STAMP Experienced Users Tutorial

John Thomas
Blandine Antoine
Cody Fleming
Melissa Spencer
Qi Hommes
Tak Ishimatsu
John Helferich

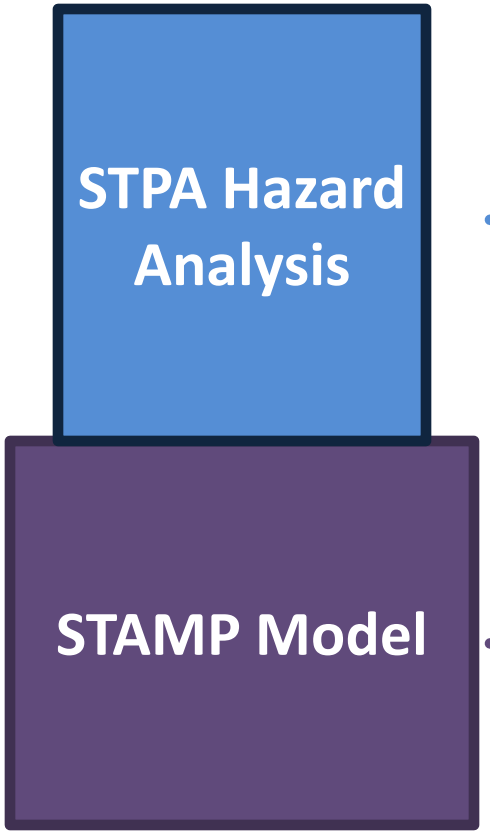
Systems approach to safety engineering (STAMP)

STAMP Model

- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not 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)

STPA
(System-Theoretic Process Analysis)

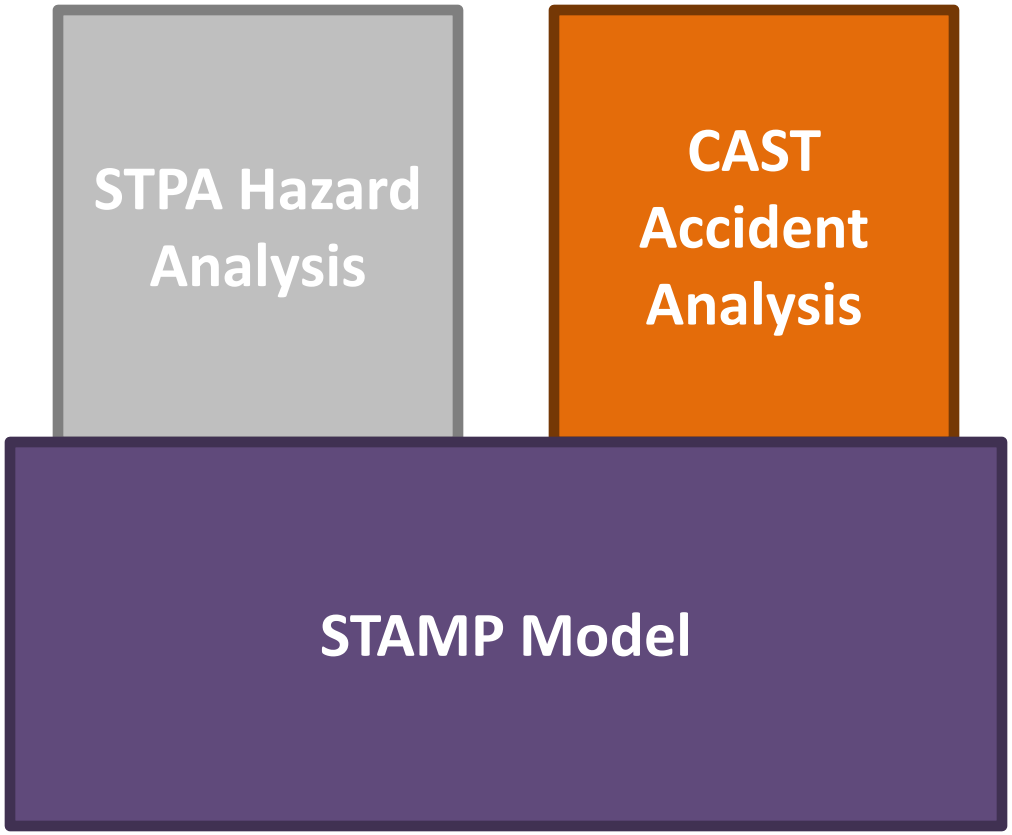


How do we find inadequate control in a system?

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)

Experienced Users Tutorial

- Morning session
  - STPA Hazard Analysis
  - Hands-on exercises
- Afternoon session
  - CAST Accident Analysis
  - Hands-on exercises

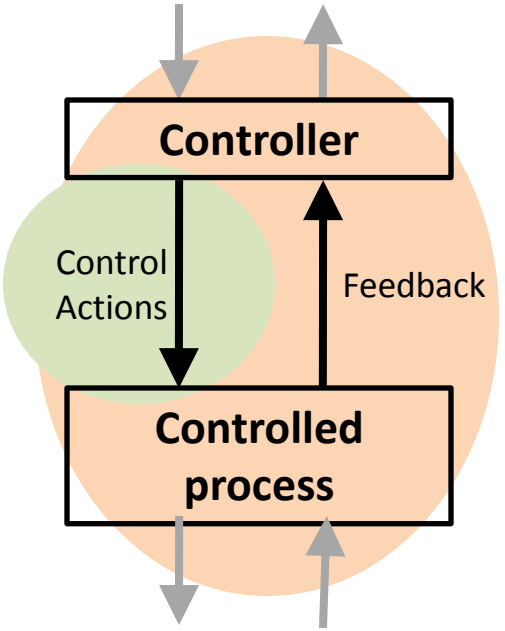
STPA Hazard Analysis

STPA
(System-Theoretic Process Analysis)

STPA Hazard Analysis

STAMP Model

- Identify the hazards
- Construct the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causes of unsafe control actions



(Leveson, 2011)

