Overview of the Afternoon

Session 1 (2:30 – 3:30) : STPA-Sec Overview – STPA within Secure Systems Engineering (and Cyber Security)

- **Introduction**
- **Observations on Cybersecurity today**
- **System Thinking and Security**
- **STPA-Sec overview**
- **Summary and Conclusion**

Session 2 (3:30 – 5:00): STPA-Sec Practice

- **Overview**
- **Concept Analysis**
- **Architectural Analysis**
- **Design Analysis**
- **User Q&A**
- **Summary and Conclusion**

To Maximize the Available Time, I Will Assume Basic Familiarity With STAMP, STPA an Will Leverage John Thomas's Example from this Morning

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU




System-Theoretic Process Analysis for Security (STPA-SEC): Secure Systems Engineering, Cyber Security and STPA

William Young Jr, PhD

2019 STAMP Conference

Boston, MA

March 25, 2019

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Disclaimer:

The views expressed in this presentation are are those of the presenters and do not reflect the official policy or position of the United States Air Force, Department of Defense, Air Combat Command, MIT Lincoln Laboratory, Syracuse University, or the U.S. Government

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Introduction

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Introduction

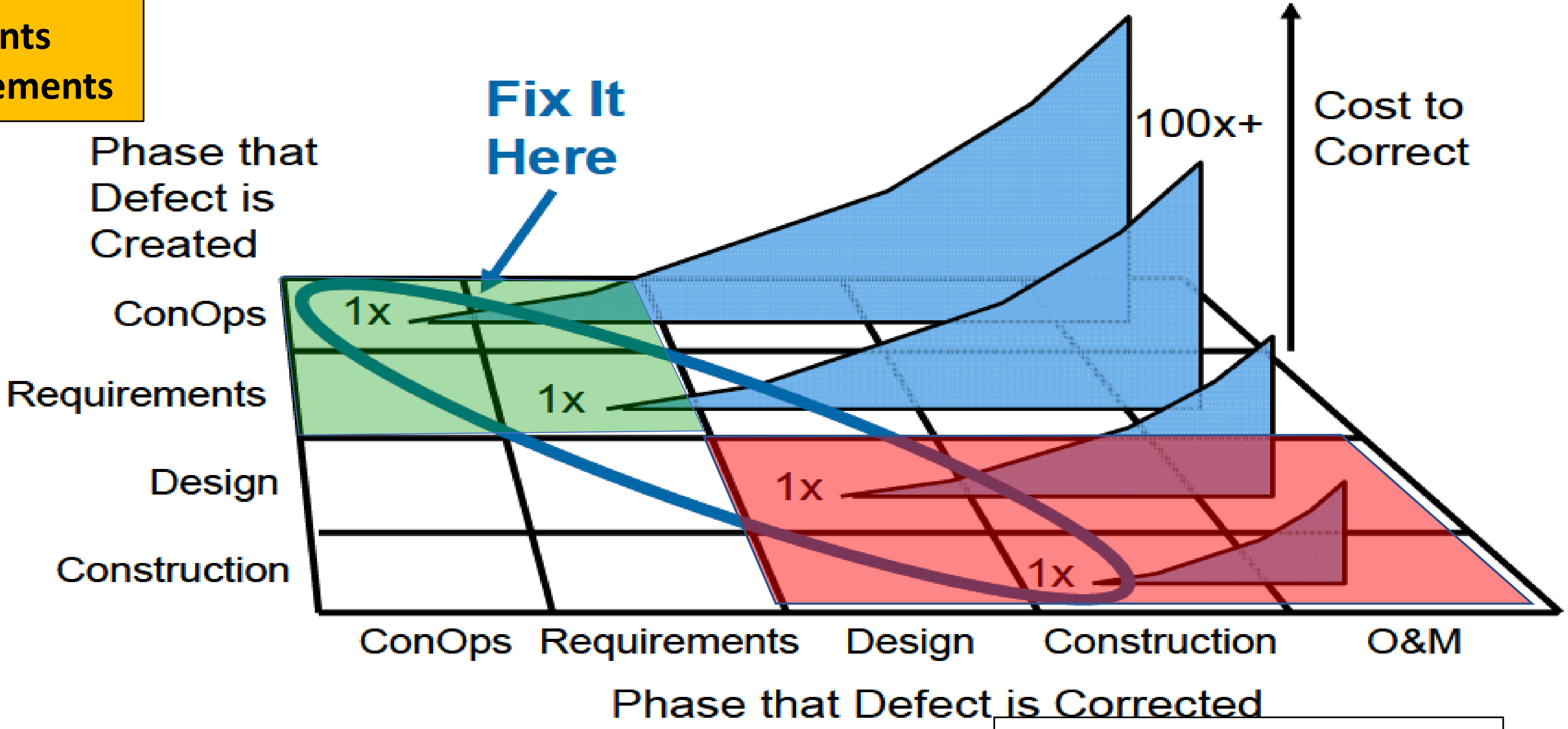
- **Losses are growing and current approaches to securing complex, software intense, designed physical systems do not appear to be working as well as desired**
- **Origins of losses fall into at least one of two categories:**
  - **Disruption prevents engineered system from fulfilling its designed purpose**
  - **Disruption does not necessarily prevent the engineered system from fulfilling its primary purpose, but it produces an unacceptable "by-product"**
- **The side with individuals best able to conceptualize the most creative ways to exploit device/designed system functionality has competitive advantage (tactics)**

Today, Security is Viewed Almost Universally as a Threat Problem

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Flawed logic
Conflicting goals
Poor Assumptions
Wrong Problem
Missing requirements
Incomplete requirements

Introduction



Design = Secure System Engineering
Construction = Secure System Development
O & M = Protect Data and IT Components

Ref: System Engineering For Intelligent Transportation Systems

Current Approaches Do Not Address Safety & Security Errors that lead to Losses When it is Most Effective and Cheapest to Do So

Observations on Cybersecurity Today

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Threat Based Approach to Developing a “Secure” Architecture

Threat Modeling

↓

Security Policy / Requirements

↓

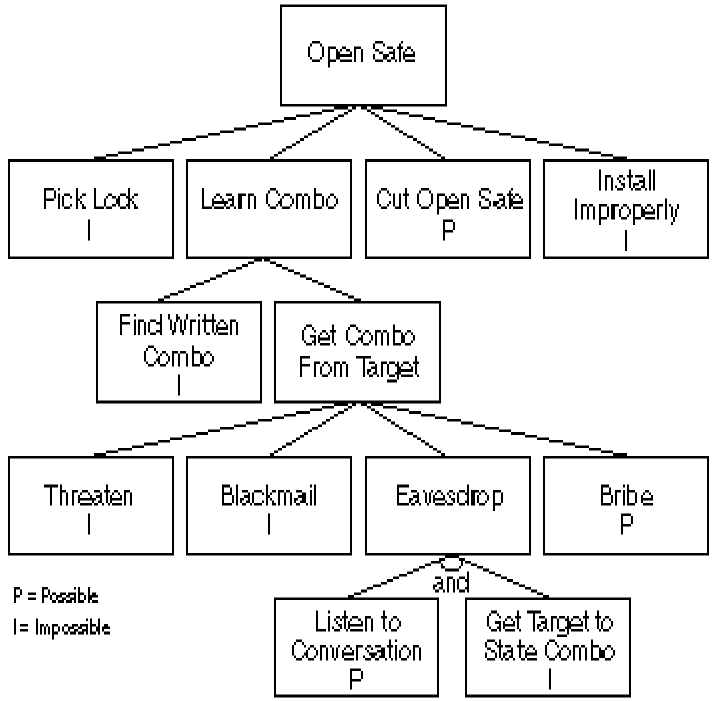
Select Security Mechanism / Controls

Current Security Analysis Depends on Identifying the Right Threat (Tactics), But Does Not Help Address the Larger Mission Assurance Goal (Strategy)

Ref: (Anderson, 2010; Shostack, 2014; Swiderski & Snyder, 2004)

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Schneier's Attack Tree Model is the Intellectual Foundation of Most Thinking on Cybersecurity

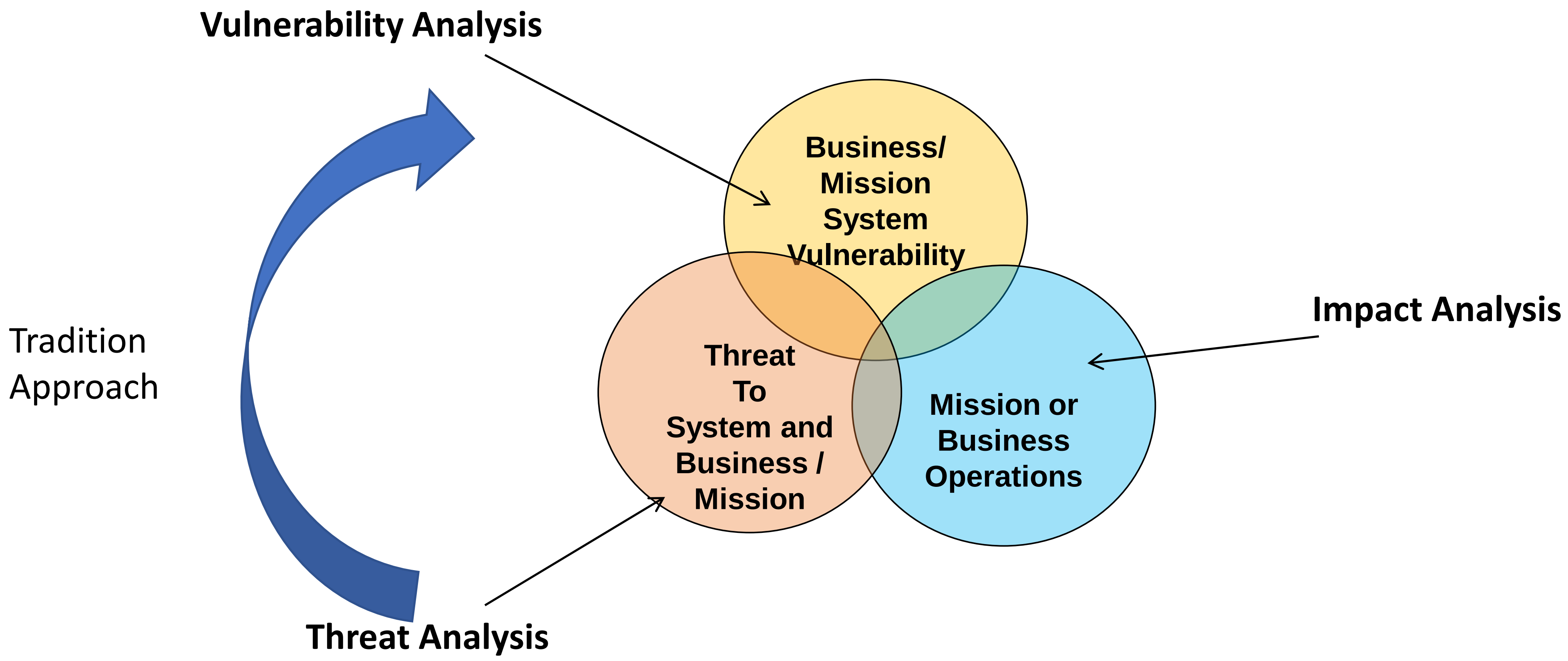


"Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks…Security is not a product -- it's a process. Attack trees form the basis of understanding that process."

Schneier Based His Security Attack Trees on Fault Trees He Saw Used for Safety

Ref; *Dr. Dobb's Journal*, December 1999

Cybersecurity Through Today's Analytic Lenses



The System Vulnerabilities are Driven by Threat Capability

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Current Security Analysis

"When you ask an engineer to make your boat go faster, you get the trade-space. You can get a bigger engine but give up some space in the bunk next to the engine room. You can change the hull shape, but that will affect your draw. You can give up some weight, but that will affect your stability. When you ask an engineer to make your system more secure, they pull out a pad and pencil and start making lists of bolt-on technology, then they tell you how much it is going to cost."

- Prof Barry Horowitz, UVA

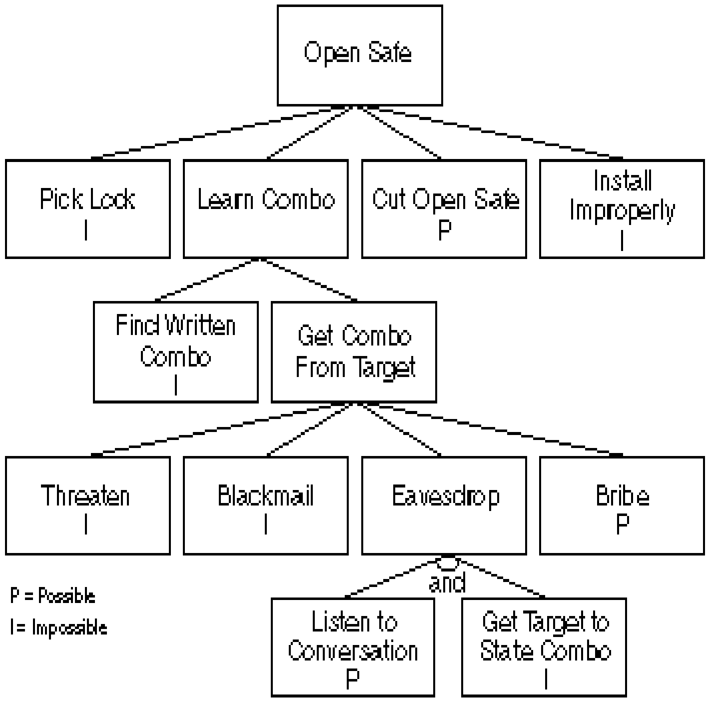
What We Need to Get to

“The first thing we need in this process is the ability to state computer security requirements clearly and precisely… so that a competent professional can study it for a reasonably short amount of time and, say, "Oh, yes, I agree. If you build that particular system to that particular requirement, it's secure enough for that particular purpose.”

