BASIC INTRODUCTION TO STPA FOR SECURITY (STPA-SEC)

2020 SYSTEM-THEORETIC ACCIDENT MODEL AND PROCESSES (STAMP) WORKSHOP

July 22, 2020

William "Dollar" Young, Jr (PhD)

WYOUNG@MIT.EDU

Acknowledgement & Disclaimer



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

This Presentation Provides Only a Brief Introduction to the 40 hour+ STPA-SEC Analysis Methodology Course

Tutorial Objective

- These short tutorials are **not training classes**
- We cannot cover everything in these tutorial sessions. The objective is just to introduce some of the core concepts and help new attendees follow the workshop presentations.
- Like most techniques, training and practice with a qualified instructor are needed to become proficient.

Overview

- Motivation & Big Ideas
- Security Through a System-Theoretic Lens
- System-Theoretic Process Analysis for Security (STPA-Sec) Practicum
  - Problem Framing
  - Scenario Development
  - Wargaming
- Does it Work in the Real World?
- Ongoing Work and STPA-Sec 2.0
- Summary

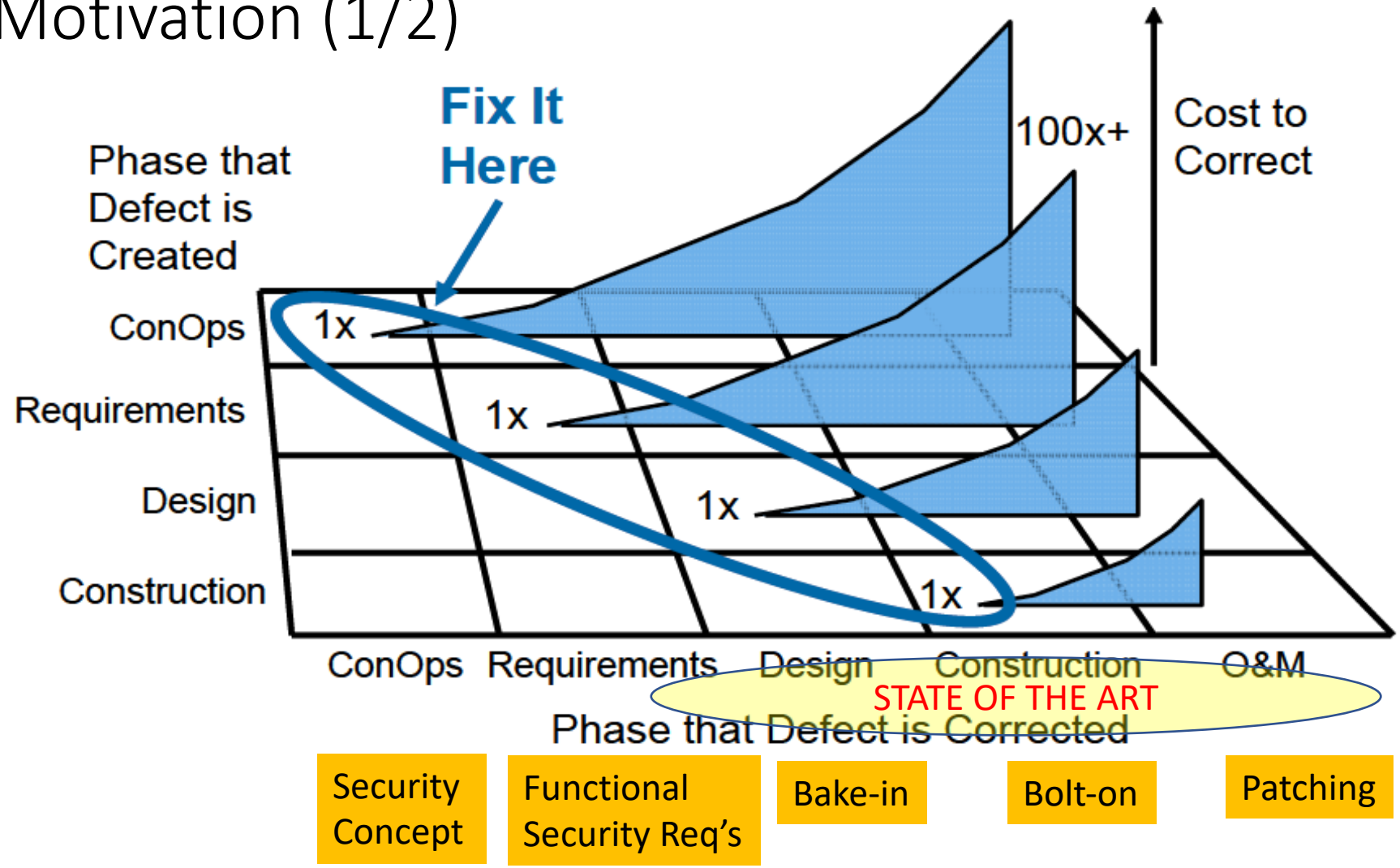
To Maximize Available Time, We Will Continue the Exercise John Thomas Introduced in Yesterday's STPA Tutorial

Overview

- **Motivation & Big Ideas**
- Security Through a System-Theoretic Lens
- System-Theoretic Process Analysis for Security (STPA-Sec) Practicum
  - Problem Framing
  - Scenario Development
  - Wargaming
- Does it Work in the Real World?
- Ongoing Work and STPA-Sec 2.0
- Summary

Business / Mission Analysis Provides the Missing Link to Implementing Security Frameworks

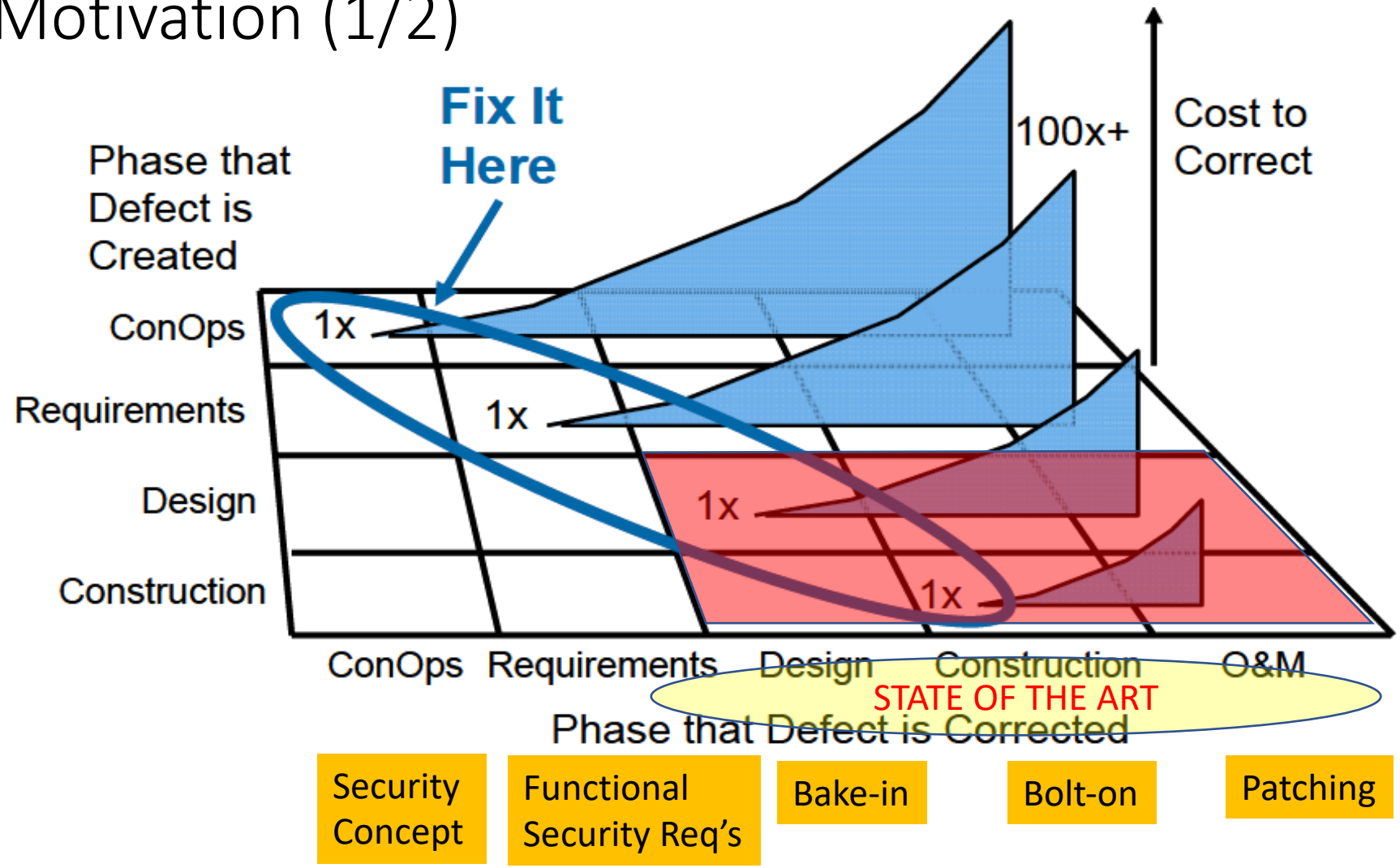
Motivation (1/2)



In Systems That You Are Familiar With, In What Phase Was Security First Addressed?

© Copyright William Young, 2020

Motivation (1/2)



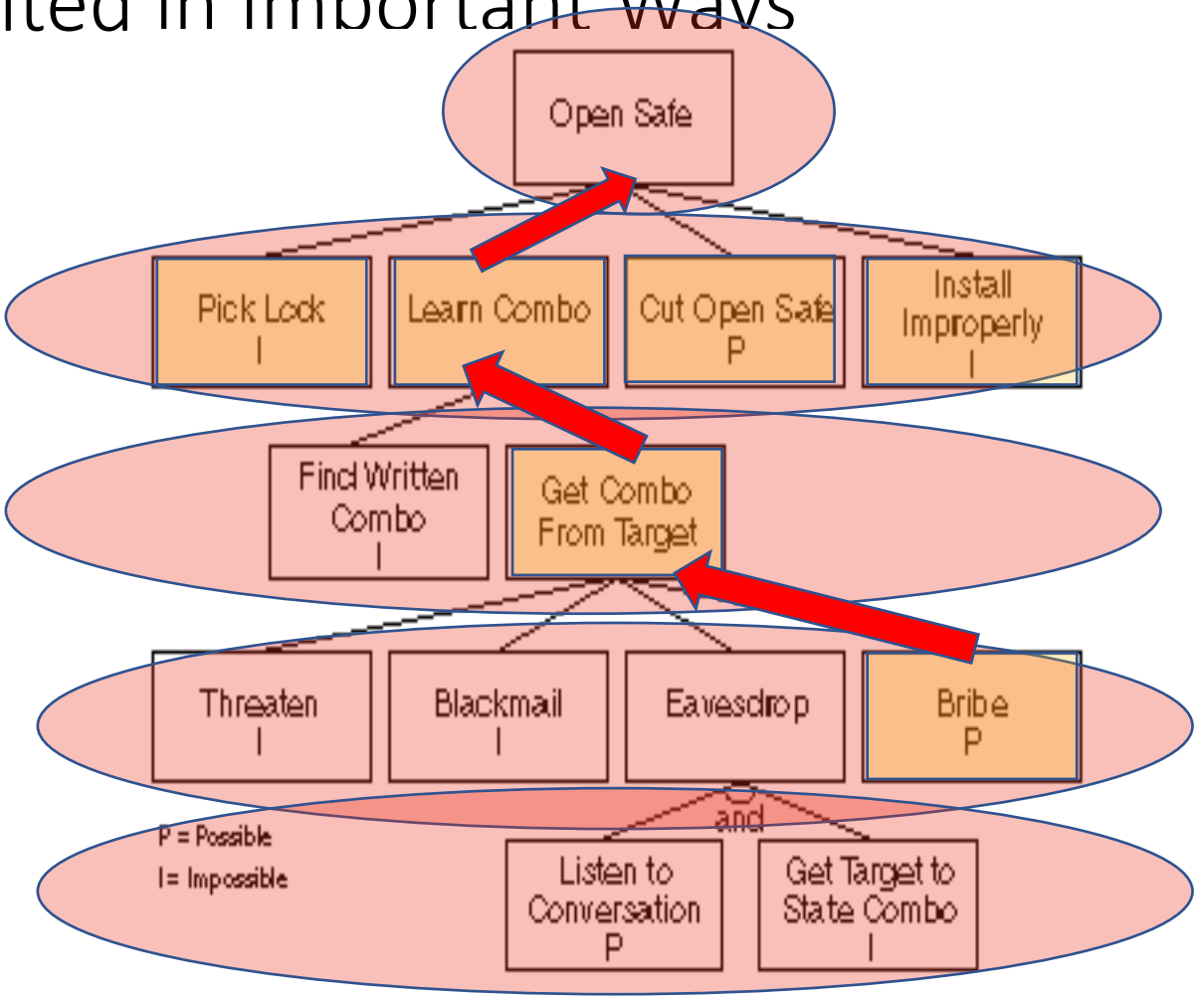
The Vast Majority of Current Security Engineering Practice Does Not Address Security until After Architecture is Well Defined

© Copyright William Young, 2020

Motivation (2/2) Dominant Security Model is Limited in Important Ways

"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"



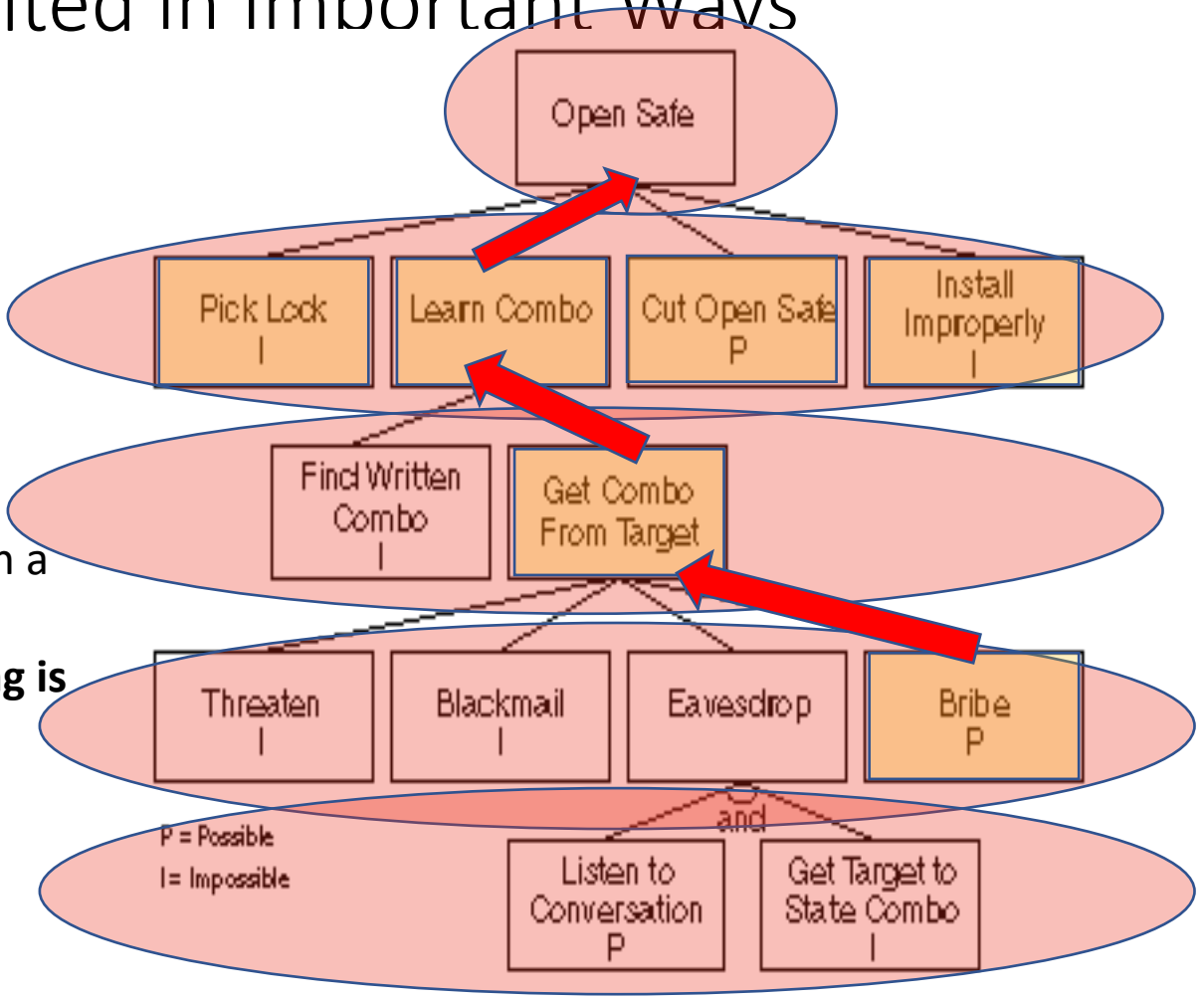


Attack Trees are Based on Fault Trees Used in Safety (and share the same shortfalls based on model weaknesses)

Ref: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

© Copyright William Young, 2020

Motivation (2) Dominant Security Model is Limited in Important Ways



Safe is A **means** to an end within a **Process**

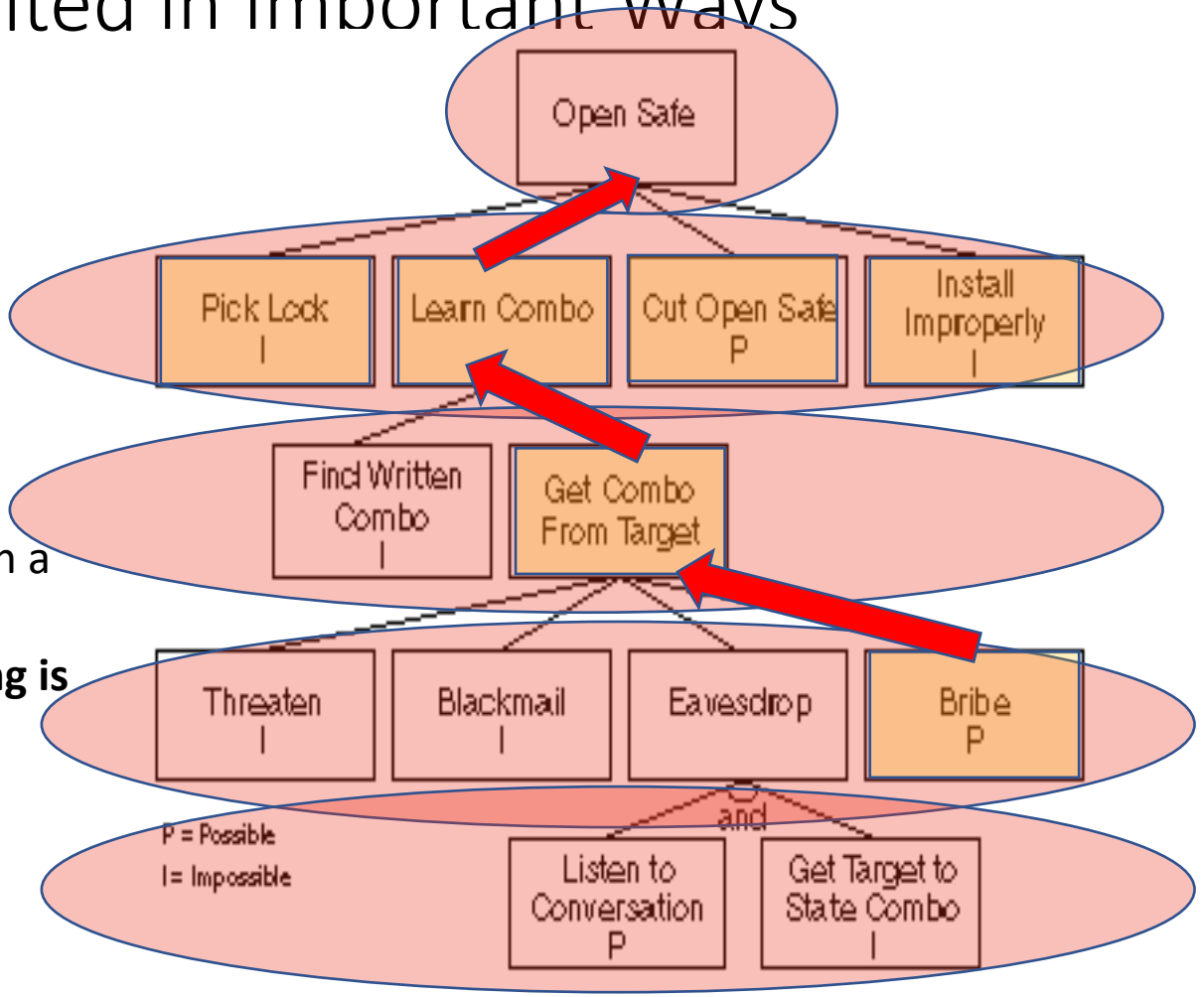
- **Preventing safe from opening is NOT the overall mission!**
- **Safe is a <u>form</u> that has been assigned mission-related functionality**

Current Security Approaches Are Built on Variations of the Same Linear Model Nancy Introduced on Monday's Talk!