Step 1: Identify Unsafe Control Actions

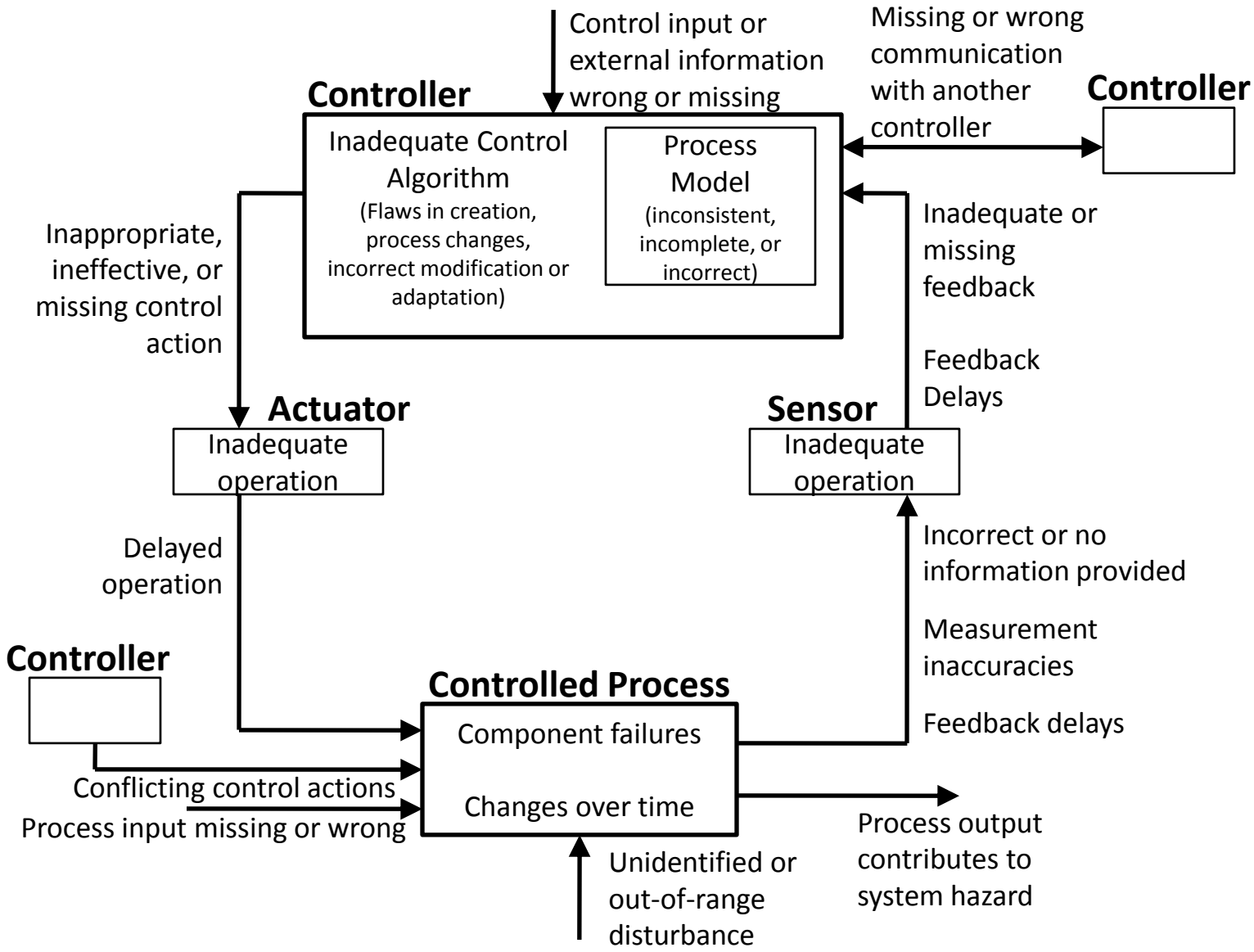
	Action required but not provided	Unsafe action provided	Incorrect Timing/ Order	Stopped Too Soon
Action (Role)				

Step 1: Identify Unsafe Control Actions

(a more rigorous method, more on this tomorrow)

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

Example System: Aviation

Accident (Loss): Aircraft crashes

STPA Exercise

- Identify 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

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 are exposed to toxic chemicals	Toxic chemicals are released into the atmosphere
People are irradiated	Nuclear power plant experiences nuclear meltdown
People are poisoned by food	Food products containing pathogens are sold

Accident (Loss): Aircraft crashes

Hazard: ?