- Donald Good "The Foundations of Computer Security, We Need Some"

SYSTEM THINKING & SECURITY

Relooking Schneier's Words

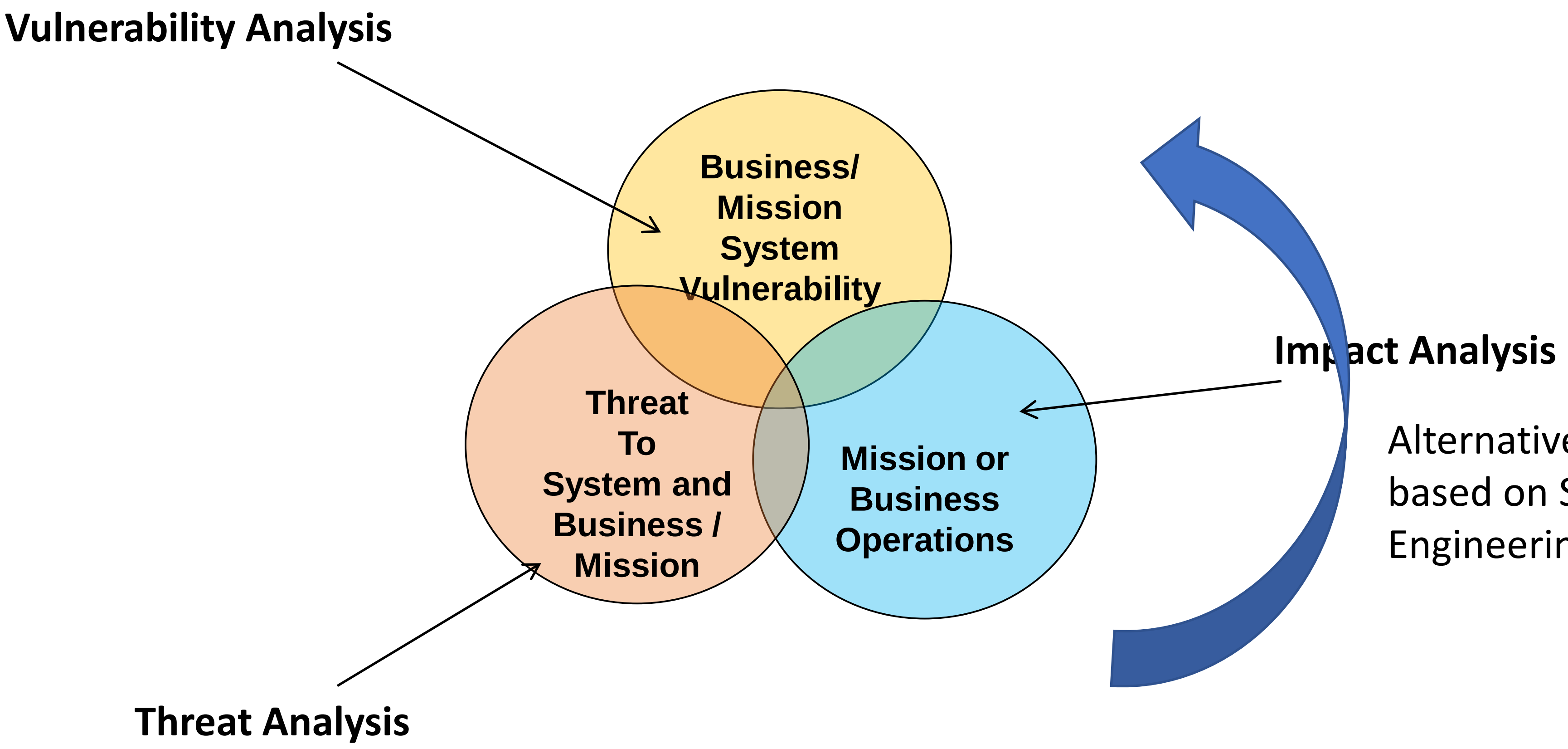


"Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks…Security is not a product -- it's a process. STPA-Sec will form the basis of understanding that process."

STAMP and STPA-SEC Provide us a Different Way to Understand (and Control) the Security Process

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Cyber Security Through Different Analytic Lenses



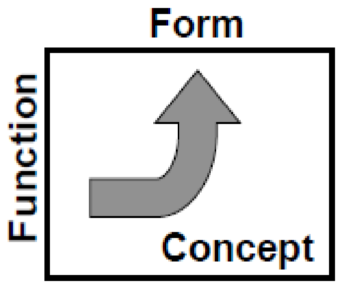
Alternative Approach based on Systems Engineering

In Systems Engineering, Threats are Just One of Many Trades

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

New Approach: Secure Form Simply Realizes Secure Function

- “Form follows function” is a central tenant of system engineering and architecture
- Generate secure Business & Mission Systems by first defining the secure functionality to be realized
- Get to security via
  - Identify functionality required to solve the problem at hand (But we must understand problem)
  - Implement all required functionality securely based on understanding problem and context
- Architecture Defined (Crawley)
  - The embodiment of concept, and the allocation of physical/informational function to elements of form, and definition of interfaces among the elements and with the surrounding context

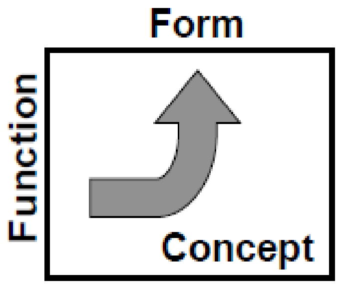


From Security Defined by Threat to Security Defined in Terms of Delivering Secure Functionality Necessary for Mission or Business Operations

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

New Approach: Secure Form Simply Realizes Secure Function

- “Form follows function” is a central tenant of system engineering and architecture
- Generate secure Business & Mission Systems by first defining the secure functionality to be realized
- Get to security via
  - Identify functionality required to solve the problem at hand (But we must understand problem)
  - Implement all required functionality securely based on understanding problem and context
- Architecture Defined (Crawley)
  - The embodiment of concept, and the allocation of physical/informational function to elements of form, and definition of interfaces among the elements and with the surrounding context



We Can Use STAMP Model to Help Craft the Security Concept

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

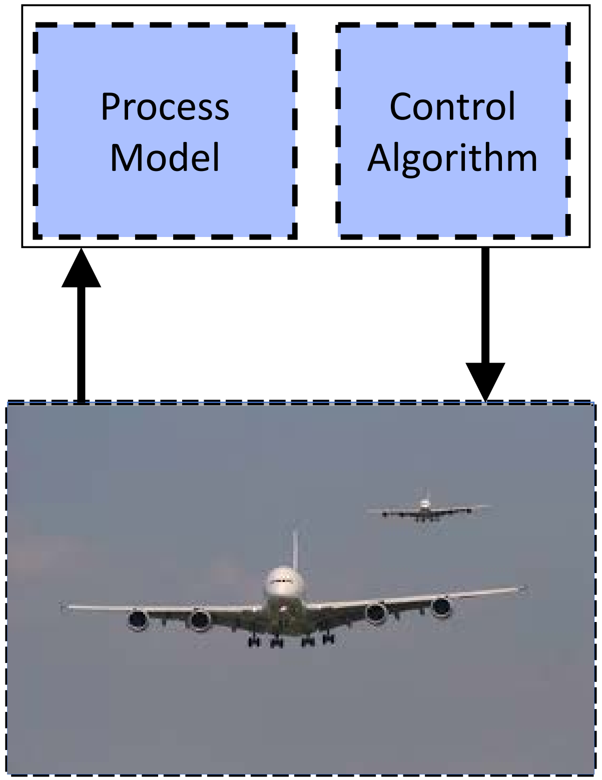
STAMP Model & Security

- **Focuses on function, not threat to guide realization (form)**
  - **Separates problem space from solution**
  - **Allows us to reason about function (and critique a proposed functional decomposition based on security related concerns)**
- **Provides a means to define and specify secure function clearly, unambiguously, and in context of the mission**
- **Functional Control Structure is simply a means to help envision how the necessary functionality can be implemented in a way that prevents losses identified**

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

"Security" Losses Can Be Reframed as (Functionality) Control Problems

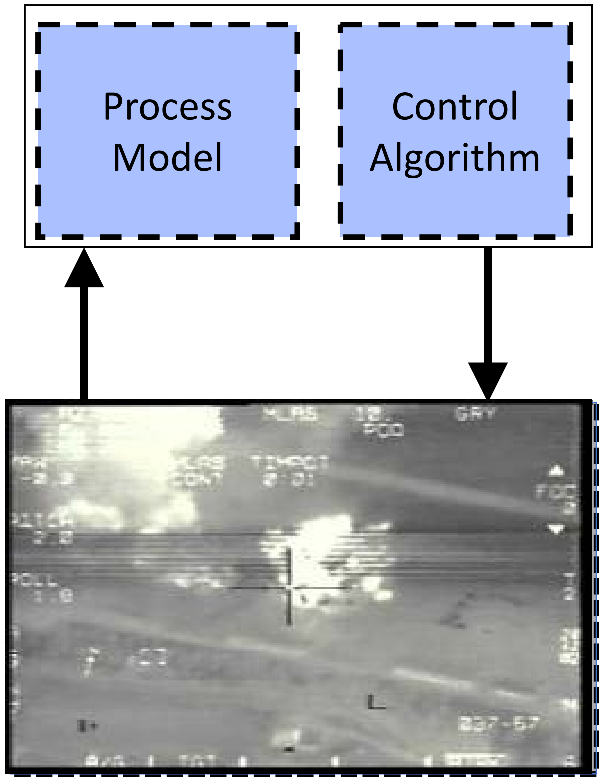
Cause a Mid Air Collision



Aircraft must maintain minimum safe separation

ENFORCE: Safe Separation

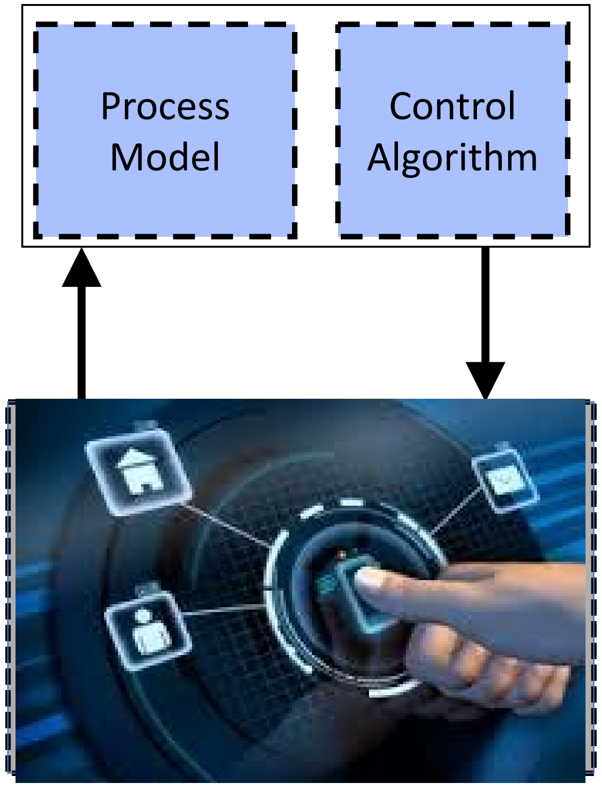
Cause Friendly Fire Loss



Only hostile forces must be engaged

ENFORCE: Engagement Rules

Steal Customer PII



PII must only be exposed to authorized entities

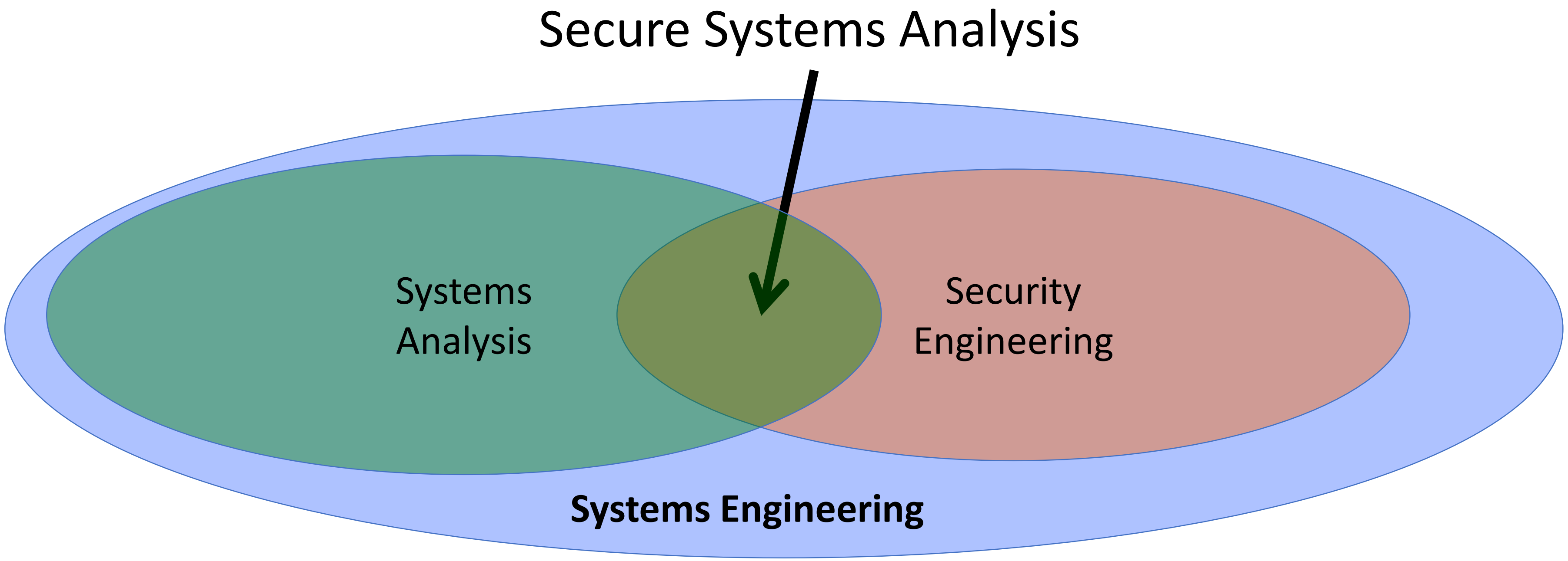
ENFORCE: Data Access Policy

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

From Systems Analysis to Secure Systems Analysis

"A systematic examination of a problem of choice in which each step of the analysis is made explicit wherever possible."

