Systems Theoretic Process Analysis (STPA) Tutorial

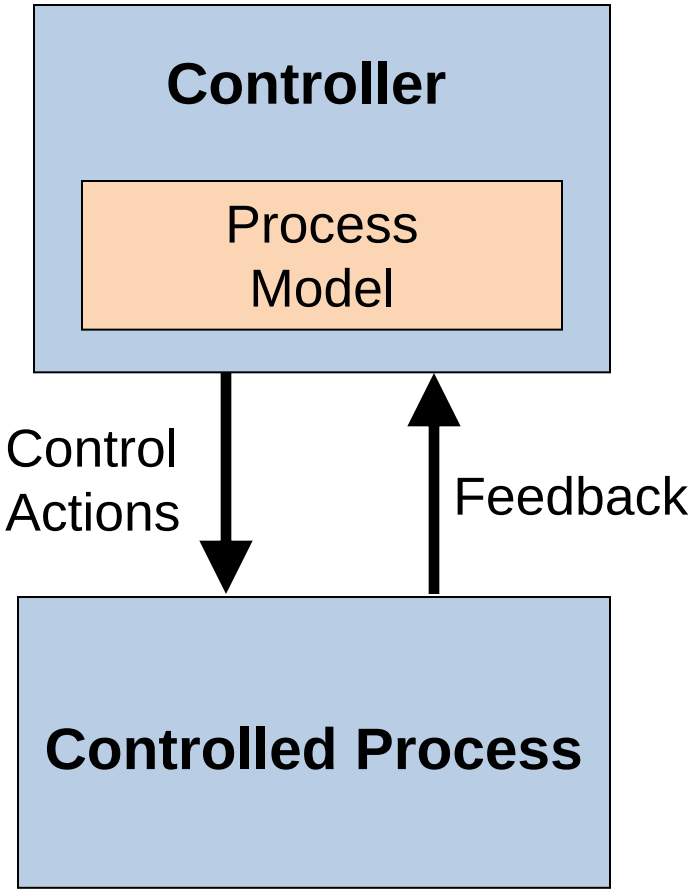
Dr. John Thomas
MIT

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

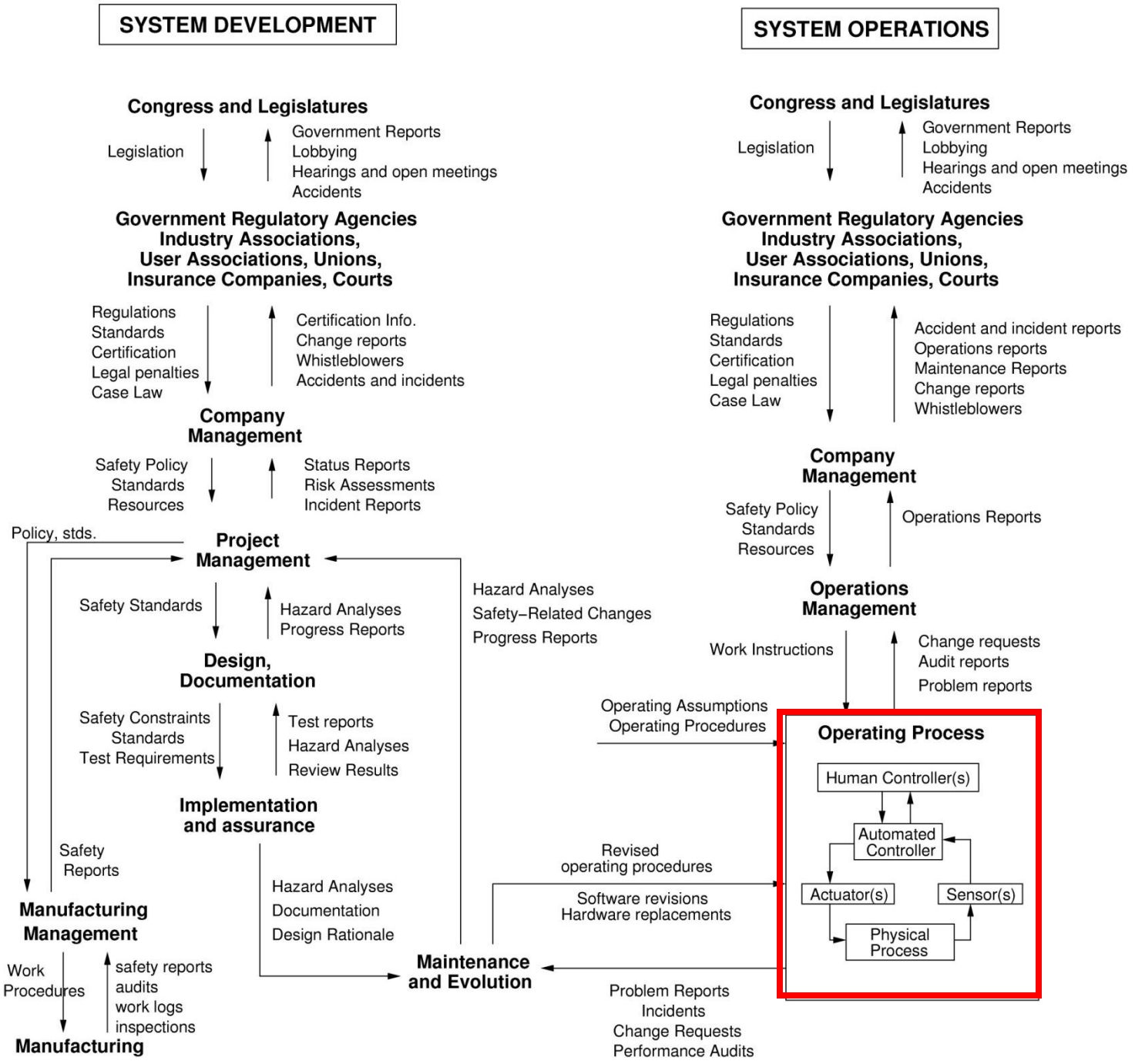
STAMP



- 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 …

Example Safety Control Structure

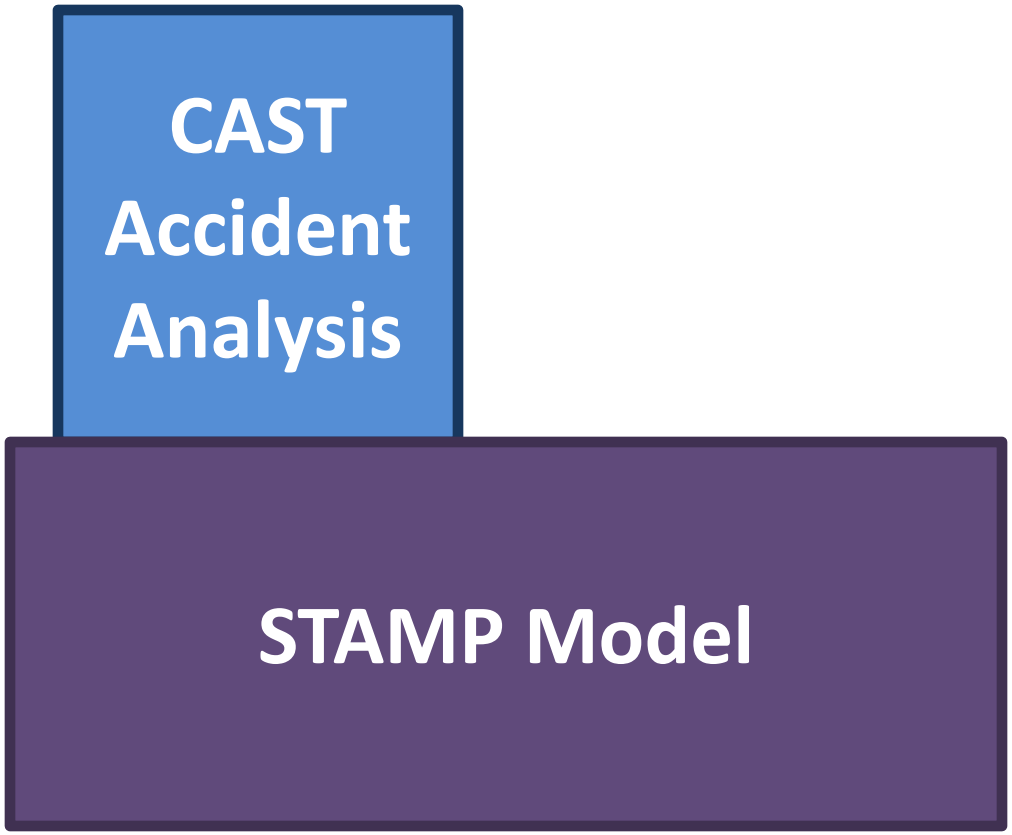


STAMP and STPA

STAMP Model

Accidents are caused by inadequate control

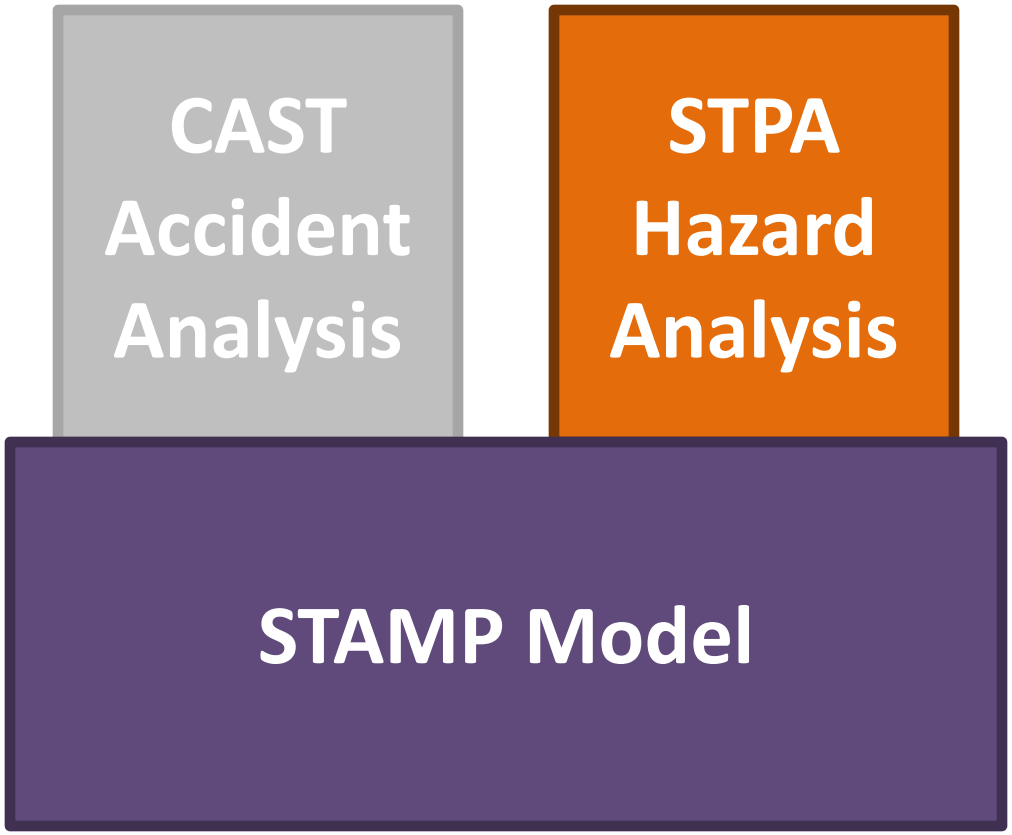
STAMP and STPA



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

Today's Tutorials

- **Basic STPA Tutorial**
  10:15am – 3pm, in 54-100
- CAST Tutorial
  10:15am – 3pm, in 56-154
- Security Tutorial (STPA-Sec)
