



:Dept. No.: J830
Project No.: 01ADM105-SC

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.

Approved for Public Release; Distribution
Unlimited. Case 14-4035

©2014 The MITRE Corporation.
All rights reserved.

Bedford, MA

Cyber Resiliency Engineering Aid – Cyber Resiliency Techniques: Potential Interactions and Effects

**Deborah Bodeau
Richard Graubart
William Heinbockel
Ellen Laderman
November 2014**

Approved By

Marnie Salisbury

November 2014

Abstract

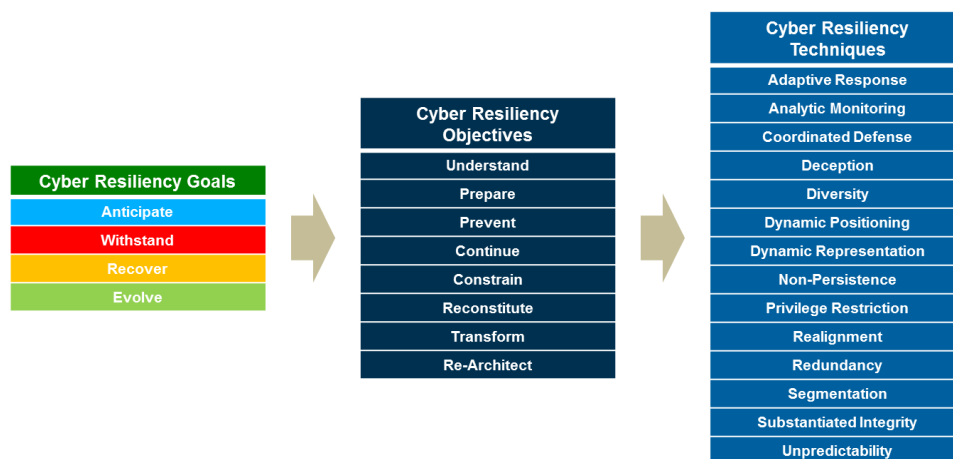
This white paper provides information on cyber resiliency techniques for systems engineers and architects. Specifically, it identifies potential interactions (e.g., dependencies, synergies, conflicts) between techniques, depending on the implementation approach. It also identifies potential effects that implementations of cyber resiliency techniques could have on adversary activities throughout different stages in the cyber attack lifecycle.

Cyber Resiliency Techniques: Potential Interactions and Effects

This white paper provides information on cyber resiliency techniques for systems engineers and architects. Specifically, it identifies potential interactions (e.g., dependencies, synergies, conflicts) between techniques, depending on the implementation approach. It also identifies potential effects that implementations of cyber resiliency techniques could have on adversary activities throughout different stages in the cyber attack lifecycle.¹

1 Introduction: The Cyber Resiliency Engineering Framework

Cyber resiliency is defined as the extent to which a nation, organization, or mission is able to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks, accidents, or naturally occurring threats or incidents to its critical cyber resources. Cyber resiliency is emerging as a key component in any effective strategy for mission assurance or operational resilience. While it builds on cyber security, cyber resiliency is based on a different assumption. Cyber security focuses on ensuring that the security objectives of confidentiality, integrity, availability, and accountability can be achieved at acceptable levels. Cyber resiliency assumes that good cyber security practices are already in place—but that nonetheless, an advanced adversary will be able to establish a presence on an enterprise's systems or networks. Thus, cyber resiliency assumes that an adversary is already positioned to deny or degrade functions; to destroy, modify, or fabricate data; to exfiltrate sensitive information; or to usurp services. Given this adversary advantage, how can cyber-dependent missions and business functions be adequately assured?











The Cyber Resiliency Engineering Framework (CREF) illustrated above organizes the cyber resiliency domain into a set of goals, objectives, and techniques. Goals are high-level statements of intended outcomes, which help scope the cyber resiliency domain. Objectives are more specific statements of

¹ This paper excerpts and updates material from *Cyber Resiliency Assessment: Enabling Architectural Improvement, Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain*, and *Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment*. These documents, as well as numerous other resources on cyber resiliency, can be found at www.mitre.org.

Cyber Resiliency Engineering Aid

intended outcomes that serve as a bridge between techniques and goals. Objectives are expressed so as to facilitate assessment, making it straightforward to develop questions of “how well,” “how quickly,” or “with what degree of confidence or trust” can each objective be achieved. Objectives enable different stakeholders to assert their different resiliency priorities based on mission or business functions.

Goal	Description
Anticipate	Maintain a state of informed preparedness in order to forestall compromises of mission function from potential adverse conditions
Withstand	Continue essential mission functions despite adverse conditions
Recover	Restore mission functions during and after the adverse conditions
Evolve	Change mission functions and/or supporting capabilities, so as to minimize adverse impacts from actual or predicted adverse conditions

Objective	Description	Goals Supported
Understand	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity	
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity	
Prevent / Avoid	Preclude successful execution of attack or the realization of adverse conditions	
Continue	Maximize the duration and viability of essential mission functions during adverse conditions	
Constrain	Limit damage from adverse conditions	
Reconstitute	Redeploy resources to provide as complete a set of mission functionality as possible subsequent to adverse conditions	
Transform	Change aspects of organizational behavior in response to prior, current or prospective adverse conditions or attack	
Re-architect	Modify architectures for improved resilience	

The CREF is deliberately incomplete: objectives and techniques that relate to organizational resilience or business continuity in the face of non-cyber threats (e.g., natural disaster, human error) are not included. The CREF assumes a good foundation of cyber security and continuity of operations (COOP).

Cyber resiliency techniques (described in more detail in a later section) are ways to achieve one or more cyber resiliency objectives. The CREF assumes that techniques will be *selectively* applied to the architecture or design of mission/business functions and their supporting cyber resources. Since natural synergies and conflicts arise between various cyber resiliency techniques, engineering trade-offs must be made. The remaining sections of this paper provide information to support the engineering analysis.

2 Cyber Resiliency Techniques: Potential Interactions

The fourteen cyber resiliency techniques identified in the Cyber Resiliency Engineering Framework must not be considered in isolation. As shown in the table below, a given implementation of a technique can support, use, depend on, or conflict with implementations of other techniques.

