



Understanding STPA-Sec Through a Simple Roller Coaster Example

William Young Jr

PhD Candidate, Engineering Systems Division

Systems Engineering Research Lab

Massachusetts Institute of Technology

2016 STAMP Conference

Boston, MA

March 23, 2016

WYOUNG@MIT.EDU

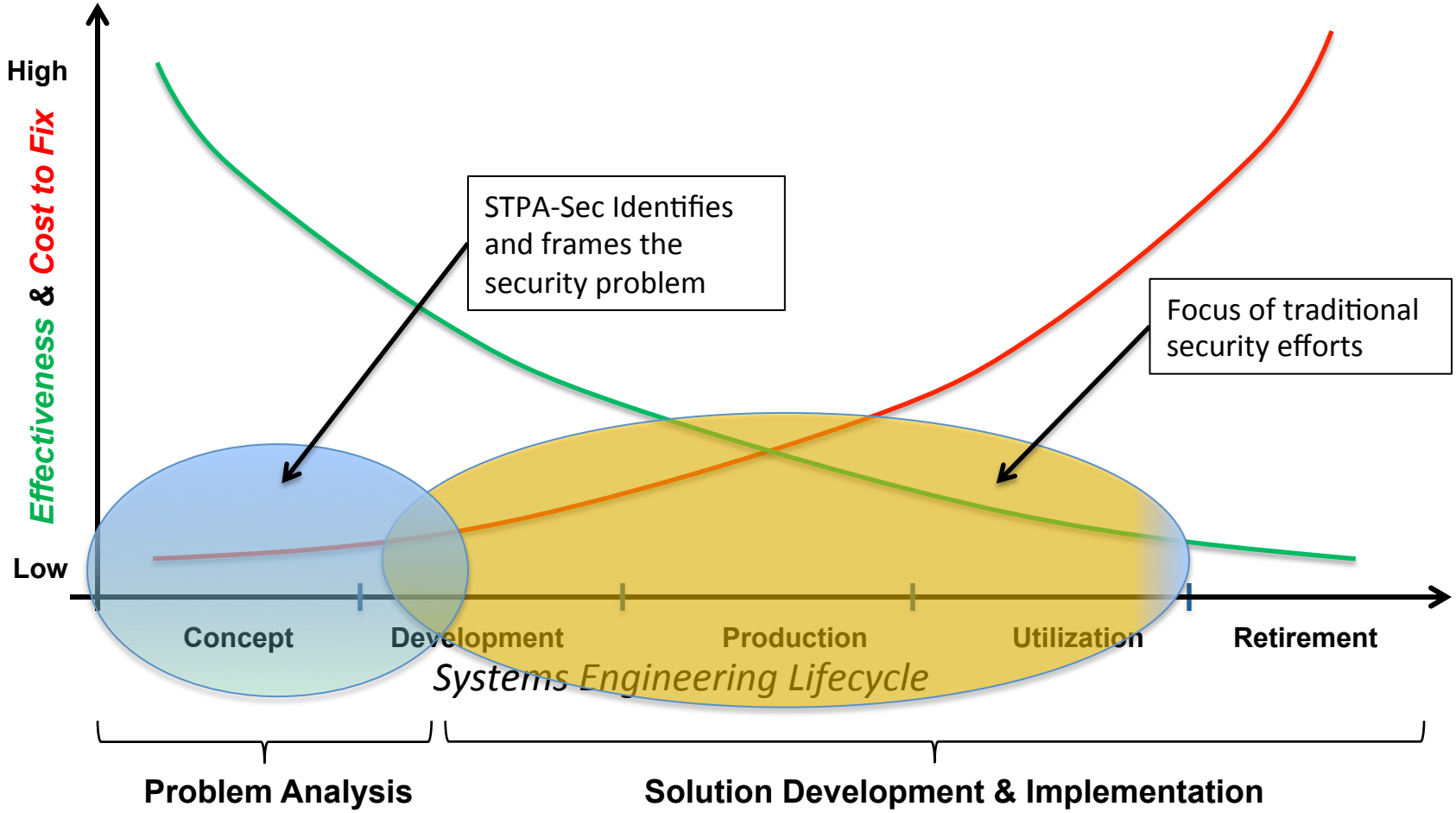
© Copyright William Young Mar 2016

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

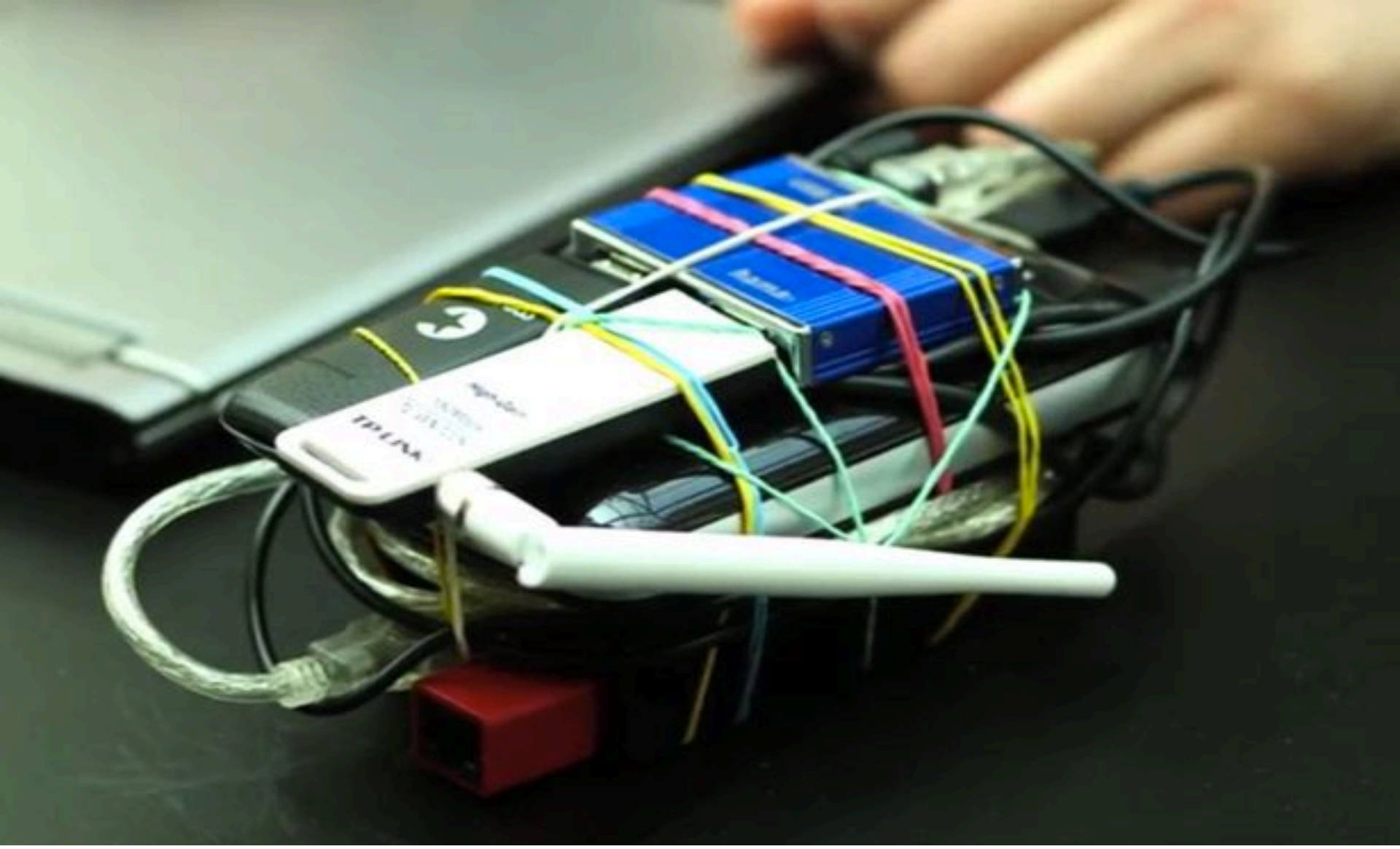
WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

Need to Address Security Pre-Architecture

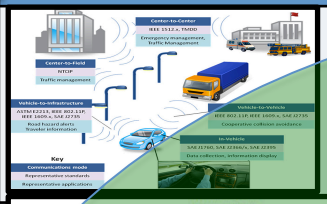
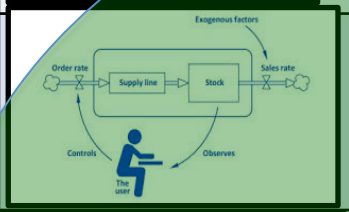
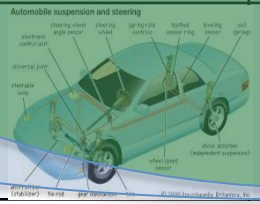
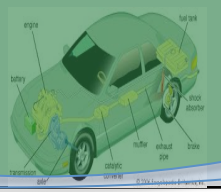
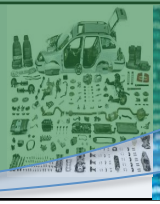
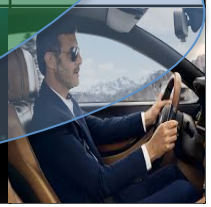


STPA-Sec Helps Rigorously Frame the "Right" Security Problem

© Copyright William Young Mar 2016



Just Because You Can, Doesn't Mean You Should…Just Because it Works, Doesn't Mean is Can Be Secured

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

STPA-Sec Focus

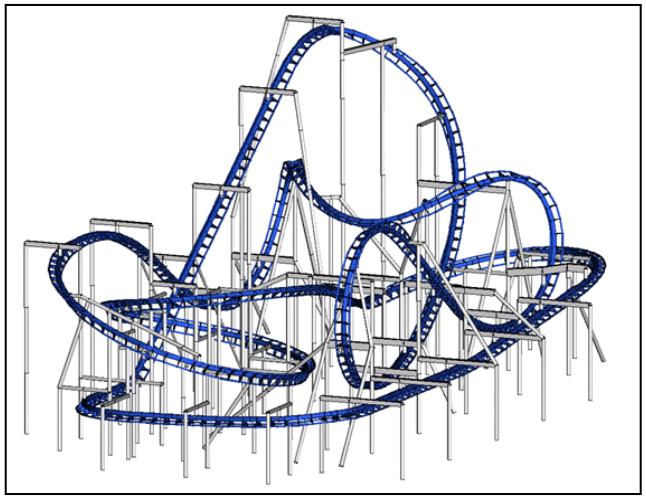
Traditional Security Engineering Focus

WYOUNG@MIT.EDU

© Copyright William Young Mar 2016

Scenario: You are part of the ACME Roller Coaster Company Security Team







