



Security Tutorial Part 1
A Systems Approach to Security

William Young Jr

PhD Candidate, Engineering Systems Division

Systems Engineering Research Lab

Massachusetts Institute of Technology

2016 STAMP Conference

Boston, MA

March 21, 2016

WYOUNG@MIT.EDU

© Copyright William Young May 2016

DISCLAIMER:

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

WYOUNG@MIT.EDU
© Copyright William Young May 2016

Overview

- Foundation-- System Theoretic Concepts
- Application– System-Theoretic Process Analysis for Security (STPA-Sec)
- Illumination– Results and Lessons Learned
- Implication– Combining Safety and Security

Brief Summary of 40+ Hour Course Focused on Why and What (not How)

WYOUNG@MIT.EDU
© Copyright William Young May 2016

Mission Failure



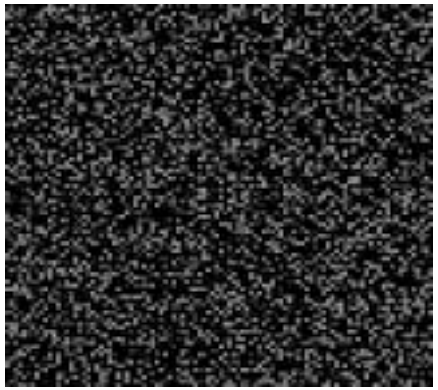
1. Target Acquired



2. Information Communications Technology transmits data



3. Commander at distant center observes



4. Mission Commander Loses surveillance and aborts



5. SOF team aborts mission



6. Attempt to determine cause

Could the Operation Have Been Designed Differently for More Assurance?

Ref: (Vautrinot, 2012)

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Securing Digital Flight Bag (DFB)



1. Decision to Employ DFB



2. Implement longer passwords and lockout



3. Aircrew experiences emergency inflight



4. Aircrew locked out of DFB

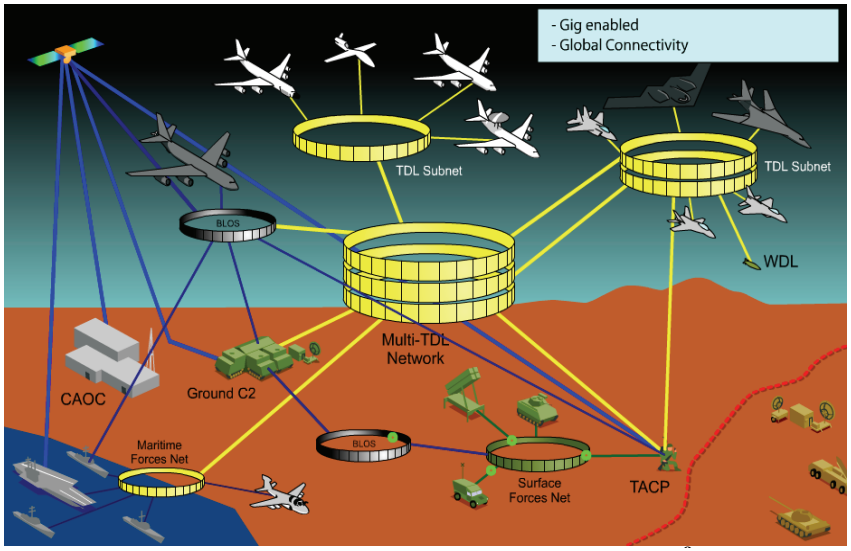
How Can Need to Protect be Balanced With Need for Access?

Ref: (Skaves, 2011)

WYOUNG@MIT.EDU

© Copyright William Young May 2013

Functionality Tradeoffs for Future Weapons



1. Design a Weapon to Leverage NCW



2. Weapon can accurately attack more targets



3. Aircraft releases weapon



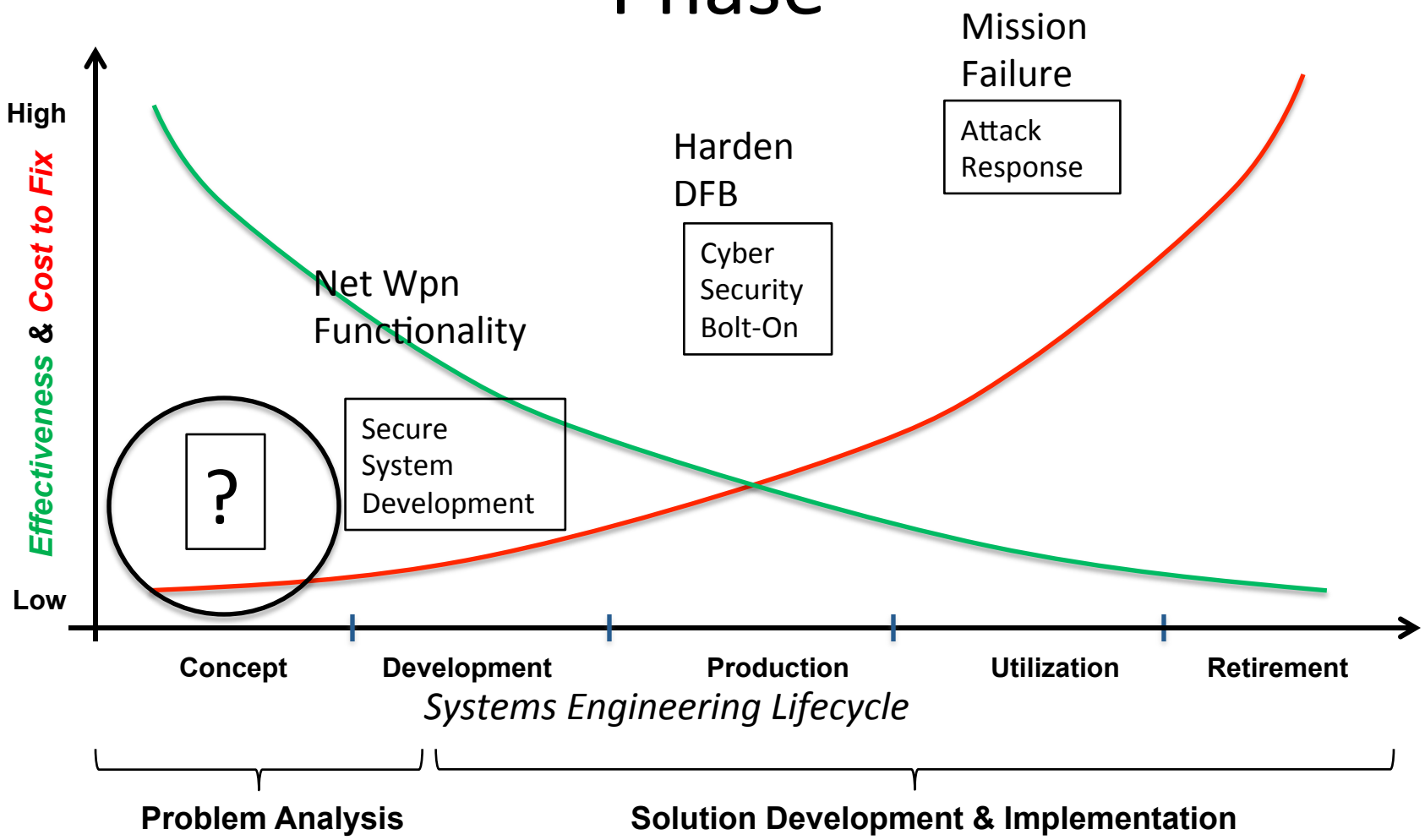
4. Civilians enter area



5. JTAC needs to abort

How Can Network Enabled Weapon Functionality Be Assured?

Need to Address Security in Concept Phase



Problem: How to Define the Right Security Problem ?

