

Applying System-Theoretic Process Analysis for Security (STPA-SEC) to Support Mission Assurance and Security

William Young

PhD Candidate, Engineering Systems Division

Massachusetts Institute of Technology

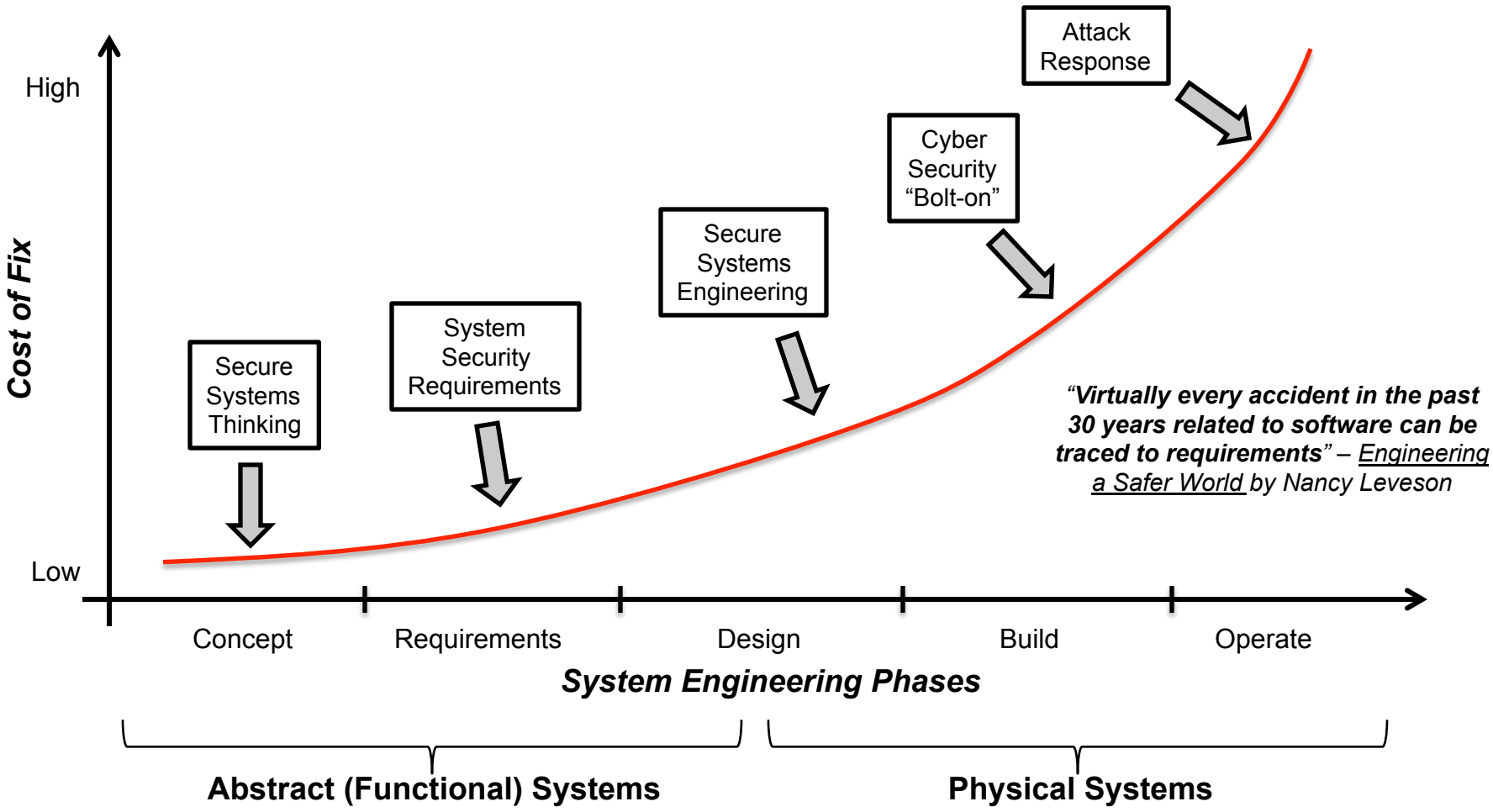


Overview

- Background / Motivation
- STPA-Sec Overview
- STPA-Sec Exercise
- Lessons Learned / Conclusions

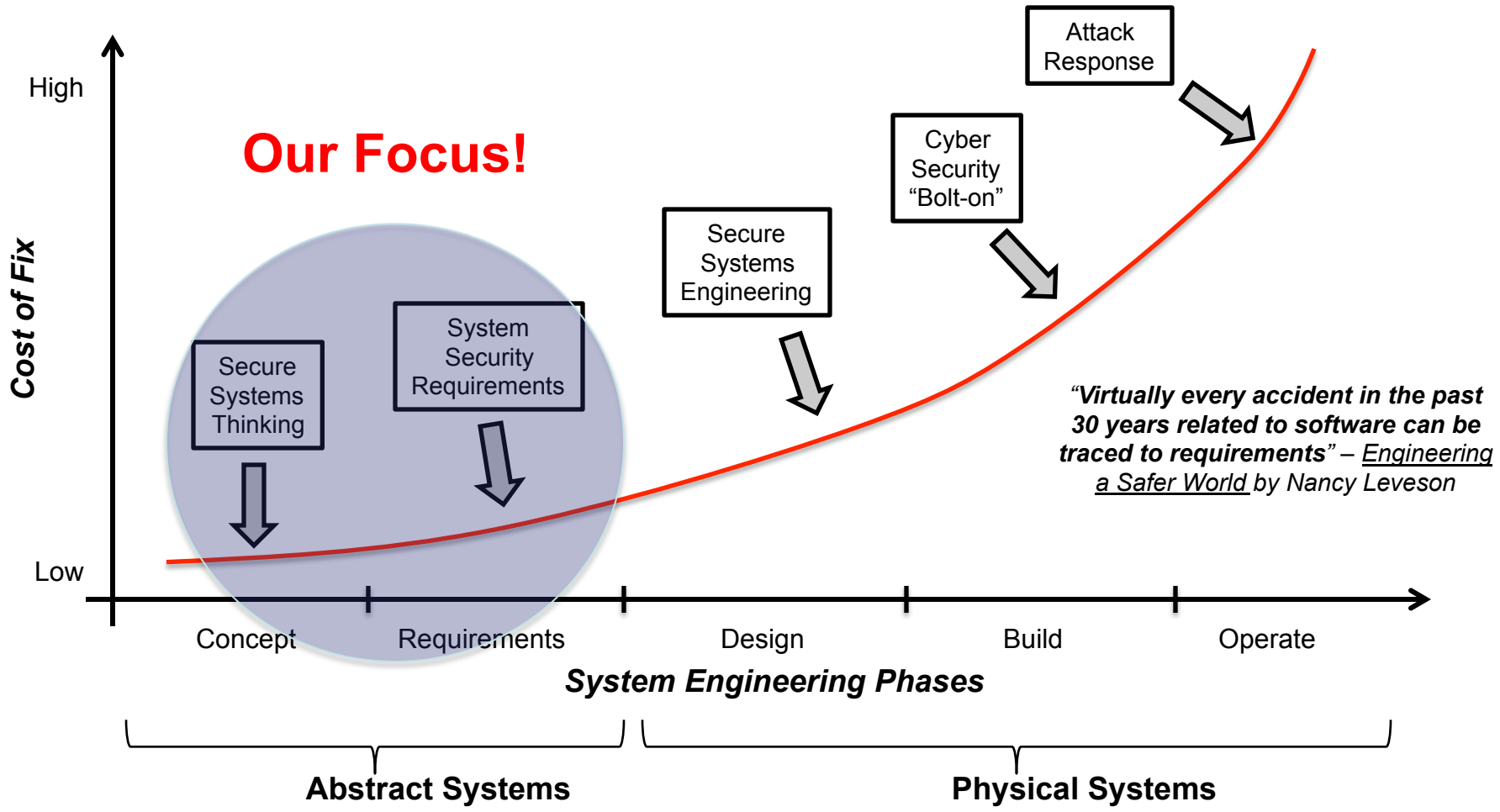
My Goal: Provide a (VERY) Condensed Tutorial

Motivation



Early Rigor Can Pay Big Dividends and Improve Assurance

Motivation



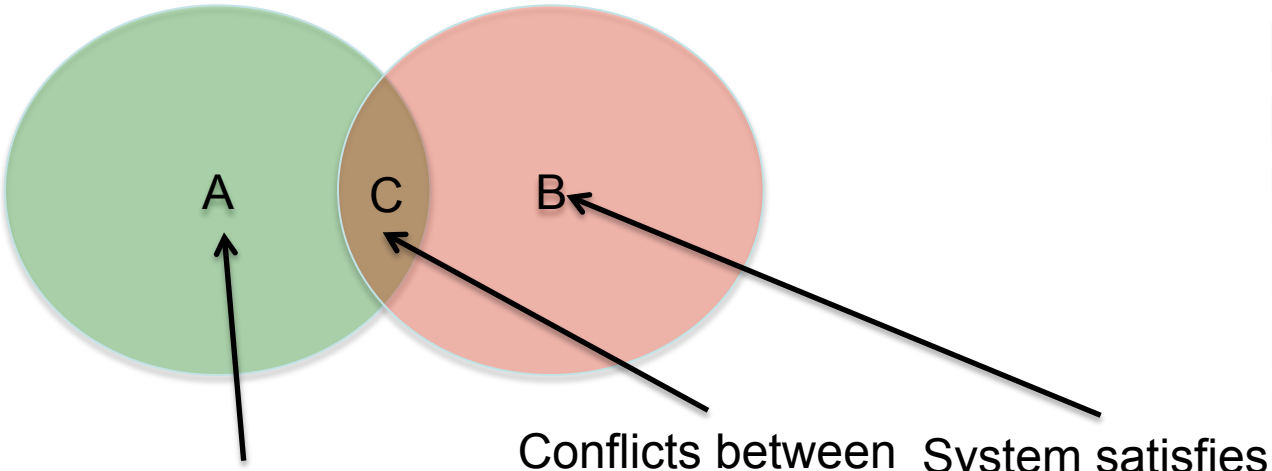
Goal: Engineer Systems Which are "Born Assurable"

WYOUNG@MIT.EDU

Functional vs Physical

(Functional)
Requirements & Constraints

Why / What ?