Ref: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

© Copyright William Young, 2020

Motivation (2) Dominant Security Model is Limited in Important Ways



Safe is A **means** to an end within a **Process**

- **Preventing safe from opening is NOT the overall mission!**
- **Safe is a <u>form</u> that has been assigned mission-related functionality**

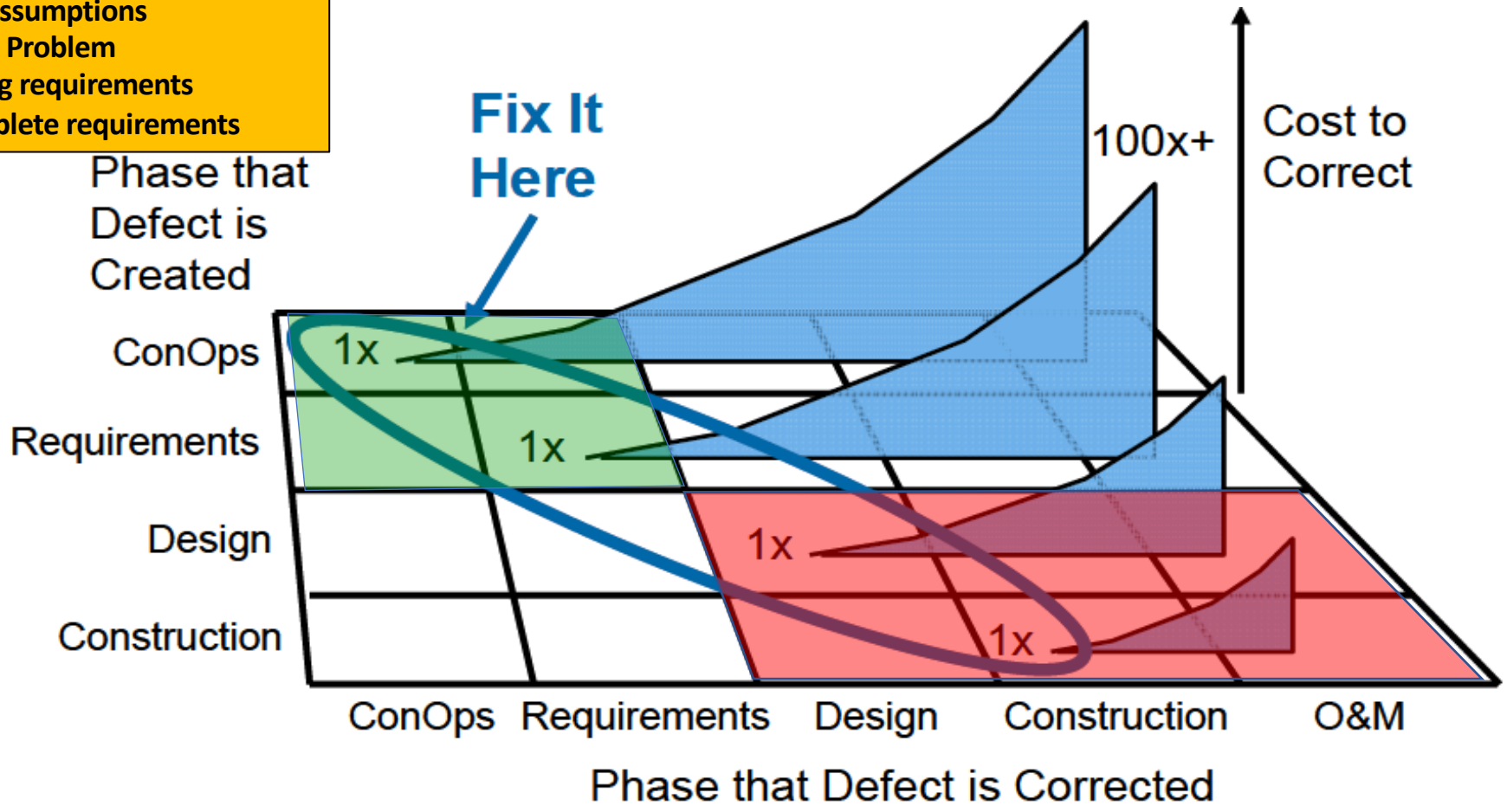
To Make Progress We Need a More Powerful Model (and Process) Capable of Providing Greater Insight, Earlier in the System Engineering Lifecycle

Ref: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

© Copyright William Young, 2020

Motivation (3)

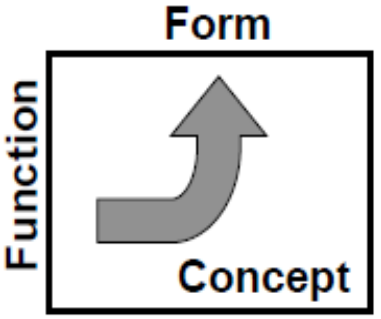
Flawed logic
Conflicting goals
Poor Assumptions
Wrong Problem
Missing requirements
Incomplete requirements



The Vast Majority of Security Related Losses are Related to Not Applying Systems Thinking to Security During the Concept Stage

© Copyright William Young, 2020

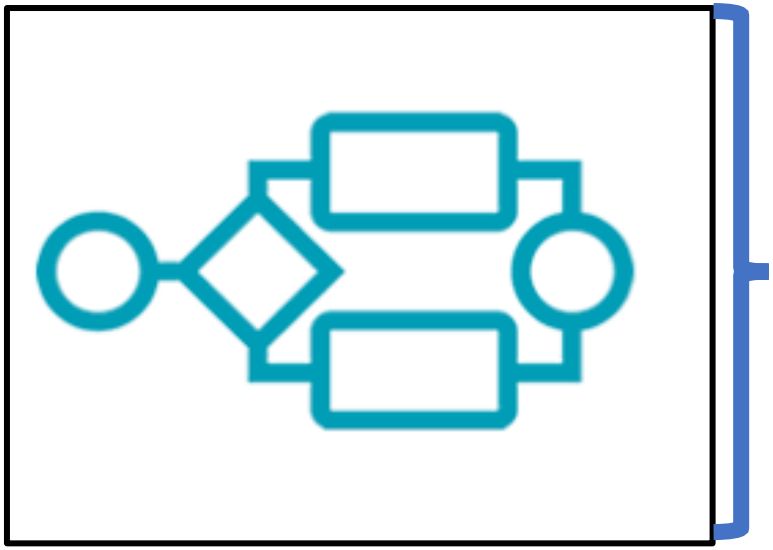
Big Idea 1: Secure Form Realizes Secure Concept & Function



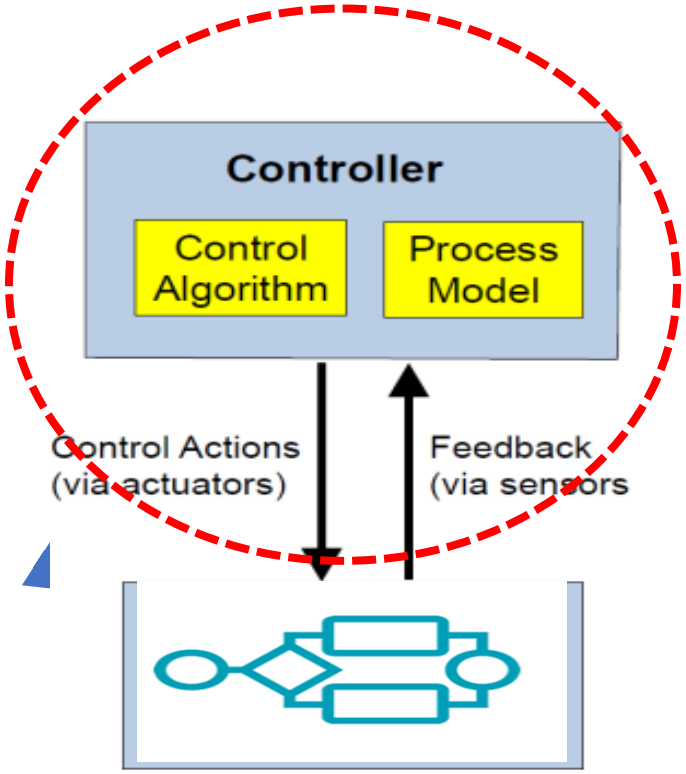
- "Form follows function" is a central tenant of system engineering and architecture
- Generate secure Business & Mission Systems by first defining the secure functionality to be realized
- Get to security via
  - Identify functionality required to solve the problem at hand (But we must understand problem)
  - 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

© Copyright William Young, 2020

Big Idea 2: Build a Strategy to Secure key Process (prevent mis-behavior that matters) then develop specific security tactics



MISSION OR BUSINESS PROCESS MODEL



Basic Control Loop

System-Theoretic PROCESS Analysis for Security

© Copyright William Young, 2020

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"

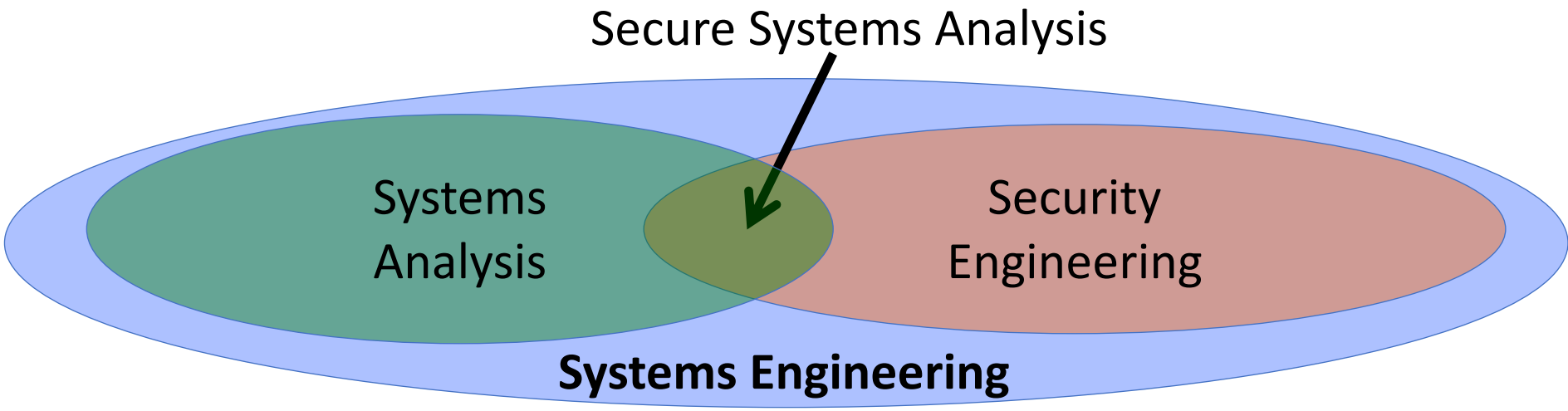
Integrate Security Principles Into Systems Engineering Via Secure Systems Analysis

© Copyright William Young, 2020

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

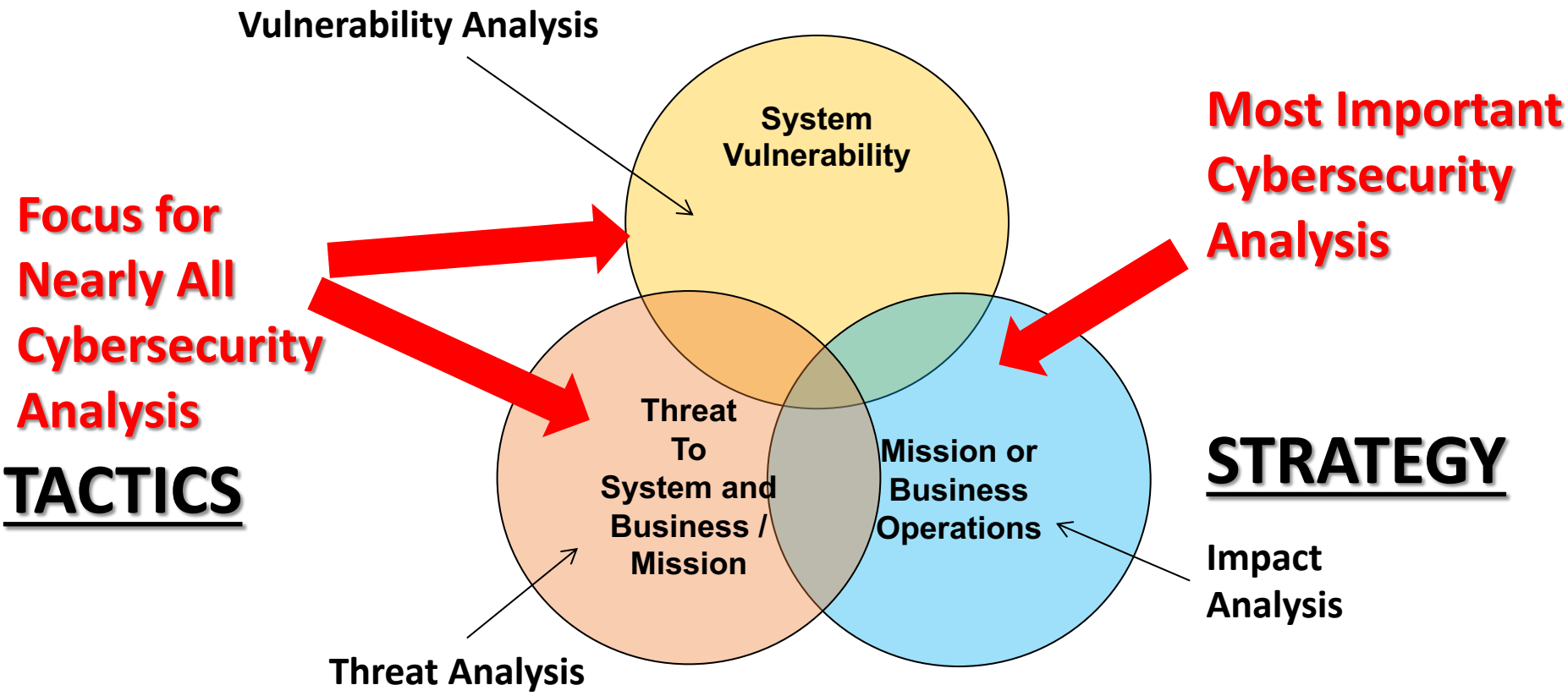
© Copyright William Young, Jr, 2019

Overview

- Motivation & Big Ideas
- **Security Through a System-Theoretic Lens**
- System-Theoretic Process Analysis for Security (STPA-Sec) Practicum
  - Problem Framing
  - Scenario Development
  - Wargaming
- Does it Work in the Real World?
- Ongoing Work and STPA-Sec 2.0
- Summary

© Copyright William Young, 2020

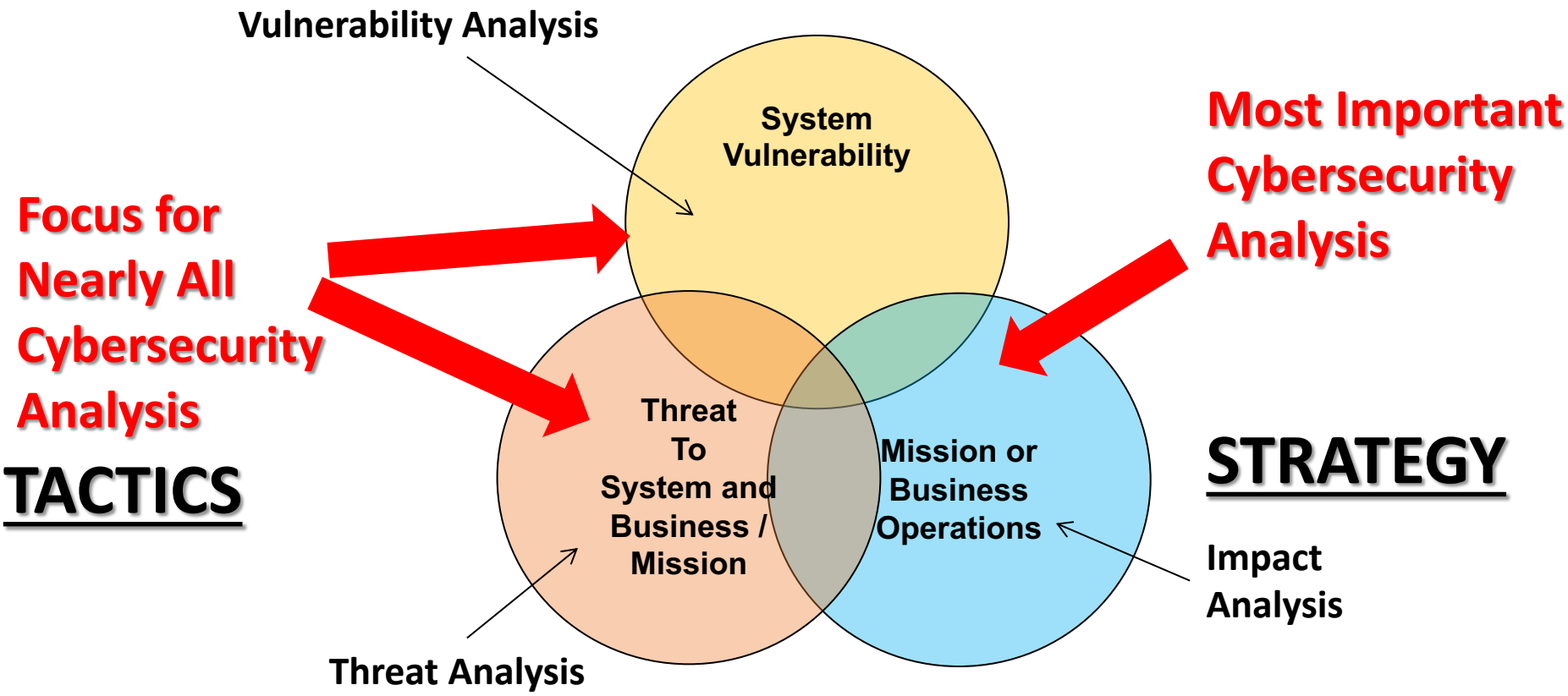
Three Types of Cybersecurity Analysis



Analyzing Cybersecurity through a Business or Mission Lens Raises Framework Implementation from a Tactics to a Strategy Issue, But Requires a Suitable Model

© Copyright William Young, 2020

Three Types of Cybersecurity Analysis (2)



The Attack Tree only Covers Two of the Three Concerns

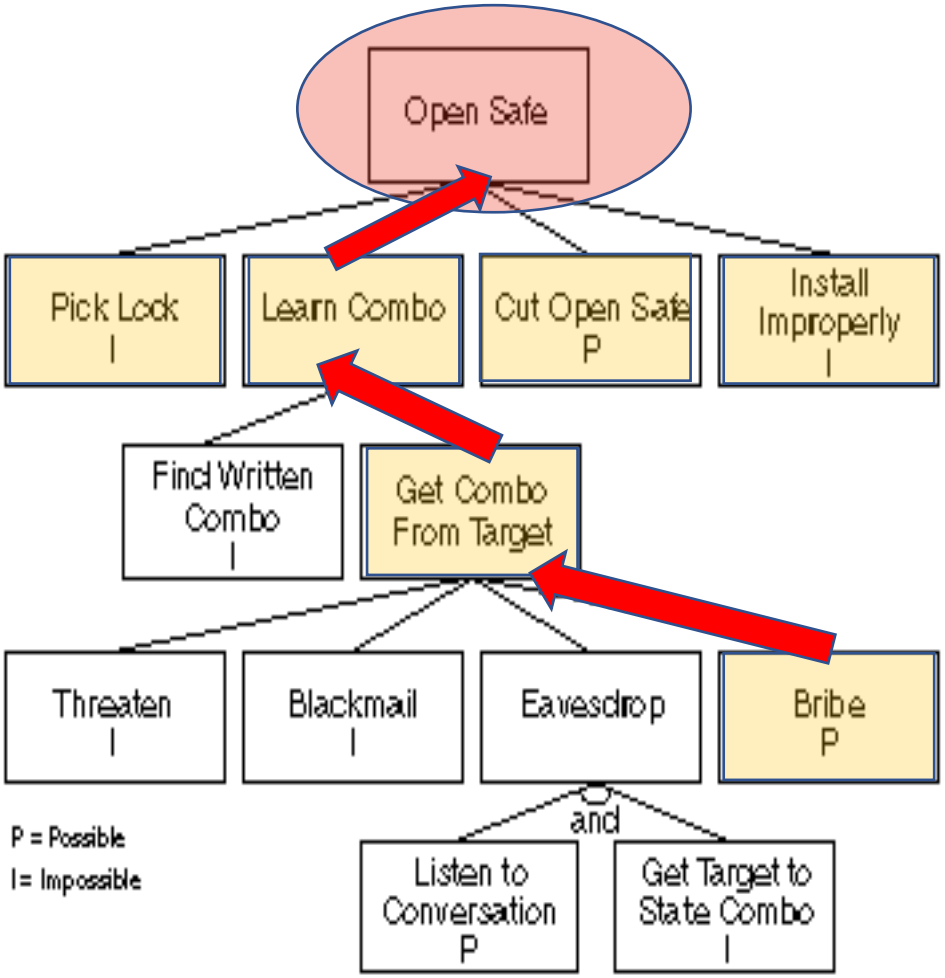
© Copyright William Young, 2020

Returning top Our Attack Tree

System (Component) Impact

System Vulnerabilities

Threat Attacks



Tacit Assumption is that the Security Problem is Protecting the Safe Contents, But We Need to Understand the Mission (process) in order to Identify the Right Actions to take

Ref: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

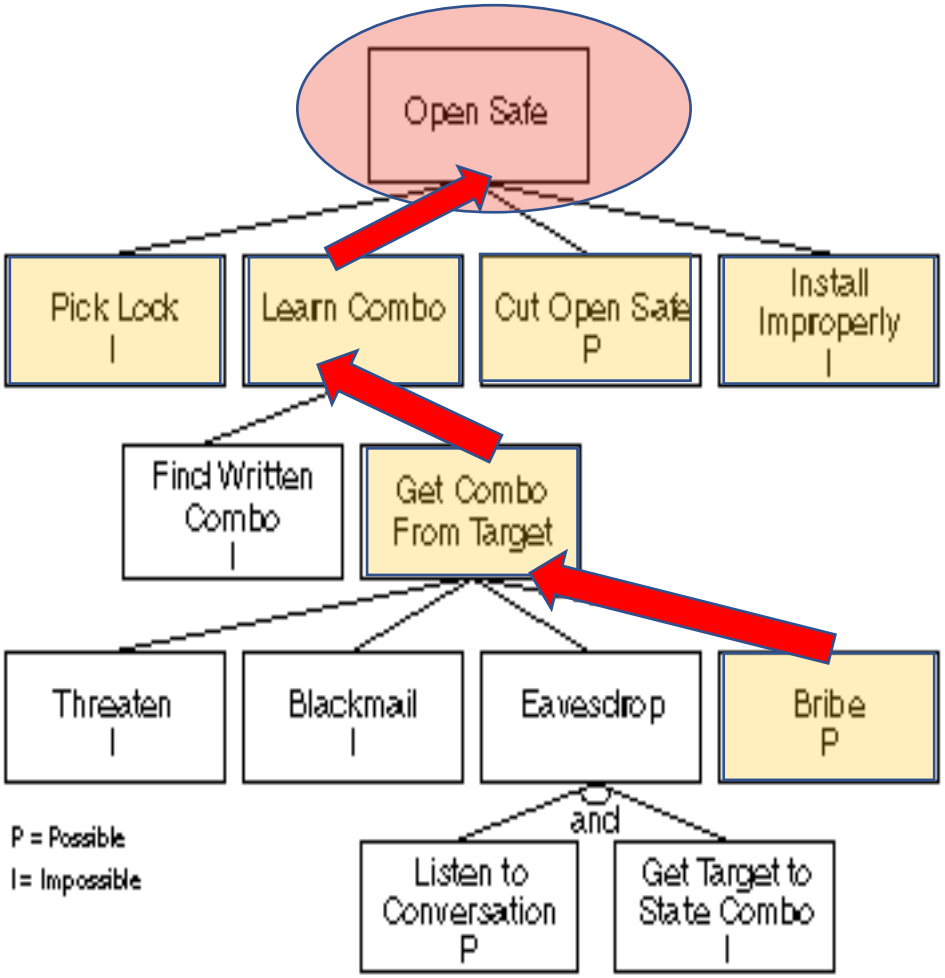
© Copyright William Young, 2020

Returning top Our Attack Tree

System (Component) Impact

System Vulnerabilities

Threat Attacks



Mission Impact, Not System Impact, Is What Matters Most

Ref: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

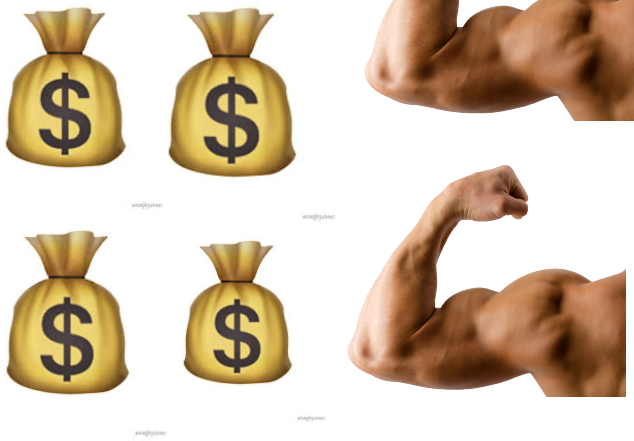
© Copyright William Young, 2020

RISK = THREAT X VULNERABILITY X IMPACT



Investment Leverage

Threat



Investment Leverage

Vulnerability



Investment Leverage

Impact

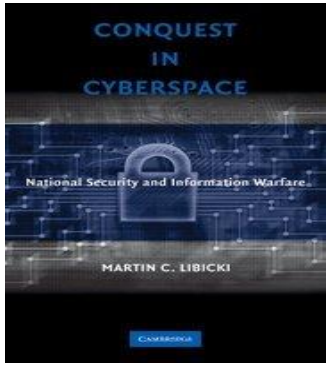
We Have Most Control over Impact!

