MP190668

MITRE PRODUCT

Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes

Enabling Controls, Requirements, Solutions, and Metrics to Be Identified

Deborah Bodeau
Richard Graubart
Ellen Laderman

September 2019

Dept. No.: T8A2
Project No.: 01ADAUAL-CR

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Bedford, MA

Abstract

Cyber resiliency and cyber survivability are closely related concepts, sharing similar technologies and practices. For historical reasons, these concepts have been built out into different frameworks, which define different constructs for describing the problem and solution domains. Cyber resiliency constructs enable system requirements to be defined, metrics and security controls to be identified, and solutions to be identified and analyzed. The identification of relationships between cyber resiliency constructs and cyber survivability attributes (CSAs) in this paper is intended to help systems engineers understand how to use cyber resiliency to improve cyber survivability, and vice versa.

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

1 Introduction

Cyber resiliency and cyber survivability are closely related concepts, sharing similar technologies and practices. For historical reasons, these concepts have been built out into different frameworks, which define different constructs for describing the problem and solution domains. Cyber resiliency constructs enable system requirements to be defined, metrics and security controls to be identified, and solutions to be identified and analyzed. Similarly, cyber survivability attributes (CSAs) enable system requirements to be defined, and metrics and security controls to be identified. This report provides an initial identification relationships between cyber resiliency constructs (e.g., design principles, techniques) and CSAs, based on publicly available sources. This identification is intended to help systems engineers understand how to use cyber resiliency to improve cyber survivability, and vice versa.

This section provides an overview of this report, and describes the limitations of this analysis.

1.1 Overview

Section 2 presents background on cyber survivability, cyber resiliency, and their relationships to controls, requirements, and metrics. Section 3 provides a descriptive mapping between the CSAs and high-level cyber resiliency constructs. Section 4 provides a more detailed mapping, in table form, to support systems engineering analysis. Section 5 identifies possible future directions. Appendix A provides additional detail on cyber resiliency constructs.

1.2 Intent and Limitations of This Report

This report identifies relationships between high-level cyber resiliency constructs and the CSAs. It also maps the cyber resiliency constructs to the System Survivability Key Performance Parameter (SS KPP) pillars, given that the CSAs are necessary for but may not be sufficient for the pillars. Cyber resiliency constructs include objectives, design principles, techniques, and implementation approaches as defined in [1] [2].

The analysis in this paper is intentionally preliminary and incomplete. First, the analysis is based solely on publicly-available material on cyber survivability and the CSAs [3] [4] [5]. A more detailed analysis could consider how the exemplar language varies, depending on a system's Cyber Survivability Risk Category (CSRC). It could also include a mapping between cyber resiliency constructs and systems security engineering (SSE) sub-elements. Second, the analysis does not include representative cyber resiliency sub-objectives and capabilities, as defined in [6]. The representative capabilities are closer to functional requirements – and thus to exemplar language including threshold and objective statements – than other cyber resiliency constructs. However, the representative sets of cyber resiliency sub-objectives and capabilities defined in [6] are oriented toward an enterprise information technology (EIT) or command, control, and communications (C3) system rather than toward weapon systems. Thus, examples of tailoring for a specific type of system or platform (e.g., a vehicle, as in [7]) may be more useful in defining requirements for CSAs or for weapon system cyber resiliency than the EIT-oriented statements in [6].

2 Background

Cyber resiliency and cyber survivability are closely related concepts, sharing similar technologies and practices. This section provides background on the concepts, their conceptual relationship, and how controls, requirements, and metrics are identified. Metrics are central to making requirements measurable and testable.

2.1 Cyber Survivability

Cyber survivability is a property – *the system's ability to prevent, mitigate, and recover from cyber events* [3] – defined for weapon systems and the critical infrastructures on which those systems depend. CSAs are system capabilities which are support, and serve as indicators of, cyber survivability. CSAs support the three mandatory pillars of the System Survivability Key Performance Parameter (SS KPP) [4]:

- "Prevent: The ability to protect critical mission functions from cyber threats.
- "Mitigate: The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.
- "Recover: The resilience to recover from cyber-attacks and prepare mission systems for the next fight."

CSAs are selected for a system based on its Cyber Survivability Risk Category (CSRC), which captures key aspects of the survivability problem domain. A CSA is implemented for a system by incorporating CSA-based language in the Initial Capabilities Document (ICD); incorporating, updating, and elaborating CSA-driven functional requirements in the Capability Development Document (CDD) as it evolves; building the required functionality into the system. The strength of the CSA implementation is determined by measuring and testing the required functionality in the as-built system.

Exemplar language for each CSA provides a starting point for defining system requirements for CSAs. When system-specific requirements establish threshold and/or objective values for performance or behavior in the context of the system's concept of operations, those values – which may be captured in tailorings of the exemplar language for the CSAs – articulate measurable and testable cyber survivability requirements and are supported by controls in NIST SP 800-53. For ease of exposition and implementation, ten CSAs have been defined. Implementation of the CSAs (i.e., the cyber survivability solution domain) entails the application of a variety of controls, technologies, practices, design principles, and procedures. These are drawn primarily from conventional cybersecurity[1] but include some solutions that fall in the domain of cyber resiliency.

[1] Conventional cybersecurity can be identified with the baselines in NIST SP 800-53 [11] or with the Framework Core of the Framework for Improving Critical Infrastructure Security (often referred to as the NIST Cybersecurity Framework or NCF [13]). Some of the functionality identified in the exemplar language for the CSAs goes beyond the baselines, e.g., anti-tamper measures identified for CSA 01.

2.1.1 Resilience and Cyber Survivability

The definitions of the Mitigate and Recover pillars, as well as exemplar language for CSA 08, use the terms "resilience" or "resilient." This use refers to the definitions in the 2015 JCIDS Manual [5]:[2]

> "(a) Resilience is the ability of the collection of systems to support the functions necessary for mission success in spite of hostile action or under adverse conditions.
>
> (b) An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities."

SS KPP attributes

> "(d) Include whether or not the system must be able to survive and operate in a cyber-contested environment or after exposure to cyber threats which prevent the completion of critical operational missions by destruction, corruption, denial, or exposure of information transmitted, processed, or stored."

Cyber survivability is shown [3] as overlapping with operational resilience, which relies on trustworthy information resources and ensures readiness for degradation or loss, so that operations have the means to prevail. Operational resilience is mission focused, rather than system focused.

2.2 Cyber Resiliency

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" [1] [2] – is a property of a system, mission or business function, organization, critical infrastructure sector or sub-sector, or region.[3] When *system* cyber resiliency is considered, the system-of-interest (i.e., the focus of analysis or other systems engineering efforts, such as those described in [8]) can range from an embedded system in a weapon system platform to a large-scale acknowledged system-of-systems that supports a mission in a critical infrastructure sector (e.g., electrical power distribution). The system-of-interest typically includes not only the technical system, but also the people, processes, procedures, and protections that are part of the technical system's operational environment.

The assumption that advanced adversaries can establish and maintain an undetected presence in a system is fundamental to the analysis of cyber resiliency and the development of cyber resiliency solutions. This assumption acknowledges the existence of undiscovered vulnerabilities in commercial off-the-shelf (COTS) technologies incorporated into systems, as well as in the COTS and free and open source software (FOSS) used in development and maintenance environments. An additional assumption underlying cyber resiliency analysis is that adversaries both exploit

[2] Appendix C to Enclosure D of the 2015 JCIDS Manual [5] provides a content guide for the System Survivability KPP, which includes discussion of resilience. This material is not present in the 2018 JCIDS Manual [17].

[3] Note that the definitions in the 2015 JCIDS Manual quoted above focus on "withstand," and that SS KPP attributes focus on "withstand" and "recover."

and emulate faults, failures, and errors; the system must be able to achieve the cyber resiliency goals independent of the source of adversity.

To capture the wide variety of concerns, technologies, and practices related to cyber resiliency, a number of cyber resiliency constructs have been defined.[4] These are characterized in Table 1, and presented in more detail in Appendix A. Each construct has a purpose, and can be applied to a system via requirements or engineering activities. Constructs related to the problem domain (the "what" of cyber resiliency) include goals, objectives, sub-objectives, and capabilities / activities. Constructs related to the solution domain (the "how" of cyber resiliency) include design principles, techniques, implementation approaches, and foundational principles for weapon systems. With the exception of the foundational principles for weapon systems, these constructs are intended to apply to any type of system that includes cyber resources. Furthermore, with the exception of the implementation approaches and the foundational principles at the technical level, the cyber resiliency constructs are technology-neutral, and can be applied to systems that do not include cyber resources – that is, the cyber resiliency constructs can be applied to a system consisting of people, processes, and physical objects (e.g., paper), as long as that system depends on, uses, or is enabled by cyber resources.

