Security Engineering

ISO/IEC/IEEE 15288:2015

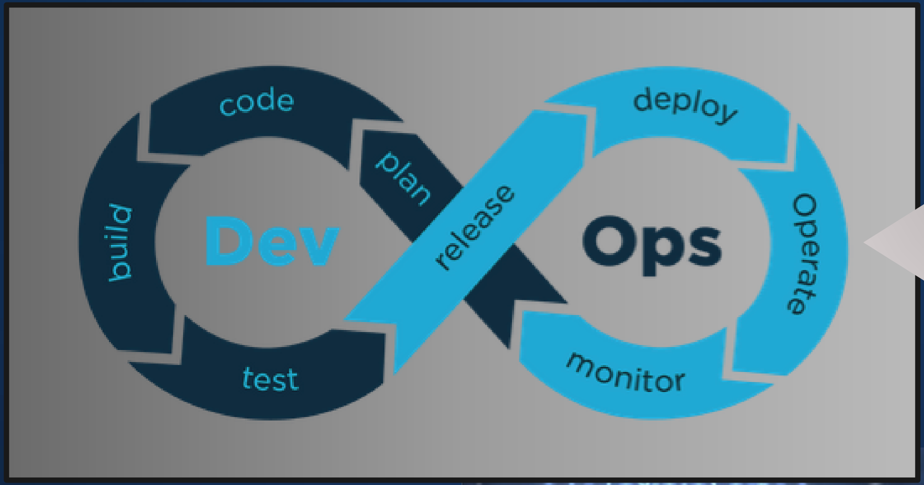
Systems and software engineering — System life cycle processes

"Secure By Design"

- 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

NIST SP 800-160 Volume 1

Next Generation Development Processes



Credit: Network Intelligence

Security Integration

DevSecOps

AGILE DEVELOPMENT
SECURE ARCHITECTURE
APPLICATION SECURITY
CODE REVIEW/TESTING
SECURE CONFIGURATION
SECURE OPERATIONS

Transparency
Traceability
Visibility
Assurance

Ron Ross

Email: ron.ross@nist.gov

Mobile: (301) 651-5083

Web: http://csrc.nist.gov

Twitter: https://twitter.com/ronrossecure

LinkedIn: https://www.linkedin.com/in/ronrossecure

SSE Project: https://csrc.nist.gov/Projects/Systems-Security-Engineering-Project