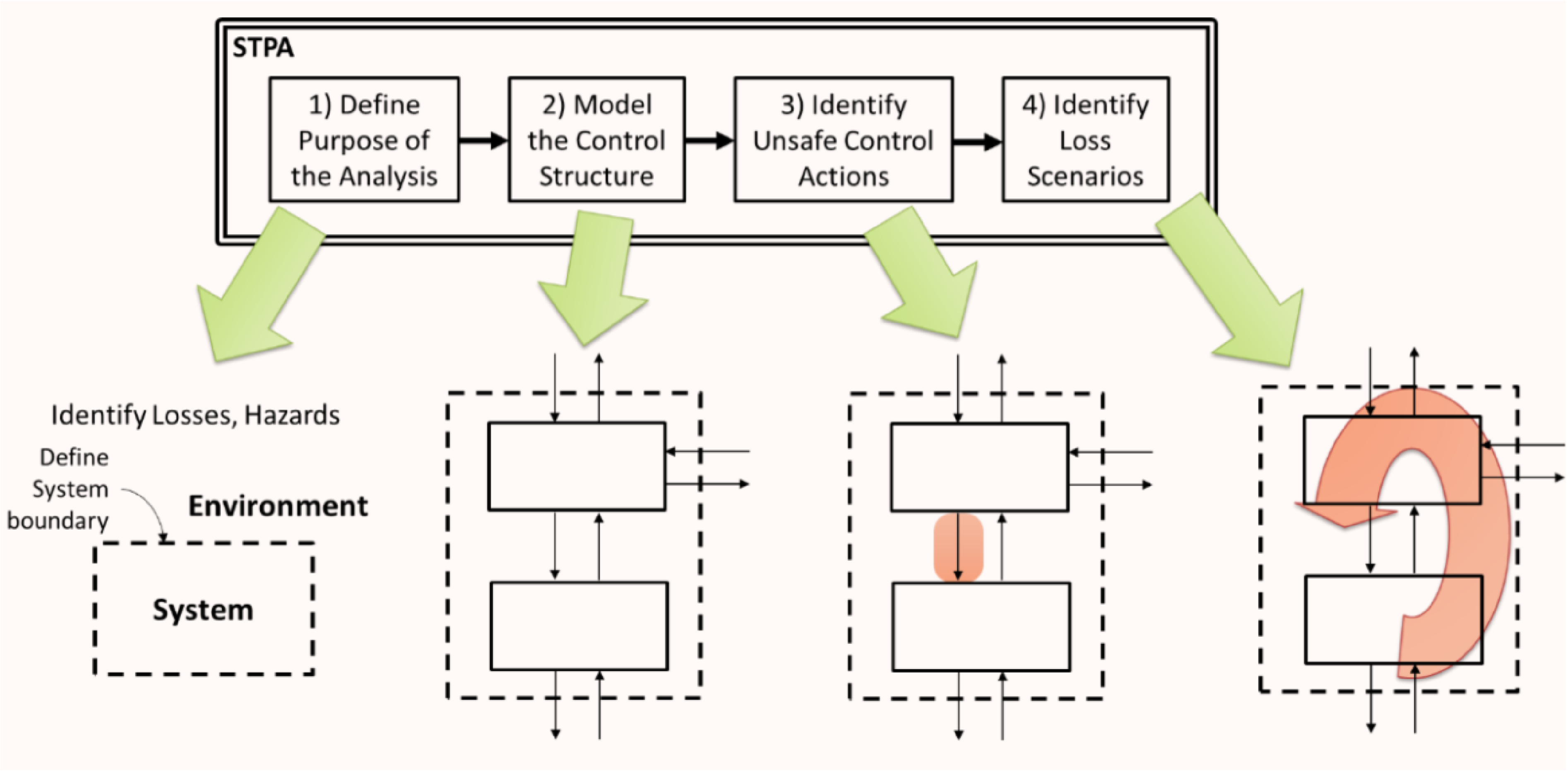
Hazard Analysis

- “Investigating an accident before it occurs”
- Identify potential causal scenarios and try to eliminate them
- Must be based on some model of how and why accidents occur
- STPA (System-Theoretic Process Analysis)
  - Based on STAMP
  - Assumes accidents are more complex processes than just chains of component failure events

STPA: System-Theoretic Process Analysis

- Identifies safety and security requirements and constraints
- Identifies scenarios leading to violation of constraints and requirements; use results to design or redesign system to be safer
- Finds hazardous design flaws in addition to failures
- Includes hardware, software, humans, organizational processes
- Supports entire life cycle:
  - Designing safety into system from beginning
  - Test and assurance
  - Production/manufacturing
  - Anomaly/incident investigation
  - Operations

STPA Process Overview


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

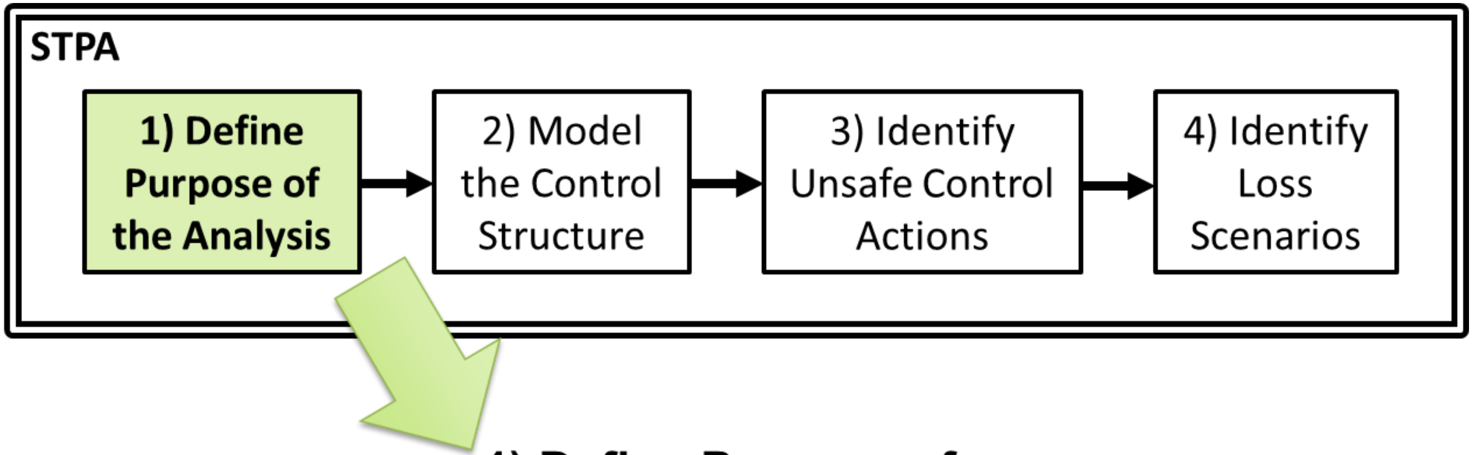
Losses to prevent

Model

Behavior to prevent

How behavior could occur

Defining the Purpose of the Analysis

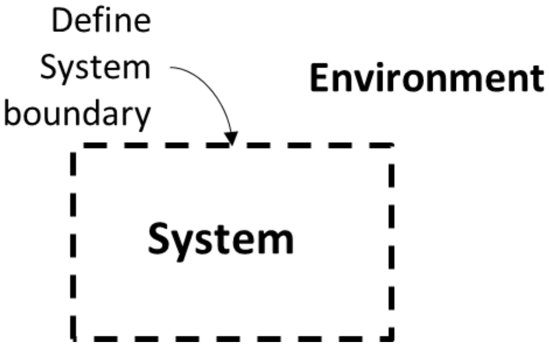


STPA

1) Define Purpose of the Analysis → 2) Model the Control Structure → 3) Identify Unsafe Control Actions → 4) Identify Loss Scenarios

1) Define Purpose of the Analysis

Identify Losses, Hazards



Establish Analysis Goals (Stakeholders)

- **Identify losses to be considered**

  L1. Death or serious injury to aircraft passengers or people in the area of the aircraft

  L2. “Unacceptable” damage to the aircraft or objects outside the aircraft

  L3: Financial losses resulting from delayed operations

  L4: Reduced profit due to damage to aircraft or airline reputation

- **Identify System-Level Hazards**

  H1: Insufficient thrust to maintain controlled flight

  H2: Loss of airframe integrity

  H3: Controlled flight into terrain

  H4: An aircraft on the ground comes too close to moving or stationary objects or inadvertently leaves the taxiway

  H5: etc.

Deceleration Hazards (H4)

H4-1: Inadequate aircraft deceleration upon landing, rejected takeoff, or taxiing

H4-2: Deceleration after the V1 point during takeoff

H4-3: Aircraft motion when the aircraft is parked

H4-4: Unintentional aircraft directional control (differential braking)

H4-5: Aircraft maneuvers out of safe regions (taxiways, runways, terminal gates, ramps, etc.)

H4-6: Main gear wheel rotation is not stopped when (continues after) the landing gear is retracted

High-Level (System) Requirements/Constraints

SC1: Forward motion must be retarded within TBD seconds of a braking command upon landing, rejected takeoff, or taxiing (H4-1).

SC2: The aircraft must not decelerate after V1 (H4-2).

SC3: Uncommanded movement must not occur when the aircraft is parked (H4-3).

SC4: Differential braking must not lead to loss of or unintended aircraft directional control (H4-4)

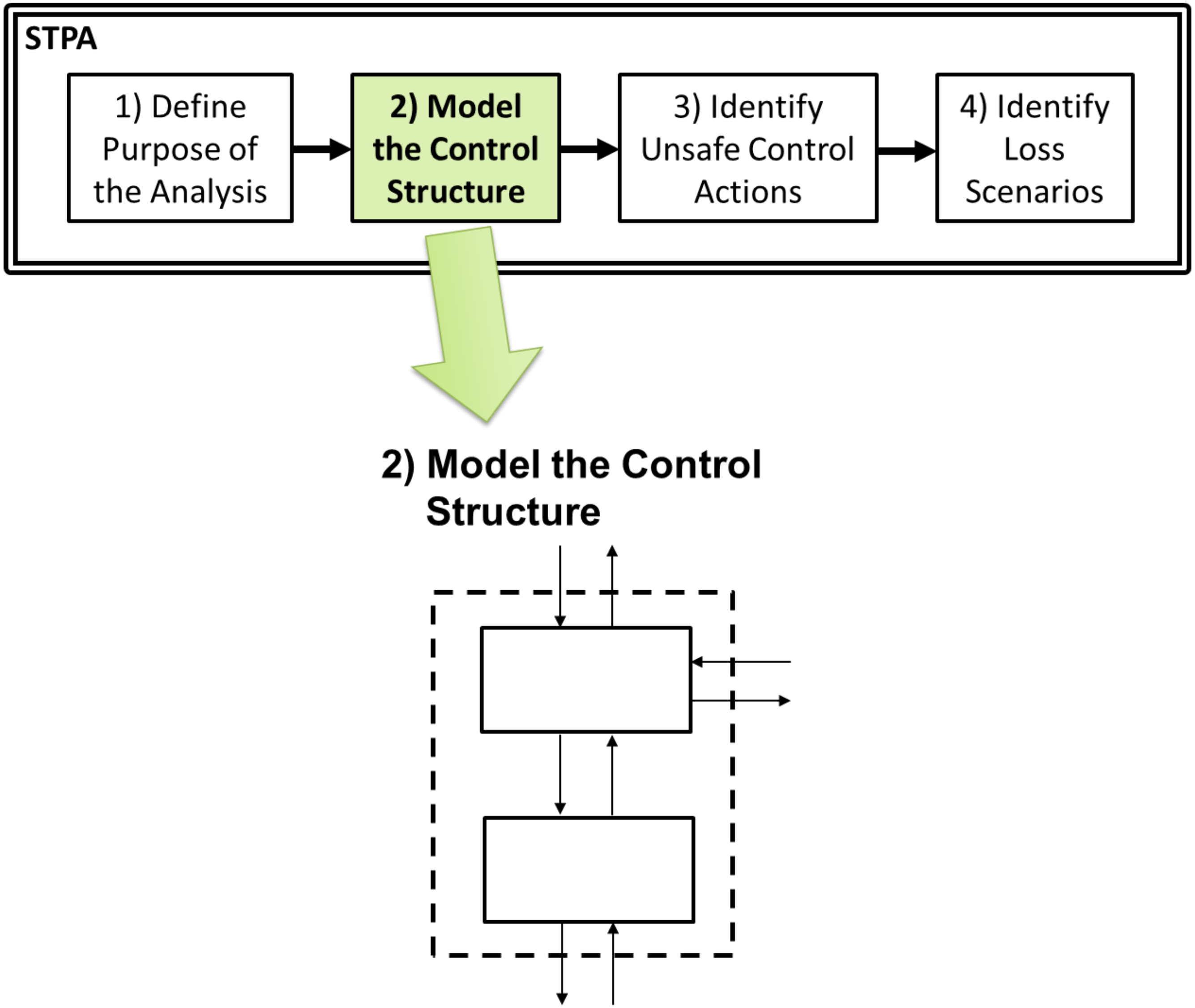
SC5: Aircraft must not unintentionally maneuver out of safe regions (taxiways, runways, terminal gates and ramps, etc.) (H4-5)