Accident (Loss): Aircraft crashes

Hazard: Two aircraft violate minimum separation

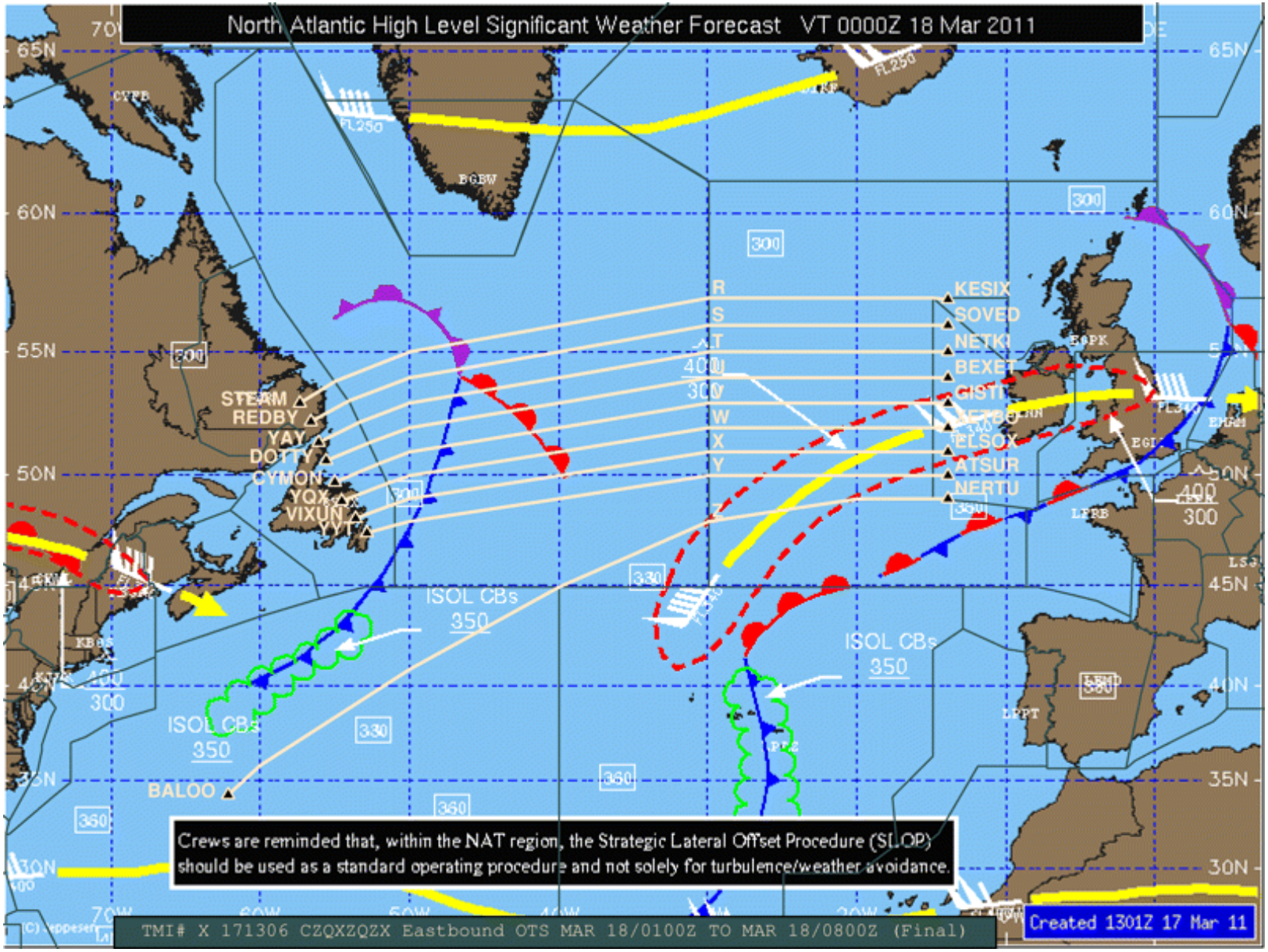
Identifying Hazards

- Loss (accident)
  - Death or Injury
- Hazards
  - Two aircraft violate minimum separation
  - Aircraft enters unsafe atmospheric region
  - Aircraft enters uncontrolled state
  - Aircraft enters unsafe attitude
  - Aircraft enters prohibited area

STPA Exercise

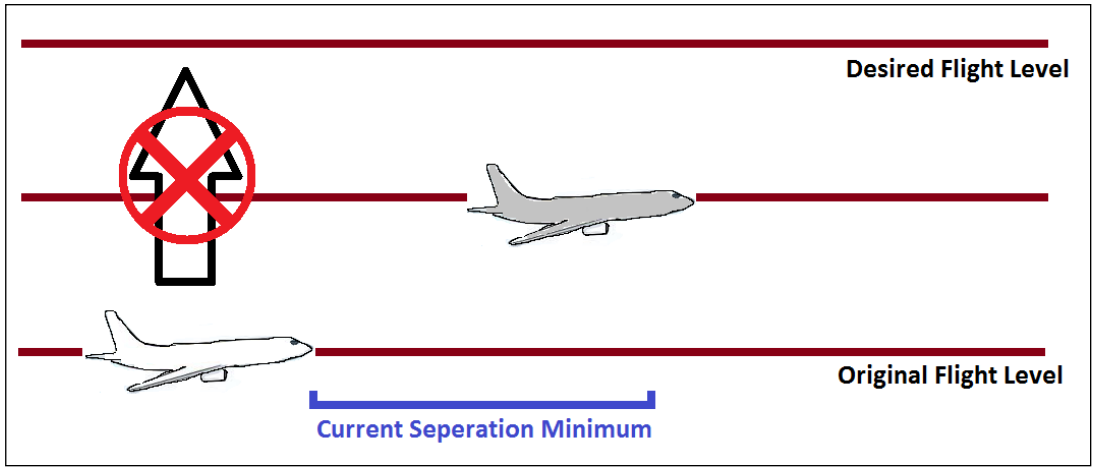
- Identify Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints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

North Atlantic Tracks



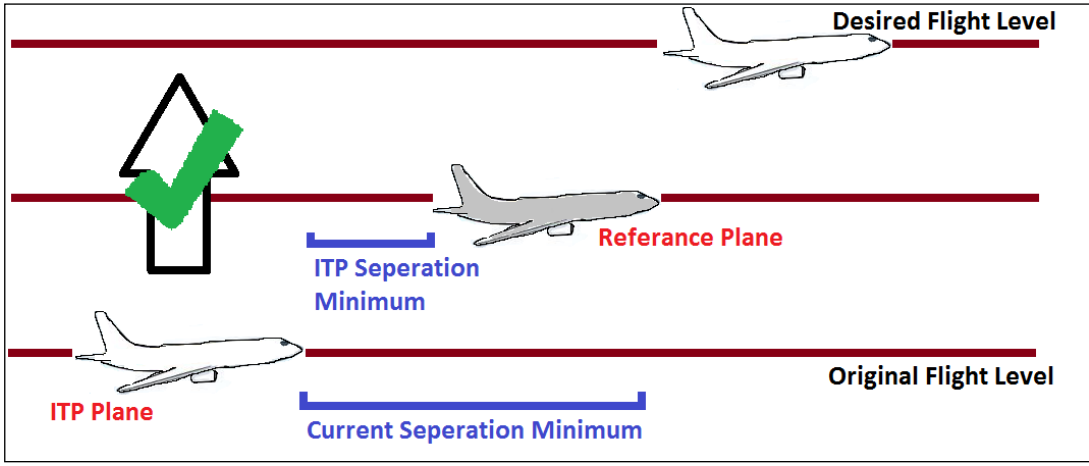
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



