NIST CYBER

Draft NIST Special Publication (SP) 800-160, Volume 2

Developing Cyber Resilient Systems: A Systems Security Engineering Approach

Victoria Yan Pillitteri
victoria.yan@nist.gov

October 16, 2019

Overview of Draft NIST SP 800-160, Volume 2

Developing Cyber Resilient Systems: A Systems Security Engineering Approach

- **Background**
- Cyber Resiliency **Fundamentals**
- Cyber Resiliency **in Practice**
- **Use Cases** and Real World Example
- Next Steps
- **Update** on NIST publications
- **Contact** Information and **Questions**

Current landscape

Today's systems are **very brittle**, rely on a **one-dimensional protection** strategy of penetration resistance, and are **highly susceptible** to devastating **cyber-attacks**.

The adversaries are **relentless**.

The need for a new paradigm

multi-dimensional protection strategy that includes developing **damage limiting system architectures** and **cyber resilient systems**.

Objective of SP 800-160, Volume 2

Supplement NIST SP 800-160, Vol 1 & NIST SP 800-37

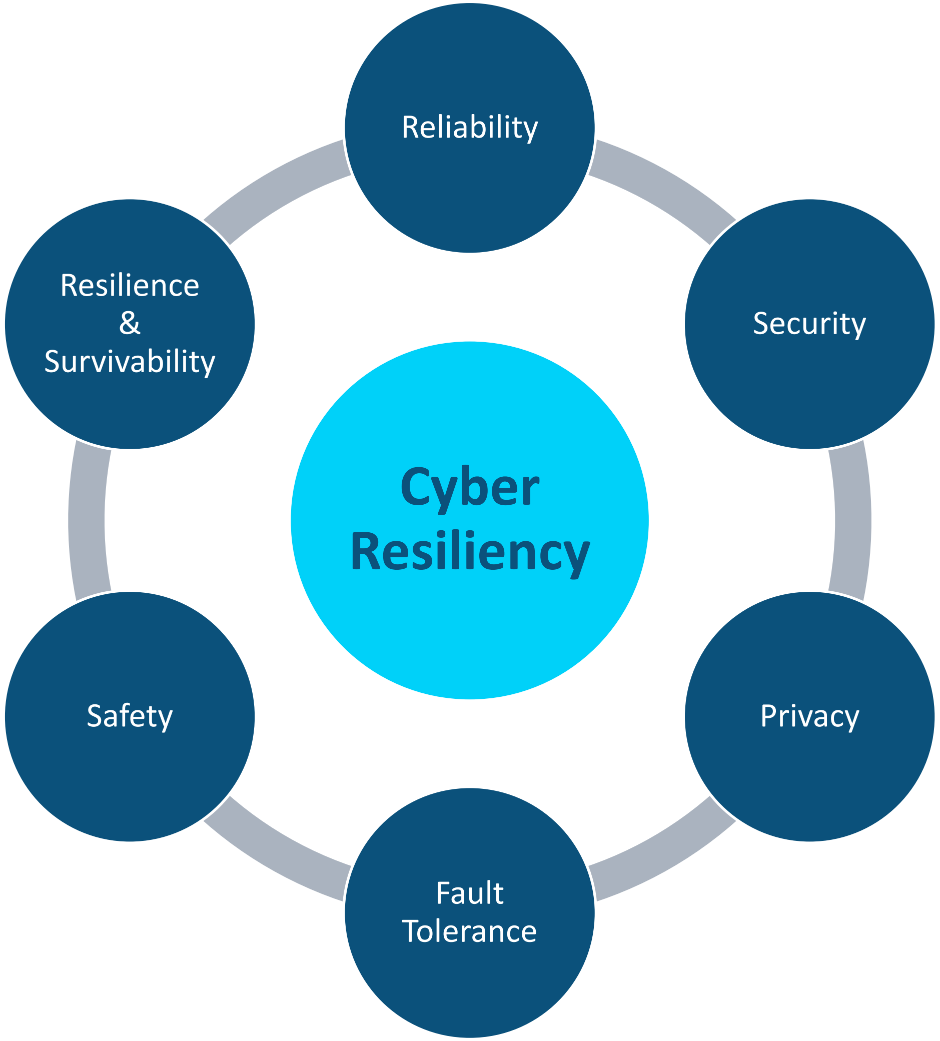
with guidance on how to apply cyber resiliency as part of systems security engineering and risk management for information systems and organizations.