Malcom W. Hoag, "An Introduction to Systems Analysis" RAND Research Memorandum, RM-1678, 18 April 1956



STPA-Sec Allows the Systems Analysis Framework to be Applied to Security

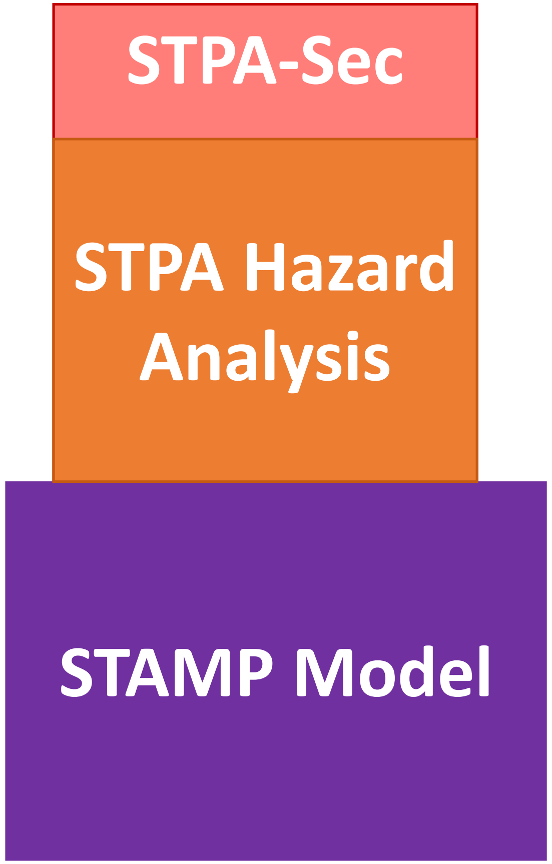
William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

STPA-Sec

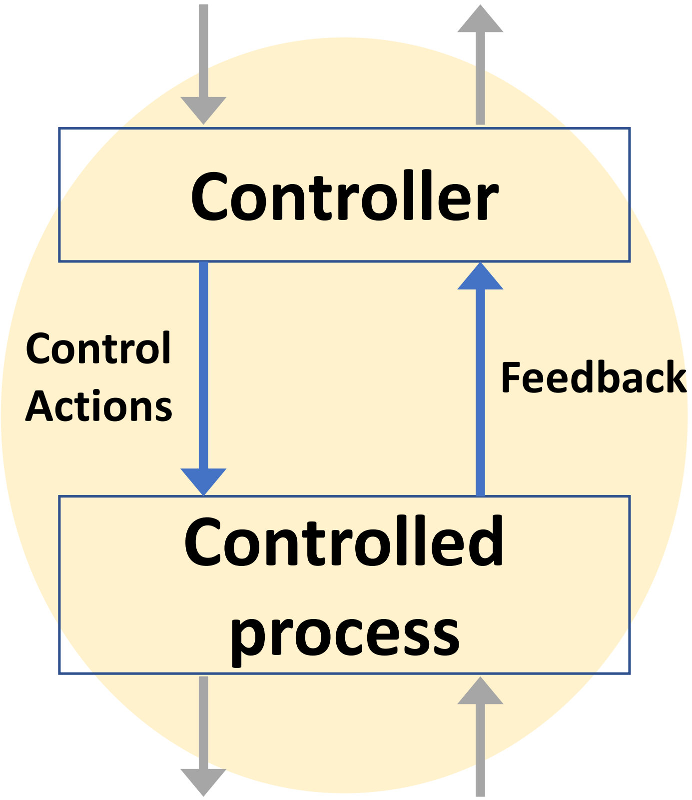
- **Analysis process to generate a security concept and framework**
- **Examines a functional process through a security lens to gain insights and craft artifacts to enable additional reasoning**
- **Threats are just another environmental hindrance to function**
  - **In fact, the threats themselves don't really matter…it's the functional disruption they can deliver**
  - **We can engineer our systems to handle the most important functional disruptions**
- **Analysis methodology supports learning and facilitates stakeholder debates and trades (can imagine "what might be")**

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

STPA-Sec Extends STPA



- Synthesize (frame) the security problem
- Define purpose of the analysis
- Model the Control Structure
- Identify unsafe/unsecure control actions
- Step 2: Identify loss scenarios
- Wargame



Security-related material or techniques

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Summary and Conclusion

- **Security engineering and underlying systems thinking offers an alternative to address the challenge and bring strategy to bear**
- **Growing realization that security engineering must begin <u>before</u> architecture development…but we need a Security Engineering Analysis methodology**
  - **All analysis is based on models, so we require a model of how losses occur**
  - **Default model today is "threats cause our security-related losses" (but we <u>don't</u> generally get to control the threats)**
- **STPA-Sec applies the STAMP model to provide a methodology to place security within a systems engineering context**
  - **Define "secure" functionality**
  - **Guide the development of an architecture to realize the functionality**
  - **We <u>DO</u> get to control our systems engineering**

We Must Ensure That We Are Defining and Solving the Right (Engineering) Problem

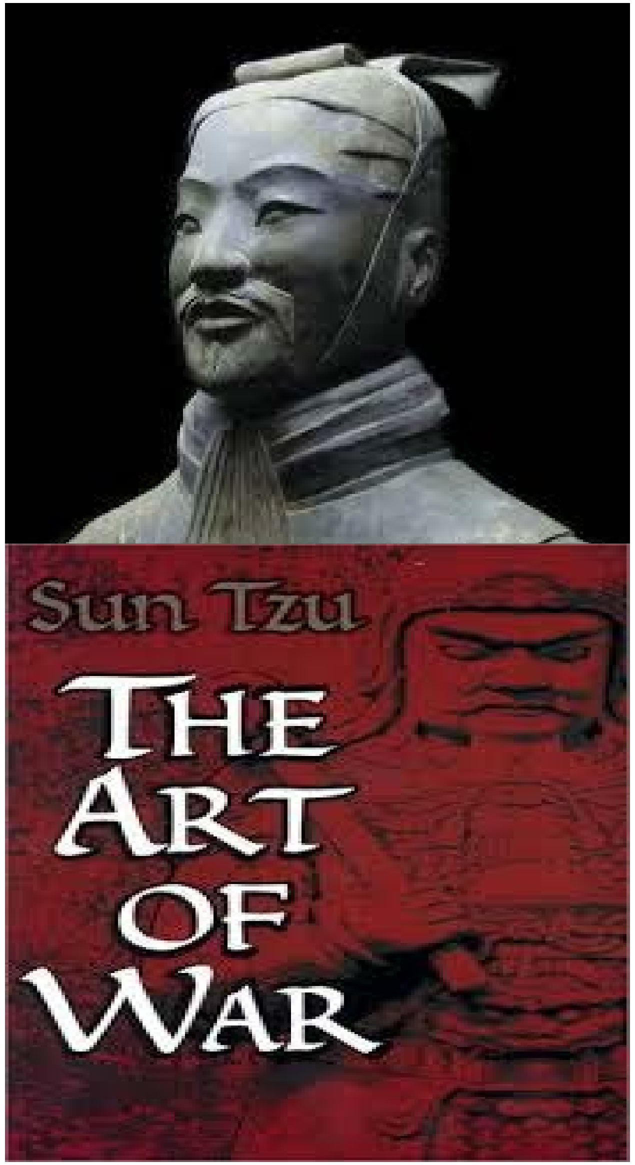
William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Concluding Thoughts from Sun Tzu

The opportunity to secure ourselves against defeat lies in our own hands.

The supreme art of war is to subdue the enemy without fighting.

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.



My Contact Information

WYOUNG@MIT.EDU – Personal Email

William.Young.3@US.AF.Mil – Government Email (for 6 more months)




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

William Young Jr, PhD

2019 STAMP Conference
Boston, MA

March 25, 2019

Disclaimer:

The views expressed in this presentation are are those of the presenters and do not reflect the official policy or position of the United States Air Force, Department of Defense, Air Combat Command, MIT Lincoln Laboratory, Syracuse University, or the U.S. Government

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Overview of the Practice Session

<u>Session 2 (3:30 – 5:00)</u>: STPA-Sec Practice

- **STPA-Sec for Security Engineering Analysis**
- **Concept Analysis**
- **Architectural Analysis**
- **Design Analysis**
- **User Q&A**
- **Summary and Conclusion**

To Maximize the Available Time, I Will Assume Basic Familiarity With STAMP, STPA an Will Leverage John Thomas's Example from this Morning

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Rules of Engagement

- Extends aspects of Dr John Thomas's morning STPA tutorial
  - Won't cover the things he discussed
  - Will Identify security-related differences and additions
  - Will offer my techniques in a few areas
- Generally follows STPA Handbook guidelines
- Available time won't allow for deep dive, but will have time over the next two days to discuss and answer detailed questions
- This is notional example and greatly simplified to fit within the time allotted
- Brevity prevents replication of the group learning that normally occurs
- Can't simulate the iterative nature and the rich conversations that occur
- I want to save time at the end to address specific user questions encountered during real-world applications

We are Summarizing 40+ Hours of Instruction into 90 Minutes…We Will Only Hit Wavetops

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

STPA-Sec For Security Engineering Analysis

Satellite System Example Based on John Thomas Example Used in Earlier STPA Tutorial (Used With Dr Thomas' Permission) and the Paper "A Top Down Approach for Eliciting Systems Security Requirements for a Notional Satellite System" by Mailoux, Span, Mills and Young

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Ends

Problem Framework – Concept Analysis
- Goal / Purpose
- Unacceptable Losses
- Hazards
- High Level Constraints

→ Initial Security Requirements

Analysis / Synthesis
(Refine & Iterate)

Ways

Intent
Increasing Detail
(Requirements)

Functional Framework – Architectural Analysis
- Model Elements
- Responsibilities
- Functional Control Structure
- Control Actions
- Control Action Analysis Table (Step 1)

→ Security Constraints & Restraints

Analysis / Synthesis
(Refine & Iterate)

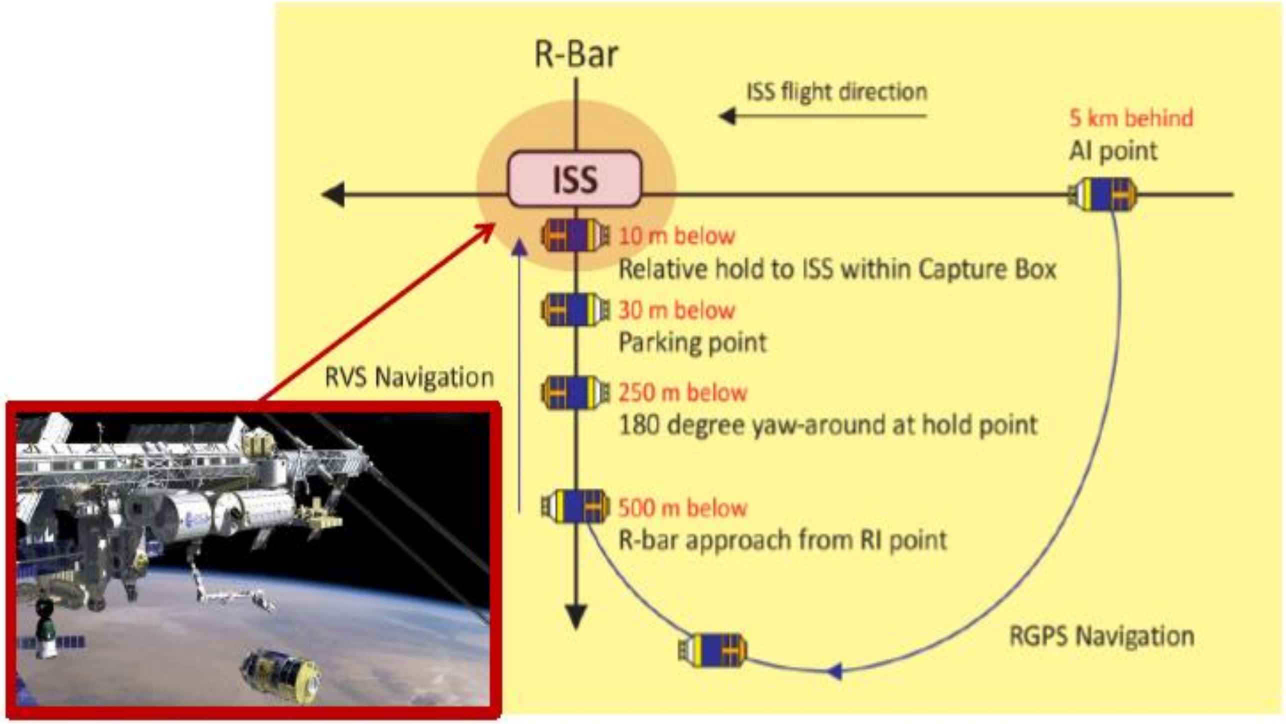
Means

Enterprise Architecture – Design Analysis
- Process Model Descriptions
- Process Model Variables (PMVs)
- PMV Values
- PMV Feedback
- Causal Scenarios (Adversary, Accident, Nature)
- War Gaming

→ Security Specifications

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Notional Spacecraft Through a Security Lens



From John Thomas' Example this Morning

- **Unmanned cargo transfer spacecraft**
- **Launched aboard rocket**
- **Rendezvous with International Space Station (ISS)**
- **Docks with ISS to deliver supplies**
- **Undocks and Returns to Earth**

Additional Factors

- **Proximity operations involve ISS (including crew), and ground stations**
- **Spacecraft employs proprietary software that company has invested significant IRAD to develop and patent**
- **System is commercially owned, operated, and maintained**
- **Company is liable for damage to supplies while enroute and for mission impact if supplies not delivered**

Additions to morning STPA Tutorial Scenario

Problem Framework: Concept Analysis

Determining Initial Security Requirements

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Concept Analysis Overview

STPA-Sec Concept Analysis.	
Step	**Description**
1. Define the System of Interest (SOI), SOI purpose and SOI goal*	Capture the mission statement and key activities of the system: 1) A system to: (What) 2) By Means of: (How) 3) In Order to: (Why) 4) While: (Bounds)
2. Identify unacceptable losses*	Define high level, intolerable system outcomes to key stakeholders (e.g., loss of life, injury, damage to equipment, reputation, mission, etc.).
3. Identify hazards	Identify system states that when coupled with worst case conditions lead to an unacceptable loss.
4. Develop system security constraints*	Develop mission-informed security constraints that prevent the system from entering hazardous states. These constraints are synonymous with early safety, security, and resiliency functional requirements.