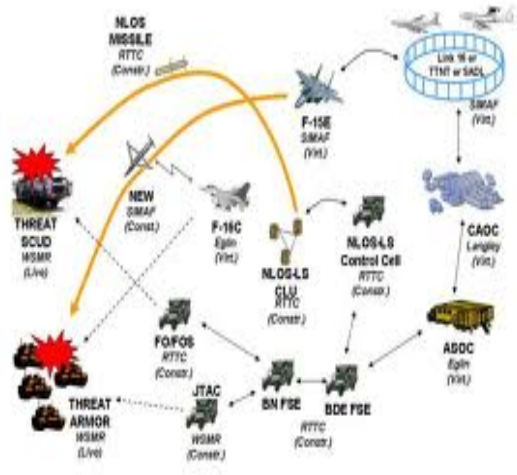
System satisfies functional behavior Requirements ("Must Do's")

Conflicts between Requirements & Constraints (Must Be Resolved)

System satisfies functional behavioral Constraints ("Must Not Do's")

(Physical)
Architecture
Design

How ?



Architecture Framework (DoDAF, FEAF, etc.)

Today we DO NOT establish Functional Constraints (B) to ensure system Satisfies Functional Requirements (A) in a secure (and safe) manner

WYOUNG@MIT.EDU

A Working Definition of Mission

- Webster:
  - a task or job that someone is given to do
  - a specific military or naval task
  - a flight by an aircraft or spacecraft to perform a specific task
- US Defense Department:
  - 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.
  - 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task.
  - 3. The dispatching of one or more aircraft to accomplish one particular task.

Purposeful Action Undertaken by Humans Using Tools (Engineered Systems) to Accomplish a Goal

WYOUNG@MIT.EDU

Mission Assurance

- "the ability to complete a wide range of missions across a wide range of degradations" --Linton Wells, Former US Defense Dept CIO
- Mission assurance is *functional*
- Focus is on mission completion NOT protecting the infrastructure humans use to complete mission
  - Some assets will need to be protected
    - Which assets?
    - Under what circumstances?
  - Should all work stop simply because "the network is down"?
  - Are all missions equal?

Mission Assurance is a Socio-Technical Strategy, You Must Start Here!

WYOUNG@MIT.EDU

Mission Assurance Versus CyberSecurity

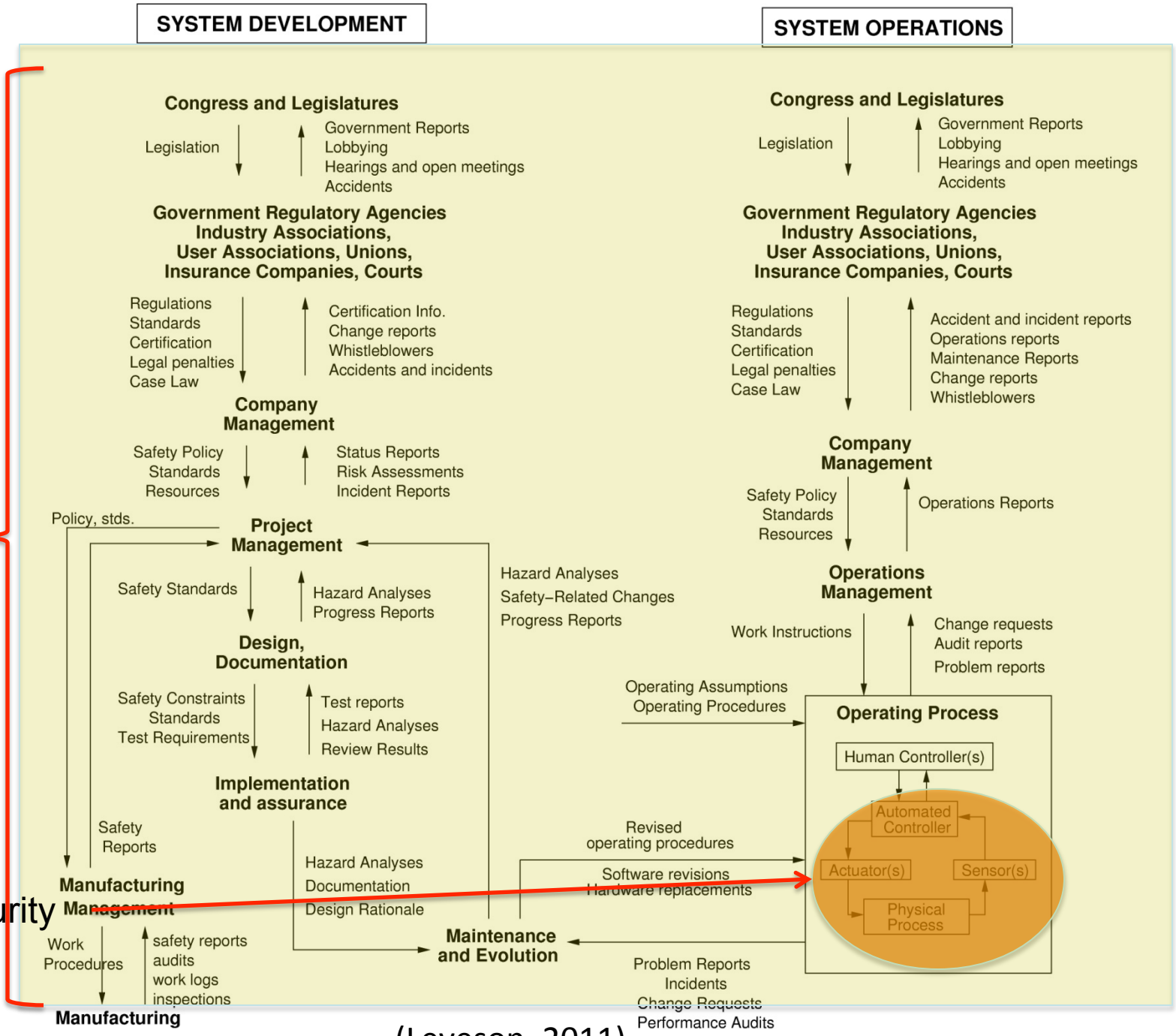
- Assure Operations
- IA_C
- Functional (operations)
- Info (semantic)-focused
- “Assure”
- Complex Interactions
- Socio-Technical
- Strategy

- Protect Assets
- C_{IA}
- Physical (Assets)
- Data-focused
- “Protect”
- Complicated Interactions
- Technical
- Tactics

WYOUNG@MIT.EDU

Required Mission Assurance Focus

Typical CyberSecurity Focus



(Leveson, 2011)

STPA-Sec: System-Theoretic Process Analysis for Security

What is STPA-Sec?

- An application of system engineering principles to cyber & cyber-physical systems
- A way to "bake-in" mission assurance from the system concept stage
- A problem framing methodology to help cope with the complexity of software-intensive systems
- A way to conduct a rigorous inquiry to identify and mitigate high-level cyber vulnerabilities at the concept stage of system development
- A defensible methodology to highlight cyber risk in potential architectures to better inform decision-makers

STPA-Sec Allows an Integrated Approach to Assuring Cyber Systems & Cyber-Physical Systems Left of Design

WYOUNG@MIT.EDU

What STPA-Sec is NOT

- A replacement for existing architectural frameworks
  - STPA-Sec augments framework views and informs early trade-offs and analysis
- A replacement for proven Secure Systems Engineering (SSE) Practice
  - STPA-Sec should complement and enhance these by establishing specific functional requirements to be implemented into physical architecture through SSE
- A new “tool” or “software program”
  - STPA-Sec is a rigorous inquiry / analysis process designed to prevent losses by controlling interactions between system components

STPA-Sec Big Picture Steps

- Establish the goal / purpose of the system
- Establish unacceptable losses for the system
- Establish the hazardous system states that place system at risk of suffering unacceptable losses
- Build Mission Functional Control Structure Model
- Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

WYOUNG@MIT.EDU

Scenario: Understand Mission Assurance Requirements for 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.