Ref: (Boehm; INCOSE, 2015; Maier, 2009)

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Primary Associated Standards

IEEE/IEC/ISO 15288

- Business or mission analysis
- Stakeholder needs and requirements
- System requirements definition

NIST SP 800-160

- Business or mission analysis process
- Stakeholder needs and requirements definition
- System requirements definition

STPA-Sec Provides a Rigorous Methodology to Implement Existing Standards

WYOUNG@MIT.EDU
© Copyright William Young May 2016

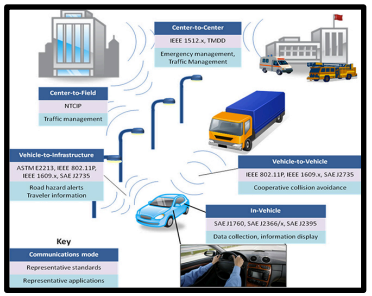
Key Concepts Behind STPA-Sec

- Abstraction Hierarchy
- Constraints
- Process Models

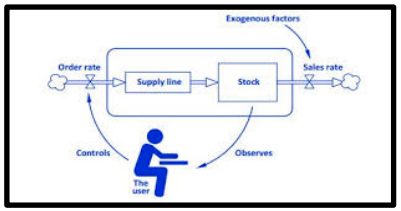
WYOUNG@MIT.EDU
© Copyright William Young May 2016

Abstraction

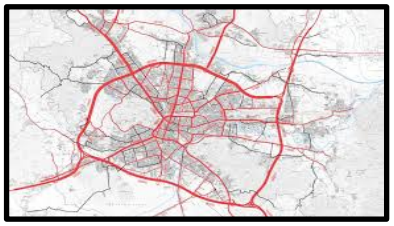
Purpose



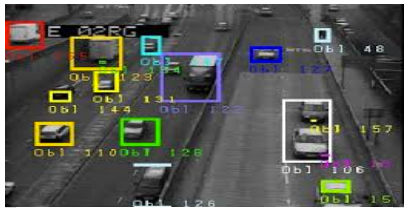
Abstract Function



General Function



Physical Process



Physical Form

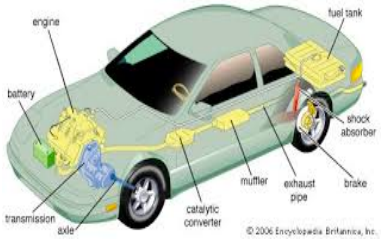


WYOUNG@MIT.EDU

© Copyright William Young May 2016

Aggregation







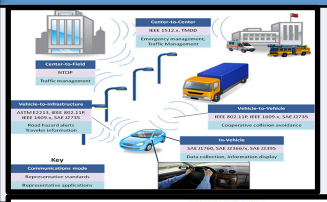
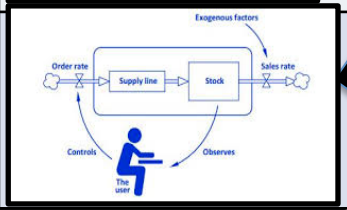
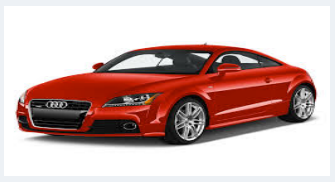
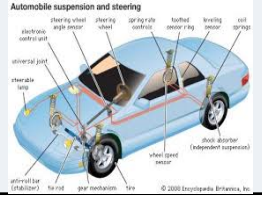
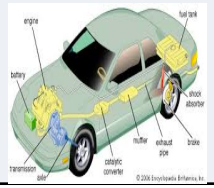




Whole System | Subsystem 1 | Hardware | Software | Human

WYOUNG@MIT.EDU

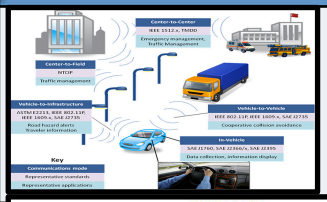
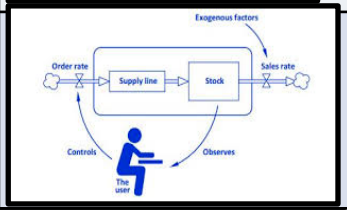
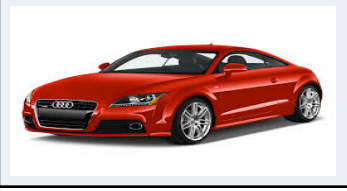
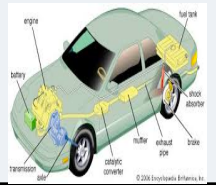
© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						

Intent & Requirements

WYOUNG@MIT.EDU

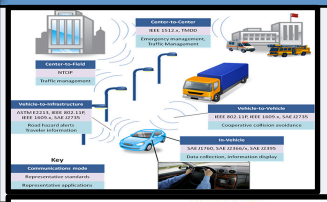
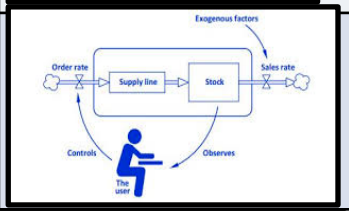
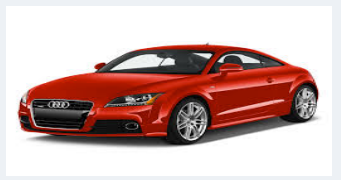
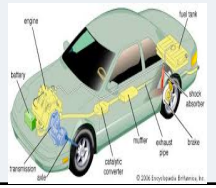
© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						

Impact & Risk

WYOUNG@MIT.EDU

© Copyright William Young May 2016

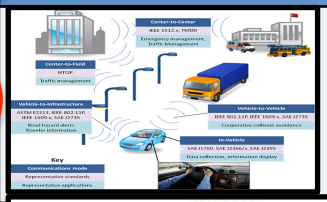
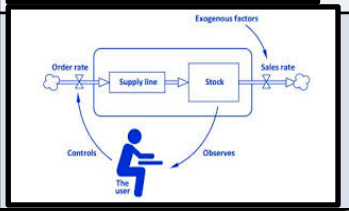
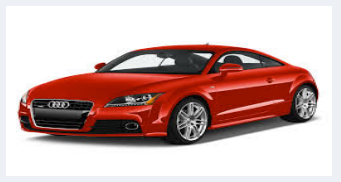
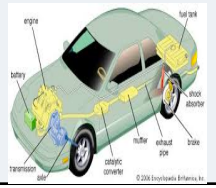
Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						

Conceptual

Physical

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Undesired System Functionality







Transportation System or Weapon System ?

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function		?				
General Function						
Physical Function						
Physical Form						

