Engineering Secure and Resilient Cyber-Physical Systems

Major Logan O. Mailloux, PhD, CISSP, CSEP
Assistant Professor, Systems Engineering
Cyber Center for Research

Disclaimer:
The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

Motivation

"The Air Force's ability to fly, fight and win in air, space and cyberspace is threatened by increasing competent adversaries in the cyberspace domain,"

-- Dennis Miller
CROWS director

U.S. AIR FORCE

HOME | NEWS | ABOUT US | AF SITES | CONTACT US

Home > News > Article Display

AF looks to ensure cyber resiliency in weapons systems through new office

By Patty Welsh, 66th Air Base Group Public Affairs / Published January 04, 2017

PRINT | E-MAIL

HANSCOM AIR FORCE BASE, Mass. (AFNS) --
The Air Force, through its Life Cycle Management Center, has stood up the Cyber Resiliency Office for Weapons Systems (CROWS).

Although the office's primary operating location and senior leadership will be at Hanscom Air Force Base, contributing staff will come from various Air Force organizations and geographic locations. It will focus on integrating activities across the Air Force to ensure weapon systems maintain mission-effective capabilities, despite cyber adversities. It reached initial operating capability Dec. 21, 2016.

"The Air Force's ability to fly, fight and win in air, space and cyberspace is threatened by increasing competent adversaries in the cyberspace domain," said Dennis Miller, the CROWS director, who also serves as Hanscom AFB's engineering and technical management associate director. "The cyber threat is more than just network intrusion or traditional malware – it also affects our weapon systems and presents a clear and present danger to successful mission assurance."

Weapon systems have real-time constraints and complexities coupled with differing sustainment strategies which means the same security management practices that are used for traditional information technology systems require tailoring and adaption to be effective and efficient in a weapon system environment.

Miller said the CROWS will focus on integration across Air Force communities to acquire, field, operate and sustain increased cyber-resilient weapon systems. It will also work to integrate activities in the Air Force Cyber Campaign Plan (CCP) focused on multiple strategic vectors.

According to Daniel Holtzman, the Air Force cyber technical director, achieving the intended mission assurance in a cyber-contested environment involves a complex combination of individual systems acquisition, including design and development; operational concerns encompassing planning and execution; and systems sustainment including maintenance and training.

In addition, when vulnerabilities, external factors and adversary tactics are combined, they create a set of complex interdependencies that must be worked in a holistic and integrated manner to reduce risk, Holtzman said.

"To effectively and efficiently combat the cyber threat, we must horizontally integrate within and across our weapon systems, working together across our Air Force and partnership communities to securely design and operate systems, conduct missions and sustain capabilities," he said. "We must educate and train our Air Force communities to be vigilant of the cyber risk at all times."

http://www.af.mil/News/Article-Display/Article/1041426/af-looks-to-ensure-cyber-resiliency-in-weapons-systems-through-new-office/

The System Security Problem

- Embedding IT or "Cyber" into nearly all core business processes, mission systems, and weapon systems
  - Increases operational efficiency and decision quality
  - Decreases confidence that defense systems will function as intended

1. Reliance on COTS technology frequently developed and manufactured outside of U.S. control is **widely available for all the world to study, reverse engineer, and identify vulnerabilities**

2. Uncertain Supply chains (i.e., prime contractors, subcontractors, suppliers, sub-suppliers) make it **difficult to know what is in the system or where it came from**

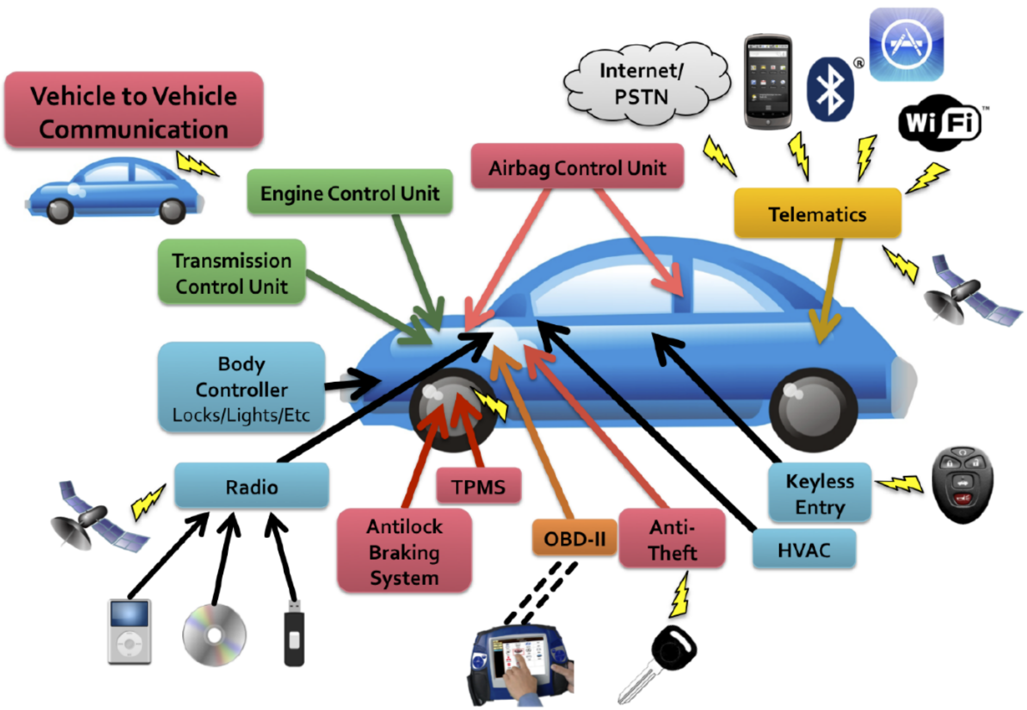
3. System complexity and interconnectedness (e.g., software-intensive, known and unknown dependencies, numerous connections to DoD networks) **obfuscate possible system states and vulnerabilities**

Baldwin, K., Miller, J., Popick, P., & Goodnight, J. (2012). The United States Department of Defense Revitalization of System Security Engineering Through Program Protection. Paper presented at the *Systems Conference (SysCon), 2012 IEEE International,* 1-7.

The Cyber-Physical Problem

The AFIT of Today is the Air Force of Tomorrow.

- "Comprehensive Experimental Analyses of Automotive Attack Surfaces" by Checkoway *et al.* https://youtu.be/RZVYTJarPFs



Fox News Reported that Iran's Revolutionary Guard captured a US drone in 2011 and built a copy

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011, August). Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Security Symposium*.
http://www.foxnews.com/world/2014/05/11/iran-says-it-has-built-copy-captured-american-drone-will-take-it-on-test-flight/

Headquarters U.S. Air Force

Integrity - Service - Excellence

Cyber Resiliency Office for Weapon Systems (CROWS)
Technical Integration & Governance

Mr. Danny Holtzman, HQE
Cyber Technical Director
daniel.holtzman.1@us.af.mil

BLUF

- **SECAF, SAF/AQ, AFMC & AFSPC teamed to establish Cyber Resiliency Steering Group (CRSG) to develop AF Cyber Campaign Plan (CCP)**
  - **Stood up dedicated office to manage execution → CROWS**
- **AF CCP's overall mission has two goals:**
  - **#1 "Bake-In" cyber resiliency into new weapon systems**
  - **#2 Mitigate "Critical" vulnerabilities in fielded weapon systems**
- **Plus coordination with:**
  - **Cyber Squadron Initiatives**
  - **Test and Evaluation (infrastructure & capability growth)**
  - **Industrial Control Systems/SCADA cyber protection measures**

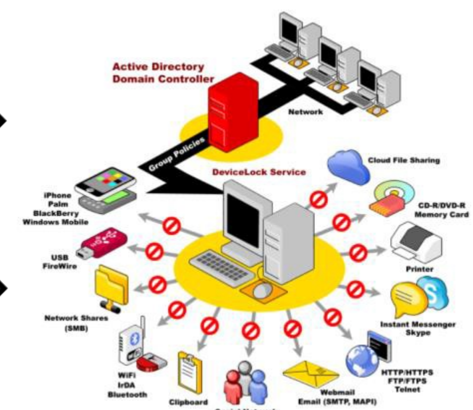
Weapon System Cyber Resiliency Critical to Mission Assurance

- We define the <u>Cyber Resiliency of Military systems</u> to be:
  - The ability of weapon systems to maintain mission effective capability under adversary offensive cyber operations
  - To manage the risk of adversary cyber intelligence exploitation
  - Weapon systems differ from general administrative and business IT systems in ways that matter for implementing Cyber Resiliency

Cyber Campaign Plan FOCUS

Weapon Systems

Weapon Systems		IT Systems
Software/Hardware Design		
Government control	⟷	COTS
Architectures		
Diverse	⟷	Common
Interfaces		
Customized	⟷	Standardized

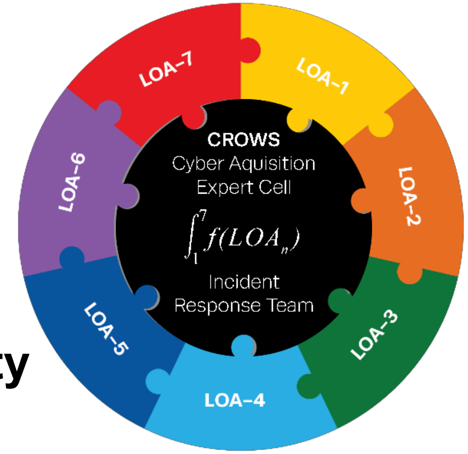


IT Systems

DISTRIBUTION A. Approved for public release: distribution unlimited.

AF Cyber Campaign Plan: Weapon System Focus

- 7 Lines of Action (LOAs)
  - LOA 1: Perform Cyber Mission Thread Analysis
  - LOA 2: "Bake-In" Cyber Resiliency
  - LOA 3: Recruit, Hire & Train Cyber Workforce
  - LOA 4: Improve Weapon System Agility & Adaptability
  - LOA 5: Develop Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Provide Cyber Intel Support



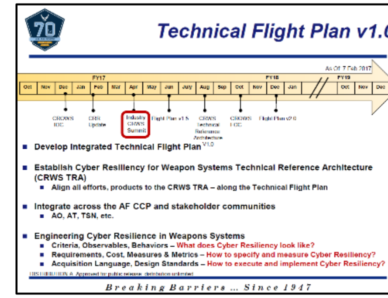
People, Processes, & Products

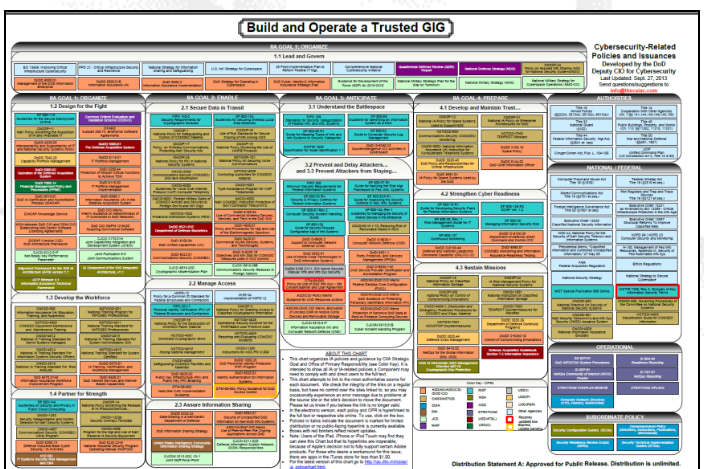
- Cyber Squadron Initiatives
- Test & Evaluation (infrastructure & capability growth)
- Industrial Control Systems/SCADA cyber protection measures

Ensure mission success in a cyber contested environment

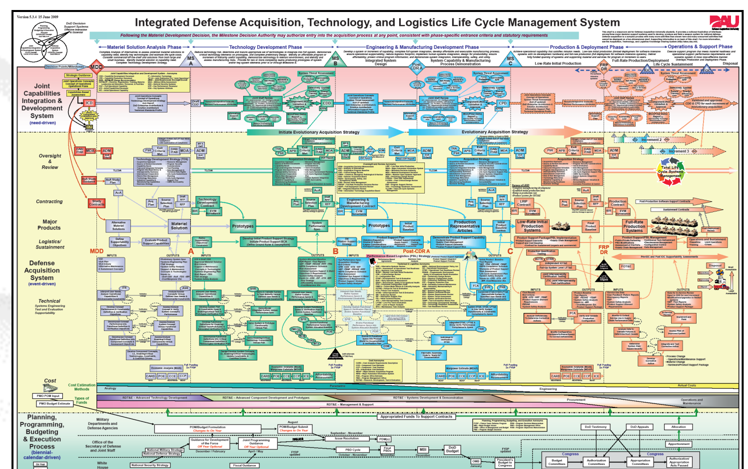
Near and Far Challenges

- Engineering Cyber Resilience in Weapons Systems
  1. Criteria, Observables, Behaviors
     - What does Cyber Resiliency look like?
  2. Requirements, Cost, Measures & Metrics
     - How to specify and measure Cyber Resiliency?
  3. Acquisition Language, Design Standards
     - How to execute and implement Cyber Resiliency?





X



#1. What does Weapon System Cyber Resiliency look like?

Term	**Definition**
Resiliency	The ability of a cyber-physical system to anticipate, withstand, and recover from actual and potential adverse events.
Attribute	**Description**
Anticipate	Planning and/or preparation for known, predicated, and even unknown adverse events to include changes in the operational environment, modes of operation, business/mission functions, emerging threats, integration of novel technologies, and other necessary changes.
Withstand	To absorb or survive the negative impacts of adverse events such as system faults, user errors, software bugs, hardware failures, and cyber attacks.
Recover	To restore business/mission operations (and more specifically desired functionality) to an acceptable level within specified time and performance requirements. Ideally, recovery also includes the ability of the system to “adapt” in order to reduce the impact(s) of future adverse events.

