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

Developing Cyber Resilient Healthcare Systems

A Systems Security Engineering Approach

Ron Ross

The Problem

Today’s healthcare systems are complex and brittle; they rely on a one-dimensional protection strategy of penetration resistance and are highly susceptible to devastating cyber-attacks.

Complexity

Attack Surface

“Two sides of the same coin”

Adversarial and Non-Adversarial

Threats to Healthcare Systems

A Holistic Systems Engineering Perspective

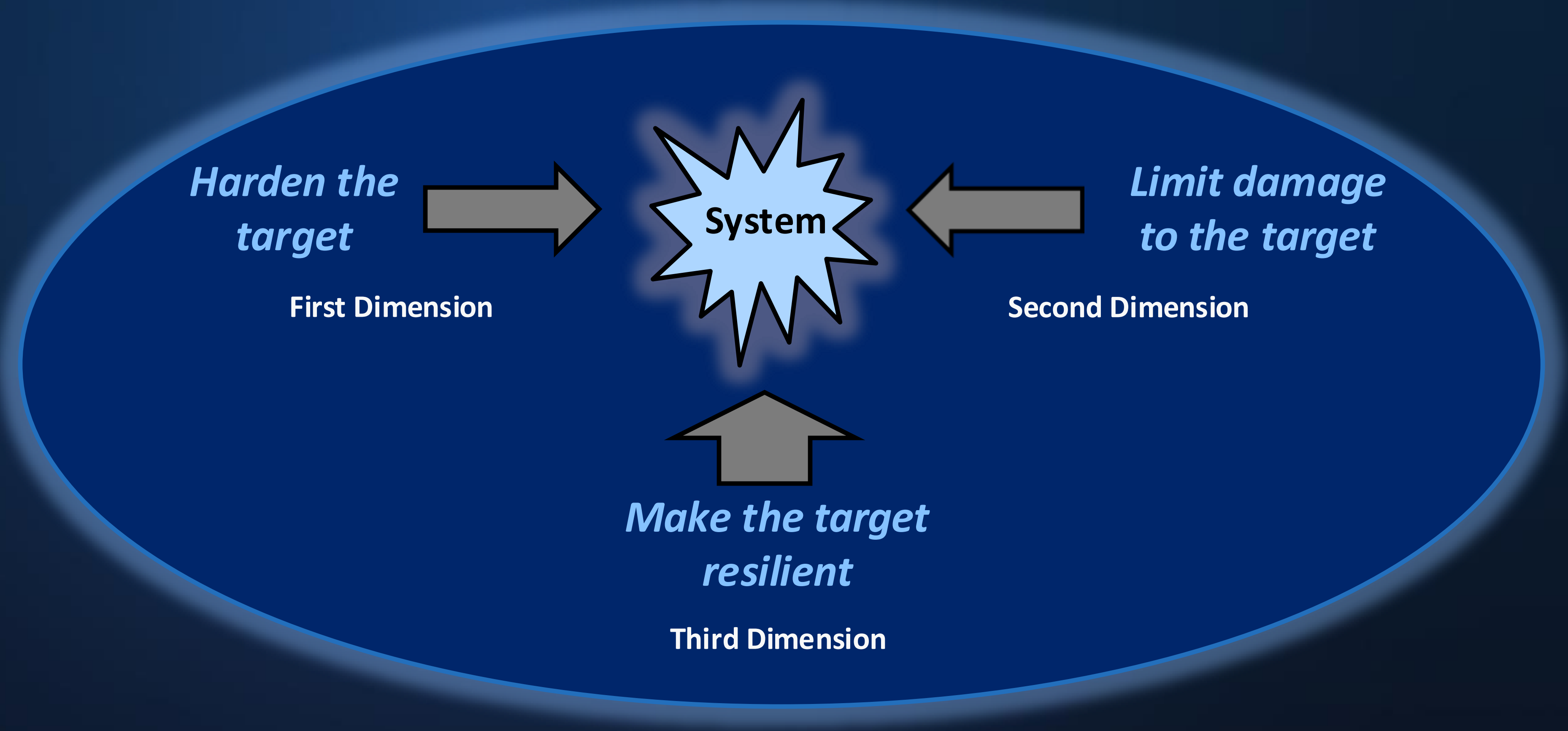
- Structural failures of organization-controlled resources
- Natural and man-made disasters, accidents, and failures
- Human errors of omission or commission
- Hostile cyber or physical attacks

Source: NIST SP 800-30

The Solution

Develop and implement a “multi-dimensional protection strategy” that includes damage limiting system architectures and systems that are cyber resilient.