Table 1. Cyber Resiliency Constructs

Construct	Definition, Purpose, and Application at the System Level
Goal [1]	**Definition**: A high-level statement unpacking the definition of cyber resiliency. **Purpose**: Align the definition of cyber resiliency with definitions of other types of resilience. **Application**: Can be used to express high-level stakeholder concerns, goals, or priorities.
Objective [1]	**Definition**: A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its lifecycle to meet stakeholder needs for mission assurance and resilient security; more specific than goals; more relatable to threats. **Purpose**: Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate definition of metrics or measures of effectiveness (MOEs). **Application**: Used in scoring methods or summaries of analyses (e.g., cyber resiliency posture assessments).
Sub-Objective [1]	**Definition**: A statement, subsidiary to a cyber resiliency objective, which emphasizes different aspects of that objective or identifies methods to achieve that objective. **Purpose**: Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. While a representative set of sub-objectives have been identified [1] [6], these are intended solely as a starting point for selection, tailoring, and prioritization. **Application**: Used in scoring methods or analyses; may be reflected in system functional requirements.

[4] Most of the constructs are part of the cyber resiliency framework in the draft NIST SP 800-160 Vol. 2; however, other documents [6] [12] define related constructs and representative metrics.

Construct	Definition, Purpose, and Application at the System Level
Activity / Capability [6]	**Definition**: A statement of a capability or action which supports the achievement of a sub-objective and hence of an objective. **Purpose**: Facilitate the definition of metrics or MOEs. While a representative set of activities or capabilities have been identified [6], these are intended solely as a starting point for selection, tailoring, and prioritization. The set in [6] is oriented toward enterprise information technology, but has been tailored to a vehicle use case in [7]. **Application**: Used in scoring methods or analyses; reflected in system functional requirements.
Strategic Design Principle [1]	**Definition**: A high-level statement which reflects an aspect of the risk management strategy that informs systems security engineering practices for an organization, mission, or system. **Purpose**: Guide and inform engineering analyses and risk analyses throughout the system life cycle. Highlight different structural design principles, cyber resiliency techniques and implementation approaches. **Application**: Included, cited, or restated in system non-functional requirements (e.g., requirements in a Statement of Work or SOW for analyses or documentation).
Structural Design Principle [1]	**Definition**: A statement which captures experience in defining system architectures and designs. **Purpose**: Guide and inform design and implementation decisions throughout the system life cycle. Highlight different cyber resiliency techniques and implementation approaches. **Application**: Included, cited, or restated in system non-functional requirements (e.g., SOW requirements for analyses or documentation); used in systems engineering to guide the use of techniques, implementation approaches, technologies, and practices.
Technique [1]	**Definition**: A set or class of technologies, processes, or practices providing capabilities to achieve one or more cyber resiliency objectives. **Purpose**: Characterize technologies, practices, products, controls, or requirements, so that their contribution to cyber resiliency can be understood. **Application**: Used in engineering analysis to screen technologies, practices, products, controls, solutions, or requirements; used in system by implementing or integrating technologies, practices, products, or solutions.
Implementation Approach [1]	**Definition**: A subset of the technologies and processes of a cyber resiliency technique, defined by how the capabilities are implemented. **Purpose**: Characterize technologies, practices, products, controls, or requirements, so that their contribution to cyber resiliency and their potential effects on threat events can be understood. **Application**: Used in engineering analysis to screen technologies, practices, products, controls, solutions, or requirements; used in system by implementing or integrating technologies, practices, products, or solutions.
Solution [1]	**Definition**: A combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices which solves a problem in the cyber resiliency domain. **Purpose**: Provide enough cyber resiliency to meet stakeholder needs and to reduce risks to mission or business capabilities in the presence of advanced persistent threats. **Application**: Integrated into the system or its operational environment.

Because the cyber resiliency problem space and solution domain are large and complex, it is unrealistic to expect that all cyber resiliency approaches, techniques, or design principles will be applicable to a given system. Factors considered in the selection of cyber resiliency constructs for a system include the cyber risk management strategy as it applies to the system, the type of system, costs and availability of technologies, and the threats to which the system is subject. In addition, as discussed in [1], synergies and frictions among cyber resiliency constructs exist; for example, the Dynamic Positioning or Deception techniques can make implementation of the Analytic Monitoring and Contextual Awareness techniques more difficult.

As illustrated in Figure 1[5], the interpretation, prioritization, and tailored application of cyber resiliency constructs are driven by cyber risk management strategies at the organizational, mission, operational, programmatic, and system levels.

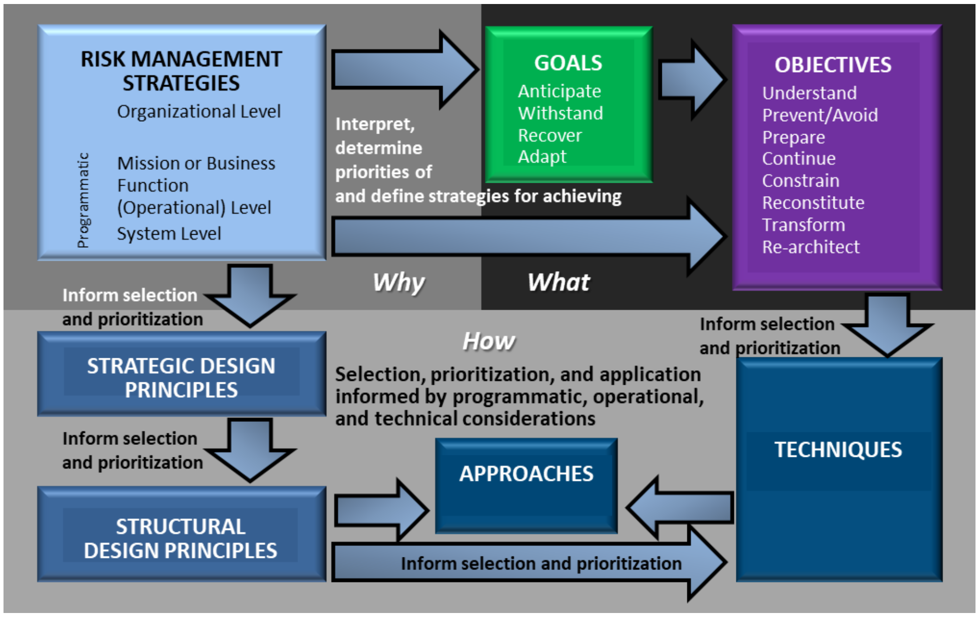

RISK MANAGEMENT STRATEGIES
Organizational Level
Mission or Business Function (Operational) Level
System Level
Programmatic
Interpret, determine priorities of and define strategies for achieving
GOALS
Anticipate
Withstand
Recover
Adapt
OBJECTIVES
Understand
Prevent/Avoid
Prepare
Continue
Constrain
Reconstitute
Transform
Re-architect
Why
What
Inform selection and prioritization
How
Selection, prioritization, and application informed by programmatic, operational, and technical considerations
Inform selection and prioritization
STRATEGIC DESIGN PRINCIPLES
Inform selection and prioritization
TECHNIQUES
APPROACHES
STRUCTURAL DESIGN PRINCIPLES
Inform selection and prioritization

Figure 1. Cyber Resiliency Constructs Are Driven by Risk Management Strategies

2.3 Conceptual Relationships and Paths to Controls, Requirements, and Metrics

Cyber survivability and cyber resiliency are closely related concepts, due to their shared recognition of advanced cyber threats and concern for mission accomplishment. However, they differ in scope, some threat assumptions[6], and risk management strategy. This means that the processes for identifying applicable controls, requirements, and metrics follow different paths.

The definition of cyber resiliency deliberately does not specify *what* can be cyber resilient. Therefore, as illustrated in Figure 2, the scope of the cyber resiliency problem domain is larger than that of cyber survivability.

[5] This figure is taken from [2], with coloring added.

[6] For both cyber resiliency and cyber survivability, analysis focuses on advanced cyber threats, but acknowledges other threat sources or types of adverse conditions. For cyber survivability, this acknowledgement is by reference to resilience, as discussed in Section 2.1.1.

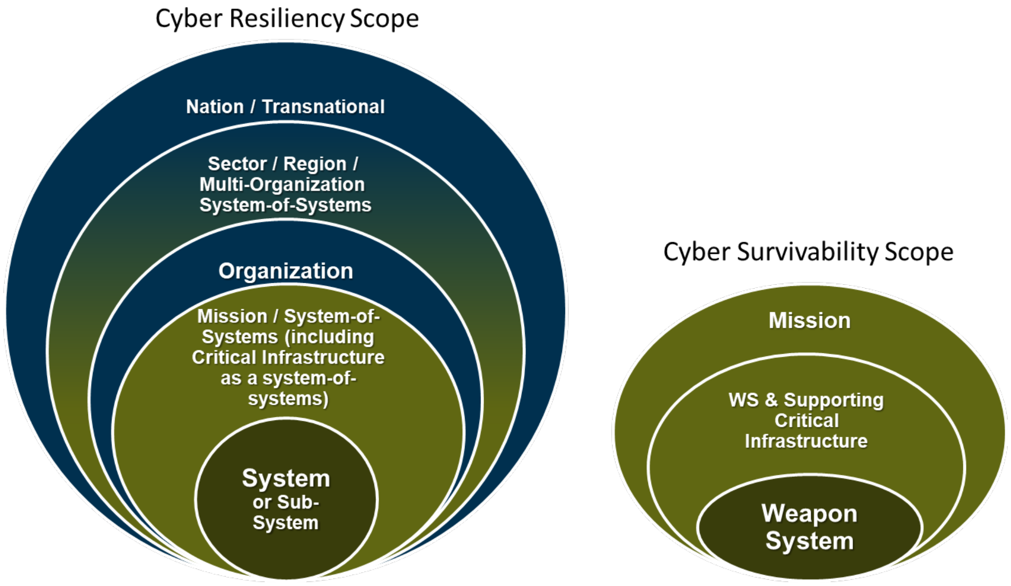

Cyber Resiliency Scope
Nation / Transnational
Sector / Region / Multi-Organization System-of-Systems
Organization
Mission / System-of-Systems (including Critical Infrastructure as a system-of-systems)
System or Sub-System
Cyber Survivability Scope
Mission
WS & Supporting Critical Infrastructure
Weapon System

