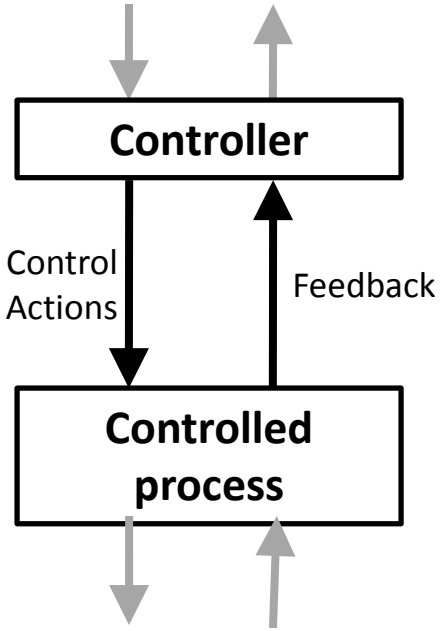
Systems Theoretic Process Analysis (STPA)

STPA
(System-Theoretic Process Analysis)

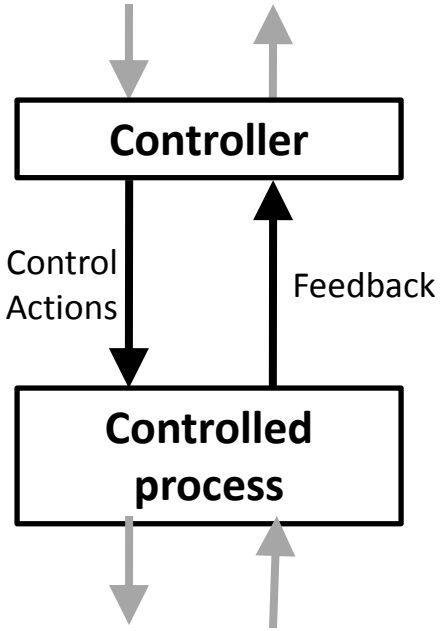
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

STPA
(System-Theoretic Process Analysis)

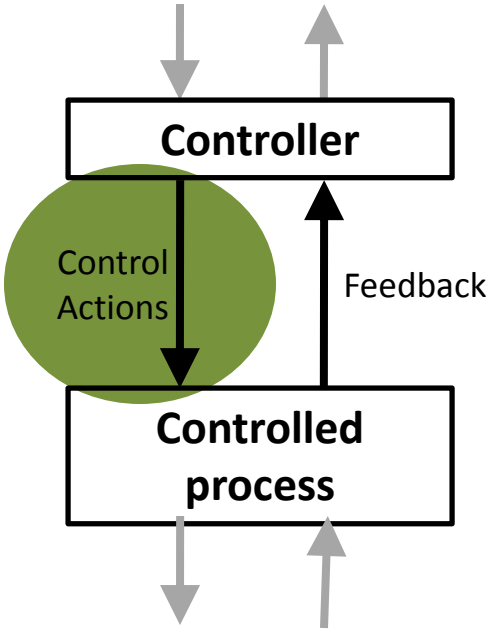
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

STPA
(System-Theoretic Process Analysis)

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



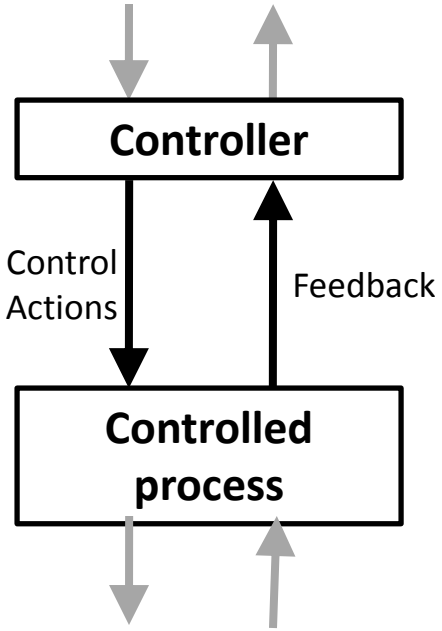
(Leveson, 2012)

ITP Exercise

a new in-trail procedure
for trans-oceanic flights

STPA
(System-Theoretic Process Analysis)

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



(Leveson, 2012)

Example System: Aviation

Image removed due to copyright restrictions.

System-level Accident (Loss): ?

Example System: Aviation

Image removed due to copyright restrictions.

System-level Accident (Loss): Two aircraft collide

Image removed due to copyright restrictions.

System-level Accident (Loss): Two aircraft collide

System-level 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

Image removed due to copyright restrictions.

System-level Accident (Loss): Two aircraft collide

System-level Hazard: Two aircraft violate minimum separation

Aviation Examples

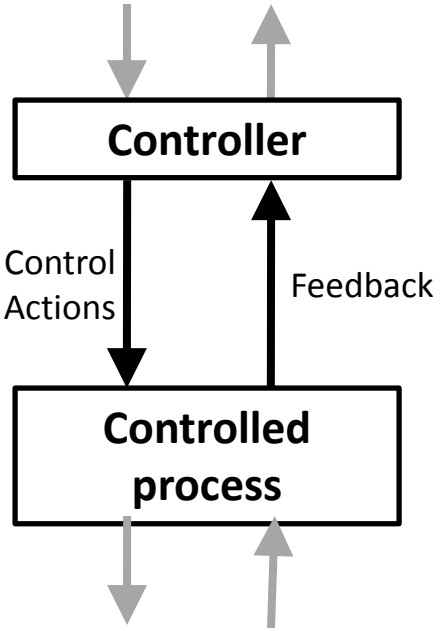
- System-level Accident (loss)
  - Two aircraft collide
  - Aircraft crashes into terrain / ocean
- System-level Hazards
  - Two aircraft violate minimum separation
  - Aircraft enters unsafe atmospheric region
  - Aircraft enters uncontrolled state
  - Aircraft enters unsafe attitude
  - Aircraft enters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

