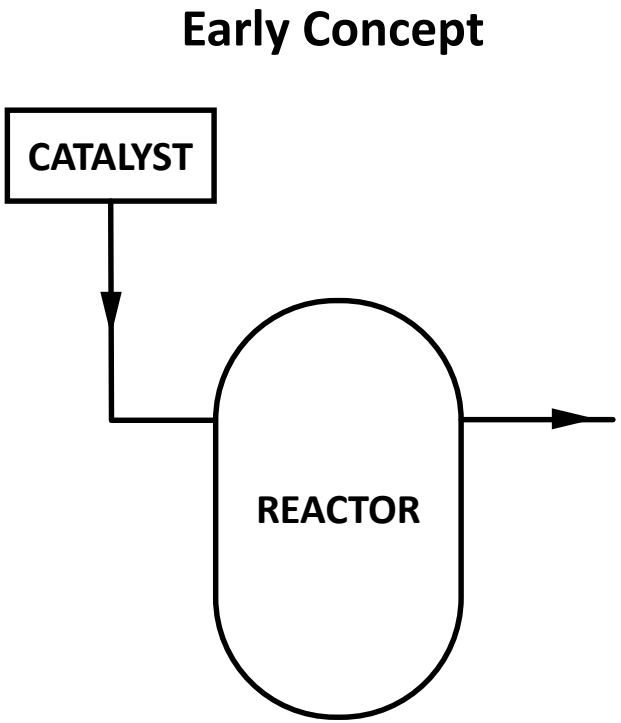
Basic STPA Exercises

Dr. John Thomas

Chemical Plant

- Goal: To produce and sell chemical X
- What (System): A chemical plant (production), …
- How (Method): By means of a chemical reaction, a catalyst, ….



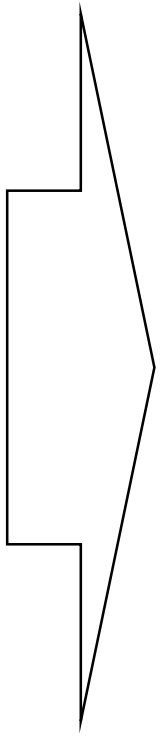
System-Theoretic Process Analysis (STPA)

- Identify accidents (losses), hazards
- Draw hierarchical control structure
- Identify unsafe control actions
- Identify accident scenarios

(Leveson, 2012)

STPA

- Goal: To produce and sell chemical X
- What (System): A chemical plant, …
- How (Method): By means of a chemical reaction, a catalyst, ….



Accidents (Mishaps)

- A-1: People exposed to chemicals
- A-2: People physically injured (e.g. explosion)
- A-3: Production loss
- Etc.

Hazards

- H-1: Plant releases toxic chemicals (e.g. to air, ground, etc.) [A-1]
- H-2: Overpressurization of plant equipment [A-1, A-2, A-3]
- H-3: Plant is unable to produce chemical X [A-3]
- Etc.

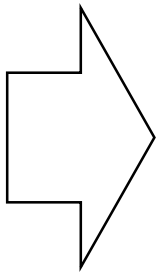
STPA

Accidents (Mishaps)

- A-1: People exposed to chemicals
- A-2: People physically injured (e.g. explosion)
- A-3: Production loss
- Etc.

Hazards

- H-1: Plant releases toxic chemicals (e.g. to air, ground, etc.) [A-1]
- H-2: Overpressurization of plant equipment [A-1, A-2, A-3]
- H-3: Plant is unable to produce chemical X [A-3]
- Etc.

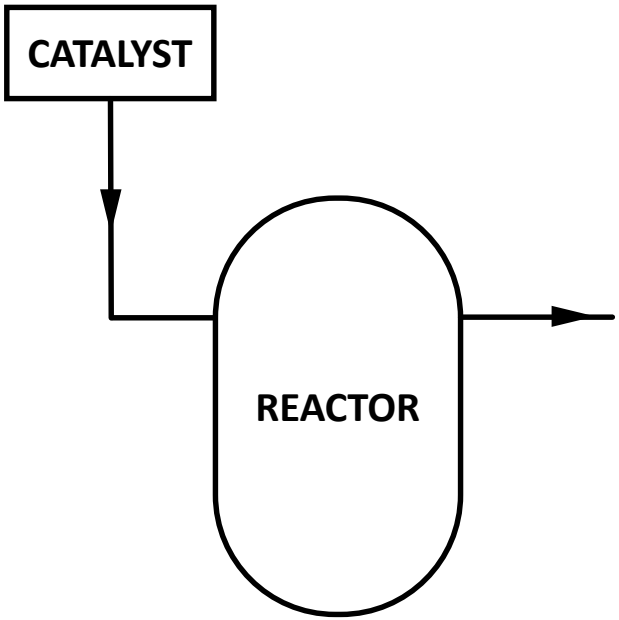


STPA

Safety Constraints

- SC-1: Toxic chemicals must be contained within plant equipment [H-1]
- SC-2: Plant must be operated within limits (pressure, temperature, etc.) [H-2]
- SC-3: If toxic chemicals are not contained, damage must be mitigated [H-1]
- Etc.

Early Concept



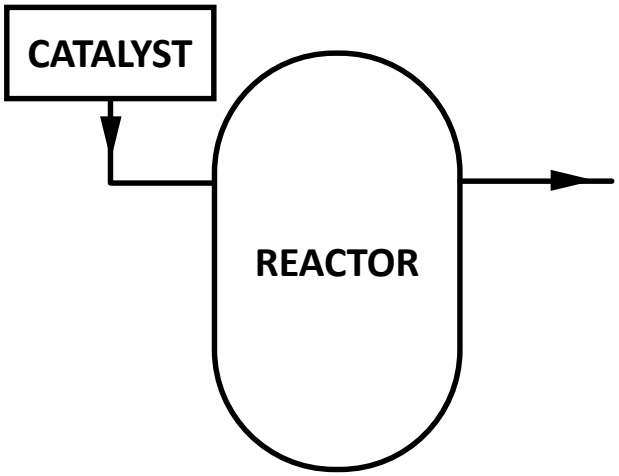
STPA

Safety Constraints

- SC-2: Plant must be operated within limits (pressure, temperature, etc.) [H-2]

How can we enforce SC-2?
How to keep pressure, temperature within limits?

Early Concept

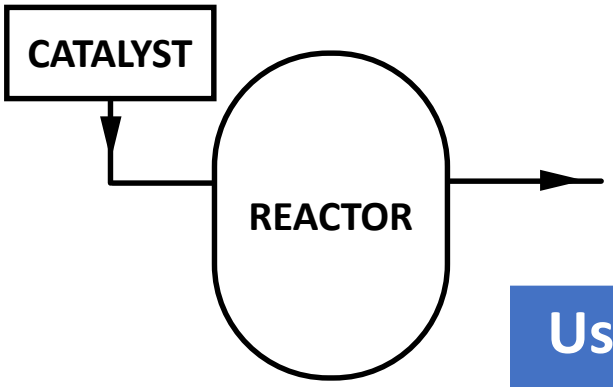


Safety Constraints

- SC-2: Plant must be operated within limits (pressure, temperature, etc.) [H-2]
  - SC-2.1: Reactor temperature must not exceed X [H-2]
  - SC-2.2: Reactor pressure must not exceed Y [H-2]
  - Etc.