Identify cyber resiliency considerations

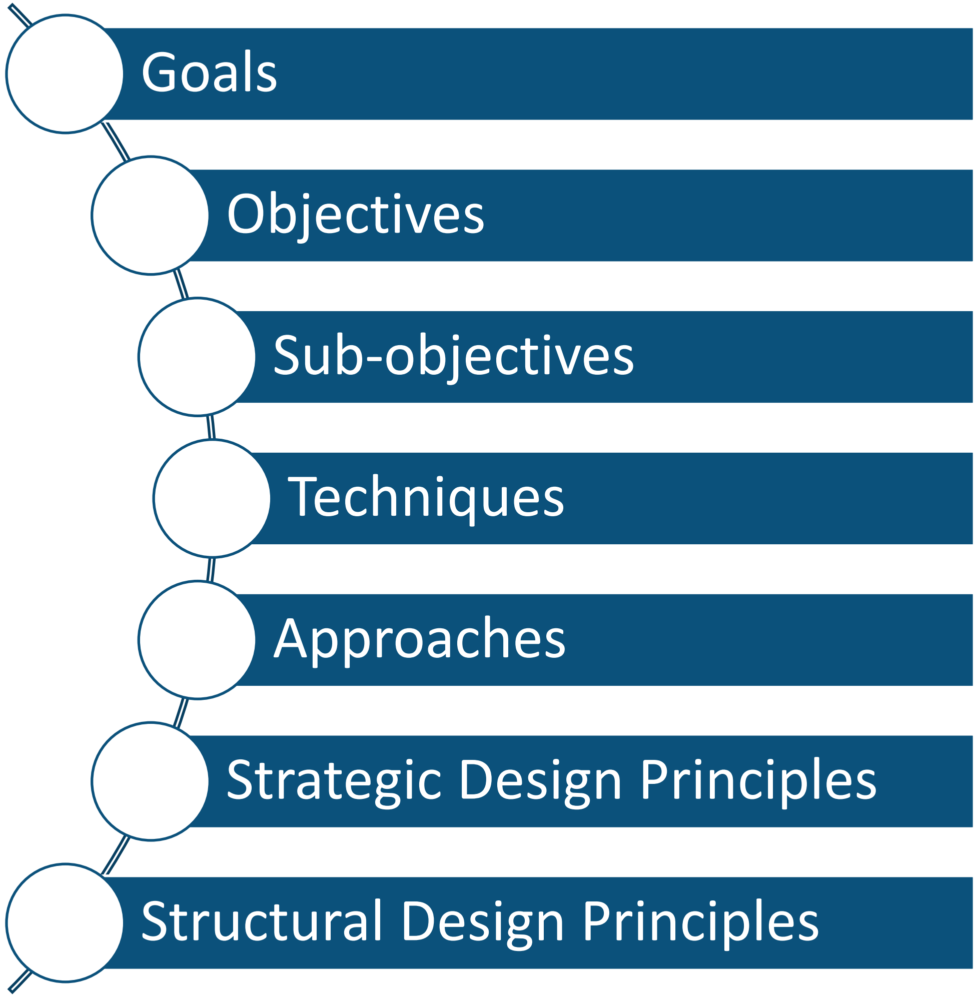
to support the engineering of trustworthy systems
that depend on cyber resources

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**.



Cyber resiliency conceptual framework



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

Section 2 describes the framework constructs, and includes the definition, purpose, application, and provides a higher-level description of the constructs