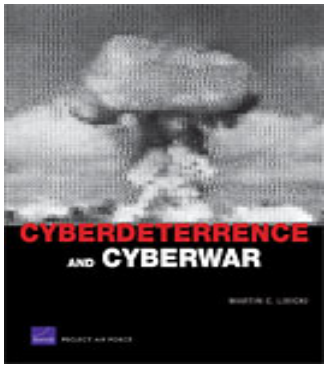
WYOUNG@MIT.EDU

© Copyright William Young, 2020

Martin Libicki on Network Security

"Start with the problem of preventing effects arising from mis-instructed systems, often understood as "defending networks." As noted earlier, such a task might otherwise be understood as an engineering task—how to prevent errant orders from making systems misbehave. One need look no further than Nancy Leveson's *Safeware* to understand that the problem of keeping systems under control in the face of bad commands is a part of a more general problem of safety engineering, a close cousin of security engineering as Ross Anderson's classic of the same name expounds."

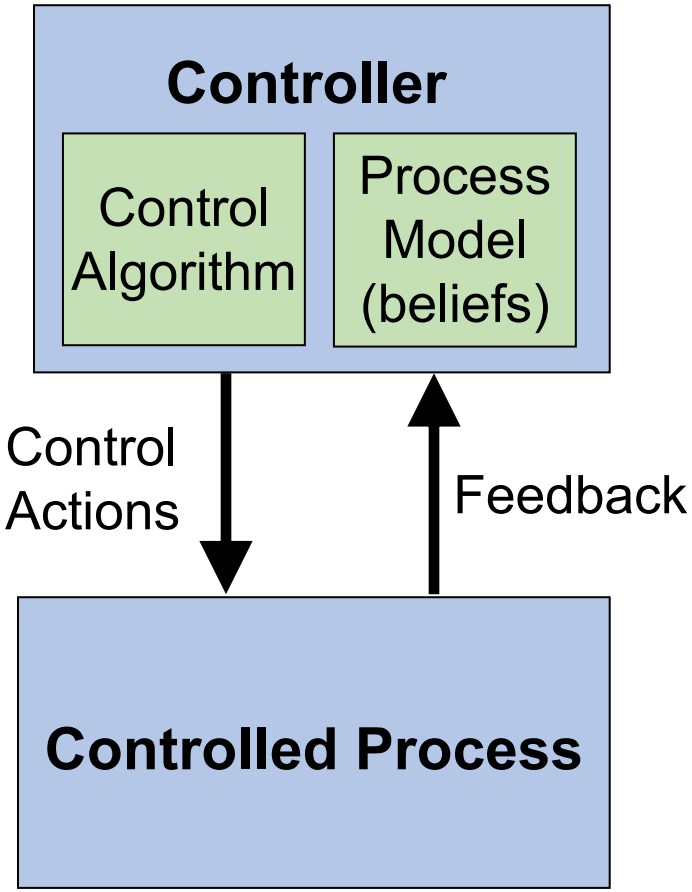




Preventing Unacceptable Losses Due to System Misbehavior from Mis-instruction is Shared in Safety and Security Engineering

WYOUNG@MIT.EDU
© Copyright William Young, 2020

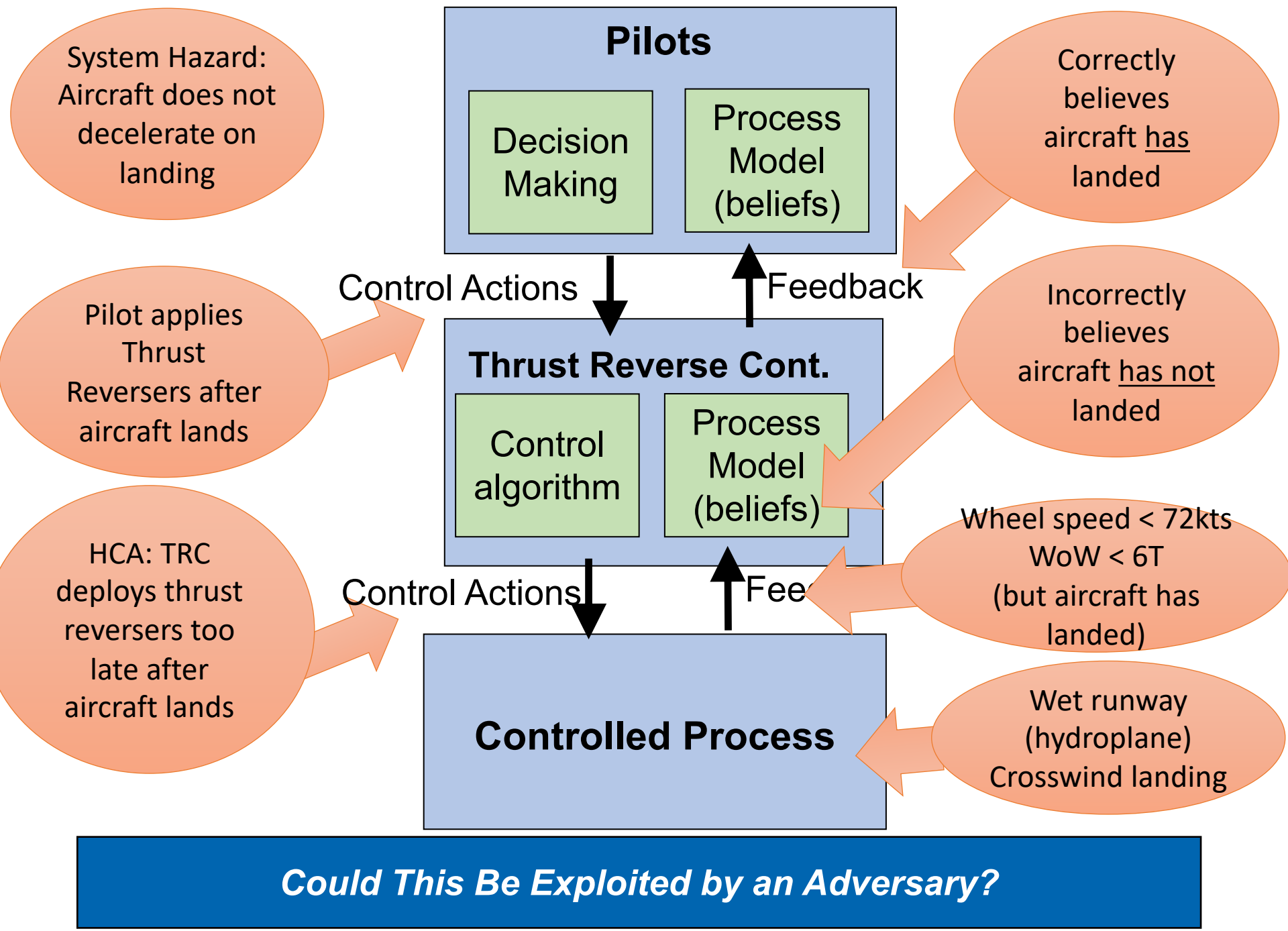
Basic Control Loop



- Provides another way to think about losses
- Forms foundation for STAMP/STPA/CAST/STPA-SEC

Another Look at Nancy's Warsaw Reverse Thrusters Loss Example from Monday





(John Thomas, 2019; jthomas4@mit.edu)
WYOUNG@MIT.EDU
© Copyright John Thomas 2019

STRIDE Mnemonic For Generating Security Scenarios (Shostack)

- **S**poofing – Pretending to be something or someone you're not
- **T**ampering – Modifying something you're not supposed to modify
- **R**epudiation – Claiming you didn't do something (whether you did or didn't)
- **I**nformation Disclosure – exposing information to people who are not authorized to see it
- **D**enial of Service – attacks meant to prevent a system from providing service, including by crashing it, making it unusably slow or filling all of its storage
- **E**levation of Privilege- when a program or user is technically able to do things that they aren't supposed to do

We will NOT be Using STRIDE to Generate Scenarios

Ref: Shostack, Threat Modeling: Designing for Security

STRIDE Mnemonic For Generating Security Scenarios (Shostack)

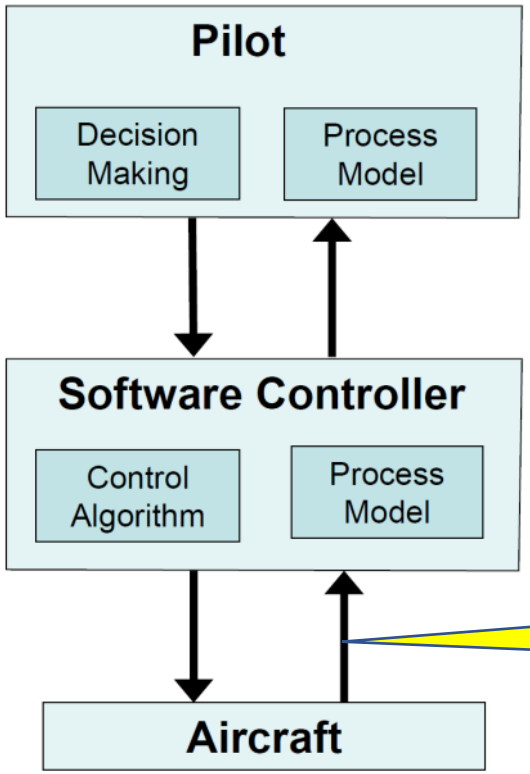
- Spoofing – Pretending to be something or someone you're not
- Tampering – Modifying something you're not supposed to modify
- Repudiation – Claiming you didn't do something (whether you did or didn't)
- Information Disclosure – exposing information to people who are not authorized to see it
- Denial of Service – attacks meant to prevent a system from providing service, including by crashing it, making it unusably slow or filling all of its storage
- Elevation of Privilege- when a program or user is technically able to do things that they aren't supposed to do

We will use STRIDE to Categorize Attacks and as a Bridge to Security Experts Who Will Help Develop Solutions

Ref: Shostack, Threat Modeling: Designing for Security

Nancy's Safety Example Captures the OUTCOMES of Successful Attacks!

Hazard: Inadequate Aircraft deceleration after landing



Spoofing

Tamper

Denial of Service

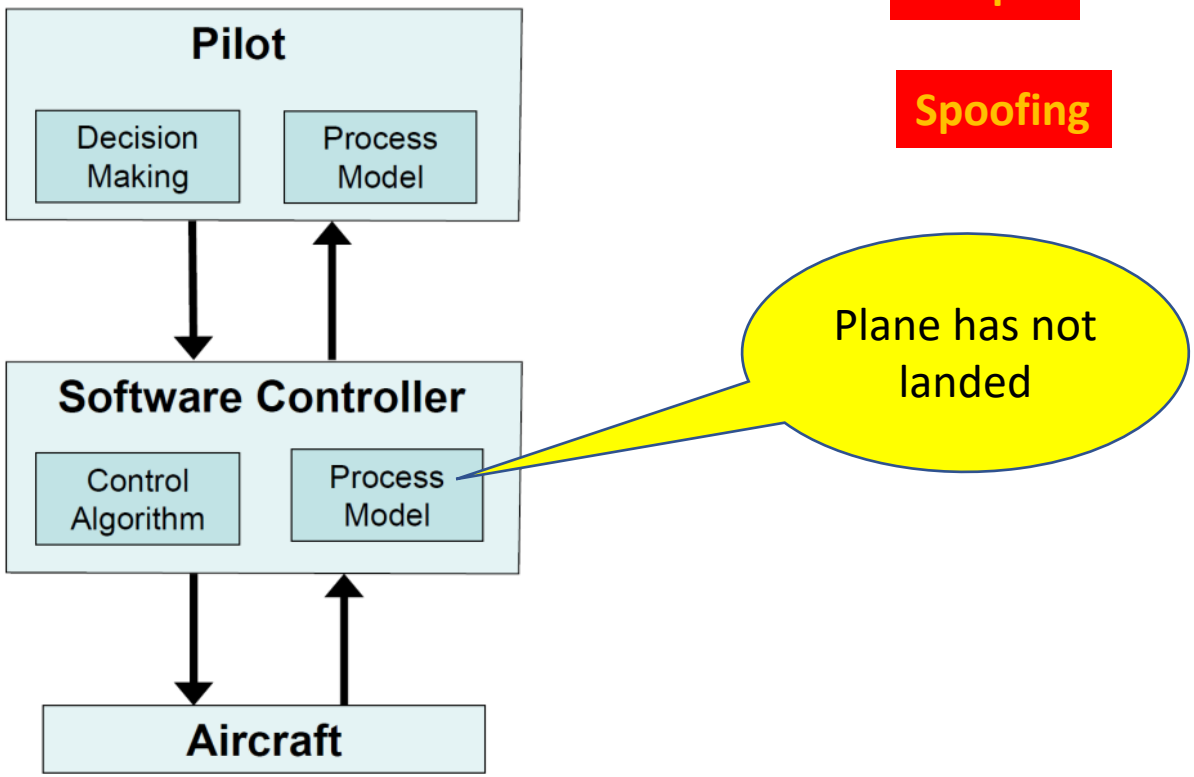
Feedback indicates plane has not landed

How Might We Categorize this Part of the Causal Scenario?

© Copyright William Young, 2020

Nancy's Safety Example Captures the OUTCOMES of Successful Attacks!

Hazard: Inadequate Aircraft deceleration after landing

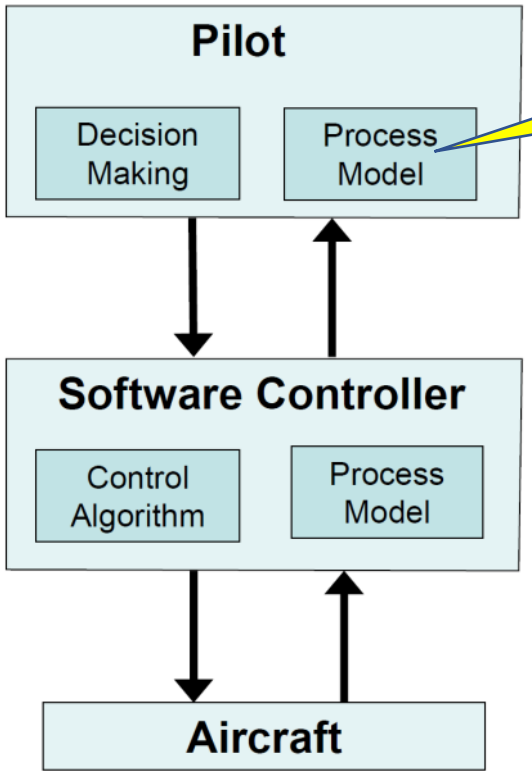


How Might We Categorize this Part of the Causal Scenario?

© Copyright William Young, 2020

Nancy's Safety Example Captures the OUTCOMES of Successful Attacks!

Hazard: Inadequate Aircraft deceleration after landing



Plane has landed

Denial of Service

Tamper

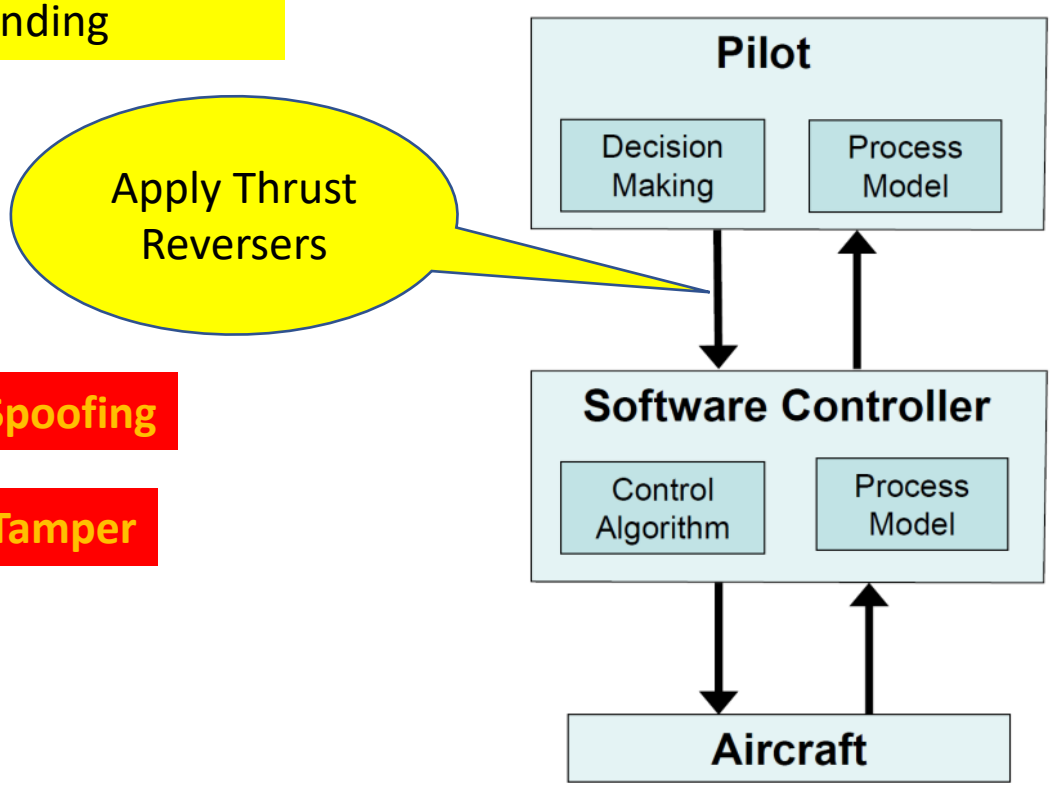
Spoofing

How Might We Categorize this Part of the Causal Scenario?

© Copyright William Young, 2020

Nancy's Safety Example Captures the OUTCOMES of Successful Attacks!

Hazard: Inadequate Aircraft deceleration after landing



Spoofing

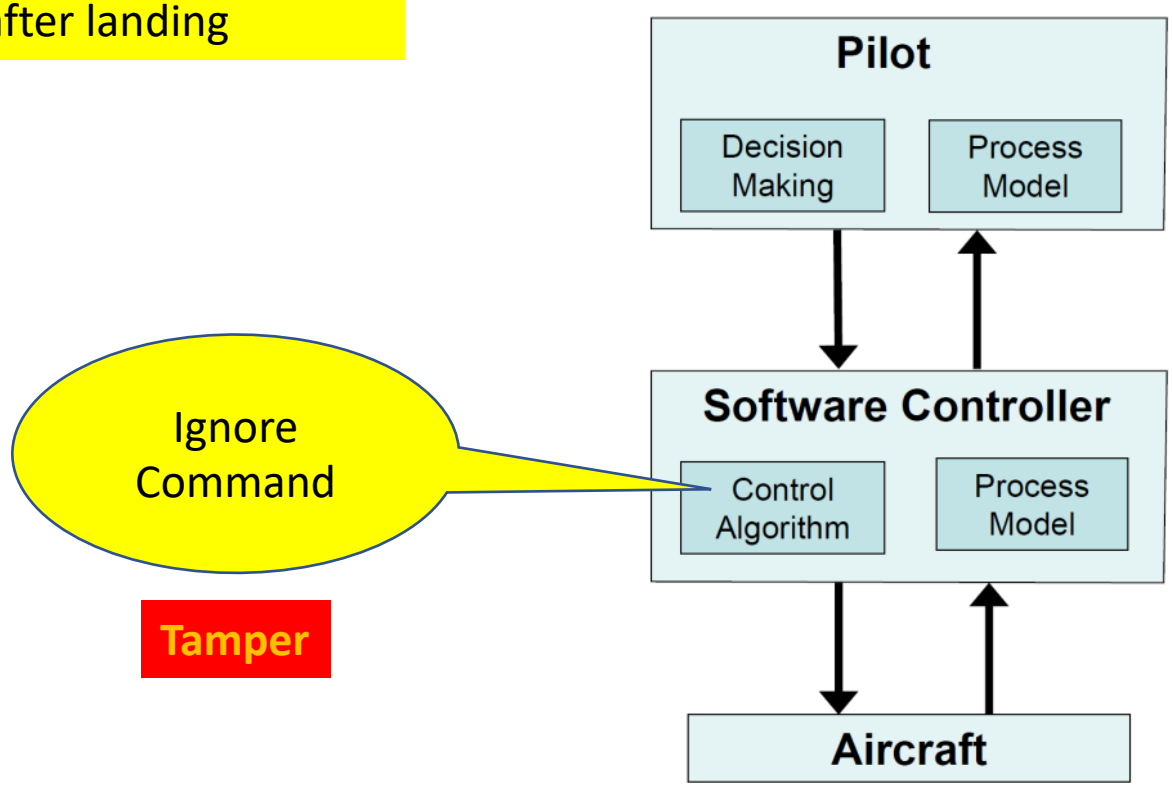
Tamper

How Might We Categorize this Part of the Causal Scenario?

