Basic STPA Tutorial

John Thomas

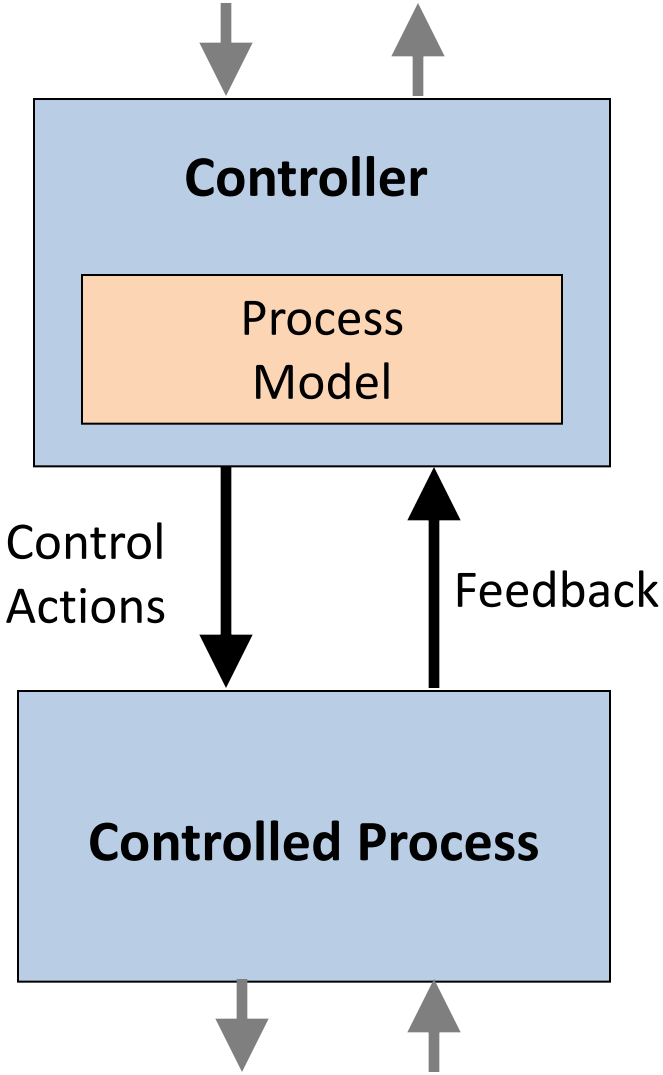
How is STAMP different?

STAMP Model

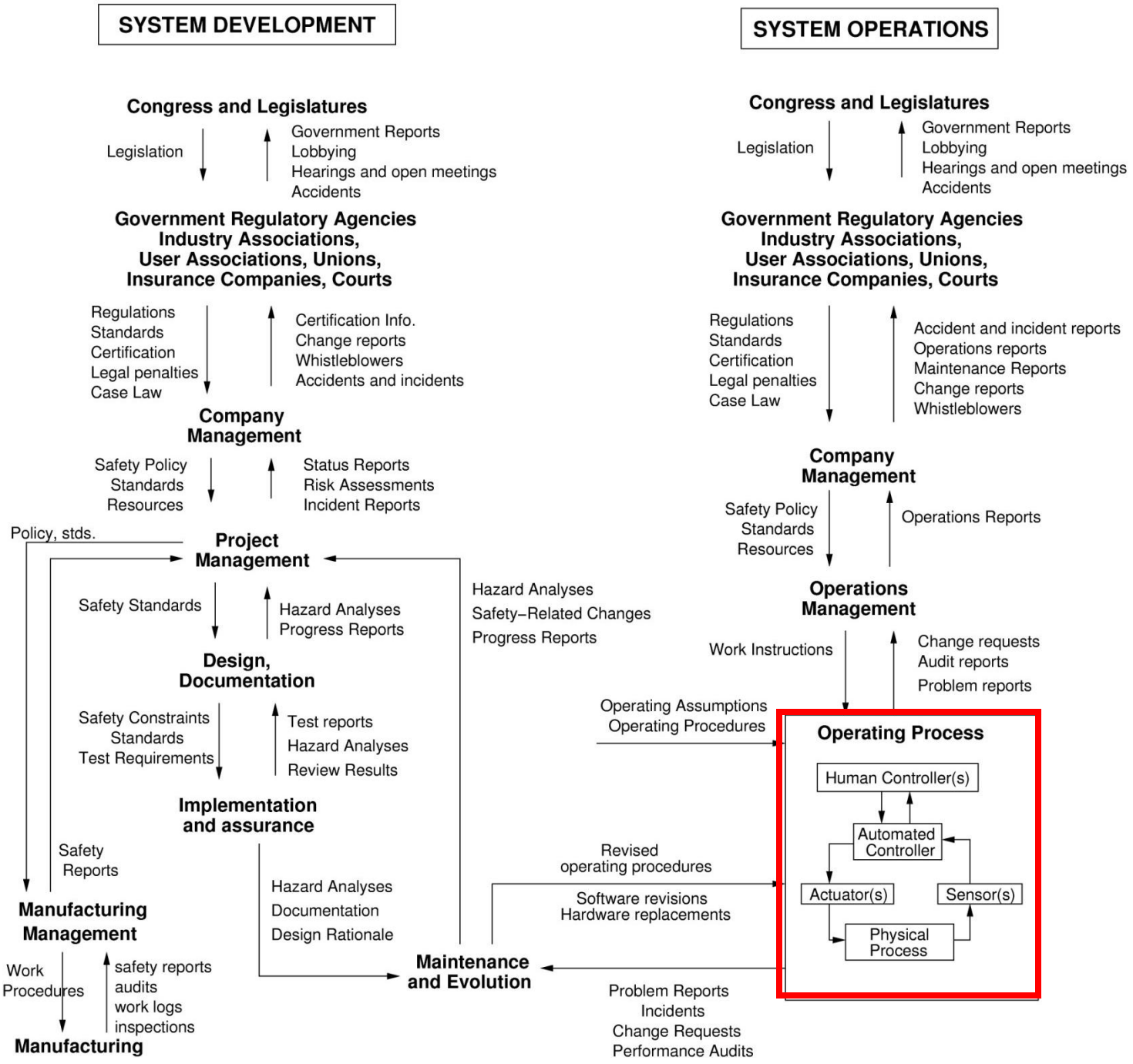
- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not a failure problem
- Prevent accidents by enforcing constraints on component behavior and **interactions**
- Captures more causes of accidents:
  - Component failure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

(Leveson, 2003); (Leveson, 2011)