Multi-Dimensional Protection Strategy



Harden the target

First Dimension

Limit damage to the target

Second Dimension

Make the target resilient

Third Dimension

Damage Limitation

In Time

- Virtualization
- Micro virtualization
- Limits time on target for adversaries

In Space

- Zero trust architectures
- Domain separation
- Network segmentation
- Micro segmentation
- Impedes lateral movement of adversaries

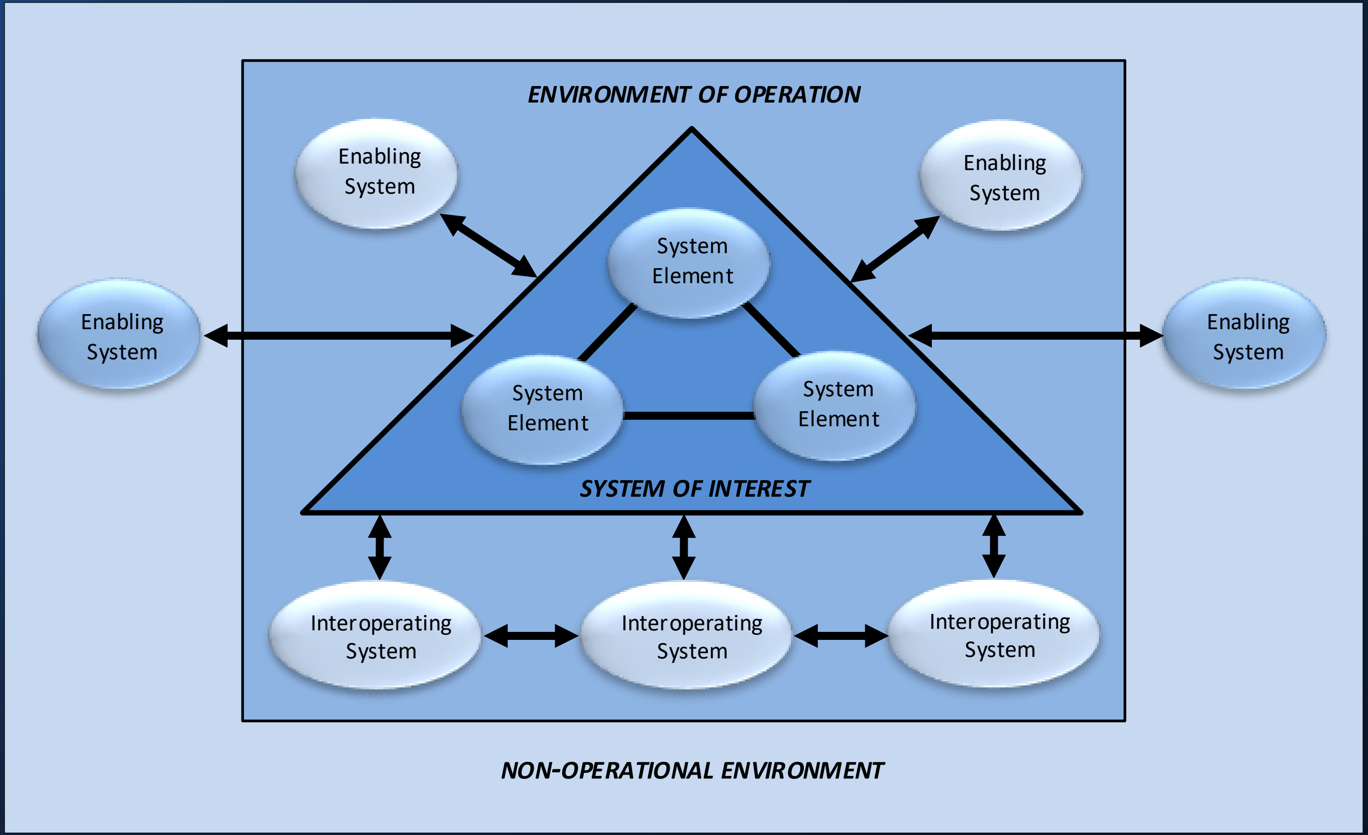
Cyber Resiliency

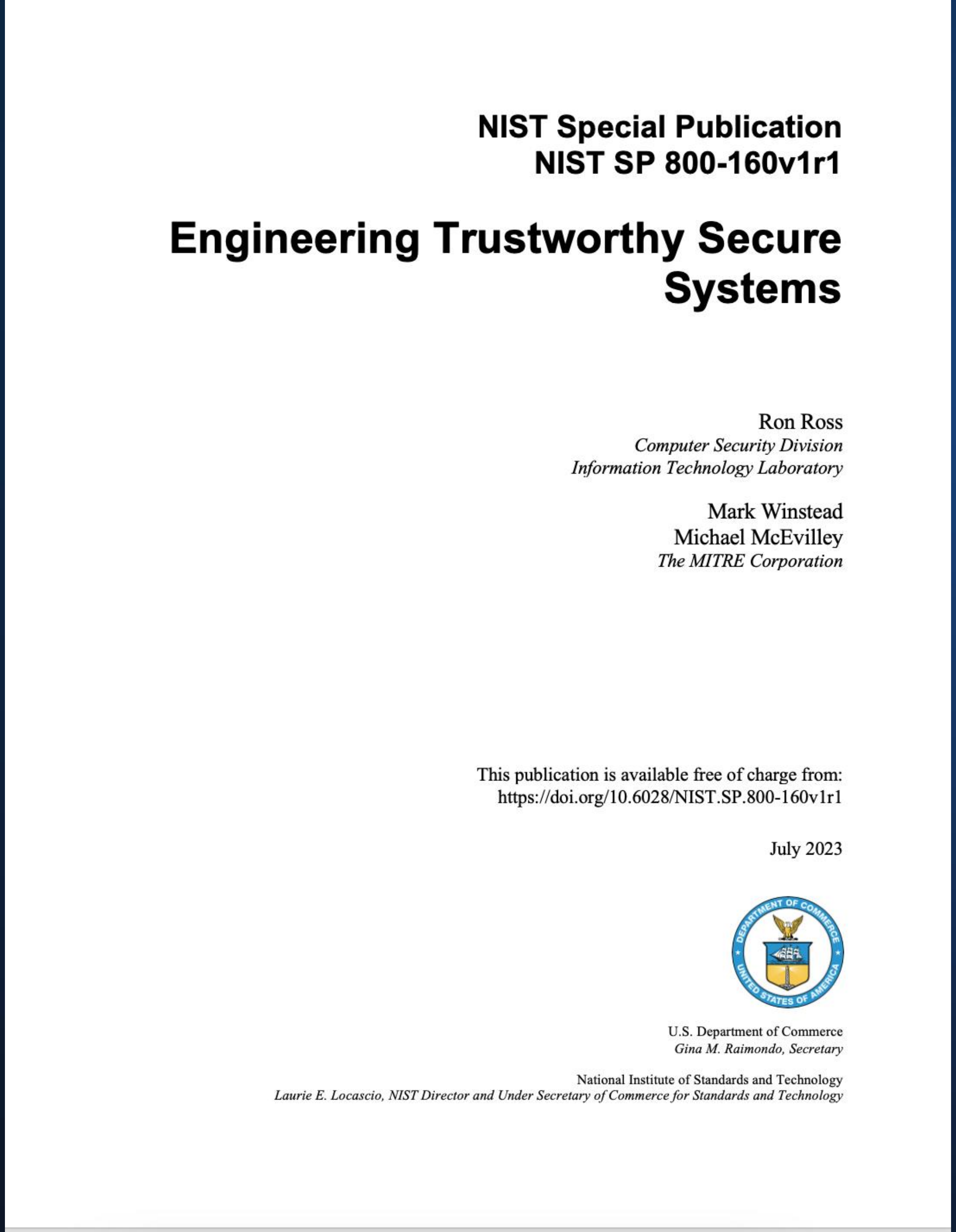
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

System of Systems

From Medical Devices to Hospital Administration Systems

Critical dependencies and relationships among internal system elements, systems within healthcare enterprise environments, and systems in external environments that affect security solutions.