© Copyright William Young, 2020

Nancy's Safety Example Captures the OUTCOMES of Successful Attacks!

Hazard: Inadequate Aircraft deceleration after landing



How Might We Categorize this Part of the Causal Scenario?

© Copyright William Young, 2020

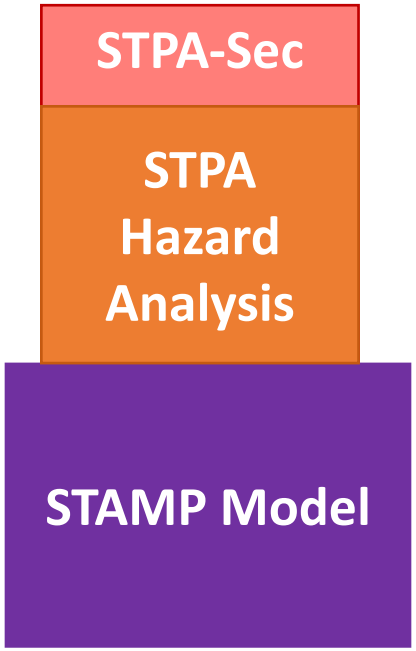
Overview

- Motivation & Big Ideas
- Security Through a System-Theoretic Lens
- **System-Theoretic Process Analysis for Security (STPA-Sec) Practicum**
  - **Problem Framing**
  - **Scenario Development**
  - **Wargaming**
- Does it Work in the Real World?
- Ongoing Work and STPA-Sec 2.0
- Summary

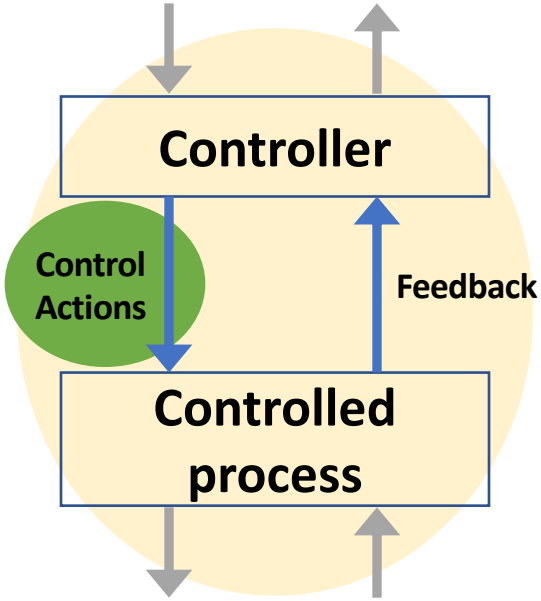
Business / Mission Analysis Provides the Missing Link to Implementing Security Frameworks

© Copyright William Young, 2020

System Security with System-Theoretic Process Analysis for Security (STPA-Sec)



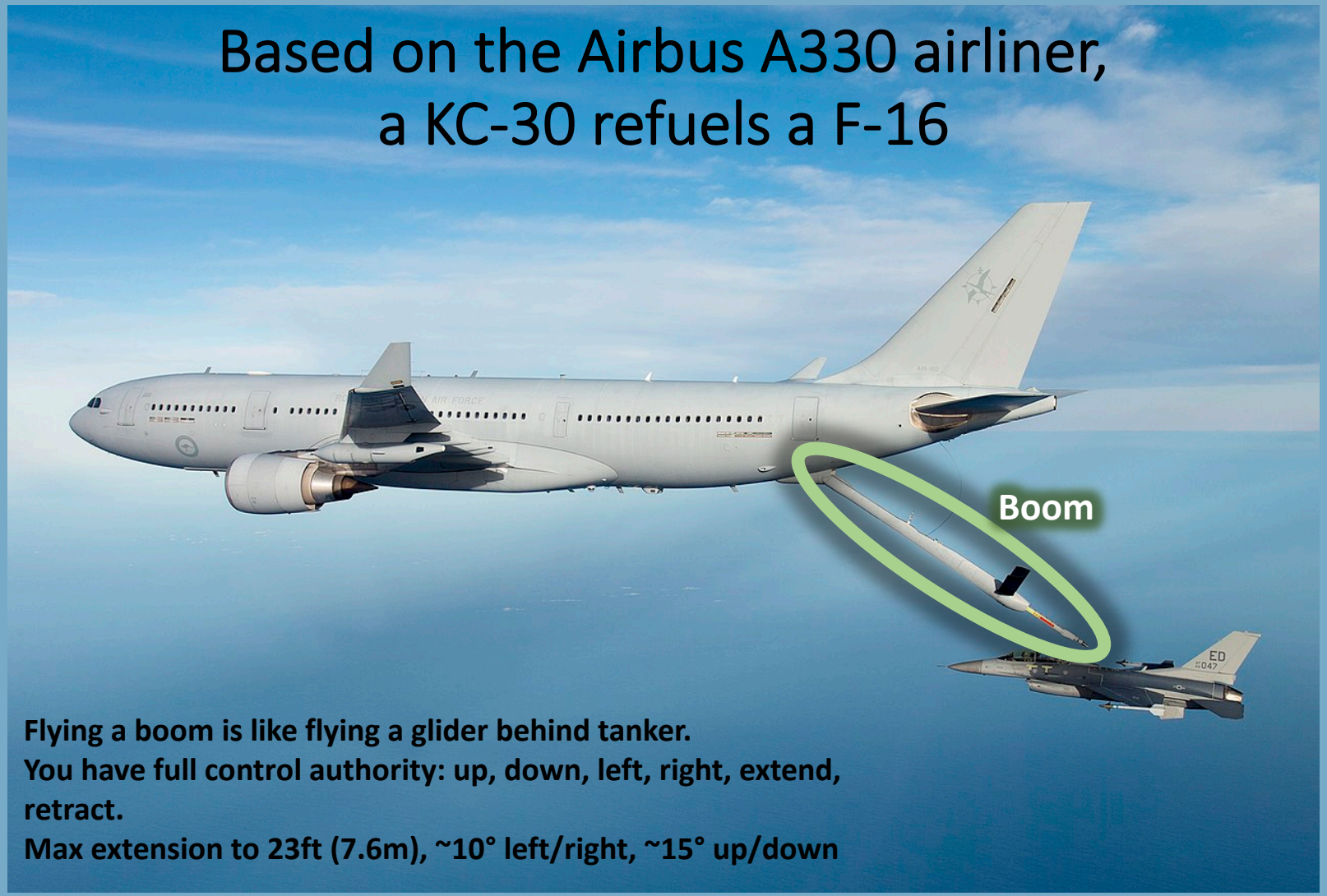
- Problem framing
- Identify accidents and hazards
- Draw the functional control structure
- Identify unsafe/unsecure control actions
- Identify security-related causal scenarios
- Wargame



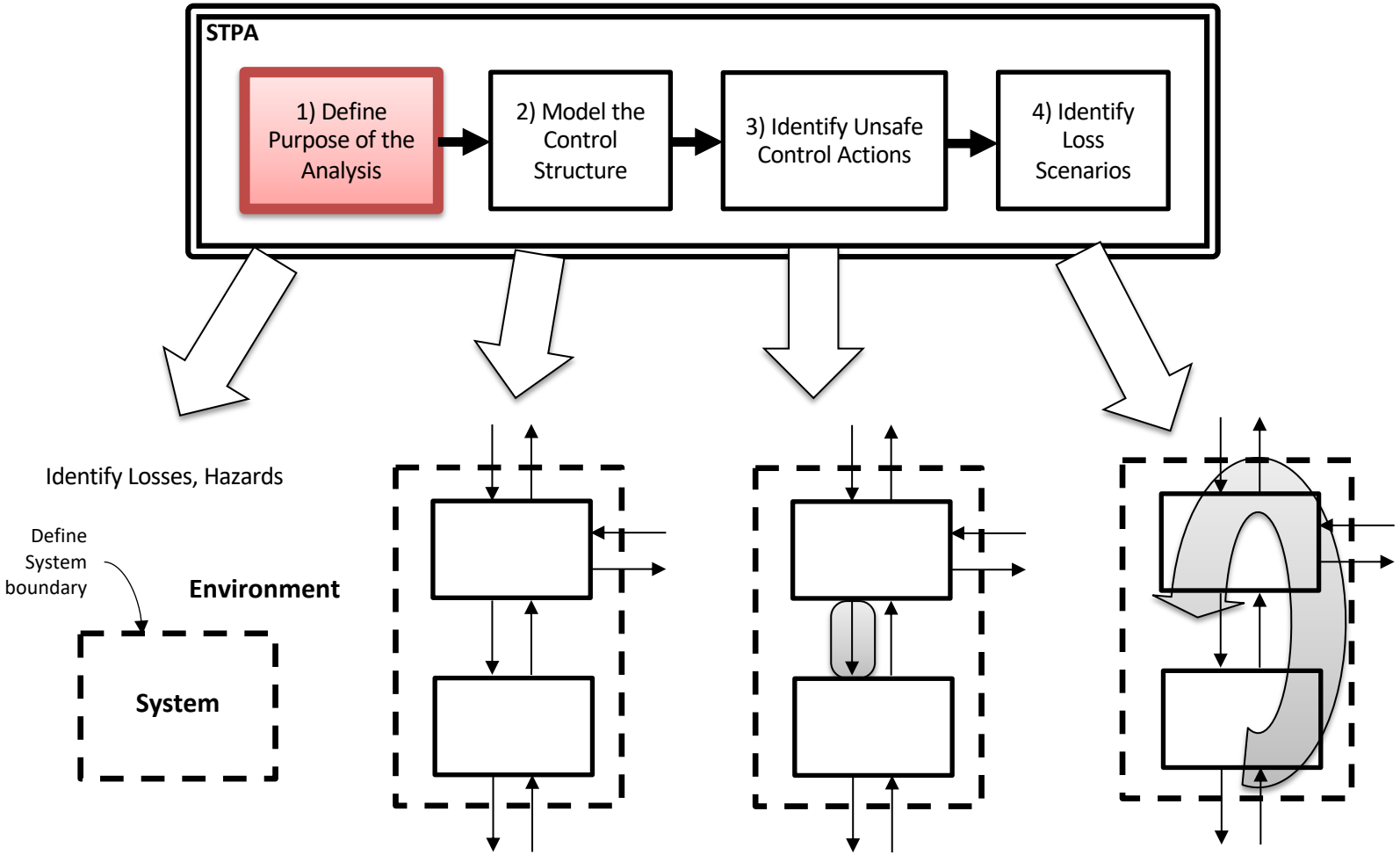
* Security Extension to STPA

© Copyright William Young, 2020

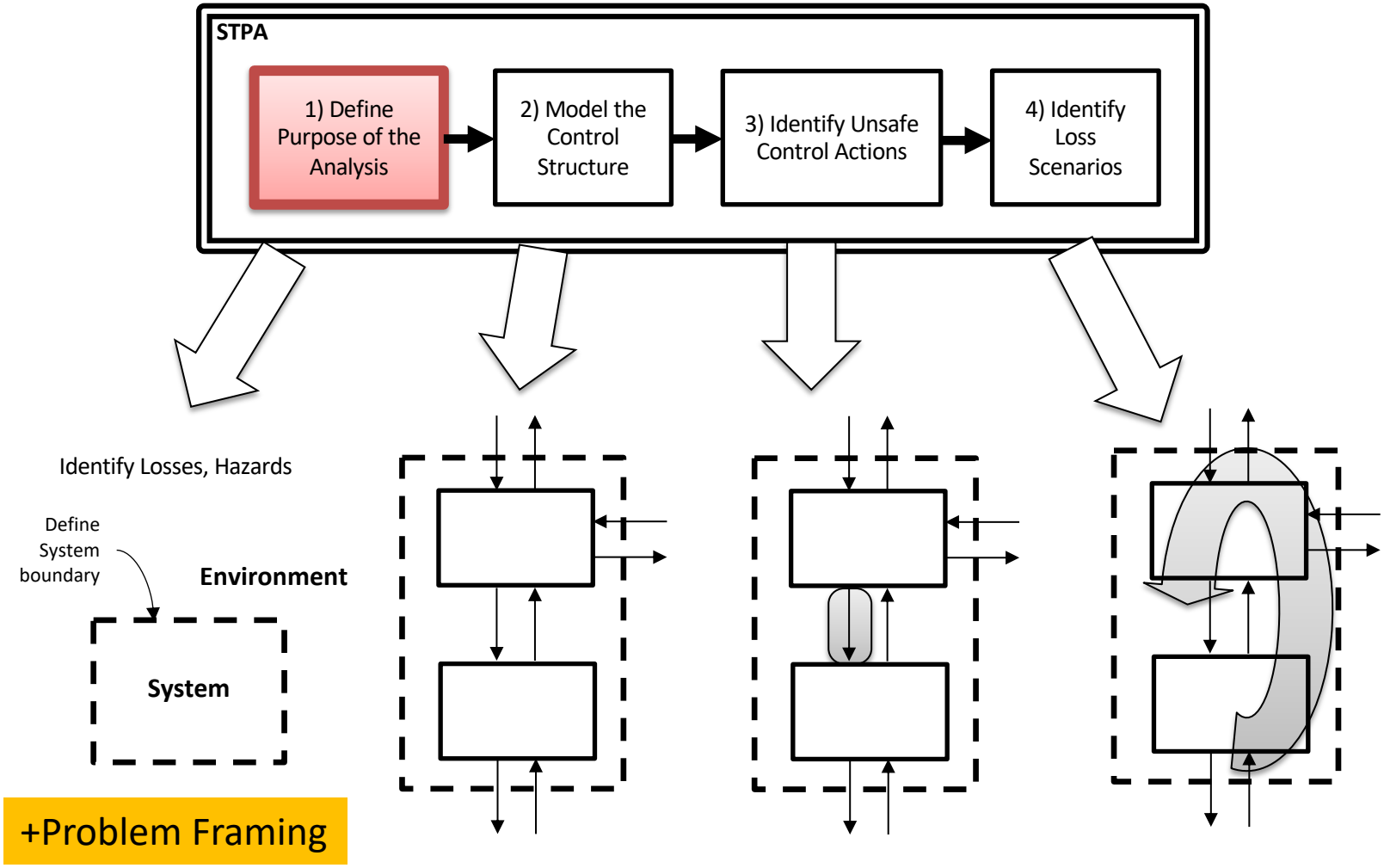
Based on the Airbus A330 airliner, a KC-30 refuels a F-16



Flying a boom is like flying a glider behind tanker.
You have full control authority: up, down, left, right, extend, retract.
Max extension to 23ft (7.6m), ~10° left/right, ~15° up/down



(Leveson and Thomas, 2018)

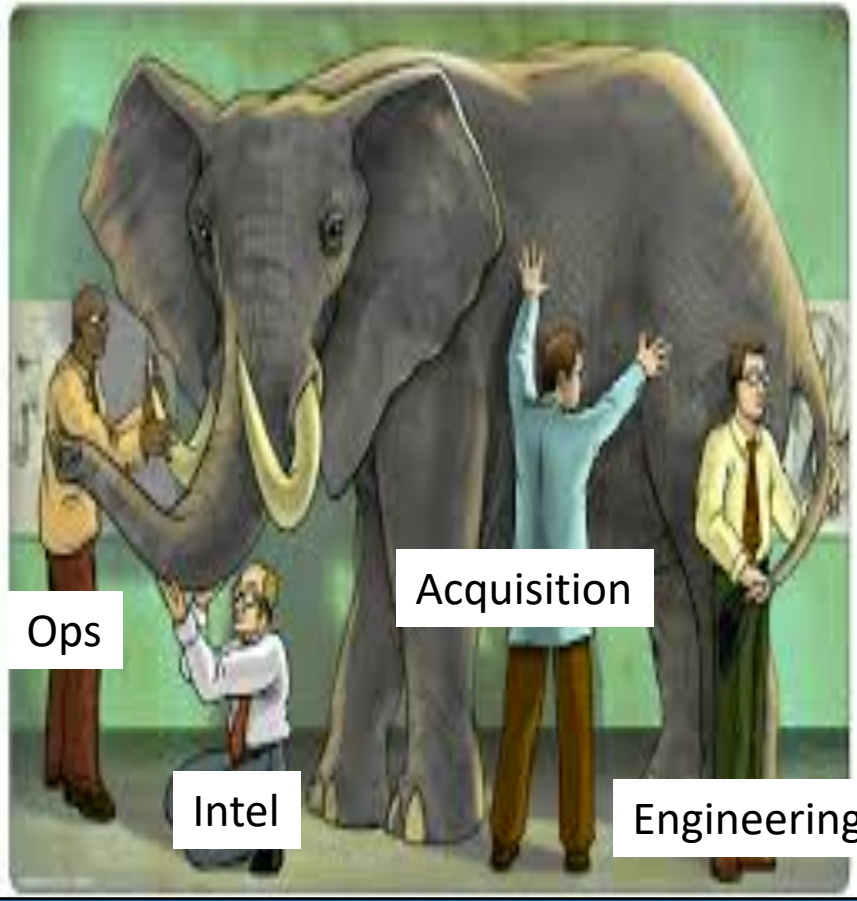


(Leveson and Thomas, 2018)

Problem Framing is Added to Defining the Purpose of the Analysis

Problem Framing

Problem Framing is Required for Wicked Problems



"By now we are all beginning to realize that one of the most intractable problems is that of defining problems (of knowing what distinguishes an observed condition from a desired condition) and of locating problems (finding where in the complex causal networks the trouble really lies). In turn, and equally intractable, is the problem of identifying the actions that might effectively narrow the gap between what-is and what-ought-to-be. "

Dilemmas in a General Theory of Planning. Horst Rittel and Melvin Webber, 1974

Wicked Problems Require Framing Before Any Progress Can Be Made

© Copyright William Young, 2020

Problem Framing in Security

- "Everything about this [cybersecurity] problem is complex: the technology, the policy, the interaction of technology and policy, also the politics, the economics, and the sociology. They're complex in many dimensions and their complexity is increasing over time…its what is known as **a wicked problem**."

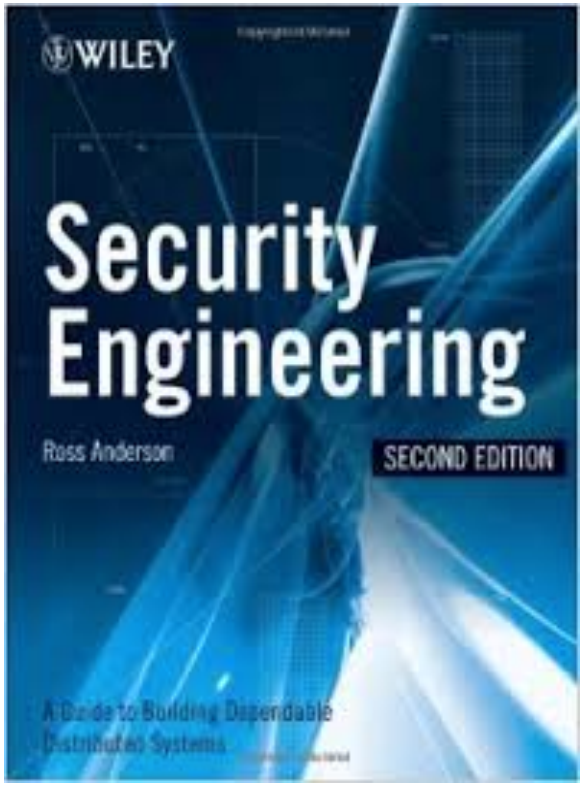
- Bruce Schneier, Click Here to Kill Everybody



Security is a Wicked Problem

Problem Framing Challenges in Security

- Determining life cycle security concepts
- Defining & specifying security objectives
- Defining & specifying security requirements
- Determining measures of success



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

Security Analysis Provides a Rigorous Manner to Identify What to Protect and How to Protect it

© Copyright William Young, 2020

Problem Framing in Security Done Right Can Be Powerful

- Military program office used the results of STPA-Sec problem framing to support limiting device functionality during a service-life extension
- Major Billion dollar military program office used STPA-Sec problem framing to gain sponsor approval to remove features

© Copyright William Young, 2020

Defining and Framing the Problem

- Overview: Synthesize a concise statement that describes what the system is supposed to do
- Elicit purpose, method, goals through discourse with stakeholders (& documents)
- Craft the description of the Functional Model
  - "A System to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"
    - Method will normally be a set of high-level activities representing stakeholders' essential tasks / activities

© Copyright William Young, 2020

Example Derived Load Alleviation System Problem Framing

PROBLEM: A System to Reduce structural loading on Boom and inadvertent disconnects

METHOD: By means of Measuring loads, Calculating corrections, Adjusting Boom position and movement

GOAL: In order to contribute to faster cycle times and lower operating costs

CONSTRAINTS / RESTRAINTS: While maximizing system autonomy and maintaining safety of flight.

STPA-Sec Process Generates Meaningful Dialogue and Learning That Sets the Foundation for Subsequent Analysis

© Copyright William Young, 2020

STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
  - L1: Loss of life or injury
  - L2: Damage to aircraft
  - L3: Loss of refueling mission
- What are some Aircraft-level Hazards?
  - H1: **Aircraft** violate minimum separation for refueling [L1,2,3]
  - H2: **Aircraft** airframe integrity is degraded [L1,2,3]
  - […]



After Problem Framing, the Rest of Part 1 is the Same Except For Adding Security-specific Losses and Hazards

STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
  - L1: Loss of life or injury
  - L2: Damage to aircraft
  - L3: Loss of refueling mission
- What are some Aircraft-level Hazards?
  - H1: **Aircraft** violate minimum separation for refueling [L1,2,3]
  - H2: **Aircraft** airframe integrity is degraded [L1,2,3]
  - […]



Can You Think of Any Security-Specific Losses?

STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
  - L1: Loss of life or injury
  - L2: Damage to aircraft
  - L3: Loss of refueling mission
  - L4: Loss of Critical Protected Information (CPI)
- What are some Aircraft-level Hazards?
  - H1: **Aircraft** violate minimum separation for refueling [L1,2,3]
  - H2: **Aircraft** airframe integrity is degraded [L1,2,3]
  - […]



Loss of CPI is a Security Related Loss that Falls Outside the Traditional Definition of Safety, But within the Definition Nancy Provided on Monday

WYOUNG@MIT.EDU

STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
  - L1: Loss of life or injury
  - L2: Damage to aircraft
  - L3: Loss of refueling mission
  - L4: Loss of Critical Protected Information (CPI)
- What are some Aircraft-level Hazards?
  - H1: **Aircraft** violate minimum separation for refueling [L1,2,3]
  - H2: **Aircraft** airframe integrity is degraded [L1,2,3]
  - […]



What is a Hazard Associated with Loss of CPI?

WYOUNG@MIT.EDU

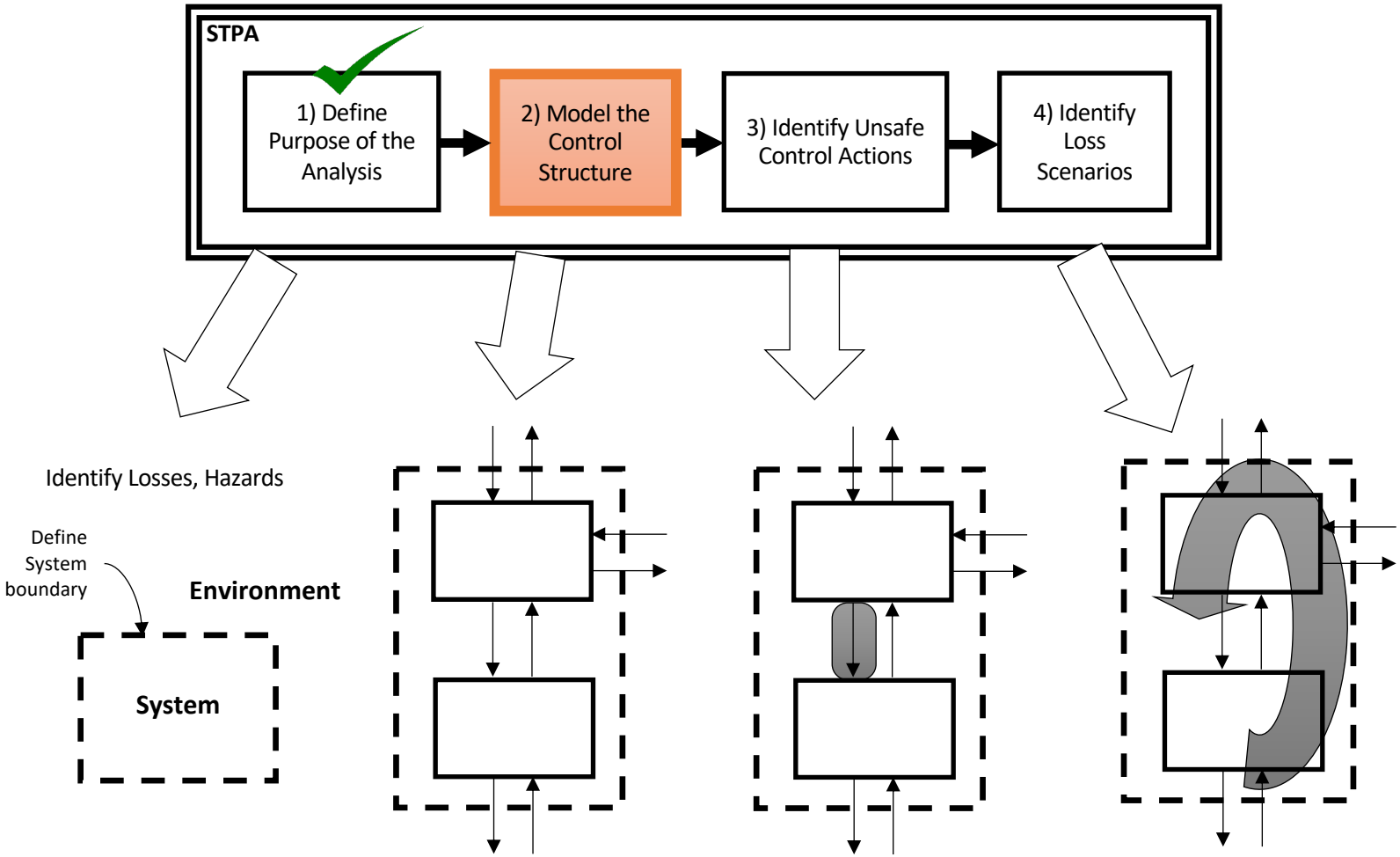
STPA Step 1: Define Purpose of the Analysis

- What are some Losses?
  - L1: Loss of life or injury
  - L2: Damage to aircraft
  - L3: Loss of refueling mission
  - L4: Loss of Critical Protected Information (CPI)
- What are some Aircraft-level Hazards?
  - H1: **Aircraft** violate minimum separation for refueling [L1,2,3]
  - H2: **Aircraft** airframe integrity is degraded [L1,2,3]
  - […]
  - Hn: **Aircraft** CPI Exposed to Unauthorized Individual



Exposing Aircraft CPI is a Hazard That Must Be Controlled

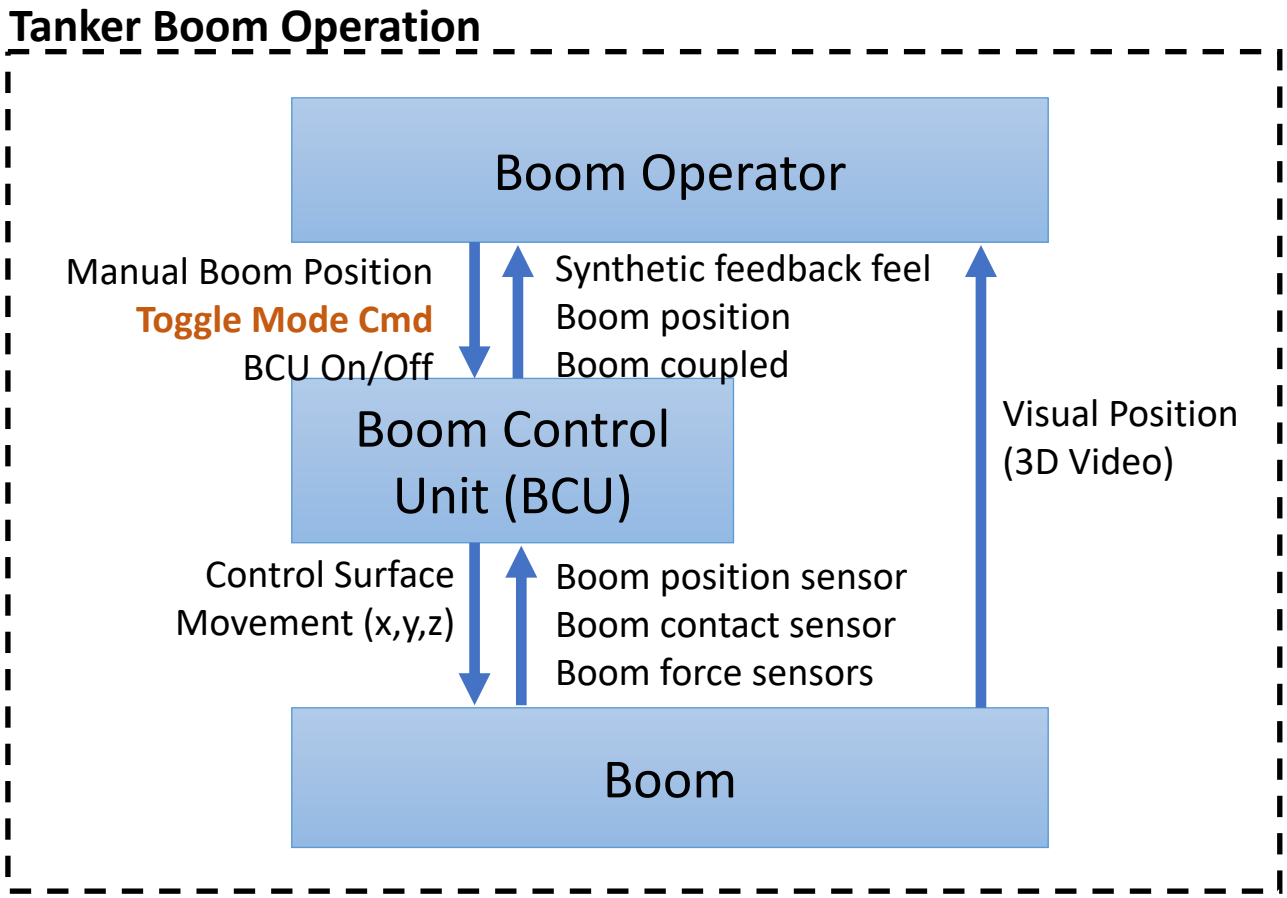
WYOUNG@MIT.EDU



Phase 2 Remains the Same

WYOUNG@MIT.EDU

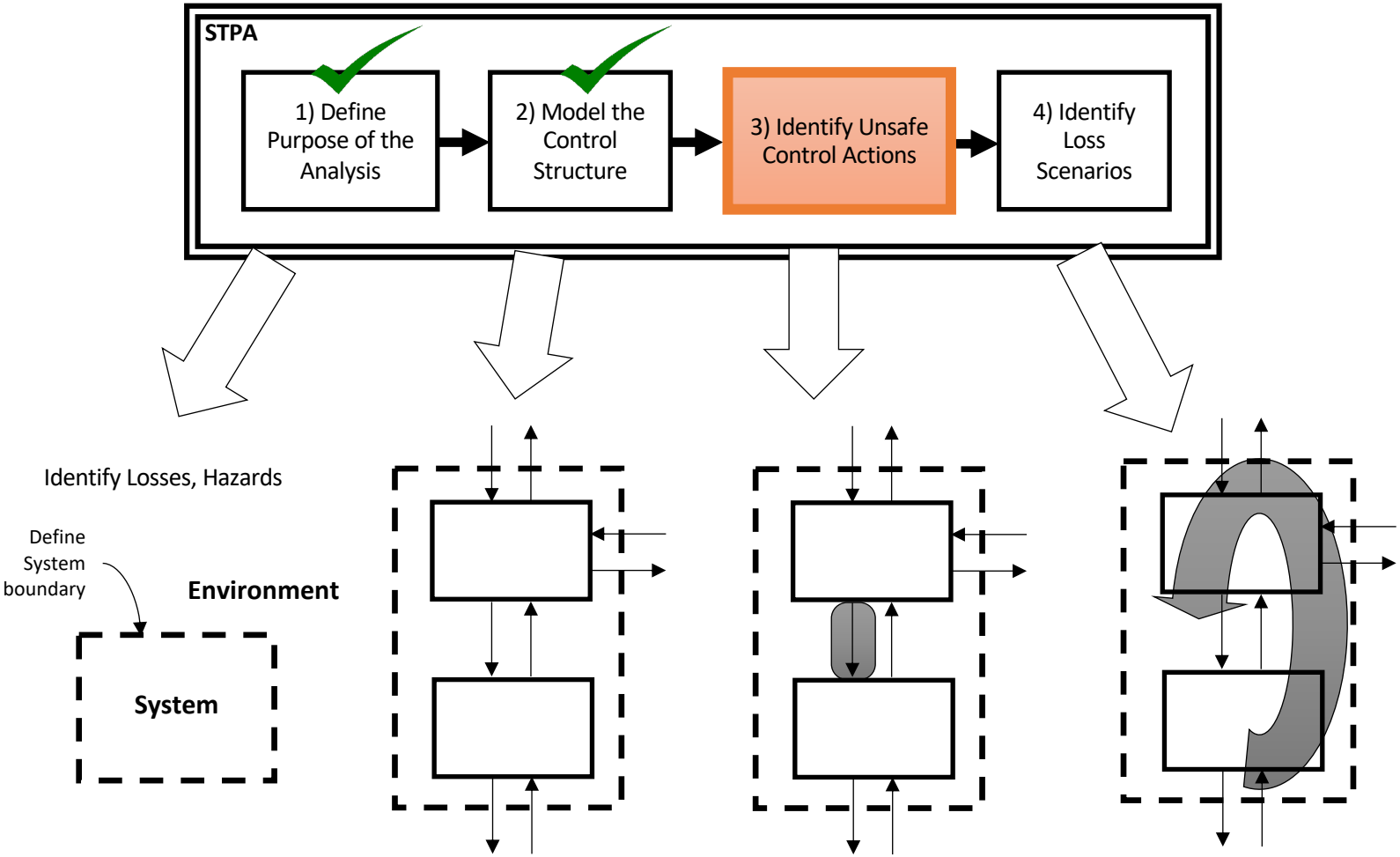
Our Control Structure From Yesterday



Please contact JThomas4@MIT.EDU with any questions!

© Copyright John Thomas 2020

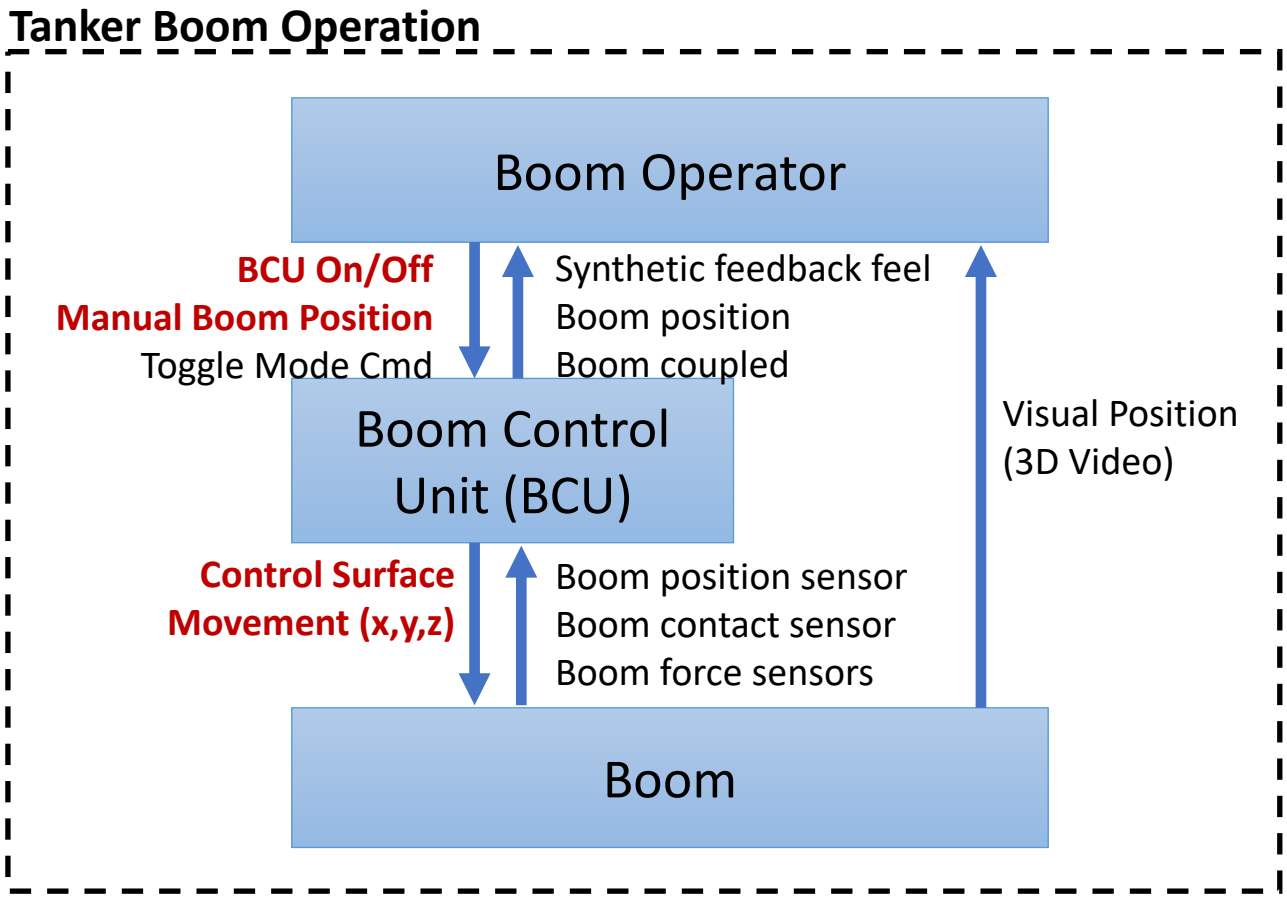
WYOUNG@MIT.EDU



Phase 3 Remains the Same

WYOUNG@MIT.EDU

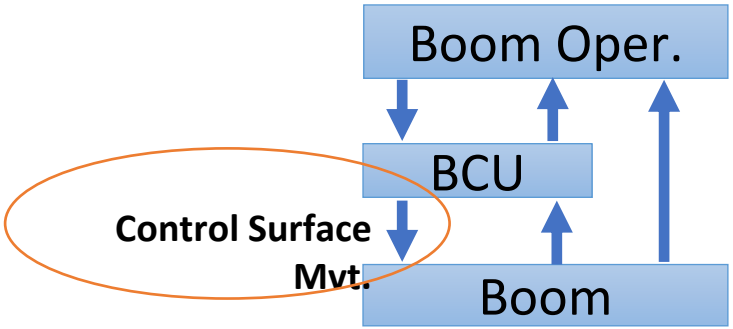
Analyze control actions



Please contact JThomas4@MIT.EDU with any questions!

© Copyright John Thomas 2020

Identify Unsafe (Hazardous) Control Actions

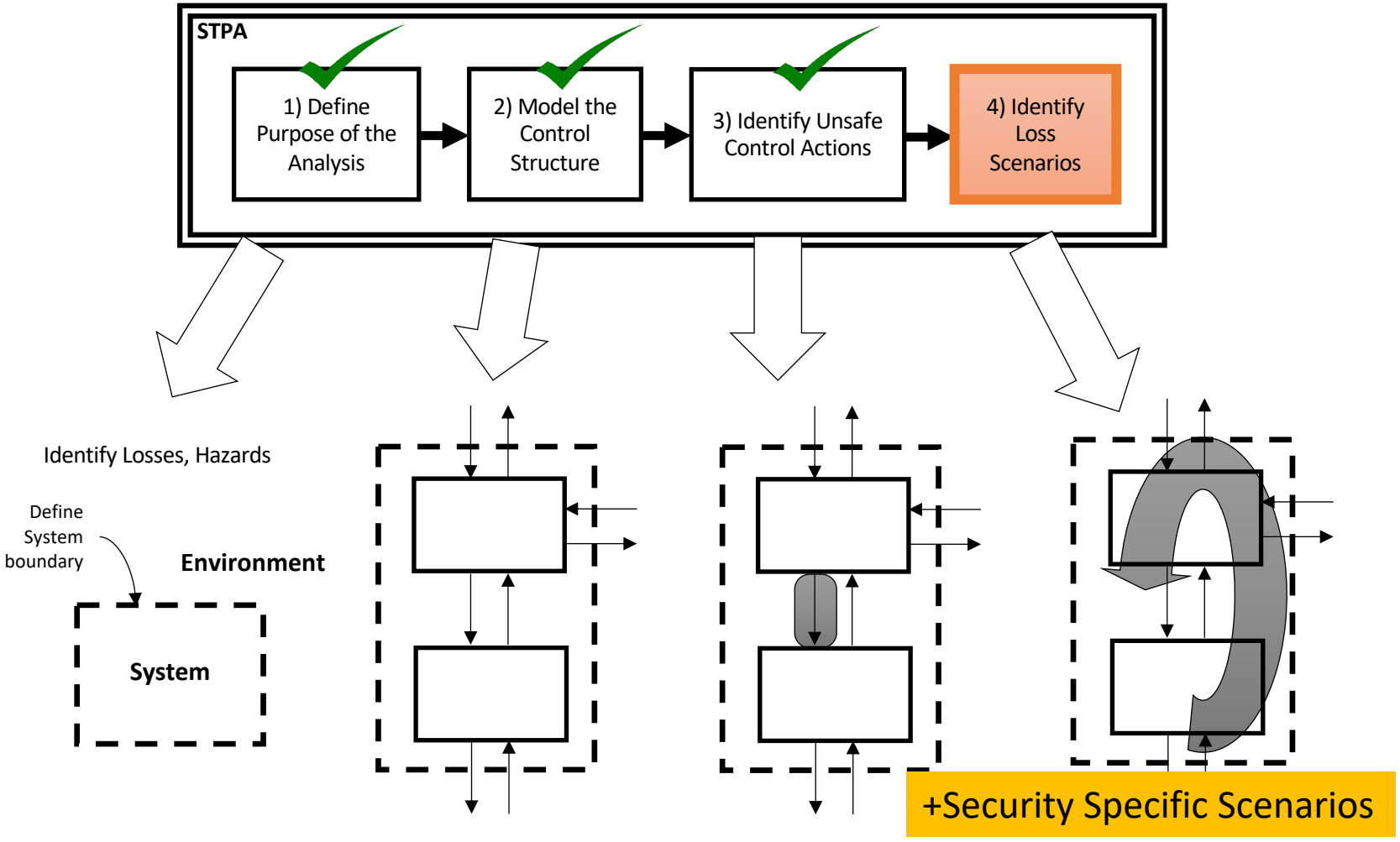


Suppose the Boom is Not Coupled…

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Control Surface Movement Cmd	BCU does not provide Movement Cmd when Boom Operator moves Stick […]	BCU provides Movement Cmd when Boom Operator does not move Stick BCU provides Movement Cmd when Boom Operator has turned BCU Off BCU provides Movement Cmd in wrong direction (does not match Stick direction) BCU provides excessive Movement Cmd beyond amount of Stick movement [insufficient, oscillatory, repetitive, etc.]	BCU provides Movement Cmd too late (more than TBD sec) after before Boom Operator moves Stick […]	BCU continues providing Movement Cmd too long after Boom reaches position commanded by Stick Cmd too soon before Boom reaches position commanded by Stick […]

Is this Safety or Security? Both!