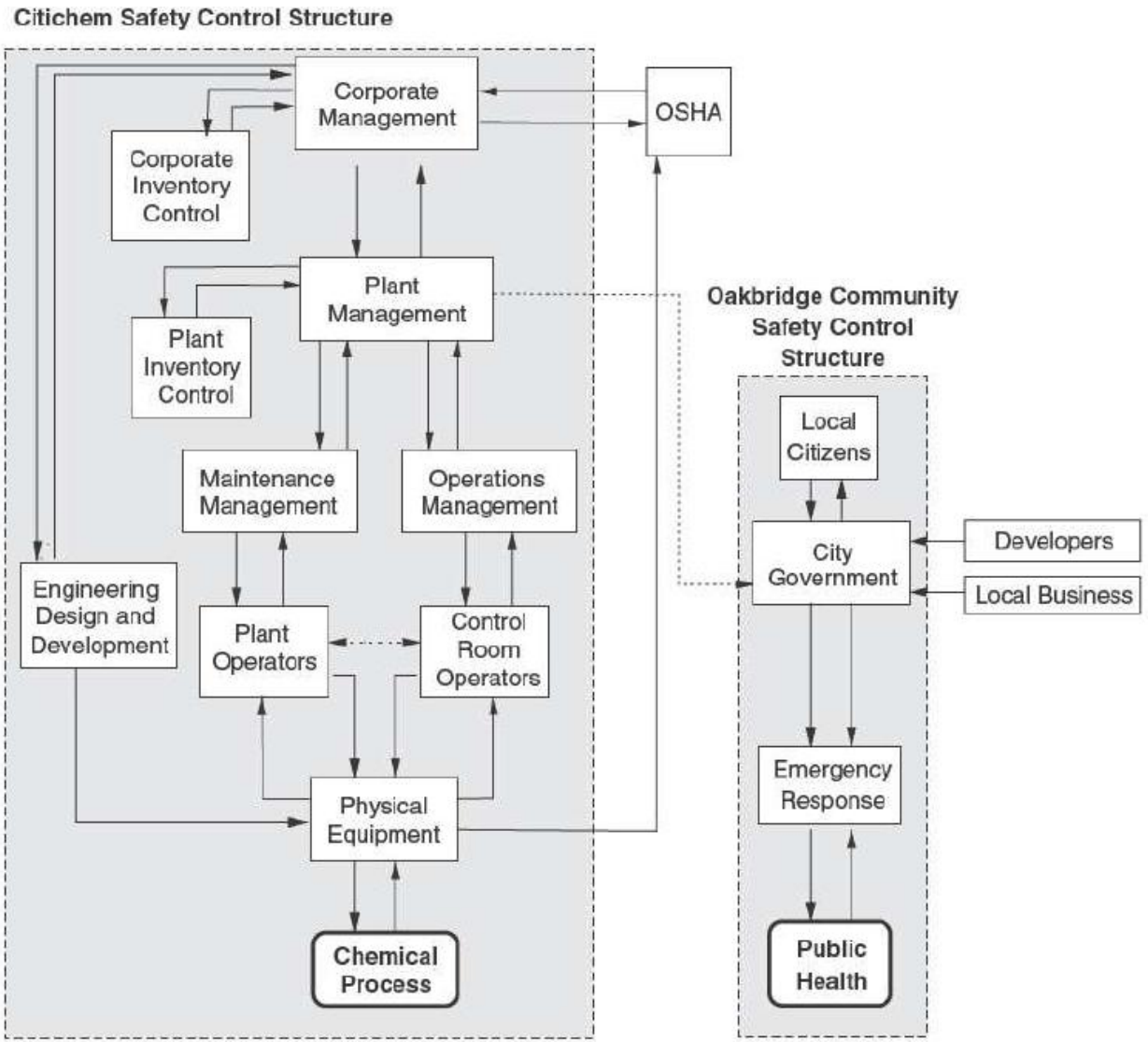
Basic Control Loop



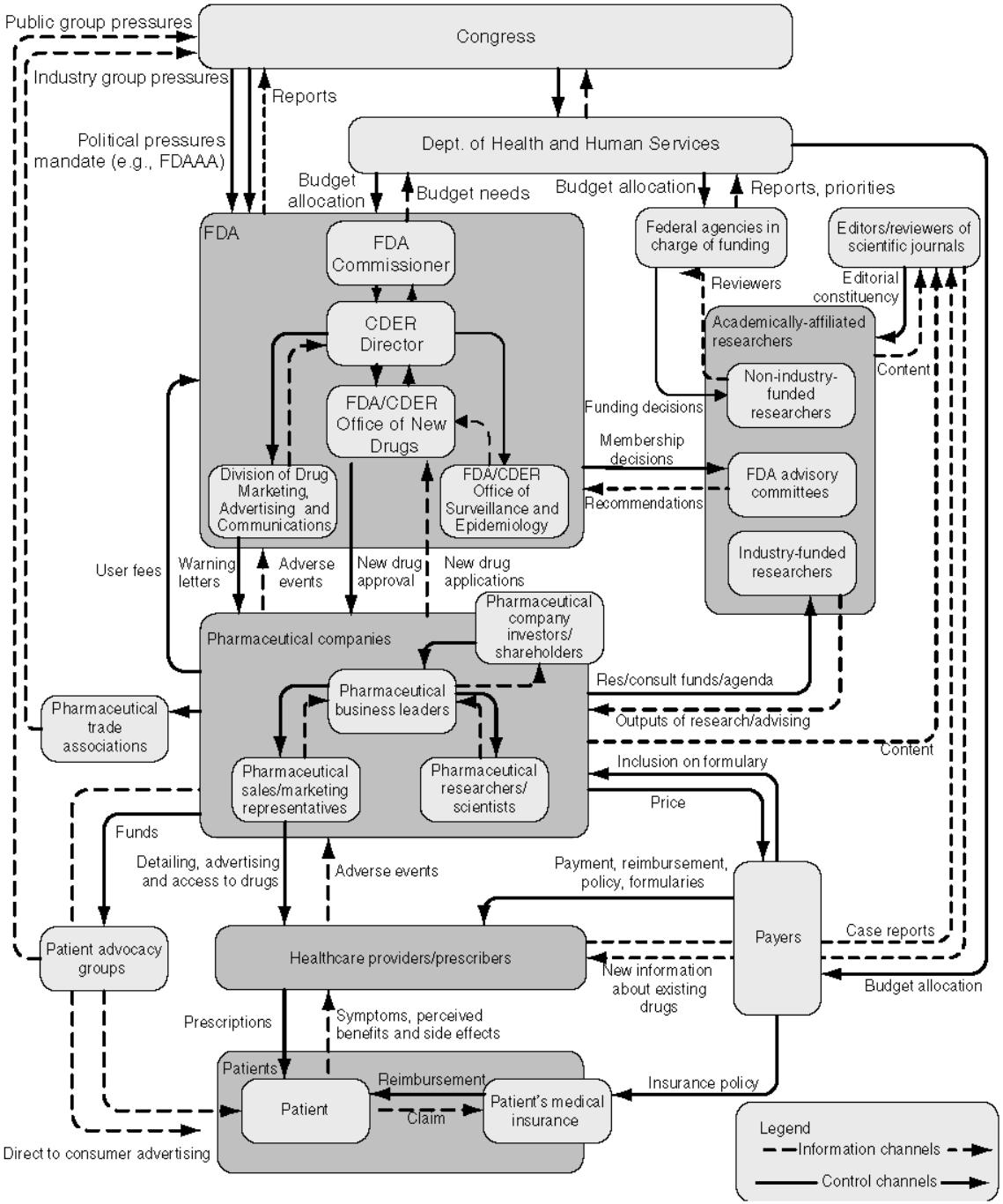
Generic Safety Control Structure



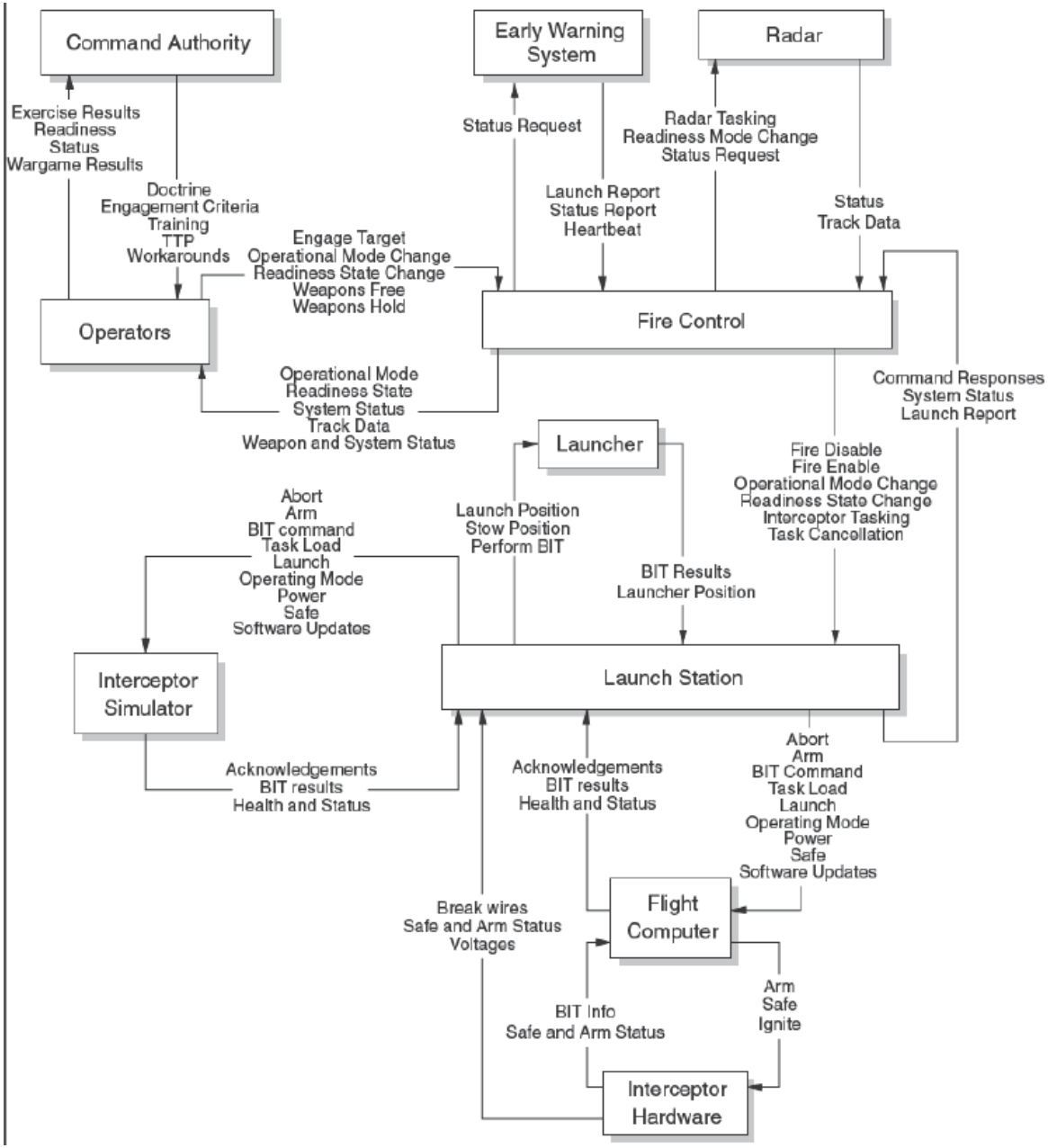
Example: Chemical plant



ESW p354

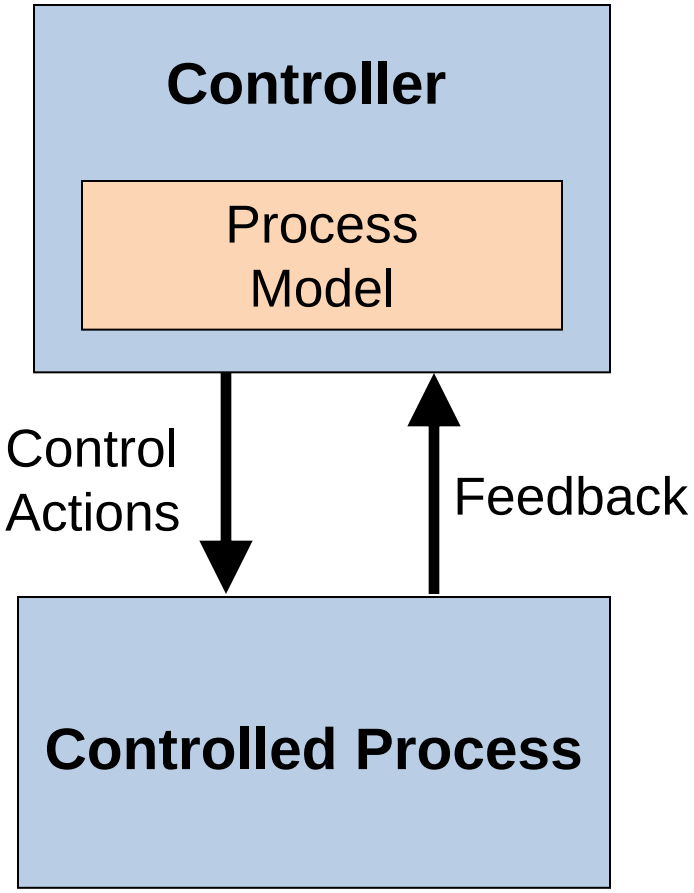


ESW p206: U.S. pharmaceutical safety control structure



ESW p216: Ballistic Missile Defense System

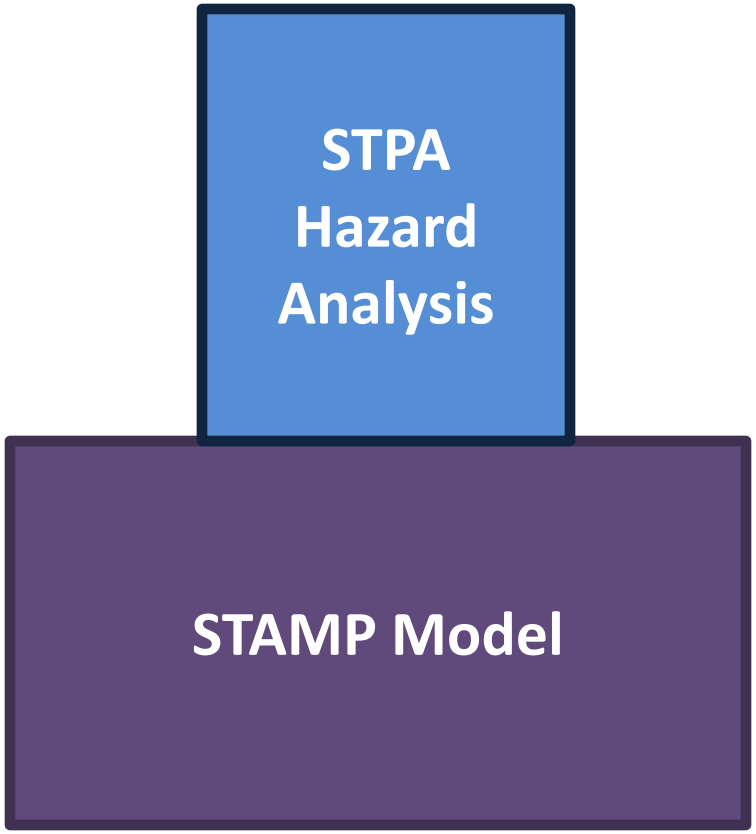
STAMP



- Controllers use a **process model** to determine control actions
- Accidents often occur when the process model is incorrect
- Four types of **hazardous 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

Explains software errors, human errors, component interaction accidents, components failures …

STPA
(System-Theoretic Process Analysis)

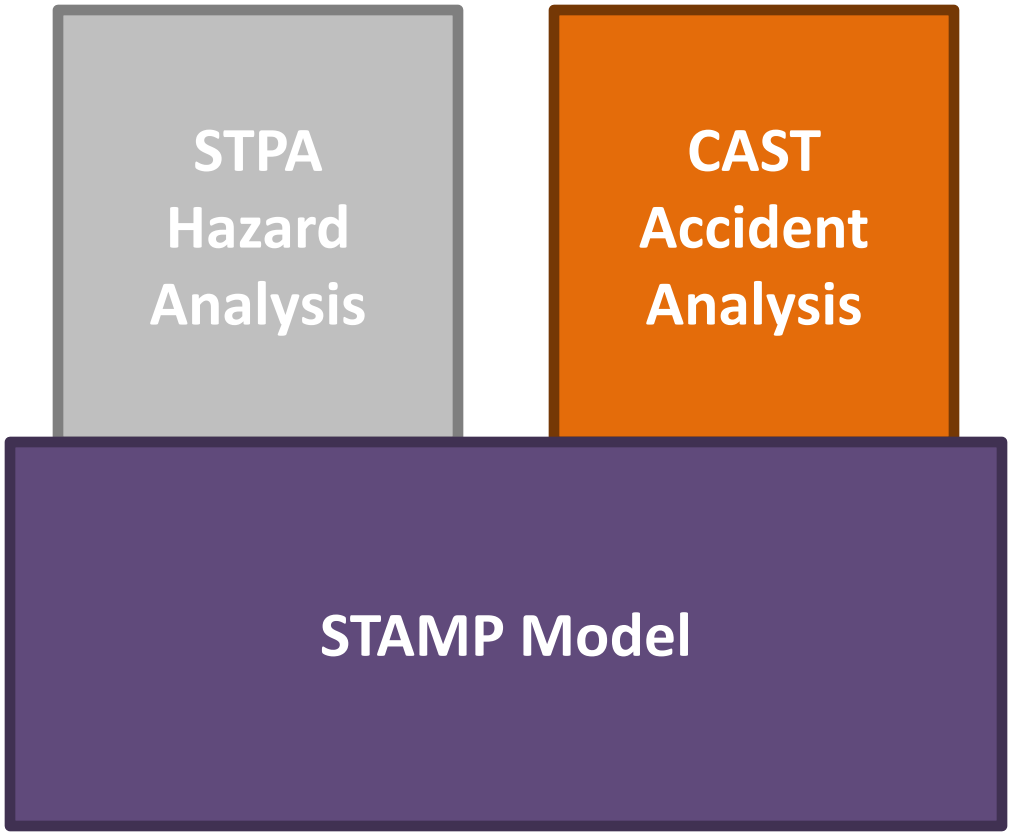


How do we find inadequate control in a system?