Aviation Examples

- System-level Accident (loss)
  - A-1: Two aircraft collide
  - A-2: Aircraft crashes into terrain / ocean
- System-level Hazards
  - H-1: Two aircraft violate minimum separation
  - H-2: Aircraft enters unsafe atmospheric region
  - H-3: Aircraft enters uncontrolled state
  - H-4: Aircraft enters unsafe attitude
  - H-5: Aircraft enters prohibited area

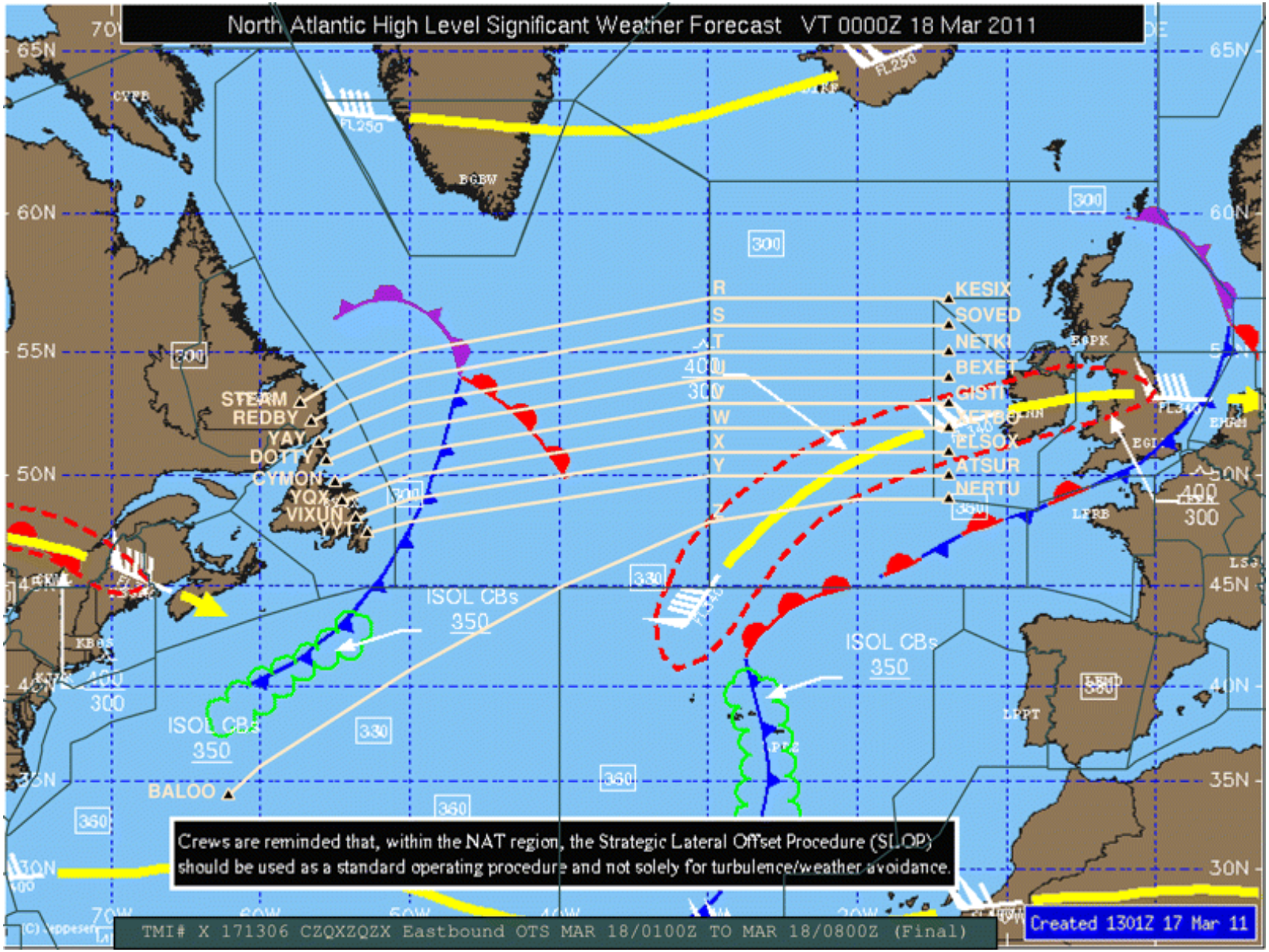
STPA
(System-Theoretic Process Analysis)

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



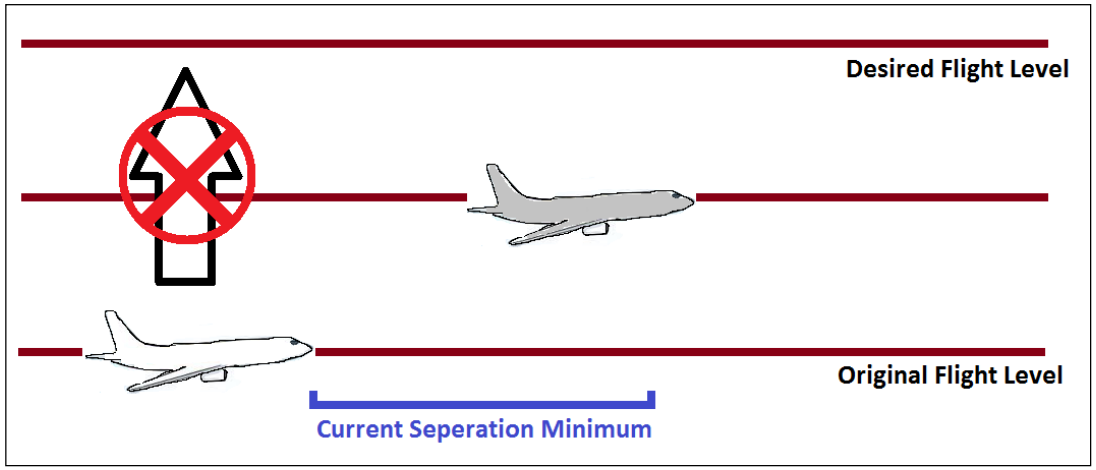
(Leveson, 2012)