  10:15am – noon, room 32-082
  (Presentations 1:30-3pm)
- Experienced users meeting
  10:15am – 3pm, room 56-114

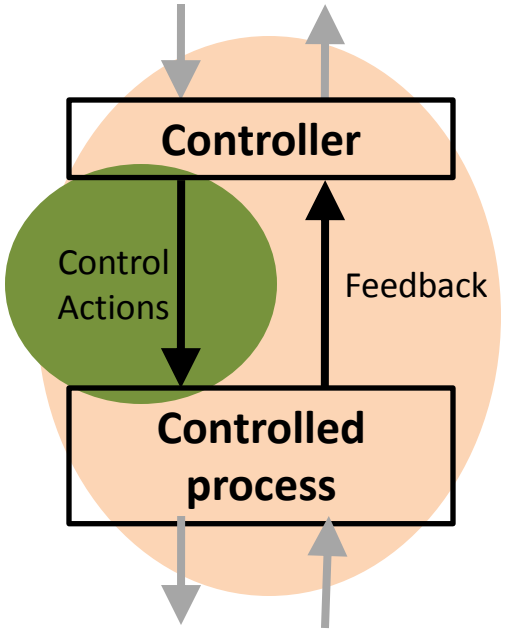
STPA Hazard Analysis

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



Can capture requirements flaws, software errors, human errors

(Leveson, 2011)

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 Accidents (Losses)
  - ?
- System-level Hazards
  - ?
- System-level Safety Constraints
  - ?

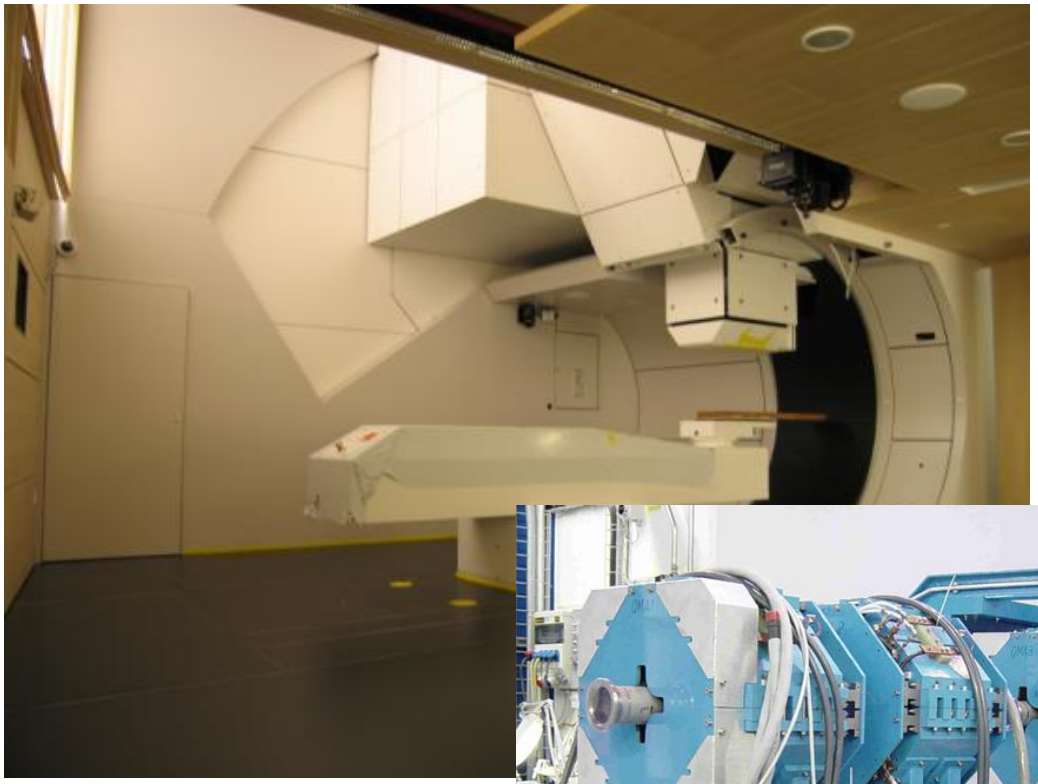
Identify Accident, Hazards, Safety Constraints

- 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

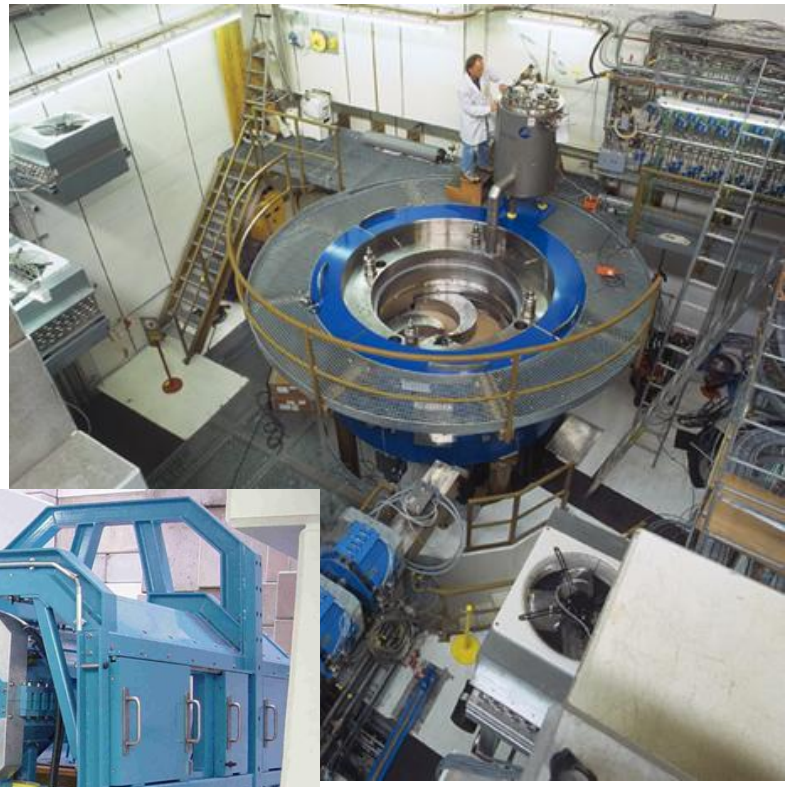
Additional hazards / constraints can be found in ESW p355

