


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

William Young Jr, PhD

Reed Porada

2018 STAMP Conference
Boston, MA

March 26, 2018

Disclaimer:

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

Overview

- **Introduction (10 Mins)**
- **Observations on Cybersecurity today (10 Mins)**
- **System Thinking and Security (20 Mins)**
- **STPA-Sec overview (50 Mins)**
- **Practitioner Q & A (25 Mins)**
- **Summary and Conclusion (5 Mins)**

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

Introduction

Before We Start, Please Tell Me

- **Name**
- **Industry**
- **Experience level with STAMP/STPA/STPA-Sec**
- **What you hope to gain**

Introduction (1/2)

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

Today, Security is Viewed Almost Universally as a Threat Problem

Introduction (2/2)

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

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

Definitions (1/3)

Security (US Gov't, CNSSI 4009)--A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Cybersecurity (US Gov't & DoD)-- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyber Security is an Overarching Term that Covers Nearly Everything

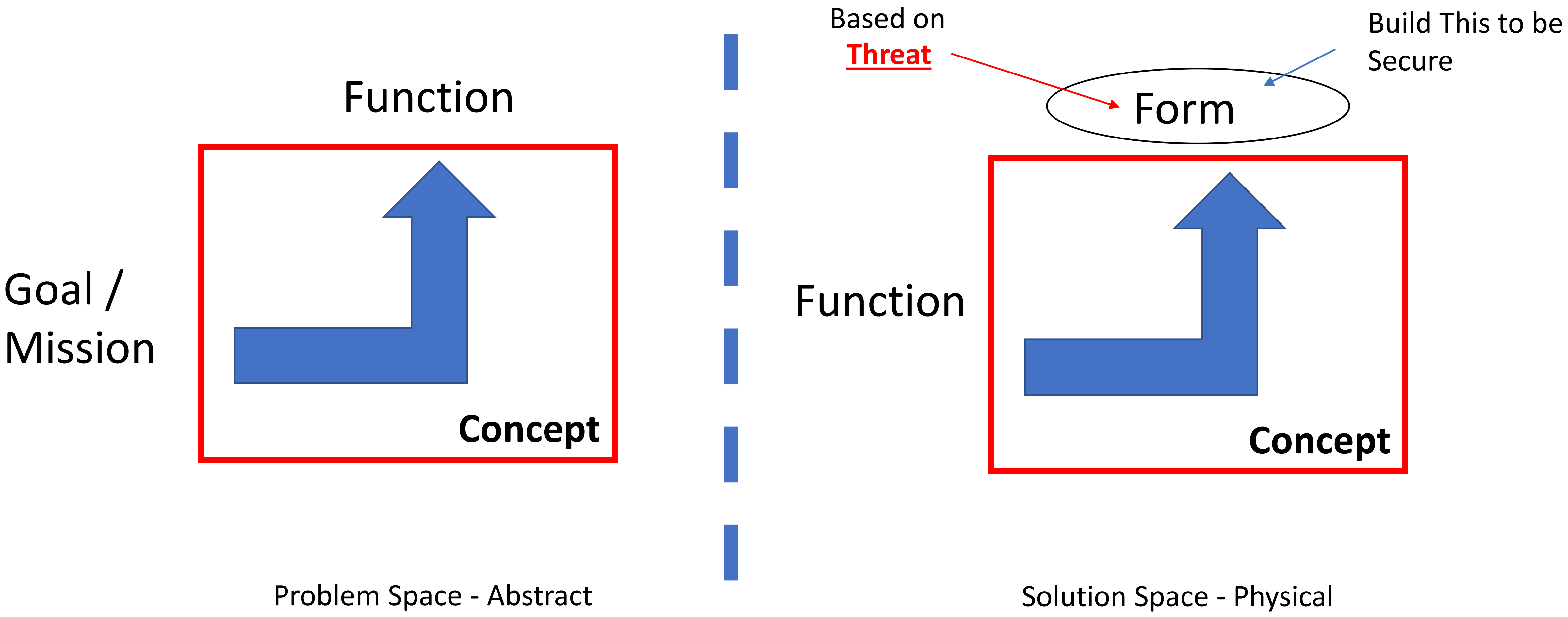
Definitions (2/3)

- **<u>Security Engineering</u>--"An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem" (US Federal Gov't)**
- **<u>Systems Security Engineering</u>—"a specialty discipline of systems engineering. It provides considerations for the security-oriented activities and tasks that produce security-oriented outcomes as part of every systems engineering process *activity* with focus given to the appropriate level of fidelity and rigor in analyses to achieve assurance and trustworthiness objectives. " (NIST SP 800-160)**

Definitions (3/3)

- **Mission (US Military Doctrine) – "The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore."**
- **Business / Mission Analysis (INCOSE) – "defining the problem domain, identifying major stakeholders, identifying environmental conditions and constraints that bound the solution domain…and developing the business requirements and validation criteria"**
- **Hazard (US Military Doctrine) --"A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation."**
- **Security Control (NIST)-- A safeguard or countermeasure prescribed for an information system or an organization designed to *protect* the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.**
- **Mission Activity System- "A notional purposive system which expresses some purposeful human activity (a mission)" (Adapted from Checkland, 1984)**

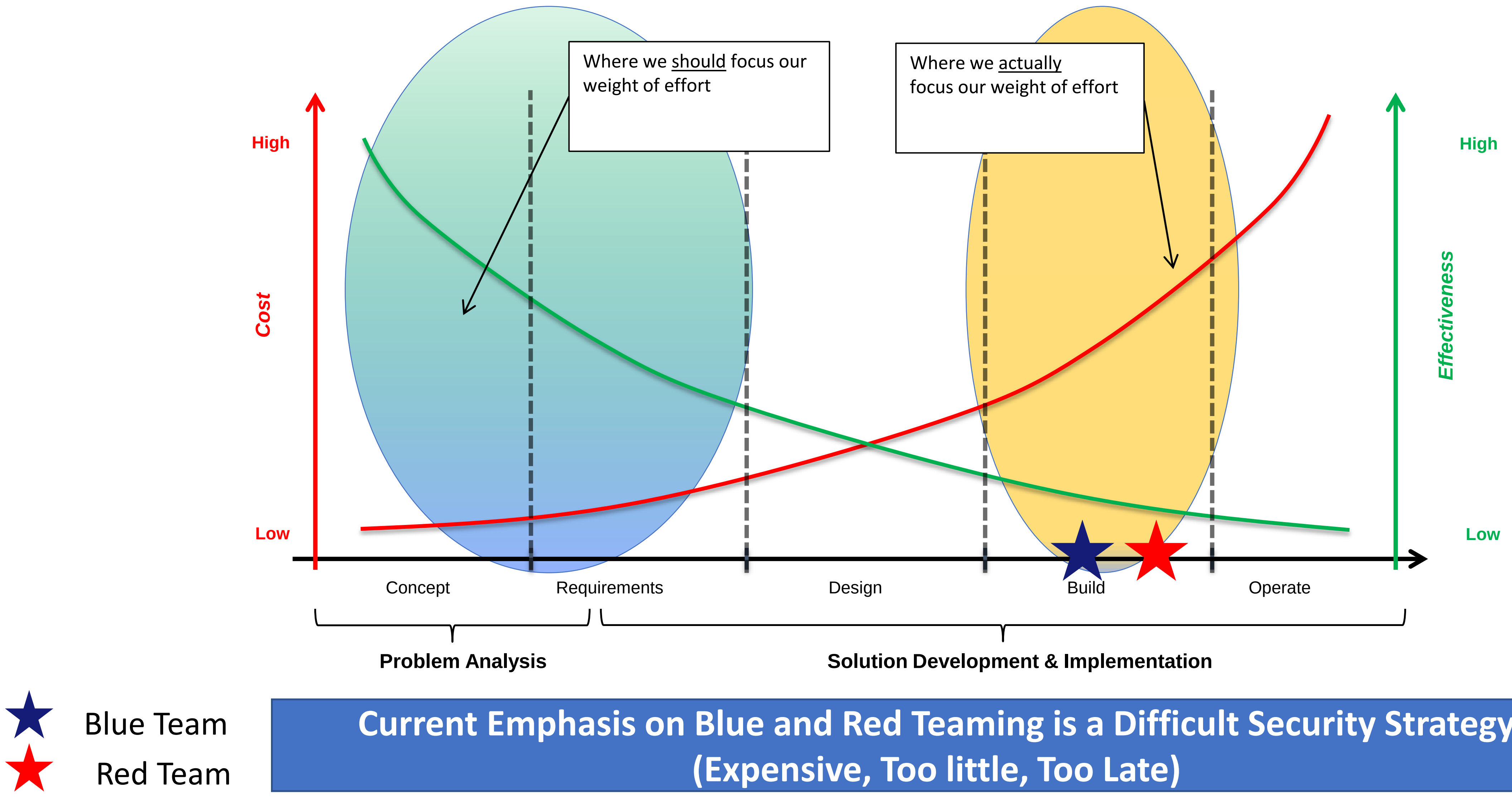
The Big Picture



Defining the Security Problem in Terms of Threats Limits Our Thinking (and Solutions)

Observations on Cybersecurity Today

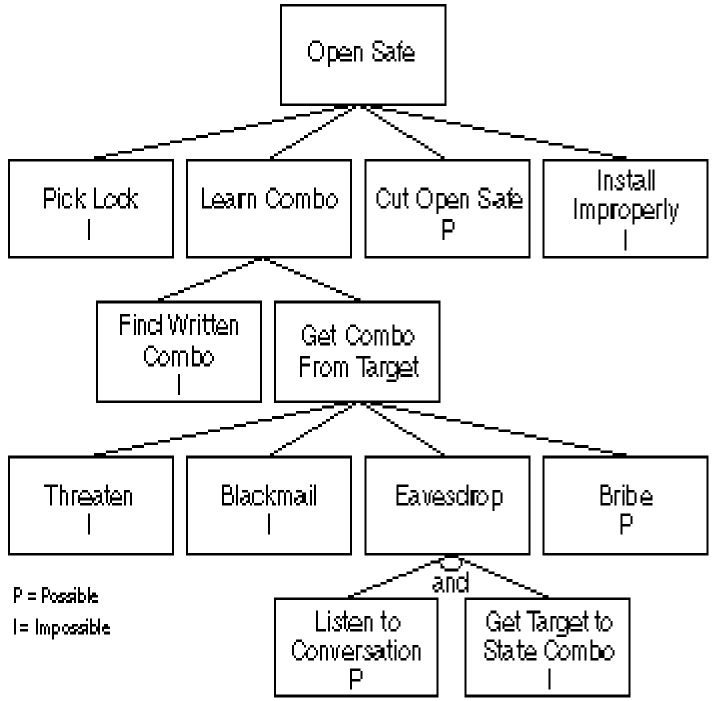
The Cybersecurity Pen-Testing Challenge



Current Emphasis on Blue and Red Teaming is a Difficult Security Strategy (Expensive, Too little, Too Late)