NIST Special Publication
NIST SP 800-160v1r1

Engineering Trustworthy Secure Systems

Ron Ross
Computer Security Division
Information Technology Laboratory

Mark Winstead
Michael McEvilley
The MITRE Corporation

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

July 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

ISO/IEC/IEEE 15288:2022

Systems and software engineering — System life cycle processes

- 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

https://doi.org/10.6028/NIST.SP.800-160v1r1

Security Design Principles

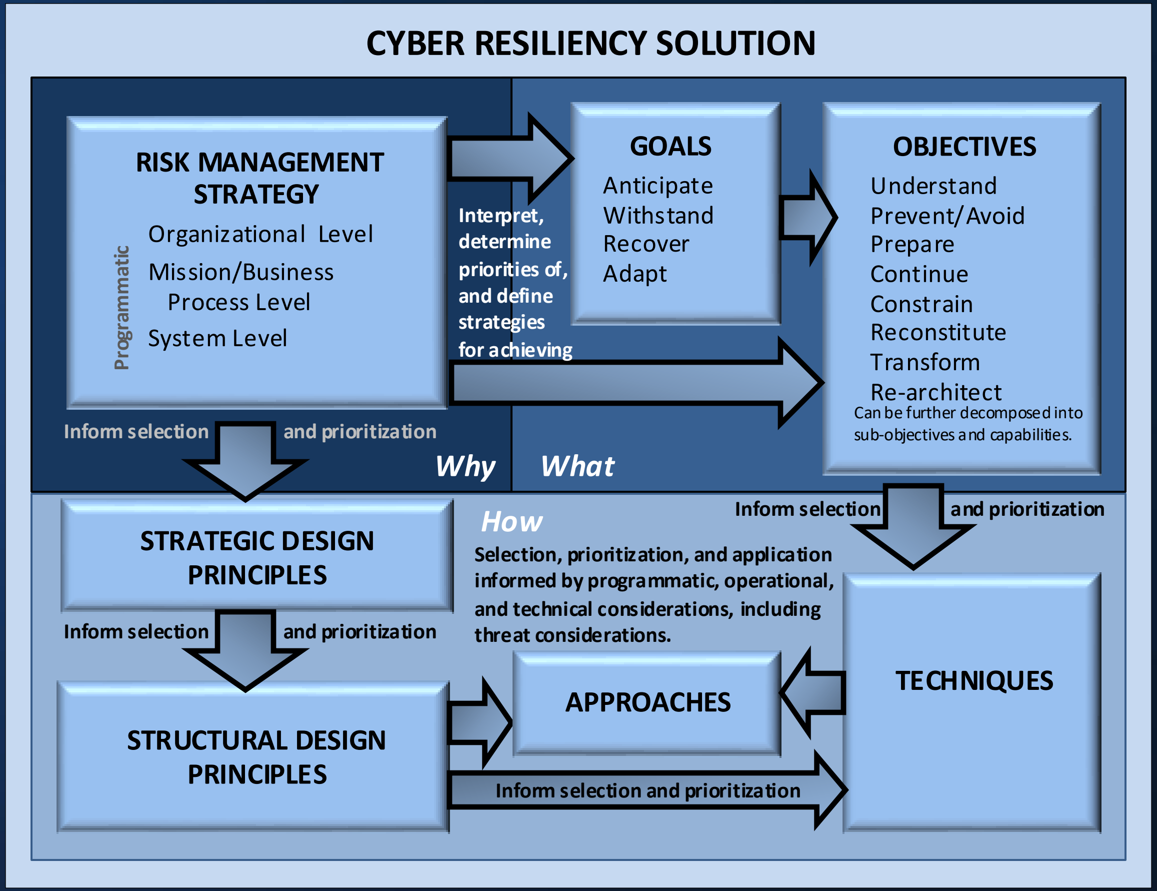
NIST SP 800-160, Volume 1

- **Anomaly Detection**
- Clear Abstractions
- Commensurate Protection
- Commensurate Response
- Commensurate Rigor
- Commensurate Trustworthiness
- Compositional Trustworthiness
- Continuous Protection
- **Defense In Depth**
- Distributed Privilege
- Diversity (Dynamicity)
- **Domain Separation**
- Hierarchical Protection
- **Least Functionality**
- **Least Persistence**
- **Least Privilege**
- Least Sharing
- Loss Margins
- **Mediated Access**
- Minimal Trusted Elements
- Minimize Detectability
- Protective Defaults
- Protective Failure
- Protective Recovery
- **Reduced Complexity**
- **Redundancy**
- Self-Reliant Trustworthiness
- Struct. Decomposition/Composition
- Substantiated Trustworthiness
- Trustworthy System Control

Cyber Resiliency Engineering Framework

- Goals
- Objectives
- Techniques
- Approaches
- Strategic Design Principles
- Structural Design Principles

NIST SP 800-160, Volume 2



CYBER RESILIENCY SOLUTION

RISK MANAGEMENT STRATEGY

Programmatic

Organizational Level

Mission/Business Process Level

System Level

Interpret, determine priorities of, and define strategies for achieving

GOALS

Anticipate
Withstand
Recover
Adapt

OBJECTIVES

Understand
Prevent/Avoid
Prepare
Continue
Constrain
Reconstitute
Transform
Re-architect

Can be further decomposed into sub-objectives and capabilities.

Inform selection and prioritization

Why

What

How

Selection, prioritization, and application informed by programmatic, operational, and technical considerations, including threat considerations.