Use Safety Constraints to refine the concept, make design decisions

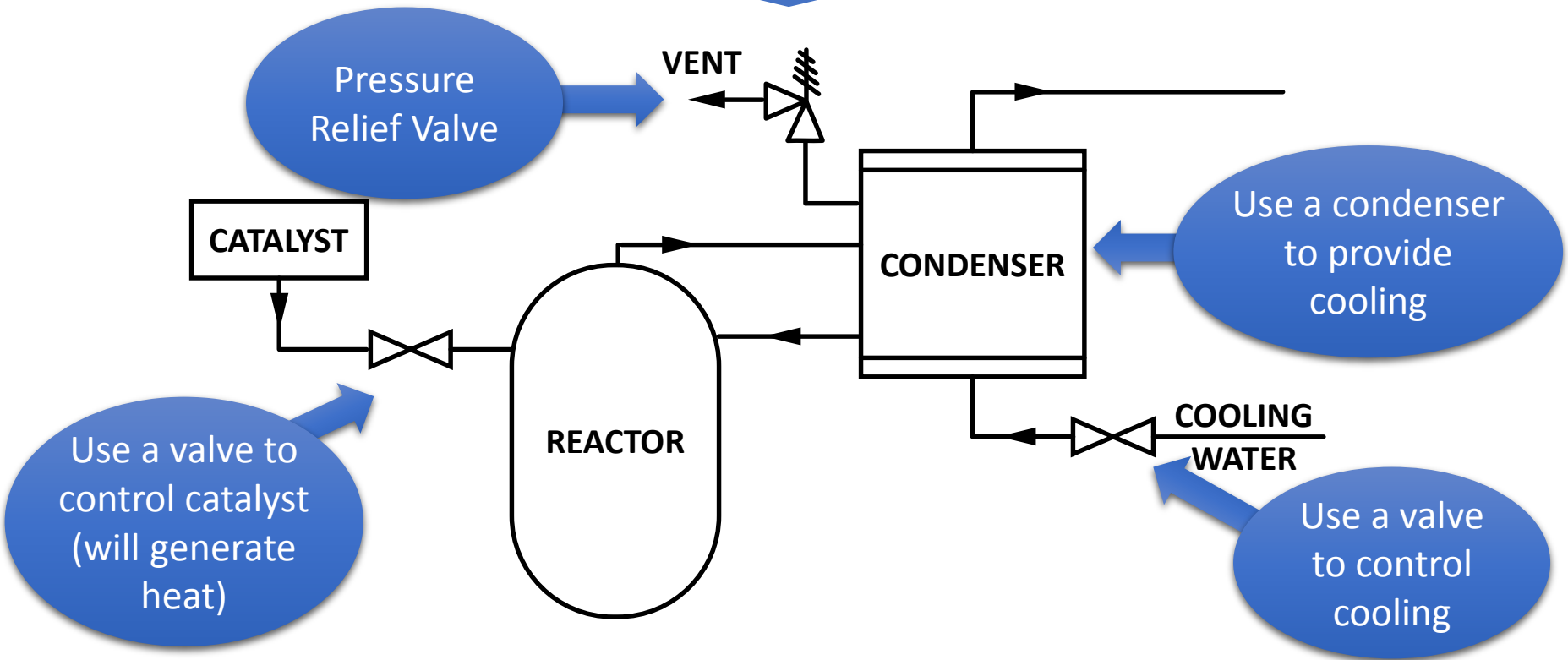
Early Concept



Safety Constraints

- SC-2: Plant must be operated within limits (pressure, temperature, etc.) [H-2]

Use Safety Constraints to refine the concept, make design decisions

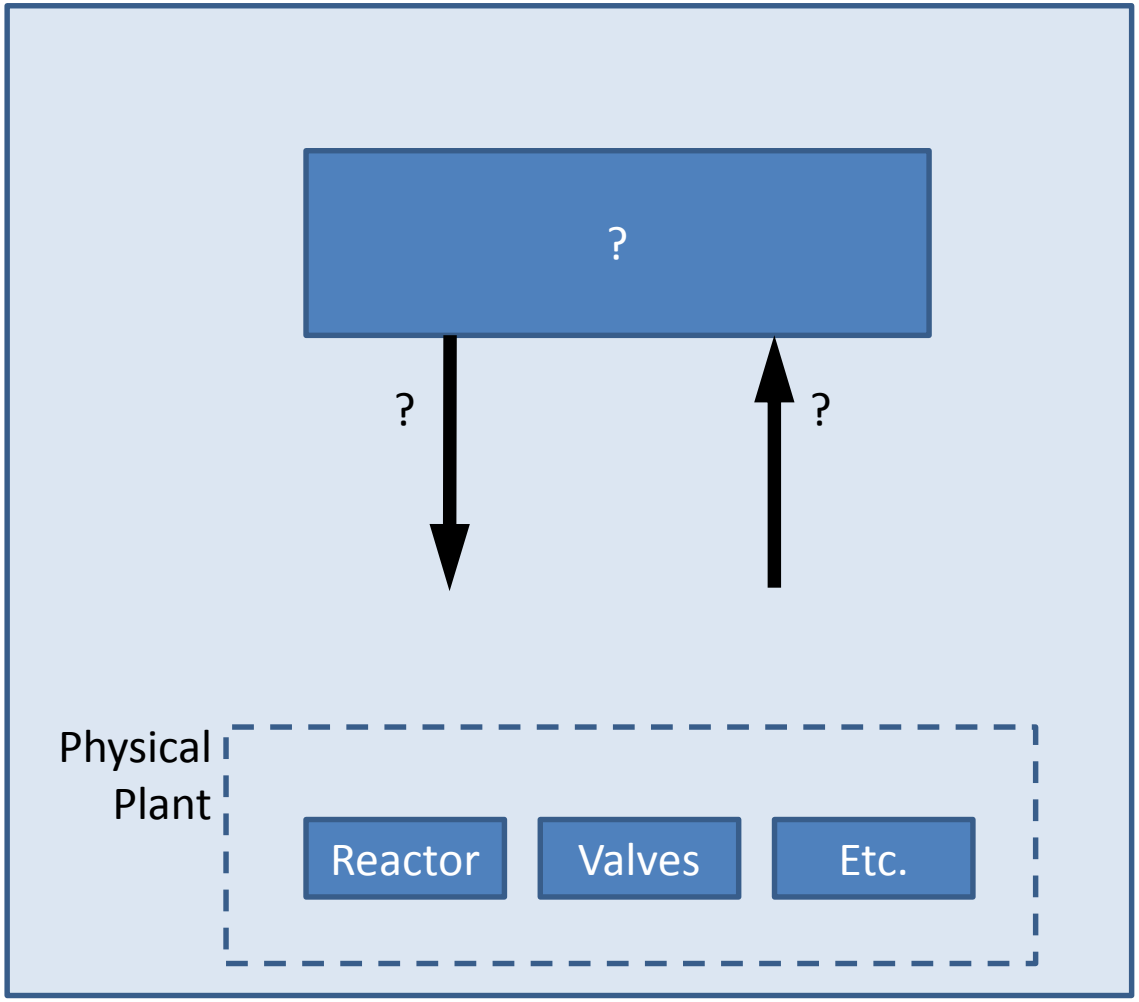


System-Theoretic Process Analysis (STPA)

- Identify accidents (losses), hazards
- Draw hierarchical control structure
- Identify unsafe control actions
- Identify accident scenarios

(Leveson, 2012)

Control structure

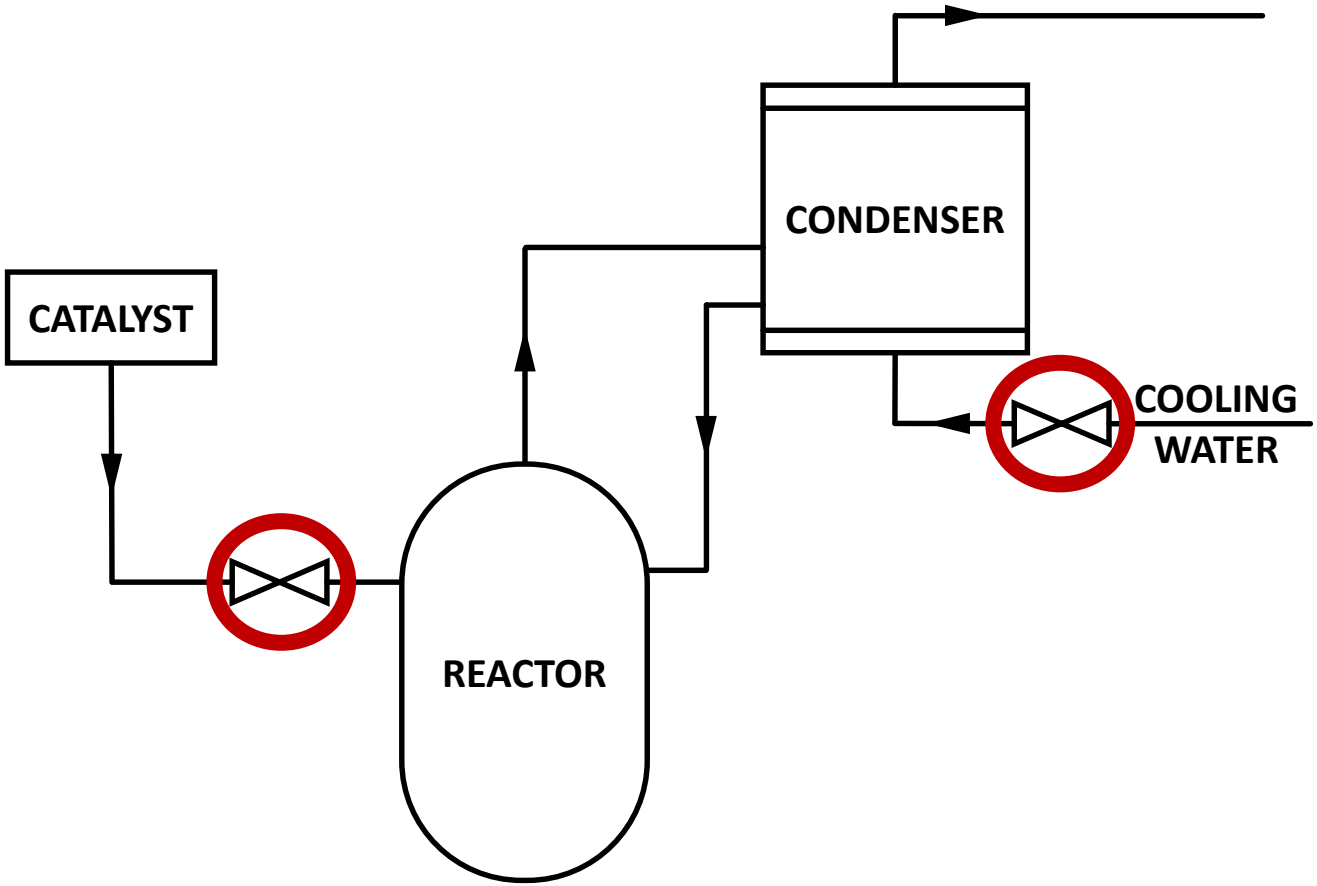


Questions to ask:

Who or what will control the physical plant?