Appendix E provides details on the constructs and relationships

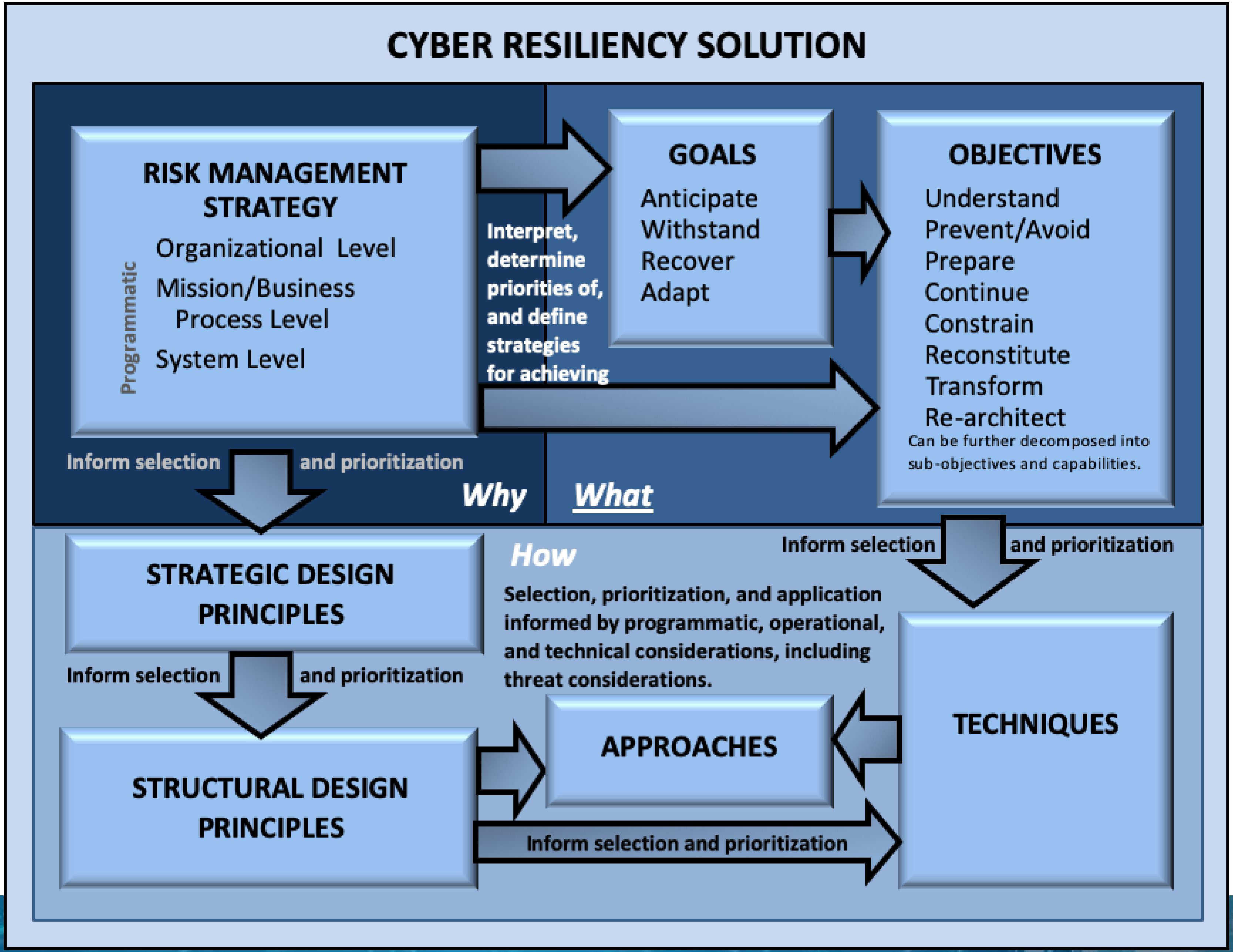
Bridging the

Risk Management Framework

and

System Security Engineering

communities



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

Inform selection and prioritization

STRATEGIC DESIGN PRINCIPLES

Inform selection and prioritization

STRUCTURAL DESIGN PRINCIPLES

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

APPROACHES

TECHNIQUES

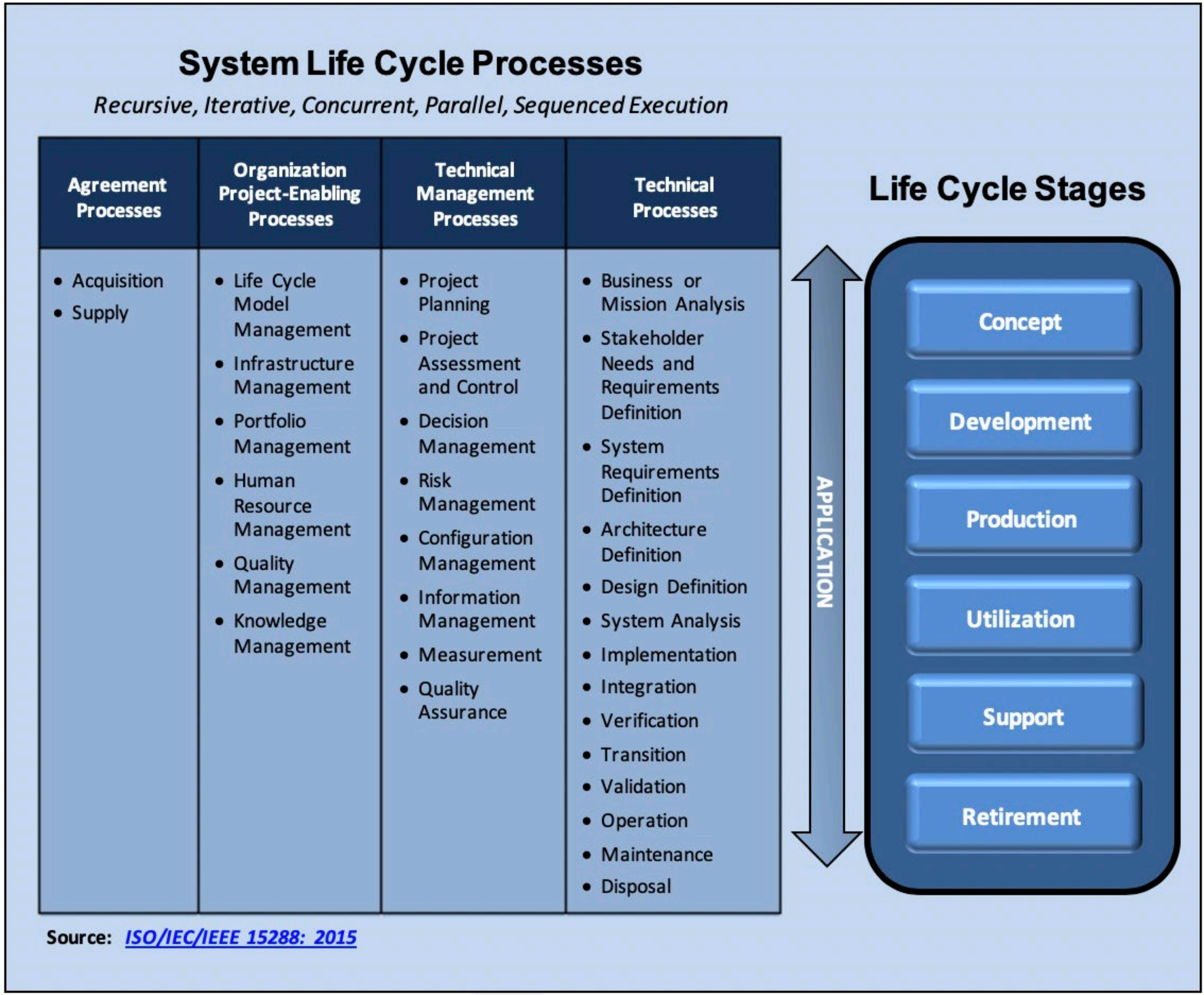
Inform selection and prioritization

FUNDAMENTALS

Cyber resiliency & security in the system life cycle

Section 2 discusses applying cyber resiliency concepts to the life cycle stages

Appendix F provides examples of cyber resiliency considerations for system life cycle processes (SP 800-160 vol 1)



System Life Cycle Processes

Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organization 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

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

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

Considerations for the system life cycle processes in NIST SP 800-160, Volume 1

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

IN PRACTICE

Considerations for the system life cycle processes in NIST SP 800-160, Volume 2

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

Considerations for the system life cycle processes in NIST SP 800-160

EXAMPLE

NIST SP 800-160, Vol 1

SR-2.2: Define system security requirements, security constraints on system requirements, and rationale.

