

Engineering Design Patterns

The Johns Hopkins Applied Physics Laboratory

Brooke Guare

Cyber Systems Engineer Brooke.Guare@jhuapl.edu

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.

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)) / Resilient Systems (RS) tasked the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to curate and develop design patterns.

Challenge: The majority of 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

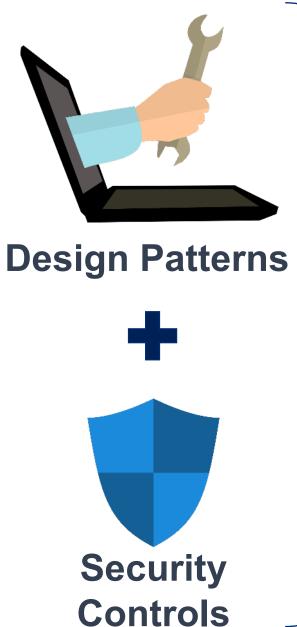
Solution: Development of design patterns

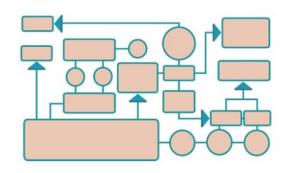
 A design pattern is a general, reusable solution to commonly occurring problems within a given context in system design

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







System Design



Resilient System



Cybersecurity-

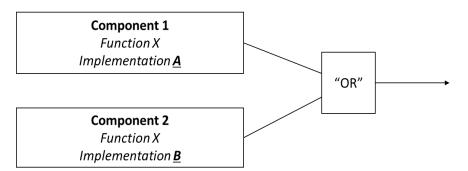
related

Requirements

Case Study: Aircraft

Flight controls are electrically controlled



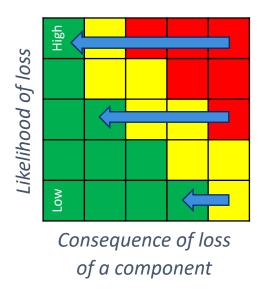


Threat:

Loss of power to mission critical components

Application of Diverse Redundancy Design Pattern:

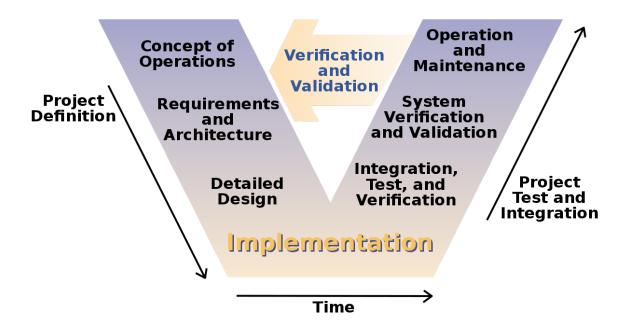
- Magnetic generator (primary source) allows power to be generated as long as engines are spinning
- 3 Electric Generators can power flight controls
- If electric backups fail, there is a battery backup



These mechanical examples can be translated to the cyber domain

When Should Design Patterns Be Used?

Integrating good design principles early in the systems engineering lifecycle helps ensure
the system will be able to be resilient to the threat event, or set of threat events



 However, design patterns can be applied throughout the systems engineering lifecycle in order to help secure existing systems