North Atlantic Tracks



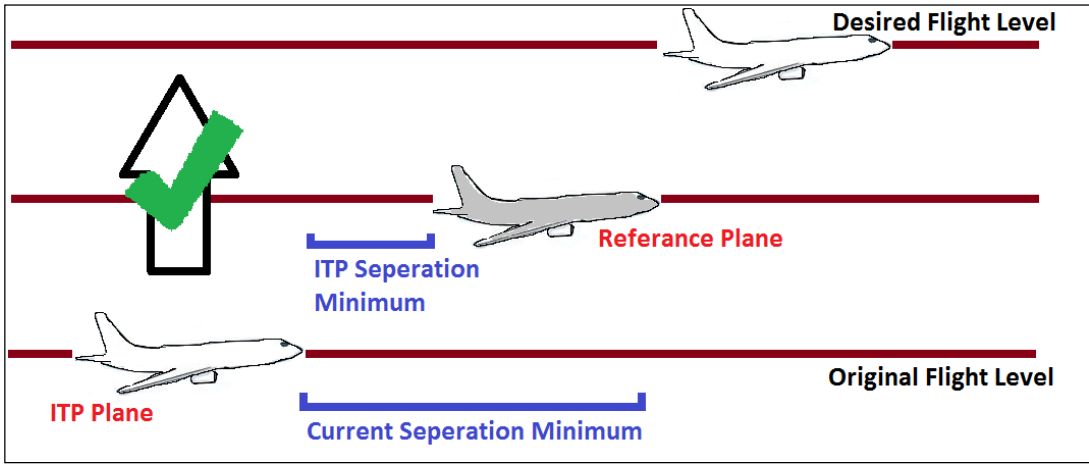
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



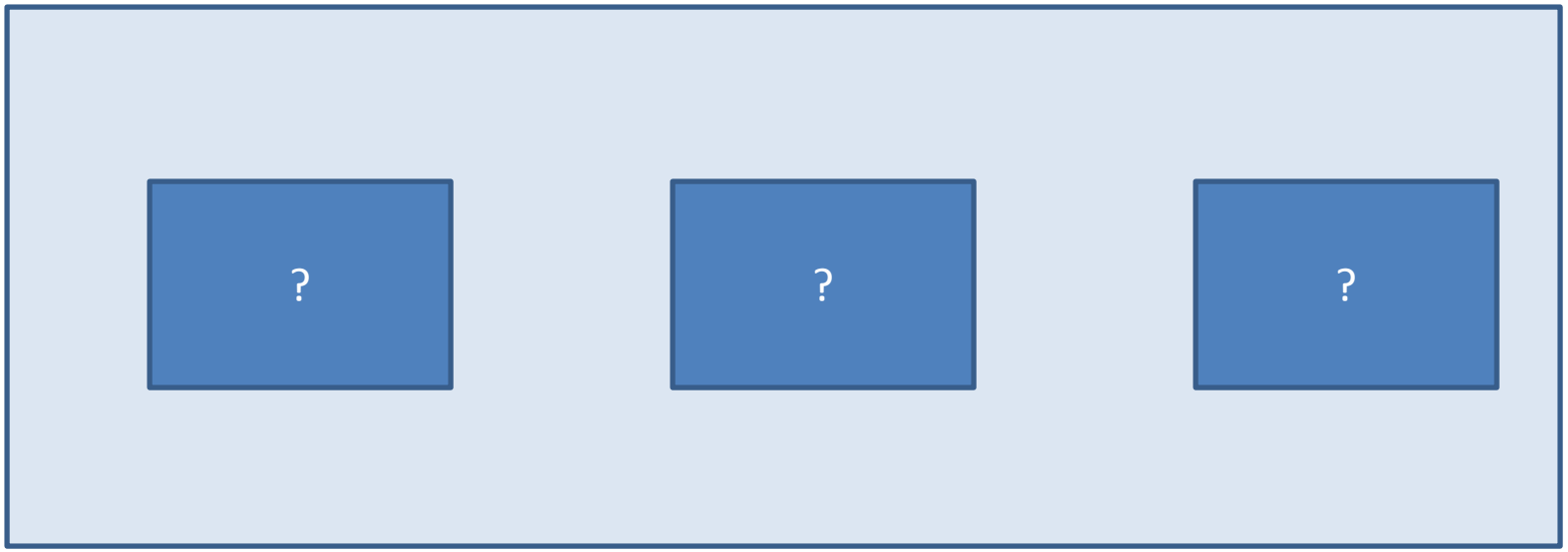
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