SC6: Main gear rotation must stop when the gear is retracted (H4-6)

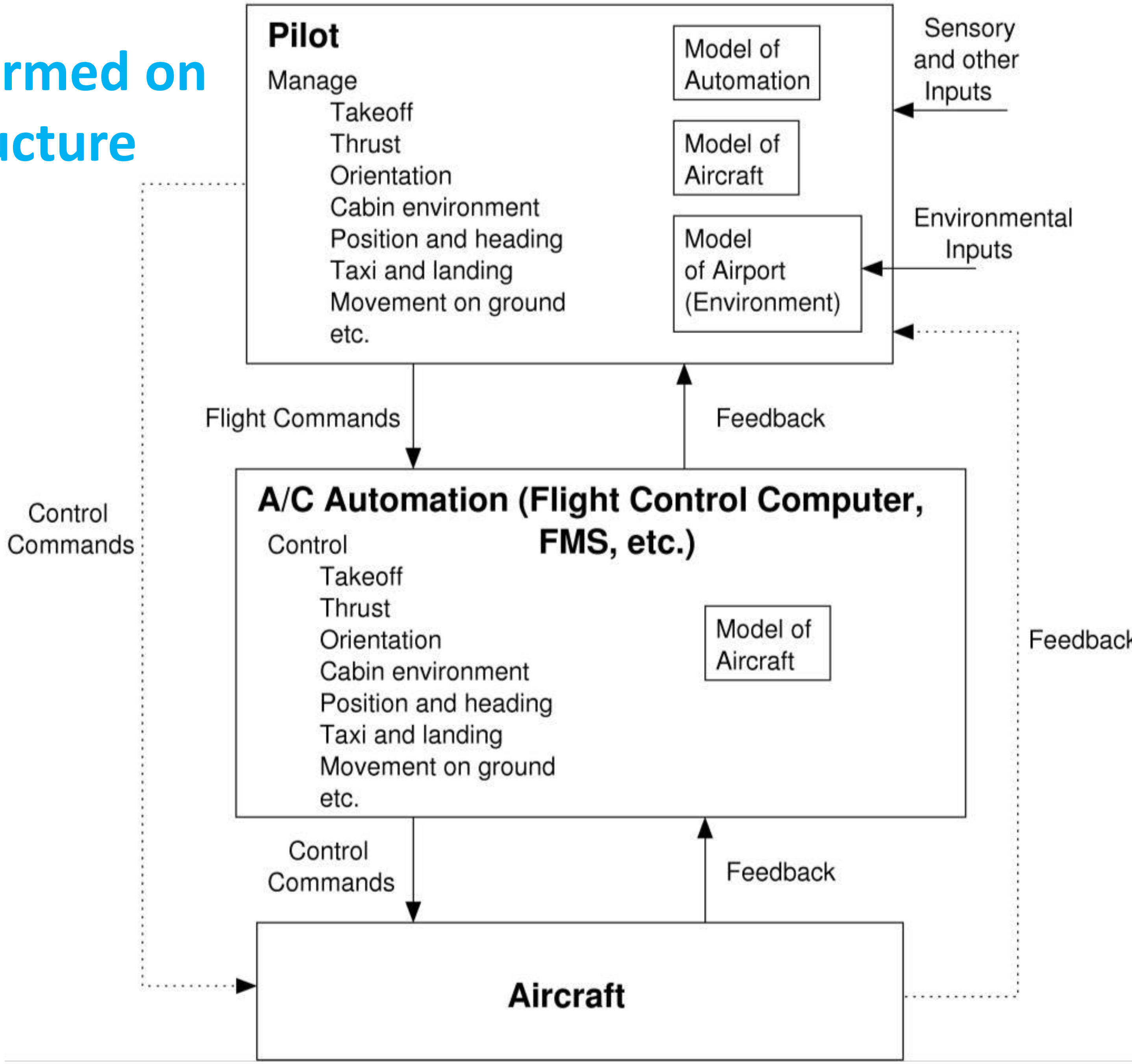
STPA analysis will refine these into detailed requirements/constraints

- **On system**
- **On components**

Modeling the Control Structure


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
2) Model the Control Structure

STPA is performed on a control structure

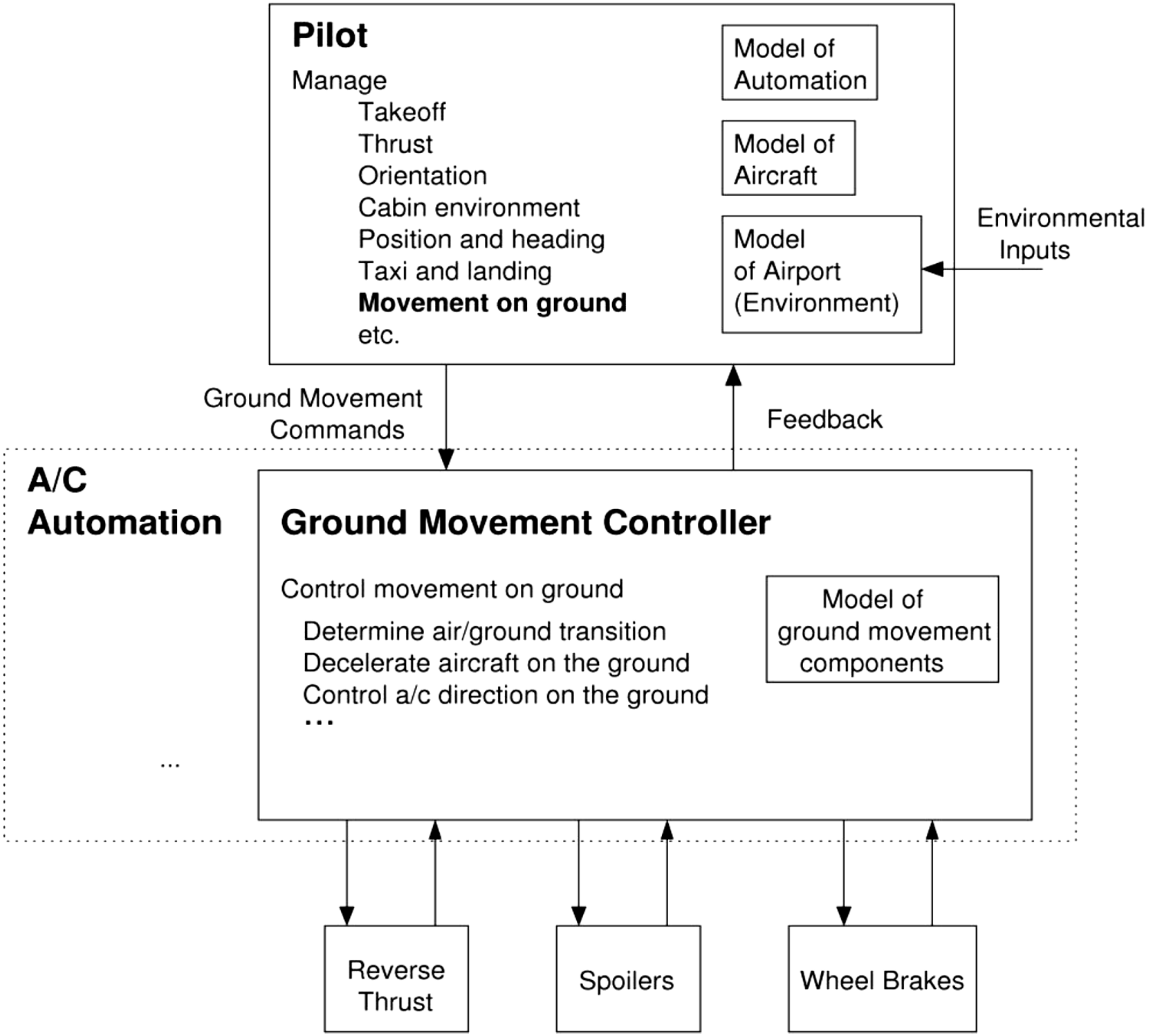


Pilot

Manage
- Takeoff
- Thrust
- Orientation
- Cabin environment
- Position and heading
- Taxi and landing
- Movement on ground
- etc.

A/C Automation (Flight Control Computer, FMS, etc.)

Control
- Takeoff
- Thrust
- Orientation
- Cabin environment
- Position and heading
- Taxi and landing
- Movement on ground
- etc.


Pilot
Manage
Takeoff
Thrust
Orientation
Cabin environment
Position and heading
Taxi and landing
Movement on ground
etc.
Model of Automation
Model of Aircraft
Model of Airport (Environment)
Environmental Inputs
Ground Movement Commands
Feedback
A/C Automation
Ground Movement Controller
Control movement on ground
Determine air/ground transition
Decelerate aircraft on the ground
Control a/c direction on the ground
...
Model of ground movement components
...
Reverse Thrust
Spoilers
Wheel Brakes

Examples of Requirements/Constraints Generated on the Interaction Between Deceleration Components