The R&D team has proposed a new 5D coaster.

***Original Scenario created by Danny Holtzman of MITRE Corp**

WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

Scenario: You are part of the ACME Corporation Security Team

The CEO would like details from your team. “I want to know if building the Smart Coaster represents a risk to our operations that we should accept,” she says! “If we do accept the risk, what can you do about it as the security team?”

© Copyright William Young Mar 2016

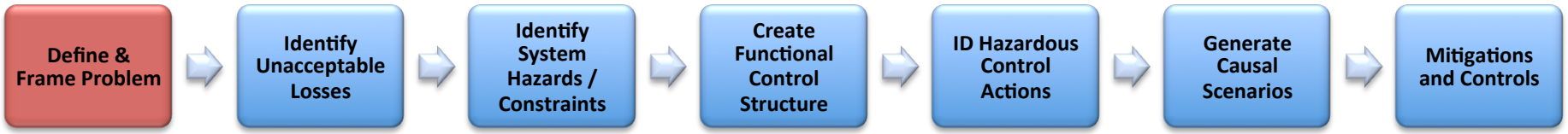
Key Stakeholder is the ACME CEO

- You interview the CEO and she provides you some key insights
  - The ride represents a bet on the company's future, she does not want the stock to take a hit
  - She is concerned about losing company IP gained through R&D for the coaster
  - She was a student of Nancy Leveson during her grad school time at MIT and cares about safety
  - She likes the concept of creating a tailored thrill profile, but states, "Don't do an OPM!"
  - She states that she is unwilling to create a ride that doesn't deliver on ACME's reputation for thrilling rides
  - Smart coaster likely will be the most expensive roller coaster ever built and she doesn't want it damaged