Accidents are caused by inadequate control

(Leveson, 2011)

CAST
(Causal Analysis using System Theory)



How do we find inadequate control that caused the accident?

Accidents are caused by inadequate control

(Leveson, 2011)

Today's Tutorials

- CAST Accident Analysis

  9am – noon, room 32-124

- **Basic STPA Hazard Analysis**

  9am – noon, room 32-141

- Advanced STPA Hazard Analysis

  9am – noon, room 32-155

Basic STPA Hazard Analysis

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

- 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**
- 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

Accident	Hazard
Satellite becomes lost or unrecoverable	Satellite maneuvers out of orbit
People die from exposure to toxic chemicals	Toxic chemicals are released into the atmosphere
People die from radiation sickness	Nuclear power plant releases radioactive materials
People die from food poisoning	Food products containing pathogens are sold

Identify Accident, Hazards, Safety Constraints

- System-level Accident (Loss)
  - ?
- System-level Hazard
  - ?
- System-level Safety Constraint
  - ?

Identify Accident, Hazards, Safety Constraints

- System-level Accident (Loss)
  - Death, illness, or injury due to exposure to toxic chemicals.
- System-level Hazard
  - Uncontrolled release of toxic chemicals
- System-level Safety Constraint
  - Toxic chemicals must not be released

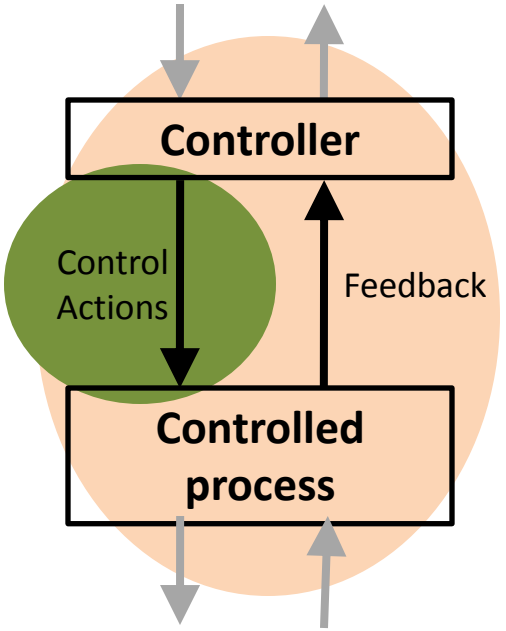
Additional hazards / constraints can be found in ESW p355

STPA
(System-Theoretic Process Analysis)

STPA Hazard Analysis

STAMP Model

- Identify accidents and hazards
- Construct the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and control flaws



(Leveson, 2011)

Step 1: Identify Unsafe Control Actions

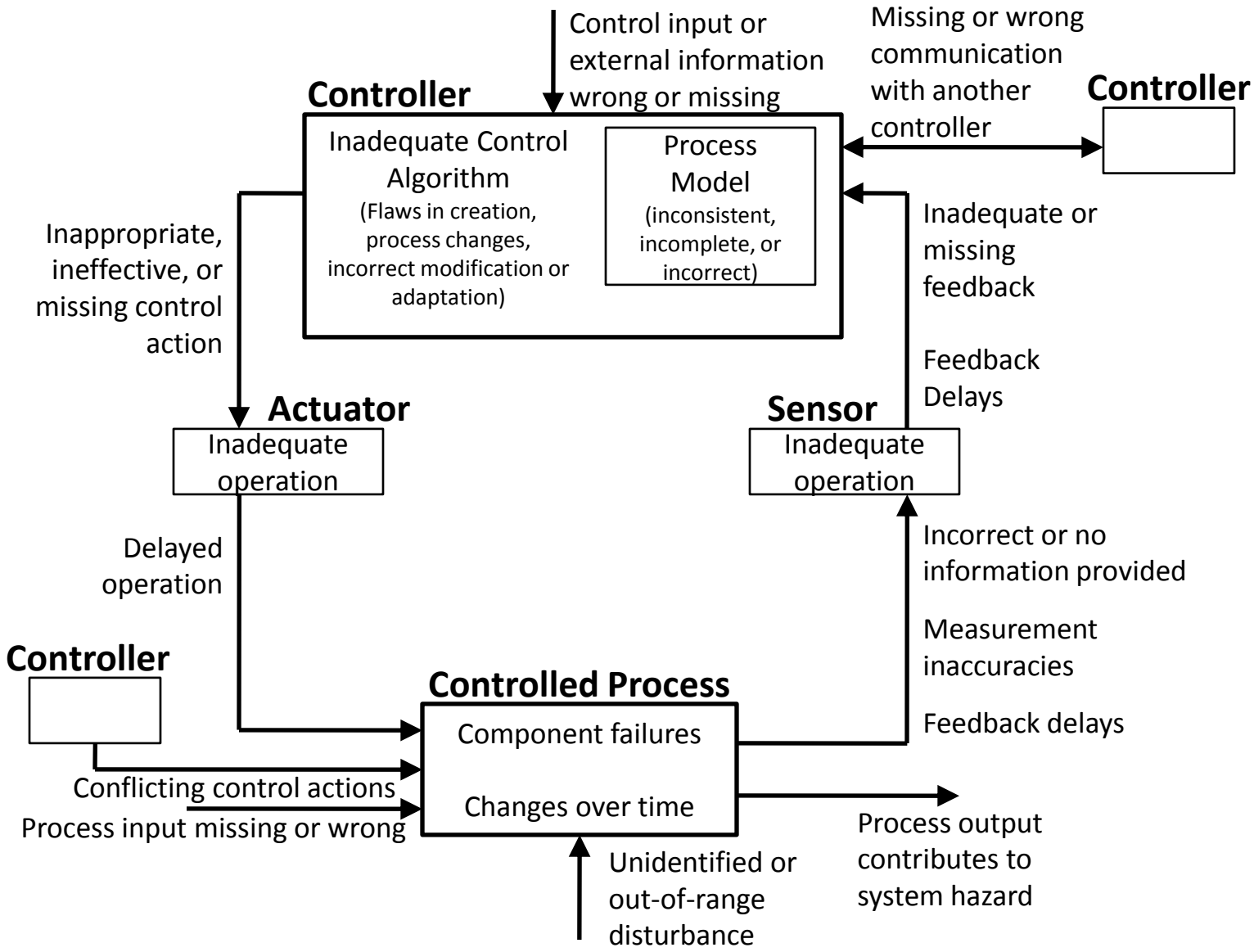
	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Action (Role)				

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?

Step 2: STPA Control Flaws



Simple STPA Exercise

a new in-trail procedure
for trans-oceanic flights

STPA Exercise

- Identify accidents and hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Example System: Aviation

Accident (Loss): ?

Accident

- Definition: 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**

- Examples:

Accident	Hazard
Satellite becomes lost or unrecoverable	Satellite maneuvers out of orbit
People die from exposure to toxic chemicals	Toxic chemicals are released into the atmosphere
People die from radiation sickness	Nuclear power plant releases radioactive materials
People die from food poisoning	Food products containing pathogens are sold

Example System: Aviation

Accident (Loss): Two aircraft collide

STPA Exercise

- Identify accidents and hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Accident (Loss): Two aircraft collide

Hazard: ?

Hazard

- Definition: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).
- Something we can ***control***
- Examples:

Accident	Hazard
Satellite becomes lost or unrecoverable	Satellite maneuvers out of orbit
People die from exposure to toxic chemicals	Toxic chemicals are released into the atmosphere
People die from radiation sickness	Nuclear power plant releases radioactive materials
People die from food poisoning	Food products containing pathogens are sold

Accident (Loss): Aircraft crashes

Hazard: Two aircraft violate minimum separation

Identifying Accidents and Hazards

- System-level Accident (loss)
  - Two aircraft collide
  - Aircraft crashes into terrain / ocean
- System-level Hazards
  - Two aircraft violate minimum separation
  - Aircraft enters unsafe atmospheric region
  - Aircraft enters uncontrolled state
  - Aircraft enters unsafe attitude
  - Aircraft enters prohibited area

Aviation examples

System-level Accidents

- Accident A-1: Two aircraft collide
- Accident A-2: Aircraft collides with terrain or sea
- Accident A-3: Aircraft collides with another object during touchdown (or during takeoff)

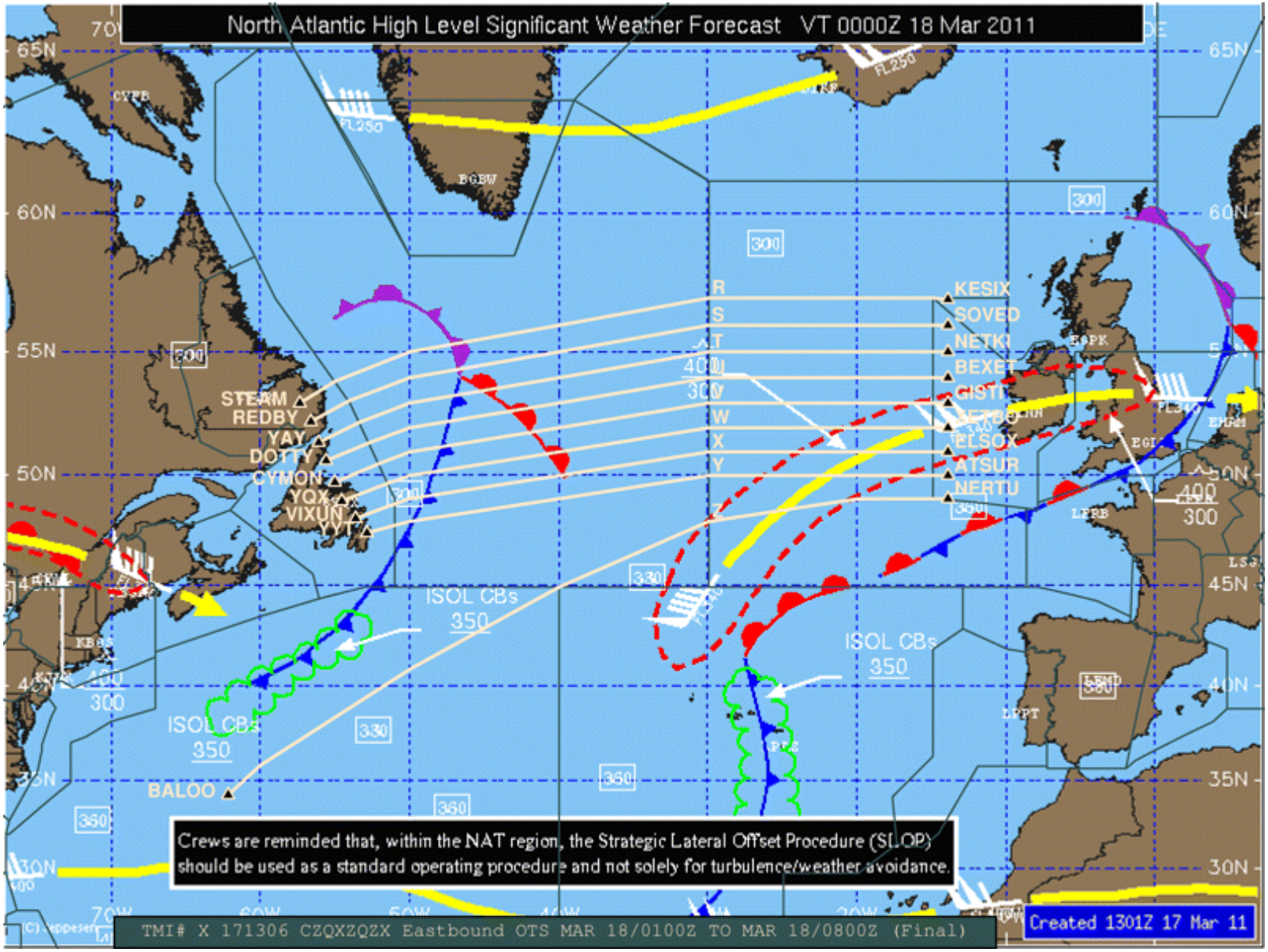
System-level Hazards

- Hazard H-1: a pair of controlled aircraft violate minimum separation standards
- Hazard H-2: aircraft enters unsafe atmospheric region
- Hazard H-3: aircraft enters uncontrolled state
- Hazard H-4: aircraft enters unsafe attitude (excessive turbulence or pitch/roll/yaw that causes passenger injury but not necessarily aircraft loss)
- Hazard H-5: aircraft enters a prohibited area

