


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

William Young Jr, PhD

Reed Porada

2017 STAMP Conference
Boston, MA

March 27, 2017

WYOUNG@MIT.EDU

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, or the U.S. Government

WYOUNG@MIT.EDU

Overview

- **Part I: Cyber Security and STPA**
  - **Introduction**
  - **<u>What</u> Aspect of Security is our Focus?**
  - **<u>Where</u> (level) of Security are We Focused on?**
  - **<u>When</u> in System Engineering Lifecycle are we Focused on?**
  - **<u>Who</u> Among the Organization's Personnel are we Focused on?**
  - **<u>Why</u> Does This Aspect of Security Matter?**
  - **<u>How</u> Does STPA-Sec Work: Simple Example Based on Chemical Reactor**
  - **Conclusion**
- **Part II: Cyber Security Practicum (Immediately Following in 32-144)**

WYOUNG@MIT.EDU

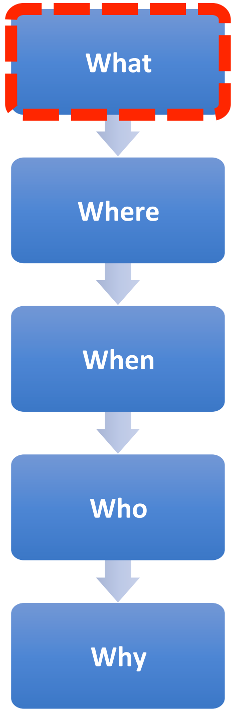
Introduction / Motivation

- System and software engineers face increased pressure to stem growing losses
- 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"
- ICT problems are ubiquitous and growing, but cybersecurity solutions extend beyond cryptography, software engineering, etc.
- Security engineering is the emerging field to address these challenges
- Growing realization that security engineering must begin before architecture development…but we need a Security Engineering Analysis methodology

We Must Ensure That We Are Solving the Right Engineering Problem

WYOUNG@MIT.EDU

Security and Cyber Security Defined



<u>Security</u> (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.

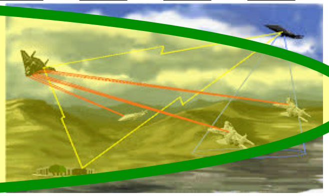
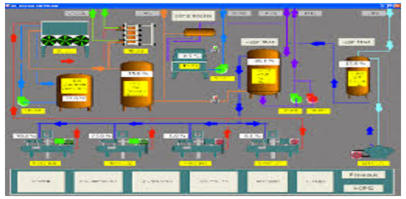
<u>Cybersecurity</u> (US Gov't & DoD)-- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity,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

Cyber Security is an Overarching Term that Covers Nearly Everything

WYOUNG@MIT.EDU

Cyber Security of What?

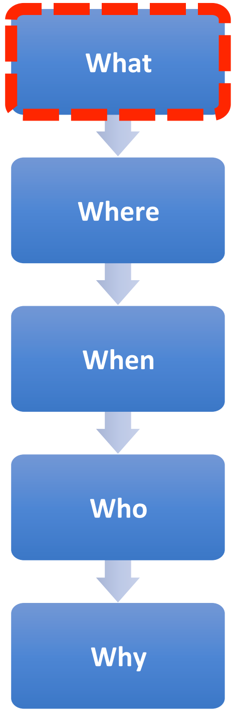
- **What**
- Where
- When
- Who
- Why

TYPE / *LEVEL*	Traditional Info Technology	Operational Technology*	Platforms
Mission / Business Level (Management / Operational / Technical Controls)			
System Level (Technical / Operational Controls)			
Component Level (Technical Controls)			

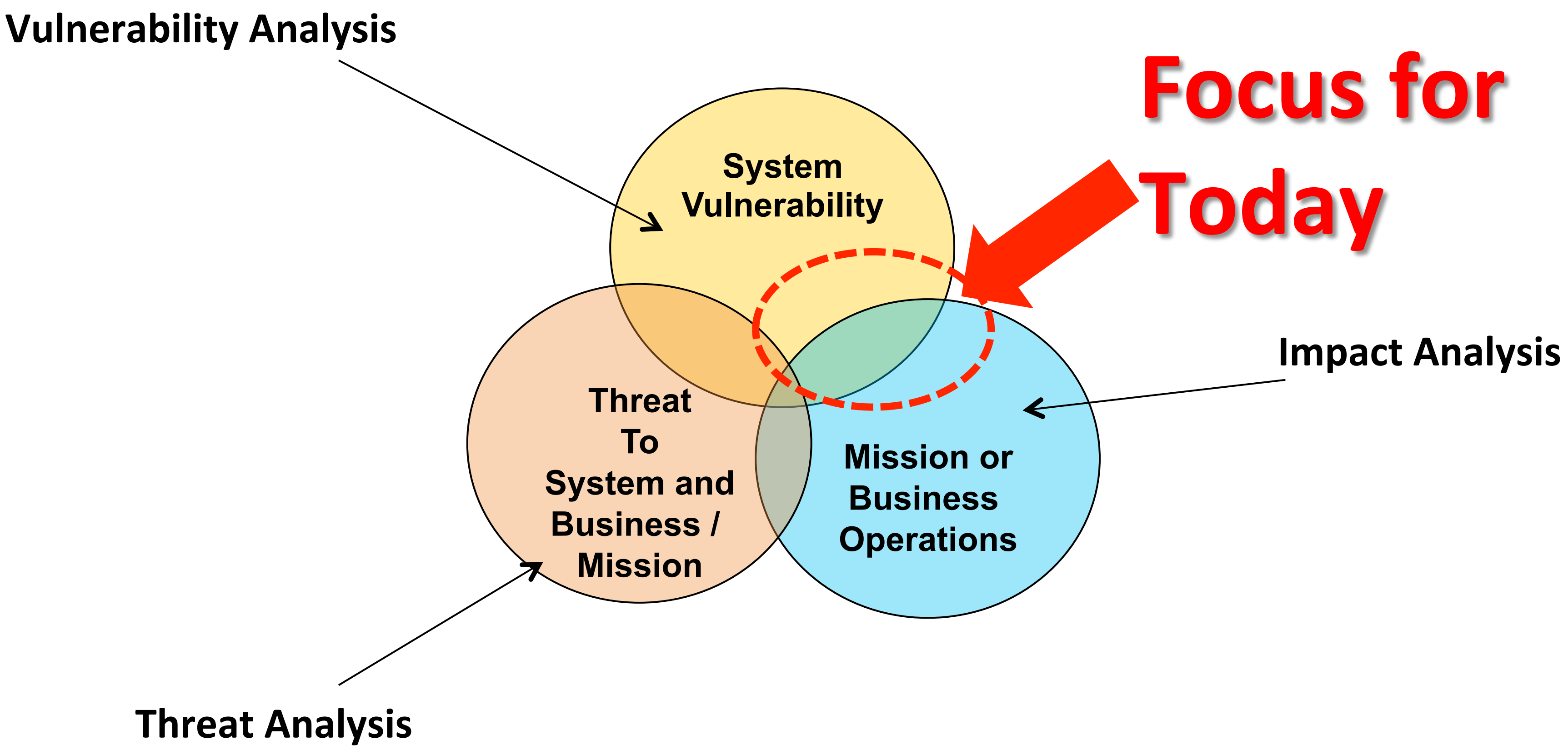
* Operational Technology – computer controlled physical processes such as ICS (i.e. power, water) logistics (fuel systems) or other control systems (i.e. building automation, security alarms)

Our Focus Today is the Top Level (Business or Mission Operations)

WYOUNG@MIT.EDU



Cyber Security Through Different Analytic Lenses



The physical system exists to enable business / mission function

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

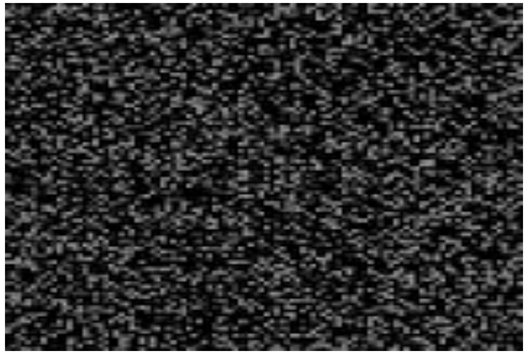
WYOUNG@MIT.EDU

Mission Failure Versus System Failure

1. Target Acquired

2. Information Communications Technology transmits data

3. Commander at distant center observes



4. Mission Commander loses surveillance and aborts

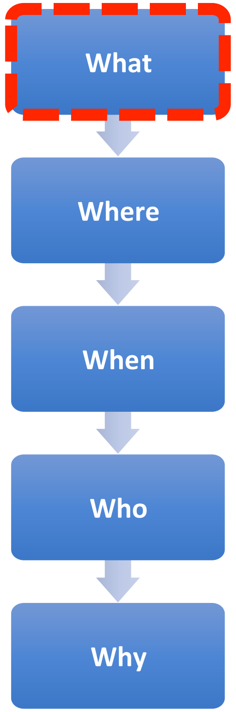
5. SOF team aborts mission

6. Attempt to determine cause

Could Mission Operation Have Been Designed Differently to Enable More Assurance?

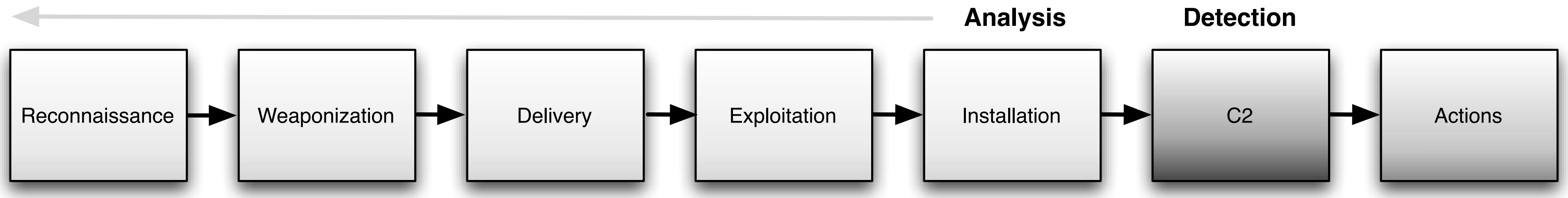
Ref: (Vautrinot, 2012)

WYOUNG@MIT.EDU



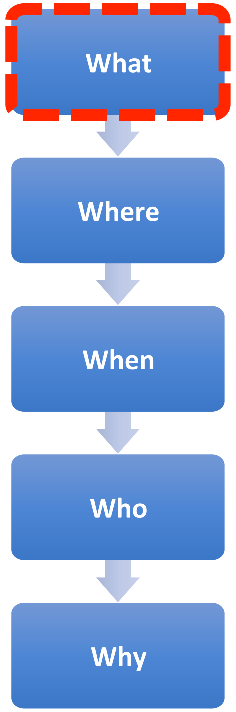
Security Today

- **Find the most important components and protect them**
- **Compliance with standards and best practice believed keep our systems secure from loss**
- **Breaking the “Kill Chain” prevents losses**
- **Surveys or questionnaires to uncover what is most important**



Do we believe that these approaches are working?

We Are Performing Security Engineering

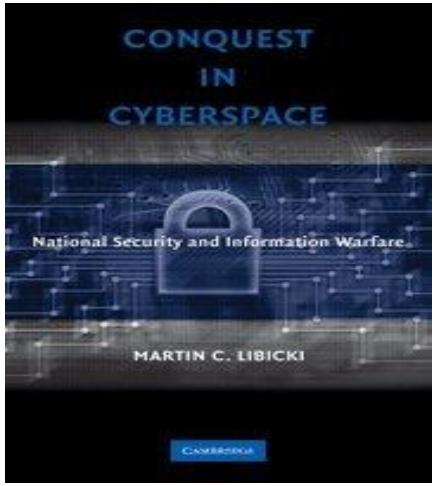


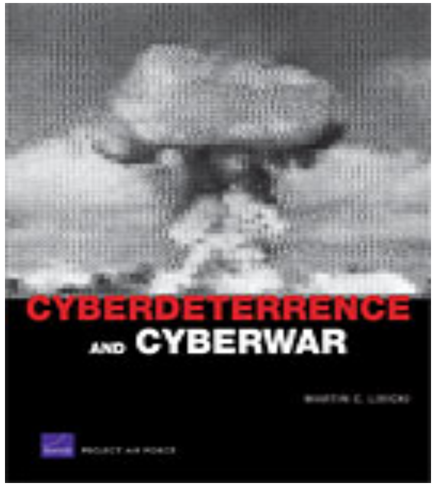
- Security Engineering--"An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem" (US Federal Gov't)
- Systems Security Engineering—"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)

NIST SP 800-160 "Systems Security Engineering" is Emerging as the US Gov't Standard

Martin Libicki on Network Security

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

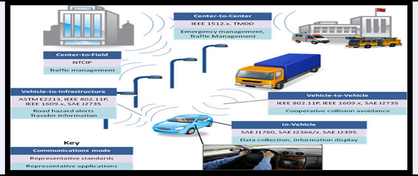
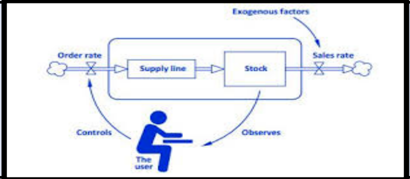
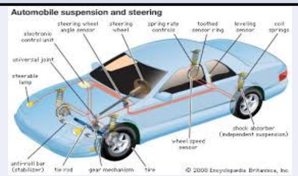
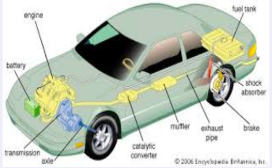




Reference:“Cyberspace is not a Warfighting Domain”

Where (Level) is Security Performed

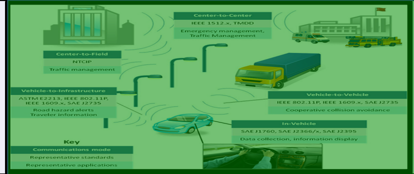
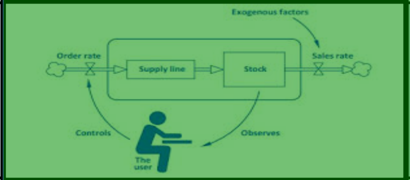
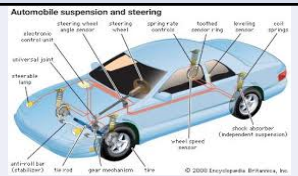
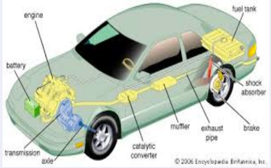
- What
- **Where**
- When
- Who
- Why

