Cybersecurity Design Patterns

The Johns Hopkins Applied Physics Laboratory

Brooke Guare
Cyber Systems Engineer
Brooke.Guare@jhuapl.edu

Introduction

Background: In order to aid engineers in designing sufficiently cyber resilient systems, the Office of the Under Secretary of Defense for Research and Engineering (OUSD (R&E)) / Systems Security tasked the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to curate and develop design patterns.

Challenge: The majority of weapon systems have been designed to meet physical performance and functional requirements, as well as be resilient to a set of kinetic threats. However, there has not been as much attention paid to the resilience of the system to cyberspace threats.

Approach

Solution: Development of design patterns

- A *design pattern* is a general, reusable solution to commonly occurring problems within a given context in system design

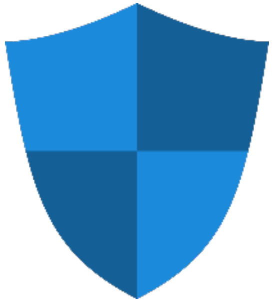
Impact: Compile design patterns proven successful or asserted to be useful, in order to:

- Allow engineers to identify gaps and mitigate potential cyber related problems in their system
- Provide building blocks for cyber resilient system design
- Provide engineers the tools and knowledge they need to build resilient systems and meet cybersecurity requirements
- Focus on usability to the community by providing searchability metadata

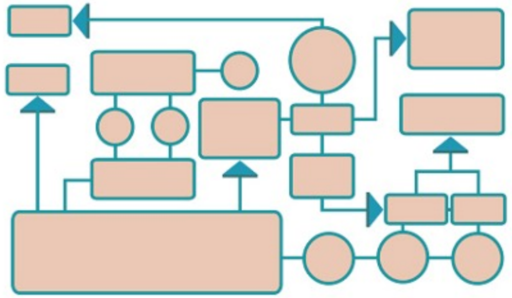
Cybersecurity-related Requirements

Design Patterns

+



Security Controls

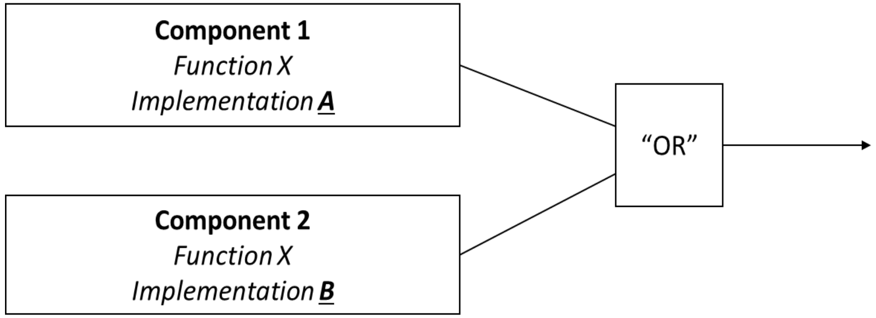


System Design

Resilient System

Case Study: Aircraft

Flight controls are electrically controlled

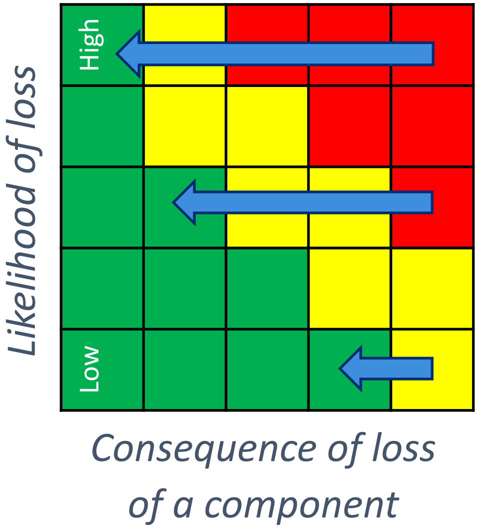


Threat:

- Loss of power to mission critical components

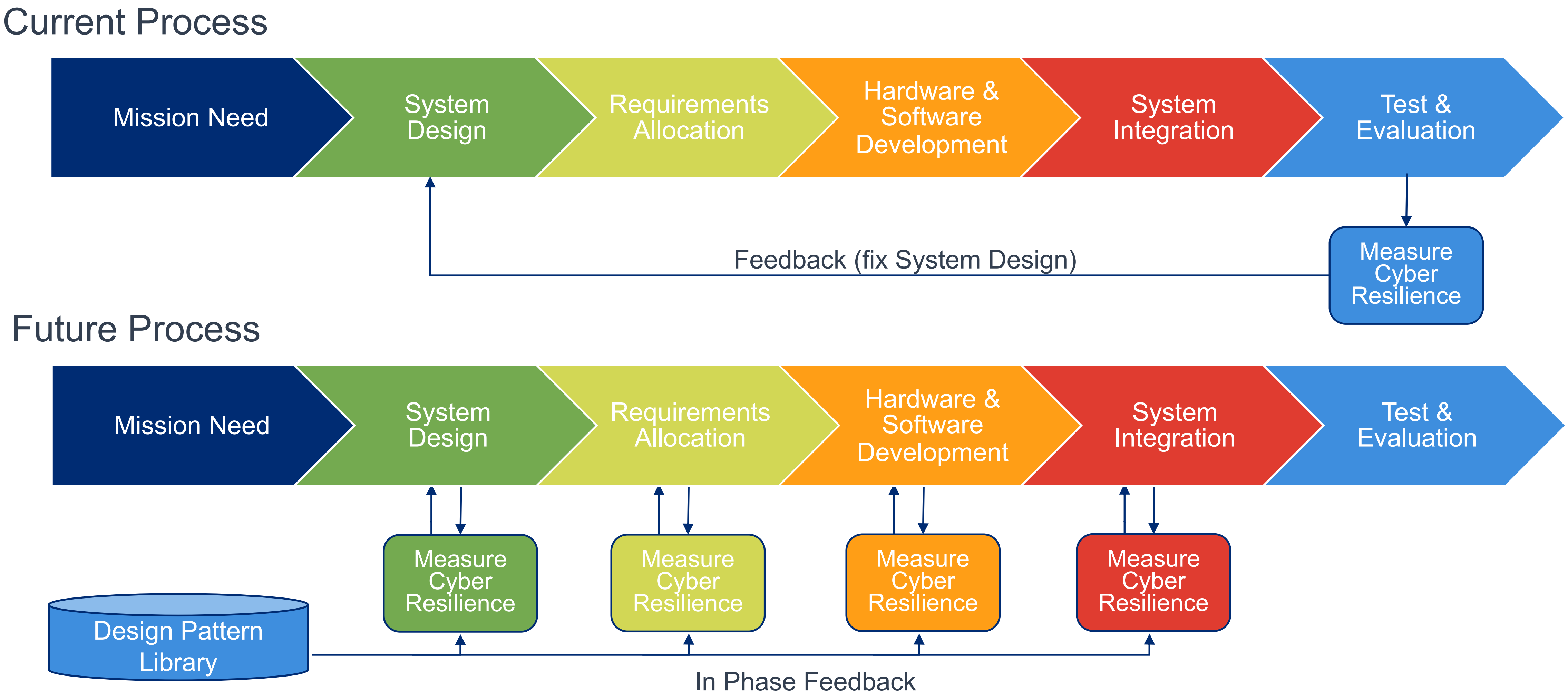
Application of Diverse Redundancy Design Pattern:

- Magnetic generator (primary source) allows power to be generated as long as engines are spinning
- 3 Electric Generators can power flight controls
- If electric backups fail, there is a battery backup