Technique A	Technique B	Adaptive Response	Analytic Monitoring	Coordinated Defense	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation / Isolation	Substantiated Integrity	Unpredictability
Adaptive Response	-	D	U, S		U	U, S	U	U, S	U, S		U	U, S	U	U	
Analytic Monitoring	S	-	D, S	U	U	U	S							U	
Coordinated Defense	U	U, D, S	-	U	U					U, S		U	U		
Deception		U, S, C	S, C	-									U	S	U
Diversity	S	C, S	C, S		-	S	C			C	S	U, S			S
Dynamic Positioning	S	C, S		S	U	-		U							U, S
Dynamic Representation	S	U	S				-				S			U	
Non-Persistence	U, S	C				S	C	-							S
Privilege Restriction	S		S							-	S			U	
Realignment			U		U		U			U	-		U		
Redundancy					D, S							-		U	
Segmentation / Isolation	U, S		S	S							S		-	U	
Substantiated Integrity	S	S	S							S		S		-	
Unpredictability	C, S	C	C	S	U	U, S		U							-

Key:

- S indicates that the technique in the row (Technique A) supports the one in the column (Technique B). Technique B is made more effective by Technique A.
- D indicates that Technique A depends on Technique B. Technique B will be ineffective if not used in conjunction with Technique A.
- U indicates that Technique A can make use of Technique B. Technique A can be implemented effectively in the absence of Technique B; however, more options become available if Technique B is also used.
- C indicates that Technique A can conflict with or complicate Technique B. Some or all implementations of Technique A could undermine the effectiveness of Technique B.

3 Effects on Adversary Activities

The implementation of a technique can impact adversary activities. To provide coverage of the entire cyber attack lifecycle or to ensure a variety of effects on the adversary, some combination of cyber resiliency techniques will be needed. The following table identifies possible effects of applying cyber resiliency techniques on adversary activities at different stages in the cyber attack lifecycle. Effects in

Cyber Resiliency Engineering Aid

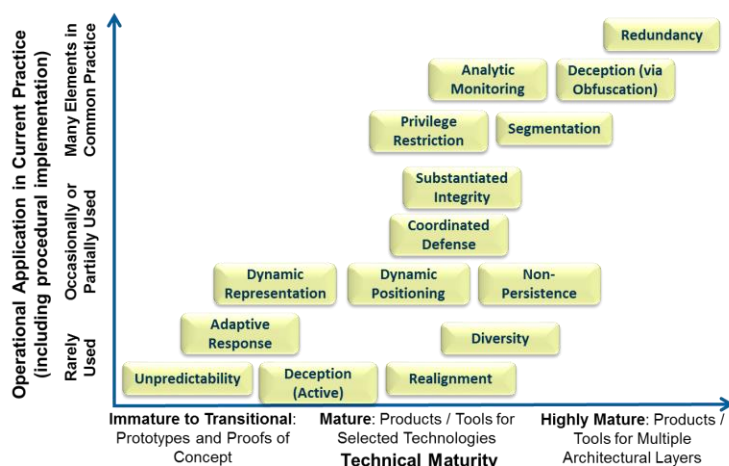
italics are second-order rather than primary effects, and are typically associated with a few approaches to implementing the technique.

Cyber Resiliency Technique	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Adaptive Response	Contain Curtail	<i>Impede</i>	Curtail	Prevent Recover	Contain Curtail	Curtail Impede Recover	Contain Curtail
Analytic Monitoring	Detect Analyze		<i>Prevent</i>	Detect Analyze	Detect Analyze	Detect Analyze	Detect Analyze
Coordinated Defense		Delay		Impede	Detect Impede		Detect Impede
Deception	Prevent Impede Divert Deceive Detect Analyze	Deter Impede Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Detect Analyze	Deter Divert Deceive Degrade Detect Analyze	Deter Deceive Detect Analyze
Diversity	Impede	Impede	<i>Prevent</i> Contain	Degrade Prevent	Degrade Contain Recover	Recover	Degrade Contain Recover
Dynamic Positioning	Divert Detect Curtail		Prevent Divert		Detect Impede Curtail Expunge Recover	Detect Impede Curtail Expunge Recover	Detect Impede Curtail Expunge Recover
Dynamic Representation	<i>Obviate</i> Analyze				<i>Obviate</i> Detect Analyze <i>Expunge</i>	Detect Analyze <i>Recover</i>	<i>Obviate</i> Analyze <i>Expunge</i>
Non-Persistence	Impede		Prevent	Curtail Expunge	Curtail Expunge	Curtail	Curtail Expunge
Privilege Restriction	Impede			Prevent Degrade Delay Contain	Prevent Degrade Delay Contain	Prevent Degrade Delay Contain	Prevent Degrade Delay Contain
Realignment	Impede	Prevent Impede	Impede	Prevent Impede	Prevent Impede	Prevent Impede	Prevent Impede
Redundancy						Degrade Curtail Recover	
Segmentation	Contain		Impede	Impede Contain	Impede Delay Contain <i>Detect</i>	Impede Delay Contain <i>Detect</i> Recover	Impede Delay Contain
Substantiated Integrity			Prevent Detect		Detect Curtail <i>Expunge</i>	Curtail Recover <i>Expunge</i>	Detect Curtail <i>Expunge</i>
Unpredictability	<i>Deter</i> Delay	Impede		Delay	Detect Delay	Delay Detect	Detect

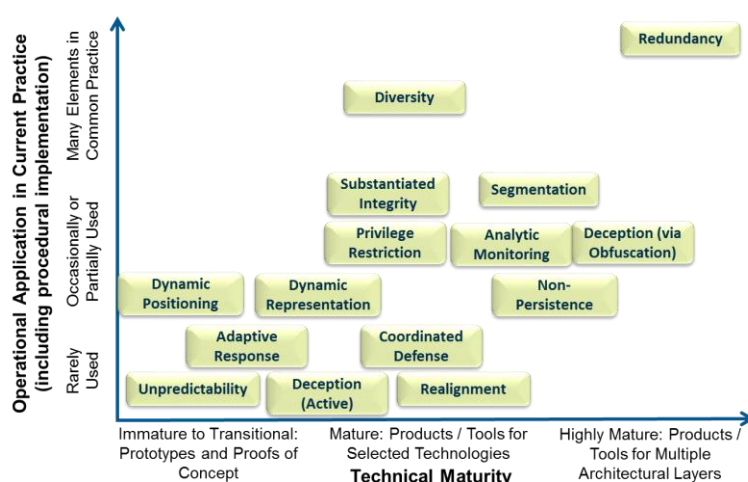
Cyber Resiliency Engineering Aid

4 Maturity

The cyber resiliency techniques (and the approaches to implementing each technique) vary in maturity and uptake (i.e., adoption as good practice). Maturity ultimately translates into functionality being integrated into commercial off-the-shelf (COTS) products and into free and open source software (FOSS). As illustrated below, maturity and uptake can be identified for general-purpose enterprise computing (i.e., common uses of information and communications technology or ICT) and for cyber-physical systems (CPS). However, it must be emphasized that these are generalizations: the product landscape continues to change; operational practices vary widely depending on sector; and trends toward converged architectures, cloud computing, and the Internet of Things introduce new challenges that affect the usefulness of existing solutions and constrain the feasibility of emerging ones.