* Security-related addition, modification, or technique

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Big Picture: Synthesize (Frame) Security Problem

- **Sets the foundation for the security analysis**
- **Must ID all relevant stakeholders**
- **Must understand how product / service fits into organizational strategy**
- **Surface key assumptions (and dependencies)**
- **Satisfies key aspects of Business or Mission Analysis (BMA) in ISO/IEEE/IEC 15288**
- **Examine required functionality from a security perspective**

"Many systems fail because their designers protect the wrong things, or protect the right things in the wrong way" – Ross Anderson in *Security Engineering*

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Define System Purpose and Goal

"A system to do {What = Purpose}

by means of {How = Method}

in order to contribute to {Why = Goals}

while {Constraints, Restraints}

Specify a gap between "as is" and "to be"

that will be addressed through a process (e.g. a transformation of some type)

Sidebar

The Story of "Bob"

Military parallel is Operational Design (applied Operational Art) as captured in Joint Pub 5-0

Iterative Process is Challenging, but Generates Rich Conversations in Practice (e.g. USAF MLV)

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Define System Purpose and Goal

<u>From John Thomas' Example this Morning</u>

- **Unmanned cargo transfer spacecraft**
- **Launched aboard rocket**
- **Rendezvous with International Space Station (ISS)**
- **Docks with ISS to deliver supplies**
- **Undocks and Returns to Earth**

<u>Additional Factors</u>

- **Proximity operations involve ISS (including crew), and ground stations**
- **Spacecraft employs proprietary software that company has invested significant IRAD to develop and patent**
- **System is commercially owned, operated, and maintained**
- **Company is liable for damage to supplies while enroute and for mission impact if supplies not delivered**

<u>Format</u>

"A system to do {What = Purpose}

by means of {How = Method}

in order to contribute to {Why = Goals}

while {constraints, restraints}

What Might Be a Possible Solution from the Spacecraft Example?

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft Example

"A system to do {What = Purpose}

by means of {How = Method}

in order to contribute to {Why = Goals}

while {constraints, restraints}"

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft Example– Potential Solution

A system to **autonomously resupply ISS**

by means of **launching, navigating, docking, and undocking a space vehicle**

in order to **support the ongoing ISS mission and research** while **maintaining profitable operations, minimizing risk to ISS/cargo, and improving the company's position and branding as a responsible world leader in space technology .**

This is one Solution, But There Others

Adapted from Dr Thomas' STPA Tutorial

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Adding Security-Related Unacceptable Losses

- **"Unacceptable Losses" and "Accidents" are the same thing**
- **Many of the security losses will overlap with safety accidents**
- **Security perspective may add nuance to a previous safety perspective**
- **Security perspective may also highlight important safety / security trades**
- **Focus on alternative "system" uses**
- **Focus on security concerns of non-traditional stakeholders**
- **Outcomes and final conditions, not failures**

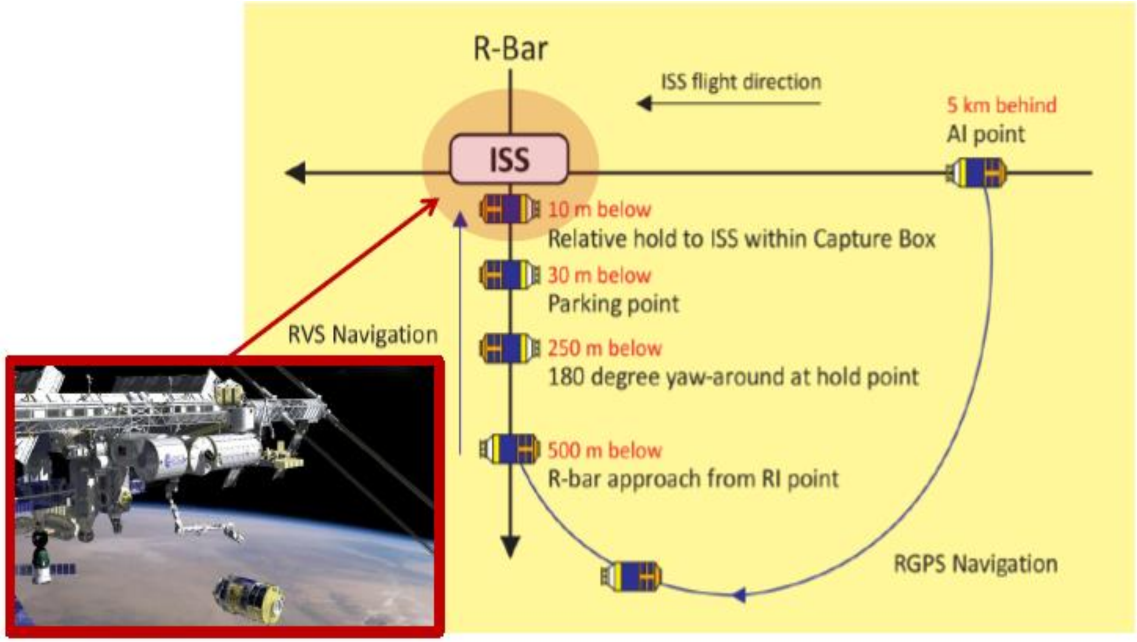
Simply Clarifying Unacceptable Losses May Provide a Significant Boost in Security Effectiveness!

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft Losses

- **Unacceptable Losses (From Earlier Today)**
- A-1: HTV collides with ISS
- A-2: Loss of delivery mission

- **Unacceptable Losses (Modified From Earlier Today)**
- L-1: Loss of Vehicle or ISS
- L-2: Significant Damage to ISS or Vehicle
- L-3: Loss of Resupply Payload

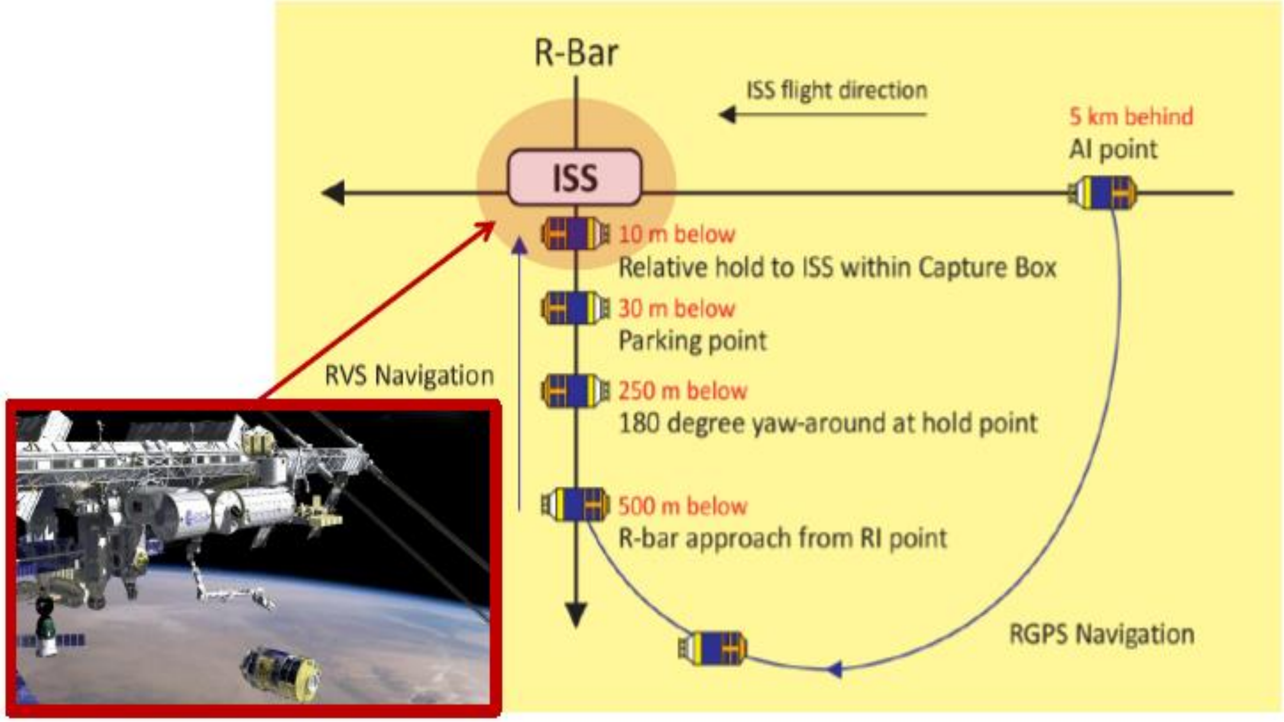


Are these Safety or Security-Related Losses?

Spacecraft Unacceptable Losses

Unacceptable Losses

- L-1: Loss of Vehicle or ISS
- L-2: Significant Damage to ISS or Vehicle
- L-3: Loss of Resupply Payload



Are there other unacceptable losses Related to Security? (Take a Few Minutes to Discuss)

 William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Expanded (Security-related) Spacecraft Unacceptable Losses

Unacceptable Losses

- L-1: Loss of Vehicle or ISS
- L-2: Significant Damage to ISS or Vehicle
- L-3: Loss of Resupply Payload
- **L-4: Loss of Reputation**
- **L-5: Loss of Intellectual Property**

A system to **autonomously resupply ISS**

by means of **launching, navigating, docking, and undocking a space vehicle**

in order to **support the ongoing ISS mission and research** while **maintaining profitable operations, minimizing risk to ISS/cargo, and improving the company's position and branding as a responsible world leader in space technology.**

Are there other unacceptable losses Related to Security? (Take a Few Minutes to Discuss)

 William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Expanded Spacecraft Unacceptable Losses

- **Unacceptable Losses**
- L-1: Loss of Vehicle or ISS
- L-2: Significant Damage to ISS or Vehicle
- L-3: Loss of Resupply Payload
- **L-4: Loss of Reputation**
- **L-5: Loss of Intellectual Property**

A system to **autonomously resupply ISS**

by means of **launching, navigating, docking, and undocking a space vehicle**

in order to **support the ongoing ISS mission and research** while **maintaining profitable operations, minimizing risk to ISS/astronauts/cargo,** and **improving the company's position and branding as a responsible world leader in space technology .**

Tip: The "Why" and "While" provide insights to guide Unacceptable Losses

Unacceptable Losses Are Traceable back to the Problem Statement

Using "How" Verbs to Help Identify System Level Hazards

Losses \ Verbs	Launch	Navigate	Dock	Undock
L1: Loss of Vehicle or ISS				
L2: Significant Damage to ISS or Vehicle				
L3: Loss of Resupply Payload				
L4: Loss of Reputation				
L5: Loss of Intellectual Property				

1 — High-level Functionality that is Required to Accomplish Goal

2 — Unacceptable Losses that Must be Avoided

Must Control "1" sufficiently to accomplish mission while not causing "2" (NOTE: This is true regardless of architecture!)

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Using “How” Verbs to Help Identify System Level Hazards

Verbs / Losses	Launch	Navigate	Dock	Undock
L1: Loss of Vehicle or ISS				
L2: Significant Damage to ISS or Vehicle				
L3: Loss of Resupply Payload				
L4: Loss of Reputation				
L5: Loss of Intellectual Property				

We can use the *functional relationship* to gain insight into our Hazards (“A **condition with the potential** to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or **mission degradation**.”[DoD])

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Using "How" Verbs to Help Identify System Level Hazards

Losses \ Verbs	Launch	Navigate	Dock	Undock
L1: Loss of Vehicle or ISS	Improper launch functionality may place vehicle in unrecoverable orbit	Navigation to wrong point or at wrong time can lead to loss of vehicle	Excessive closure during docking can cause damage to ISS or ship	Inadvertent undocking may compromise vehicle or ISS
L2: Significant Damage to ISS or Vehicle	Excessive launch forces may damage vehicle or cargo	Navigation through space radiation fields may damage vehicle	Excessive closure during docking can cause damage to ISS or ship	Inadvertent undocking may compromise vehicle or ISS
L3: Loss of Resupply Payload	Excessive forces during launch may damage payload	Excessive forces on payload during enroute portion	Docking attempted when ISS not ready or docking functionality applied when not docking	Undocking functionality applied before desired
L4: Loss of Reputation	Failed launch attempt or vehicle destruction	Losing vehicle enroute	Vehicle colliding with ISS when under control of company	Vehicle undocking with ISS when commanded
L5: Loss of Intellectual Property	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data

Using "How" Verbs to Help Identify System Level Hazards

Losses / Verbs	Launch	Navigate	Dock	Undock
L1: Loss of Vehicle or ISS	Improper launch functionality may place vehicle in unrecoverable orbit	Navigation to wrong point or at wrong time can lead to loss of vehicle	Excessive closure during docking can cause damage to ISS or ship	Inadvertent undocking may compromise vehicle or ISS
L2: Significant Damage to ISS or Vehicle	Excessive launch forces may damage vehicle or cargo	Navigation through space radiation fields may damage vehicle	Excessive closure during docking can cause damage to ISS or ship	Inadvertent undocking may compromise vehicle or ISS
L3: Loss of Resupply Payload	Excessive for… launch ma… payload		…when … g	Undocking functionality applied before desired
L4: Loss of Reputation	Failed launch … or vehicle destruction		…n ISS … control of company	Vehicle undocking with ISS when commanded
L5: Loss of Intellectual Property	**Monitored telemetry may reveal proprietary data**	**Monitored telemetry may reveal proprietary data**	**Monitored telemetry may reveal proprietary data**	**Monitored telemetry may reveal proprietary data**

Telemetry must be provided for remote operations. But it may also potentially disclose propriety data

Using "How" Verbs to Help Identify System Level Hazards

Losses \ Verbs	Launch	Navigate	Dock	Undock
L1: Loss of Vehicle or ISS	Improper launch functionality may place vehicle in unrecoverable orbit	Navigation to wrong point or at wrong time can lead to loss of vehicle	Excessive closure during docking can cause damage to ISS or ship	Inadvertent undocking may compromise vehicle or ISS
L2: Significant Damage to ISS or Vehicle	Excessive launch forces may damage vehicle or cargo	Navigation through space radiation fields may damage vehicle	**Excessive closure during docking can cause damage to ISS or ship**	Inadvertent undocking may compromise vehicle or ISS
L3: Loss of Resupply Payload	Excessive forces during launch may damage payload	Excess…		…ocking …applied …red
L4: Loss of Reputation	Failed launch attemp… or vehicle destruction			…king …en …nded
L5: Loss of Intellectual Property	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data	…telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data

Docking Maneuver (e.g. thrust) must be constrained within limits while vehicle is in close proximity to ISS