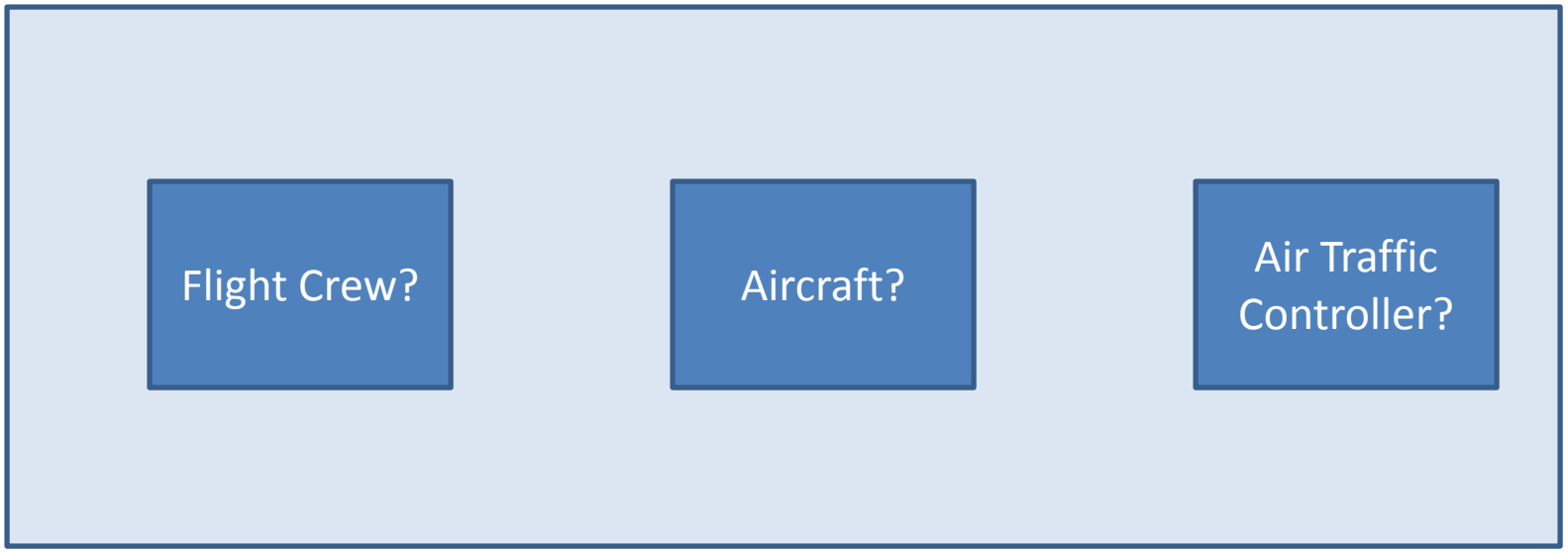
STPA Analysis

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



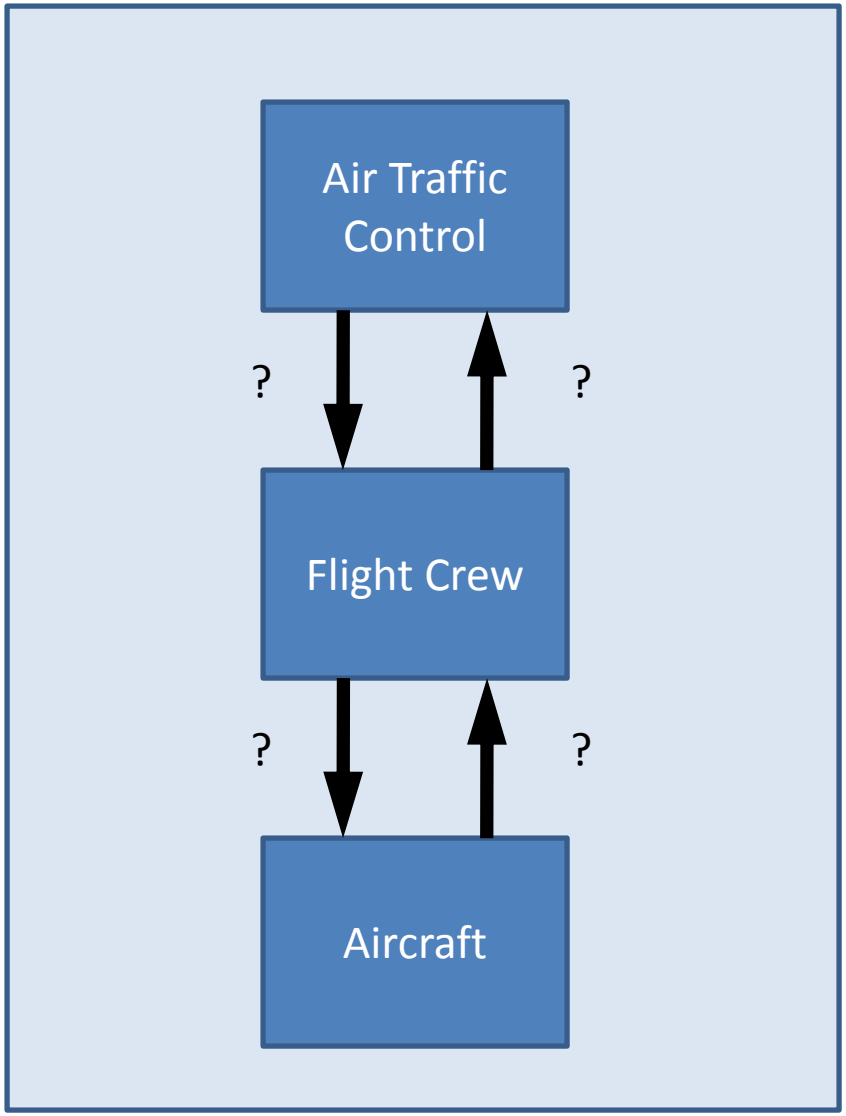
STPA Analysis

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