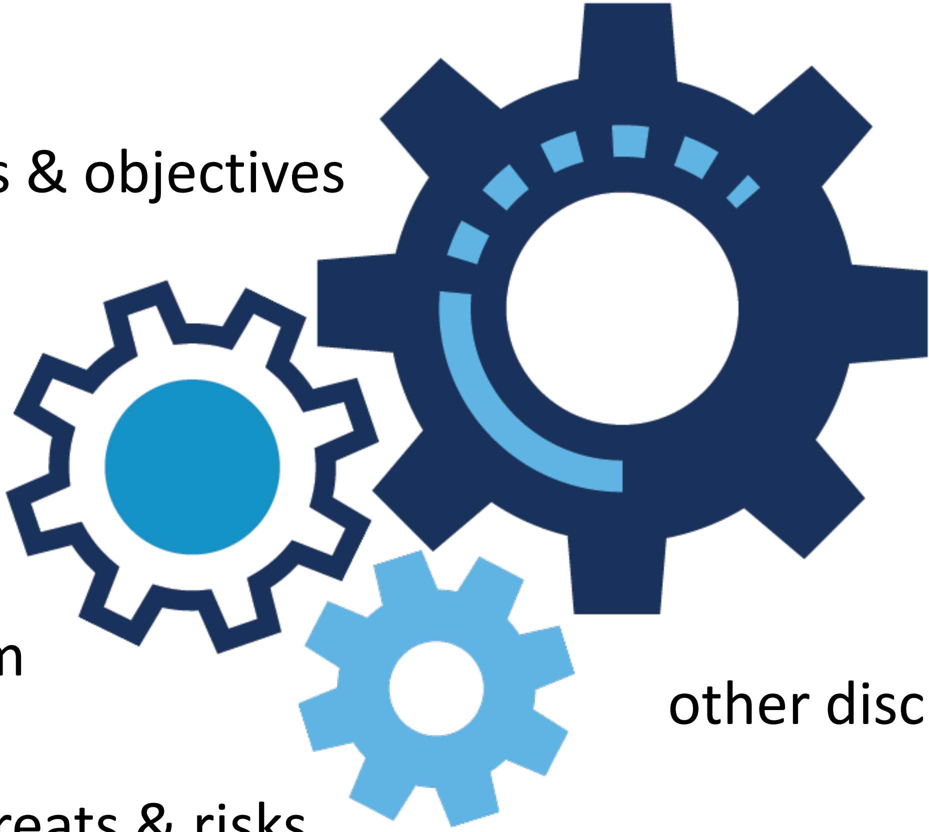
Discussion: The system security requirements express security functions provided by the system and security-driven constraints levied on the entire system. System security applies to the entire system (to include the security functions) in terms of susceptibility to disruption, hazard, and threat resulting in adverse consequences.…

NIST SP 800-160, Vol 2

SR-2.2: Define system security **and cyber resiliency** requirements, security **and cyber resiliency** constraints on system requirements, and rationale.

Discussion: From a cyber resiliency perspective, susceptibility to disruption, hazard, and threat should be considered not only with respect to direct consequences, but also to deferred and indirect consequences. Direct consequences disrupt, destroy, disable, or otherwise impact the ability of the system to support the mission or business functions.…