Inform selection and prioritization

STRATEGIC DESIGN PRINCIPLES

Inform selection and prioritization

STRUCTURAL DESIGN PRINCIPLES

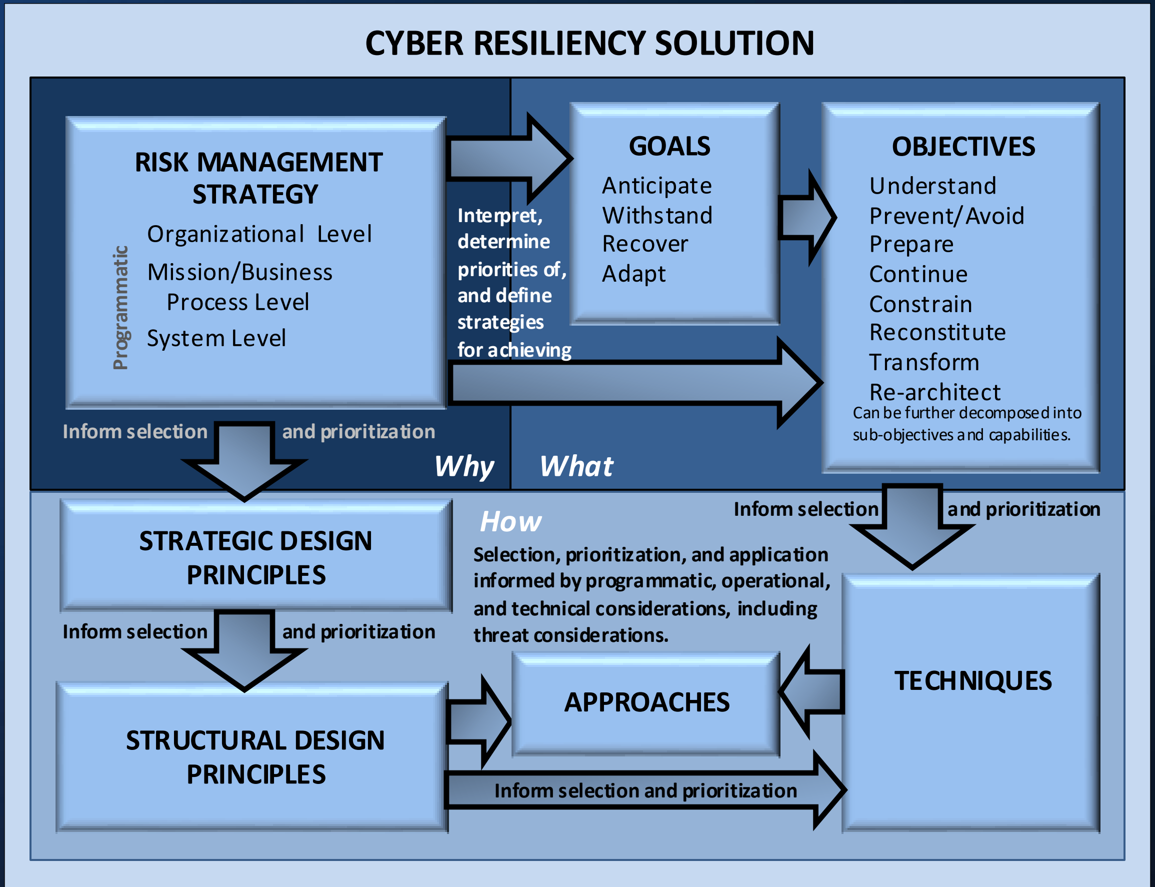
APPROACHES

TECHNIQUES

Inform selection and prioritization

Cyber Resiliency Techniques

- Adaptive Response
- Analytic Monitoring
- Contextual Awareness
- Coordinated Protection
- Deception
- Diversity
- Dynamic Positioning
- Non-Persistence
- Privilege Restriction
- Realignment
- Segmentation
- Substantiated Integrity
- Unpredictability



CYBER RESILIENCY SOLUTION

RISK MANAGEMENT STRATEGY

Organizational Level

Mission/Business Process Level

System Level

Programmatic

Interpret, determine priorities of, and define strategies for achieving

GOALS

Anticipate
Withstand
Recover
Adapt

OBJECTIVES

Understand
Prevent/Avoid
Prepare
Continue
Constrain
Reconstitute
Transform
Re-architect

Can be further decomposed into sub-objectives and capabilities.

Inform selection and prioritization

Why

What

How

Selection, prioritization, and application informed by programmatic, operational, and technical considerations, including threat considerations.