Figure 2. Scope of Cyber Resiliency and Cyber Survivability Problem Domains

A key difference in threat assumptions relates to detectability. However, cyber survivability (e.g., via CSA-08, supporting the Mitigate SS KPP Pillar) assumes that anomalies or degradation can be detected. For cyber resiliency at the system level, the ability to withstand adversity does not depend on its detection or on the attribution of detected adverse events or conditions to a cyber attacker.[7]

The risk management strategy for cyber survivability is fairly prescriptive. The application of cyber survivability involves selecting the set of CSAs, and selecting and tailoring the exemplar language, based on the CSRC of the weapon system or critical infrastructure. The subset of CSAs most critical to achieving each SS KPP Pillar are selected, but in general, for the highest CSRC, at most one CSA might not be selected. The CSAs are not prioritized. Figure 3 illustrates how controls, requirements, and metrics can be derived for cyber survivability, using the Cyber Survivability Endorsement Implementation Guide (CSEIG).

[7] Note that the expectation that detection will inform response is also a characteristic of the NIST Cybersecurity Framework (NCF) [13], which the Cyber Survivability Endorsement leverages [3].

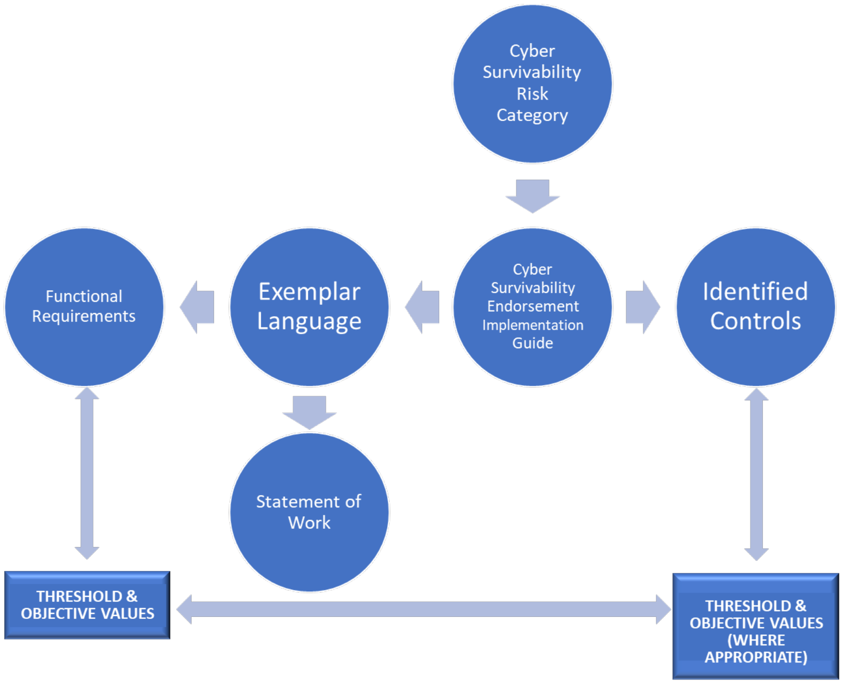

Cyber Survivability Risk Category
Functional Requirements
Exemplar Language
Cyber Survivability Endorsement Implementation Guide
Identified Controls
Statement of Work
THRESHOLD & OBJECTIVE VALUES
THRESHOLD & OBJECTIVE VALUES (WHERE APPROPRIATE)

Figure 3. Identifying Controls, Requirements, and Metrics for Cyber Survivability

In addition, the risk management strategy for cyber survivability depends strongly on conventional cybersecurity, as embodied in the control baselines for the Risk Management Framework (RMF, [9]) [10] [11].

For system cyber resiliency, no prescriptive or *a priori* risk management strategy is defined. This is intentional, to accommodate the wide variety of systems for which cyber resiliency is a desired property, as well as the wide variety of technologies, processes, and architectural decisions represented by the cyber resiliency techniques. It is assumed that one size cannot fit all, and that only a subset of the cyber resiliency techniques and design principles will be applied to a given system. Rather than assuming an *a priori* risk management strategy, systems engineers work with stakeholders, or apply stakeholder risk management strategies, to determine how the cyber resiliency constructs will be applied.[8] In particular, stakeholder risk management strategies drive the interpretation and prioritization of cyber resiliency objectives and/or design principles. Some objectives or design principles might have no priority, and hence not be selected for application to the system; however, this determination is made after these constructs have been interpreted – translated into terms meaningful to the mission, system architecture, and the operational environment – for the system. Some lower-level cyber resiliency constructs (i.e., sub-objectives, capabilities) are also interpreted and prioritized. While the more technical constructs (i.e., techniques, approaches) may be interpreted in terms of the system architecture, the more usual practice is to downselect based on the priorities established for the higher-level constructs.

[8] Stakeholders include the organizations that procure, own, operate, and/or use the system. In many cases, these are not separate organizations. Even within a single organization, these may be separate operating units, each interpreting and applying the overarching organizational risk management strategy based on their own equities and experience.

The cyber resiliency framework [1] [2] and supporting documents [12] [6] provide multiple, complementary paths for identifying cyber resiliency controls, requirements, and corresponding metrics. This enables a variety of systems engineering analysis processes to be used.

As Figure 4 illustrates, one path goes from the risk management strategy to strategic design principles to structural design principles to techniques, and thereby to controls. A system's design can be evaluated with respect to how well it applies the structural design principles, using metrics identified in [12].

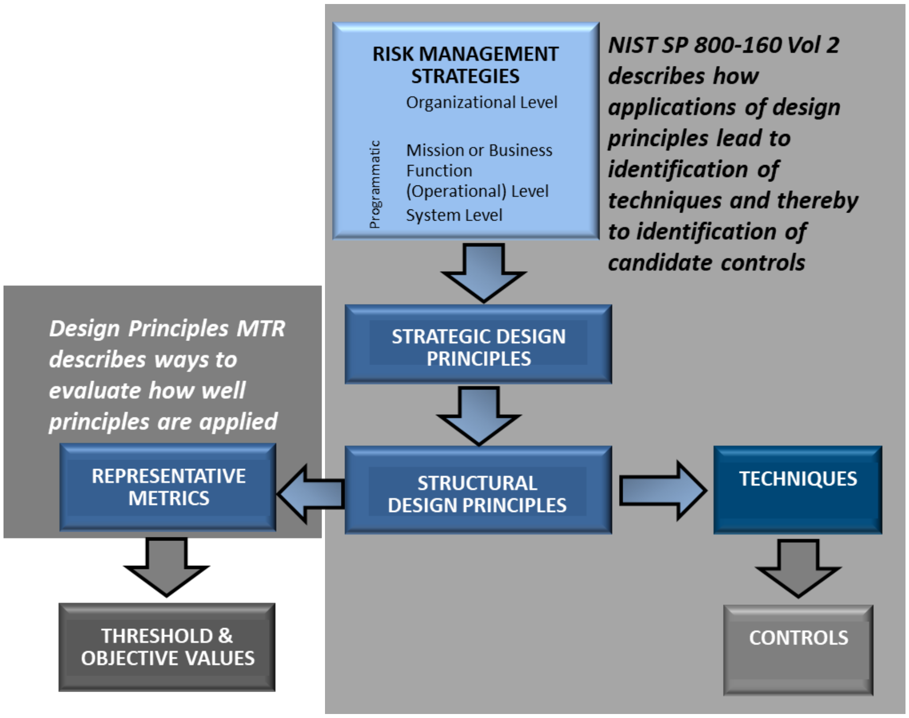

RISK MANAGEMENT STRATEGIES
Organizational Level
Programmatic
Mission or Business Function (Operational) Level
System Level
NIST SP 800-160 Vol 2 describes how applications of design principles lead to identification of techniques and thereby to identification of candidate controls
STRATEGIC DESIGN PRINCIPLES
Design Principles MTR describes ways to evaluate how well principles are applied
REPRESENTATIVE METRICS
STRUCTURAL DESIGN PRINCIPLES
TECHNIQUES
THRESHOLD & OBJECTIVE VALUES
CONTROLS

Figure 4. Identifying Controls via Design Principles

Following a second path, illustrated in Figure 5, identification of objectives leads to identification of techniques and approaches and thereby to identification of candidate controls. The selection of techniques, approaches, and controls, and their allocations to locations in the system architecture, depend on a variety of factors as identified in [1] [2]. This path does not identify related metrics.