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

Form follows function

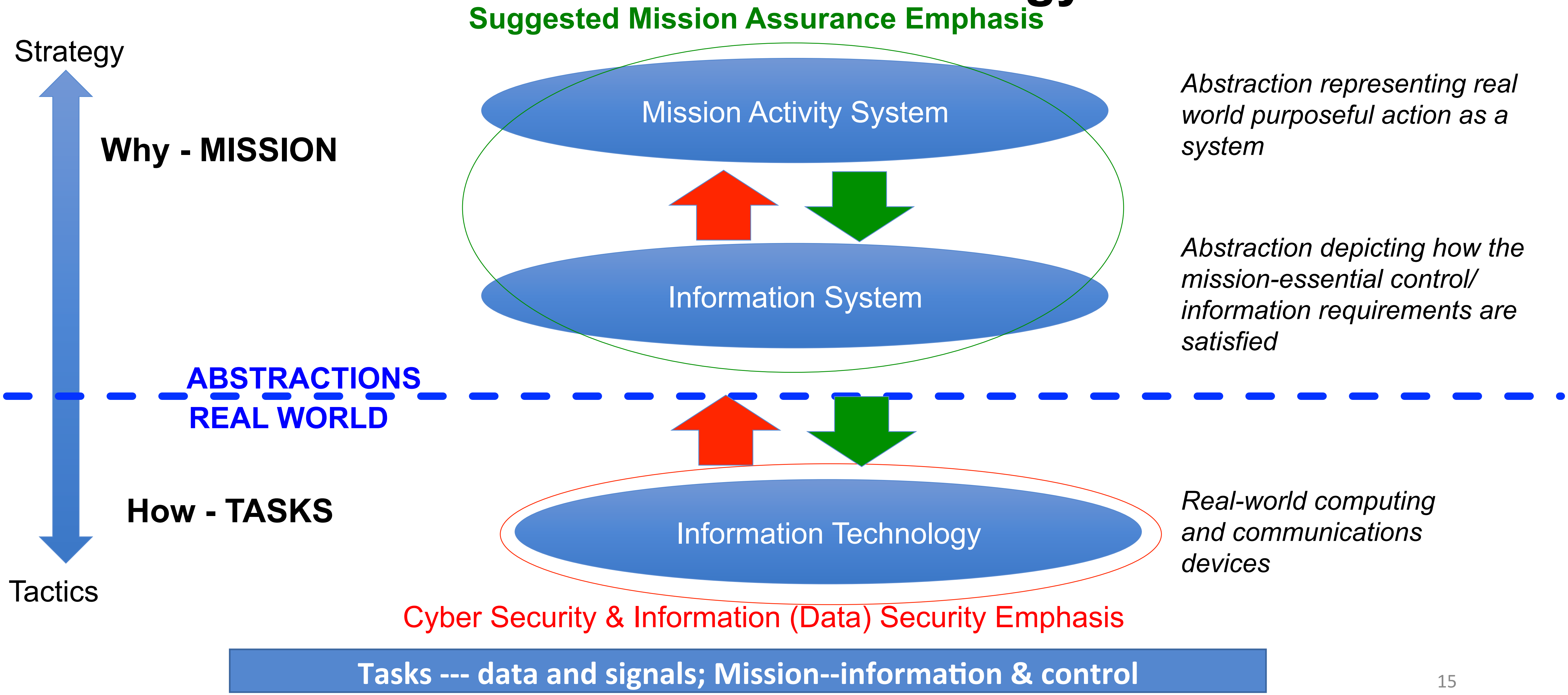
Where (Level) is Security Performed

- What
- **Where**
- When
- Who
- Why

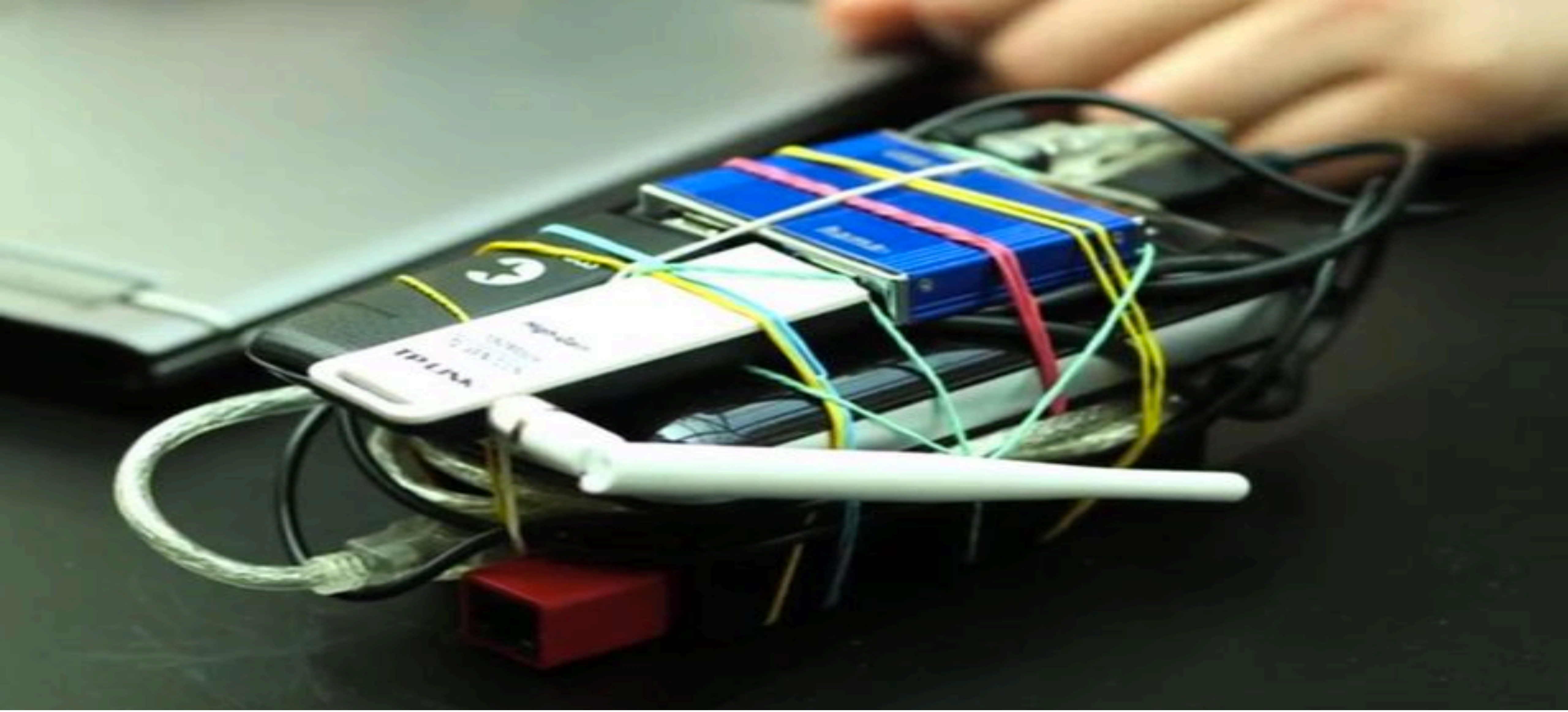
Whole - Part / Ends - Means	Whole System	Subsystem 1	Subsystem 2	Component		
				HW	SW	Human
Functional Purpose						
Abstract Function		Problem Space				
General Function						
Physical Function						
Physical Form						

Ignoring the problem space prevents taking advantage of improved problem definition

Systems, Information Systems, Information Technology



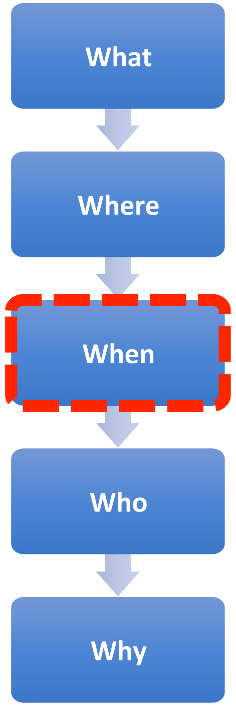
Reference: Checkland, 1995; Checkland and Howell 1998

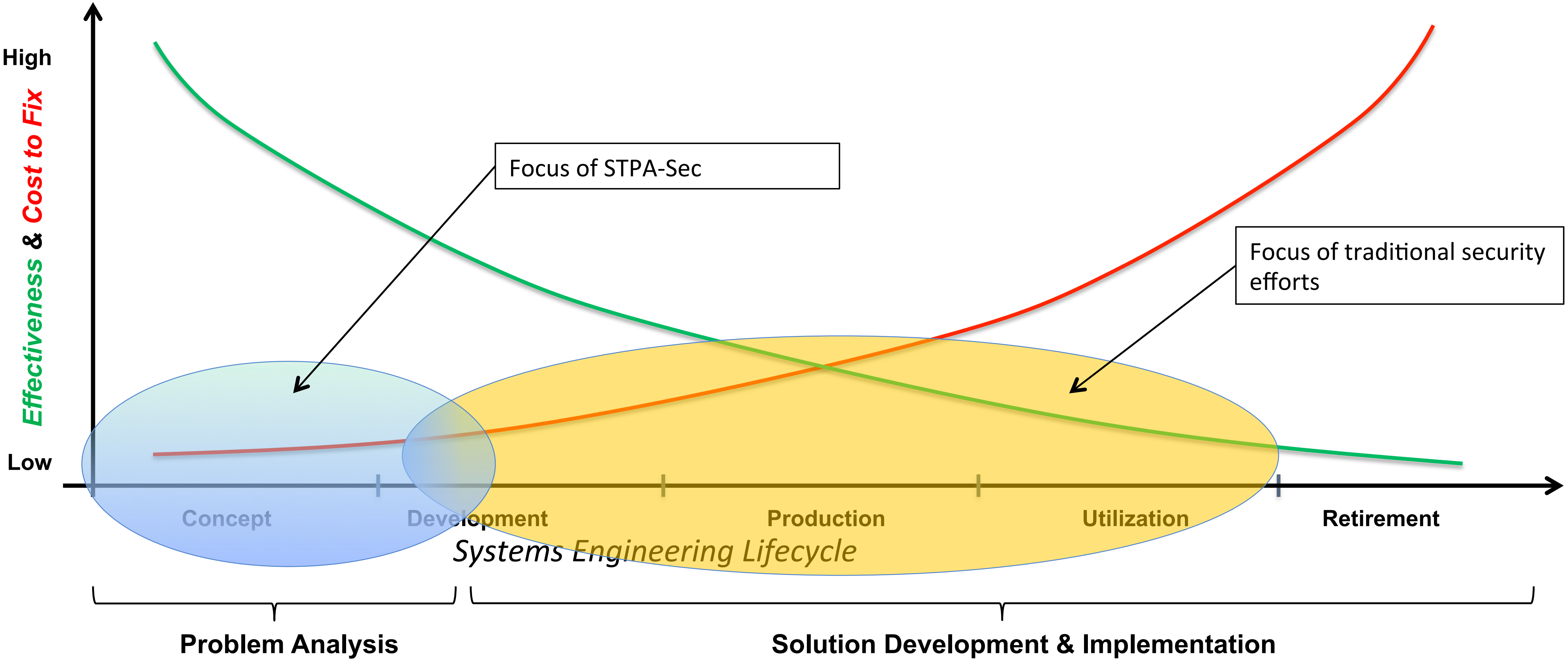


Just Because you Can, Doesn't Mean you Should…
Just Because it Works, Doesn't Mean it Can Be Secured

WYOUNG@MIT.EDU

When to Address Security-- Pre-Architecture





We Must Rigorously Identify and Frame the "Right" Security Problem

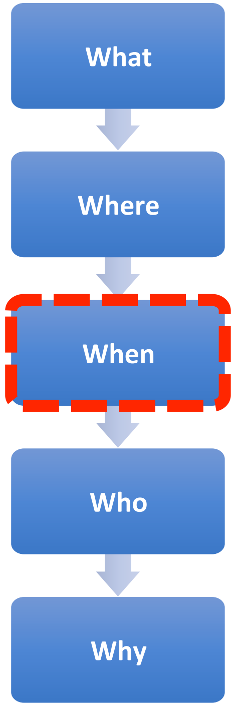
WYOUNG@MIT.EDU

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

Performed During Early Engineering Technical Processes



IEEE/IEC/ISO 15288 (System Engineering Standards)

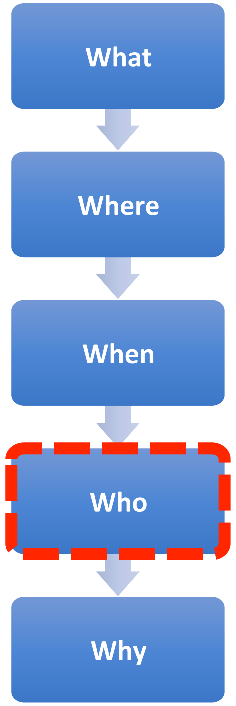
- Business or mission analysis
- Stakeholder needs and requirements
- System requirements definition

NIST SP 800-160 (Emerging Secure System Engineering Standards)

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

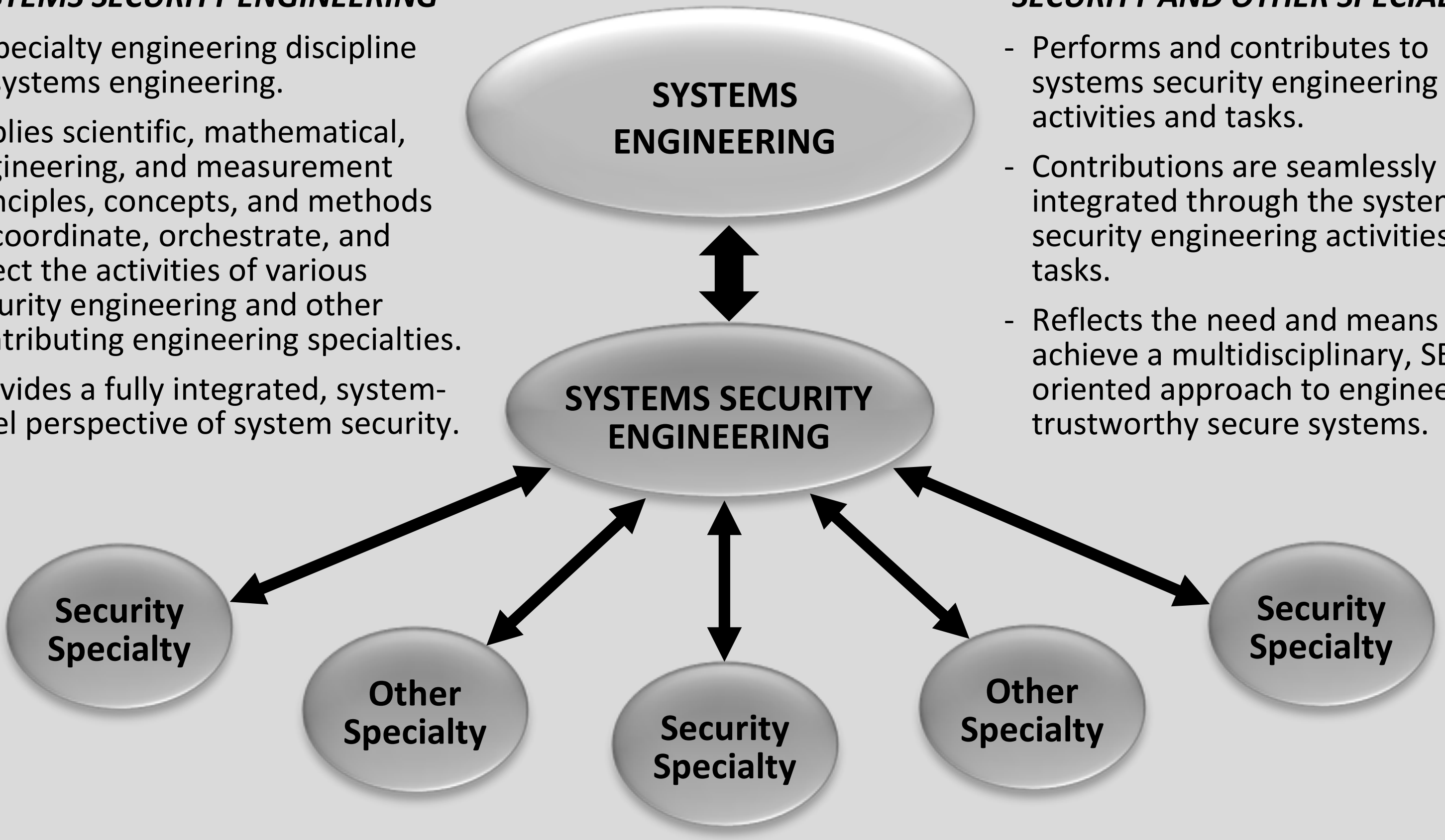
WYOUNG@MIT.EDU

Who Are We Focused On



SYSTEMS SECURITY ENGINEERING

- A specialty engineering discipline of systems engineering.
- Applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering and other contributing engineering specialties.
- Provides a fully integrated, system-level perspective of system security.



SECURITY AND OTHER SPECIALTIES

- Performs and contributes to systems security engineering activities and tasks.
- Contributions are seamlessly integrated through the systems security engineering activities and tasks.
- Reflects the need and means to achieve a multidisciplinary, SE-oriented approach to engineering trustworthy secure systems.

Source: *Adapted from Bringing Systems Engineering and Security Together, INCOSE SSE Working Group, February 2014.*

Cross Functional Team Required to Address Cross Functional Challenge

Ref: NIST SP 800-160

WYOUNG@MIT.EDU

Cybersecurity is a Wicked Problem

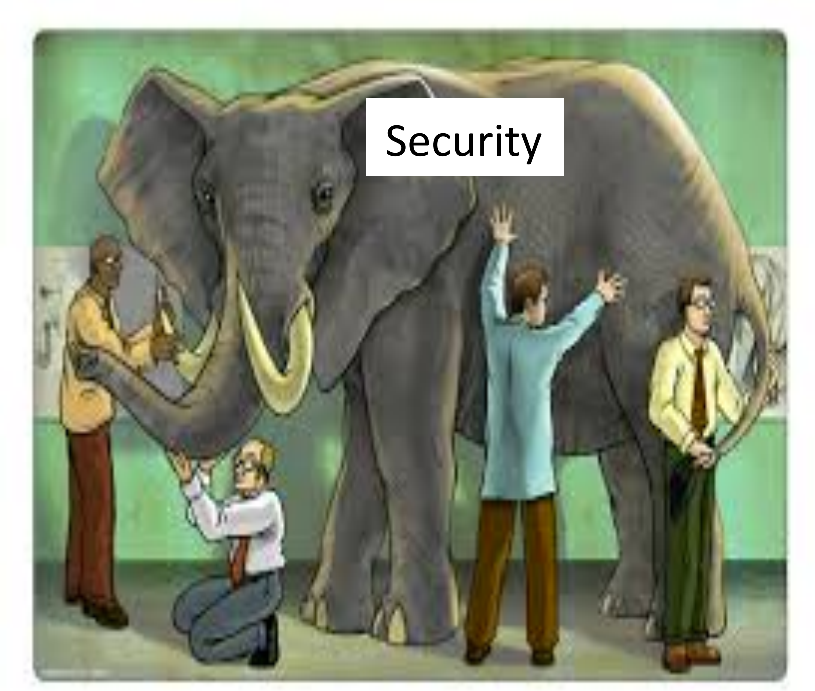
What

Where

When

Who

Why



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!