Considerations for selecting & prioritizing cyber resiliency constructs



achievement of goals & objectives

architectural locations

type of system

effects on adversaries, threats & risks

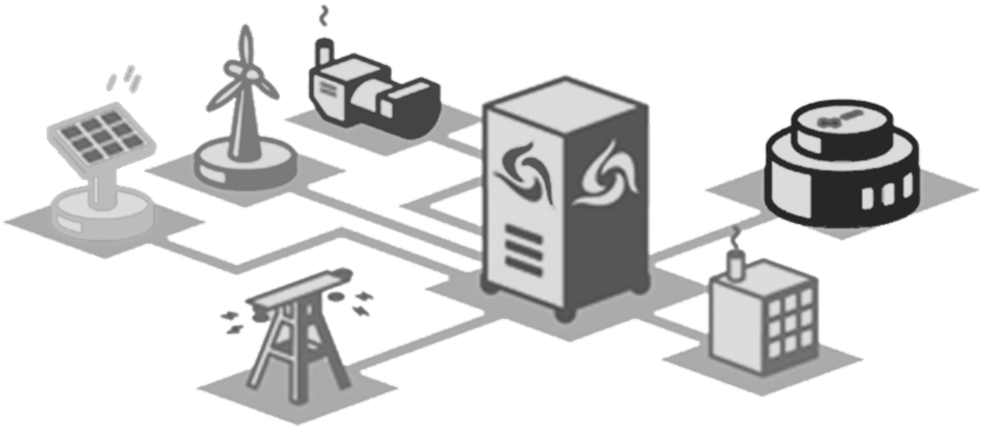
cyber resiliency conflicts & synergies

maturity & potential adoption

cyber risk management strategy

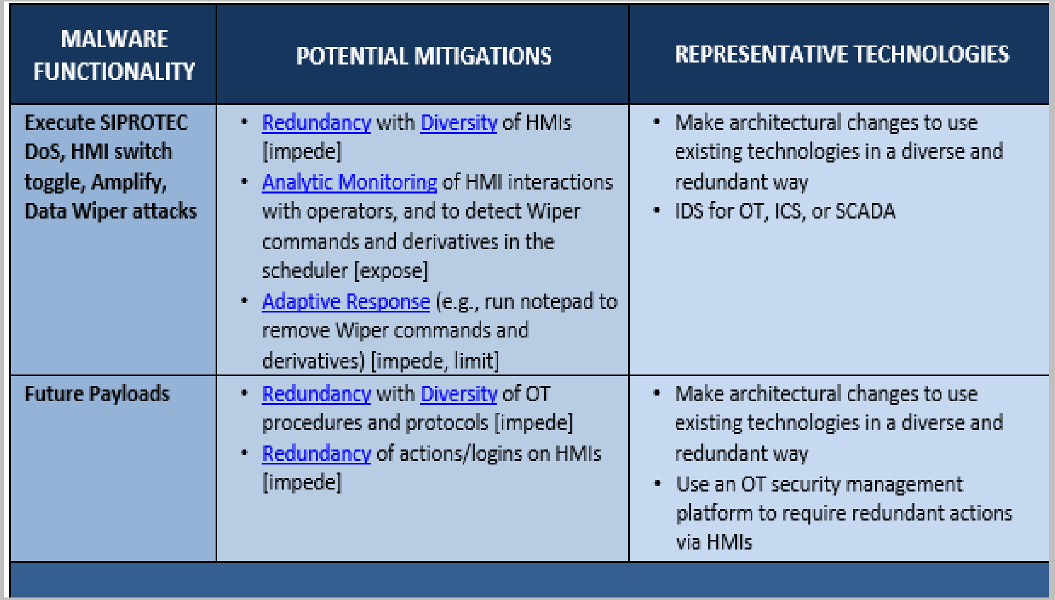
other disciplines & existing investments

3 use cases



Real-world example: Ukrainian power grid attack

For each step of the attack, identifies potential cyber resiliency mitigations and representative technologies.



MALWARE FUNCTIONALITY	POTENTIAL MITIGATIONS	REPRESENTATIVE TECHNOLOGIES
Execute SIPROTEC DoS, HMI switch toggle, Amplify, Data Wiper attacks	- Redundancy with Diversity of HMIs [impede] - Analytic Monitoring of HMI interactions with operators, and to detect Wiper commands and derivatives in the scheduler [expose] - Adaptive Response (e.g., run notepad to remove Wiper commands and derivatives) [impede, limit]	- Make architectural changes to use existing technologies in a diverse and redundant way - IDS for OT, ICS, or SCADA
Future Payloads	- Redundancy with Diversity of OT procedures and protocols [impede] - Redundancy of actions/logins on HMIs [impede]	- Make architectural changes to use existing technologies in a diverse and redundant way - Use an OT security management platform to require redundant actions via HMIs