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Mid Air Collision



Aircraft must maintain minimum safe separation

Friendly Fire Loss



Only hostile forces must be engaged

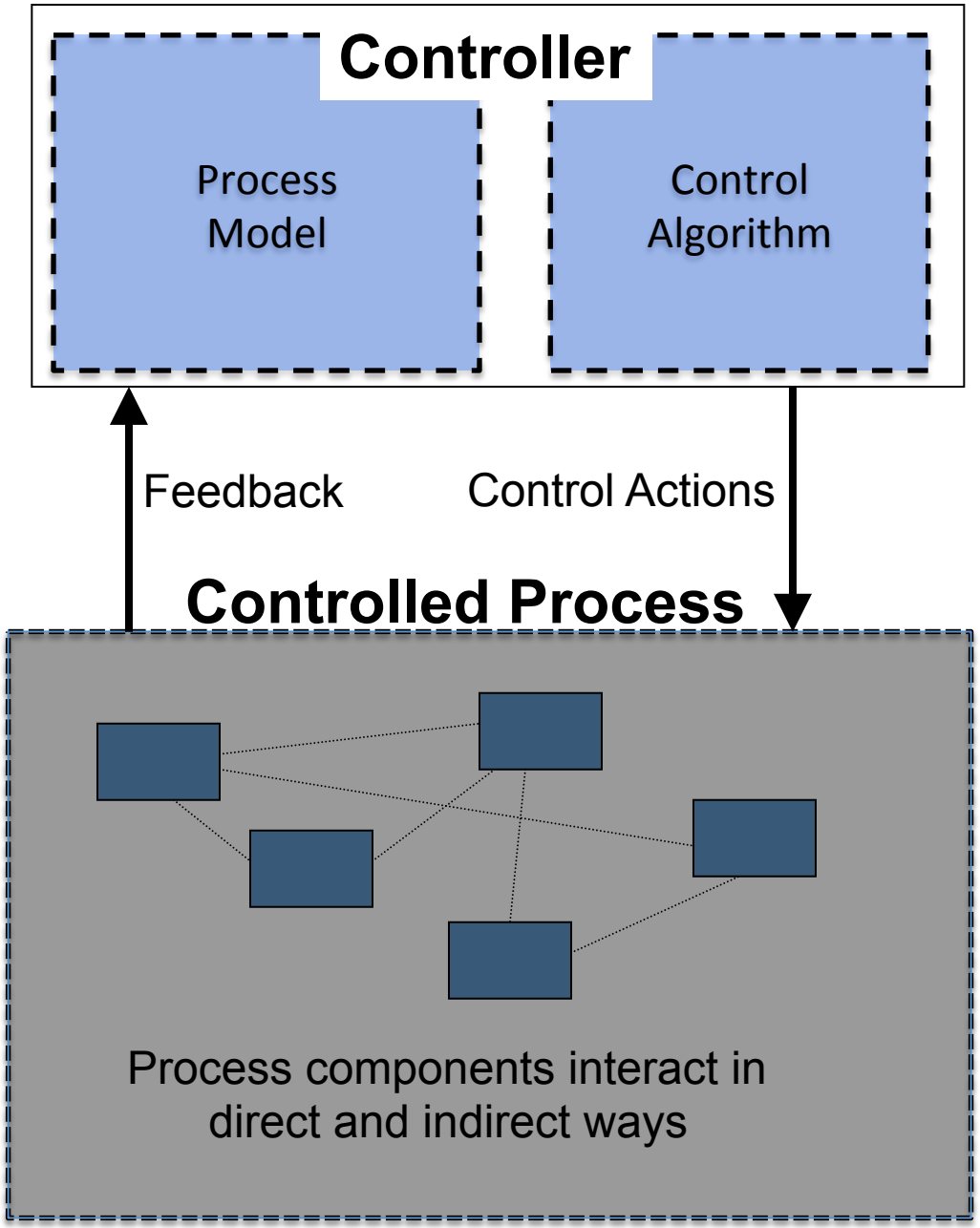
Customer PII Theft



PII must only be exposed to authorized entities

WYOUNG@MIT.EDU

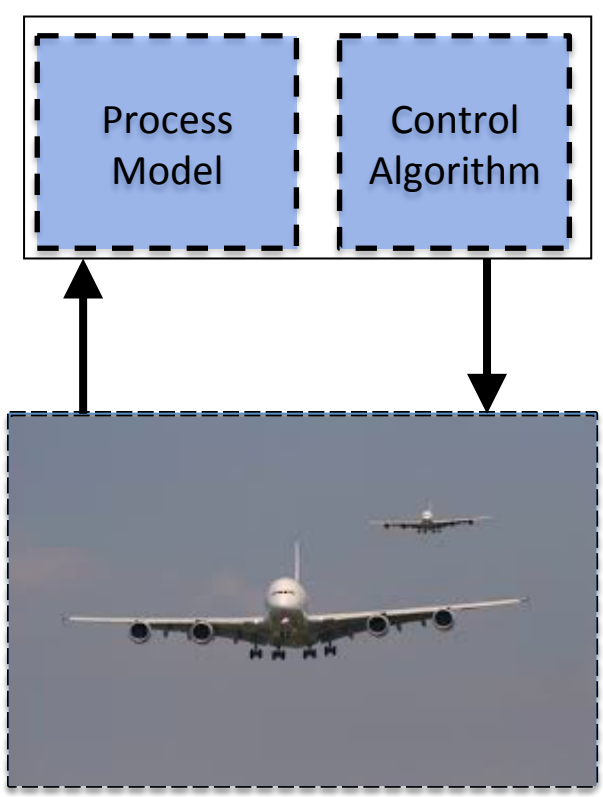
© Copyright William Young May 2016



- Four types of hazardous control actions:
  - Failing to issue a command gives rise to hazard
  - Issuing a command gives rise to a hazard
  - Issuing a command too early, too late gives rise to a hazard
  - Stopping a command too soon or applying it too long gives rise to a hazard

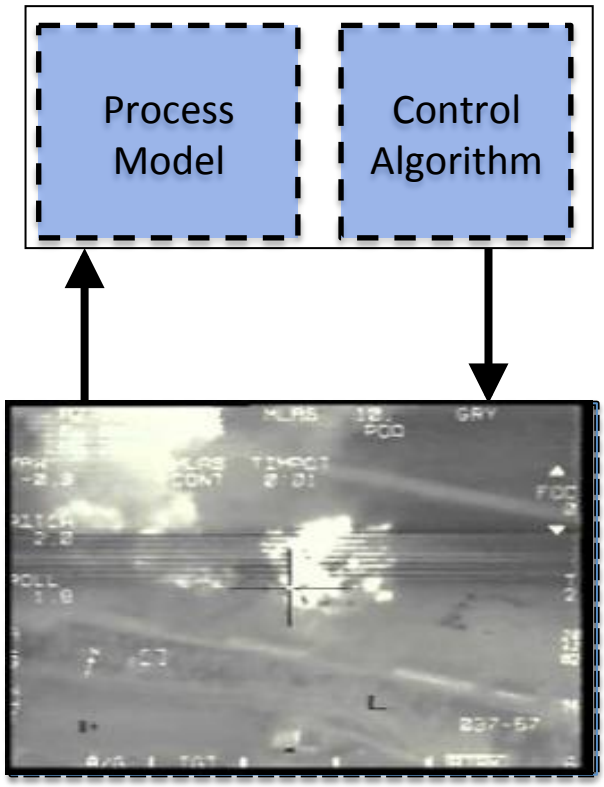
© Copyright William Young May 2016

Unacceptable Losses Reframed as Control Problems



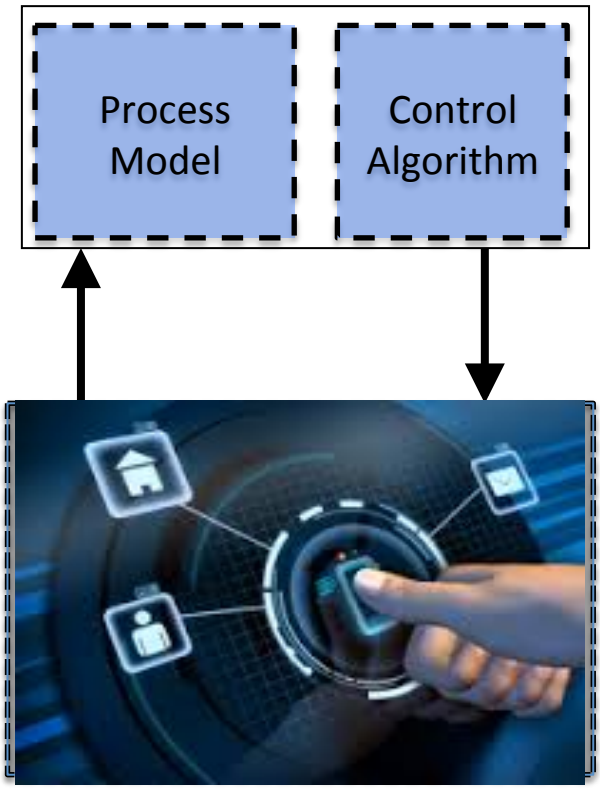
Aircraft must maintain minimum safe separation