Identifying a Missing Verb

Verbs / Losses	Launch	Navigate	Dock	Undock
L1: Loss of Vehicle or ISS	Improper launch functionality may place vehicle in unrecoverable o	Navigation to wrong point or at wrong time	Excessive closure during docking can cause damage	Inadvertent undocking may compromise vehicle or ISS
L2: Significant Damage to ISS or Vehicle	Excessiv may ca			tent may
L3: Loss of Resupply Payload	pa			y ore ed
L4: Loss of Reputation	Failed lau or vehicle destru			le undocking with ISS when commanded
L5: Loss of Intellectual Property	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data	Monitored telemetry may reveal proprietary data

We can also use the matrix to help ID previously missed functionality

Identifying a Missing Verb

Verbs / Losses	Launch	Navigate	Dock	Undock	Maintain (environment)
L1: Loss of Vehicle or ISS					
L2: Significant Damage to ISS or Vehicle					
L3: Loss of Resupply Payload					
L4: Loss of Reputation					
L5: Loss of Intellectual Property					

L3 Highlights functionality that is required to achieve the goal and has an associated unacceptable loss, but no associated verb

Hazards

Hazard	Description	Worst Case Environment	Associated Losses
H2: Safe Closure Rate Between Space Vehicle and ISS exceeded	Commanded or uncommanded thrust provided in close proximity to ISS that takes vehicle out of safe closure parameters	ISS Crew or GSS crew does not detect deviation and/or is unable to take corrective actions to prevent a collision	L1, L2 , L3

What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss? (Just like this Morning's STPA Tutorial)

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Hazards to Losses Cross Walk

		Losses				
		L1: Loss of Vehicle or ISS	L-2: Significant Damage to ISS or Vehicle	L-3: Loss of Resupply Payload	L-4: Loss of Reputation	L-5: Loss of Intellectual Property
Hazards	**H1:** H1: Failure to Maintain Safe Separation between the Space Vehicle and the ISS	X	X	X	X	
	H2: Exceed Safe Closure Rate Between Space Vehicle and ISS	X	X	X		
	H3: Payload Environment not Maintained Within Operational Limits			X		
	H4: Launch parameter limits exceeded	X	X	X		
	H5: Proprietary data disclosed to unauthorized entity				X	X

Develop High-level System Security Constraints

Hazard	System Constraint
H1: H1: Failure to Maintain Safe Separation between the Space Vehicle and the ISS	
H2: Exceed Safe Closure Rate Between Space Vehicle and ISS	C2: System must maintain safe closure rate with ISS during docking and undocking
H3: Payload Environment not Maintained Within Operational Limits	
H4: Launch parameter limits exceeded	
H5: Proprietary data disclosed to unauthorized entity	

We Will Leverage ABORT functionality to Enforce this Constraint

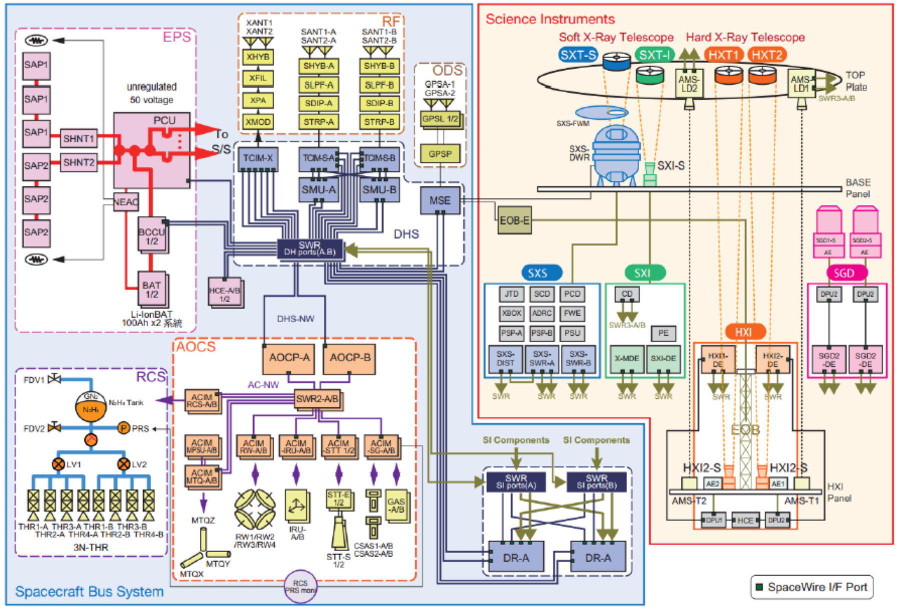
Functional Framework: Architectural Analysis

Developing Security Constraints and Restraints

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

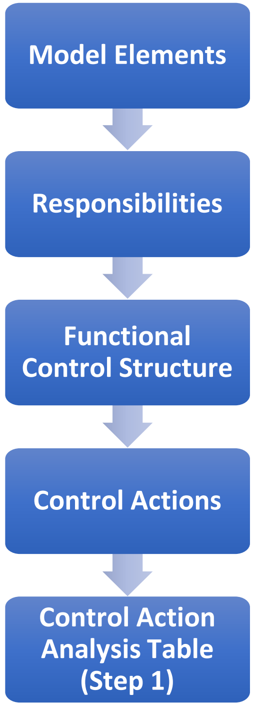
Spacecraft Example– Architectural Analysis Overview

Need Functional Equivalent



Adapted from Dr Thomas' STPA Tutorial William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

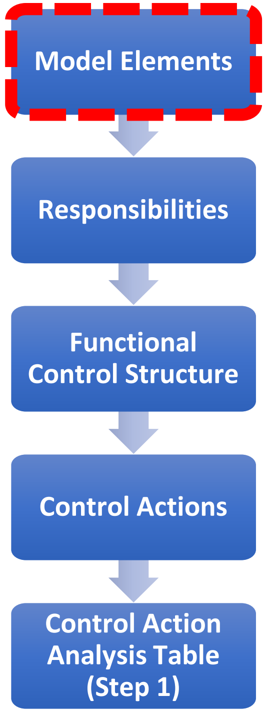
Architectural Analysis Overview



STPA-Sec Architectural Analysis.	
Step	**Description**
1. Identify model elements	Identify actor(s), controller(s), and controlled process(es) for the SoI at the desired level of abstraction.
2. Identify each elements' responsibilities	Capture the description and actions planned to be taken for the model elements identified.
3. Build Initial Functional Control Structure to Model control relationships	Organize the model elements to pictorial show the relationships between elements in a functional control structure.
4. Identify Control Actions (CA)	Captures (in verb form) the actions necessary for each element to execute their responsibilities.
5. Complete the CA analysis table	The CA analysis table systematically enumerates which hazards are caused by each CA identified in step 4.

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft– Model Elements



Problem Space (Function)

A system to **autonomously resupply ISS**

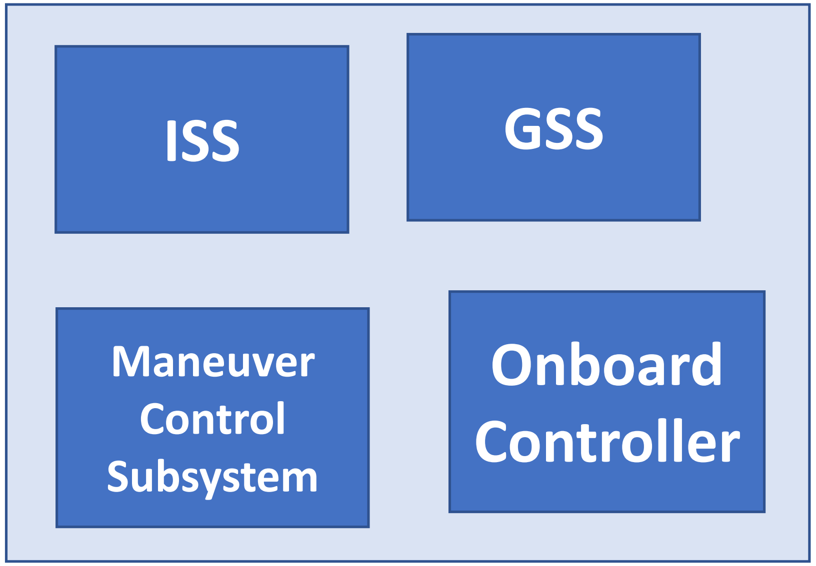
by means of **launching, navigating, docking, and undocking a space vehicle and maintaining cargo**

in order to **support the ongoing ISS mission and research**

while **preserving payload, maintaining cost effective operations, minimizing risk to the astronauts, and improving the organization's position and branding as a responsible community partner and world leader in technology .**

Developed in Initial Problem Framing

Solution Space (Form)



Entities are Specified and Implied in Initial Documentation (But must Parse)

Adapted from Dr Thomas' STPA Tutorial William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft– Model Elements

- **Model Elements**
- Responsibilities
- Functional Control Structure
- Control Actions
- Control Action Analysis Table (Step 1)

A system to **autonomously resupply ISS**

by means of **launching, navigating, docking, and undocking a space vehicle** and maintaining cargo

in order to **support the ongoing ISS mission and research**

while **preserving payloa... taining cost effective operations, minimizing risk to the a... uts, and improving the organization's position and branding ... sponsible community partner and ... der in technology .**

High-Lev Functio Act	Model Elemen	Description

Architectural Sketches (e.g. DoDAF)

INITIAL CAPABILITIES DOCUMENT

Our Example Problem will focus on analyzing the statement: "System will be capable of ABORTING docking maneuver if unsafe conditions arise"

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

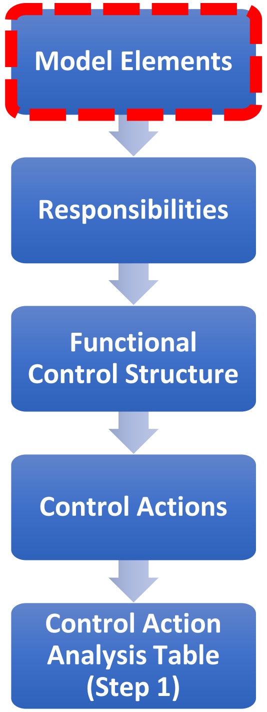
Entity Activity Diagram

Verbs / Entity	Launch	Navigate	Dock	Undock	Maintain (environment)
ISS Segment					
GSS Segment					
Onboard Vehicle Control System					
Maneuver Subsystem					
Environmental control subsystem					
Other Subsystems					

Identify data (Parse) documents and place specified and implied responsibilities for the entities inside the various boxes

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft– Model Elements

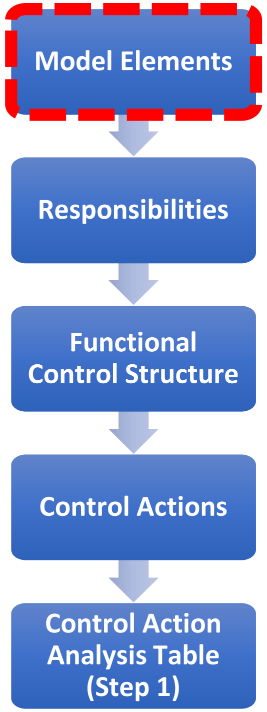


High-Level Functional Activity	Model Elements	Description
Dock	ISS	ISS be capable of commanding an ABORT if unsafe conditions arise during docking
Dock	GSS	GSS be capable of commanding an ABORT if unsafe conditions arise during docking
Dock	Onboard Control System	**?**

Do we Expect the Spacecraft to be capable of internally (OCS) directed ABORT? (Implied Functionality ?)

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

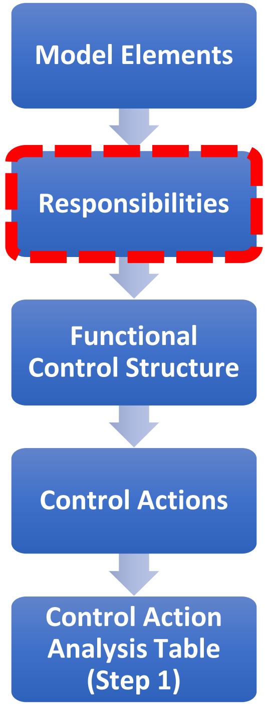
Spacecraft– Model Elements



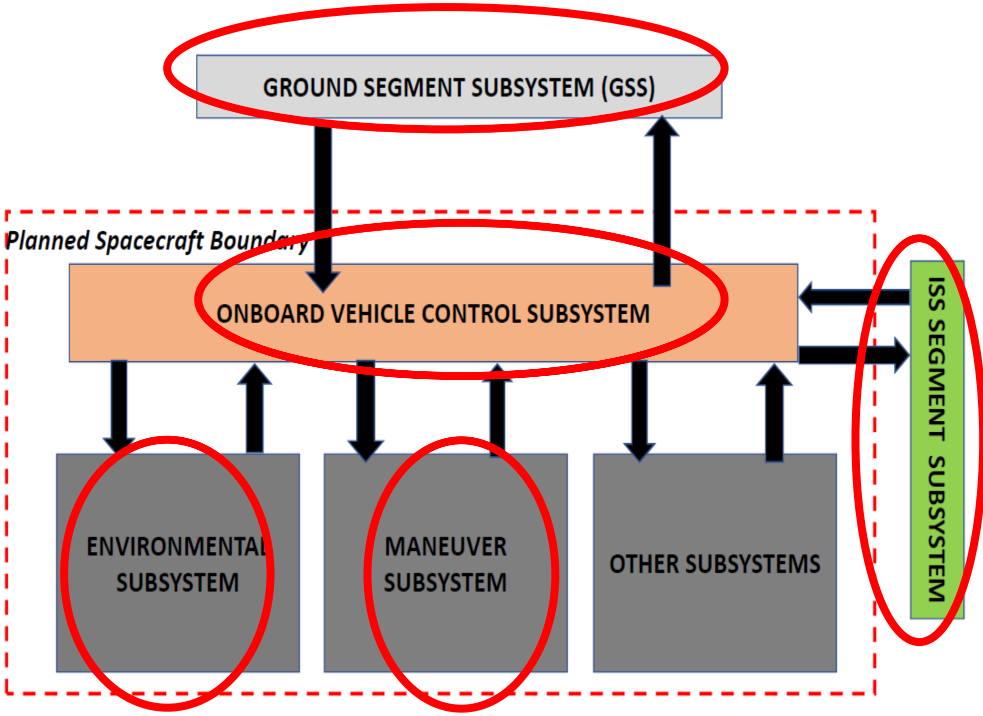
High-Level Functional Activity	Model Elements	Description
Dock	ISS	GSS be capable of commanding an ABORT if unsafe conditions arise during docking
Dock	GSS	GSS be capable of commanding an ABORT if unsafe conditions arise during docking
Dock	Onboard Control System	**OCS** receive (encrypted) ABORT when issued by ISS or GSS, decrypt (if required), terminate unsafe maneuver, command Attitude Control System to return vehicle to a safe distance from ISS and safe operational parameters. OCS will be capable of automatically sensing and commanding the Attitude Control System to ABORT docking maneuver if unsafe conditions arise during docking