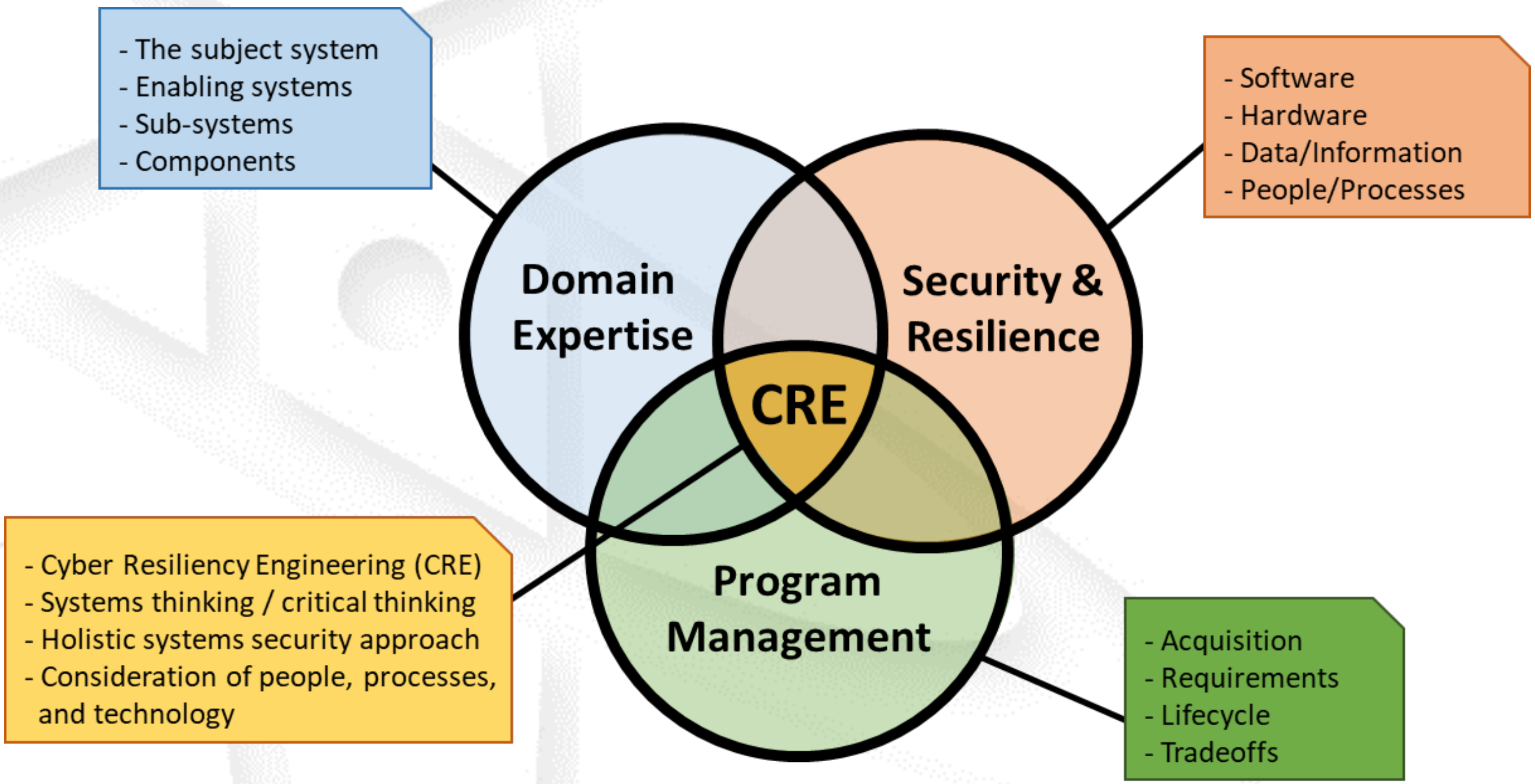
Adapted from:

Deborah J. Bodeau and Richard Graubart, "Cyber Resiliency Engineering Framework," MITRE, Bedford, MA, 2011.
Systems Engineering Handbook Working Group International Council on Systems Engineering, "Systems Engineering Handbook," INCOSE, San Diego, 2015.

Cyber Resiliency Engineering

The AFIT of Today is the Air Force of Tomorrow.

- **Multiple areas of expertise are required for the Cyber Resiliency Engineering (CRE) workforce**



Weapon System Resiliency Job Responsibilities

The AFIT of Today is the Air Force of Tomorrow.

Develop holistic, resiliency-informed system views that thoroughly account for the complexities and real-time operational constraints associated with operationally-oriented cyber-physical systems.	Accomplish program management activities to ensure timely and integrated cybersecurity and resiliency solutions into program schedules, designs, and milestones.
Analyze the system's execution of essential mission operations in dynamic cyber-physical environments to include consequences from advanced cyber threats, disruptions, disasters, and unpredictable emergent behaviors.	Execute innovative engineering approaches towards the successful development, fielding, operation, and maintenance of secure and resilient cyber-physical systems.
Define mission and system-level problem spaces which account for cyber-related operational challenges and complex system-of-systems cyber dependencies.	Analysis of potential solutions and their impact on personnel, processes, and technologies that reduce both technical and operational risk while meeting the system's performance expectations.
Develop feasible resiliency strategies and objectives by considering current and future cyber threat capabilities, criticality of the cyber-physical system's operation, and potential risks.	Perform tradeoff analysis of potential security and resiliency solutions for feasibility to include cost, performance, and schedule impacts.
Perform security and resiliency requirements definition, engineering, and traceability tasks across the system's entire lifecycle.	Conduct testing activities which produce evidences of correct implementation of selected security and resiliency solutions.

A Multidisciplinary Approach to Building Trustworthy Secure Systems

Protecting the Nation's Critical Assets in the 21st Century

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NIST Special Publication 800-160

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
JANET CARRIER OREN

This publication contains systems security engineering considerations for **ISO/IEC/IEEE 15288:2015**, *Systems and software engineering — System life cycle processes*. It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

NIST Special Publication 800-160

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

Previous subtitle was…. "An Integrated Approach to Building Trustworthy Resilient Systems"

RON ROSS
MICHAEL McEVILLEY
JANET CARRIER OREN

This publication contains systems security engineering considerations for **ISO/IEC/IEEE 15288:2015**, *Systems and software engineering — System life cycle processes*. It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Systems Security Engineering in 1 Picture

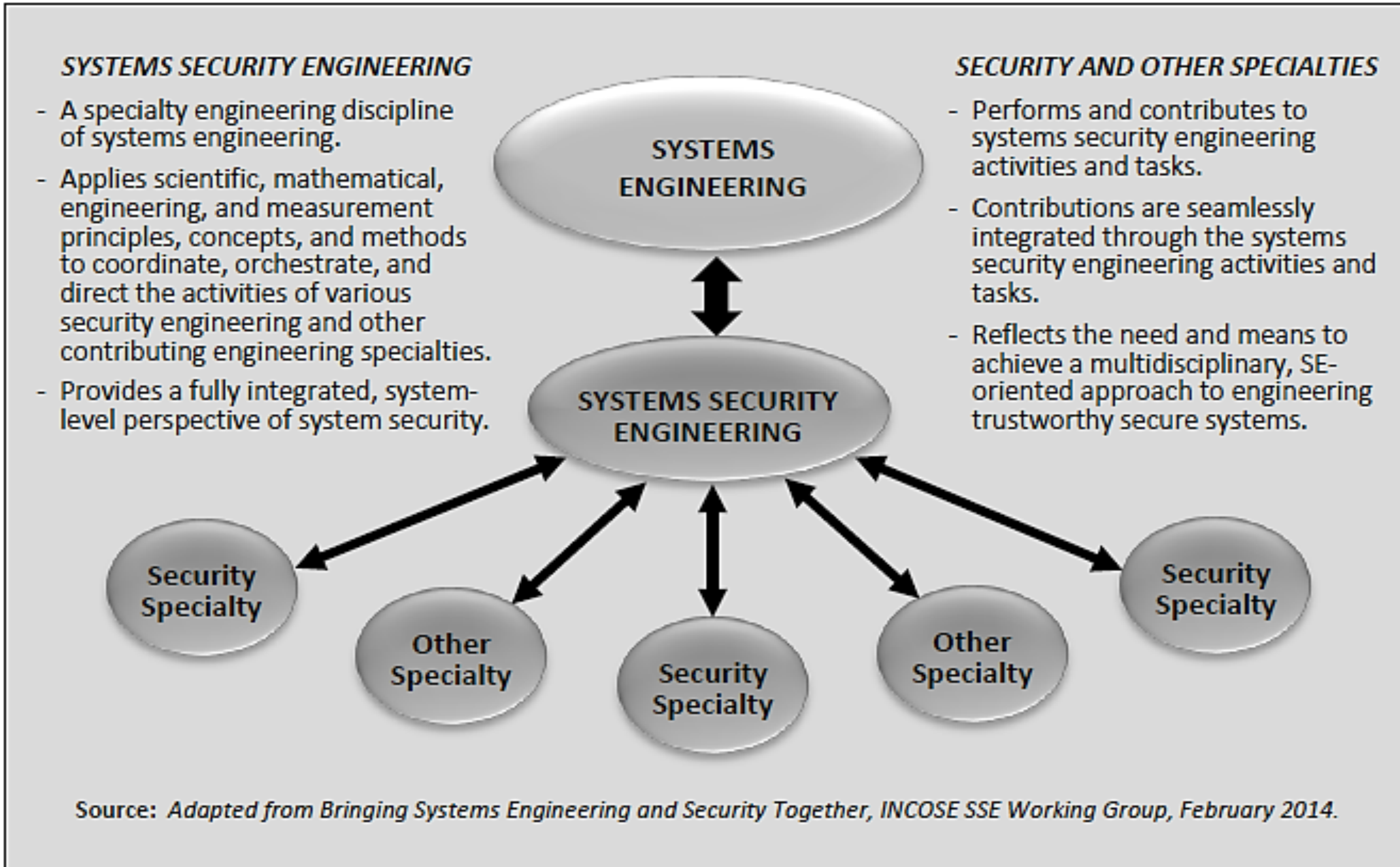


FIGURE 1: SYSTEMS ENGINEERING AND OTHER SPECIALITY ENGINEERING DISCIPLINES

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf, page 11

#2. How to Specify and Measure Cyber Resiliency?

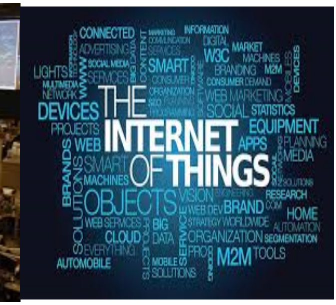
- NIST SP 800-160, page 2, defines **Security** as
  - The freedom from those conditions that can cause loss of *assets*[3] with unacceptable consequences.[4]
  - *The specific scope of security must be clearly defined by stakeholders in terms of the assets to which security applies and the consequences against which security is assessed.*

3. The term *asset* refers to an item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., data, information, software, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is driven by the stakeholders in consideration of life cycle concerns that include, but are not limited to, those concerns of business or mission. Refer to Section 2.3 for discussion of the system security perspective on assets.

4. Security is concerned with the protection of *assets*. Assets are entities that someone places value upon. Summarized from [ISO/IEC 15408-1], Section 7.1 *Assets and countermeasures*.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf



System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA

William Young Jr, PhD

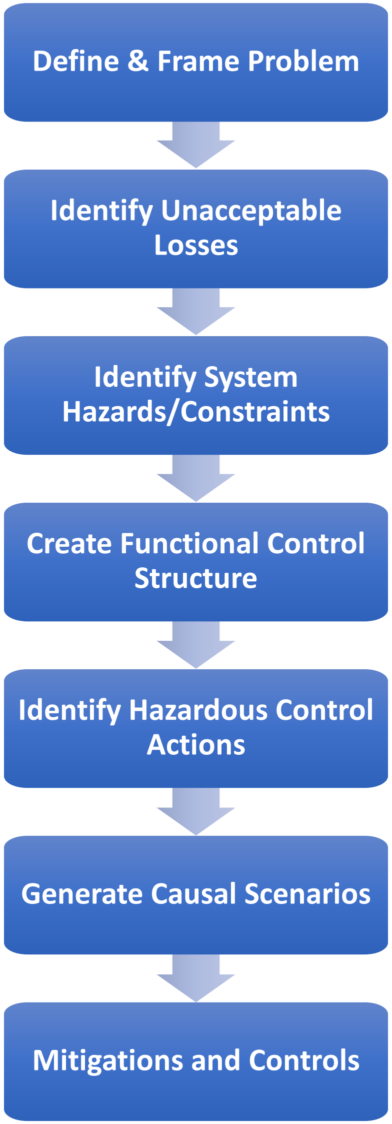
Reed Porada

2017 STAMP Conference
Boston, MA

March 27, 2017

WYOUNG@MIT.EDU

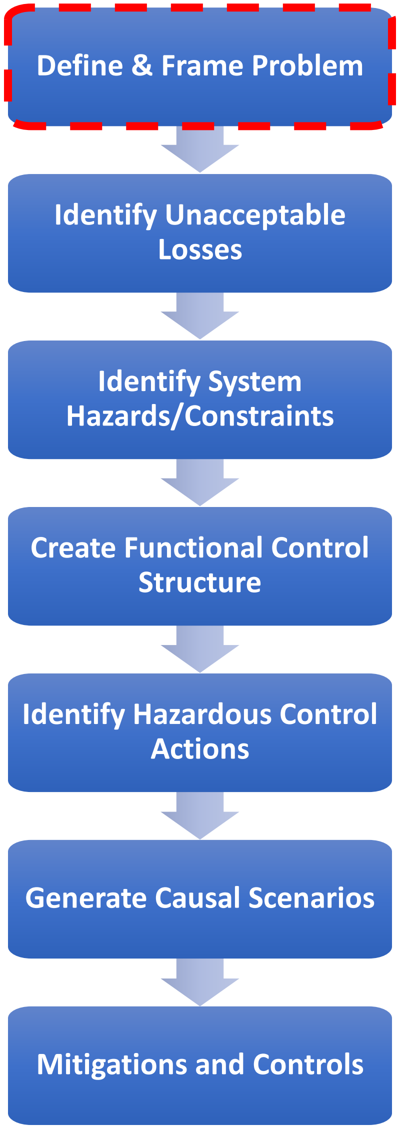
Why Use the STPA-Sec Process?