ENFORCE: Safe Separation



Only hostile forces must be engaged

ENFORCE: Engagement Rules



PII must only be exposed to authorized entities

ENFORCE: Data Access Policy

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						

Existing Approaches Define Security Problem as How to Secure Components

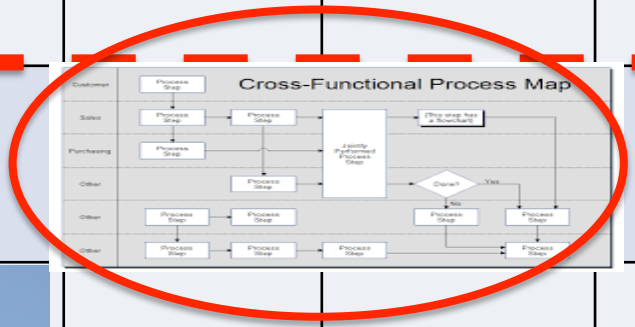
WYOUNG@MIT.EDU

© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						

Or Comply with Certain

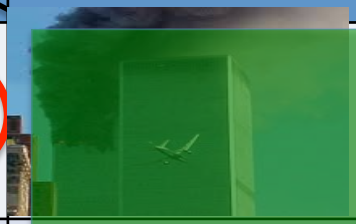
Procedures



WYOUNG@MIT.EDU

© Copyright William Young May 2016

Whole - Part / Ends - Means	Whole System	SubSystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function						
General Function						
Physical Function						
Physical Form						