Next steps: submit comments on Draft SP 800-160 Vol. 2

September 4 - **November 1, 2019**

https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft

sec-cert@nist.gov

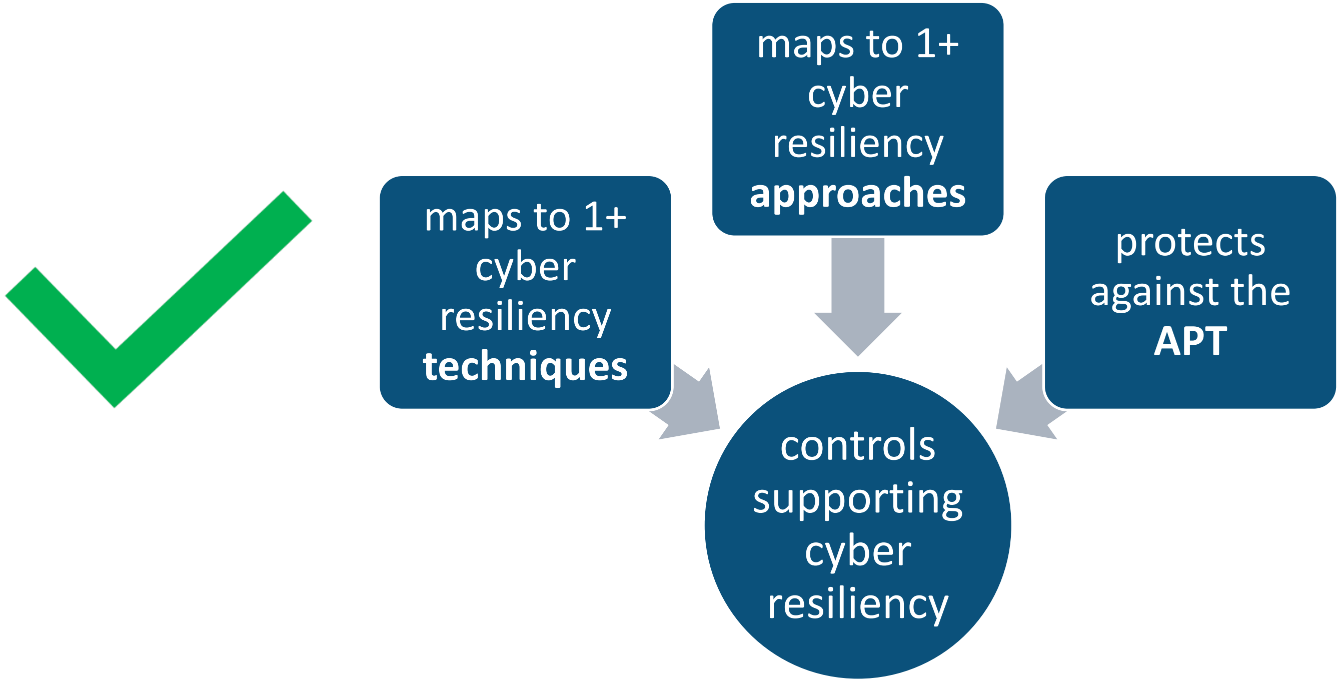
STAY IN TOUCH

CONTACT US

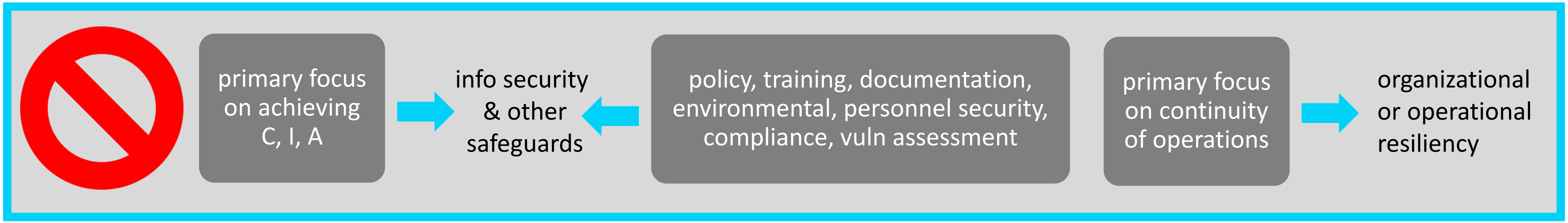
✉ sec-cert@nist.gov

@NISTcyber

NIST SP 800-53 controls supporting cyber resiliency


maps to 1+ cyber resiliency **techniques**
maps to 1+ cyber resiliency **approaches**
protects against the **APT**
controls supporting cyber resiliency