References: Boehm; Leveson; Frola & Miller; Fleming

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



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

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

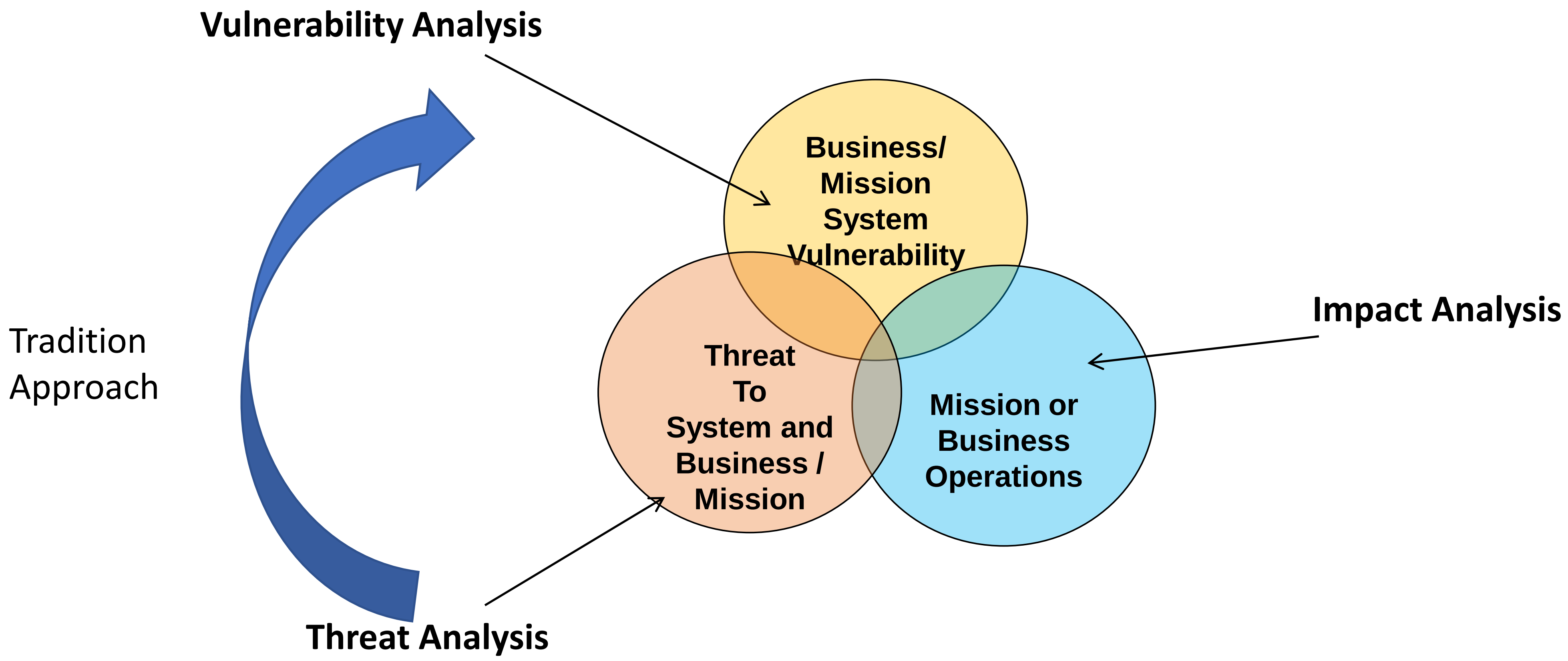
Current Security Analysis

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

- Prof Barry Horowitz, UVA

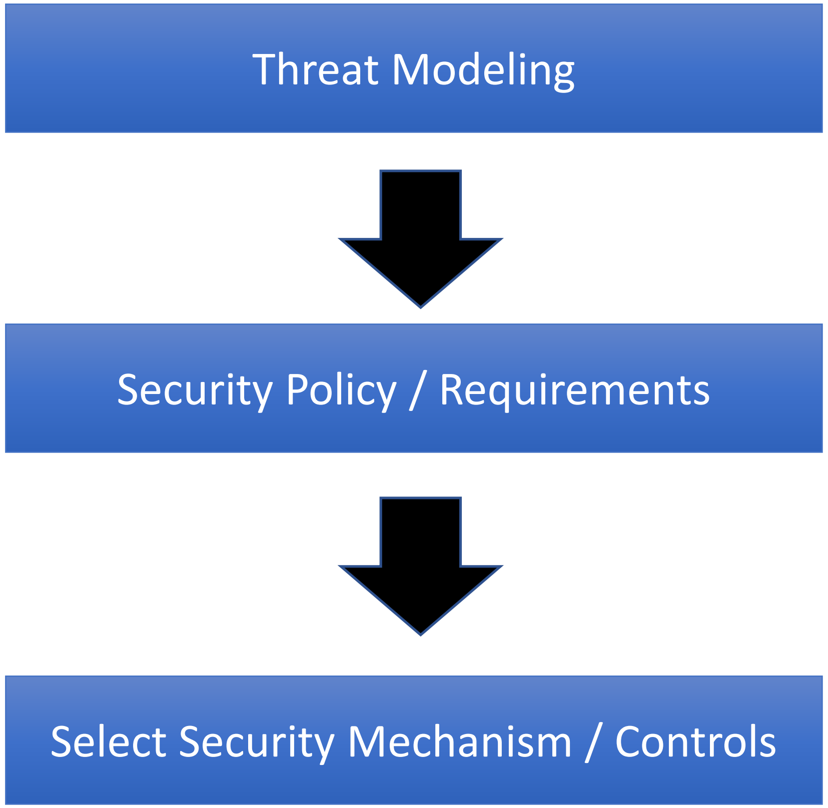
SYSTEM THINKING & SECURITY

Cybersecurity Through Today's Analytic Lenses



The System Vulnerabilities are Driven by Threat Capability

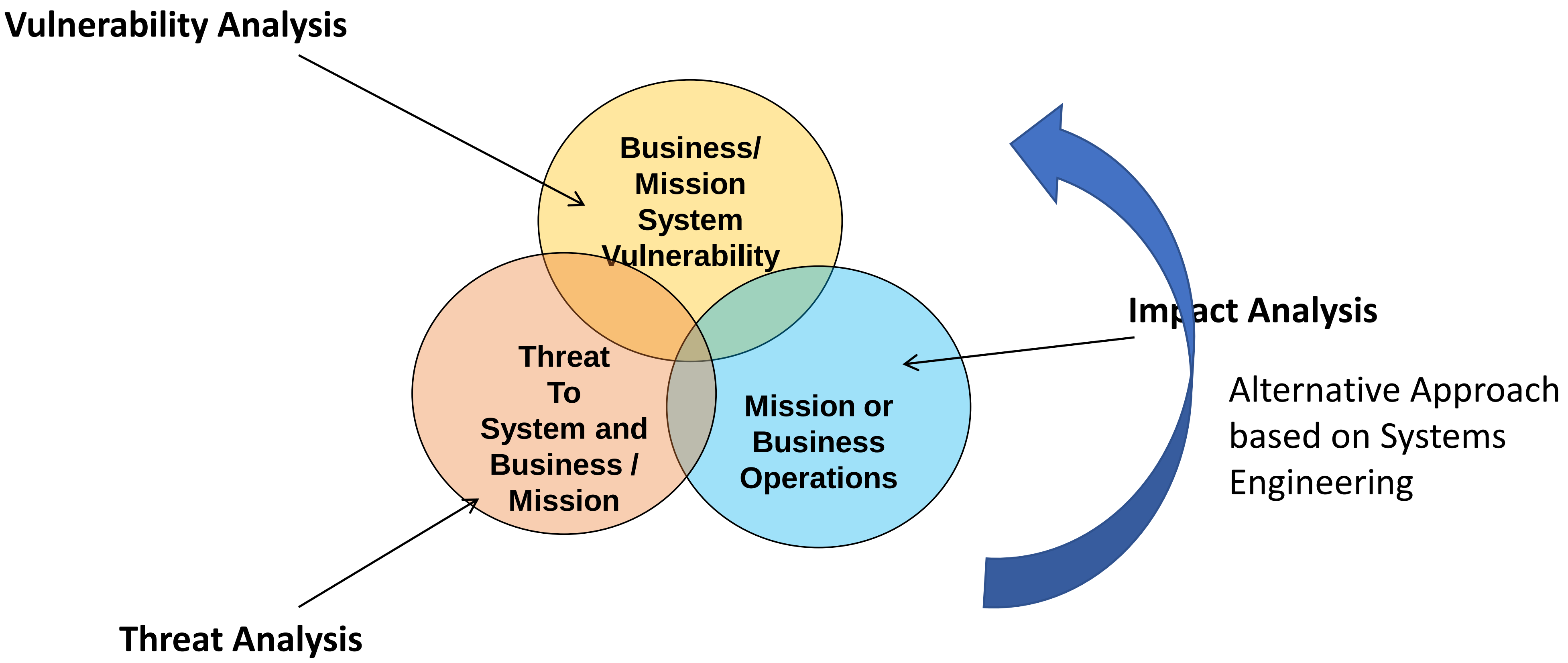
Threat Based Approach to Developing a Secure Architecture



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

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

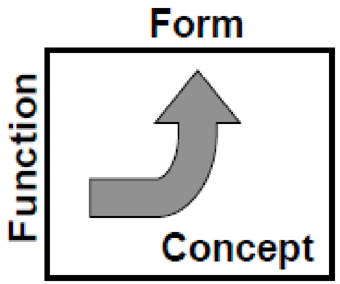
Cyber Security Through Different Analytic Lenses



In Systems Engineering, Threats are Just One of Many Trades

New Approach: Secure Form Simply Realizes Secure Function

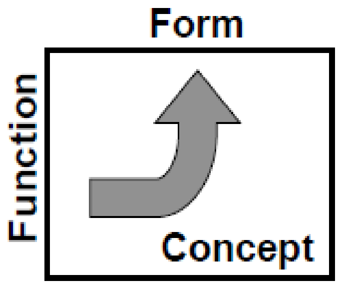
- "Form follows function" is a central tenant of system engineering and architecture
- Generate secure Business & Mission Systems by first defining the secure functionality to be realized
- Get to security via
    - Identify functionality required to solve the problem at hand (But we must understand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



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

New Approach: Secure Form Simply Realizes Secure Function

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



We Require a Model to Help Craft the Security Concept

STAMP Model & Security

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

STPA-Sec

- **STAMP model allows us to create an analysis process to generate a security concept**
- **We want to examine a functional process for security to gain insights and craft a novel artifact or set of artifacts to realize our goal**
- **Threats are just another environmental hindrance to function**
  - **In fact, the threats themselves don’t really matter…it’s the functional disruption they can deliver**
  - **We can engineer our systems to handle the most important functional disruptions**

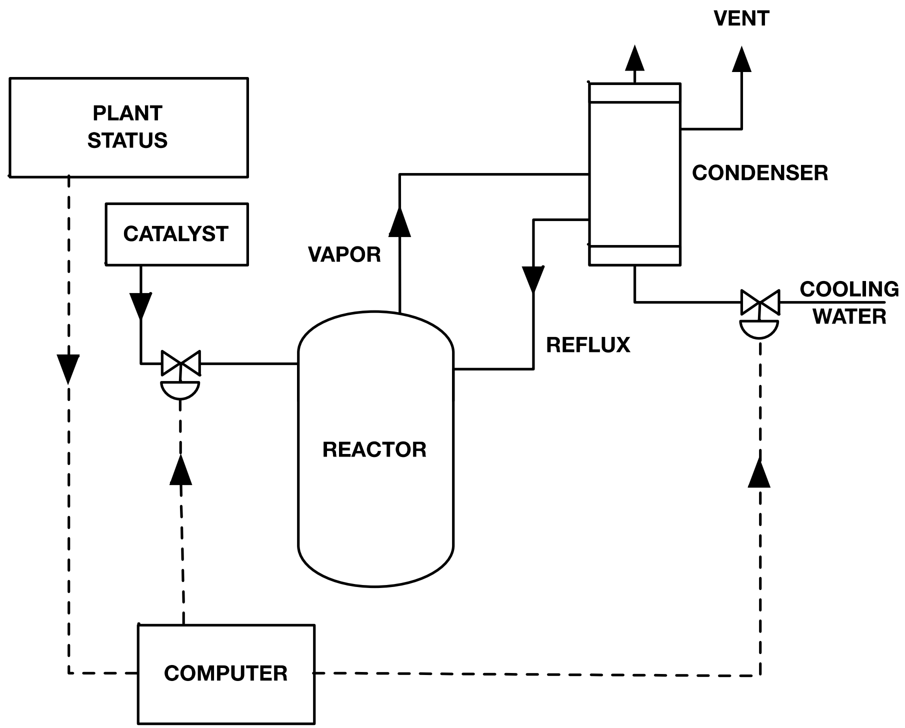
STPA-Sec For Security Engineering Analysis

Chemical Reactor Example Based on John Thomas Example Used in Earlier STPA Tutorial. Example is Used With Dr Thomas' Permission.

Chemical Reactor Design Through a Security Lens

From John Thomas' Example this Morning

- **Toxic catalyst flows into reactor**
- **Chemical reaction creates heat, pressure**
- **Water and condenser provide cooling**

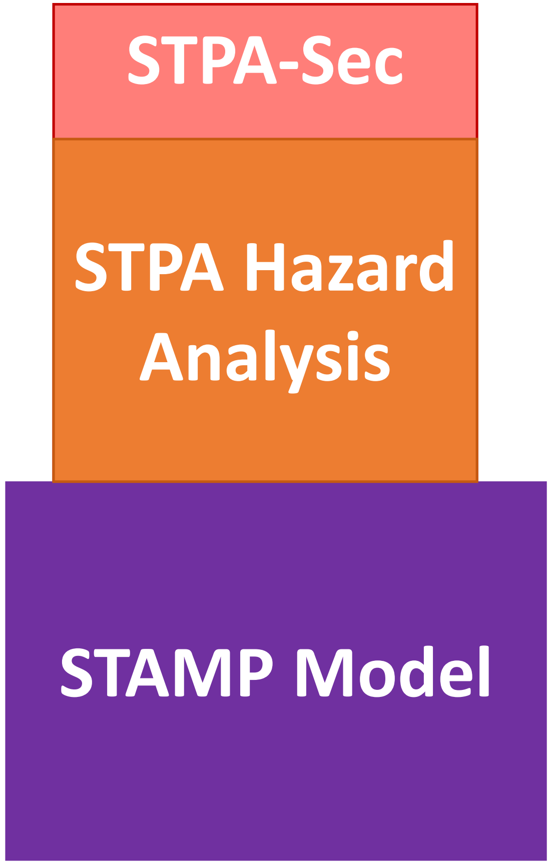


Additional Factors

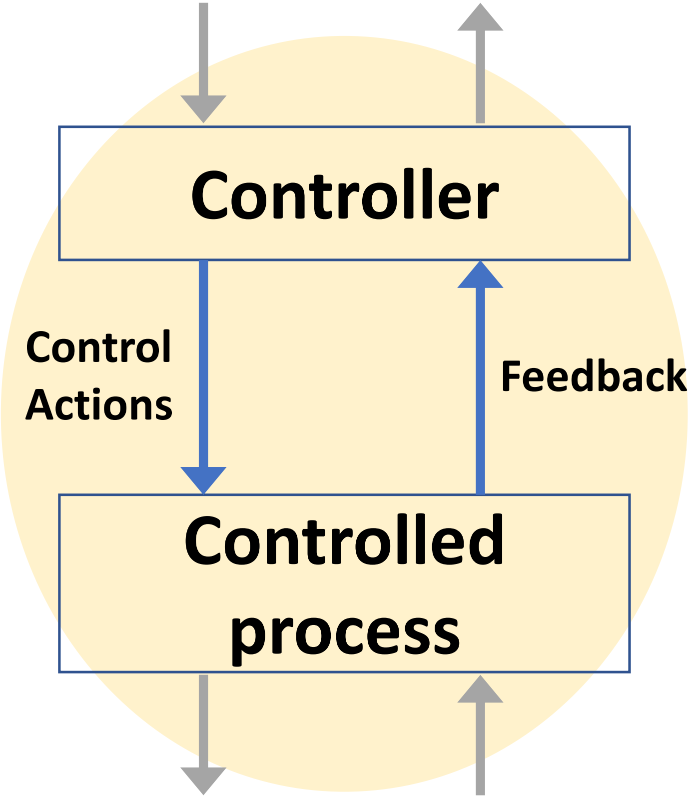
- **Plant is expected to be the primary source of local jobs**
- **Company is expected to employ proprietary technology**
- **Plant is expected to be the company's crown jewel and has received a great deal of press attention**