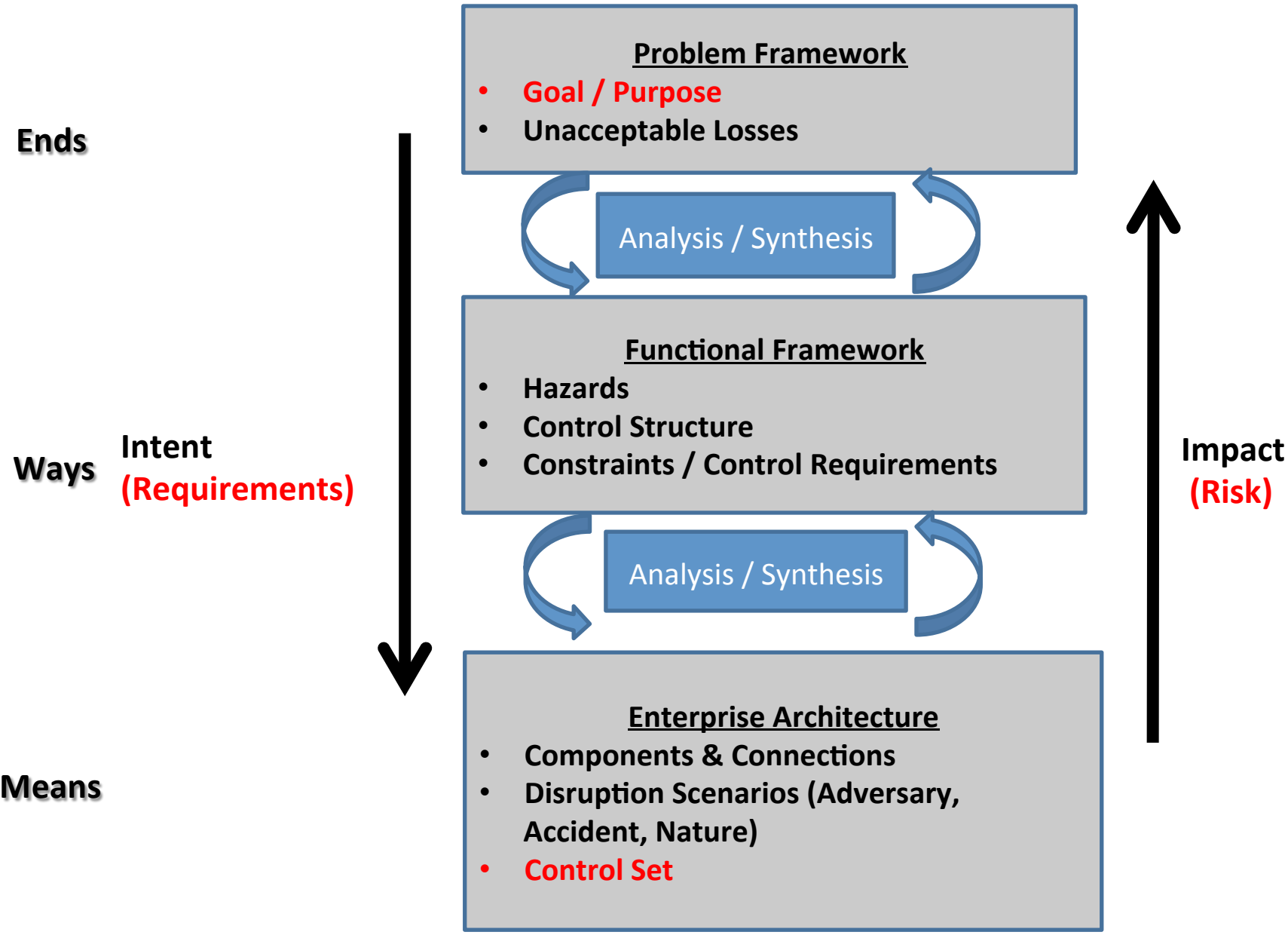
Problem Space

BUT WE MISS THE OPPORTUNITY TO TAKE ADVANTAGE OF IMPROVED PROBLEM DEFINITION



WYOUNG@MIT.EDU

© Copyright William Young May 2016



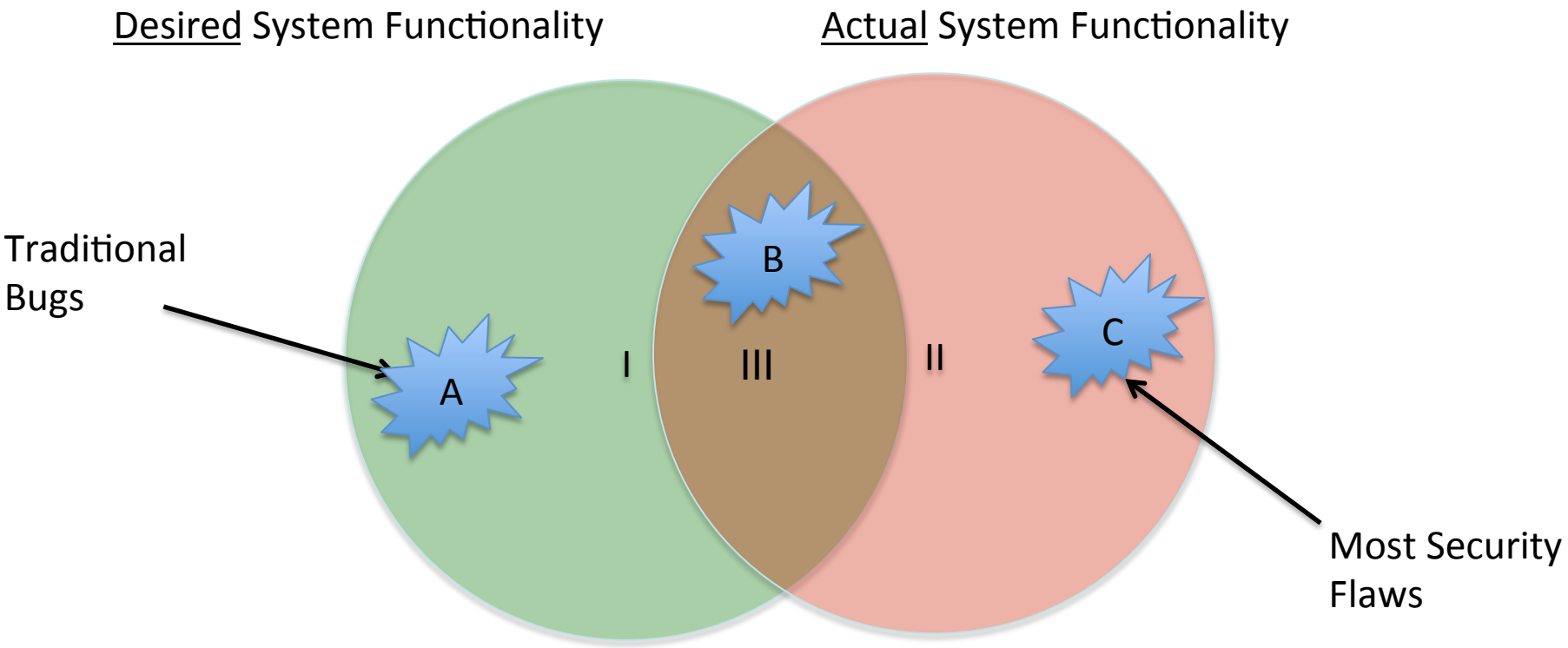
WYOUNG@MIT.EDU

© Copyright William Young May 2016

Examples of Improved Problem Definition

- Never including a particular feature that cannot be reasonably secured
- Replacement of software with mechanical features
- Deliberate separation of components delivering critical functionality

WYOUNG@MIT.EDU
© Copyright William Young May 2016

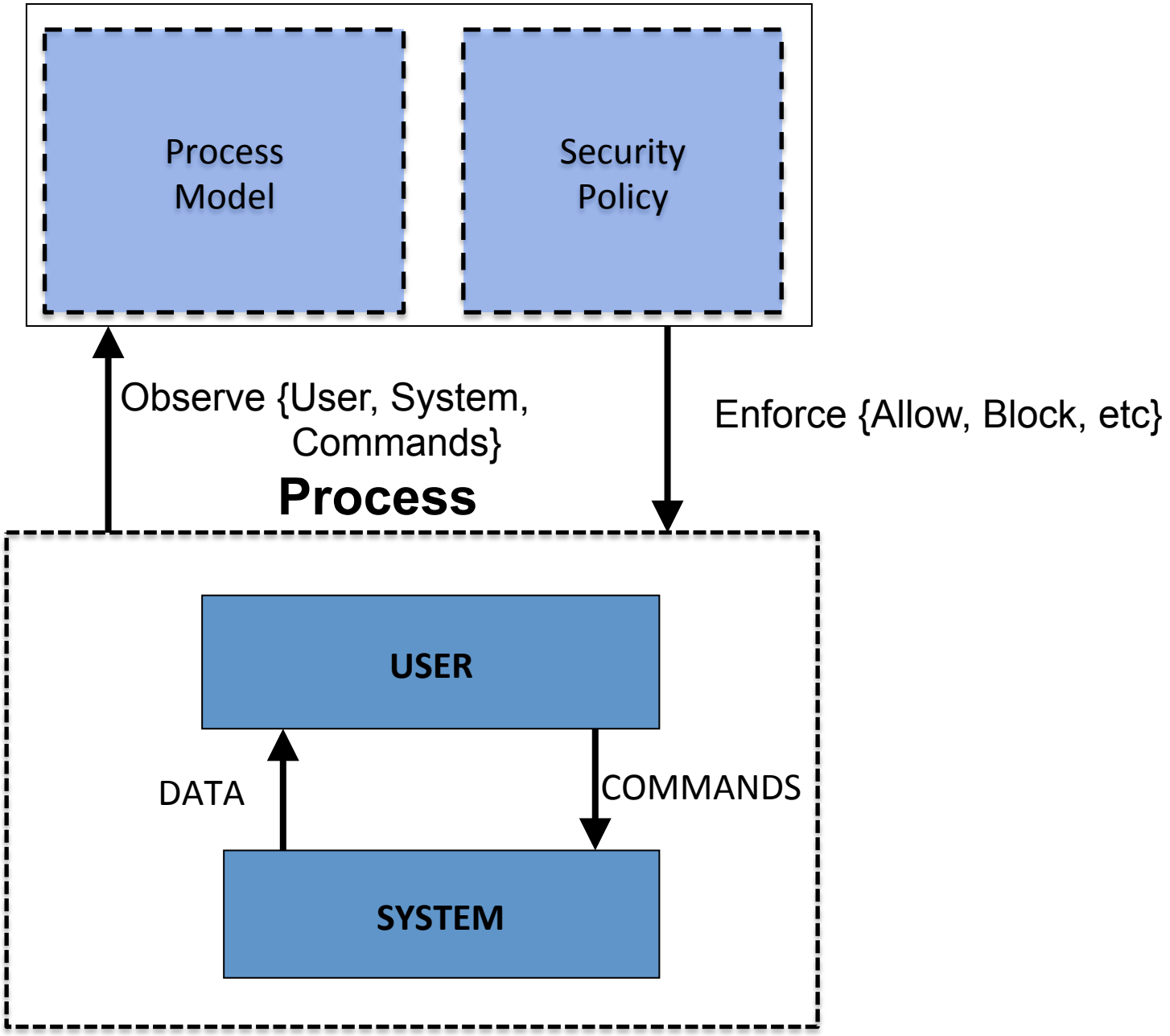


Region I: Desired System Functionality Specified
Region II: Actual System Functionality Delivered
Region III: Degree to Which Actual System Satisfies Specs

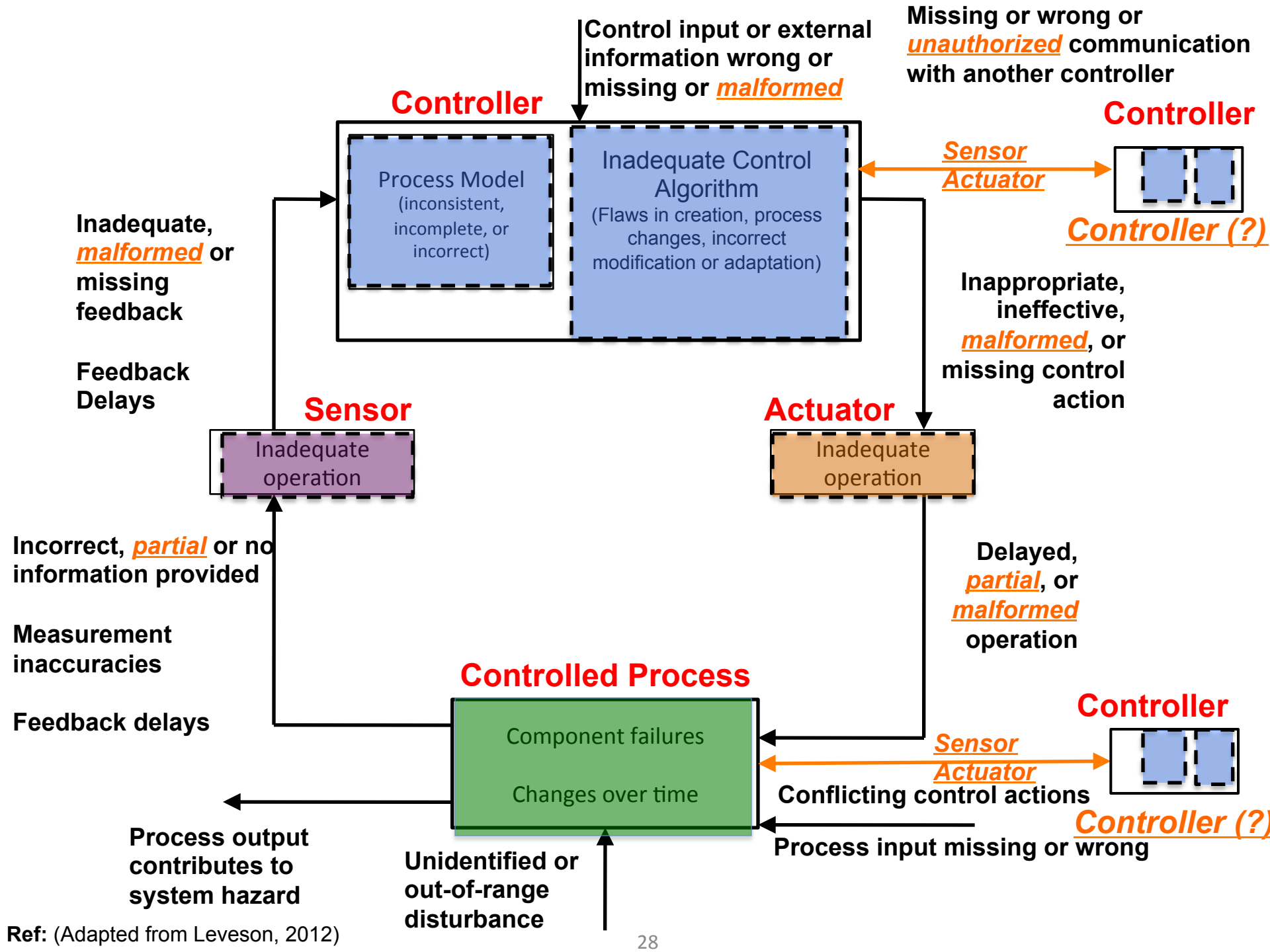
Region A: Traditional "Bug" Where System Doesn't Meet Specs
Region B: Flaw or Known Vulnerability– Specs satisfied in Unsecure Manner
Region C: Unknown Flaw than can be Exploited to Deliver Undesired Functionality