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft– Responsibilities



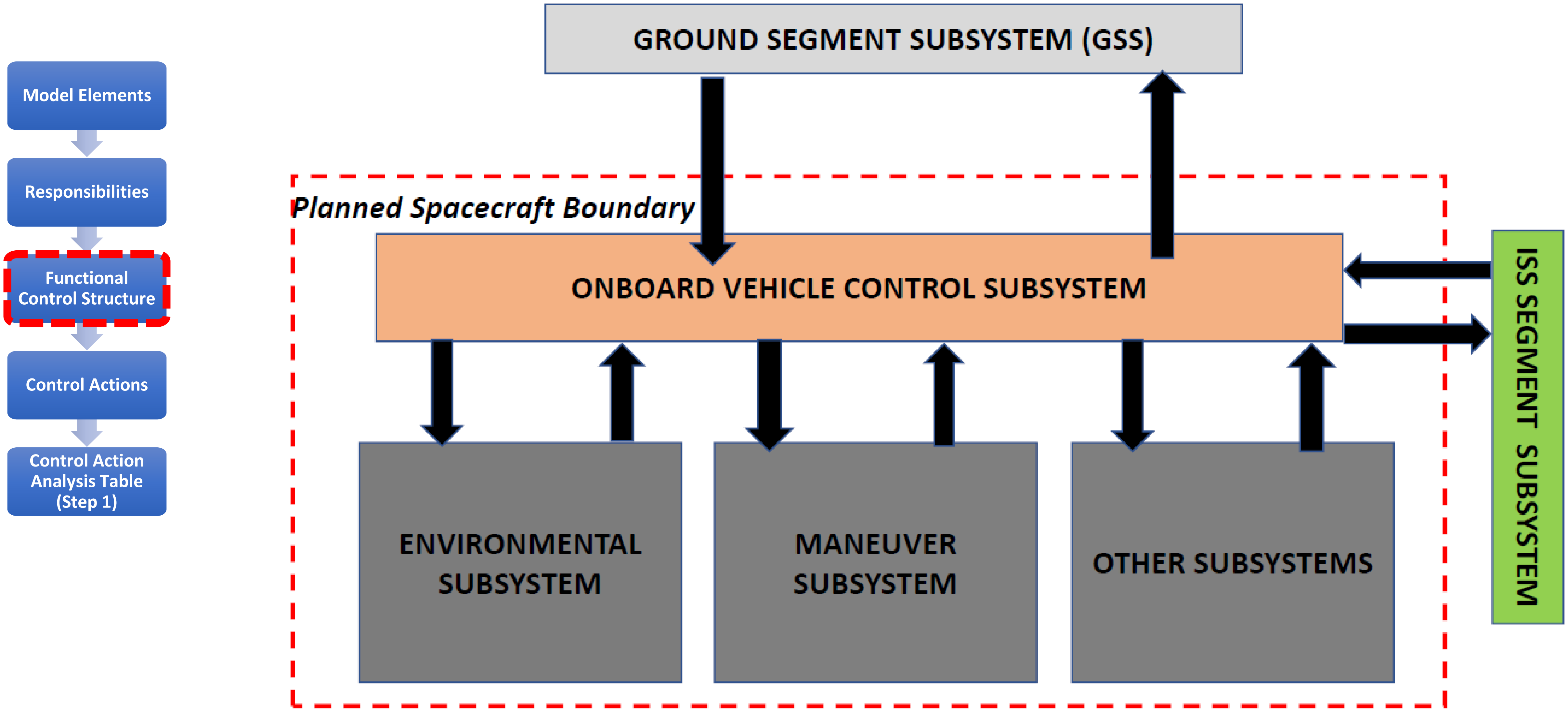
Key Activity: Docking	
Element	**Responsibility Description**
Ground Segment	• Initiate process • Send ABORT signal (encrypt?) • Monitor progress
ISS Segment	• Monitor progress • Manually Intervene if required
Onboard Control System	• Receive ABORT signal • Command ABORT to ACS • Command ABORT if required and not otherwise commanded • Decrypt?
Maneuver Subsystem	
Environmental Subsystem	



Adapted from Dr Thomas' STPA Tutorial

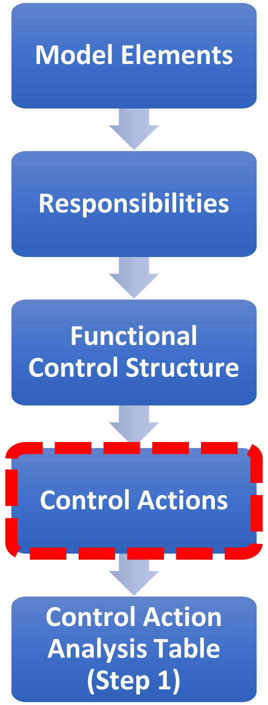
William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

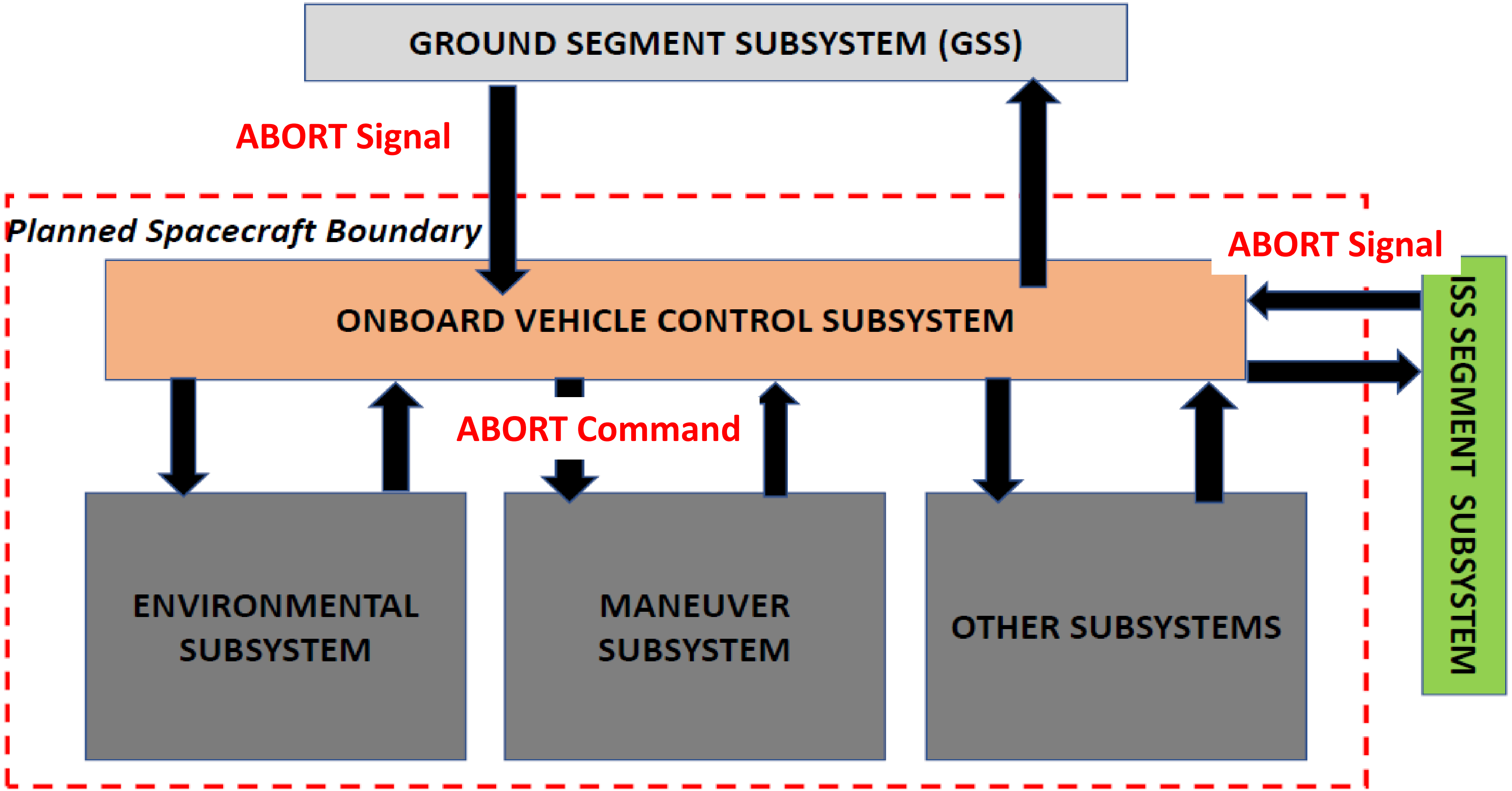
Spacecraft– Control Structure



 William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft– HCAs (Unsafe / Unsecure)

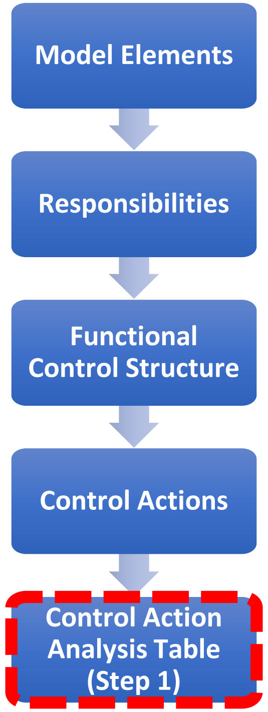




HCA - Hazardous Control Action

Adapted from Dr Thomas' STPA Tutorial William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Spacecraft– HCAs (Unsafe / Unsecure)



Control Action	Not providing causes hazard	Providing causes hazard	Incorrect Timing or Order	Stopped too soon or applied too long
CA1: ABORT	OCS not providing ABORT command is hazardous when spacecraft closure is outside planned parameters in close proximity to ISS [H-1, H-2]	OCS providing ABORT command is hazardous when command places vehicle outside safe operating envelope [H-1, H-2]	OCS providing ABORT command too late is hazardous when corrective measures allow insufficient time to prevent collision [H-1, H-2]	OCS providing ABORT command for too short a period is hazardous when corrections are not applied long enough to prevent collision [H-1, H-2]

HCA - Hazardous Control Action

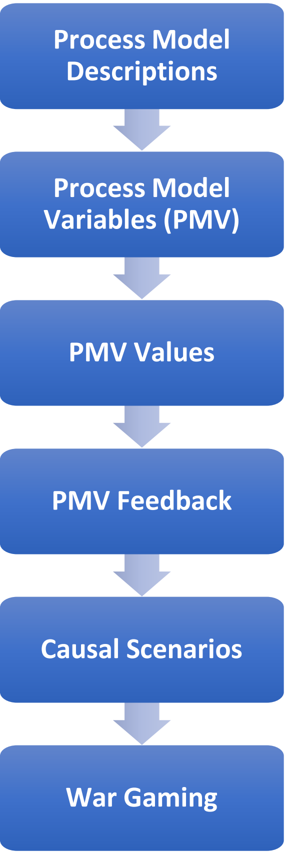
 William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Enterprise Architecture: Design Analysis

Establishing Initial Security Specifications

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Design Analysis Overview



STPA-Sec Design Analysis.	
Step	**Description**
1. Develop process model descriptions	Describes the decision logic ("in plain English") for executing a given CA.
2. Identify Process Model Variables (PMV)	PMVs are measurable indicators of the conditions that trigger a CA.
3. Specify PMV values	PMV values are all the possible values a PMV can be assigned both acceptable and hazardous.
4. Identify PMV sensors	Identifies which sensors provide PMV values to the actors and controller for decision making.
5. Develop causal scenarios	Brainstorm how a specific implementation of the system may be compromised. Identifies critical CAs and validates the thoroughness of the model, CAs, and constraints.