Adapted from Dr Thomas' STPA Tutorial

STPA-Sec Extends STPA



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



Security-related material or techniques

Synthesize (Frame) the Security Problem: Answering the “Why” Question

Big Picture: Synthesize (Frame) Security Problem

- **Purpose is to set the foundation for the security analysis**
- **Must uncover / elicit unknown concerns**
- **Must ID all relevant stakeholders**
- **Must understand how product / service fits into organizational strategy**
- **Surface key assumptions**
- **Includes key aspects of Business or Mission Analysis (BMA) in ISO/IEEE/IEC 15288**

Best Tactics and Tools Cannot Overcome a Flawed Strategy

The Maginot Line Remains an Incredible Engineered System, But Failed Operationally (Perfectly Solved the Wrong Problem)

Cybersecurity is a Wicked Problem

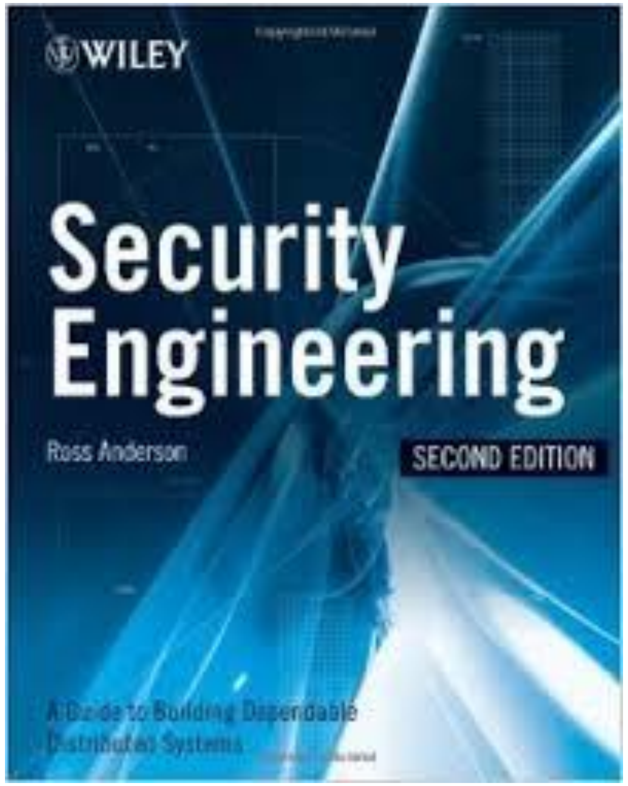
By now we are all beginning to realize that one of the most intractable problems is that of defining problems (of knowing what distinguishes an observed condition from a desired condition) and of locating problems (finding where in the complex causal networks the trouble really lies). In turn, and equally 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

Formulating (Framing) a Wicked Problem is the Problem!

The Security Problem is Not Generally Obvious or Easy to Specify

- **Determining life cycle security concepts**
- **Defining security objectives**
- **Defining 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”



It is impossible to Develop Solutions to A Problem We Do Not Understand

Define Purpose and Goal

"A system to do {What = Purpose}

by means of {How = Method}

in order to contribute to {Why = Goals}

while {constraints, restraints}

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

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

Sidebar

The Story of "Bob"

What Might Be an Example from the Plant Example?

Define System Purpose and Goal

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

- **Toxic catalyst flows into reactor**
- **Chemical reaction creates heat, pressure**
- **Water and condenser provide cooling**

<u>Additional Factors</u>

- **Plant is expected to be the primary source of local jobs**
- **Company is expected to employ proprietary technology**
- **Plant is expected to be the company's crown jewel and has received a great deal of press attention**

<u>Format</u>

"A system to do {What = Purpose}
by means of {How = Method}
in order to contribute to {Why = Goals}
while {constraints, restraints}

What Might Be an Example from the Plant Example?

Chemical Reactor – Potential Solution

A system to **contain and process chemicals**

by means of **transferring, mixing, and cooling chemicals**

in order contribute to **production of chemicals sold by the company** while **maintaining and improving the company's position and branding as a responsible community partner and world leader in technology .**

This is one Solution, But are There Others Based Upon Looking at the Plant Through other Stakeholders' lenses?

Adapted from Dr Thomas' STPA Tutorial

Define Purpose of the Analysis

Security Perspective on Defining the Purpose of the Analysis

- **The purpose of the analysis draws upon the insights generated through the problem framing**
- **Need to include security related losses and hazards**
- **Need to examine other required functionality from a security perspective**

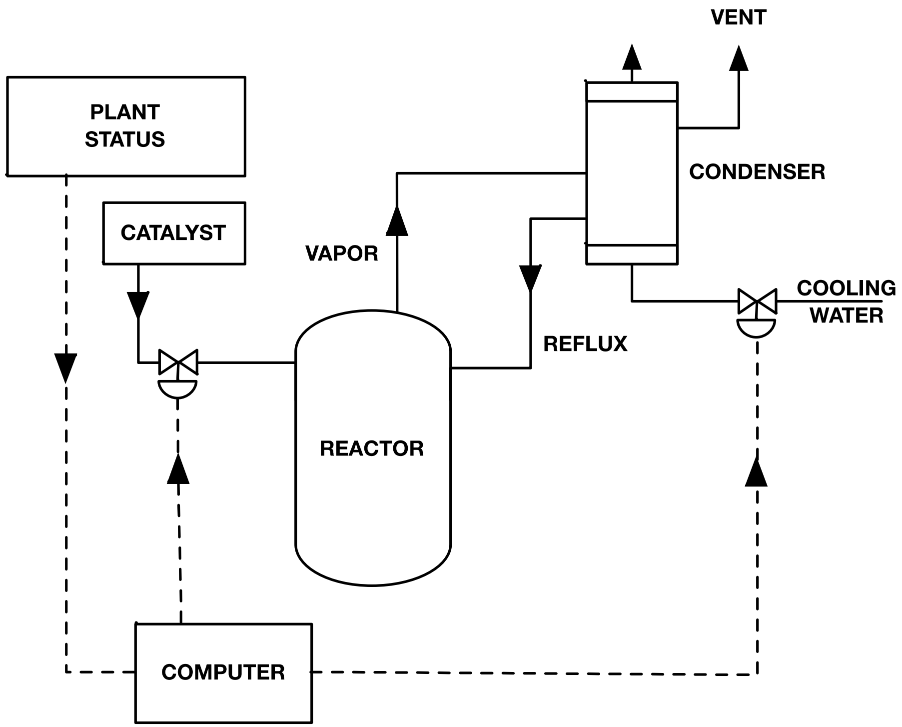
Adding Security Related Losses

- **Many of the losses will overlap with safety**
- **Security perspective may add nuance to a previous safety perspective**
- **Security perspective may also highlight an important safety / security trade**
- **Focus on alternative “system” uses**
- **Focus on security concerns of other stakeholders**

Simply Gaining Clarification on Unacceptable Losses May Provide a Significant Gain in Security Effectiveness!

Chemical Reactor - Losses

- **Unacceptable Losses (From Earlier Today)**
- L-1: People die or become injured
- L-2: Production loss

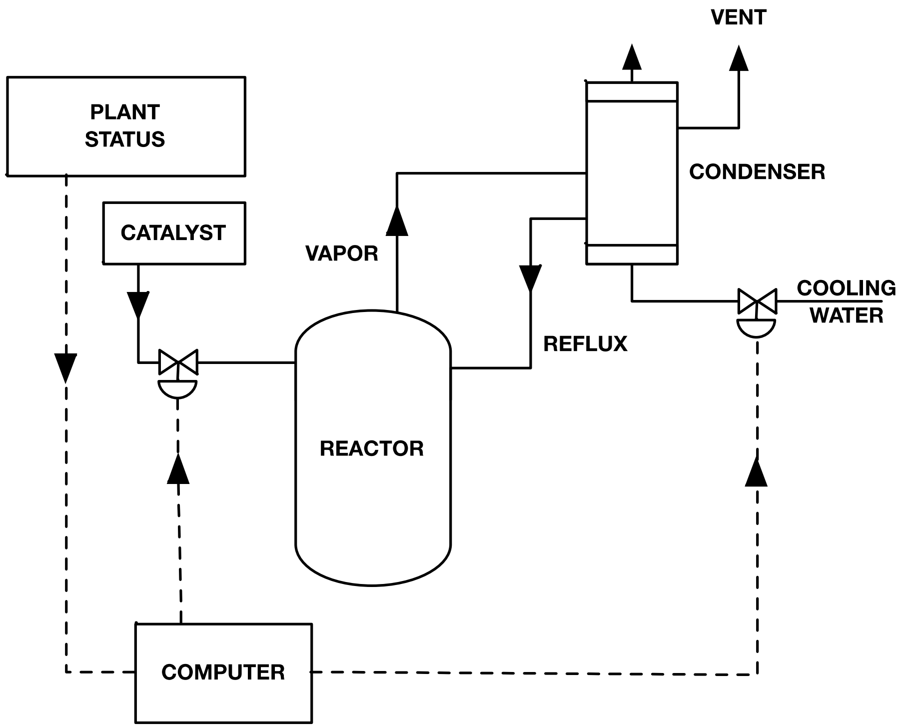


Are there other unacceptable losses Related to Security?

Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor - Losses

- **Unacceptable Losses**
- L-1: People die or become injured
- L-2: Production loss
- **L-3: Loss of Reputation**
- **L-4: Loss of Intellectual Property**

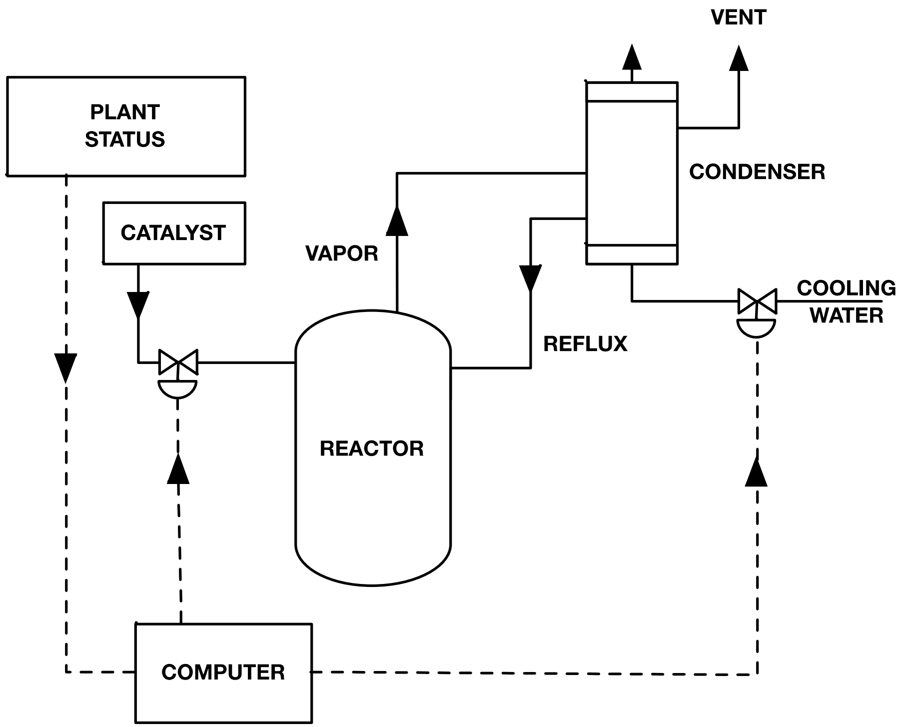


Are these Distinct, Security-Related Losses?

Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor - Losses

- **Unacceptable Losses**
- L-1: People die or become injured
- L-2: Production loss
- L-3: Loss of Reputation
- L-4: Loss of Intellectual Property



Are There Strategic Actions We Might Want to Take that Could Improve Our Ability to Prevent These Losses?