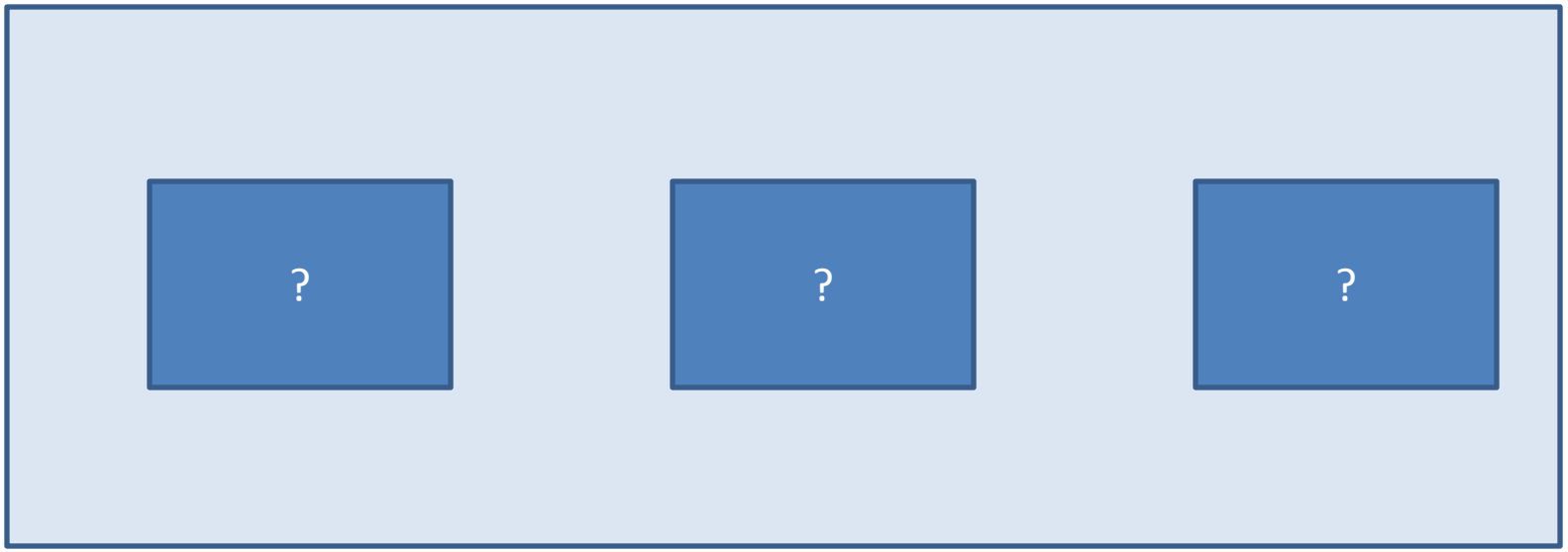
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