WYOUNG@MIT.EDU

Story of “Bob”

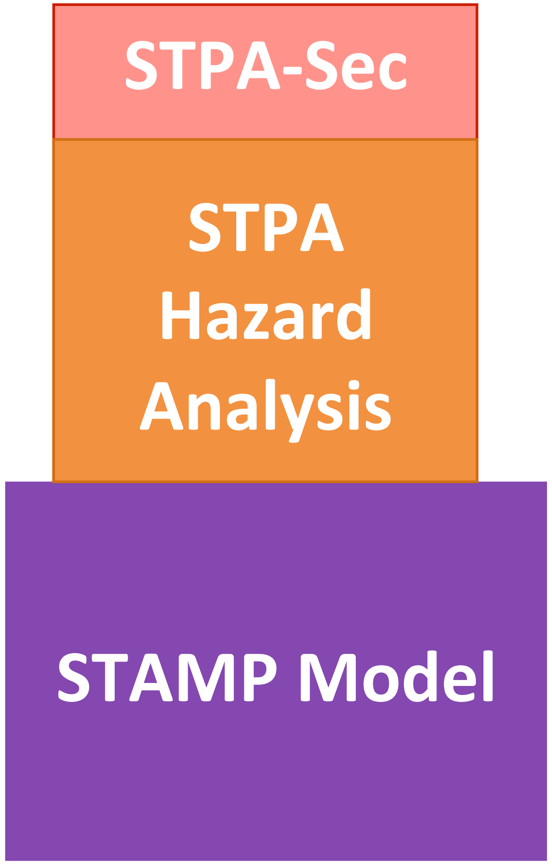
Just Because You Know What You Want To Build, Doesn’t Mean You Have Defined the Problem

WYOUNG@MIT.EDU

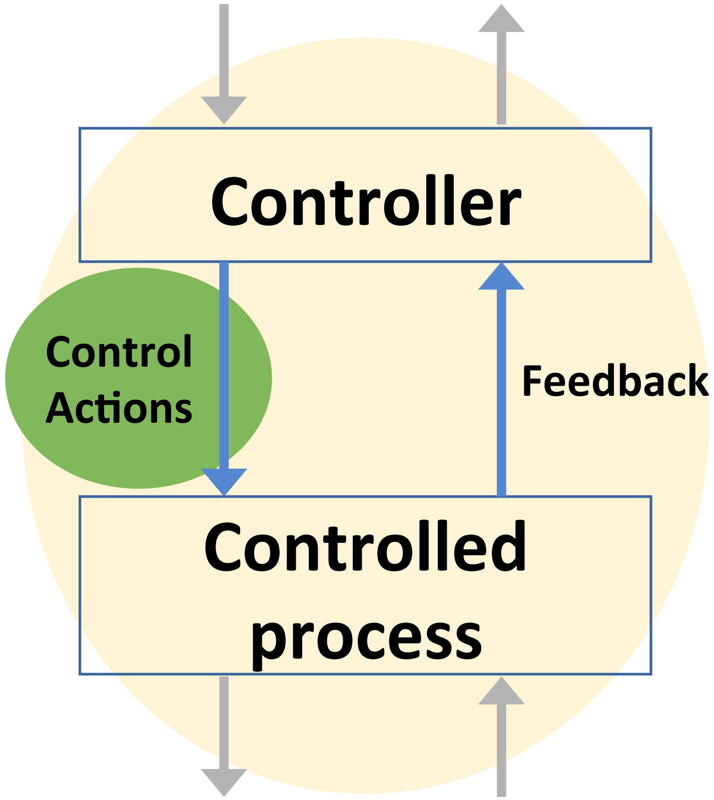
SYSTEM THEORETIC PROCESS ANALYSIS FOR SECURITY (STPA-Sec)

WYOUNG@MIT.EDU

STPA-Sec Extends STPA



- Define system purpose and goal
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe/unsecure control actions
- Step 2: Identify causal scenarios
- Wargame



WYOUNG@MIT.EDU

STPA-Sec Process

System Engineering Foundations

- Define and frame security problem
- Identify losses/accidents
- Identify system hazards/constraints

Identify Types of Unsafe/Unsecure Control

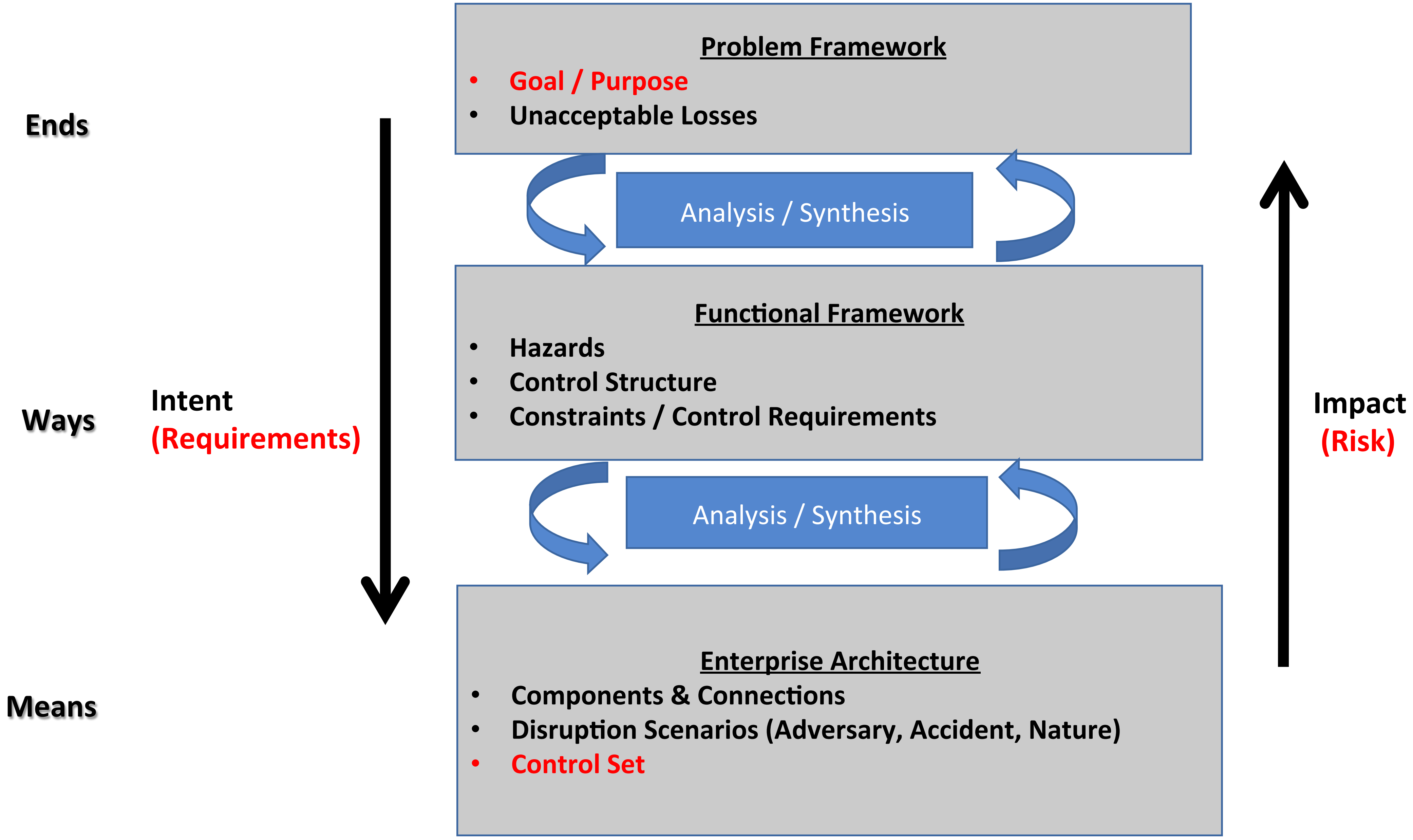
- Model functional control structure
- Identify unsafe/unsecure control actions

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



WYOUNG@MIT.EDU

Definitions

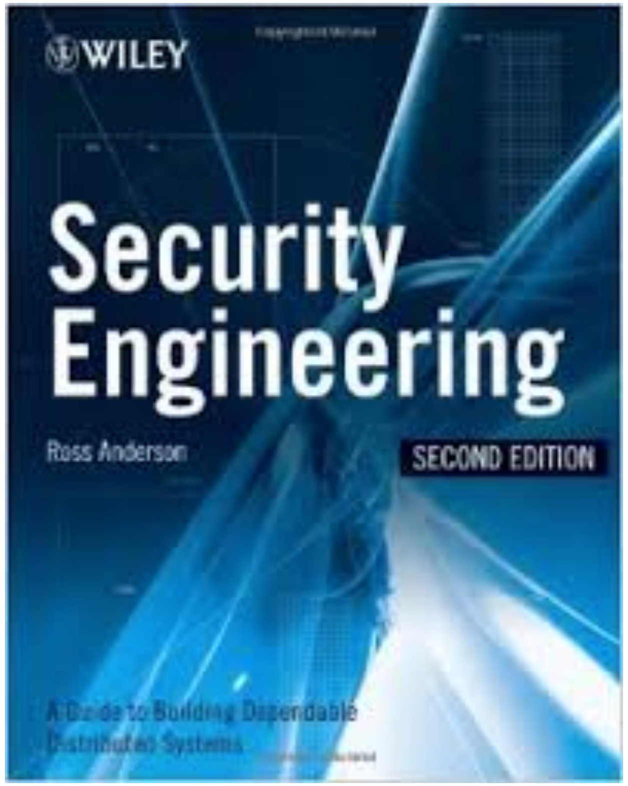
- **Mission (US Military Doctrine) – "The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore."**
- **Business / Mission Analysis (INCOSE) – "defining the problem domain, identifying major stakeholders, identifying environmental conditions and constraints 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)**

WYOUNG@MIT.EDU

Security Engineering Analysis

- **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"



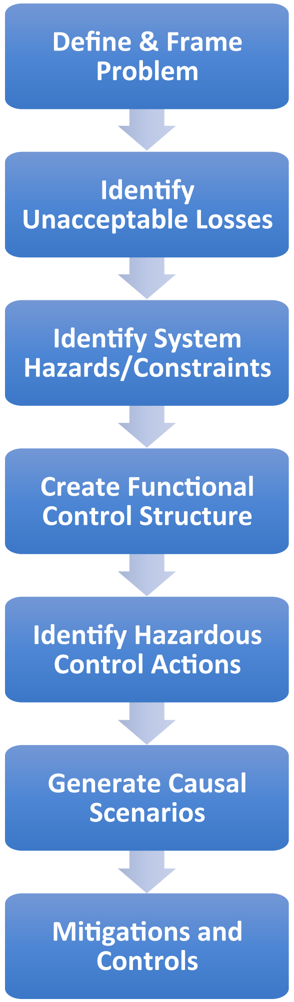
Security Analysis Provides a Rigorous Manner to Identify What to Protect and How to Protect it

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.

WYOUNG@MIT.EDU

STPA-Sec Process

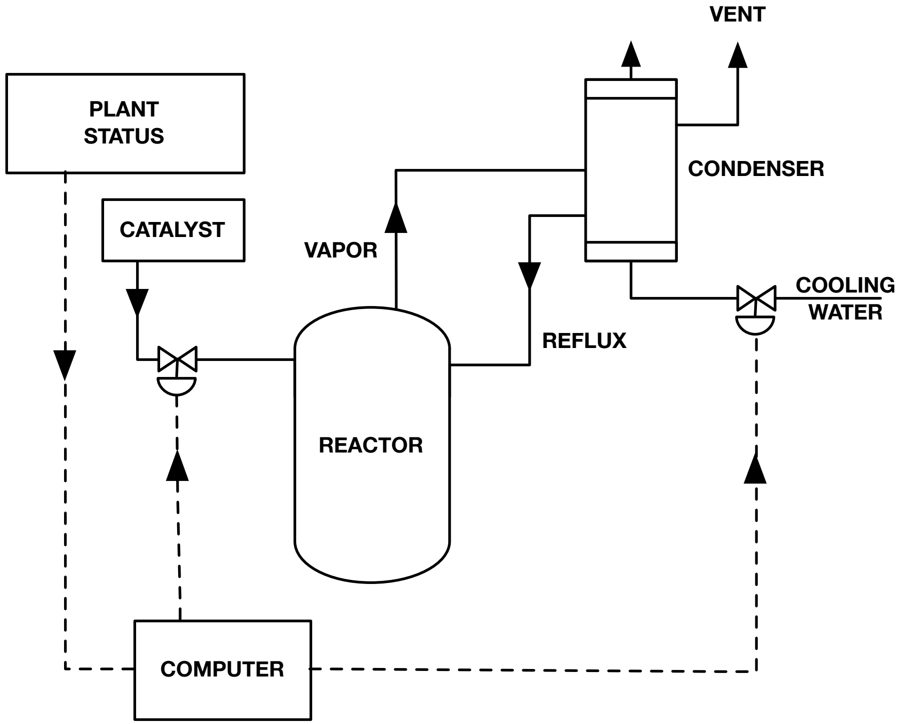


- **Use STPA-Sec to perform the security engineering analysis to inform the security engineering process**
- **Use results to inform early system engineering trades**
- **Set the foundation to understand, inform and document security requirements**

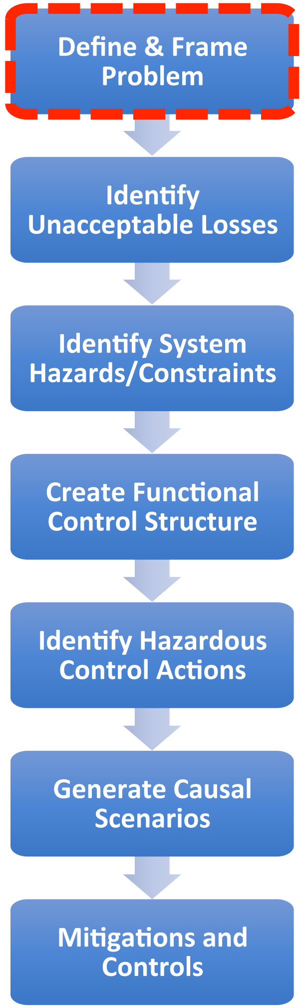
WYOUNG@MIT.EDU

Chemical Reactor Design

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

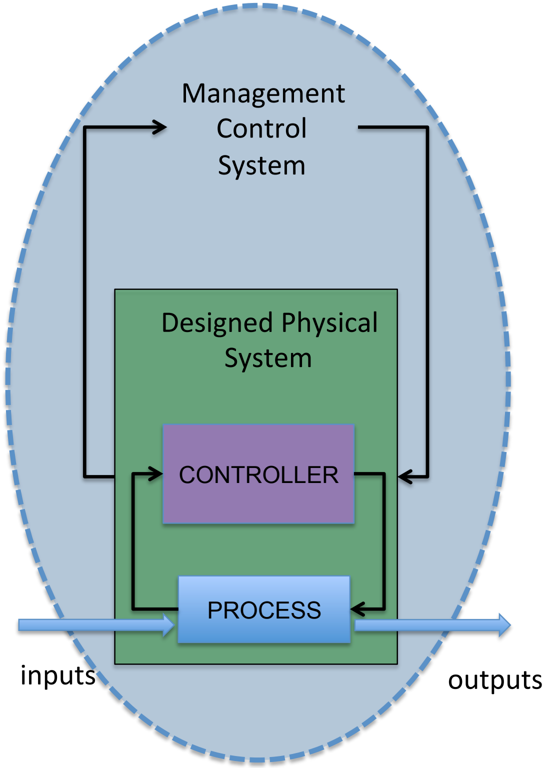


Define & Frame Security Problem

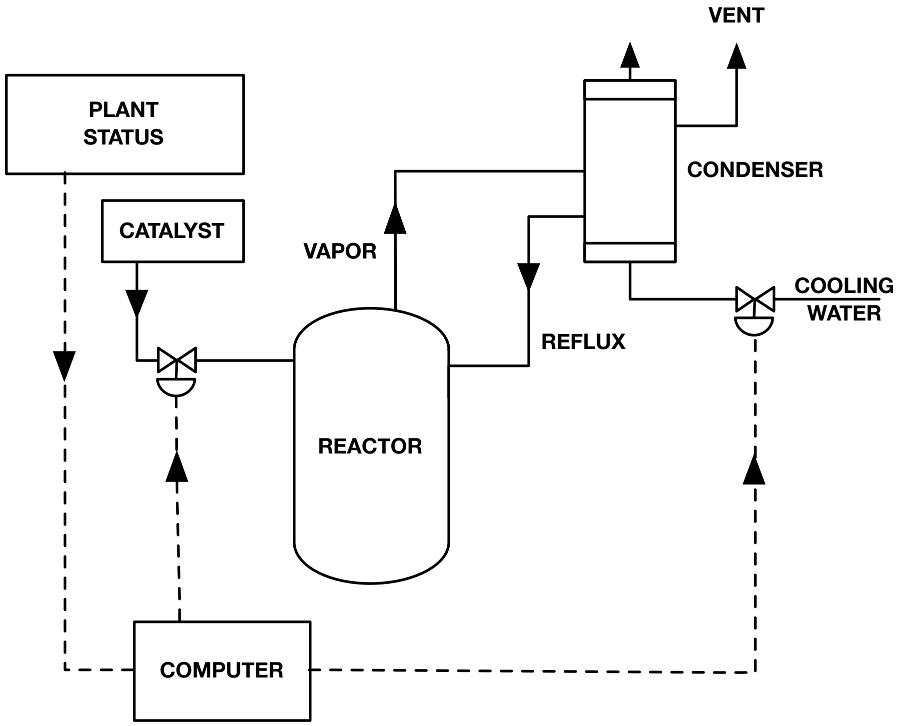


- **Define the system purpose and goal:**

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



SYSTEM



REACTOR DESIGN

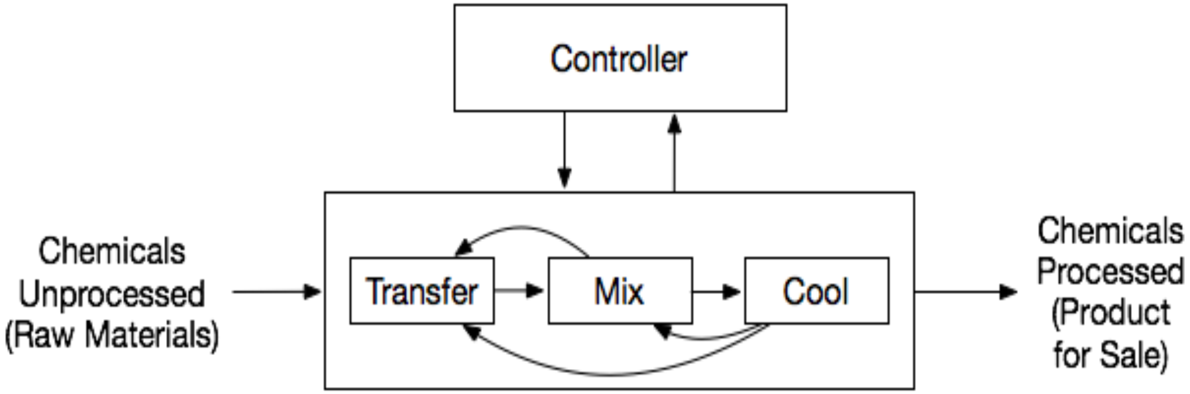
Mission Activity System Creation Confirms Our Understanding and Aids Control Structure Development