Control Structure Examples

Proton Therapy Machine
High-level Control Structure



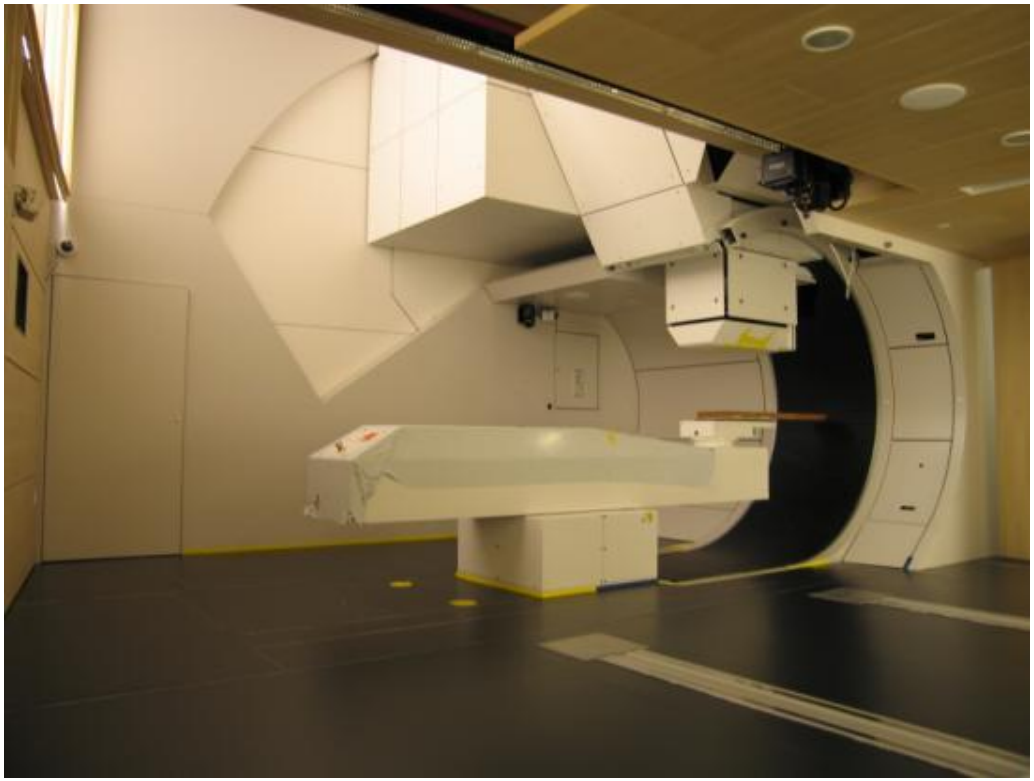
Gantry



Cyclotron

Beam path and
control elements

Proton Therapy Machine
High-level Control Structure



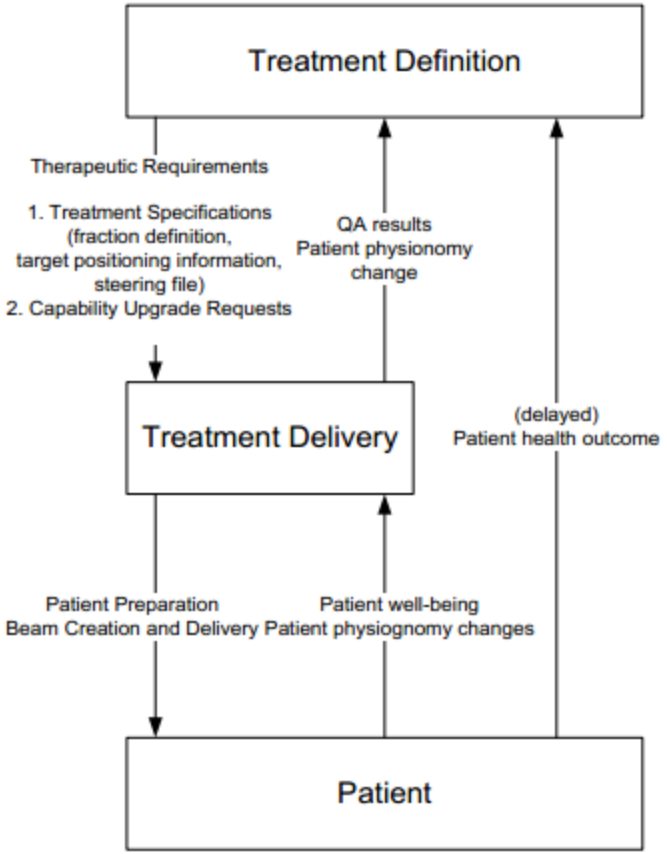
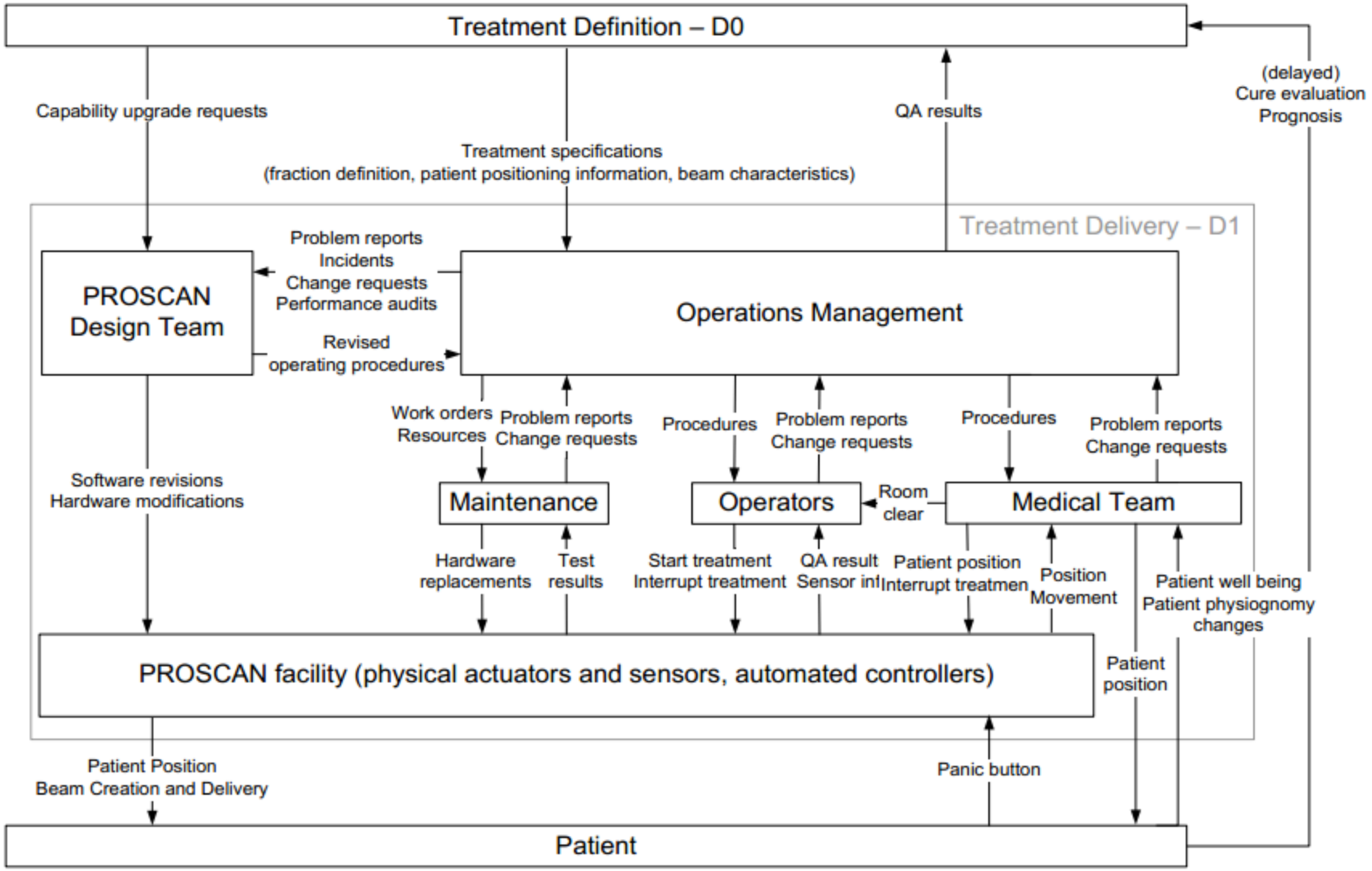