Adapted from Dr Thomas' STPA Tutorial

Thinking Broadly About Loss Mechanisms

Stakeholders	Stake or Value	Associated Loss
S&T Division	Developed proprietary algorithm implementing new chemical mixing scheme.	Financial loss if competitors become aware of the new mixing scheme and apply it before patent issued or apply it undetected after patent is issued

How Might We Think Differently About How We Implement the "Mixing" Function in the Plant to Prevent the Associated Loss?

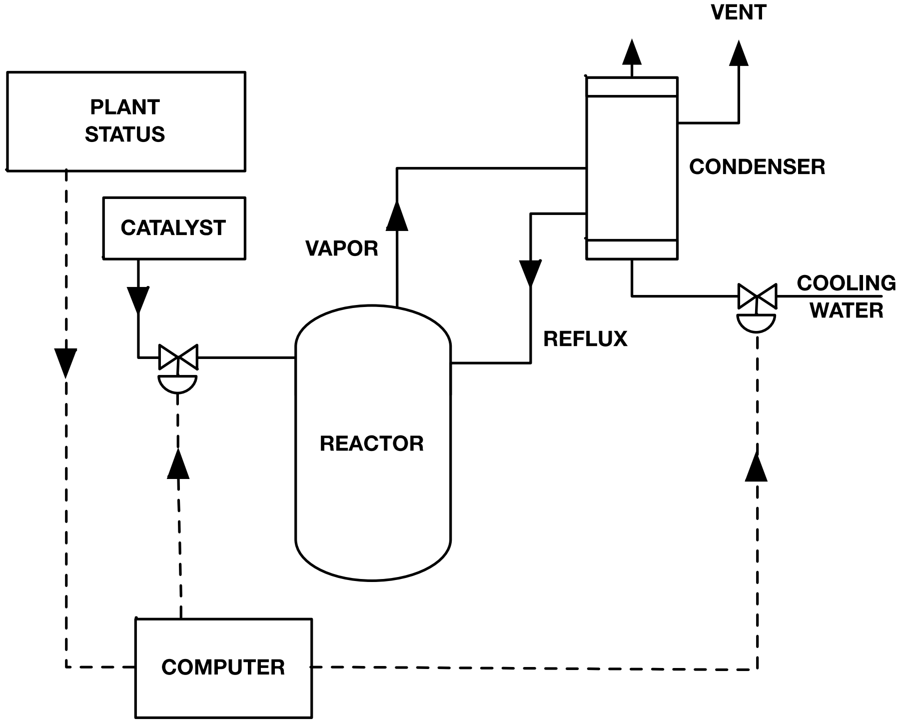
Thinking Broadly About Loss Mechanisms

Stakeholders	Stake or Value	Associated Loss
S&T Division	Developed proprietary algorithm implementing new chemical mixing scheme.	Financial loss if competitors become aware of the new mixing scheme and apply it before patent issued or apply it undetected after patent is issued

We are Beginning to Define our Business/Mission Related Tactical Context for Confidentiality but Effective Security Strategy Extends Beyond IT Security Professionals

Chemical Reactor - Hazards

Hazard	Description	Worst Case Environment	Associated Losses
H1: Plant releases toxic chemicals			
H2: Plant is unable to produce chemical			

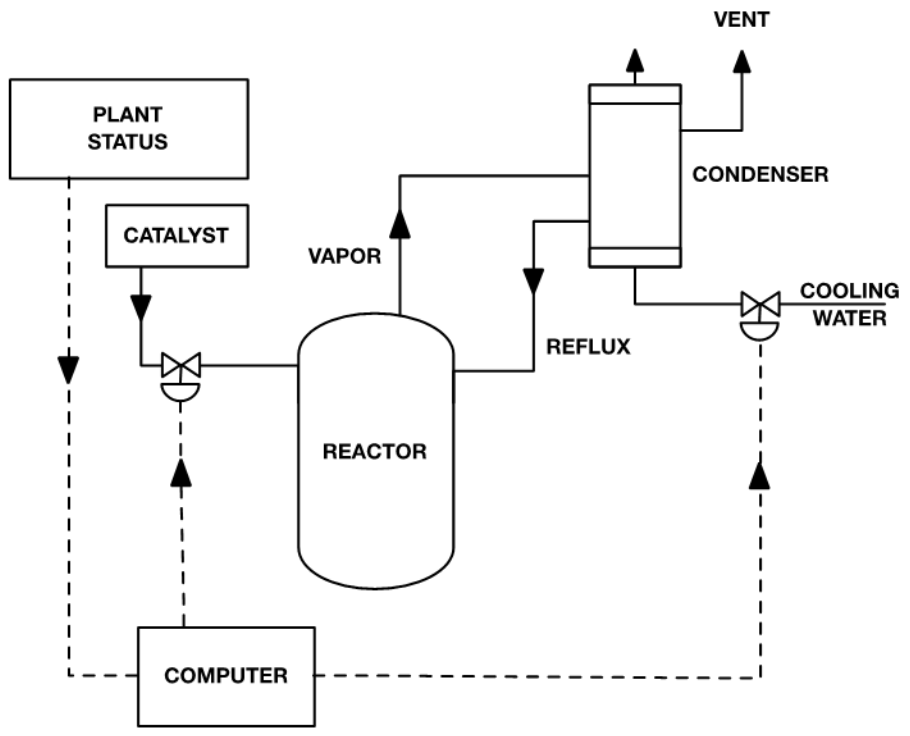


What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss?

Adapted from Dr Thomas' STPA Tutorial

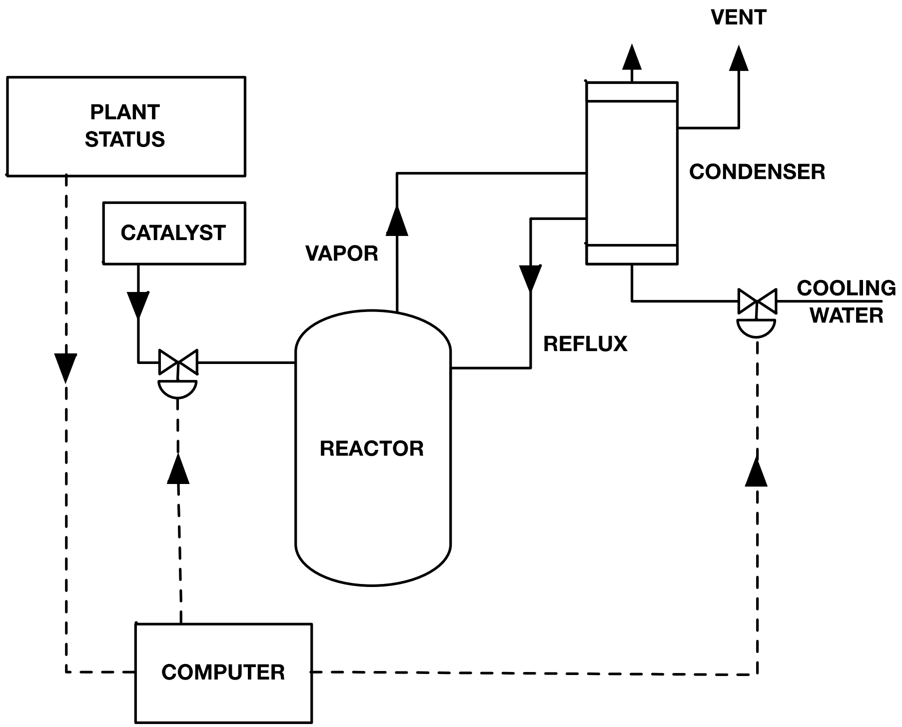
Using Verbs to Help Identify System Level Hazards

Loss	Transfer	Cool	Mix
L1: Death or Injury	Transferring lethal chemicals into the environment inadvertently	Cooling insufficient to maintain safe operating conditions	Mixing the wrong chemicals
L2: Production Loss		Cooling insufficient to maintain operating limits for equipment	Exceeding operating conditions in the mixer might lead to equipment damage



Chemical Reactor - Constraints

Hazard	Safety Constraint
H1: Chemicals inadvertently released	C1:
H2: ??	

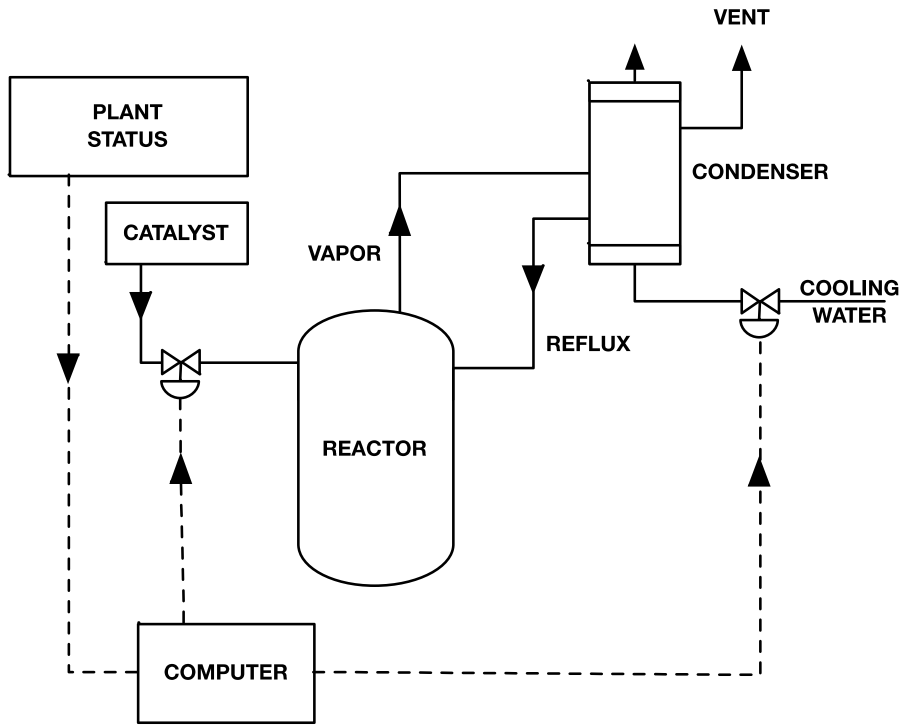


What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss?

Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor - Constraints

Hazard	Safety Constraint
H1: Chemicals in air or ground after release from plant	Chemicals must never be released inadvertently from plant
H2: ??	



What are the system constraints?