Technical Maturity for and Uptake in General-Purpose ICT Environments



Technical Maturity for and Uptake in CPS (Preliminary Assessment)

5 Details on Approaches, Interactions, and Effects

For each technique, a given implementation will use one or more identifiable approaches. The potential interactions among these approaches must be understood as representative – that is, the extent to which, for example, Dynamic Reconfiguration (DReconfig) depends on Monitoring and Damage Assessment (M&DA) will be determined by the specific DReconfig and M&DA implementations. The tables in this section provide more detail on such potential interactions among, and effects of the approaches to implementing the cyber resiliency techniques.

Similarly, the effects (as defined in the following table) of a given approach on adversary activities will depend on the specific implementation and on the specific adversary tactics, techniques, and procedures (TTPs). For example, some of the cyber resiliency implementation approaches affect adversary reconnaissance. However, those implementations will not affect recon performed outside the systems in which the techniques are implemented (e.g., social engineering activities in external social networks frequented by system users or administrators).

Defender Goal	Definition	Effect
Redirect (includes Deter, Divert, and Deceive)	<i>Direct adversary activities away from defender-chosen targets.</i>	<i>The adversary's efforts cease, or become mistargeted or misinformed.</i>
Deter	Discourage the adversary from undertaking further activities, by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).	The adversary ceases or suspends activities.
Divert	Lead the adversary to direct activities away from defender-chosen targets.	The adversary refocuses activities on different targets (e.g., other organizations, defender-chosen alternate targets). The adversary's efforts are wasted.
Deceive	Lead the adversary to believe false information about defended systems, missions, or organizations, or about defender capabilities or TTPs.	The adversary's perception of defenders or defended systems is false. The adversary's efforts are wasted.
Obviate (includes Prevent and Preempt)	<i>Render the adversary's efforts or intentions ineffective by ensuring that adversary efforts or resources cannot be used or will have no effects.</i>	<i>The adversary's efforts or resources cannot be applied or are wasted.</i>
Prevent	Make the adversary's activity ineffective.	The adversary's efforts are wasted, as no intended effects can be achieved.
Preempt	Ensure that the adversary cannot apply resources or perform activities.	The adversary's resources cannot be applied and/or the adversary cannot perform activities (e.g., because resources are destroyed or made inaccessible).
Impede (includes Degrade and Delay)	<i>Make the adversary work harder or longer to achieve intended effects.</i>	<i>The adversary achieves the intended effects, but only by investing more resources or undertaking additional activities.</i>

Defender Goal	Definition	Effect
Degrade	Decrease the effectiveness of an adversary activity, i.e., the level of impact achieved.	The adversary achieves some but not all of the intended effects, or achieves all intended effects but only after taking additional actions.
Delay	Increase the amount of time needed for an adversary activity to achieve its intended effects.	The adversary achieves the intended effects, but may not achieve them within the intended time period. (The adversary's activities may therefore be exposed to greater risk of detection and analysis.)
Detect	<i>Identify adversary activities or their effects by discovering or discerning the fact that an adversary activity is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.</i>	<i>The adversary's activities become susceptible to defensive responses.</i>
Limit (includes Contain, Curtail, Recover, & Expunge)	<i>Restrict the consequences of adversary efforts by limiting the damage or effects of adversary activities in terms of time, cyber resources, and/or mission impacts.</i>	<i>The adversary's effectiveness is limited.</i>
Contain	Restrict the effects of the adversary activity to a limited set of resources.	The value of the activity to the adversary, in terms of achieving the adversary's goals, is reduced.
Curtail	Limit the duration of an adversary activity.	The time period during which the adversary's activities have their intended effects is limited.
Recover	Roll back adversary gains, particularly with respect to mission impairment.	The adversary fails to retain mission impairment due to recovery of the capability to perform key mission operations.
Expunge	Remove adversary-directed malware, repair corrupted data, or damage an adversary-controlled resource so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.	The adversary loses a capability for some period of time.

6 What about ...?

One question often posed about the CREF is: "What about moving target?" The phrase "moving target defense" is often used to describe ways of changing the attack surface to make the adversary's job harder. That phrase is used to encompass two approaches, which are achieved in different ways. First, some moving target defenses actually move the target; in the CREF, these fall under Dynamic Positioning. Second, many moving target defenses involve changing configurations or swapping out components; these fall under Adaptive Response. While the CREF provides one way to structure discussion of the cyber resiliency space, others are equally viable. The CREF, by separating goals and objectives from techniques, reflects the assumption that the set of cyber resiliency techniques will

Cyber Resiliency Engineering Aid

change over time, as research in some of them fails to prove out, as others become standard cybersecurity or COOP practice, and as new research ideas emerge.

Another question that is frequently posed is: “Why isn’t virtualization a technique?” Virtualization refers to a largely mature and commonly used set of technologies used to create (and subsequently destroy) virtual platforms, operating system (OS) environments, or networks, which present themselves as separate to higher architectural layers while sharing resources at lower layers. Many of the approaches to implementing cyber resiliency techniques depend on or use virtualization technology. These include Adaptive Response, Deception, Dynamic Positioning, Realignment, and Segmentation / Isolation. However, virtualization *per se* is not intended to provide resilience against advanced cyber threats; separation is motivated by accountability (so that resource use can be charged) and limitation of the effects of errors.

Finally, a question that can be posed of this engineering aid is: “What about unpredictability?” While interactions between Unpredictability and other techniques are identified, a separate discussion of Unpredictability as a technique is not included below. Unpredictability techniques make changes, frequently and randomly, to make the attack surface unpredictable. These changes, which may use Diversity, Dynamic Positioning, and Non-Persistence, make it more difficult for an adversary to predict behavior, which can delay or impede adversary actions or increase the chance of adversary actions being detected. However, the interactions between Unpredictability and other techniques depend so strongly on how those techniques are implemented, and on operational considerations in the environment where they are used, that a general discussion of Unpredictability is unlikely to be useful.