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Antoine PhD Thesis, 2012

Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

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

Adaptive Cruise Control

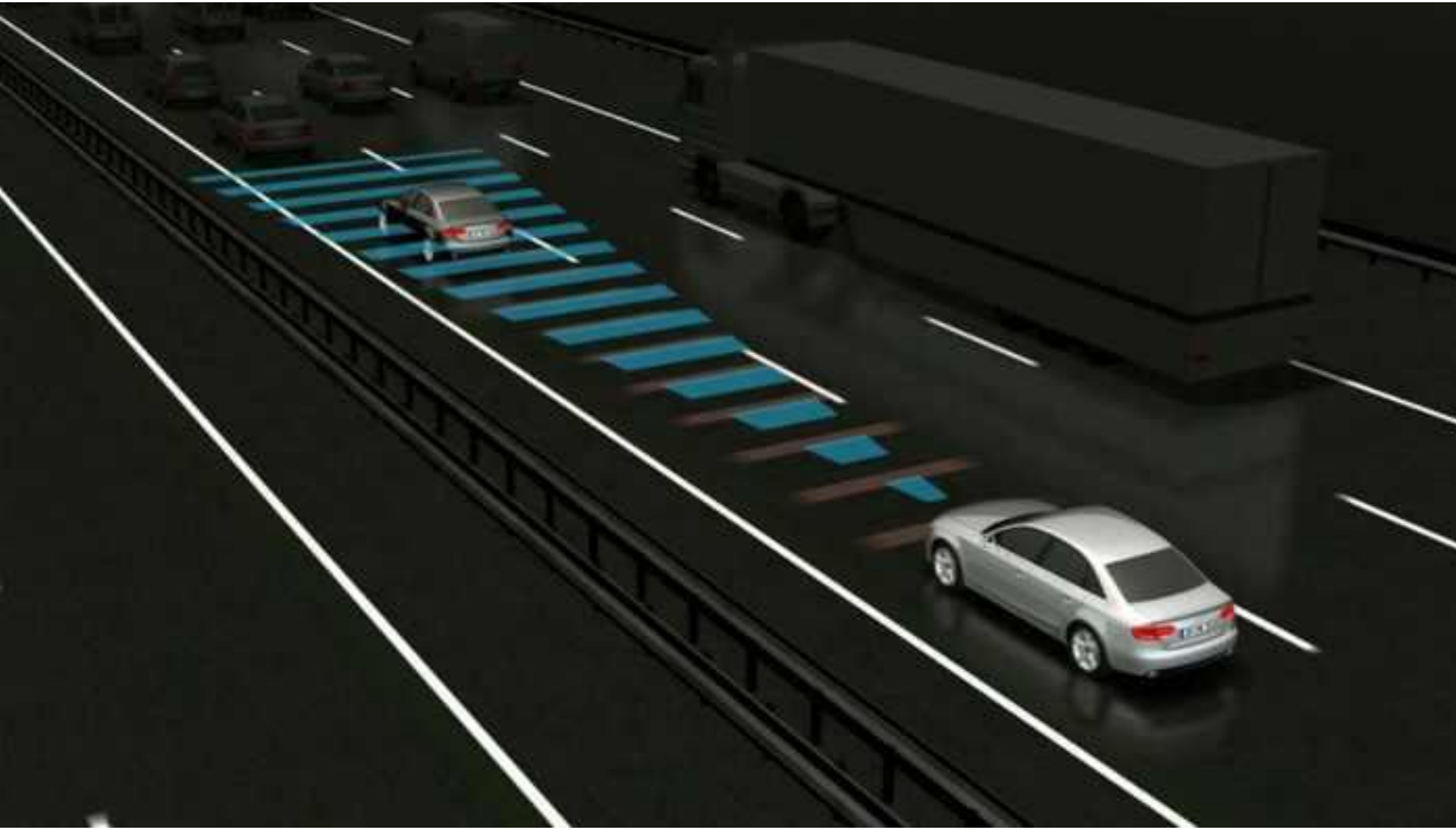
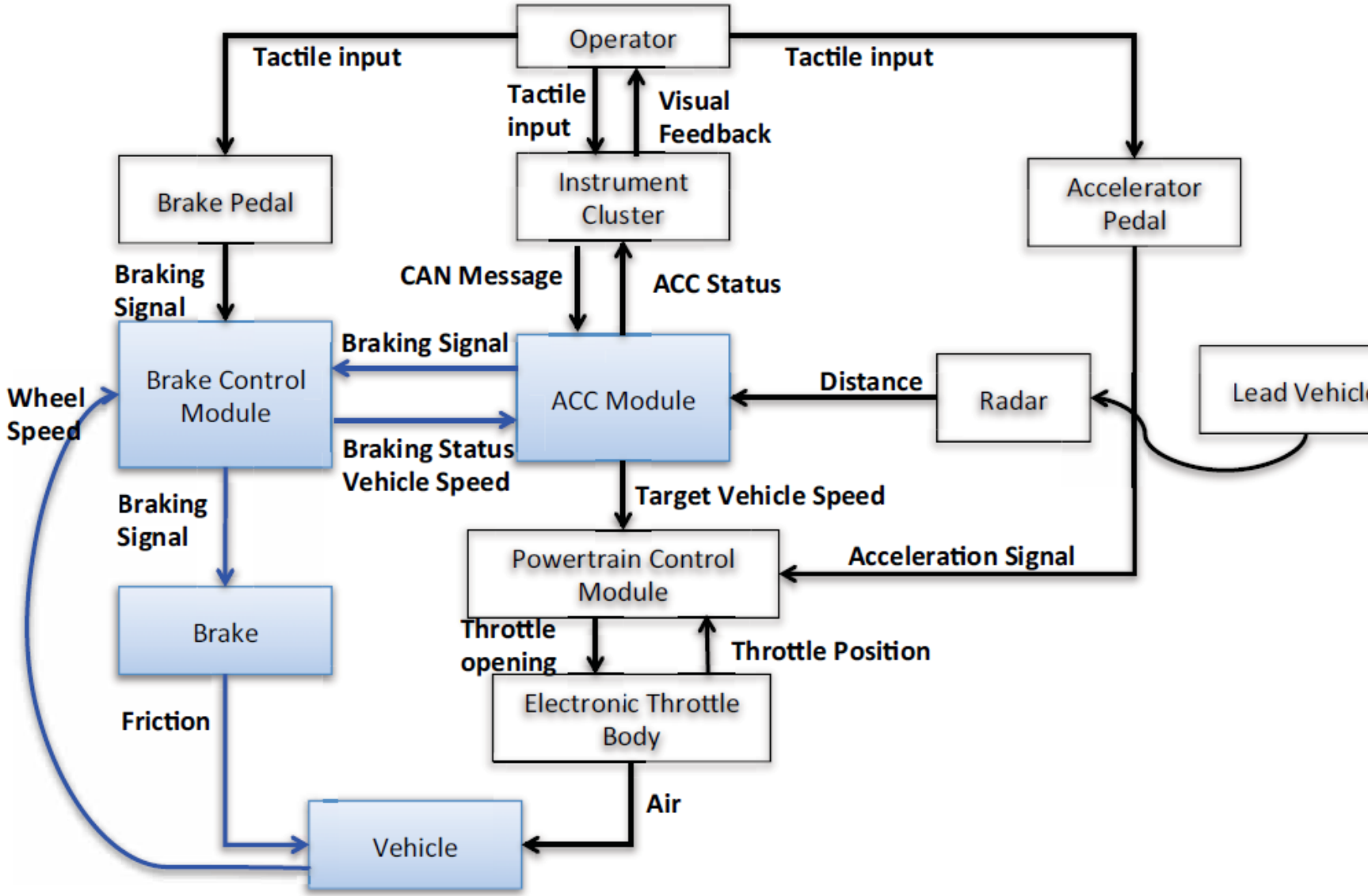


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

Example: ACC – BCM Control Loop



Chemical Plant

Image from: http://www.cbgnetwork.org/2608.html

Chemical Plant

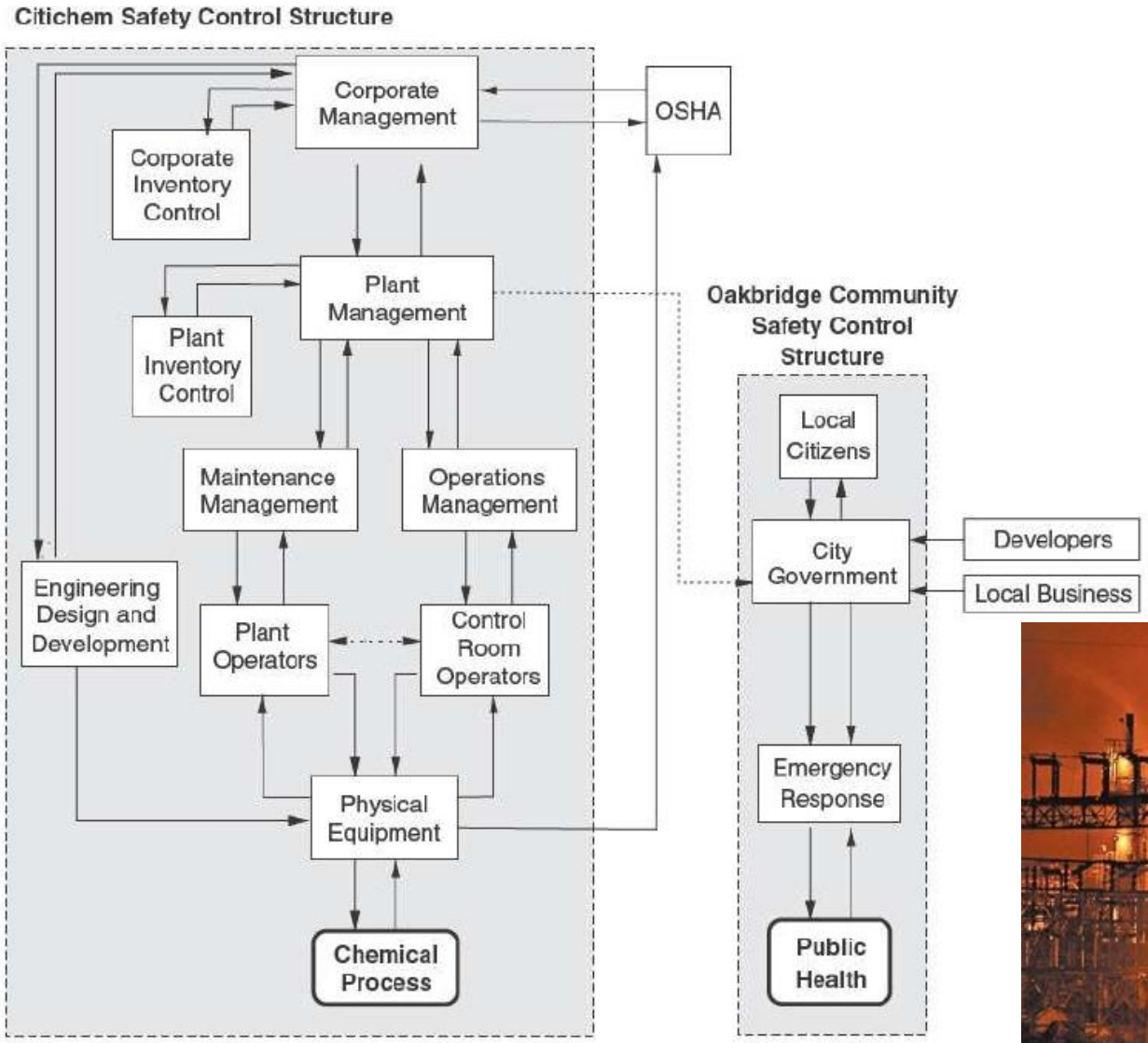
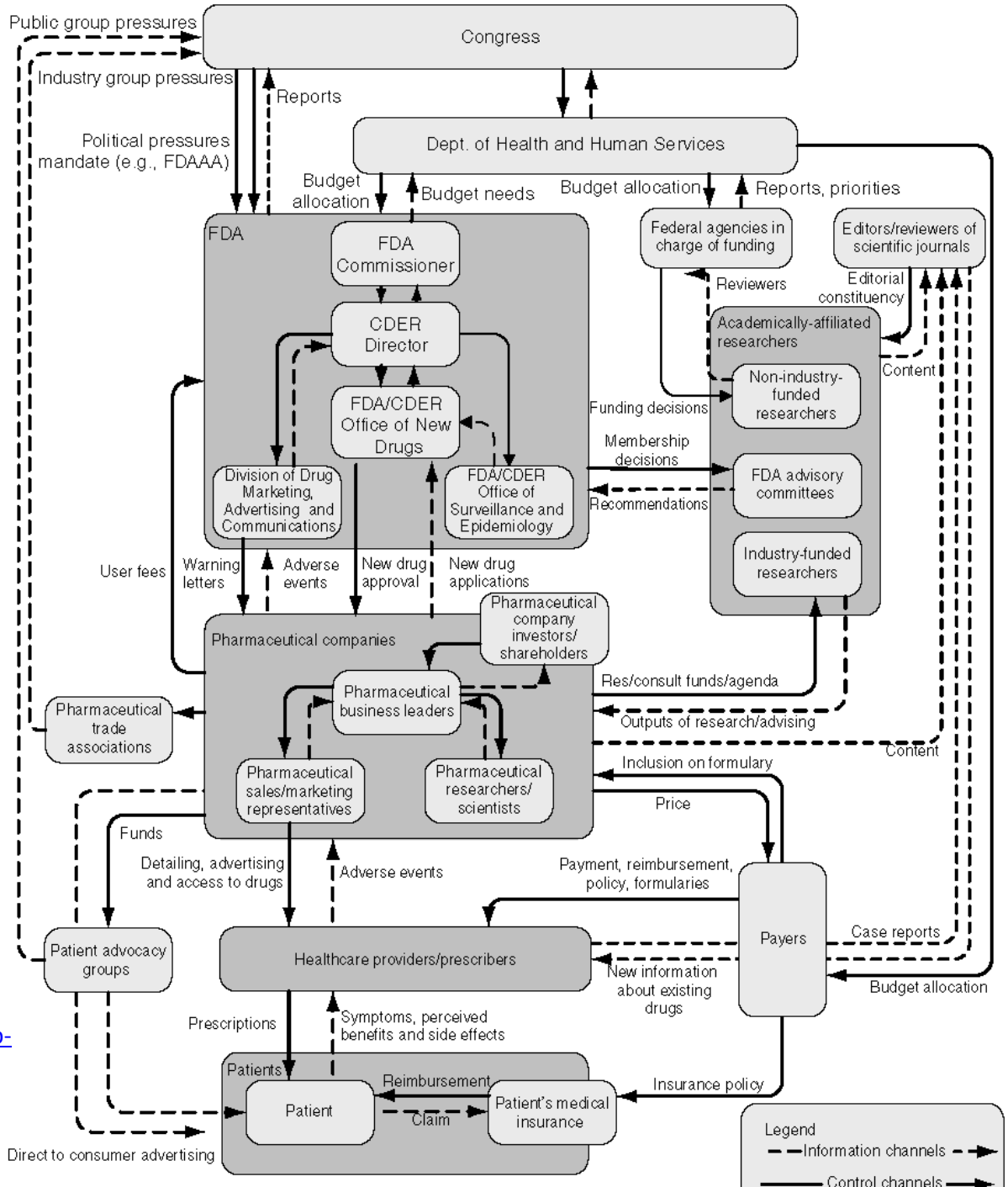