Design Pattern Template

Redundancy	Design Pattern T	Citle DRAFT				
ccumuancy		Diagram illustrating pattern components in relation to one another				
Diversity	Description	Summary of the main ideas about the illustrated design pattern.				
Data Diode	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				
Authentication	SZ/A	dependences for the pattern's application.				
A 41, ; 4;	Limitations	Cautions regarding the pattern's efficacy and applicable contexts.				
Authorization	Abstraction Level	An enumerated pattern category, one of either "base" or "compound." A base pattern is the lowest				
Trust Anchor	chor decomposition level. Combining base patterns results in <i>compound</i> patterns.					
1 D	Consequences of Ap	plying the Pattern				
Root of Trust C	Benefits	Desirable outcomes the pattern may enable; specifically, outcomes that address the stated problem.				
3 5	Trade-Offs	Acknowledgment of possible consequences imposed by applying the pattern, possibly necessitating some				
	5 (2)	compromises to otherwise beneficial system qualities elsewhere.				
	Related					
	Loss Control	An enumerated set of loss-related goals (from "Design Tenets Review," Draft, MITRE Corporation). The				
	Objective	pattern can support one or more of these goals. The term "loss" may apply both to a component and to a				
	Addressed	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:				
L] Provincia		Prevent the loss from occurring				
P1 Description		Limit the extent of the loss				
		Fully or partially recover from the loss				
l Sc Problem	Implementation	To help bridge the gap between abstract concept and specific implementation, this section provides				
A: Solution	Considerations	considerations on how to implement the design pattern.				
Li Sommon	Related Design	Additional design patterns that, when used in conjunction with this pattern, contribute to solving this				
Assumptions	Patterns	pattern's problem scope. Patterns listed here may complement this pattern to overcome limitations or				
Rela Assumptions Limitations	9	combine to yield a more powerful capability.				
	Related Design	This is a placeholder for tracing design patterns to draft MITRE Design Tenets document. Will be added				
Abstraction Level	Principles	once document is finalized.				
Consequences of App	Technical	Texts, standards, applications, and/or examples that present the design pattern and/or describe its employed				
Danasta	Standards and	use cases. The references listed here may call the design pattern by a different name, but the application still				
	Examples	meets the spirit and intent of the design pattern described in the template.				
	Potential Security	The given pattern could be used to satisfy the listed security controls in NIST SP800-53. This is not meant to				
	Controls	be a comprehensive list, only a subset of examples.				