STPA Exercise

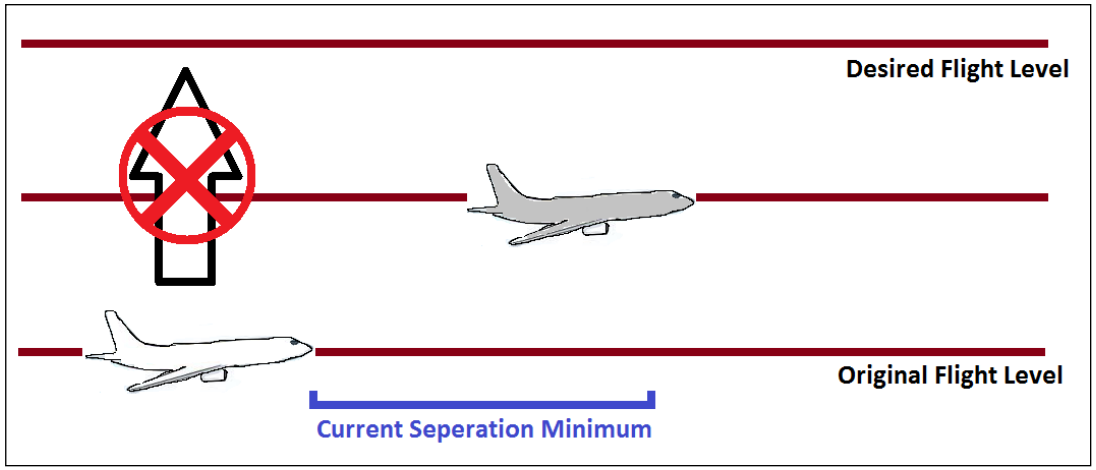
- ✓ Identify accidents and hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

North Atlantic Tracks



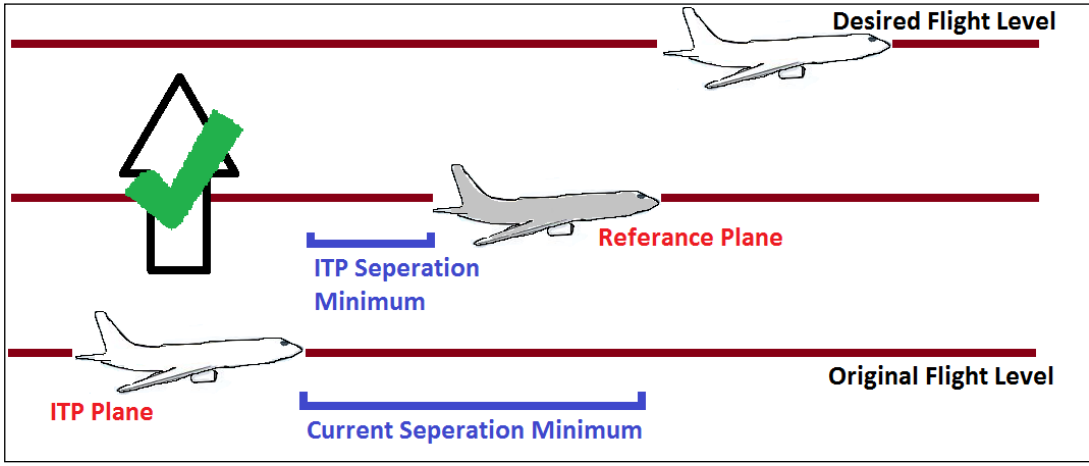
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



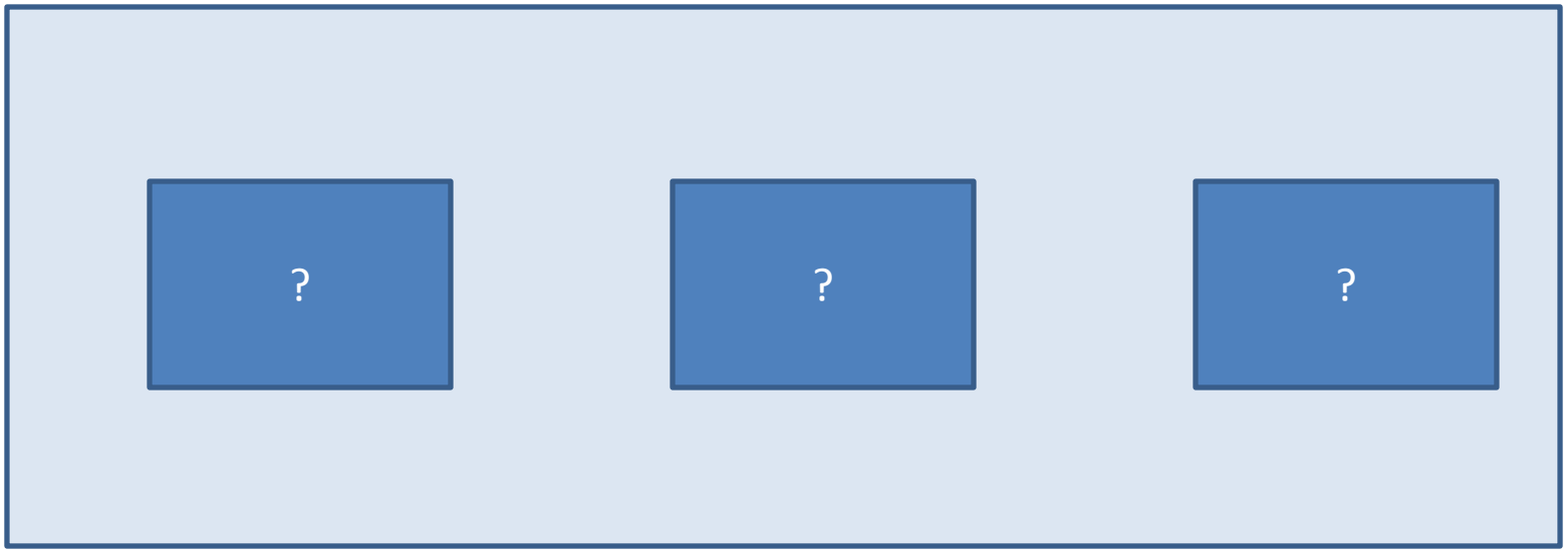
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



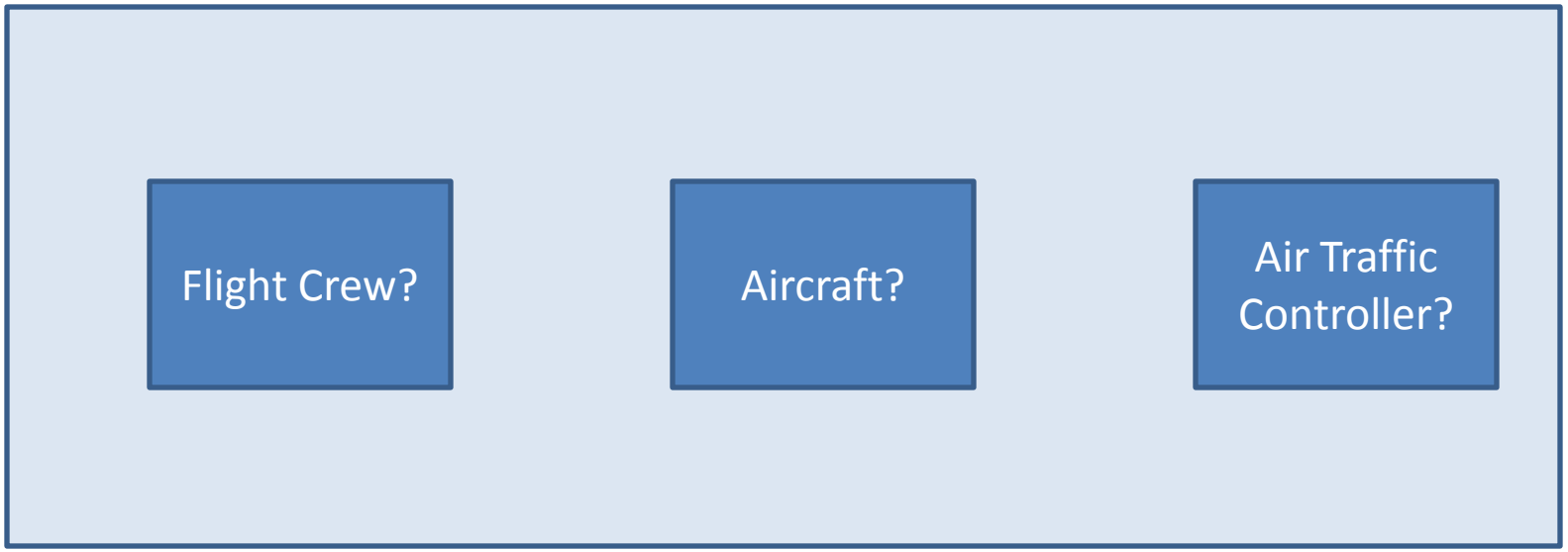
STPA Analysis

- High-level (simple) Control Structure
  - Main components and controllers?



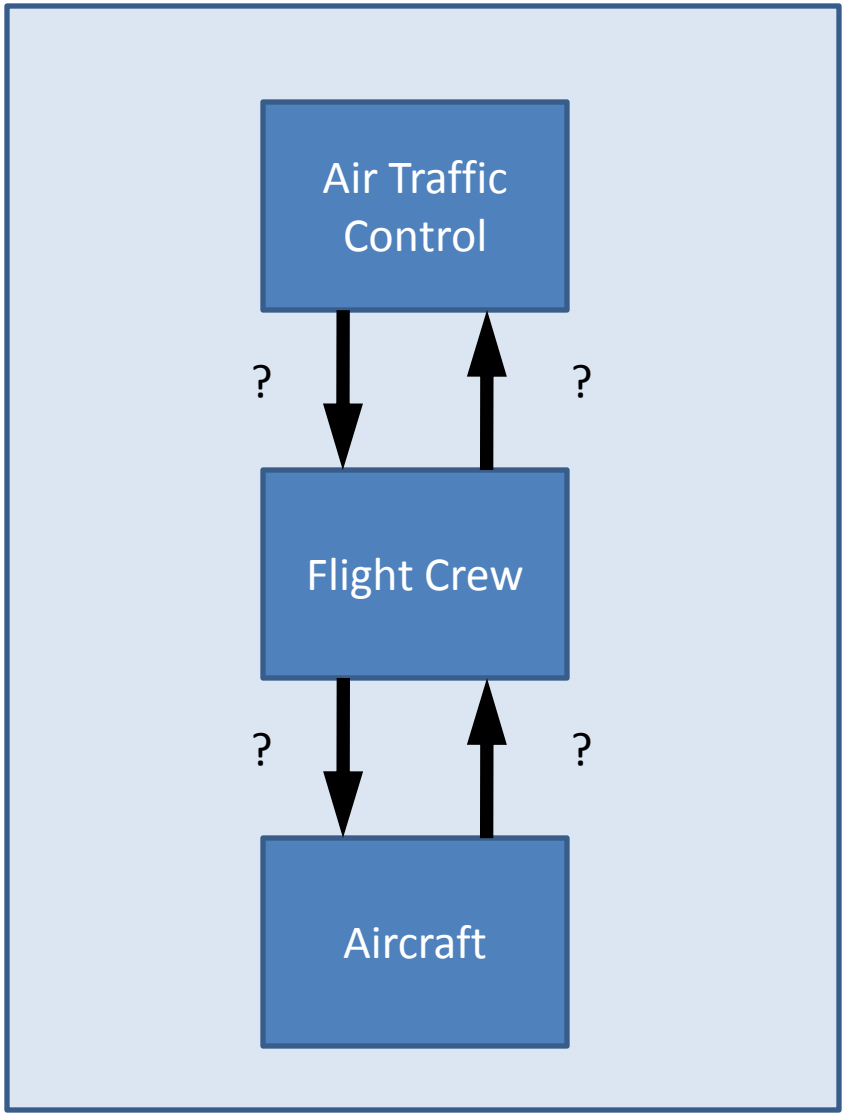
STPA Analysis

- High-level (simple) Control Structure
  - Who controls who?