Image from:
http://www.cbgnetwork.org/2608.html

ESW p354

U.S. pharmaceutical safety control structure

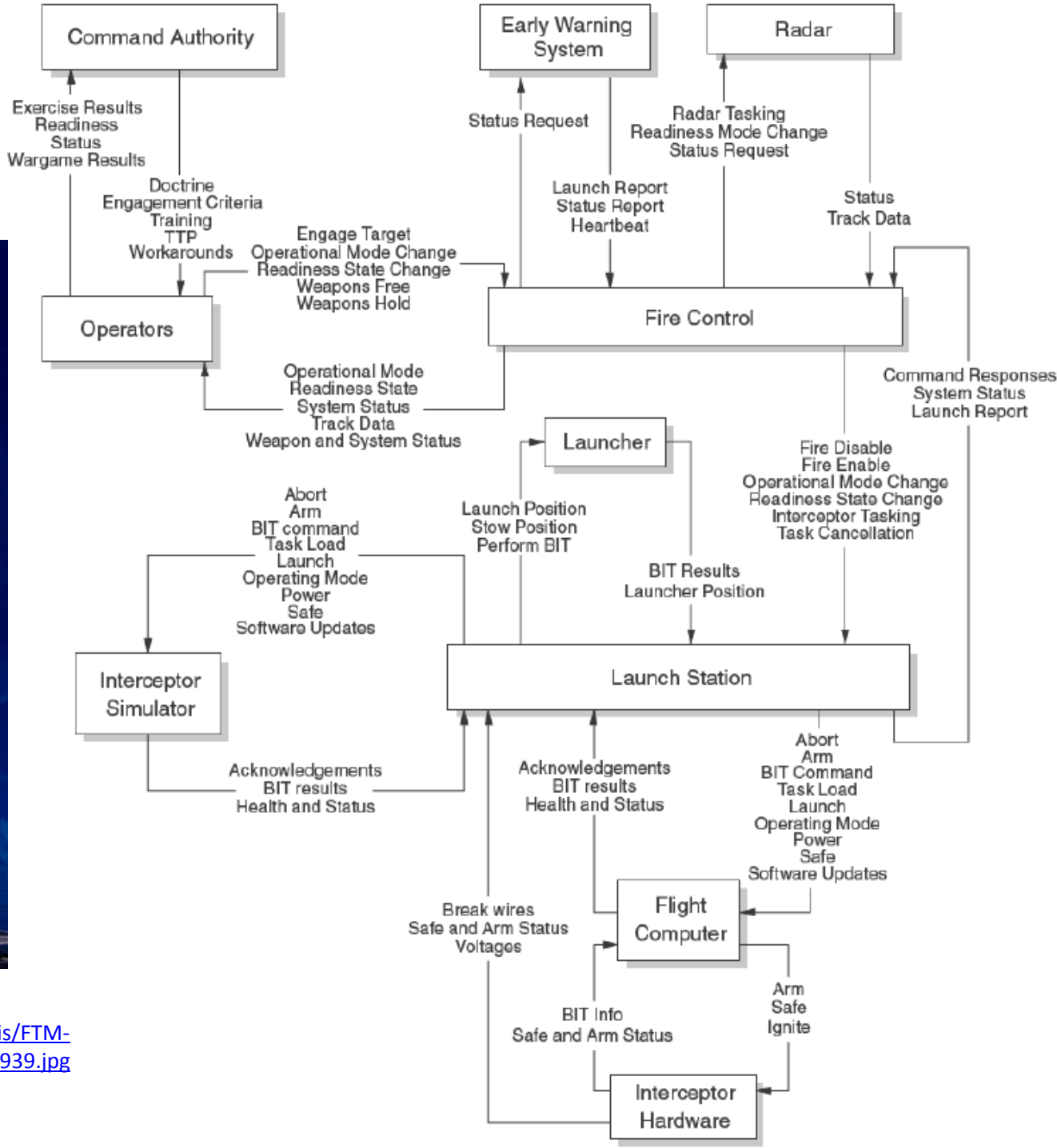
Image from: http://www.kleantreatmentcenter.com/wp-content/uploads/2012/07/vioxx.jpeg



Ballistic Missile Defense System

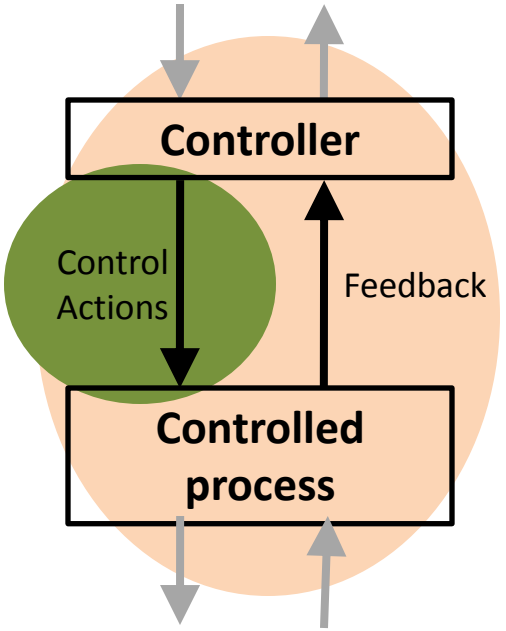
Image from:
http://www.mda.mil/global/images/system/aegis/FTM-21_Missile%201_Bulkhead%20Center14_BN4H0939.jpg

Safeware Corporation



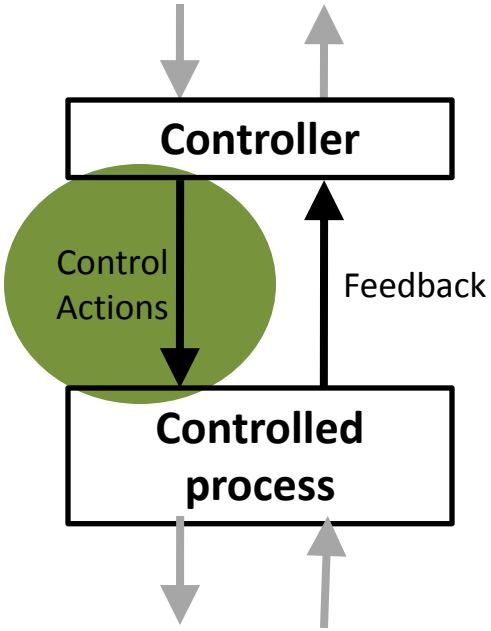
STPA
(System-Theoretic Process Analysis)

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



(Leveson, 2012)

STPA Step 1: Unsafe Control Actions (UCA)



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

Step 1: Identify Unsafe Control Actions

(a more rigorous approach)

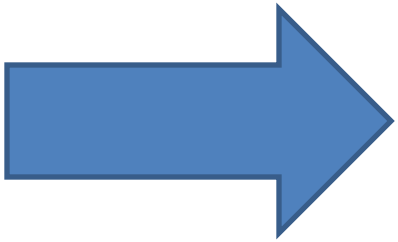
Control Action	Process Model Variable 1	Process Model Variable 2	Process Model Variable 3	Hazardous?