Inform selection and prioritization

STRATEGIC DESIGN PRINCIPLES

Inform selection and prioritization

STRUCTURAL DESIGN PRINCIPLES

APPROACHES

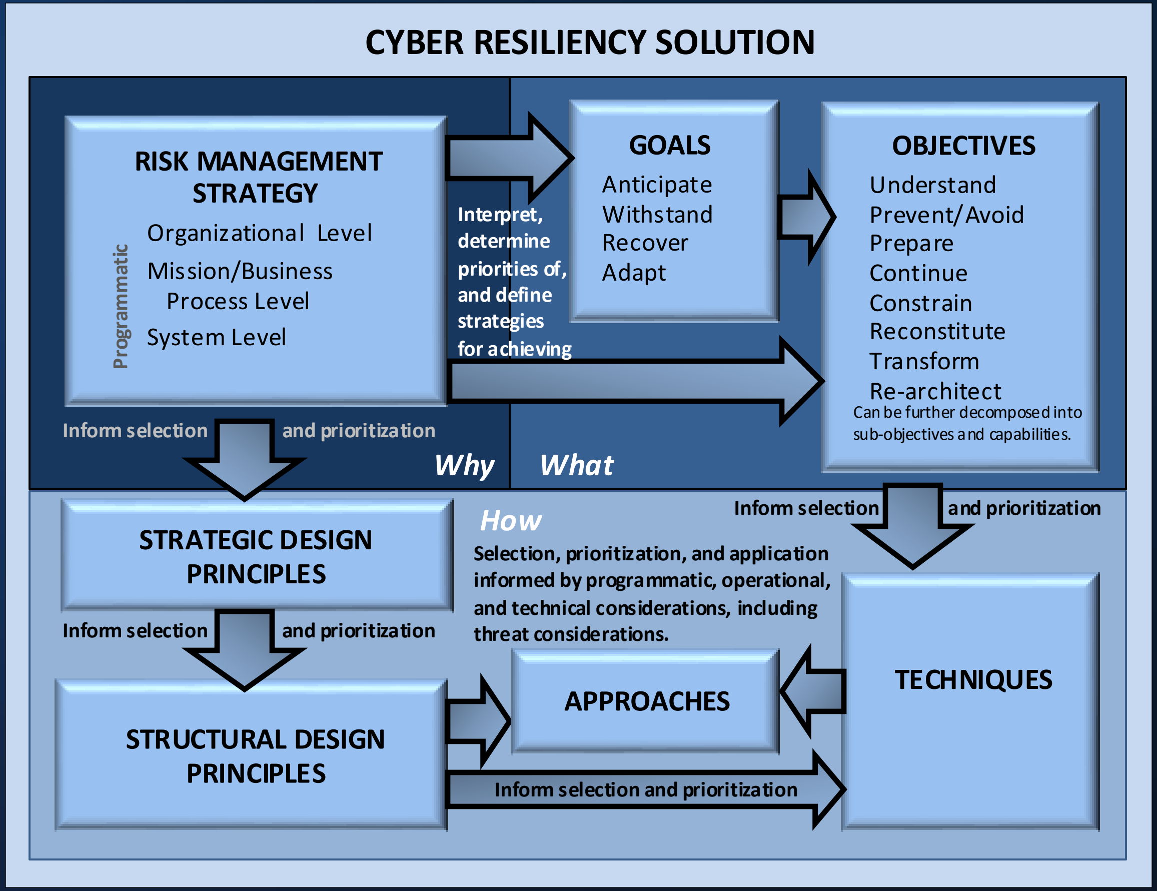
TECHNIQUES

Inform selection and prioritization

Cyber Resiliency Implementation Approaches

- Adaptive Response
- Analytic Monitoring
- Contextual Awareness
- Coordinated Protection
- Deception
- Diversity
- Dynamic Positioning
- **Non-Persistence**
- Privilege Restriction
- Realignment
- Segmentation
- Substantiated Integrity
- Unpredictability

- **Non-Persistent Information**
- **Non-Persistent Services**
- **Non-Persistence Connectivity**



CYBER RESILIENCY SOLUTION

RISK MANAGEMENT STRATEGY

Programmatic

Organizational Level

Mission/Business Process Level

System Level

Interpret, determine priorities of, and define strategies for achieving

GOALS