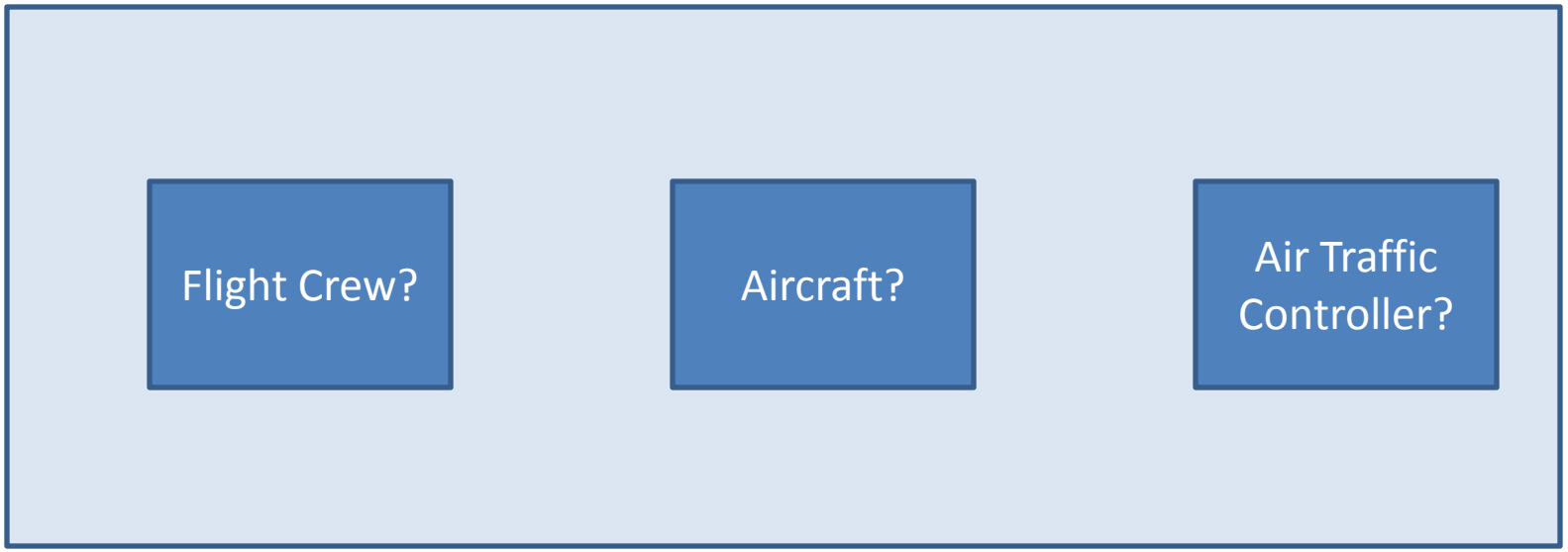
STPA Analysis

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



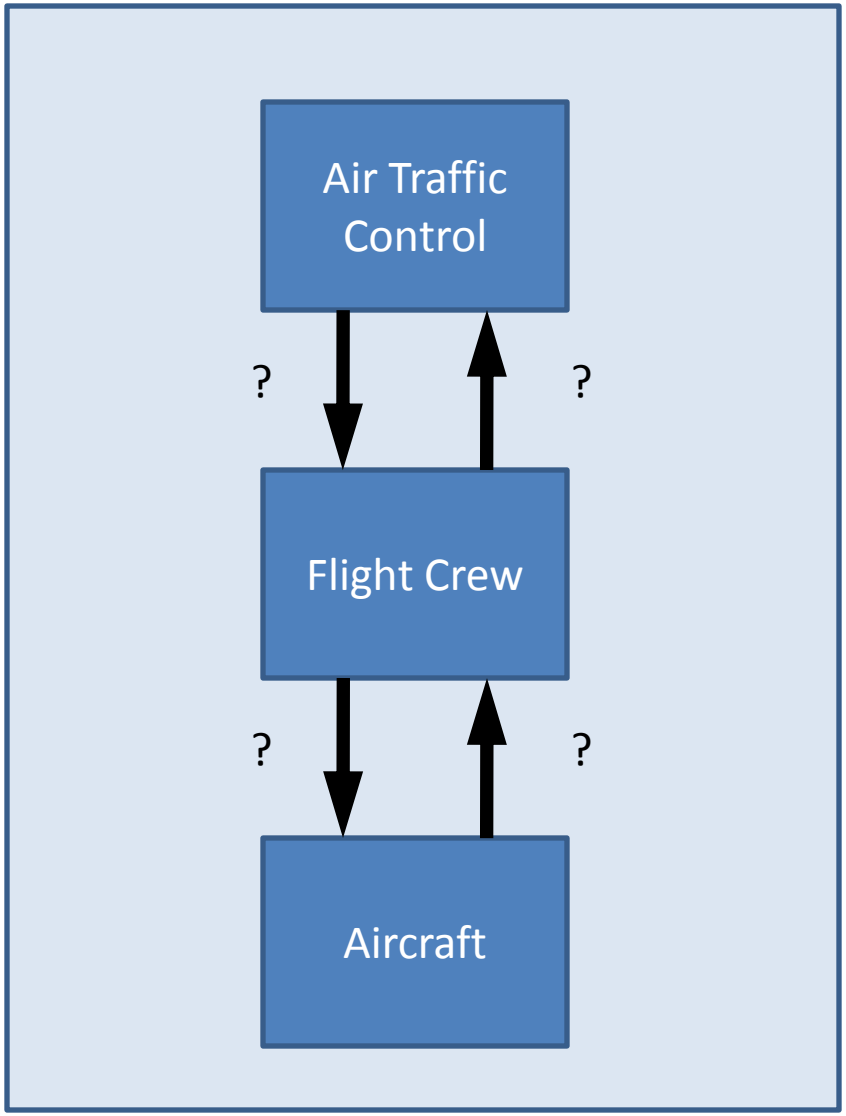
STPA Analysis

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



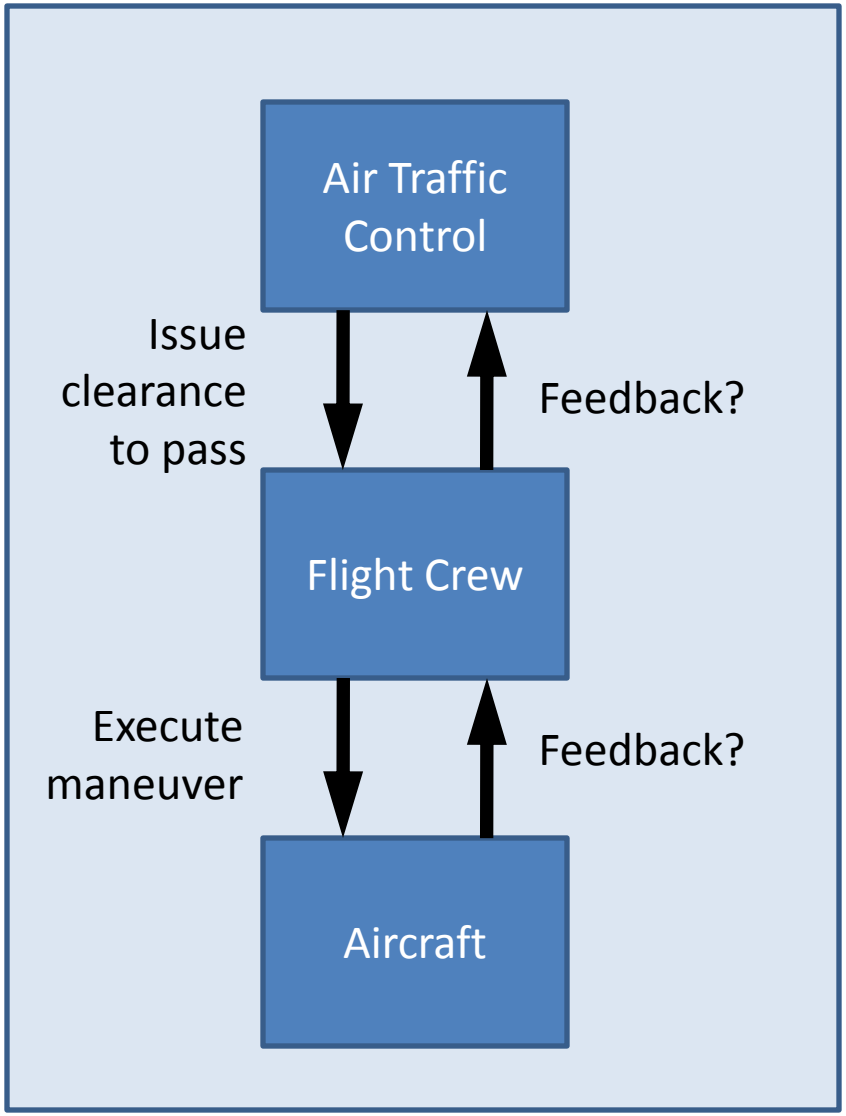
STPA Analysis

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



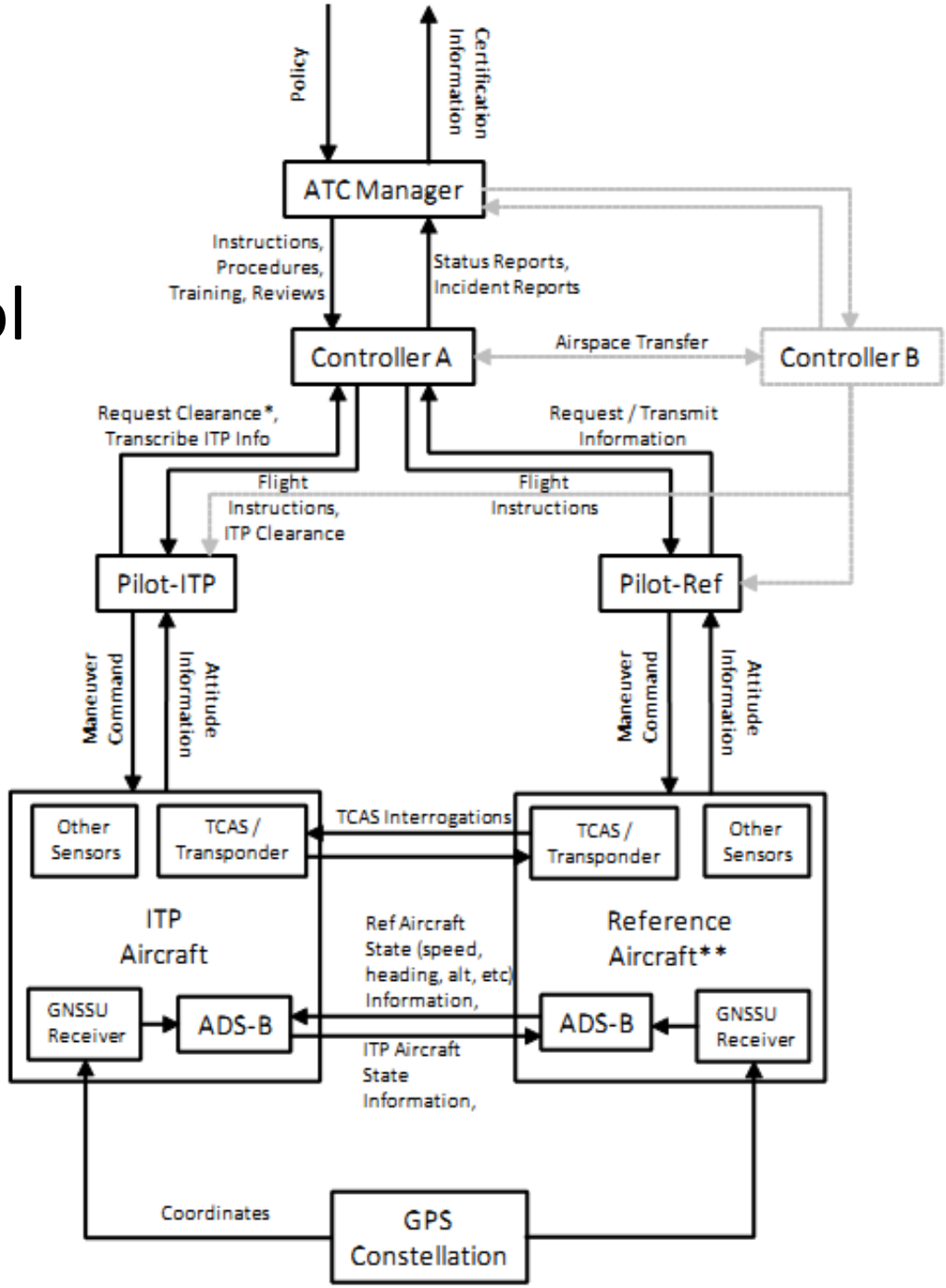
STPA Analysis

- High-level (simple) Control Structure



STPA Analysis

- More complex control structure



STPA Exercise