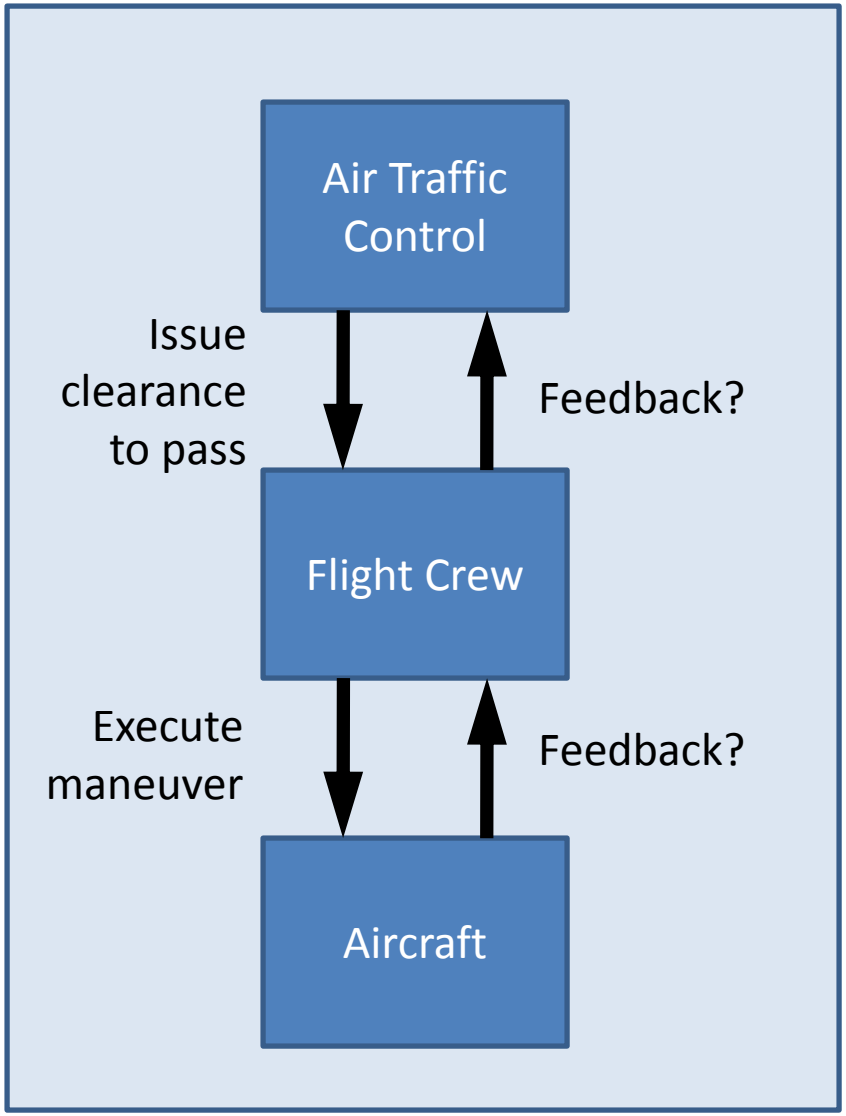
STPA Analysis

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



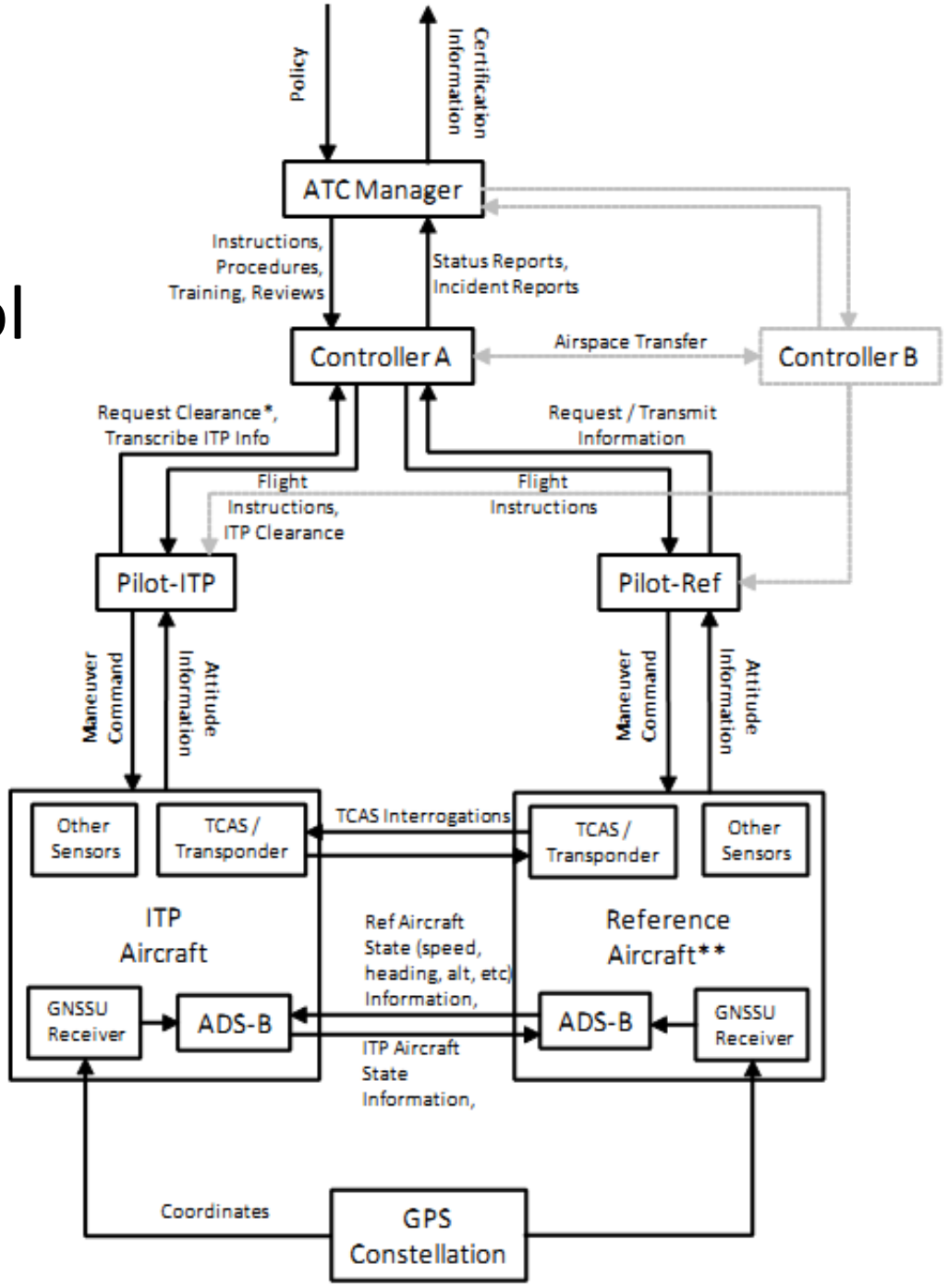
STPA Analysis

- High-level (simple) Control Structure