© Copyright William Young Mar 2016

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 Mar 2016

A Potential Solution Based on Scenario:

- A System to deliver a safe, but thrilling experience to riders by means of loading, tailoring, launching, thrilling, offloading in order to contribute to continuing profitability and enhance reputation of ACME

This is a Statement Explicitly Describing the Problem, our Preferred Approach and the Overall Goal

© Copyright William Young Mar 2016

Unacceptable Losses from Scenario:

L1: Death or serious injury to rider or operator

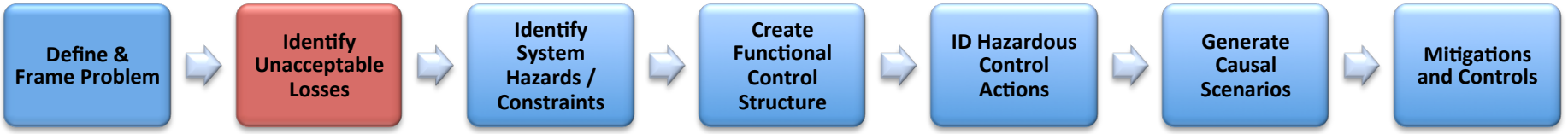
L2: Significant devaluation of Acme stock

L3: Significant Damage to Smart Coaster

L4: Loss of Acme Intellectual Property

L5: Loss of company reputation

L6: Loss of consumer (rider) PII



L4 & L6 Would Generally Be Outside the Scope of Traditional Safety Analysis

© Copyright William Young Mar 2016

Hazards for the Example

H1: Rider or operator exposed to dangerous physiological conditions

H2: Rider unsecure during ride operations

H3: Smart Coaster operated outside of established parameters

H4: Intellectual Property exposed to unauthorized individuals

H5: Company takes actions inconsistent with stated values

H6: Consumer (rider) PII exposed to unauthorized individuals

H7: Smart coaster fails to deliver calculated rider experience

H8: Worker in close proximity to track or car while ride in motion

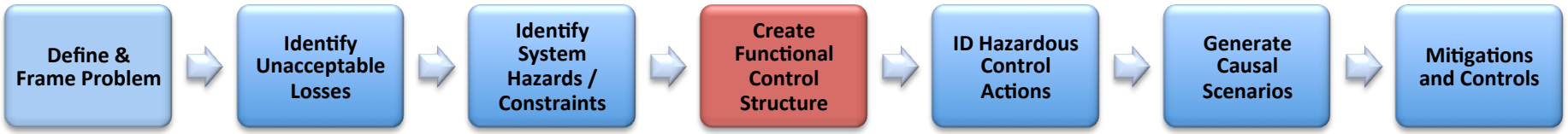


H4 & H6 are Security Concerns, but all Others Could be Safety or Security

© Copyright William Young Mar 2016

Entity / Activity Diagram

	ACTIVITIES						
ENTITIES	Onboard	Diagnose	Profile	Launch	Analyze	Offboard	Charge
Attendant							
Operator							
Operator Station							
Track							
Car							
Rider							