STPA
(System-Theoretic Process Analysis)

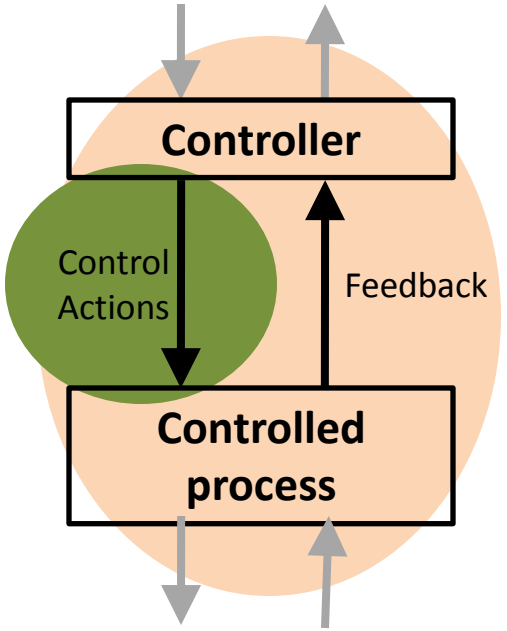
- Identify accidents and hazards

- Construct the control structure

- Step 1: Identify unsafe control actions

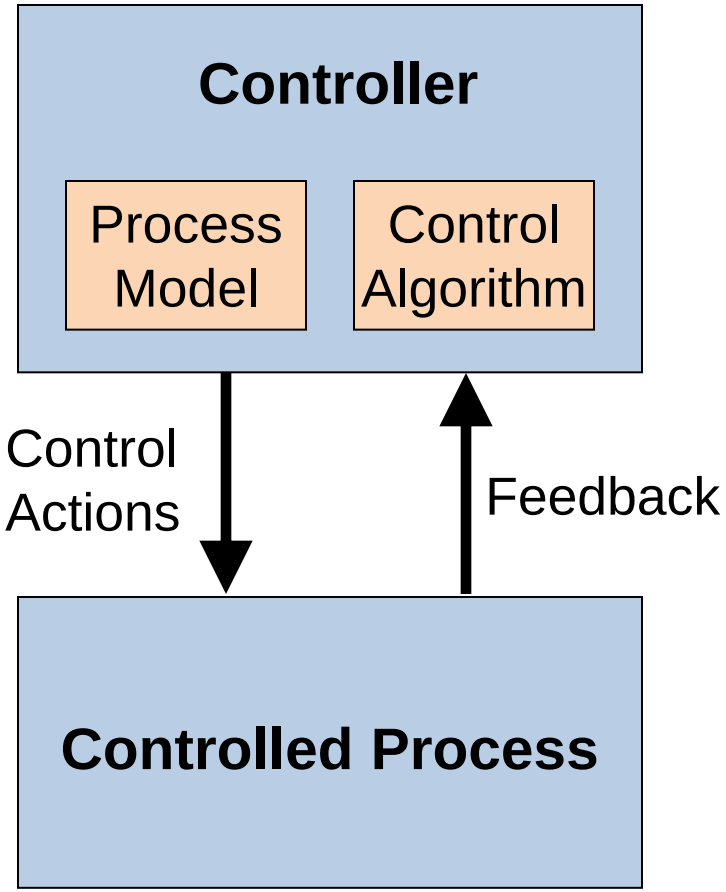


- Step 2: Identify causal factors and control flaws



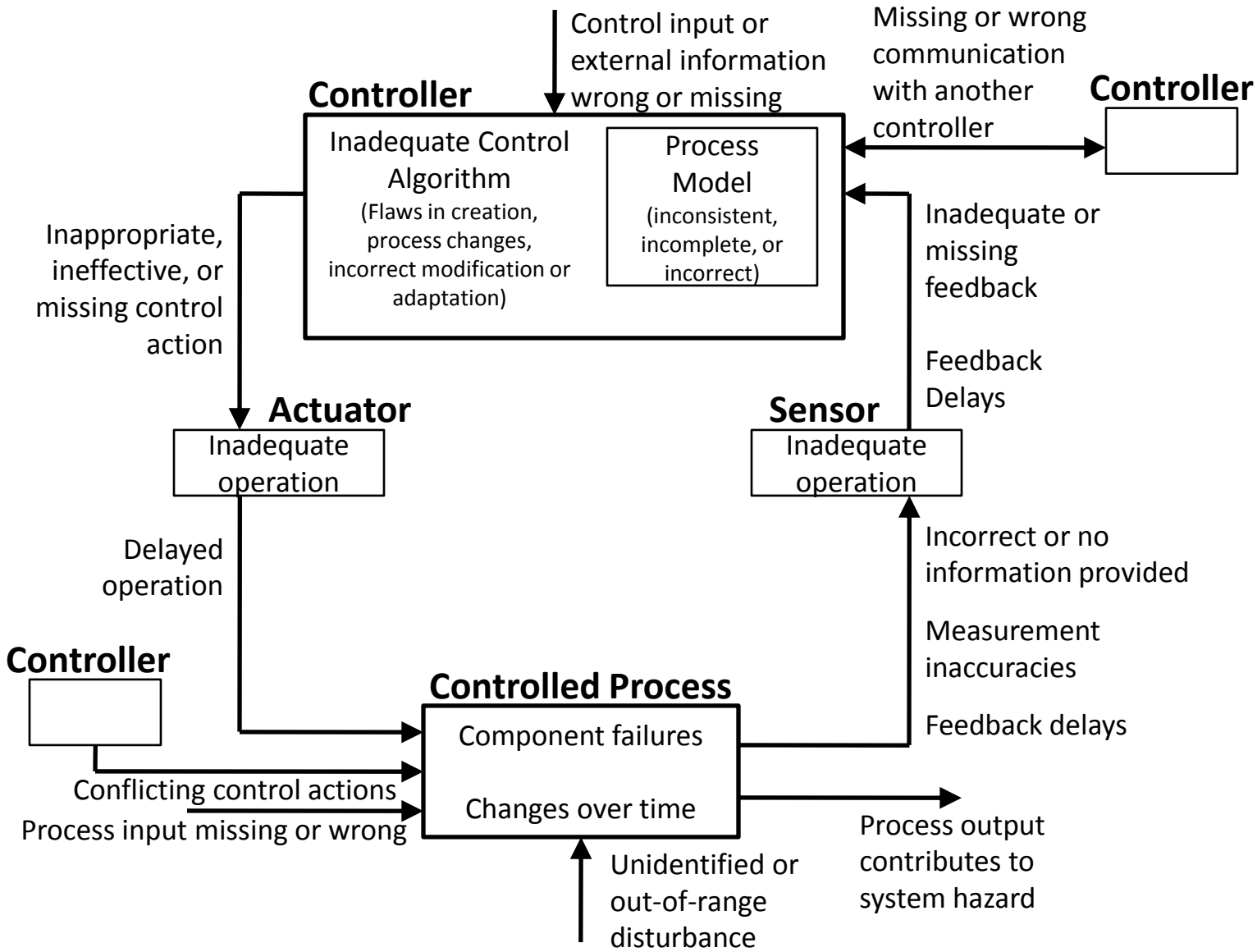
(Leveson, 2012)

System Theoretic Process Analysis



- Explain *why* and *how* UCAs may occur
- Control actions are based on:
  - Process model
  - Control algorithm
  - Feedback
- Flaws?

STPA Step 2: Identify Control Flaws



STPA Examples

ITP 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 providing causes hazard, Providing causes hazard, Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Example System: Aviation

System-level Accident (Loss): ?