Anticipate

Withstand

Recover

Adapt

OBJECTIVES

Understand

Prevent/Avoid

Prepare

Continue

Constrain

Reconstitute

Transform

Re-architect

Can be further decomposed into sub-objectives and capabilities.

Inform selection and prioritization

Why

What

How

Selection, prioritization, and application informed by programmatic, operational, and technical considerations, including threat considerations.

STRATEGIC DESIGN PRINCIPLES

Inform selection and prioritization

STRUCTURAL DESIGN PRINCIPLES

Inform selection and prioritization

APPROACHES

TECHNIQUES

Inform selection and prioritization

Security Design Principle Traceability

- **Anomaly Detection (Security Design Principle)**
  NIST SP 800-160, Volume 1

↓

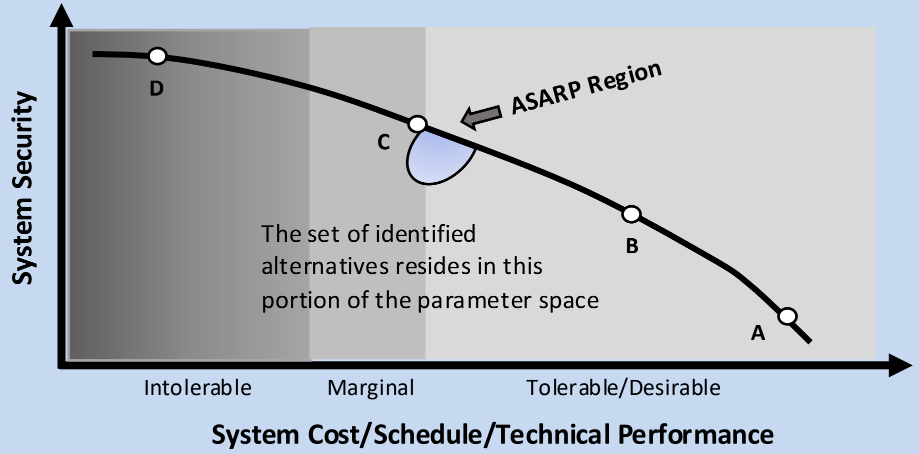
- **Analytic Monitoring (Resiliency Technique)**
  NIST SP 800-160, Volume 2