Please contact JThomas4@MIT.EDU with any questions!
© Copyright John Thomas 2020



Phase 4 Adds Security Specific Scenario Generation and Wargaming

WYOUNG@MIT.EDU
© Copyright William Young, 2020

Developing Security Scenarios

Challenges to Developing Security-related Scenarios Using Traditional Model

- Difficult to understand interactions among components
- Difficult to capture “non-technical” aspects (e.g. policy)
- May waste efforts on scenarios that aren’t valued by stakeholders
- Difficult to calibrate how secure is “secure enough”
- Require a complete or nearly complete architecture

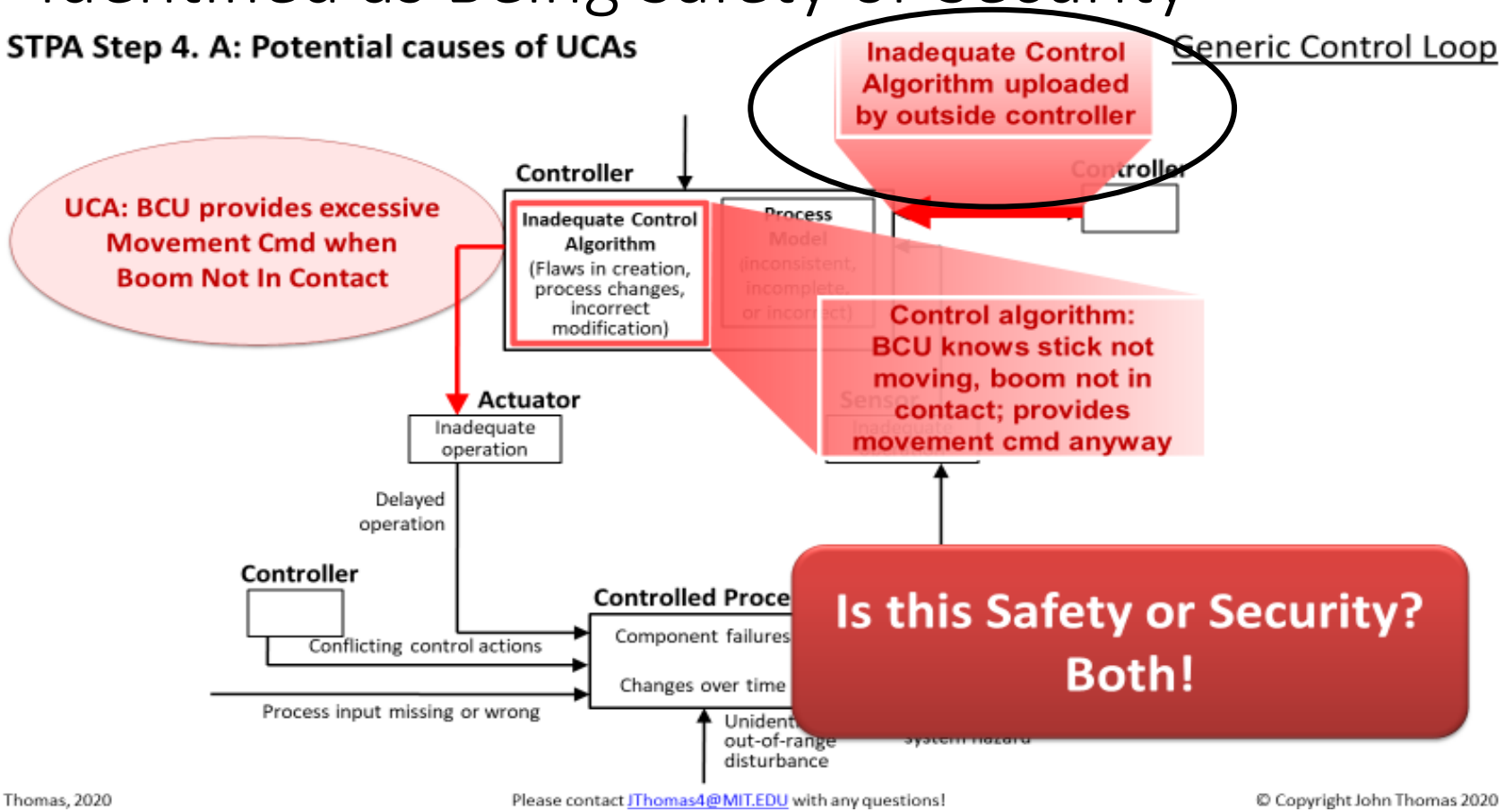
© Copyright William Young, 2020

Security Scenarios with STPA-Sec

- Best Practice is to have safety and security experts developing scenarios together
- Generate more scenarios with more interactive complexity
- STPA-Sec scenarios help identify functional vulnerabilities
- Scenarios developed using
  - STPA Analysis if available
  - Formal STPA
- Security-related tools such as STRIDE can be used to classify attacks and translate results for security-related solutions

Security Scenarios are Often Same as "Safety" Scenarios, but have Security Related Causes and Solutions

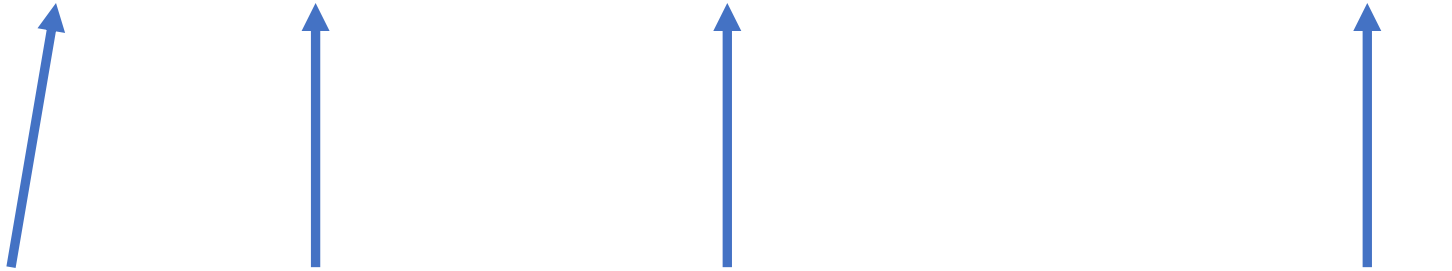
Lets Walk Through a Scenario John Thomas Identified as Being Safety or Security



Scenario: BCU Provides Excessive Movement Command when Boom Not in Contact Because BCU has a Flawed Control Algorithm

Security-Related Scenarios

- To launch a successful cyber attack, adversary has to solve their own control problem
  - <**Exploit**> <**Provides**><**Update to BCU Control Algorithm**> when <**Context**>

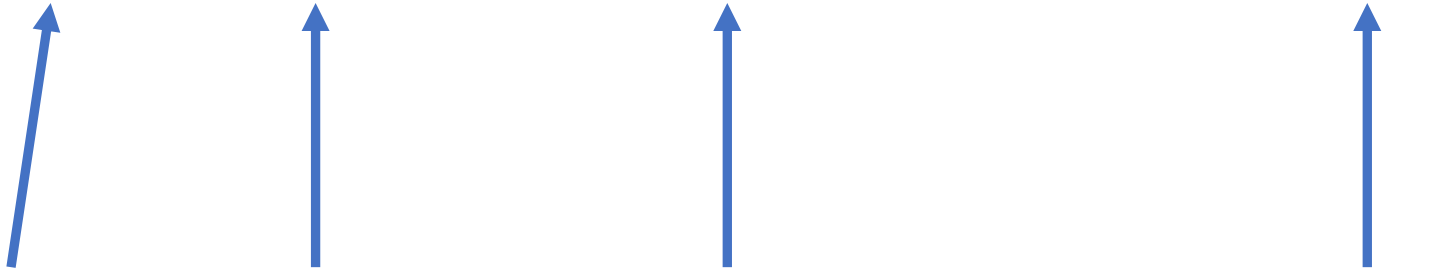


These are the Same Elements of a Hazardous (Unsafe) Control Action

© Copyright William Young, 2020

Security-Related Scenarios

- To launch a successful cyber attack, adversary has to solve their own control problem
  - <**Exploit**> <**Provides**><**Update to BCU Control Algorithm**> when <**Context**>

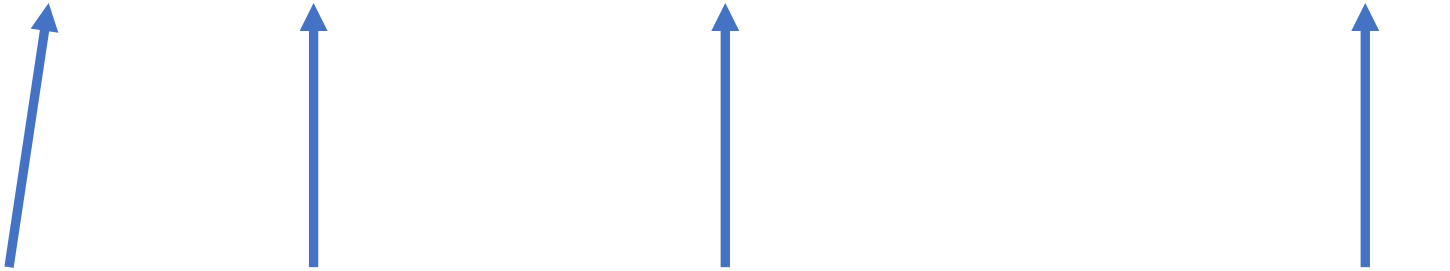


The Adversary Has to Solve Their Own Control Problem to Cause the Hazardous Scenario (via Successful Attack) on our System!

© Copyright William Young, 2020

Security-Related Scenarios

- To launch a successful cyber attack, adversary has to solve their own control problem
  - <**Exploit**> <**Provides**><**Update to BCU Control Algorithm**> when <**Context**>

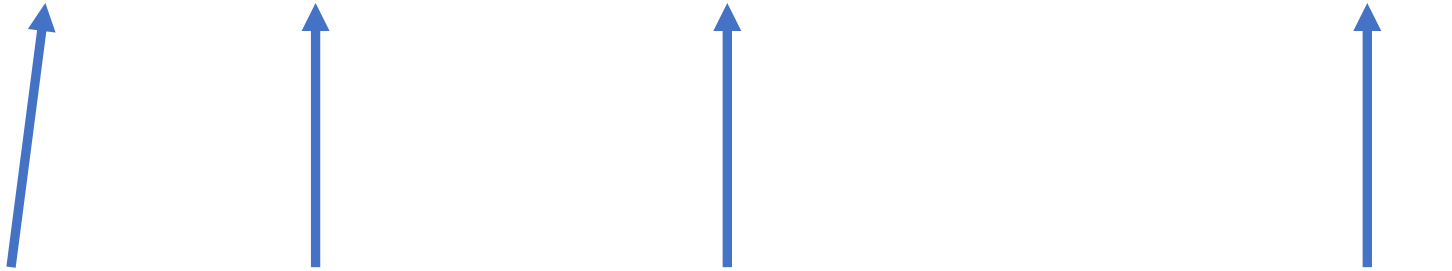


Might Viewing Security Through this Lens Open Entirely New Opportunities to Build More Secure Systems?

© Copyright William Young, 2020

Security-Related Scenarios

- To launch a successful cyber attack, adversary has to solve their own control problem
  - <**Exploit**> <**Provides**><**Update to BCU Control Algorithm**> when <**Context**>



We Will Discuss in Much Greater Detail As Part of Wargaming

© Copyright William Young, 2020

WARGAMING

Wargaming History

- Help officers visualize and adapt to changing and unpredictable socio-technical events
- “Free, practical, artistic activity” that set conditions for success
- Part of a learning toolkit, predict what hasn’t happened yet
  - “Discover weaknesses before adversaries do”
- Helps combat against “failures of imagination”
- Combat cognitive bias



Von Moltke the Elder

Wargaming is Pen-testing Your Security Concept

© Copyright William Young, 2020

Wargaming in Security Engineering

- Adds a human adversary into the process
  - "Thinking adversary" is often highlighted as the difference between safety and security
  - Captures well-intentioned "work-arounds" necessary to execute missions but posing hazard (safety connection)?
- Provides Insight into feasibility and level of effort necessary to execute scenarios
- Can point out unintended bias and facilitate new insights into novel solutions

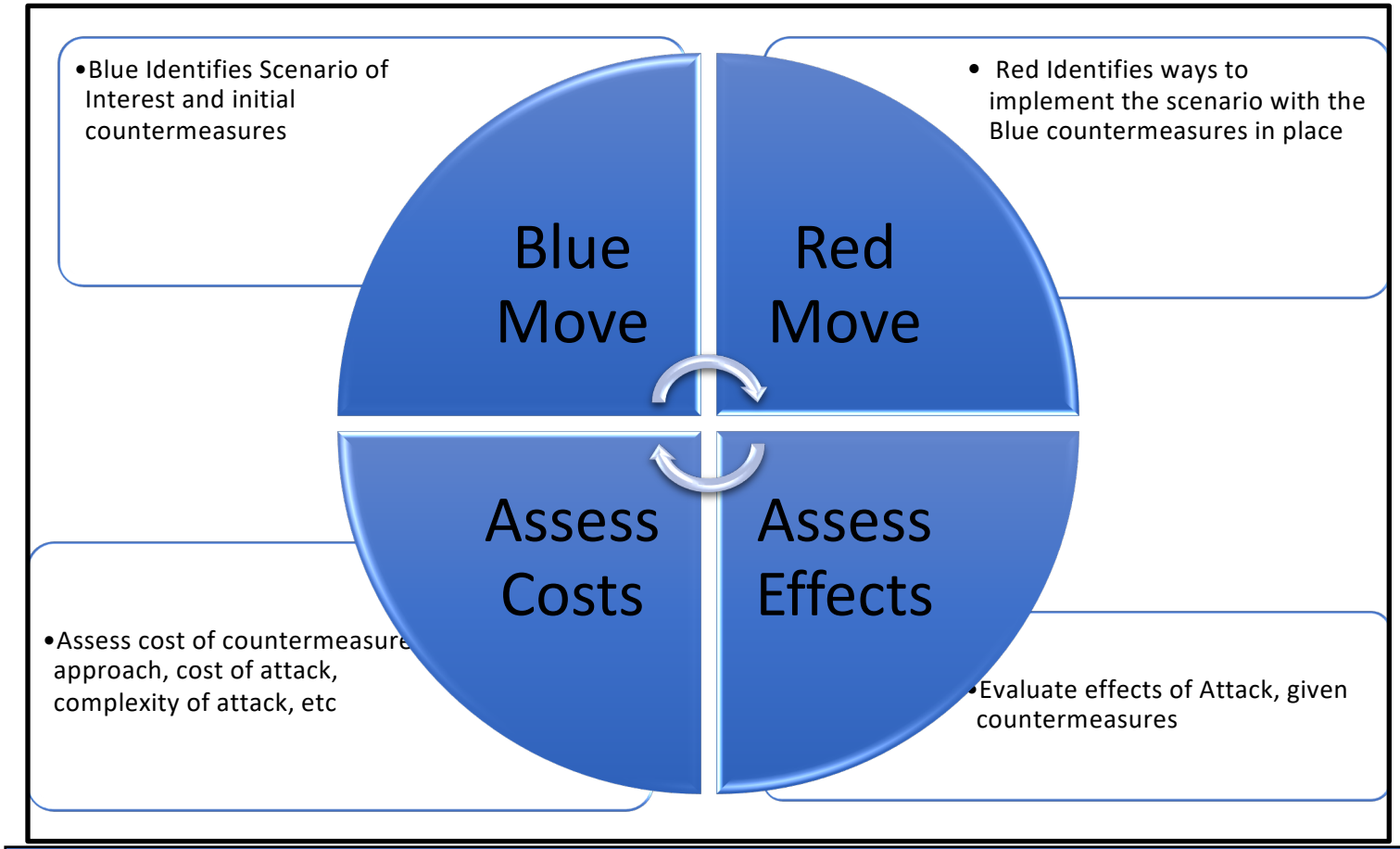
© Copyright William Young, 2020

STPA-Sec Wargaming Approach

- Begins at Concept Stage of Engineering Design Lifecycle
- Assess classes of attacks that can produce particular scenarios identified via STPA-Sec (or STPA)
- Assess potential effectiveness of classes of controls
- Understand complexity of executing classes of attacks
- Supports assessment of operational risk associated with particular functions or features under consideration

© Copyright William Young, 2020

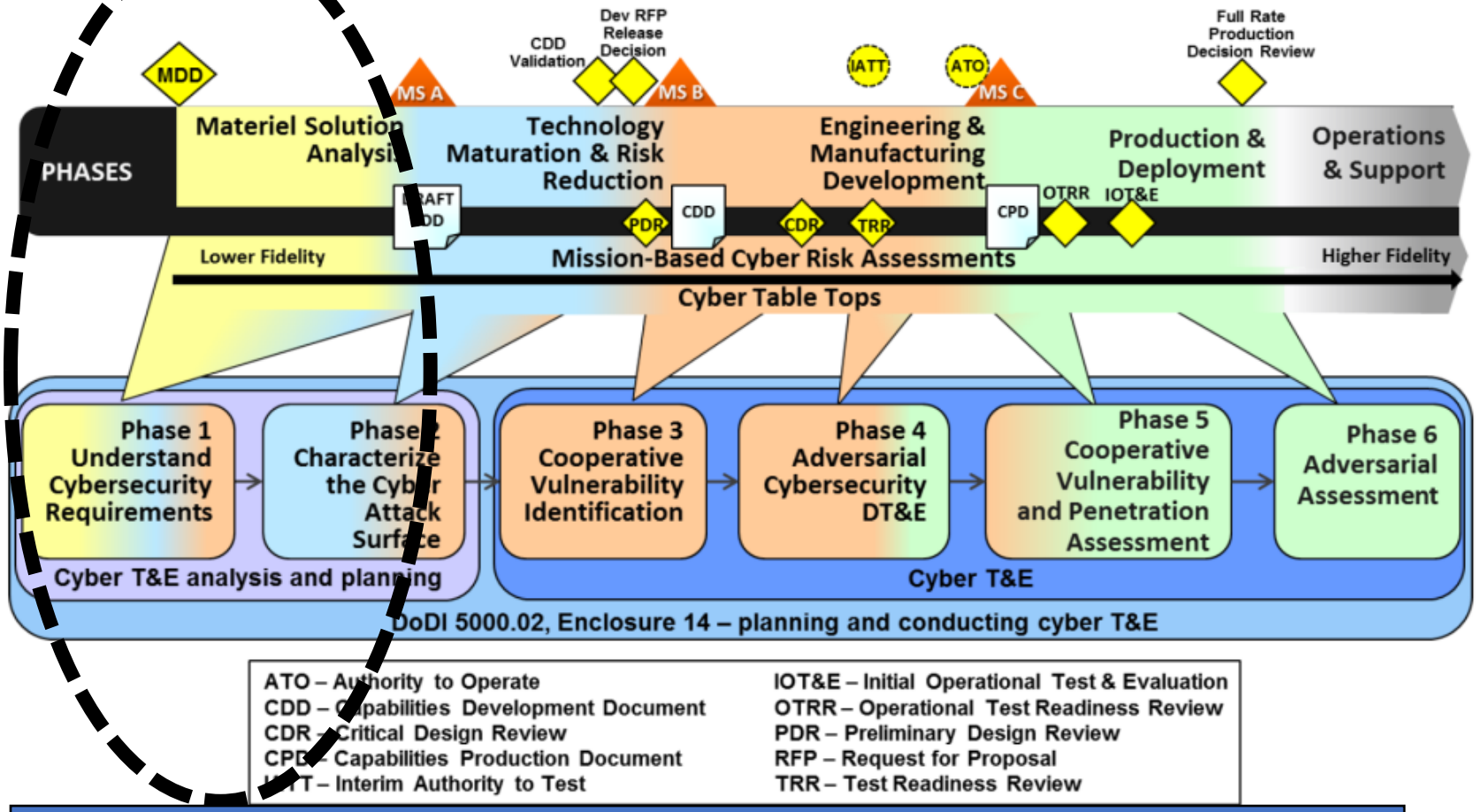
STPA-Sec Wargaming Approach



STPA-Sec Wargaming Can Be Implemented Through Any Preferred Methodology (e.g. DoD Cyber Table Top)