Cyber Resiliency Engineering Aid

Adaptive Response: Respond dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, limit consequences, and avoid destabilization			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Dynamic Reconfiguration (DReconf): Make changes to an element or component while it continues operating.	Mature and widely used, primarily for system / network management. Research underway for CPS, focused on stability rather than cyber resilience.	Depends on Analytic Monitoring (M&DA, SF&A) Supports and uses Coordinated Defense (AM, CoAA) Uses Dynamic Positioning Uses Dynamic Representation (DM&P, MD&SV) Supports and uses Non-Persistence Supports and uses Privilege Restriction Supports and uses Segmentation / Isolation Uses Substantiated Integrity Uses Unpredictability	Recon: Curtail: The adversary's knowledge of resources and configuration becomes outdated. Contain: The resources against which the adversary can conduct recon are restricted. Weaponize: Impede: The adversary's development or acquisition of exploits is based on outdated or incorrect premises, making the exploits less effective. Deliver: Curtail: The adversary's delivery mechanism stops working. Exploit: Prevent: The adversary's exploit is based on outdated premises. Control, Maintain: Contain: The adversary's activities are limited to resources that have not been reconfigured. Curtail: Reconfiguration (e.g., changing internal communications or call paths) renders the adversary's activities ineffective. Execute: Prevent: Reconfiguration (e.g., blocking ports and protocols) renders ineffective the activities the adversary could take to achieve consequences. Delay: Reconfiguration requires the adversary to revise plans or take additional steps in order to achieve consequences.

Cyber Resiliency Engineering Aid

Adaptive Response (concluded): Respond dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, limit consequences, and avoid destabilization			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Dynamic Resource Allocation (DRA): Change the allocation of resources to tasks or functions without terminating functions or processes.	Mature and widely used, primarily for performance optimization.	Depends on Analytic Monitoring (M&DA, SF&A) Supports and uses Coordinated Defense (AM, CoAA) Uses Diversity (DDH) Supports and uses Dynamic Positioning (FR, DF) Uses Dynamic Representation (DM&P, MD&SV) Uses Redundancy (SC, Replication) Uses Unpredictability	Control, Execute, Maintain: Curtail: Resource reallocation removes resources from the adversary's control. Execute: Degrade: Resource reallocation enables mission continuity at some level, reducing the effectiveness of the adversary's goal of denying mission capabilities. Delay: The adversary must revise plans or take additional steps, due to changes in available resources. Recover: Resource reallocation enables recovery of mission functions when the adversary's goal is denial of service.
Dynamic Composability (DC): Replace software elements with equivalent functionality without disrupting service.	Immature at lower layers; mature and widely used for mobile applications. Research underway for CPS.	Depends on Analytic Monitoring (M&DA, SF&A) Uses Diversity (D-S) Uses Dynamic Representation (DM&P, MD&SV) Uses Unpredictability	Control, Execute, Maintain: Contain: The adversary's activities are limited to resources that conform to behavioral templates (e.g., interfaces, call sequences, implementation languages and libraries) that existed when the adversary began probing; thus, lateral movement is restricted.

Cyber Resiliency Engineering Aid

Analytic Monitoring: Continuously gather, fuse, and analyze threat intelligence data to identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Monitoring and Damage Assessment (MD&A): Behavior and characteristics of elements are monitored and analyzed to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.	Increasingly mature for indicators; mature and widely used for detection and damage assessment; immature in the context of recovery and evolution. Research underway for CPS.	Supports Adaptive Response Supports Analytic Monitoring (SF&A) Supports and depends on Coordinated Defense (AM; CC&A respectively) Uses Deception (Dis, Sim) to obtain data Uses Diversity (DDH for different sensors) Uses Dynamic Positioning (FR) for sensor relocation Supports Dynamic Representation (DM&P, MD&SV) Uses Substantiated Integrity (BV)	Recon, Deliver, Control, Maintain: Detect: Monitoring provides indications and warning (I&W) or attack sensing and warning (AS&W), making the adversary's activities visible to defenders. Damage assessment reveals the extent of the effects of adversary activities. Execute: Analyze: Damage assessment determines the extent of adversary effects on capabilities and data.
Sensor Fusion and Analysis (SF&A): Monitoring data and preliminary analysis results from different elements are fused and analyzed, together with externally provided threat intelligence, to look for indicators of adversary activity that span elements; to identify attack trends; and (in conjunction with Malware and Forensic Analysis) to develop threat intelligence.	Increasingly mature for ICT; widely used within the enterprise and by CND service providers; SF&A beyond the enterprise face policy and data quality challenges, while SF&A for CPS is an area of active research.	Supports Adaptive Response Supports and depends on Coordinated Defense (AM; CC&A respectively) Uses Deception (Dis, Sim) to obtain data Uses Diversity (InfoD) Uses Dynamic Positioning (DF) Supports Dynamic Representation (DM&P, MD&SV)	Recon, Control, Maintain: Detect: Sensor fusion enables enhanced I&W or AS&W, making the adversary's activities visible to defenders. Analyze: Sensor fusion enables more complete and comprehensive analysis of adversary activities.

Cyber Resiliency Engineering Aid

Analytic Monitoring (concluded): Continuously gather, fuse, and analyze threat intelligence data to identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage

Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Malware and Forensic Analysis (M&FA): Malware and other artifacts left behind by adversary activities are analyzed to develop observables, indicators, and adversary tactics, techniques, and procedures (TTPs).	Mature for widely used technologies (particularly at the network and OS layers); immature for cyber-physical components (considerable research related to Smart Grid).	Supports Adaptive Response Supports and depends on Coordinated Defense (AM; CC&A respectively) Uses Deception (Dis, Sim) to obtain data Uses Diversity (DDH for different malware analysis tools)	Deliver: Prevent: The use of a detonation chamber for suspected malicious emails or attachments can prevent delivery. Deliver, Exploit, Control, Maintain: Analyze: The adversary's TTPs and capabilities are better understood.