Adapted from Dr Thomas' STPA Tutorial

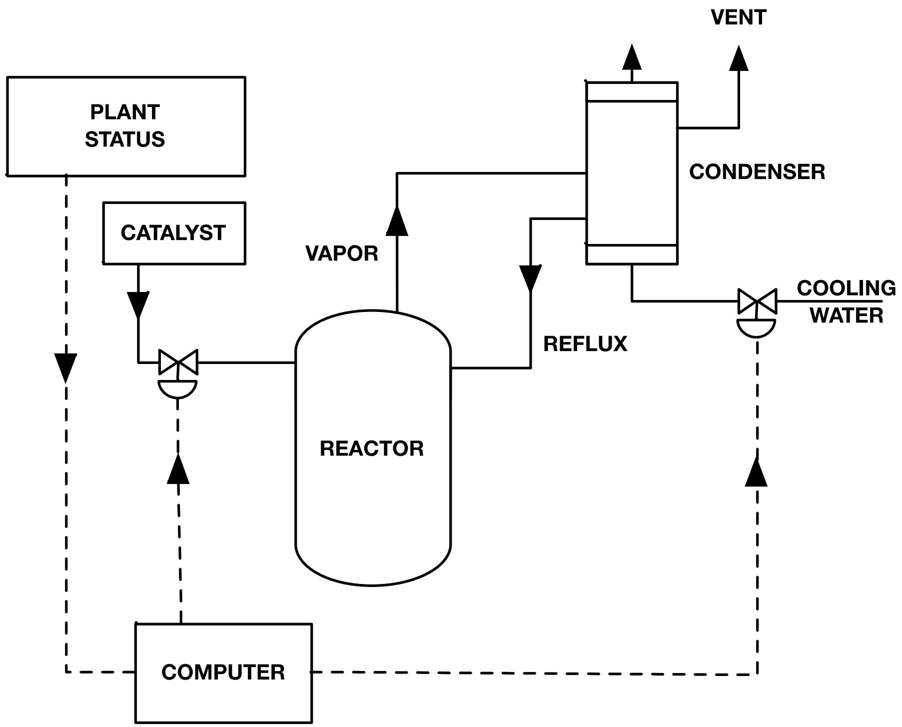
Model the Control Structure

Chemical Reactor – Control Structure

A system to **contain and process chemicals**

by means of **transferring, mixing, and cooling chemicals**

in order contribute to **production of chemicals sold by the company.**

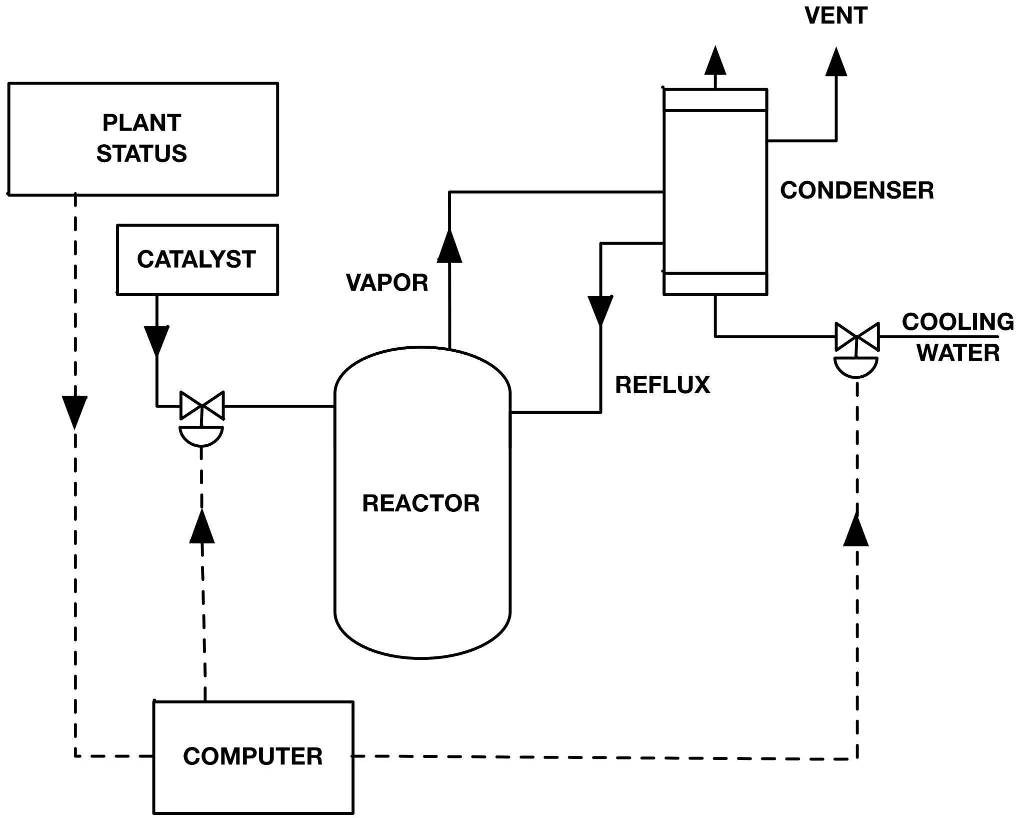


- **What Processes Must Be Controlled in Order to Accomplish Business or Mission Objective**
  - **Transfer and mixing catalyst**
  - **Cooling reflux**
- **Use Insights to understand Controller requirements**

Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor – Control Structure

Need Functional Equivalent



Adapted from Dr Thomas' STPA Tutorial

Functional Control Structure

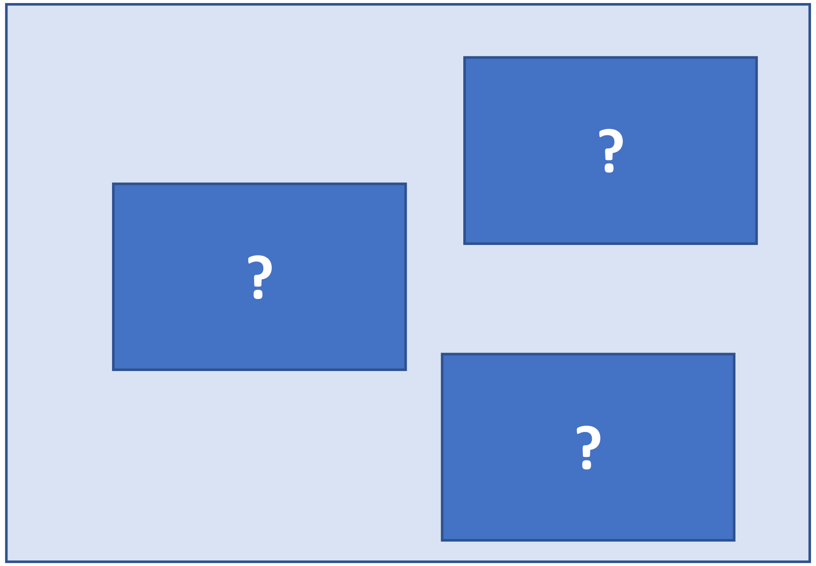
1. **Identify *Model Elements***
2. **Identify each *Model Element's* responsibilities in carrying out each of the key activities necessary conduct the mission**
3. **Identify *Control Relationships***
4. **Identify the *Control Actions* necessary for each element to execute their responsibilities**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

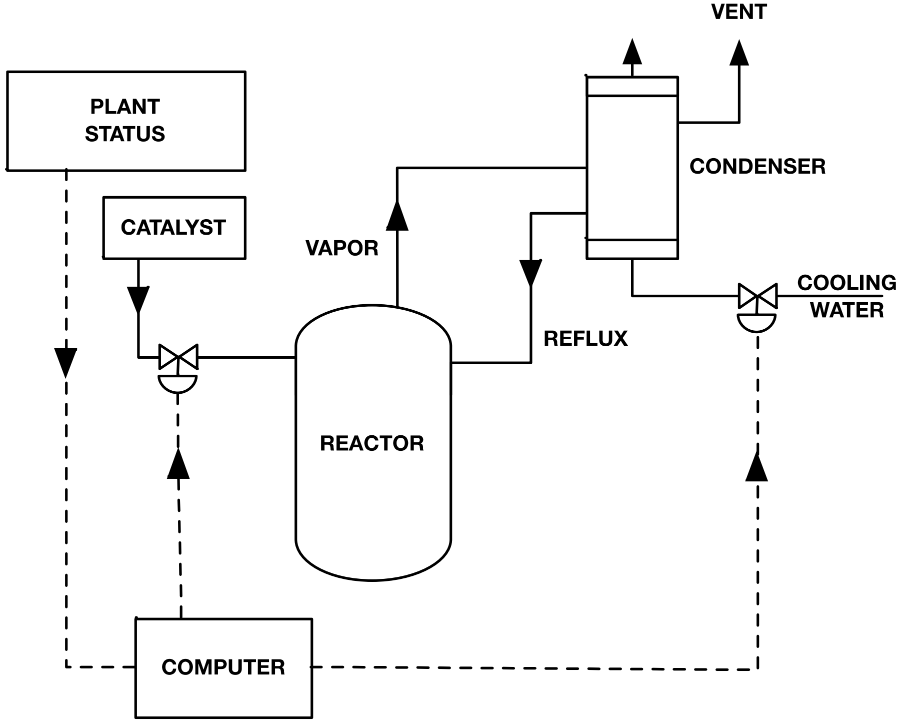
Chemical Reactor – Control Structure

A system to **contain and process chemicals**

by means of **transferring, mixing, and cooling chemicals**

in order contribute to **production of chemicals sold by the company.**





Adapted from Dr Thomas' STPA Tutorial

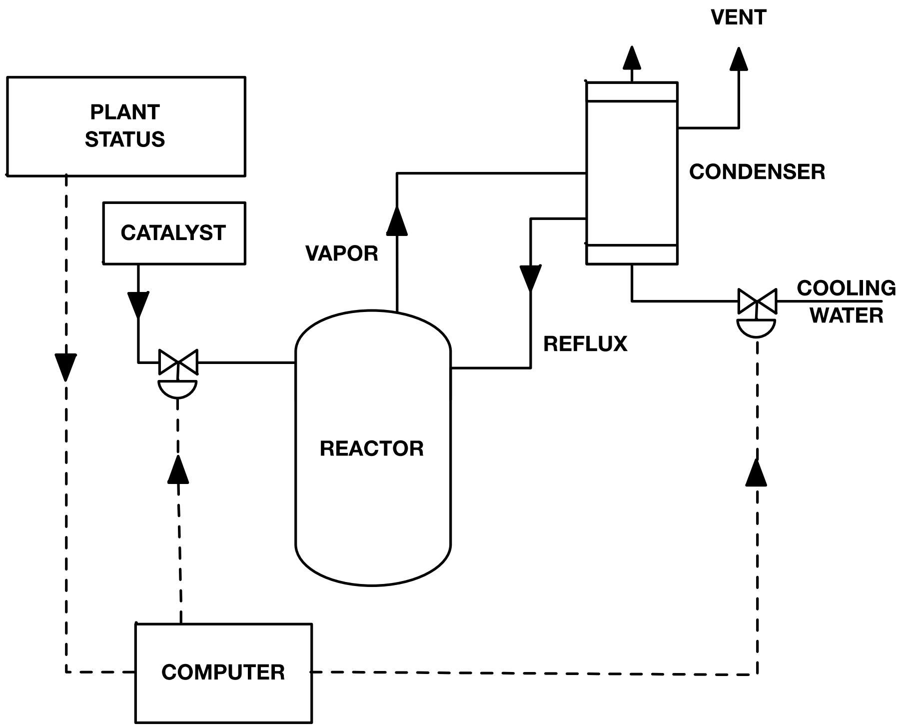
Chemical Reactor – Control Structure

A system to **contain and process chemicals**

by means of **transferring, mixing, and cooling chemicals**

in order contribute to **production of chemicals sold by the company.**

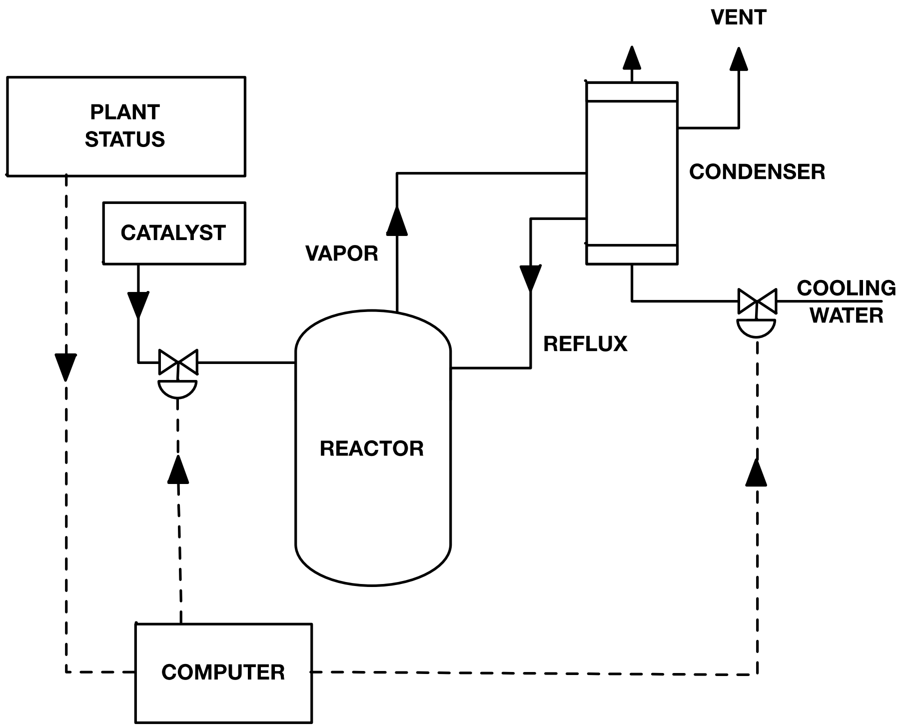
High-Level Functional Activity	Model Elements	Description



Adapted from Dr Thomas' STPA Tutorial

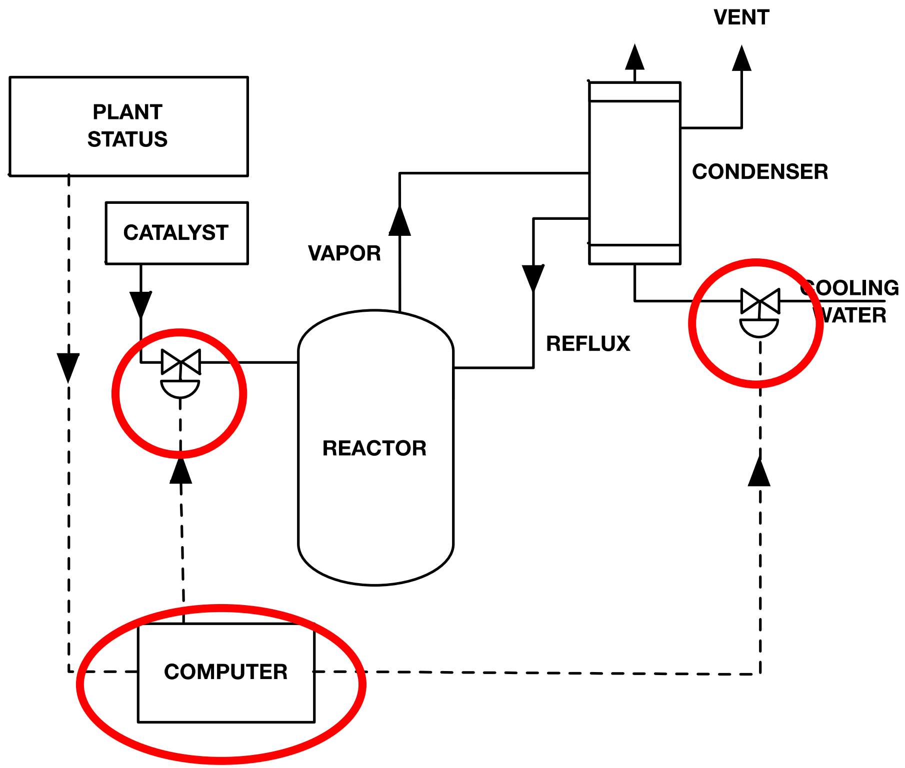
Chemical Reactor – Control Structure

High-Level Functional Activity	Model Elements	Description
Transfer	Operator, Computer, Valves	
Mix	Operator, Computer, Valves, Reactor	
Cool	Operator, Computer, Valves, Condenser	