Example System: Aviation

System-level Accident (Loss): Two aircraft collide

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

System-level Accident (Loss): Aircraft crashes

System-level Hazard: Two aircraft violate minimum separation

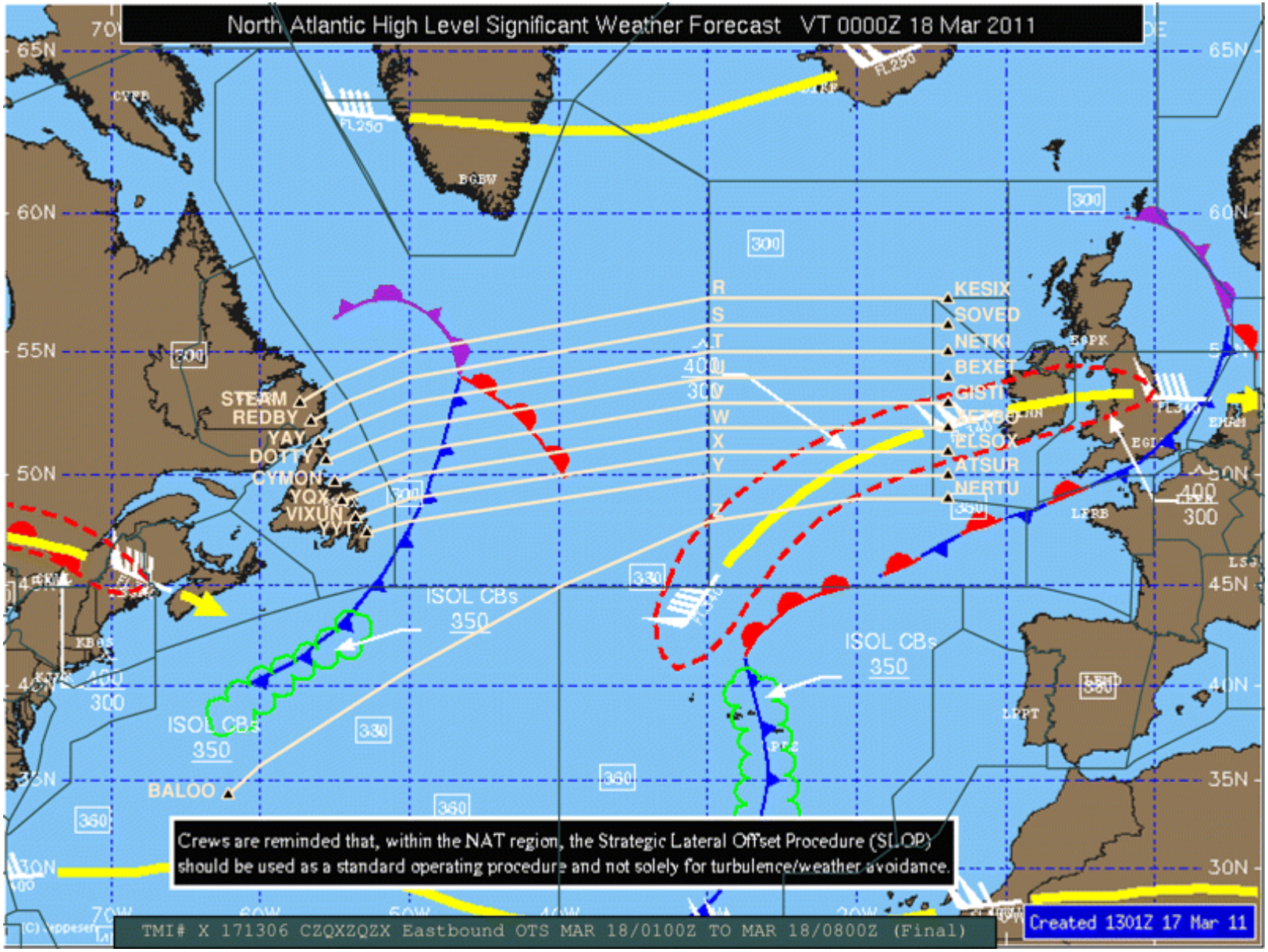
Aviation Examples

- 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

STPA Exercise

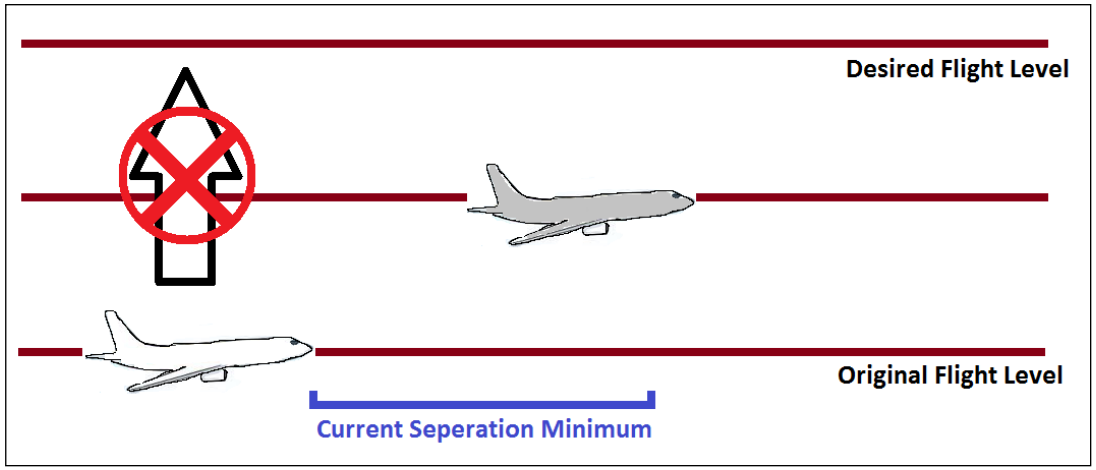
- ✓ Identify accidents and hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not providing causes hazard, Providing causes hazard, Wrong timing, Stopped too soon
  -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

North Atlantic Tracks



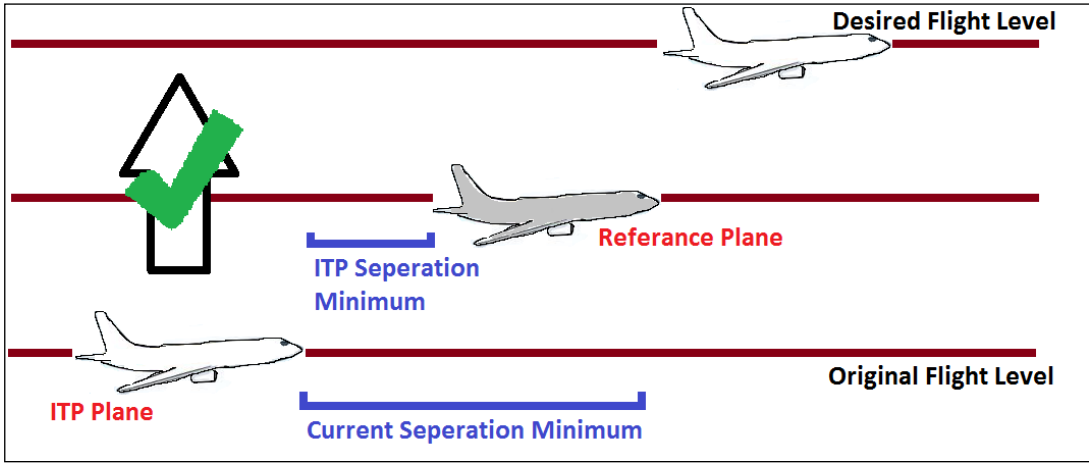
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



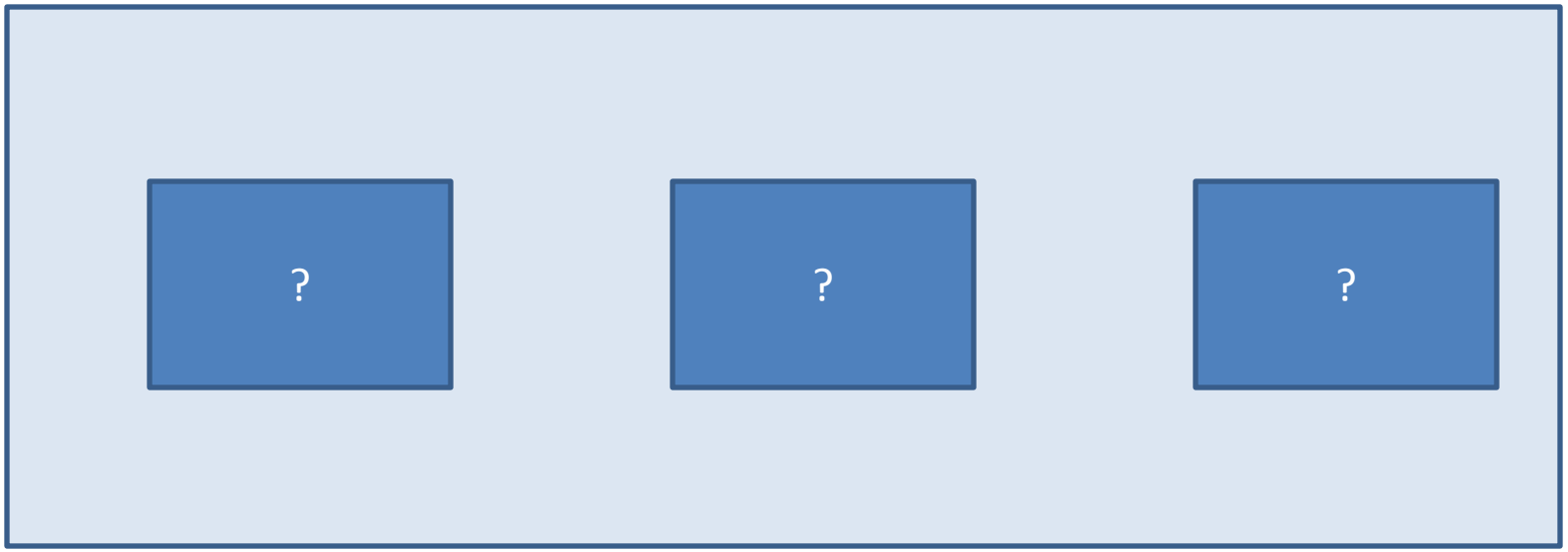
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