How?

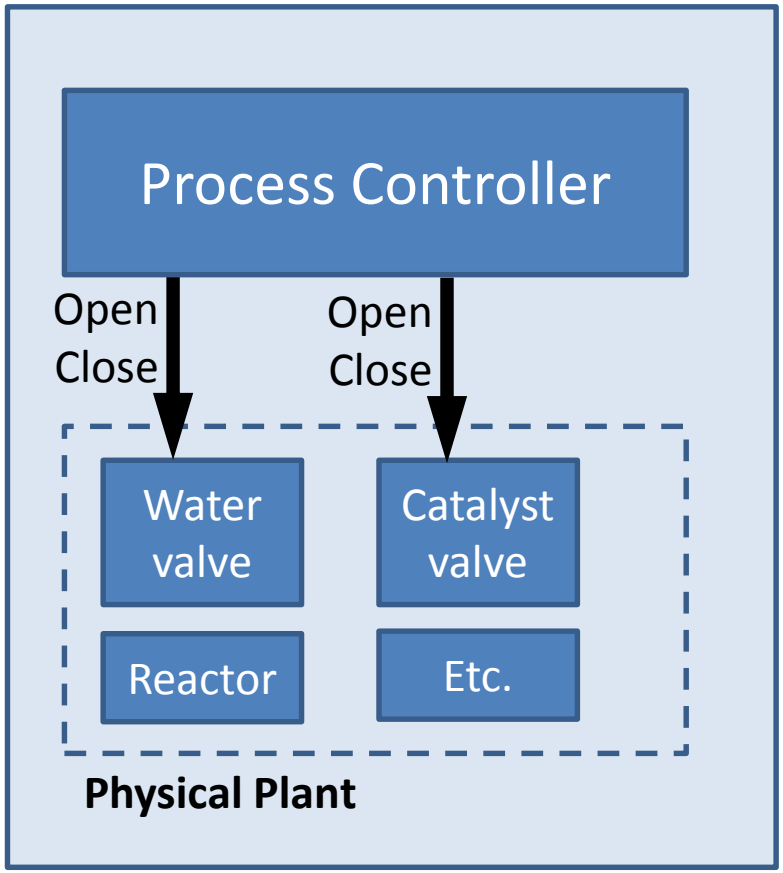
What are the control actions and feedback?



These valves were added to regulate temperature/pressure (SC-2).

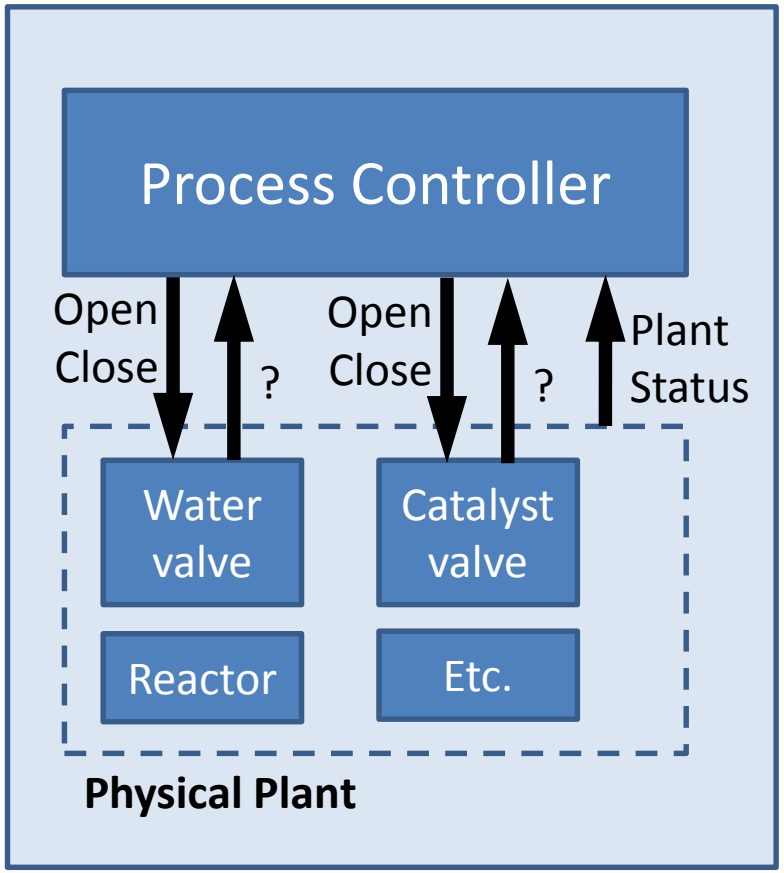
Who or what will control them?

Control structure



Feedback?

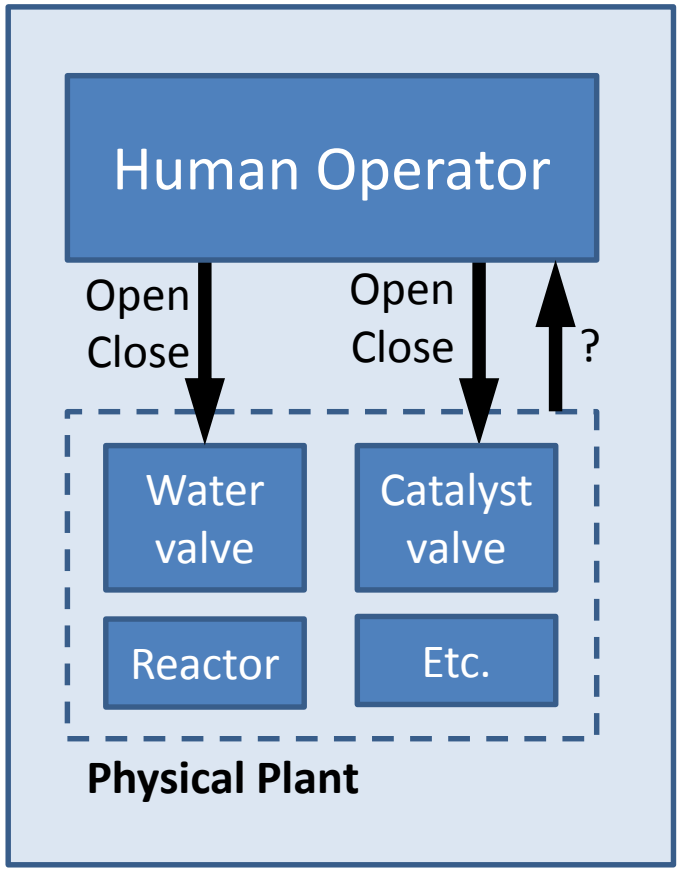
Control structure

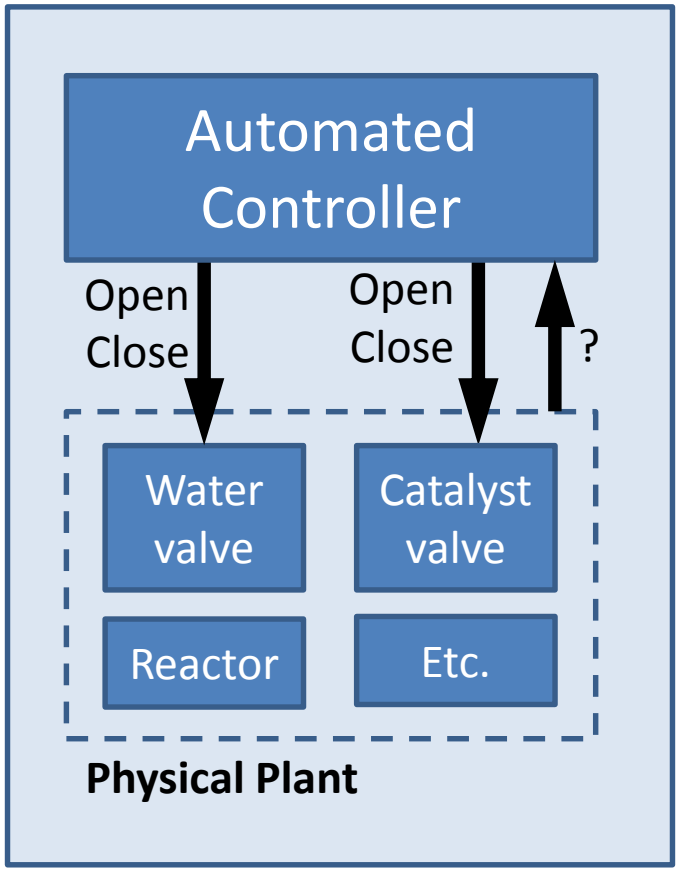


"Process Controller" could be a human operator, a computer, or a combination of the two.

STPA can be applied in any of these cases or before the implementation is known.