Traditional Approaches Identify A & B; STPA-Sec Identifies B & C

WYOUNG@MIT.EDU
© Copyright William Young May 2016

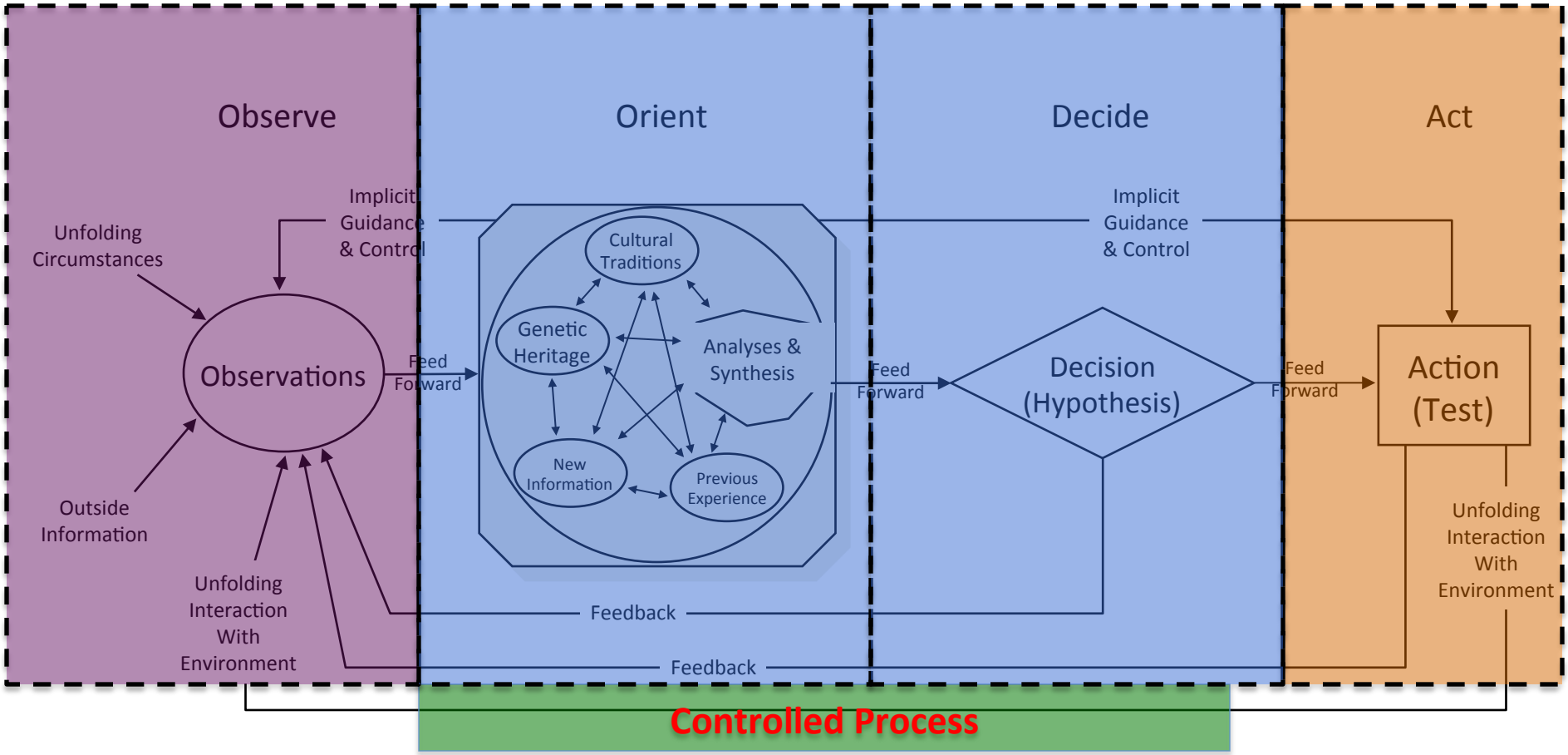


© Copyright William Young May 2016



Ref: (Adapted from Leveson, 2012)

SENSOR PROCESS MODEL CONTROL ALGORITHM ACTUATOR

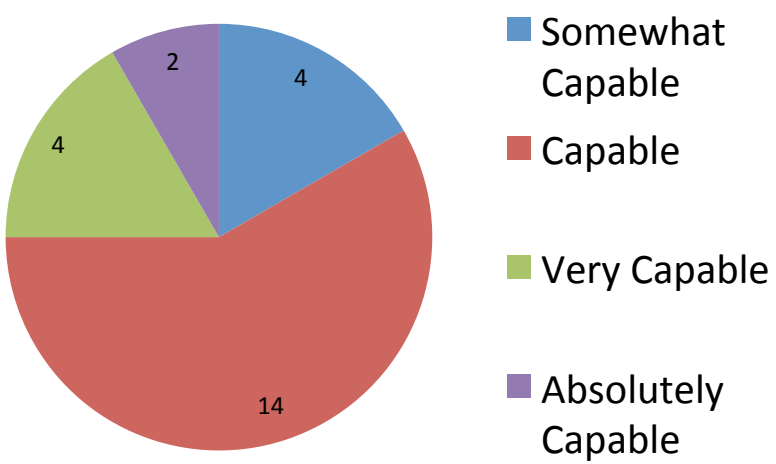


STPA-Sec Applies John Boyd's OODA Loop

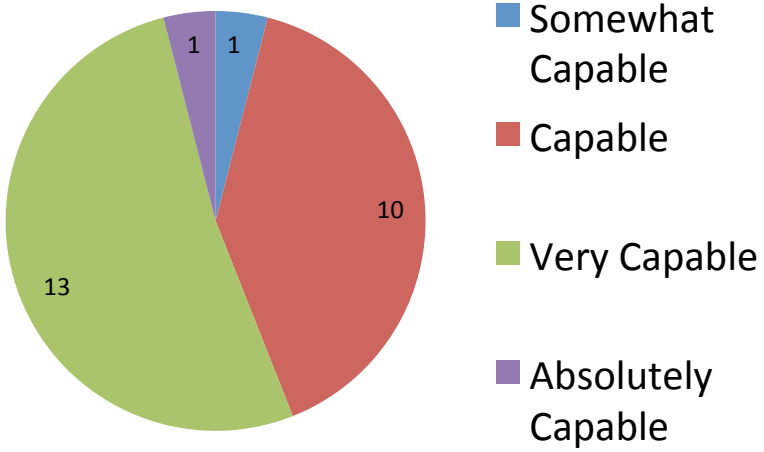
WYOUNG@MIT.EDU
© Copyright William Young May 2016