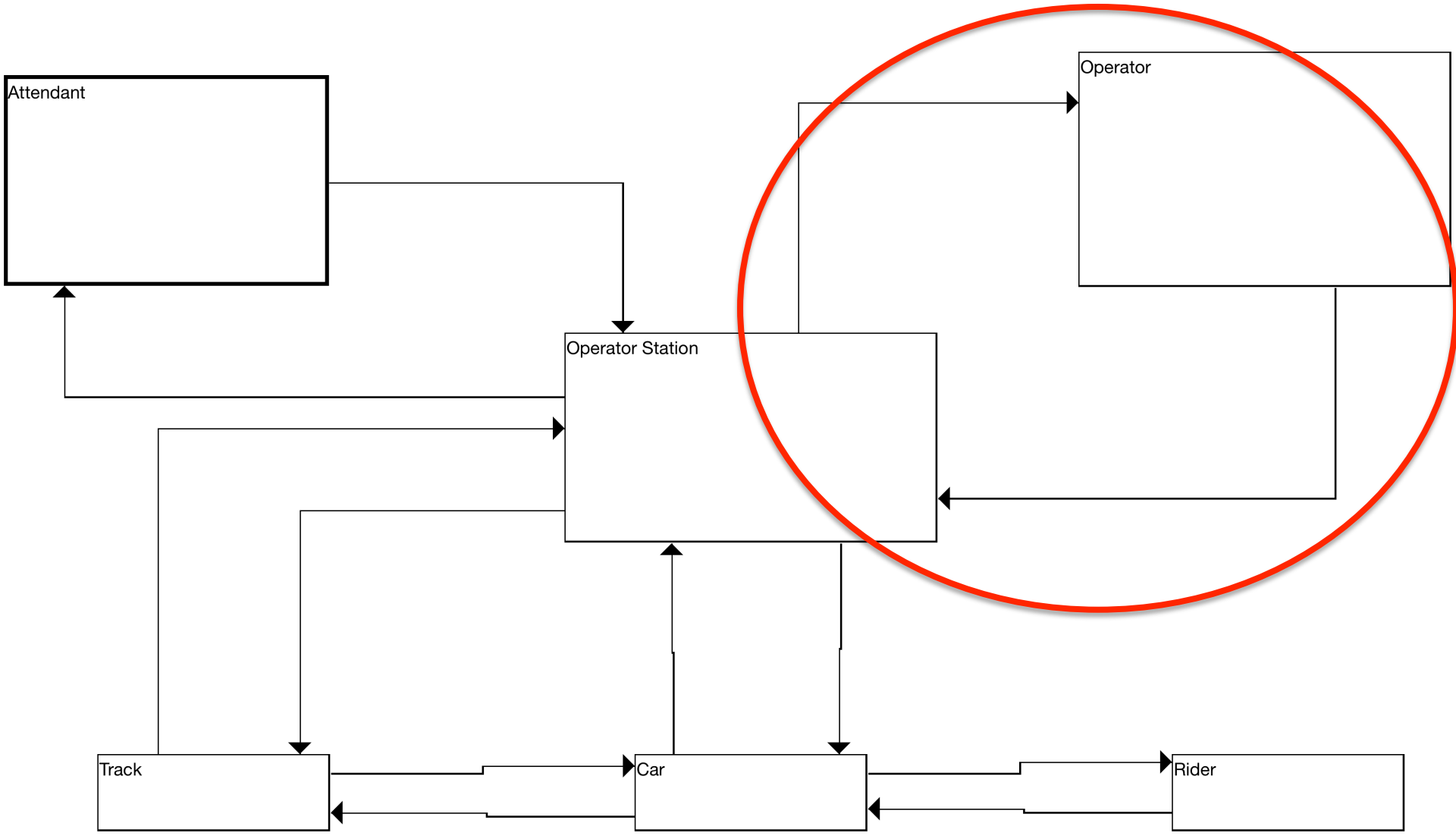


WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

E-A Diagram Block in Detail

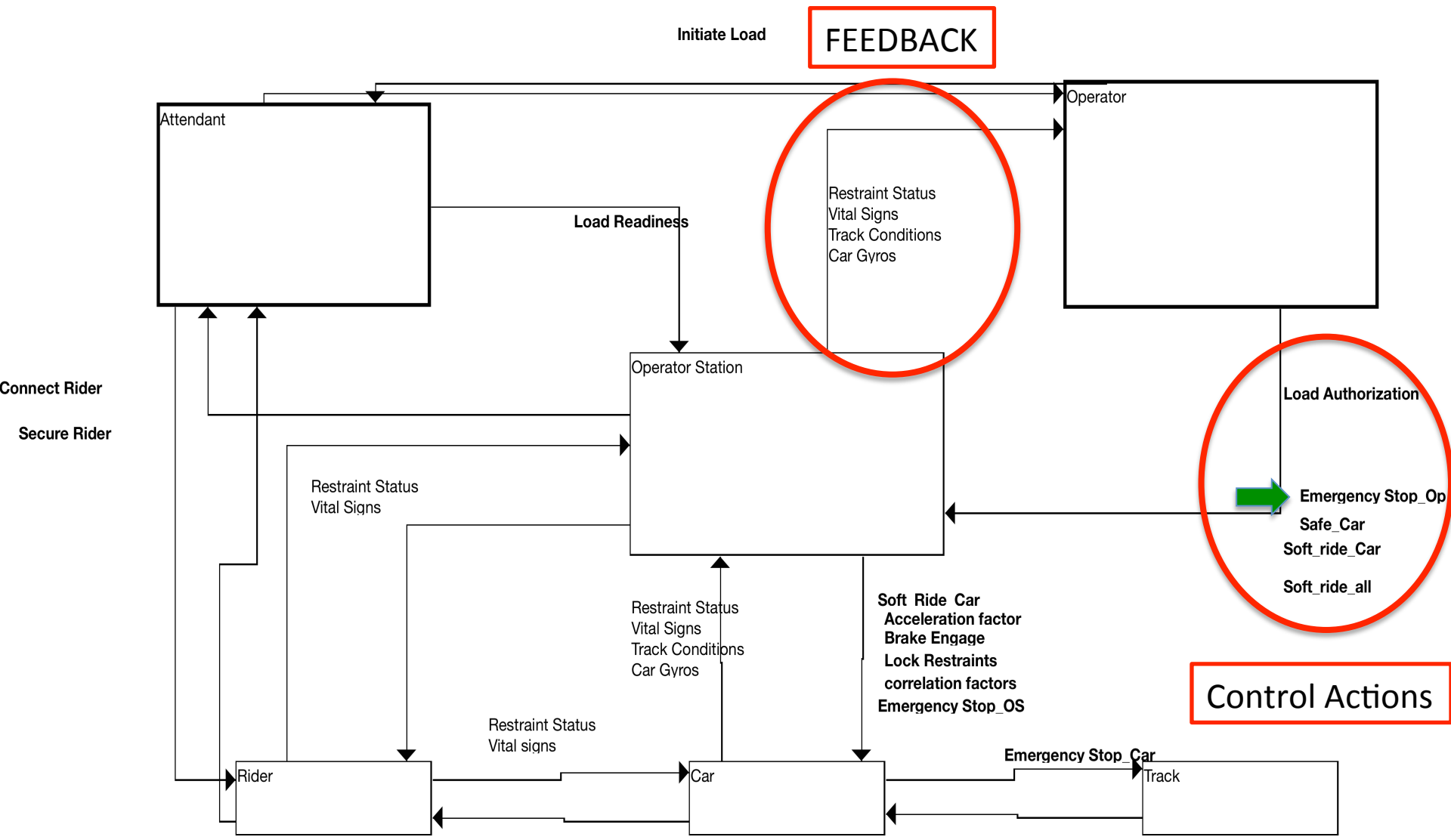
	Analyze
Operator	Monitors system for alerts via the operator station displays. Warning indications provided for unsafe conditions, status of rider restraints, status of car gyros and readiness for expected maneuvers. **Provides emergency stop command** if required to stop ride and return to a safe state.