↓

- **Monitoring and Damage Assessment (Resiliency Approach)**
  NIST SP 800-160, Volume 2

Adequate Security

Means as secure as reasonably practicable…



The set of identified alternatives resides in this portion of the parameter space

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.

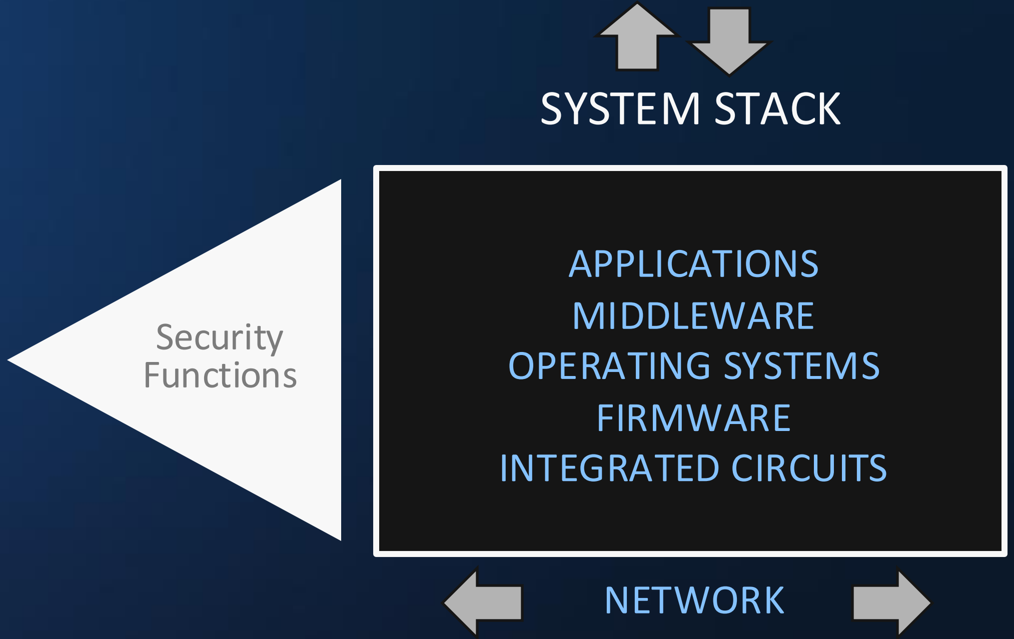
D: Limit of achievable security has been met. Increased security cannot be "bought" at any cost.

Adapted from NASA.

Evidence-Based Assurance

Essential for the development of trustworthy secure systems…

Transparency
Traceability
Visibility



SYSTEM STACK

Security Functions

APPLICATIONS
MIDDLEWARE
OPERATING SYSTEMS
FIRMWARE
INTEGRATED CIRCUITS

NETWORK

Produced routinely during the systems engineering verification, validation, and system analyses processes…

SSE and Cyber Resiliency Resources

NIST SP 800-160, Volume 1
https://doi.org/10.6028/NIST.SP.800-160v1r1

NIST SP 800-160, Volume 2
https://doi.org/10.6028/NIST.SP.800-160v2r1

CREF Navigator (Automated Cyber Resiliency Tool)
https://crefnavigator.mitre.org/navigator

NIST System Security Engineering Project
https://csrc.nist.gov/projects/systems-security-engineering-project

NASA-NIST SSE SunRISE Satellite Pilot Project
https://csrc.nist.gov/csrc/media/Presentations/2024/protecting-cyber-physical-space-systems/SunRISE-v1.0-Updated9.25.24.pdf

Ron Ross

National Institute of Standards and Technology

Email: **ron.ross@nist.gov**

Mobile: **301.651.5083**

Protection. Damage Limitation. System Resilience.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE