STPA
Systems Theoretic Process Analysis

Agenda

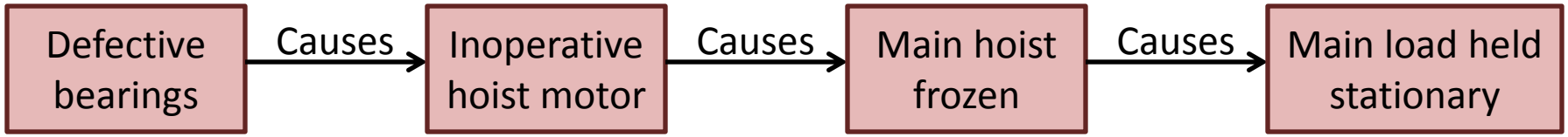
- Quick review of hazard analysis
- Quick review of STAMP
- Intro to STPA hazard analysis

Hazard Analysis vs. Accident Model

Dates back to…	Hazard Analysis Method	Accident Model
1949	Failure Modes and Effect Analysis*	Chain of events
1961	Fault Tree Analysis	Chain of events
1967	Event Tree Analysis	Chain of events
1960s	Hazard and Operability Analysis	Parameter deviation
2002	**Systems Theoretic Process Analysis**	**STAMP** (Systems-Theoretic Accident Model and Process)

*Technically a reliability technique, but sometimes used for safety analyses

Domino "Chain of events" Model



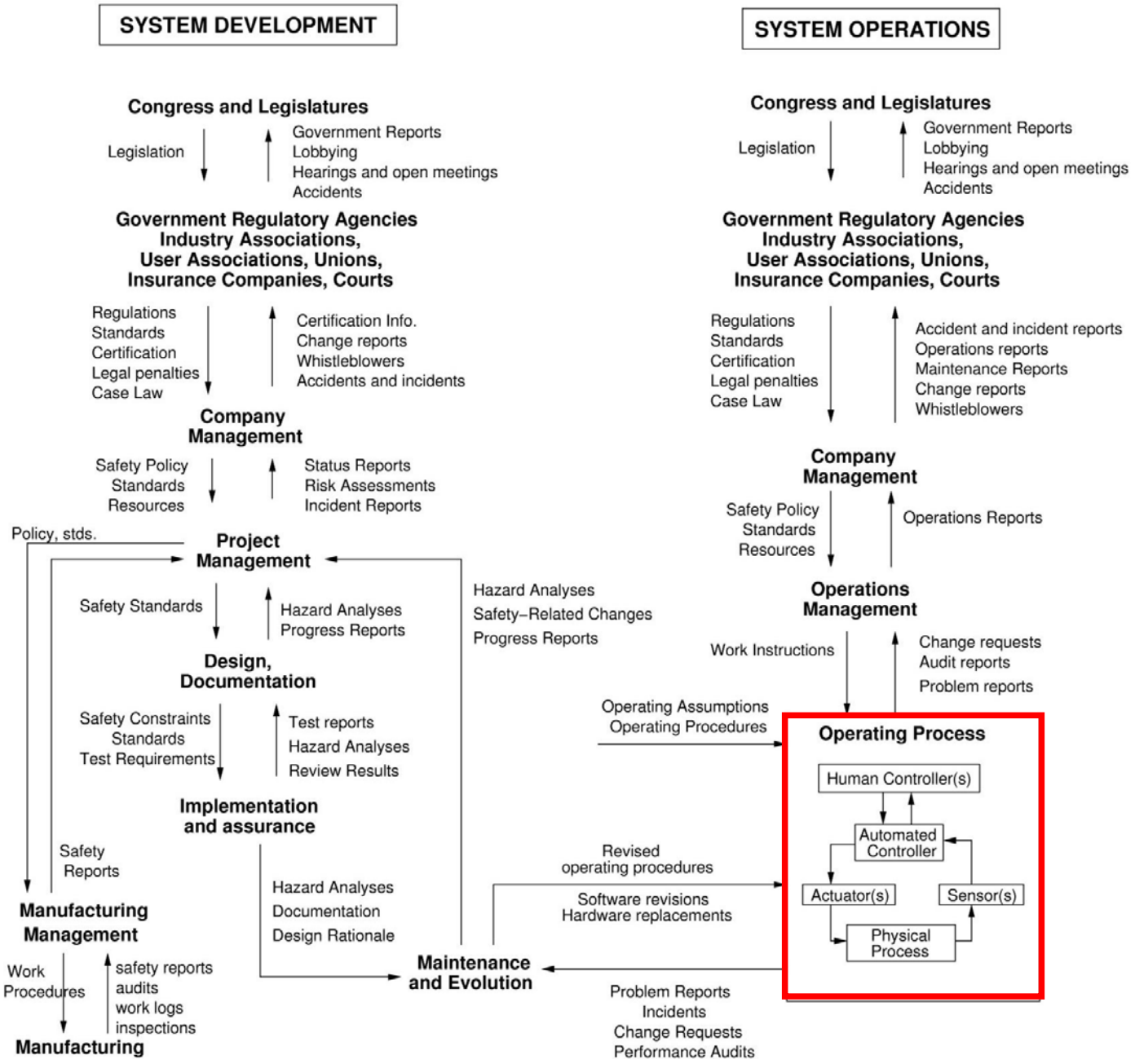
Event-based

Systems approach to safety engineering (STAMP)

STAMP Model

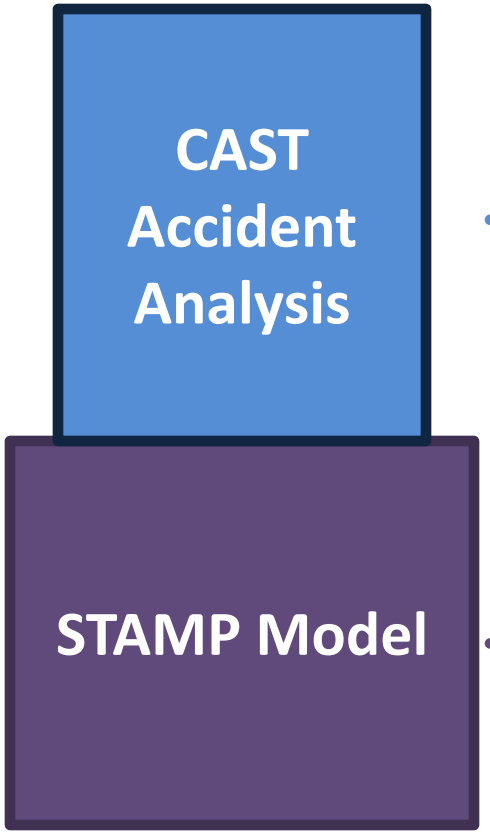
- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not a failure problem
- Prevent accidents by enforcing constraints on component behavior and **interactions**
- Captures more causes of accidents:
  - Component failure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

Example Safety Control Structure



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

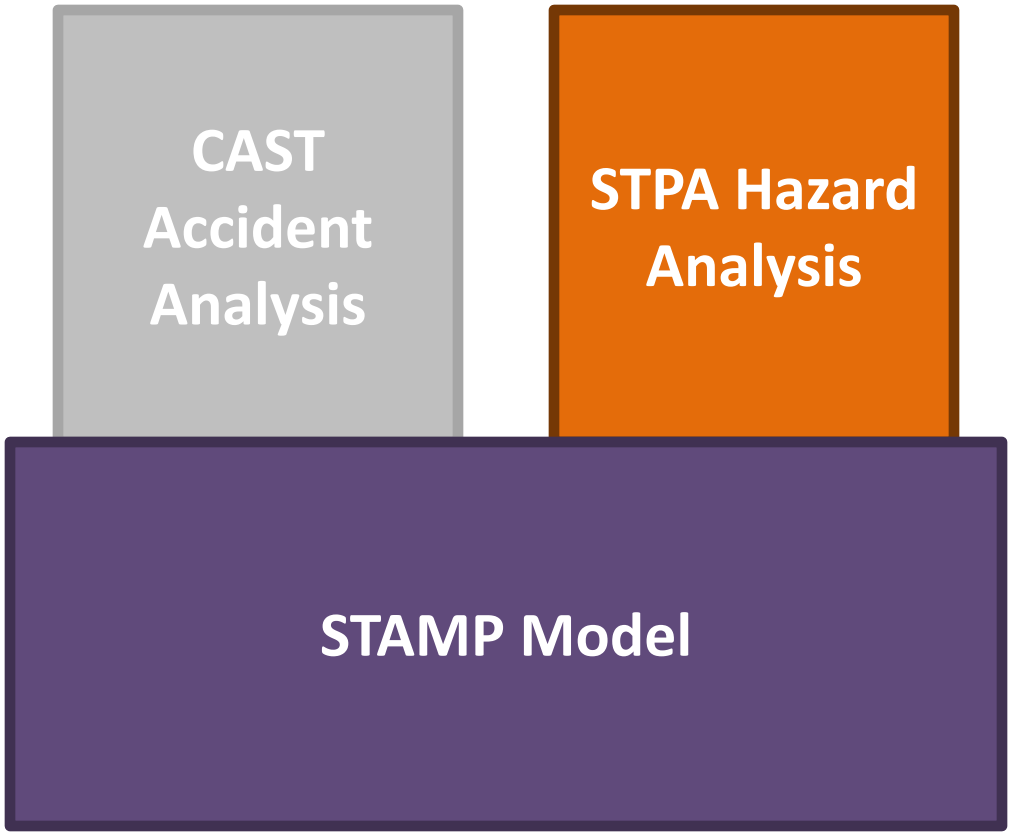
STAMP and CAST



How do we find inadequate control that caused the accident?

Accidents are caused by inadequate control

STAMP and STPA

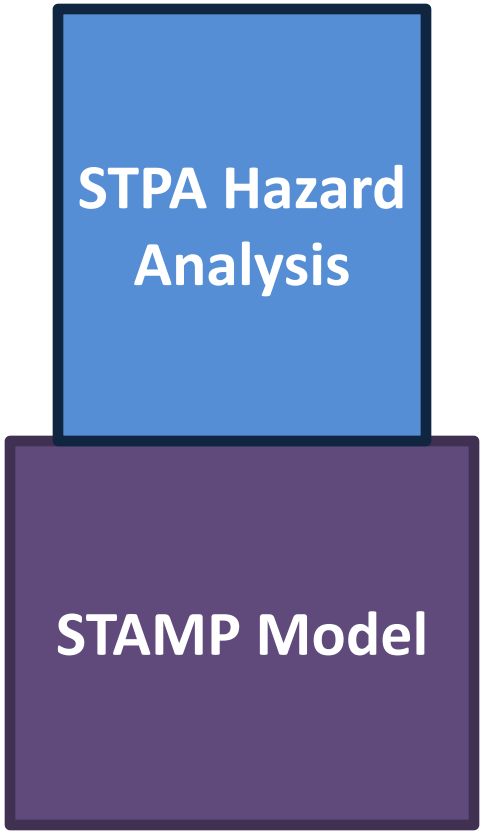


How do we find inadequate control in a design?

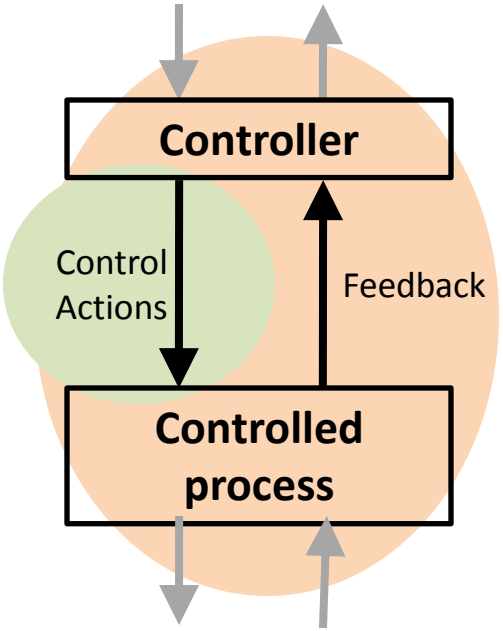
Accidents are caused by inadequate control

STPA Hazard Analysis

STPA
(System-Theoretic Process Analysis)



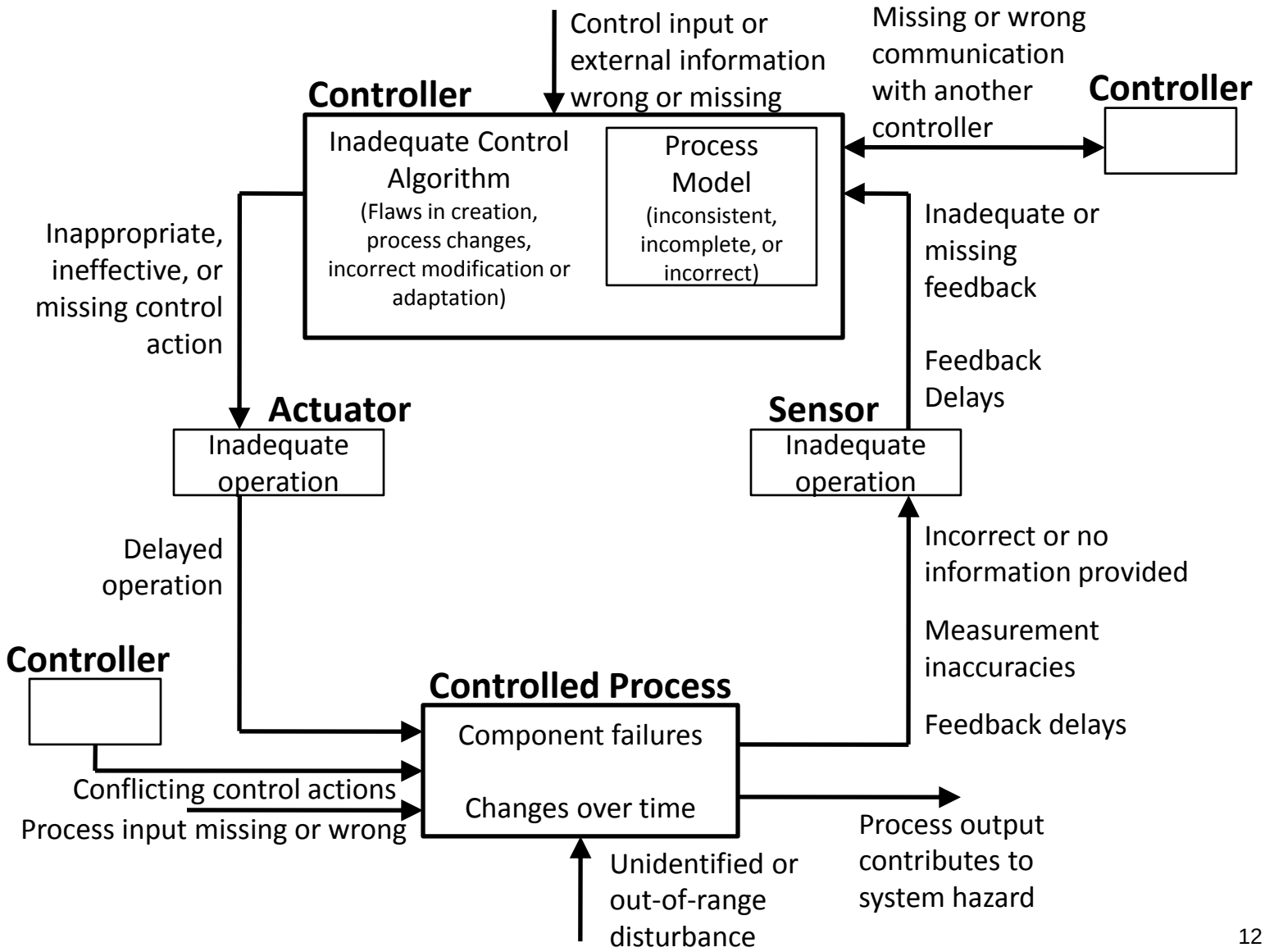
- Identify the hazards
- Construct the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors



STPA Step 1: Identify Unsafe Control Actions

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
(Control Action)				

STPA Step 2: Identify Control Flaws



STPA Exercise

a new in-trail procedure
for trans-oceanic flights

Example System: Aviation

Accident (Loss): Two aircraft collide

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 providing causes hazard, providing causes hazard, 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***
  - (accidents may depend on factors outside our 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): Two aircraft collide

Hazard: Two aircraft violate minimum separation

Identifying Hazards

- Loss (accident)
  - Two aircraft collide with each other
  - Aircraft collides with terrain / ocean
- 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 providing causes hazard, providing causes hazard, 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

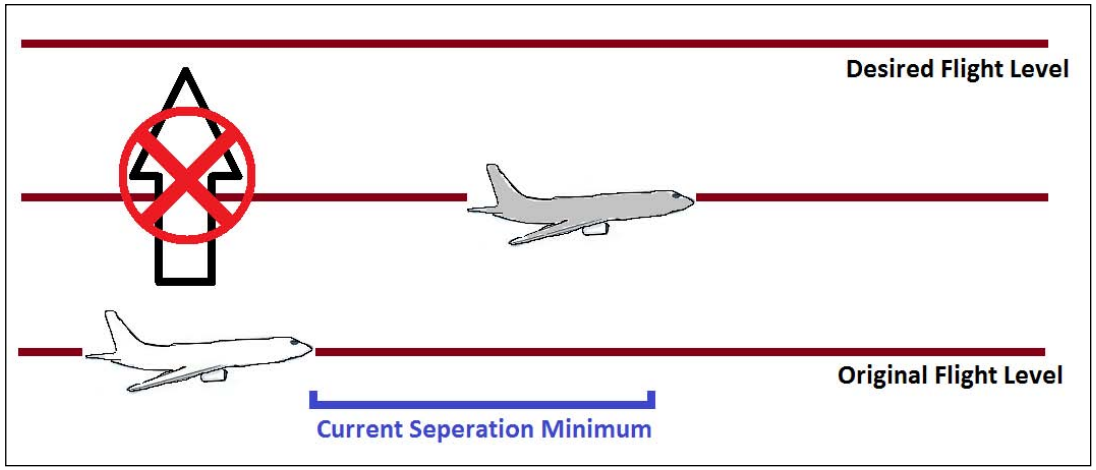
North Atlantic Track eastbound image removed due to copyright restrictions. See:
http://www.turbulenceforecast.com/atlantic_eastbound_tracks.php

- No radar coverage. Pilots check in periodically; at any given time ATC can estimate where aircraft are.

- ITP video: (watch 0:44 to 3:18)
- http://www.youtube.com/watch?v=-KFx9oGHm_w

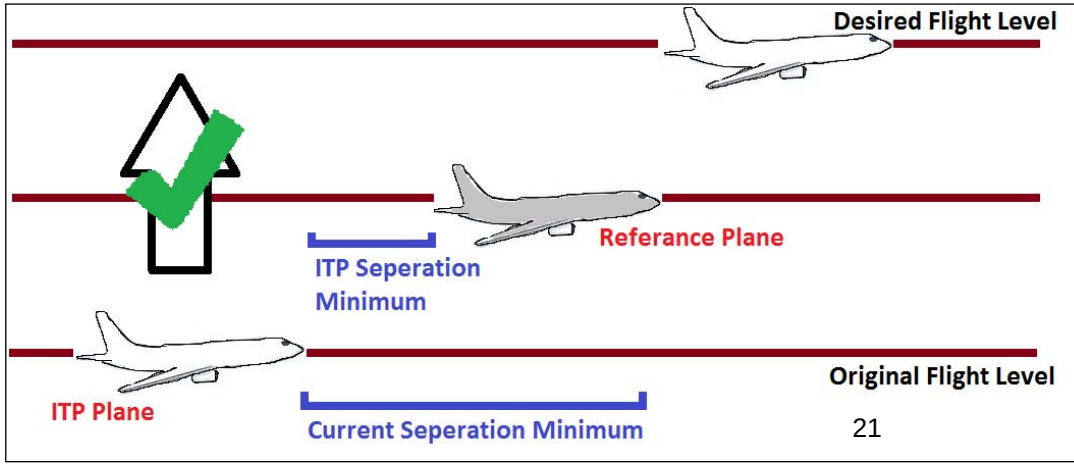
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



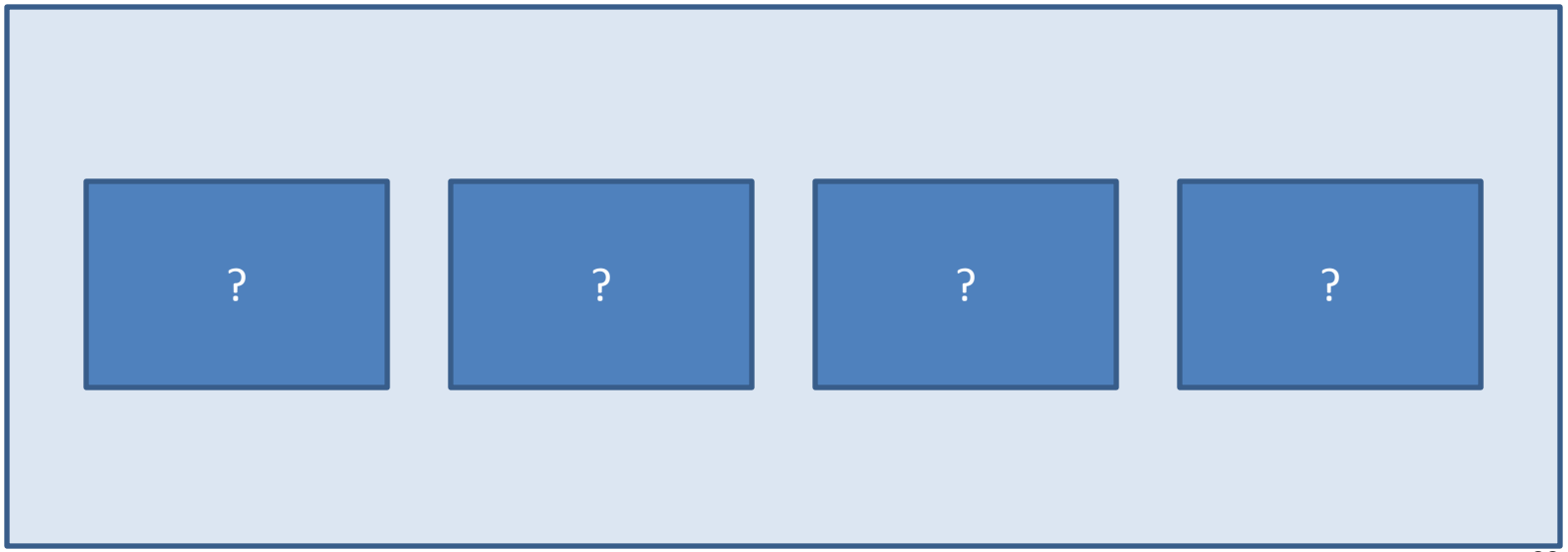
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



STPA Analysis

- High-level (simple) Control Structure
  - What are the main components and controllers?
  - Who controls who?
  - Draw and label control actions / feedback arrows



STPA Analysis

- More complex control structure

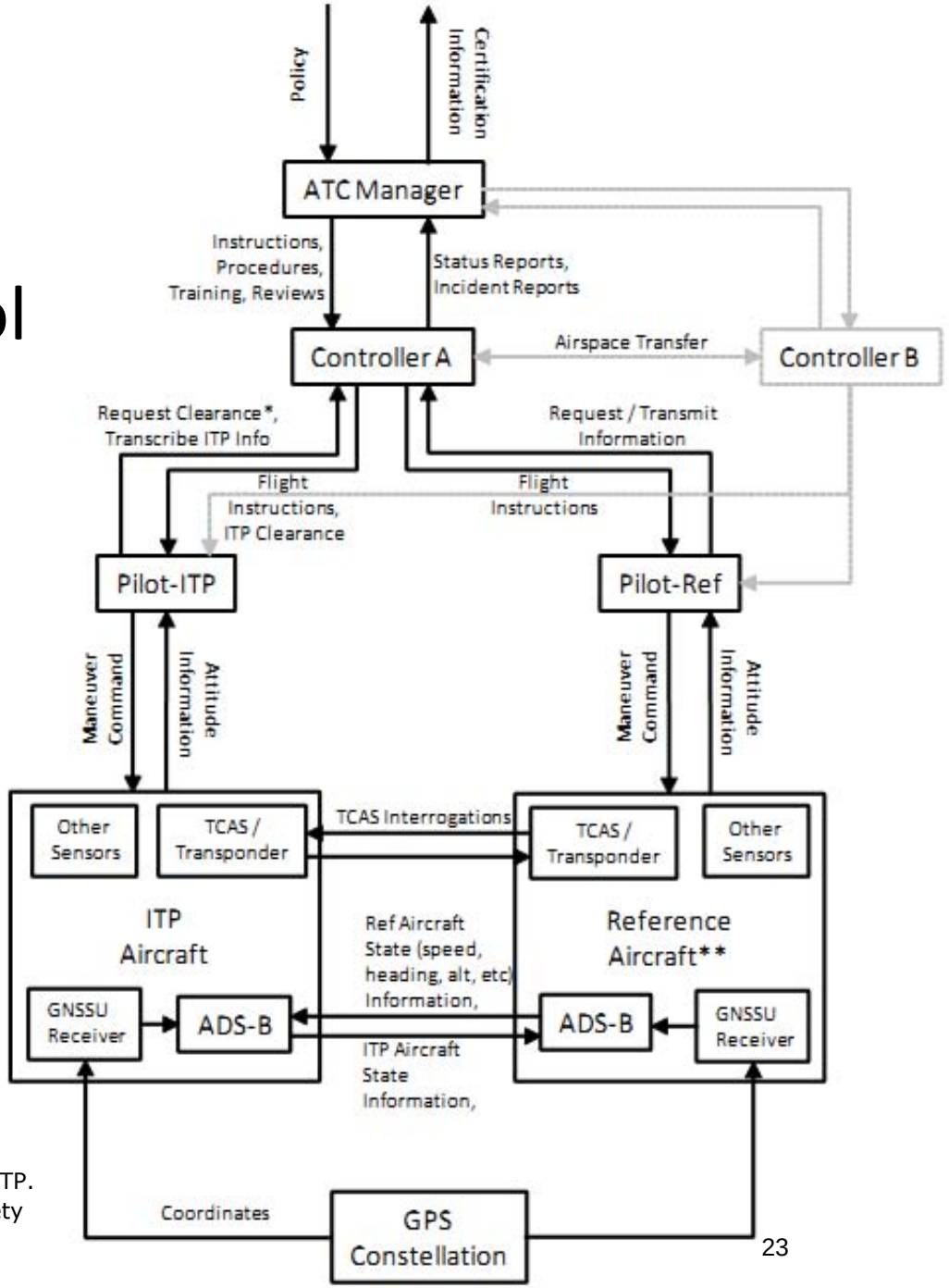


Image: Public Domain. Figure 7: Safety Control Structure for ATSA-ITP. Fleming, Cody Harrison, Melissa Spencer, Nancy Leveson et al. "Safety Assurance in NextGen." March 2012. NASA/CR–2012-217553.

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 providing causes hazard, providing causes hazard, 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:
Basic Unsafe Control Action Table

Flight Crew Action (Role)	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon
Execute Passing Maneuver	Pilot does not execute maneuver once it is approved ?	?	?	?

STPA Analysis:
Basic Unsafe Control Action Table

Flight Crew Action (Role)	Not providing causes hazard	Providing causes hazard*	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 Perform ITP when 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

Defining Safety Constraints

Unsafe Control Action	Safety Constraint
UCA 1: Pilot does not execute maneuver once it is approved	**SC 1:** Maneuver must be executed once it is approved
UCA 2: Pilot performs ITP when ITP criteria are not met	**SC 2:** ITP must not be performed when criteria are not met
UCA 3: Pilot executes maneuver late after having re-verified ITP criteria	**SC 3:** Maneuver must be executed 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 providing causes hazard, providing causes hazard, 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