Control structure



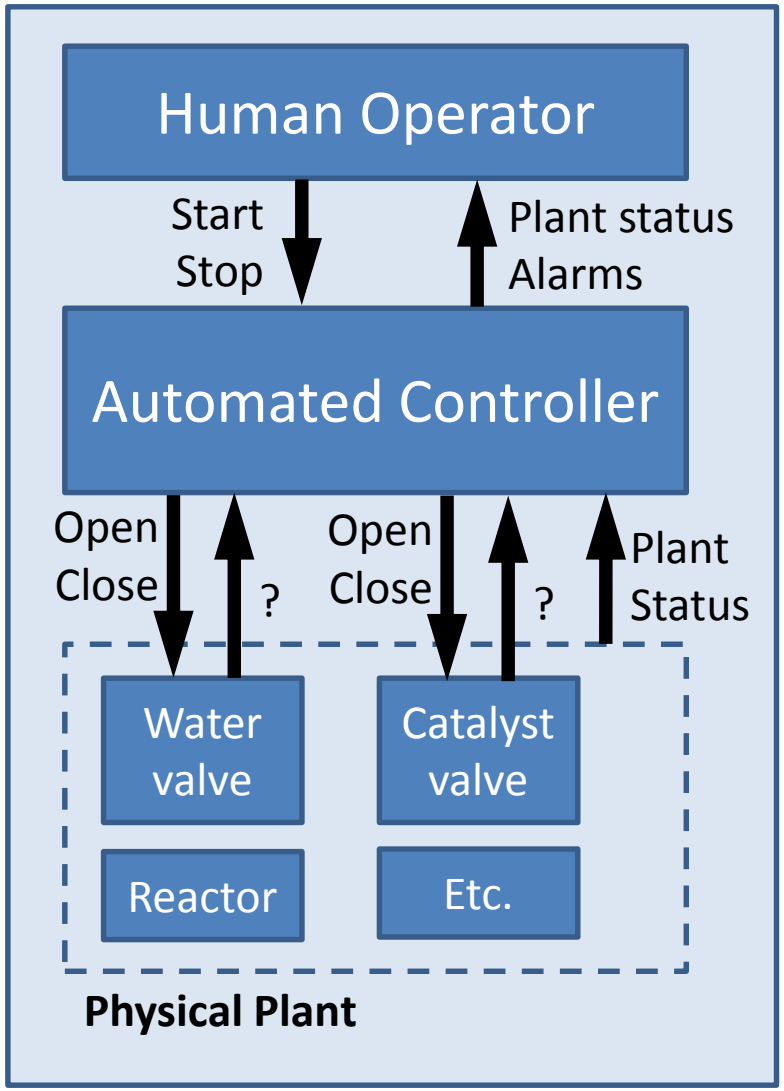


(discuss tradeoffs)

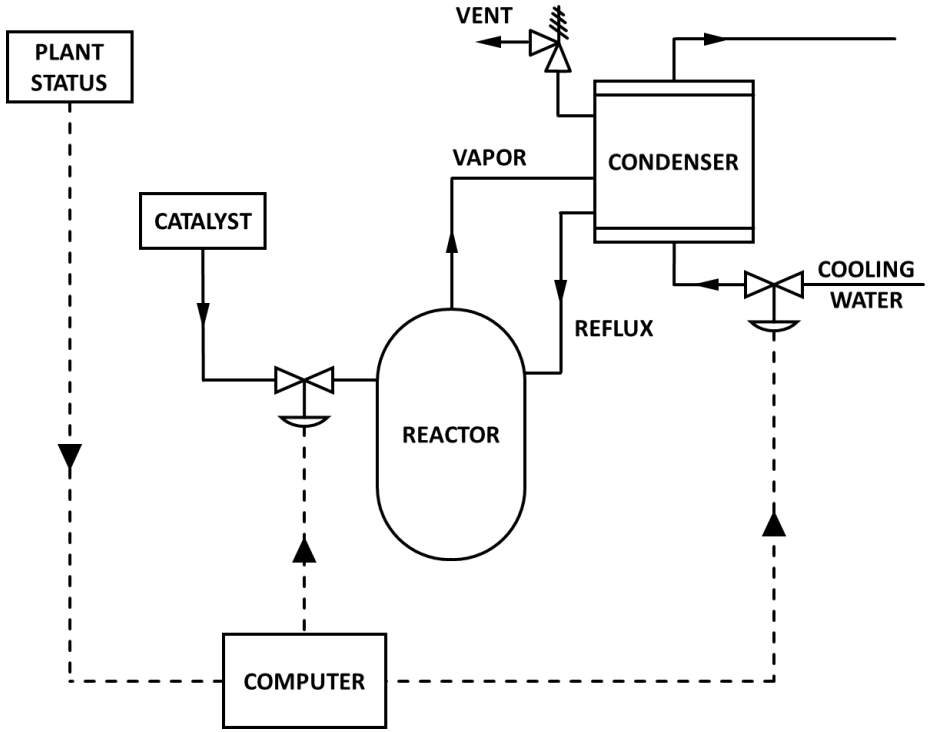
STPA can be applied to either case—the process is the same

One option

Control Structure



Physical Diagram



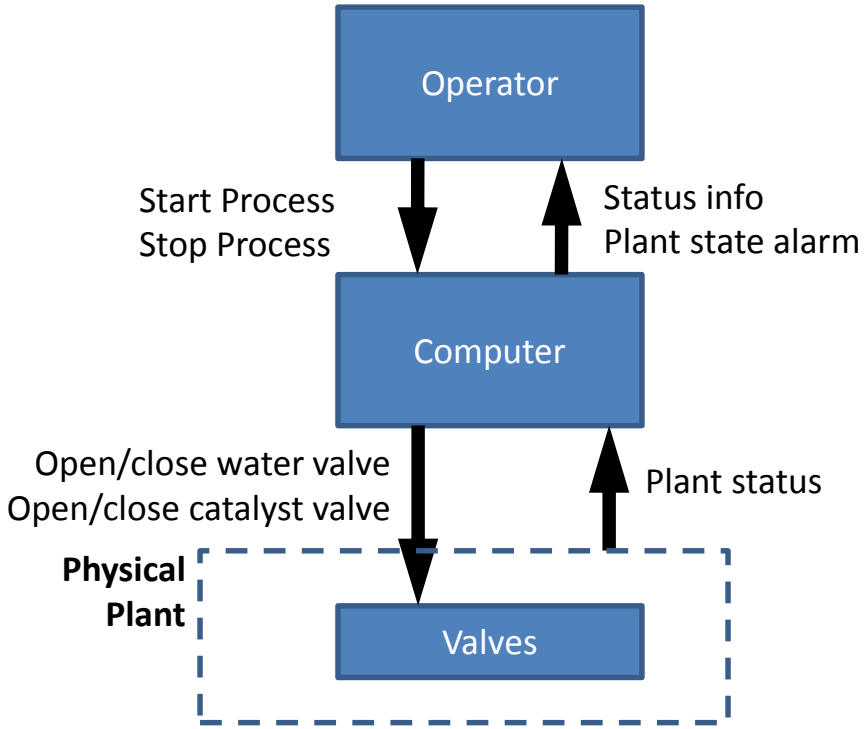
System-Theoretic Process Analysis (STPA)

- Identify accidents (losses), hazards
- Draw hierarchical control structure
- Identify unsafe control actions
- Identify accident scenarios

(Leveson, 2012)

Chemical Reactor: Unsafe Control Actions

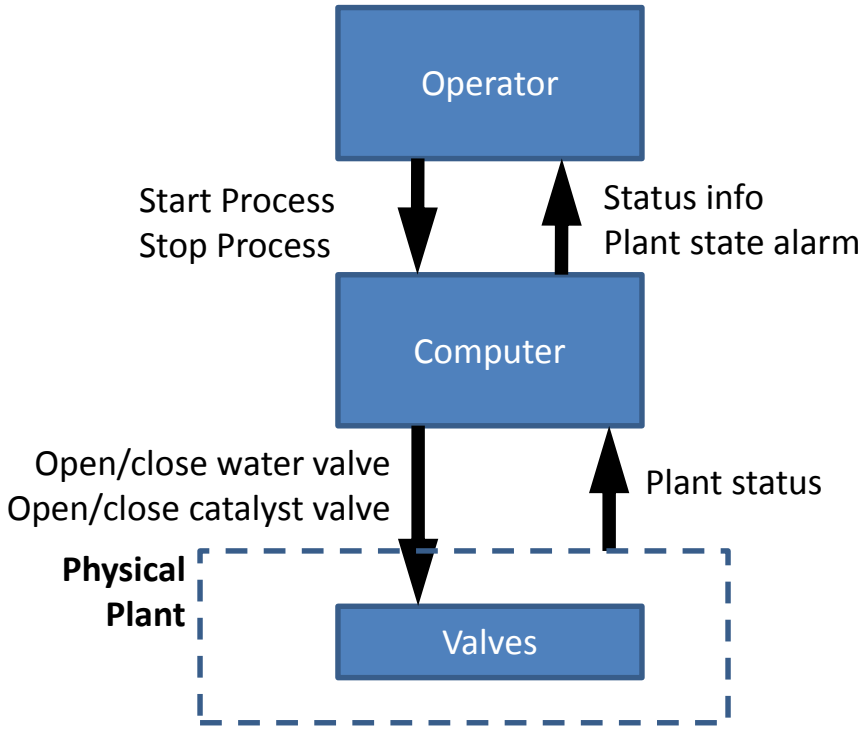
Control Structure:



	?	?	?	?
Close Water Valve Cmd				

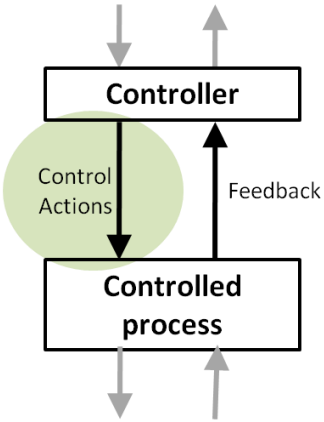
Chemical Reactor: Unsafe Control Actions

Control Structure:



	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Open Water Valve Cmd	**Computer does not provide open water valve cmd when catalyst open/flowing**	**?**	**?**	**?**

Structure of an Unsafe Control Action



Example:

"Computer does not provide open water valve command when catalyst open"

Source Controller

Type

Control Action

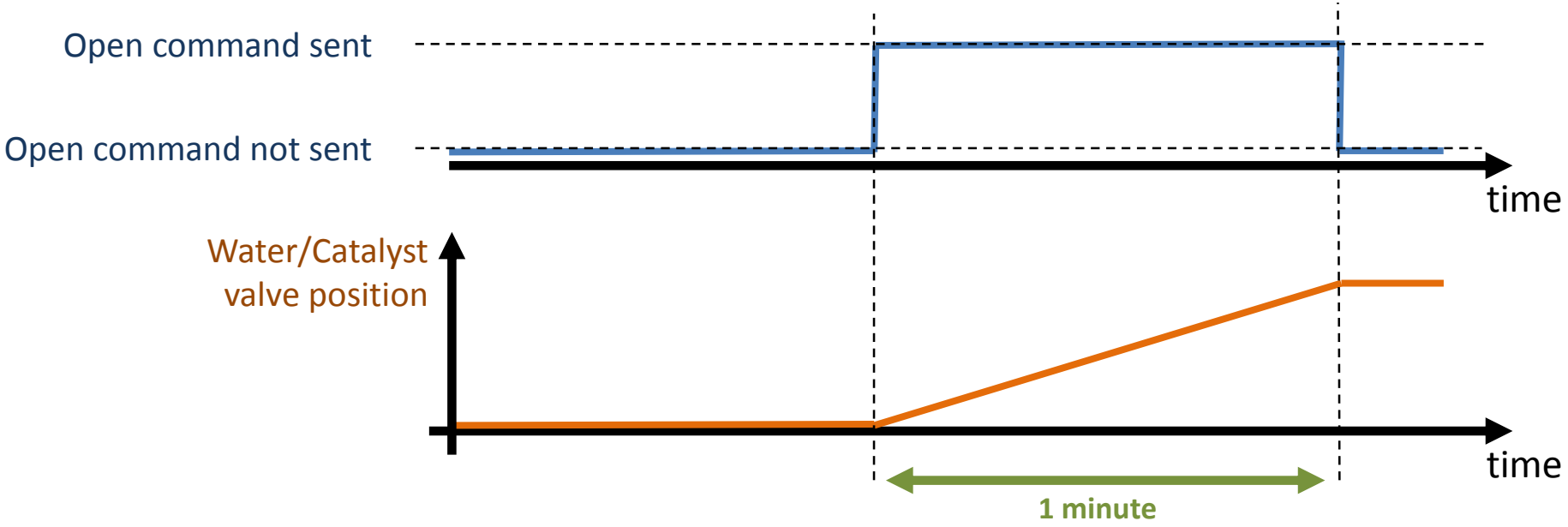
Context

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)

(Thomas, 2013)

Command duration

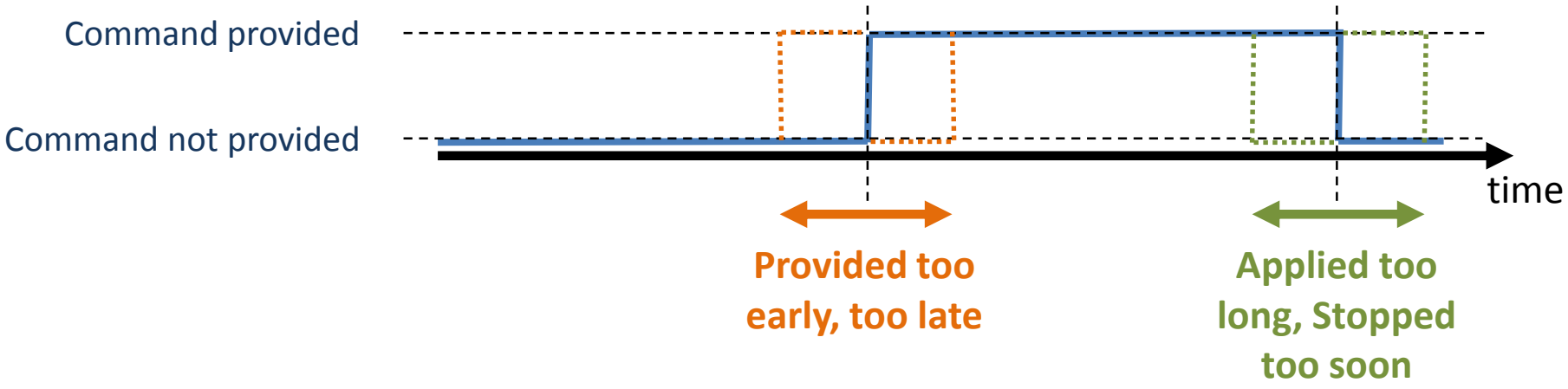


In our system, no variable metering.

- **During normal operation: valves fully open**
- **During shutdown: valves fully closed**
- **When switching between: 1 minute transition time**

"Stopped too soon", "Applied too long"
-> only for commands with a duration

Command duration



Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Open Water Valve cmd	**Computer does not provide open water valve cmd when catalyst open/flowing [H-1,2,3]**		**Computer provides open water valve cmd after catalyst open**	**Computer stops providing open water valve cmd too soon before fully opened**
Close Water Valve cmd				
Open Catalyst Valve cmd				
Close Catalyst Valve cmd				

Common Clarifications:

- This is not a list of hazardous states. This is about control actions that cause hazards.
- Each cell may have 0, 1, 2, or more UCAs.
- “When is the command unsafe”

Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Open Water Valve cmd	**Computer does not provide open water valve cmd when catalyst open/flowing [H-1,2,3]**		**Computer provides open water valve cmd after catalyst open**	**Computer stops providing open water valve cmd too soon before fully opened**
Close Water Valve cmd				
Open Catalyst Valve cmd				
Close Catalyst Valve cmd				

Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Open Water Valve cmd	Computer does not provide open water valve cmd when catalyst valve open/flowing [H-1,2,3]		Computer provides open water valve cmd more than X seconds after catalyst open	Computer stops providing open water valve cmd too soon before fully opened
Close Water Valve cmd		Computer provides close water valve cmd while catalyst open	Computer provides close water valve cmd more than X seconds before catalyst closes	
Open Catalyst Valve cmd		Computer provides open catalyst valve cmd when water not open	Computer provides open catalyst valve cmd more than X seconds before water open/flowing	
Close Catalyst Valve cmd	Computer does not provide close catalyst valve cmd when water closed/not flowing		Computer provides close catalyst valve cmd more than X seconds after water closed/not flowing	Computer stops providing close catalyst valve cmd too soon before fully closed

Chemical Reactor

Unsafe

Is this Safety or Security?

	Not providing causes hazard	Providing causes hazard	Too Early, Too Late, Order	Stopped Too Soon / Applied too long
Open Water Valve cmd	Computer does not provide open water valve cmd when catalyst valve open/flowing [H-1,2,3]		Computer provides open water valve cmd more than X seconds after catalyst open	Computer stops providing open water valve cmd too soon before fully opened
Close Water Valve cmd		Computer provides close water valve cmd while catalyst open	Computer provides close water valve cmd more than X seconds before catalyst closes	
Open Catalyst Valve cmd		Computer provides open catalyst valve cmd when water not open	Computer provides open catalyst valve cmd more than X seconds before water open/flowing	
Close Catalyst Valve cmd	Computer does not provide close catalyst valve cmd when water closed/not flowing		Computer provides close catalyst valve cmd more than X seconds after water closed/not flowing	Computer stops providing close catalyst valve cmd too soon before 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
- 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]**