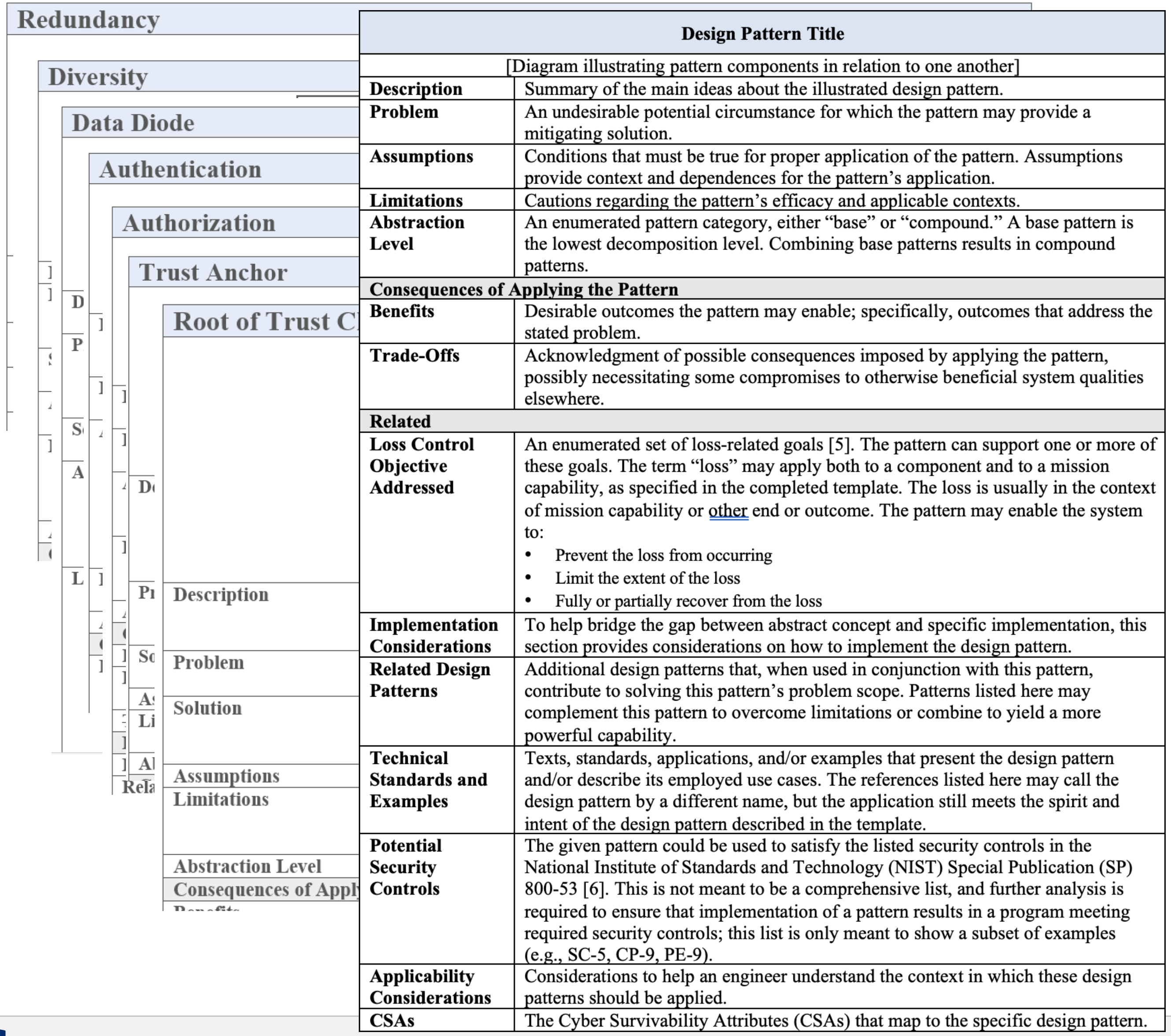


These mechanical examples can be translated to the cyber domain

Overall Landscape



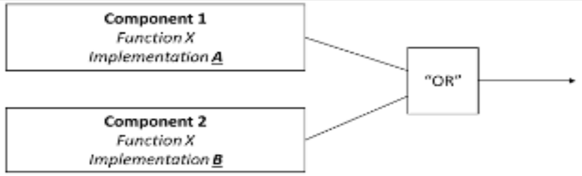
Design Pattern Template



Design Pattern Title	
[Diagram illustrating pattern components in relation to one another]	
Description	Summary of the main ideas about the illustrated design pattern.
Problem	An undesirable potential circumstance for which the pattern may provide a mitigating solution.
Assumptions	Conditions that must be true for proper application of the pattern. Assumptions provide context and dependences for the pattern's application.
Limitations	Cautions regarding the pattern's efficacy and applicable contexts.
Abstraction Level	An enumerated pattern category, either "base" or "compound." A base pattern is the lowest decomposition level. Combining base patterns results in compound patterns.
Consequences of Applying the Pattern	
Benefits	Desirable outcomes the pattern may enable; specifically, outcomes that address the stated problem.
Trade-Offs	Acknowledgment of possible consequences imposed by applying the pattern, possibly necessitating some compromises to otherwise beneficial system qualities elsewhere.
Related	
Loss Control Objective Addressed	An enumerated set of loss-related goals [5]. The pattern can support one or more of these goals. The term "loss" may apply both to a component and to a mission capability, as specified in the completed template. The loss is usually in the context of mission capability or other end or outcome. The pattern may enable the system to: • Prevent the loss from occurring • Limit the extent of the loss • Fully or partially recover from the loss
Implementation Considerations	To help bridge the gap between abstract concept and specific implementation, this section provides considerations on how to implement the design pattern.
Related Design Patterns	Additional design patterns that, when used in conjunction with this pattern, contribute to solving this pattern's problem scope. Patterns listed here may complement this pattern to overcome limitations or combine to yield a more powerful capability.
Technical Standards and Examples	Texts, standards, applications, and/or examples that present the design pattern and/or describe its employed use cases. The references listed here may call the design pattern by a different name, but the application still meets the spirit and intent of the design pattern described in the template.
Potential Security Controls	The given pattern could be used to satisfy the listed security controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [6]. This is not meant to be a comprehensive list, and further analysis is required to ensure that implementation of a pattern results in a program meeting required security controls; this list is only meant to show a subset of examples (e.g., SC-5, CP-9, PE-9).
Applicability Considerations	Considerations to help an engineer understand the context in which these design patterns should be applied.
CSAs	The Cyber Survivability Attributes (CSAs) that map to the specific design pattern.

Non-Exhaustive List

24 Design Patterns:		
Redundancy	Data Collection	Secure Logging
Diverse Redundancy	Analytics	Watch Dog
Data Diode	Alerts	Defer to Kernel
Segmentation	Response	Privilege Reduction
Authentication	Load from Known State	Single Access Point
Authorization	Data Flow Control	Triple Modular Hardware Redundancy with Replicate Voters
Trust Anchor	Data Input validation	Pair and a Spare (Active (Dynamic) Hardware Redundancy)
Watch Dog	Distributed Privileges	Watching the Watchdog