- Identify 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:
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 critera 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	Crew starts maneuver late after having re-verified ITP critera 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		

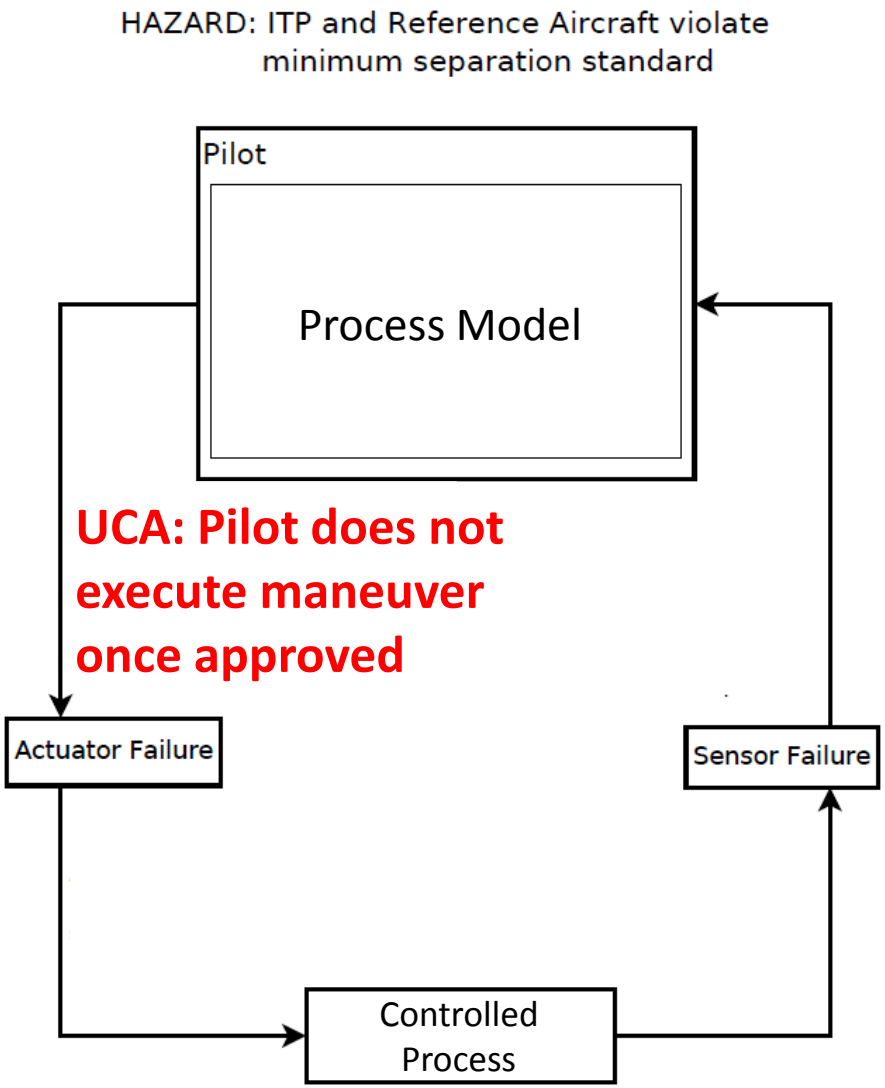
Defining Safety Constraints

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 critera	Pilot must start maneuver within X minutes of re-verifying ITP criteria