WYOUNG@MIT.EDU

Scenario: Smart Grid Power for F.O.B Operations



You are engineering a new deployable smart-grid to power a FOB. The computers running the grid may be subjected to cyber attack and operations must continue even if the system is attacked.

How Can You Integrate Mission Assurance Considerations During Concept Development and Requirement Generation?

WYOUNG@MIT.EDU

Question: What "Mission" is Being Assured?

The Grid

The People

The Operations of the People Operating the Grid

Perhaps the Most Important Step is to Understand the Mission the Technology Supports

WYOUNG@MIT.EDU

PHASE I: SYSTEM ENGINEERING FOUNDATION

WYOUNG@MIT.EDU

STPA-Sec Big Picture Steps

- Establish the goal / purpose of the system
- Establish unacceptable losses for the system
- Establish the hazardous system states that place system at risk of suffering unacceptable losses
- Build Mission Functional Control Structure Model
- Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

WYOUNG@MIT.EDU

Establishing the Goal / Purpose for the System

- Overview: Synthesize a concise statement that describes what the system is supposed to do
- Elicit purpose, method, goals through discourse with stakeholders (& early architecture, concept documents)
- Craft the description of the Mission 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

Create the Functional Model to Complement Architecture Model

WYOUNG@MIT.EDU

Key Stakeholder is the FOB Commander

- 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

WYOUNG@MIT.EDU

What Might a Reasonable Description of a Mission Functional Model Be?

WYOUNG@MIT.EDU

A Solution Based on Scenario:

- "A system to provide uninterrupted, stable power through grid generation, transmission and distribution in order to support the FOB mission."
  - Priorities are base security, medical, operational Command & Control (C2), and fire direction (radars). If power is interrupted, immediate backup power must support priority base functions. Life support requires not less than 2 hours of dependable power in the event of a loss."

Important Note: The Key Activities Necessary to Conduct the Mission Include Generating, Transmitting, and Distributing Power

WYOUNG@MIT.EDU

STPA-Sec Big Picture Steps

Establish the goal / purpose of the system

Establish unacceptable losses for the system

- Establish the hazardous system states that place system at risk of suffering unacceptable losses
- Build Mission Functional Control Structure Model
- Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

WYOUNG@MIT.EDU

Identify Unacceptable Losses

- Overview: Must first understand what losses the system owner / stakeholders care about so we can help prevent them
- Owner / stakeholders must identify the unacceptable consequences or outcomes
  - This sets foundation for analysis because resources are limited
- A loss is a specific, high-level outcome
- Should be a very short list
  - Avoid confusing causes of losses (mistakes, failures, enemy activity, etc) with the losses themselves (outcomes)
  - Should ID areas where owners / stakeholders are unwilling to accept adverse outcome
  - Must prioritize because everything cannot be protected

Mission Assurance Should "Protect" System Function Against These Specified Losses (Regardless of Source)

WYOUNG@MIT.EDU

Determining Unacceptable Losses

- Ultimately come from mission "owner"
  - Subject matter experts can assist
- Very high level initially
- Will impact how mission is conducted
- Example
  - Injure or kill non-combatants
  - Corporate reputation irreparably damaged
  - Loss of PII
  - Expose residents to dangerous radiation

What Might a Reasonable Set of Losses Be?

WYOUNG@MIT.EDU

Example Scenario:

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

WYOUNG@MIT.EDU

*Perform In-Progress Review (IPR) 1

- Overview: Formal review with owner / stakeholders to validate initial Functional Model description and losses
  - Similar in concept used in military planning
  - Conducted for same purpose
    - "to shape the plan as it is developed"
  - Bring stakeholders along on the journey

The IPR Provides Mission Owner / Stakeholders An Early Opportunity to Not Only Shape the Analysis, but to Help Ensure the Eventual Analysis Output is Useful

*Optional, But Recommended

WYOUNG@MIT.EDU

STPA-Sec Big Picture Steps

- ✓ Establish the goal / purpose of the system
- ✓ Establish unacceptable losses for the system
- ⇨ Establish the hazardous system states that place system at risk of suffering unacceptable losses
- Build Mission Functional Control Structure Model
- Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

WYOUNG@MIT.EDU

Identify Hazards (Mission Functional Vulnerabilities)

- Overview: Must specify a set of high-level mission functional vulnerabilities that are linked to the losses identified in previous step
- Hazard + worst case environmental conditions will yield a loss
  - Environmental conditions are those things outside system boundary
  - Hazard presence is necessary, but insufficient for loss
- STPA-Sec focus is preventing losses by constraining system from entering hazardous state

Hazards Have the Potential to Lead to the Losses Previously Identified

Hazards are System Functional Vulnerabilities that Can Lead to Losses

- Determine system vulnerabilities
  - "System state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss"
  - Similar to Swiderski & Snyder Threat Modeling
    - "Set of conditions that must occur or be true for a threat to be realized"
  - Should be small, exhaustive set
    - "Designating a weapon impact area containing non-combatants"
    - "Customer PII exposed to unauthorized individuals"
    - "Inadvertently releasing radiation"

Focus: Identify and Control System Vulnerable States to Prevent Intentional (and Unintentional) Losses

Example: The Forest is the System of Interest, Loss is Forest Fire, What is Hazard?

Remember: Hazards Have the Potential to Lead to Losses, So Where Would You Focus The majority of Your Attention?

WYOUNG@MIT.EDU

What Might a Reasonable Set of Hazards Be for the Example?

WYOUNG@MIT.EDU

Hazards – Example

- H1. power distribution not IAW FOB Commander priorities
- H2. power output not within prescribed limits (voltage / freq)
- H3. loss of power

Hazards Have the Potential to Lead to the Losses Previously Identified

Hazards – Example

- H1. power distribution not IAW FOB Commander priorities
- H2. power output not within prescribed limits (voltage / freq)
- H3. loss of power

	L1:Inability to Support FOB CC Mission	L2: Inadvertantly causing unacceptable degrade to FOB	L3: Loss of Life /Serious Injury	L4: Significant damage to equipment (FOB or Grid)
H1:		X	X	
H2:		X	X	X
H3:	X			X

Hazards Have the Potential to Lead to the Losses Previously Identified

WYOUNG@MIT.EDU

35

STPA-Sec Big Picture Steps

- ✓ Establish the goal / purpose of the system
- ✓ Establish unacceptable losses for the system
- ✓ Establish the hazardous system states that place system at risk of suffering unacceptable losses
- ⇨ Build Mission Functional Control Structure Model
- Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

WYOUNG@MIT.EDU

BREAK

WYOUNG@MIT.EDU

PHASE II: MODEL DEVELOPMENT

WYOUNG@MIT.EDU

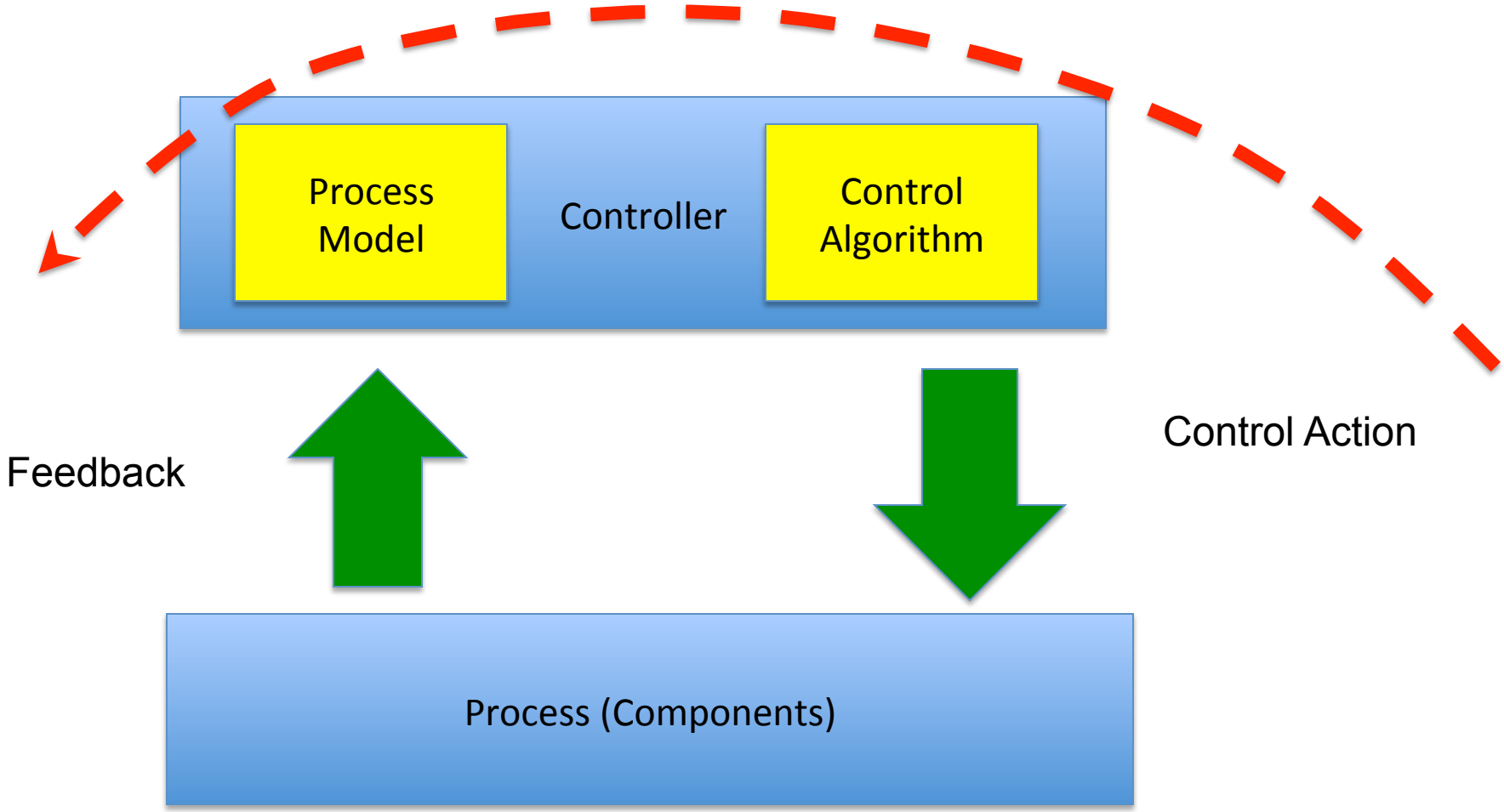
Build Mission Functional Control Structure Model (MFCSM)