Recent Self-Reported Assessment Results

Before Training : Ability to Develop Mitigation Strategy



After Training : Ability to Develop Mitigation Strategy



WYOUNG@MIT.EDU

© Copyright William Young May 2016

STPA-Sec Process

System Engineering Foundations

Define and frame problem

Identify losses/accidents

Identify system hazards/constraints

Identify Types of Unsafe/Unsecure Control

Model functional control structure

Identify unsafe/unsecure control actions

Identify Causes of Unsafe/Unsecure Control and Eliminate or Control Them

Trace hazardous control actions using information life cycle

Identify scenarios leading to unsafe control actions

Identify scenarios leading to unsecure control actions

Place scenarios on D4 Chart to ID more critical security scenarios

Wargame security scenarios to select control strategy

Develop new requirements, controls, and design features to eliminate or mitigate unsafe/unsecure scenarios

RED = STPA-Sec Extension on STPA

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Scenario: Secure a new Smart Power Grid to Support F.O.B Operations





A **forward operating base** (FOB) is any secured forward military position, commonly a military base, that is used to support tactical operations.

© Copyright William Young May 2016



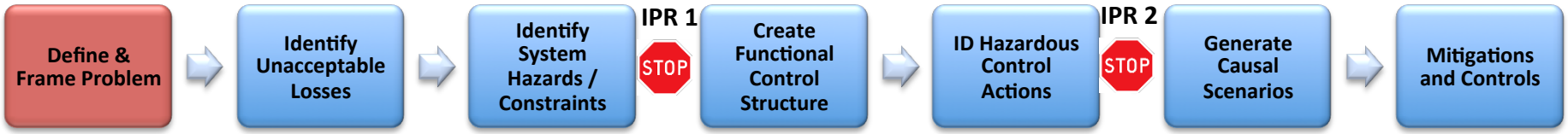
"Power must be uninterrupted, but if interrupted immediate backup must be available to several critical functions: Medical, Operational Command and Control, Fire Direction

Life support functions are critical since there may be wounded troops present. As a result, dependable power must be provided for a minimum of two hours if there is an overall interruption."

"A System to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"

SYSTEM PURPOSE & GOAL

"A system to provide uninterrupted, stable power through grid generation, transmission and distribution in order to support the FOB mission."



WYOUNG@MIT.EDU

© Copyright William Young May 2016

"What areas is the supported commander unwilling to accept adverse outcomes?"

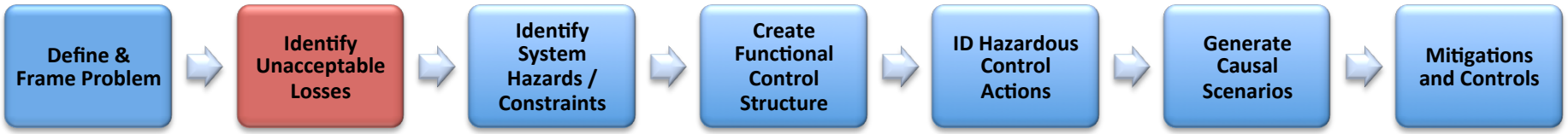
UNACCEPTABLE LOSSES



- **L1:** Inability to execute FOB mission
- **L2:** *Inadvertently* causing an unacceptable degrade to FOB mission
- **L3:** Loss of life / Serious injury
- **L4:** Damage to equipment (FOB or Grid)



- **Focus on outcomes not causes**
- **List should be exhaustive**



WYOUNG@MIT.EDU

© Copyright William Young May 2016

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

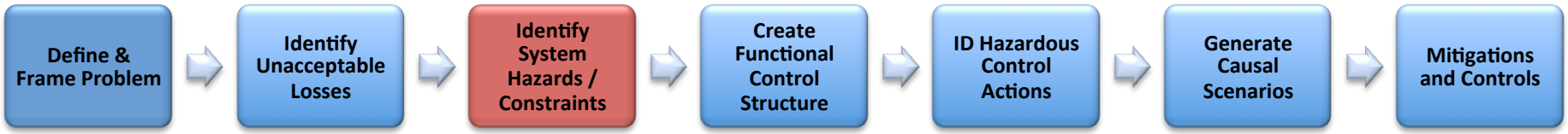
HAZARDS



- **H1:** Power distribution not IAW FOB commander priorities
- **H2:** Power output not within prescribed limits (voltage / freq)
- **H3:** Loss of power



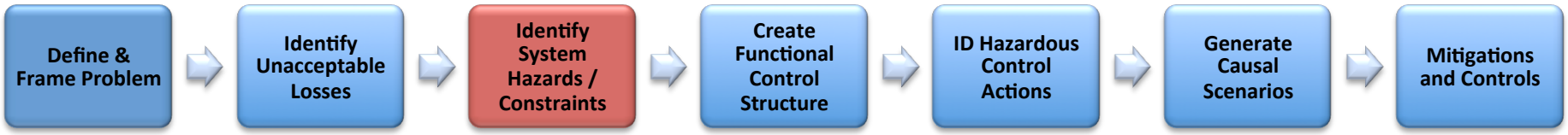
- **Focus on scope of stakeholder**
- **Small exhaustive set**



WYOUNG@MIT.EDU

© Copyright William Young May 2016

	L1:Inability to Execute FOB Mission	L2: Inadvertently causing unacceptable degrade to FOB mission	L3: Loss of Life / Serious Injury	L4: Significant damage to equipment (FOB or Grid)
H1: Wrong Power Distribution Priority		X	X	
H2: Wrong Power Output Voltage/Freq		X	X	X
H3: Loss of Power	X			X



WYOUNG@MIT.EDU
© Copyright William Young May 2016

HAZARDS

- **H1:** Power distribution not IAW FOB commander priorities
- **H2:** Power output not within prescribed limits (voltage / freq)
- **H3:** Loss of power



CONSTRAINTS

- **C1:** Power must be distributed IAW FOB commander priorities
- **C2:** Power output must be within prescribed limits (voltage / freq)
- **C3:** Power must be maintained

"What constraints (functional requirements) should prevent hazardous conditions from occurring?"

Define & Frame Problem → Identify Unacceptable Losses → Identify System Hazards / Constraints → Create Functional Control Structure → ID Hazardous Control Actions → Generate Causal Scenarios → Mitigations and Controls

WYOUNG@MIT.EDU

© Copyright William Young May 2016

1. Identify *Model Elements*
2. Identify each *Model Element's* responsibilities in carrying out each of the key activities necessary conduct the mission
3. Identify *Control Relationships*
4. Identify the *Control Actions* necessary for each element to execute their responsibilities
5. Develop *Process Model Description*
6. Identify *Process Model Variables*
7. Identify *Process Model Variable Values*
8. Identify *Feedback* providing *PMV Values*
9. Check MFCSM for completeness









WYOUNG@MIT.EDU

© Copyright William Young May 2016

"Do hazard states occur when control actions are disputed (affected)?"