STPA Exercise

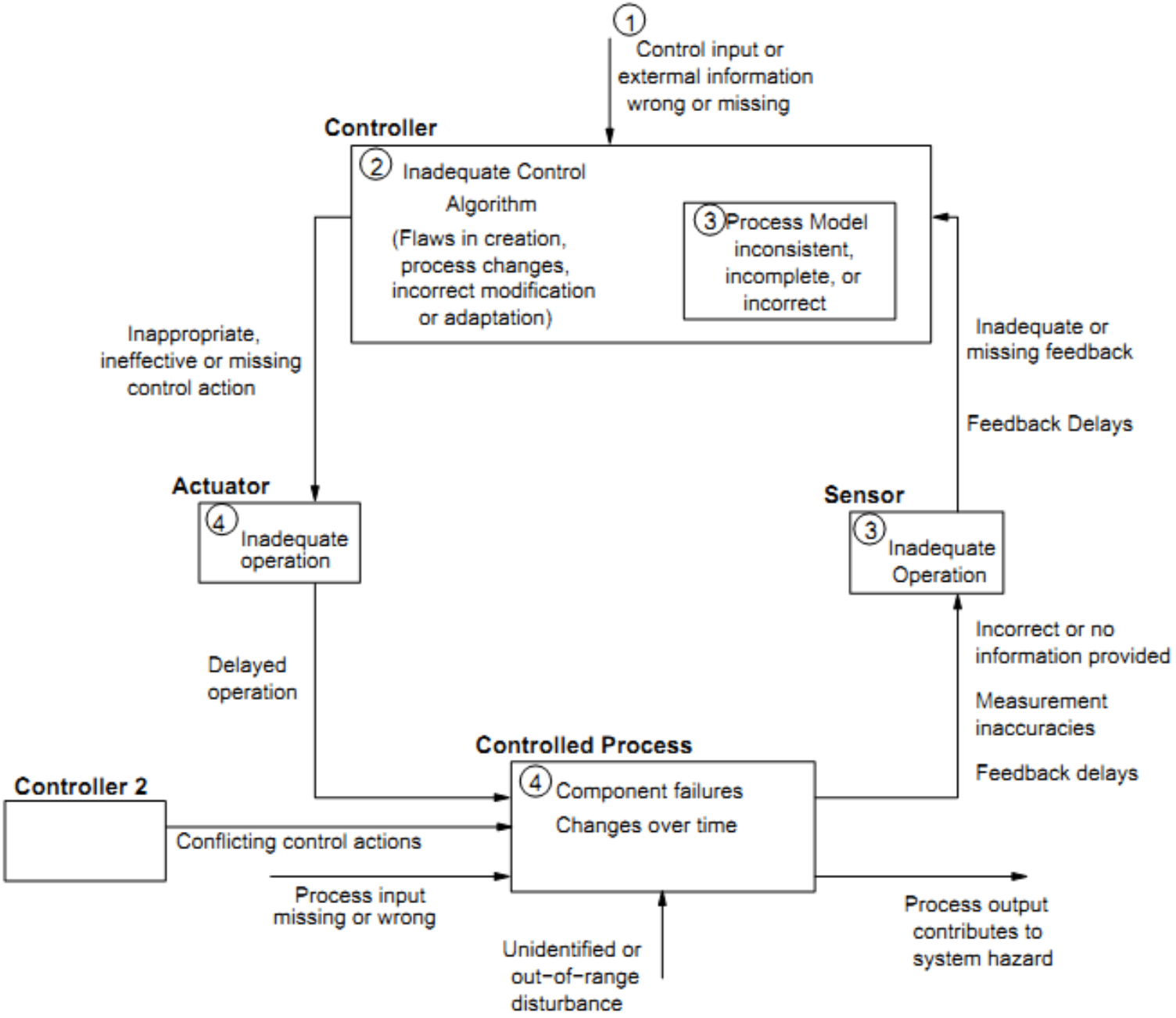
- Identify Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints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