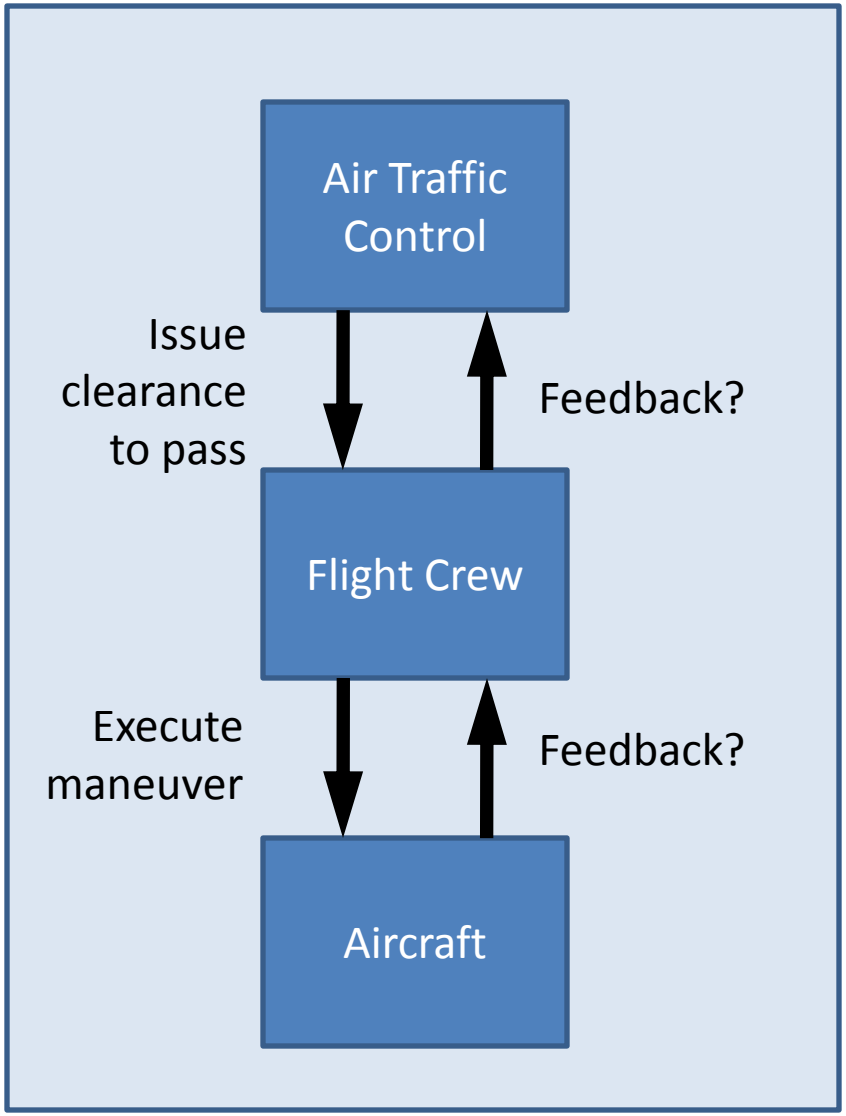
STPA Analysis

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



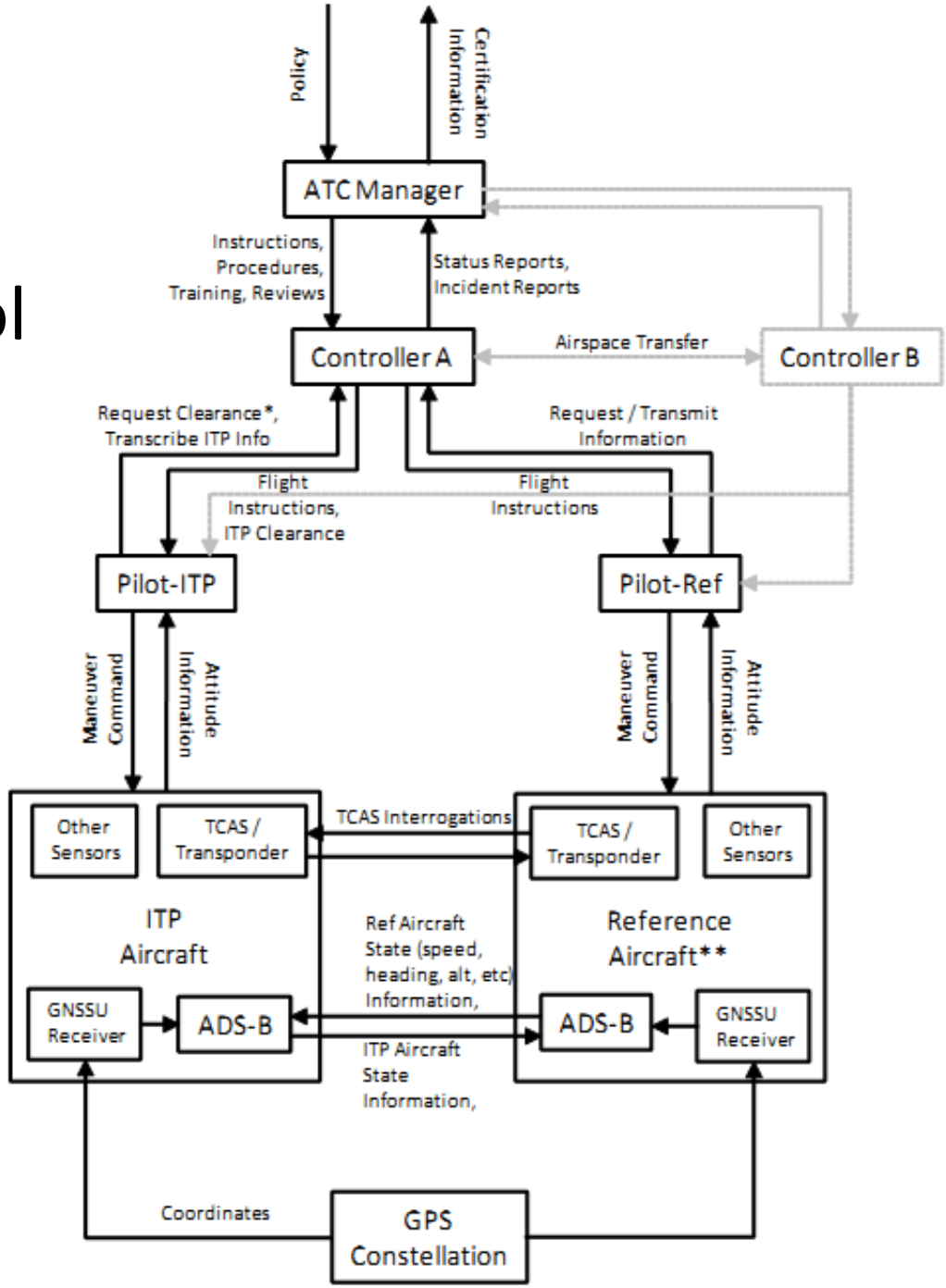
STPA Analysis

- High-level (simple) Control Structure

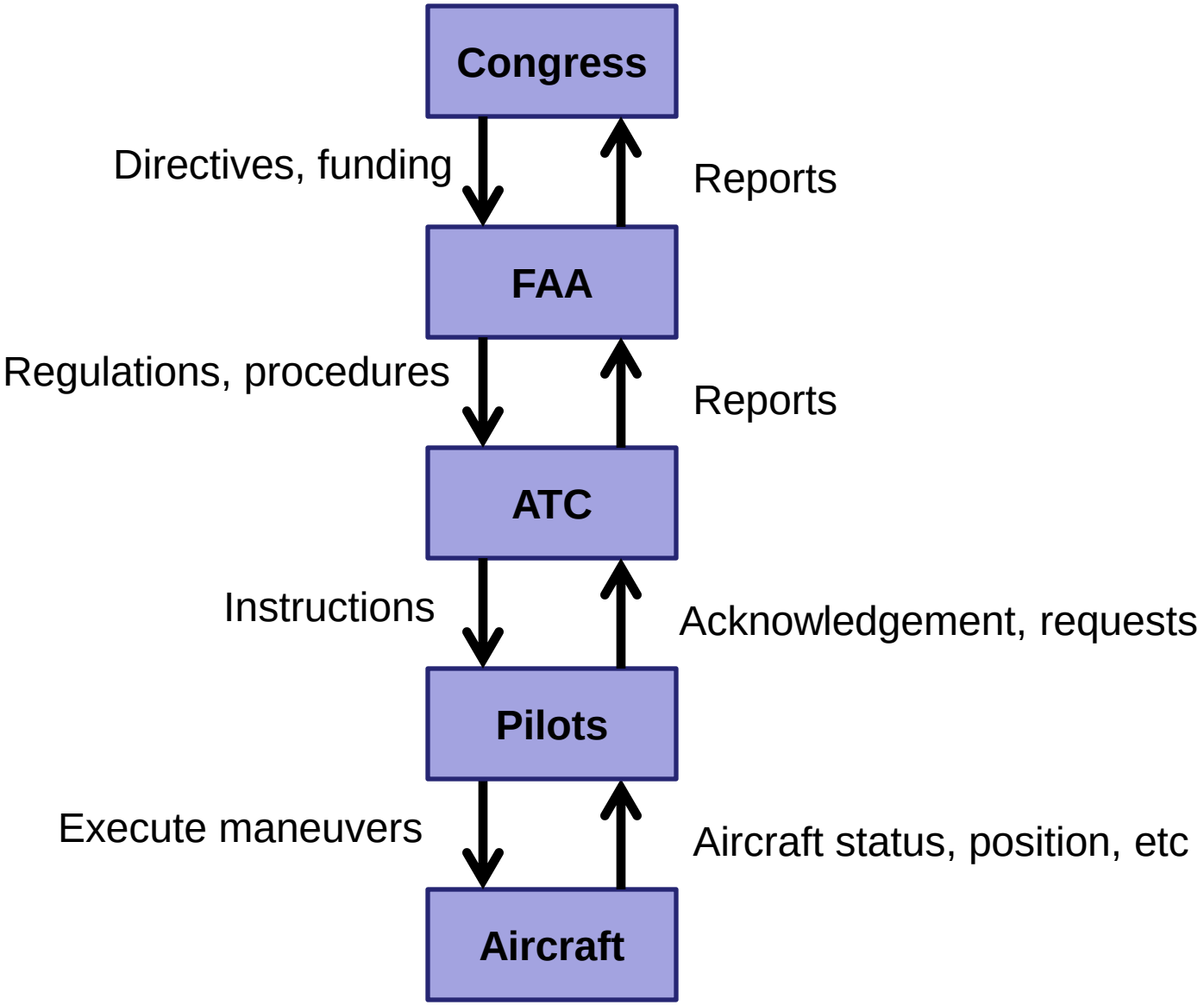


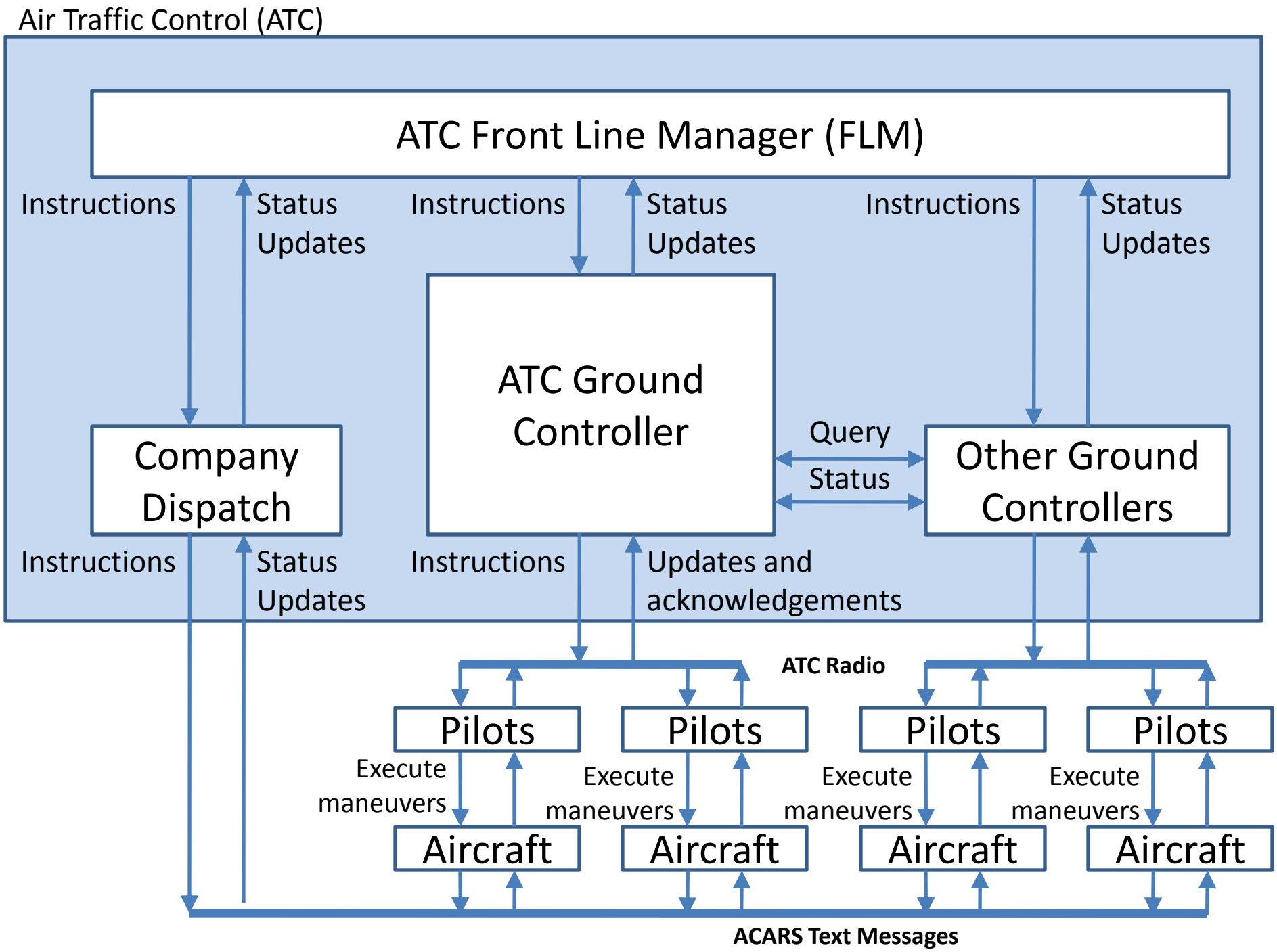
STPA Analysis

- More complex control structure

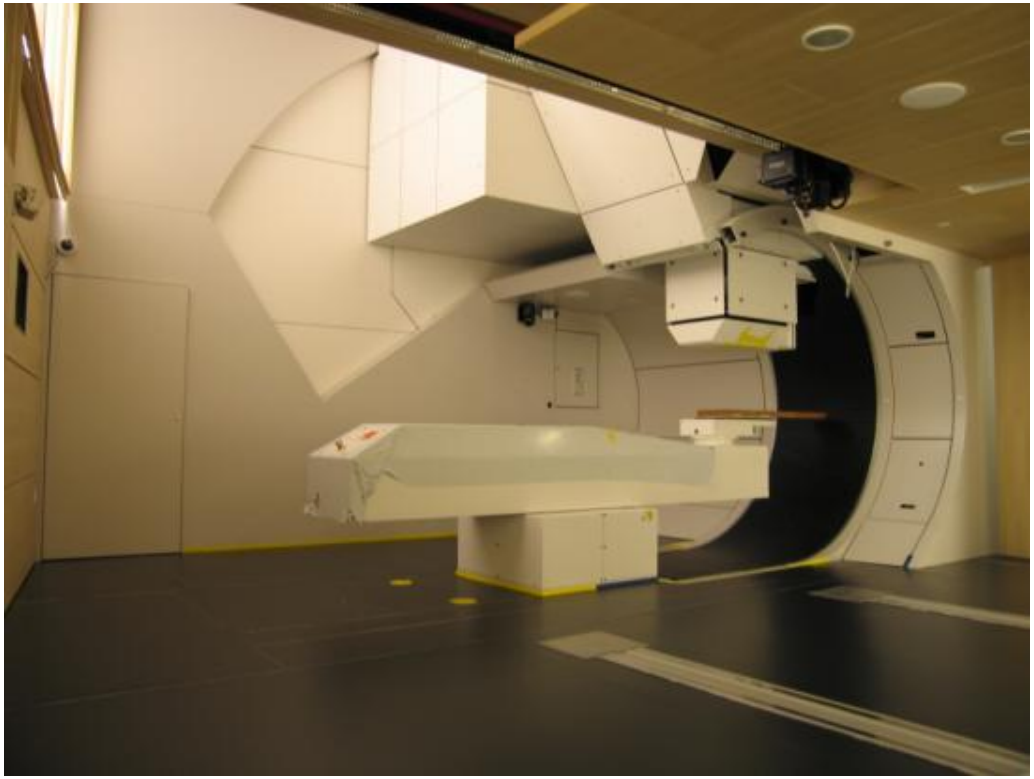


Example High-level control structure




Air Traffic Control (ATC)
ATC Front Line Manager (FLM)
Instructions
Status Updates
Instructions
Status Updates
Instructions
Status Updates
ATC Ground Controller