Diverse Redundancy	DRAFT					
						
Description	Two or more components provide redundant functionality, where only one component is absolutely necessary to deliver nominal system capability. The redundant components provide equivalent functionality, but differ in their implementations.					
Problem	If a system depends on a single component to perform a mission-critical function, and if that single component is compromised, the dependent mission-critical function is also lost. Further, if systems employ redundancy but use identical redundant components, common-mode failures (which possibly affect all components of a particular type) can thwart the intended benefits of redundancy.					
Assumptions	The likelihood of simultaneous loss of both components to the same adverse occurrence is acceptably low. Also, each individual component's reliability is acceptable. Separate teams or vendors have developed these components to ensure there is a sufficient amount of diversity between them.					
Limitations	The likelihood of loss of both components because of adverse conditions is inversely proportional to this pattern's efficacy. Despite attempts to introduce diversity between components, some form of commonality may be overlooked that makes them susceptible to the same exploit.					
Abstraction Level	Base (Tier 1)		Compound (Tier 2)	X	(Combines redundancy and diversity)	
Consequences of Applying the Pattern						
Benefits	Despite losing a single component, the system can continue providing critical mission functionality by relying on the diverse redundant component. In other words, a *component* loss does not necessarily result in a *mission function* loss. The likelihood that an identical vulnerability is exploited across separate diverse components is lower than if all components have the same implementation. Apart from cyber, redundancy may allow for increased performance, help handle load balances, etc.					
Trade-Offs	• Potentially increases material cost, space, weight, power, and system complexity, likely beyond that of a homogenously redundant system. Applying this pattern throughout the entire system is probably impractical. Vetting diverse components adds cost and may increase implementation and compatibility complexity. Implementing diversity across all system aspects (e.g., power, CPU architecture) is challenging; thus, one may be forced to prioritize to which aspects to apply diversity. • Diverse redundancy requires adding multiple training and maintenance pipelines.					
Related						
Loss Control Objective Addressed	Loss Prevention	X	Loss Limitation	X	Loss Recovery	X
	Losing a single critical component does not necessarily result in loss of mission function.		Even if losing a component initially results in degraded mission functionality, switching to the redundant component thereafter can limit the duration of the degradation.		The "OR" box is where the logic for the recovery is held, determining whether one component goes down, to then seamlessly fall back to the diverse redundant second component.	
Implementation Considerations	• Are the redundant components operating all the time, or operating in a failover capacity • For failover capabilities, what are the detection and response actions necessary to failover to one to another • What are the time constraints for implementing redundant solutions					
Related Design Patterns	• Segmentation: To reduce likelihood that the same attack that degrades one component also degrades the other. • Redundancy: To have duplicate components in the system for failover purposes. • Diversity: Diverse components limit the ability for a single vulnerability to propagate throughout the entire system.					
Technical Standards and Examples	• CSfC – DAR • Analog backups, manual workarounds					
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling					

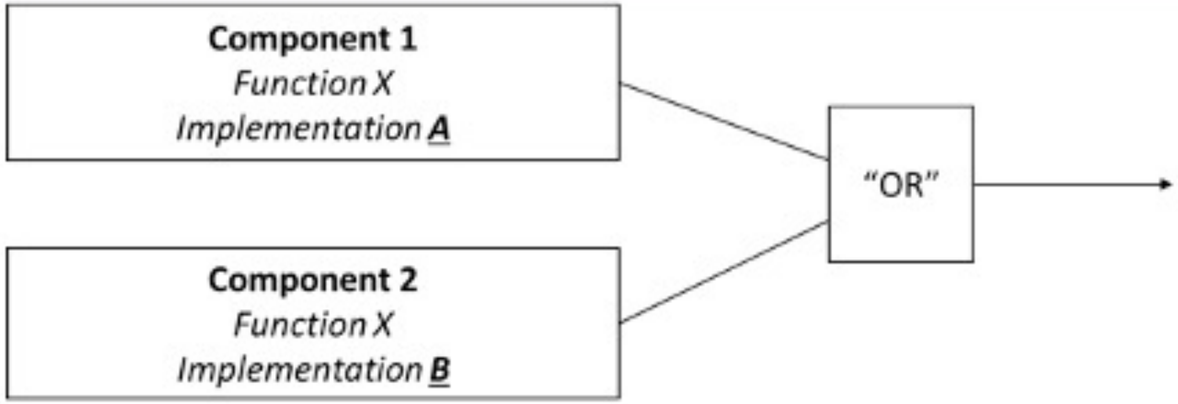
Subset of Design Patterns Developed:

- Redundancy
- Diverse Redundancy
- Data Diode
- Segmentation
- Authentication
- Authorization
- Trust Anchor
- Watch Dog
- Data Collection
- Analytics
- Alerts
- Response
- Load from Known State
- …. & More

Diverse Redundancy

DRAFT

Diverse Redundancy



Description	Two or more components provide redundant functionality, where only one component is absolutely necessary to deliver nominal system capability. The redundant components provide equivalent functionality, but differ in their implementations.				
Problem	If a system depends on a single component to perform a mission-critical function, and if that single component is compromised, the dependent mission-critical function is also lost. Further, if systems employ redundancy but use identical redundant components, common-mode failures (which possibly affect all components of a particular type) can thwart the intended benefits of redundancy.				
Assumptions	The likelihood of simultaneous loss of both components to the same adverse occurrence is acceptably low. Also, each individual component's reliability is acceptable. Separate teams or vendors have developed these components to ensure there is a sufficient amount of diversity between them.				
Limitations	The likelihood of loss of both components because of adverse conditions is inversely proportional to this pattern's efficacy. Despite attempts to introduce diversity between components, some form of commonality may be overlooked that makes them susceptible to the same exploit.				
Abstraction Level	Base (Tier 1)		Compound (Tier 2)	X	(Combines redundancy and diversity)