Cyber Resiliency Engineering Aid

Coordinated Defense: Coordinate multiple, distinct mechanisms (defense-in-depth) to protect critical resources across subsystems, boundaries, layers, systems, and organizations			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Technical Defense-in-Depth (DiD): Make use of multiple protective mechanisms, applied at different architectural layers or locations.	Mature for widely used technologies; immature for CPS.	Supports Analytic Monitoring (M&DA, SF&A) to ensure coverage Uses Deception Uses Diversity Uses Redundancy (SC, Replication) Uses Segmentation / Isolation	Weaponize: Delay: The adversary must develop or acquire exploits effective against multiple defensive technologies to be successful. Exploit: Impede: The adversary must use multiple exploits to obtain a foothold.
Coordination and Consistency Analysis (CC&A): Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent, and non-disruptive way.	Transitional-to-Mature, depending on governance and interoperability; immature for CPS.	Supports Analytic Monitoring (M&DA, SF&A) to ensure coverage Supports Coordinated Defense (DiD) Supports and uses Privilege Restriction Uses Substantiated Integrity (BV)	Control, Maintain: Detect: Inconsistencies (e.g., in configurations or in privilege assignments) provide indications of adversary activities.
Adaptive Management (AM): Change how defensive mechanisms are used based on changes in the operational environment as well as changes in the threat environment.	Transitional, but uptake largely depends on governance and interoperability; highly immature for CPS.	Uses Adaptive Response (DReconfig, DRA) Depends on Analytic Monitoring	Control, Maintain: Impede: The adversary must adapt to changing processes.
CoA Analysis (CoAA): Maintain a set of alternative CoAs, with supporting analysis of resource requirements, contingencies for meeting those requirements, and effects of CoAs on current and future mission capabilities.	Transitional-to-Mature, depending on governance and interoperability; immature for CPS.	Uses Analytic Monitoring Uses Dynamic Representation [Uses all other techniques as components of CoAs]	Recon, Control, Execute, Maintain: The effects are indirect; by defining adequately-resourced CoAs, cyber defenders can identify intended effects and select CoAs to achieve those effects.

Cyber Resiliency Engineering Aid

Deception: Establish a scope of deception (internal systems, supply chain, DMZ, etc.); confuse, deceive, and mislead the adversary			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Obfuscation: Hide, transform, or otherwise obfuscate information from the adversary.	Mature and widely used, particularly in the form of encryption.	Conflicts with Analytic Monitoring (M&DA) Supports Substantiated Integrity (IQC, PT) by making adversary fabrication or modification harder	Recon: Prevent: The adversary cannot make the observations needed to inform further activities. Impede: The adversary must perform additional analysis to determine or acquire the utility of repackaged data (e.g., configuration files). Execute: Degrade: The adversary cannot reliably determine which targets are valuable, and hence must either try to affect more targets (e.g., exfiltrate more files, bring down more VMs) than necessary to achieve objectives, or accept more uncertainty as to effectiveness. <i>or</i> The adversary cannot make as effective use of target data (e.g., the adversary must make additional transformations, possibly with data loss).
Dissimulation/Disinformation (Dis): Provide deliberately confusing responses to adversary requests.	Immature, and must be tied to an OPSEC strategy.	Supports Analytic Monitoring (M&DA) Supports Dynamic Representation (DTM) Uses Unpredictability	Recon: Deter: The adversary is convinced that the target is not worth pursuing. Recon, Control, Execute, Maintain: Detect: The adversary's use of fabricated control data (e.g., configuration, network topology, or asset inventory data) serves as an indicator of adversary activity. Deceive: The adversary's knowledge about mission or defender activities is incomplete or (if defenders place false information on C3 paths to which the adversary has access) false. Recon, Execute: Detect: Attempts to access fabricated targets provides an indication of adversary activities. Divert: The adversary directs efforts at fabricated targets (e.g., fabricated mission, configuration, or topology data). Weaponize: Deceive: The adversary's efforts are based on false information (e.g., configuration data) and thus are wasted. Impede: The adversary must develop or acquire exploits effective against multiple technologies. Analyze: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting. All phases post-Recon: Deter: Adversary reconnaissance falsely indicates that the expected value of carrying out a cyber attack does not justify the expected costs or risks.

Cyber Resiliency Engineering Aid

Deception (concluded): Establish a scope of deception (internal systems, supply chain, DMZ, etc.); confuse, deceive, and mislead the adversary			
Implementation Approach	Maturity/ Uptake	Potential Interactions	Potential Effects on Adversary Activities
Misdirection/ Simulation (Sim): Maintain deception resources or environments and direct adversary activities there.	Mature, with wide variations in operational use. Immature at best for CPS.	Supports and uses Analytic Monitoring (MD&A) Supports and conflicts with Coordinated Defense (informs AM; increases complexity of CoAA) Supports Dynamic Representation (DTM) Uses Segmentation / Isolation (PS) to maintain deception sub-networks Uses Unpredictability	<p>Recon:</p> <p>Deter: The adversary is convinced that the target is not worth pursuing.</p> <p>Divert: The adversary is directed to false targets; the adversary's efforts are wasted.</p> <p>Deceive: The adversary develops false intelligence about the defender's cyber resources, mission / business function dependencies, or TTPs.</p> <p>Analyze: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting.</p> <p>Weaponize:</p> <p>Deter: The adversary is daunted by the technical complexity of the system for which exploits must be developed, and seeks an easier target elsewhere.</p> <p>Deceive: The adversary develops or acquires exploits compatible with the deception environment rather than the operational environment; the adversary's efforts are wasted.</p> <p>Exploit:</p> <p>Deceive: The adversary's exploits falsely appear to succeed and grant access to targets; the adversary's efforts are wasted.</p> <p>Analyze: Analysis of the adversary's exploits increases understanding of adversary TTPs and capabilities.</p> <p>Deliver, Control, Execute, Maintain:</p> <p>Deter: The adversary determines that the potential consequences or the required effort of achieving effects is not worth the potential benefits.</p> <p>Divert: The adversary's efforts are wasted on false targets.</p> <p>Deceive: The adversary develops a false understanding of the operational environment and of the effects achieved, leading to wasted efforts.</p> <p>Analyze: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting.</p>