	ancy		DRAFT				
		omponent 1					
		Function X	_				
	Imp	lementation <u>A</u>					
			"(OR"	•		
	Co	omponent 2					
		Function X					
	Imp	lementation <u>B</u>					
Description	Two or more compone	ente provide r	edundant functionality syl	here only	y one component is absolutely		
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				ion-critic	cal function, and if that single		
	component is compror	mised, the dep	pendent mission-critical fu	inction is	s also lost. Further, if systems em	ploy	
					failures (which possibly affect all		
			n thwart the intended bene				
Assumptions					dverse occurrence is acceptably l		
					teams or vendors have developed	these	
T toutentle			ficient amount of diversity				
Limitations					ons is inversely proportional to th		
					mponents, some form of common	anty	
Abstraction Level		at makes then	n susceptible to the same e Compound (Tier 2)		Combines and advantages on 1 12-		
Consequences of A	Base (Tier 1)		Compound (Tier 2)	TXT(Combines redundancy and divers	ny)	
			dh		and the standard of the standard standa		
Benefits					critical mission functionality by		
					nent loss does not necessarily rest		
					exploited across separate diverse ation. Apart from cyber, redundar		
			iponents nave the same im	ipiemeni	ation. Apart from cyber, redundai	ECY .	
	man allow for increase	ad marfarman	on halm handle load balan				
Trada Offe	-	-	ce, help handle load balan	ces, etc.			
Trade-Offs	 Potentially increase 	es material cos	st, space, weight, power, a	ces, etc. ind syste	m complexity, likely beyond that		
Trade-Offs	Potentially increase homogenously redu	es material cos indant system	st, space, weight, power, a . Applying this pattern thr	ces, etc. and syste roughout	m complexity, likely beyond that the entire system is probably	of a	
Trade-Offs	 Potentially increase homogenously redu impractical. Vetting 	es material cos indant system g diverse com	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may	ces, etc. and syste roughout y increas	em complexity, likely beyond that the entire system is probably se implementation and compatibil	of a	
Trade-Offs	 Potentially increase homogenously redu impractical. Vetting complexity. Implen 	es material cos indant system g diverse com menting divers	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe	ces, etc. and syste roughout y increas cts (e.g.,	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is	of a	
Trade-Offs	Potentially increase homogenously redu impractical. Vetting complexity. Implem challenging; thus, or	es material cos andant system g diverse com menting divers one may be for	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which	nd syste roughout y increas cts (e.g., aspects	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity.	of a	
	Potentially increase homogenously redu impractical. Vetting complexity. Implem challenging; thus, or	es material cos andant system g diverse com menting divers one may be for	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe	nd syste roughout y increas cts (e.g., aspects	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity.	of a	
Related	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy	es material cos andant system g diverse com nenting divers one may be for y requires add	st, space, weight, power, a a. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and	ces, etc. and syste roughout y increas cts (e.g., aspects mainten	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines.	of a	
Related Loss Control	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, or Diverse redundancy Loss Prevention	es material cos undant system g diverse com nenting divers one may be for y requires add	st, space, weight, power, a . Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a	ces, etc. and syste roughout y increas cts (e.g., aspects maintens	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines.	of a	
Related Loss Control Objective	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, or Diverse redundancy Loss Prevention Losing a single critical	es material cos undant system g diverse com menting divers one may be for y requires add	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon	ces, etc. and syste roughout y increas cts (e.g., aspects maintena	the complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f	of a ity	
Related Loss Control	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critical component does not	es material cos andant system g diverse com menting divers one may be for y requires add X d secessarily	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon initially results in degrace	ces, etc. and syste roughout y increas cts (e.g., aspects maintena X I nent 7 ded r	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining where	of a ity	
Related Loss Control Objective	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, or Diverse redundancy Loss Prevention Losing a single critical	es material cos andant system g diverse com menting divers one may be for y requires add X d secessarily	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality,	ces, etc. und syste roughout y increas ets (e.g., aspects maintena X I nent 7 ded r	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining whe one component goes down, to ther	of a	
Related Loss Control Objective	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critical component does not	es material cos andant system g diverse com menting divers one may be for y requires add X d secessarily	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrat mission functionality, switching to the redunda	ces, etc. and syste roughout y increas ets (e.g., aspects maintena X I ent 7 ded r cant s	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic fe ecovery is held, determining whet one component goes down, to there teamlessly fall back to the diverse	of a	
Related Loss Control Objective	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critical component does not	es material cos andant system g diverse com menting divers one may be for y requires add X d secessarily	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sired to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca	ces, etc. and systeroughout y increas cts (e.g., aspects mainten X I nent I ded r c ant s	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining whe one component goes down, to ther	of a	
Related Loss Control Objective	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critical component does not	es material cos andant system g diverse com menting divers one may be for y requires add X d secessarily	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrat mission functionality, switching to the redunda component thereafter ca limit the duration of the	ces, etc. and systeroughout y increas cts (e.g., aspects mainten X I nent I ded r c ant s	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic fe ecovery is held, determining whet one component goes down, to there teamlessly fall back to the diverse	of a	