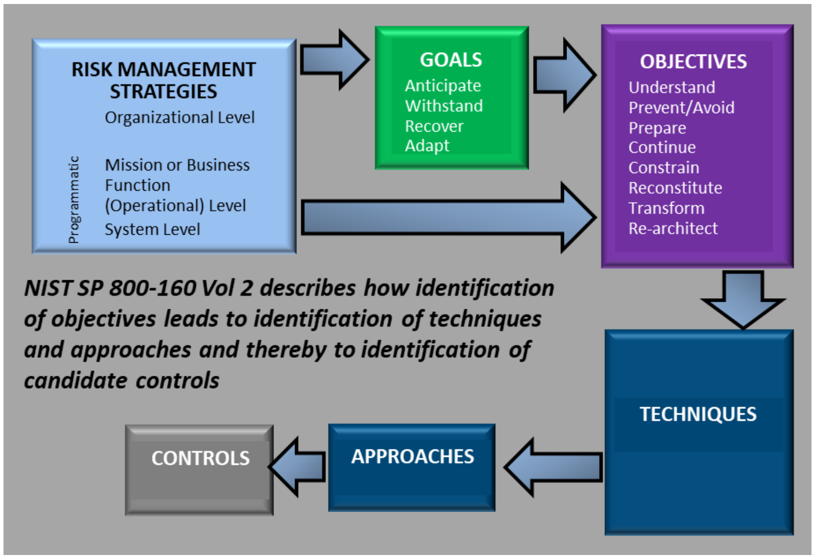

RISK MANAGEMENT STRATEGIES
Organizational Level
Mission or Business Function (Operational) Level
System Level
Programmatic
GOALS
Anticipate
Withstand
Recover
Adapt
OBJECTIVES
Understand
Prevent/Avoid
Prepare
Continue
Constrain
Reconstitute
Transform
Re-architect
NIST SP 800-160 Vol 2 describes how identification of objectives leads to identification of techniques and approaches and thereby to identification of candidate controls
TECHNIQUES
APPROACHES
CONTROLS

Figure 5. Identifying Controls via Objectives

A third path, illustrated in Figure 6, provides traceability from prioritized objectives to sub-objectives to capabilities, from which requirements can be defined and metrics identified. The set of representative sub-objectives and capabilities currently documented in [6] have a strong EIT flavor, and would need to be revised to apply to a weapon system. An illustration of such a revision, for a vehicle fleet, is given in [7].

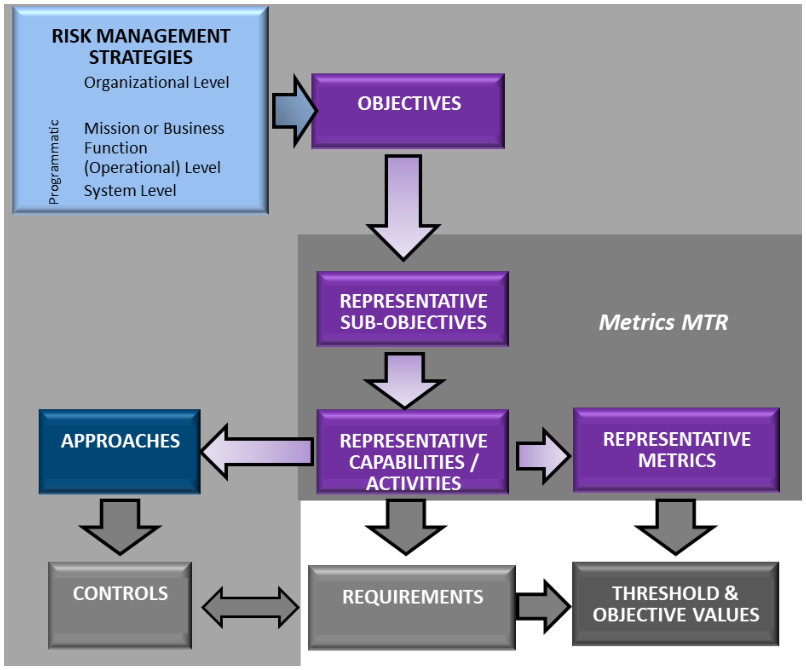

RISK MANAGEMENT STRATEGIES
Organizational Level
Mission or Business Function (Operational) Level
System Level
Programmatic
OBJECTIVES
REPRESENTATIVE SUB-OBJECTIVES
Metrics MTR
APPROACHES
REPRESENTATIVE CAPABILITIES / ACTIVITIES
REPRESENTATIVE METRICS
CONTROLS
REQUIREMENTS
THRESHOLD & OBJECTIVE VALUES

Figure 6. Using Sub-Objectives and Capabilities to Identify Requirements and Metrics

Sections 3 and 4 provide mappings between the CSAs and the cyber resiliency constructs that enable cyber resiliency goals, objectives, design principles, techniques, and approaches – as driven by a cyber risk management strategy – to be applied in the context of, and to enhance, cyber survivability.

3 High-Level Mappings

This section presents mappings between the high-level cyber resiliency constructs – goals, objectives, design principles, and techniques – and the CSAs.

3.1 Cyber Resiliency Goals and Objectives

The cyber resiliency goals and objectives relate to the SS KPP Pillars, rather than to individual CSAs. The Prevent pillar (which roughly corresponds to the Identify and Protect functions in the NIST Cybersecurity Framework or NCF [13]) is covered by the Anticipate goal and the Understand, Prevent / Avoid, and Prepare objectives. That is, achieving those objectives will ensure that the pillar is achieved. Conversely, the pillar supports the Anticipate goal and the Understand, Prevent / Avoid, and Prepare objectives; by achieving the pillar, many of the sub-objectives will be achieved in whole or in part.

The Mitigate pillar (which corresponds roughly to the NCF Detect and Respond functions) is covered by the Withstand goal and the Understand, Continue, and Constrain objectives. The Recover pillar (which corresponds to the Recover NCF function) is covered by the Recover goal and the Understand and Reconstitute objectives. Note that the Adapt goal – "modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments" – and the Transform and Re-Architect objectives which support that goal are not addressed by the SS KPP pillars or the NCF functions, which treat the system and its operational environment as relatively static.

3.2 Cyber Resiliency Design Principles and Techniques

As illustrated in Figure 4 above, one approach to identifying cyber resiliency constructs that apply to a system or situation involves sequentially identifying relevant strategic design principles, structural design principles, and techniques, based on [12]. Table 2 identifies cyber resiliency design principles and techniques which **support** the implementation of the CSAs.[9] More specifically,

- Strategic design principle: If the identified strategic cyber resiliency design principles are not applied to the system, then analysis of whether the system can implement the CSA may be more challenging.
- Structural design principle: If the identified structural design principles are not applied to the system, then the system architecture and design may not accommodate the CSA.
- Cyber resiliency technique: If the identified cyber resiliency techniques are not reflected in system requirements, then implementation of the CSA may be more difficult, or options for its implementation may be more limited.

System requirements written to implement the CSA, or documentation providing implementation evidence, may cite the supporting cyber resiliency design principle or technique. Documentation about the cyber resiliency design principle or technique (in the draft NIST SP 800-160 Vol. 2 [1]

[9] See the bulleted list preceding Table 7 for descriptions of possible relationships between CSAs and cyber resiliency constructs.

[2] or other cyber resiliency reports) may assist in determining how to implement the CSA most effectively.

Table 2 is structured as follows: For each CSA, supporting strategic design principles are identified in the second column. As described in [1], each strategic design principle drives the selection of multiple structural design principles; those that support the CSA are identified in the third column, aligned with the strategic design principle. Each structural design principle provides guidance on how to apply multiple cyber resiliency techniques; those that support the CSA in the context of the design principle are identified in the fourth column.[10] Techniques which are most strongly supportive of the CSA are **bolded**.[11]

Table 2. Cyber Resiliency Design Principles and Techniques Supporting CSAs

CSA	Supporting CR Strategic Design Principle(s)	Supporting CR Structural Design Principle(s)	Supporting CR Technique(s) or *Implementation Approach(es)*
CSA 01: Control access (CA)	Assume compromised resources	Control visibility and use	**Privilege Restriction** Segmentation
		Determine ongoing trustworthiness	Substantiated Integrity
CSA 02: Reduce system's cyber detectability (RSCD)	Reduce attack surfaces	Control visibility and use	Segmentation ***Obfuscation***
		Maximize transience	**Non-Persistence** Unpredictability
	Support agility and architect for adaptability	Make resources location-versatile	Dynamic Positioning Unpredictability
CSA 03: Secure transmissions and communications (STC)	Focus on common critical assets	Layer defenses and partition resources	Coordinated Protection Segmentation
		Determine ongoing trustworthiness	**Substantiated Integrity**[12]
		Limit the need for trust	Realignment
		Maximize transience	Non-Persistence
	Assume compromised resources	Change or disrupt the attack surface	Dynamic Positioning Non-Persistence
		Limit the need for trust	Privilege Restriction Realignment
		Control visibility and use	Privilege Restriction Segmentation ***Obfuscation***
CSA 04: Protect system's information from exploitation (PSIFE)	Assume compromised resources	Contain and exclude behaviors	**Privilege Restriction** **Segmentation**
		Layer defenses and partition resources	Coordinated Protection Segmentation

[10] In general, the techniques identified in Table 2 are required by the structural design principle; an underline indicates that the technique is not required but is typically used in conjunction with the required techniques to apply the principle more effectively. Redundancies within a strategic design principle are suppressed: For example, for the "Reduce attack surfaces" strategic principle supporting CSA 02, since Non-Persistence is required by the "Maximize transience" structural principle, it is not mentioned as a supporting-but-not-required technique for the "Control visibility and use" principle.