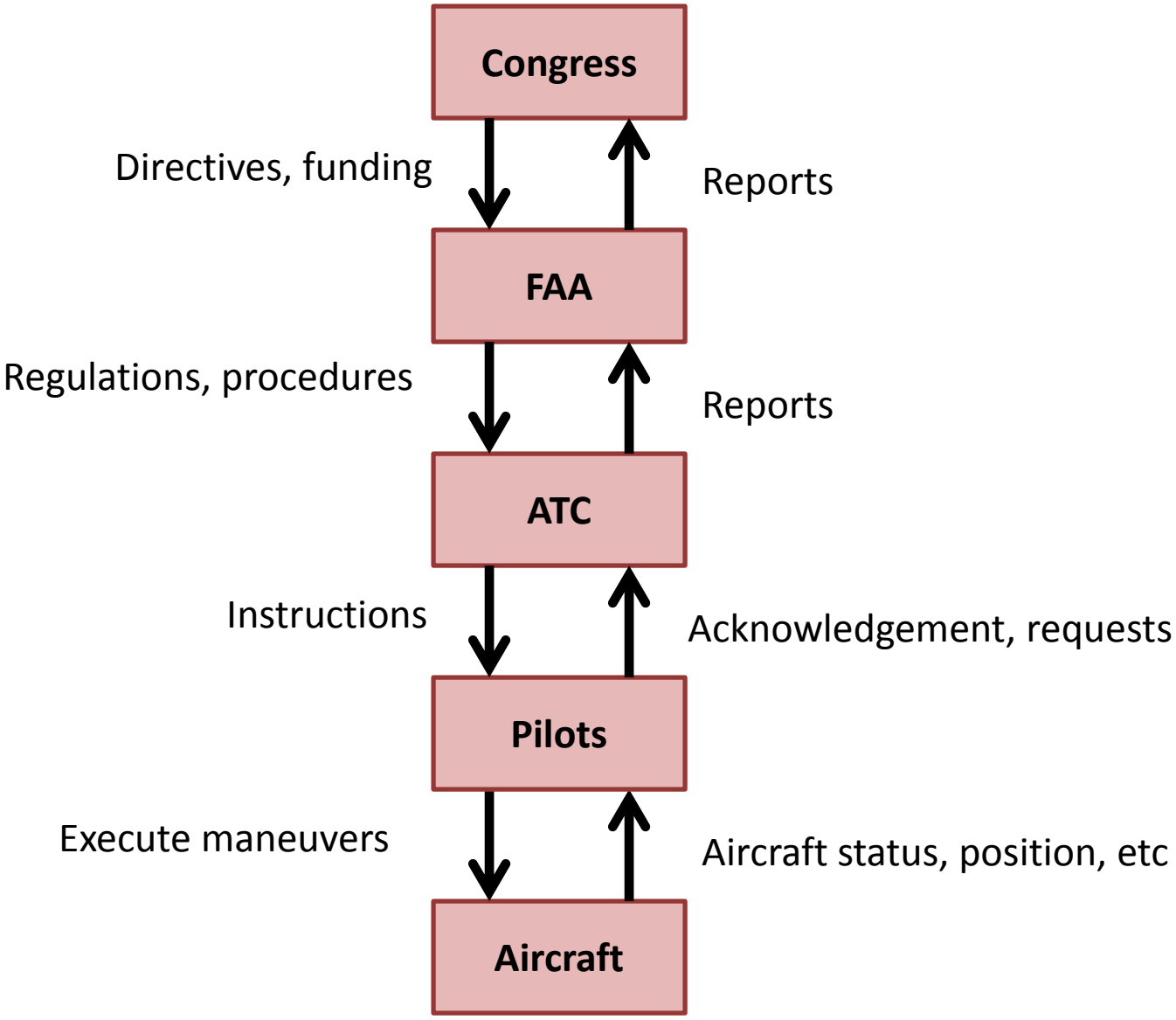


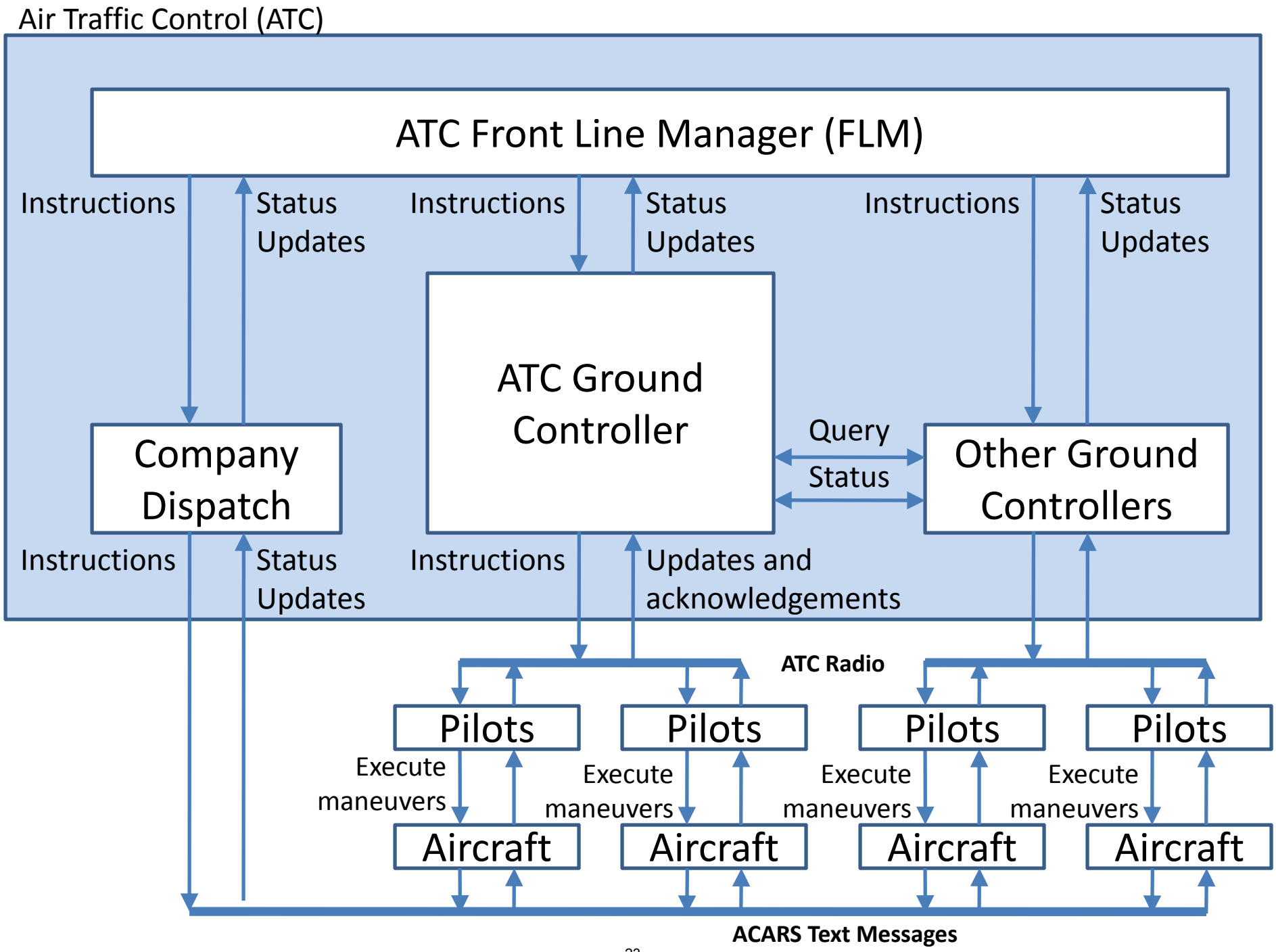
STPA Analysis

- More complex control structure



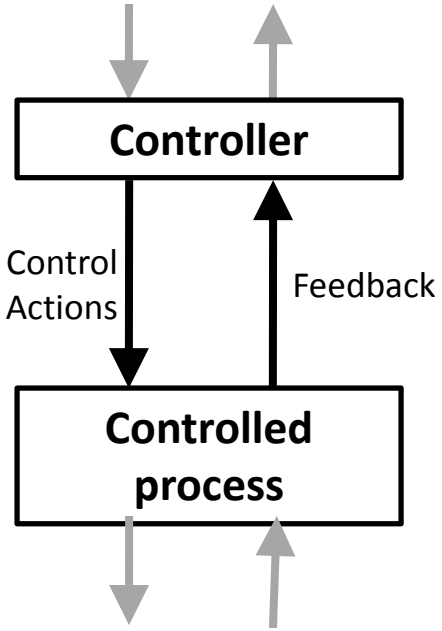
Example High-level control structure