Company Dispatch
Query
Status
Other Ground Controllers
Instructions
Status Updates
Instructions
Updates and acknowledgements
ATC Radio
Pilots
Pilots
Pilots
Pilots
Execute maneuvers
Execute maneuvers
Execute maneuvers
Execute maneuvers
Aircraft
Aircraft
Aircraft
Aircraft
ACARS Text Messages

Proton Therapy Machine
High-level Control Structure



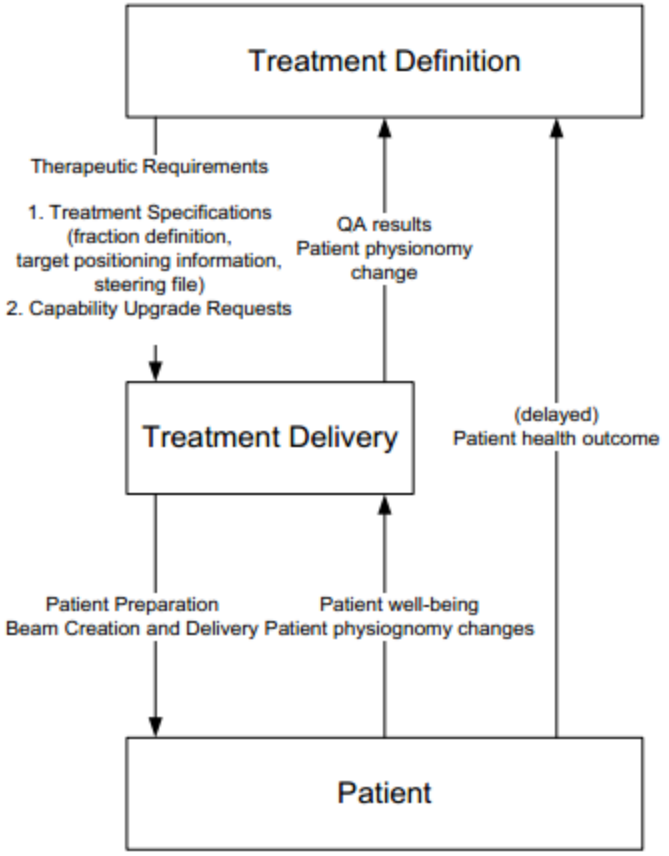


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Proton Therapy Machine Control Structure

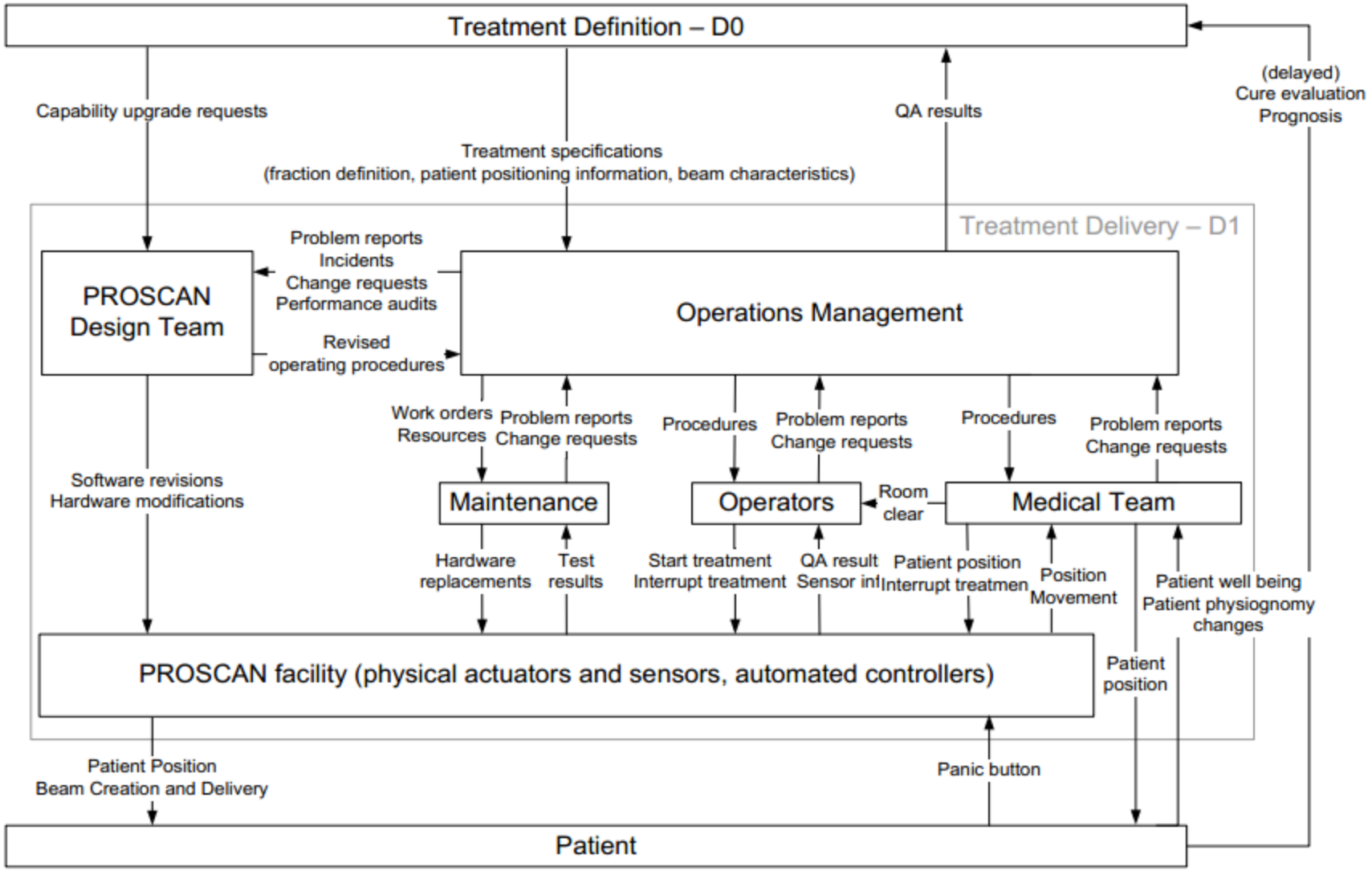
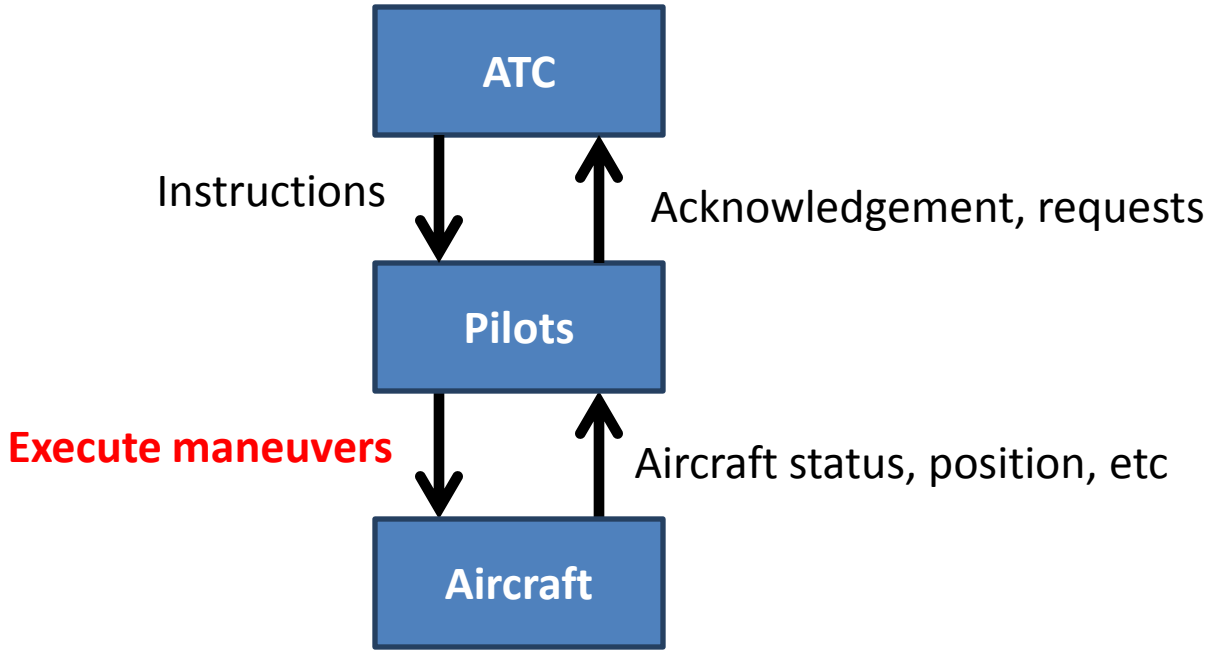