- **Upfront security engineering analysis to inform the detailed (and costly) security engineering effort**
- **Results inform early engineering trades (where the trade space is the largest and cheapest)**
- **Set the foundation to understand, inform, and document security needs, objectives, and requirements**

Adapted with permission from Col/Dr. William “Dollar” Young’s STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

Define & Frame the Security Problem



Define the system purpose and goal:

A system to do {What = Purpose}

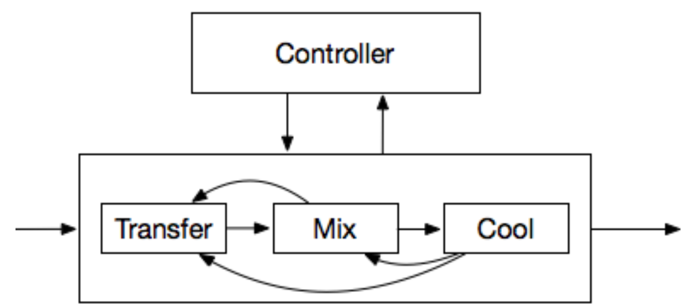
by means of {How = Method}

in order to contribute to {Why = Goals}

A system to **contain and process chemicals**

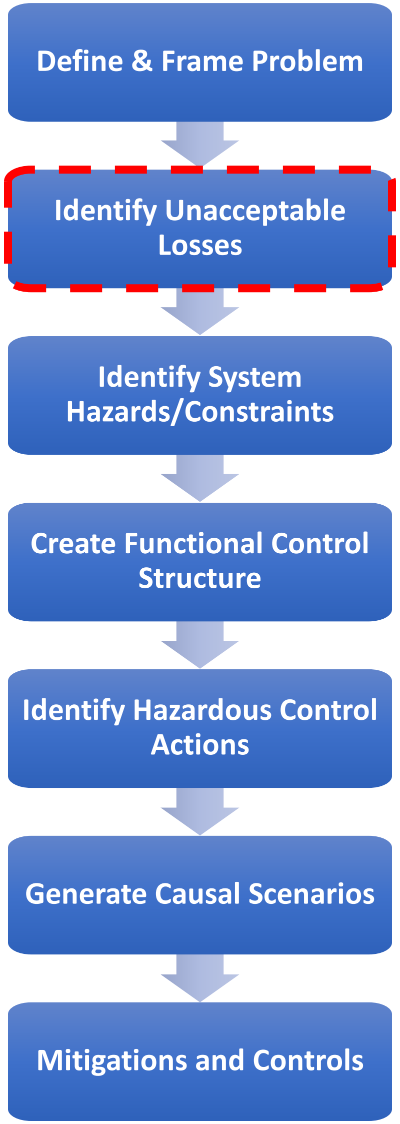
by means of **transferring, mixing, and cooling chemicals**

in order contribute to **production of chemicals sold by the company.**



Adapted with permission from Col/Dr. William "Dollar" Young's STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

What are OUR System's Unacceptable Losses?



Identify and define unacceptable losses (consider the entire system… its people, processes, and technology)

L-1: People die or become injured

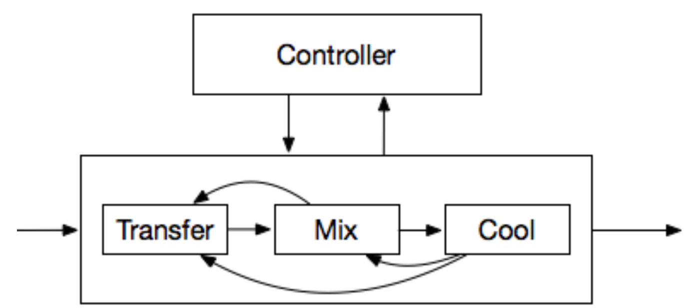
L-2: Production loss

L-3: … … ….

A system to **contain and process chemicals**

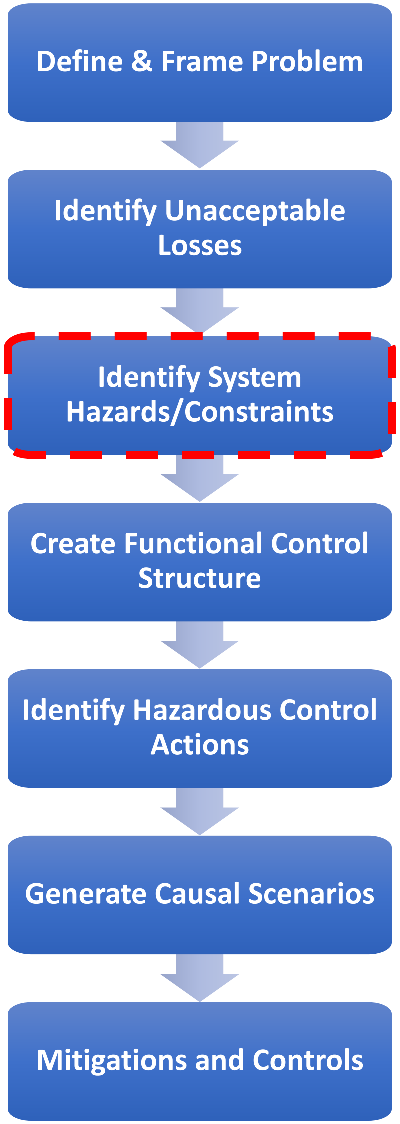
by means of **transferring, mixing, and cooling chemicals**

in order contribute to **production of chemicals sold by the company.**



Adapted with permission from Col/Dr. William "Dollar" Young's STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

What Hazards contribute to Unacceptable Losses?

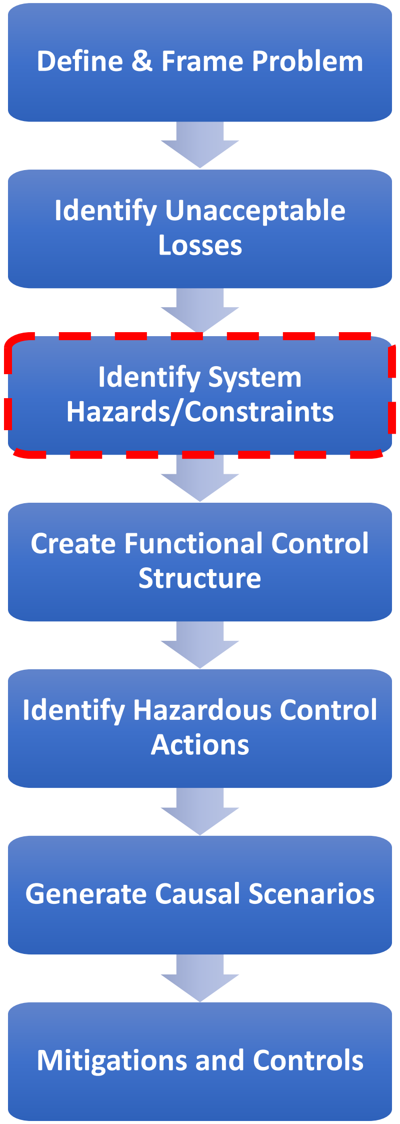


What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss?

Hazard	**L1:** People die or become injured	**L2:** Production loss	**L3:**	**L4:**
H1: Plant releases toxic chemicals				
H2: Plant is unable to produce chemical				

Adapted with permission from Col/Dr. William "Dollar" Young's STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

What Constraints Prevent the Hazards?

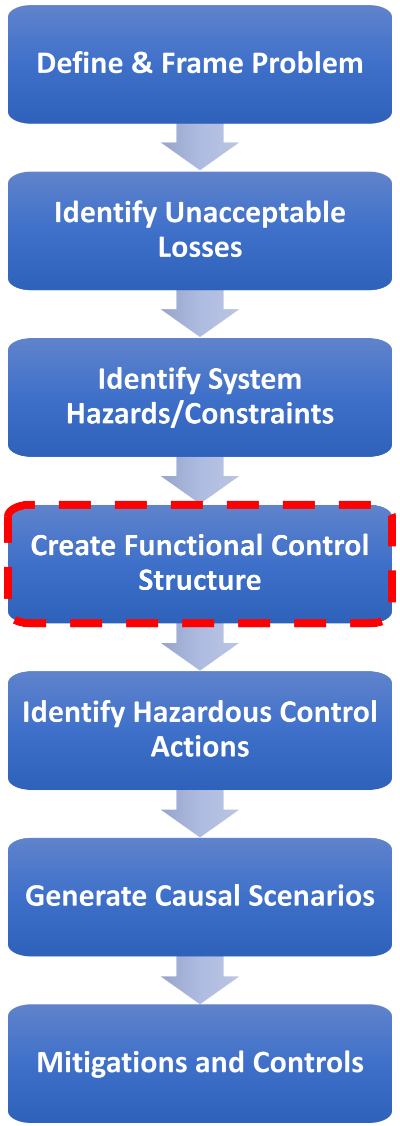


Thinking about the constraints forces you to validate and refine your list of unacceptable losses and associated hazards!

Hazard	Constraint
H1: Plant releases toxic chemicals… Chemicals in air or ground after release from plant	Chemicals must never be released inadvertently from plant
H2: Plant is unable to produce chemical…	…

Identify, Elicit, and Define Functional-Level Cyber Security and Resiliency Requirements

What Processes Must Be Controlled?

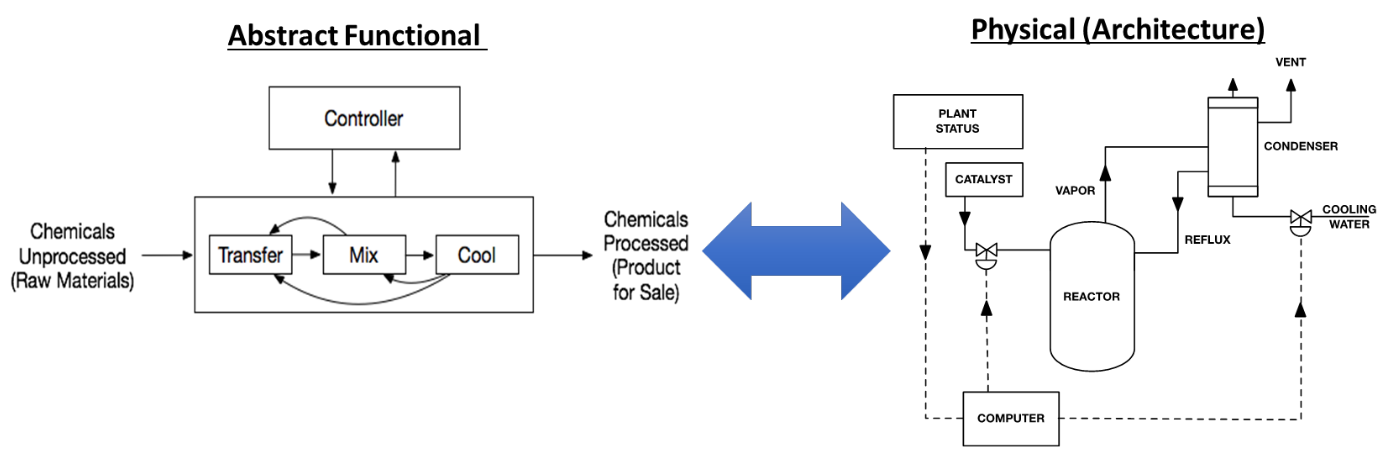


What processes must be controlled in order to accomplish the mission objectives?