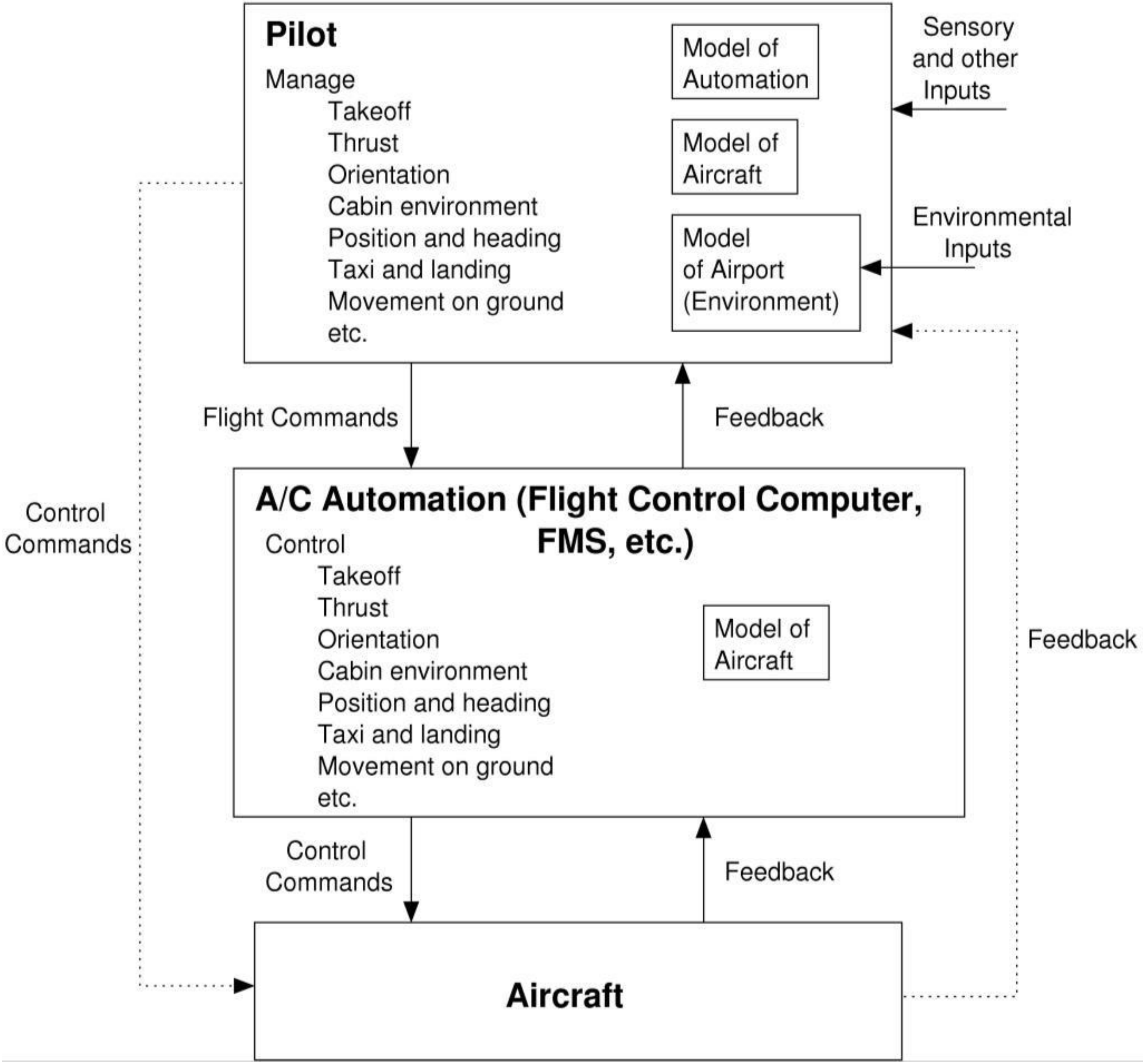
- **SC-BS-1**: Spoilers must deploy when the wheel brakes are activated manually or automatically above TBD speed.

- **SC-BS-2**: Wheel brakes must activate upon retraction of landing gear.

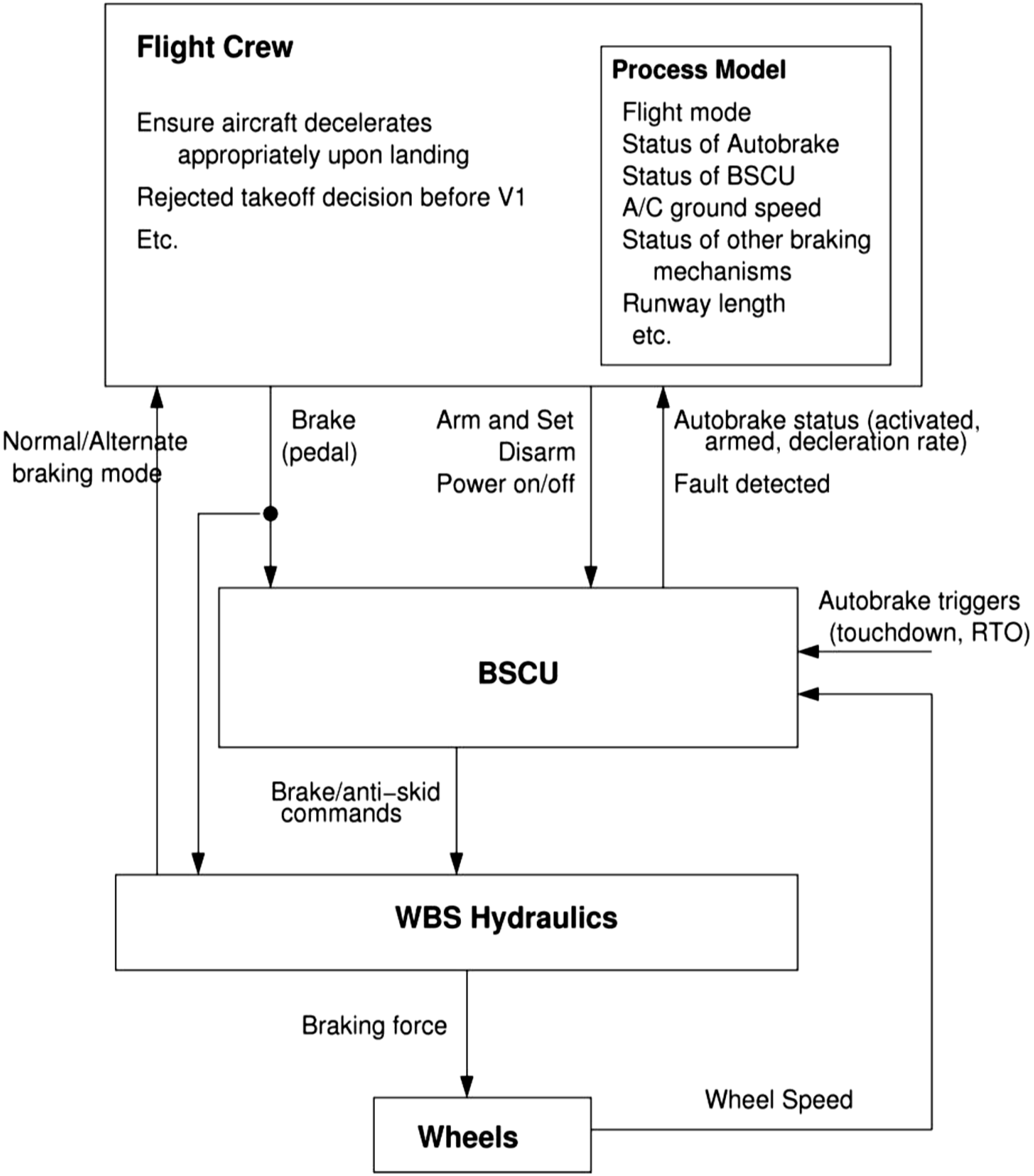
- **SC-BS-3**: Activation of ground spoilers must activate armed automatic braking (autobrake) system.

- **SC-BS-4**: Automatic braking system must not activate wheel brakes with forward thrust applied.

- **SC-BS-5**: Automatic spoiler system must retract the spoilers when forward thrust is applied.

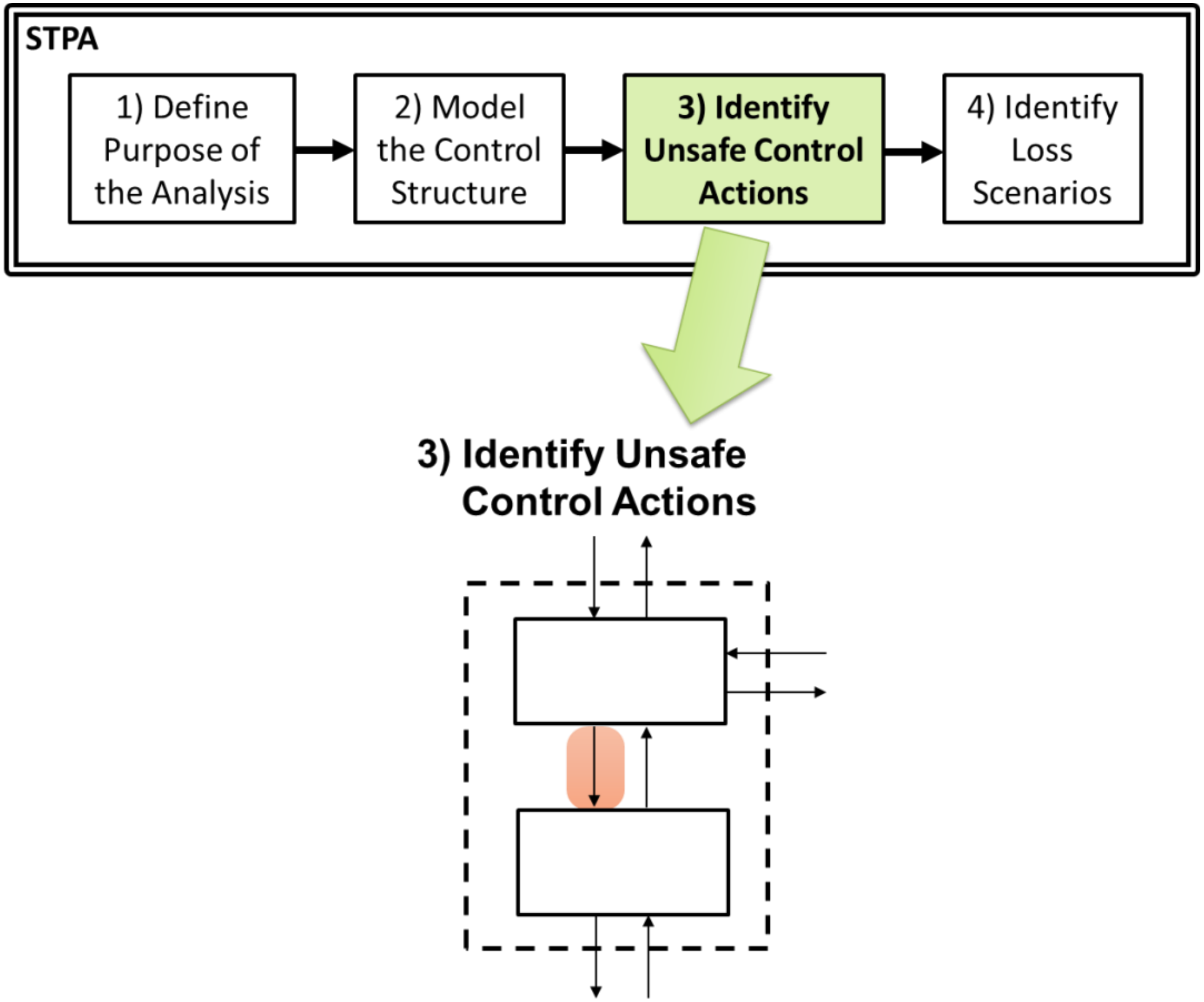

Pilot
Manage
Takeoff
Thrust
Orientation
Cabin environment
Position and heading
Taxi and landing
Movement on ground
etc.
Model of Automation
Model of Aircraft
Model of Airport (Environment)
Sensory and other Inputs
Environmental Inputs
Flight Commands
Feedback
Control Commands
A/C Automation (Flight Control Computer, FMS, etc.)
Control
Takeoff
Thrust
Orientation
Cabin environment
Position and heading
Taxi and landing
Movement on ground
etc.
Model of Aircraft
Feedback
Control Commands
Feedback
Aircraft