© Copyright William Young, 2020

DoD Cyber Table Top

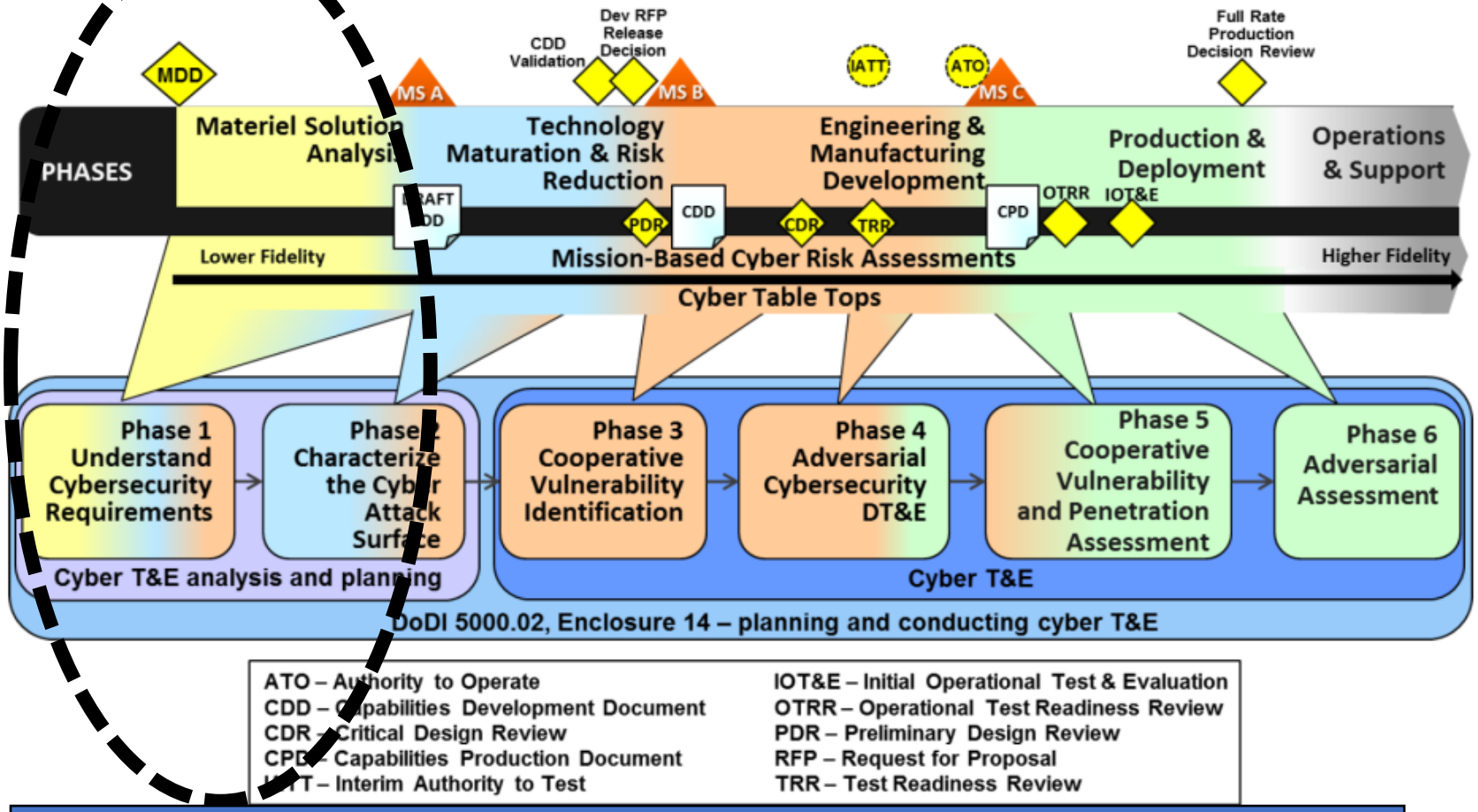


CTTs can be us at any Time in the System Life Cycle

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

DoD Cyber Table Top

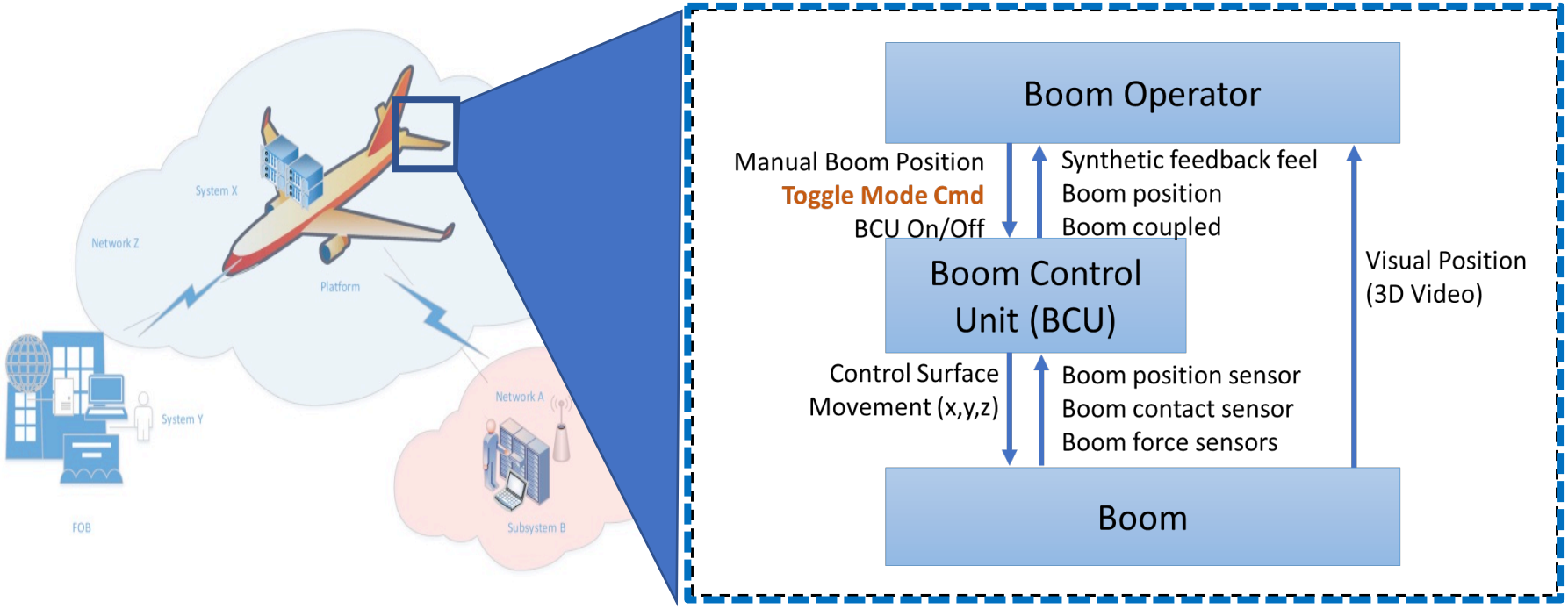


Lets Look at STPA-Sec Support to Early CTT

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

Identifying Sub-System Under Analysis in CTT

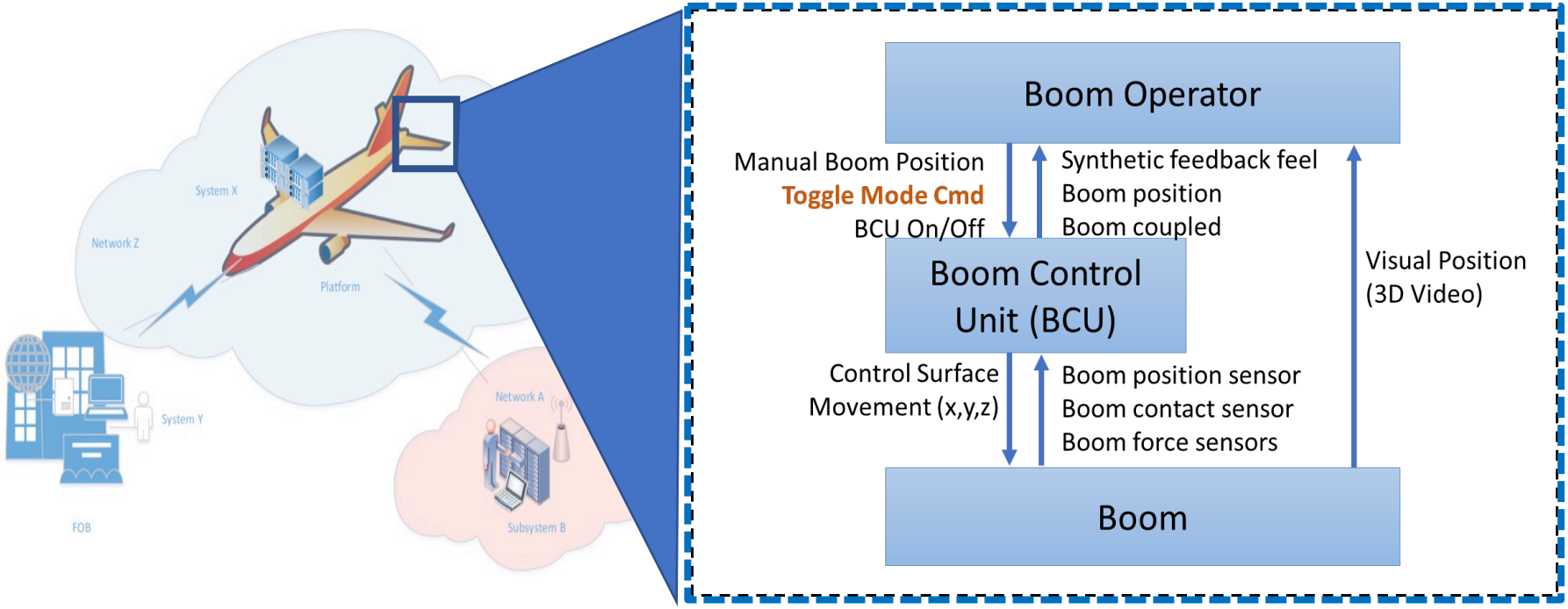


The Previously Developed Control Structure Captures Functions of the Sub-System Under Analysis

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

Identifying Sub-System Under Analysis in CTT

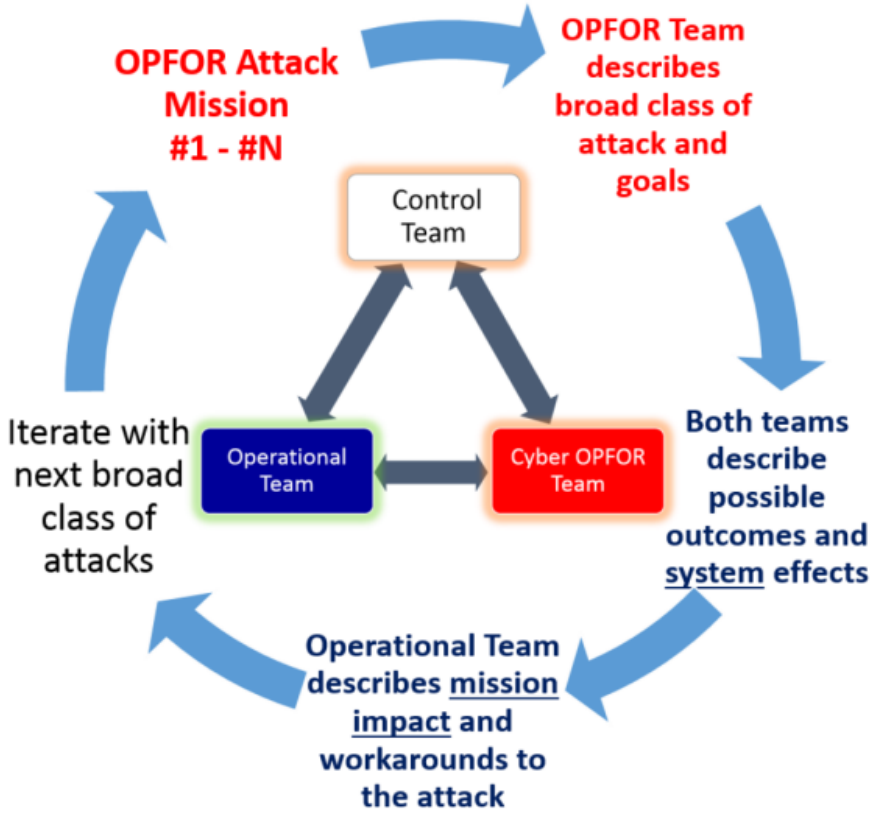


The Control Structure is Representative of the Level of Detail Available Very Early in the Concept Stage of the System Development Lifecycle

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

DoD Cyber Table Top (CTT) Process

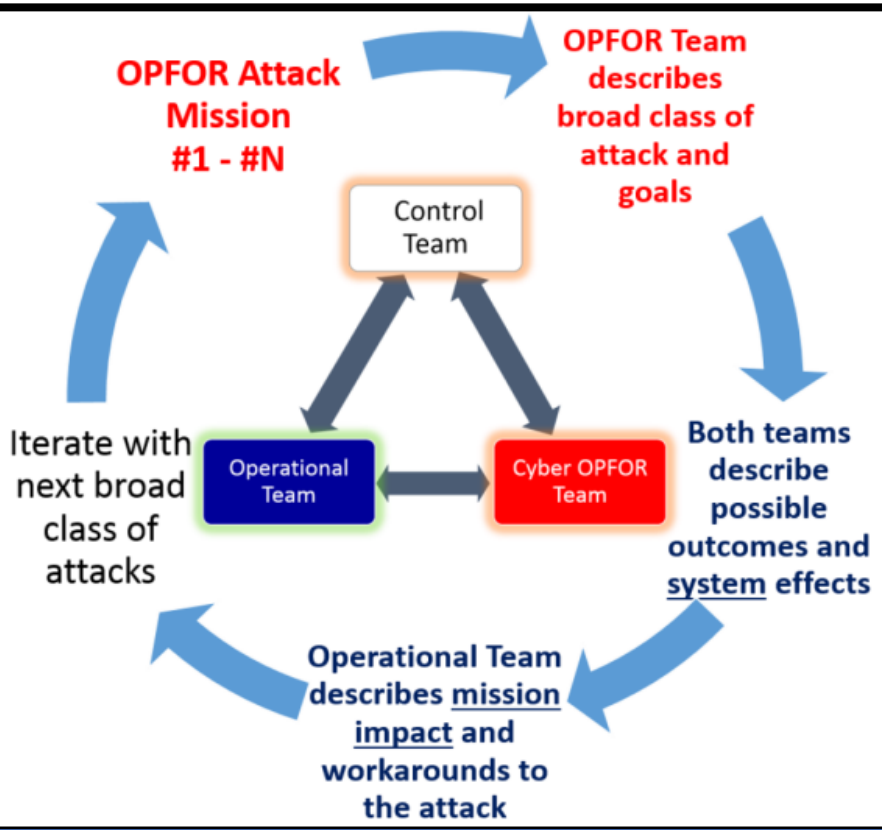


Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT)

BCU provides excessive Movement CMD when Boom is in Contact because BCU believes Boom is Not in contact due to delayed pulse feedback



Begin Move with HCA and Scenario Identified via STPA-Sec (or STPA)

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Scenario

BCU provides excessive Movement CMD when Boom is in Contact because BCU believes Boom is Not in contact due to delayed pulse feedback

Based on the Scenario, What are the Relevant Effects of a Successful Attack on the Sub-System Under Analysis (BCU)?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Scenario

BCU provides excessive Movement CMD when Boom is in Contact because BCU believes Boom is Not in contact due to **delayed pulse feedback**

Successful Attack will Delay Pulse Feedback

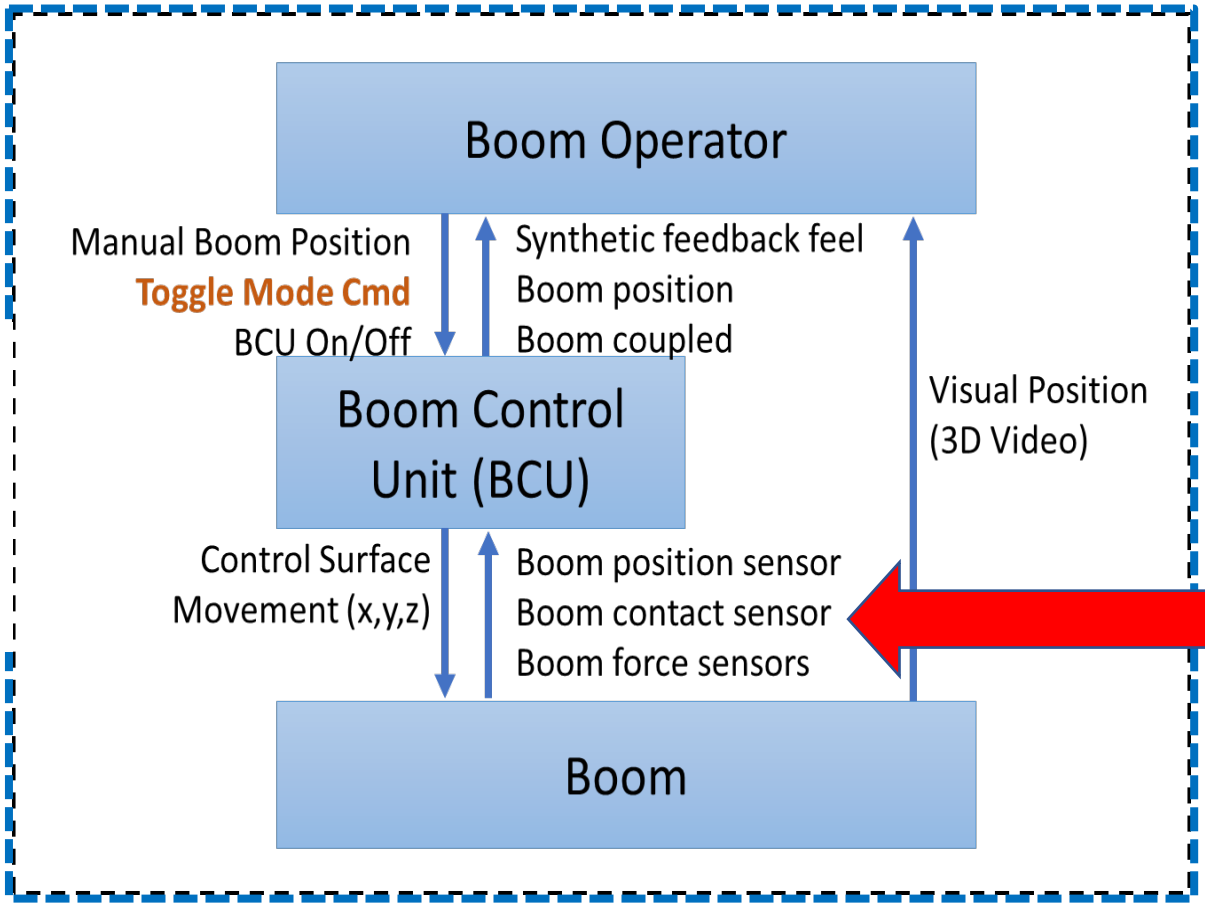
Examining the Control Structure Provides Additional Insight Into the Broad Class(es) of Potential Attacks

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals





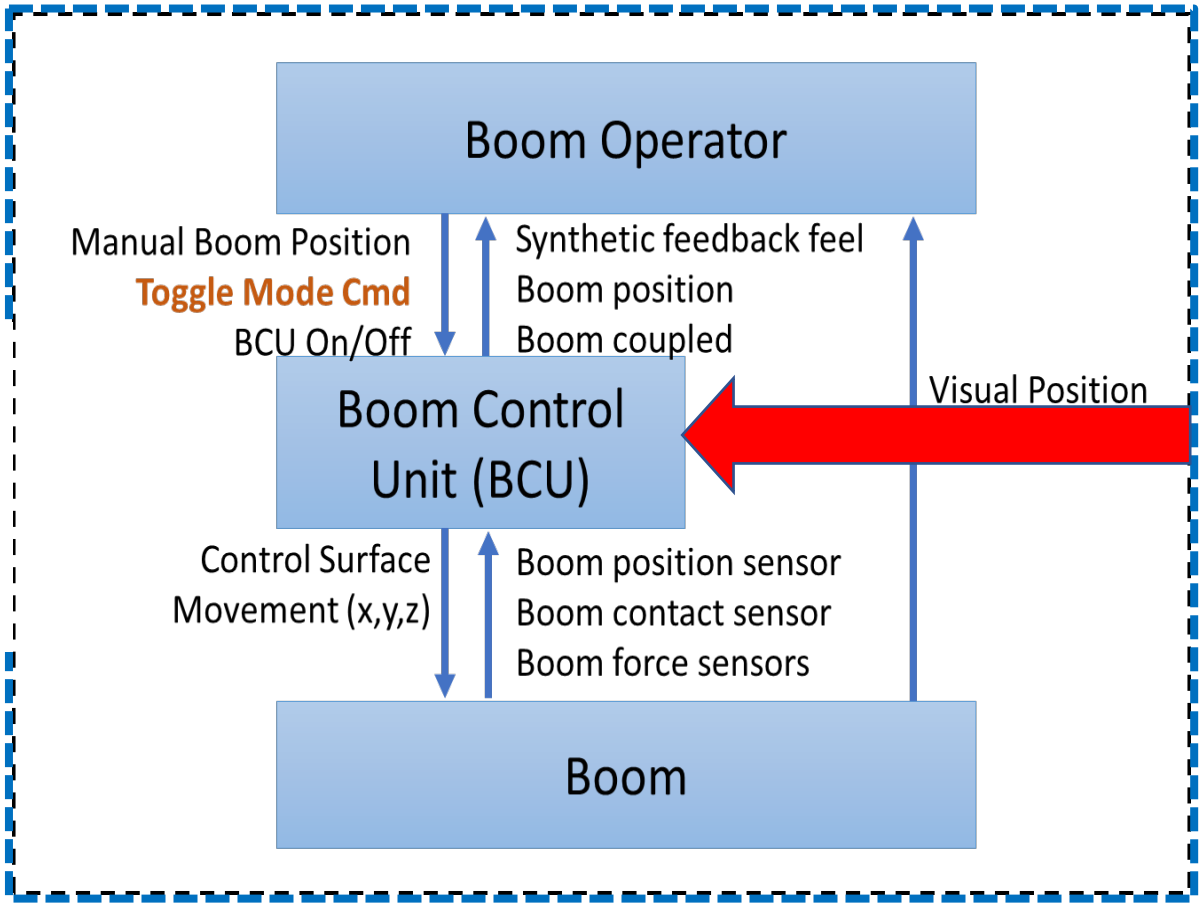
What Element(s) Does the Attack Impact?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals





Delayed *Processing* of Pulse Feedback

What Element(s) Does the Attack Impact?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Element Impacted	Effect	Attack Class
Boom Contact Sensor	Delayed Pulse Feedback	
Boom Control Unit	Delayed Processing of Boom Contact Sensor Pulse	

Using STRIDE, What Broad Classes of Attack Might Delay the Pulse Feedback from the Boom Contact Sensor?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Element Impacted	Effect	Attack Class
Boom Contact Sensor	Delayed Pulse Feedback	Denial of Service, Tampering
Boom Control Unit	Delayed Processing of Boom Contact Sensor Pulse	

Using STRIDE, What Broad Classes of Attack Might Delay BCU processing of the Pulse Feedback from the Boom Contact Sensor?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Element Impacted	Effect	Attack Class
Boom Contact Sensor	Delayed Pulse Feedback	Denial of Service, Tamper
Boom Control Unit	Delayed Processing of Boom Contact Sensor Pulse	Denial of Service

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Scenario

BCU provides excessive Movement CMD when Boom is in Contact because BCU believes Boom is Not in contact due to delayed pulse feedback

Returning to the Scenario, What is the Goal of the Attack?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



Scenario

BCU provides excessive Movement CMD when Boom is in Contact because BCU believes Boom is Not in contact due to delayed pulse feedback

OPFOR Must Not Cause the BCU to Provide Excessive Movement CMD, BUT Must do so when the Boom is in Contact

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 1-OPFOR Describes Broad Class Of Attack and Goals



OPFOR Details for Move Derived from STPA-Sec Analysis

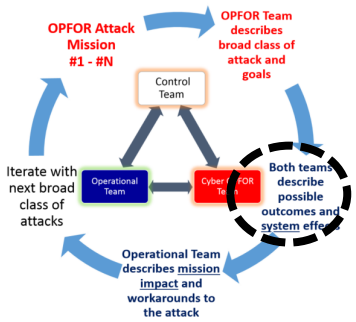
1) Potential Targets
2) Desired Effects
3) Goals of Attack
4) Potential Attack Classes
5) Context under which Attack must succeed

OPFOR Is Now Equipped to Provide A Much Richer Attack Move!