Related Loss Control Objective Addressed	Potentially increase homogenously redu impractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critica component does not nesult in loss of mission	es material coundant system g diverse commenting divers commenting divers me may be for y requires add X II eccessarily on function.	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation.	ces, etc. and systeroughout y increase cts (e.g., a aspects maintena X I nent 1 ded r c ant s in r	em complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to ther seamlessly fall back to the diverse redundant second component.	of a	
Related Loss Control Objective Addressed	Potentially increase homogenously reduimpractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critica component does not n result in loss of missic Are the redundant of	es material coundant system g diverse com menting divers com menting divers menting diversing menting diversing menting diversing menting diversing add X x x x x x x x x x x x x x x x x x x	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrae mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or or	ces, etc. und syster roughout y increas cts (e.g., a aspects maintena X I ded r cont r	em complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining whe one component goes down, to the seamlessly fall back to the diverse redundant second component.	of a	
Related Loss Control Objective Addressed	Potentially increase homogenously reduimpractical. Vetting complexity. Implementally impractical in Diverse redundancy Diverse redundancy Loss Prevention Losing a single critical component does not not result in loss of mission Are the redundant of For failover capability.	es material coundant system g diverse com menting divers com menting divers menting diversing menting diversing menting diversing menting diversing add X x x x x x x x x x x x x x x x x x x	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrae mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or or	ces, etc. und syster roughout y increas cts (e.g., a aspects maintena X I ded r cont r	em complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to ther seamlessly fall back to the diverse redundant second component.	of a	
Related Loss Control Objective Addressed	Potentially increase homogenously reduimpractical. Vetting complexity. Implementally impractical incomplexity in the challenging; thus, or diverse redundancy. Loss Prevention Losing a single critical component does	es material cos andant system g diverse com menting divers one may be for y requires add X If we construction.	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrat mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op- e the detection and respon	ces, etc. und syste roughout y increas, aspects mainten X I nent 1 ded r cant s n r operating use action	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining when ecomponent goes down, to ther seamlessly fall back to the diverse edundant second component. in a failover capacity as necessary to failover to one to	of a	
Related Loss Control Objective Addressed Implementation Considerations	Potentially increase homogenously reduimpractical. Vetting complexity. Implementally impractical incomplexity in the challenging; thus, or diverse redundancy. Loss Prevention Losing a single critical component does	es material cos andant system g diverse com menting divers one may be for y requires add X If we construction.	st, space, weight, power, a h. Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrae mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or or	ces, etc. und syste roughout y increas, aspects mainten X I nent 1 ded r cant s n r operating use action	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining when ecomponent goes down, to ther seamlessly fall back to the diverse edundant second component. in a failover capacity as necessary to failover to one to	of a	
Related Loss Control Objective Addressed Implementation Considerations	Potentially increase homogenously reduimpractical. Vetting complexity. Implementallenging; thus, or Diverse redundancy Loss Prevention Losing a single critical component does not no result in loss of mission Are the redundant or For failover capabilianother What are the time or	es material coundant systems g diverse commenting diverse commenting diverse ne may be for y requires add a lecessarily on function.	st, space, weight, power, a . Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon	ces, etc. und syste roughout y increas cts (e.g., a spects mainten X II ent T ded r c ant s in r perating see action solution	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining when ecomponent goes down, to ther seamlessly fall back to the diverse edundant second component. in a failover capacity as necessary to failover to one to	of a X or the ther	
Related Loss Control Objective Addressed Implementation Considerations	Potentially increase homogenously reduimpractical. Vetting complexity. Implementallenging; thus, or Diverse redundancy Loss Prevention Losing a single critical component does not no result in loss of mission Are the redundant or For failover capabilianother What are the time or	es material coundant systems g diverse commenting diverse commenting diverse ne may be for y requires add a lecessarily on function.	st, space, weight, power, a . Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon	ces, etc. und syste roughout y increas cts (e.g., a spects mainten X II ent T ded r c ant s in r perating see action solution	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining when the component goes down, to ther seamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to	of a X or the ther	
Related Loss Control Objective Addressed Implementation Considerations	Potentially increase homogenously reduimpractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critica component does not no result in loss of mission Are the redundant o For failover capabilianother What are the time of Segmentation: To rother.	es material coundant system g diverse commenting divers commenting divers me may be for y requires add X II secessarily on function.	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon implementing redundant	ces, etc. und syster roughout y increase aspects mainten X I nent 1 ded r ant s in r occating ase action solution.	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining whe one component goes down, to ther seamlessly fall back to the diverse edundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades	of a X or the ther	
Related Loss Control Objective Addressed Implementation Considerations	Potentially increase homogenously reduimpractical. Vetting complexity. Implen challenging; thus, o Diverse redundancy Loss Prevention Losing a single critica component does not no result in loss of mission Are the redundant o For failover capabilianother What are the time of Segmentation: To rother. Redundancy: To ha	es material coundant system g diverse commenting diverse commenting diversione may be for y requires add a linear system of the components	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon implementing redundant in components in the system	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	x x x x x x x x x x x x x x x x x x x	