- **Transfer and mixing catalyst**
- **Cooling reflux**

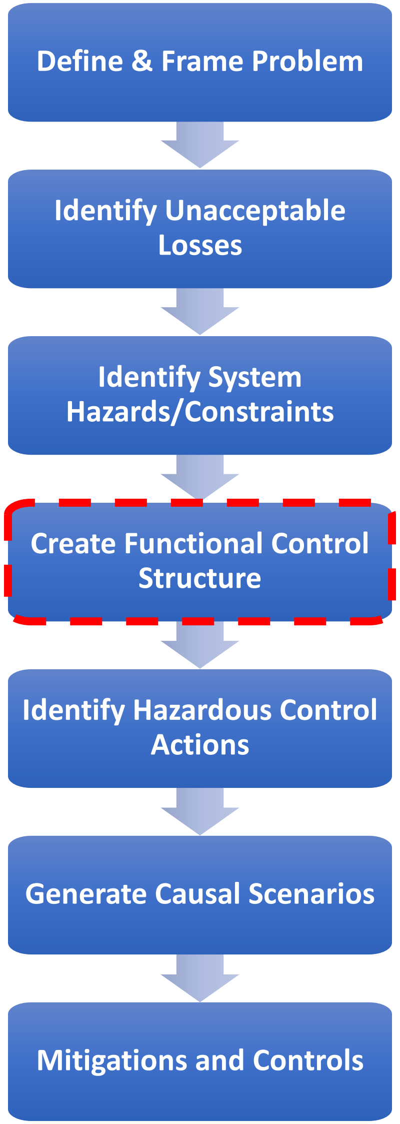
Use insights to understand controller requirements

Consider both the functional equivalent and physical architecture



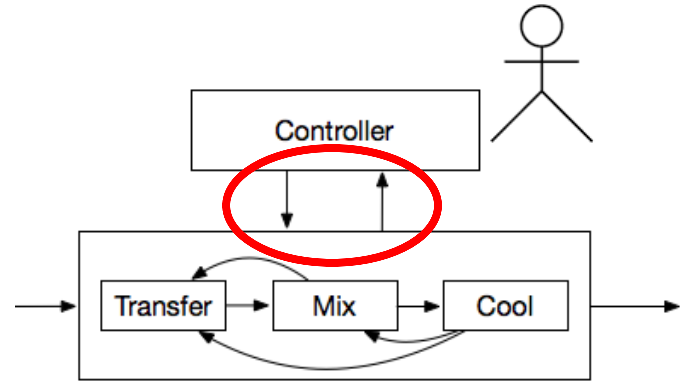
Adapted with permission from Col/Dr. William "Dollar" Young's STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

Define the Control Structure



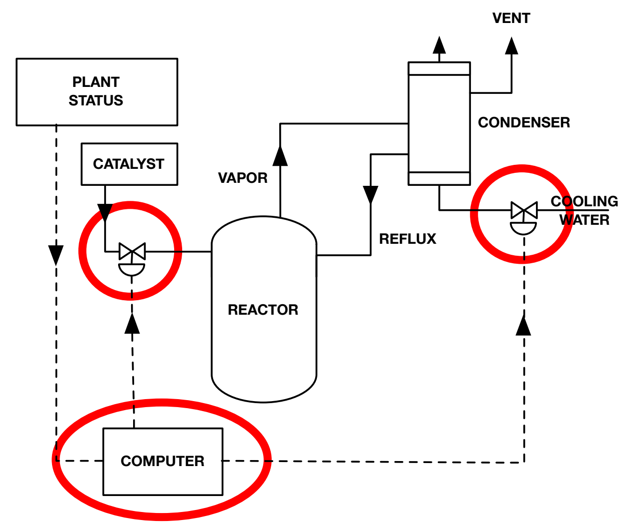
Enumerate each key activity

- **Consider each element**
- **Define respective responsibilities**



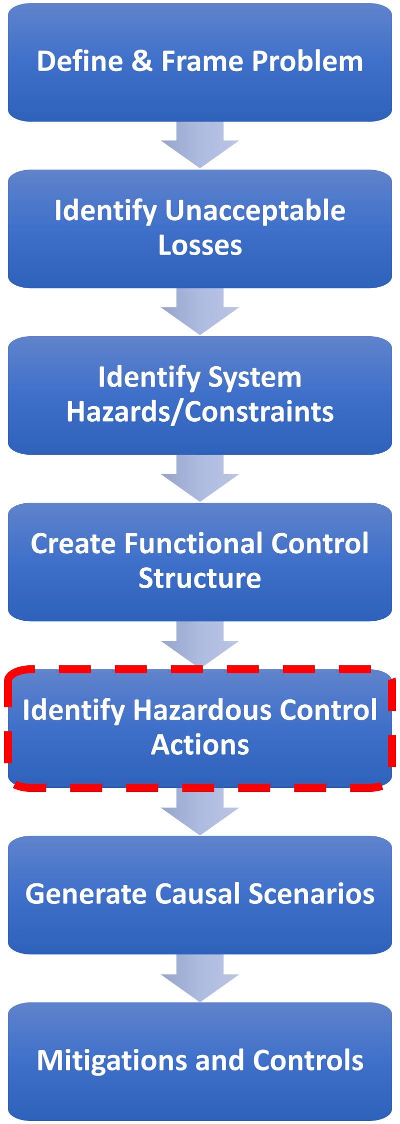
Key Activity: Transfer

Element	Responsibility Description
Operator	• Initiate process • Monitor progress • Manually Intervene
Computer	• Control valves • Report status
Valves	• Open/close on command • Fail open? / Fail closed?



Adapted with permission from Col/Dr. William "Dollar" Young's STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

The Four Hazardous Control Action States



Control Action	Not providing Causes Hazard	Providing Causes Hazard	Incorrect Timing / Order	Stopped Too Soon / Applied Too Long
CA1: Start Process		Operator provides command when condenser water valve not functioning	Operator manually overrides valves and computer misses signal	
CA2: Open Water Valve	Computer does not provide open water valve cmd when catalyst open		Computer provides open water valve cmd more than X seconds after open catalyst	Computer stops providing open water valve cmd too soon when catalyst open
CA3: Close Water Valve		Computer provides close water valve cmd while catalyst open	Computer provides close water valve cmd before catalyst closes	
CA4: Open Catalyst Valve		Computer provides open catalyst valve cmd when water valve not open	Computer provides open catalyst valve cmd more than X seconds before open water	
CA5: Close Catalyst Valve	Computer does not provide close catalyst valve cmd when water closed		Computer provides close catalyst valve cmd more than X seconds after close water	Computer stops providing close catalyst valve cmd too soon when water closed

We now have, Detailed Implementation-Level Cyber Security and Resiliency Requirements

Adapted with permissio
Tutorial: Warning contai

#3. How to Execute and Implement Cyber Resiliency?

- The NIST SP 800-160 presents a SSE framework which supports tailoring of the ISO/IEC/IEEE 15288 processes but where to start?
  - 30 SSE Processes
  - 111 SSE Activities
  - 428 SSE Tasks

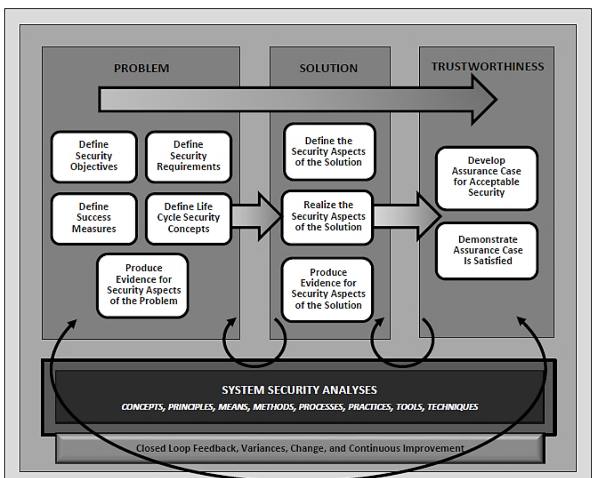


FIGURE 3: SYSTEMS SECURITY ENGINEERING FRAMEWORK

X

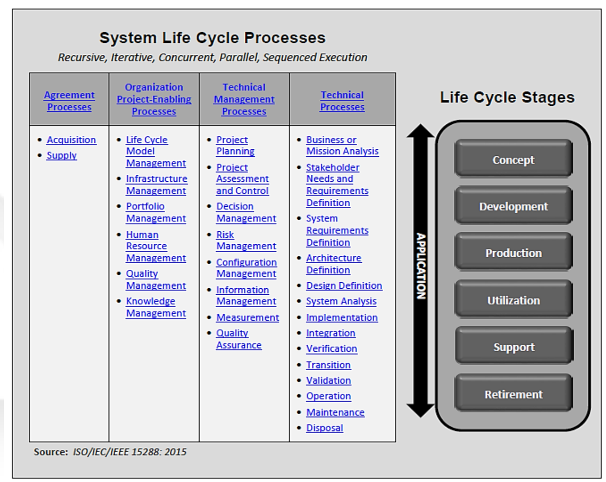
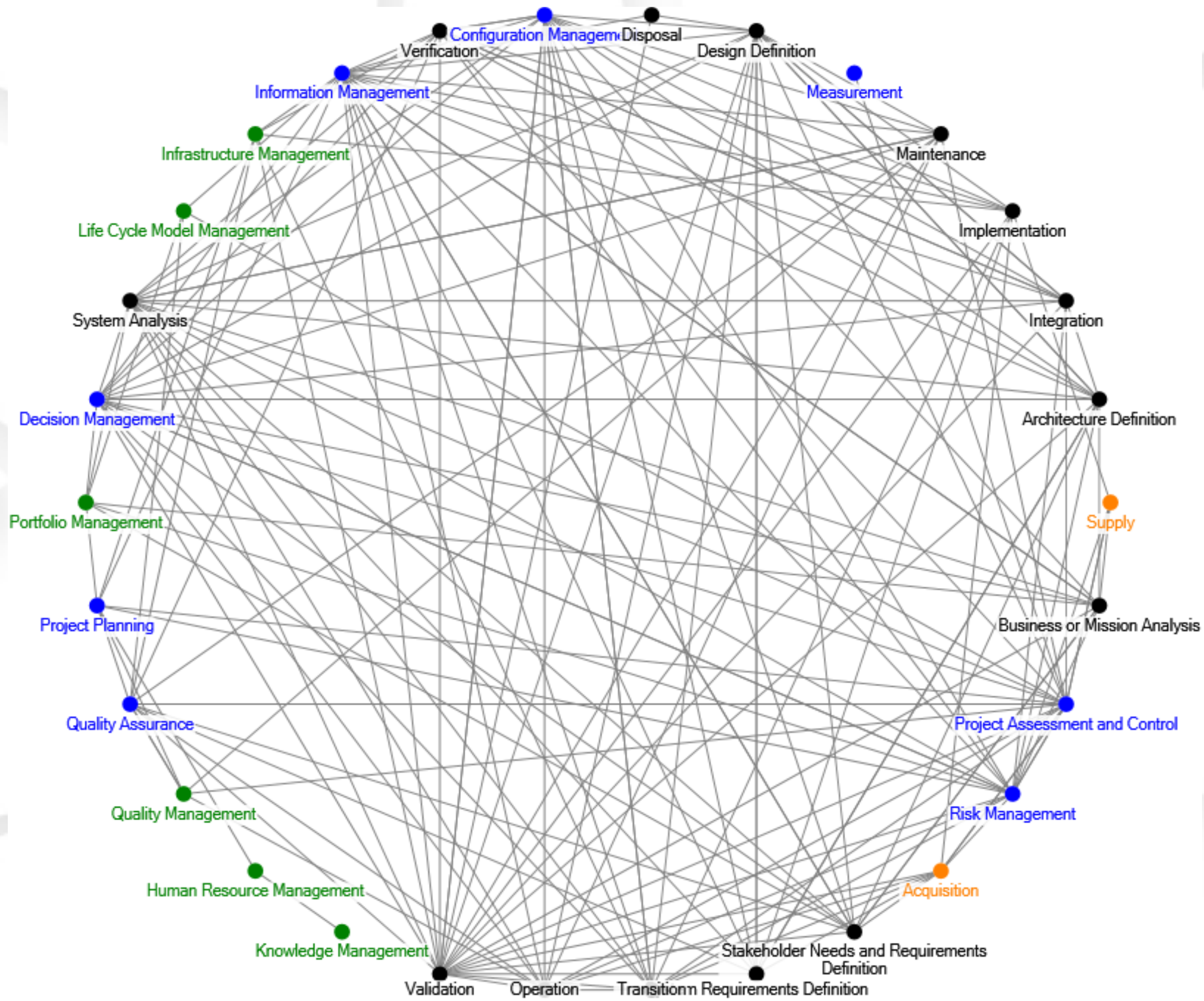


FIGURE 4: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

NIST SP 800-160 Process Relationships

The AFIT of Today is the Air Force of Tomorrow.



Processes (Nodes)	Clustering Coefficient
Disposal	1.000
Integration	0.867
Quality Management	0.800
Architecture Definition	0.773
Business or Mission Analysis	0.689
Maintenance	0.689
Transition	0.667
Decision Management	0.650
Configuration Management	0.633
Operation	0.628
Verification	0.621
Infrastructure Management	0.619
Design Definition	0.590
System Requirements Definition	0.583
System Analysis	0.583
Stakeholder Needs/Req Definition	0.564
Acquisition	0.536
Implementation	0.533
Risk Management	0.525
Validation	0.500
Portfolio Management	0.476
Information Management	0.415
Project Assessment and Control	0.375
Quality Assurance	0.345
Supply	0.333
Project Planning	0.286
Life Cycle Model Management	0.167
Measurement	0.000
Human Resource Management	0.000
Knowledge Management	0.000

Khou, S., Mailloux, L., Pecarina, J. M., & McEvilley, M. A. (2017). A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks. *IEEE Access*.

Customizable SSE Framework

The AFIT of Today is the Air Force of Tomorrow.