[11] With the exception of the Obfuscation approach to Deception, which includes but is not limited to encryption, cyber resiliency implementation approaches are not identified in Table 2. If a technique is identified in the fourth column, multiple approaches to that technique – but not necessarily all approaches – support the CSA in the first column; see Table 7 for details.

[12] Substantiated Integrity can be applied to validate that the crypto devices have not been modified or replaced.

CSA	Supporting CR Strategic Design Principle(s)	Supporting CR Structural Design Principle(s)	Supporting CR Technique(s) or *Implementation Approach(es)*
		Maximize transience	**Non-Persistence**
		Determine ongoing trustworthiness	Substantiated Integrity
		Change or disrupt the attack surface	Dynamic Positioning Non-Persistence
		Control visibility and use	Privilege Restriction Segmentation ***Obfuscation***
		Layer defenses and partition resources	Segmentation Coordinated Protection
CSA 05: Partition and ensure critical functions at mission completion performance levels (PECF)	Focus on common critical assets	Plan and manage diversity	**Diversity**
		Maintain redundancy	Redundancy
		Manage resources (risk-) adaptively	**Adaptive Response**
		Leverage health and status data	Analytic Monitoring Contextual Awareness
		Maximize transience	Non-Persistence
	Assume compromised resources	Change or disrupt the attack surface	Dynamic Positioning Non-Persistence
		Limit the need for trust	Coordinated Protection Realignment
		Maximize transience	Non-Persistence Unpredictability
		Layer defenses and partition resources	**Segmentation**
CSA 06: Minimize and harden attack surfaces (MHAS)	Reduce attack surfaces	Limit the need for trust	**Privilege Restriction** **Realignment**
		Change or disrupt the attack surface	Dynamic Positioning Non-Persistence
		Make the effects of deception and unpredictability user-transparent	Coordinated Protection
		Determine on-going trustworthiness	Substantiated Integrity
		Contain and exclude behaviors	Privilege Restriction Segmentation
		Layer defenses and partition resources	Coordinated Protection Segmentation
	Expect adversaries to evolve	Contain and exclude behaviors	Privilege Restriction Segmentation
	Assume compromised resources	Leverage health and status data	**Analytic Monitoring** Contextual Awareness
CSA 07: Baseline and monitor systems and detect anomalies (BMDA)	Focus on common critical assets	Leverage health and status data	**Analytic Monitoring** **Contextual Awareness**
		Maintain situational awareness	Analytic Monitoring Contextual Awareness
CSA 08: Manage system performance if degraded by cyber events (MSP)	Focus on common critical assets	Control visibility and use	Privilege Restriction Segmentation
		Contain and exclude behaviors	Privilege Restriction Segmentation

CSA	Supporting CR Strategic Design Principle(s)	Supporting CR Structural Design Principle(s)	Supporting CR Technique(s) or *Implementation Approach(es)*
		Maintain situational awareness	Contextual Awareness
		Maintain redundancy	Redundancy
	Assume compromised resources	Layer defenses and partition resources	**Coordinated Protection** Segmentation
		Leverage health and status data	**Analytic Monitoring** **Contextual Awareness**
	Expect adversaries to adapt	Manage resources (risk-) adaptively	**Adaptive Response**
		Determine ongoing trustworthiness	Substantiated Integrity
CSA 09: Recover system capabilities (RSC)	Support agility and architect for adaptability	Plan and manage diversity	Diversity
		Maintain redundancy	Redundancy
		Manage resources (risk-) adaptively	**Adaptive Response**
	Assume compromised resources	Contain and exclude behaviors	Privilege Restriction Segmentation
		Layer defenses and partition resources	**Coordinated Protection** Segmentation
		Determine ongoing trustworthiness	Substantiated Integrity
	Expect adversaries to adapt	Make resources location versatile	Dynamic Positioning
		Leverage health and status data	Analytic Monitoring Contextual Awareness
		Maintain situational awareness	Contextual Awareness
CSA 10: Actively manage system configuration to counter vulnerabilities at tactically relevant speeds (AMCV)	Focus on common critical assets	Contain and exclude behaviors	Privilege Restriction Segmentation
		Plan and manage diversity	**Coordinated Protection** Diversity
		Leverage health and status data	Analytic Monitoring Contextual Awareness
		Manage resources (risk-) adaptively	**Adaptive Response**
		Determine ongoing trustworthiness	**Substantiated Integrity**

Cyber resiliency capabilities are based on a foundation of technologies and practices for cybersecurity, system resilience, and continuity of operations (COOP). Therefore, the application of cyber resiliency techniques and implementation approaches can depend on or can use implementation of CSAs; if the CSA is not provided, the application of the cyber resiliency construct can be significantly or somewhat restricted. Specifically,

- CSA 01: The Attribute-Based Usage Restriction approach to Privilege Restriction depends on identification and authentication (I&A). The Integrity Checks approach to Substantiated Integrity can use anti-tamper measures.
- CSA 02: The Misdirection approach to Deception can use the electronic and physical masking of the system and its behavior, since a deception environment can be made visible.

- CSA 03: The Integrity Checks and Provenance Tracking approaches to Substantiated Integrity can use the encryption of transmitted data.
- CSA 04: The Trust-Based Privilege Management and Attribute-Based Usage Restriction approaches to Privilege Restriction can use the access restriction mechanisms. The Integrity Checks approach to Substantiated Integrity can use encryption.
- CSA 05: The Predefined Segmentation approach to Segmentation depends on the definitions of logical and physical partitions.
- CSA 06: The Attribute-Based Usage Restriction approach to Privilege Restriction can use the attributes used to determine restrictions on ports, protocols, and services. The Monitoring and Damage Assessment approach to Analytic Monitoring and the Dynamic Resource Awareness approach to Contextual Awareness can use the logging of cyber attack surfaces.
- CSA 07: The Monitoring and Damage Assessment approach to Analytic Monitoring and the Dynamic Resource Awareness approach to Contextual Awareness depend on monitoring and anomaly detection.
- CSA 08: All approaches to Adaptive Response depend on prioritization of functions.
- CSA 09: The Adaptive Management approach to Adaptive Response depends on prioritization of functions and capabilities to replace or reconfigure functionality.
- CSA 10: The Dynamic Reconfiguration approach to Adaptive Response, the Monitoring and Damage Assessment approach to Analytic Monitoring, and the Dynamic Resource Awareness approach to Contextual Awareness can use the monitoring of system configuration and patch status.

4 Detailed Mapping

Table 3 summarizes the mappings in Section 3, and adds more detail by identifying relationships between cyber resiliency approaches and CSAs. This mapping is initial, independent of any specific system architecture or mission type, based on general understanding of the technologies and practices involved in the cyber resiliency and cyber survivability constructs. Relationships considered are as follows:

- **E**: The cyber resiliency construct is **essential to** the CSA or SS KPP Pillar; the CSA or SS KPP Pillar *depends* on the cyber resiliency construct. If the cyber resiliency construct is not applied (i.e., is not used as intended, as described in Table 1), implementation of the CSA may be extremely difficult or even impossible.
- **S**: The cyber resiliency construct **supports** the CSA or SS KPP Pillar; that is, the CSA *uses* (or can use) the cyber resiliency construct. If the cyber resiliency construct is not applied, the alternatives for implementing the CSA may be limited. (See the description of "support" prior to Table 2.)
- **I**: The cyber resiliency construct **indirectly supports** the CSA or SS KPP Pillar; that is, application of the cyber resiliency construct lays the analytic, operational, or technical foundation for implementing the CSA. If the cyber resiliency construct is not applied, additional effort may be needed to implement the CSA.
- **D**: The cyber resiliency construct **depends** on implementation of the CSA; the CSA is *essential* to the cyber resiliency construct. If the CSA has not been selected, the cyber resiliency construct may be difficult or impossible to apply.
- **U**: The cyber resiliency construct **uses** (or can use) implementation of the CSA or Pillar; the CSA or Pillar *supports* the cyber resiliency construct. If the CSA has not been selected, the alternatives for applying the cyber resiliency construct are more limited than they would be.
- **F**: Potential **friction** exists between the cyber resiliency construct and the CSA or Pillar, so that implementation of one can complicate or conflict with implementation of the other. For example, some approaches to Diversity can complicate monitoring and recovery, even as they provide alternatives that support recovery. However, added complexity can often be managed (usually by applying the Consistency Analysis and Orchestration approaches to Coordinated Protection); when complexity is properly managed, application of the cyber resiliency construct may increase the effectiveness of the CSA, or vice versa.