STPA Analysis: Causal Factors

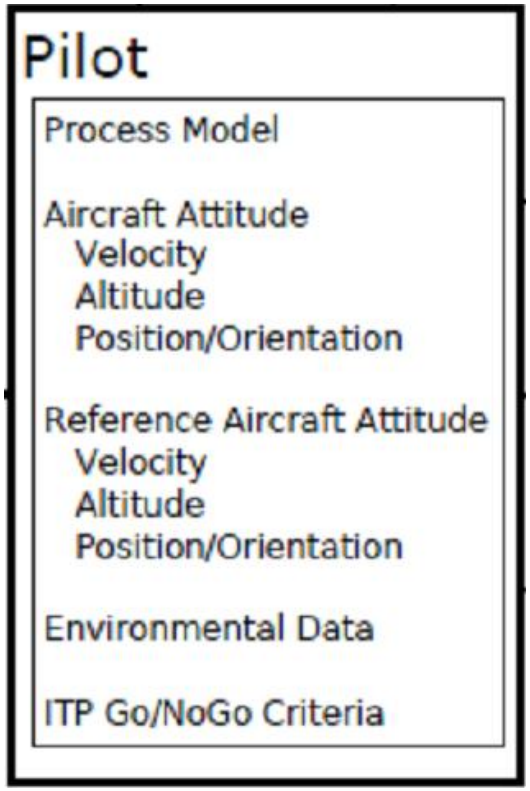


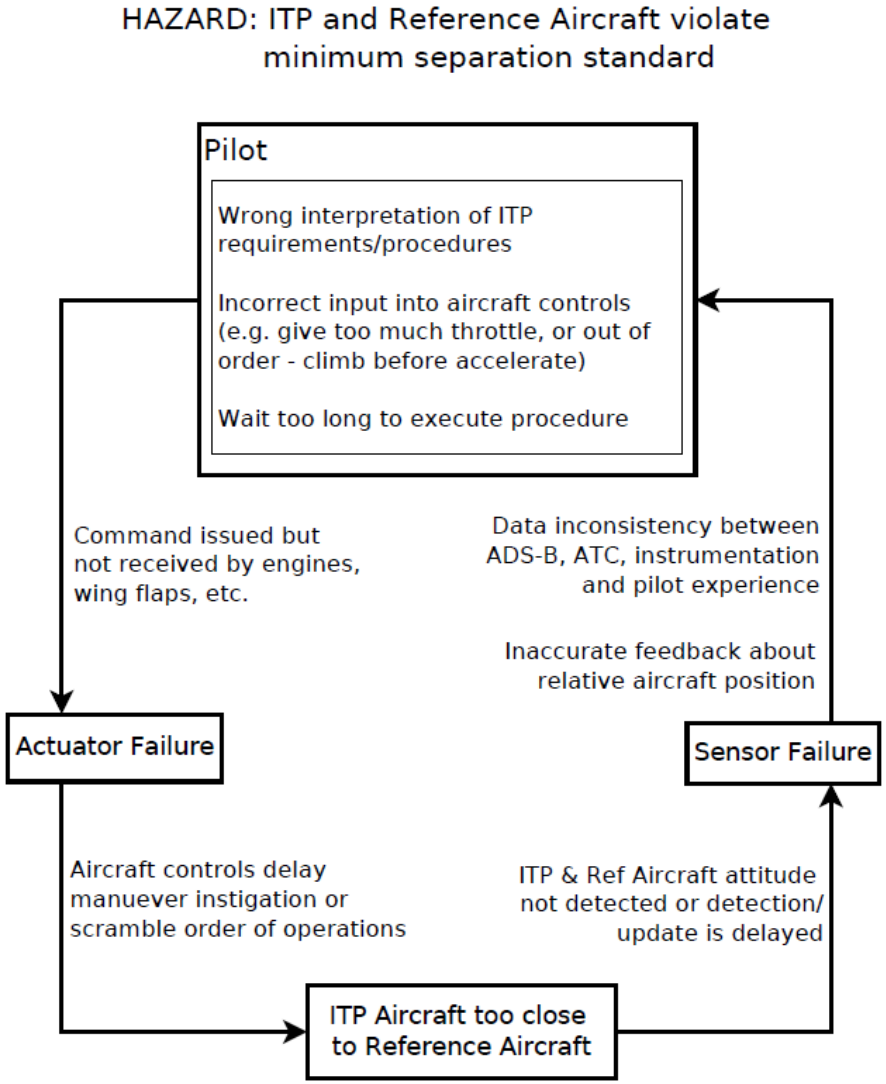
- How could this action be caused by:
  - Process model
  - Feedback
  - Sensors
  - Etc?

Hint: Causal Factors



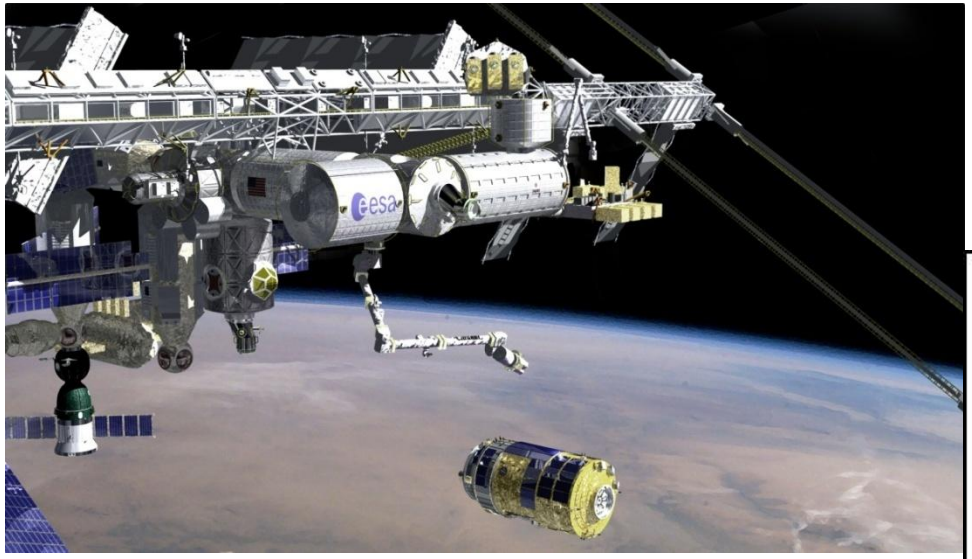
STPA Analysis: Causal Factors



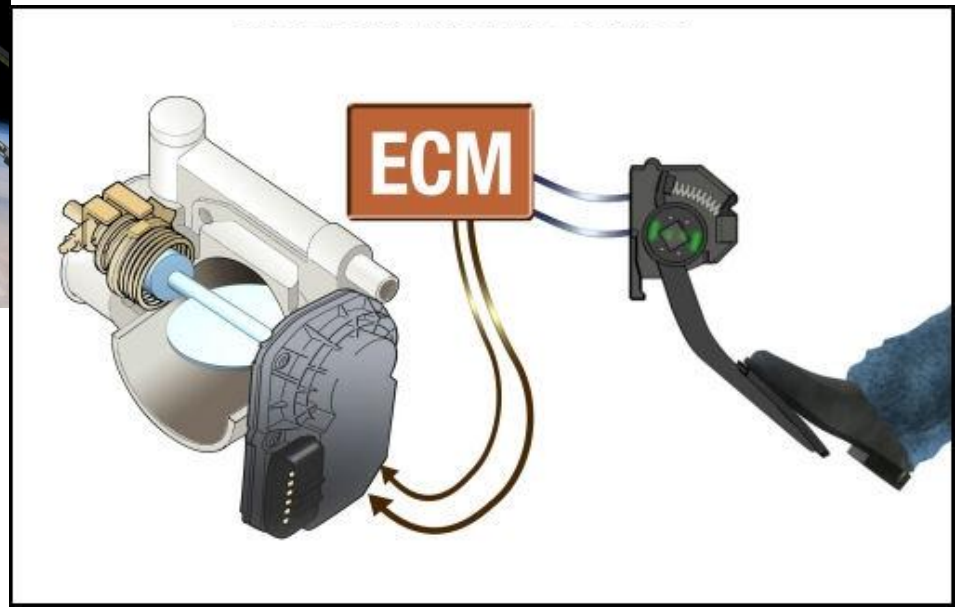


STPA Group Exercise

Choose a system to analyze:



International Space Station unmanned cargo vehicle



Electronic Throttle Control

STPA Group Exercise

- Identify Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions
  - 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