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

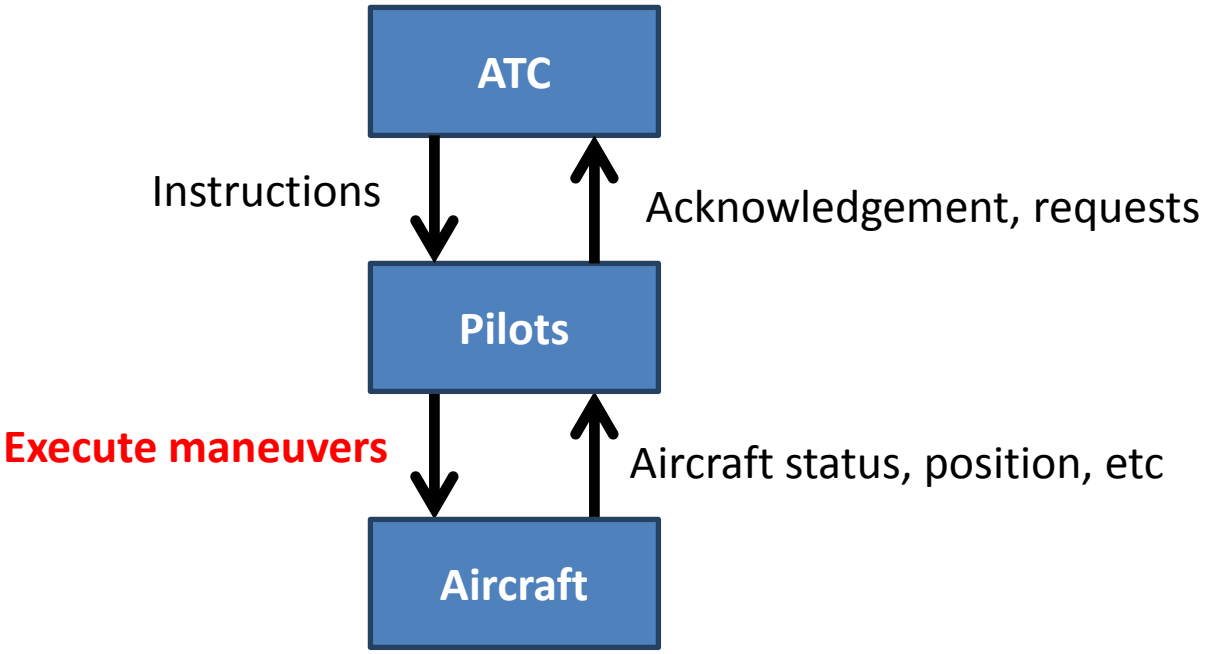
STPA
(System-Theoretic Process Analysis)

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



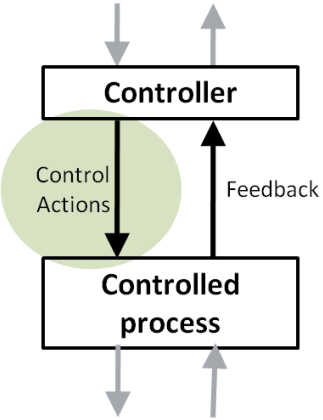
(Leveson, 2012)