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Developing Process Model Descriptions

- **Process Model Descriptions**
- Process Model Variables (PMV)
- PMV Values
- PMV Feedback
- Causal Scenarios
- War Gaming

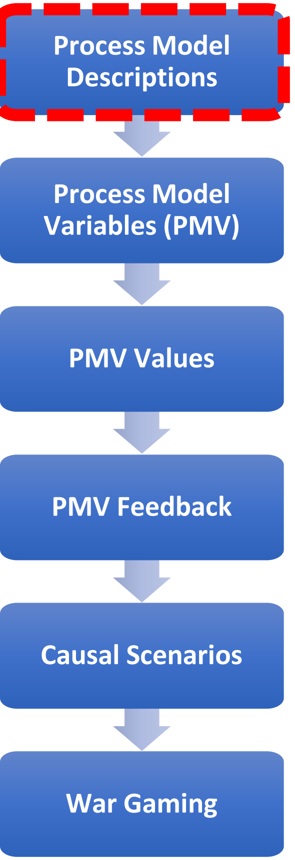
Element: Onboard Control System

Responsibilities: Receive (encrypted) ABORT when issued by ISS or GSS, decrypt (if required), terminate unsafe maneuver, command Attitude Control System to return vehicle to a safe distance from ISS and safe operational parameters. OCS will be capable of automatically sensing and commanding the Attitude Control System to ABORT docking maneuver if unsafe conditions arise

Control Actions	Key Activity	Process Model Description / Decision Logic
ABORT	Docking	Issue ABORT Signal when___{context}___
		Issue ABORT Signal when___{context}___
		Issue ABORT Signal when___{context}___

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Developing Process Model Descriptions



Element: Onboard Control System		
Responsibilities: Receive (encrypted) ABORT when issued by ISS or GSS, decrypt (if required), terminate unsafe maneuver, command Attitude Control System to return vehicle to a safe distance from ISS and safe operational parameters. OCS will be capable of automatically sensing and commanding the Attitude Control System to ABORT docking maneuver if unsafe conditions arise		
Control Actions	**Key Activity**	**Process Model Description / Decision Logic**
ABORT	Docking	Issue ABORT when ***ABORT SIGNAL RECEIVED FROM GSS*** and Vehicle is X Distance from ISS
		Issue ABORT when ***ABORT SIGNAL RECEIVED FROM ISS*** and Vehicle is X Distance from ISS
		Issue ABORT Signal when ***UNSAFE MANEUVER SENSED*** and Vehicle is X Distance from ISS

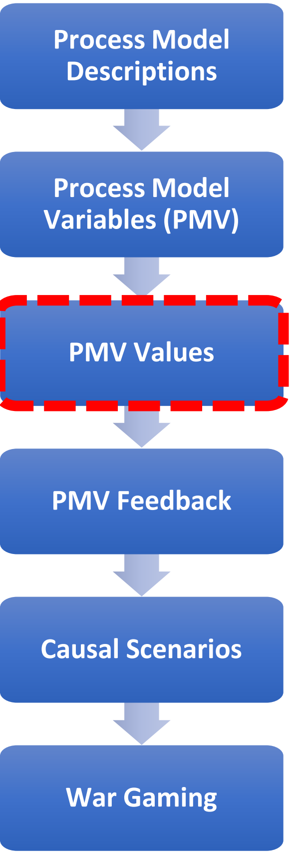
William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Identify Process Model Variables

- Process Model Descriptions
- **Process Model Variables (PMV)**
- PMV Values
- PMV Feedback
- Causal Scenarios
- War Gaming

Element: Onboard Control System			
Responsibilities: Receive (encrypted) ABORT when issued by ISS or GSS, decrypt (if required), terminate unsafe maneuver, command Attitude Control System to return vehicle to a safe distance from ISS and safe operational parameters. OCS will be capable of automatically sensing and commanding the Attitude Control System to ABORT docking maneuver if unsafe conditions arise			
Control Actions	Key Activity	Process Model Description / Decision Logic	Process Model Variables
ABORT	Docking	Issue ABORT when *ABORT SIGNAL RECEIVED FROM GSS* and Vehicle is X Distance from ISS	1) ABORT Signal Received from GSS 2) Distance from ISS
		Issue ABORT when *ABORT SIGNAL RECEIVED FROM ISS* and Vehicle is X Distance from ISS	1) ABORT Signal Received from ISS 2) Distance from ISS
		Issue ABORT when *UNSAFE MANEUVER SENSED* and Vehicle is X Distance from ISS	1) Unsafe Maneuver Sensed 2) Distance from ISS

Specify Process Model Variable Values



- ABORT Signal Received From GSS
  - Yes
  - No
  - Unknown
- ABORT Signal Received From ISS
  - Yes
  - No
  - Unknown
- Unsafe Maneuver Sensed
  - Match
  - Mismatch
  - Unknown
- Distance from ISS
  - Close
  - Not Close
  - Unknown

How Should We Initially Specify the Values for “Distance to ISS”?

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Specify Process Model Variable Values

- Process Model Descriptions
- Process Model Variables (PMV)
- **PMV Values**
- PMV Feedback
- Causal Scenarios
- War Gaming

Issue ABORT (YES / NO)	ABORT Rec'd from GSS			ABORT Rec'd from ISS			UNSAFE Maneuver Sensed			Distance from ISS		
	Yes	No	Unk	Yes	No	Unk	Mat	Mis	Unk	Close	Not Close	Unk

Complete Context Table (Truth Table for Potential Contexts)

Can Now Define When Onboard Control System Must and Must Not Invoke ABORT functionality

Entire Context Table Can Be Captured in Leveson's SpecTRM-RL Tables

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Specify Process Model Variable Values

- Process Model Descriptions
- Process Model Variables (PMV)
- **PMV Values**
- PMV Feedback
- Causal Scenarios
- War Gaming

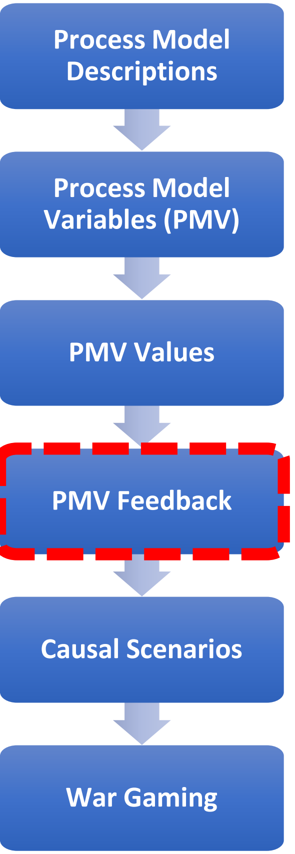
Issue ABORT (YES / NO)	ABORT Rec'd from GSS			ABORT Rec'd from ISS			UNSAFE Maneuver Sensed			Distance from ISS		
	Yes	No	Unk	Yes	No	Unk	Mat	Mis	Unk	Close	Not Close	Unk

Complete Context Table (Truth Table for Potential Contexts)

Can Now Define When Onboard Control System Must and Must Not Invoke ABORT functionality

SpecTRM-RL Tables are Testable Software Specifications

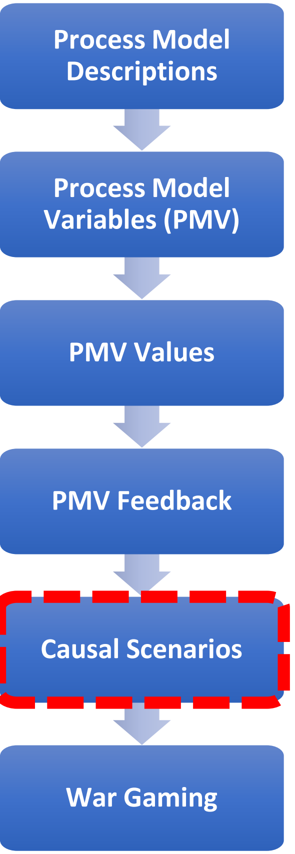
Identify Process Model Variable Sensor Feedback



- **Establish required feedback for each PMV**
- **How will each value be determined?**
  - **ABORT Command Received From GSS, ISS**
  - **Distance from ISS**
  - **Unsafe maneuver sensed**
- **Easily catch missing feedback in documents**

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

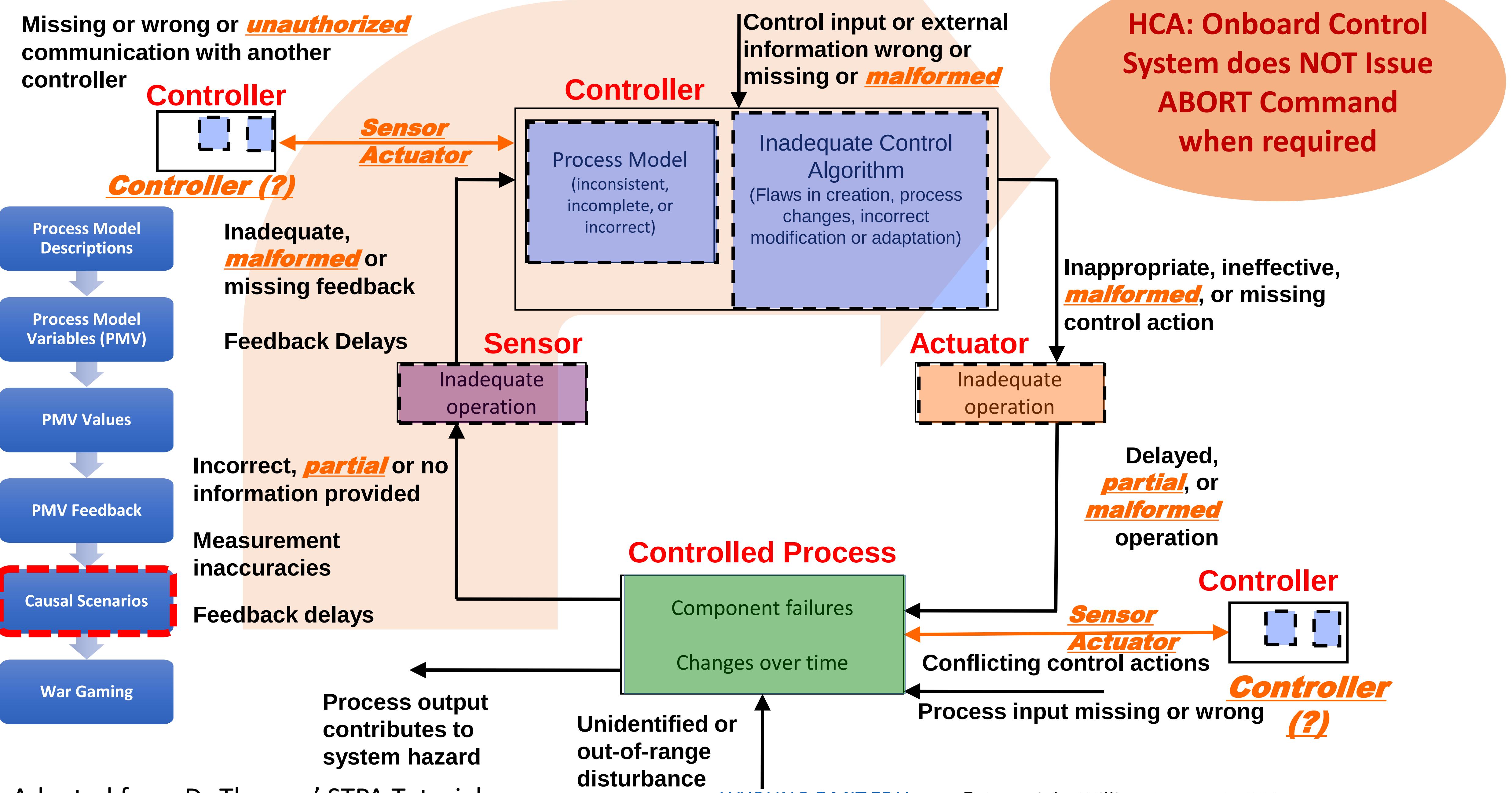
Identifying Scenarios that Lead to Hazardous Control Actions



- **Scenarios should be used to facilitate deeper insights and understanding, they are not a checklist**
- **Scenarios provide an opportunity to engage technical experts and ask key questions necessary to support improved requirements**
- **Scenarios form a connected narrative to understand and explain interactions across the system (and set appropriate requirements)**
- **Scenarios should provide useful insight or generate additional questions for deeper debate and discussion**
  - **Scenarios such as "denial of service attack prevents controller from issuing ABORT command" aren't really as useful as "controller doesn't issues ABORT command when vehicle exceeds safe closure rate because ISS and GSS disagreed on need to ABORT."**

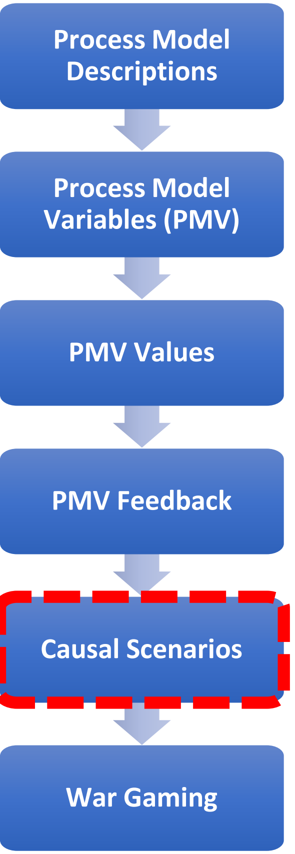
William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Potential causes of HCAs



WYOUNG@MIT.EDU

Scenario Discussion

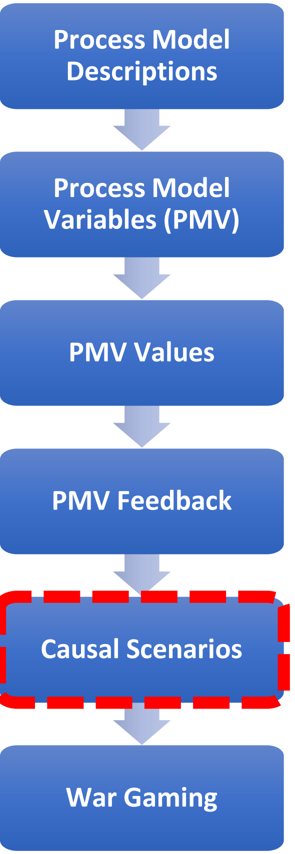


HCA: Onboard Control System (OCS) Does Not Command ABORT to Maneuver Subsytem after receiving ABORT signal from ISS and in close proximity BECAUSE ____SCENARIO____

Scenario	Associated Causal Factors	Rationale/Notes
GSS did not issue or confirm the command.		