WYOUNG@MIT.EDU
© Copyright William Young Mar 2016



WYOUNG@MIT.EDU

© Copyright William Young Mar 2016



- Fairly detailed control structure model can be created from a very abstract document
- We can then do analysis for security to facilitate early trades

WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

Partial Step I Table Entries for Emergency Stop Command from the Operator

UCA1.7	UCA1.10	UCA1.12	UCA1.11
Not providing Emergency stop when unsafe conditions arise is hazardous	Providing Emergency Stop when conditions are not unsafe can threaten "thrills" associated with ride.	Providing Emergency Stop too late (delayed) beyond some amount of time (based on distance and velocity of car) is hazardous	Continuing to provide Emergency Stop command after situation has been resolved presents hazard to ride operation
[H-1] [H-3]	[H-7]	[H-1] [H-3]	[H-7]
UCA1.8			
Not Providing Emergency Stop Command when a rider is unrestrained is hazardous			
[H-2]	Add given incorrectly UCA	Add wrong timing UCA	Add stopped too soon UCA
UCA1.9			
Not providing Emergency Stop Command when an operator is in close proximity to moving cars is hazardous			
[H-8]			



WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

Screen Shot from XSTAMPP

Why Would Operator Not Provide Emergency Stop When Required?

- HCA: Operator Does Not Provide Emergency Stop to Operator Control Station when Dangerous Conditions Present

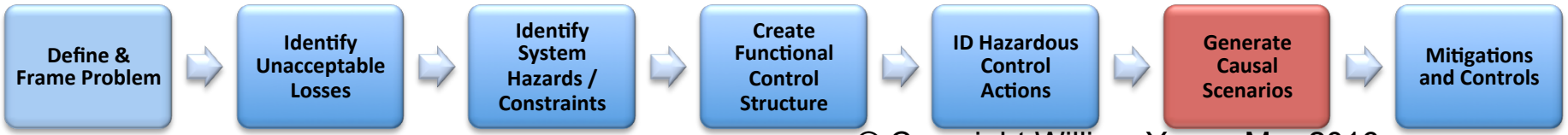
High Level Problems to be Resolved:

1) Inadequate process behavior– Operator control station doesn't provide Emergency Stop Command when Operator has sent it

2) Inadequate control – Operator issues the Emergency Stop but it is not received by the operator station

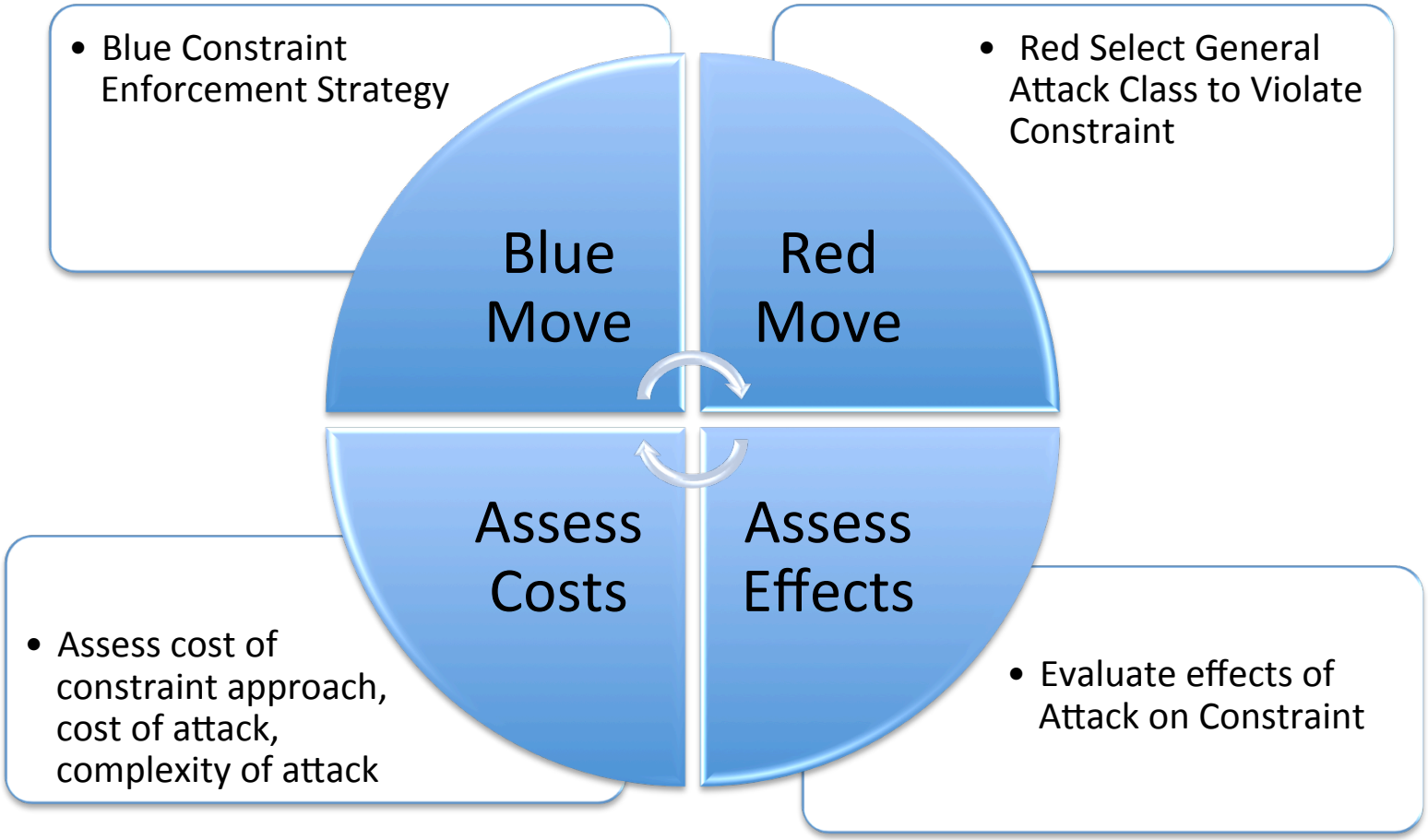
3) Inappropriate decision – Operator doesn't issue the Emergency Stop with indications that dangerous conditions are present

4) Inadequate feedback– Operator never receives indications of dangerous conditions when conditions are present



WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

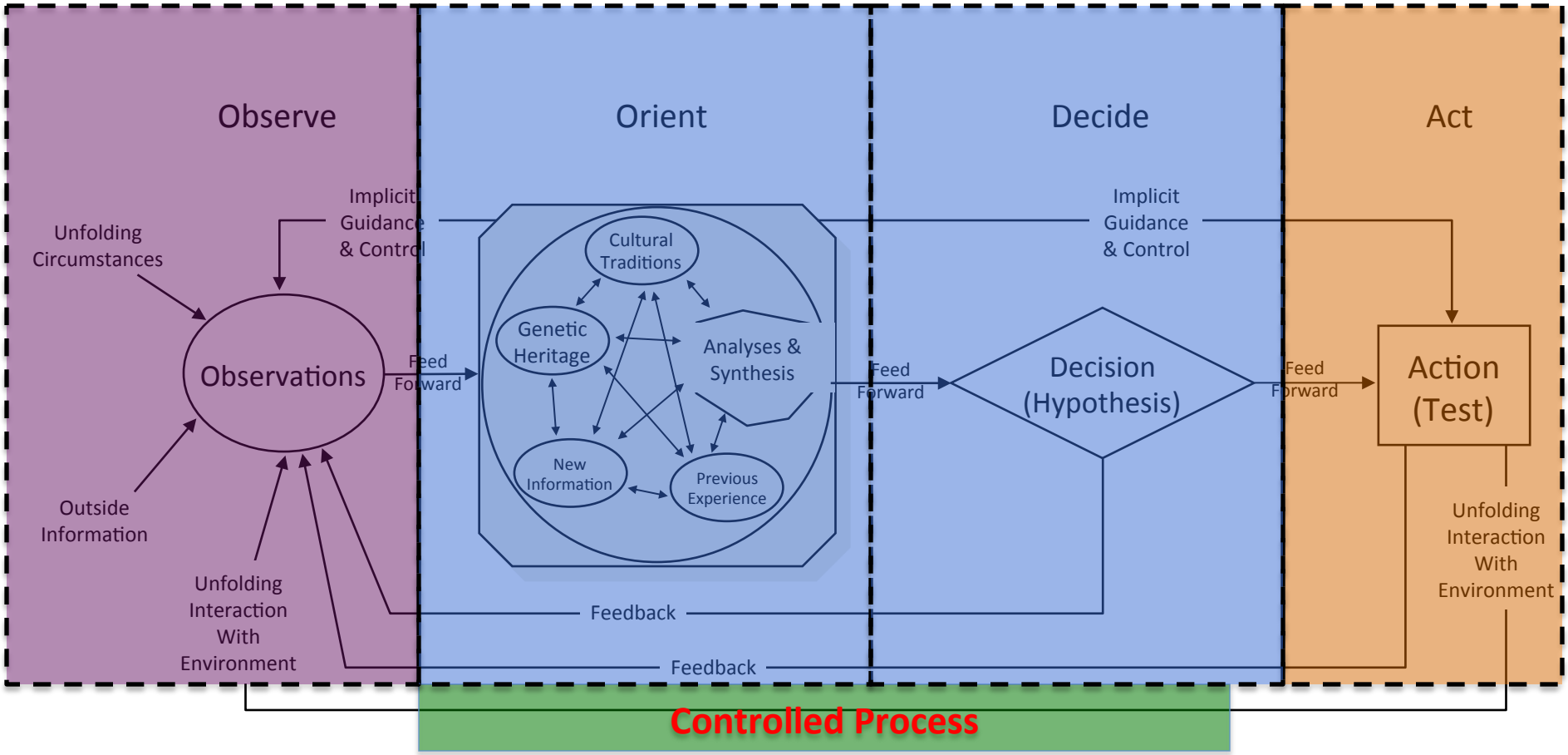
Wargaming



Blue Focus on Enforcing Constraint, Red Focus on Violating Constraint…
Goal is to "Fix" Problem Through Elimination or Mitigation Above Component

© Copyright William Young Mar 2016

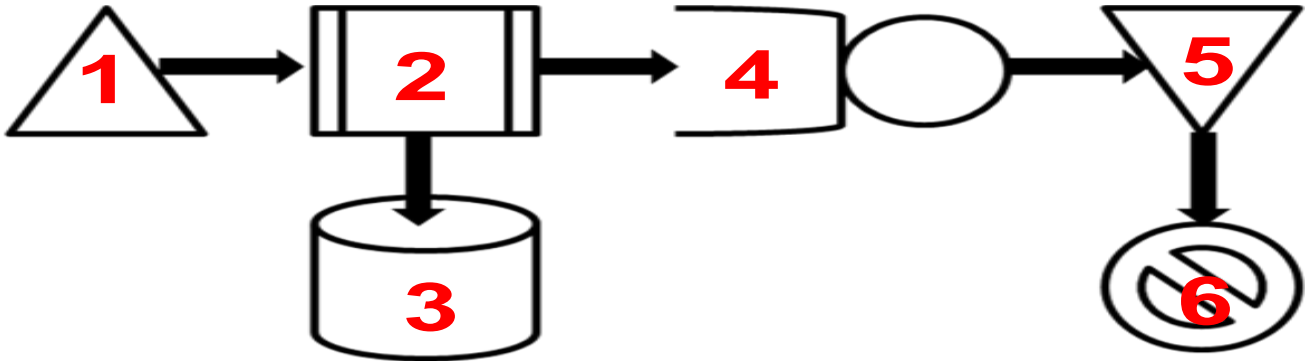
SENSOR PROCESS MODEL CONTROL ALGORITHM ACTUATOR



STPA-Sec Operationalizes John Boyd's OODA Loop (Defense Department's Operational Framework for Cyber Warfare)

WYOUNG@MIT.EDU
© Copyright William Young Mar 2016

Information Lifecycle



Information Lifecycle Stages

1) *information generation*
2) *information processing*
3) *information storage*
4) *information communication*
5) *information consumption*
6) *information destruction*