Based on this table, two general observations can be made. First, some cyber resiliency constructs do not map to any CSAs or Pillars; these are highlighted. This is due to differences in the scope of cyber survivability, which is focused on the system level and does not include cyber defense capabilities. Second, the matrix is relatively sparse. This reflects the fact that both the cyber resiliency constructs and the CSAs are relatively well defined; vague statements would have resulted in more entries.

Table 3. Mapping Cyber Resiliency Constructs to Cyber Survivability Attributes

SS KPP Pillar →	Prevent							Mitigate			Recover		All Pillars
Cyber Resiliency Construct ↓	**CSA 01: CA**	**CSA 02: RSCD**	**CSA 03: STC**	**CSA 04: PSIFE**	**CSA 05: PECF**	**CSA 06: MHAS**	***Prevent* Pillar in General**	**CSA 07: BMDA**	**CSA 08: MSP**	***Mitigate* Pillar in General**	**CSA 09: RSC**	***Recover* Pillar in General**	**CSA 10: AMCV**
Cyber Resiliency Objectives													
Prevent / Avoid							S, U						
Prepare							S, U			S, U		S, U	
Continue										S, U		S, U	
Constrain										S, U		S, U	
Reconstitute												S, U	
Understand							S, U			S, U		S, U	S, U
Transform							S			S		S	
Re-Architect							S			S		S	
Strategic Cyber Resiliency Design Principles													
Focus on common critical assets.			S		S			S	S				S
Support agility and architect for adaptability.		S									S		
Reduce attack surfaces.		S				S							
Assume compromised resources.	S		S	S	S	S			S		S		
Expect adversaries to evolve.						S			S		S		
Structural Cyber Resiliency Design Principles													
Limit the need for trust.			S		S	S							
Control visibility and use.	S	S		S					S				
Contain and exclude behaviors.				S		S			S		S		S
Layer defenses and partition resources.			S	S	S				S		S		
Plan and manage diversity.					S						S		S
Maintain redundancy.					S				S		S		
Make resources location-versatile.		S									S		

SS KPP Pillar →	**Prevent**							**Mitigate**			**Recover**		**All Pillars**
Cyber Resiliency Construct ↓	**CSA 01: CA**	**CSA 02: RSCD**	**CSA 03: STC**	**CSA 04: PSIFE**	**CSA 05: PECF**	**CSA 06: MHAS**	***Prevent* Pillar in General**	**CSA 07: BMDA**	**CSA 08: MSP**	***Mitigate* Pillar in General**	**CSA 09: RSC**	***Recover* Pillar in General**	**CSA 10: AMCV**
Leverage health and status data.					S	S		S	S		S		S
Maintain situational awareness.								S	S		S		
Manage resources (risk-) adaptively.					S				S		S		S
Maximize transience.		S	S	S	S								
Determine ongoing trustworthiness.	S		S	S		S			S		S		S
Change or disrupt the attack surface.			S	S	S	S							
Make the effects of deception and unpredictability user-transparent.						S							
Cyber Resiliency *Techniques* and Implementation Approaches													
Adaptive Response	F				S			F	S		S		S
Dynamic Reconfiguration	F				S			F	S, D		S		S, U
Dynamic Resource Allocation	F				S			F	S, D		S		S
Adaptive Management	F				S			F	S, D		S, D		S
Analytic Monitoring					S	S		S	S		S		S
Monitoring and Damage Assessment					S	S, U		E, D	S		S		S, U
Sensor Fusion and Analysis					S				S		S		S
Forensic and Behavioral Analysis									S		S		
Coordinated Protection			S	S	S	S			S		S		S
Calibrated Defense-in-Depth						S			S				
Consistency Analysis			S	S	S	S			S		S		S
Orchestration			S	S	S	S			S		S		S
Self-Challenge								F	S				F
Contextual Awareness					S	S		S	S		S		S

SS KPP Pillar →	Prevent							Mitigate			Recover		All Pillars
Cyber Resiliency Construct ↓	CSA 01: CA	CSA 02: RSCD	CSA 03: STC	CSA 04: PSIFE	CSA 05: PECF	CSA 06: MHAS	*Prevent* Pillar in General	CSA 07: BMDA	CSA 08: MSP	*Mitigate* Pillar in General	CSA 09: RSC	*Recover* Pillar in General	CSA 10: AMCV
Dynamic Resource Awareness					S	S, U		S, D					S, U
Dynamic Threat Awareness													
Mission Dependency and Status Visualization													
Deception													
Obfuscation		S	E	S									
Disinformation													
Misdirection		U											
Tainting													
Diversity					S						S		S
Architectural Diversity					S						S		S, F
Design Diversity					S						S		S, F
Synthetic Diversity					S								
Information Diversity													S, F
Path Diversity					S						S		S, F
Supply Chain Diversity													
Dynamic Positioning		S	S	S	S	S, F					S		
Functional Relocation of Sensors			F		S	S					S		
Functional Relocation of Cyber Resources		S	S	S	S	F					S		F
Asset Mobility		S			S	F					S		F
Fragmentation		S		S	S	F					S, F		F
Distributed Functionality		S			S	F					S, F		F
Non-Persistence		S	S	S	S	S							
Non-Persistent Information		S		S									
Non-Persistent Services		S	S	S	S	S							
Non-Persistent Connectivity		S	S	S	S	S							

SS KPP Pillar →	**Prevent**							**Mitigate**			**Recover**		**All Pillars**
Cyber Resiliency Construct ↓	**CSA 01: CA**	**CSA 02: RSCD**	**CSA 03: STC**	**CSA 04: PSIFE**	**CSA 05: PECF**	**CSA 06: MHAS**	***Prevent* Pillar in General**	**CSA 07: BMDA**	**CSA 08: MSP**	***Mitigate* Pillar in General**	**CSA 09: RSC**	***Recover* Pillar in General**	**CSA 10: AMCV**
Privilege Restriction	S			S		S			S		S		
Trust-Based Privilege Management	S			S, U		S			S		S		
Attribute-Based Usage Restriction	S, D			S, U		S, U			S		S		
Dynamic Privileges	S	S		S					S		S		
Realignment			S		S	S							
Purposing			S		S	S							
Offloading			S		S	S							
Restriction			S		S	S							
Replacement					S								
Specialization			S		S								
Redundancy					S				S		S		
Protected Backup and Restore									S		E		
Surplus Capacity					S				S		S		
Replication					S				S		S		
Segmentation	S	S	S	S	S	S			S		S		
Predefined Segmentation	S	S	S	S	E, D	S, U			S		S		
Dynamic Segmentation and Isolation				S	S				S		S		
Substantiated Integrity	S		S	S		S		S	S		S		S
Integrity Checks	S, U		S, U	S, U		S		S	S		S		S
Provenance Tracking	S		S, U	S							S		S
Behavior Validation	S					S			S		S		S
Unpredictability		S			S			F	F				F
Temporal Unpredictability		S			S			F	F				F
Contextual Unpredictability		S			S			F	F				F

5 Conclusion

Cyber survivability and cyber resiliency are closely related but not identical concepts, each with its own framework of constructs and relationships between those constructs. This report provides an initial identification of relationships between cyber resiliency constructs and the cyber survivability constructs of CSAs and SS KPP Pillars. Both cyber resiliency constructs and CSAs can serve as starting points for defining system requirements. Both can also be used to define threshold and objective values for functional requirements. By understanding the potential relationships among these constructs, systems security engineers can describe how system requirements support both cyber survivability and cyber resiliency, can identify relevant metrics to be measured during test and evaluation, can avoid defining redundant requirements expressed in different terms but with the same intent, and can avoid defining a set of system requirements that are difficult to satisfy simultaneously.

The identification of relationships in this report is intended to serve as a starting point for identifying the interdependencies between cyber resiliency and cyber survivability constructs in the context of a specific weapon system. This will enable systems engineers to identify controls, requirements, metrics, and alternative solutions that meet both cyber resiliency and cyber survivability needs. This identification can only be a starting point: For any given system, the applicability of the cyber resiliency constructs needs to be determined and the statements of those constructs tailored to be meaningful. Similarly, the relevant CSAs need to be determined based on CSRC, and the exemplar language for CSAs and SSE sub-elements needs to be tailored to the system.

The analysis in this paper could be extended in several ways. First, a more detailed analysis could consider how the exemplar language varies, depending on a system's Cyber Survivability Risk Category (CSRC). Second, it could also include a mapping between cyber resiliency constructs and SSE sub-elements. Third, the analysis could include representative cyber resiliency sub-objectives and capabilities, as defined in [6]. Finally, the analysis could identify an additional possible relationship:

- C: Application of the cyber resiliency construct and implementation of the CSA depend on the implementation of a **common** control or use of a common mechanism. (Note that this relationship would in some cases supersede the entry of "S, U" in Table 7.)

These extensions, relying on the Cyber Survivability Endorsement Implementation Guide and its annexes, would produce a For Official Use Only (FOUO) analysis, while this report is based solely on publicly available information. Finally, the analysis in this paper could be aligned with, and possibly incorporated into, the knowledge base of the Air Force Research Laboratory (AFRL) CSA Tool [14].

6 References

[1] NIST, "Initial Public Draft of NIST SSP 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," 21 March 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

[2] NIST, "Draft NIST Special Publication 800-160 Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach," 4 September 2019. [Online]. Available: https://csrc.nist.gov/publications/sp800.