Description

Problem

Assumptions

Limitations

Abstraction Level

Consequences of Apply

Benefits

Trade-Offs

Related

Loss Control Objectives Addressed

Implementation Considerations

Related Design Patterns

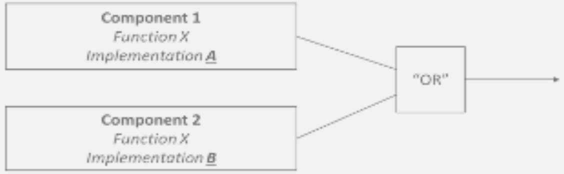
Technical Standards and Examples

Security Controls

- CP-9 Information System Backup
- PE-9 Power Equipment and Cabling | Redundant cabling

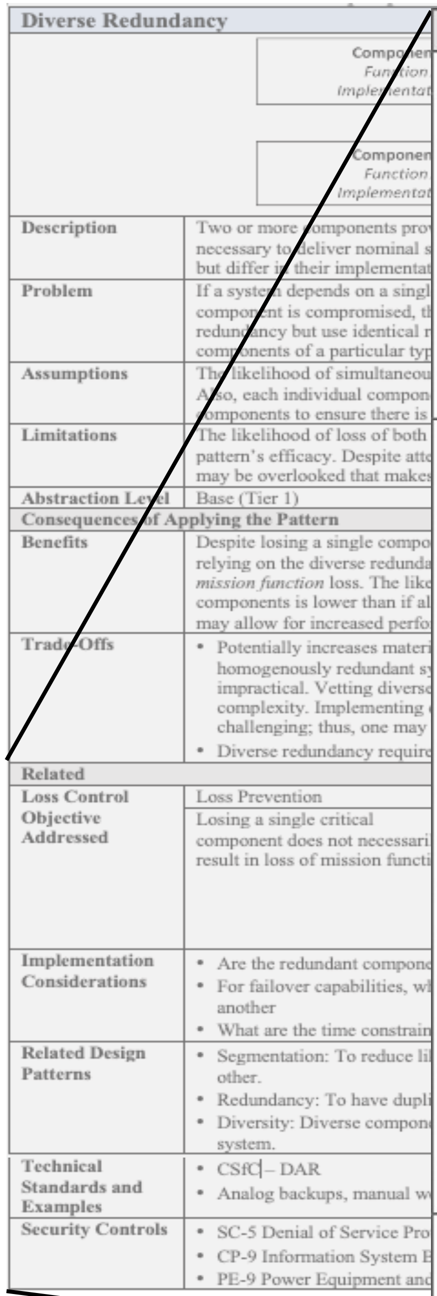
Diverse Redundancy

DRAFT



Description	Two or more components provide redundant functionality, where only one component is absolutely necessary to deliver nominal system capability. The redundant components provide equivalent functionality, but differ in their implementations.
Problem	If a system depends on a single component to perform a mission-critical function, and if that single component is compromised, the dependent mission-critical function is also lost. Further, if systems employ redundancy but use identical redundant components, common-mode failures (which possibly affect all components of a particular type) can thwart the intended benefits of redundancy.
Assumptions	The likelihood of simultaneous loss of both components to the same adverse occurrence is acceptably low. Also, each individual component's reliability is acceptable. Separate teams or vendors have developed these components to ensure there is a sufficient amount of diversity between them.
Limitations	The likelihood of loss of both components because of adverse conditions is inversely proportional to this pattern's efficacy. Despite attempts to introduce diversity between components, some form of commonality may be overlooked that makes them susceptible to the same exploit.
Abstraction L…	
Consequences…	
Benefits	
Trade-Offs	
Related Loss Control Objective Addressed	
Implementation Considerations	
Related Design Patterns	• Diversity: Diverse components limit the ability for a single vulnerability to propagate throughout the entire system.
Technical Standards and Examples	• CSfC – DAR • Analog backups, manual workarounds
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling

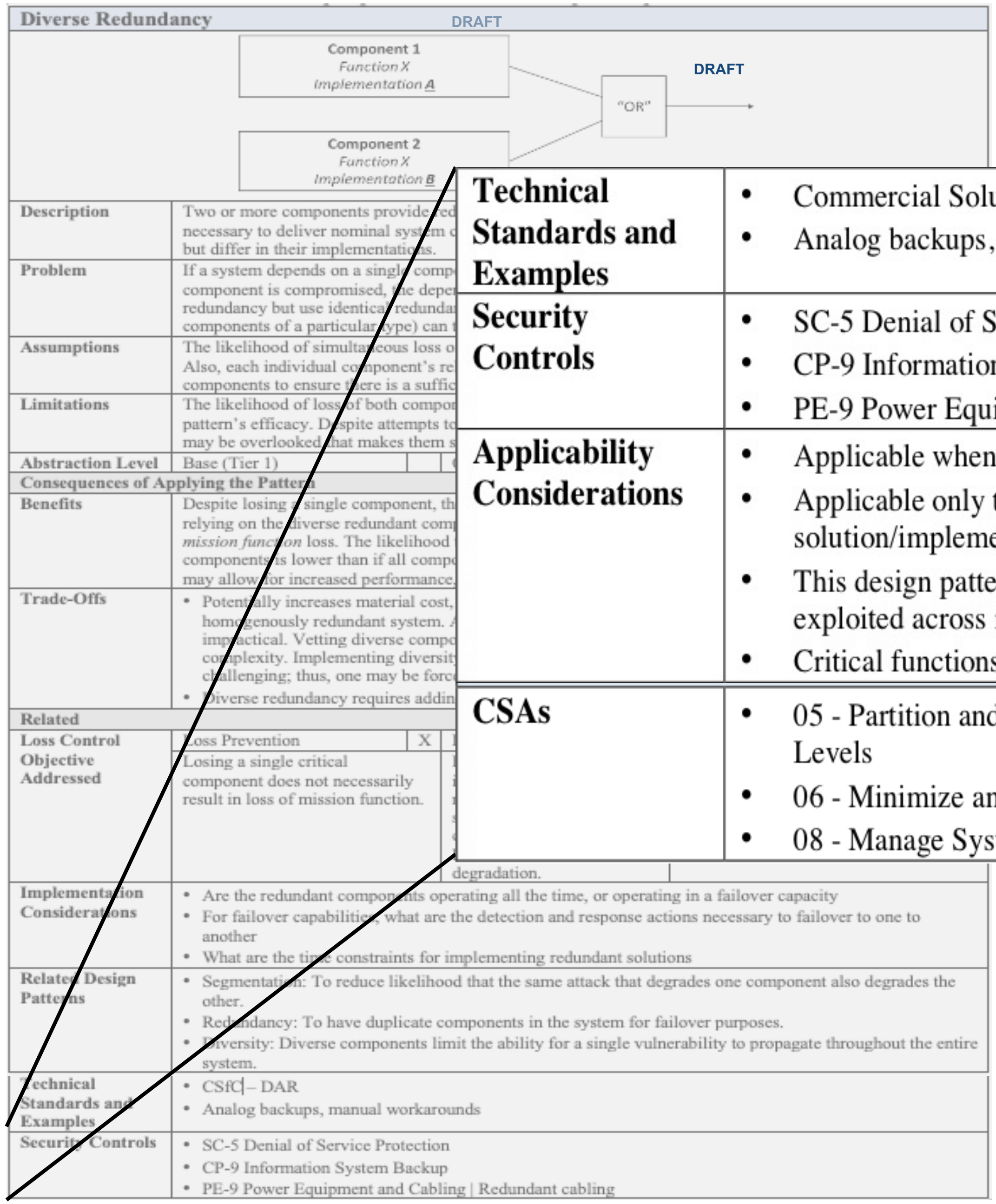
Consequences of Applying the Pattern	
Benefits	Despite losing a single component, the system can continue providing critical mission functionality by relying on the diverse redundant component. In other words, a *component* loss does not necessarily result in a *mission function* loss. The likelihood that an identical vulnerability is exploited across separate diverse components is lower than if all components have the same implementation. Apart from cyber, redundancy may allow for increased performance, help handle load balances, etc.
Trade-Offs	• Potentially increases material cost, space, weight, power, and system complexity, likely beyond that of a homogenously redundant system. Applying this pattern throughout the entire system is probably impractical. Vetting diverse components adds cost and may increase implementation and compatibility complexity. Implementing diversity across all system aspects (e.g., power, CPU architecture) is challenging; thus, one may be forced to prioritize to which aspects to apply diversity. • Diverse redundancy requires adding multiple training and maintenance pipelines.



Related						
Loss Control Objective Addressed	Loss Prevention	X	Loss Limitation	X	Loss Recovery	X
	Losing a single critical component does not necessarily result in loss of mission function.		Even if losing a component initially results in degraded mission functionality, switching to the redundant component thereafter can limit the duration of the degradation.		The "OR" box is where the logic for the recovery is held, determining whether one component goes down, to then seamlessly fall back to the diverse redundant second component.	

Implementation Considerations	• Redundant components should be implemented so that they are not susceptible to the anticipated threats. For example, redundant hydraulic lines run right next to one another would both be susceptible to one kinetic impact. In cyberspace, redundant components should use segmentation or other resilience techniques to ensure they both do not fail as a result of the same cyberspace attack.
	• How the redundant components operate is important.
	  • How quickly does one component need to perform the functions of a failed component?
	  • Are all redundant components on all the time or are redundant components operating in a failover capacity?
	  • If all components are on all the time and one component goes bad (via a failure or an integrity attack,) how does the system determine which component is correct?
	  • For failover capabilities, what are the detection and response actions necessary to failover from one component to another component?
	  • Is the failover mechanism automatic or manual?
	  • How will the system or the operator know when to switch from one redundant component to another?
	• Having multiple components with the same functionality comes with a funding tail. A training and maintenance pipeline must be established and maintained for each of the components.					