Figure 13 - Zooming into the Treatment Delivery group (D1)

STPA Exercise

- ✓ Identify accidents and hazards
- ✓ Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Identify Unsafe Control Actions



Flight Crew Action (Role)	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Execute Passing Maneuver	Pilot does not execute maneuver once it is approved			

STPA Analysis: Identify Unsafe Control Actions

Flight Crew Action (Role)	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Execute passing maneuver	Pilot does not execute maneuver Aircraft remains In-Trail	Perform ITP when ITP criteria are not met or request has been refused Pilot instructs incorrect attitude, e.g. throttle and/or pitch	Crew starts maneuver late after having re-verified ITP criteria Pilot throttles before achieving necessary altitude	Crew does not complete entire maneuver e.g. Aircraft does not achieve necessary altitude or speed

STPA Analysis: Identify UCAs

Flight Crew Action (Role)	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Read Back Clearance	Crew does not read-back ITP clearance	Confirm clearance but clearance had not been granted	Reads back clearance in non-standard order	
Verify ITP Criteria to Confirm Validity of Clearance	Crew does not perform ITP criteria verification	Confirm clearance when criteria are not met	Verifies criteria late after clearance was initially granted or too early before maneuver is actually performed	
Perform ITP Maneuver	Pilot does not execute maneuver Aircraft remains In-Trail	Perform ITP when ITP criteria are not met or request has been refused Pilot instructs incorrect attitude, e.g. throttle and/or pitch	Crew starts maneuver late after having re-verified ITP criteria Pilot throttles before achieving necessary altitude	Crew does not complete entire maneuver e.g. Aircraft does not achieve necessary altitude or speed
Provide data to ATC & other aircraft	Does not communicate position & attitude information	Transmit unnecessary data or information Transmit incorrect data		

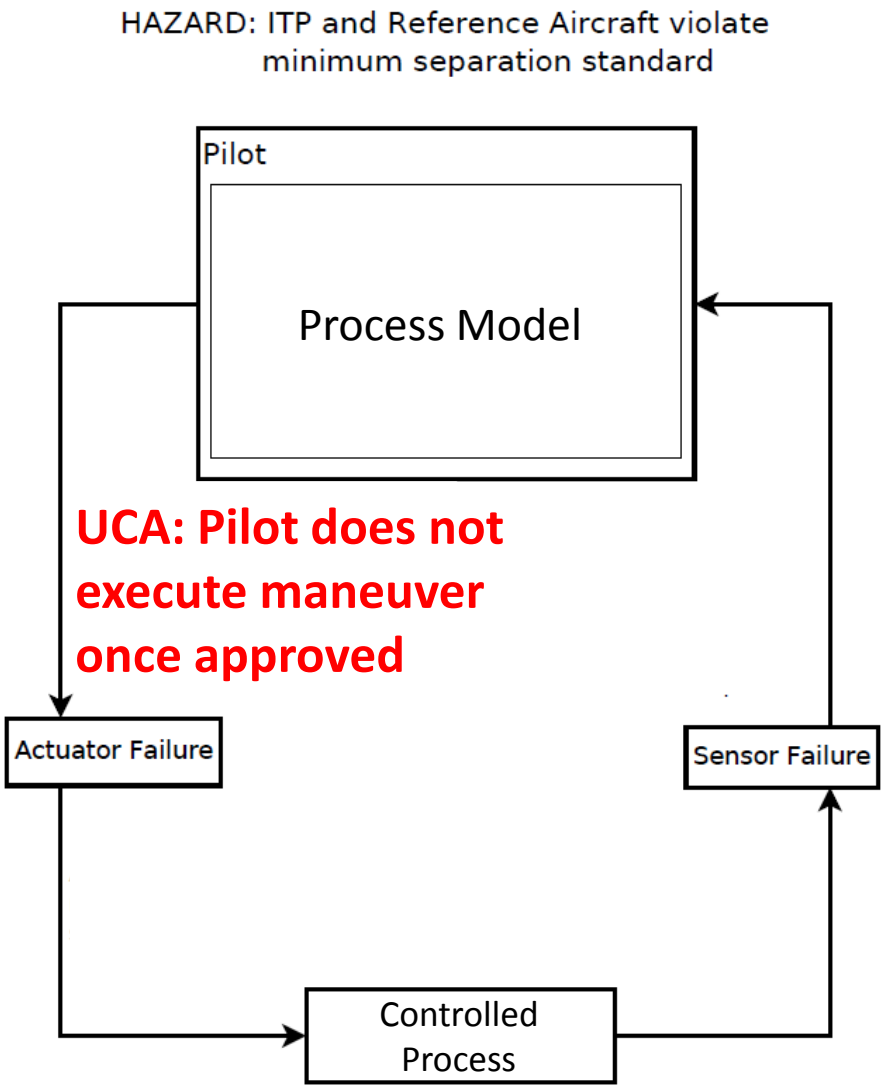
Defining Safety Constraints

Unsafe Control Action	Safety Constraint
Pilot does not execute maneuver once it is approved	Pilot must execute maneuver once it is approved
Pilot performs ITP when ITP criteria are not met or request has been refused	Pilot must not perform ITP when criteria are not met or request has been refused
Pilot starts maneuver late after having re-verified ITP criteria	Pilot must start maneuver within X minutes of re-verifying ITP criteria

STPA Exercise

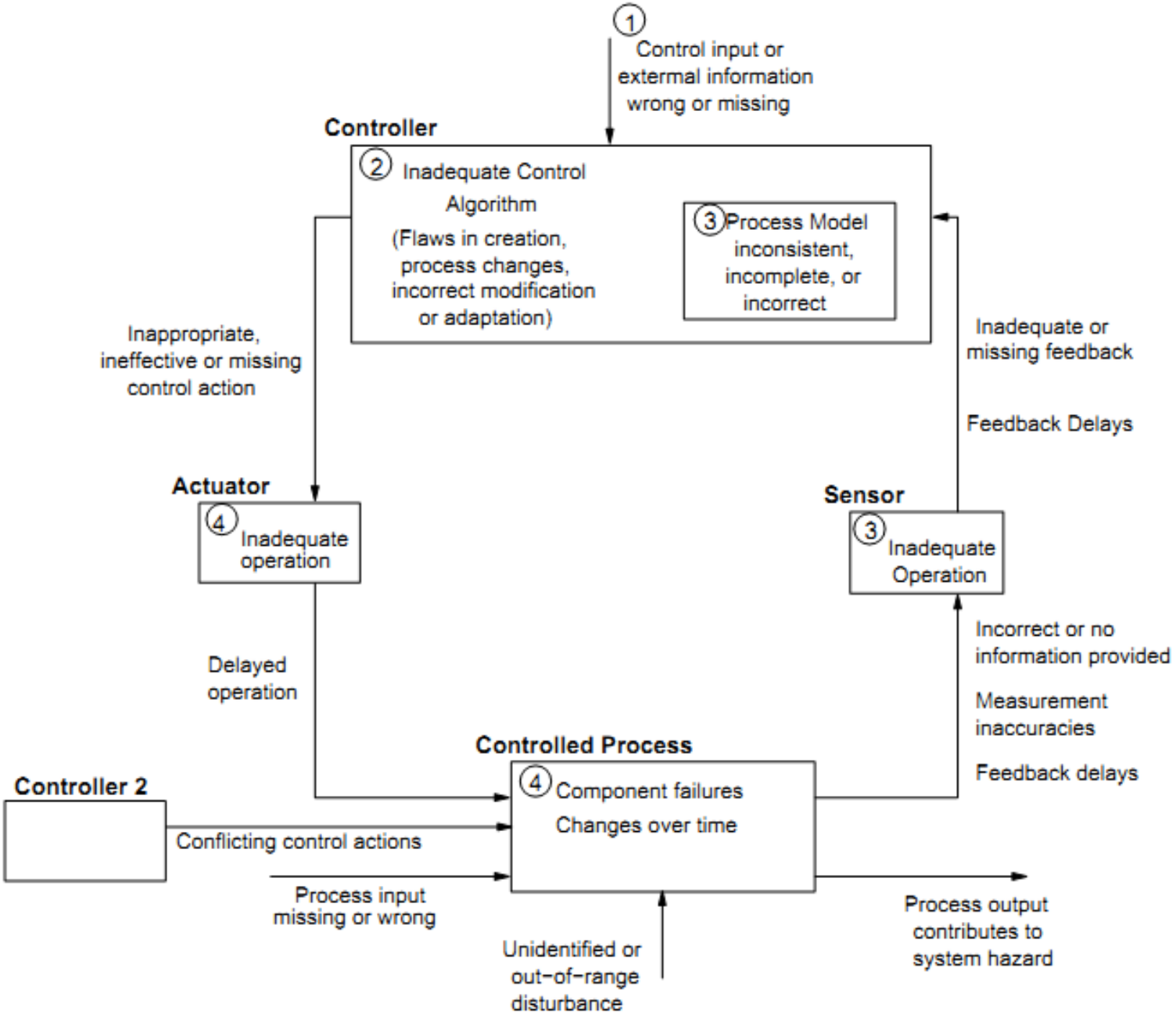
- ✓ Identify accidents and hazards
- ✓ Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- ✓ Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