[3] S. Pitcher, "New DoD Approaches on the Cyber Survivability of Weapon Systems (25 March 2019)," 25 March 2019. [Online]. Available: https://www.itea.org/wp-content/uploads/2019/03/Pitcher-Steve.pdf.

[4] Department of Defense, "Department of Defense Cybersecurity Test and Evaluation Guidebook, Version 2.0," 25 April 2018. [Online]. Available: https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf.

[5] DoD, "Manual for the Operations of the Joint Capabilities Integration and Development System (JCIDS), including errata as of 18 December 2015," 18 December 2015. [Online]. Available: http://www.acqnotes.com/wp-content/uploads/2014/09/Manual-for-the-Operationsof-the-Joint-Capabilities-Integration-and-Development-System-JCIDS-18-Dec-2015.pdf.

[6] D. Bodeau, R. Graubart, R. McQuaid and J. Woodill, "Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods (MTR 180314)," The MITRE Corporation, Bedford, MA, 2018.

[7] D. J. Bodeau, R. D. Graubart, R. M. McQuaid and J. Woodill, "Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodology and Examples (MTR 180449)," The MITRE Corporation, Bedford, MA, 2018.

[8] NIST, "NIST SP 800-160 Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (including updates as of 3-21-2018)," 15 November 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.

[9] NIST / Joint Task Force, "NIST SP 800-37R2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[10] CNSS, "CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems," 27 March 2014. [Online]. Available: http://www.cnss.gov/CNSS/openDoc.cfm?PNw3S8vHSJe2vEzG4g0sWw==.

[11] NIST, "NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[12] D. J. Bodeau and R. D. Graubart, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," January 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[13] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[14] J. Reilly, *Cyber Survivability Attributes: CSA Tool (8ABW-2019-2267),* Rome, NY: Air Force Research Laboratory, 2019.

[15] The Joint Staff J6/J8, DCIO-CSCISO (CSI&AI), and NSA IAC, "Volume II Annex: Systems Security engineer (SSE) Sub-Elements Supporting Volume II – Risk-Managed Performance Measures for System Survivability, DCIO-CS/CISO Discussion Draft V 0.9.5," 2017.

[16] D. Fitzpatrick, D. Bodeau, R. Graubart, R. McQuaid, C. Olin and J. Woodill, "(DRAFT) Cyber Resiliency Evaluation Framework for Weapon Systems: Foundational Principles and Their Potential Effects on Adversaries," The MITRE Corporation, Bedford, MA, 2019.

[17] DoD, "Manual for the Operation of The Joint Capabilities Integration and Development System (JCIDS)," 31 August 2018. [Online]. Available: https://www.dau.mil/cop/rqmt/DAU%20Sponsored%20Documents/Manual%20-%20JCIDS,%2031%20Aug%202018.pdf.

Appendix A Cyber Resiliency Constructs

This appendix describes the cyber resiliency constructs used in the mappings in Table 3. It also describes the relationship between a cyber resiliency solution and those constructs.

Table 4. Cyber Resiliency Goals

Goal	Description
Anticipate	Maintain a state of informed preparedness for adversity.
Withstand	Continue essential mission or business functions despite adversity.
Recover	Restore mission or business functions during and after adversity.
Adapt	Modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments.

Table 5. Cyber Resiliency Objectives

Objective	Description
Prevent or Avoid	Preclude the successful execution of an attack or the realization of adverse conditions.
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.
Constrain	Limit damage from adversity.
Reconstitute	Restore as much mission or business functionality as possible after adversity.
Understand	Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.
Transform	Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.
Re-architect	Modify architectures to handle adversity and address environmental changes more effectively.

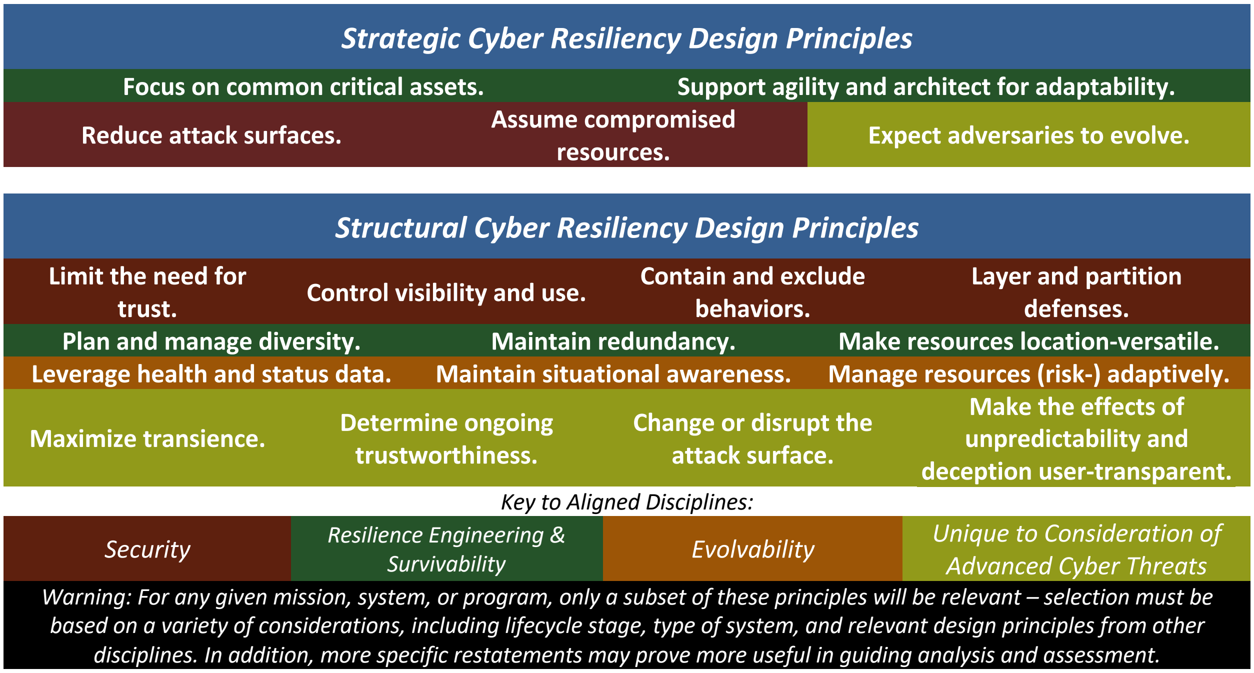
Table 6. Cyber Resiliency Techniques and Approaches

Resiliency Technique	Cyber Resiliency Implementation Approach
Adaptive Response: Implement agile cyber courses of action to manage risks.	**Dynamic Reconfiguration**: Make changes to individual systems, system elements, components, or sets of cyber resources to change functionality or behavior without interrupting service.
	Dynamic Resource Allocation: Change the allocation of resources to tasks or functions without terminating critical functions or processes.
	Adaptive Management: Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.
Analytic Monitoring: Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	**Monitoring and Damage Assessment**: Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, and to detect and assess damage from adversity.
	Sensor Fusion and Analysis: Fuse and analyze monitoring data and analysis results from different information sources or at different times, together with externally provided threat intelligence.
	Malware and Forensic Analysis: Analyze adversary TTPs, including observed behavior as well as malware and other artifacts left behind by adverse events.

Resiliency Technique	Cyber Resiliency Implementation Approach
Contextual Awareness: Construct and maintain current representations of the posture of missions or business functions considering cyber events and cyber courses of action.	**Dynamic Resource Awareness**: Maintain current information about resources, status of resources, and resource connectivity.
	Dynamic Threat Modeling: Maintain current information about threat actors, indicators, and potential, predicted, and observed adverse events.
	Mission Dependency and Status Visualization: Maintain current information about the status of missions or business functions, dependencies on resources, and the status of those resources with respect to threats.
Coordinated Protection: Ensure that protection mechanisms operate in a coordinated and effective manner.	**Calibrated Defense-in-Depth:** Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value.
	Consistency Analysis: Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps.
	Orchestration: Coordinate the ongoing behavior of mechanisms and processes at different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps.
	Self-Challenge: Affect mission/business processes or system elements adversely in a controlled manner, to validate the effectiveness of protections and to enable proactive response and improvement.
Deception: Mislead, confuse, hide critical assets from, or expose covertly tainted assets to, the adversary.	**Obfuscation**: Hide, transform, or otherwise obfuscate information from the adversary.
	Disinformation: Provide deliberately misleading information to adversaries.
	Misdirection: Maintain deception resources or environments and direct adversary activities there.
	Tainting: Embed covert capabilities in resources.
Diversity: Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.	**Architectural Diversity**: Use multiple sets of technical standards, different technologies, and different architectural patterns.
	Design Diversity: Use different designs to meet the same requirements or provide equivalent functionality.
	Synthetic Diversity: Transform implementations of software to produce a variety of instances.
	Information Diversity: Provide information from different sources or transform information in different ways.
	Path Diversity: Provide multiple independent paths for command, control, and communications.
	Supply Chain Diversity: Use multiple independent supply chains for critical components.
Dynamic Positioning: Distribute and dynamically relocate functionality or system resources.	**Functional Relocation of Sensors**: Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adverse events.
	Functional Relocation of Cyber Resources: Change the location of cyber resources that provide functionality or information, either by moving the assets or by transferring functional responsibility.
	Asset Mobility: Securely move physical resources.
	Fragmentation: Fragment information and distribute it across multiple components.
	Distributed Functionality: Decompose a function or application into smaller functions and distribute those functions across multiple components.
Non-Persistence: Generate and retain resources as needed or for a limited time.	**Non-Persistent Information**: Refresh information periodically, or generate information on demand, and delete it when no longer needed.
	Non-Persistent Services: Refresh services periodically, or generate services on demand and terminate services when no longer needed.