Related Design Patterns	• Segmentation • Redundancy • Diversity					



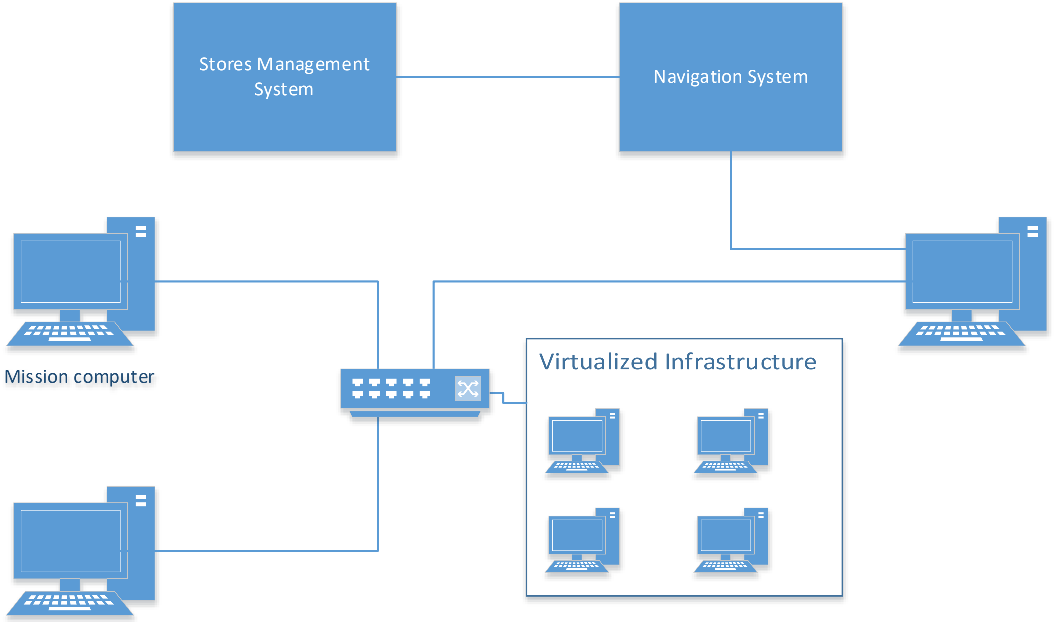
Diverse Redundancy	DRAFT
	Component 1 *Function X* *Implementation A* / Component 2 *Function X* *Implementation B* → "OR" (DRAFT)
Description	Two or more components provide red... necessary to deliver nominal system ... but differ in their implementations.
Problem	If a system depends on a single comp... component is compromised, the depe... redundancy but use identical redunda... components of a particular type) can ...
Assumptions	The likelihood of simultaneous loss o... Also, each individual component's re... components to ensure there is a suffic...
Limitations	The likelihood of loss of both compo... pattern's efficacy. Despite attempts to... may be overlooked that makes them s...
Abstraction Level	Base (Tier 1)
Consequences of Applying the Pattern	
Benefits	Despite losing a single component, th... relying on the diverse redundant comp... *mission function* loss. The likelihood ... components is lower than if all compo... may allow for increased performance...
Trade-Offs	• Potentially increases material cost, ... homogenously redundant system. ... impractical. Vetting diverse compo... complexity. Implementing diversit... challenging; thus, one may be force... • Diverse redundancy requires addin...
Related	
Loss Control Objective Addressed	Loss Prevention — X — Losing a single critical component does not necessarily result in loss of mission function. ... degradation.
Implementation Considerations	• Are the redundant components operating all the time, or operating in a failover capacity • For failover capabilities, what are the detection and response actions necessary to failover to one to another • What are the time constraints for implementing redundant solutions
Related Design Patterns	• Segmentation: To reduce likelihood that the same attack that degrades one component also degrades the other. • Redundancy: To have duplicate components in the system for failover purposes. • Diversity: Diverse components limit the ability for a single vulnerability to propagate throughout the entire system.
Technical Standards and Examples	• CSfC – DAR • Analog backups, manual workarounds
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling

Technical Standards and Examples	• Commercial Solutions for Classified (CSfC) – Data-at-Rest (DAR) • Analog backups, manual workarounds
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling
Applicability Considerations	• Applicable when the system has a High RMF characterization for availability. • Applicable only to system components that have more than one technical solution/implementation available. • This design pattern should be applied when the risk of the same vulnerability being exploited across multiple systems is high. • Critical functions, such as mission, safety, and flight, should also be redundant.
CSAs	• 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels • 06 - Minimize and Harden Cyber Attack Surfaces • 08 - Manage System performance if Degraded by Cyber Events

Design Pattern Implementation

Design Pattern Lab implementation:

- Tangible results proving the efficacy and applicability of the design pattern
- Comprehensive understanding of the trade-offs of the design pattern
- Insight into the implementation nuances for different systems and subsystems