Wheel Braking System Control Structure

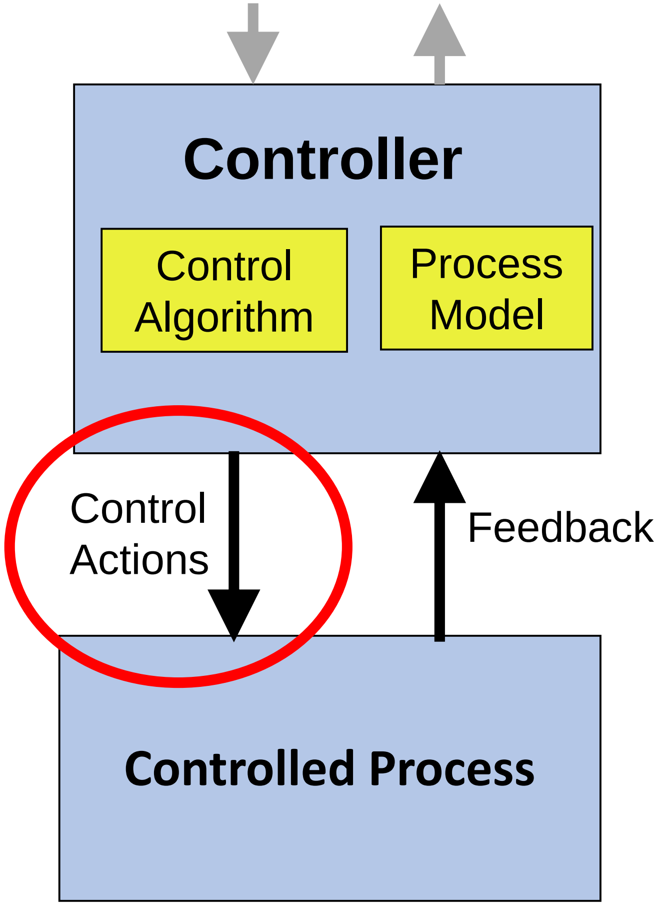


Flight Crew
Ensure aircraft decelerates appropriately upon landing
Rejected takeoff decision before V1
Etc.
Process Model
Flight mode
Status of Autobrake
Status of BSCU
A/C ground speed
Status of other braking mechanisms
Runway length
etc.
Normal/Alternate braking mode
Brake (pedal)
Arm and Set
Disarm
Power on/off
Autobrake status (activated, armed, decleration rate)
Fault detected
BSCU
Autobrake triggers (touchdown, RTO)
Brake/anti–skid commands
WBS Hydraulics
Braking force
Wheels
Wheel Speed

Identifying Unsafe Control Actions (UCAs)


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
3) Identify Unsafe Control Actions

Hazard and Accident Analysis with STPA



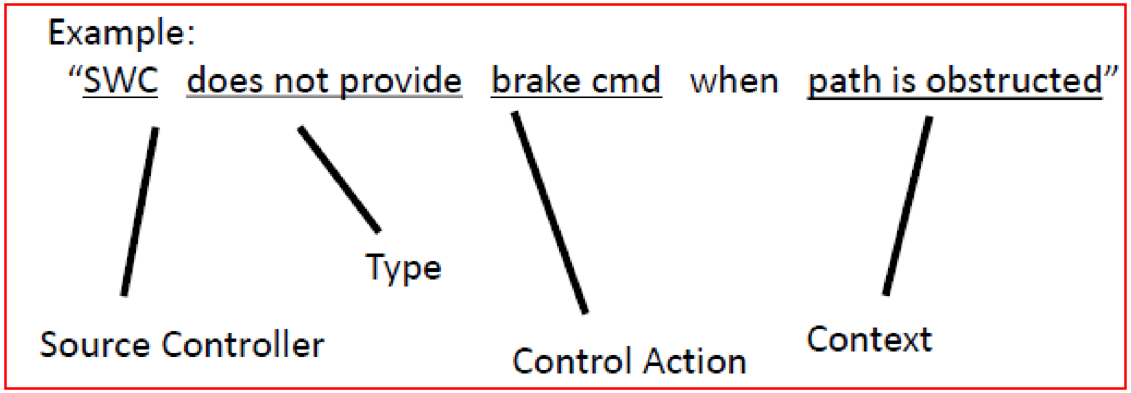
Four types of unsafe control actions

1) Control commands required for safety are not given
2) Unsafe commands are given
3) Potentially safe commands but given too early, too late, or in wrong order
4) Control action stops too soon or applied too long (continuous control)

Analysis and Design:

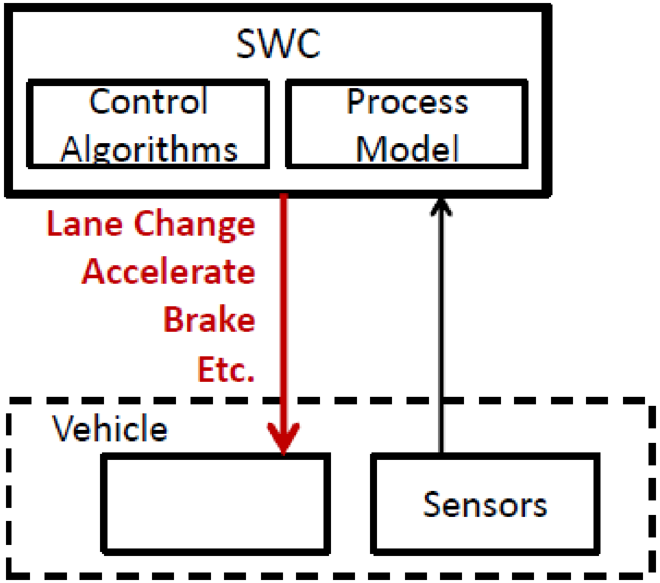
1. Identify potential unsafe control actions
2. Identify why they might be given (scenarios)
3. Eliminate scenarios through design or operations
4. If safe ones provided, then why not followed?

STPA: Unsafe Control Actions (UCA)



Example:

"SWC does not provide brake cmd when path is obstructed"



	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Brake Command	UCA-1: SWC does not provide Brake cmd when vehicle path is obstructed			

© Copyright John Thomas 2018

Unsafe Control Actions for Crew (Context Table)

Control Action By Flight Crew:	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
CREW.1 Manual braking via brake pedals	CREW.1a1 Crew does not provide manual braking during landing, RTO, or taxiing **when Autobrake is not providing braking (or insufficient braking),** leading to overshoot [H4-1, H4-5]	CREW.1b1 Manual braking provided with **insufficient pedal pressure,** resulting inadequate deceleration during landing [H4-1, H4-5]	CREW.1c1 Manual braking applied **before touchdown** causes wheel lockup, loss of control, tire burst [H4-1, H4-5]	CREW.1d1 Manual braking command is **stopped before safe taxi speed (TBD) is reached,** resulting in overspeed or overshoot [H4-1, H4-5]

What is another UCA for "providing"?

Unsafe Control Actions for Crew (Context Table)

Control Action By Flight Crew:	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
CREW.1 Manual braking via brake pedals	CREW.1a1 Crew does not provide manual braking during landing, RTO, or taxiing **when Autobrake is not providing braking (or insufficient braking),** leading to overshoot [H4-1, H4-5]	CREW.1b1 Manual braking provided with **insufficient pedal pressure,** resulting inadequate deceleration during landing [H4-1, H4-5] Manual braking **after V1 point** resulting in …	CREW.1c1 Manual braking applied **before touchdown** causes wheel lockup, loss of control, tire burst [H4-1, H4-5]	CREW.1d1 Manual braking command is **stopped before safe taxi speed (TBD) is reached,** resulting in overspeed or overshoot [H4-1, H4-5]

Unsafe Control Actions by Autobraking

Control Action by BSCU	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
BSCU.1 Brake command	BSCU.1a1 Brake command not provided **during RTO (to V1)**, resulting in inability to stop within available runway length [H4-1, H4-5]	BSCU.1b1 Braking commanded excessively **during landing roll**, resulting in rapid deceleration, loss of control, occupant injury [H4-1, H4-5]	BSCU.1c1 Braking commanded **before touchdown**, resulting in tire burst, loss of control, injury, other damage [H4-1, H4-5]	BSCU.1d1 Brake command stops **during landing roll before taxi speed attained**, causing reduced deceleration [H4-1, H4-5]

What is another UCA for “too late”?

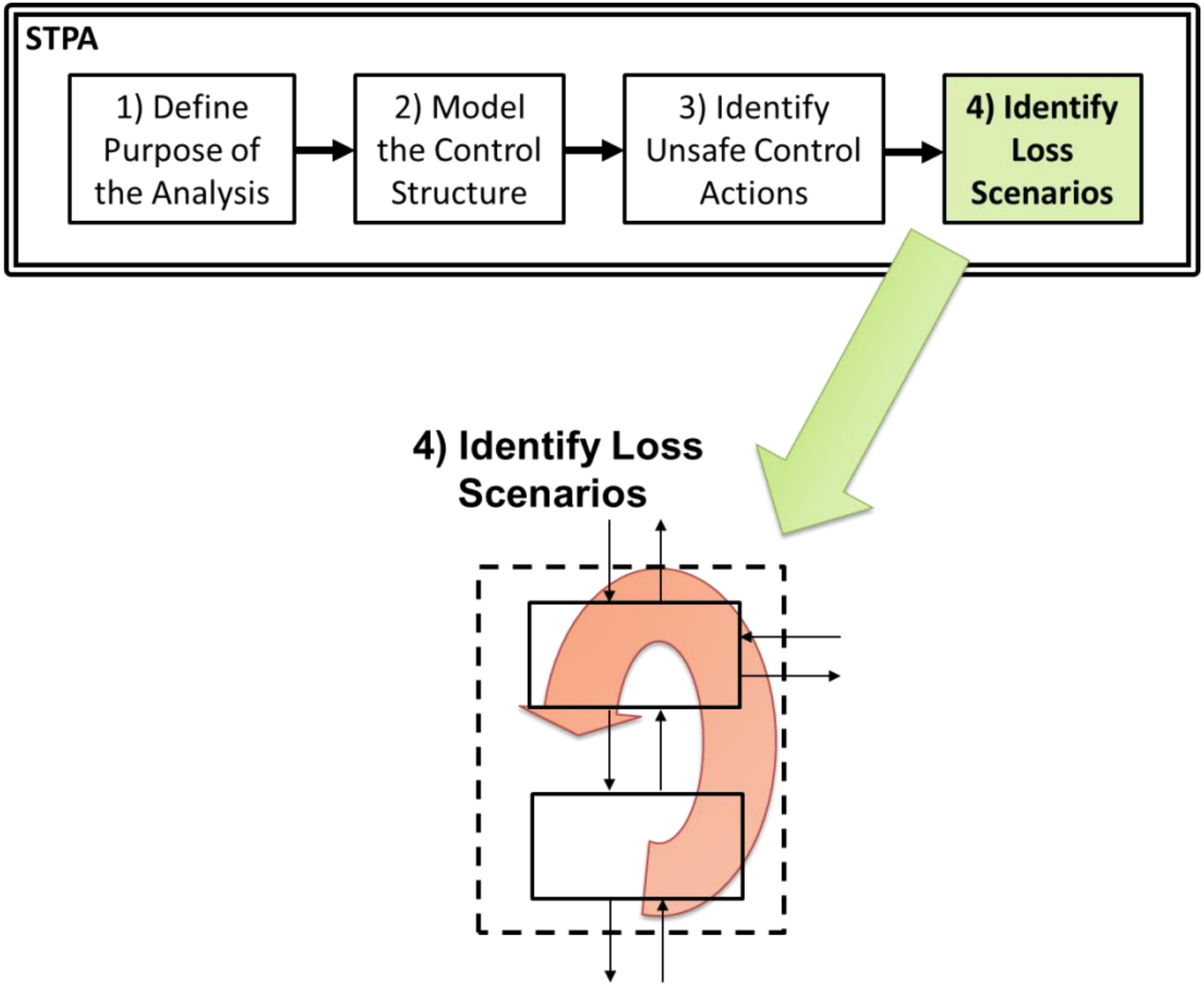
Unsafe Control Actions by Autobraking

Control Action by BSCU	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
BSCU.1 Brake command	BSCU.1a1 Brake command not provided **during RTO (to V1)**, resulting in inability to stop within available runway length [H4-1, H4-5]	BSCU.1b1 Braking commanded excessively **during landing roll**, resulting in rapid deceleration, loss of control, occupant injury [H4-1, H4-5]	BSCU.1c1 Braking commanded **before touchdown**, resulting in tire burst, loss of control, injury, other damage [H4-1, H4-5] BSCU.1.c.2: Braking commanded **too late after touchdown** resulting in …	BSCU.1d1 Brake command stops **during landing roll before taxi speed attained**, causing reduced deceleration [H4-1, H4-5]

STPA-Generated Safety Requirements/Constraints

Unsafe Control Action	Description	Rationale
FC-R1	Crew must not provide manual braking before touchdown [CREW.1c1]	Could cause wheel lockup, loss of control, or tire burst
FC-R2	Crew must not stop manual braking more than TBD seconds before safe taxi speed reached [CREW.1d1]	Could result in overspeed or runway overshoot
FC-R3	The crew must not power off the BSCU during autobraking [CREW.4b1]	Autobraking will be disarmed
BSCU-R1	A brake command must always be provided during RTO [BSCU.1a1]	Could result in not stopping within the available runway length
BSCU-R2	Braking must never be commanded before touchdown [BSCU.1c1]	Could result in tire burst, loss of control, injury, or other damage
BSCU-R3	Wheels must be locked after takeoff and before landing gear retraction [BSCU.1a4]	Could result in reduced handling margins from wheel rotation in flight

Identifying Loss Scenarios



STPA

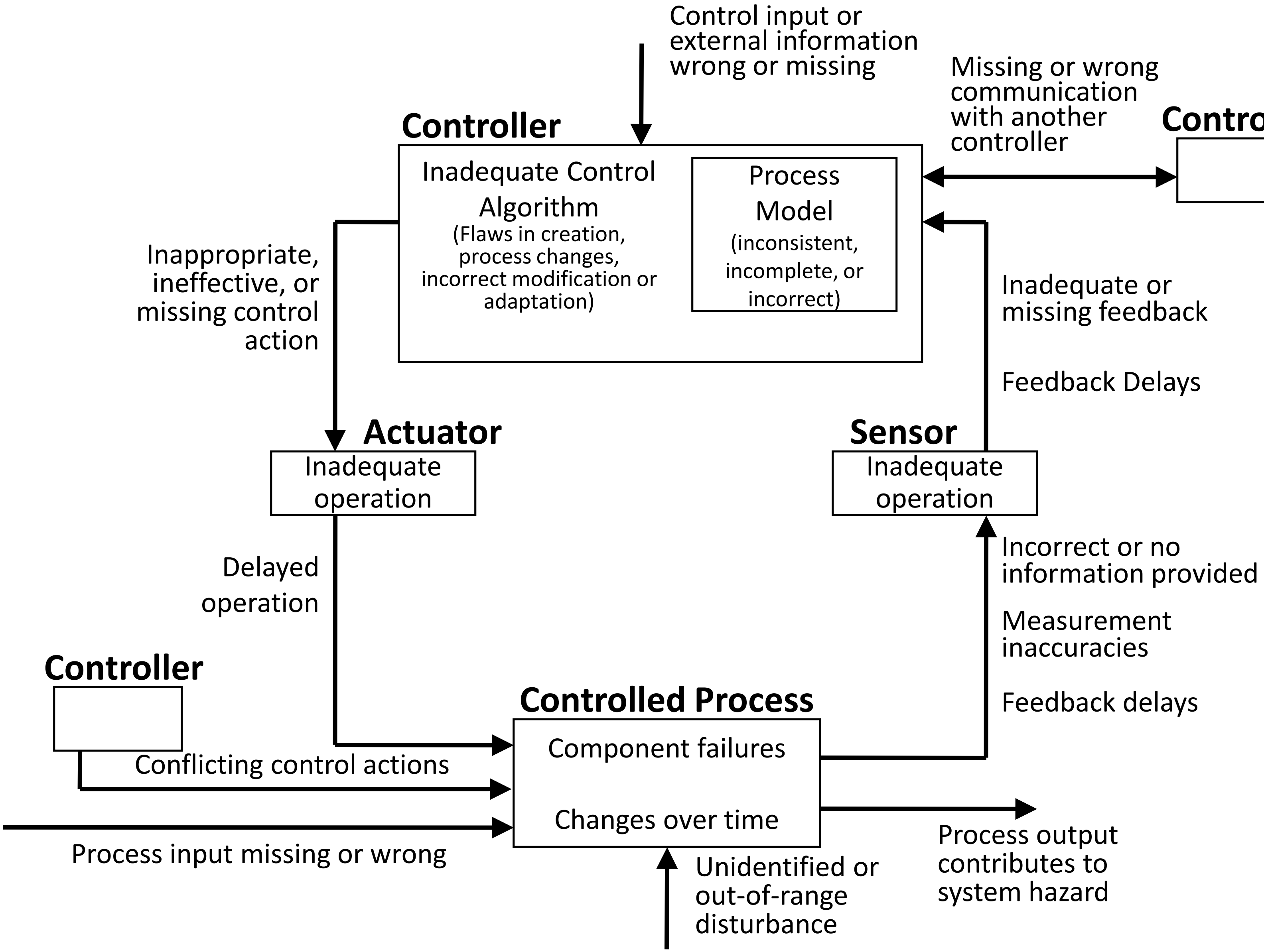
1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

4) Identify Loss Scenarios



Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

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

Process Model (inconsistent, incomplete, or incorrect)

Controller

Inappropriate, ineffective, or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delayed operation

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

Unidentified or out-of-range disturbance

Process output contributes to system hazard

UNSAFE CONTROL ACTION – CREW.1a: Crew does not provide manual braking when there is no Autobraking and braking is necessary to prevent H4-1 and H4-5.

Scenario 1: Crew incorrectly believes that the Autobrake is armed and expect the Autobrake to engage (process model flaw)

Reasons that their process model could be flawed include:

- The crew previously armed Autobrake and does not know it later became unavailable

AND/OR

- Crew receives feedback when the BSCU Hydraulic Controller detects a fault. The crew would be notified of a generic BSCU fault but they are not notified that Autobraking is no longer available

AND/OR

- The crew is notified that the Autobrake controller is still armed and ready, because the Autobrake controller does not detect when the BSCU has detected a fault. When the BSCU detects a fault, it makes Autobrake commands ineffective, but the Autobrake system itself does not notify the crew.
- The crew cannot process feedback due to multiple messages, conflicting messages, alarm fatigue, etc.

Possible new requirements for S1: The BSCU hydraulic controller must provide feedback to the Autobrake when it is faulted and the Autobrake must disengage (and provide feedback to crew).

Other requirements may be generated from a human factors analysis of the ability of the crew to process the feedback under various worst-case conditions.

Generate Potential Causal Scenarios

Crew: Crew provides manual braking **after V1,** leading to …

Scenario 1: Crew thinks …

Possible Requirement for S1: …

BSCU.1a2: Brake command not provided during landing roll, resulting in insufficient deceleration and potential overshoot

Scenario 1: Autobrake believes the desired deceleration rate has already been achieved or exceeded (incorrect process model). The reasons Autobrake may have this process model flaw include:

- If wheel speed feedback influences the deceleration rate determined by the Autobrake controller, inadequate wheel speed feedback may cause this scenario. Rapid pulses in the feedback (e.g. wet runway, brakes pulsed by anti-skid) could make the actual aircraft speed difficult to detect and an incorrect aircraft speed might be assumed.
- Inadequate external speed/deceleration feedback could explain the incorrect Autobrake process model (e.g. inertial reference drift, calibration issues, sensor failure, etc.)
- **[Security related scenarios, e.g., intruder changes process model]**

Possible Requirement for S1: Provide additional feedback to Autobrake to detect aircraft deceleration rate in the event of wheel slipping (e.g. fusion of multiple sensors)

Generate Potential Causal Scenarios

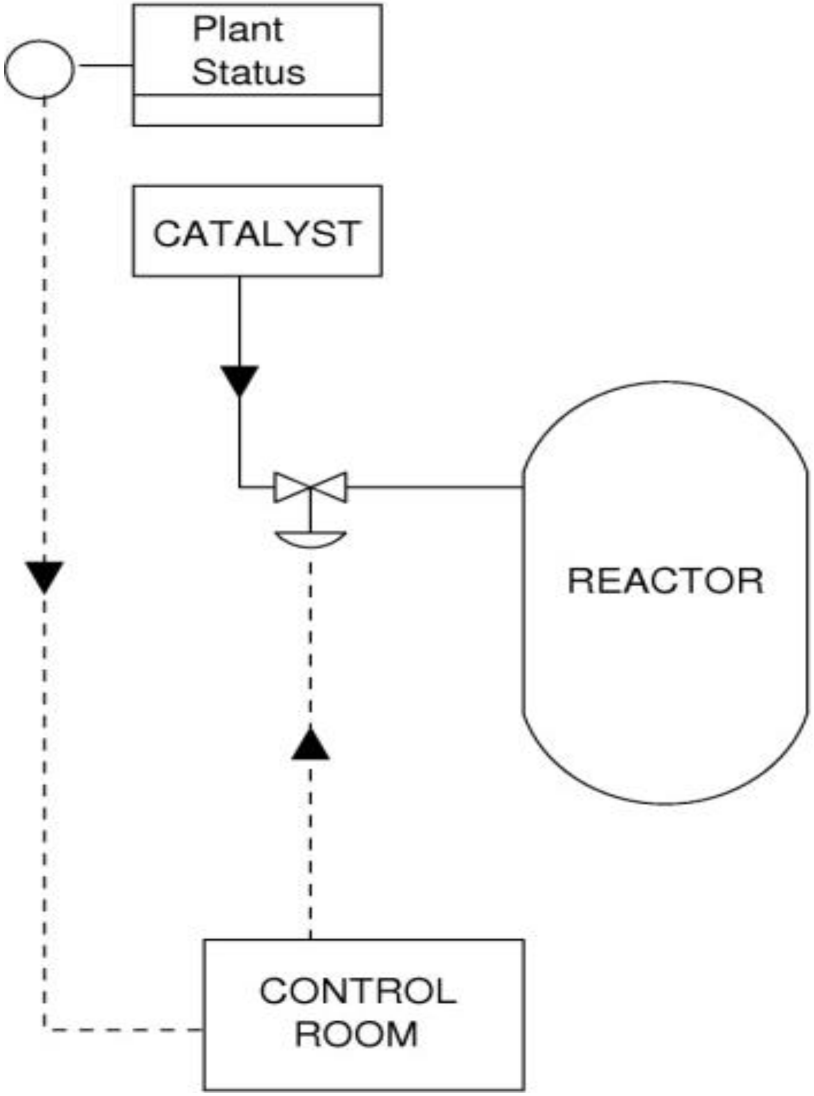
Crew 1a1: BSCU provides autobraking **too late after touchdown** resulting in overshoot, … [H4-1, H4-5]

Scenario 1: Autobrake process model …

Possible Requirement for S1: …

Chemical Reactor Example

Using STPA to Guide Design Decisions



Requirements:

- Produce product

  (add chemicals and catalyst to reactor)
- Monitor plant status

Mishaps/accidents?

Hazards?

Safety Constraints?

Steps in STPA

- Establish foundation for analysis
  - Define "accident" for your system
  - Define hazards
  - Rewrite hazards as constraints on system design
- Draw preliminary (high-level) functional control structure
- Step 1: Identify potentially unsafe control actions (high-level safety requirements and constraints)
- Step 2: Determine how each potentially hazardous control action could occur

Define Mishaps, Hazards, Safety Constraints

- System Requirements
  - Produce product (add chemicals and catalyst to reactor)
  - Monitor plant status
- Mishaps
  - M-1: Explosion
  - M-2: Chemical ingestion by human
  - M-3: Environmental pollution
- Hazards
  - H-1: Overheating/overpressurization of reactor (M-1)
  - H-2: Release of chemicals within or outside plant (M-2, M-3)
- Safety Constraints/Requirements
  - SC1: Pressure/temperature in reactor must stay in safe range (H-1)
  - SC2: Chemicals must not be released outside plant boundaries (H-2)
  - SC3: If chemicals are released, damage must be mitigated (H-2)

Steps in STPA

- Establish foundation for analysis
  - Define “accident” for your system
  - Define hazards
  - Rewrite hazards as constraints on system design
- Draw preliminary (high-level) functional control structure
- Step 1: Identify potentially unsafe control actions (high-level safety requirements and constraints)
- Step 2: Determine how each potentially hazardous control action could occur

Draw the Functional Control Structure

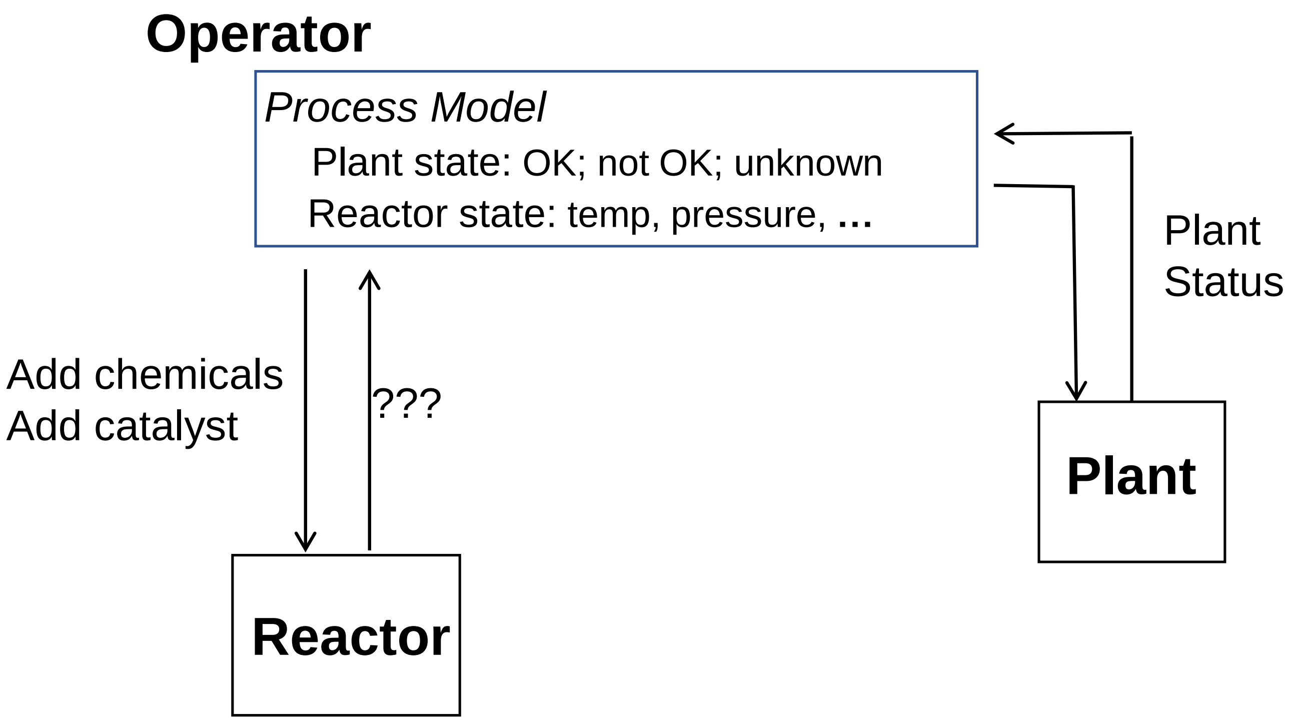
- Identify major components and controllers

  (HINT: Start at very high level)

- Label control and feedback arrows

- Create the preliminary process models

Highest Level Initial Control Structure



Operator

Process Model

Plant state: OK; not OK; unknown

Reactor state: temp, pressure, **…**

Plant Status

Add chemicals
Add catalyst

???

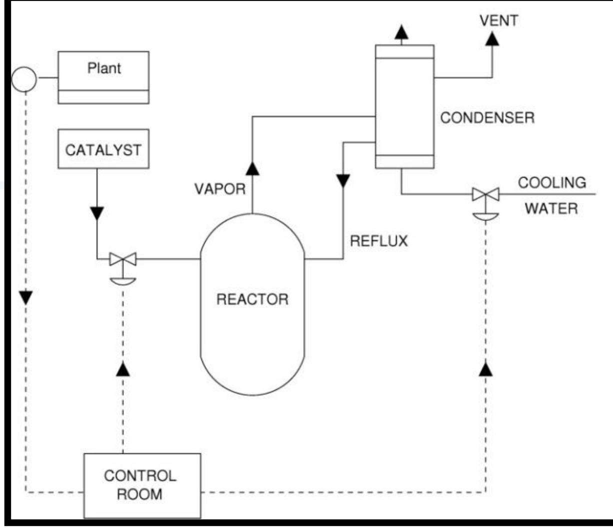
Plant

Reactor

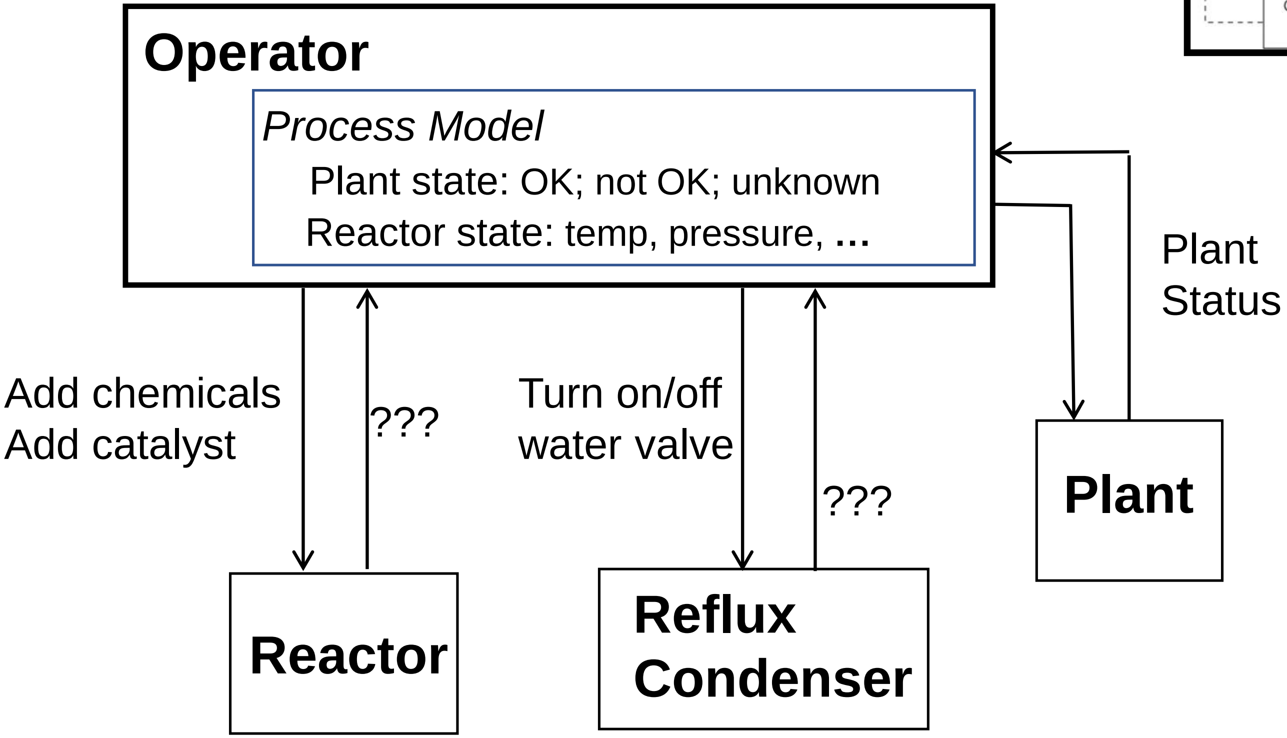
How will we control the hazards?

- Decide to add a reflux condenser to cool reaction, relief valve to reduce pressure
- High-level (system) hazard: Overheating, overpressurization of reactor
- Refined hazard: ???

Construct Control Model



[Note difference between the control model and the physical model (architecture)]



Refine system-level hazards after add reflux condenser

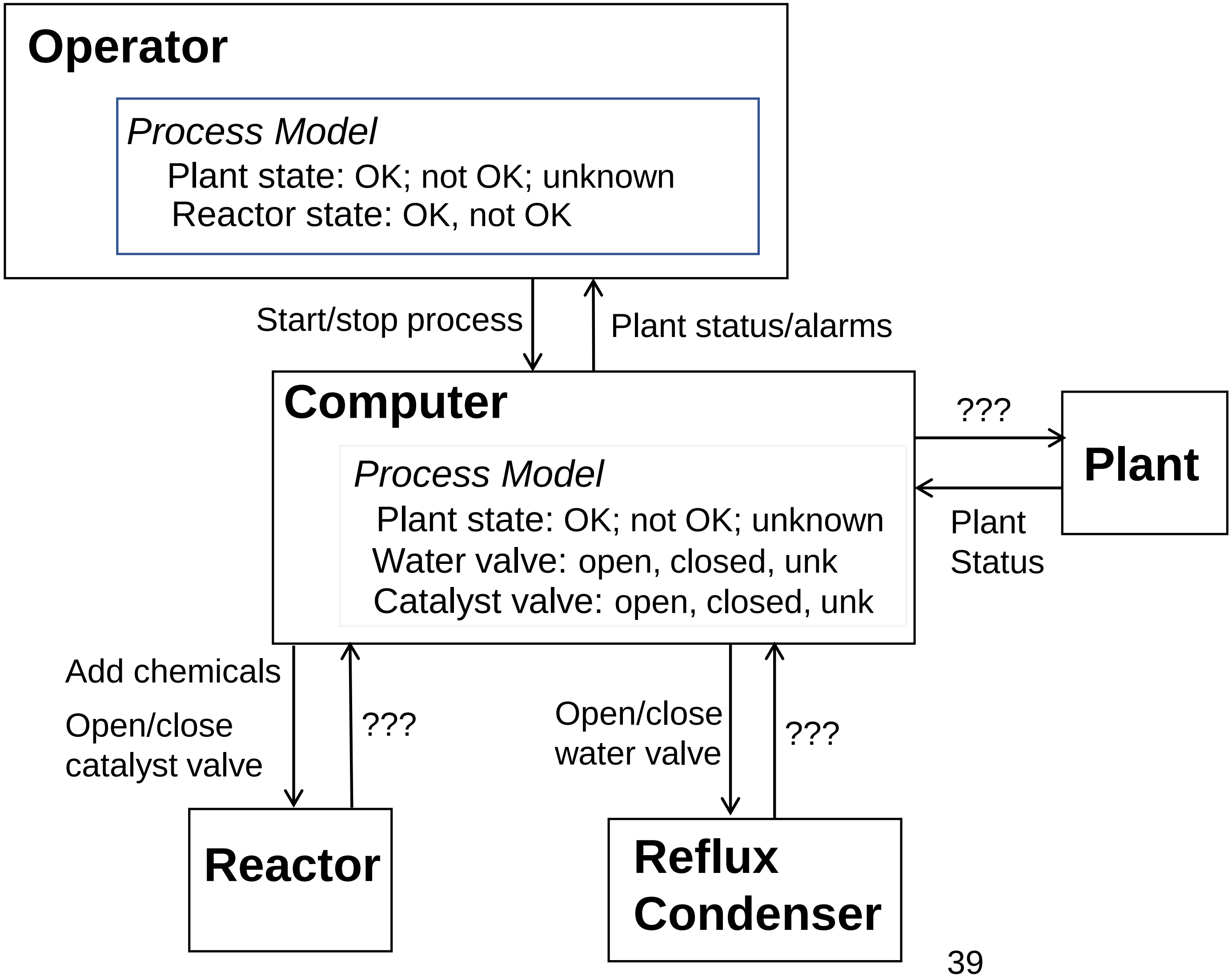
- High-level (system) hazard: Overheating, overpressurization of reactor;
- Refined hazard:
  1. Reflux condenser does not adequately control temperature [keep temp < X]

     1a. Reflux condenser not operating when catalyst in reactor

     1b. Reflux condenser design not adequate to control temp

  2. Relief valve does not eliminate overpressurization (H-1b)

Decide to Add a Computer



Operator

Process Model

Plant state: OK; not OK; unknown

Reactor state: OK, not OK

Start/stop process

Plant status/alarms

Computer

Process Model

Plant state: OK; not OK; unknown

Water valve: open, closed, unk

Catalyst valve: open, closed, unk

???