Cyber Resiliency Engineering Aid

Diversity: Use heterogeneous technologies, data sources, processing locations, and communication paths to minimize common mode failures (including attacks exploiting common vulnerabilities)			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Architectural Diversity/ Heterogeneity (ADH): Use multiple sets of technical standards, different technologies, and different architectural patterns.	Maturity varies depending on technology, with wide variations in intentional operational use. Limited but high-value use for CPS.	Supports Adaptive Response (DRA) Supports and conflicts with Analytic Monitoring (multiple sensor architectures support M&DA, but make SF&A harder; multiple technologies make M&FA harder) Supports and conflicts with Coordinated Defense (improves options for DiD, but makes CC&A, AM, and CoAA harder) Conflicts with Dynamic Representation (makes DM&P harder) Supports Redundancy (makes Replication much more effective) Uses Unpredictability	Weaponize: Impede: The adversary must develop or acquire exploits effective against variant implementations. Exploit: Prevent: The adversary's exploits will not work against variant implementations. Degrade: The adversary's exploits will work only against a subset of the variant implementations. Control, Maintain: Degrade: The adversary must control a set of compromised resources with different characteristics (requiring greater expertise and effort). Contain: The adversary is limited to controlling compromised resources about which they have expertise and for which they have control tools. Execute: Recover: Recovery from the mission effects of adversary activities can create opportunities for further adversary activities. Secure recovery is facilitated by using components against which the adversary does not have exploits or control tools.
Design Diversity/ Heterogeneity (DDH): Use different designs to meet the same requirements or provide equivalent functionality.	Mature but rarely used, due to costs. Limited but high-value use for CPS.	Supports Adaptive Response (DRA) Supports and conflicts with Analytic Monitoring as above Supports and conflicts with Coordinated Defense as above Conflicts with Dynamic Representation Supports Redundancy (Replication)	Weaponize, Exploit, Control, Execute, Maintain: Same as for Architectural Diversity / Heterogeneity.

Cyber Resiliency Engineering Aid

Diversity (concluded): Use heterogeneous technologies, data sources, processing locations, and communication paths to minimize common mode failures (including attacks exploiting common vulnerabilities)			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Dynamic or Synthetic Diversity (D-S): Transform implementations so that for no specific instance is the implementation completely predictable.	Mature for a few software components, but immature for most.	Supports Adaptive Response (DC) Supports Redundancy (Replication)	Weaponize, Exploit, Control, Execute, Maintain: Same as for Architectural Diversity / Heterogeneity.
Information Diversity (InfoD): Provide information from different sources or transform information in different ways.	Maturity and operational use vary, depending on technology and mission / business process. Immature at best for CPS.	Supports Adaptive Response (DReconf) Conflicts with Analytic Monitoring (M&DA) Conflicts with Dynamic Representation Supports Redundancy (Replication)	Control, Execute, Maintain: Degrade: The adversary must modify or replace multiple different versions of information in order to corrupt mission or system information without detection. Recover: Reconstruction of mission or system information is facilitated by having multiple sources.
Command, Control, and Communications (C3) Path Diversity: Provide multiple paths, with demonstrable degrees of independence, for information to flow between elements.	Technically and operationally challenging to determine degrees of independence, particularly in federated or cloud environments. Mature for many CPS, but degrading due to trends toward convergence.	Supports Adaptive Response (DReconf) Conflicts with Analytic Monitoring (M&DA) Supports Coordinated Defense (DiD) Supports Dynamic Positioning (DF) Conflicts with Dynamic Representation Supports Redundancy (Replication)	Control, Execute, Maintain: Recover: Recovery from the mission effects of adversary activities is facilitated by the use of C3 paths to which the adversary lacks access (e.g., out-of-band communications among defenders).

Cyber Resiliency Engineering Aid

Supply Chain Diversity (SCD): Use multiple, demonstrably independent, supply chains for critical components.	Technically and operationally challenging to establish that supply chains are truly independent, particularly for COTS / FOSS. Mature for some CPS, but degrading due to trends toward COTS / FOSS.	Supports Coordinated Defense (DiD) Uses Realignment (Purposing)	Recon: Impede: The adversary must investigate multiple supply chains. Deliver: Impede: The adversary must compromise multiple supply chains, or accept that only a subset of target components will be compromised. Contain: The adversary's effects are limited to a subset of target components. Detect: Attempts to compromise multiple supply chains are easier to detect.
--	---	--	---

Dynamic Positioning: Distribute and dynamically relocate functionality and assets to ensure consistent protection			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Functional Relocation of Sensors (FRS): Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adversary activity, and to watch for adversary activities during recovery and evolution.	Immature-to-transitional for ICT; immature for CPS.	Supports Analytic Monitoring (M&DA) Uses Non-Persistence (NPS, NPC)	Recon, Control, Execute, Maintain: Detect: The adversary's ability to remain hidden, assuming a fixed monitoring infrastructure, is decreased.

Cyber Resiliency Engineering Aid

Functional Relocation of Cyber Assets (FRA): Change the location of assets that provide functionality (e.g., services, applications) or information (e.g., data stores), either by moving the assets or by transferring functional responsibility.	Mature in virtual environments, but for performance rather than cyber resilience. Immature for CPS.	Conflicts with Analytic Monitoring (M&DA) Supports Deception (Obfuscation, Sim) Uses Non-Persistence (NPS, NPC)	Recon, Control, Execute, Maintain: Curtail: The period in which adversary activities are effective against a given location or instance of an asset is limited. Deliver: Divert: The adversary's activity is diverted to a different target, as the intended target has moved. Prevent: The target asset has moved before the adversary's delivery mechanism can be used. Control, Execute, Maintain: Expunge: Compromised running software is deleted, if relocation involves re-instantiating software from a clean version. Recover: Mission capabilities are restored, and trust can also be restored when relocation involves re-instantiating software from a clean version.
Asset Mobility (AM): Physical assets (e.g., platforms or vehicles, mobile computing devices) are physically relocated.	Mature in limited set of operational environments, which include some CPS.	Conflicts with Analytic Monitoring (MD&A, SF&A) Supports Deception (Obfuscation) Uses Non-Persistence (NPC)	Recon, Control, Execute, Maintain: Curtail: The period in which adversary activities are effective against a given location or instance of an asset is limited.
Distributed Functionality (DF): Functionality (e.g., processing, storage, communications) is distributed across multiple elements.	Mature in many enterprise architectures. Immature for CPS.	Conflicts with Analytic Monitoring (MD&A, SF&A) Supports Deception (Obfuscation, Sim) Uses Diversity (C3)	Control, Execute, Maintain: Impede: The adversary must compromise more elements in order to deny or corrupt functionality. Recover: Mission functionality is available from a combination of elements.