Related Loss Control Objective Addressed Implementation Considerations	Potentially increase homogenously reduimpractical. Vetting complexity. Implem challenging; thus, or Diverse redundancy Diverse redundancy Loss Prevention Losing a single critical component does not	es material coundant system g diverse commenting diverse commenting diversione may be for y requires add a linear system of the components	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon implementing redundant in components in the system	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f ecovery is held, determining whe one component goes down, to ther seamlessly fall back to the diverse edundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades	x x x x x x x x x x x x x x x x x x x	
Related Loss Control Objective Addressed Implementation Considerations Related Design Patterns	Potentially increase homogenously reduimpractical. Vetting complexity. Implementally impractical in the property of the prope	es material coundant system g diverse commenting diverse commenting diversione may be for y requires add a linear system of the components	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon implementing redundant in components in the system	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	x x x x x x x x x x x x x x x x x x x	
Related Loss Control Objective Addressed Implementation Considerations Related Design Patterns Technical	Potentially increase homogenously reduimpractical. Vetting complexity. Implementallenging; thus, or Diverse redundancy Loss Prevention Losing a single critical component does not not nesult in loss of mission Are the redundant or For failover capability another What are the time of Segmentation: To nother. Redundancy: To have been system. CSfC - DAR	es material coundant systems g diverse commenting diverse commenting diversine may be for y requires add where the components of the components of the components for the components becomponents by the components by the comp	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon- initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or or e the detection and respon- implementing redundant cod that the same attack the components in the system imit the ability for a single	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	x X X X X X X X X X X X X X X X X X X X	
Related Loss Control Objective Addressed Implementation Considerations Related Design Patterns Technical Standards and	Potentially increase homogenously reduimpractical. Vetting complexity. Implementally impractical in the property of the prope	es material coundant systems g diverse commenting diverse commenting diversine may be for y requires add where the system of the secondary of the secondary of the system	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and to Loss Limitation Even if losing a compon- initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or or e the detection and respon- implementing redundant cod that the same attack the components in the system imit the ability for a single	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	x X X X X X X X X X X X X X X X X X X X	
Related Loss Control Objective Addressed Implementation Considerations Related Design Patterns Technical Standards and Examples	Potentially increase homogenously reduimpractical. Vetting complexity. Implem challenging; thus, or Diverse redundancy. Loss Prevention Losing a single critical component does not not result in loss of mission. Are the redundant or For failover capability another. What are the time of Segmentation: To nother. Redundancy: To have been supported by the province of the component of the province of the component of the province of the component of the province of the provi	es material coundant system g diverse commenting divers commenting diversione may be for y requires add a lecessarily on function. Ecomponents of littles, what are constraints for reduce likelihous diverse duplicate of components littles annual workard	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon initially results in degrac mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op e the detection and respon implementing redundant components in the system imit the ability for a single ounds	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	x X X X X X X X X X X X X X X X X X X X	
Related Loss Control Objective Addressed Implementation Considerations Related Design Patterns Technical Standards and	Potentially increase homogenously reduimpractical. Vetting complexity. Implem challenging; thus, or Diverse redundancy. Diverse redundancy. Loss Prevention Losing a single critical component does not not result in loss of mission. Are the redundant or For failover capability another. What are the time of Segmentation: To result to the diversity: Diverse of System. CSFC Denial of Services of Services and Services of S	es material coundant system g diverse com menting divers com menting divers menting diverse ne may be for y requires add a lecessarily on function. Components of lities, what are constraints for reduce likelihed an undanged mention and workar wice Protection.	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon- initially results in degrac- mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op- e the detection and respon- implementing redundant in components in the system imit the ability for a single ounds	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	x X X X X X X X X X X X X X X X X X X X	
Related Loss Control Objective Addressed Implementation Considerations Related Design Patterns Technical Standards and Examples	Potentially increase homogenously reduimpractical. Vetting complexity. Implem challenging; thus, or Diverse redundancy. Diverse redundancy. Loss Prevention Losing a single critical component does not not nesult in loss of mission. Are the redundant or For failover capability another. What are the time of Segmentation: To nother. Redundancy: To have Diversity: Diverse or system. CSfC - DAR Analog backups, m. SC-5 Denial of Ser. CP-9 Information S	es material cocandant system g diverse com menting diverse com menting diverse menting diverse com grequires add X I leccessarily on function. Components of lities, what are constraints for reduce likelihe are duplicate of components lities and worker wice Protection system Backu	st, space, weight, power, a Applying this pattern thr ponents adds cost and may sity across all system aspe- reed to prioritize to which ling multiple training and a Loss Limitation Even if losing a compon- initially results in degrac- mission functionality, switching to the redunda component thereafter ca limit the duration of the degradation. perating all the time, or op- e the detection and respon- implementing redundant in components in the system imit the ability for a single ounds	ces, etc. und syster roughout y increas, a sepects maintens X I nent 1 ded r cant s un r occating se action solution at degra for faile	m complexity, likely beyond that the entire system is probably se implementation and compatibil power, CPU architecture) is to apply diversity. ance pipelines. Loss Recovery The "OR" box is where the logic f recovery is held, determining where one component goes down, to the reamlessly fall back to the diverse redundant second component. in a failover capacity as necessary to failover to one to s des one component also degrades over purposes.	X X X X X X X X X X X X X X X X X X X	