Resiliency Technique	Cyber Resiliency Implementation Approach
	Non-Persistent Connectivity: Establish connections on demand, and terminate connections when no longer needed.
Privilege Restriction: Restrict privileges based on attributes of users and system elements as well as on environmental factors.	**Trust-Based Privilege Management**: Define, assign, and maintain privileges associated with active entities, based on established trust criteria, consistent with principles of least privilege.
	Attribute-Based Usage Restrictions: Define, assign, maintain, and apply usage restrictions on systems containing cyber resources based on the criticality of missions or business functions and other attributes (e.g., data sensitivity).
	Dynamic Privileges: Elevate or decrease privileges assigned to a user, process, or service based on transient or contextual factors.
Realignment: Align system resources with core aspects of organizational mission or business function needs to reduce risk.	**Purposing**: Ensure systems containing cyber resources are used consistent with critical mission or business function purposes and approved uses.
	Offloading: Offload supportive but non-essential functions to other systems or to an external provider that is better able to support the functions.
	Restriction: Remove or disable unneeded functionality or connectivity, or add mechanisms to reduce the chance of vulnerability or failure.
	Replacement: Replace low-assurance or poorly understood implementations with more trustworthy implementations.
	Specialization: Modify the design of, augment, or configure critical cyber resources uniquely for the mission or business function to improve trustworthiness.
Redundancy: Provide multiple protected instances of critical resources.	**Protected Backup and Restore**: Back up information and software (including configuration data and virtualized resources) in a way that protects its confidentiality, integrity, and authenticity, and enable restoration in case of disruption or corruption.
	Surplus Capacity: Maintain extra capacity for information storage, processing, or communications.
	Replication: Duplicate hardware, information, backups, or functionality in multiple locations and keep them synchronized.
Segmentation: Define and separate system elements based on criticality and trustworthiness.	**Predefined Segmentation**: Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.
	Dynamic Segmentation and Isolation: Change the configuration of enclaves or protected segments, or isolate resources, while minimizing operational disruption.
Substantiated Integrity: Ascertain whether critical system elements have been corrupted.	**Integrity Checks**: Apply and validate checks of the integrity or quality of information, components, or services.
	Provenance Tracking: Identify and track the provenance of data, software, or hardware elements.
	Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).
Unpredictability: Make changes randomly or unpredictably.	**Temporal Unpredictability:** Change behavior or state at times that are determined randomly or by complex functions.
	Contextual Unpredictability: Change behavior or state in ways that are determined randomly or by complex functions.

Table 7. Cyber Resiliency Design Principles



Strategic Cyber Resiliency Design Principles		
Focus on common critical assets.		Support agility and architect for adaptability.
Reduce attack surfaces.	Assume compromised resources.	Expect adversaries to evolve.

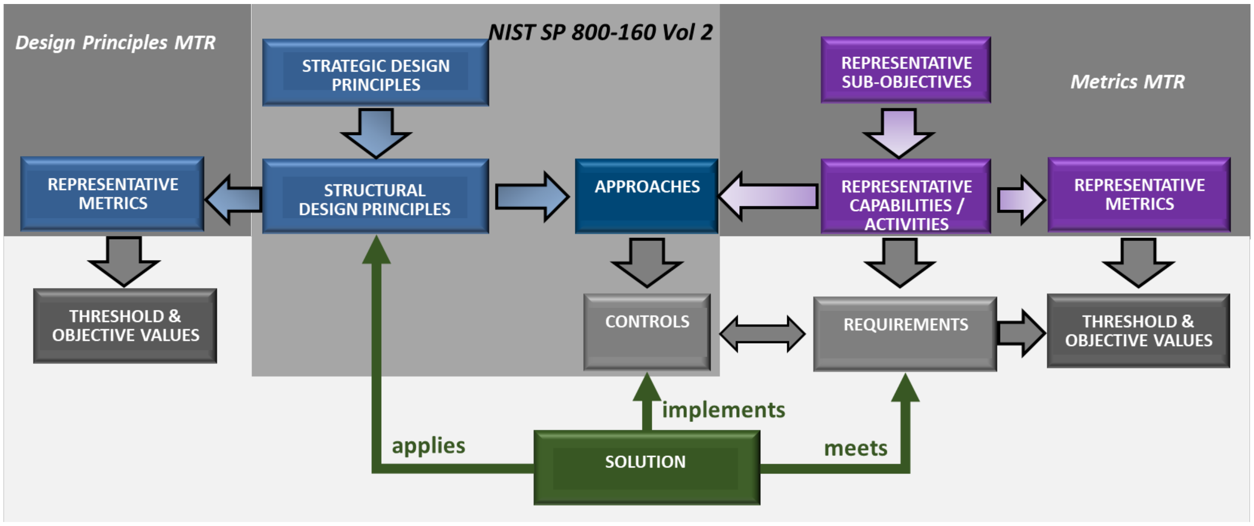
Structural Cyber Resiliency Design Principles			
Limit the need for trust.	Control visibility and use.	Contain and exclude behaviors.	Layer and partition defenses.
Plan and manage diversity.	Maintain redundancy.	Make resources location-versatile.	
Leverage health and status data.	Maintain situational awareness.	Manage resources (risk-) adaptively.	
Maximize transience.	Determine ongoing trustworthiness.	Change or disrupt the attack surface.	Make the effects of unpredictability and deception user-transparent.

Key to Aligned Disciplines:

Security	*Resilience Engineering & Survivability*	*Evolvability*	*Unique to Consideration of Advanced Cyber Threats*

Warning: For any given mission, system, or program, only a subset of these principles will be relevant – selection must be based on a variety of considerations, including lifecycle stage, type of system, and relevant design principles from other disciplines. In addition, more specific restatements may prove more useful in guiding analysis and assessment.

A cyber resiliency solution is a combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices which solves a problem in the cyber resiliency domain. In the context of a specific system, a cyber resiliency solution implements the identified controls, meets the identified requirements, and conforms with the relevant design principles. Threshold and objective requirements can be defined in terms of metrics related to the cyber resiliency capabilities identified in [6]. This is illustrated in Figure 7.



Design Principles MTR
STRATEGIC DESIGN PRINCIPLES
NIST SP 800-160 Vol 2
REPRESENTATIVE SUB-OBJECTIVES
Metrics MTR
REPRESENTATIVE METRICS
STRUCTURAL DESIGN PRINCIPLES
APPROACHES
REPRESENTATIVE CAPABILITIES / ACTIVITIES
REPRESENTATIVE METRICS
THRESHOLD & OBJECTIVE VALUES
CONTROLS
REQUIREMENTS
THRESHOLD & OBJECTIVE VALUES
implements
applies
SOLUTION
meets

Figure 7. Relationship of a Cyber Resiliency Solution to Controls, Requirements, and Design Principles

Appendix B Abbreviations and Acronyms

AFRL	Air Force Research Laboratory
AMCV	Actively Manage System Configuration to Counter Vulnerabilities at Tactically Relevant Speeds (CSA 10)
BMDA	Baseline and Monitor Systems and Detect Anomalies (CSA 07)
C3	Command, Control, and Communications
CA	Control Access (CSA 01)
CDD	Capability Development Document
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan (or Planning)
COTS	Commercial Off-the-Shelf
CR	Cyber Resiliency
CREF	Cyber Resiliency Engineering Framework
CSA	Cyber Survivability Attribute
CSEIG	Cyber Survivability Endorsement Implementation Guide
CSRC	Cyber Survivability Risk Category
DIB	Defense Industrial Base
EIT	Enterprise Information Technology
FOSS	Free and Open Source Software
FOUO	For Official Use Only
I&A	Identification and Authentication
ICD	Initial Capabilities Document
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
MHAS	Minimize and Harden Attack Surfaces (CSA 06)
MOE	Measure of Effectiveness
MSP	Manage System Performance if Degraded by Cyber Events (CSA 08)
NCF	NIST Cybersecurity Framework
NIST	National Institute of Standards and Technology

OPSEC	Operations Security
PECF	Partition and Ensure Critical Functions at Mission Completion Performance Levels (CSA 05)
PSIFE	Protect System’s Information From Exploitation (CSA 04)
RMF	Risk Management Framework
RSC	Recover system capabilities (CSA 09)
RSCD	Reduce System’s Cyber Detectability (CSA 02)
SDLC	System Development Lifecycle
SOW	Statement of Work
SP	Special Publication
SS	System Survivability
SSE	Systems Security Engineering
SSP	System Security Plan
STC	Secure Transmissions and Communications (CSA 03)
TTPs	Tactics, Techniques, and Procedures