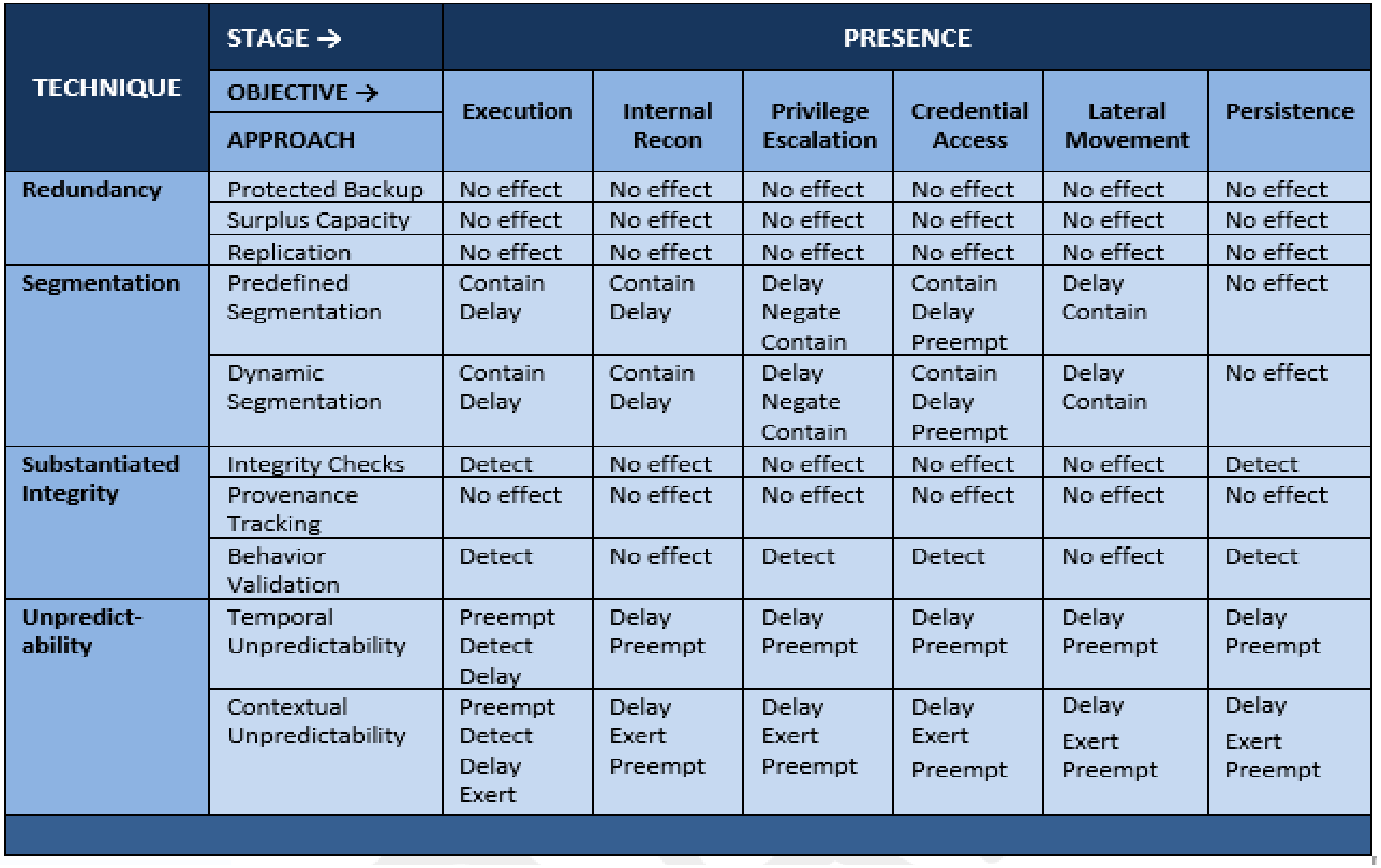
Control Name	Resiliency Technique [Approaches]
AC-6: Least Privilege	Privilege Restriction [Attribute-Based Usage Restriction]
CP-12: Safe Mode	Adaptive Response [Adaptive Management]
RA-9: Criticality Analysis	Contextual Awareness [Mission Dependency and Status Visualization] Realignment [Offloading]


primary focus on achieving C, I, A
info security & other safeguards
policy, training, documentation, environmental, personnel security, compliance, vuln assessment
primary focus on continuity of operations
organizational or operational resiliency

IN PRACTICE

Adversary-oriented analysis

Appendix H provides a mapping of the NSA/CSS Technical Cyber Threat Framework (NTCTF) against the cyber resiliency techniques and approaches.



TECHNIQUE	STAGE →	PRESENCE					
	OBJECTIVE →	Execution	Internal Recon	Privilege Escalation	Credential Access	Lateral Movement	Persistence
	APPROACH						
Redundancy	Protected Backup	No effect	No effect	No effect	No effect	No effect	No effect
	Surplus Capacity	No effect	No effect	No effect	No effect	No effect	No effect
	Replication	No effect	No effect	No effect	No effect	No effect	No effect
Segmentation	Predefined Segmentation	Contain Delay	Contain Delay	Delay Negate Contain	Contain Delay Preempt	Delay Contain	No effect
	Dynamic Segmentation	Contain Delay	Contain Delay	Delay Negate Contain	Contain Delay Preempt	Delay Contain	No effect
Substantiated Integrity	Integrity Checks	Detect	No effect	No effect	No effect	No effect	Detect
	Provenance Tracking	No effect	No effect	No effect	No effect	No effect	No effect
	Behavior Validation	Detect	No effect	Detect	Detect	No effect	Detect
Unpredict-ability	Temporal Unpredictability	Preempt Detect Delay	Delay Preempt	Delay Preempt	Delay Preempt	Delay Preempt	Delay Preempt
	Contextual Unpredictability	Preempt Detect Delay Exert	Delay Exert Preempt	Delay Exert Preempt	Delay Exert Preempt	Delay Exert Preempt	Delay Exert Preempt