STPA Analysis: Causal Factors

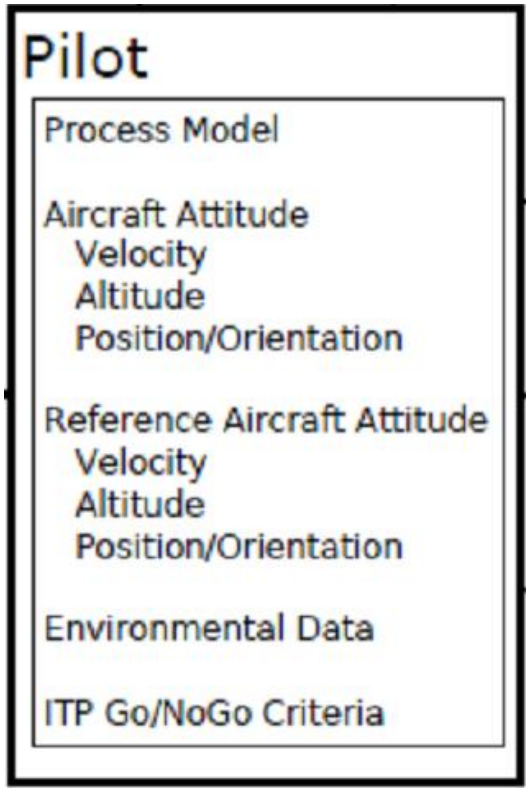


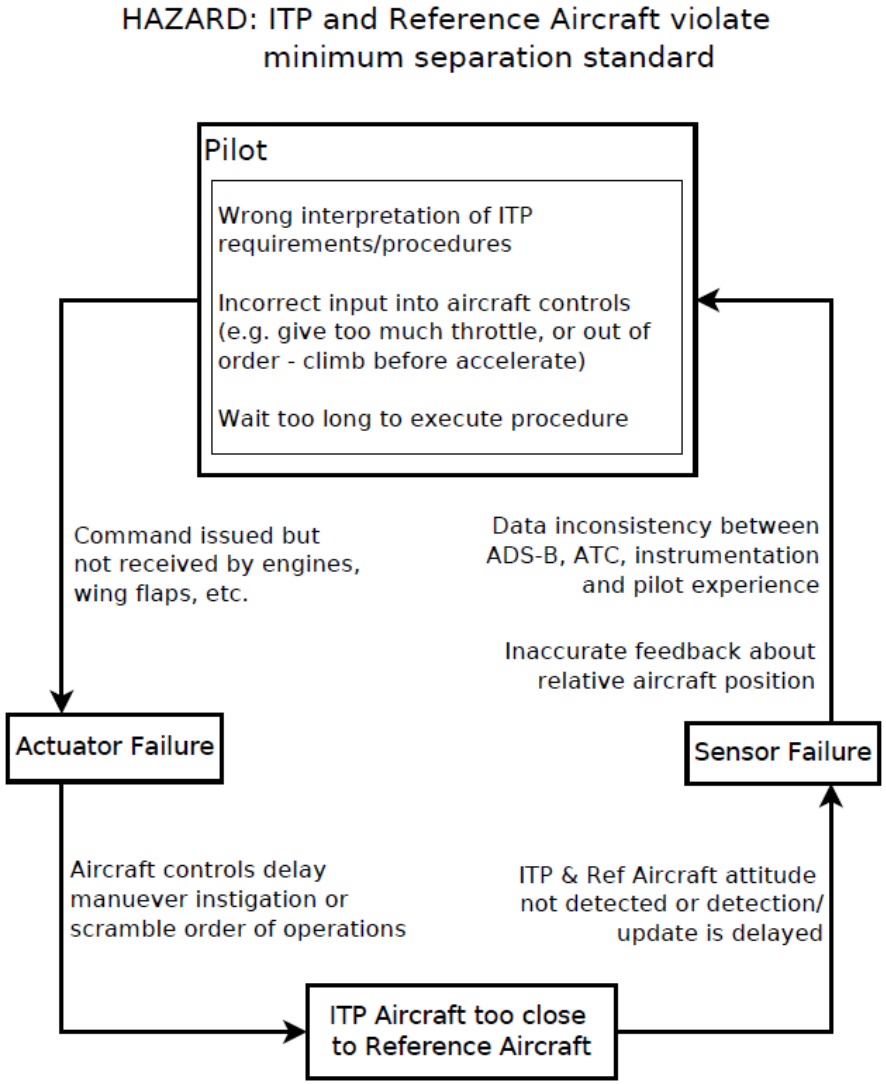
- How could this action be caused by:
  - Process model
  - Feedback
  - Sensors
  - Etc?

Hint: Causal Factors

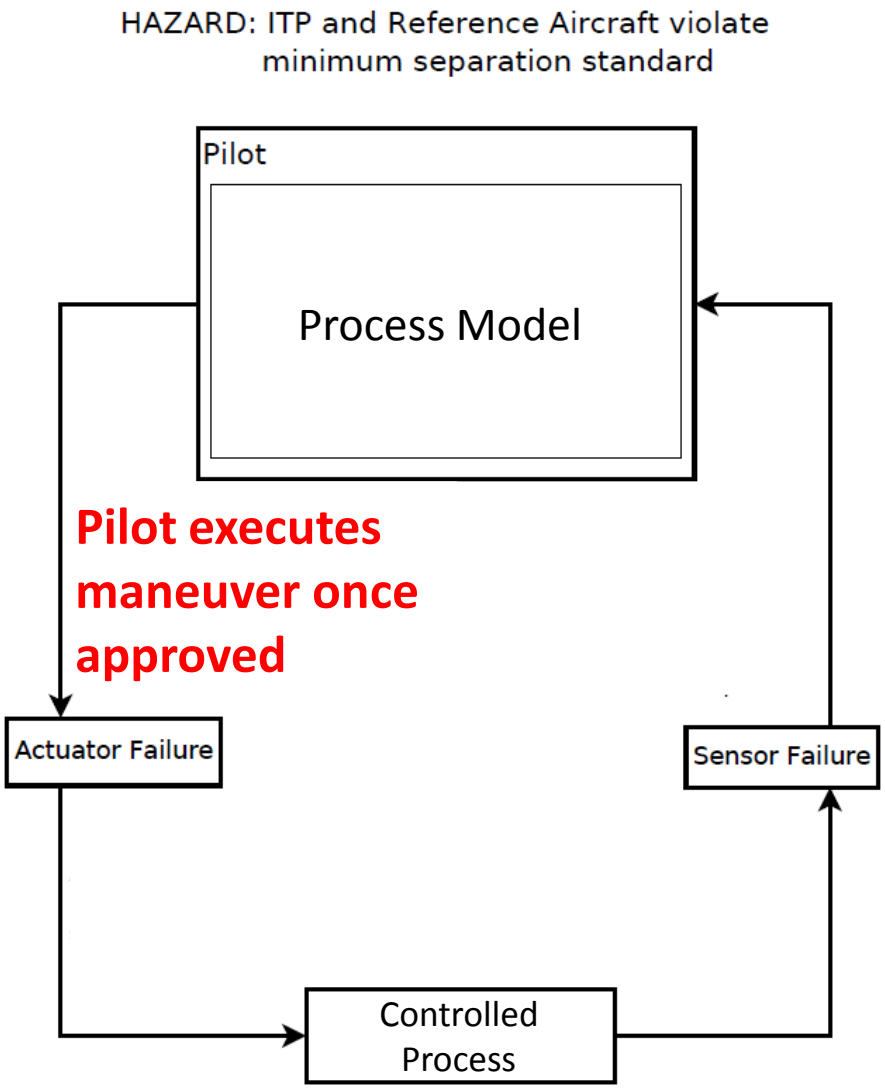


STPA Analysis: Causal Factors





STPA Analysis: Causal Factors

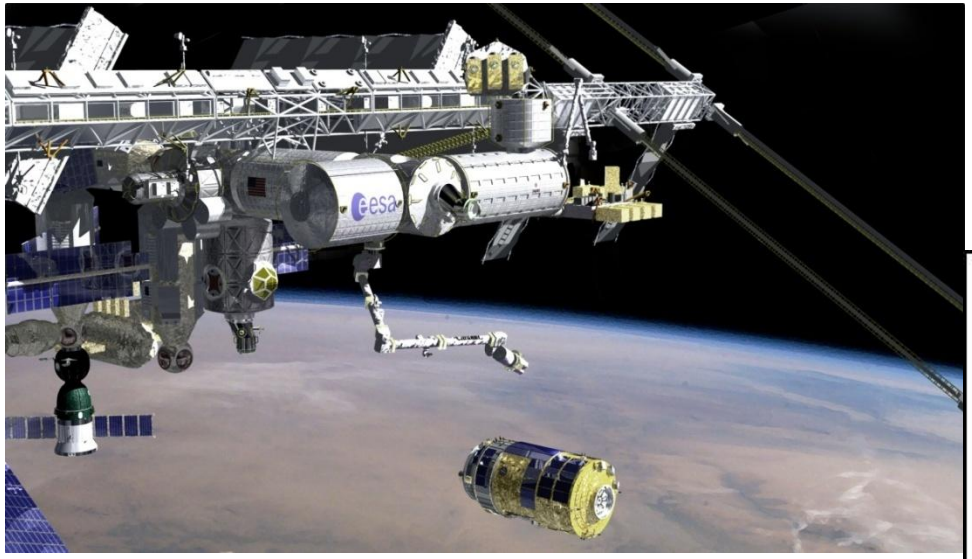


Safety Constraint: Maneuver must be executed once approved

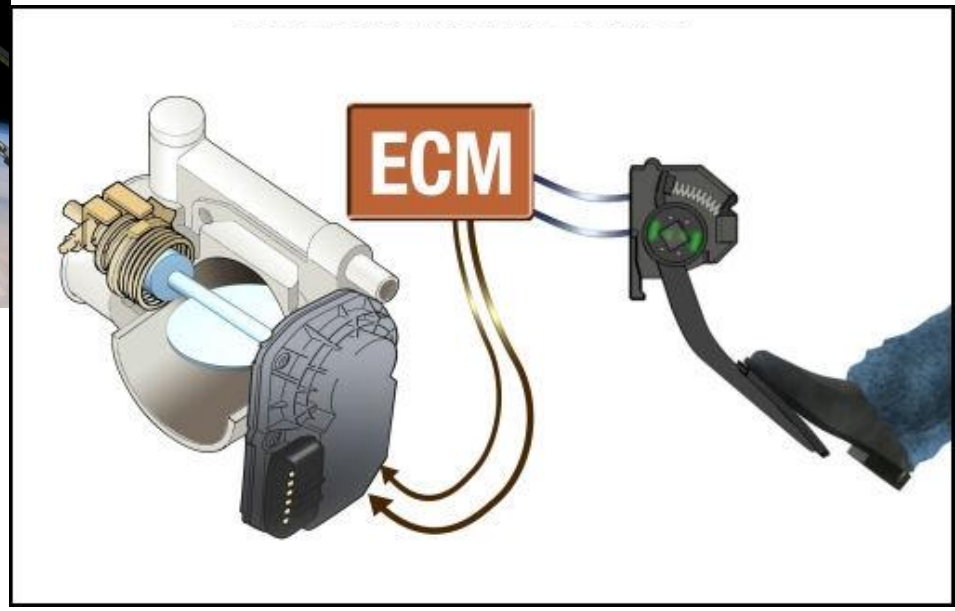
- Safety Constraint: Maneuver must be executed once approved
- How else could the Safety Constraint be violated?

STPA Group Exercise

Choose a system to analyze:



International Space Station unmanned cargo vehicle



Electronic Throttle Control

STPA Group Exercise

- Identify accidents and hazards (**15 min**)
- Draw the control structure (**15 min**)
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (**15 min**)
  - Control Table:
    Not given, Unsafe action provided, Wrong timing, Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors (**15 min**)
  - Identify controller process models
  - Analyze controller, control path, feedback path, process