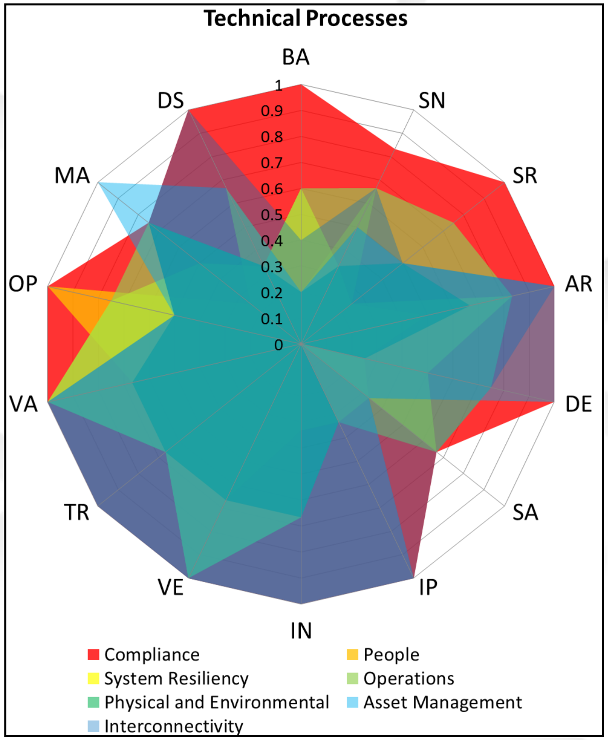
			Compliance	People	System Resiliency	Operations	Physical and Environmental	Asset Management	Interconnectivity
1									
2									
3	TECHNICAL PROCESSES								
4	BA	Business or Mission Analysis	1	0.2	0.6	0.6	0.2	0.2	0.4
5	BA-1	PREPARE FOR THE SECURITY ASPECTS OF BUSINESS OR MISSION ANALYSIS	x						
6	BA-2	DEFINE THE SECURITY ASPECTS OF THE PROBLEM OR OPPORTUNITY SPACE	x		x	x			
7	BA-3	CHARACTERIZE THE SECURITY ASPECTS OF THE SOLUTION SPACE	x	x	x	x	x	x	x
8	BA-4	EVALUATE AND SELECT SOLUTION CLASSES	x		x	x			
9	BA-5	MANAGE THE SECURITY ASPECTS OF BUSINESS OR MISSION ANALYSIS	x						x
10	SN	Stakeholder Needs and Requirements Definition	[illegible]	0.6667	0.3333	0.6667	0.3333	0.5	0.66667
11	SN-1	PREPARE FOR STAKEHOLDER PROTECTION NEEDS AND SECURITY REQUIREMENTS DEFINITION		x					
12	SN-2	DEFINE STAKEHOLDER PROTECTION NEEDS	x	x	x	x	x	x	x
13	SN-3	DEVELOP THE SECURITY ASPECTS OF OPERATIONAL AND OTHER LIFE CYCLE CONCEPTS		x		x			x
14	SN-4	TRANSFORM STAKEHOLDER PROTECTION NEEDS INTO SECURITY REQUIREMENTS	x	x	x	x	x	x	x
15	SN-5	ANALYZE STAKEHOLDER SECURITY REQUIREMENTS	x			x			
16	SN-6	MANAGE STAKEHOLDER PROTECTION NEEDS AND SECURITY REQUIREMENTS DEFINITION	x					x	x
17	SR	System Requirements Definition	1	0.25	0.25	0.75	0.5	0.5	0.5
18	SR-1	PREPARE FOR SYSTEM SECURITY REQUIREMENTS DEFINITION	x			x	x		
19	SR-2	DEFINE SYSTEM SECURITY REQUIREMENTS	x	x	x	x	x	x	x
20	SR-3	ANALYZE SYSTEM SECURITY IN SYSTEM REQUIREMENTS	x			x			
21	SR-4	MANAGE SYSTEM SECURITY REQUIREMENTS	x					x	x
22	AR	Architecture Definition	1	0.5	0.3333	0.3333	0.6667	1	1
23	AR-1	PREPARE FOR ARCHITECTURE DEFINITION FROM THE SECURITY VIEWPOINT	x	x	x	x		x	x
24	AR-2	DEVELOP SECURITY VIEWPOINTS OF THE ARCHITECTURE	x	x	x	x	x	x	x
25	AR-3	DEVELOP SECURITY MODELS AND SECURITY VIEWS OF CANDIDATE ARCHITECTURES	x	x	x	x	x	x	x
26	AR-4	RELATE SECURITY VIEWS OF THE ARCHITECTURE TO DESIGN	x		x	x	x	x	x
27	AR-5	SELECT CANDIDATE ARCHITECTURE	x		x	x	x	x	x
28	AR-6	MANAGE THE SECURITY VIEW OF THE SELECTED ARCHITECTURE	x					x	x
29	DE	Design Definition	1	0.25	0.5	0.75	0.25	1	0.75
30	DE-1	PREPARE FOR SECURITY DESIGN DEFINITION	x		x	x		x	x
31	DE-2	ESTABLISH SECURITY DESIGN CHARACTERISTICS AND ENABLERS FOR EACH SYSTEM ELEMENT	x	x	x	x	x	x	x

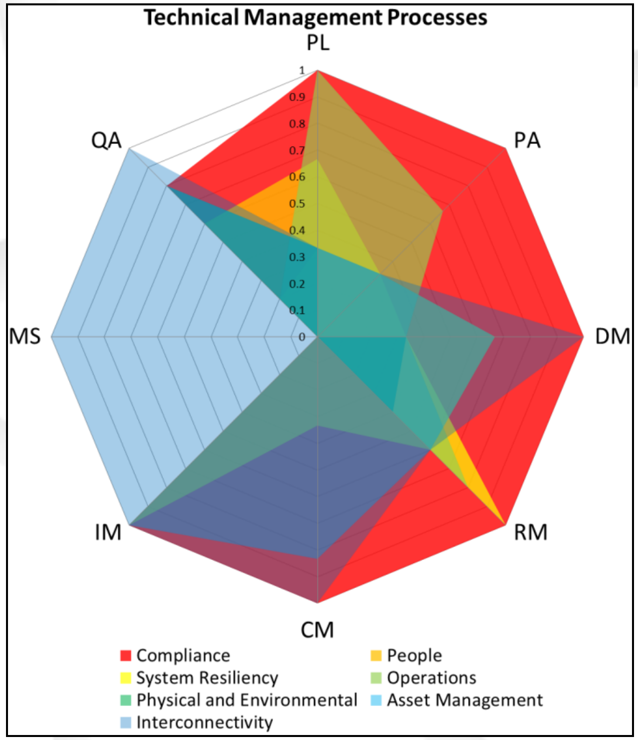
Domains	Graph
Compliance	No
People	No
System Resiliency	Yes
Operations	No
Phjysical and Environmental	No
Asset Management	Yes
Interconnectivity	No

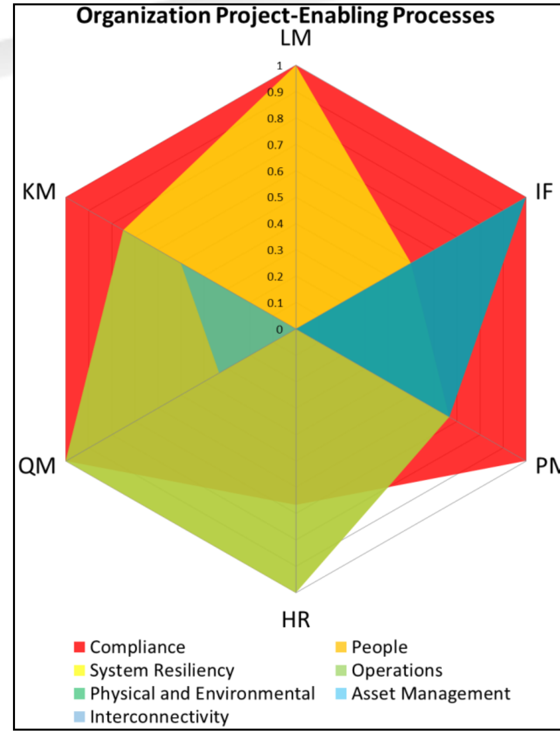
Khou, S., Mailloux, L., Pecarina, J. M., & McEvilley, M. A. (2017). A Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks. *IEEE Access*.

Domain-to-Process Mappings

The AFIT of Today is the Air Force of Tomorrow.







ID	Process	ID	Process	ID	Process	ID	Process
AQ	Acquisition	IF	Infrastructure Management	OP	Operation	SN	Stakeholder Needs and Requirements Definition
AR	Architecture Definition	IM	Information Management	PA	Project Assessment and Control	SP	Supply
BA	Business or Mission Analysis	IN	Integration	PL	Project Planning	SR	System Requirements Definition
CM	Configuration Management	IP	Implementation	PM	Portfolio Management	TR	Transition
DE	Design Definition	KM	Knowledge Management	QA	Quality Assurance	VA	Validation
DM	Decision Management	LM	Life Cycle Model Management	QM	Quality Management	VE	Verification
DS	Disposal	MA	Maintenance	RM	Risk Management		
HR	Human Resource Management	MS	Measurement	SA	System Analysis		

Application Example: Defense Acquisition

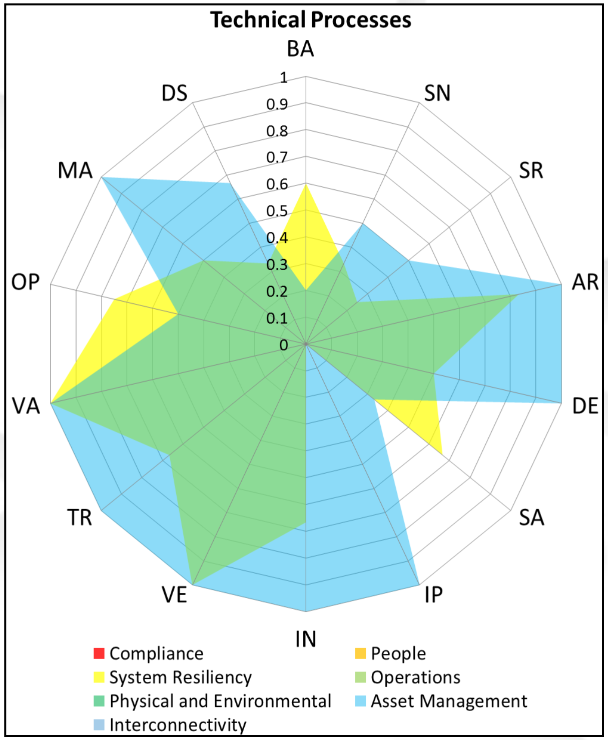
- Prioritization of NIST SP 800-160 SSE Processes and Activities based on the Defense Acquisition Guidebook (DAG)
  - Focuses on classical systems engineering processes for the development of unprecedented systems
  - Uses criticality analysis to protect mission-critical system functions, technologies, and information throughout the acquisition lifecycle

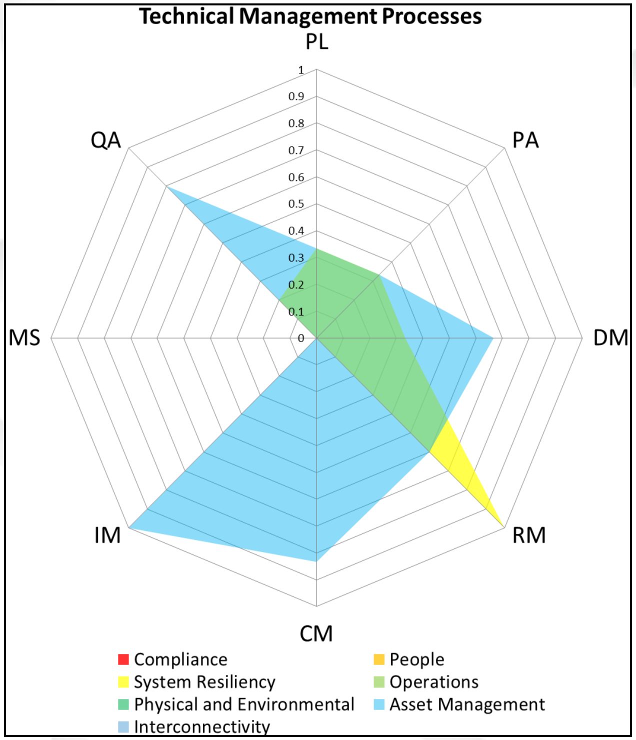
TABLE 4. **Priority scheme for the defense acquisition guidebook.**

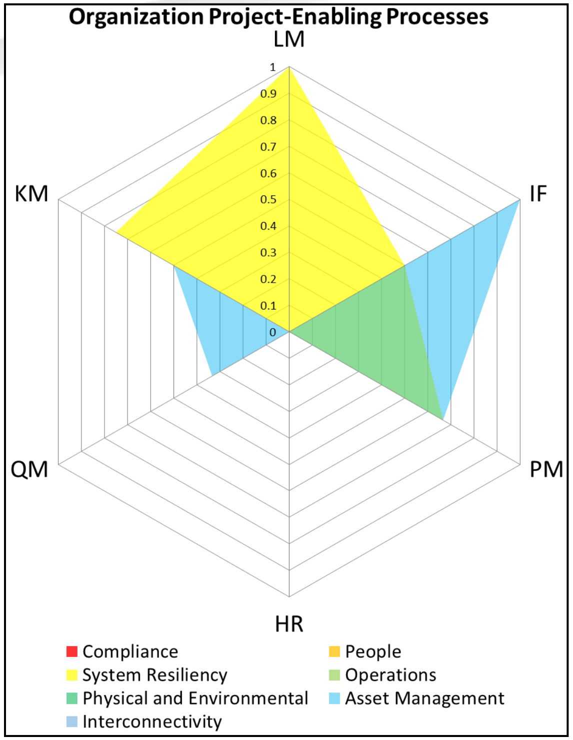
Defense Acquisition Guidebook	Compliance	People	System Resiliency	Operations	Physical and Environmental	Asset Management	Interconnectivity
Missions/Mission-Essential Functions		X	X			X	X
Critical Subsystems, Configuration Items, and Components			X			X	X
Initial Start Conditions			X	X			
Operating Environment	X				X		
Critical Suppliers	X					X	
Sum	**2**	**1**	**3**	**1**	**1**	**3**	**2**

Khou, S., Mailloux, L., Pecarina, J. M., & McEvilley, M. A. (2017). System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts. *IEEE Access*.