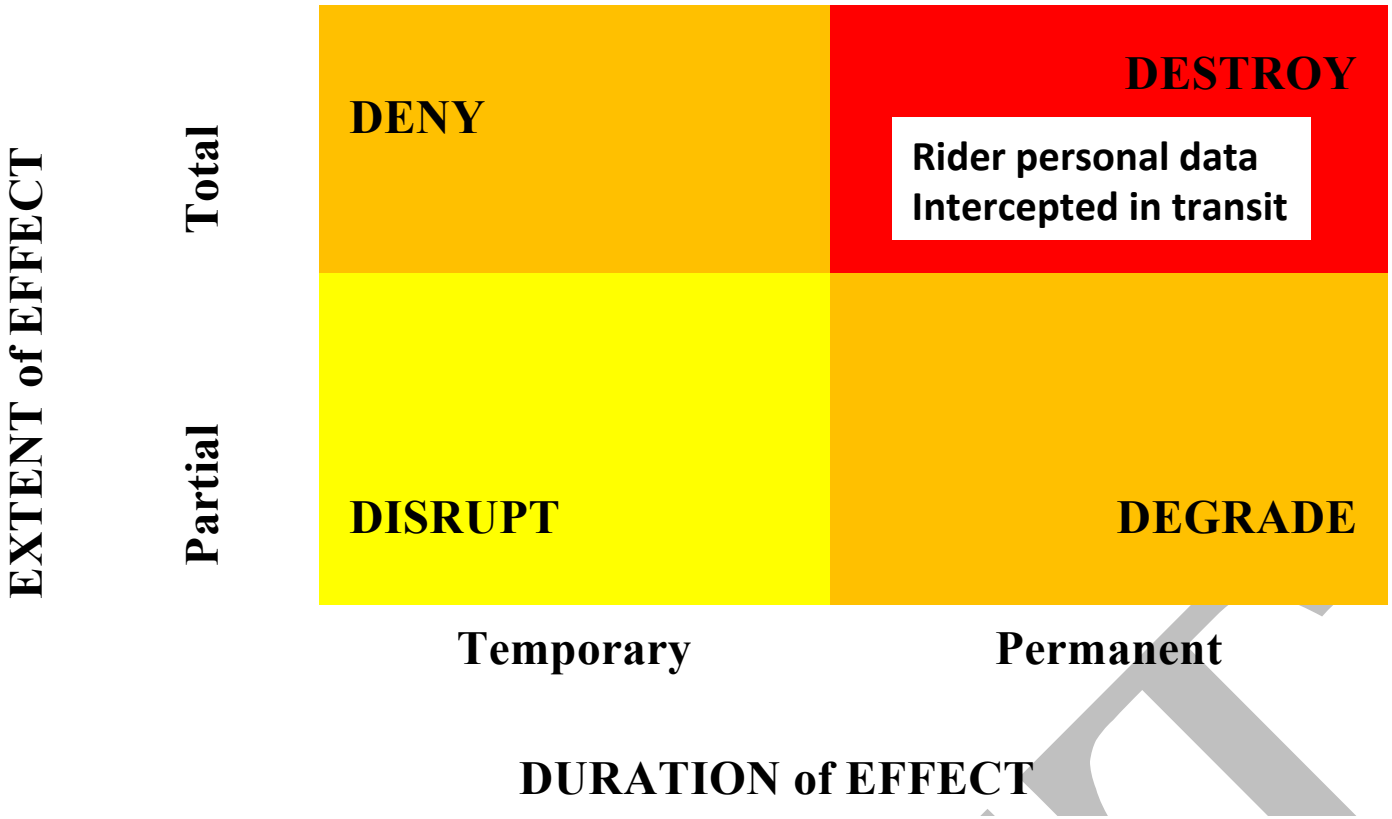
Information Lifecycle Adds Considerations to STPA-Sec

© Copyright William Young Mar 2016

Ref: (K. Jabbour & Muccio, 2013; K. M. Jabbour, Sarah, 2011)

D4 Evaluation

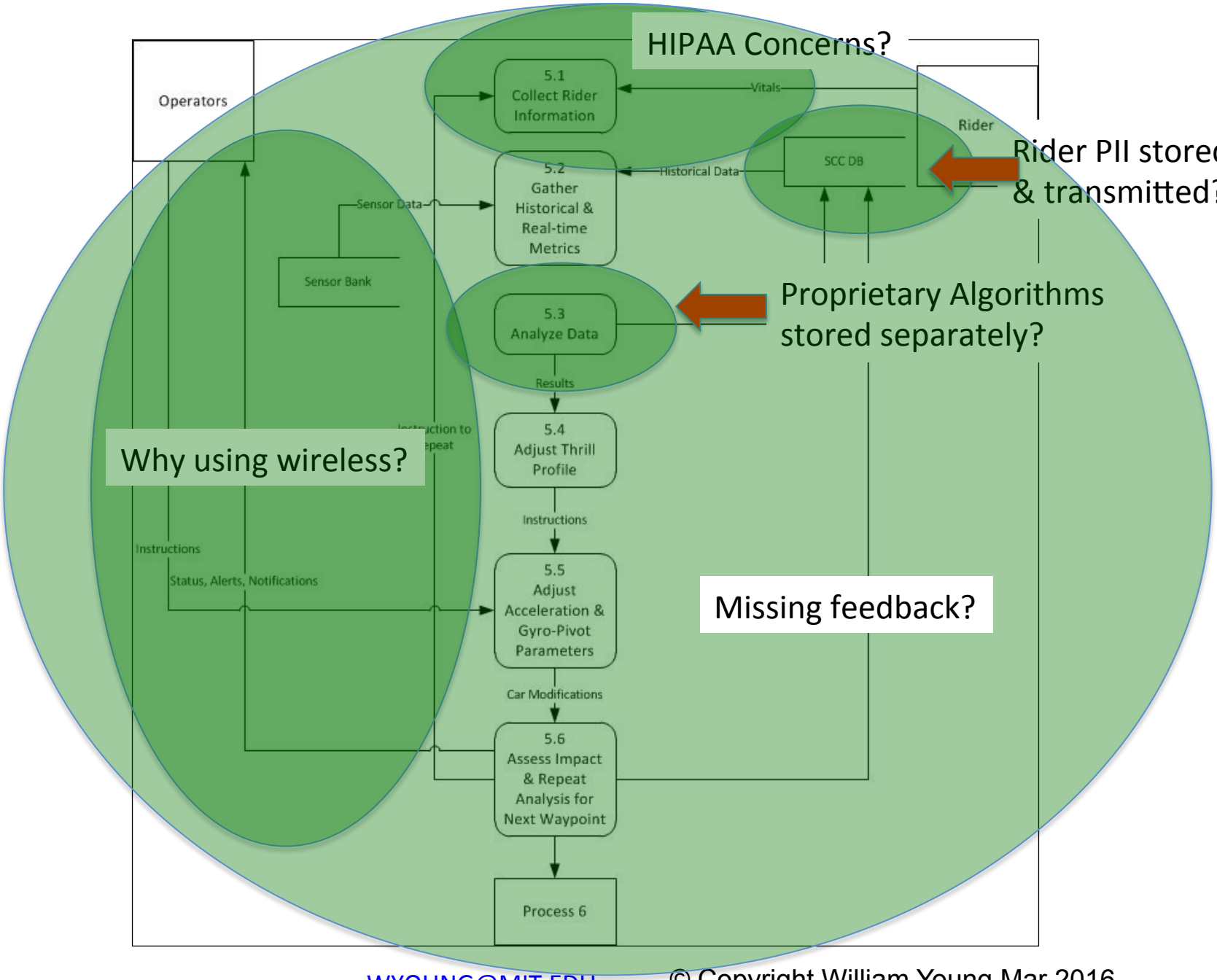
Goal: "continuing profitability and enhance reputation of ACME"