Plant

Plant Status

Add chemicals

Open/close catalyst valve

???

Open/close water valve

???

Reactor

Reflux Condenser

Steps in STPA

- Establish foundation for analysis
  - Define “accident” for your system
  - Define hazards
  - Rewrite hazards as constraints on system design
- Draw preliminary (high-level) functional control structure
- Step 1: Identify potentially unsafe control actions (high-level safety requirements and constraints)
- Step 2: Determine how each potentially hazardous control action could occur

Four Ways Unsafe Control Can Occur

- Providing the control action leads to a hazard
- Not providing the control action leads to a hazard
- Timing or sequencing of control actions leads to a hazard
- Duration (too long, too short) leads to a hazard

Identify conditions (context) under which control action can lead to a hazard

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order	Stopped too soon/ applied too long

UCA Context Table for: Reflux condenser not operating when catalyst in reactor (H-1a)

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Open Water Valve	Water valve not opened **when catalyst open**		Open water **more than X seconds after open catalyst**	Stop **before fully opened**
Close Water Valve				
Open Catalyst Valve				
Close Catalyst Valve				

Hazard: Catalyst in reactor without reflux condenser operating (water flowing through it)

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early/too late, wrong order**	**Stopped too soon/ applied too long**
Open water	Not opened **when catalyst open (H-1)**		Open water **more than X seconds after open catalyst**	Stop **before fully opened**
Close water		Close **while catalyst open**	Close water **before catalyst closes**	
Open catalyst		Open **when water valve not open**	Open catalyst **more than X seconds before open water**	
Close catalyst	Do not close **when water closed**		Close catalyst **more than X seconds after close water**	Stop **before fully closed**

STPA generates the following high-level safety constraints on the batch reactor:

- Water valve must always be fully open before catalyst valve is opened.
  - Water valve must never be opened (complete opening) more than X seconds after catalyst valve opens

- Catalyst valve must always be fully closed before water valve is closed.
  - Catalyst valve must never be closed more than X seconds after water valve has fully closed.

Next step is to identify scenarios leading to the unsafe control actions (violation of safety constraints) and eliminate or mitigate them

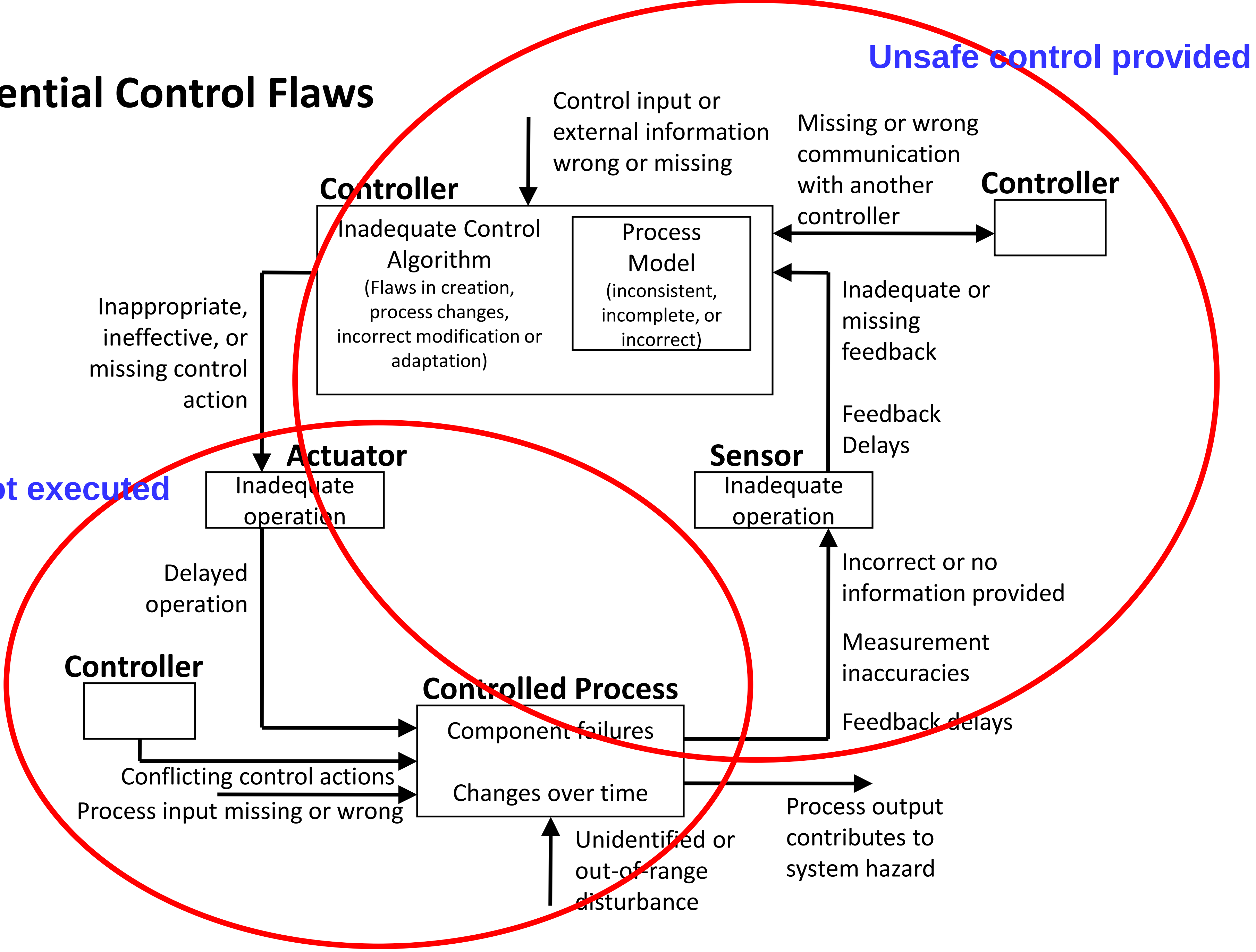
Steps in STPA

- Establish foundation for analysis
  - Define “accident” for your system
  - Define hazards
  - Rewrite hazards as constraints on system design
- Draw preliminary (high-level) functional control structure
- Step 1: Identify potentially unsafe control actions (high-level safety requirements and constraints)
- Step 2: Determine how each potentially hazardous control action could occur

Generating Causal Scenarios

- Identify causes of the hazardous control actions (why hazardous control actions given)
- Identify causes for a required control action (e.g., open water valve) being given by the software but not executed.
- What design features (controls) might you use to protect the system from the scenarios you found?

Potential Control Flaws



Unsafe control provided

Not executed

Controller

Control input or external information wrong or missing

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

Process Model (inconsistent, incomplete, or incorrect)

Missing or wrong communication with another controller

Controller

Inappropriate, ineffective, or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delayed operation

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

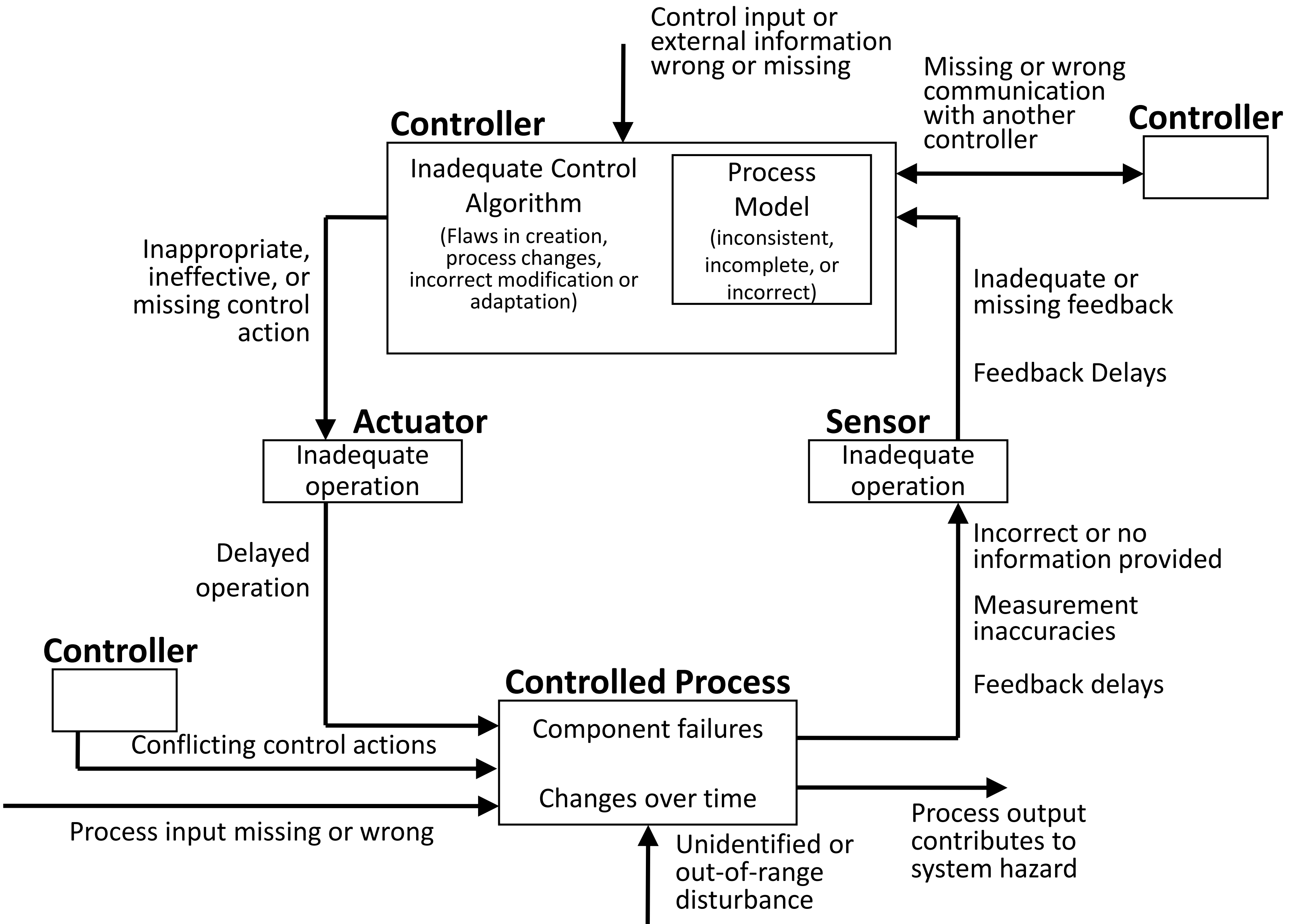
Unidentified or out-of-range disturbance

Process output contributes to system hazard

Causes of Unsafe Control Actions

- Identify causes of the hazardous control actions: *Open catalyst valve when water valve not open*
  - HINT: Consider how controller’s process model could identify that water valve is open when it is not.
- What design features (controls) might you use to protect the system from the scenarios you found?