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 2-Teams Describe Outcomes and Move Effects



Basic Rules (STPA-Sec)

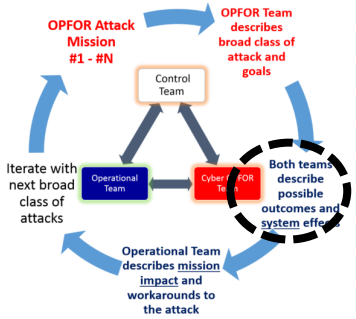
1) Control Structure is "playing field"
2) Remain at current level of abstraction
3) Assumptions must be clearly stated
4) OPFOR Must adhere to context requirements

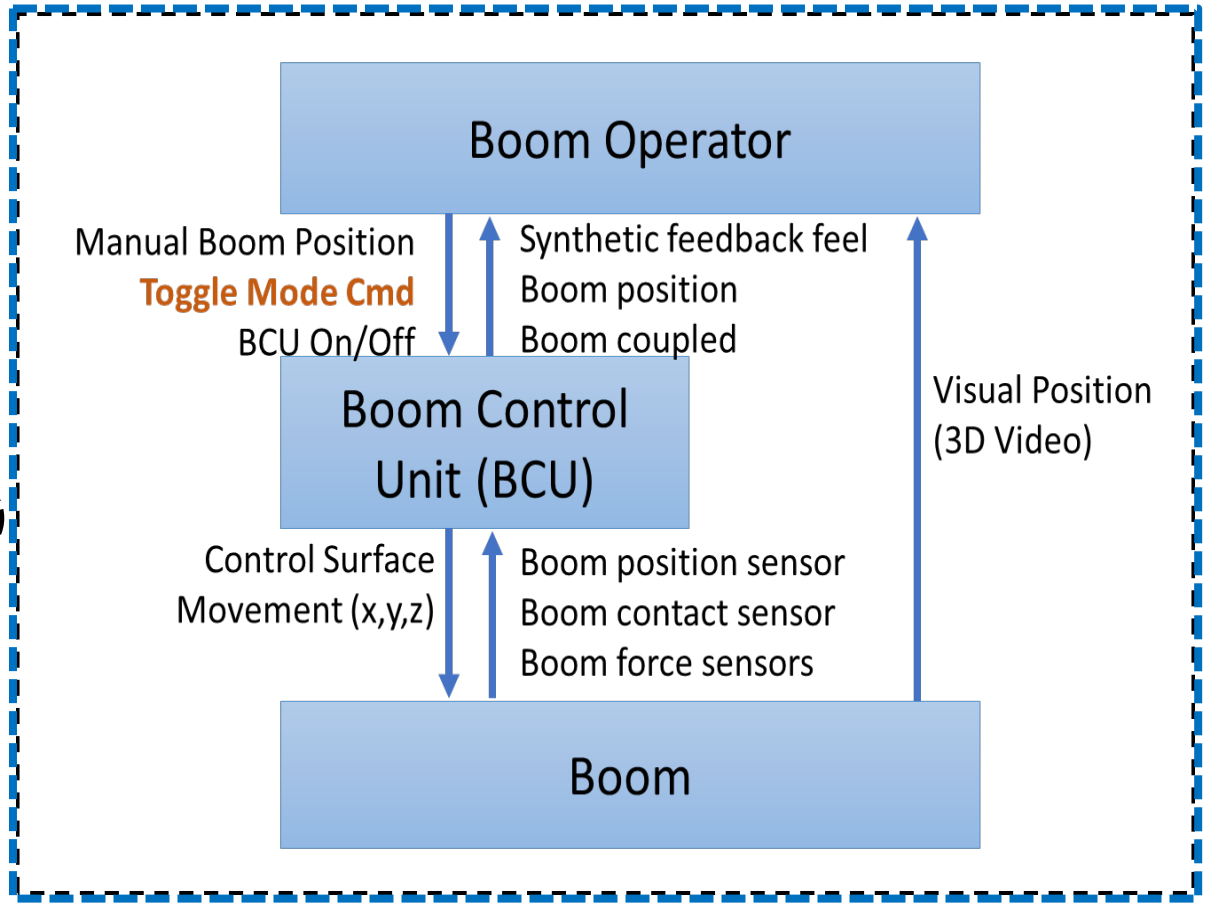
Lets Look at the Context Requirement

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 2-Teams Describe Outcomes and Move Effects



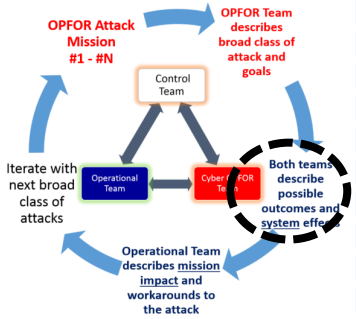


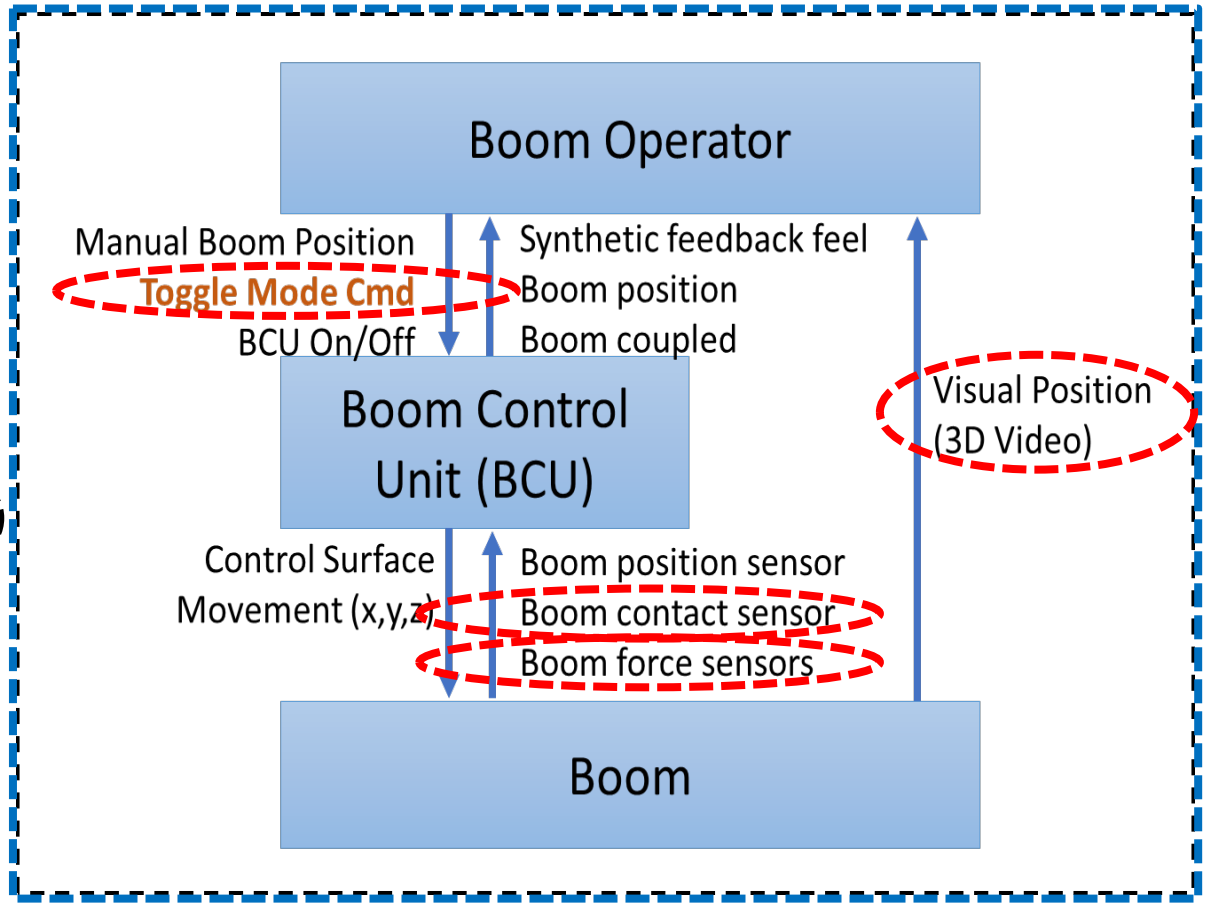
Based on the Control Structure, How Might OPFOR Determine when "Boom is in Contact" to Launch a Denial of Service Attack?

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 2-Teams Describe Outcomes and Move Effects

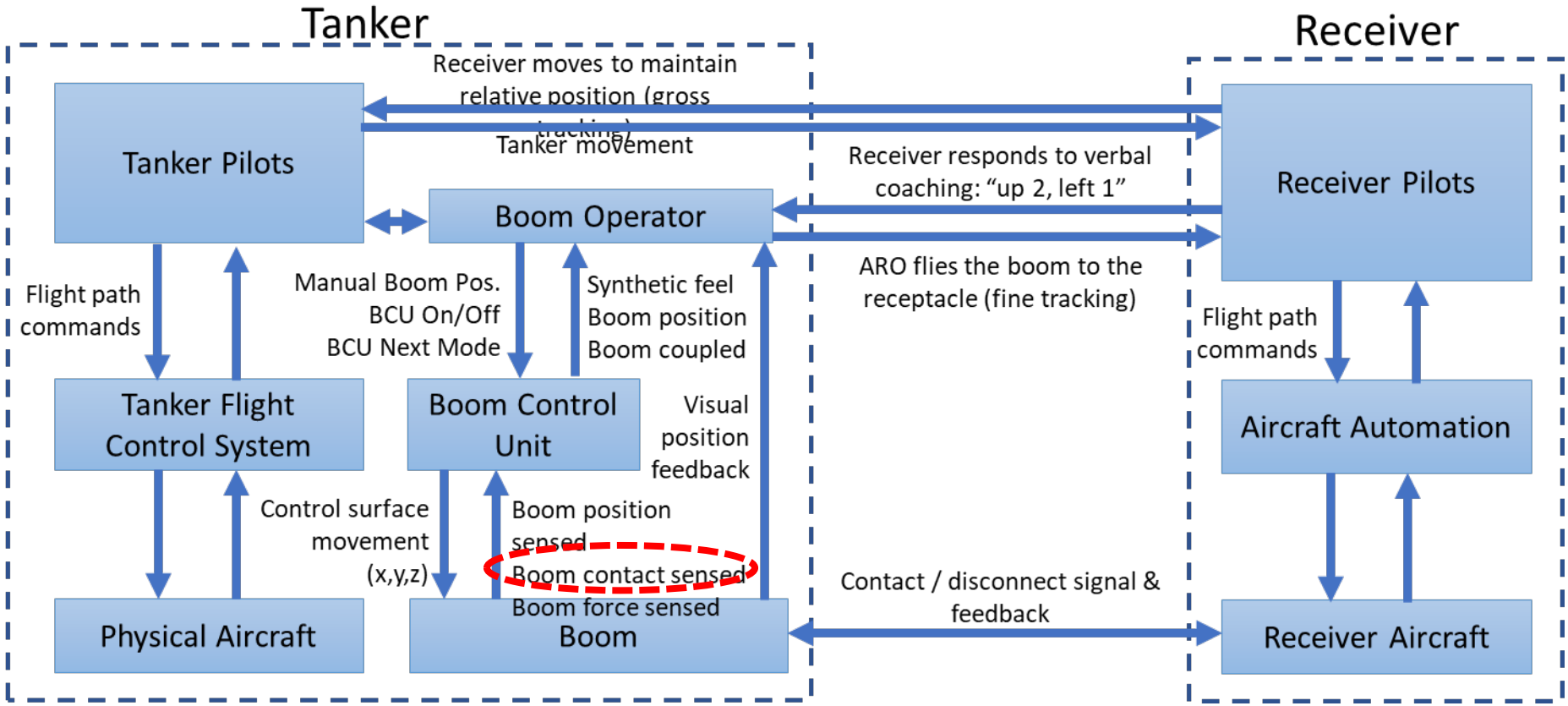




Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 3-Operations Team Describes Mission Effects and Identifies Workarounds



Effects of Attack Can Be Evaluated Across the Entire System (and up to Mission-Level)

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 3-Operations Team Describes Mission Effects and Identifies Workarounds



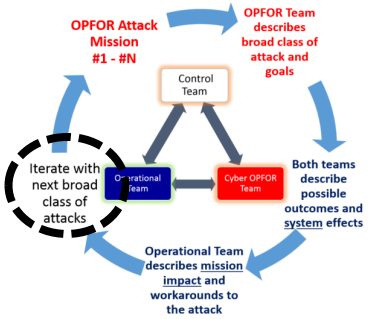
- Operational Team work-arounds must remain consistent with current level of detail, but can recommend changes to requirements, design rationale, etc.
- Four broad approaches to address the threat class
  - Mitigate
  - Eliminate
  - Transfer
  - Accept

Proactive Action at the Concept Stage Can Mitigate or Eliminate Whole Classes of Attacks!

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

STPA-Sec Wargaming Using DoD Cyber Table Top (CTT): Step 4-Iterate with Next Class of Attacks



Element Impacted	Effect	Attack Class
Boom Contact Sensor	Delayed Pulse Feedback	Denial of Service, **Tampering**
Boom Control Unit	Delayed Processing of Boom Contact Sensor Pulse	Denial of Service

Repeat Process for Tampering Against Boom Contact Sensor

Ref: DoD Cyber Table Top Guidebook Version 1.0

© Copyright William Young, 2020

A Few More Thoughts on STPA-Sec Wargaming using DoD CTT Process

- Results and insights should be captured and cataloged
- Approach is particularly useful in providing data to refute faulty assumptions, highlight flawed logic, etc.
- Wargaming supports better estimate of operational risk and can be used to support risk / reward discussions for a particular feature / function
- Removing features is most effective action in decreasing complexity and increasing security

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

Wargaming via STPA-Sec Provides Another Opportunity to Catch and Fix Flaws that Drive Up Costs in Complex Software Intensive Systems

© Copyright William Young, 2020

Overview

- Motivation & Big Ideas
- Security Through a System-Theoretic Lens
- System-Theoretic Process Analysis for Security (STPA-Sec) Practicum
  - Problem Framing
  - Scenario Development
  - Wargaming
- **Does it Work in the Real World?**
- Ongoing Work and STPA-Sec 2.0
- Summary

© Copyright William Young, 2020

Akamai

President and CEO Tom Leighton's advice in Whitehouse meeting of Tech CEOs on improving Federal Cybersecurity

"Cybersecurity is a growing area of Akamai's business, one where IT organizations seek expert help repeatedly. Solutions that work for private companies can also work for federal agencies, specifically:…

- Protecting federal data through role and policy-based access controls
- Encouraging "security by design" through systems analysis methodologies like STPA-SEC



Ref: https://www.linkedin.com/pulse/technology-ceos-share-best-practices-us-government-cios-tom-leighton-1/

© Copyright William Young, 2020

IT Alliance for Public Sector Cybersecurity

- Key Recommendation: Institutionalize "security by design" for federal IT modernization and development.
  - Included within a DevSecOps approach needs to be a "security by design" process, such as a System- Theoretic Process Analysis for Security (STPA-Sec) for all future development. Security is not an add-on, it needs to be a fundamental part of all IT design, from start to finish. (p.37-38)



***Ref: IT Alliance for Public Sector, "Tech Industry's Recommendations for Federal IT Modernization"**

WYOUNG@MIT.EDU

© Copyright William Young, 2020

Embraer



- Conclusions from Embraer's STPA-Sec pilot study
  - "The application of STPA-Sec, in the aerospace area (FMS),was a good example of its potential to identify design recommendations
  - STPA Sec shows to be an alternative method to current ED-203/DO-356 implementations
    - Identification of security environment and security perimeter is addressed during elaboration of the functional control structure
    - Security Risk Assessment activity is covered during Step1 and Step2 of STPA-Sec
  - Embraer has proposed STPA-Sec as an alternative means of compliance to ED-202A/DO-326A"

STPA-Sec is Now Appendix G of DO-356A Aircraft Airworthiness Security

***Ref: Pereira, Hirata, Pagliares, de Lemos " STPA-Sec: System-Theoretic Process Analysis for Security – Flight Management System"**

USAF Experience with Functional Mission Analysis (Variant of STPA-Sec)

"Highlighted during the sprint was that Functional Mission Analysis (FMA) is not simply a cyber tool; FMA is about understanding how cyber impacts the AF missions and how using FMA to tailor cyber defenses assures operational missions and decision superiority for Airmen. Cyber FMA will present cyber to the base and wing commanders in terms of mission assurance and mission impact"

-- Air Force CYBERWORX



CYBERWORX™

AIR FORCE CYBERWORX REPORT 17-001
Functional Mission Analysis for
the Air Force Cyber Squadron Initiative

MICHAEL V. CHIARAMONTE, Lt Col, USAF
Senior Designer & Facilitator

LUCILLE R. McMINN, Capt, USAF
#FMA4CSI Project Lead

JEFFREY A. COLLINS, Col, USAF
Director of AF CyberWorx

DESIGN PROJECT CONDUCTED
13 FEB – 17 FEB 17

Produced with input from numerous units including SAF/CIO A6, AF/A3, AFSPC A2/3/6, Air University, the Air Force Institute of Technology, the Joint Space Operations Center, 1 CBCS, 137 CS, 38 EIG, 39 IOS, 434 CS, 50 SCS, 52 CS, 53 EWG, 56 ACOMS, 673 CS, 721 CS, 744 CS, 752 OSS, and 92 COS.
Designed by USAFA Officers and our valuable partners in Industry.

Air Force CyberWorx™
2354 Fairchild Dr, Ste 2N300
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–4278

UNCLASSIFIED - Distribution A: Approved for public release; distribution unlimited

Ref: Air Force CyberWorx Report 17-001: Functional Mission Analysis for the Air Force Cyber Squadron Initiative

Overview

- Motivation & Big Ideas
- Security Through a System-Theoretic Lens
- System-Theoretic Process Analysis for Security (STPA-Sec) Practicum
  - Problem Framing
  - Scenario Development
  - Wargaming
- Does it Work in the Real World?
- **Ongoing Work and STPA-Sec 2.0**
- Summary

© Copyright William Young, 2020

Ongoing Work That's "Cooking up in the Lab"

- Tighter MBSE Integration (e.g. "Thomas Method" for security)
- Tailored analysis of security logs to support "Cyber HATR" (Hazardous Air Traffic Report)
  - Force Adversary to be Perfect, not just lucky
- Support to Adversarial Machine Learning
- New security-related graphics to support improved mission-related decision making
- Improved Support for Risk Management Framework integration
- Rapid, focused Cyber Risk Assessment of prototypes

These Likely Just Scratch the Surface of What's Possible Within the New Paradigm Enabled by the STAMP Model

© Copyright William Young, 2020

Overview

- Motivation & Big Ideas
- Security Through a System-Theoretic Lens
- System-Theoretic Process Analysis for Security (STPA-Sec) Practicum
  - Problem Framing
  - Scenario Development
  - Wargaming
- Does it Work in the Real World?
- Ongoing Work and STPA-Sec 2.0
- **Summary**

© Copyright William Young, 2020

Summary

- STPA-Sec addresses security through a strategy lens, beginning at the concept stage
- STPA-Sec enhances security by defining secure functionality and a suitable security concept to guide development of a securable architecture (form)
- STPA-Sec adds elements to the basic STPA and enables the STAMP model to serve as the foundation for a new secure systems analysis
- STPA-Sec directly address the key elements of cybersecurity and mission assurance
  - Impact is addressed through **Problem Framing**
  - Vulnerability is addressed through additional **Security-Specific Scenarios**
  - Threats are addressed through **Wargaming**

STPA-Sec's Emphasis on Mission Raises Security from a Tactical to a Strategic Engineering Discussion

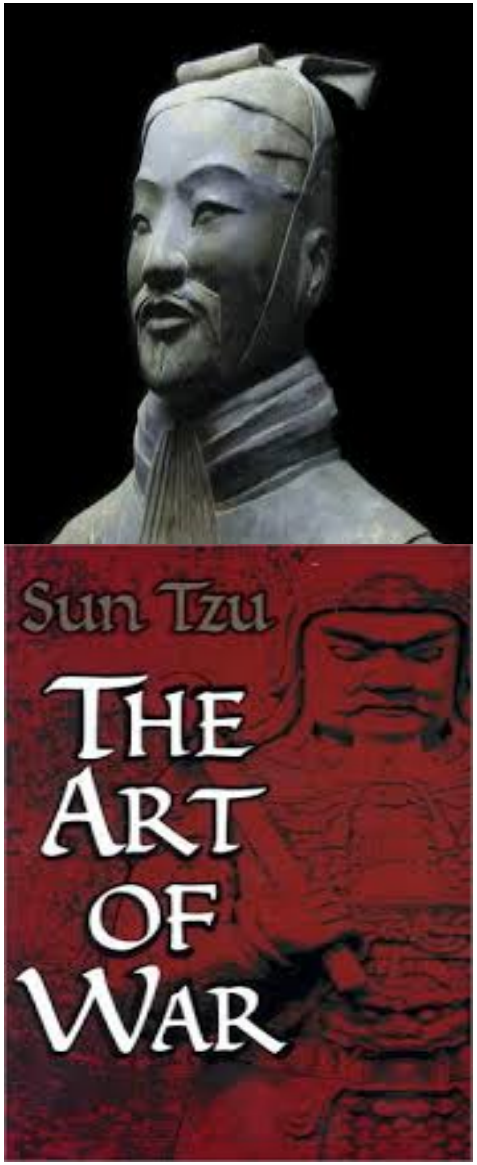
© Copyright William Young, 2020

Parting Thoughts and Wisdom 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

© Copyright William Young, 2020

Please Feel Free to Contact Me For More Information and Details on Applying STPA-Sec

- Government-related
- William.Young.3@US.AF.Mil
- Academia
- WEYoung@Syr.edu
- Industry
- Wyoung@MIT.edu