Cyber Resiliency Engineering Aid

Dynamic Representation: Ensure existence of and then expand upon static representations of components, systems, services, and adversary actions to support mission situation awareness and response			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Dynamic Mapping and Profiling (DM&P): Maintain current information about resources, their status, and their connectivity.	Mature, but focused on performance.	Supports Adaptive Response Uses Analytic Monitoring (M&DA, SF&A) Supports Coordinated Defense (AM, CoAA) Uses Substantiated Integrity (BV)	Control, Maintain: Detect: Software and components that do not conform to policy requirements or that are behaving in unexpected ways are identified. Expunge: Discovered software or components that do not fit asset policy requirements can be removed.
Dynamic Threat Modeling (DTM): Maintain current information about threat activities and characteristics (e.g., observables, indicators, TTPs).	Immature-to-transitional. Highly immature for CPS.	Uses Analytic Monitoring (M&FA) Supports Coordinated Defense (AM, CoAA)	Recon, Control, Maintain: Obviate: Information about threat activities and characteristics enables selection of cyber courses of action to prevent the adversary from achieving (what the defender perceives as) their objectives or to take preemptive action. Analyze: Patterns and trends in adversary behavior are revealed.
Mission Dependency and Status Visualization (MD&SV): Maintain current information about mission dependencies on resources, and the status of those resources with respect to threats.	Existing methods mature but too manually intensive to provide current information; immature-to-transitional w.r.t. threat representation.	Supports Adaptive Response Uses Analytic Monitoring Supports Coordinated Defense (AM, CoAA) Supports Realignment (O/O, A/R)	Execute: Recover: Recovery of mission capabilities from adversary activities is facilitated by knowledge of which resources were or will be needed.

Non-Persistence: Retain information, services, and connectivity for a limited time, thereby reducing exposure to corruption, modification, or usurpation			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Non-Persistent Information (NPI): Information is refreshed to a known trusted state and deleted when no longer needed.	Mature for some technologies.	Supports Adaptive Response (DRA) Depends on Substantiated Integrity (IQC)	Execute: Curtail: The period during which the adversary can acquire mission or control information is limited, as the information is deleted when no longer needed.
Non-Persistent Services (NPS): Services are refreshed periodically and/or terminated after completion of a request.	Mature in some architectures (especially virtualized or cloud services).	Supports and uses Adaptive Response (DRA) Conflicts with Analytic Monitoring (M&DA) Supports Dynamic Positioning (FR, DF) Conflicts with Dynamic Representation (DM&P, MD&SV) Supports Unpredictability	Exploit: Curtail: The adversary's attempt to exploit a vulnerability is curtailed when the attacked service is terminated. Control, Execute, Maintain: Curtail: The period during which adversary activities are effective against a given instance of a service is limited. Exploit, Control, Maintain: Expunge: Compromised services are terminated when no longer needed; if re-instantiated from a clean version, new instances will not be compromised.
Non-Persistent Connectivity (NPC): Connections are terminated after completion of a request or after a period of non-use.	Mature for some technologies; for others, designed-away.	Supports and uses Adaptive Response (DRA) Conflicts with Analytic Monitoring (M&DA) Supports Dynamic Positioning Conflicts with Dynamic Representation (DM&P, MD&SV) Supports Unpredictability	Recon: Impede: The adversary must re-establish connections in order to complete reconnaissance. Deliver: Prevent: A connection is terminated before the adversary can take advantage of it to deliver malware. Control, Execute, Maintain: Curtail: The period during which the adversary can make use of a C3 channel is limited.

Privilege Restriction: Design to restrict privileges assigned to users and cyber entities, and to set privilege requirements on resources based on criticality			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Privilege Management (PM): Define, assign, and maintain privileges associated with end users and cyber entities (e.g., systems, services, devices), based on established trust criteria, consistent with principles of least privilege.	Mature but often poorly applied or designed-away. Immature or designed-away for many CPS.	Supports Adaptive Response (DReconfig, DRA based on trust criteria) Supports and uses Coordinated Defense (CC&A) Supports Realignment (Purposing, O/O)	Recon: Impede: The adversary must invest more time and effort in obtaining credentials. Exploit, Control, Execute, Maintain: Contain: Privilege-based restrictions limit the adversary's activities to resources for which the false credentials the adversary has obtained allow use. Delay: The adversary's lack of credentials delays access to restricted resources. Prevent: The adversary's lack of credential prevents access to restricted resources.
Privilege-Based Usage Restrictions (PUR): Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes (e.g., data sensitivity).	Mature but often poorly applied or designed-away. Immature or designed-away for many CPS.	Supports Adaptive Response (DReconfig, DRA based on usage restrictions) Supports and uses Coordinated Defense (CC&A, CoAA) Supports Realignment (Purposing, O/O)	Exploit, Control, Execute, Maintain: Prevent: Privilege-based usage restrictions prevent the adversary from accessing critical or sensitive resources. Contain: Privilege-based usage restrictions limit the adversary's activities to non-critical resources, or to resources for which the false credentials the adversary has obtained allow use. Degrade: The adversary's lack of credentials delays access to restricted resources or requires the adversary to invest more effort to circumvent access controls.
Dynamic Privileges: Elevate or deprecate privileges assigned to a user, process, or service based on transient or contextual factors (e.g., using RAdAC)	Mature for some ICT environments. Immature or designed-away for many CPS.	Supports Adaptive Response (DReconfig, DRA based on usage restrictions) Supports and uses Coordinated Defense (CC&A, CoAA) Supports Realignment (A/R)Exp,	Exploit, Control, Execute, Maintain: Delay: The adversary must obtain additional privileges in order to perform activities.

Cyber Resiliency Engineering Aid

Realignment: Analyze mission processes to identify non-essential resources for offloading to reduce the attack surface, the potential for unintended consequences, and the potential for cascading failures

Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Purposing: The mission purposes of functions, services (including connectivity as well as processing), information, and systems are identified, to prevent uses that increase risk without any corresponding mission benefit.	Mature but often not applied; runs counter to trends toward cloud and converged architectures.	Uses Dynamic Representation (DM&P, MD&SV) Supports Diversity (SCD)	Deliver, Exploit: Impede: The adversary cannot take advantage of unnecessarily risky uses of resources (e.g., exposure of services to the Internet without offsetting mission benefits).
Offloading/Outsourcing (O/O): Supportive but non-essential functions are offloaded to a service provider that is better able to support the functions.	Mature but often poorly applied; outsourcing more commonly driven by economics, with security implications poorly considered.	Uses Dynamic Representation (DM&P, MD&SV) Uses Privilege Restriction	Deliver, Exploit: Impede: The set of opportunities the adversary can take advantage of is reduced.
Agility/Repurposing (A/R): System elements are repurposed to provide services, information, and connectivity to meet new or changing mission needs.	Transitional-to-mature, but often applied without sufficient security analysis.	Uses Coordinated Defense (CC&A) Uses Diversity (ADH, DDH) Uses Dynamic Representation (DM&P, MD&SV) Uses Privilege Restriction	Recon, Control, Maintain: Impede: The adversary must invest additional resources to maintain a current visualization of system elements.
Customization: Critical components are custom-developed or re-implemented.	Mature but often not applied; runs counter to reliance on COTS / FOSS. Mature but decreasingly common for some CPS.	Conflicts with Analytic Monitoring (M&DA) Supports and conflicts with Coordinated Defense (DiD; CC&A) Supports Diversity (ADH, DDH)	Weaponize: Prevent: The adversary lacks insight into critical customized components, and thus cannot develop exploits. Impede: The adversary must develop exploits against customized components.
Restriction: Risky functionality or connectivity is removed, or replaced with less-risky implementations.	Mature but often not applied; runs counter to reliance on COTS / FOSS.	Supports Coordinated Defense (DiD) Supports and conflicts with Privilege Restriction (PM, PUR)	Deliver, Control, Execute, Maintain: Prevent: The functionality or connectivity can no longer be used by the adversary. Impede: The set of opportunities the adversary can take advantage of is reduced.