Application Example: Defense Acquisition



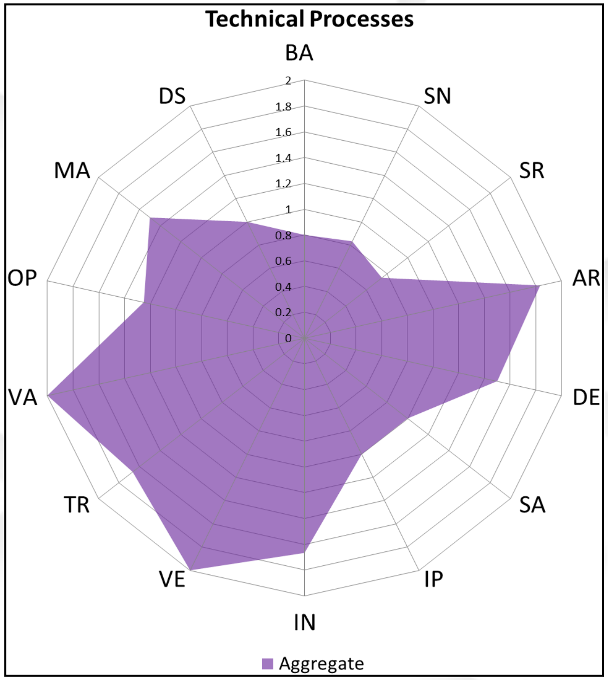


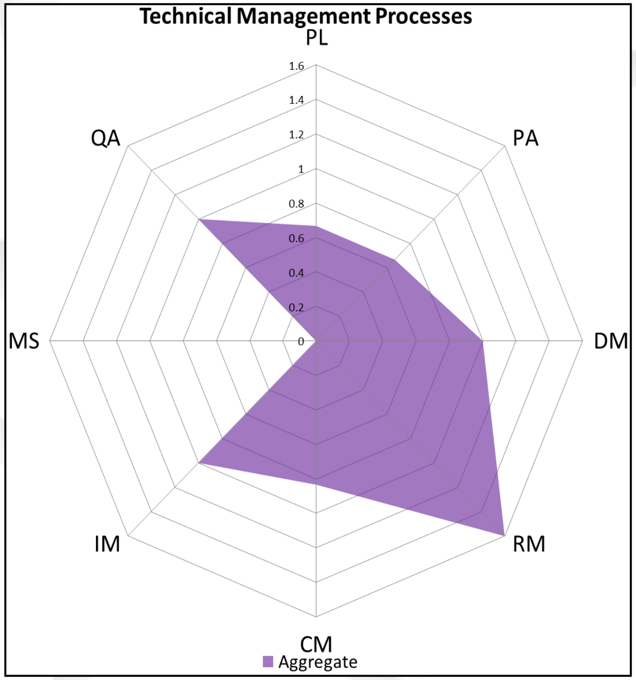


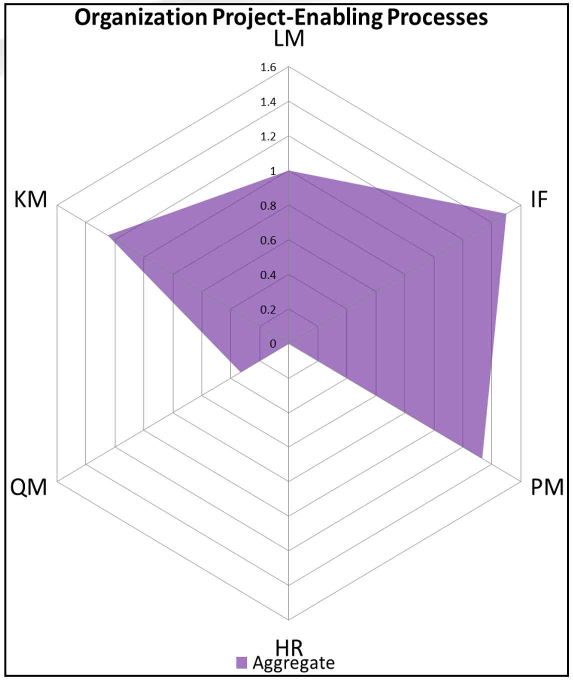
	System Resiliency	Asset Management
Process Families		
Technical Processes	Verification; Validation	Architecture Definition; Design Definition; Implementation; Integration; Verification; Transition; Validation; Maintenance
Technical Management Processes	Risk Management	Information Management
Organization Project-Enabling Processes	Life Cycle Model Management	Infrastructure Management
Agreement Processes	N/A	Acquisition

Application Example: Defense Acquisition

The AFIT of Today is the Air Force of Tomorrow.







First Level Processes (by domain association)	Related Processes (by explicit relationship)
Architecture Definition, Design Definition Implementation, Integration, **Verification**, Transition, **Validation** Maintenance, **Risk Management** Information Management, Life Cycle Model Management, **Infrastructure Management**, Acquisition	Decision Management, Configuration Management, Stakeholder Needs and Requirements Definition , System Requirements Definition, System Analysis, Operation, Disposal, Supply, Project Assessment and Control, Quality Assurance, Quality Management, Business or Mission Analysis

Security should be a by-product of good design and development practices—integrated throughout the system life cycle.

A Tailorable Approach to SSE

The AFIT of Today is the Air Force of Tomorrow.

- The NIST SP 800-160 presents a SSE framework which supports tailoring of the ISO/IEC/IEEE 15288 processes but where to start?
  - 30 SSE Processes
  - 111 SSE Activities
  - 428 SSE Tasks

+ SSE Strategies
+ SSE Principles
+ SSE Tailoring

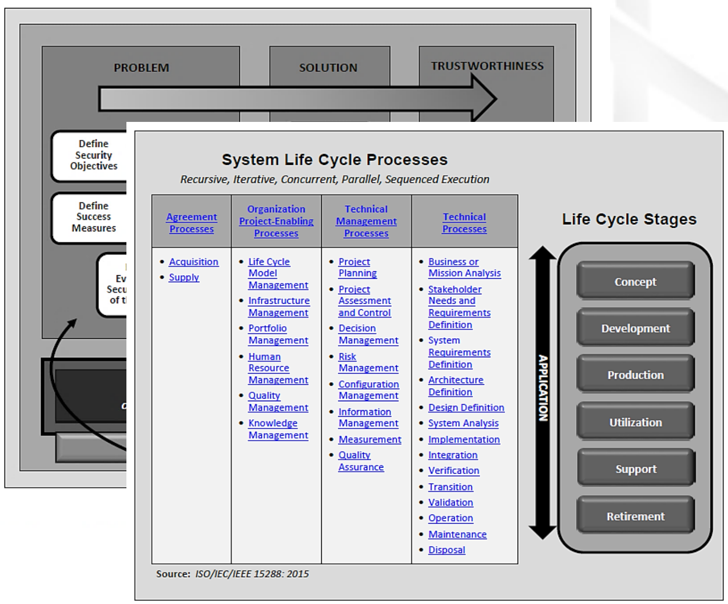
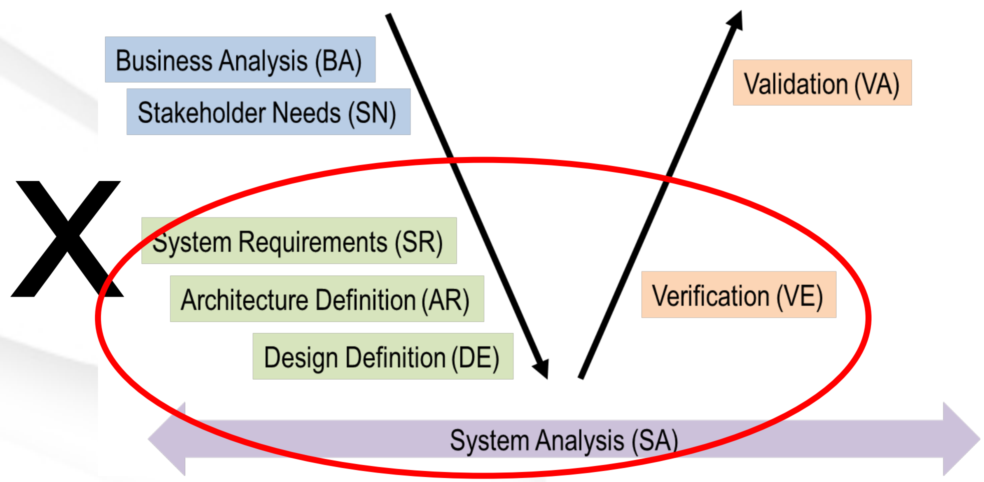


FIGURE 4: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES



http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

The SSE Design Principles

The AFIT of Today is the Air Force of Tomorrow.

Principle Name	Definition - modified from NIST SP 800-160 to emphasize system-level applicability
Clear Abstractions	A system should have simple, well-defined interfaces and functions to provide a consistent and intuitive view of the SoI's data, data elements, and how the data is utilized and managed.
Least Common Mechanism	If multiple components in a system require the same functionality (e.g., a necessary security feature), the desired functionality should be built into a single mechanism (physical or logical) which can be used by all components who require it.
Modularity and Layering	Modularity organizes and isolates functionality and related data flows into well-defined logical groupings (conceptual elements or "objects"), while layering orders and defines relationships between entities and their associated data flows.
Ordered Dependencies (Partially)*	Ordered dependencies refers to the logical arrangement of layers (and modules) such that linear (or hierarchical) functional calls, synchronization, and other dependencies are achieved, and circular dependencies are minimized.
Efficiently Mediated Access	Policy enforcement mechanisms (physical and logical) should utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints.
Minimized Sharing	No resources should be shared between system components (e.g., elements, processes, etc.) unless it is absolutely necessary to do so.
Reduced Complexity	The system design should be as simple and small as possible.
Secure Evolvability	A system should be developed to facilitate secure maintenance when changes to its functionality, architecutre, structure, interfaces, interconnections, or its functionality configuration occur.
Trusted Components	A component must be trustworthy to at least a level commensurate with the security dependencies it supports.
Hierarchical Trust	Building upon the principle of trusted components, hierarchial trust provides the basis for trustworthiness reasoning when composing a system from a variety of components with differing trustworthiness.
Commensurate Protection*	The degree of protection provided to a component must be commensurate with its trustworthiness – as the trust placed in a component increases, the protection against unauthorized modification of the component should increase to the same degree.
Hierarchical Protection	A component need not be protected from more trustworthy components.
Minimize Trusted Components	A system should not have extraneous trusted elements, components, data, or functions.
Least Privilege	Each system element (e.g., enabling systems, components, data elements, users, etc.) should be allocated sufficient privileges to accomplish its specified function, but no more.
Proportional Permissions*	Requiring multiple authorizing entities or operators to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is granted.
Self-Reliance*	Systems should minimize their reliance on other systems, elements, or components for their own trustworthiness.
Secure Composition*	The composition of various components that enforce the same security policy should result in a system that enforces that policy at least as well as the individual components do.
Trusted Communication	Each communication channel (i.e., an interface, link, or network) must be trustworthy to a level commensurate with the security dependencies it supports.

Design Principles

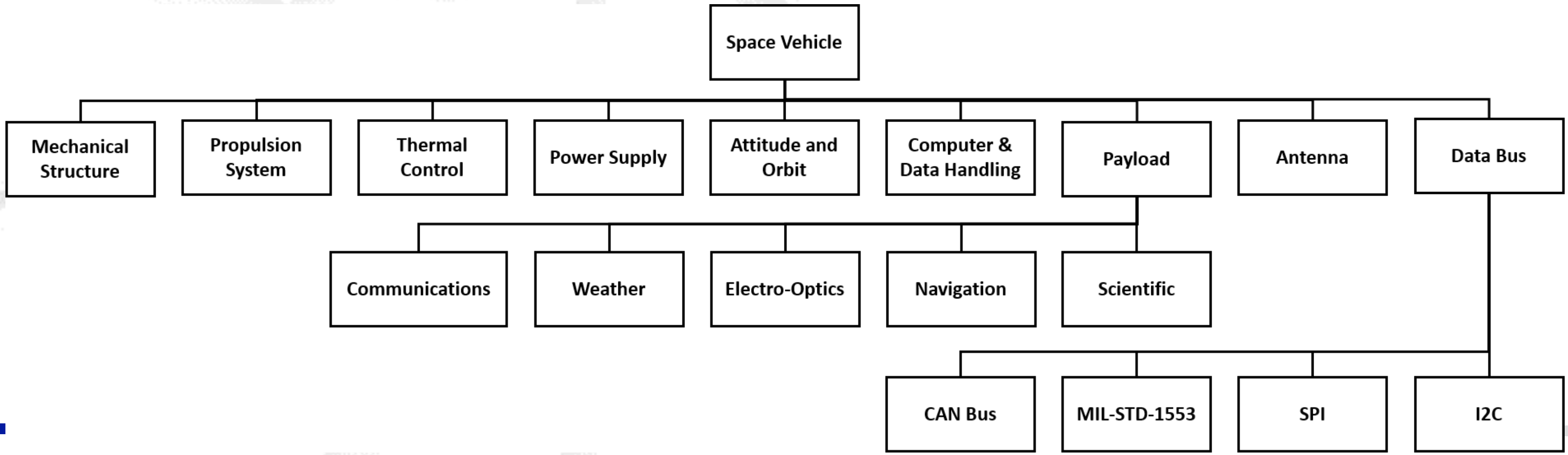
Legend
"●" indicates a strong positive relationship
"o" indicates a weak positive relationship
"–" indicates a conflicting relationship
"X" indicates a relationship that could be either positive or negative

		Security Strategies				Structural Security Principles																	
		Access Control	Defense in Depth	Isolation	Cyber Resiliency	Clear Abstractions	Least Common Mechanism	Modularity and Layering	Ordered Dependencies (Partially)	Efficiently Mediated Access	Minimized Sharing	Reduced Complexity	Secure Evolvability	Trusted Components	Hierarchical Trust	Commensurate Protection	Hierarchical Protection	Minimize Trusted Components	Least Privilege	Proportional Permissions	Self-Reliance	Secure Composition	Trusted Communication
Security Strategies	Access Control			●	●	Intentionally left blank																	
	Defense in Depth			o	●																		
	Isolation	●			●																		
	Cyber Resiliency		●																				
Structural Security Principles	Clear Abstractions	●	o	●			●	o	o	●	●	●	●	o	o	o	o	●	●	o	o	o	o
	Least Common Mechanism	●		●	X			o	X	o	–	●	●		o			●	o				
	Modularity and Layering	●	●	●	●		o		●	●	o	●	●					o				o	
	Ordered Dependencies (Partially)			o				●				●			●		●						
	Efficiently Mediated Access	●		●			●	o			●	●											
	Minimized Sharing	●	o	●	o		–	●	●			●	o					o					
	Reduced Complexity	●	–	X	X	o	o	●	●	●	●		●	●	o	●	●	●	●	o	●	●	●
	Secure Evolvability	–	o	o	●	o	●	●	●	●	●	o		o	o	o	o	●	o	o	o	o	o
	Trusted Components		●		o			o	o						●	●	o					●	
	Hierarchical Trust	●	o		o				●							●	●						
	Commensurate Protection	●	●	o	●										●		o	–	o	o	●	o	●
	Hierarchical Protection	●	o	o	●			o													o		
	Minimize Trusted Components	o	–	o	●		●	o		●	●	●	o									o	o
	Least Privilege	●		●	●					o	●	o	o	●				●		o	●		
	Proportional Permissions	●	o	–	X							●	o										
	Self-Reliance			●	X	o	●	●		●	●	●											
	Secure Composition	o	●	–		o	–	o	●	o	●	–	X	●	●	●	●	●	●	●	●		
	Trusted Communication	●	o	●	o	o		o		●	o		o	●	●							●	