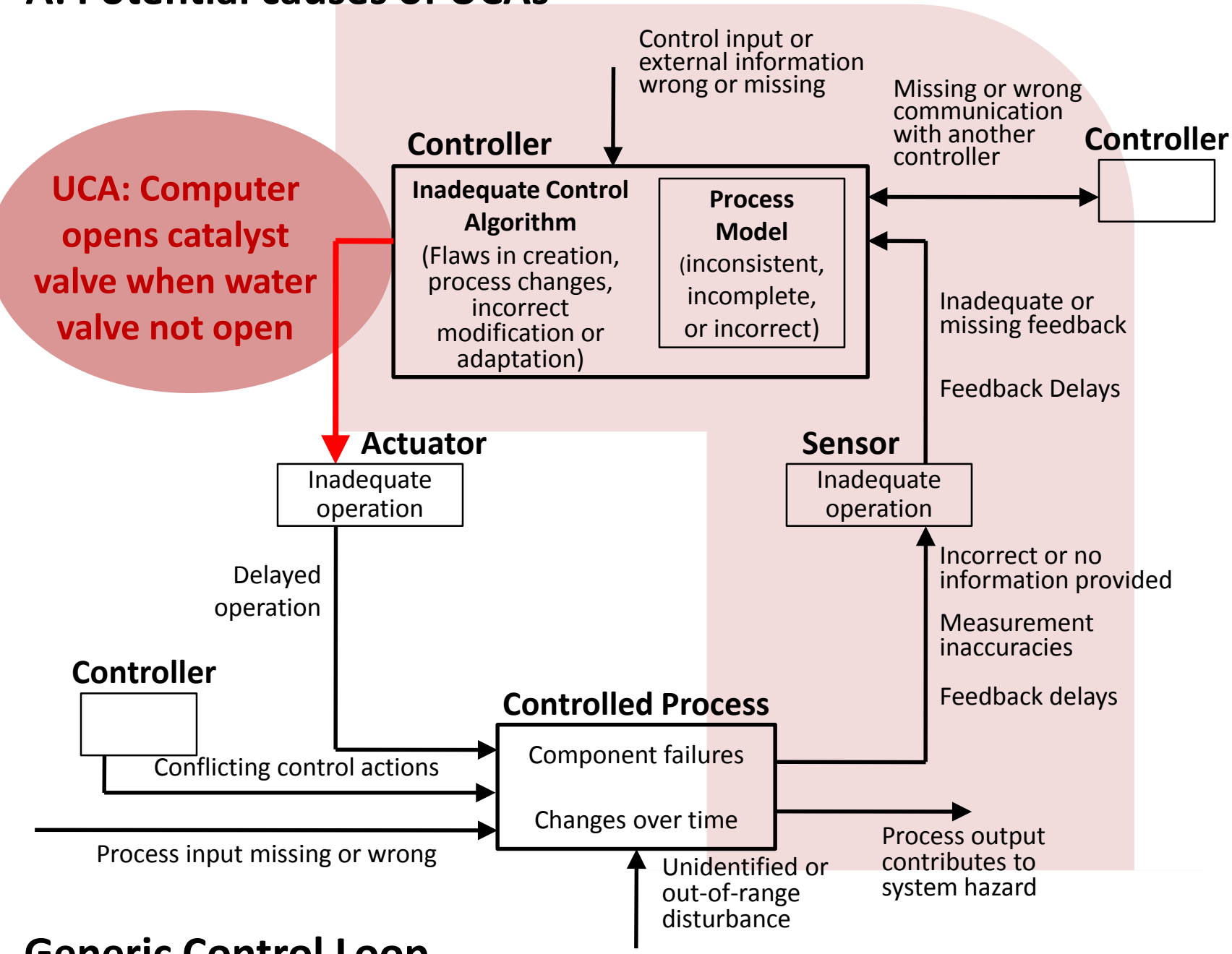
(Thomas, 2013)

System-Theoretic Process Analysis (STPA)

- Identify accidents (losses), hazards
- Draw hierarchical control structure
- Identify unsafe control actions
- Identify accident scenarios

(Leveson, 2012)