- Overview: Developing the MFCSM proceeds from general to specific
- This is the actual model of the system that will be evaluated to identify mission functional vulnerabilities
- This task includes multiple sub-tasks
- The sub-tasks are accomplished in an iterative manner

The Mission Functional Control Structure Model is a Graphic that Supports Reasoning about the Functional Security Requirements for Architecture

WYOUNG@MIT.EDU

Developing MFCSM Big Picture



Work Top-Down in a Rigorous Manner to Prevent Missing Something

Build Mission Functional Control Structure Model

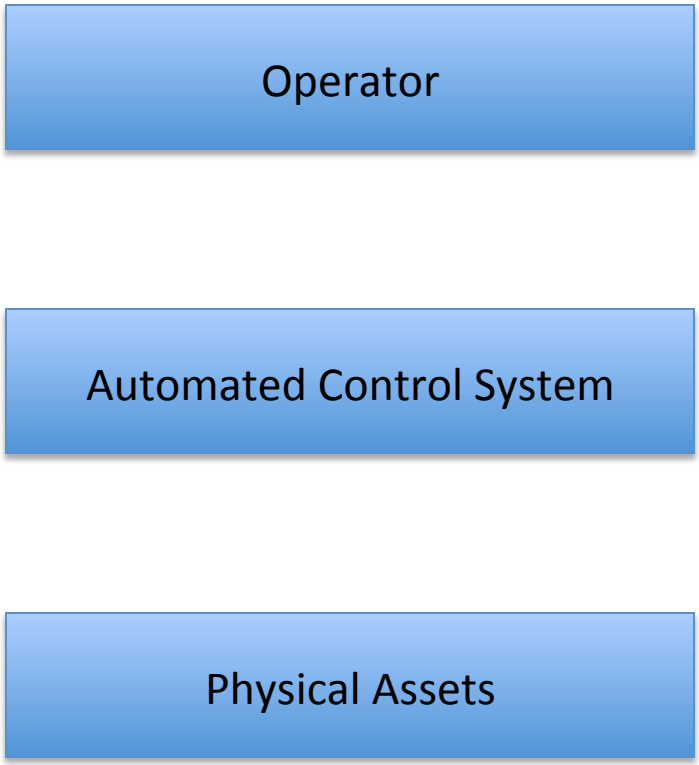
- Identify Model Elements

Identify Model Elements

- Look at description of Mission Functional Control Structure Model from earlier
  - What "things" are required to perform the overall function?
  - Connect the elements according to planned policy and procedures
  - Start with a very abstract model and then refine through analysis
- Place elements as blocks on diagram
  - Include hierarchy information if possible

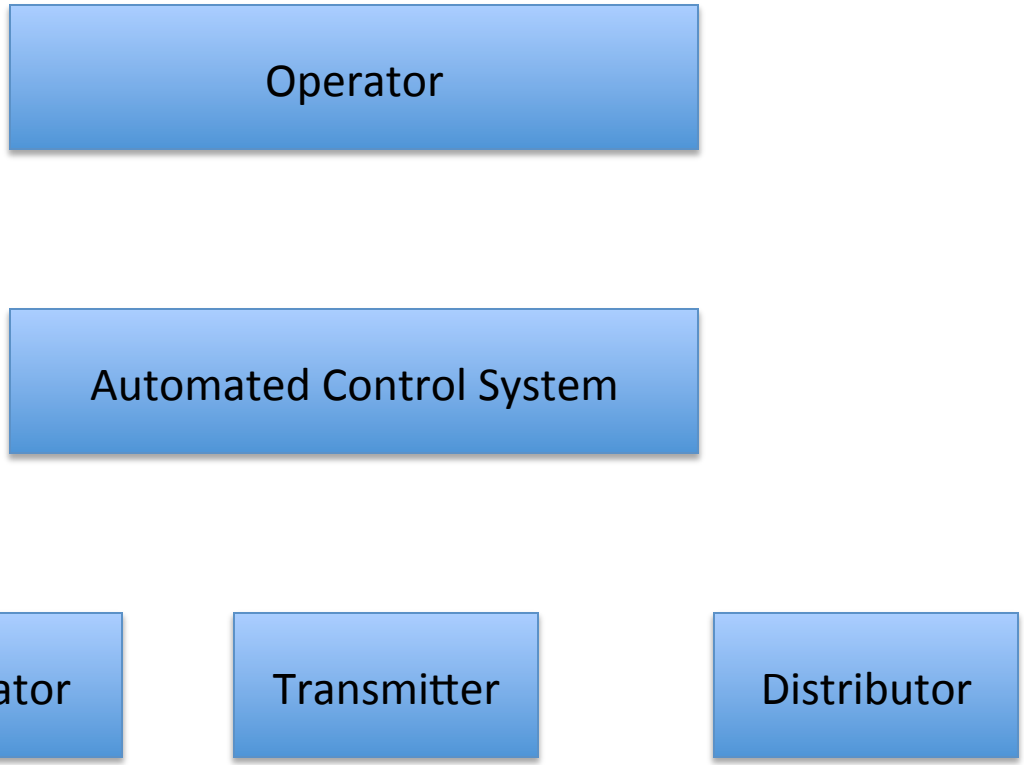
What Might a Reasonable Set of Initial Elements be for the Example?

High-Level "Building Blocks"



Each of the Elements Can Be Further Decomposed As the Analysis Evolves, but the Goal is to Understand the Interactions Between Elements

High-Level “Building Blocks” alternative



Each of the Functional Elements are Representative at This Point Because we Haven’t Actually Specified The Architecture Yet

Build Mission Functional Control Structure Model

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission

Identify Each Element's Responsibilities in Carrying out Each Key Activity

Key Activity #?: (NAME)	
Element	Responsibilities
Operator	
Automatic Control System	

- Capture the responsibility each element has in carrying out each of the key activities
  - Prepare a table for each key activity
- You can check here to ensure you haven't missed anything

Capture How Each of the Elements is Envisioned to Contribute to Accomplishing the Key Activities Previously Identified

Pick an Activity and Identify How One of the Elements Contributes to Its Function

Key Activity: (Generate, Transmit, Distribute)	
Element	**Responsibilities**
Operator	
Automatic Control System	
Generator	
Transmitter	
Distributor	

- Helpful hints:
  - Refer back to the Mission Functional Control Structure Model description
  - Focus on how each element contributes to each of the key activities being accomplished to include “tracing” backward to ID something missed earlier
  - Write explanatory statements and then summarize in an abbreviated responsibilities column

Pick an Activity and Identify How One of the Elements Contributes to Its Function

Key Activity: Distribute	
Element	**Responsibilities**
Automatic Control System	Transmit distribution control information (instructions) to distribution element so that power is distributed IAW FOB commander's priorities and the state of the external environment (e.g. emergency, under attack). Adjust distribution if system suffers damage and power must be used to support a particular function. Know the status of current distribution and report it to operator. Provide acknowledgement of reveipt and execution of operator control information

Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission

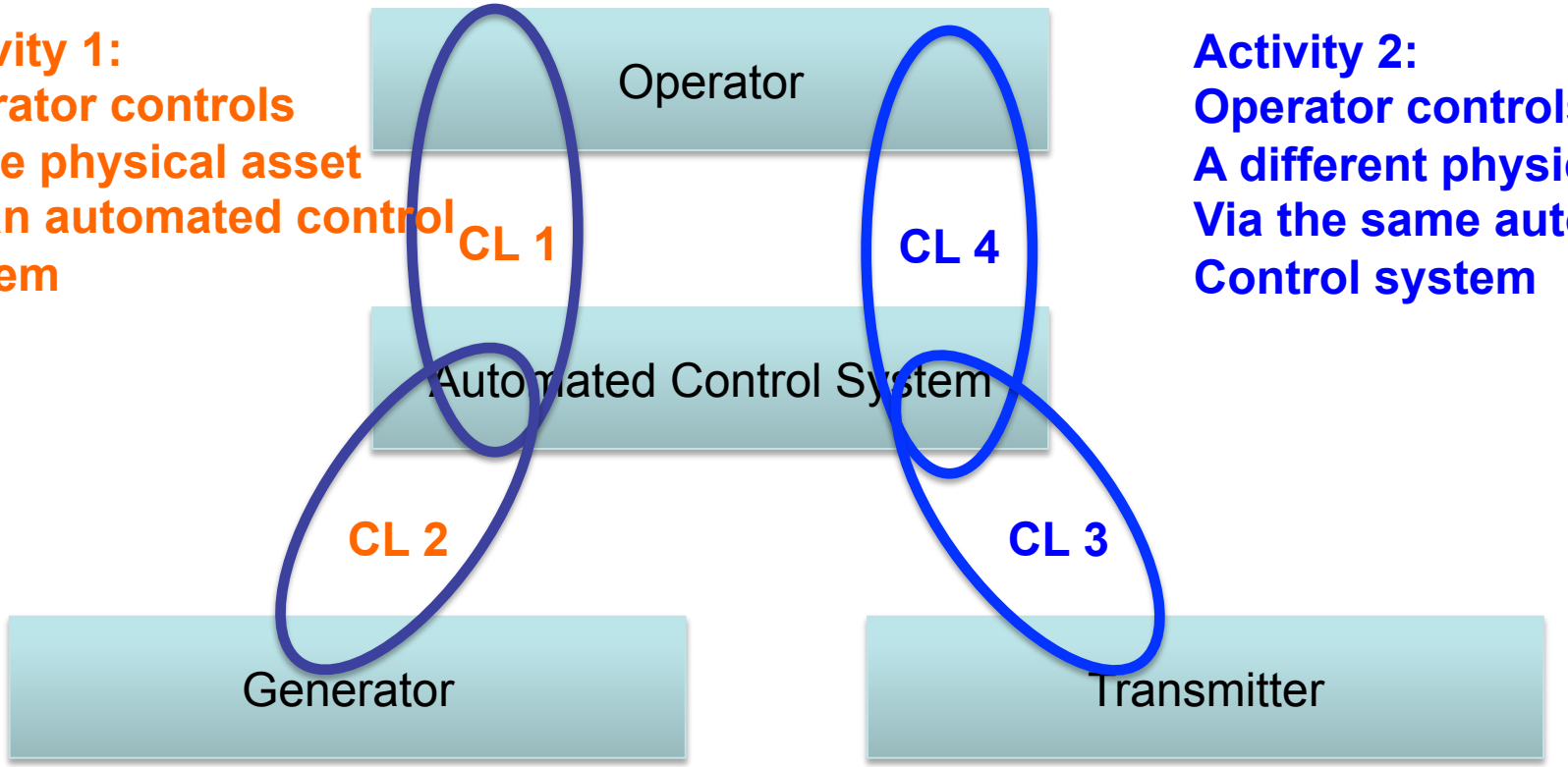
Identify Control Relationships

Identify Control Relationships

- Some elements “control” others
  - Issue Direction and Monitor feedback
- Identify the key activities within which the control takes place
  - Specify which of the activities involve the particular control loop

Control Loops & Associated Activities

Activity 1:
Operator controls
Some physical asset
via an automated control system



Activity 2:
Operator controls
A different physical asse
Via the same automated
Control system

The Controller (Higher Level Element) is Responsible for Enforcing Constraints on the Controlled Process (Lower Level Element)

Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission
- Identify Control Relationships
- Identify the Control Actions necessary for each element to execute their responsibilities

ID Specific Control Actions (Directions) Necessary for Each Element to Execute Key Activities

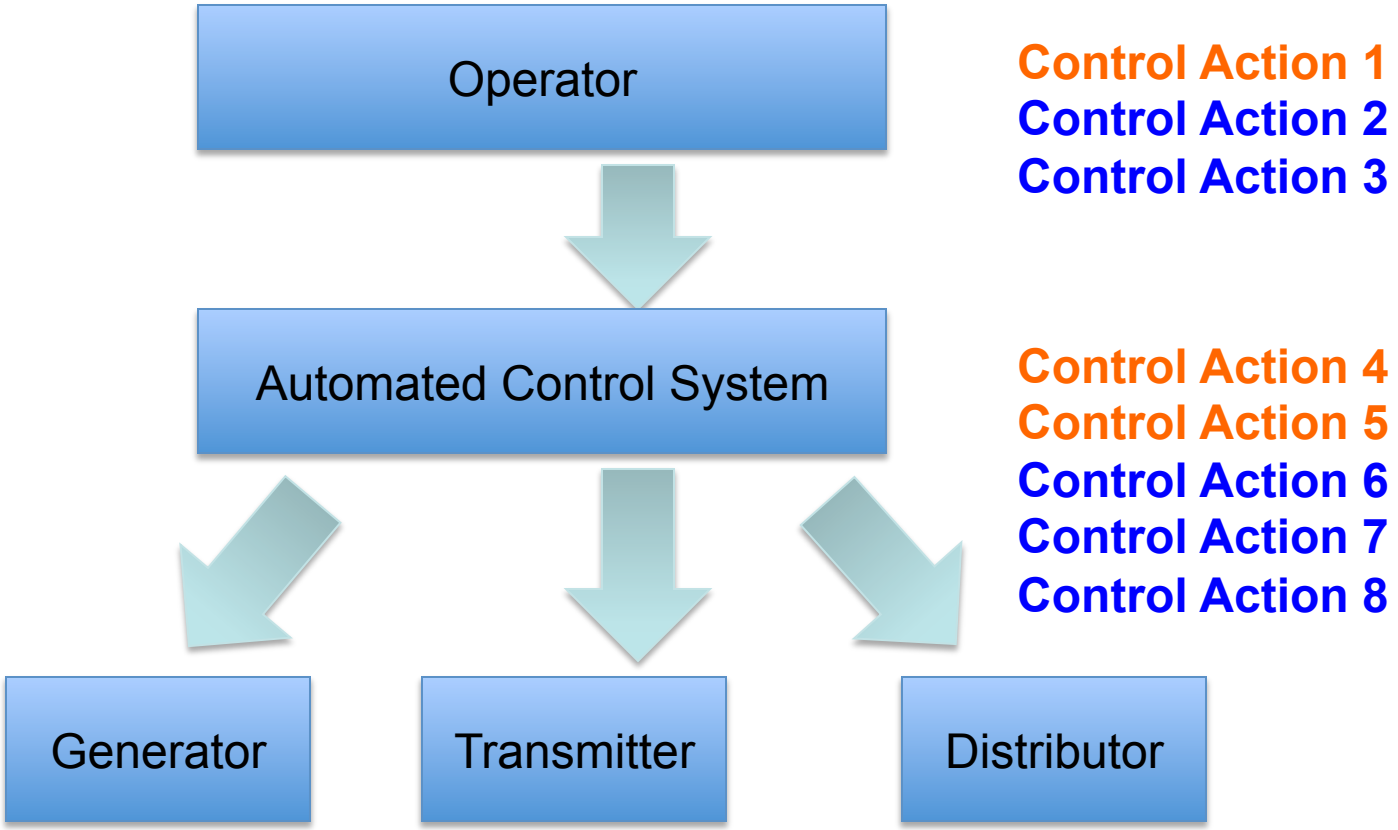
Key Activity: NAME (Generate, Transmit, Distribute)		
Element	Responsibilities	Required Control Actions

- Add a column to table created earlier
- When complete, add each of the control actions to the appropriate element with a down arrow
  - Can color code to denote the particular activity associations

Pick an Activity and Identify How One of the Elements Contributes to Its Function Based on the Responsibilities Previously Identified

Key Activity: Distribute		
Element	Responsibilities	Required Control Actions
ACS	Transmit Distribution instructions…	Distribution Priorities,

Updating the MFCSM



Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission
- Identify Control Relationships
- Identify the Control Actions necessary for each element to execute their responsibilities

Develop Process Model Description

Develop Process Model Description

- Describe in Words How Each Element Processes Information (Makes Decisions for Issuing Control Actions
- This should be a short description of the high-level logic
  - Includes how the element determines the situation (state) and then decides what needs to be done

Do Not Get Overwhelmed by the Magnitude of This Task, Start at the Broad, High Level and Refine Where Necessary

Develop Process Model Description

Element: (NAME)		
Responsibilities		
Control Actions	Key Activity	Process Model Description / Decision Logic
CA1		e.g. “Execute CA when___{context}___”
CA		
CA		

- Helpful hints:
  - Reorganize spreadsheet information previously entered to reflect the structure depicted above
  - Work “backward” from Control Actions and responsibilities to determine the decision logic that is desired
  - This step can often identify information that was missed previously

Pick an Activity and Element, then Develop the Process Model for one Control Action

Element: ACS		
Responsibilities: Control and Synchronize grid generation, transmission…		
Control Actions	Key Activity	Process Model Description / Decision Logic
Emergency Override	Distribution	Execute *Emergency Override* when power must be routed to priority functions

Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission
- Identify Control Relationships
- Identify the Control Actions necessary for each element to execute their responsibilities
- Develop Process Model Description
- Identify Process Model Variables

Identify Process Model Variables (PMV)

- PMV determine the context of the mission and enable the controlling element to issue the proper CAs
- Append table created in previous step
- What Information is required to execute decision logic
- When complete, annotate a PM block in each element

Element: (NAME)			
Responsibilities			
Control Actions	Key Activity	Process Model Description / Decision Logic	Process Model Variables
CA1		e.g. “Execute CA when___{context}___”	PMV 1, PMV 2
CA			PMV 1
CA			PMV 3

Develop the Process Model Variables For the Process Model You Chose in the Previous Step (or Choose another)

Element: (NAME)			
Responsibilities			
Control Actions	Key Activity	Process Model Description / Decision Logic	Process Model Variables

Develop the Process Model Variables For the Process Model You Chose in the Previous Step (or Choose another)

Element: ACS			
Responsibilities			
Control Actions	Key Activity	Process Model Description / Decision Logic	Process Model Variables
Emergency Override	Dist	Execute when power must be routed to priority functions	Mission state, Grid Status

How does the ACS know when this is?