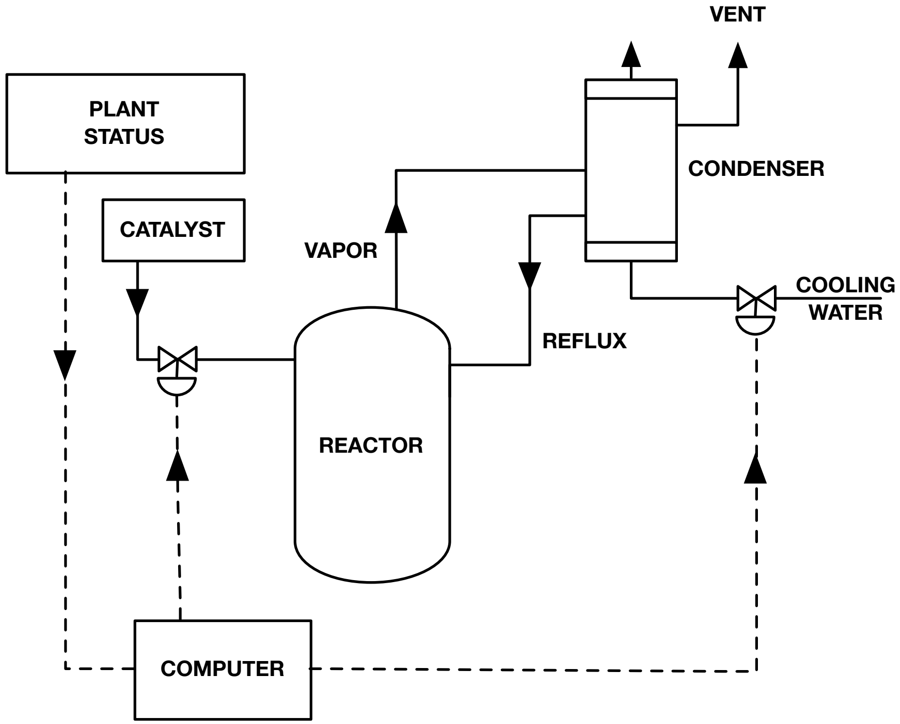
WYOUNG@MIT.EDU

Chemical Reactor - Problem

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

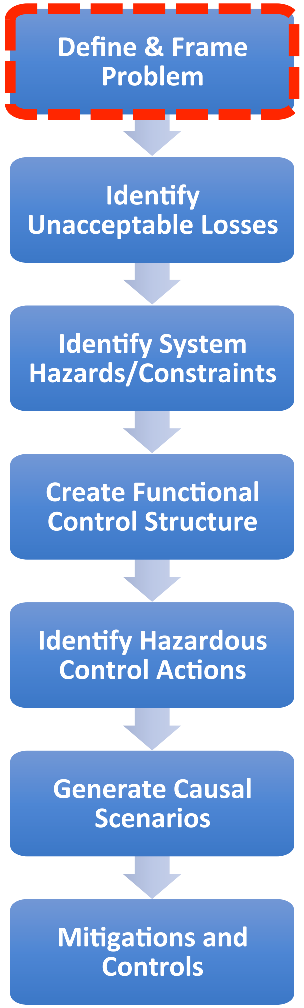
- **Toxic catalyst flows into reactor**
- **Chemical reaction creates heat, pressure**
- **Water and condenser provide cooling**





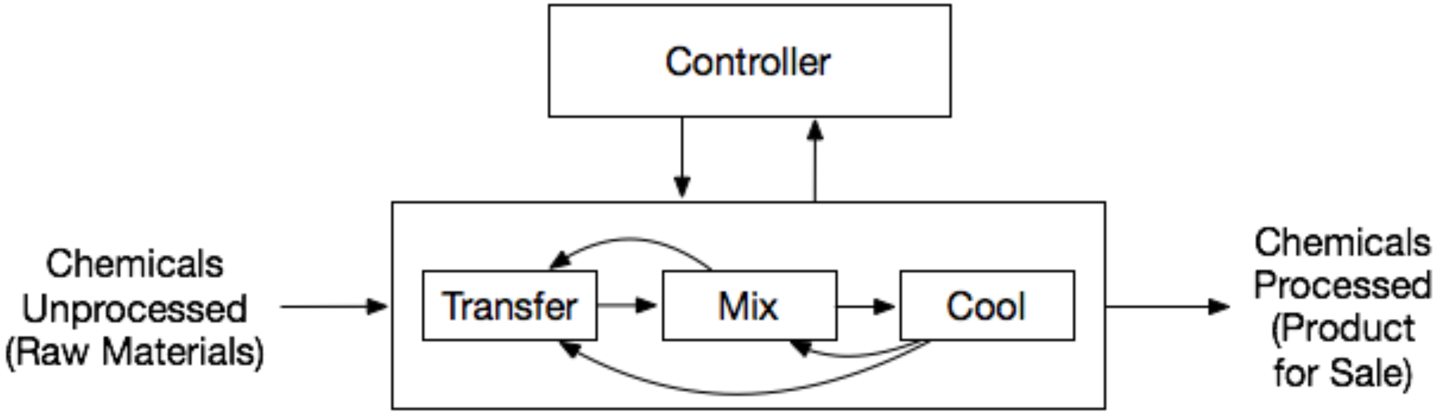
What does the system do? How does it accomplish it? Why does the system exist?

WYOUNG@MIT.EDU



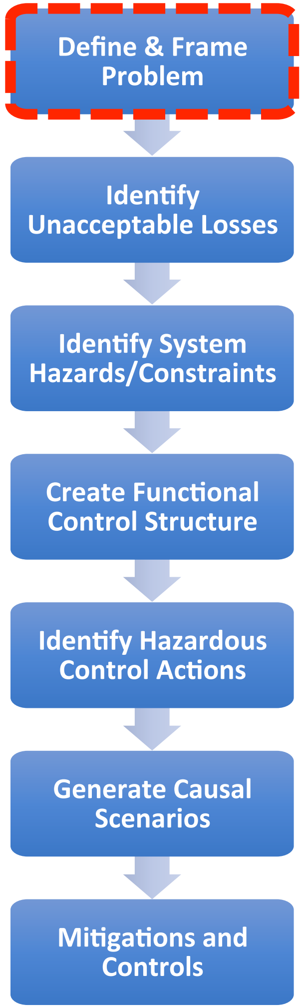
Chemical Reactor - Problem

- **Verbs in the description point to the key processes that must be controlled**
  - **Flow**
  - **Heat**
  - **Condensing**



What does the system do? How does it accomplish it? Why does the system exist?

WYOUNG@MIT.EDU

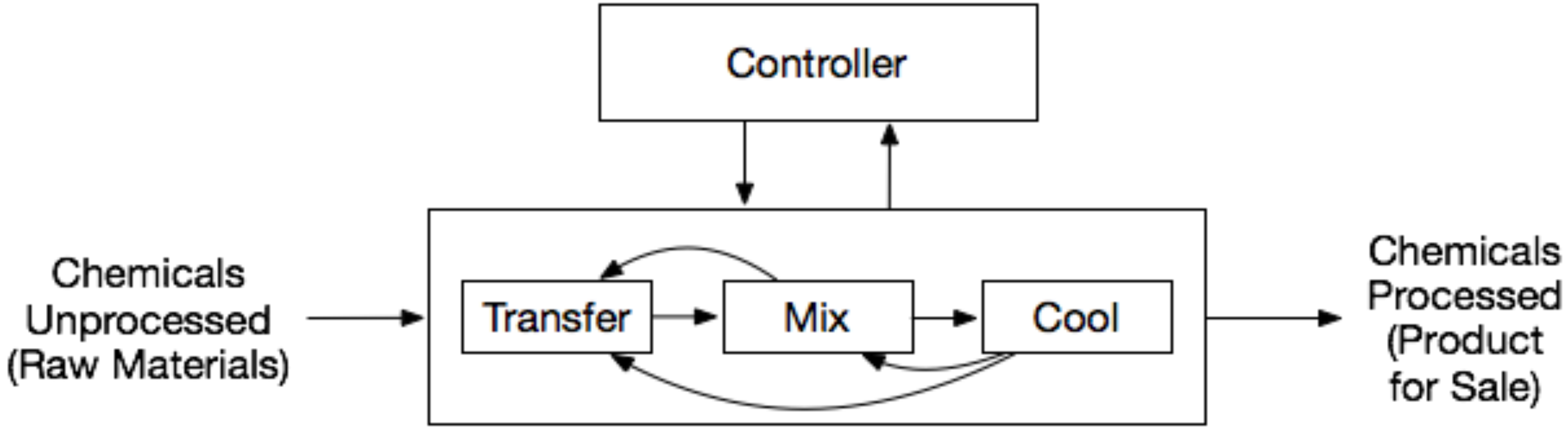


Chemical Reactor - Problem

A system to **contain and process chemicals**

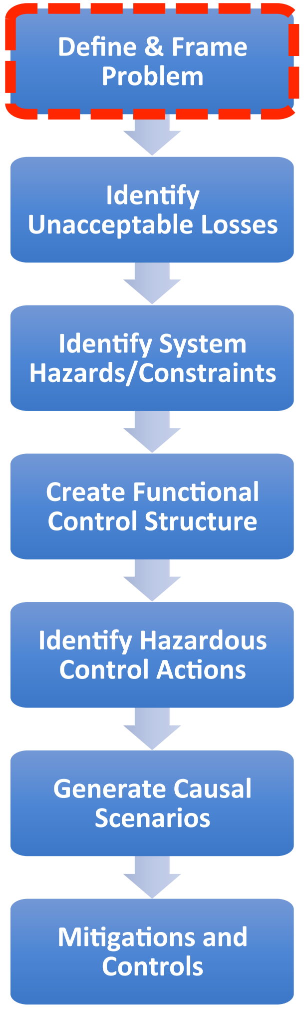
by means of **transferring, mixing, and cooling chemicals**

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



WYOUNG@MIT.EDU

Chemical Reactor - Problem

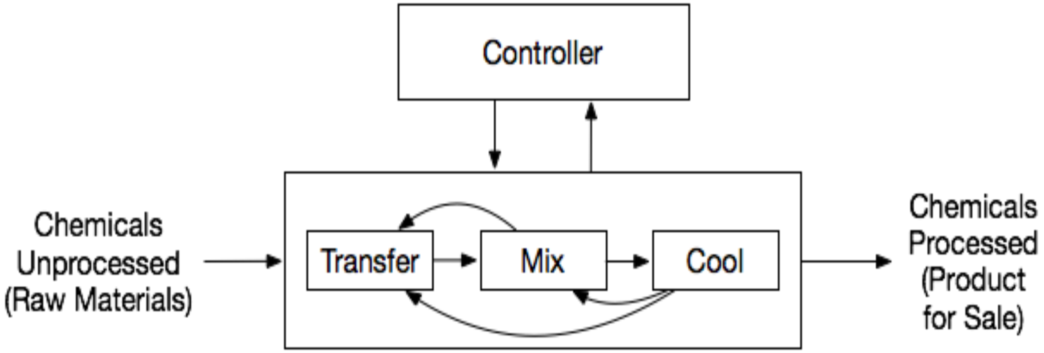


A system to **contain and process chemicals**

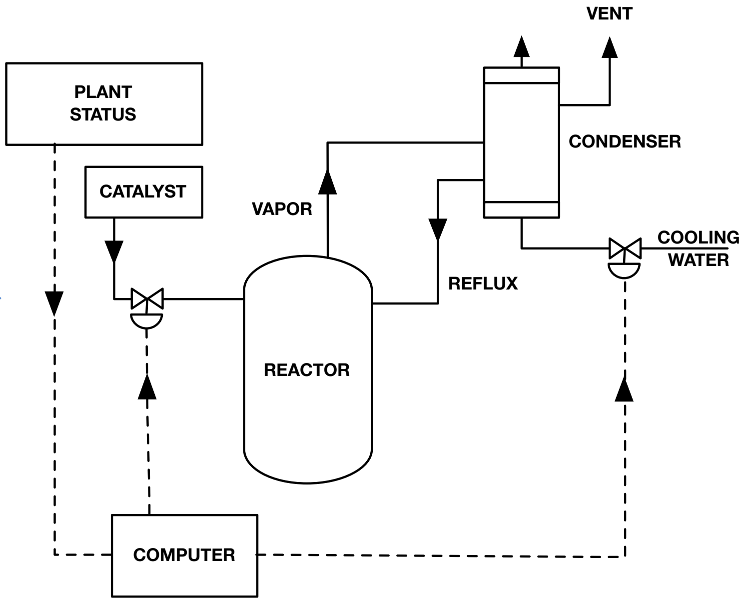
by means of **transferring, mixing, and cooling chemicals**

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

Abstract Functional



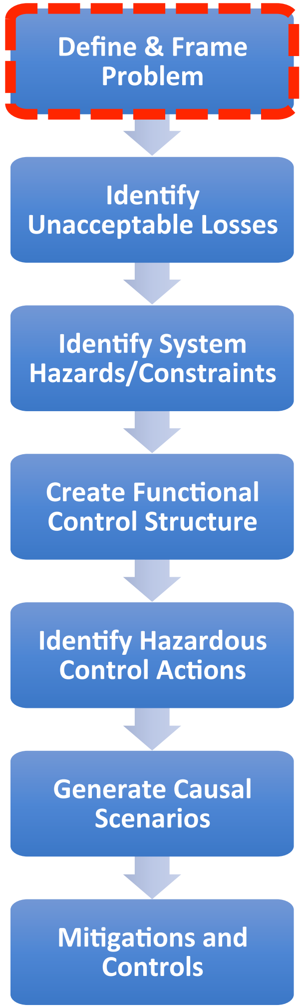
Physical (Architecture)



The Mission Activity System Description is Abstract & Functional, NOT physical

WYOUNG@MIT.EDU

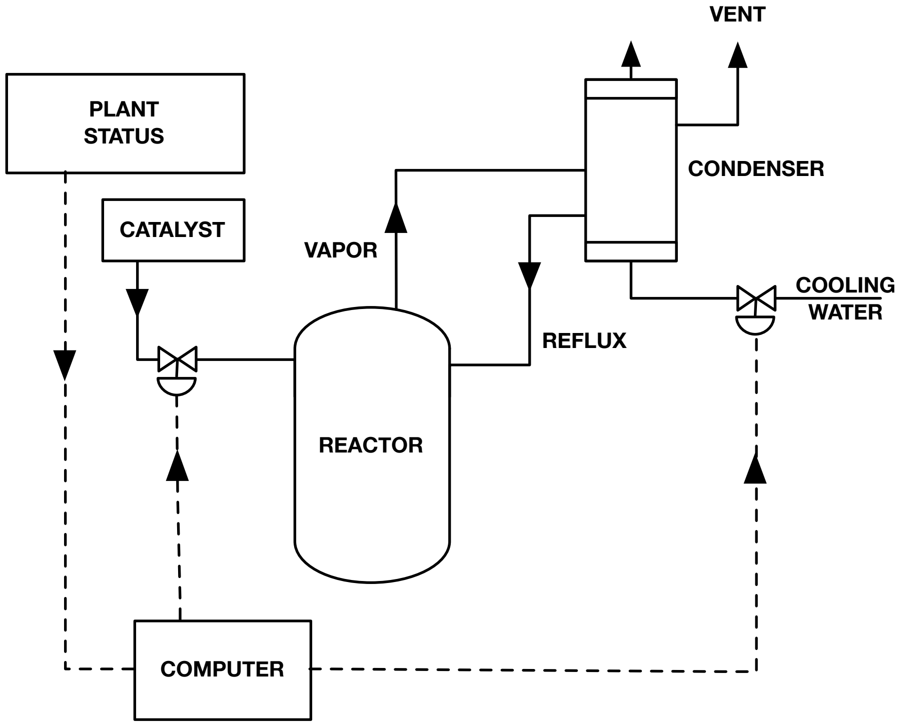
Chemical Reactor - Problem



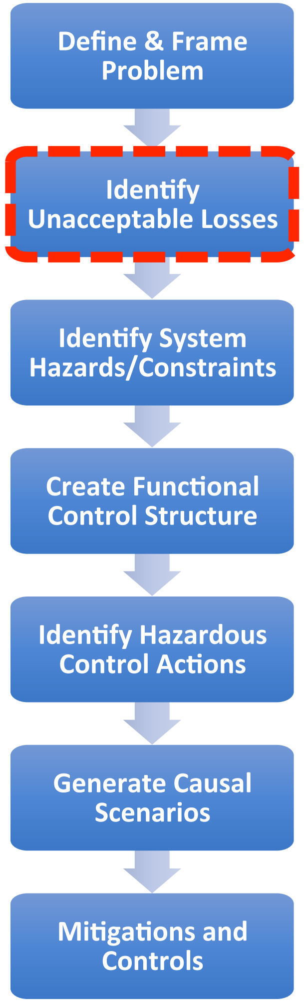
A system to **contain and process chemicals**

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

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

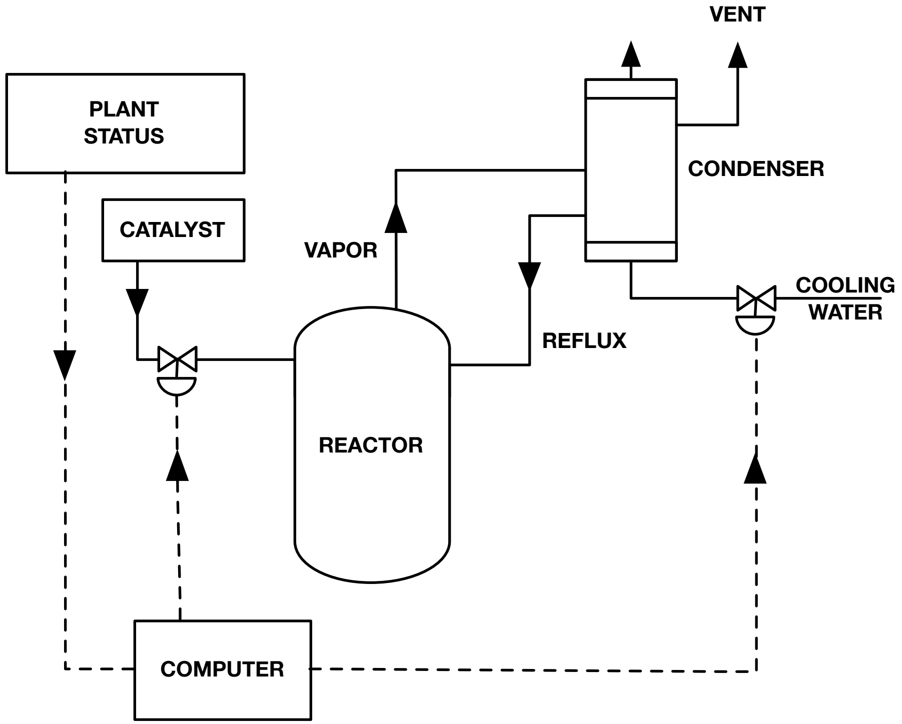


WYOUNG@MIT.EDU



Chemical Reactor - Losses

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

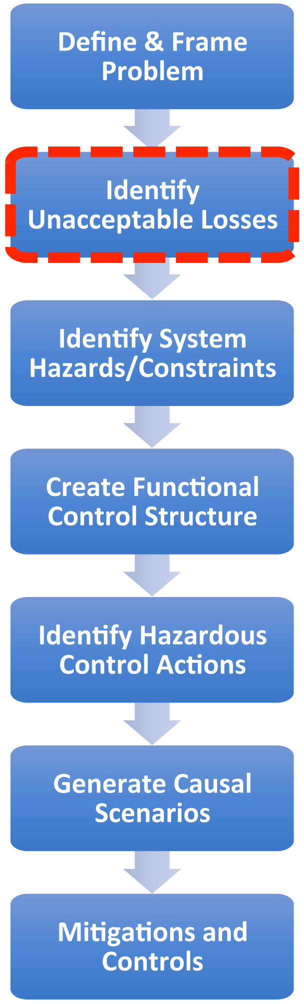


Are there other unacceptable losses?

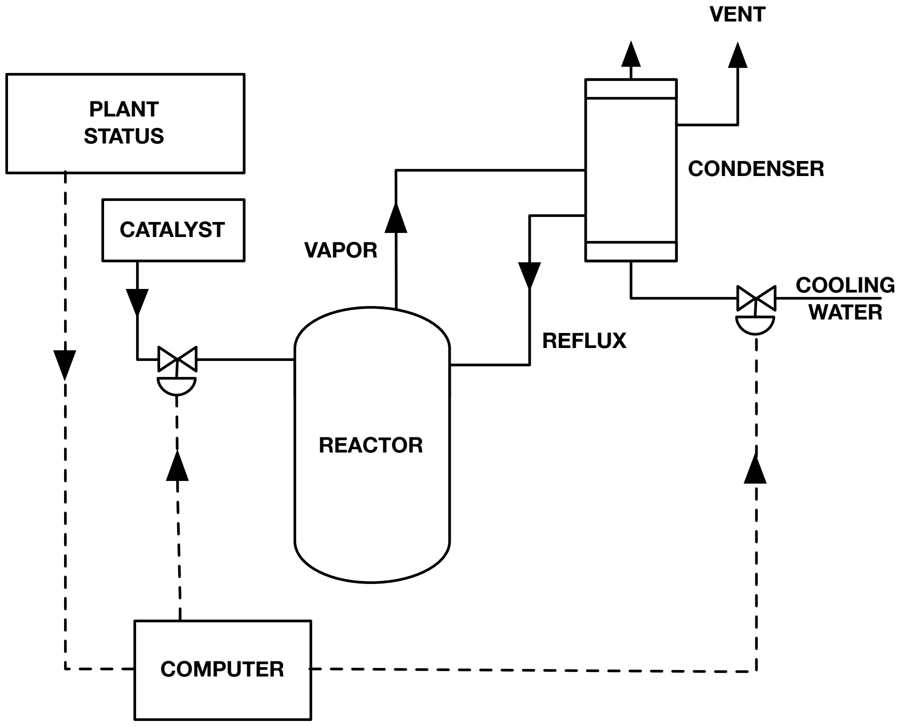
Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Chemical Reactor - Losses



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



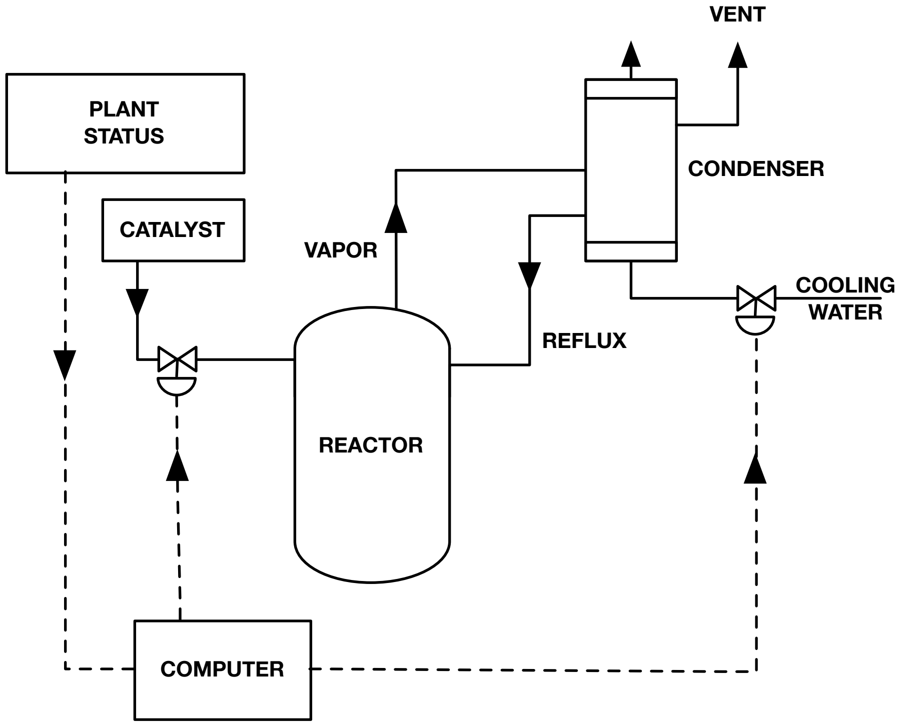
Are there unacceptable losses related to security?

WYOUNG@MIT.EDU

Chemical Reactor - Hazards

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

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?

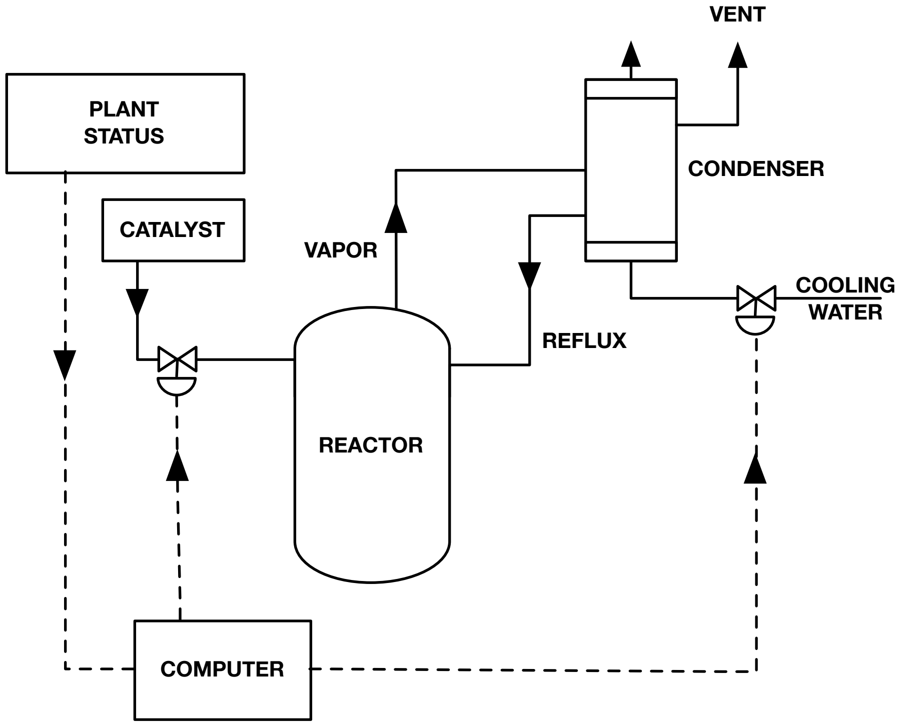
Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Chemical Reactor - Hazards

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

Hazard	**L1:**People die or become injured	**L2:** Production loss	
H1: Plant releases toxic chemicals			
H2: Plant is unable to produce chemical			



Hazards cross check

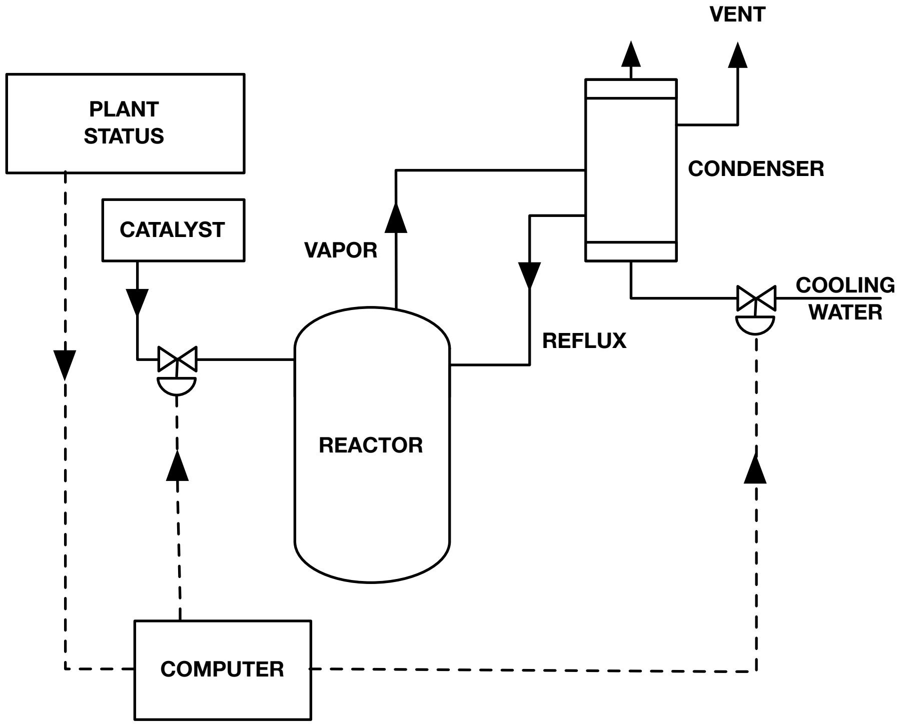
Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Chemical Reactor - Hazards

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

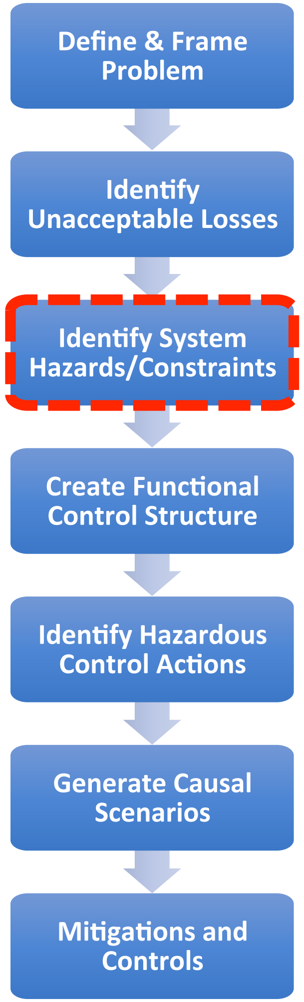
Hazard	Safety Constraint
H1: Chemicals inadvertently released	C1:
H2: ??	



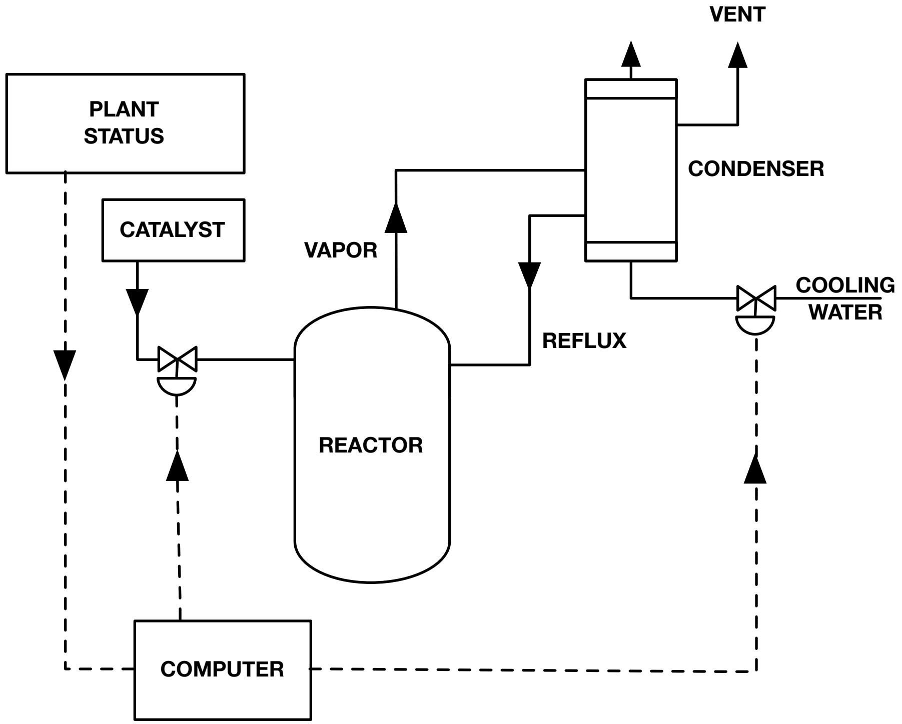
What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss?

WYOUNG@MIT.EDU

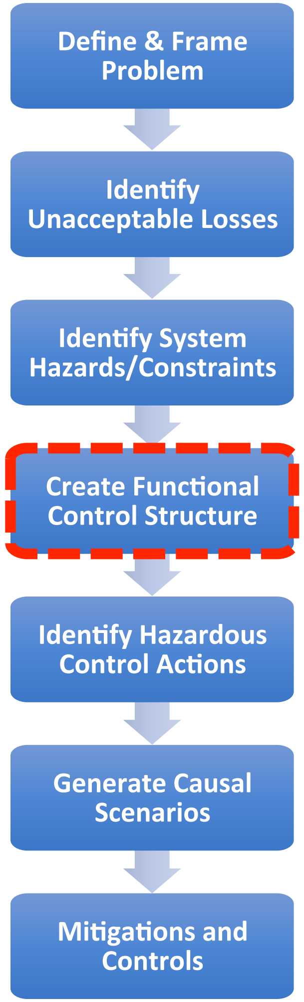
Chemical Reactor - Hazards



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?



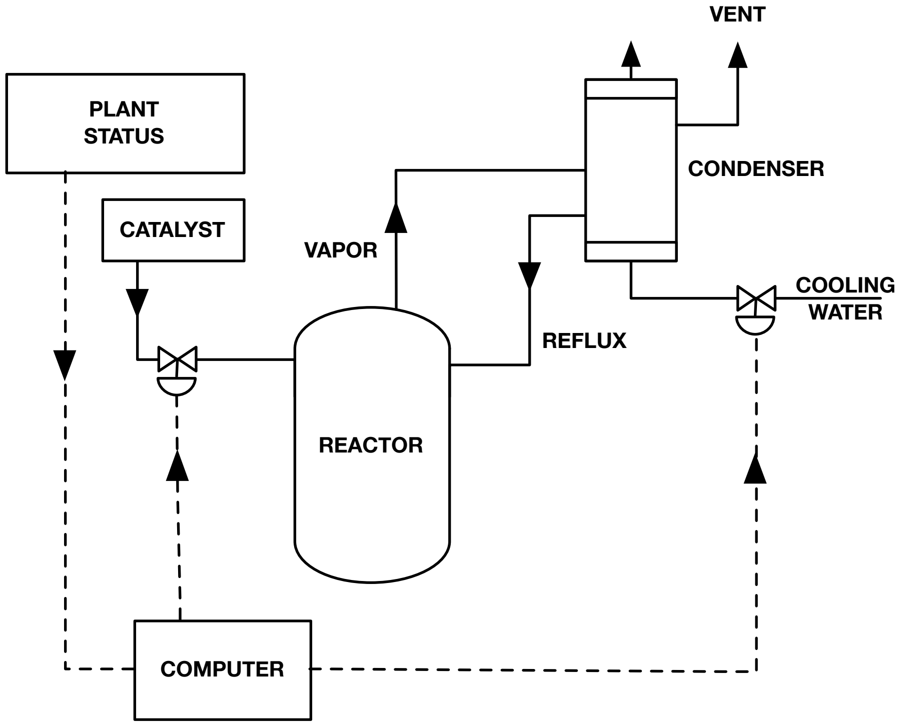
Chemical Reactor – Control Structure

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.**

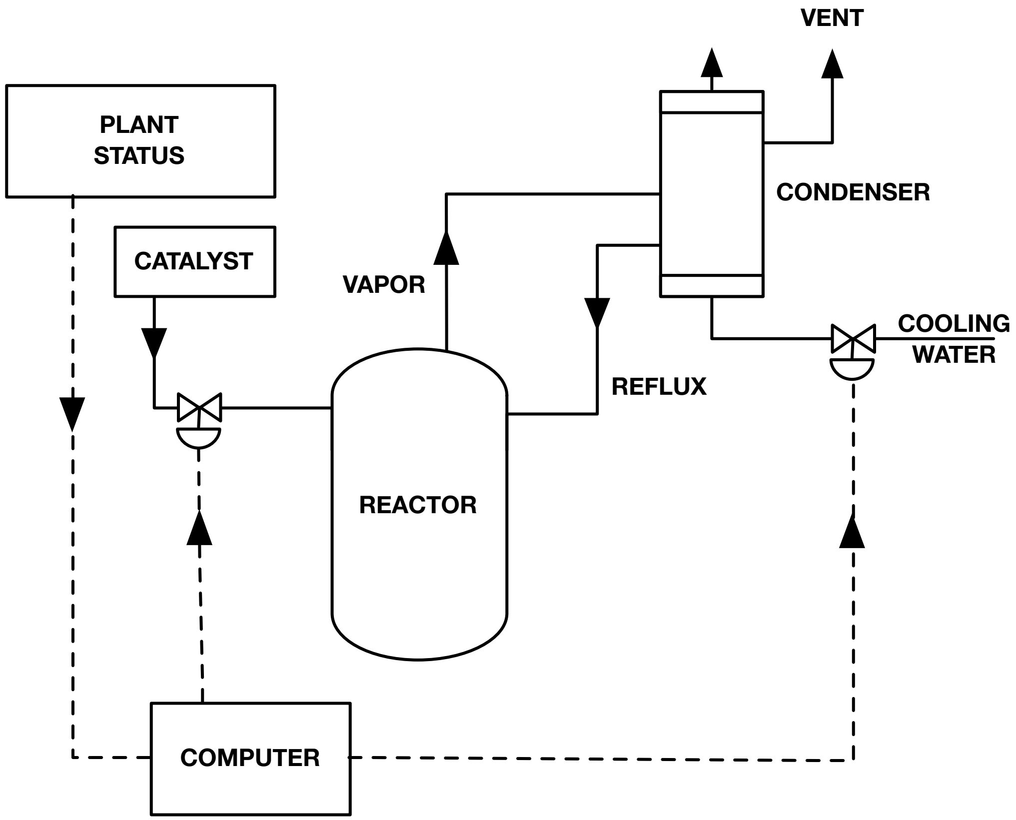
- **What Processes Must Be Controlled in Order to Accomplish Business or Mission Objective**
  - **Transfer and mixing catalyst**
  - **Cooling reflux**
- **Use Insights to understand Controller requirements**