Cyber Resiliency Measures

- How to specify and measure cyber resiliency?
  - Largely an open question
  - Some network-based research available

- Cyber Resiliency Appendix to NIST SP 800-160 to understand
- NIST Cyber-Physical Systems Working Group to apply
- Leverage the Unified Architectural Framework (UAF) to study

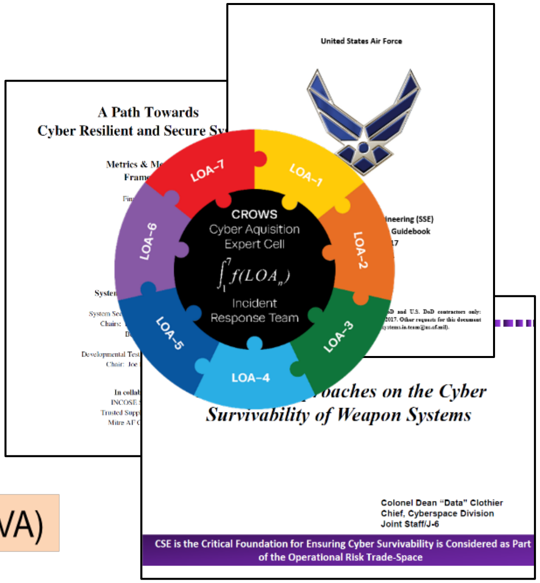


Conclusion

The AFIT of Today is the Air Force of Tomorrow.

<u>GOAL: Engineer Secure and Resilient Cyber-Physical Systems</u>

1. Criteria, Observables, Behaviors
   - What does Cyber Resiliency look like?
2. Requirements, Cost, Measures & Metrics
   - How to specify and measure Cyber Resiliency?
3. Acquisition Language, Design Standards
   - How to execute and implement Cyber Resiliency?



Business Analysis (BA)

Stakeholder Needs (SN)

System Requirements (SR)

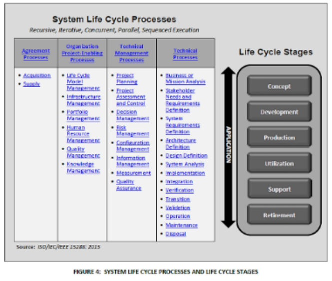
Architecture Definition (AR)

Design Definition (DE)

Validation (VA)

Verification (VE)

System Analysis (SA)



Backup Slides

STPA-Sec Conclusion

Define & Frame Problem

Identify Unacceptable Losses

Identify System Hazards/Constraints

Create Functional Control Structure

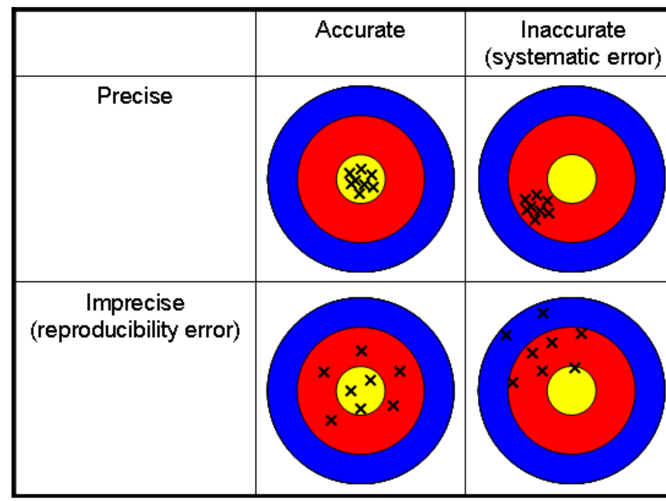
Identify Hazardous Control Actions

Generate Causal Scenarios

Mitigations and Controls

- **Must think carefully about the security problem**
  - **Perfectly solving the wrong security problem doesn't really help**
  - **Consider accuracy vs. precision**

- **STPA-Sec provides a means to clearly link security to the broader mission objectives**

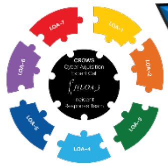


- **STPA-Sec does not replace systems security engineering methods, but enhances their effectiveness**

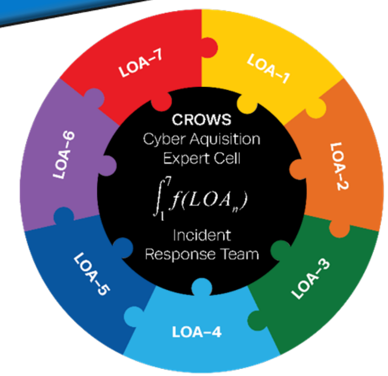
Adapted with permission from Col/Dr. William "Dollar" Young's STPA-Sec For Security Engineering Analysis Tutorial: Warning contains copyrighted material

Roadmap to Resiliency

Present



Future



Mission Assurance

- Mission Thread Analysis

- Develop assessment methodology framework
- Develop cyber acquisition workforce

System Assurance

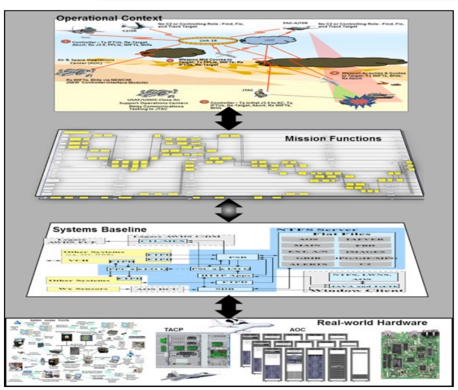
- Assess and Fix

- Assess cyber posture of fielded systems
- Enable weapon system adaptability

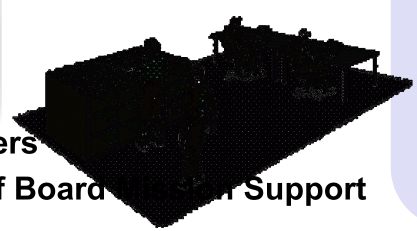
Institutionalize

- "Baked" in resiliency

- Institutionalized methodology, tools, T&E infrastructure
- Skilled workforce
- Integrated cyber tools, policy, etc.



Mx and Aircrew Trainers



Off Board [illegible] Support

DISTRIBUTION A. Approved for public release: distribution unlimited.

Why NIST SP 800-160?

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is:

- To provide a basis to formalize a discipline for systems security engineering in terms of its principles, concepts, and activities;
- To foster a common mindset to deliver security for any system, regardless of its scope, size, complexity, or stage of the system life cycle;
- To provide considerations and to demonstrate how systems security engineering principles, concepts, and activities can be effectively applied to systems engineering activities;
- To advance the field of systems security engineering by promulgating it as a discipline that can be applied and studied; and
- To serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

System Life Cycle Processes

Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

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

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

Life Cycle Stages

FIGURE 4: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Application Example: Cyber-Physical

- SCADA Security Policy, developed by Sandia National Laboratories
  - Creation of SCADA security policies
  - Ensure coverage of critical areas
  - Develop customized policies for specific operations

TABLE 5. **Priority scheme for the framework for scada security policy.**

SCADA Security Policy Framework	Compliance	People	System Resiliency	Operations	Physical and Environmental	Asset Management	Interconnectivity
Data Security						X	X
Platform Security				X	X	X	
Communication Security				X			X
Personnel Security		X			X		
Configuration Management	X					X	
Audit	X	X					
Applications			X	X		X	
Physical Security					X		
Manual Operations		X	X				
Sum	**2**	**3**	**2**	**3**	**3**	**4**	**2**

Khou, S., Mailloux, L., Pecarina, J. M., & McEvilley, M. A. (2017). System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts. *IEEE Access*.

Application Example: Cyber-Physical

- SCADA Security Polic atories
  - Creation of SCADA
  - Ensure coverage of
  - Develop customized

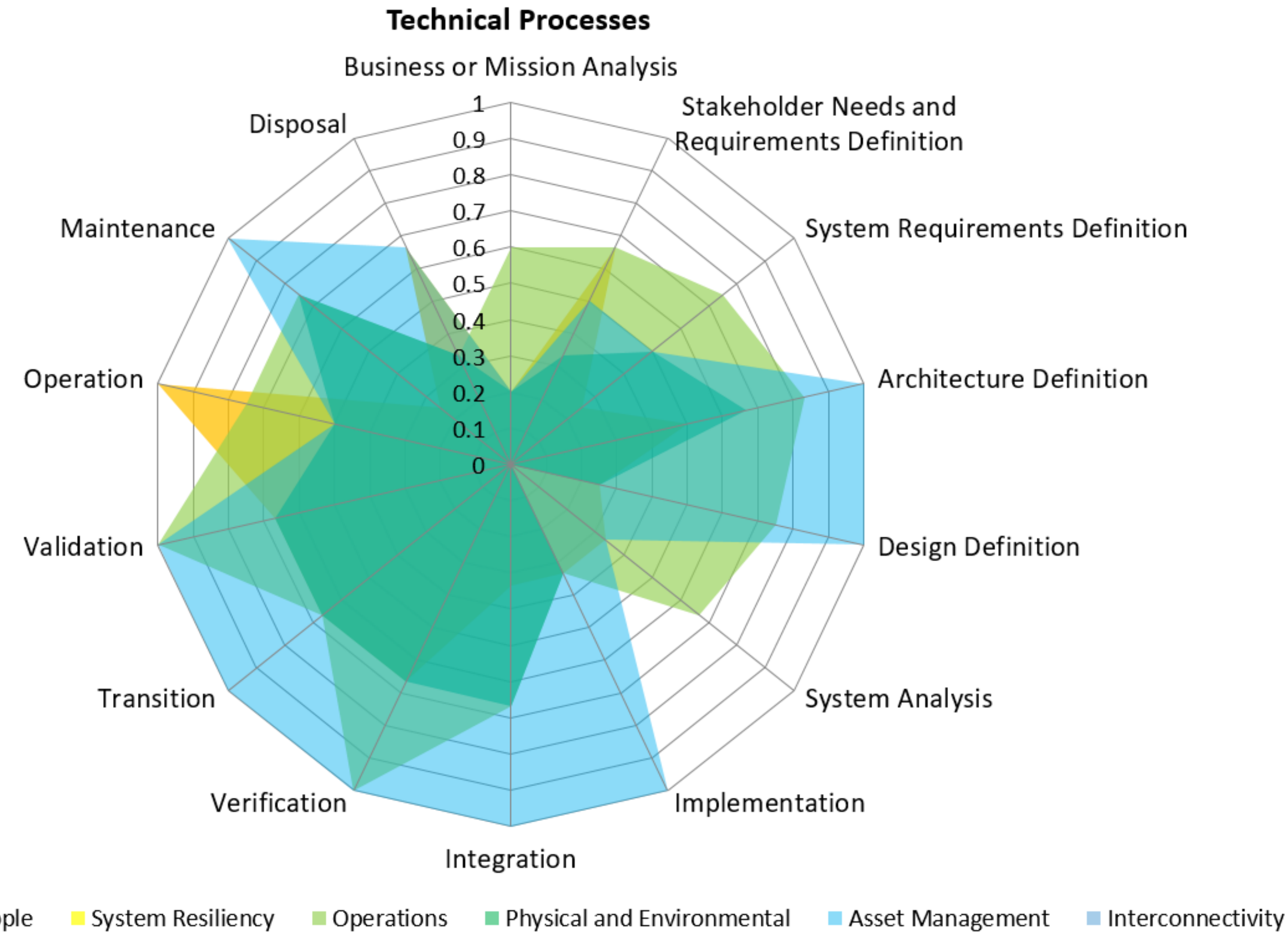
But I'm interested in these too!

TABLE 5. Priority scheme for the framework for scada security policy.