By Deciding Based on this information

Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission
- Identify Control Relationships
- Identify the Control Actions necessary for each element to execute their responsibilities
- Develop Process Model Description
- Identify Process Model Variables
- Identify Process Model Variable Values

Identify Process Model Variable Values

- Values the Process Model Variables can assume
- Be sure to include “unknown”
- Don’t need to be fine-grain
- But must be inclusive

Element (e.g. operator)	PMV 1:	- PMV Val 1 - PMV Val 2 - Unknown
	PMV 2:	
	PMV 3:	

Develop the Process Model Variable Values For the Process Model Variable You Chose in the Previous Step (or Choose another)

Element: ACS			
Responsibilities			
Control Actions	Key Activity	Process Model Description / Decision Logic	Process Model Variables
Emergency Override	Dist	Execute when power must be routed to priority functions	Mission state, Grid Status

Develop the Process Model Variable Values For the Process Model Variable You Chose in the Previous Step (or Choose another)

- Mission State
  - Normal
  - Abnormal
  - Unknown
- Grid Status
  - Normal
  - Emergency
  - Unknown

Can You Already See How The ACS Issuing the Emergency Override for Distribution Could Create a Hazard that Might Lead to One of the Losses We Identified Initially?

Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission
- Identify Control Relationships
- Identify the Control Actions necessary for each element to execute their responsibilities
- Develop Process Model Description
- Identify Process Model Variables
- Identify Process Model Variable Values
- Identify Feedback providing PMV Values

Identify Source of Feedback Information Providing PMV Values

- Do this for each element
- Add to the MFCSM the arrow going into the appropriate element
- Can color code if desired to differentiate

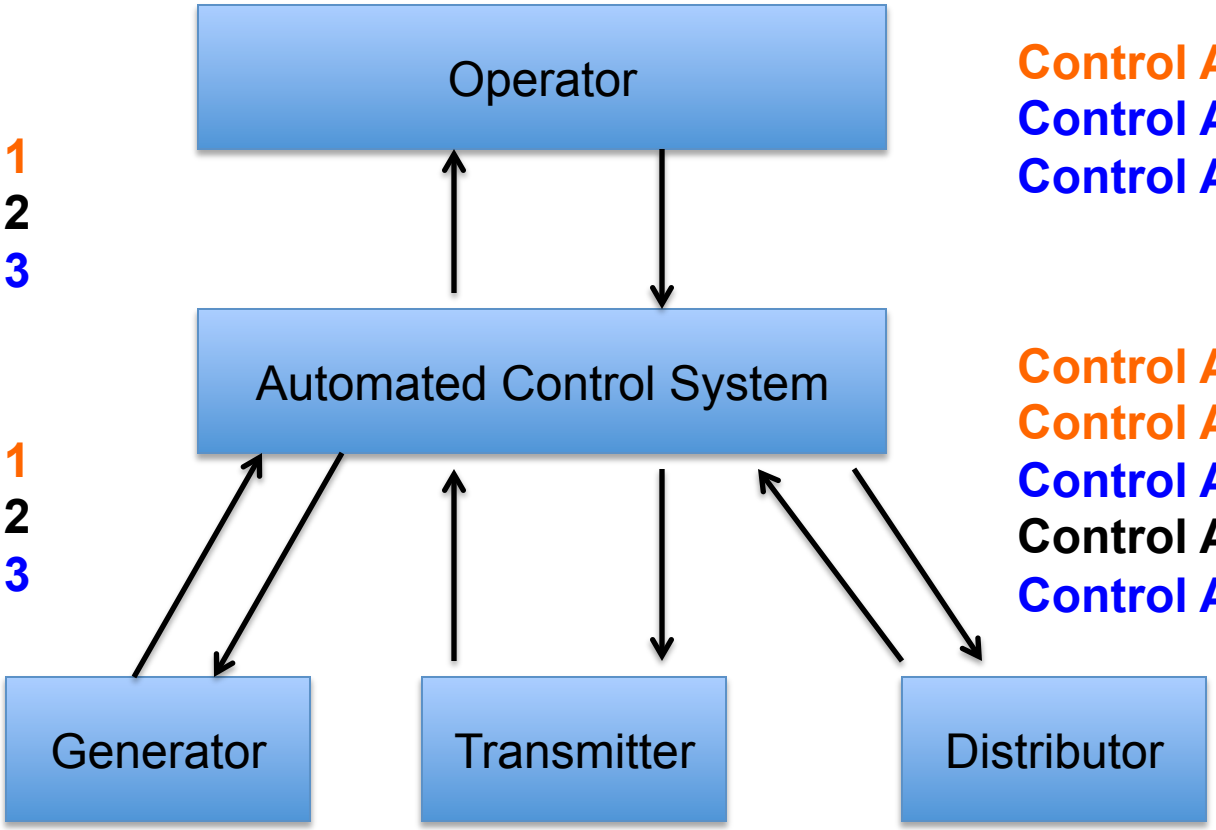
Build Functional Model Control Structure

- Identify Model Elements
- Identify each model element's responsibilities in carrying out each of the key activities necessary conduct the mission
- Identify Control Relationships
- Identify the Control Actions necessary for each element to execute their responsibilities
- Develop Process Model Description
- Identify Process Model Variables
- Identify Process Model Variable Values
- Identify Feedback providing PMV Values
- Check MFCSM for Completeness

Check the MFCSM for Completeness

- MFCSM should now be complete at the highest level
  - All Elements Identified
  - All Control Actions necessary to execute the activities
  - Process Models/Control Logic for all decisions required to execute the mission described at the start
  - All Feedback information necessary to deliver the PMV values required by PMVs
- Should be able to trace execution of each of the key activities at a high level on the FMCS
- Start at some sensible point on the model
  - What is the first thing that causes activity initiation?
  - Trace the feedback flow up and the control actions down.

Updating the MFCSM



Feedback 1
Feedback 2
Feedback 3

Control Action 1
Control Action 2
Control Action 3

Feedback 1
Feedback 2
Feedback 3

Control Action 4
Control Action 5
Control Action 6
Control Action 7
Control Action 8

*Perform In-Progress Review (IPR) 2

- Overview: Formal review with owner / stakeholder to validate that desired system functional requirements have been captured in the model
- May need to do this repeatedly as increased detail is required
- This may present an excellent opportunity to ensure that you have built a useful model that includes all key functions that must be assured against disruption

*Optional, But Recommended

STPA-Sec Big Picture Steps

- ✓ Establish the goal / purpose of the system
- ✓ Establish unacceptable losses for the system
- ✓ Establish the hazardous system states that place system at risk of suffering unacceptable losses
- ✓ Build Mission Functional Control Structure Model
- ⇨ Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

PHASE III: MODEL ANALYSIS & APPLICATION

PHASE III: Analyzing the Model

- Phase II developed the MFCSM
  - The MFCS Model is the control structure that assures the operation of the architectural model
- Phase III identifies how control actions given incorrectly, out of sequence, or missing can represent a hazard to the mission

Identify the Interactions that Give Rise to Hazards Using Modified Step 1 Table

hazard 1 (WORDS)							
Source (element) 1	Control Action 1	Missing creates Vul 1	Issuing under wrong context creates Vul 1	E/L	S/L	Control Loop	Required Restraints
	CA2						
	CA3						
Source 2	CA4						
	CA 5						

STPA-Sec Big Picture Steps

- ✓ Establish the goal / purpose of the system
- ✓ Establish unacceptable losses for the system
- ✓ Establish the hazardous system states that place system at risk of suffering unacceptable losses
- ✓ Build Mission Functional Control Structure Model
- ✓ Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- ⇨ Develop constraints to control these interactions
- Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

Develop Constraints to Prevent System from Entering Hazards States

- Based on developed understanding, identify a high-level functional constraint
  - This identifies a degree of control that must be present to prevent the losses previously identified
  - Limits how system can securely accomplish the mission
  - These constraints are actually high-level mission assurance requirements
- Each candidate architecture (even high level) must implement these requirements