Controller: [TBD]				
Control Actions	Hazardous Control Actions			
	Not Proving CA Causes Hazard	Providing CA Causes Hazard	Providing CA Too Soon or Applying Too Long Causes Hazard	Providing CA in the Wrong Sequence or Order Causes Hazard
Emergency Override				



WYOUNG@MIT.EDU
© Copyright William Young May 2016

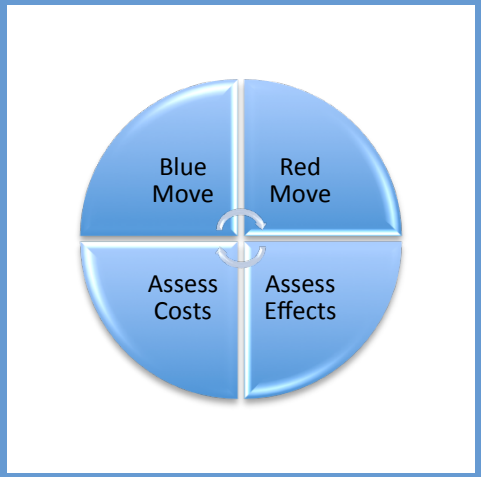
Using the results of terrain mapping, for each critical information flow identify the following for each control action:

- Information Generation
- Information Processing
- Information Storage
- Information Communication
- Information Consumption
- Information Destruction



"What might an adversary do to violate the constraint and cause the hazardous control action?"

"What is our strategy to enforce the constraint?"



Define & Frame Problem → Identify Unacceptable Losses → Identify System Hazards / Constraints → Create Functional Control Structure → ID Hazardous Control Actions → Generate Causal Scenarios → Mitigations and Controls

WYOUNG@MIT.EDU

© Copyright William Young May 2016



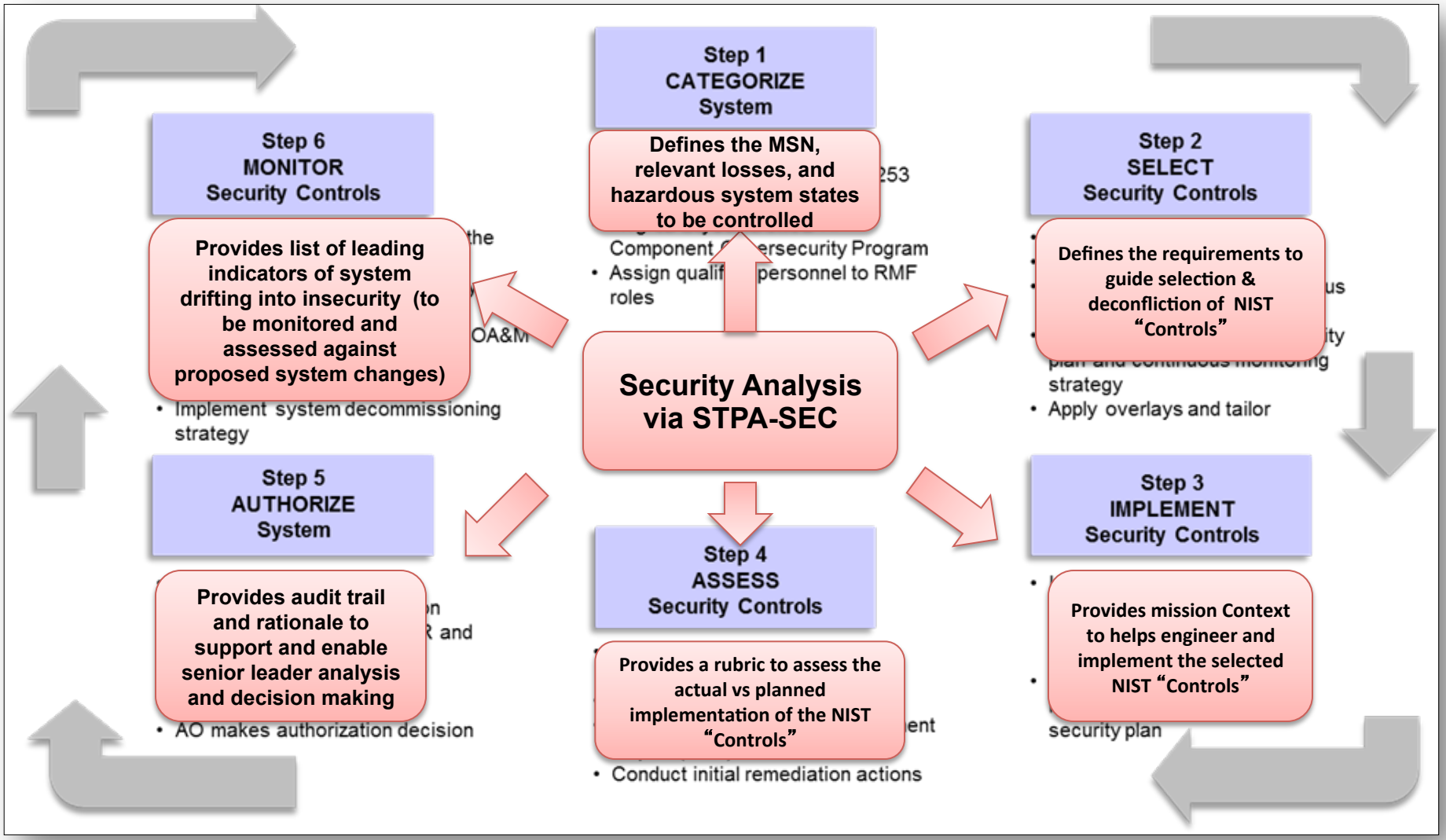




Define & Frame Problem → Identify Unacceptable Losses → Identify System Hazards / Constraints → Create Functional Control Structure → ID Hazardous Control Actions → Generate Causal Scenarios → Mitigations and Controls

© Copyright William Young May 2016

STPA-Sec Integration with NIST Risk Management Framework (DoD Example)



WYOUNG@MIT.EDU

© Copyright William Young May 2016

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!

WYOUNG@MIT.EDU
© Copyright William Young May 2016

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

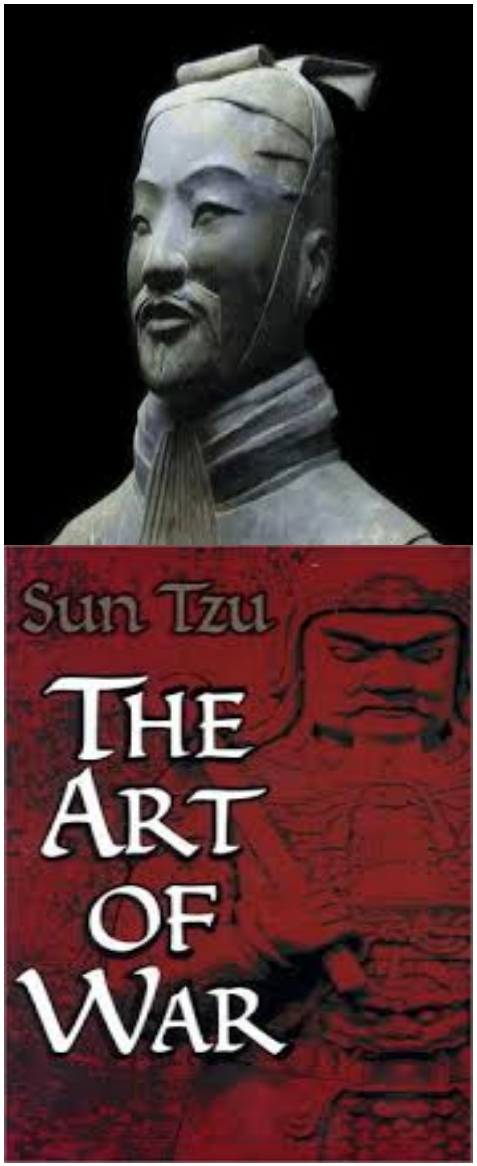
WYOUNG@MIT.EDU
© Copyright William Young May 2016

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
© Copyright William Young May 2016

QUESTIONS ??

WYOUNG@MIT.EDU

© Copyright William Young May 2016

Thank You for Your Time

- Wyoung@MIT.EDU

© Copyright William Young May 2016