Redundancy: Provide multiple protected instances of critical information and resources to reduce the consequences of loss			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Protected Backup and Restore (PB&R): Functionality is maintained to back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction.	Unprotected backup & restore is mature and widely used; integration of protections with basic B&R is technically mature but not widely used for ICT, immature for CPS.	Depends on and uses Diversity (ADH, DDH) Uses Substantiated Integrity (IQC, PT)	Execute: Curtail: The time during which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.
Surplus Capacity (SC): Extra capacity for information storage, processing, or communications is maintained.	Mature and widely used.	Depends on and uses Diversity (ADH, DDH)	Execute: Degrade: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.
Replication: Information and/or functionality is replicated (reproduced exactly) and kept synchronized in multiple locations.	Mature and widely used.	Depends on and uses Diversity (ADH, DDH) Uses Substantiated Integrity (IQC, PT)	Execute: Degrade: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.

Segmentation / Isolation: Define and separate (logically or physically) components on the basis of criticality and trustworthiness to limit the spread of damage			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Modularity / Layering: Define and implement services and capabilities in a modular way, and in a way that respects the differences between layers in a layered architecture, to enable separation, substitution, and privilege restriction based on criticality.	Mature and widely used in some environments; runs counter to trends toward reuse / wholesale inclusion of software in many design environments.	Supports Coordinated Defense (DiD) Supports Privilege Restriction (PBUR)	<p>Deliver:</p> <p>Delay: The adversary must sequentially penetrate defenses at multiple layers or in multiple modular components.</p> <p>Exploit, Control, Execute, Maintain:</p> <p>Impede: The adversary must do additional work (e.g., obtain additional privileges) to gain access to protected regions (e.g., in a ring architecture).</p>
Predefined Segmentation (PS): 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.	Mature and widely used in some environments; runs counter to trends toward cloud and converged architectures.	Supports Coordinated Defense (DiD) Supports Deception (Sim) Supports Privilege Restriction (PBUR)	<p>Recon, Control, Execute, Maintain:</p> <p>Contain: The adversary's activities (e.g., perform network mapping, propagate malware, exfiltrate data or bring down servers) is restricted to the enclave on which the adversary has established a presence.</p> <p>Deliver:</p> <p>Degrade: The number of possible targets to which malware can easily be propagated is limited to the network segment.</p> <p>Control, Execute:</p> <p>Detect: Adversary activities involving C3 across network segments that violate policies enforced at barriers between segments are detected.</p> <p>Control, Execute, Maintain:</p> <p>Delay: The adversary's ability to perform C3 is delayed, as the adversary must find ways to overcome barriers between network segments.</p>

Cyber Resiliency Engineering Aid

Segmentation / Isolation (concluded): Define and separate (logically or physically) components on the basis of criticality and trustworthiness to limit the spread of damage			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Dynamic Segmentation / Isolation (DSI): Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption.	Mature and widely used in some environments; runs counter to trends toward cloud and converged architectures.	Supports and uses Adaptive Response (DReconfig) Supports Coordinated Defense (CoAA) Supports Deception (Sim) Supports Privilege Restriction (PBUR)	Recon, Exploit, Control, Execute, Maintain: Contain: The adversary's activities (e.g., observe characteristics of running processes, insert malware into running process, control compromised process, use compromised process to achieve mission objectives, maintain covert presence in running process) are limited to the set of processes or services within a segment (e.g., with a specific set of characteristics or context). Execute: Recover: A protected environment is provided, in which mission-essential capabilities can be reconstituted.

Cyber Resiliency Engineering Aid

Substantiated Integrity: Provide mechanisms to ascertain whether critical services, information stores, information streams, and components have been corrupted			
Implementation Approach	Maturity/Uptake	Potential Interactions	Potential Effects on Adversary Activities
Integrity/Quality Checks (IQC): Apply and validate checks of the integrity or quality of information or devices.	Mature and widely used for many technologies; immature for emerging technologies. Mature and widely used, from data quality perspective, in CPS.	Supports Adaptive Response (DReconfig) Supports Privilege Restriction Supports Redundancy (PB&R, Replication)	Deliver: Prevent: Malware payloads the adversary tries to deliver (e.g., counterfeit software updates, email attachments) or embed in apparently harmless objects (e.g., documents) are discarded or quarantined before the malware can exploit a vulnerability. Detect: The attempted delivery of malware payloads is detected. Execute: Recover: Contaminated data is removed, restoring mission or control data to a known good state. Control, Maintain: Detect: The presence of contaminated data or compromised software that the adversary seeks to maintain is detected. Expunge: Software or data that does not meet integrity requirements is removed, thus removing or reducing the adversary's foothold.
Provenance Tracking (PT): Identify and track the provenance of data, software, and/or hardware elements.	Maturity varies depending on architectural layer and technology; uptake lags maturity.	Supports Adaptive Response (DReconfig, DC) Supports Privilege Restriction Supports Redundancy (PB&R, Replication)	Deliver: Detect: The adversary's attempts to deliver compromised data, software, or hardware are detected. Execute: Expunge: Compromised elements are identified so they can be removed.
Behavior Validation (BV): Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).	Maturity varies depending on technology; uptake lags maturity. Mature and widely used for many CPS components, from quality / dependability rather than cyber resiliency perspective.	Supports Analytic Monitoring (M&DA) Supports Coordinated Defense (CC&A)	Control, Execute, Maintain: Detect: The presence of adversary-controlled processes is detected by peer cooperating processes. Curtail: Adversary-controlled processes are isolated or terminated by peer cooperating processes.