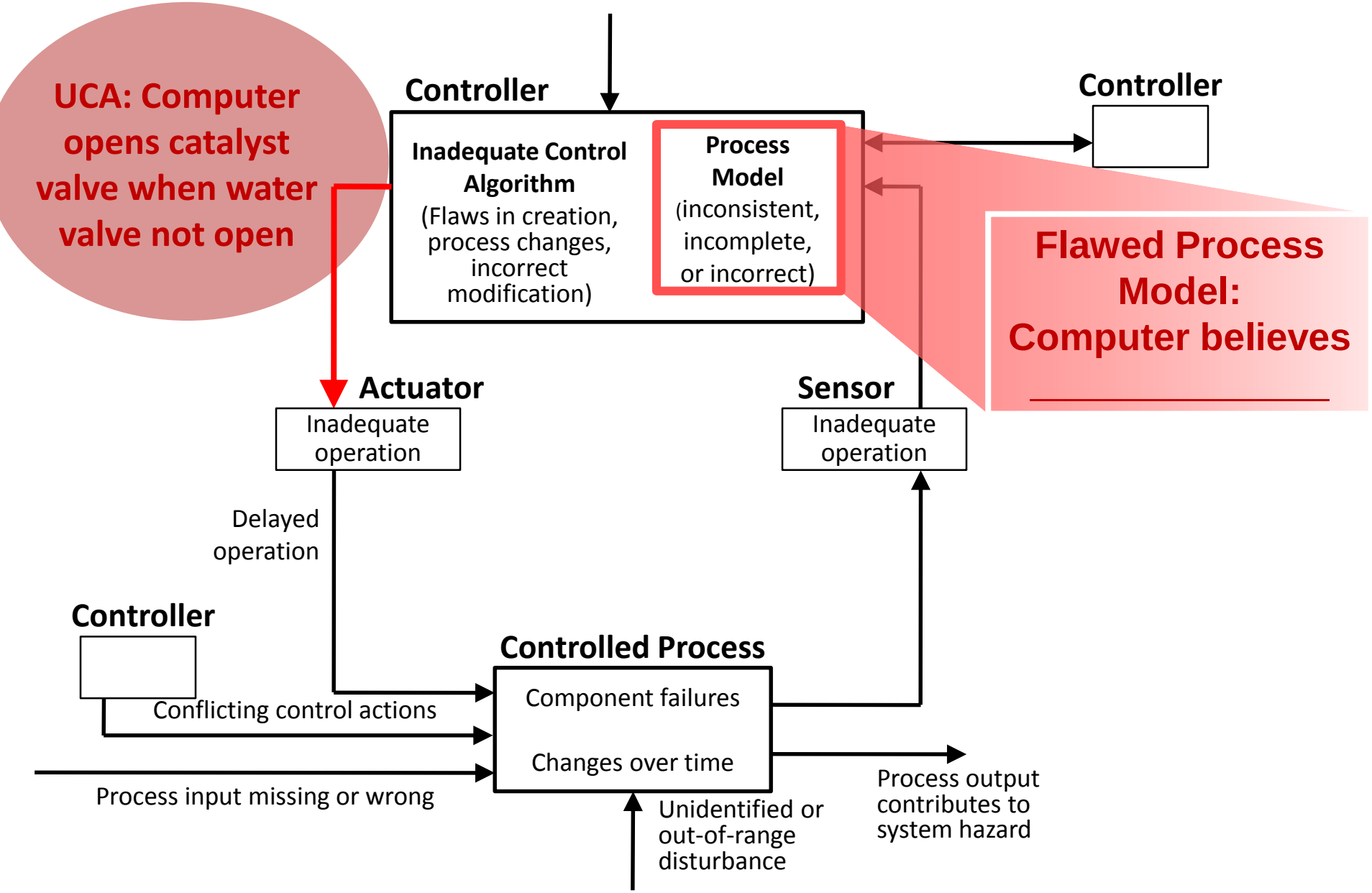
A: Potential causes of UCAs



Generic Control Loop

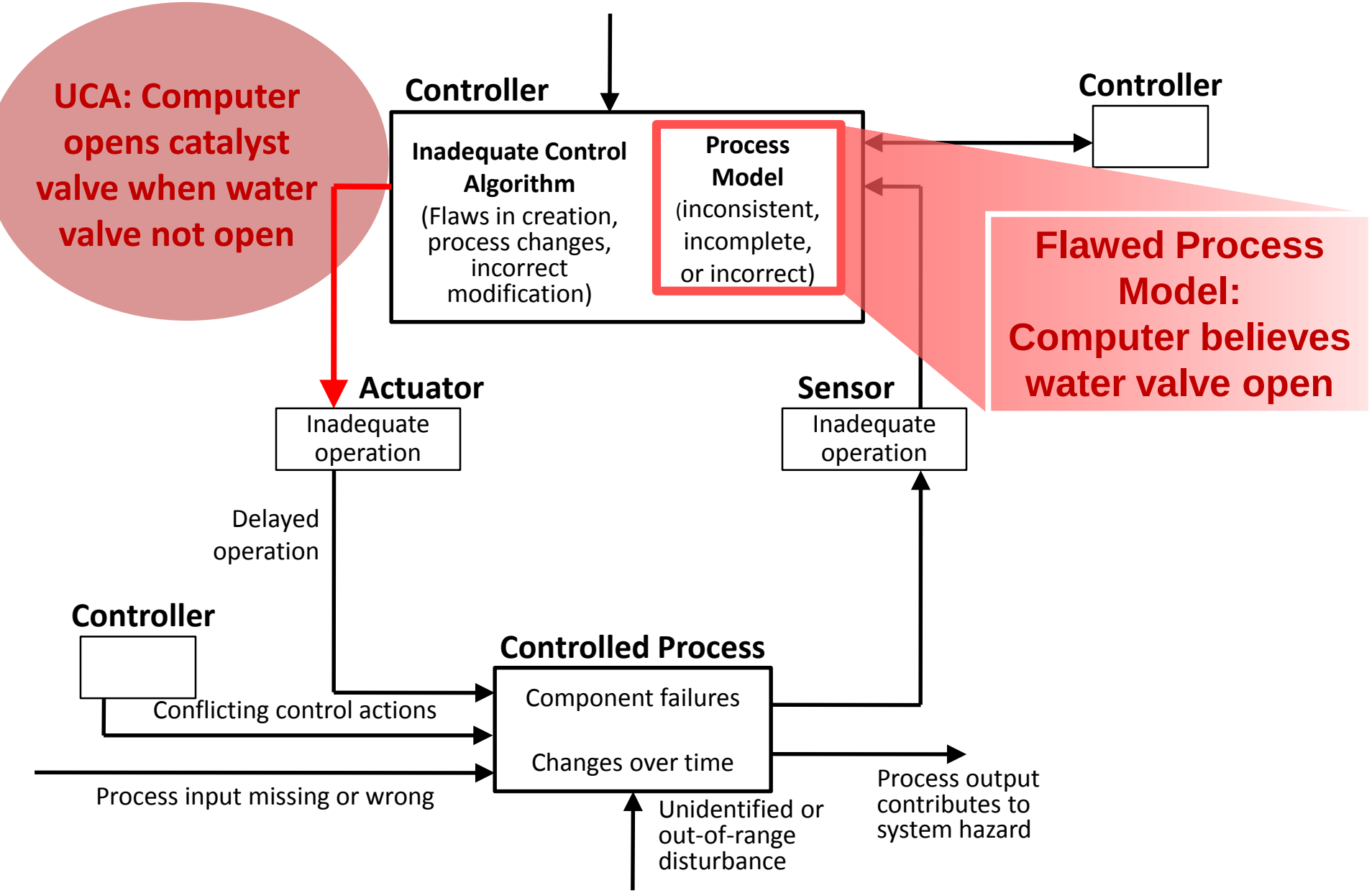
A: Potential causes of UCAs

Generic Control Loop!



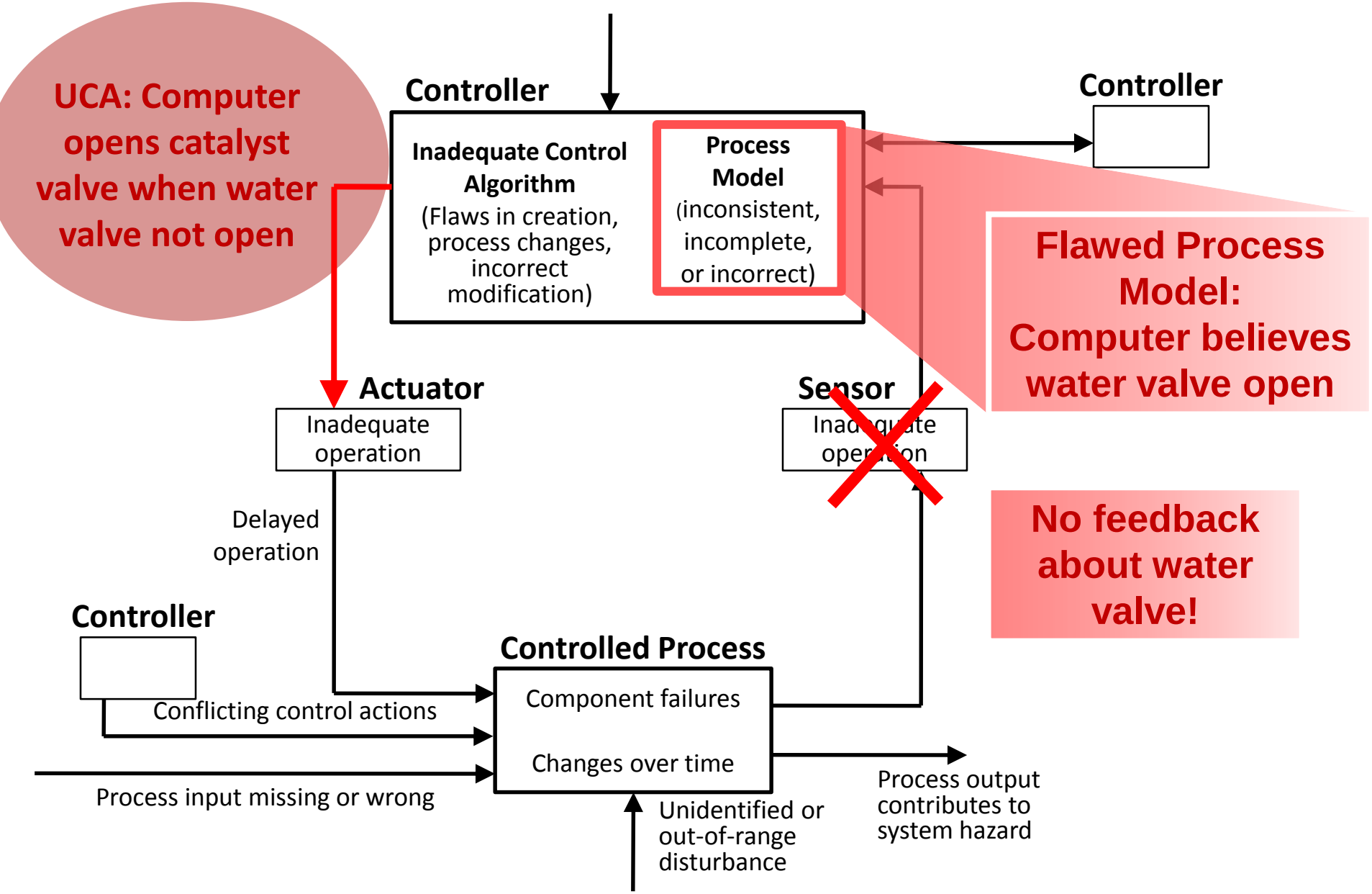
A: Potential causes of UCAs

Generic Control Loop!

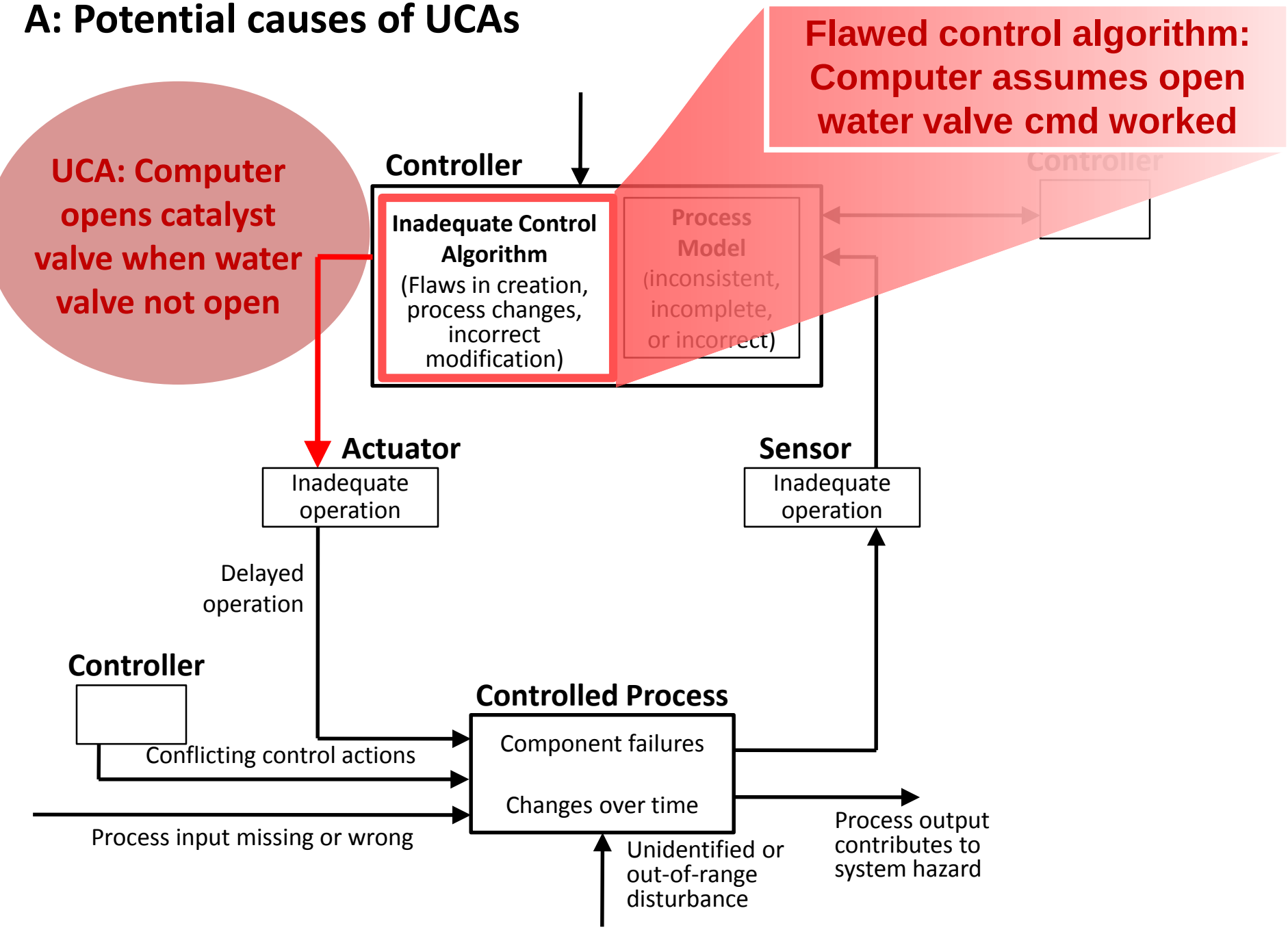


A: Potential causes of UCAs

Generic Control Loop!