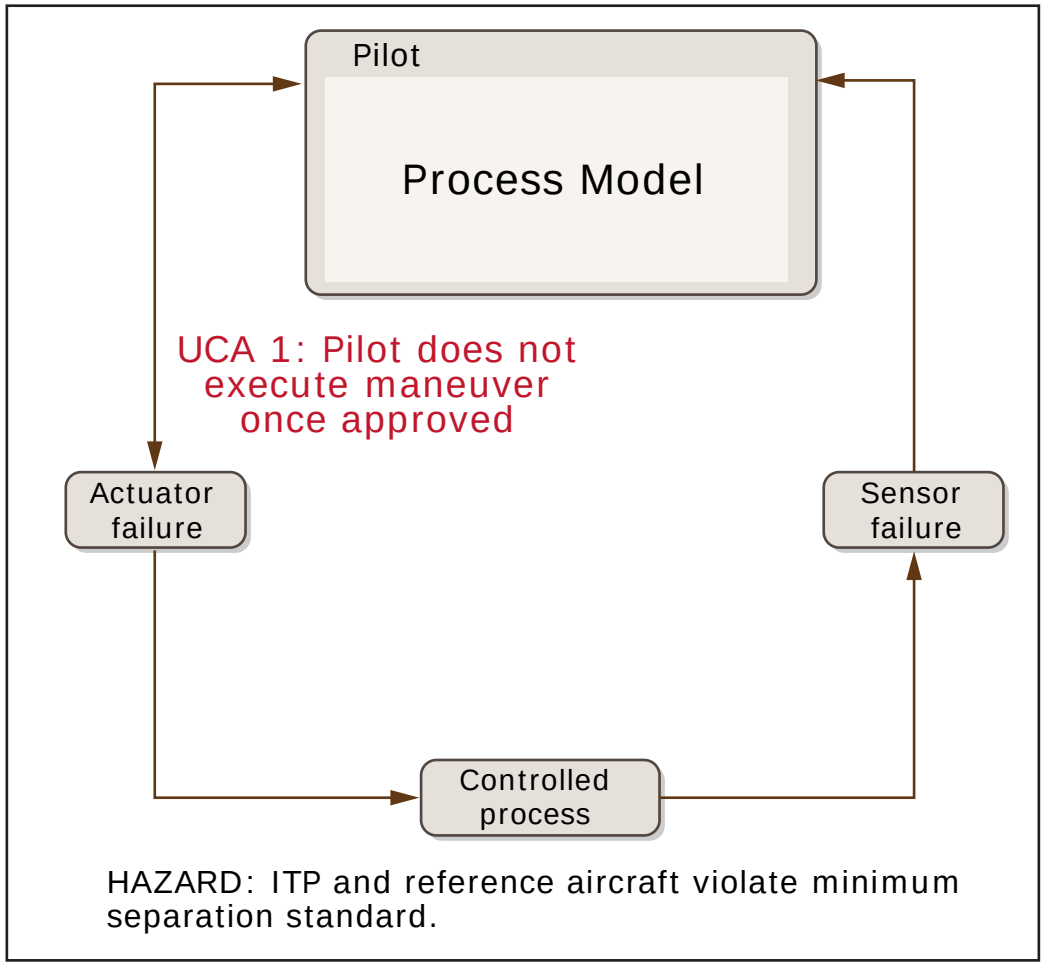


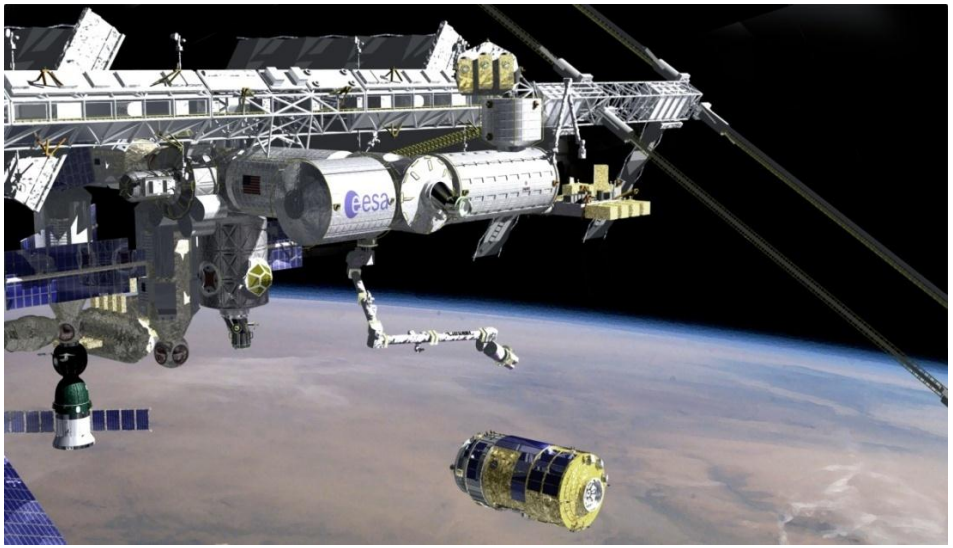
Image by MIT OpenCourseWare.

How could this action be caused by:

- Process model
- Feedback
- Sensors
- Etc?

STPA Group Exercise

STPA Group Exercise



International Space Station unmanned cargo vehicle

Watch HTV grapple: (0:40 – 1:30)
https://www.youtube.com/watch?v=TL_WysC8eb0

View first 4 slides at:
http://psas.scripts.mit.edu/home/get_pdf.php?name=1-4-HTV-system-description.pdf

STPA Group Exercise

- Identify 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, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors (**next time**)

16.63J / ESD.03J System Safety
Fall 2012