Adapted from Dr Thomas' STPA Tutorial William.Young.3@US.AF.Mil

Scenario Discussion

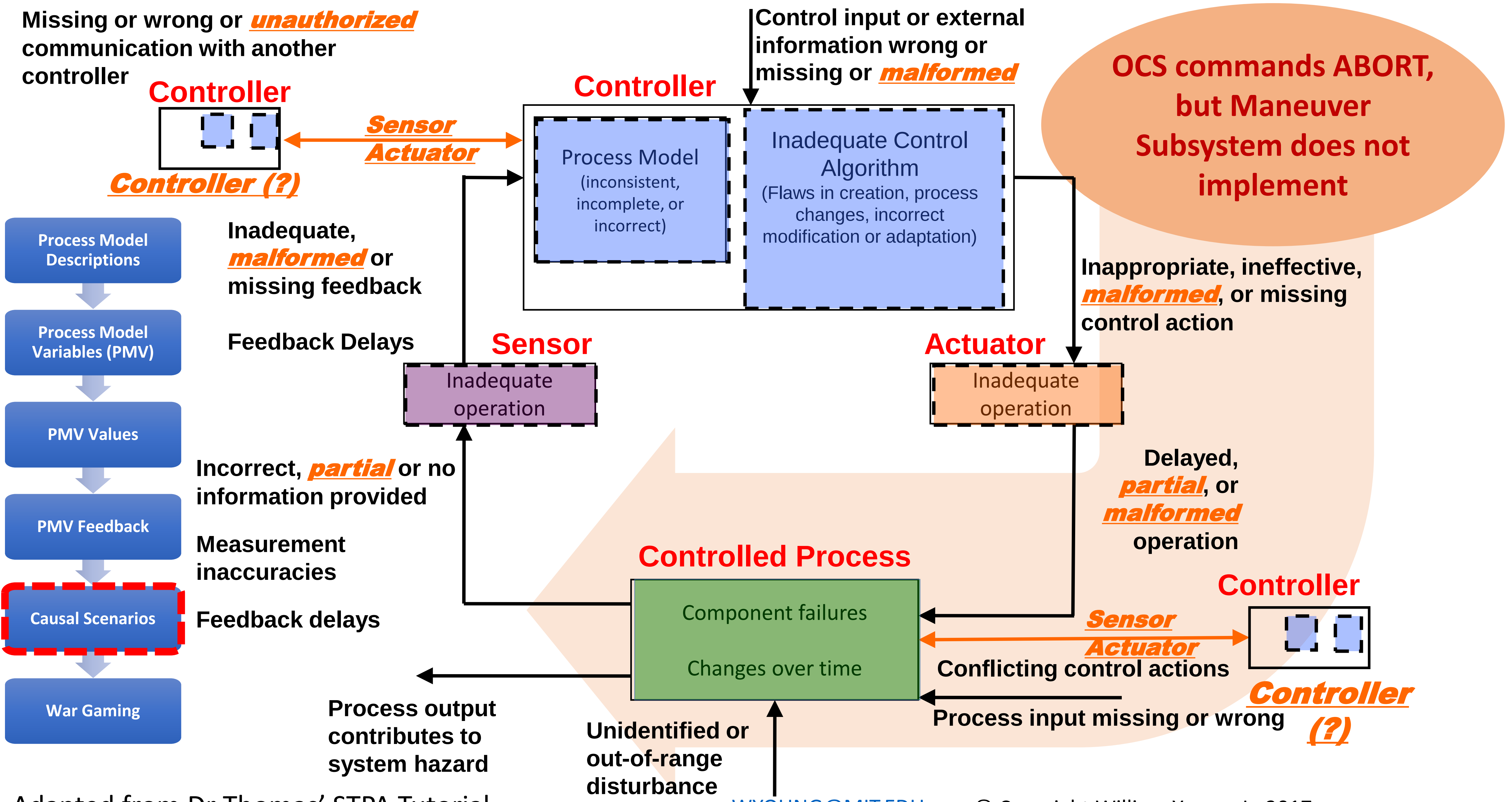


HCA: Onboard Control System (OCS) Does Not Command ABORT to Maneuver Subsytem after receiving ABORT signal from ISS and in close proximity BECAUSE ____SCENARIO____

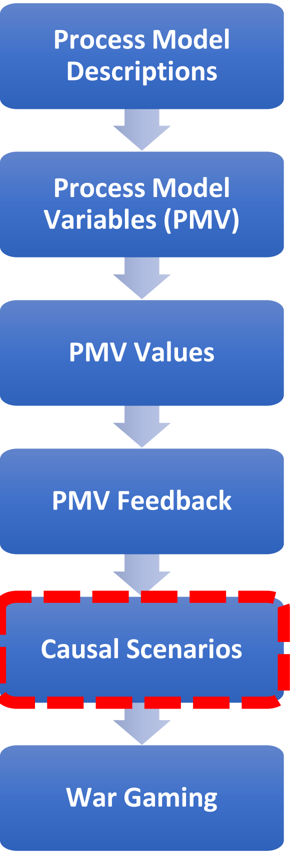
Scenario	Associated Causal Factors	Rationale/Notes
GSS did not issue or confirm the command.	•Malformed signal from GSS •Partial signal from GSS •Missing signal from GSS •Inconsistent process model	Malicious logic on OCS reports false/delayed/malformed information. Malicious logic on computer modifies process model variable to indicate that ISS is NOT in close proximity.

Adapted from Dr Thomas' STPA Tutorial William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Potential control actions not followed



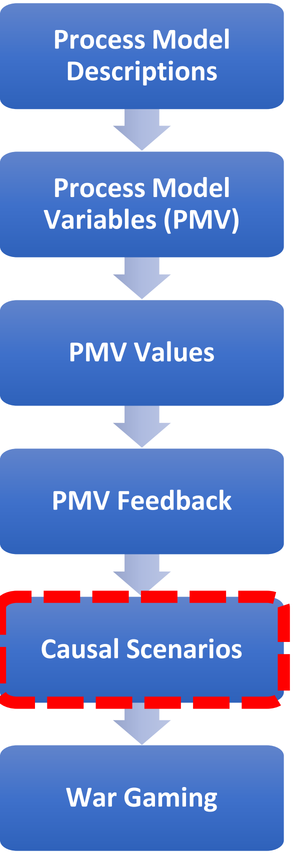
Scenario Discussion



HCA: Onboard Control System provides ABORT command in close proximity to ISS after receiving ABORT signal from ISS & GSS and close proximity but Maneuver Subsystem does not execute ABORT functionality BECAUSE ___ Scenario___

Scenario	Associated Causal Factors	Rationale/Notes
Maneuver subsystem prioritizes inputs from its internal measurements on whether or not vehicle has exceeded safe docking parameters. Does not adequately handle a case where local sensor data is incorrect AND there are still good comms with ISS / GSS		

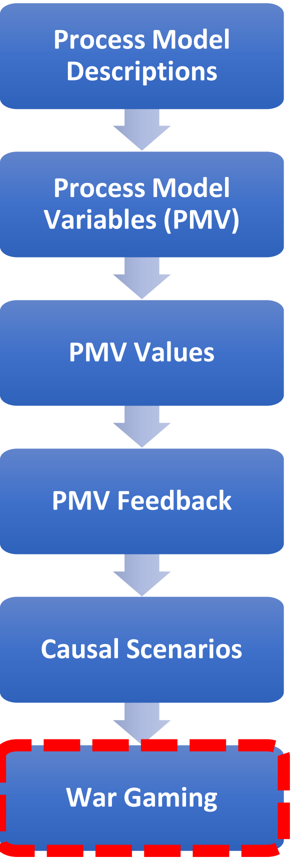
Scenario Discussion

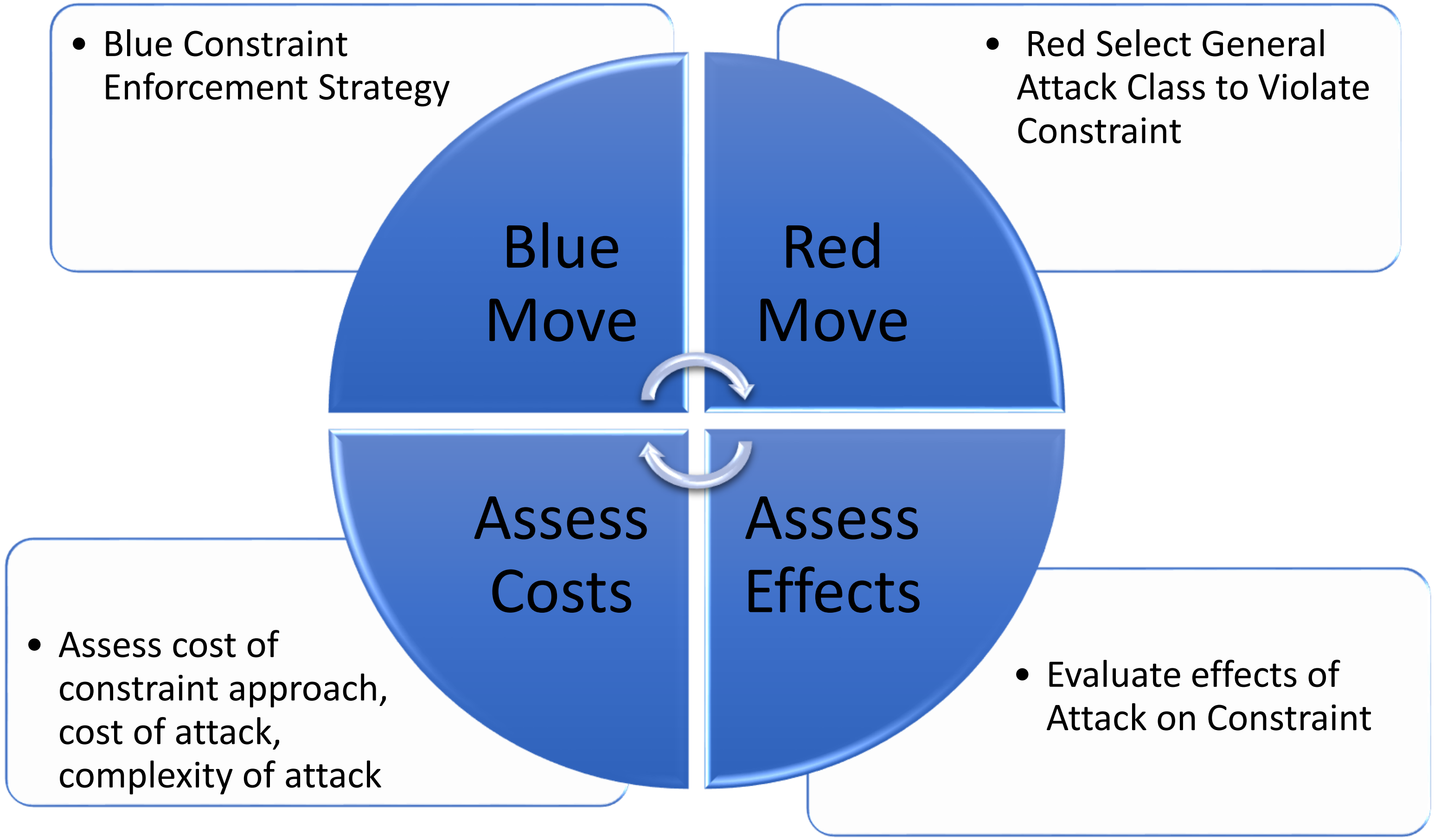


HCA: Onboard Control System provides ABORT command in close proximity to ISS after receiving ABORT signal from ISS & GSS and close proximity but Maneuver Subsystem does not execute ABORT functionality BECAUSE ___ Scenario___

Scenario	Associated Causal Factors	Rationale/Notes
Maneuver subsystem prioritizes inputs from its internal measurements on whether or not vehicle has exceeded safe docking parameters. Does not adequately handle a case where local sensor data is incorrect AND there are still good comms with ISS / GSS	• Inadequate control algorithm • Potential conflicting control between Maneuver subsystem and Onboard control system	Attacking sensor inside Maneuver Subsystem creates the potential to block GSS/ISS if the ABORT logic requires onboard confirmation that the vehicle is in close proximity or outside parameters.

Wargaming





Blue focus on Enforcing Constraint, Red focus on violating constraint…
Goal is to "Fix" Problem Through Elimination or Mitigation Above Component Level

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

User Questions and Answers

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Summary and Conclusions

William.Young.3@US.AF.Mil WYOUNG@MIT.EDU

Lessons Learned Applying STPA-Sec

- Often heard comments:
  - “You’re starting at a much higher level of abstraction…”
  - “We try to do something like that, but STPA-Sec is much more rigorous…”
  - “This requires a great deal of thought…from more than just security experts”
- Difficult or impossible to implement if system owner is unable cannot specify what system is supposed to do
- Initial expert guess on what is most important to assure tends to be too broad to be actionable
  - E.g. “Power grid”

STPA-Sec is NOT a silver bullet, but appears to enable increased rigor “Left of Design”

Safety and Security

- **Goal is loss prevention and risk management**
- **Source is probably irrelevant and may be unknowable**
- **Method is the development and engineering of controls**
- **Focus on what we have the ability to address, not the environment**
- **STPA/STPA-Sec provide opportunity for a unified and integrated effort through shared control structure!**

Conclusion

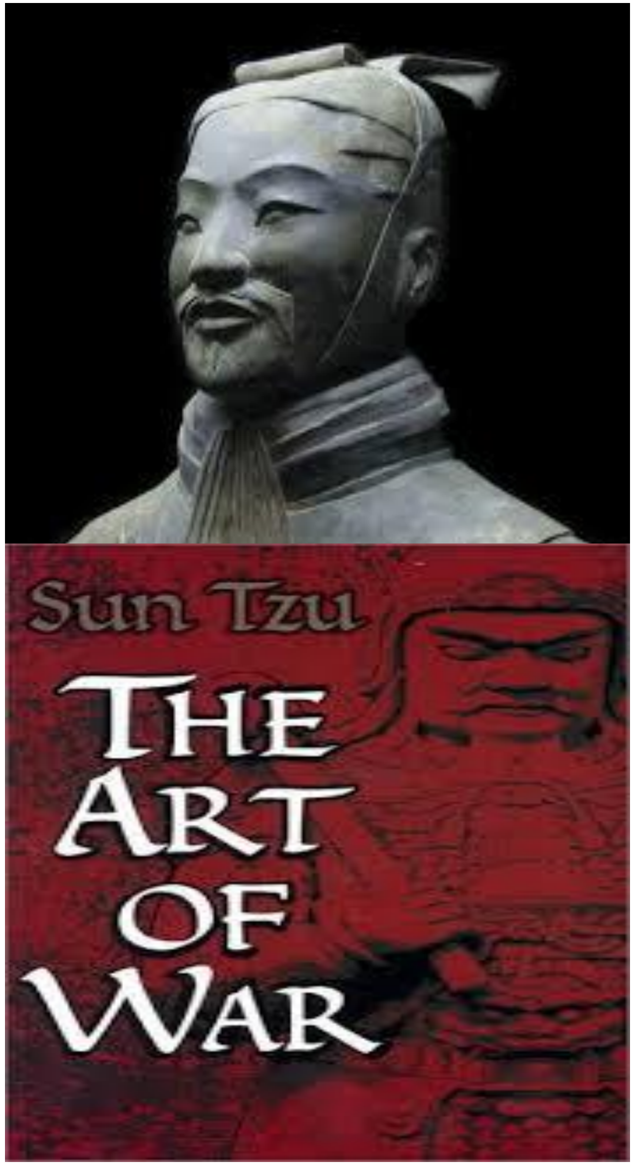
- **Must think carefully about defining the security problem**
- **Perfectly solving the wrong security problem doesn't really help**
- **STPA-Sec provides a means to clearly link security to the broader mission or business objectives**
- **STPA-Sec does not replace existing security engineering methods, but enhances their effectiveness**

Concluding Thoughts from Sun Tzu

The opportunity to secure ourselves against defeat lies in our own hands.

The supreme art of war is to subdue the enemy without fighting.

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.



WYOUNG@MIT.EDU

QUESTIONS ??