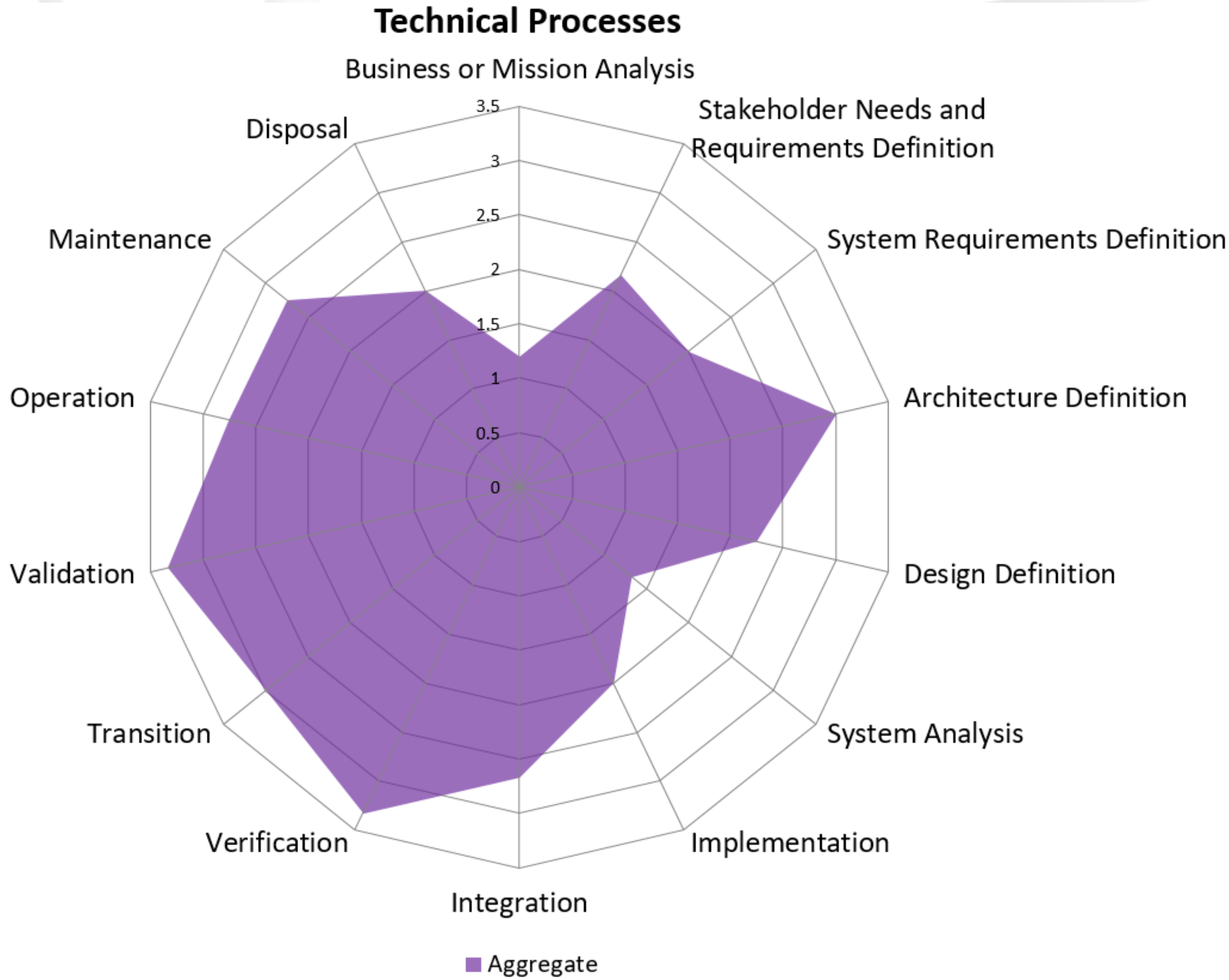
SCADA Security Policy Framework	Compliance	People	System Resiliency	Operations	Physical and Environmental	Asset Management	Interconnectivity
Data Security						X	X
Platform Security				X	X	X	
Communication Security				X			X
Personnel Security		X			X		
Configuration Management	X					X	
Audit	X	X					
Applications			X	X		X	
Physical Security					X		
Manual Operations		X	X				
Sum	**2**	**3**	**2**	**3**	**3**	**4**	**2**

Khou, S., Mailloux, L., Pecarina, J. M., & McEvilley, M. A. (2017). System-Agnostic Security Domains for Understanding and Prioritizing Systems Security Engineering Efforts. *IEEE Access*.

Application Example: Cyber-Physical



Application Example: Cyber-Physical



NIST SP 800-160
Three Chapters + Appendices

The AFIT of Today is the Air Force of Tomorrow.

CHAPTER 1 Introduction: 7 pages
- Develop a basis to formalize SSE discipline and mindset
- Consider and demonstrate how SSE can be applied to SE processes

CHAPTER 2 The Fundamentals: 15 pages
- Ensure appropriate security principles, concepts, methods, and practices are applied
- Perform security analyses with the appropriate fidelity and rigor to substantiate adequate security claims

CHAPTER 3 SSE Processes, Activities, and Tasks: 128 pages

14 Technical Processes (54 Activities, 232 Tasks)

8 Technical Management Processes (29 Activities, 116 Tasks)

6 Organizational Project-Enabling Processes (18 Activities, 57 Tasks)

2 Agreement Processes (10 Activities, 23 Tasks)

Appendices (Guides To Fundamental Knowledge): 100+ pages
- Systems Security Activities and Tasks
- Roles, Responsibilities, and Skills
- Design Principles for Security
- Engineering and Security Fundamentals
- System Resiliency
- Security Requirements and Considerations
- Hardware Security and Assurance
- Software Security and Assurance
- System Security Analyses
- Risk Management Framework

Management Activities

- Project Planning
- Project Assessment and Control
- Decision Management

. . .

- Configuration Management
- Information Management
- Measurement
- Quality Assurance

Detailed SSE Management Tasks

- Prepare for security quality assurance
- Perform product or service security evaluations
- Perform process security evaluations
- Manage quality assurance security records and reports
- Treat security incidents and problems

L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST SP 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.

NIST SP 800-160
Overview and Fundamentals

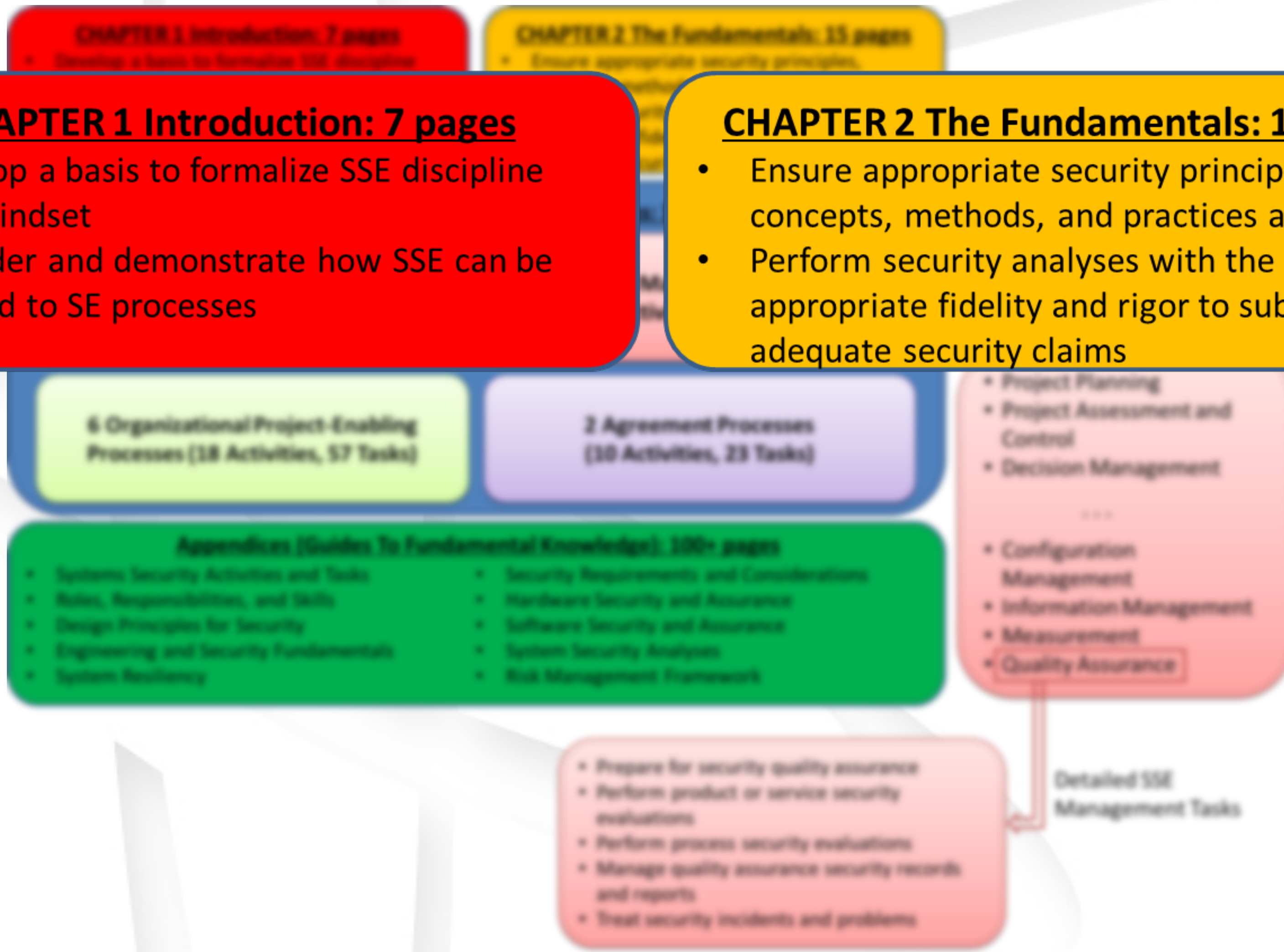
The AFIT of Today is the Air Force of Tomorrow.

CHAPTER 1 Introduction: 7 pages

- Develop a basis to formalize SSE discipline and mindset
- Consider and demonstrate how SSE can be applied to SE processes

CHAPTER 2 The Fundamentals: 15 pages

- Ensure appropriate security principles, concepts, methods, and practices are applied
- Perform security analyses with the appropriate fidelity and rigor to substantiate adequate security claims



L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST SP 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.

NIST SP 800-160
SSE Processes

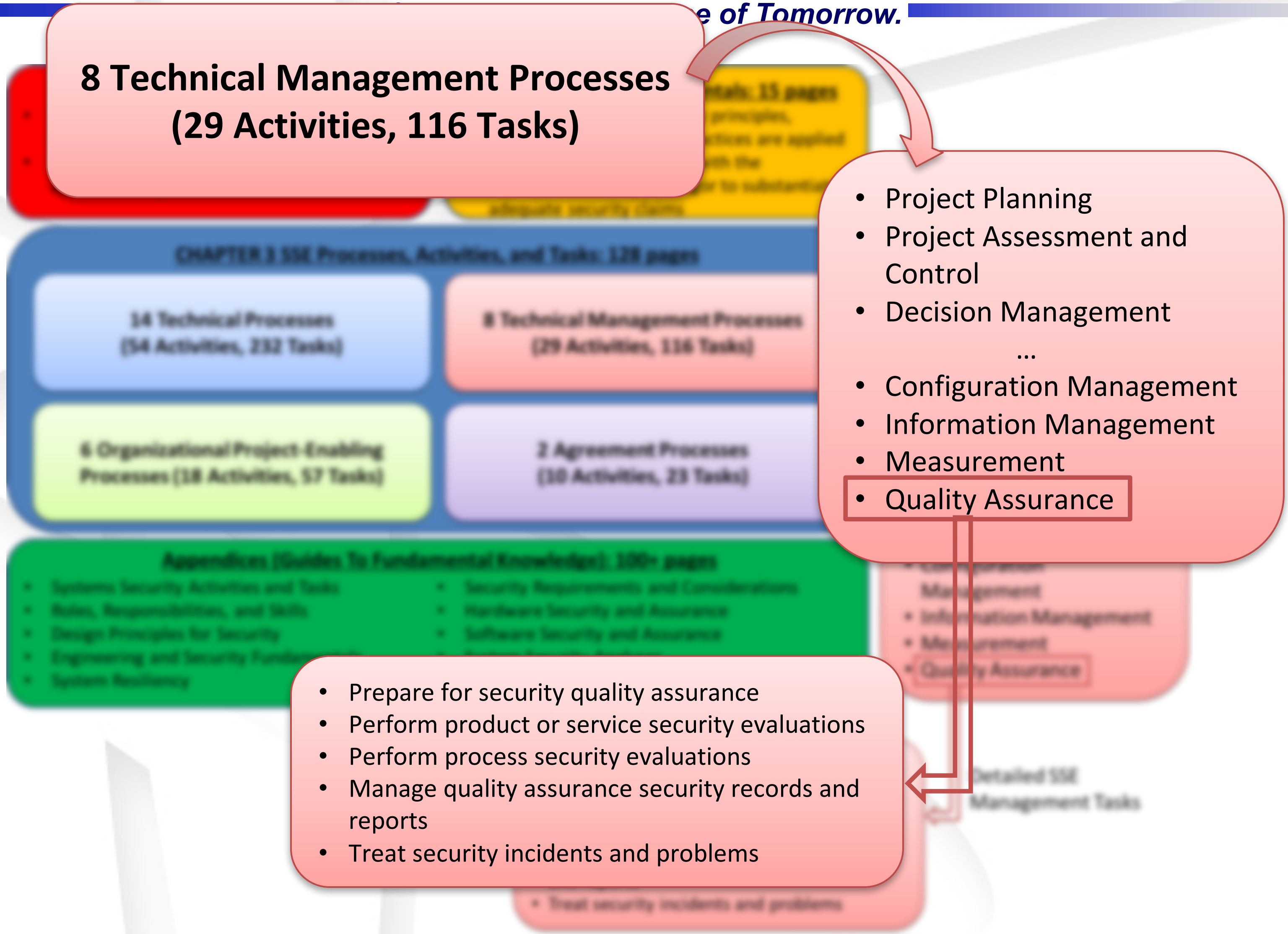
The AFIT of Today is the Air Force of Tomorrow.

<u>CHAPTER 3 SSE Processes, Activities, and Tasks: 128 pages</u>

14 Technical Processes (54 Activities, 232 Tasks)	8 Technical Management Processes (29 Activities, 116 Tasks)
6 Organizational Project-Enabling Processes (18 Activities, 57 Tasks)	2 Agreement Processes (10 Activities, 23 Tasks)

L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST SP 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.

NIST SP 800-160
SSE Processes



L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST SP 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.

NIST SP 800-160 Guidance

The AFIT of Today is the Air Force of Tomorrow.

Appendices (Guides To Fundamental Knowledge): 100+ pages

- Systems Security Activities and Tasks
- Roles, Responsibilities, and Skills
- Design Principles for Security
- Engineering and Security Fundamentals
- System Resiliency
- Security Requirements and Considerations
- Hardware Security and Assurance
- Software Security and Assurance
- System Security Analyses
- Risk Management Framework

L. O. Mailloux, M. A. McEvilley, S. Khou and J. M. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST SP 800-160," IEEE Security & Privacy, vol. 14, no. 4, pp. 76-80, 2016.