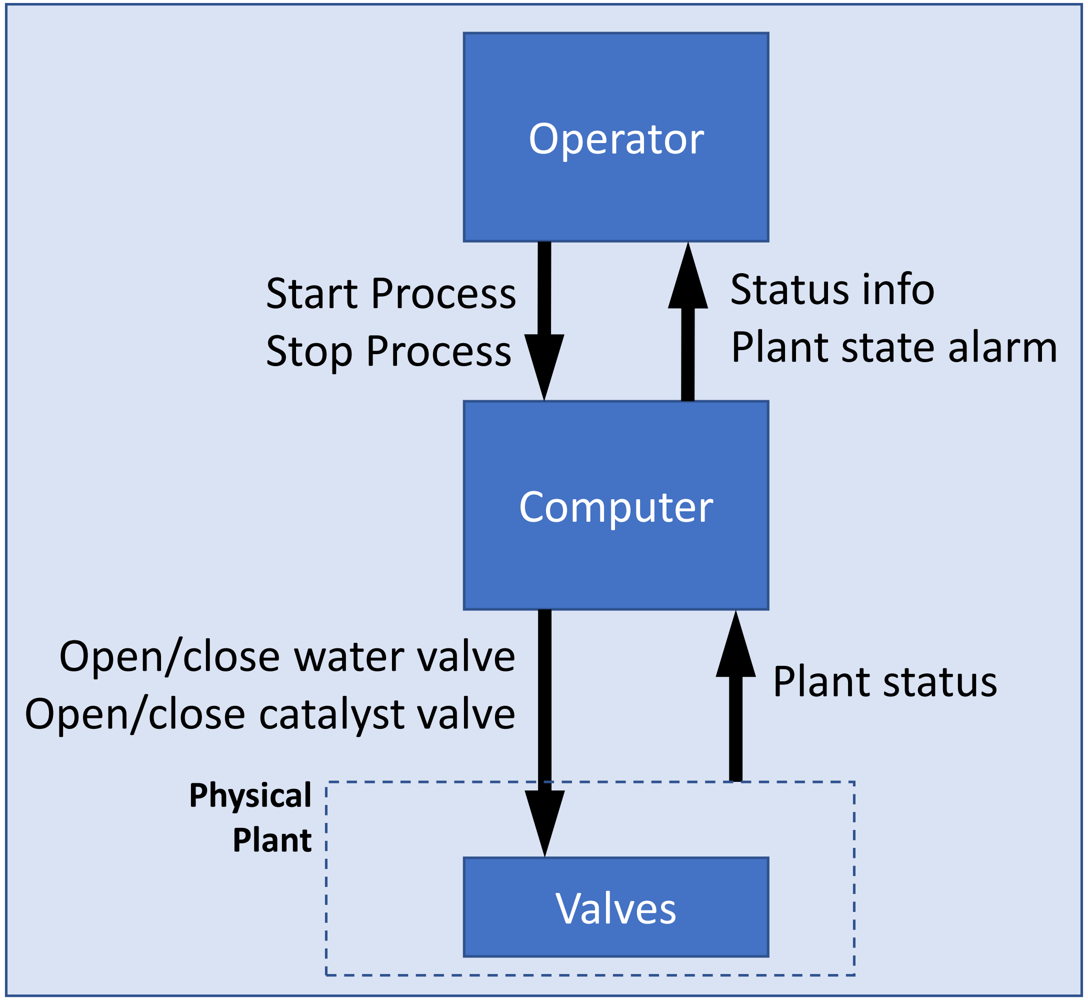
Chemical Reactor – Control Structure

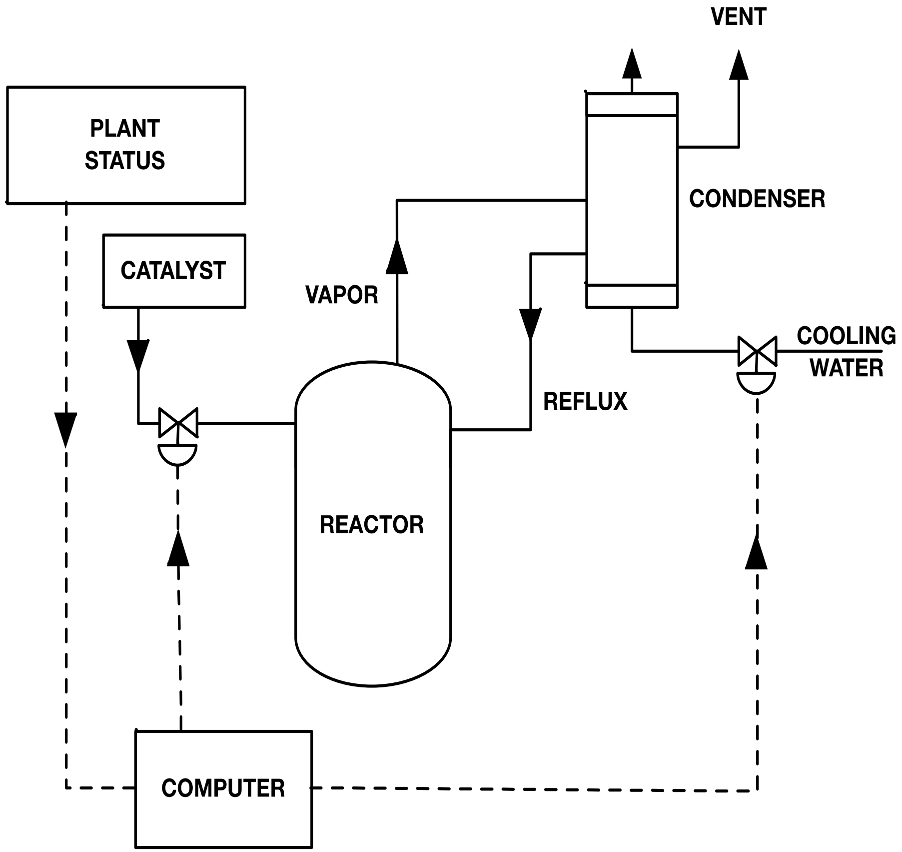
Key Activity: Transfer	
Element	**Responsibility Description**
Operator	• Initiate process • Monitor progress • Manually Intervene
Computer	• Control valves • Report status
Valves	• Open/close on command • Fail open? / Fail closed?