Subset of Design Patterns Developed:

Redundancy

Diverse Redundancy

Data Diode

Segmentation

Authentication

Authorization

Trust Anchor

Watch Dog

Data Collection

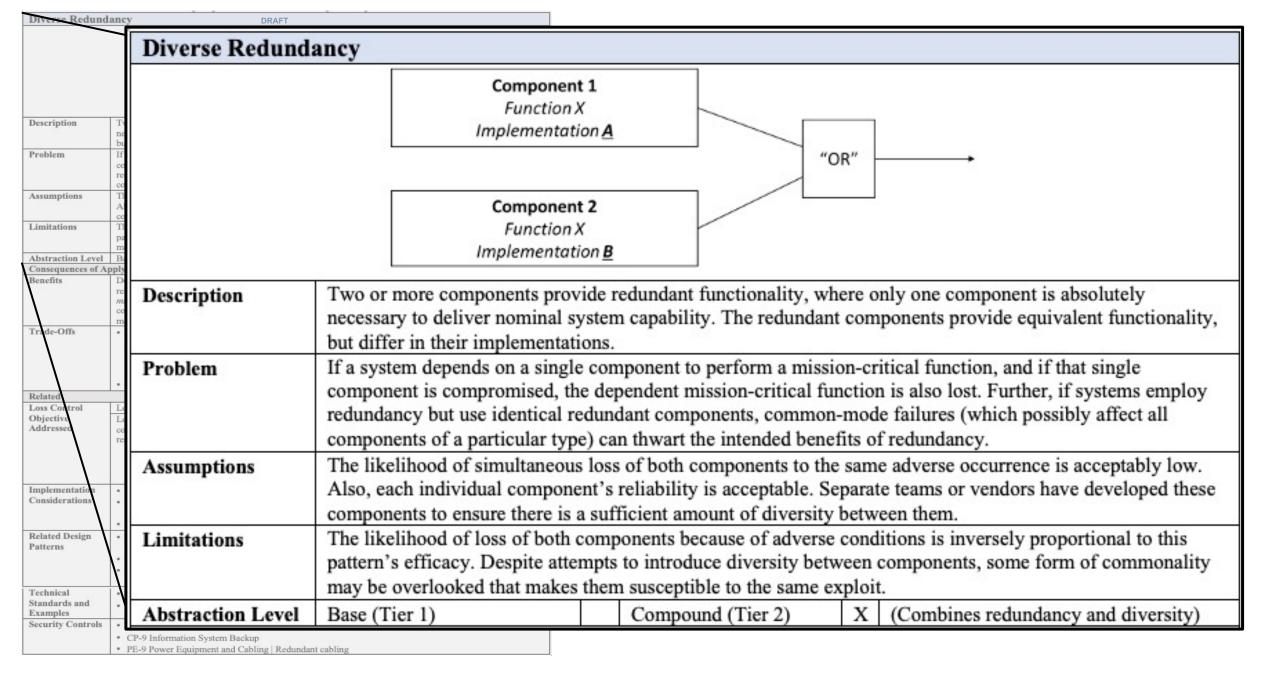
Analytics

Alerts

Response

Load from Known State

.... & More



DI D 1						
Diverse Redu		FT				
	Component 1 Function X implementation <u>A</u>	"OR"				
	Component 2 Function X Implementation <u>B</u>					
Description		ant functionality, where only one component is absolutely bility. The redundant components provide equivalent functionality,				
Problem	component is compromised, the depender	nt to perform a mission-critical function, and if that single tt mission-critical function is also lost. Further, if systems employ components, common-mode failures (which possibly affect all art the intended benefits of redundancy.				
Assumptions		th components to the same adverse occurrence is acceptably low. ility is acceptable. Separate teams or vendors have developed these amount of diversity between them.				
Limitations		s because of adverse conditions is inversely proportional to this roduce diversity between components, some form of commonality entitle to the same exploit				
Abstraction Lo Consequences Benefits	Consequences of A	pplying the Pattern				
Trade-Offs Related Loss Control	Benefits	relying on the diverse redundant mission function loss. The likelih components is lower than if all components	t, the system can continue providing critical mission functionality by component. In other words, a <i>component</i> loss does not necessarily result in a bod that an identical vulnerability is exploited across separate diverse emponents have the same implementation. Apart from cyber, redundancy ince, help handle load balances, etc.			
Addressed Implementatic Consideration	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. 				
Related Design Patterns		Diverse redundancy requires	adding multiple training and maintenance pipelines.			
	 Diversity: Diverse components limit the system. 	e ability for a single vulnerability to propagate throughout the entire				
Technical Standards and Examples	CSfC - DAR Analog backups, manual workarounds					
Security Control	le CC & Doniel of Commiss Boots ation					

SC-5 Denial of Service Protection

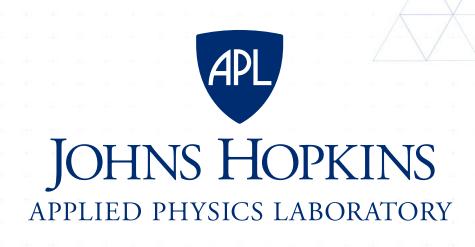
CP-9 Information System Backup
 PE-9 Power Equipment and Cabling | Redundant cabling

Security Controls

Diverse Redund	ancy	Related	4600					7
	Componer Function	Loss Control	Loss Prevention	Х	Loss Limitation	Х	Loss Recovery	X
tmpley enta Componer Function Implementa		Objective Addressed	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		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	or the
Problem	Two or more components pro necessary to deliver nominal but differ in their implementa If a system depends on a sing comportant is compromised, t		component thereafter of limit the duration of the degradation.			i	redundant second component.	