Chemical Reactor – Control Structure

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

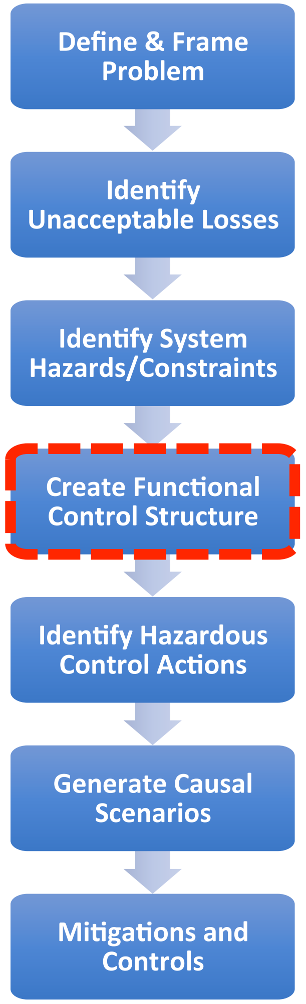
Need Functional Equivalent



Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

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**

WYOUNG@MIT.EDU

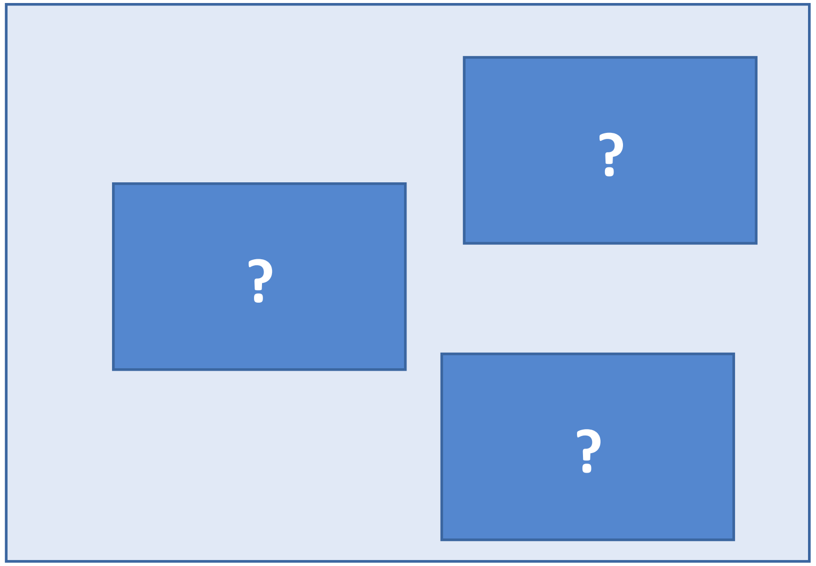
Chemical Reactor – Control Structure

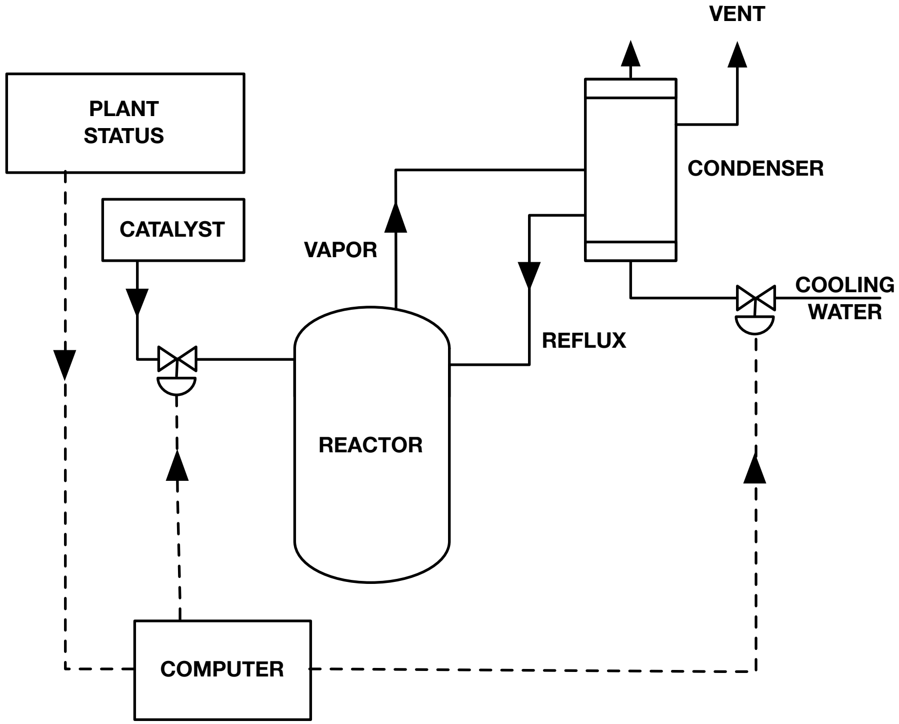
- Define & Frame Problem
- Identify Unacceptable Losses
- Identify System Hazards/Constraints
- **Create Functional Control Structure**
- Identify Hazardous Control Actions
- Generate Causal Scenarios
- Mitigations and Controls

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

WYOUNG@MIT.EDU

Chemical Reactor – Control Structure

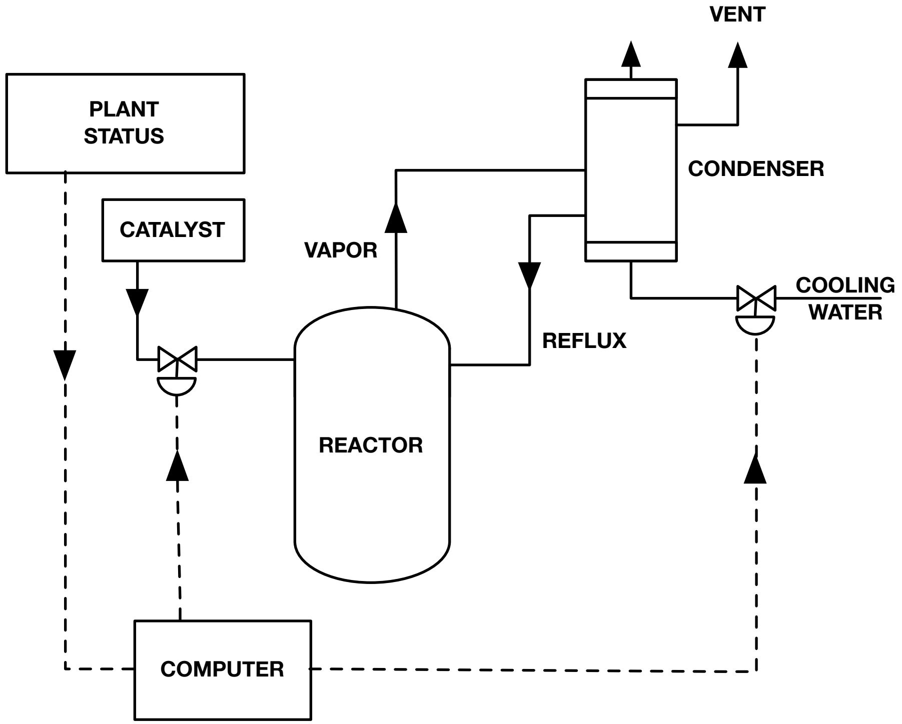
- Define & Frame Problem
- Identify Unacceptable Losses
- Identify System Hazards/Constraints
- Create Functional Control Structure
- Identify Hazardous Control Actions
- Generate Causal Scenarios
- Mitigations and Controls

A system to **contain and process chemicals**

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

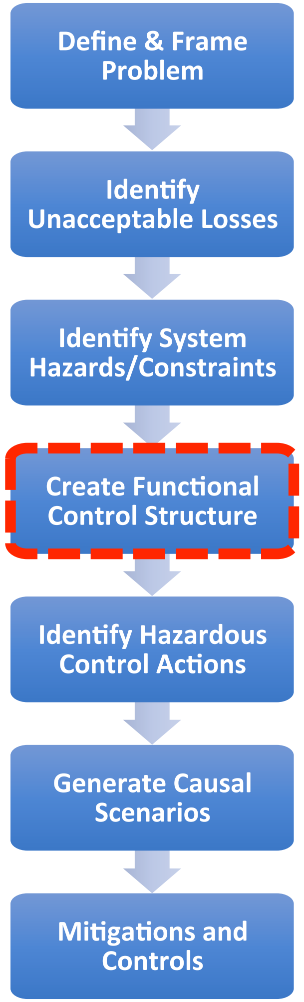
in order contribute to **production of chemicals sold by the company.**

High-Level Functional Activity	Model Elements	Description

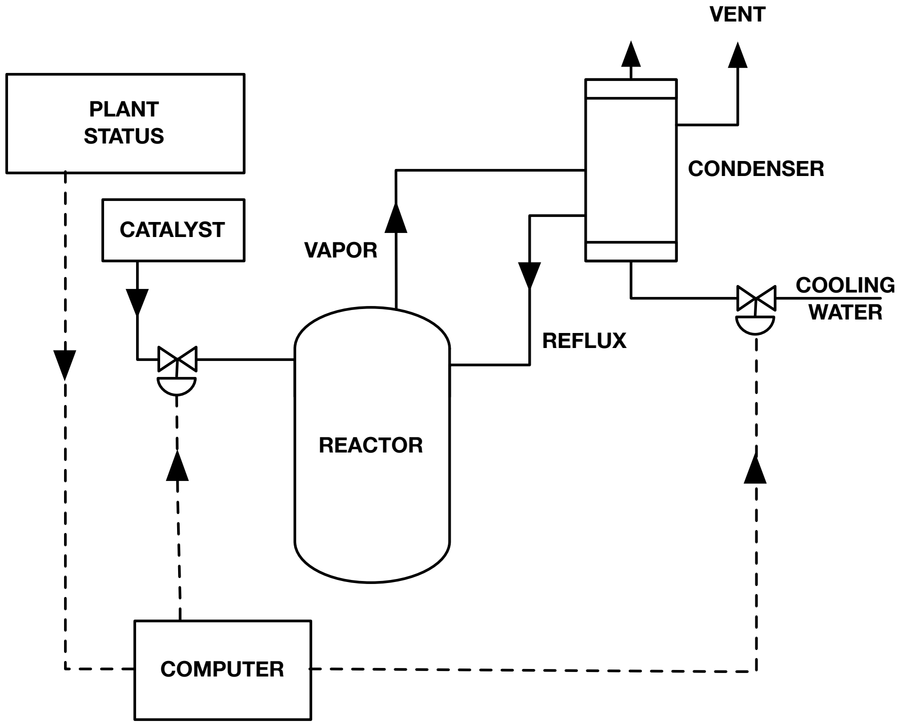


WYOUNG@MIT.EDU

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	

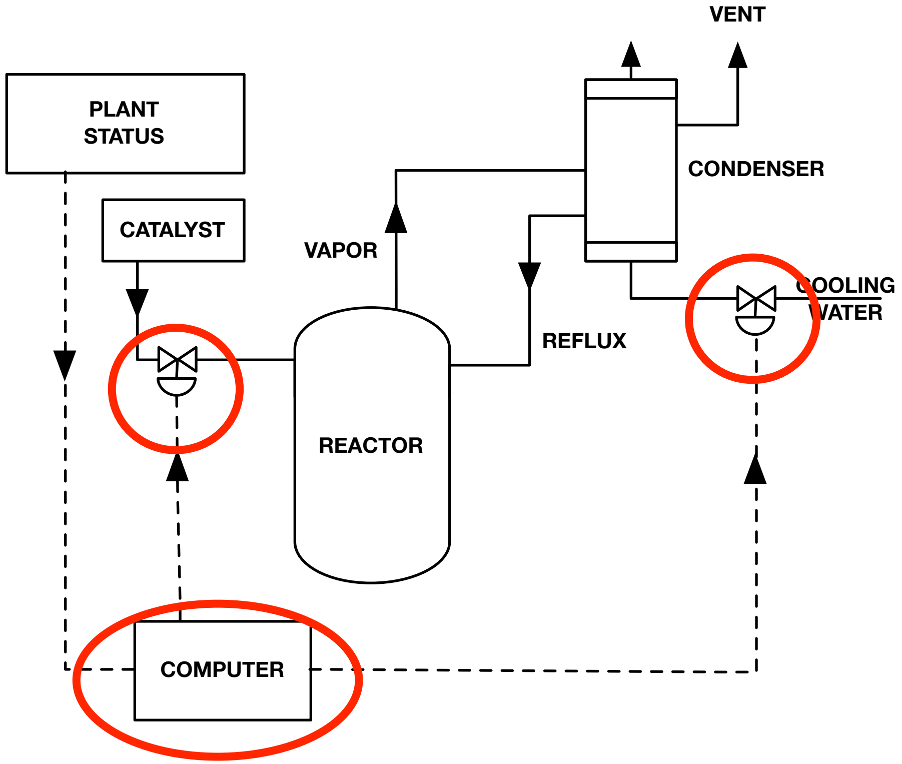


Chemical Reactor – Control Structure

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

Key Activity: Transfer

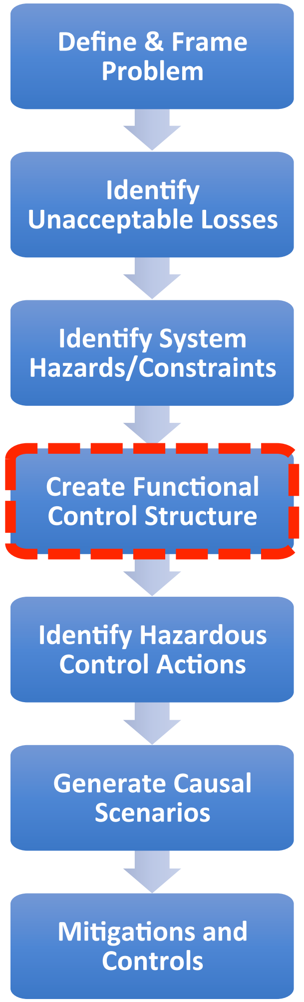
Element	Responsibility Description
Operator	• Initiate process • Monitor progress • Manually Intervene
Computer	• Control valves • Report status
Valves	• Open/close on command • Fail open? / Fail closed?

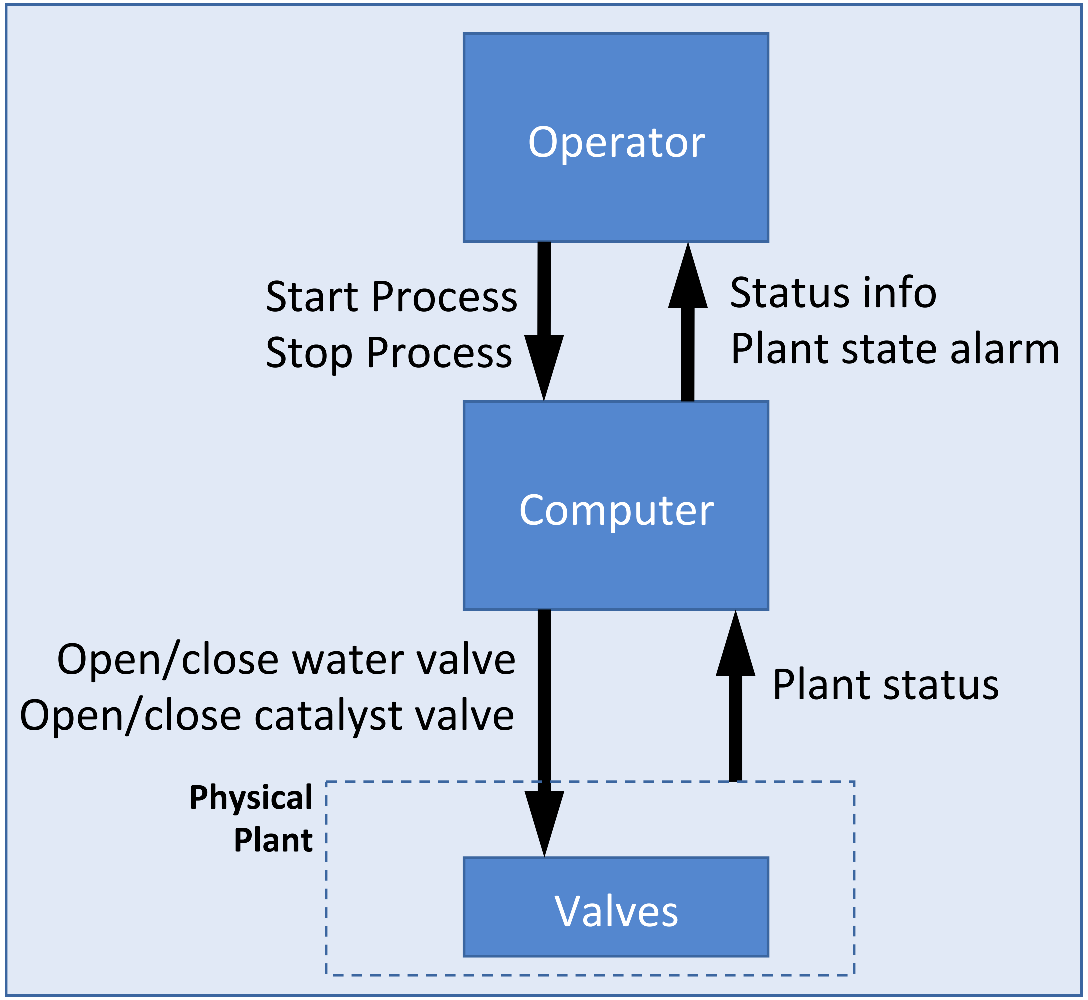


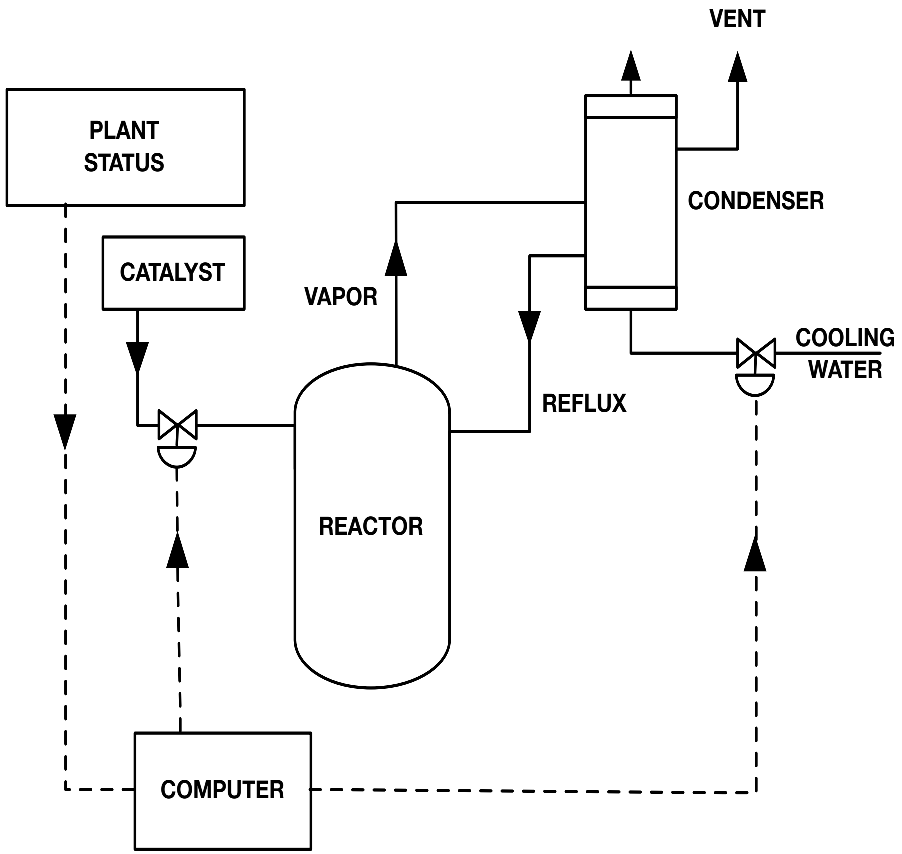
Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Chemical Reactor – Control Structure

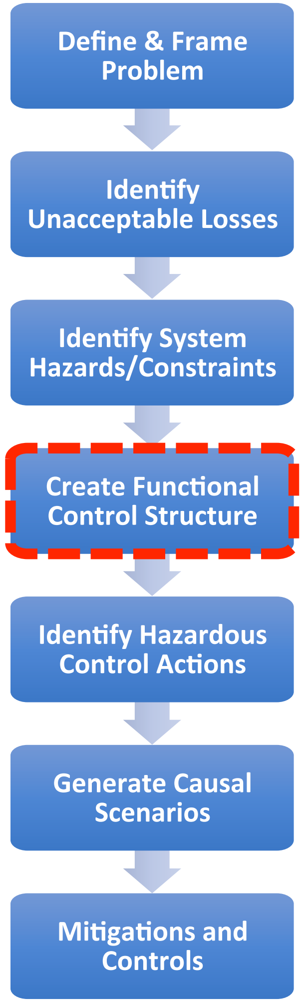


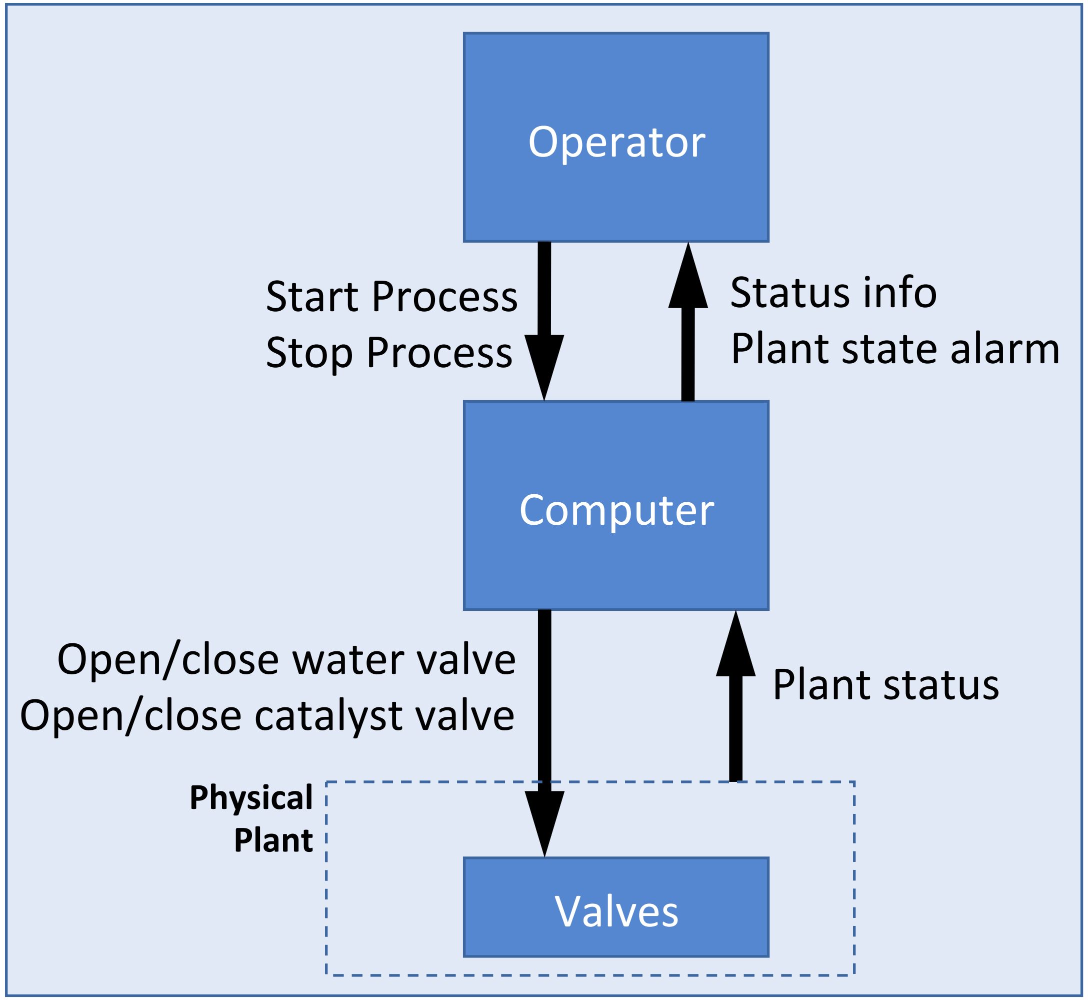


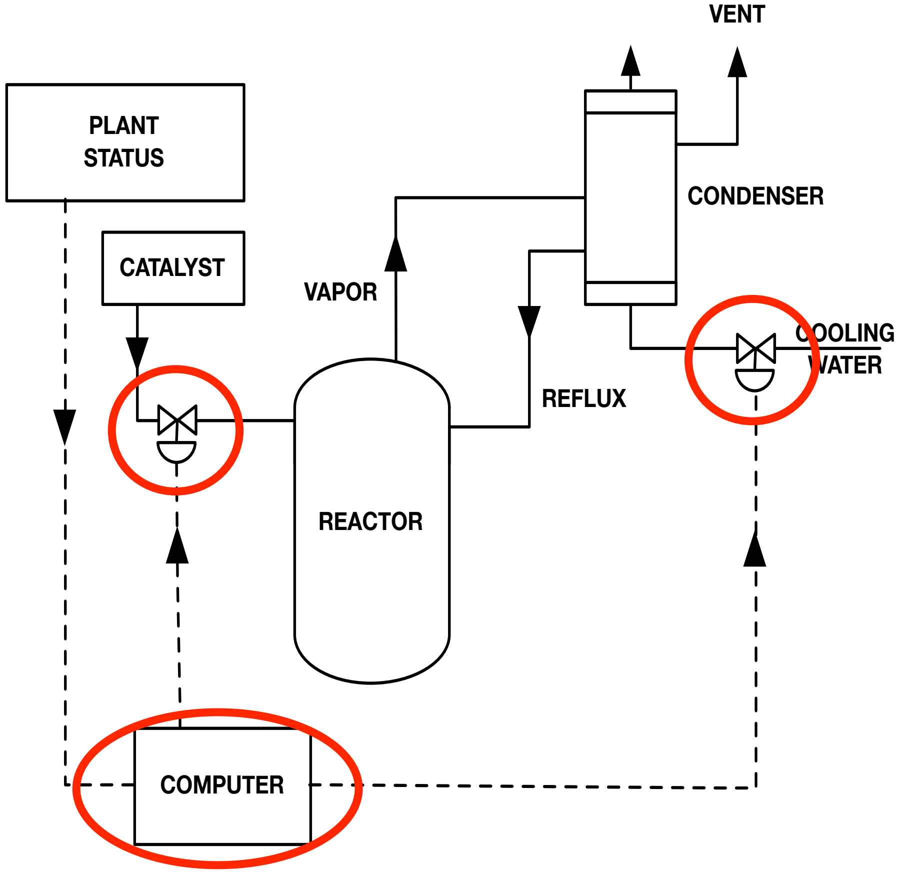


WYOUNG@MIT.EDU

Chemical Reactor – Control Structure





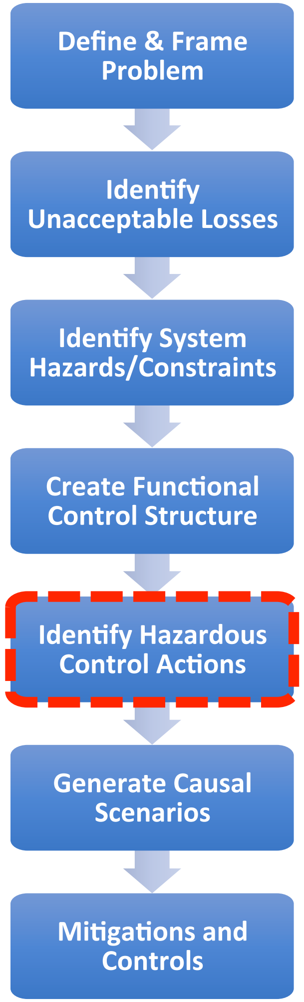


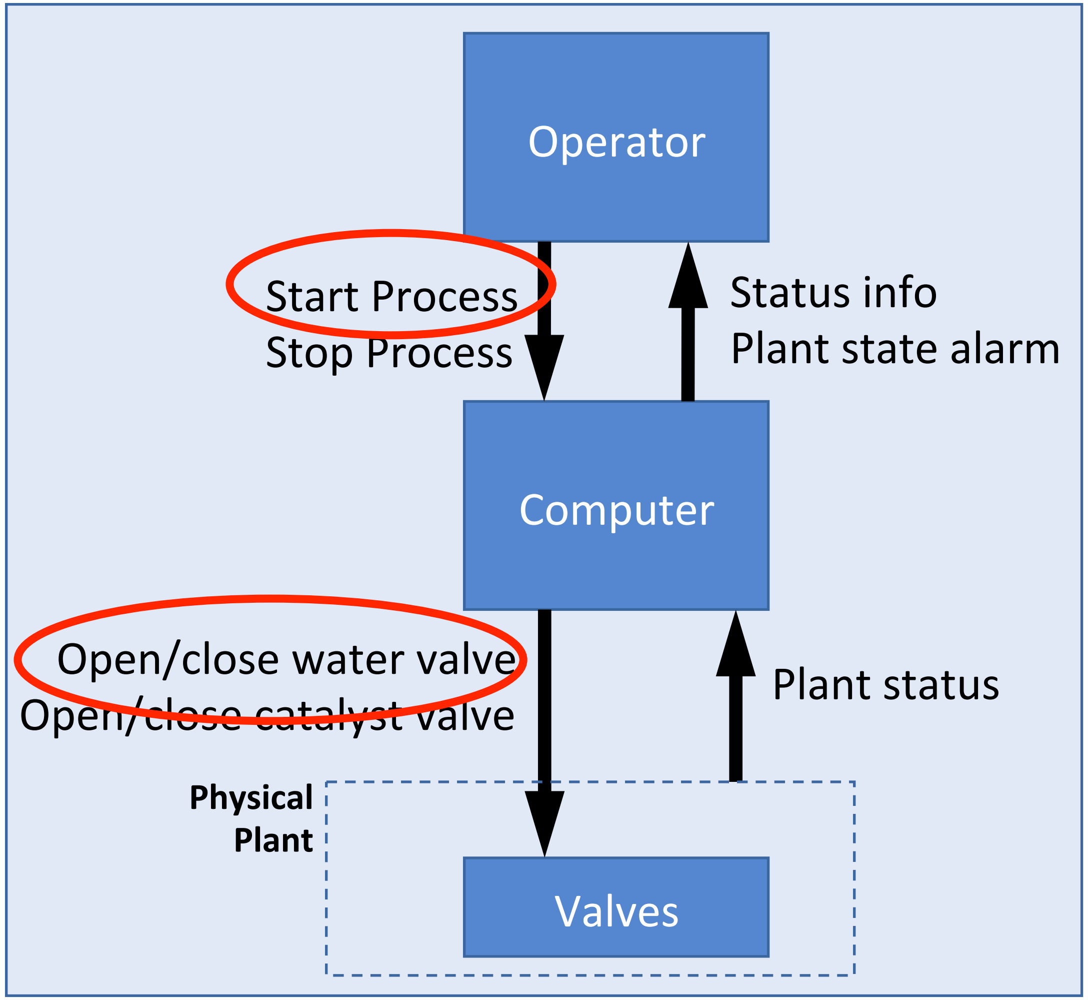
What are the unacceptable losses ?

Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Chemical Reactor – HCAs (Unsafe / Unsecure)





HCA - Hazardous Control Action

What are the unacceptable losses ?

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				

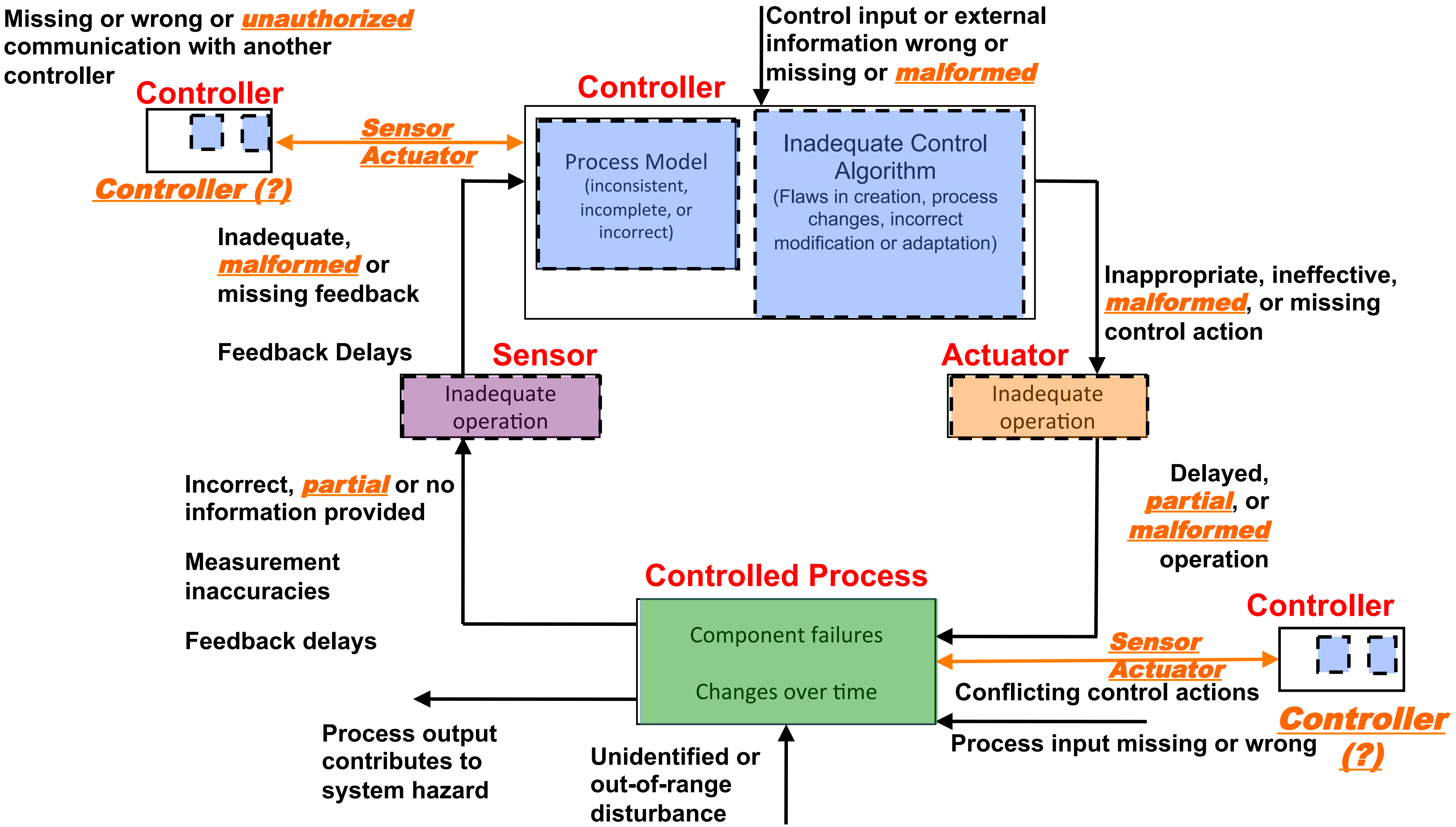
Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Chemical Reactor: Hazardous Control Actions (HCA)