Adapted from Dr Thomas' STPA Tutorial

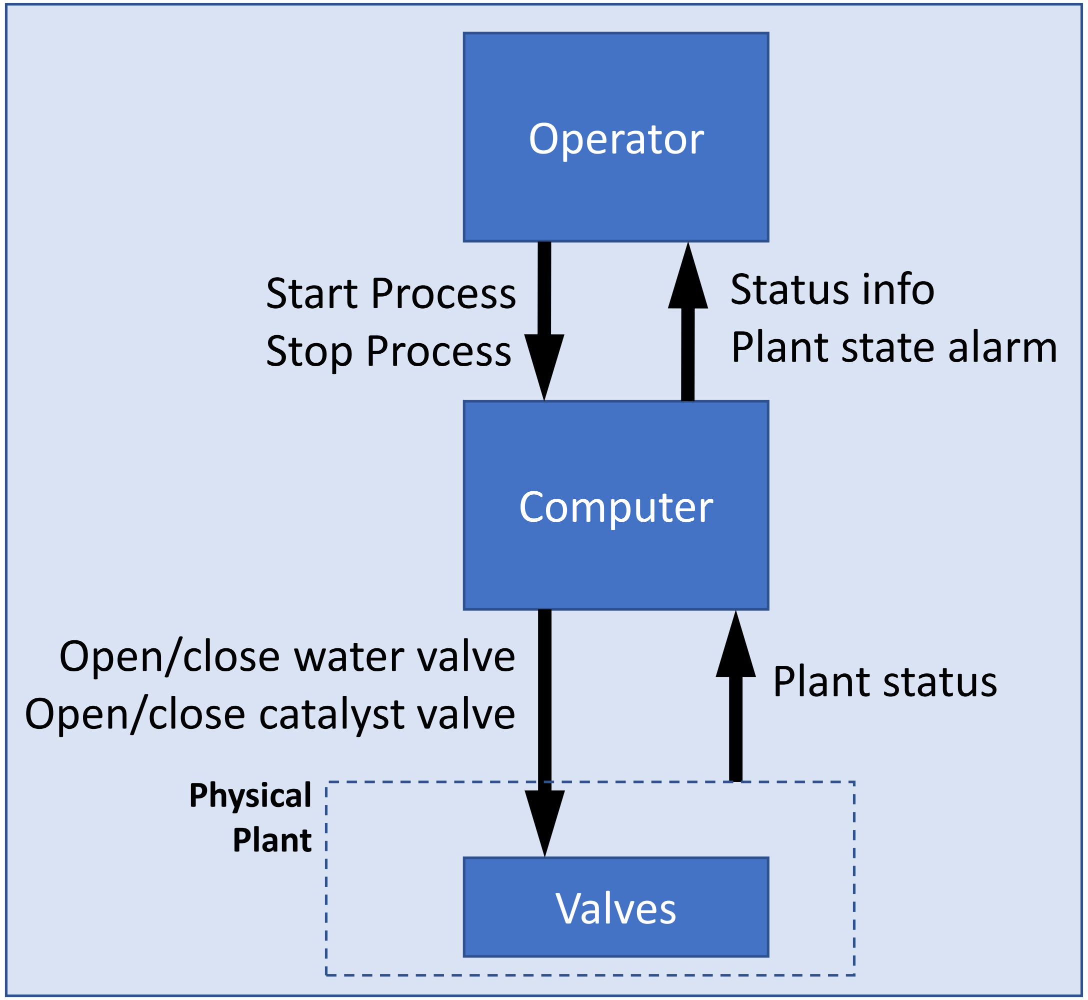
Chemical Reactor – Control Structure

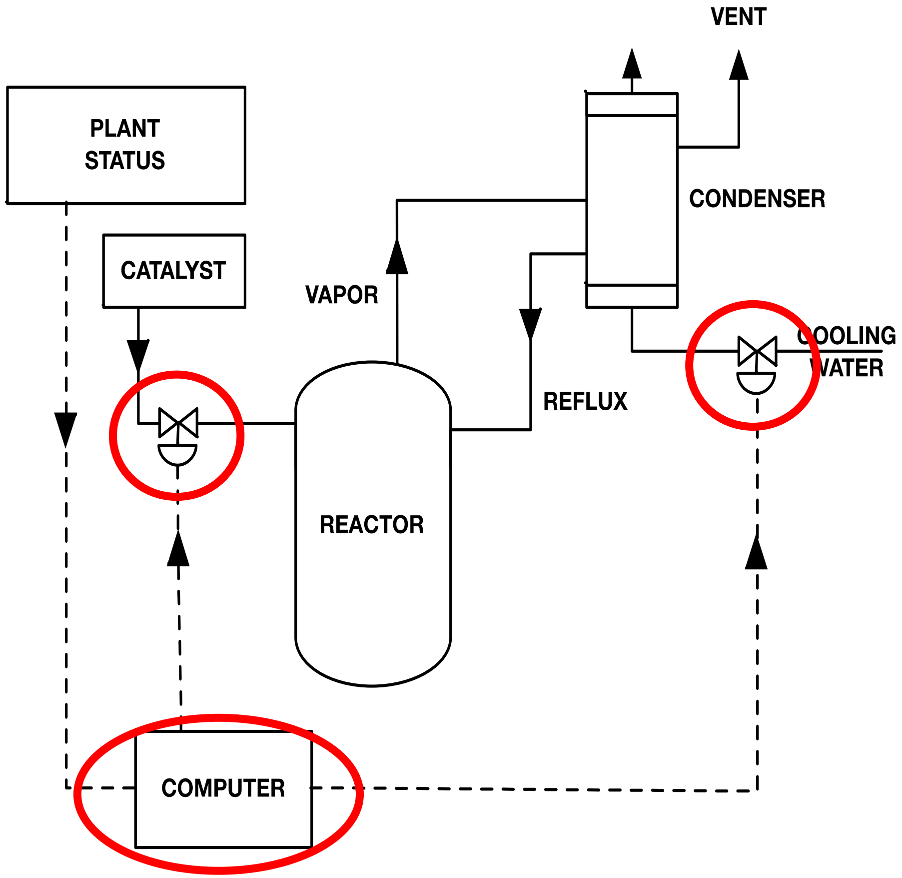




Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor – Control Structure

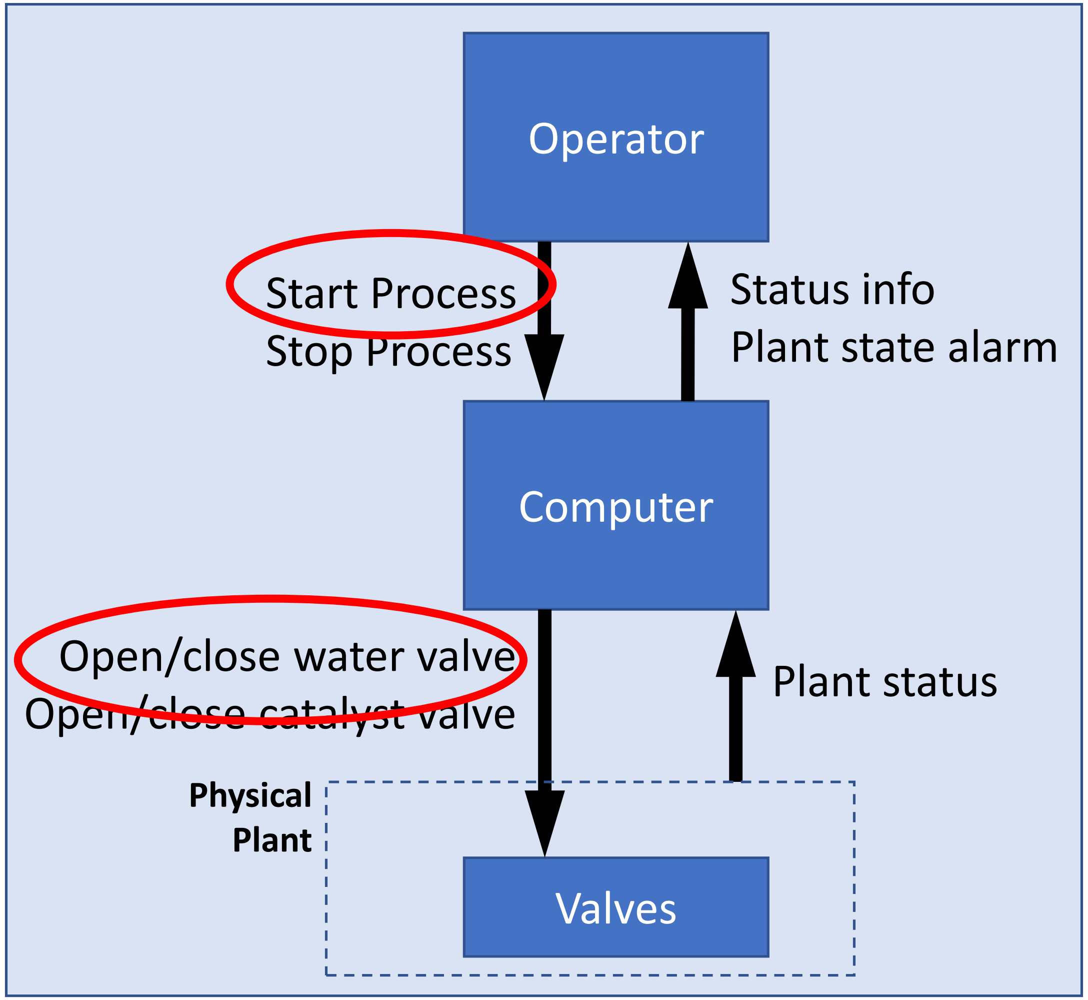




What are the unacceptable losses ?

Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor – HCAs (Unsafe / Unsecure)



HCA - Hazardous Control Action

What are the unacceptable losses ?

Adapted from Dr Thomas' STPA Tutorial

Identify Hazardous Control Actions

Chemical Reactor – HCAs (Unsafe / Unsecure)

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect Timing or Order	Stopped too soon or applied too long
CA1: Start Process				
CA2: Open Water Valve				

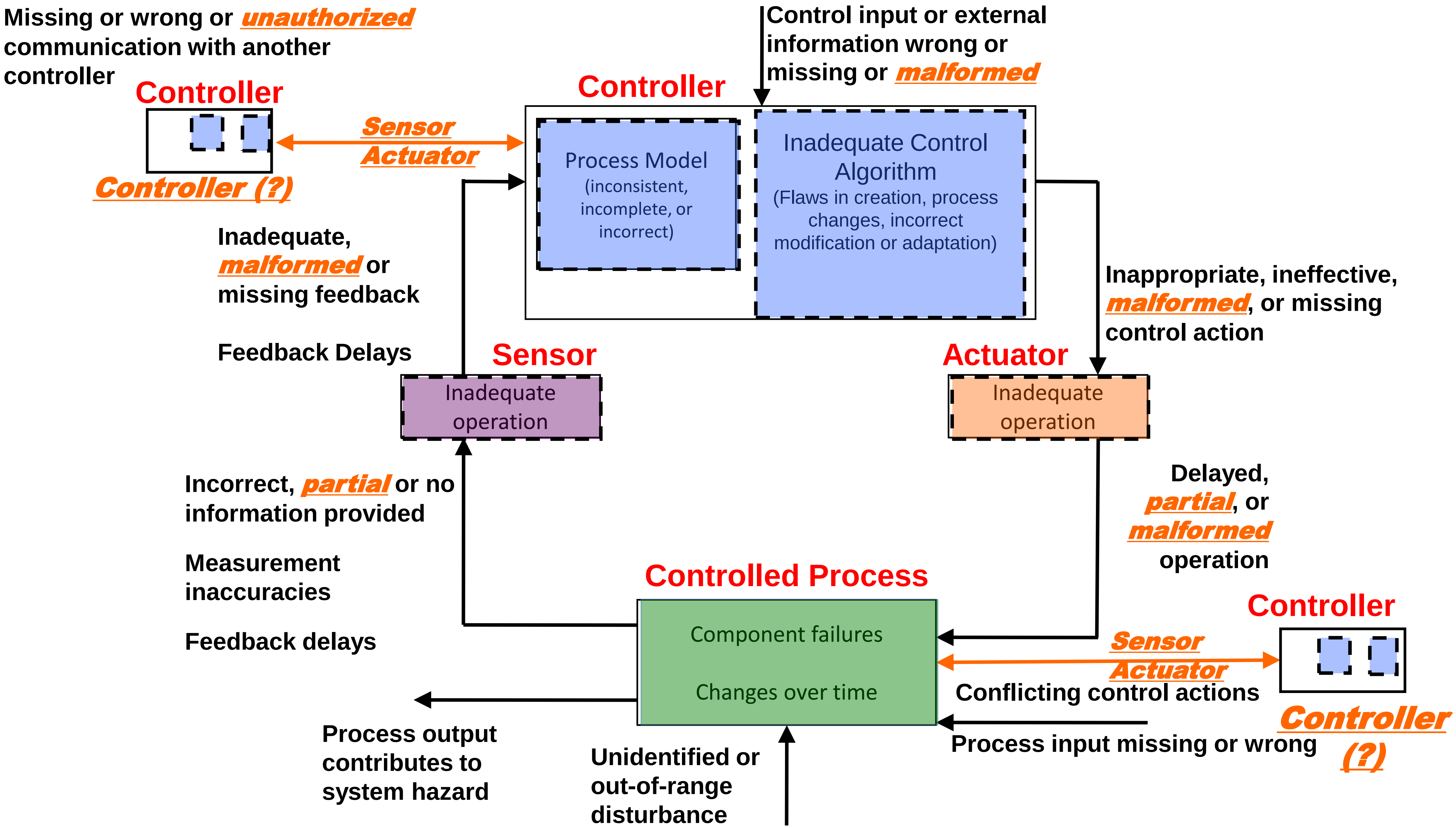
Adapted from Dr Thomas' STPA Tutorial

Chemical Reactor:
Hazardous Control Actions (HCA)

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect Timing or Order	Stopped too soon or applied too long
CA1: Start Process		Operator provides command when condenser water valve not functioning	Operator manually overrides valves and computer misses signal	
CA2: Open Water Valve	Computer does not provide open water valve cmd when catalyst open		Computer provides open water valve cmd more than X seconds after open catalyst	Computer stops providing open water valve cmd too soon when catalyst open
CA3: Close Water Valve		Computer provides close water valve cmd while catalyst open	Computer provides close water valve cmd before catalyst closes	
CA4: Open Catalyst Valve		Computer provides open catalyst valve cmd when water valve not open	Computer provides open catalyst valve cmd more than X seconds before open water	
CA5: Close Catalyst Valve	Computer does not provide close catalyst valve cmd when water closed		Computer provides close catalyst valve cmd more than X seconds after close water	Computer stops providing close catalyst valve cmd too soon when water closed

Adapted from Dr Thomas' STPA Tutorial

Identify Loss Scenarios

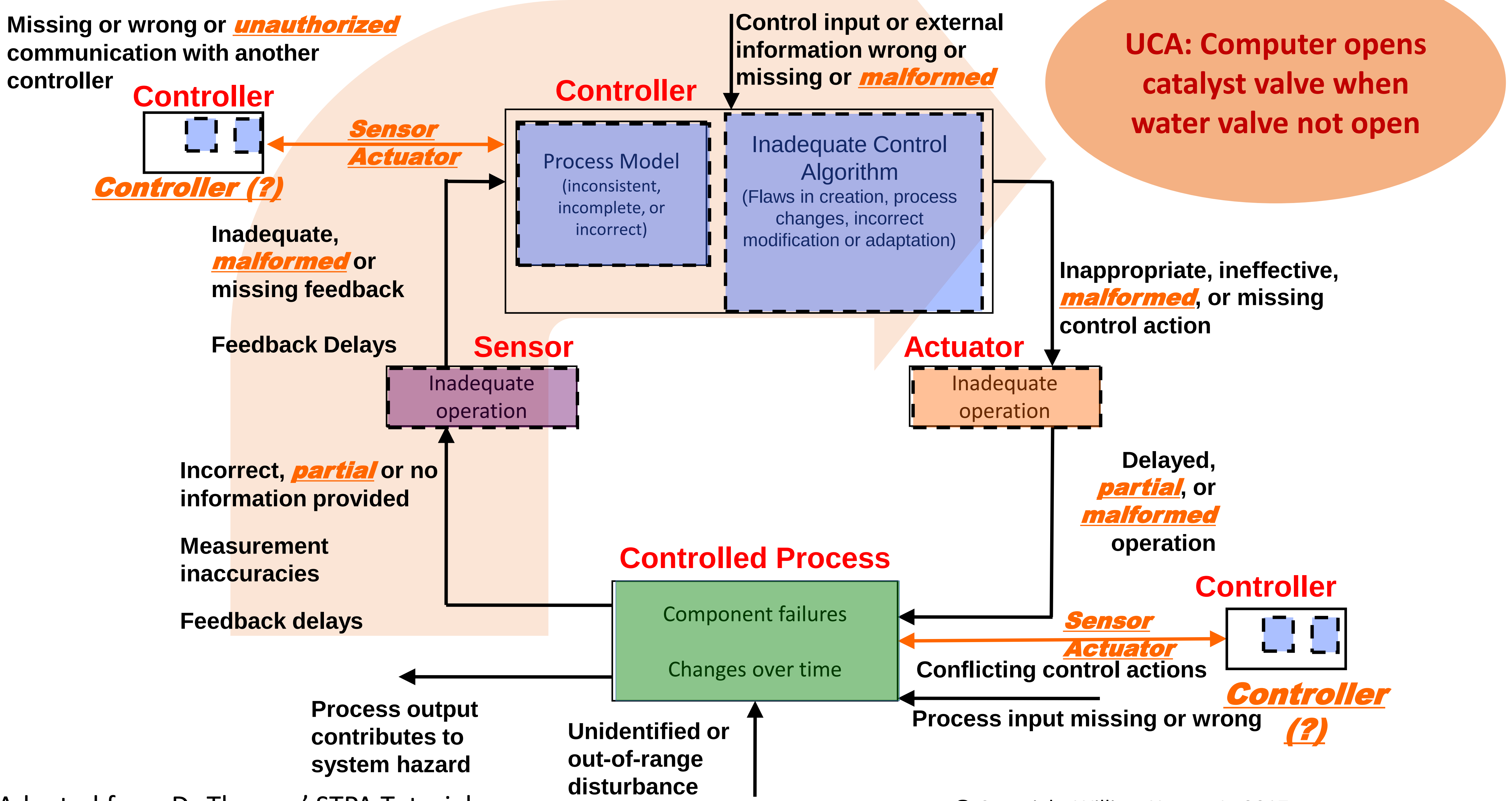


Missing or wrong or unauthorized communication with another controller
Controller
Controller (?)
Sensor
Actuator
Controller
Control input or external information wrong or missing or malformed
Process Model
(inconsistent, incomplete, or incorrect)
Inadequate Control Algorithm
(Flaws in creation, process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