Once the Required Constraints Have Been Determined, Candidate Architectures Can Be Evaluated Against Them or They Can Serve as Direct Input Into the Design Process

Specify the Required Functional Constraints (Initial Functional Security Requirements)

- Based on Vulnerabilities
- Identify necessary constraints on overall system function
- Examples
  - "Weapons must not be designated on areas containing non-combatants"
  - "Customer PII must not be disclosed to unauthorized individuals"
  - "Radiation must not be inadvertently released"

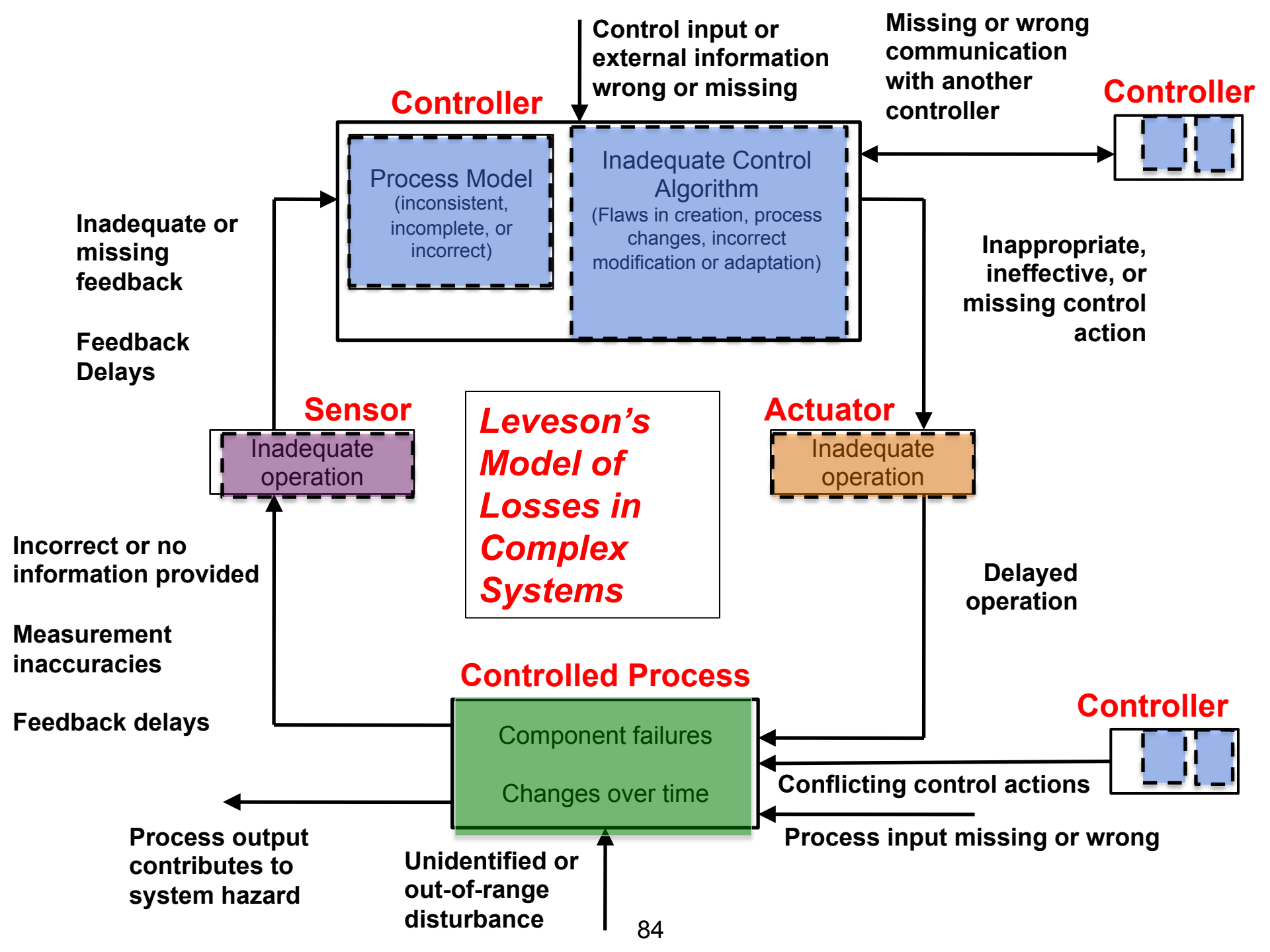
Note That We Haven't Talked About Technology Yet

STPA-Sec Big Picture Steps

- ✓ Establish the goal / purpose of the system
- ✓ Establish unacceptable losses for the system
- ✓ Establish the hazardous system states that place system at risk of suffering unacceptable losses
- ✓ Build Mission Functional Control Structure Model
- ✓ Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- ✓ Develop constraints to control these interactions
- → Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- Use insights to improve existing architecture
- Iterate