Why might software open catalyst valve when water valve not open? *[Hint: Start with Process Model]*



Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

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

Process Model (inconsistent, incomplete, or incorrect)

Controller

Inappropriate, ineffective, or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delayed operation

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

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Some Reasons for Incorrect Process Model

- Previously issued an Open Water Valve command but valve did not open (jammed, failed, etc.)

- Assumed that command had been executed. Why?

  i. No feedback about effect of previous command was designed into system
  (Control: put feedback in design)

  ii. Feedback not received. [could go on to determine "why" here if want]
  (Control: Wait predetermined time and assume not executed)

  iii. Feedback delayed (could go on to determine "why" if want)
  (Control: wait predetermined time and then assume not opened)

  iv. Incorrect feedback received. Why? (maybe assumed that if reached valve, it would open [design error]
  (Control: add flow meter to detect water flow through pipe)

  etc.

Generates Potential New Requirements:

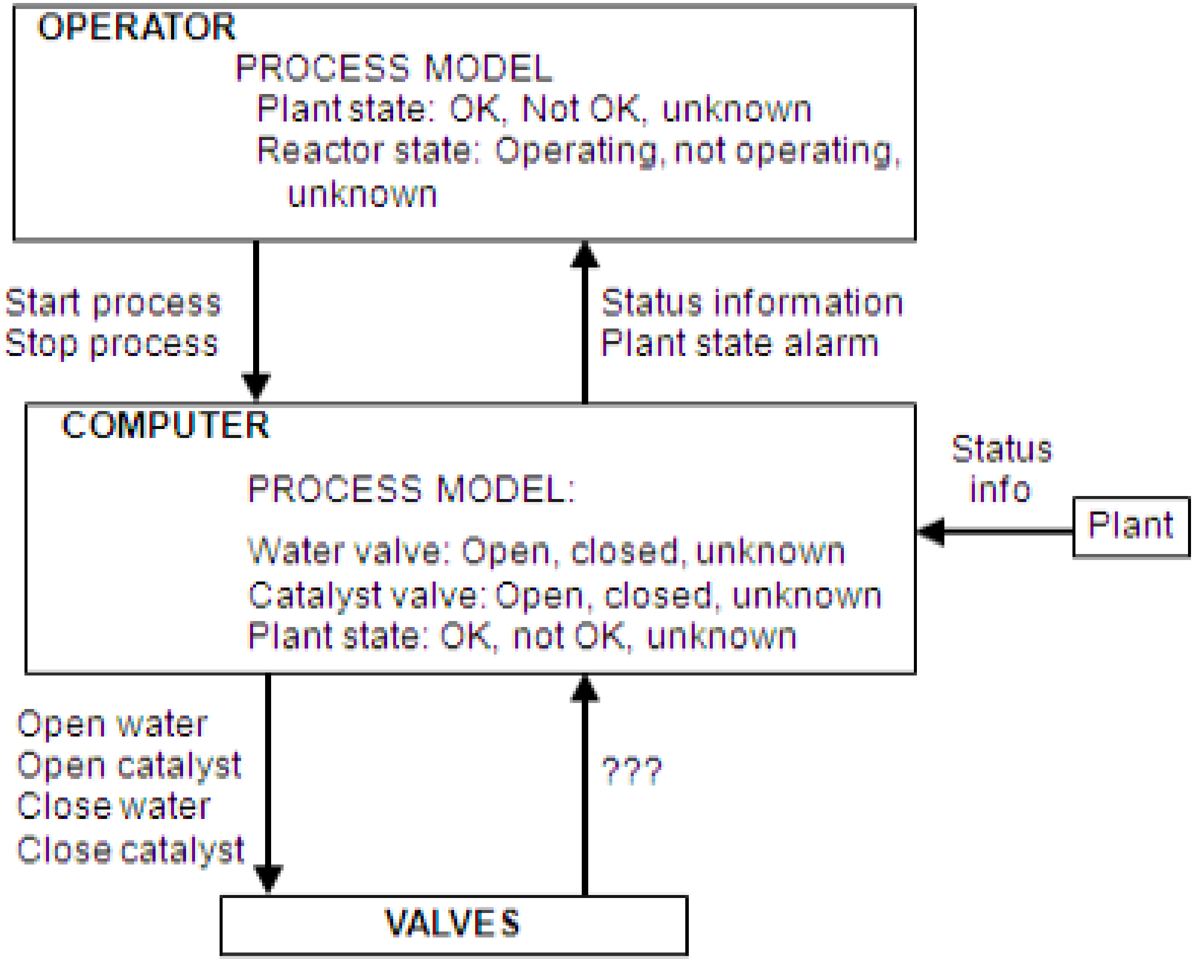
- Include feedback for Open Valve and Close Valve commands.
- Software shall check for feedback after issuing an Open/Close command. If not received in a specified time period, then assume valve not opened or closed and …
- There must be feedback to controller to determine that water is actually flowing through pipe before issuing an Open Catalyst command (perhaps use a flow monitor).
- …

Do Analysis on All Parts of System

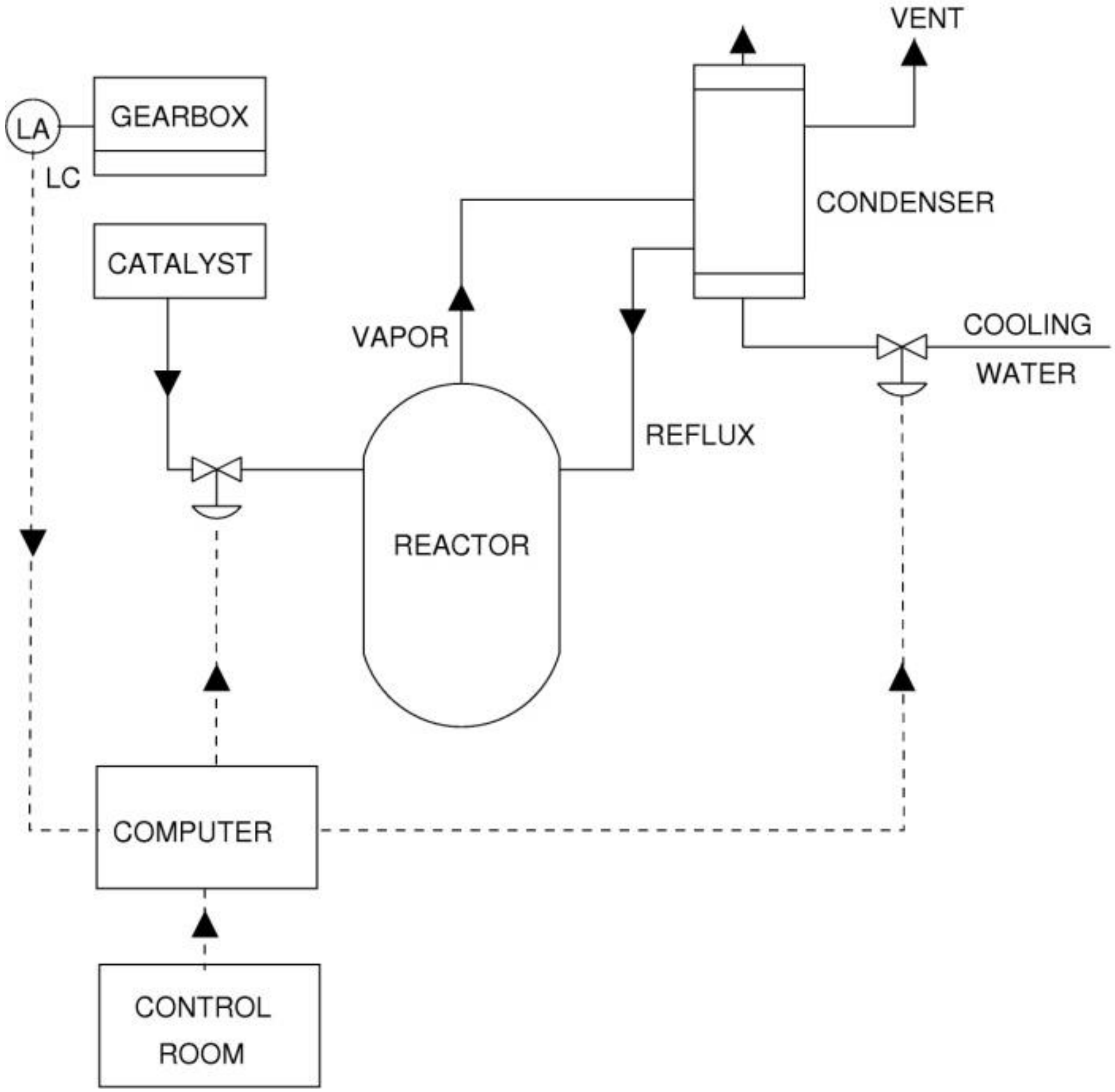
- Hardware, software, operators
- Use results to design accidents/losses out of system
- Can build tools and automation to assist in analysis

Could do same for human operator

Control Structure:


OPERATOR
PROCESS MODEL
Plant state: OK, Not OK, unknown
Reactor state: Operating, not operating, unknown
Start process
Stop process
Status information
Plant state alarm
COMPUTER
PROCESS MODEL:
Water valve: Open, closed, unknown
Catalyst valve: Open, closed, unknown
Plant state: OK, not OK, unknown
Status info
Plant
Open water
Open catalyst
Close water
Close catalyst
???
VALVES

An Actual Mishap (you found the problem)



Common Mistakes

- Identifying component hazards instead of system hazards

  Software adds chemicals before adding catalyst

  vs. Overheating/overpressurization of reactor (M-1)

  Relief valve opens inadvertently

  vs. Release of chemicals within or outside plant (M-2, M-3)

Why a problem? Potential Incompleteness

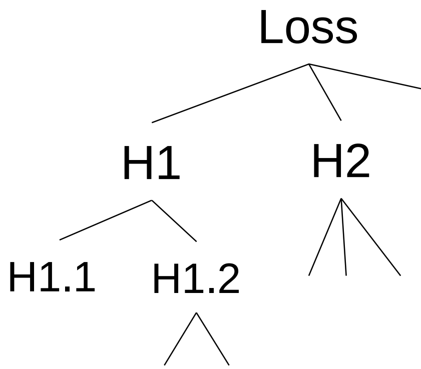
May miss other causes of overpressurization

STPA is a step-by-step process to assist in the analysis

Will only be a few (usually less than 10

If more, then go to a higher level of abstraction

Creating a “Tree” Structure



Helps organize the search so don’t omit things

Human factors consideration: This is a way humans

Organize their thoughts

Review things

Common Mistakes (2)

- Failures as hazards
  - "Valve fails closed" or "Reactor fails"
  - "Human fails"

    Humans do not "fail"

    Leads to missing human factors problems
  - "Software fails"

    Says nothing

    Omits all important software-related causes

    Specific incorrect wrong behavior is what you need to identify

    Unsafe software behavior usually related to unsafe requirements
    (requirements implemented correctly)

In general, avoid use of "fails" unless hardware (even then, not in
system hazard list because this is not a hazard or system state, it is a cause of a hazard).

Common Mistakes (3)

- Causes as hazards

  Correct:

  Overpressurization

  Incorrect:

  Relief valve does not open

  Chemicals added before catalyst

  Again, will miss things, not an organized method

- Needs to be within the system scope