Where Does HCA Violation Scenario Fall on D4 Impact to Goal?

© Copyright William Young Mar 2016

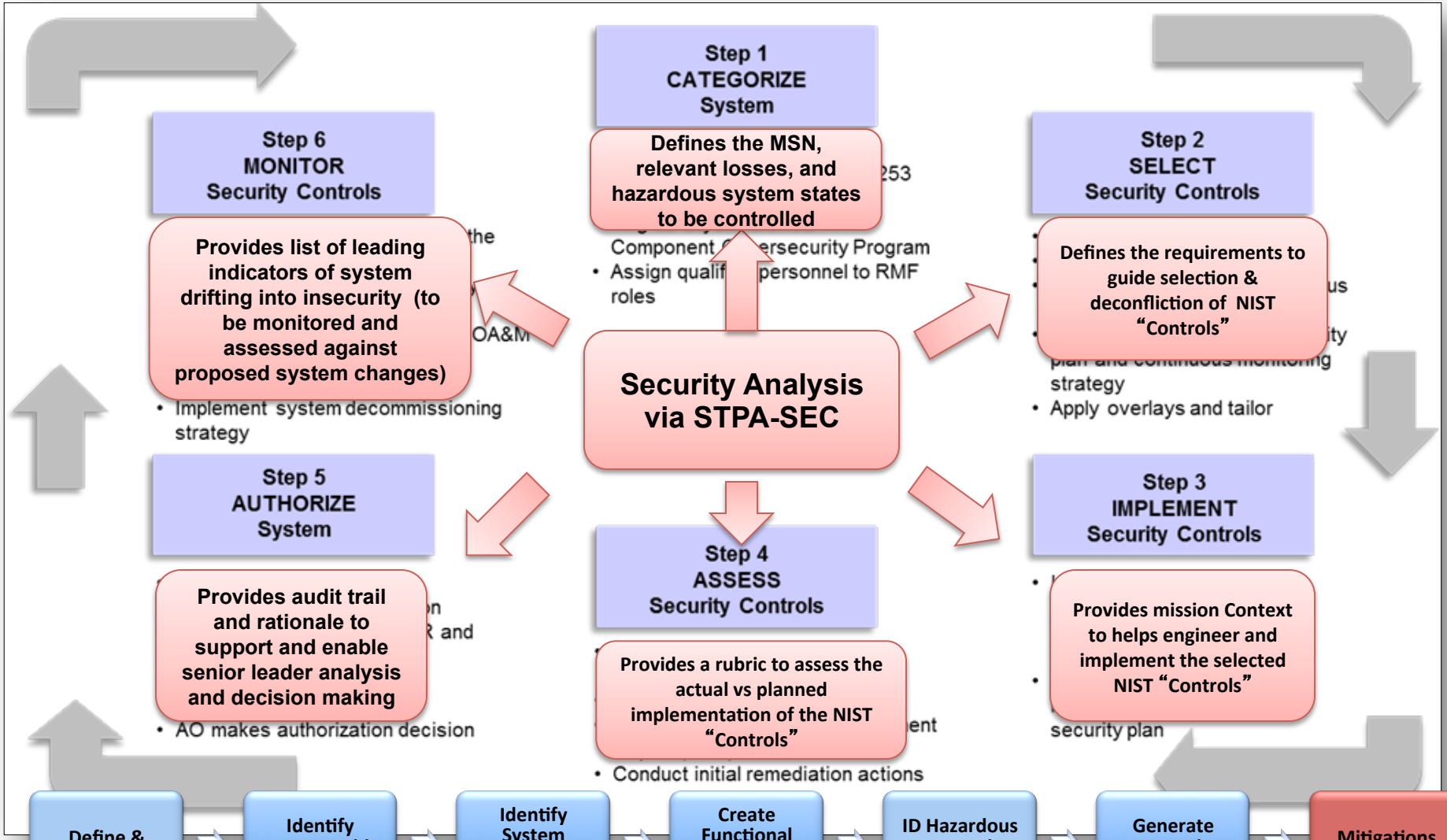
Ref: (K. Jabbour & Muccio, 2013; K. M. Jabbour, Sarah, 2011)



WYOUNG@MIT.EDU

© Copyright William Young Mar 2016

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



WYOUNG@MIT.EDU

© Copyright William Young Mar 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 Mar 2016





Understanding STPA-Sec Through a Simple Roller Coaster Example

William Young Jr

PhD Candidate, Engineering Systems Division

Systems Engineering Research Lab

Massachusetts Institute of Technology

2016 STAMP Conference

Boston, MA

March 23, 2016

WYOUNG@MIT.EDU

© Copyright William Young Mar 2016