Assumptions	redundancy but use identical components of a particular ty The likelihood of simultaneou Also, each individual components to ensure there is	Templementation Considerations • Redundant components should be implemented so that they aren't 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						
Limitations	The likelihood of loss of both pattern's efficacy. Despite att may be overlooked that make		techniques to ensure they both don't fail due to the same cyberspace attack. • How quickly does one component need to perform the functions of a failed component?					
Abstraction Level Consequences of A Benefits	Base (Tier 1) pplying the Pattern Despite losing a single comporelying on the diverse redund	 Are all redundant components on all the time or are redundant components operating in a failover capacity? 						
Trady-Offs	mission function loss. The lik components is lower than if a may allow for increased perfe • Potentially increases mater		If all component 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? How will the system or the operator know when to switch from one redundant component to another?					
	homogenously redundant s impractical. Vetting divers complexity. Implementing challenging; thus, one may		 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 different components. 					
Related Loss Control	Diverse redundancy requir Loss Prevention	Related Design Patterns	 Segmentation: To reduce l other. 	ikelil	hood that the same attack t	hat d	egrades one component also degrade	es the
Objective Addressed	Losing a single critical component does not necessar result in loss of mission funct		 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. 					
Implementation Considerations	Are the redundant compon For failover capabilities, w another	The system shall maintain mission capability despite malicious data being written to the system. The system shall maintain mission capability despite the execution of malicious code. The system shall maintain mission capability despite the malicious execution of authorized instructions.						
Related Design Patterns	What are the time constrain Segmentation: To reduce li other. Redundancy: To have dupl Diversity: Diverse components system.		The system shall maintain mission capability despite the denial of authorized data. The system shall remove adversary access to system data, without degrading mission capability, upon the detection of an adversary obtaining restricted (e.g., classified or sensitive) system data.					
Technical Standards and Examples Security Controls	CSfC - DAR Analog backups, manual w SC-5 Denial of Service Pro	Technical Standards and Examples	CSfC – DAR Analog backups, manual workarounds					
	CP-9 Information System I PE-9 Power Equipment an	Security Controls	SC-5 Denial of Service Protection CP-9 Information System Backup					
			 PE-9 Power Equipment an 	d Ca	bling Redundant cabling			

Next Steps

- Integrate design pattern into CRWS-BoK repository
- Demonstrate design pattern applicability and interoperability
- Continue development and refinement of existing patterns and template



UNCLASSIFIED.