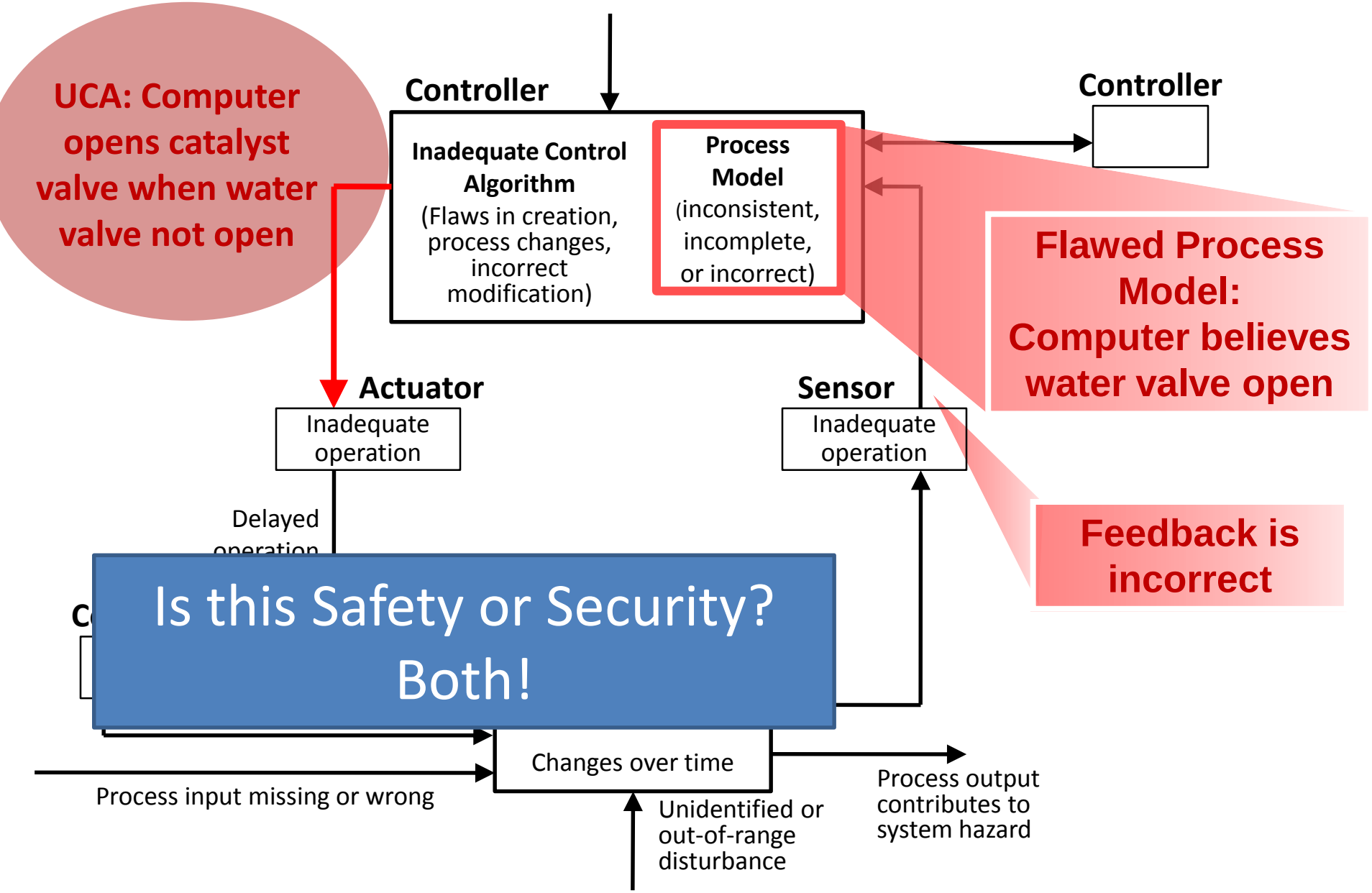


A: Potential causes of UCAs



A: Potential causes of UCAs

Generic Control Loop!



Chemical Reactor: Real accident

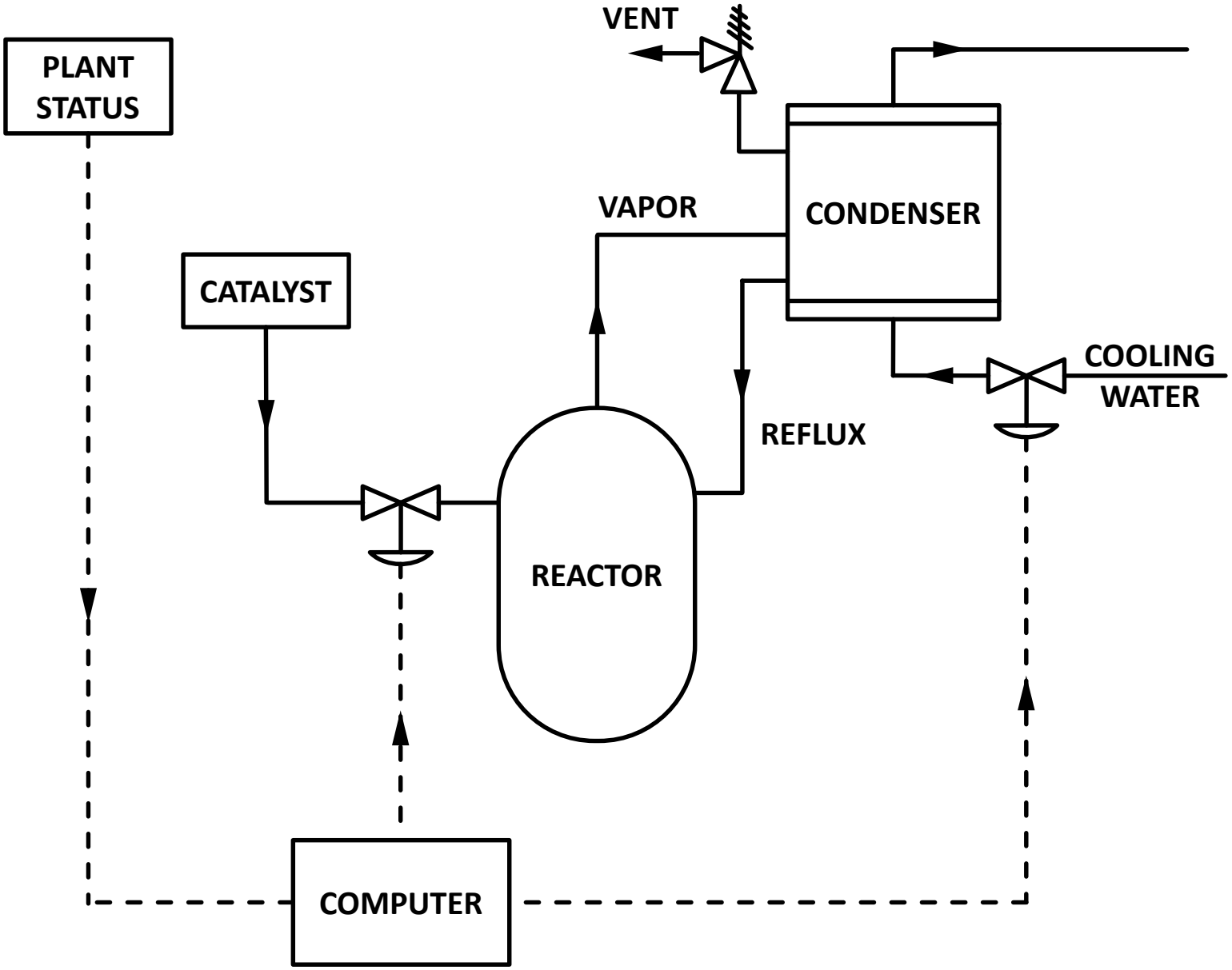


Diagram adapted Trevor Kletz, 1982

Some problems we found

- Water valve could fail closed
- There are missing requirements
  - R-1: Computer must not open catalyst valve when open water valve closed (missing)
- The design is missing feedback
  - Design has no way to verify or check when water valves open
- The design assumption is incorrect
  - Computer algorithm assumes open water valve cmd is successful (causes process model flaws)