Identifying Scenarios that Lead to Unsecure Control Actions

- **Scenarios should be used to facilitate deeper insights and understanding, they are not a checklist**
- **Scenarios provide an opportunity to engage technical experts and ask key questions necessary to support improved requirements**
- **Scenarios form a connected narrative to understand and explain interactions across the system (and set appropriate requirements)**
- **Scenarios should provide useful insight or generate additional questions for deeper debate and discussion**
    - **Scenarios such as "denial of service attack prevents controller from issuing close valve command" aren't really as useful as "controller issues command to initiate the process because it received inputs from sensor X indicating that valve is closed when the valve was only partially closed due to sensor logic declaring the valve closed when XXXX"**

Step 2: Potential causes of UCAs



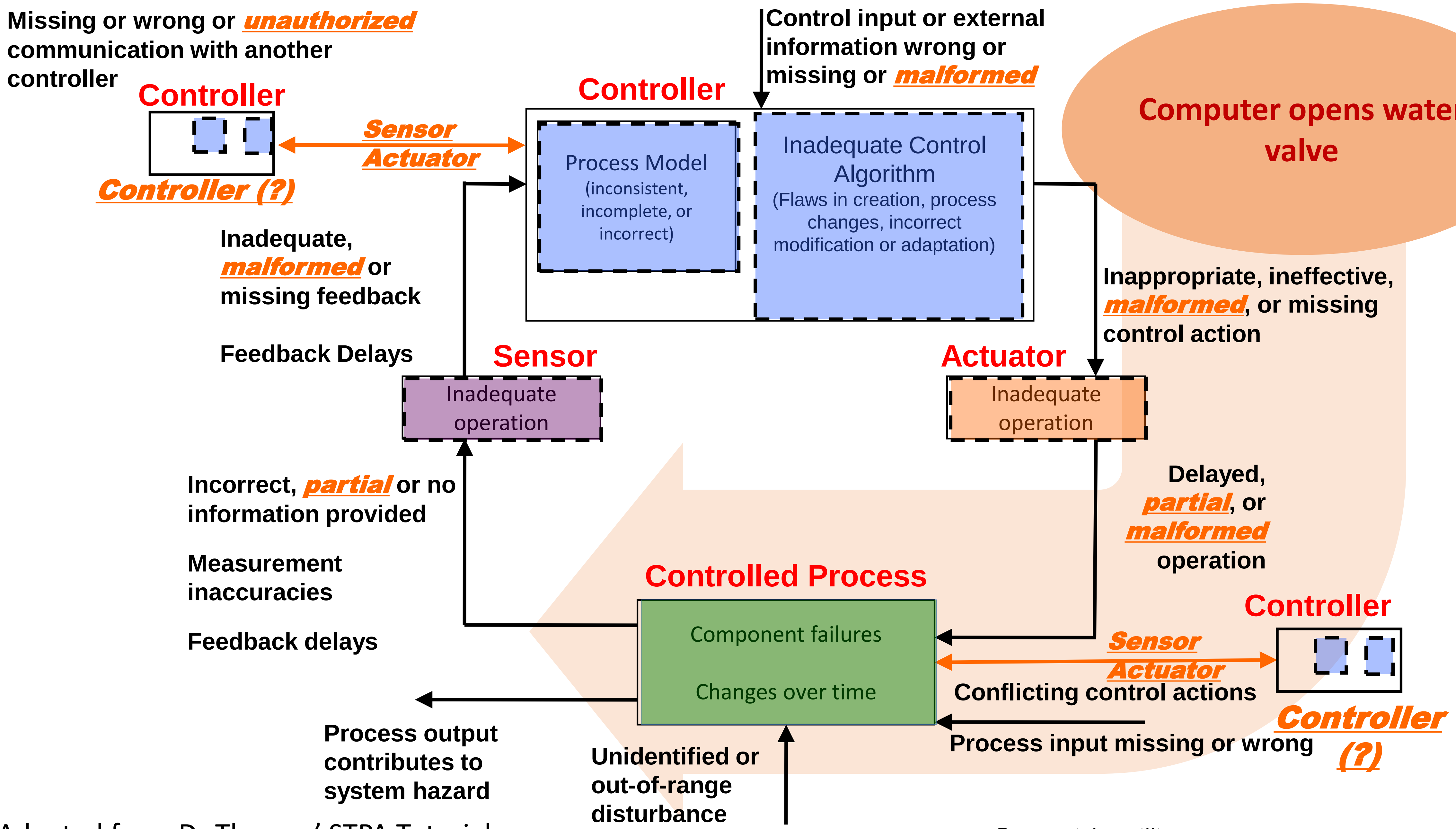
Adapted from Dr Thomas' STPA Tutorial

Scenario

UCA: Computer does not provide close catalyst valve cmd when water closed		
Scenario	Associated Causal Factors	Rationale/Notes
Water valve status signal is incorrectly processed by computer.	•Malformed signal from valve •Partial signal from valve •Missing signal from valve •Inconsistent process model	Malicious logic on water valve system reports false/delayed/malformed information. Malicious logic on computer modifies process model variable to indicate that water valve is open.

Adapted from Dr Thomas' STPA Tutorial

Step 2: Potential control actions not followed



Adapted from Dr Thomas' STPA Tutorial

Causal Scenarios

UCA: Computer provides open water valve cmd more than X seconds after open catalyst		
Scenario	Associated Causal Factors	Rationale/Notes
Code on the computer processes asynchronously. Assumptions about the latency of commands violated causing a delayed send to water valve.	• Inadequate control algorithm • Delayed partial operation	Test and operational environment were low latency and timing errors were not tested. Malicious logic on computer or other system causes delay in the sending or receiving of command.

Adapted from Dr Thomas' STPA Tutorial

Causal Scenarios

UCA: Operator provides command when condenser water valve not functioning		
Scenario	Associated Causal Factors	Rationale/Notes
Operator believes that systems are fully functioning, and commands the start of the reaction process.	• Inadequate feedback from computer on water valve status • Malformed sensor data incorrectly indicates green • Partial data coming from sensor causes computer to indicate wrong state • Missing status feedback from valve	Unaccounted for error state in software used by malicious logic in valve and/or computer.

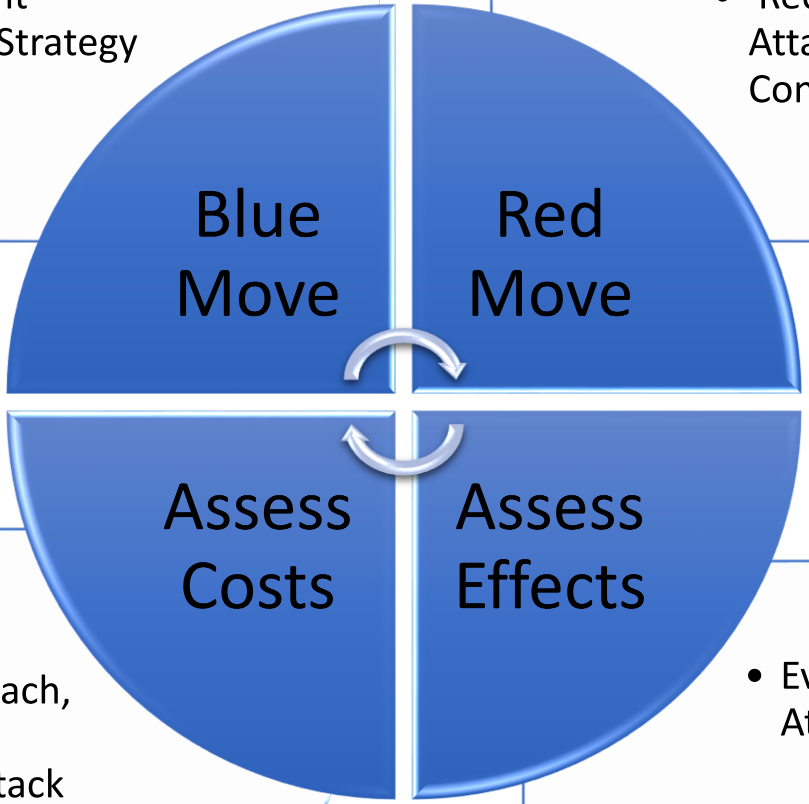
Adapted from Dr Thomas' STPA Tutorial

War Gaming

Wargaming

- Blue Constraint Enforcement Strategy

- Red Select General Attack Class to Violate Constraint



- Assess cost of constraint approach, cost of attack, complexity of attack

- Evaluate effects of Attack on Constraint

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

Summary and Conclusions

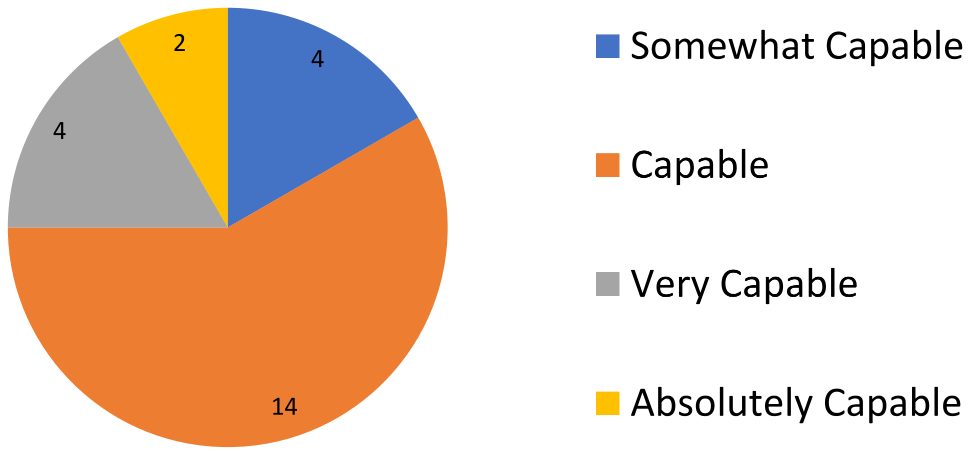
Lessons Learned Applying STPA-Sec

- 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"

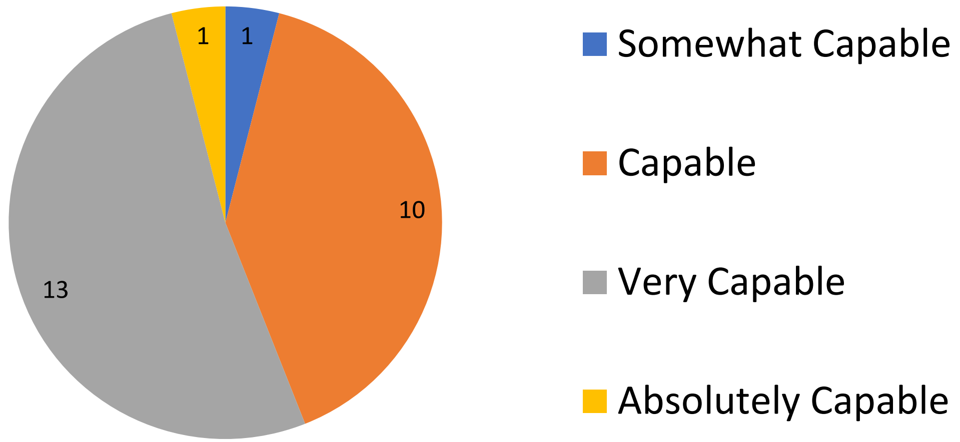
STPA-Sec is NOT a silver bullet, but appears to enable increased rigor "Left of Design"

Recent Self-Reported Assessment Results

Before Training : Ability to Develop Mitigation Strategy



After Training : Ability to Develop Mitigation Strategy



Safety and Security

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

Conclusion

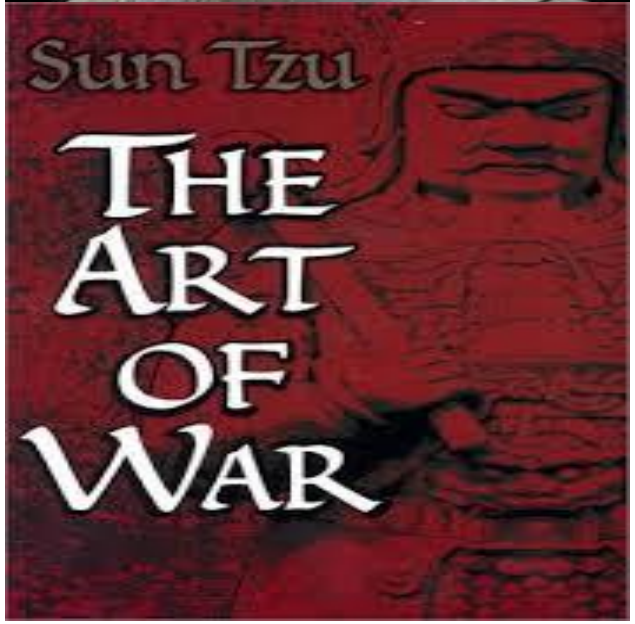
- **Must think carefully about defining the security problem**
- **Perfectly solving the wrong security problem doesn't really help**
- **STPA-Sec provides a means to clearly link security to the broader mission or business objectives**
- **STPA-Sec does not replace existing security engineering methods,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

Concluding Thoughts from Sun Tzu

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

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

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



QUESTIONS ??

QUESTIONS ??