Identify Unsafe Control Actions



Flight Crew Action (Role)	Not providing causes hazard	Providing Causes hazard	Incorrect Timing/ Order	Stopped Too Soon
Execute Passing Maneuver		Pilots perform ITP when ITP criteria are not met or request has been refused [H-1]		

Structure of a Hazardous Control Action



Example:

"Pilots provide ITP maneuver when ITP criteria not met"

Source Controller

Type

Control Action

Context

Four parts of a hazardous control action

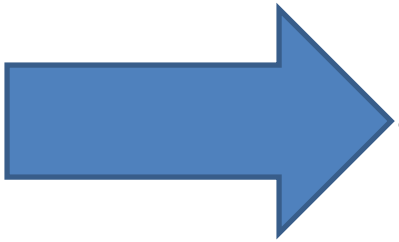
- Source Controller: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)

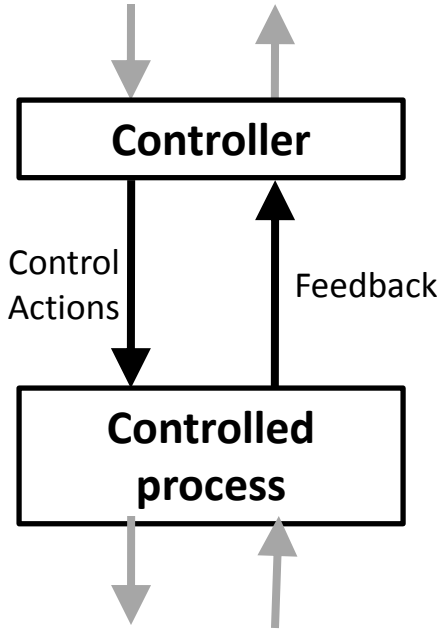
Defining Safety Constraints

Unsafe Control Action	Safety Constraint
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
Etc.	Etc.

STPA
(System-Theoretic Process Analysis)

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

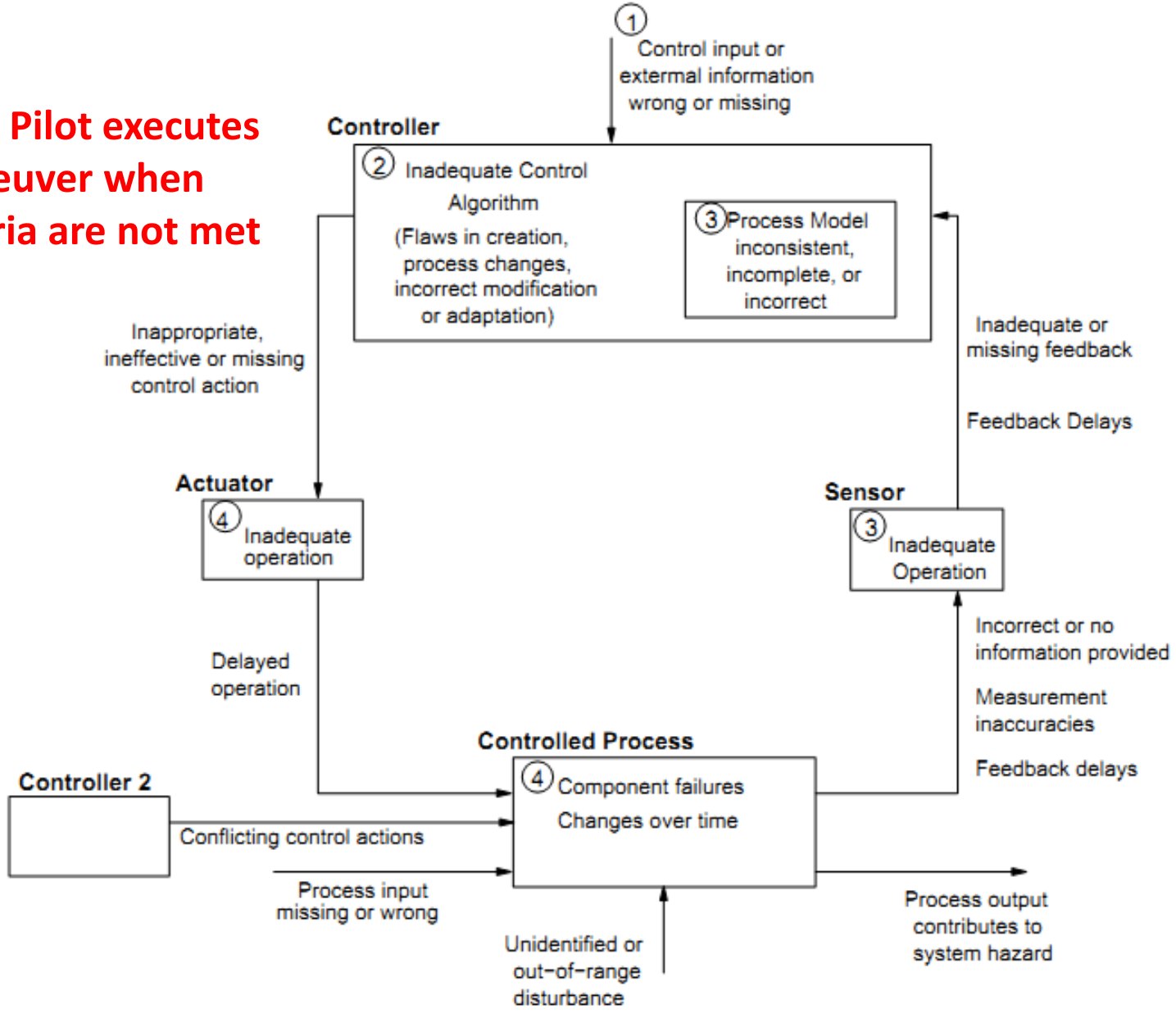




(Leveson, 2012)

STPA Step 2: Causal scenarios

UCA: Pilot executes maneuver when criteria are not met [H-1]



From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

16.63J / ESD.03J System Safety
Spring 2016