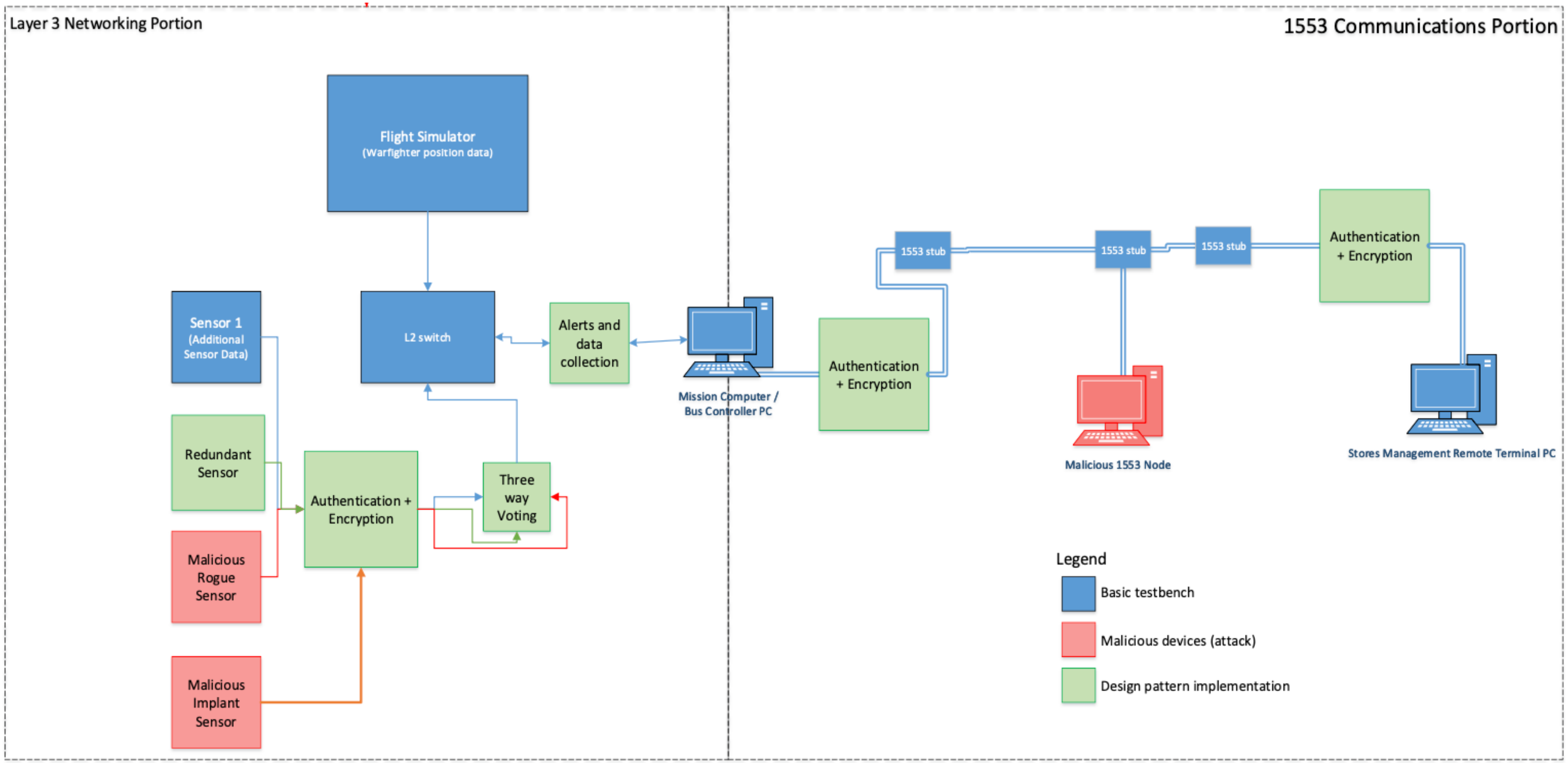
- **Example Use Case - Notional Weapons System Mission:** Deliver an explosive payload within a 25 mile radius of a specific target

- **Weapon system consists of:**
  - MIL-STD-1553 communications bus
  - Layer 3 Ethernet communications
  - Target position system, own position system

Goal: Create a notional weapon system to demonstrate an increase in system resiliency via design pattern implementation

Design Pattern Implementation

1. Build a baseline testbench
   - Measure performance metrics during normal operations
2. Attack testbench
   - Measure performance metrics during attack
3. Add a design pattern
4. Attack again and note any improvement in resilience
   - Measure performance metrics during attack
5. Repeat Steps 3 & 4 for initial selection of design patterns



Summary

- JHU/APL tested the applicability and efficacy of a subset of the cybersecurity design patterns in a specific weapon system context by building and executing a notional, representative weapon system testbed
  - Testbed not an exhaustive test for all 24 cybersecurity design patterns, but did provide insight into the usefulness and pertinence of the design patterns
  - Introduction of design patterns did create some performance impacts as compared to the baseline performance, but multiple classes of cyberattack were thwarted as a result of the patterns' introduction to the system
  - Measurements gathered show trends that could be captured and used to feed other design patterns as well, including, but not limited to, situational awareness and similar patterns

Next Steps

- Consider how to do similar testing with digital twins produced through model-based systems engineering (MBSE)

- Consider creating design pattern template representations in MBSE and digital twin environments. The goal would be to create modular representations that can be applied to a variety of systems in their design stages to test the use cases and verify where specific design patterns add value toward improved measures of performance, measures of effectiveness, and overall cyber resilience.

- Continue to refine the patterns to include include any information gaps from the end users

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY