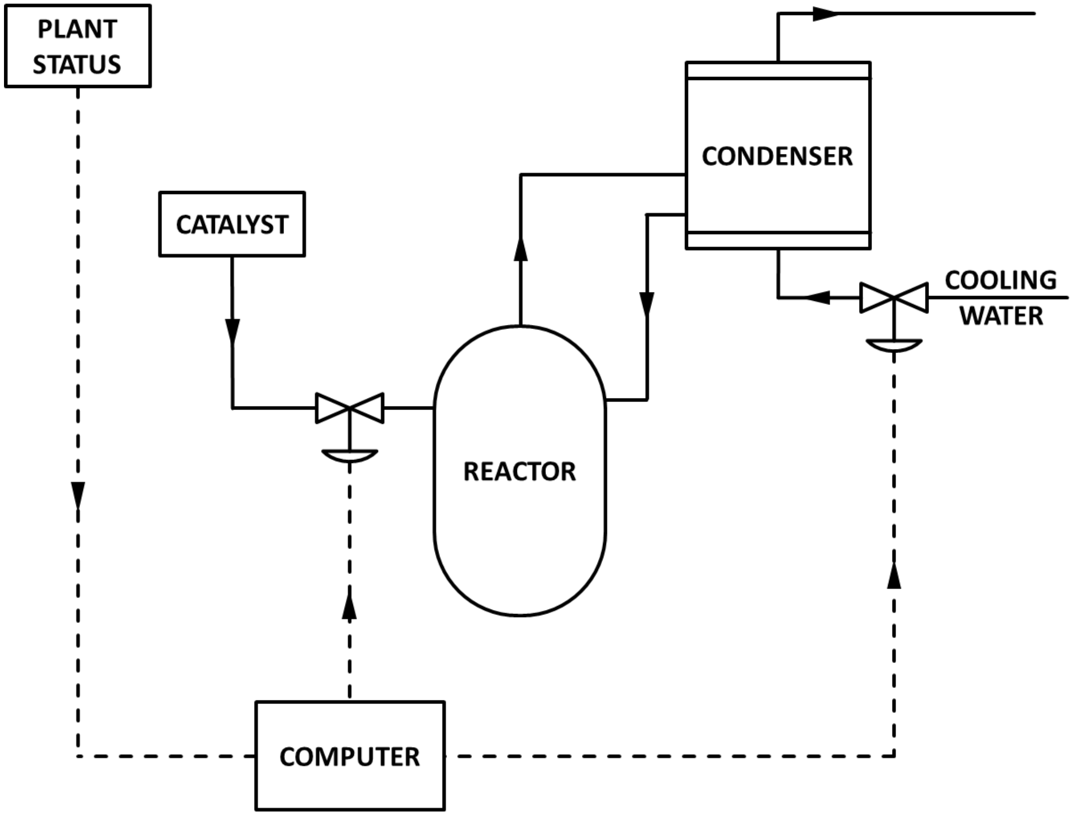
Basic STPA: Exercises

Dr. John Thomas

Any Questions? Email me! JThomas4@mit.edu

Chemical Reactor Design

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



What are the system accidents and system hazards?

Diagram adapted Trevor Kletz, 1982

Chemical Reactor Design

System Accidents

- A-1: People die or become injured
- A-2: Production loss
- Etc.

System Hazards

- H-1: Plant releases toxic chemicals
- H-2: Plant is unable to produce chemical X
- Etc.

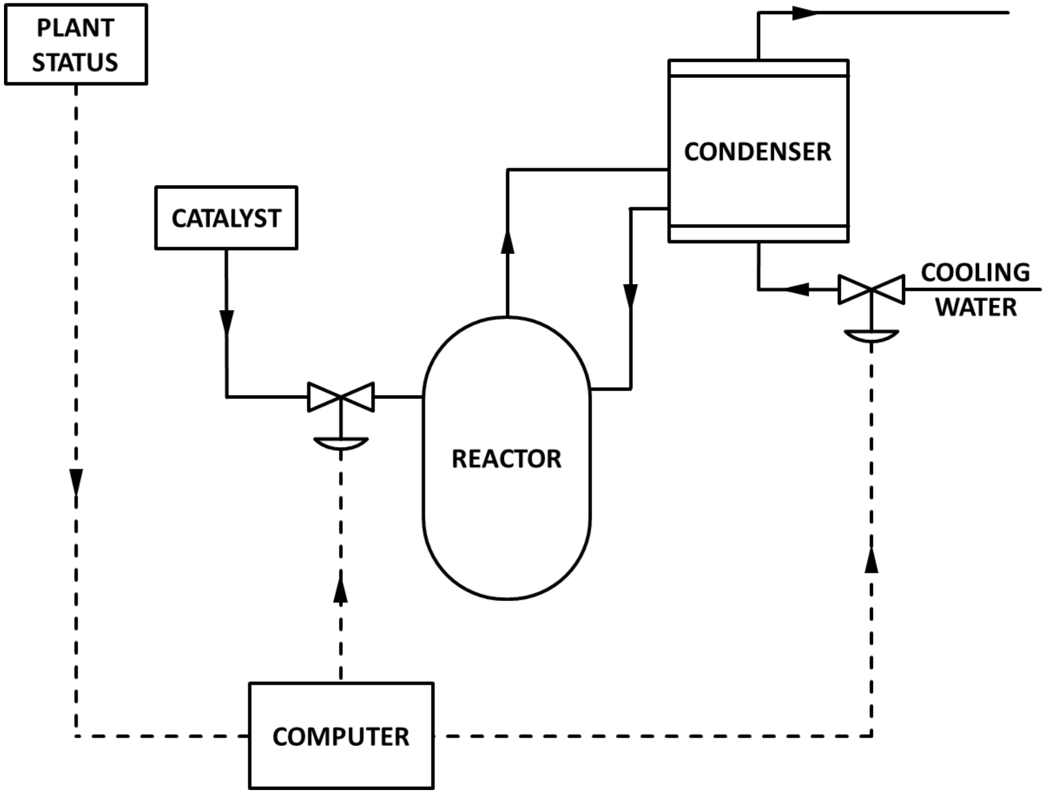
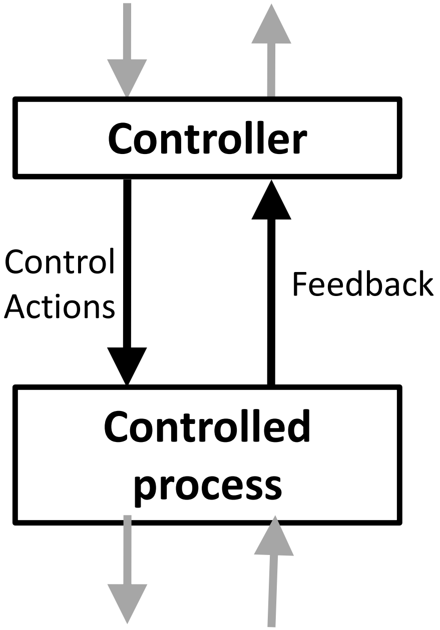


Diagram adapted Trevor Kletz, 1982

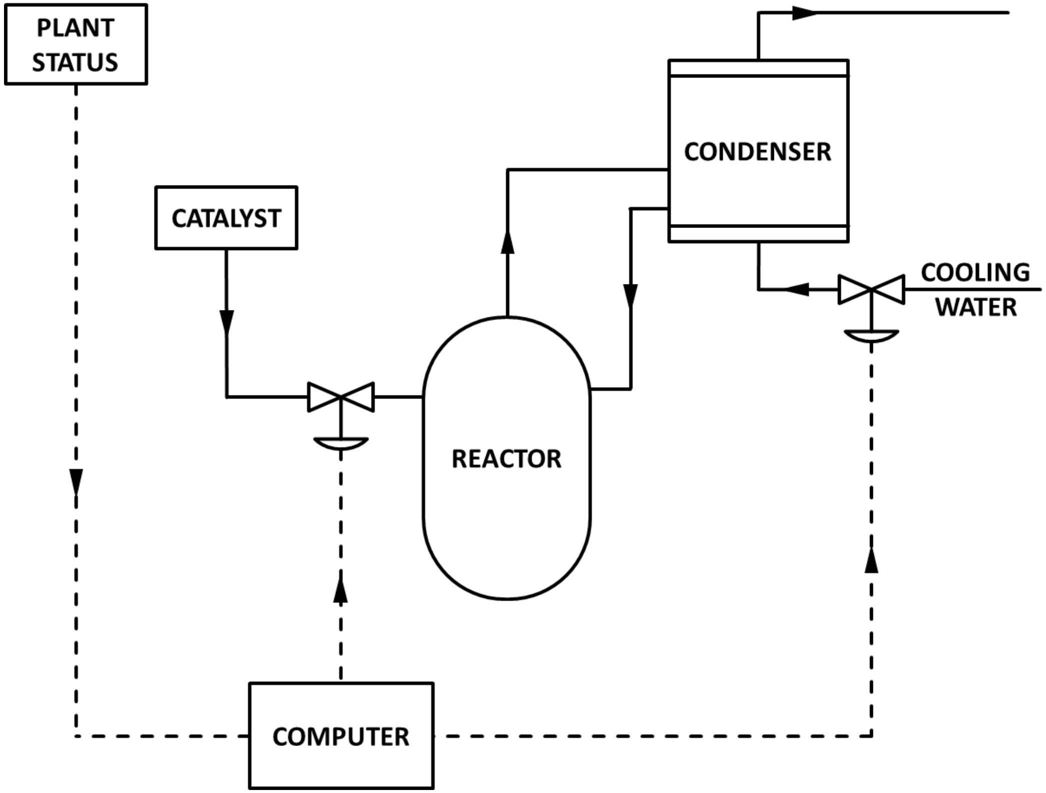
STPA
(System-Theoretic Process Analysis)

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



Chemical Reactor Design

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



Create Control Structure

Diagram adapted Trevor Kletz, 1982

STPA Analysis

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

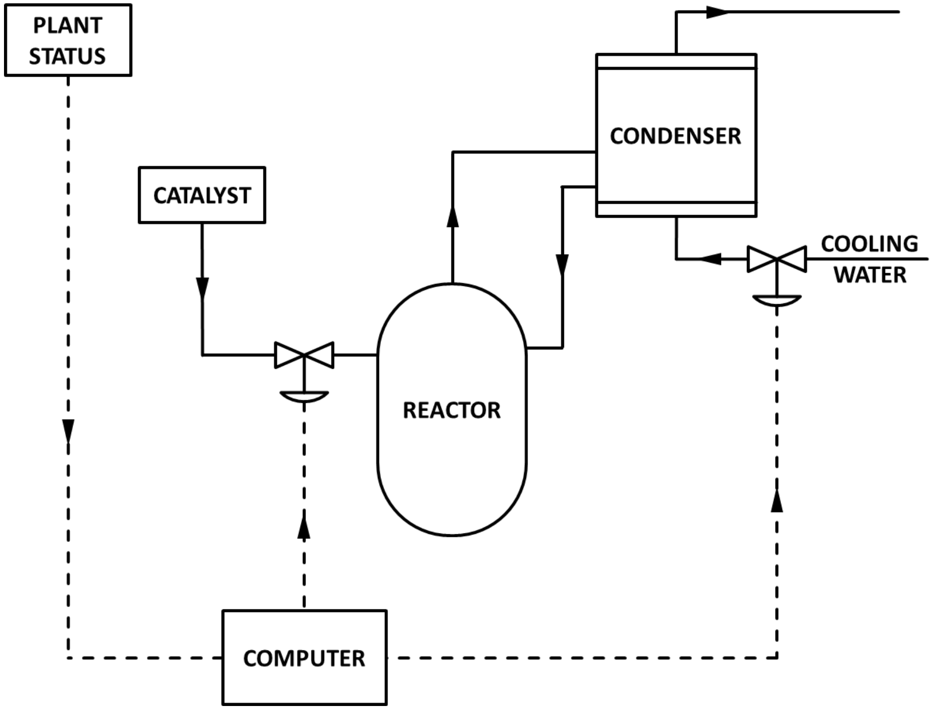
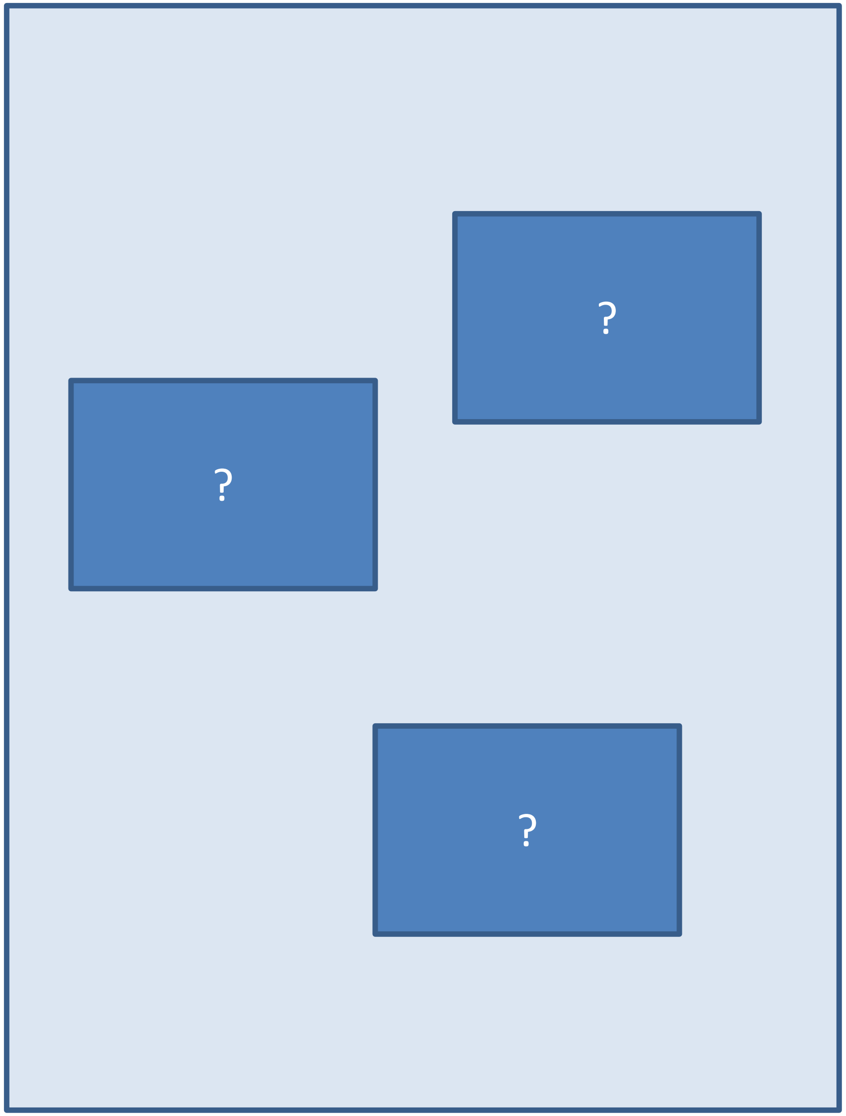


Diagram adapted Trevor Kletz, 1982



STPA Analysis

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

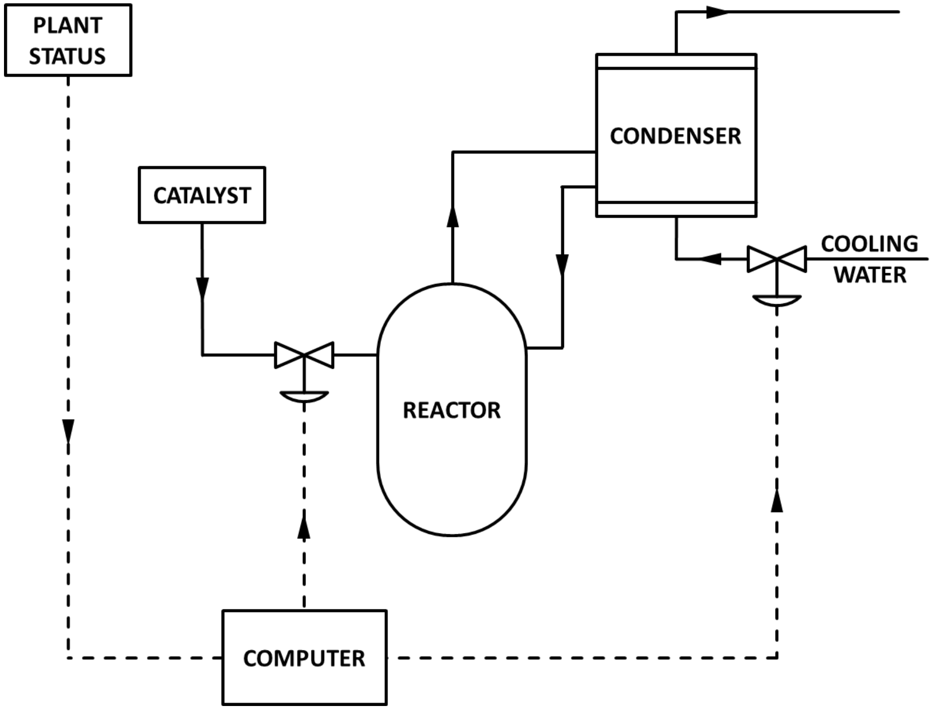
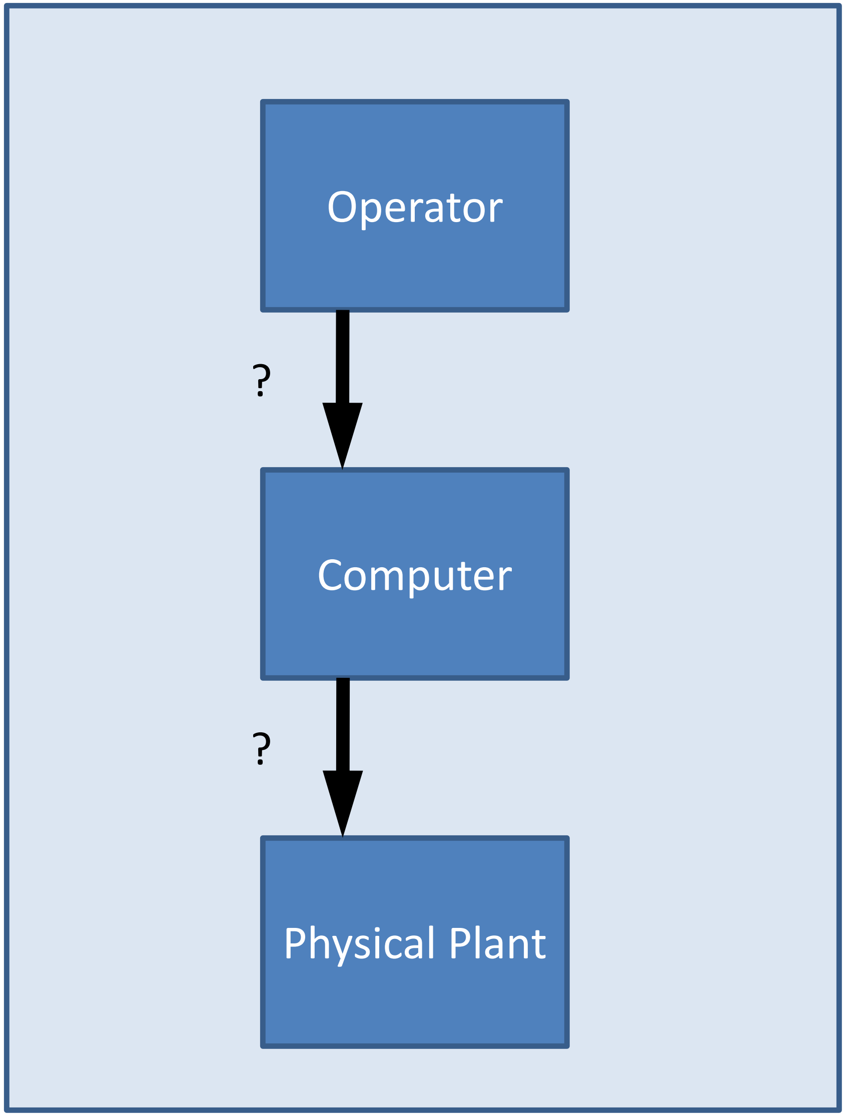


Diagram adapted Trevor Kletz, 1982



STPA Analysis

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

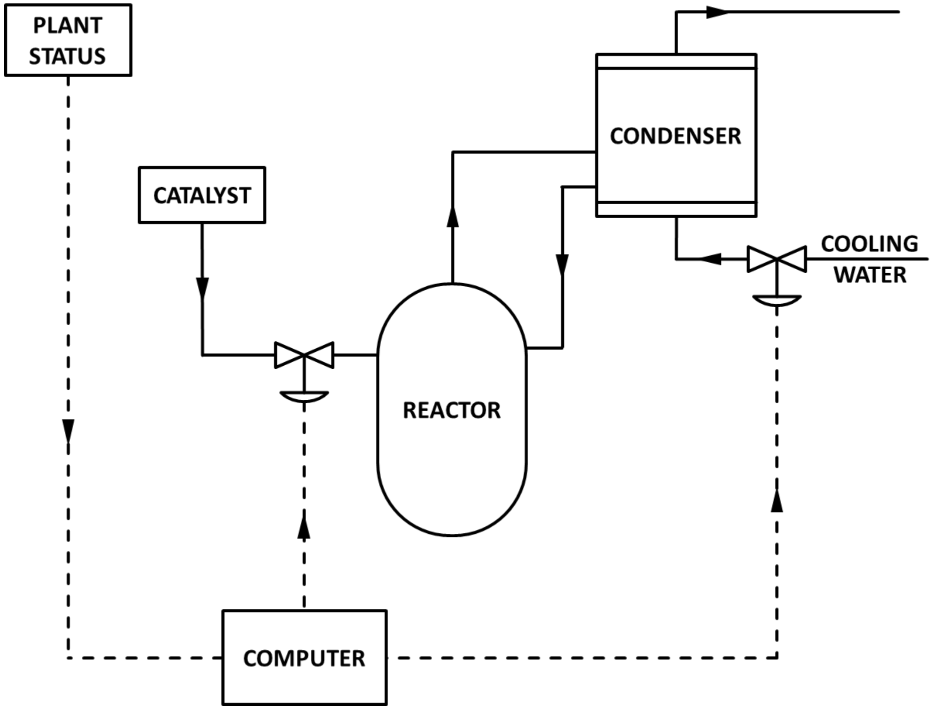
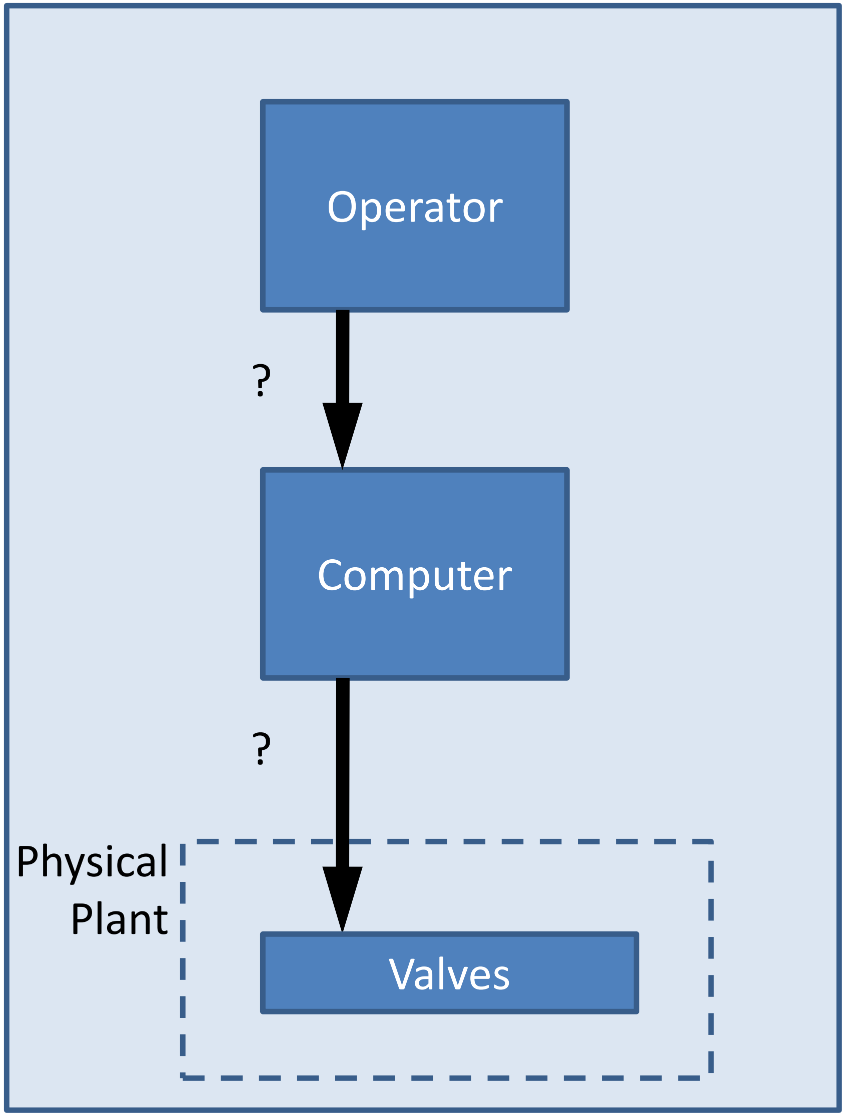


Diagram adapted Trevor Kletz, 1982



STPA Analysis

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

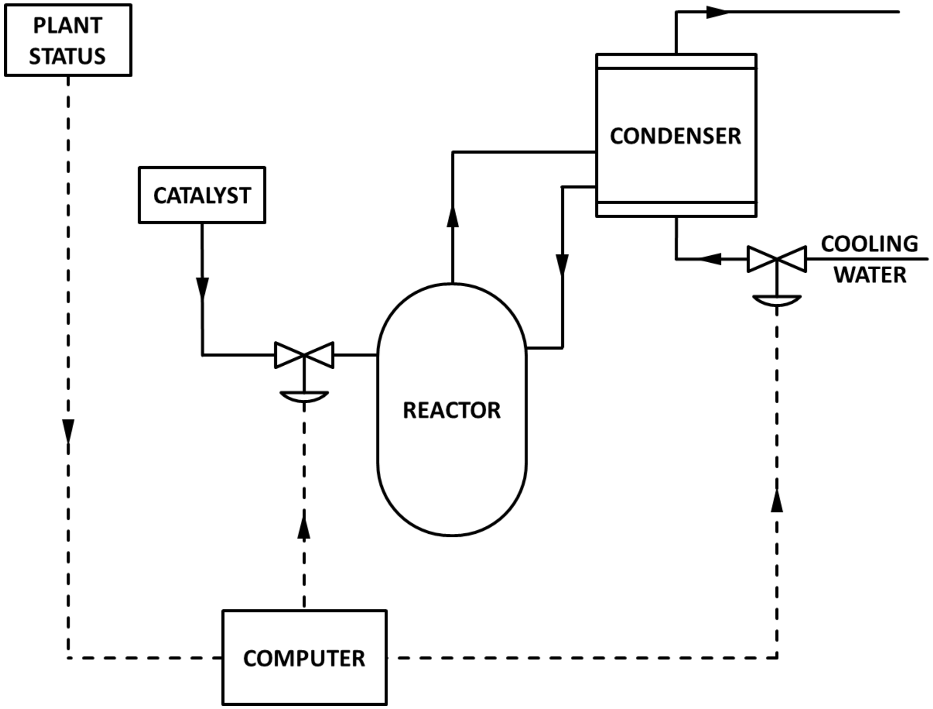
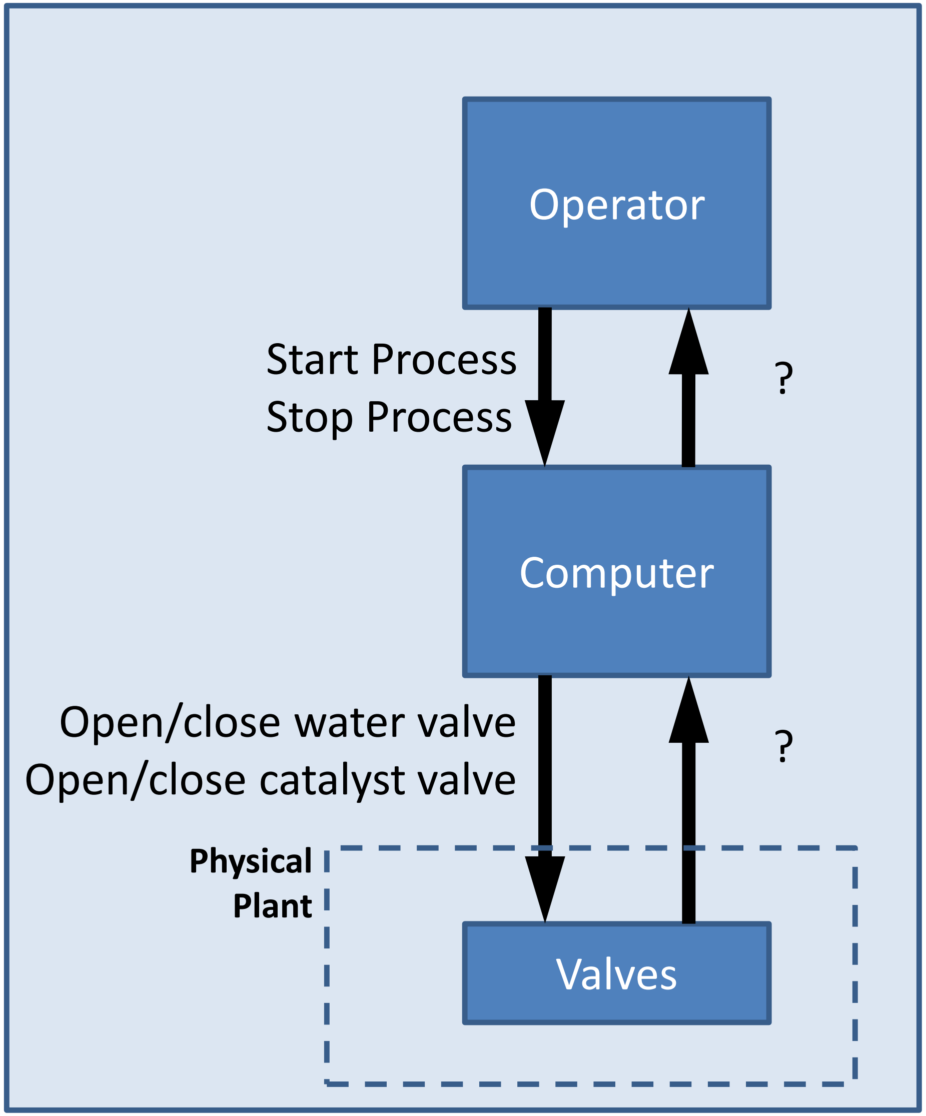


Diagram adapted Trevor Kletz, 1982



STPA Analysis: Control Structure

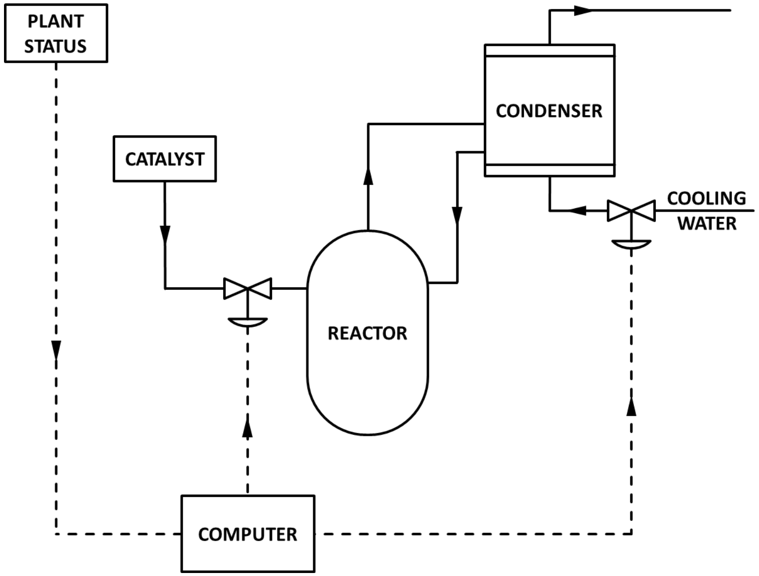
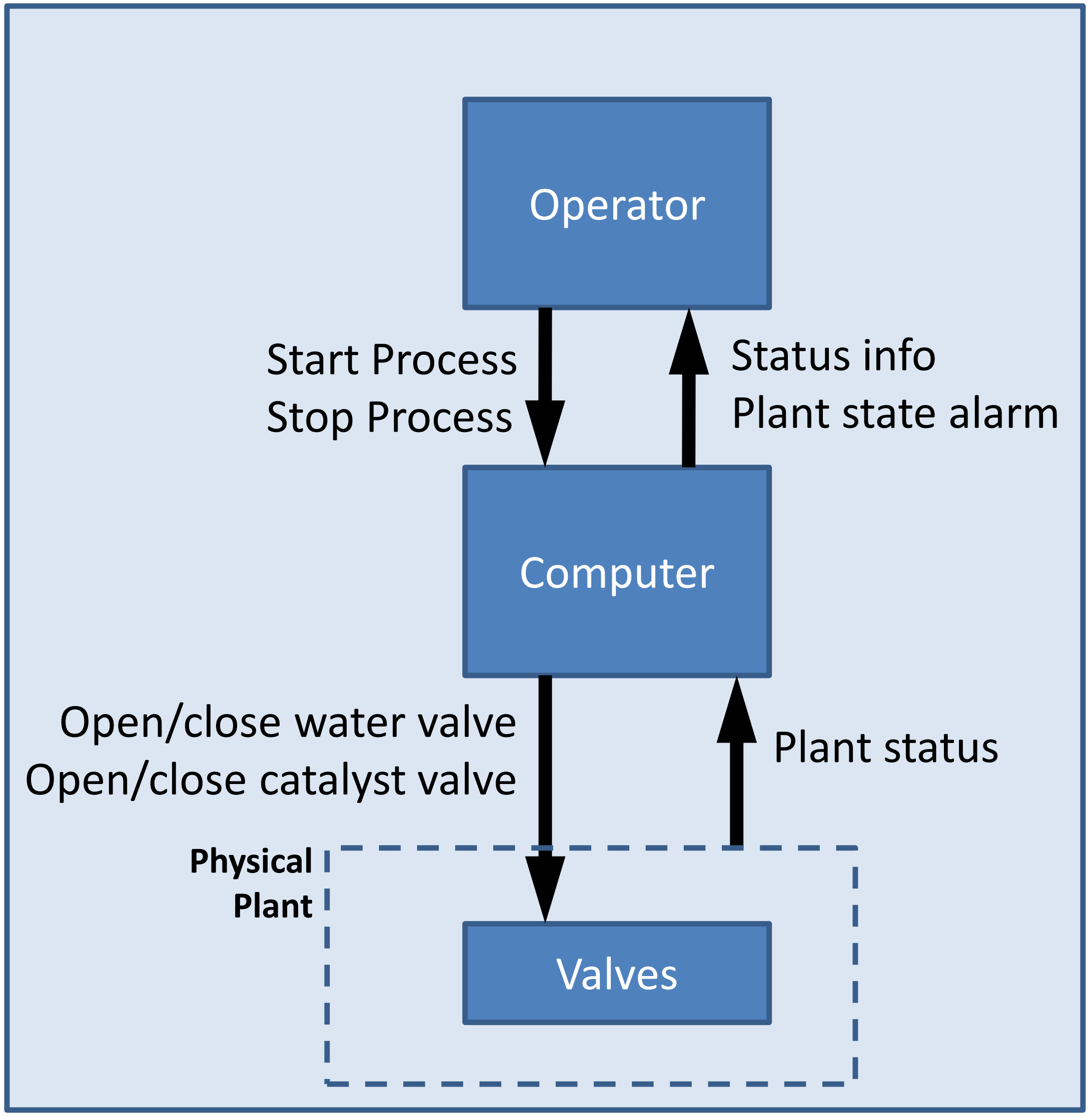
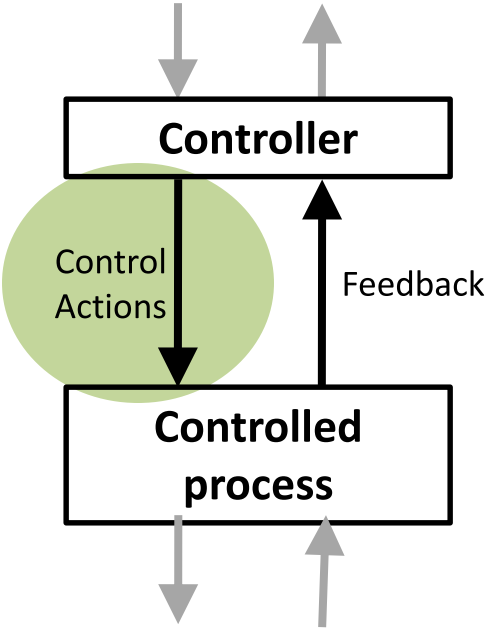


Diagram adapted Trevor Kletz, 1982



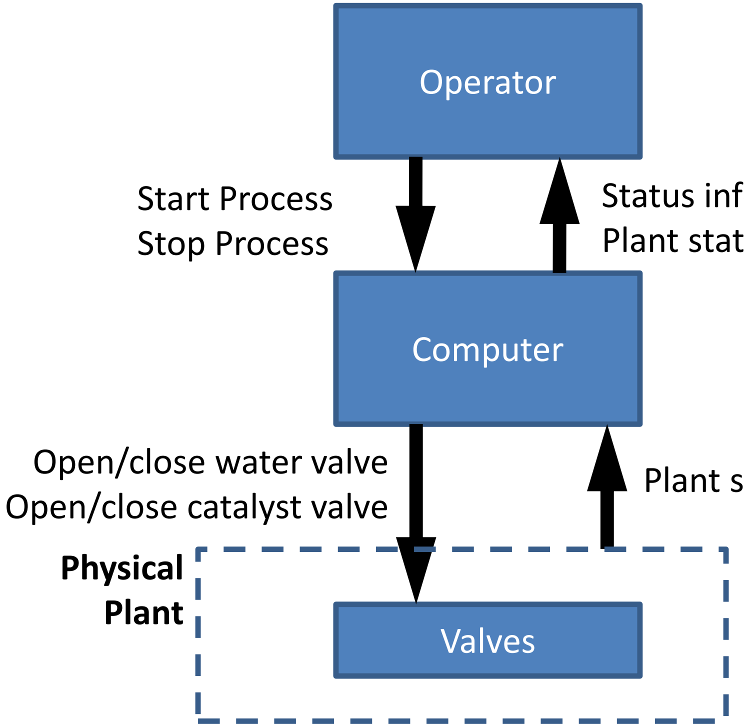
STPA
(System-Theoretic Process Analysis)

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



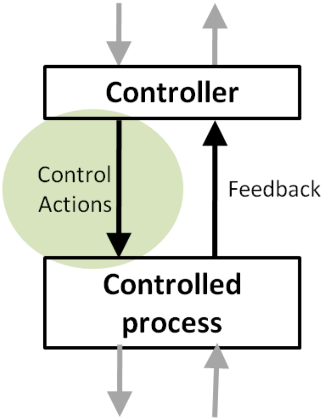
Chemical Reactor: Unsafe Control Actions

Control Structure:

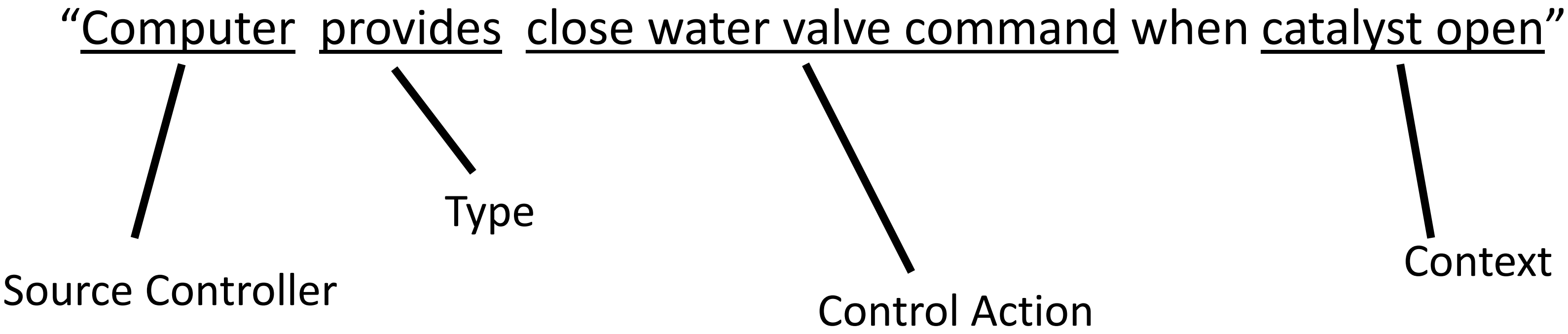


	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve	?	Computer provides Close Water Valve cmd while catalyst open	?	?

Structure of an Unsafe Control Action



Example:



“Computer provides close water valve command when catalyst open”

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)

(Thomas, 2013)

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 provides close water valve cmd while catalyst open	Computer provides close water valve cmd before catalyst closes	
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
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	
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

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
- 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	OK	No	No
Open water valve when:	Open	Closed	OK	No	No
Open water valve when:	Closed	Open	OK	No	Yes
Open water valve when:	Closed	Closed	OK	No	No
Open water valve when:	Open	Open	Not OK	No	No
Open water valve when:	Open	Closed	Not OK	No	No
Open water valve when:	Closed	Open	Not OK	No	Yes
Open water valve when:	Closed	Closed	Not OK	No	No

(Thomas, 2013)

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

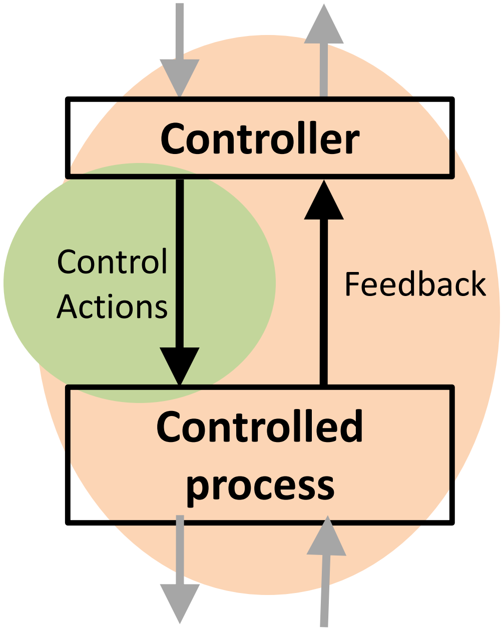
UCA-1: Computer does not opens water valve when catalyst valve is open and water valve is closed

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

(Thomas, 2013)

STPA
(System-Theoretic Process Analysis)

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



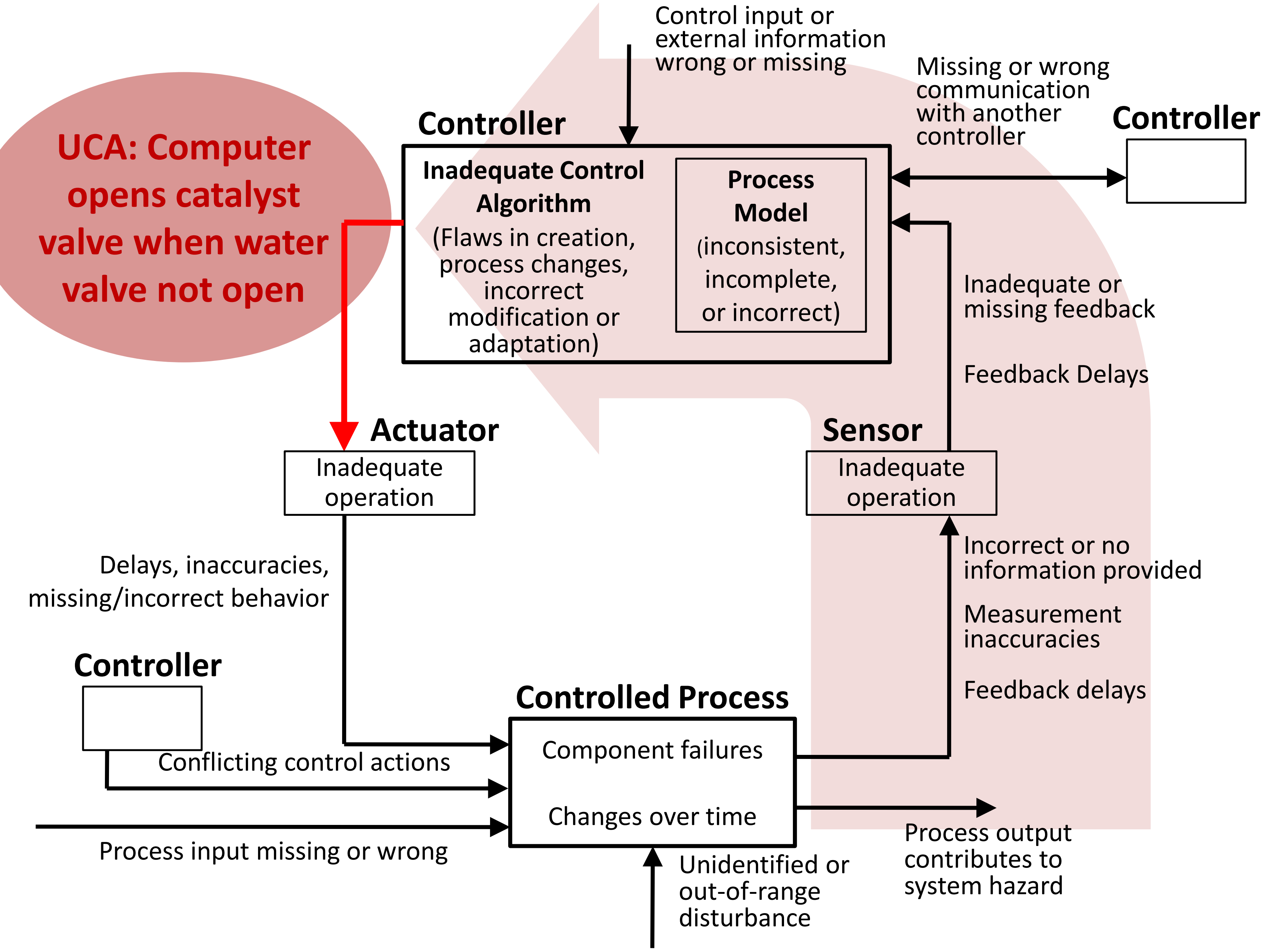
Controller

Control Actions

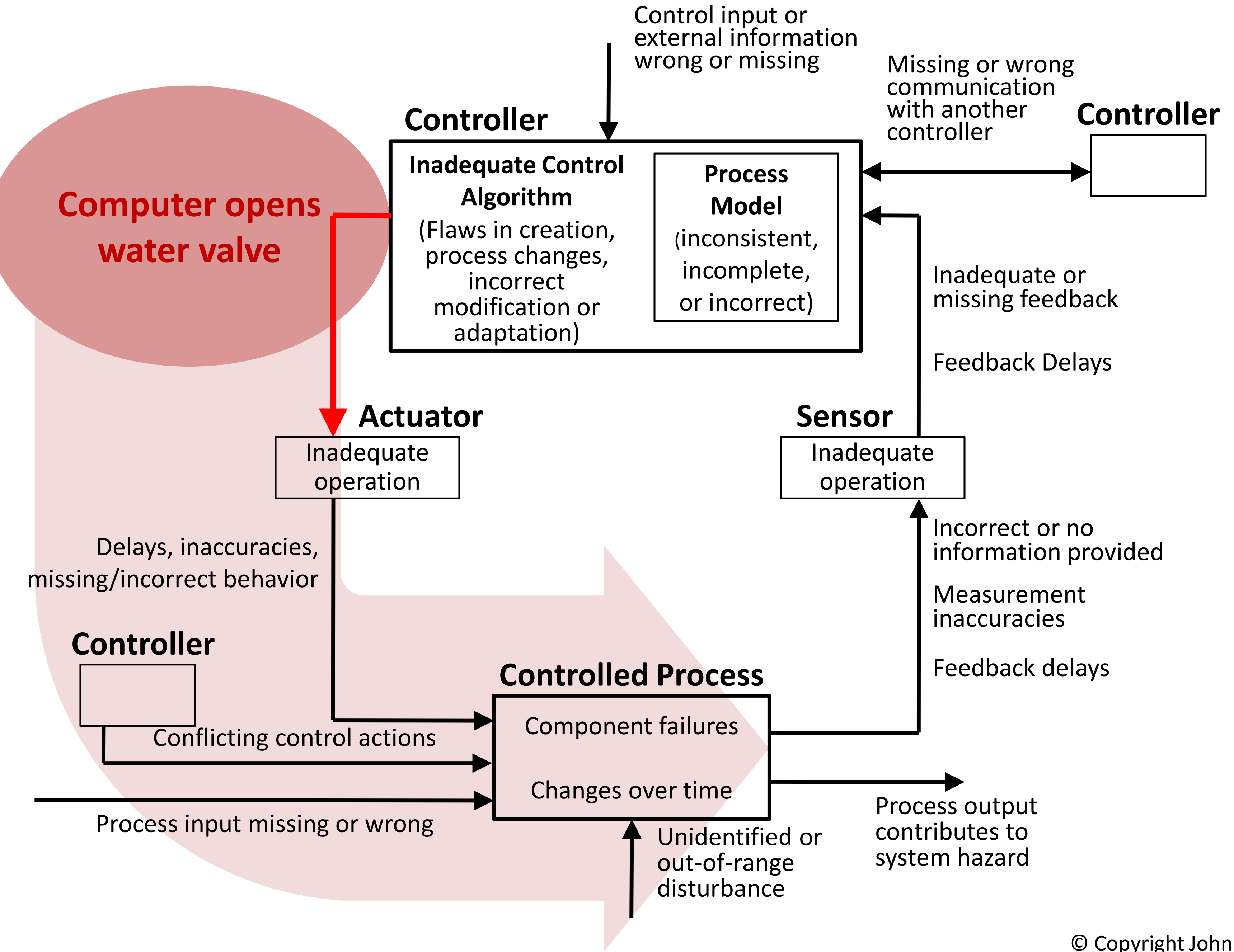
Feedback

Controlled process

Step 2: Potential causes of UCAs


UCA: Computer opens catalyst valve when water valve not open
Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or incorrect)
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delays, inaccuracies, missing/incorrect behavior
Controller
Conflicting control actions
Controlled Process
Component failures
Changes over time
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Step 2: Potential control actions not followed



Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)

Process Model
(inconsistent, incomplete, or incorrect)

Computer opens water valve

Inadequate or missing feedback

Feedback Delays

Actuator
Inadequate operation

Sensor
Inadequate operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Delays, inaccuracies, missing/incorrect behavior

Controller

Controlled Process
Component failures
Changes over time

Conflicting control actions

Process input missing or wrong

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Chemical Reactor: Real accident

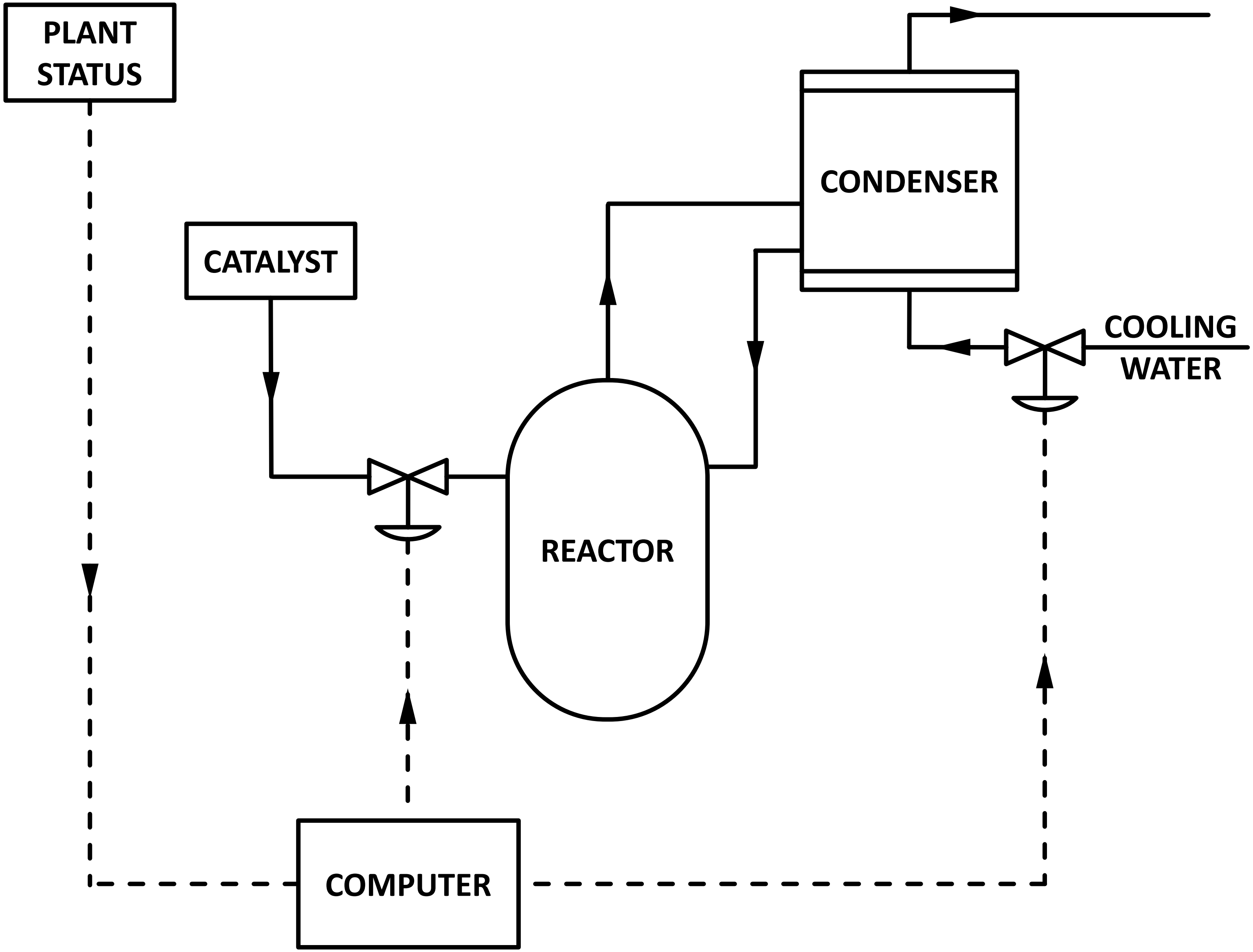


Diagram adapted Trevor Kletz, 1982

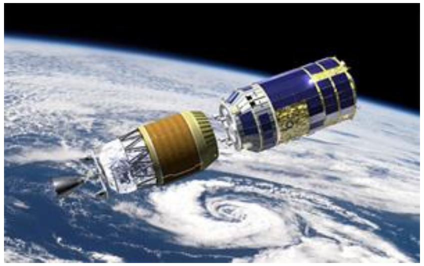
STAMP/STPA – Advanced Tutorial

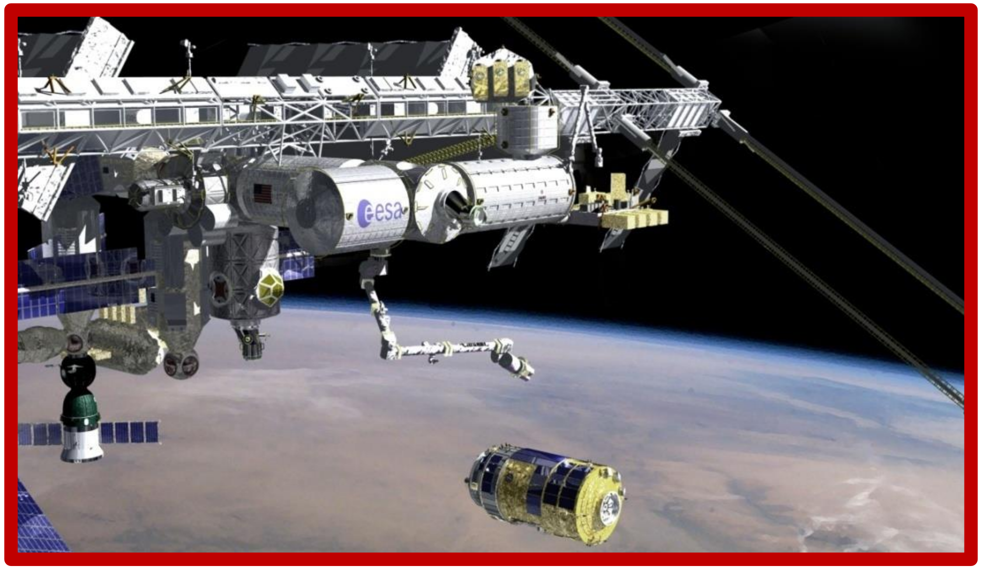
JAXA H-II Transfer Vehicle (HTV)

Takuto Ishimatsu

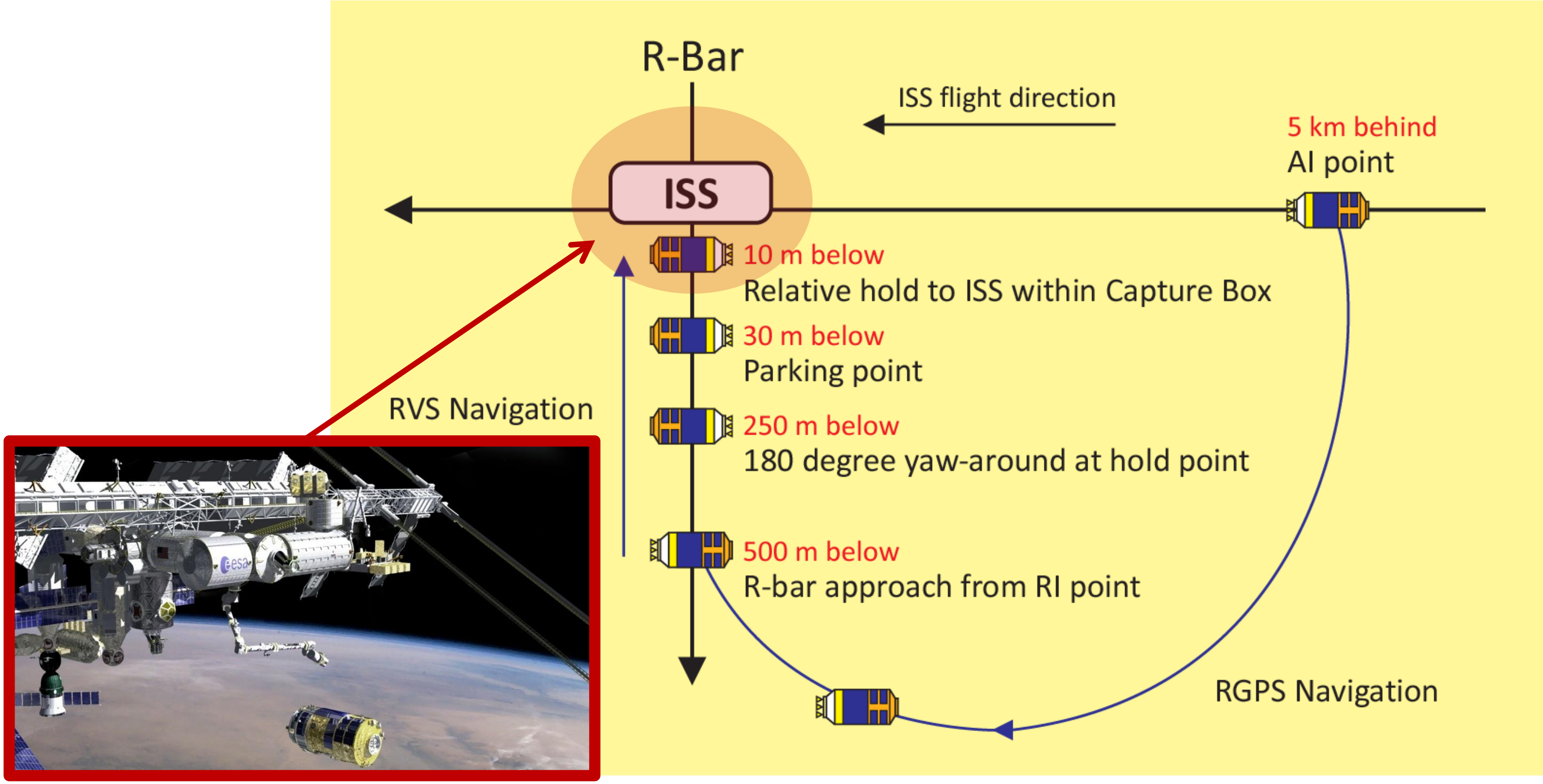
HTV: H-II Transfer Vehicle

- 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



R-Bar

ISS flight direction

ISS

5 km behind
AI point

10 m below
Relative hold to ISS within Capture Box

30 m below
Parking point

250 m below
180 degree yaw-around at hold point

500 m below
R-bar approach from RI point

RVS Navigation

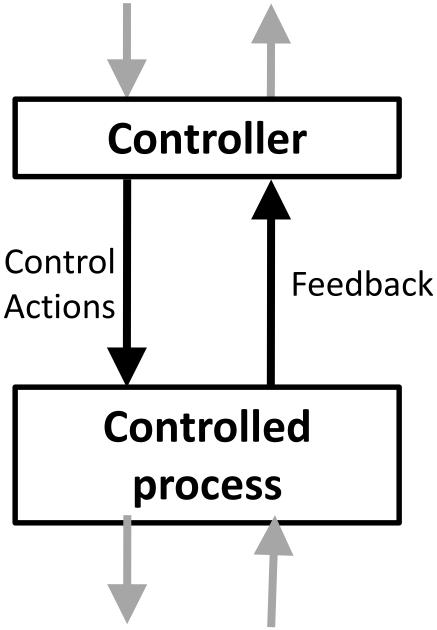
RGPS Navigation

Basic Information

- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA ground station**
  - **JAXA ground station**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to deactivate HTV (by radio) to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (activated/deactivated mode, fault status) to ISS and ground stations
    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, NASA, or JAXA must activate HTV by sending ***Abort/Retreat/Hold*** commands to the HTV. Abort is final (HTV ignores all future commands) and irrecoverable; HTV will fire thrusters to maneuver away from ISS.
  - 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 system hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



Accidents / Hazards

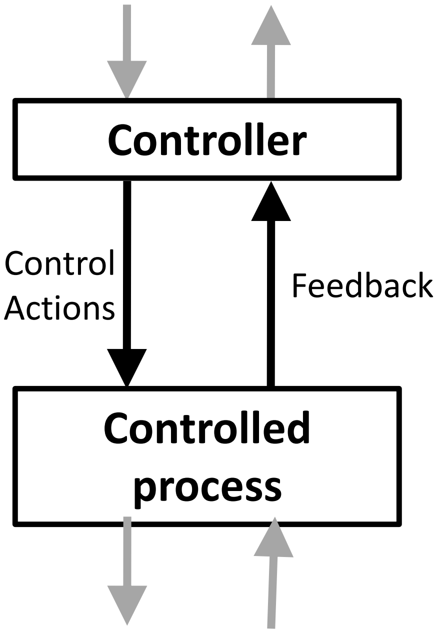
- Loss event (Accident)
  - – HTV collides with ISS
- Hazards
  - – HTV too close to ISS (for given speed)

Accidents / Hazards

- Loss events (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 system hazards
- ➡ Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios

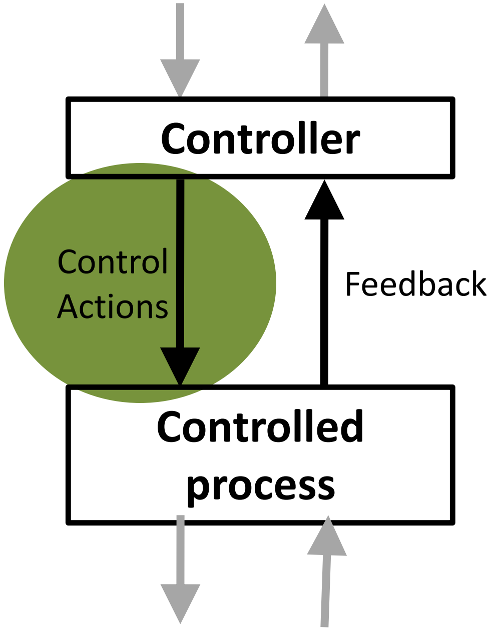


Basic Information

- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA ground station**
  - **JAXA ground station**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to deactivate HTV (by radio) to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (activated/deactivated mode, fault status) to ISS and ground stations
    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, NASA, or JAXA must activate HTV by sending ***Abort/Retreat/Hold*** commands to the HTV. Abort is final (HTV ignores all future 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 system hazards
- ✓ Draw the control structure
- **Step 1: Identify unsafe control actions**
- Step 2: Identify causal factors and create scenarios



STPA Step 1: Unsafe Control Actions

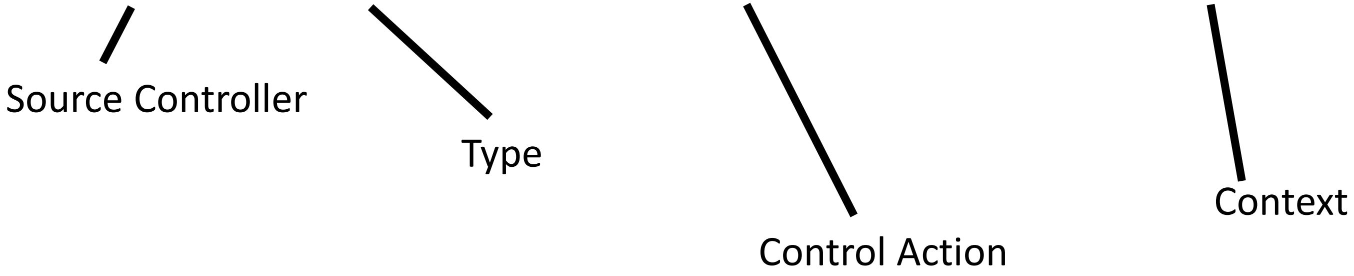
ISS Crew UCAs

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

STPA Step 1: Unsafe Control Actions

Example:

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



Source Controller

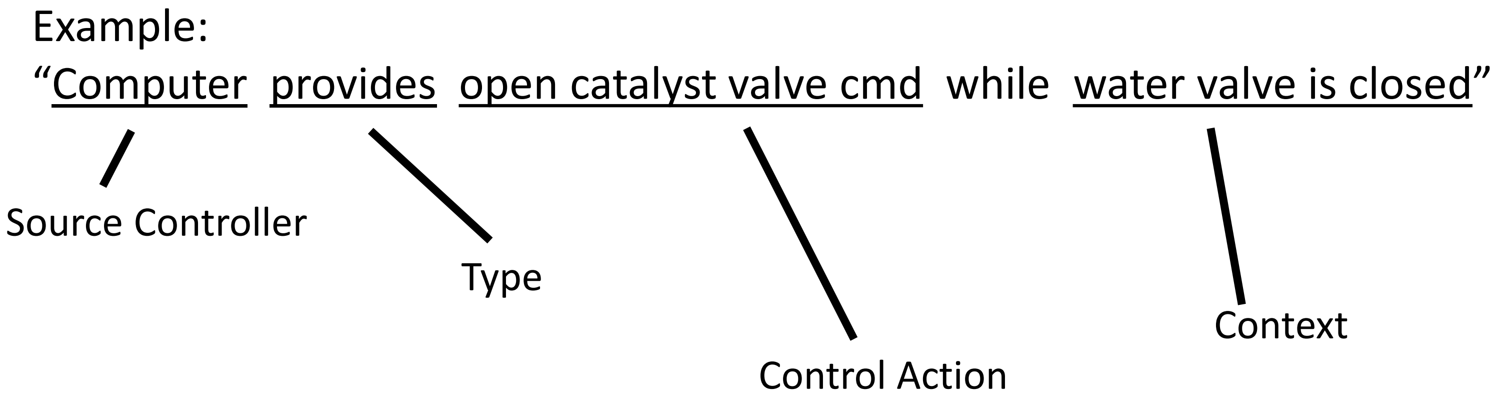
Type

Control Action

Context

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

STPA Step 1: Unsafe Control Actions

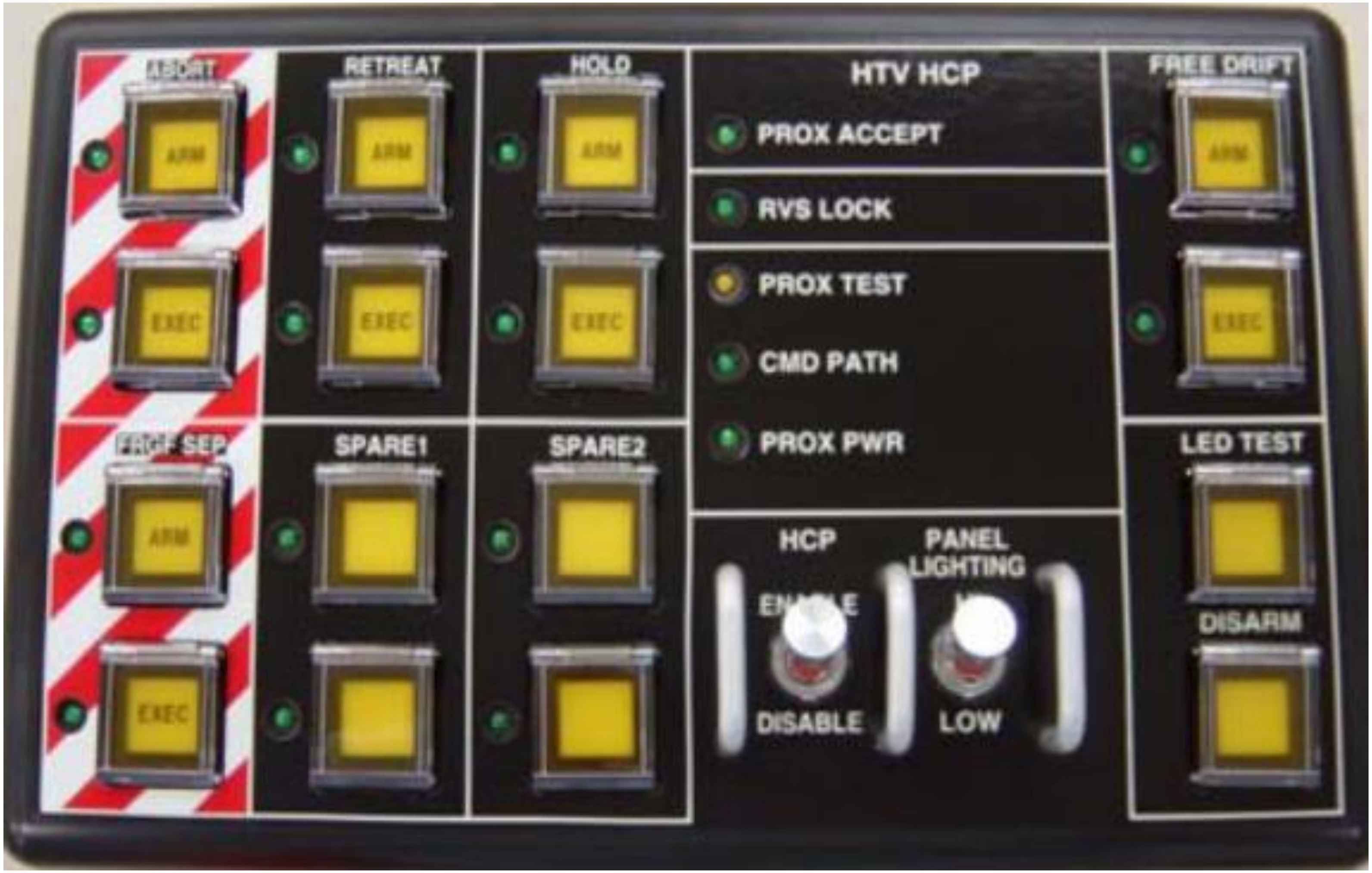


Example:

"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	ISS crew does not provide abort when ______	ISS crew provides abort when ______	ISS crew provides abort too late after ______	
Free Drift				
Capture				

Actual Astronaut Control Interface



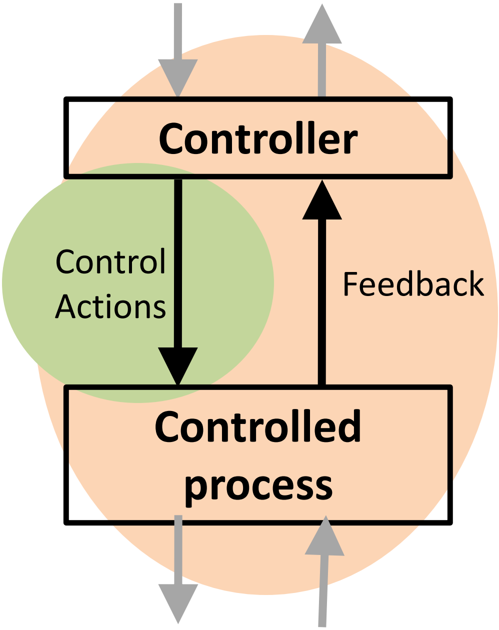
Step 1: Unsafe Control Actions

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
(System-Theoretic Process Analysis)

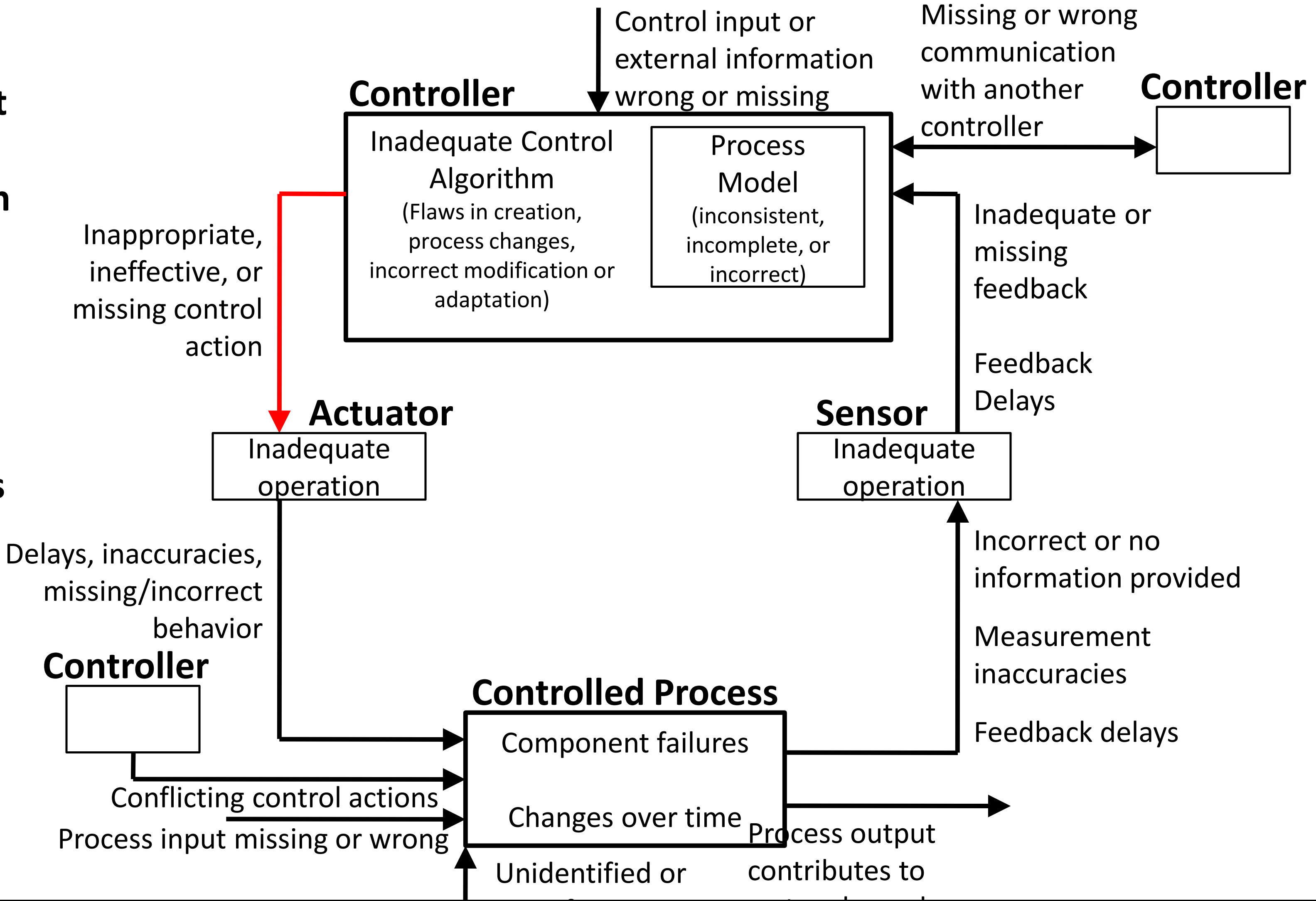
- ✓ Identify accidents and system hazards
- ✓ Draw the control structure
- ✓ Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



STPA Step 2: Accident Scenarios

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]


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

Actual Astronaut Control Interface