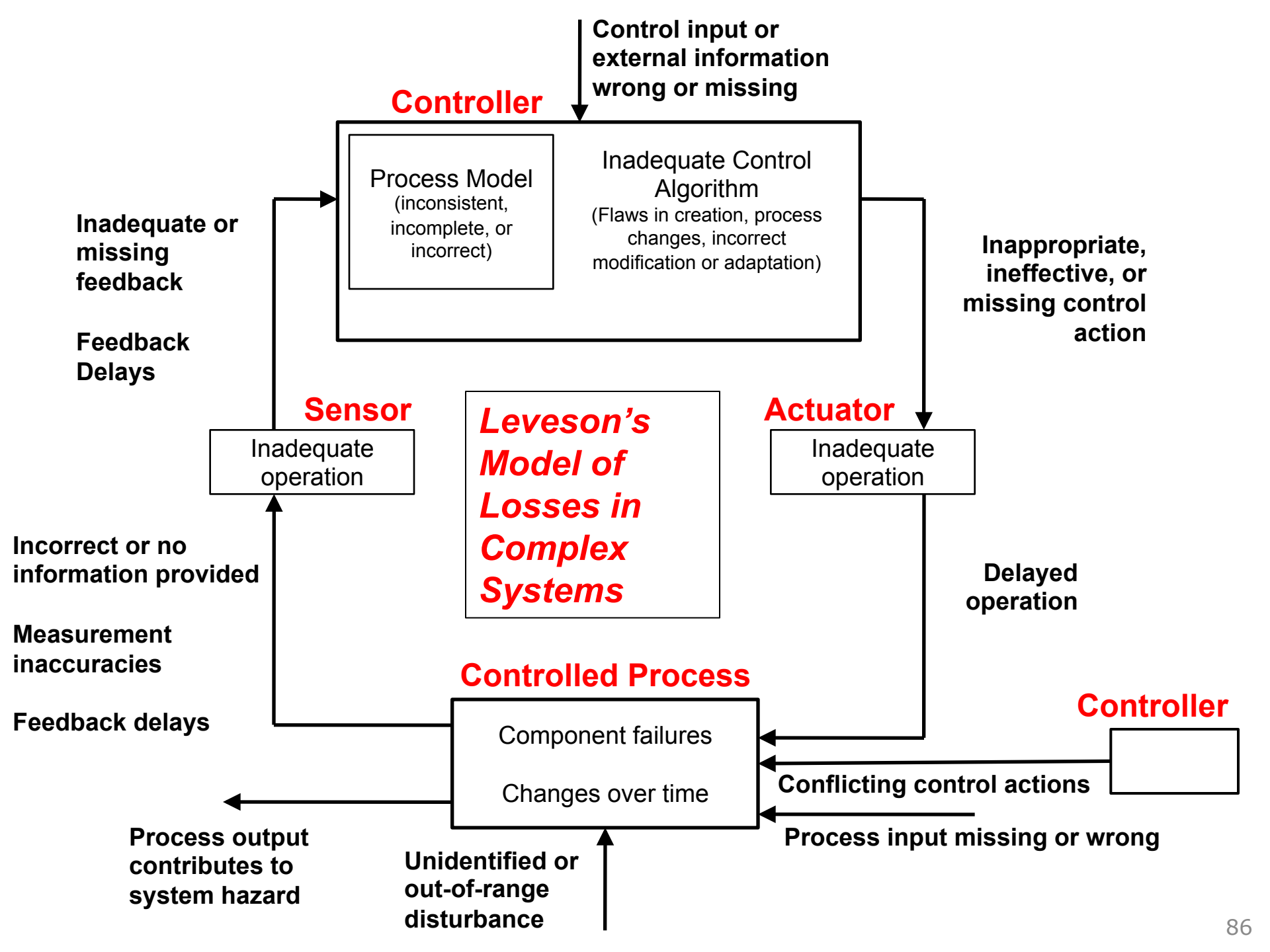
Identifying Causal Scenarios

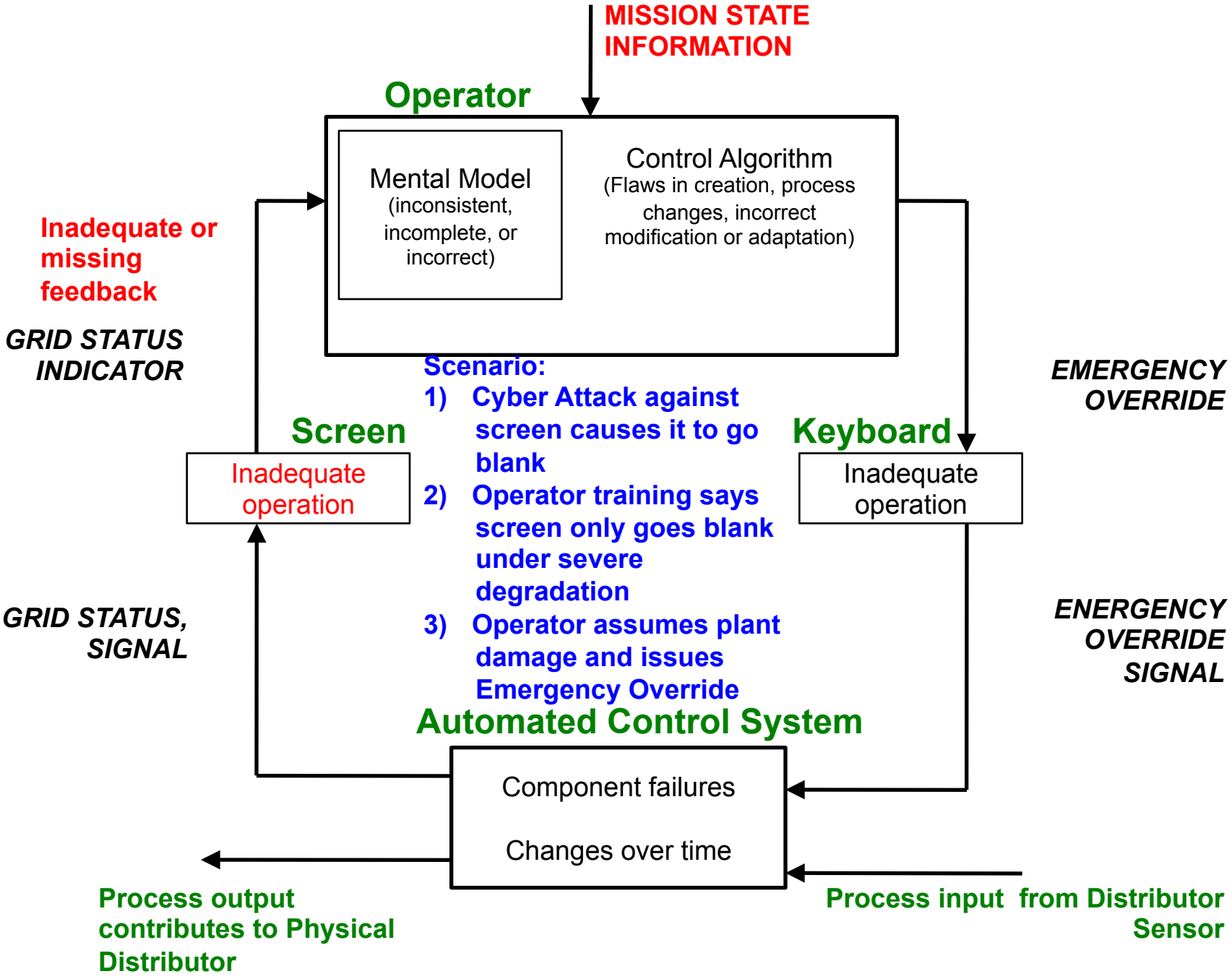
- Overview: Gain an understanding of the dependence of mission function on particular aspects of cyberspace to understand what is actually important
- For the Restraints Identified, go to particular control loop and change the generic STPA Step 2 Table into the specifics for the particular loop in the Control Structure
- Identify the restraint to be violated
- Discuss how this might occur
  - Note: This may well include the functional effects of threat activity (e.g. denial of required information).


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Process Model (inconsistent, incomplete, or incorrect)
Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
Inadequate or missing feedback
Feedback Delays
Inappropriate, ineffective, or missing control action
Sensor
Actuator
Inadequate operation
Inadequate operation
Leveson's Model of Losses in Complex Systems
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controlled Process
Component failures
Changes over time
Controller
Conflicting control actions
Process input missing or wrong
Process output contributes to system hazard
Unidentified or out-of-range disturbance

Perform Model Analysis

- Will evaluate each control action under various contexts
- EXPERT judgment and research necessary to answer question of whether or not the context leads to a potential violation of the high-level restraint
  - How/when could issuing a particular command lead to the hazard in the particular table?
  - Identify necessary restraints for those contexts deemed hazard
  - Identify the control loop that the CA resides as a part of


Control input or external information wrong or missing
Controller
Process Model (inconsistent, incomplete, or incorrect)
Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
Inadequate or missing feedback
Feedback Delays
Inappropriate, ineffective, or missing control action
Sensor
Inadequate operation
Leveson's Model of Losses in Complex Systems
Actuator
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controlled Process
Component failures
Changes over time
Controller
Conflicting control actions
Process input missing or wrong
Process output contributes to system hazard
Unidentified or out-of-range disturbance


MISSION STATE INFORMATION
Operator
Mental Model (inconsistent, incomplete, or incorrect)
Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
Inadequate or missing feedback
GRID STATUS INDICATOR
EMERGENCY OVERRIDE
Scenario:
1) Cyber Attack against screen causes it to go blank
2) Operator training says screen only goes blank under severe degradation
3) Operator assumes plant damage and issues Emergency Override
Screen
Keyboard
Inadequate operation
Inadequate operation
GRID STATUS, SIGNAL
ENERGENCY OVERRIDE SIGNAL
Automated Control System
Component failures
Changes over time
Process output contributes to Physical Distributor
Process input from Distributor Sensor

STPA-Sec Big Picture Steps

- ✓ Establish the goal / purpose of the system
- ✓ Establish unacceptable losses for the system
- ✓ Establish the hazardous system states that place system at risk of suffering unacceptable losses
- ✓ Build Mission Functional Control Structure Model
- ✓ Identify the interactions that give rise to the hazardous system states using modified Step 1 Table
- ✓ Develop constraints to control these interactions
- ✓ Identify scenarios to understand how constraints might be violated (given existing architecture) using Step 2 Table
- ⇨ Use insights to improve existing architecture
- Iterate

Use Insights to Improve Architecture

- Multi-Disciplinary Discussion
- Adjust architecture so that Hazards are eliminated if possible
- If not possible, then information should be passed on to designers
- Competing architectures can be evaluated on the basis of the insight gained
  - This has proven to be particularly useful in helping explain mission assurance problems associated with particular architectures under consideration

Real World Evaluation of STPA-Sec to Date

- Demonstrated ability to identify unknown vulnerabilities in a global mission
- Demonstrated ability to identify vulnerabilities in early system concept documents
- Demonstrated ability to improve ability of network defenders to identify and prioritize network assets based on mission assurance goals
  - Real mission, Real mission owner, Real network
  - Defenders able to more precisely identify what to defend & why (e.g. set of servers → integrity of a single file)
  - Defenders able to provide traceability allowing non-cyber experts to better understand mission impact of cyber disruptions

Lessons Learned Applying STPA-Sec

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

STPA-Sec is NOT a Silver Bullet, but Appears to Enable Increased Rigor "Left of Design"

Summary

- Key question: How to control vulnerabilities, not how to avoid threats
- Starts with system vulnerabilities and moves down to identify threats (top-down systems engineering approach) vs. starting with threats
- Elevates security problem from guarding network to higher-level problem of assuring overall function of enterprise.
- Includes managerial and social factors (entire socio-technical system)



Applying System-Theoretic Process Analysis for Security (STPA-SEC) to Support Mission Assurance and Security

William Young

PhD Candidate, Engineering Systems Division

Massachusetts Institute of Technology



BACKUPS

Hot Off the Presses: CNAS Cyber Security Recommendations

- Articulate a national security standard defining what it is imperative to protect in cyberspace
- Pursue a strategy that self-consciously sacrifices some cyber benefits in order to ensure greater security for key systems
- Recognize that some private-sector systems fall within the national security standard
- Use the model of voluntary reporting of near miss incidents in aviation to establish a data collection consortium that will illuminate the character and magnitude of cyber attacks against the U.S. private sector

Must Prioritize What Functions Are Most Important to Assure Against What Losses

Example: Stuxnet

- Loss: damage to reactor (in this case centrifuges)
- Hazard/Vulnerability: Centrifuges are damaged by spinning too fast
- Constraint: Centrifuges must never spin above maximum speed
- Hazardous control action: Issuing *increase speed* command when already spinning at maximum speed
- One potential causal scenario:
  - Incorrect process model: thinks spinning at less than maximum speed
    - Could be inadvertent or advertent
- One potential improvement:
  - Mechanical limiters, Analog RPM gauge

Strategy vs. Tactics

- Strategy vs. tactics
  - Cyber security often framed as battle between adversaries and defenders (tactics)
  - Requires correctly identifying attackers motives, capabilities, targeting
- Can reframe problem in terms of strategy
  - Identify and control system vulnerabilities (vs. reacting to potential threats)
  - Top-down vs. bottom-up tactics approach
  - Tactics tackled later