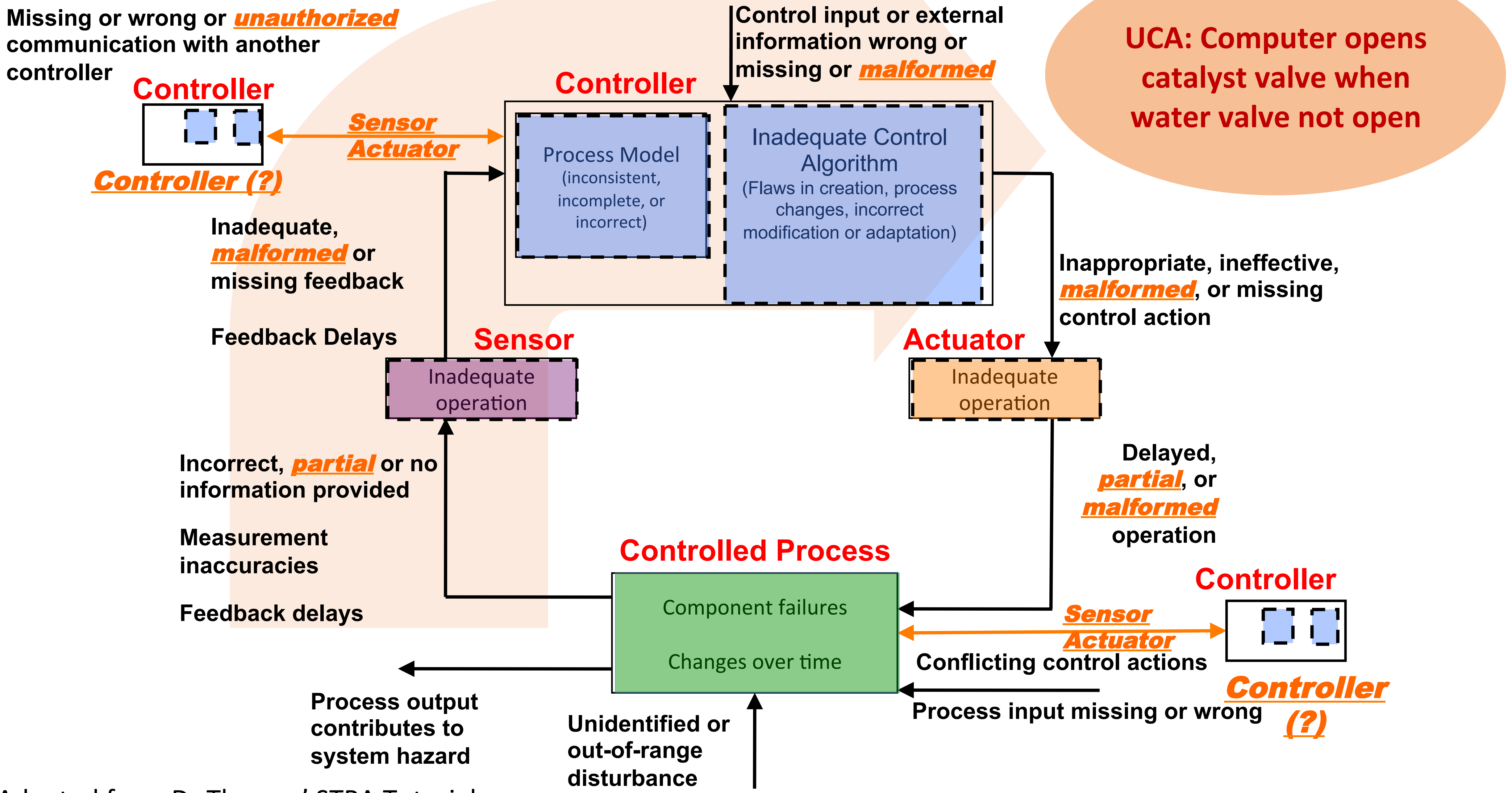
Control Action	Not providing causes hazard	Providing causes hazard	Incorrect Timing or Order	Stopped too soon or applied too long
CA1: Start Process		Operator provides command when condenser water valve not functioning	Operator manually overrides valves and computer misses signal	
CA2: Open Water Valve	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



WYOUNG@MIT.EDU

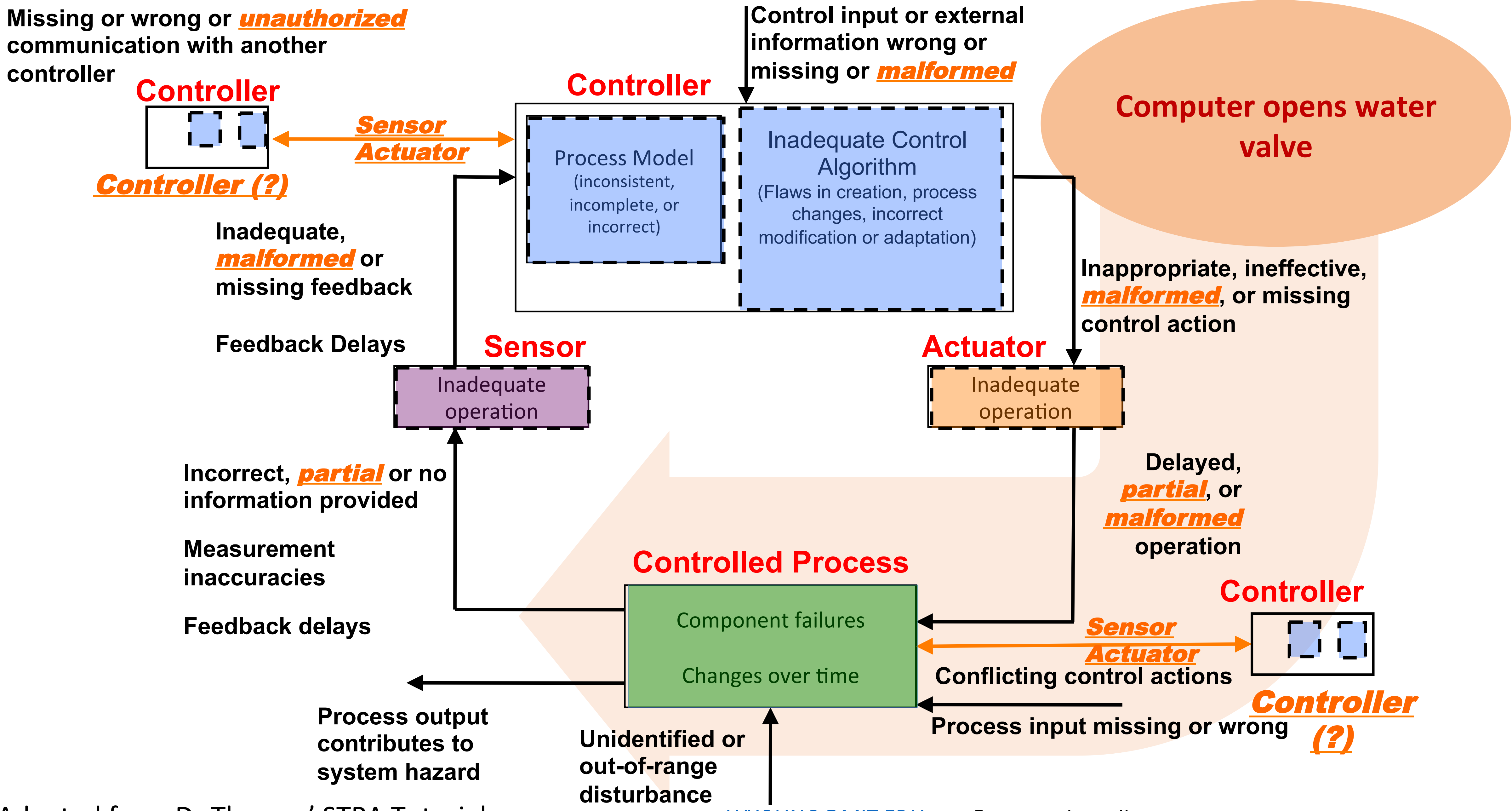
Step 2: Potential causes of UCAs



Adapted from Dr Thomas' STPA Tutorial

WYOUNG@MIT.EDU

Step 2: Potential control actions not followed



WYOUNG@MIT.EDU

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

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.

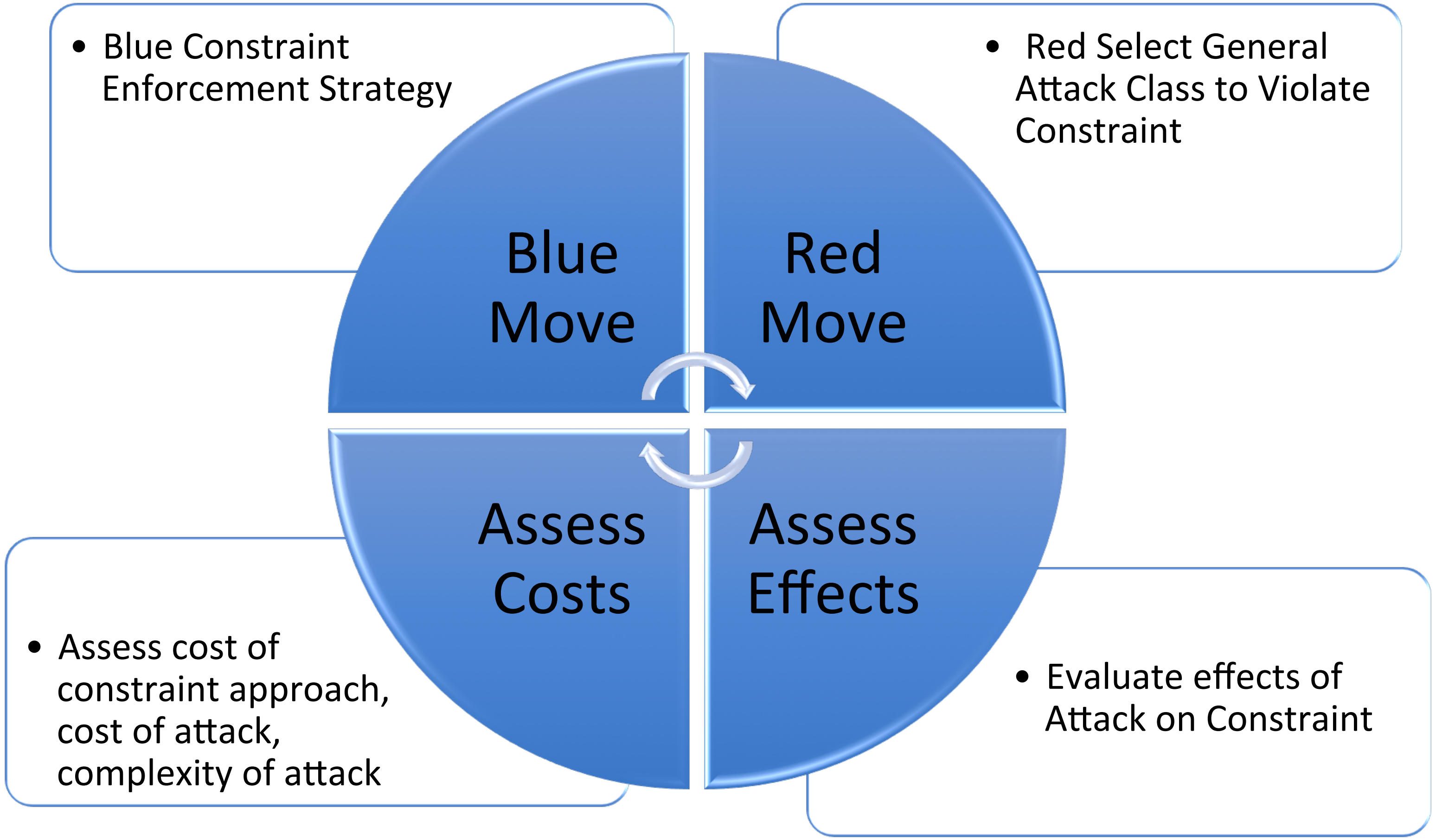
Adapted from Dr Thomas' STPA Tutorial

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

Wargaming



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

WYOUNG@MIT.EDU

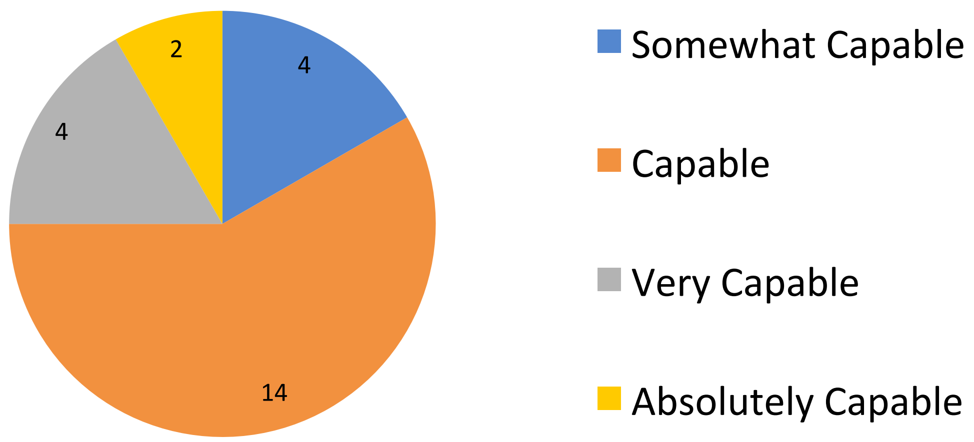
Lessons Learned Applying STPA-Sec

- **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"**

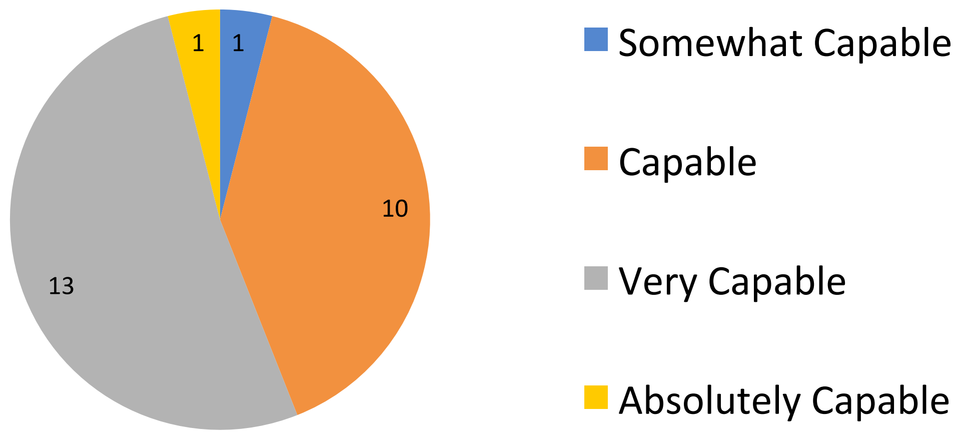
STPA-Sec is NOT a silver bullet, but appears to enable increased rigor "Left of Design"

Recent Self-Reported Assessment Results

Before Training : Ability to Develop Mitigation Strategy



After Training : Ability to Develop Mitigation Strategy



WYOUNG@MIT.EDU

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

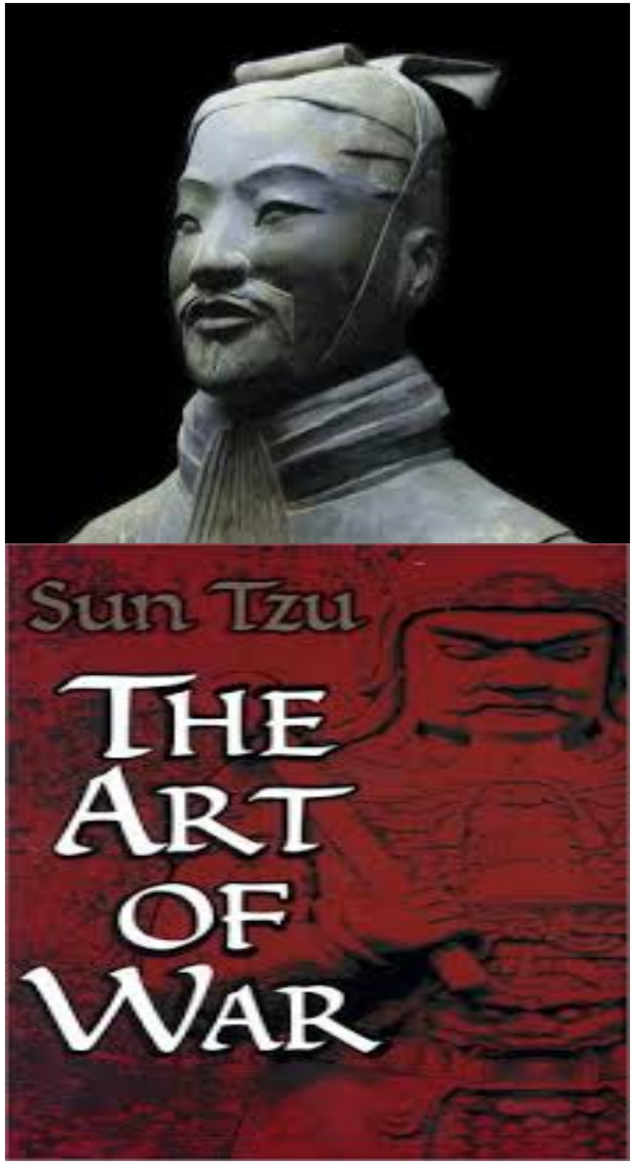
- **Must think carefully about defining the security problem**
- **Perfectly solving the wrong security problem doesn't really help**
- **STPA-Sec provides a means to clearly link security to the broader mission or business objectives**
- **STPA-Sec does not replace existing security engineering methods,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



WYOUNG@MIT.EDU

QUESTIONS ??

My Contact Information

WYOUNG@MIT.EDU

Special Thanks

Dr John Thomas for providing the baseline reactor problem framework and initial STPA analysis