Intro to Systems Theoretic Process Analysis (STPA)

Dr. John Thomas

Systems approach to safety engineering (STAMP)

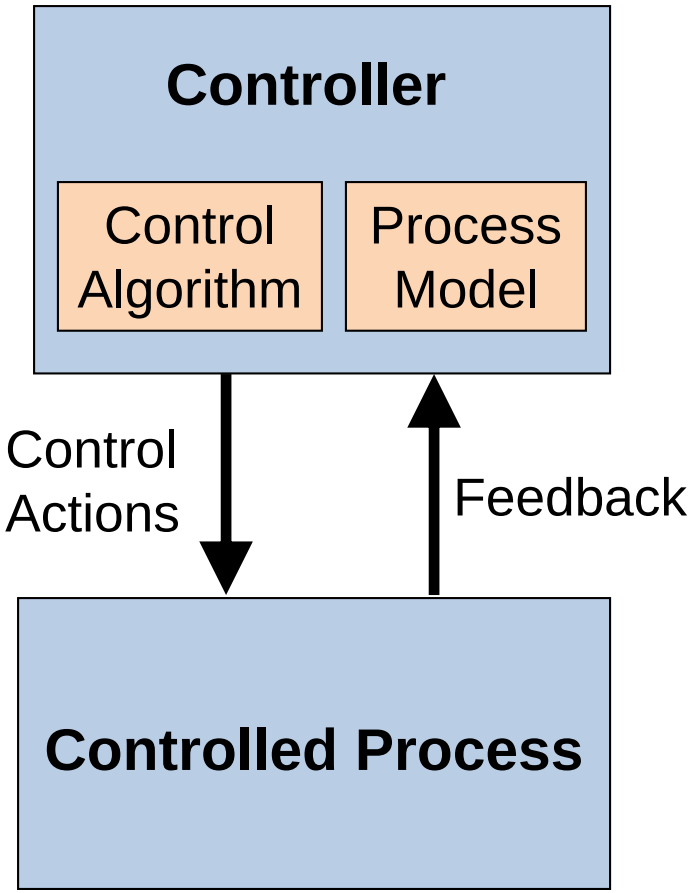
STAMP Model

- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not just a failure problem
- Prevent accidents by enforcing constraints on component behavior and **interactions**
- Captures more causes of accidents:
  - Component failure accidents
  - Unsafe interactions among components
  - Complex human, software behavior
  - Design errors
  - Flawed requirements
    - esp. software-related accidents

(Leveson, 2012)

©

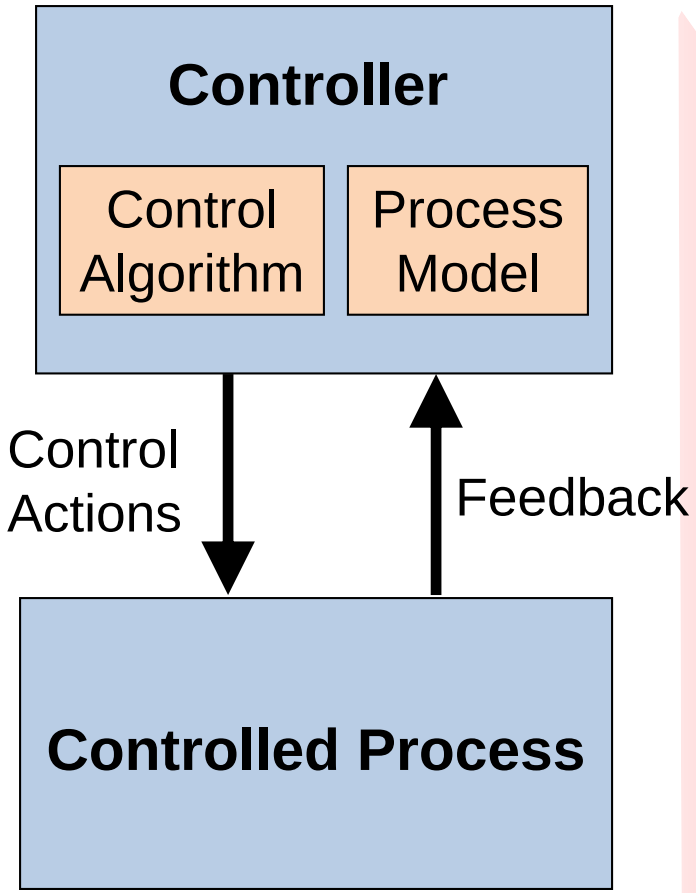
STAMP: basic control loop

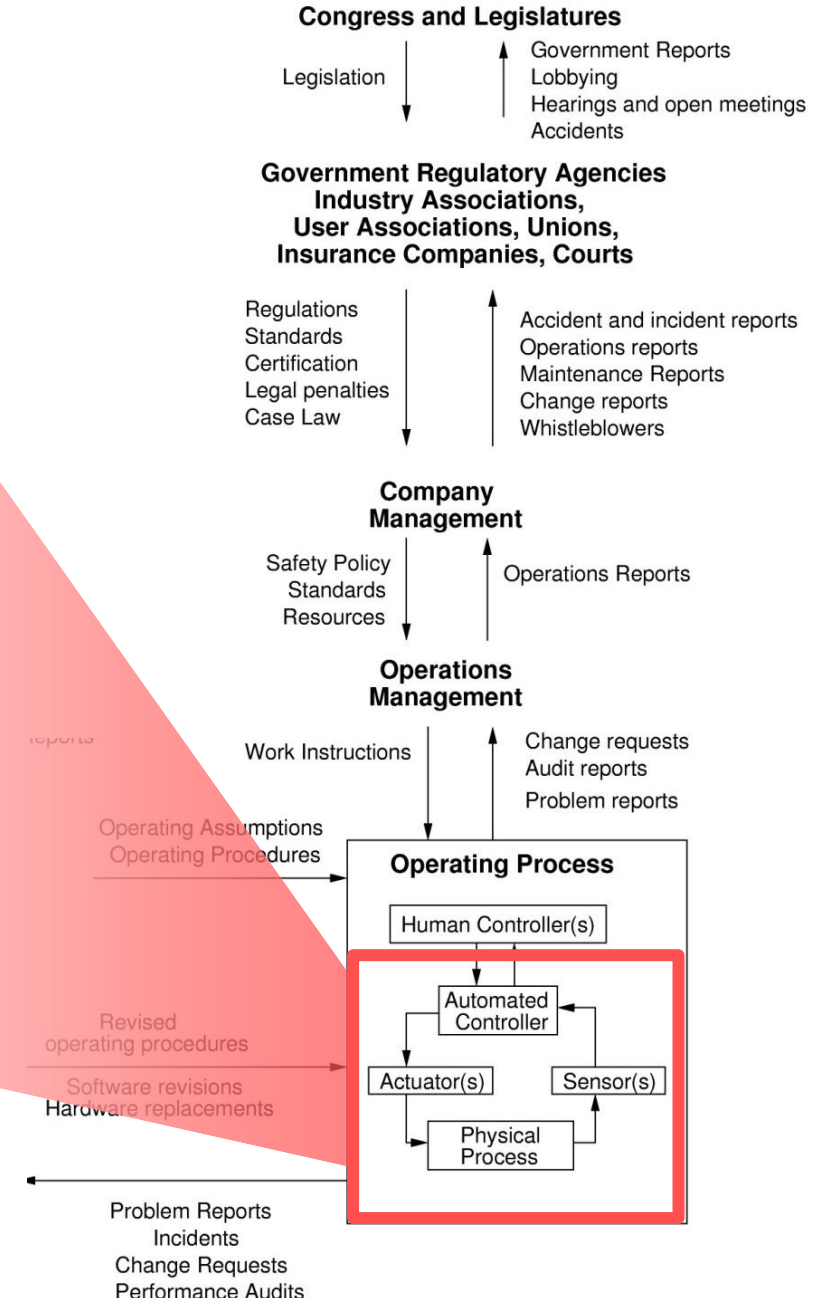


- Controllers use a **process model** to determine control actions
  - Accidents often occur when the process model is incorrect
- A good model of both software and human behavior in accidents
- Four types of **unsafe control actions**:
  1) Control commands required for safety are not given
  2) Unsafe ones are given
  3) Potentially safe commands but given too early, too late
  4) Control action stops too soon or applied too long

©

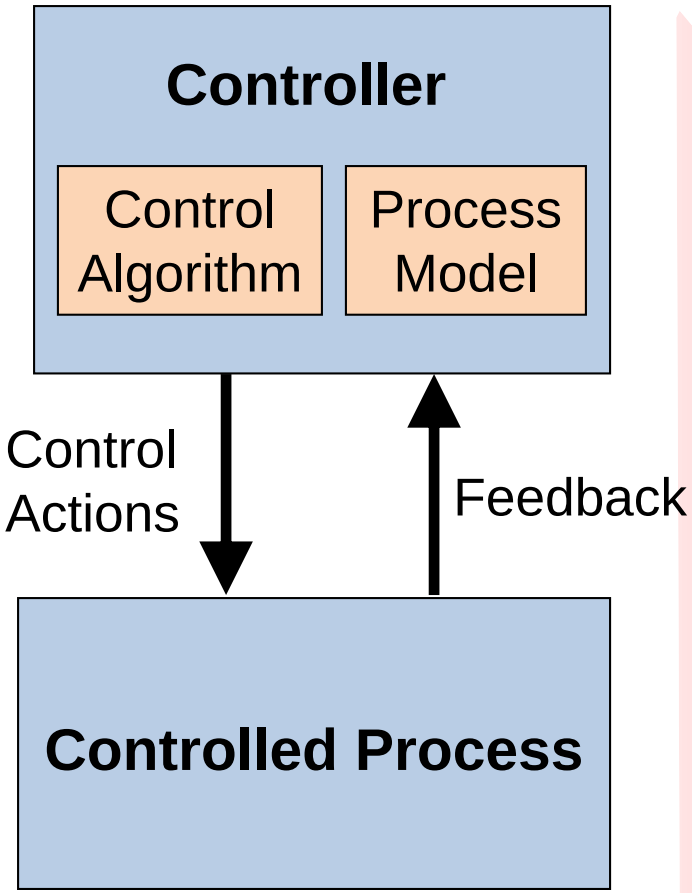
Using control theory

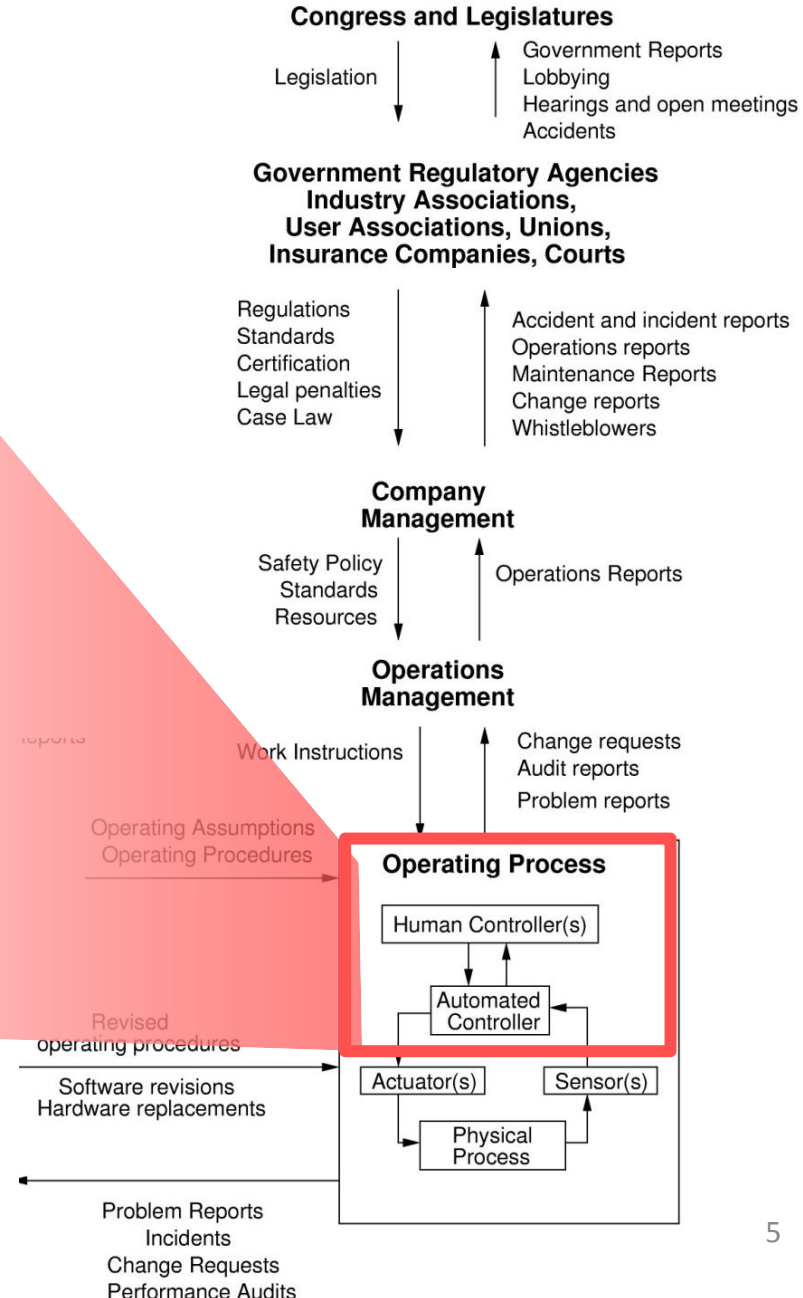




©

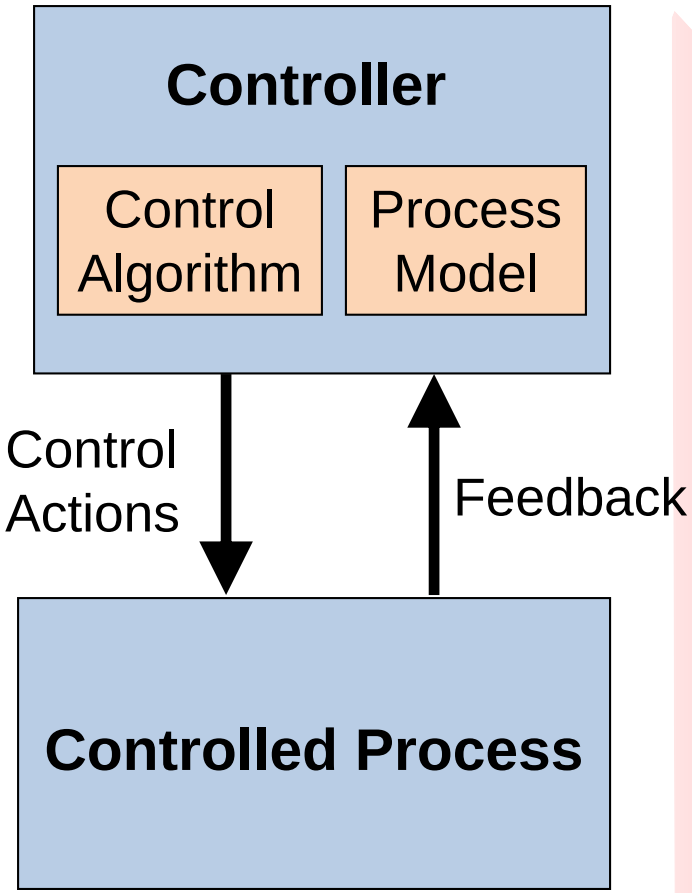
Using control theory

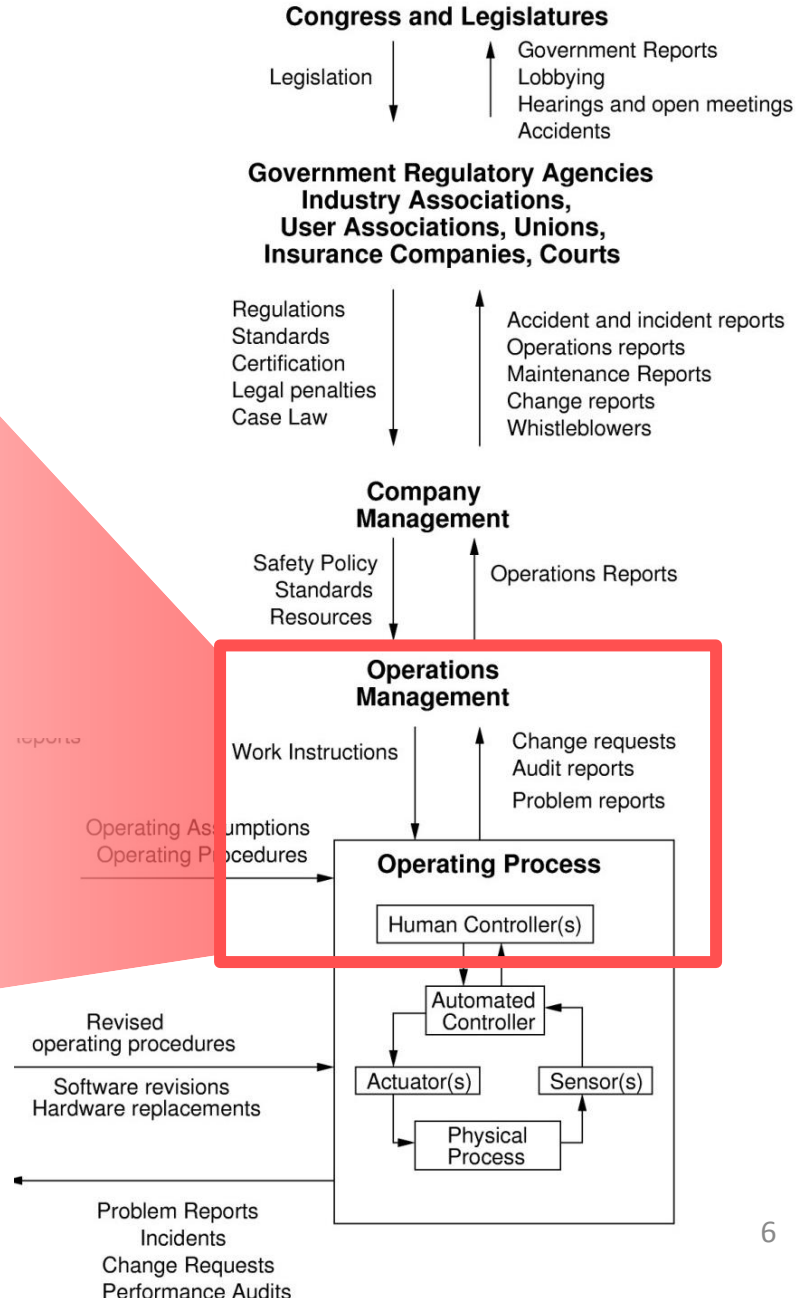




©

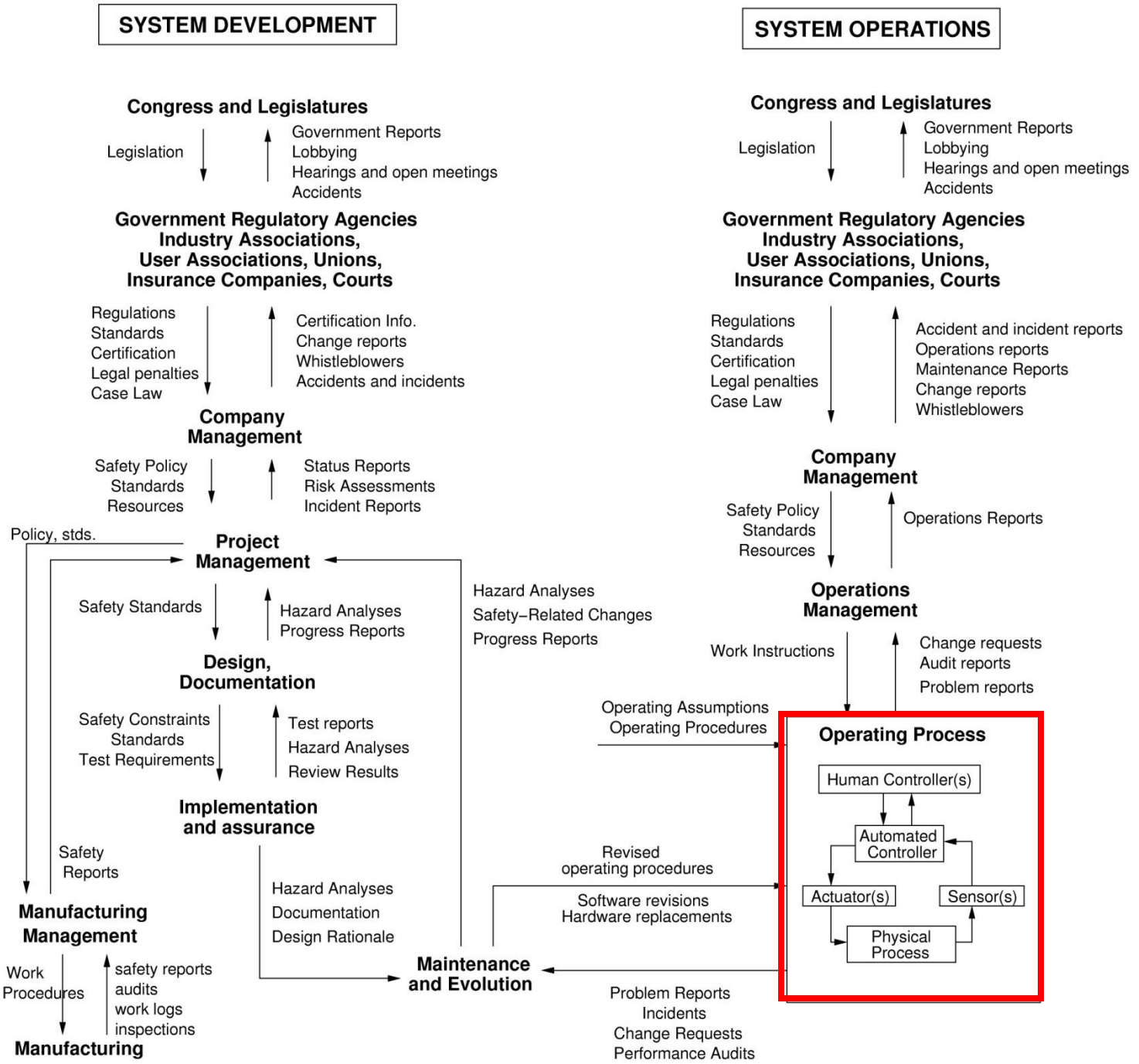
Using control theory





©

Example Safety Control Structure



(Leveson, 2012)

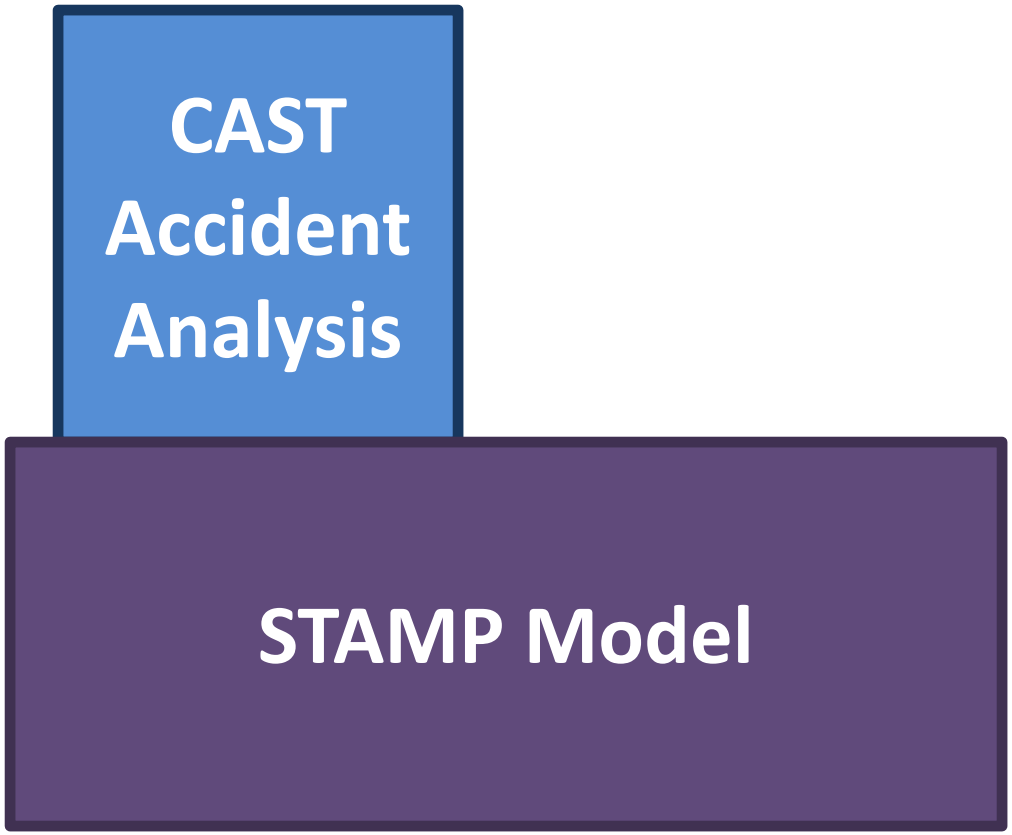
STAMP and STPA

STAMP Model

Accidents are caused by inadequate control

©

STAMP and STPA

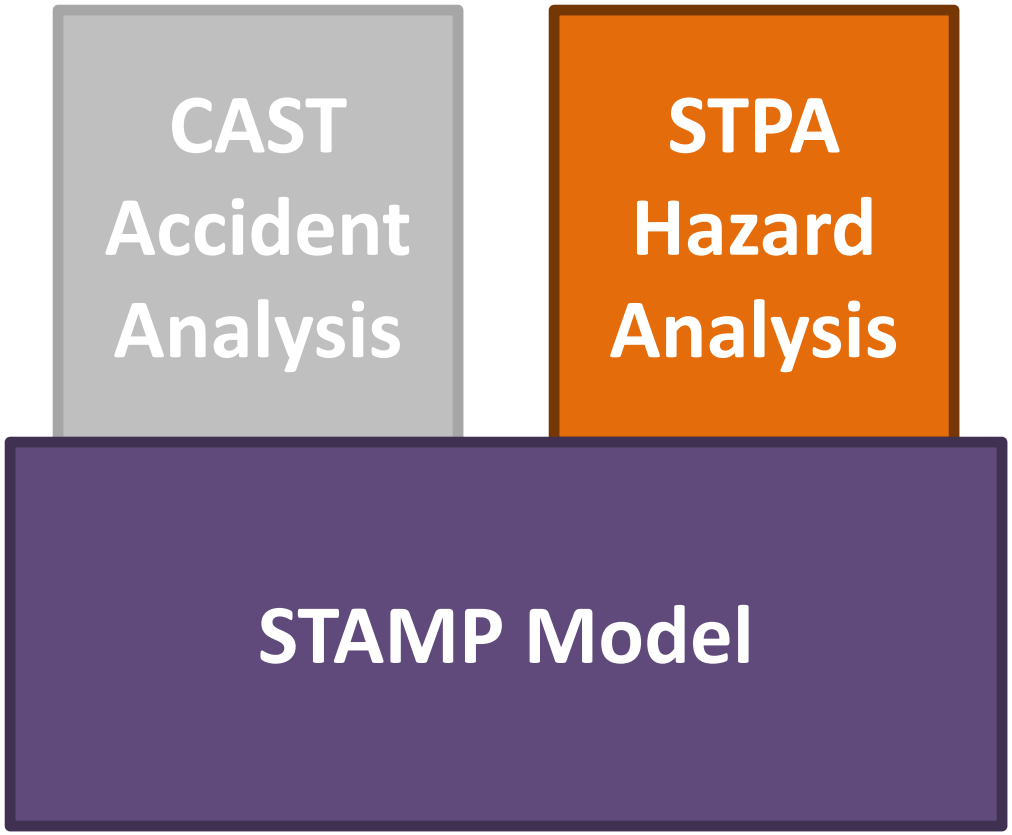


How do we find inadequate control that caused an accident?

Accidents are caused by inadequate control

©

STAMP and STPA



How do we find inadequate control in a design?

Accidents are caused by inadequate control

©

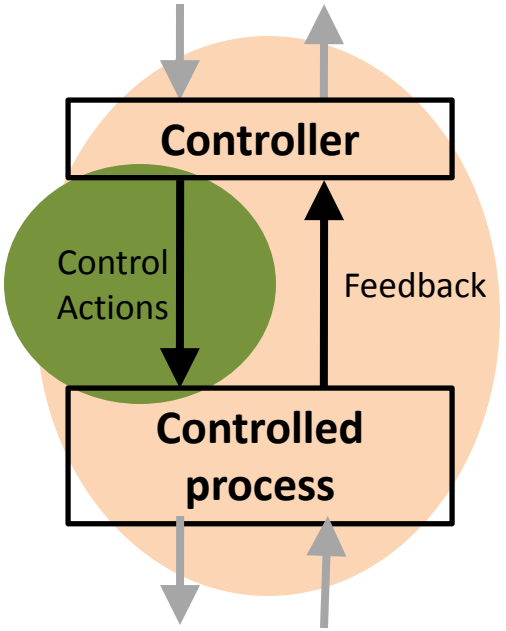
STPA Hazard Analysis

STPA
(System-Theoretic Process Analysis)

STPA Hazard Analysis

STAMP Model

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



Can capture requirements flaws, software errors, human errors

(Leveson, 2012)

©

Definitions

- Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

- Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).

Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors **outside our control**
- System Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

System Accident	System Hazard
People die from exposure to toxic chemicals	Toxic chemicals from the plant are in the atmosphere

©

Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors **outside our control**
- System Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

System Accident	System Hazard
People die from exposure to toxic chemicals	Toxic chemicals from the plant are in the atmosphere
People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

©

Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

Broad view of safety

"Accident" is anything that is unacceptable, that must be prevented.

Not limited to loss of life or human injury!

People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

System Safety Constraints

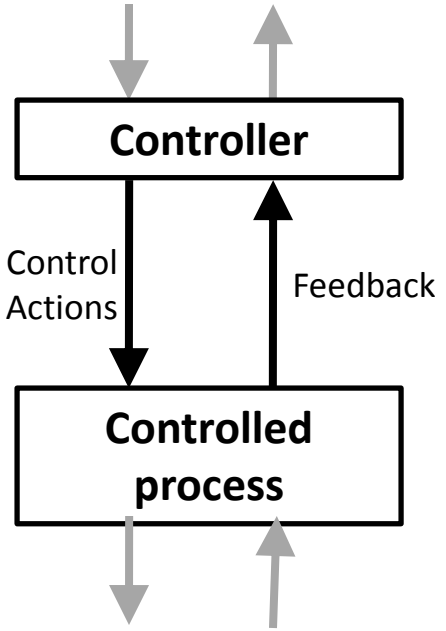
System Hazard	System Safety Constraint
Toxic chemicals from the plant are in the atmosphere	Toxic plant chemicals must not be released into the atmosphere
Nuclear power plant radioactive materials are not contained	Radioactive materials must note be released
Vehicles do not maintain safe distance from each other	Vehicles must always maintain safe distances from each other
Food products for sale contain pathogens	Food products with pathogens must not be sold

Additional hazards / constraints can be found in ESW p355

©

STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



(Leveson, 2012)

©

Control Structure Examples

Adaptive Cruise Control

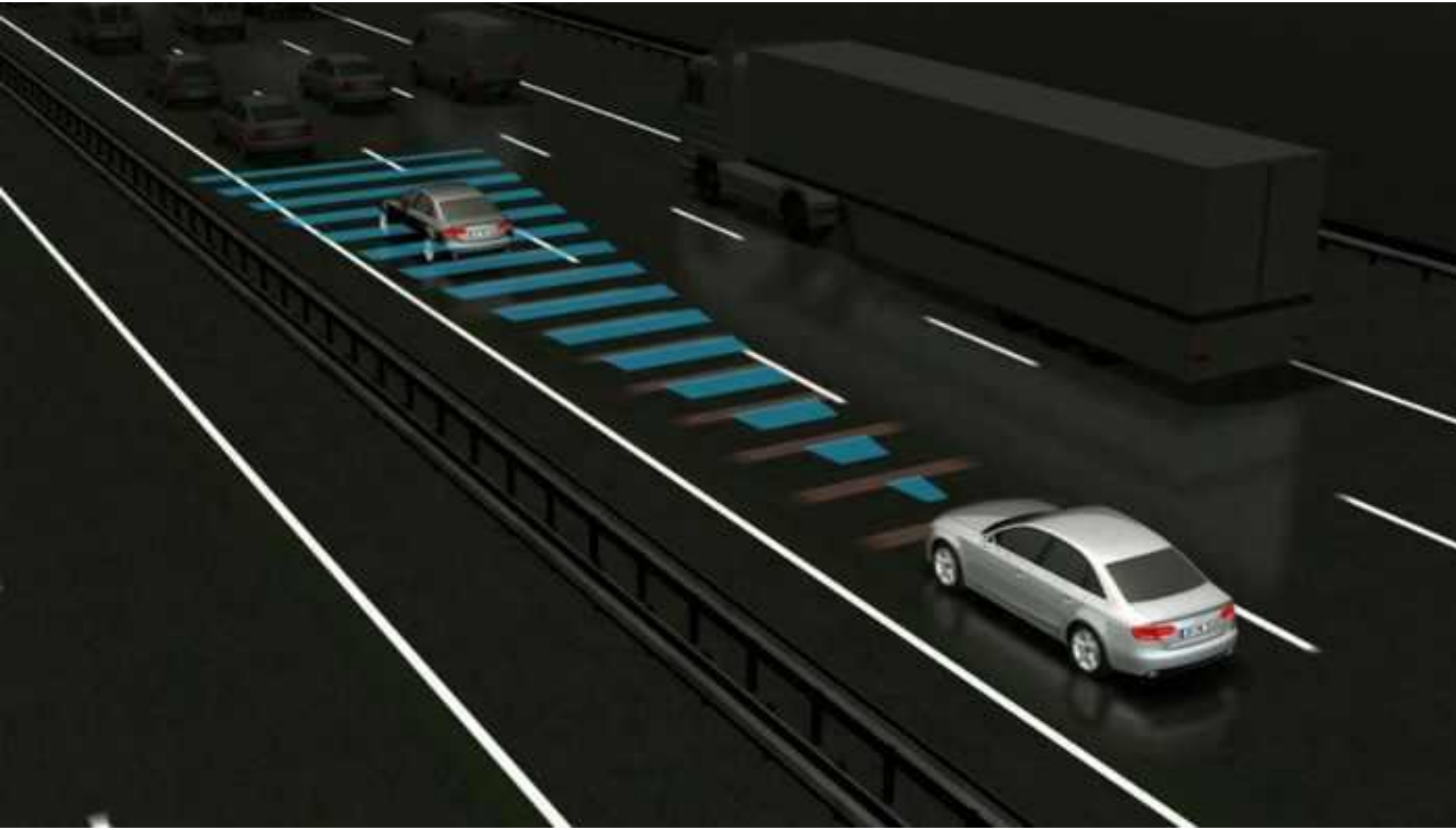
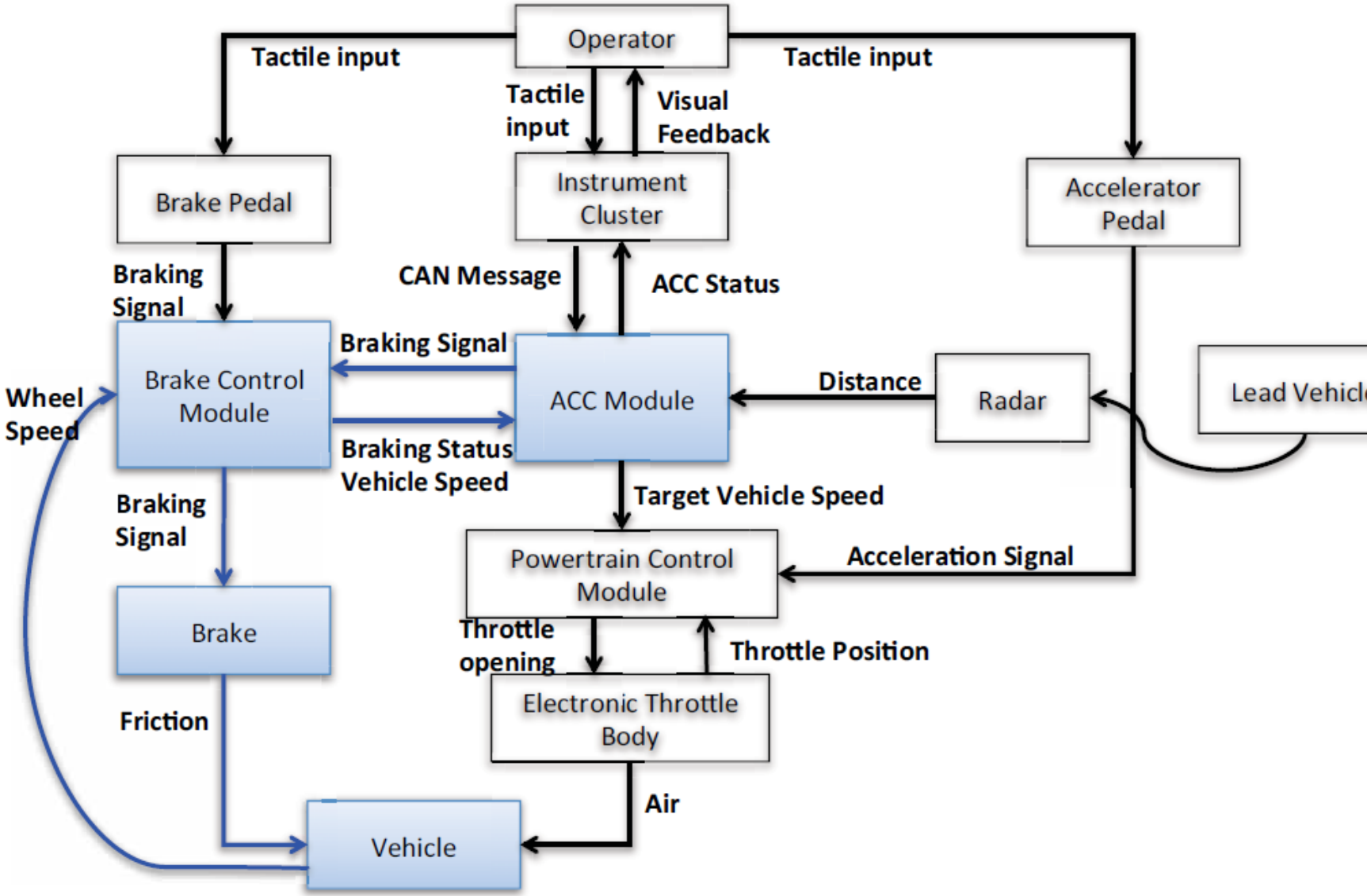
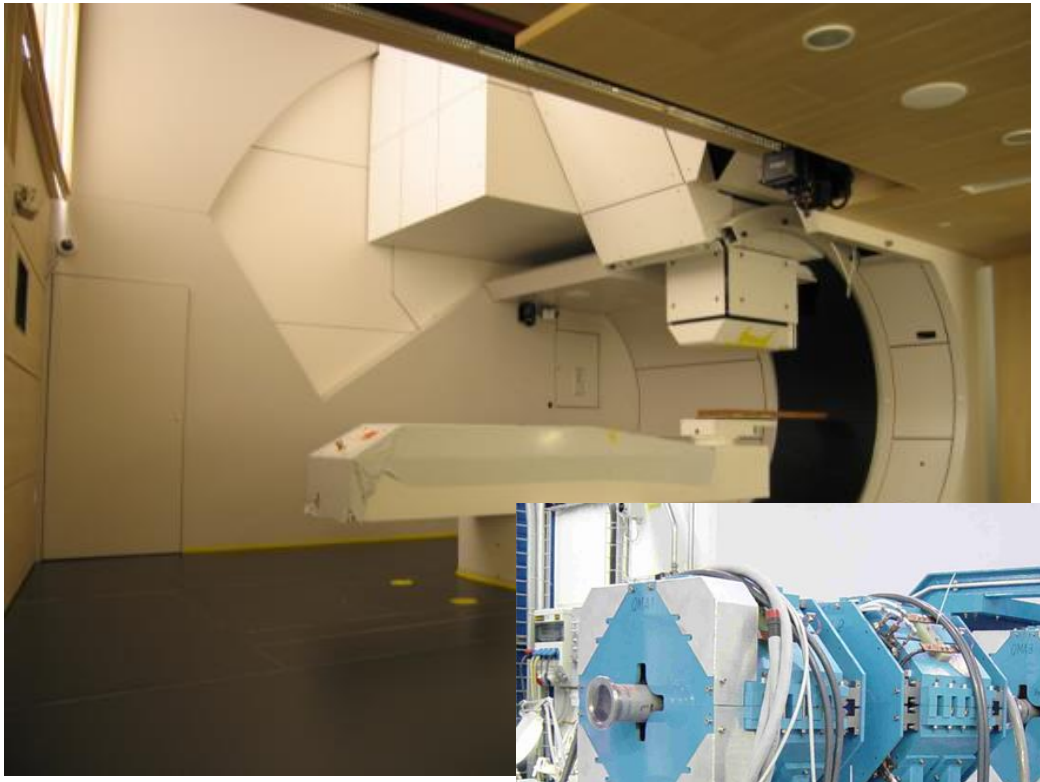


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

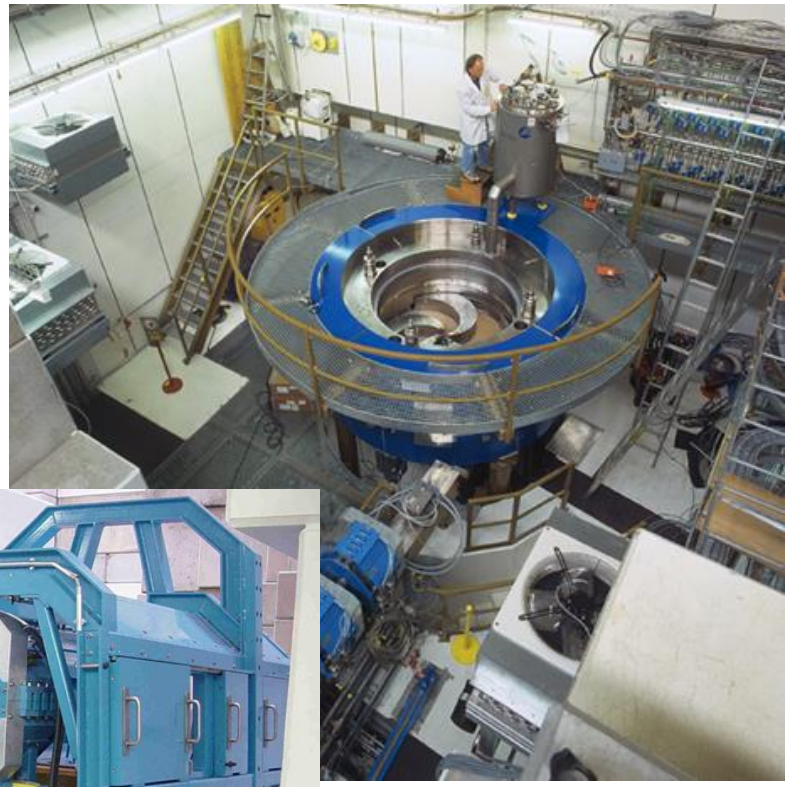
Example: ACC – BCM Control Loop



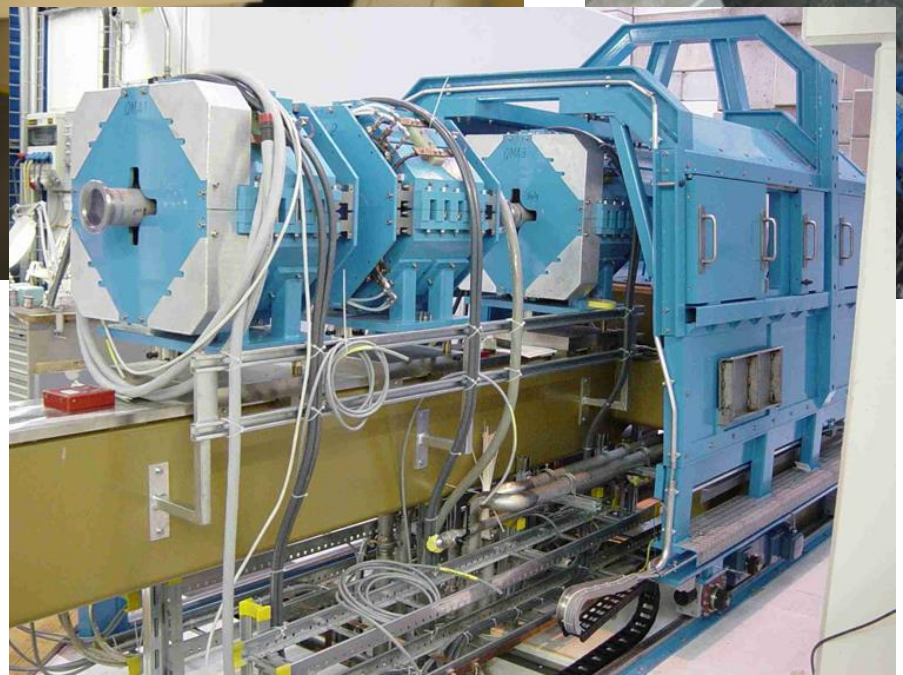
Proton Therapy Machine
High-level Control Structure



Gantry



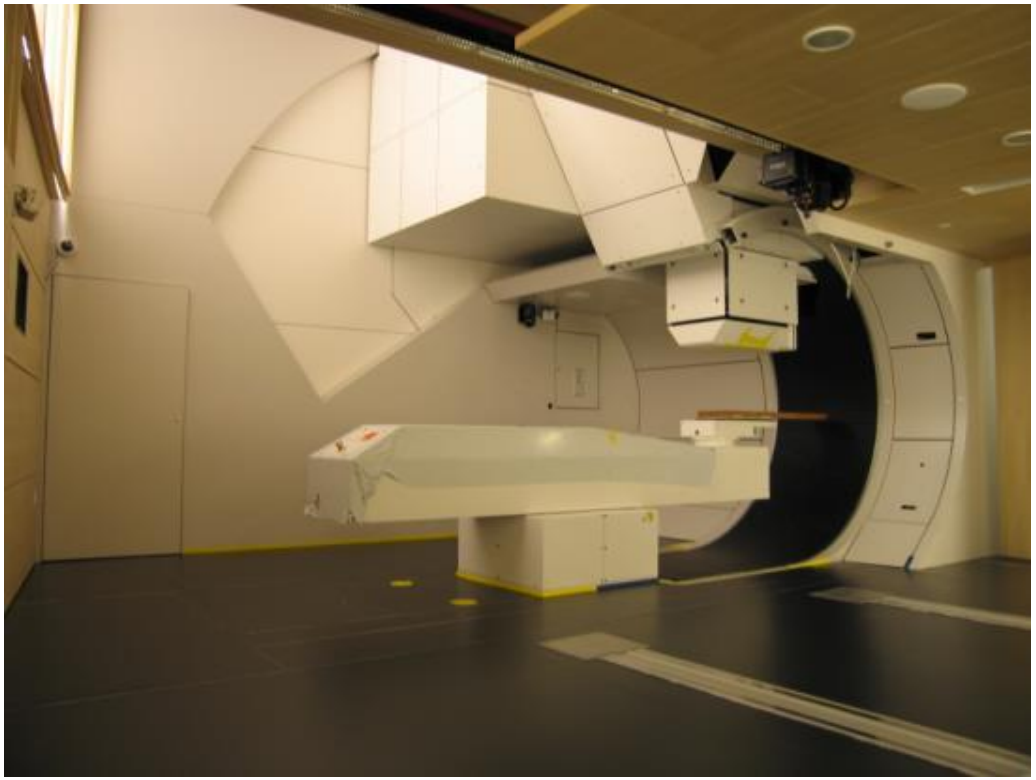
Cyclotron



Beam path and
control elements

©

Proton Therapy Machine
High-level Control Structure



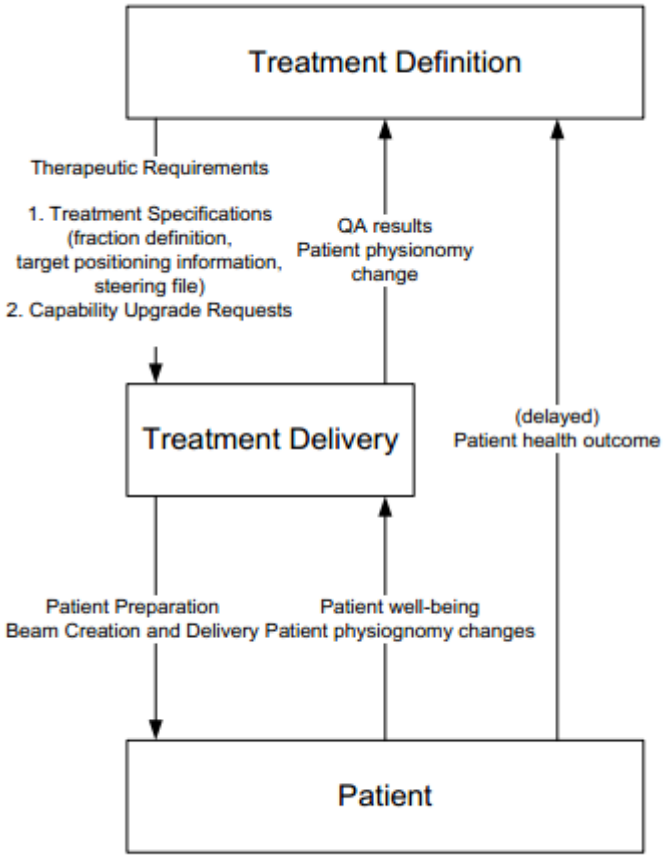
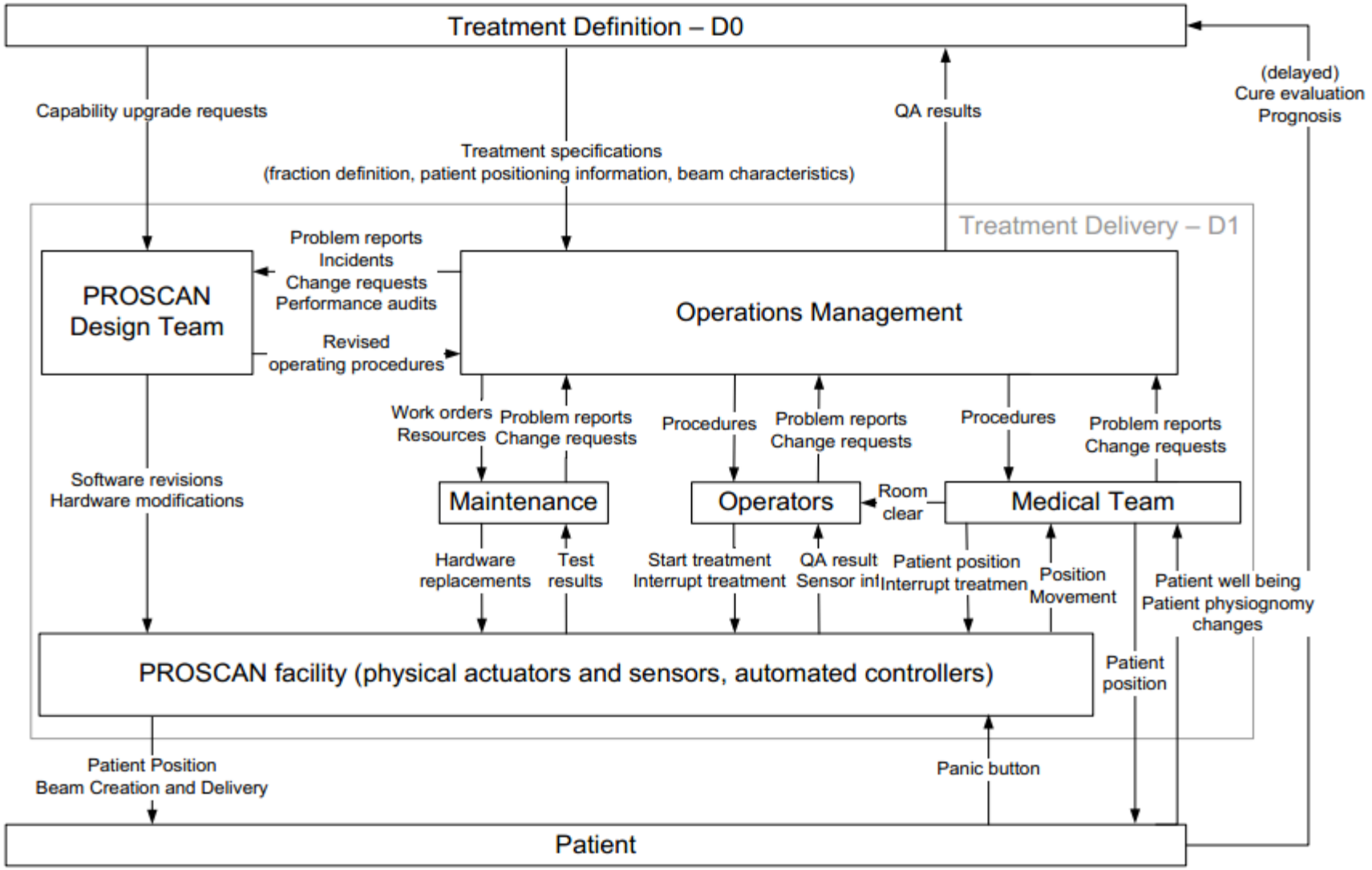


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Antoine PhD Thesis, 2012

©

Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

Figure 13 - Zooming into the Treatment Delivery group (D1)

©

Chemical Plant

Image from: http://www.cbgnetwork.org/2608.html

Chemical Plant

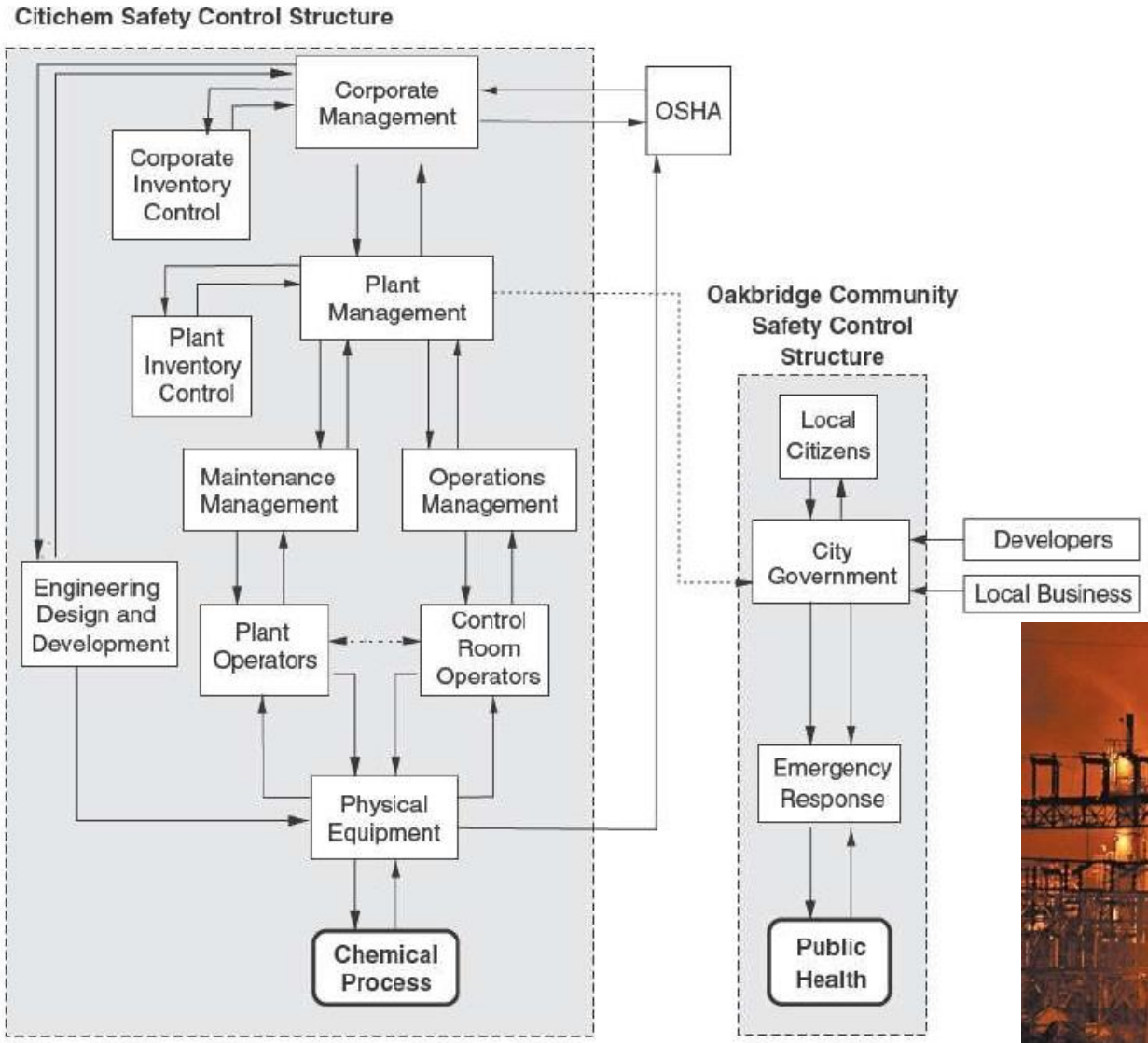


Image from:
http://www.cbgnetwork.org/2608.html

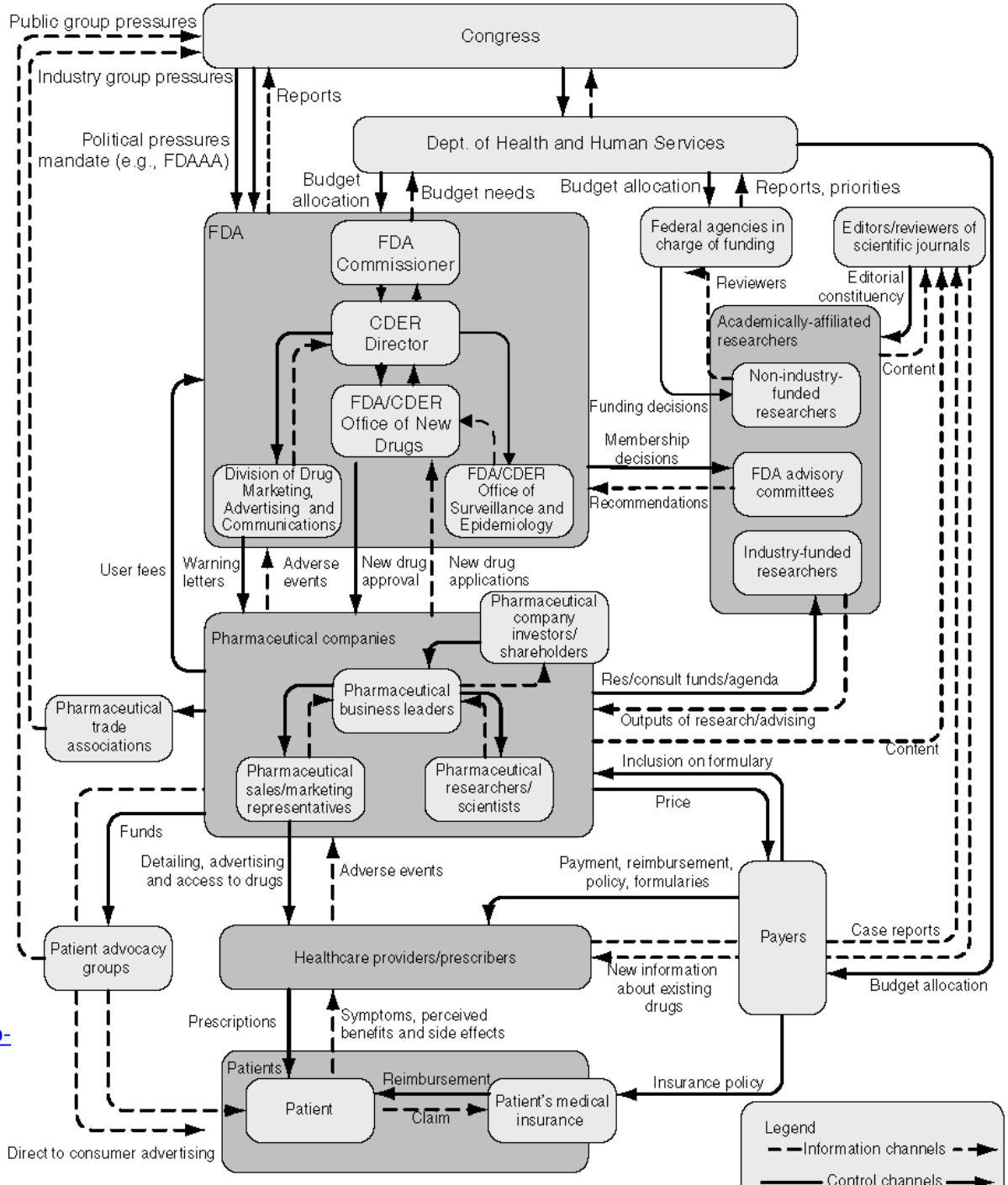
ESW p354

©

U.S. pharmaceutical safety control structure

Image from: http://www.kleantreatmentcenter.com/wp-content/uploads/2012/07/vioxx.jpeg

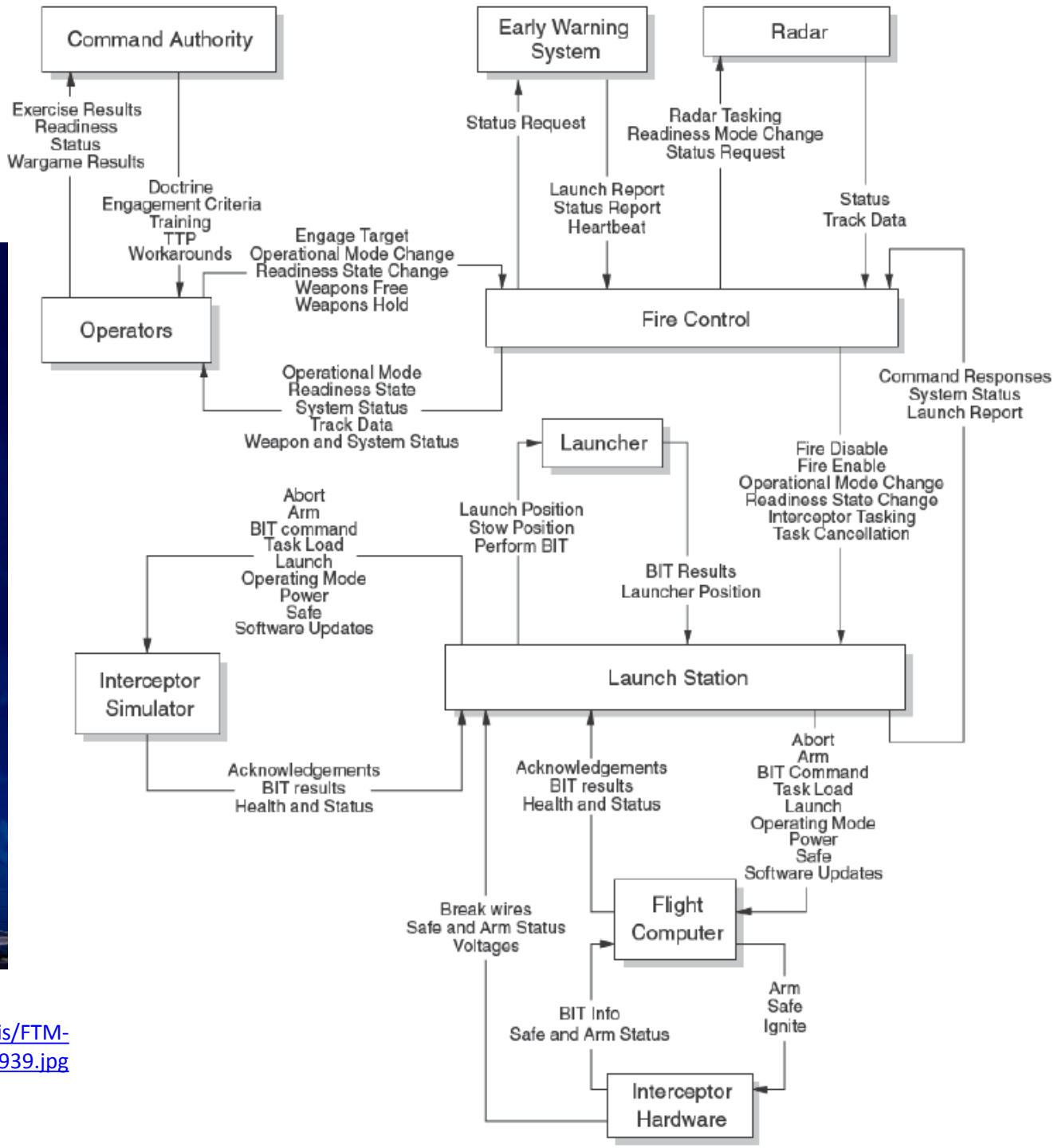
©



Ballistic Missile Defense System

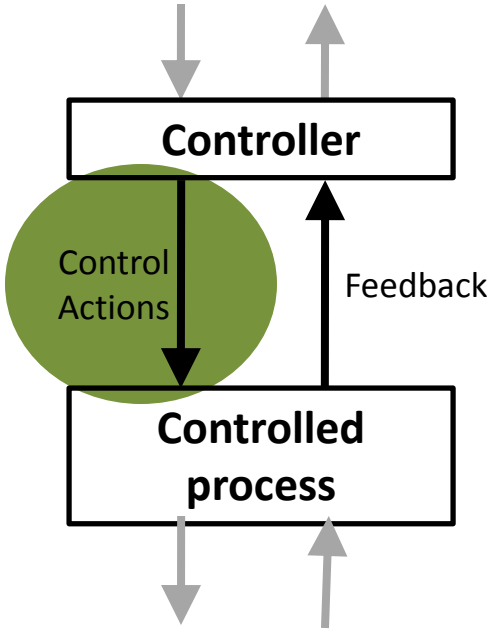
Image from:
http://www.mda.mil/global/images/system/aegis/FTM-21_Missile%201_Bulkhead%20Center14_BN4H0939.jpg

Safeware Corporation



STPA
(System-Theoretic Process Analysis)

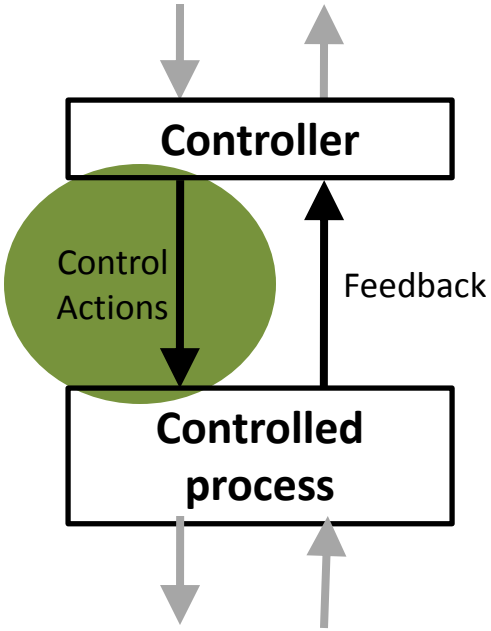
- Identify accidents and hazards
- Draw the control structure
- **Step 1: Identify unsafe control actions**
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

©

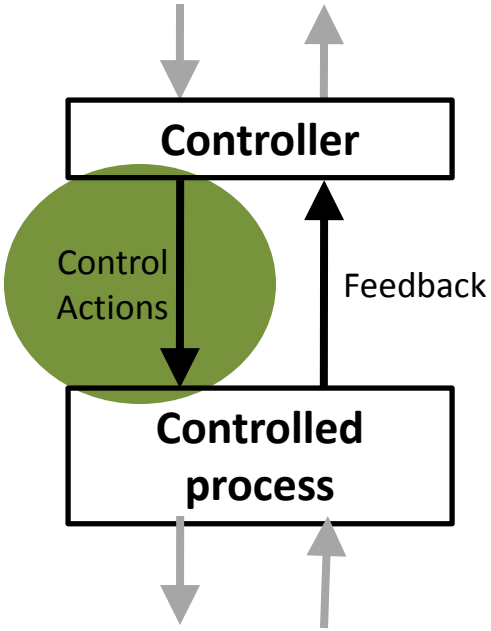
STPA Step 1: Unsafe Control Actions (UCA)



Control Action A				

©

STPA Step 1: Unsafe Control Actions (UCA)



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
(Control Action)				

©

Step 1: Identify Unsafe Control Actions

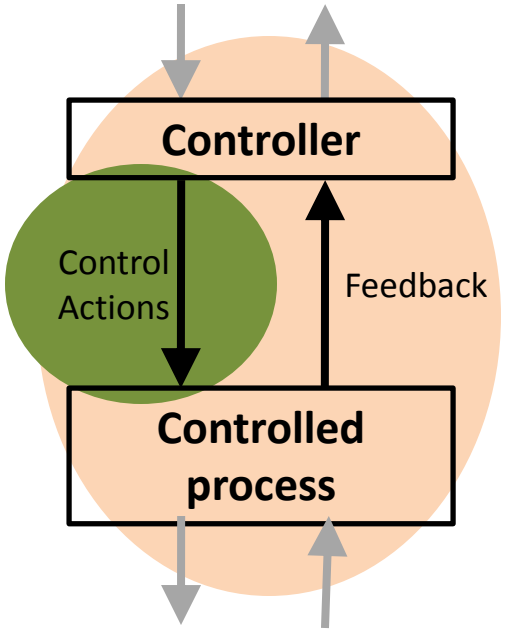
(a more rigorous approach)

Control Action	Process Model Variable 1	Process Model Variable 2	Process Model Variable 3	Hazardous?

©

STPA
(System-Theoretic Process Analysis)

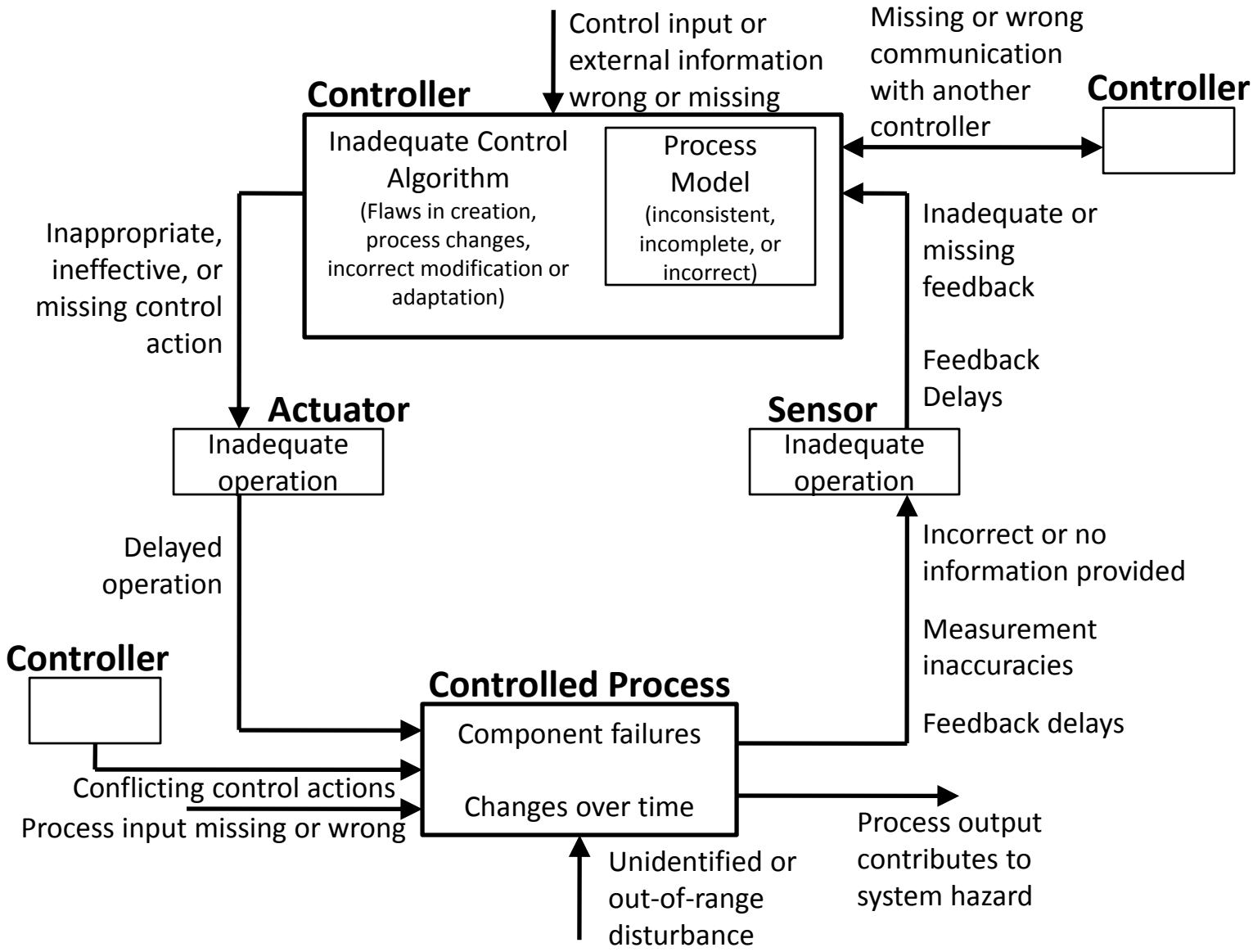
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



(Leveson, 2012)

©

STPA Step 2: Identify Control Flaws

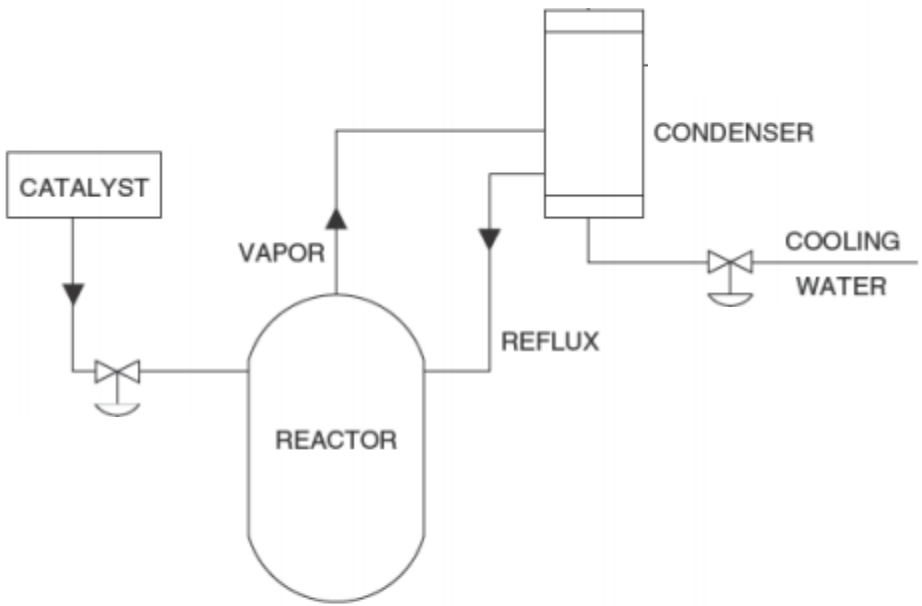


STPA Examples

Chemical Reactor

Chemical Reactor Design

- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

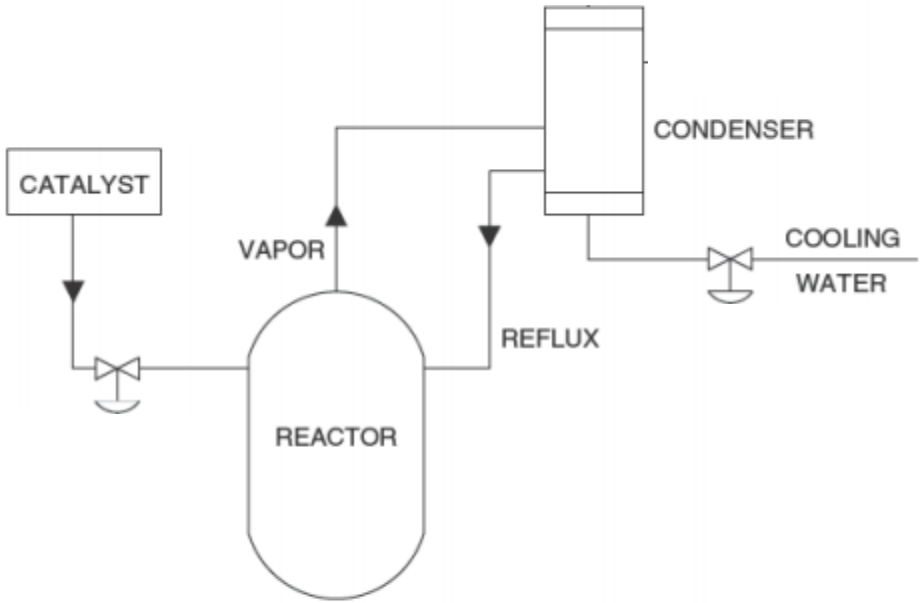


What are the accidents, system hazards, system safety constraints?

©

Chemical Reactor Design

- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

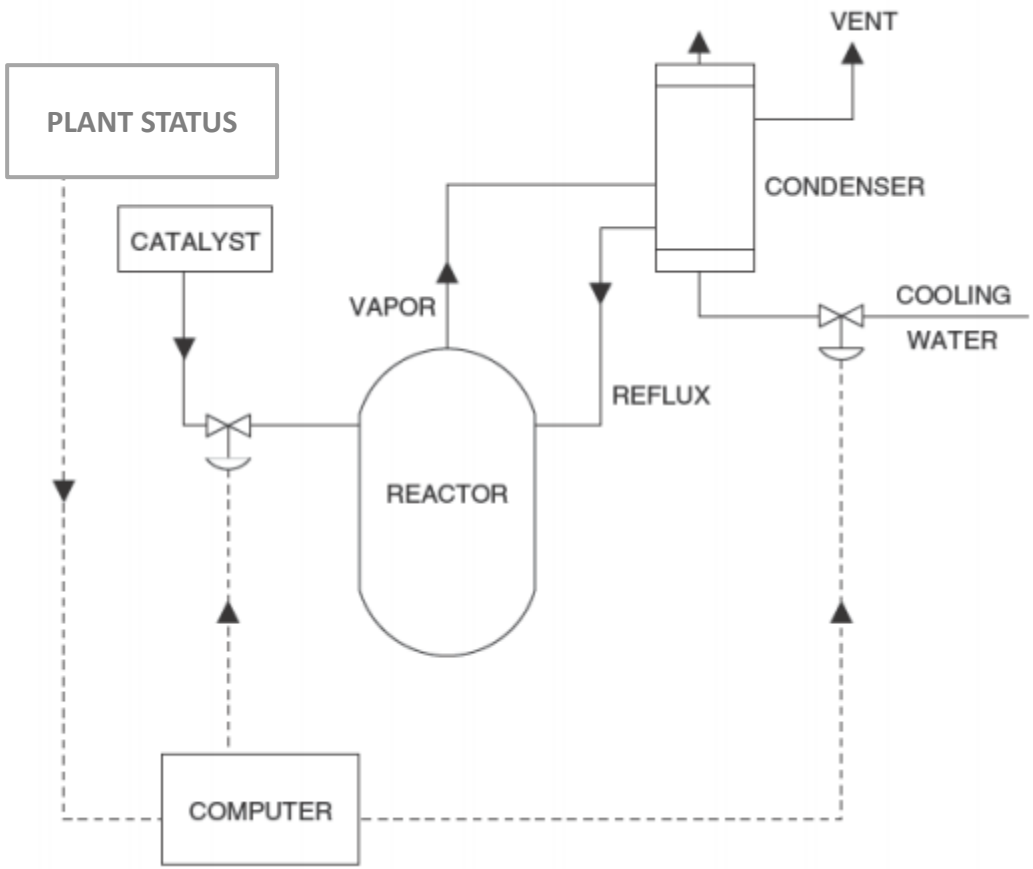


What else is needed?

©

Chemical Reactor Design

- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

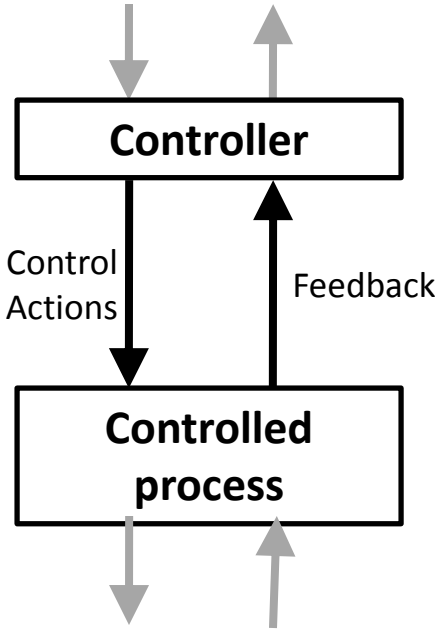


One approach: use an automated computer

©

STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

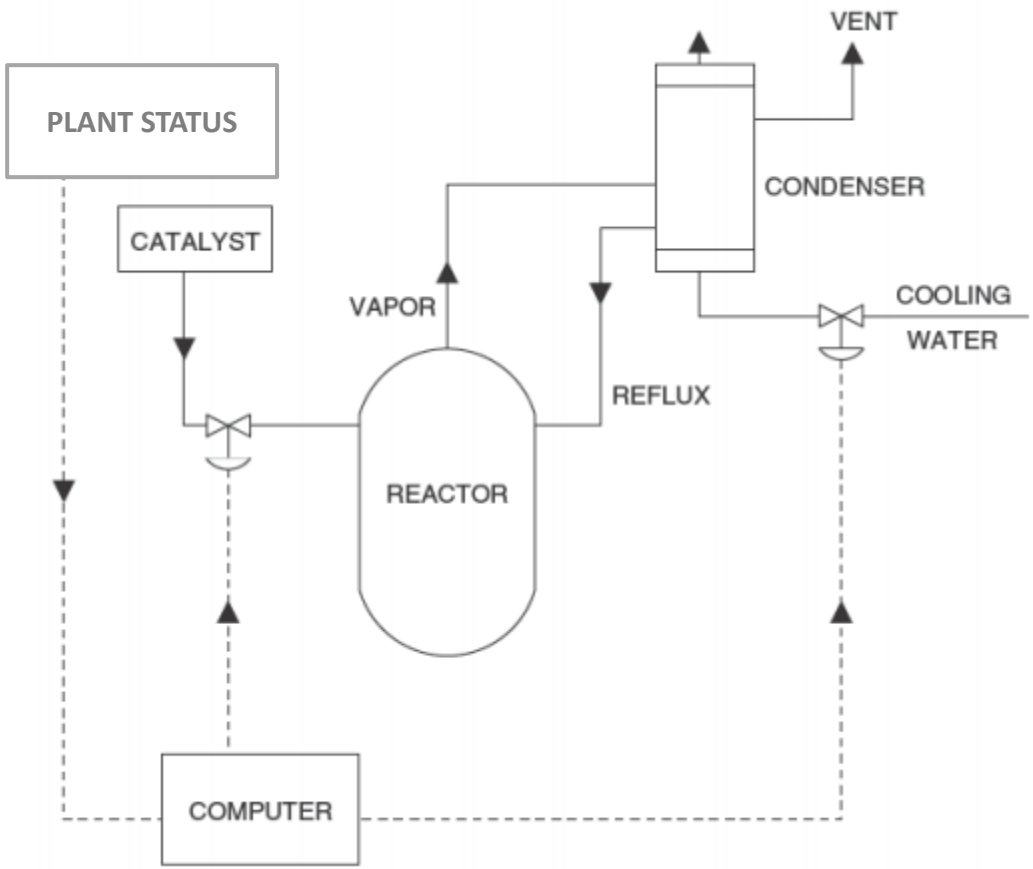


(Leveson, 2012)

©

Chemical Reactor Design

- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

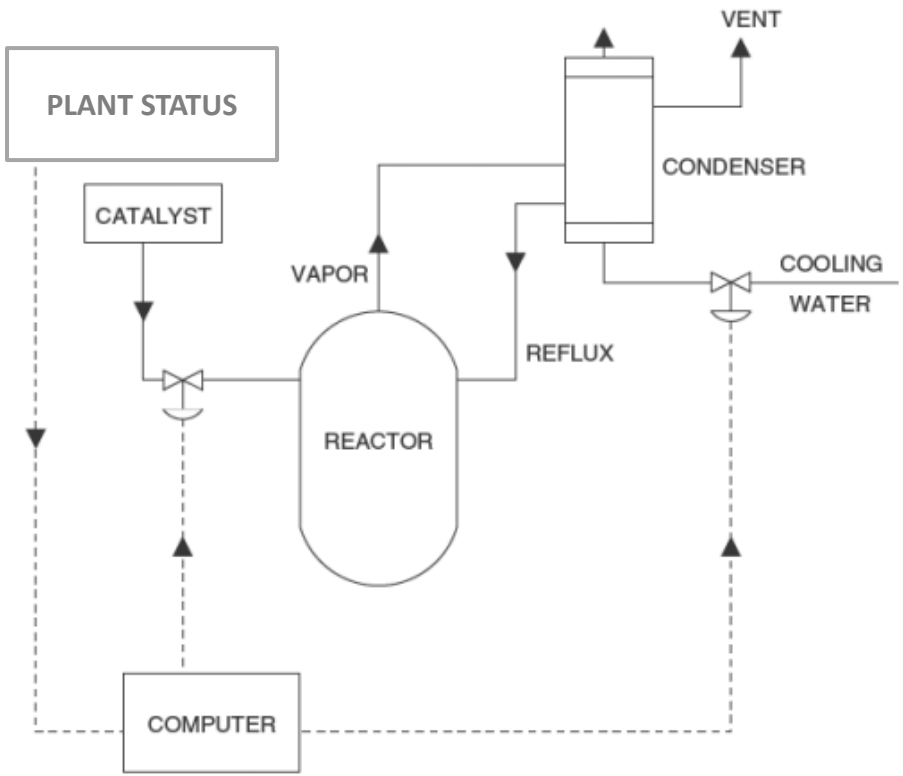


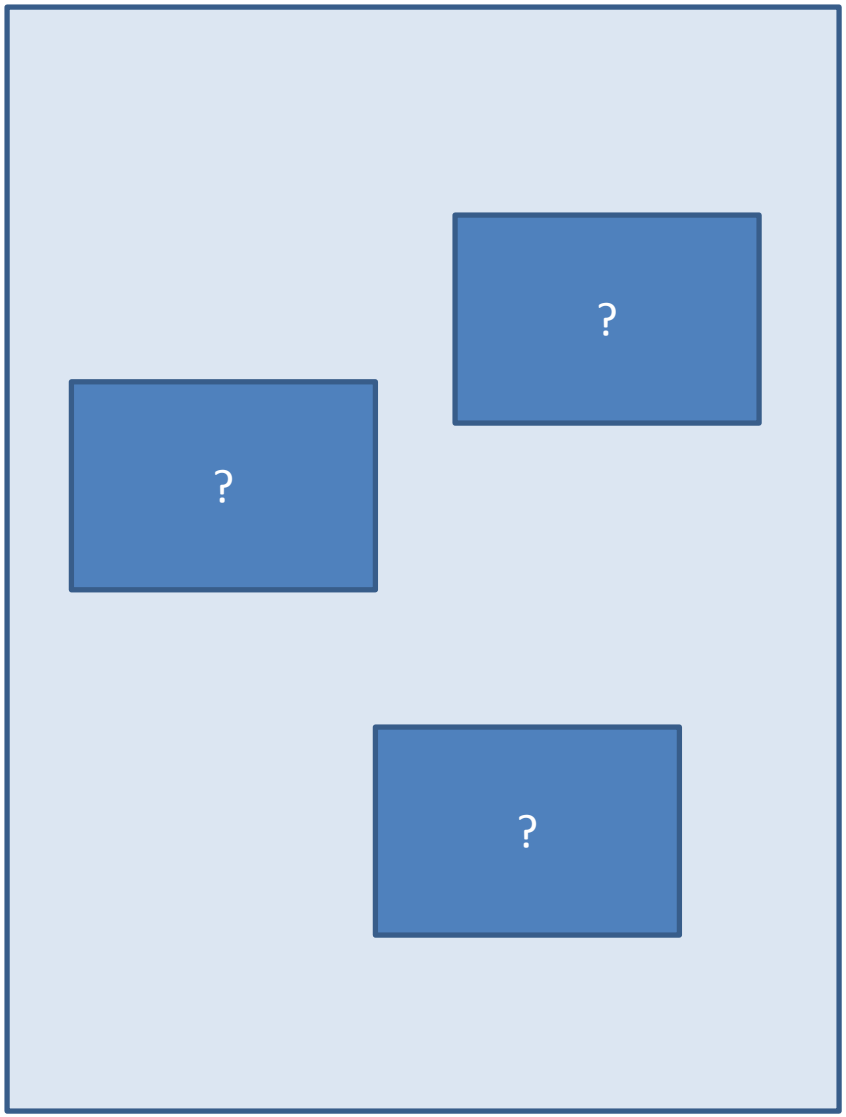
Create Control Structure

©

STPA Analysis

- High-level (simple) Control Structure
  - What are the main parts?

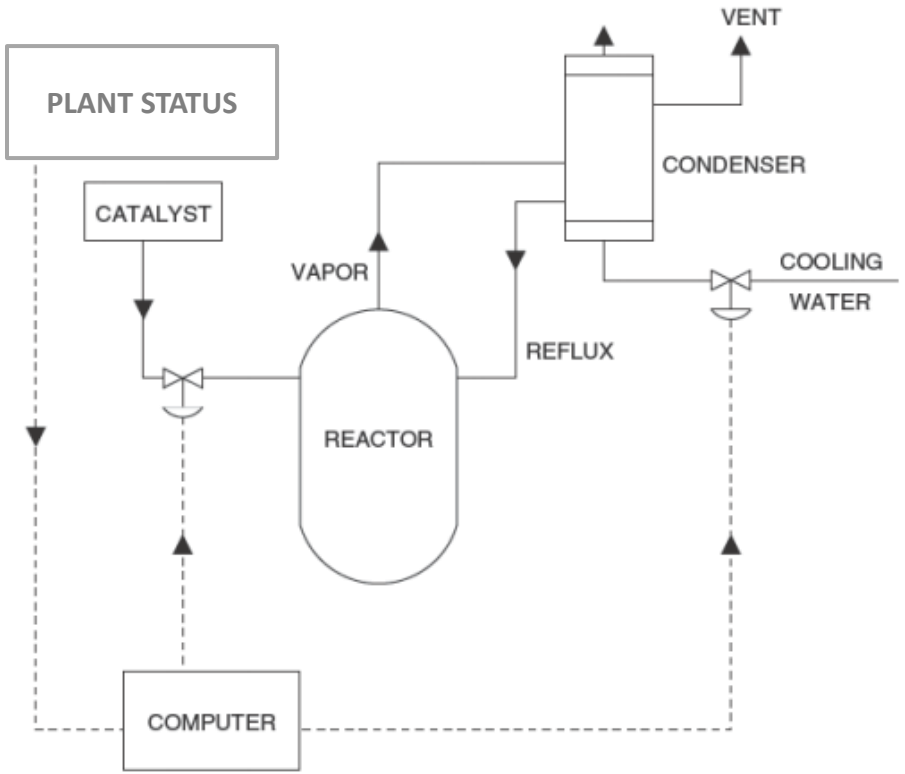


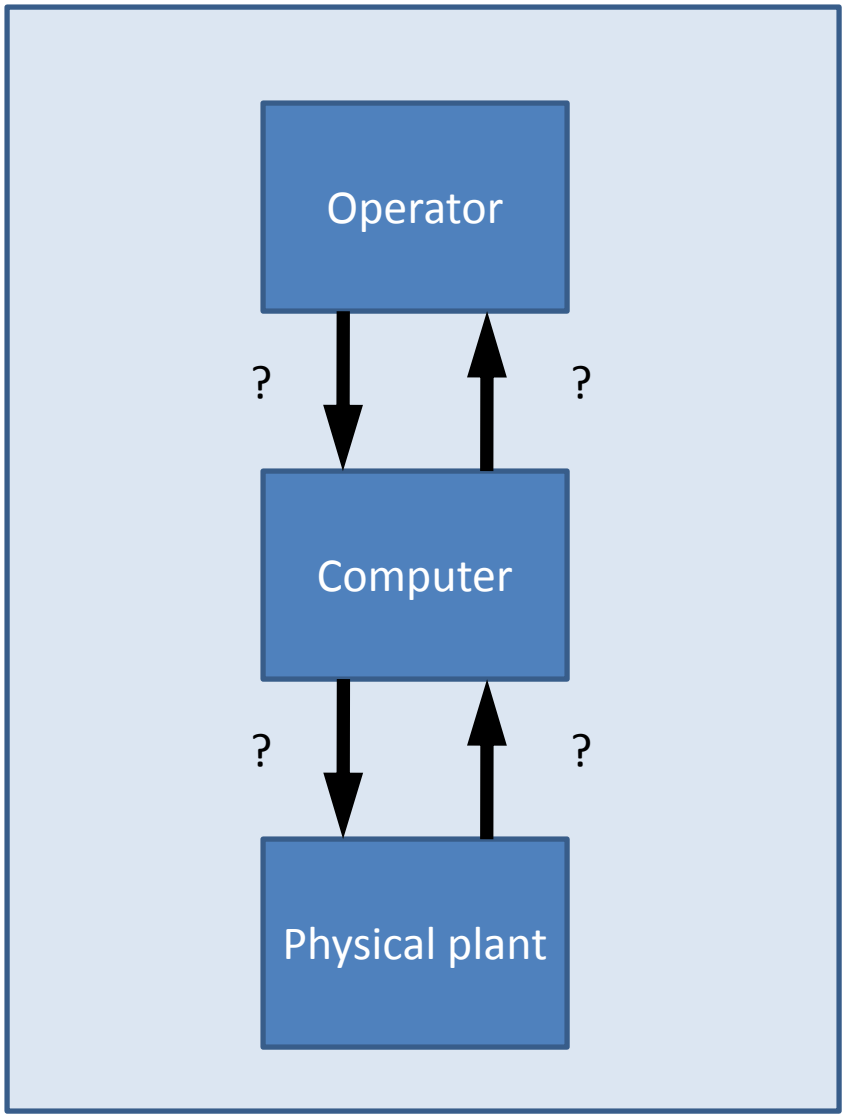


©

STPA Analysis

- High-level (simple) Control Structure
  - What commands are sent?

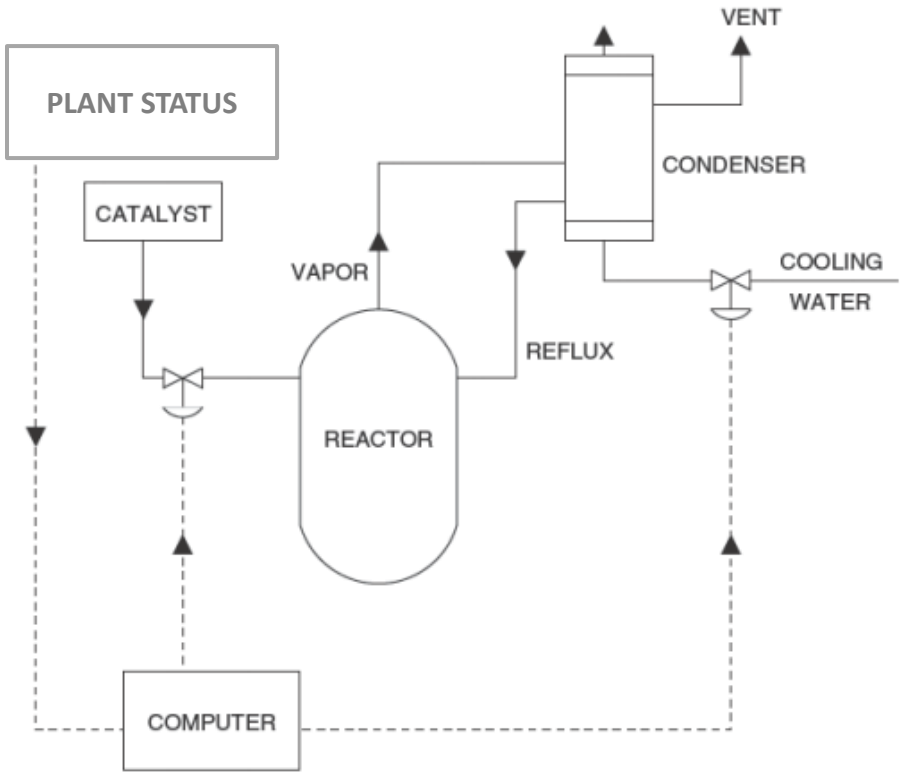


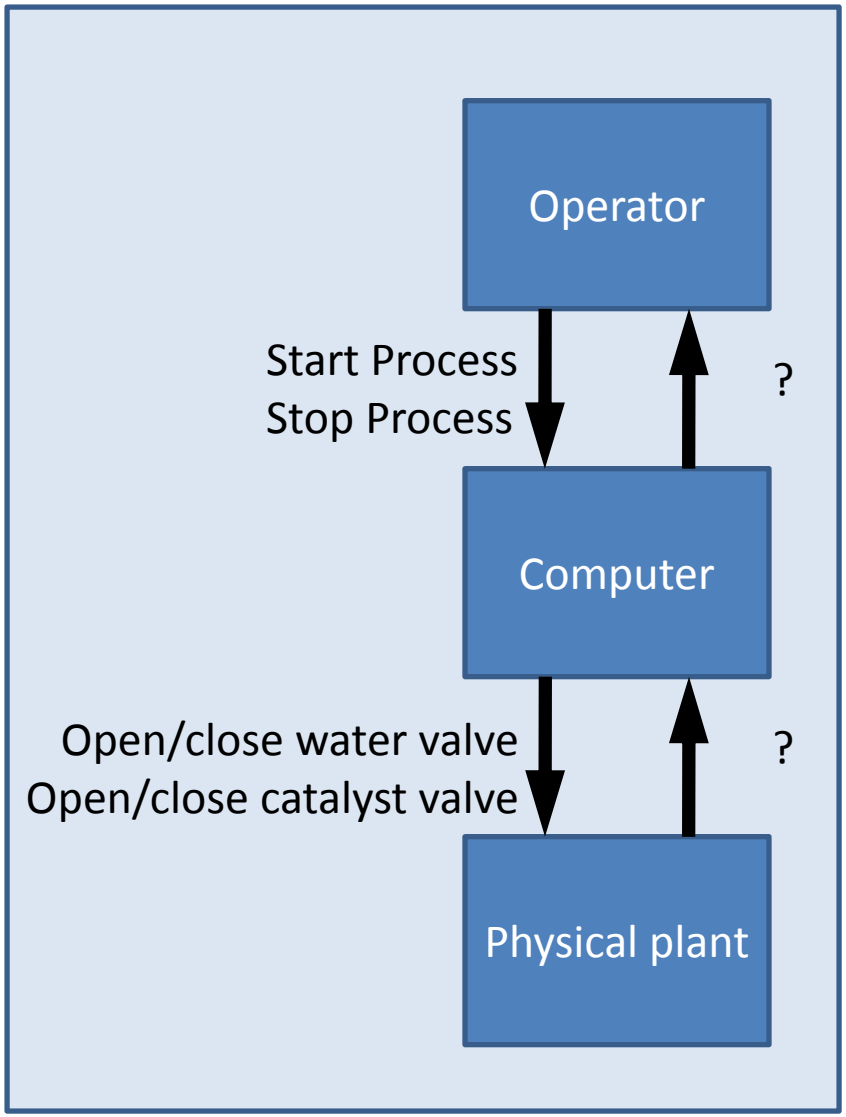


©

STPA Analysis

- High-level (simple) Control Structure
  - What feedback is received?

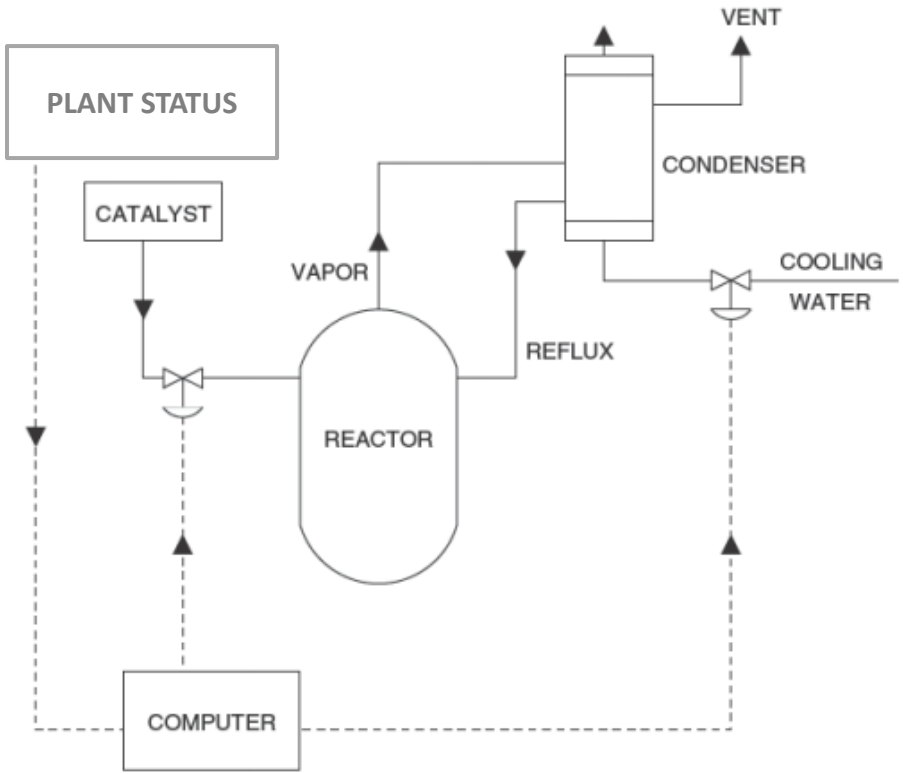


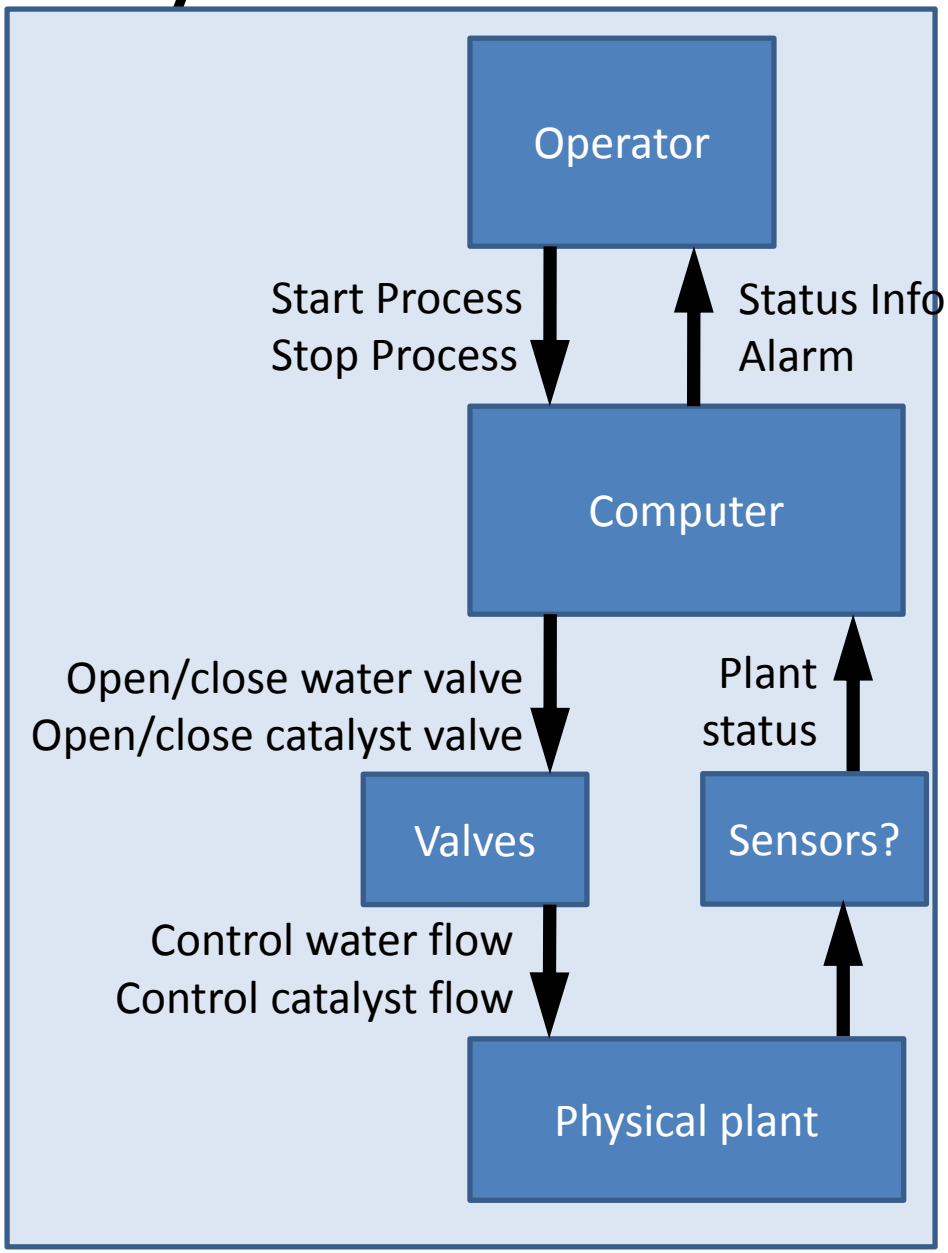


©

STPA Analysis

- High-level (simple) Control Structure



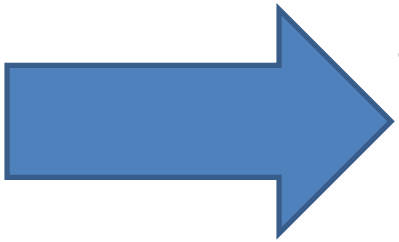


©

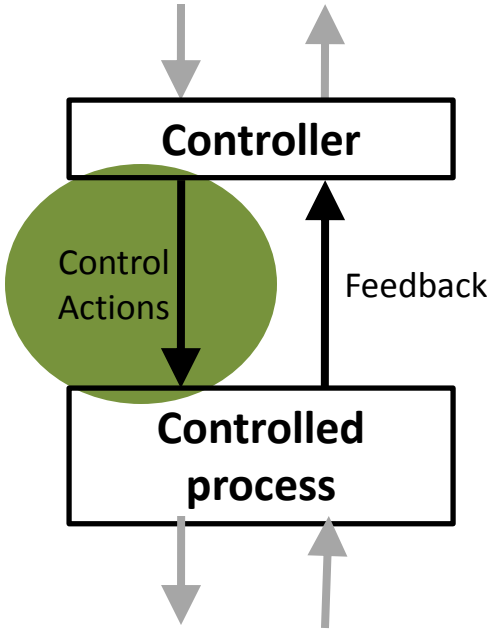
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards

- Draw the control structure



- **Step 1: Identify unsafe control actions**
- Step 2: Identify causal scenarios

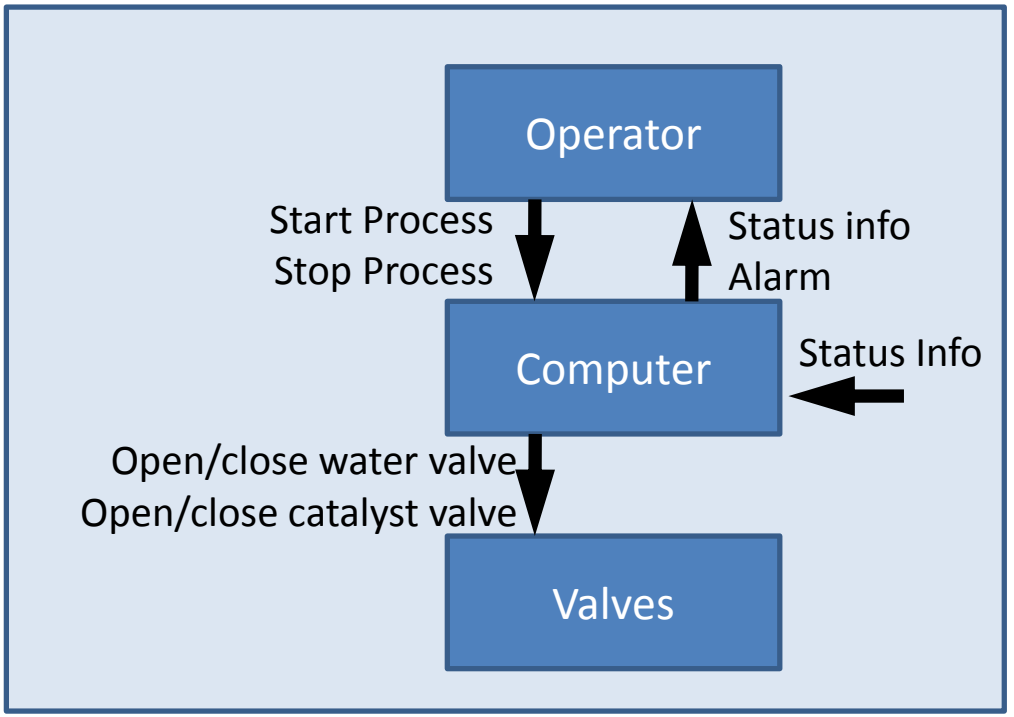


(Leveson, 2012)

©

Chemical Reactor: Unsafe Control Actions

Control Structure:

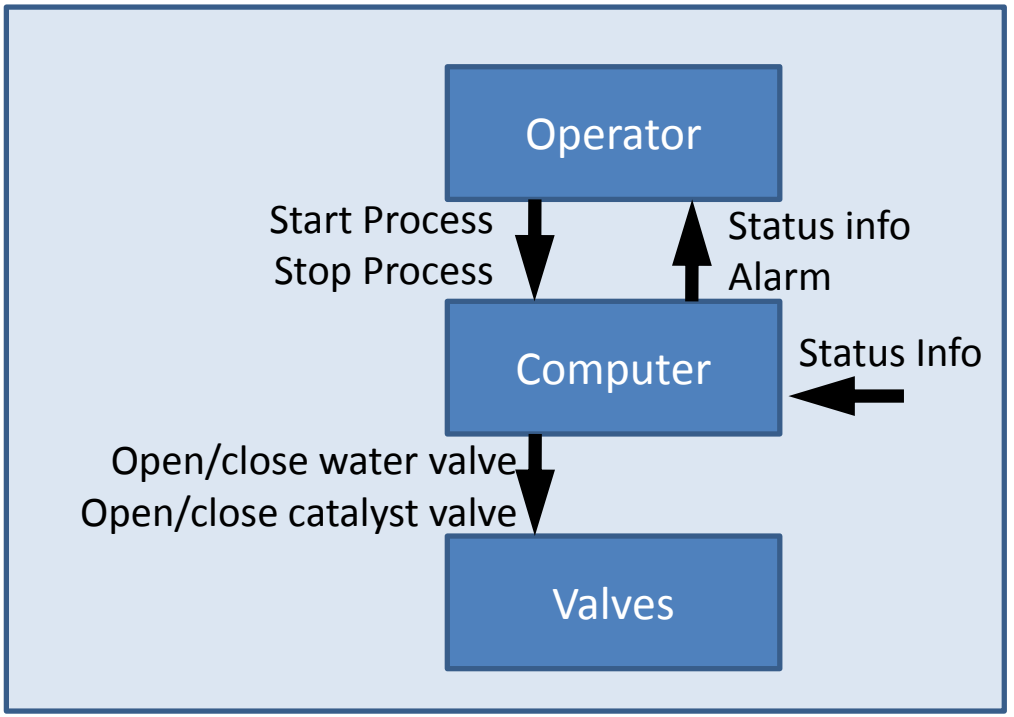


	?	?	?	?
Close Water Valve				

©

Chemical Reactor: Unsafe Control Actions

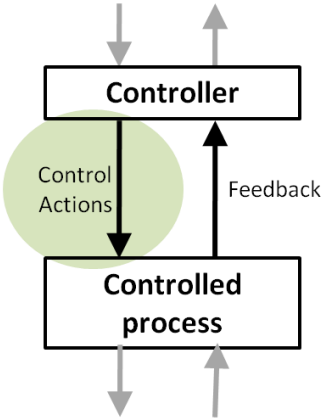
Control Structure:



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve	?	**Computer closes water valve while catalyst open**	?	?

©

Structure of an Unsafe Control Action



Example:

"Computer provides close water valve command when catalyst open"

Source Controller

Type

Control Action

Context

Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)

©

Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve		**Computer closes water valve while catalyst open**	**Computer closes water valve before catalyst closes**	
Open Water Valve				
Open Catalyst Valve				
Close Catalyst Valve				

©

Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve		Computer closes water valve while catalyst open	Computer closes water valve before catalyst closes	
Open Water Valve	Computer does not open water valve when catalyst open		Computer opens water valve more than X seconds after open catalyst	Computer stops opening water valve before it is fully opened
Open Catalyst Valve		Computer opens catalyst valve when water valve not open	Computer opens catalyst more than X seconds before open water	
Close Catalyst Valve	Computer does not close catalyst when water closed		Computer closes catalyst more than X seconds after close water	Computer stops closing catalyst before it is fully closed

©

Safety Constraints

Unsafe Control Action	Safety Constraint
Computer does not open water valve when catalyst valve open	Computer must open water valve whenever catalyst valve is open
Computer opens water valve more than X seconds after catalyst valve open	?
Computer closes water valve while catalyst valve open	?
Computer closes water valve before catalyst valve closes	?
Computer opens catalyst valve when water valve not open	?
Etc.	Etc.

Safety Constraints

Unsafe Control Action	Safety Constraint
Computer does not open water valve when catalyst valve open	Computer must open water valve whenever catalyst valve is open
Computer opens water valve more than X seconds after catalyst valve open	Computer must open water valve within X seconds of catalyst valve open
Computer closes water valve while catalyst valve open	Computer must not close water valve while catalyst valve open
Computer closes water valve before catalyst valve closes	Computer must not close water valve before catalyst valve closes
Computer opens catalyst valve when water valve not open	Computer must not open catalyst valve when water valve not open
Etc.	Etc.

Traceability

- Always provide traceability information between UCAs and the hazards they cause.
  - Same for Safety Constraints and the hazards that result if violated.
- Two ways:
  - Create one UCA table (or safety constraint list) per hazard, label each table with the hazard
  - Create one UCA table for all hazards, include traceability info at the end of each UCA
    - E.g. **Computer closes water valve while catalyst open [H-1]**

Rigorous UCA identification

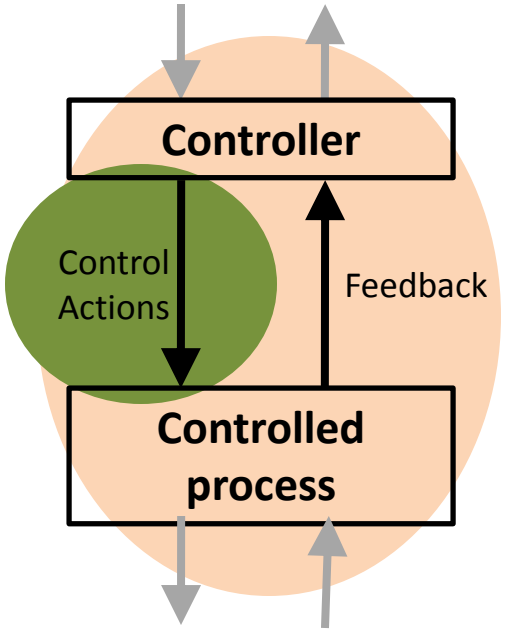
Control Action	Water valve	Catalyst valve	Plant state	Hazardous if provided?	Hazardous if not provided?
Open water valve when:	Open	Open	(doesn't matter)	No	No
Open water valve when:	(doesn't matter)	Closed	(doesn't matter)	No	No
Open water valve when:	Closed	Open	(doesn't matter)	No	Yes

UCA-1: Computer does not opens water valve when catalyst valve is open and water valve is closed

SC-1: Computer must open the water valve whenever the catalyst valve is open

STPA
(System-Theoretic Process Analysis)

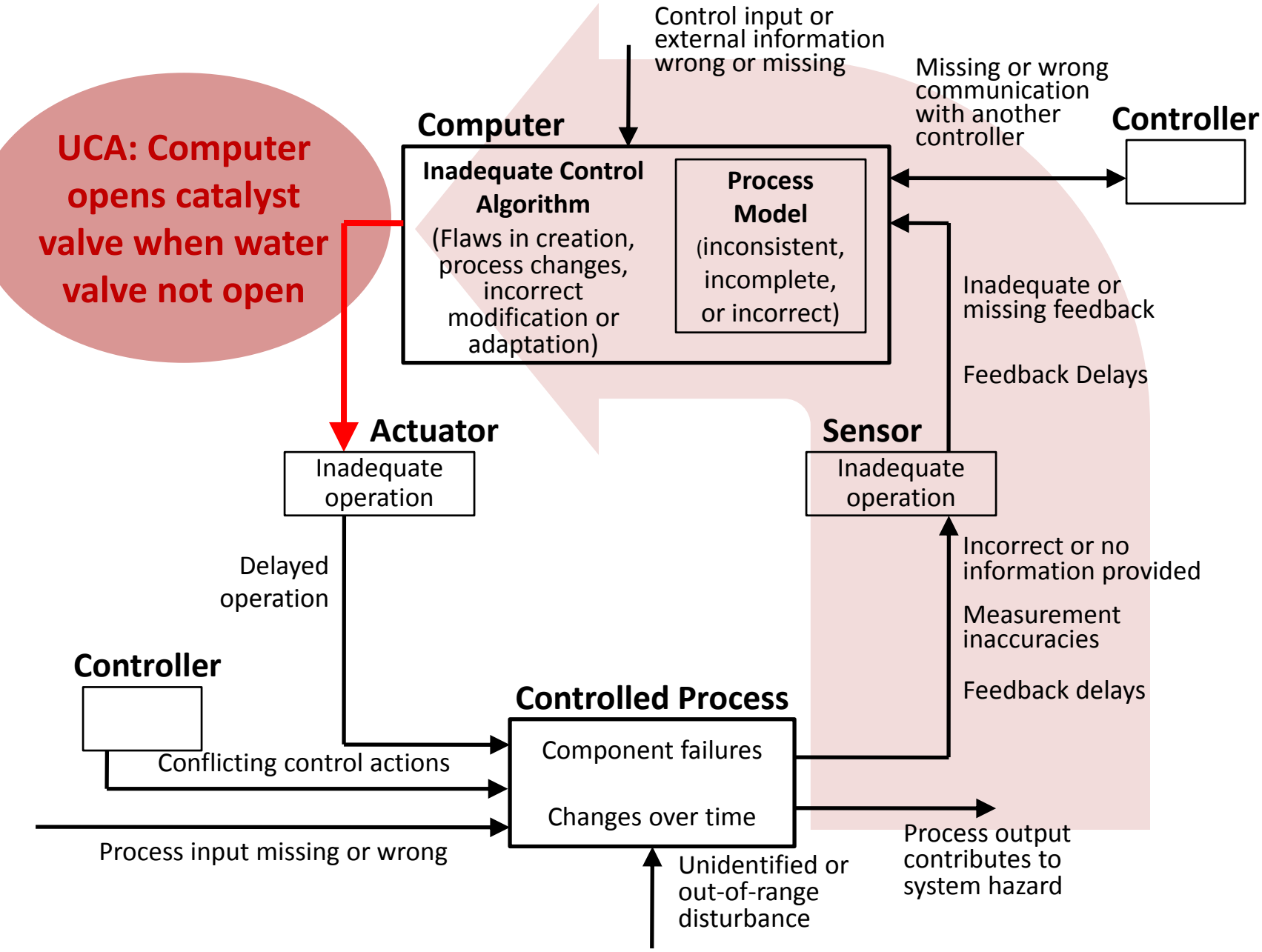
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



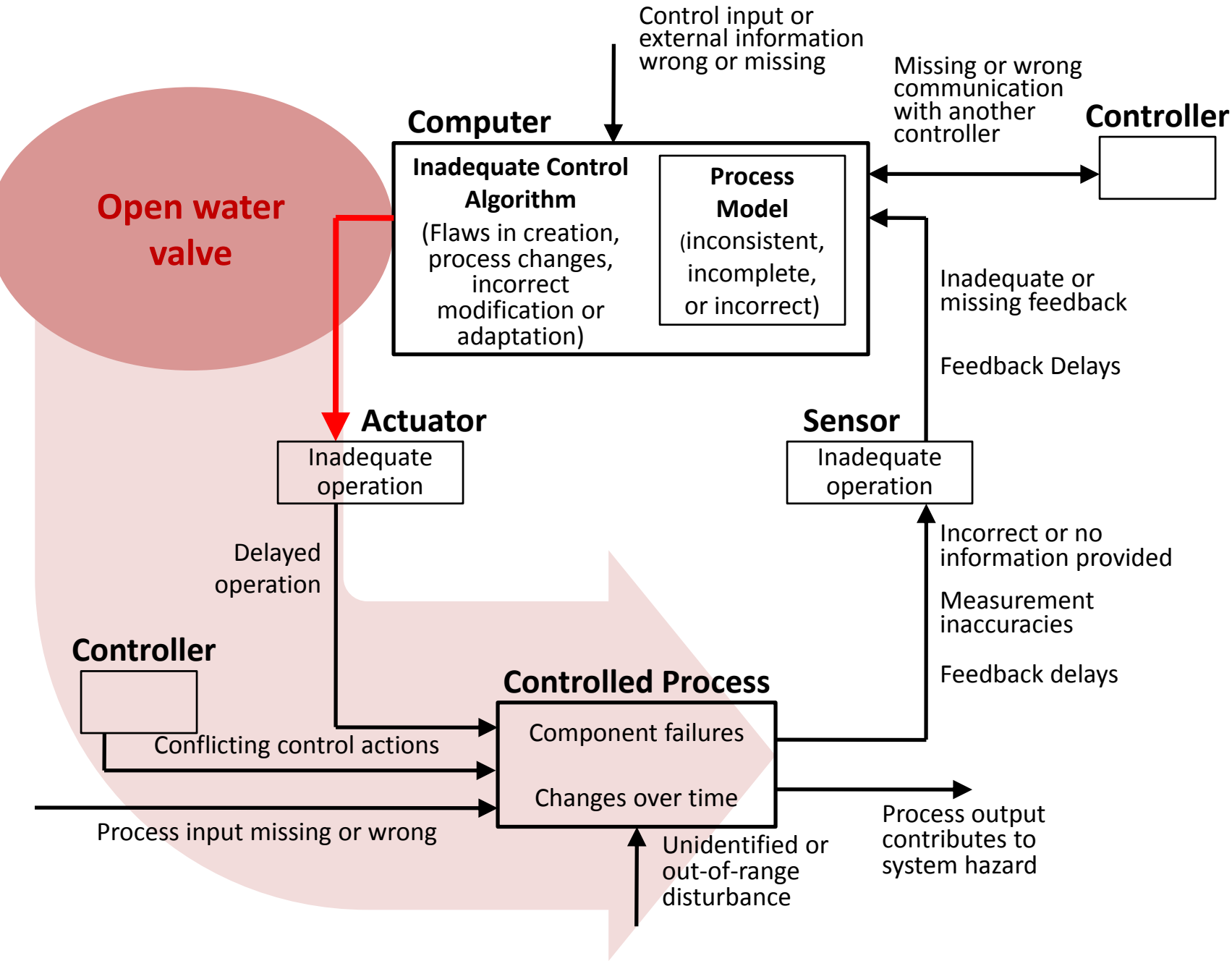
(Leveson, 2012)

©

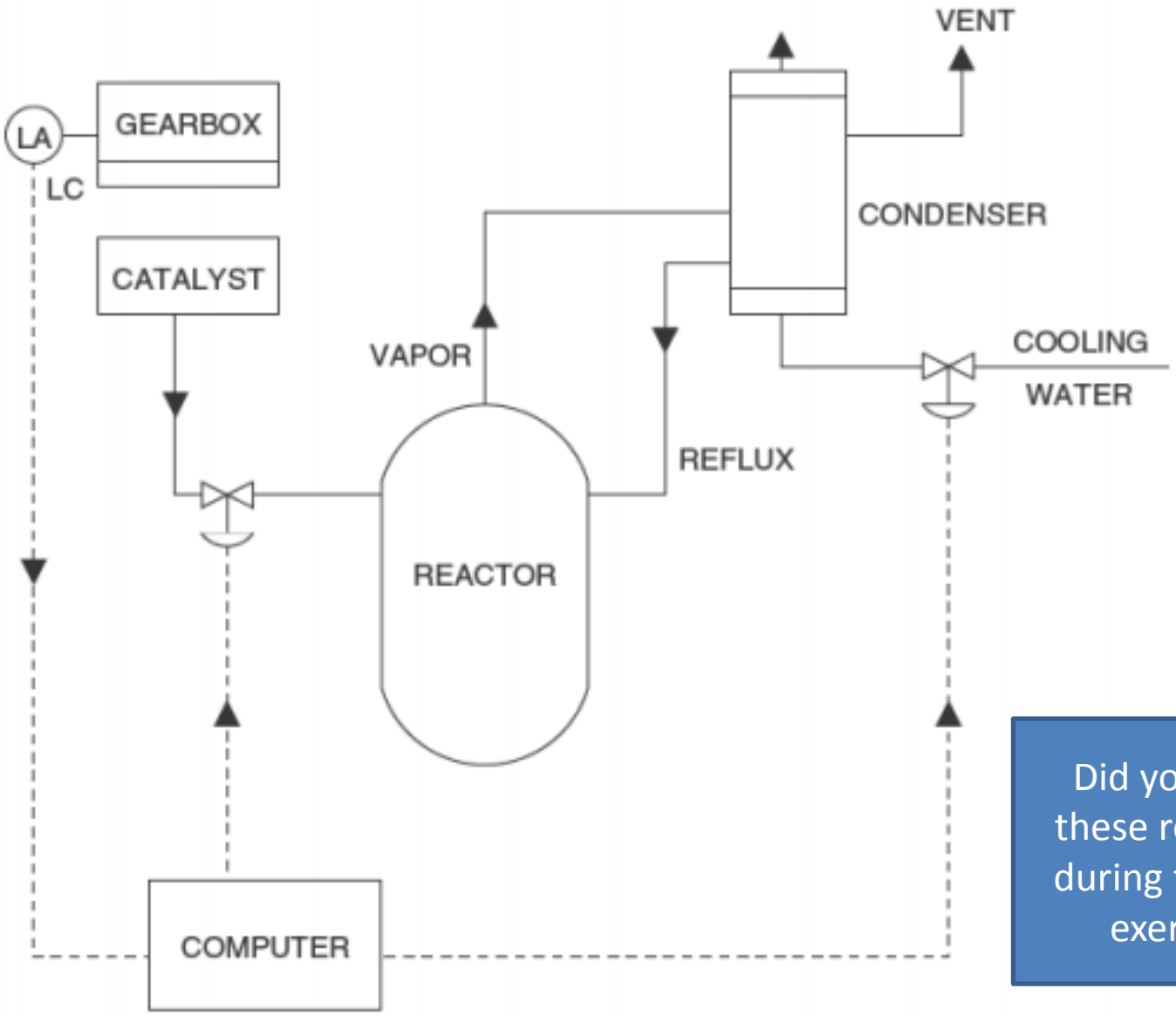
Step 2: Potential causes of UCAs



Step 2: Potential control actions not followed



Chemical Reactor: Real accident



Did you catch these real flaws during the STPA exercise?

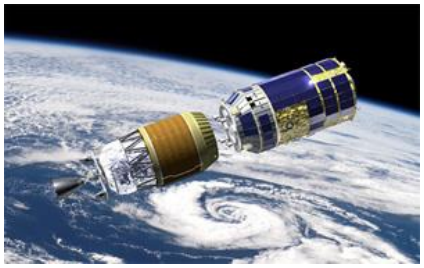
STAMP/STPA – Advanced Tutorial

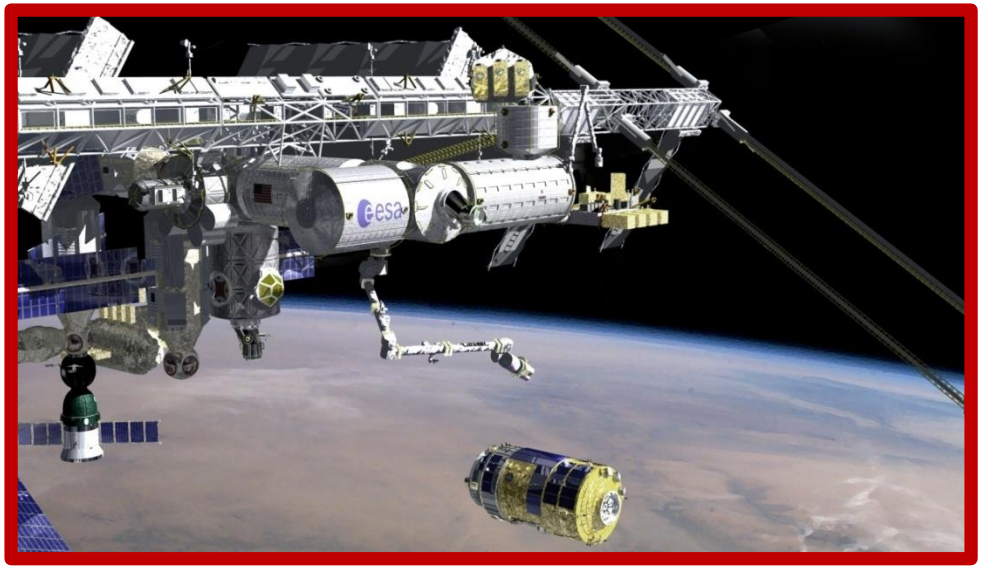
JAXA H-II Transfer Vehicle (HTV)

Takuto Ishimatsu

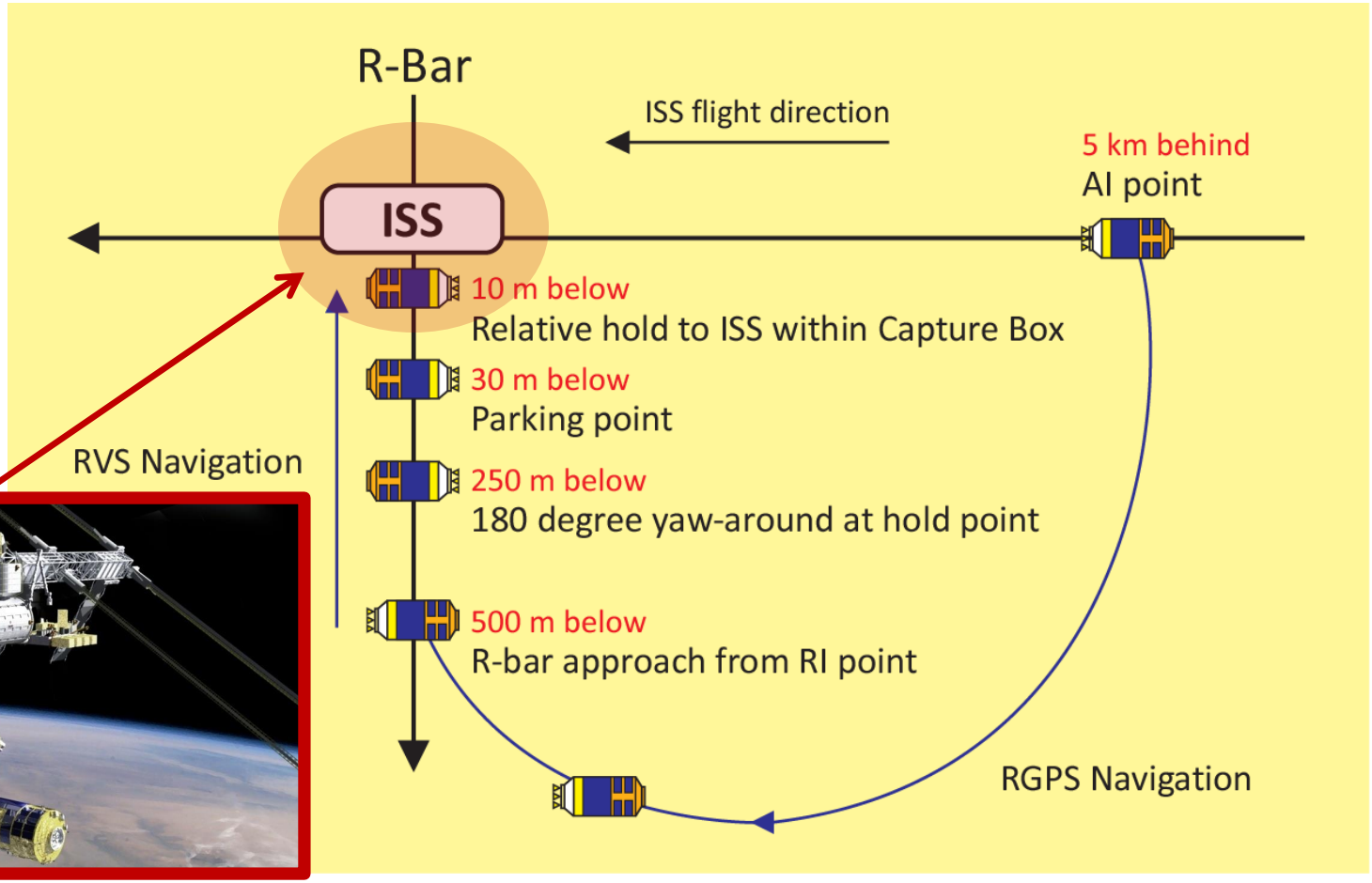
HTV: H-II Transfer Vehicle

- JAXA's unmanned cargo transfer spacecraft
  - Launched from the Tanegashima Space Center aboard the H-IIB rocket
  - Delivers supplies to the International Space Station (ISS)
  - HTV-1 (Sep '09) and HTV-2 (Jan '11) were completed successfully
  - **Proximity operations** involve the ISS (including crew) and NASA and JAXA ground stations





Capture Operation

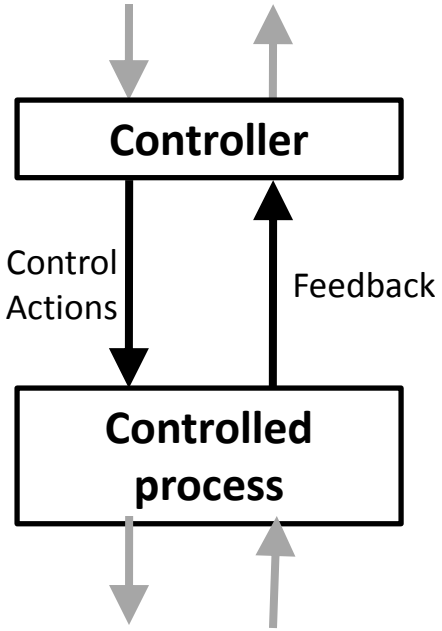


Basic Information

- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA/JAXA ground stations**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to HTV to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (state vectors and flight mode)
    3. ISS crew manipulates SSRMS (robotic arm) to grapple HTV
  - If HTV drifts out of Capture Box before capture (since it is deactivated), either ISS crew or NASA/JAXA ground stations must activate HTV by sending ***Abort/Retreat/Hold*** commands
  - ISS crew and NASA/JAXA ground stations can communicate with each other using a **voice loop connection** through the entire operation

STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

©

Accidents / Hazards

- Accidents
  - HTV collides with ISS
- Hazards
  - HTV too close to ISS (for given speed)

©

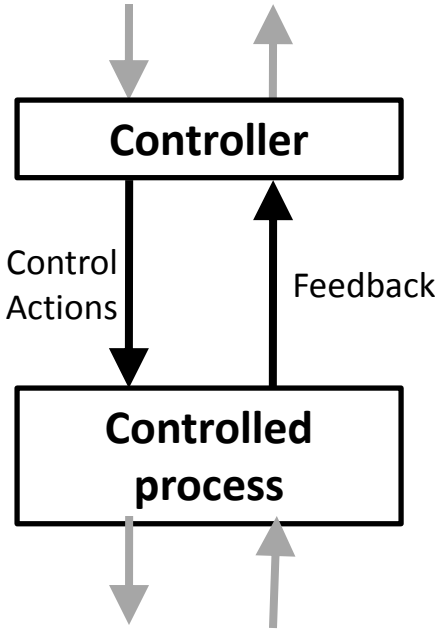
Accidents / Hazards

- Accidents
  - A-1: HTV collides with ISS
  - A-2: Loss of delivery mission
- Hazards
  - H-1: HTV too close to ISS (for given operational phase)
  - H-2: HTV trajectory makes delivery impossible
- System Safety Constraints
  - ?

©

STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

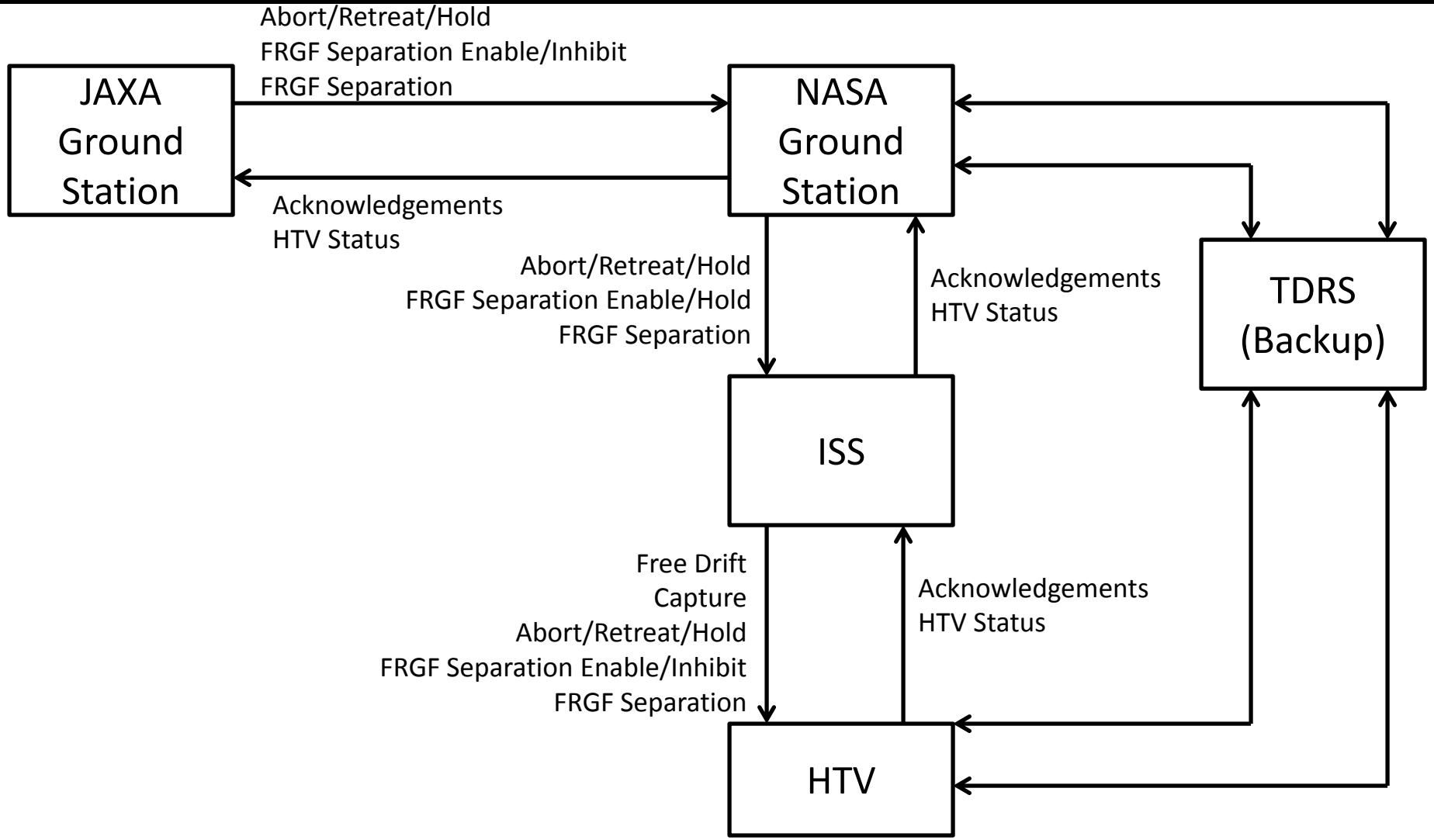
©

Control structure

- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA/JAXA ground stations**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to HTV to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (state vectors and flight mode)
    3. ISS crew manipulates SSRMS (robotic arm) to grapple HTV
  - If HTV drifts out of Capture Box before capture (since it is deactivated), either ISS crew or NASA/JAXA ground stations must activate HTV by sending ***Abort/Retreat/Hold*** commands
  - ISS crew and NASA/JAXA ground stations can communicate with each other using a **voice loop connection** through the entire operation

©

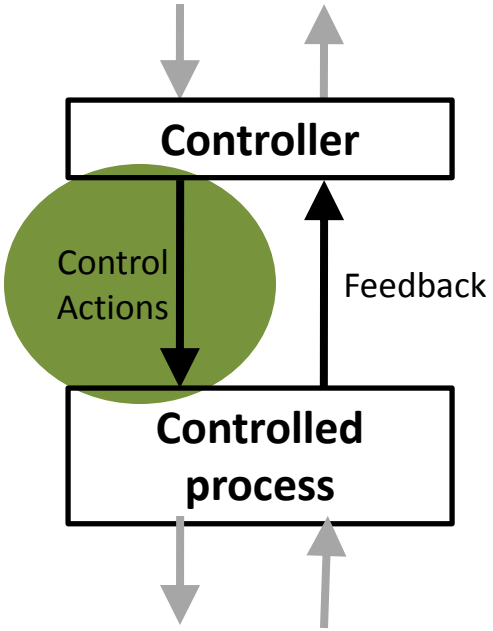
Control Structure



©

STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- **Step 1: Identify unsafe control actions**
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

©

Unsafe Control Actions

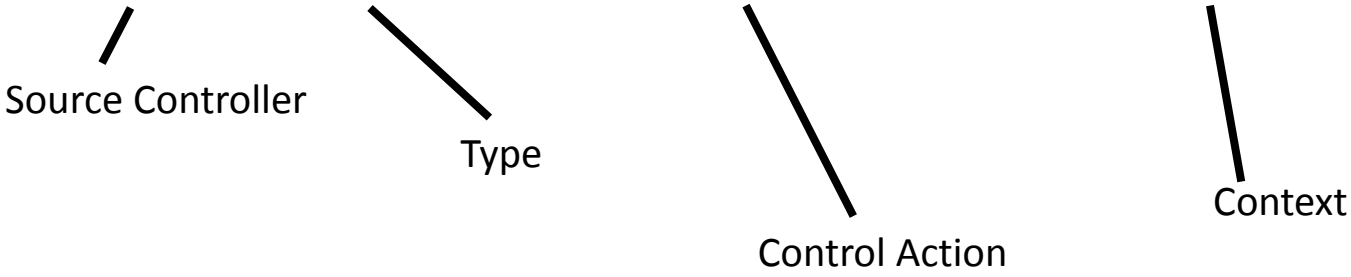
	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Abort				
Free Drift				
Capture				

©

Actual Astronaut Control Interface

Unsafe Control Actions

Example:
"Computer provides open catalyst valve cmd while water valve is closed"



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Abort				
Free Drift				
Capture				

© Copyright John Thomas 2014

Step 1: Unsafe Control Actions

Unsafe control actions leading to Hazard H-1: HTV too close to ISS (for given operational phase)

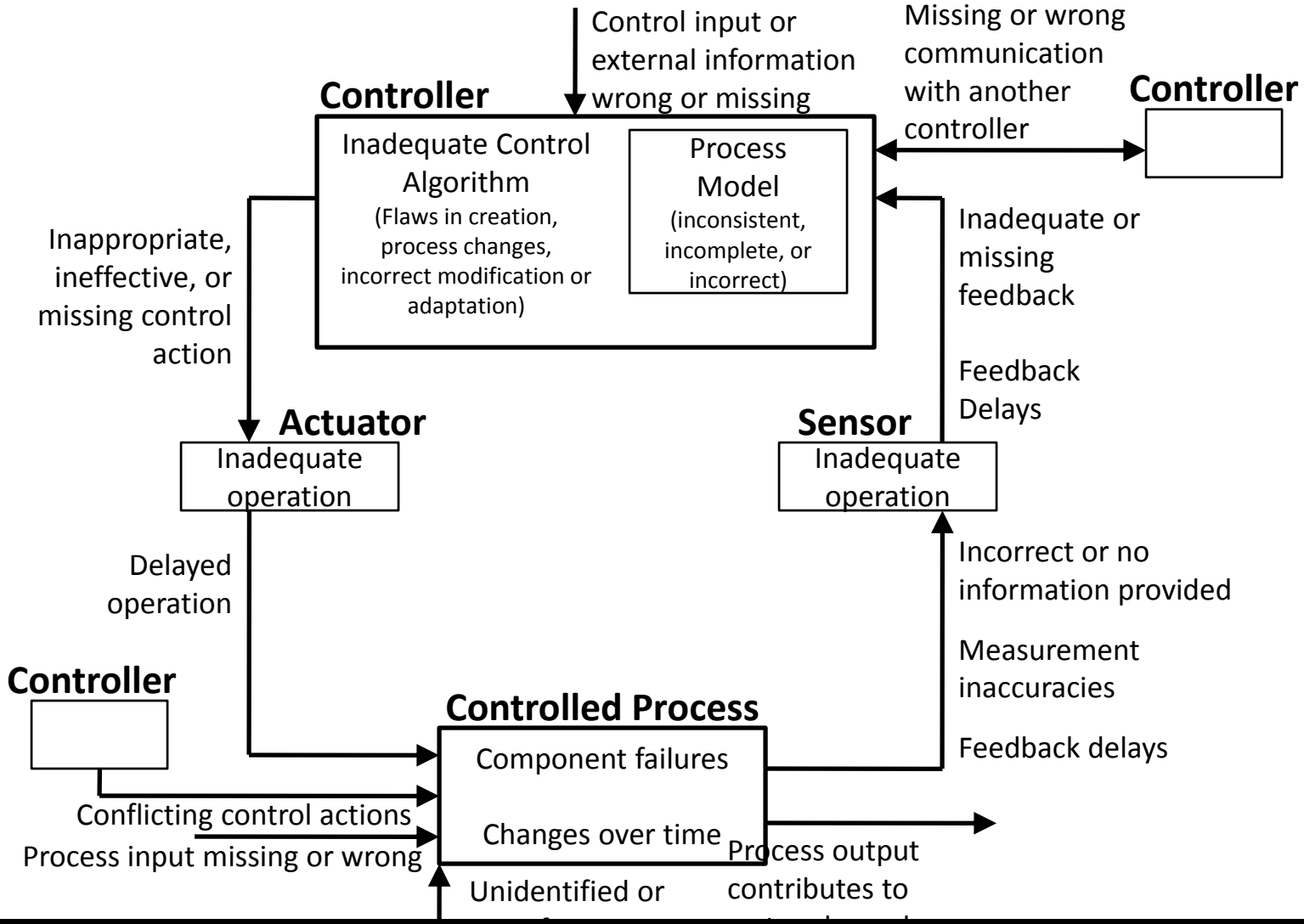
Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
Free Drift (Deactivation)	**[UCA4]** HTV is not deactivated when ready for capture	**[UCA5]** HTV is deactivated when not appropriate (e.g., while still approaching ISS)	EARLY: **[UCA6]** HTV is deactivated while not ready for immediate capture LATE: **[UCA7]** HTV is not deactivated for a long time while FRGF separation is enabled	
Execute Capture	**[UCA8]** Capture is not executed while HTV is deactivated	**[UCA9]** Capture is attempted when HTV is not deactivated **[UCA10]** SSRMS hits HTV inadvertently	EARLY: **[UCA11]** Capture is executed before HTV is deactivated LATE: **[UCA12]** Capture is not executed within a certain amount of time	**[UCA13]** Capture operation is stopped halfway and not completed
Abort Retreat Hold	**[UCA17]** Abort/Retreat/Hold is not executed when necessary (e.g., when HTV is drifting to ISS while uncontrolled)	**[UCA18]** Abort/Retreat/Hold is executed when not appropriate (e.g. after successful capture)	LATE: **[UCA19]** Abort/Retreat/Hold is executed too late when immediately necessary (e.g., when HTV is drifting to ISS while uncontrolled)	

©

STPA Control Flaws

UCA-1: ISS Crew does not perform capture within X sec of HTV deactivation [H-1, H-2]

UCA-2: ISS Crew provides free drift command while HTV approaching ISS [H-1, H-2]



Actual Astronaut Control Interface

Actual operating events

- Did you anticipate these actual issues during the STPA exercise?
- If you applied this process early, how much would it cost to address them?