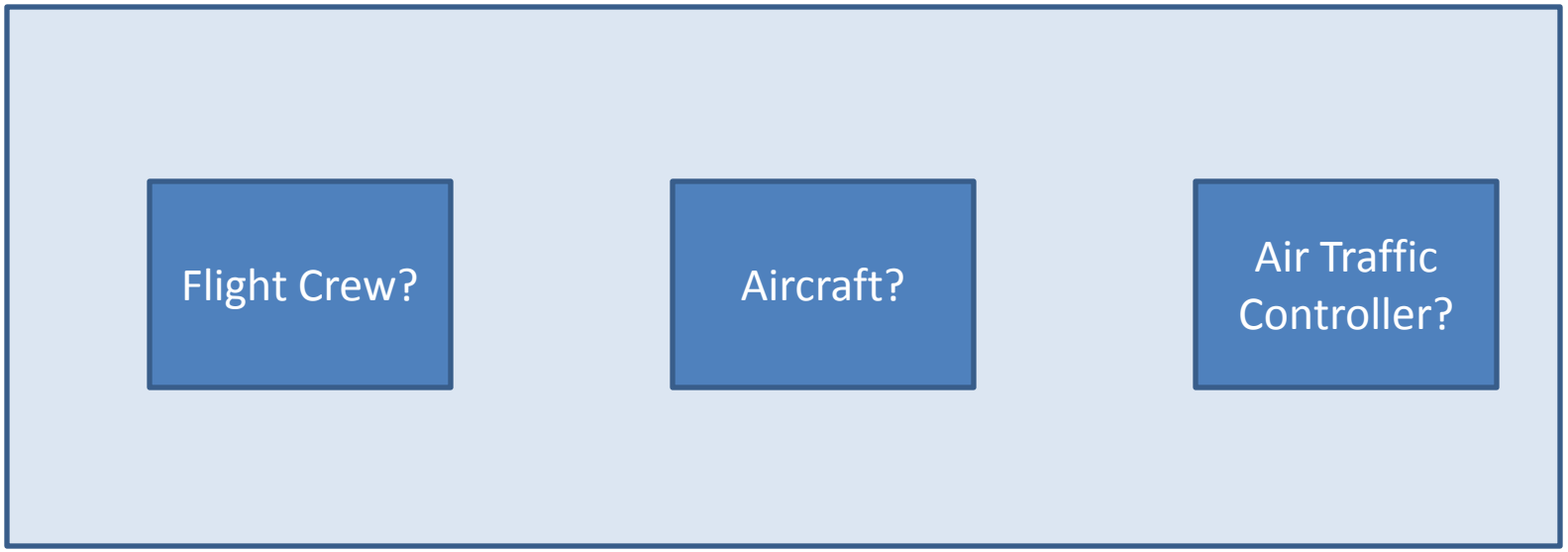
STPA Analysis

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



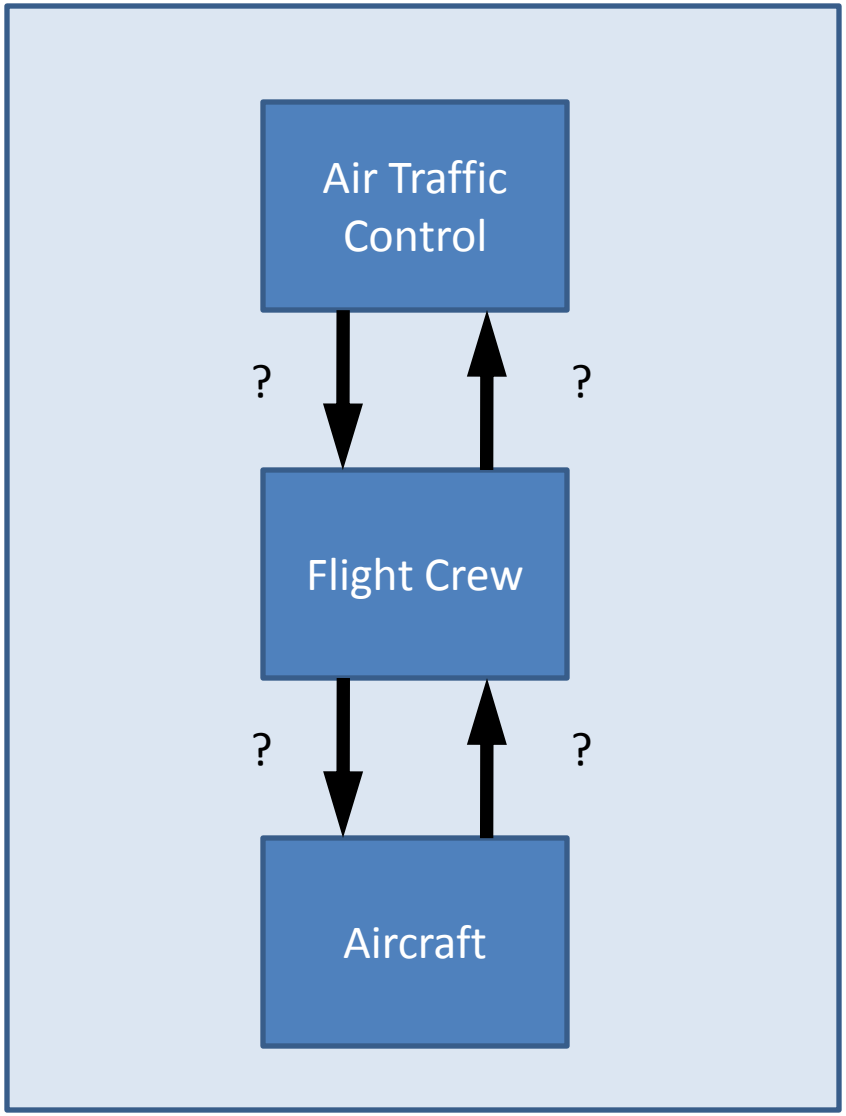
STPA Analysis

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



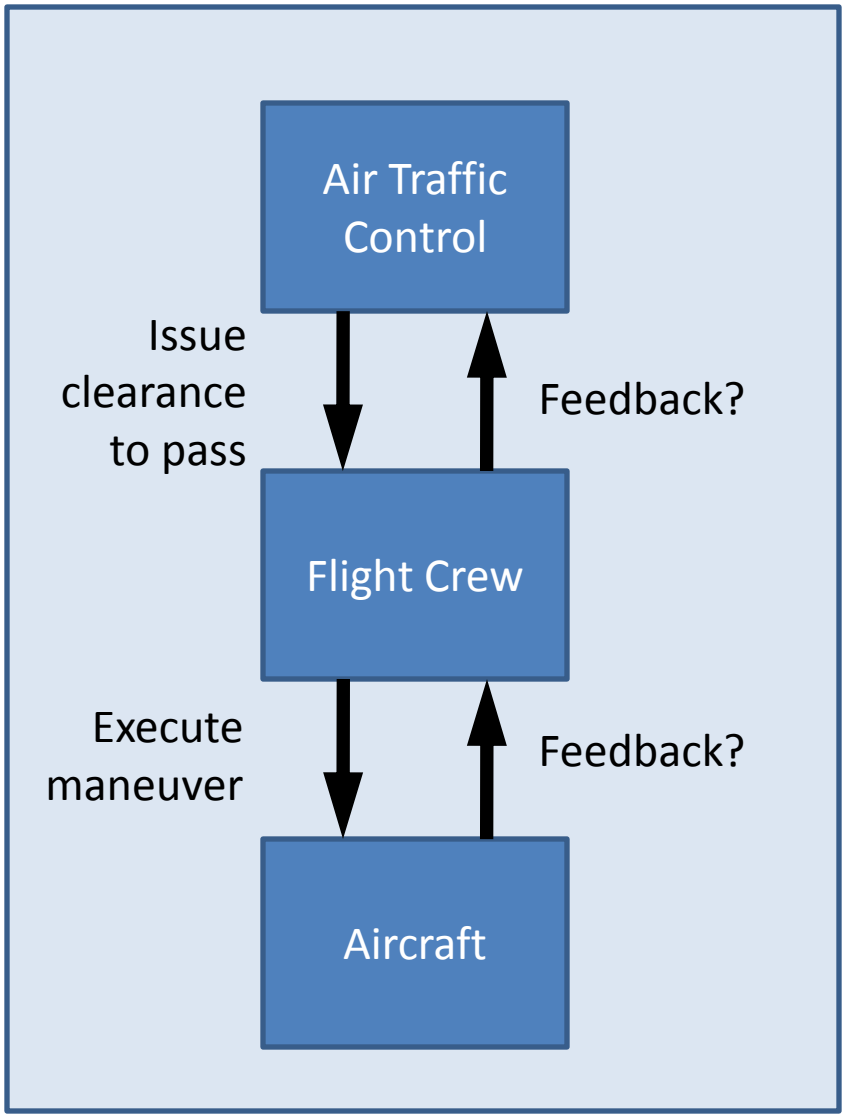
STPA Analysis

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



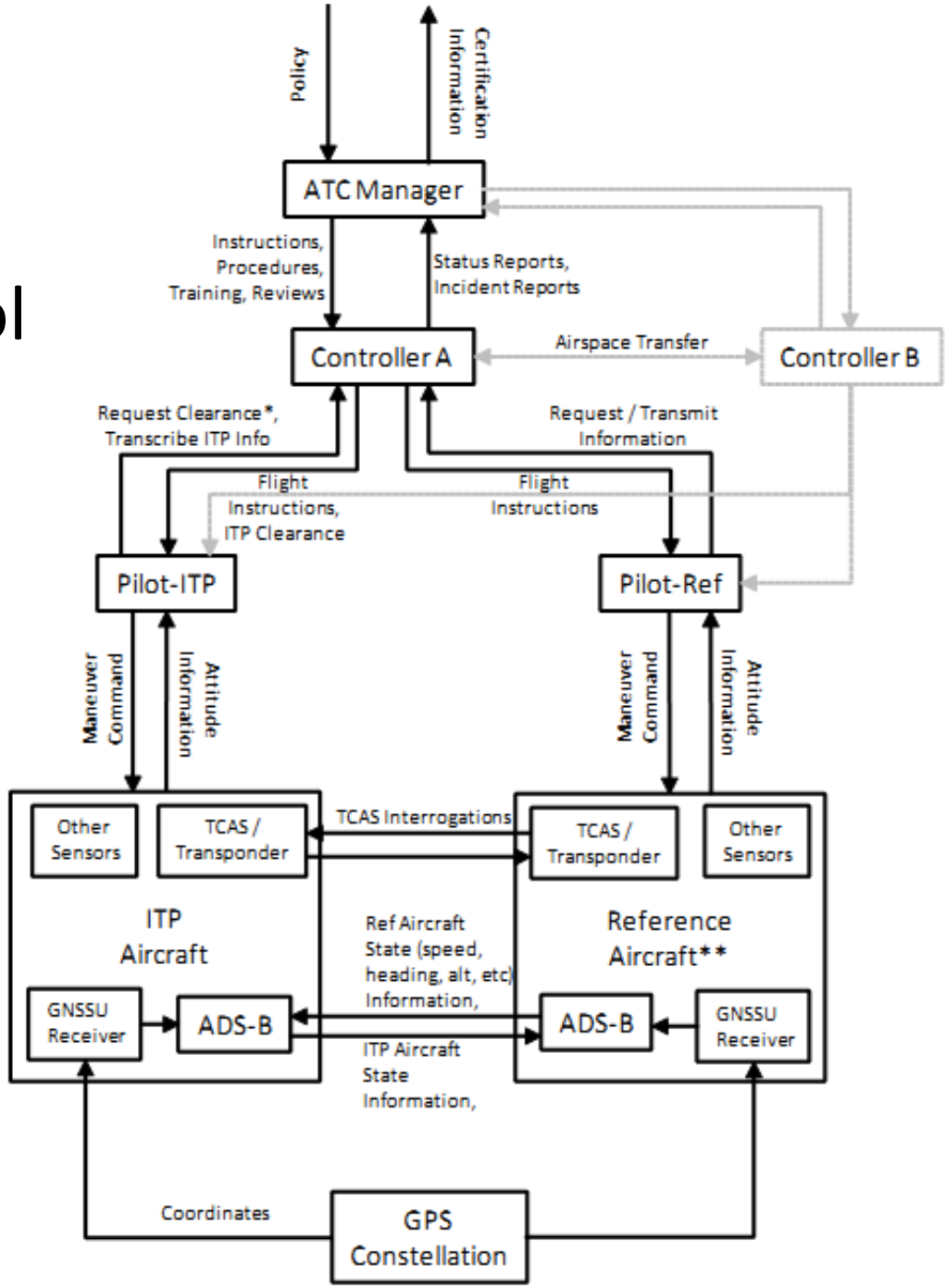
STPA Analysis

- High-level (simple) Control Structure

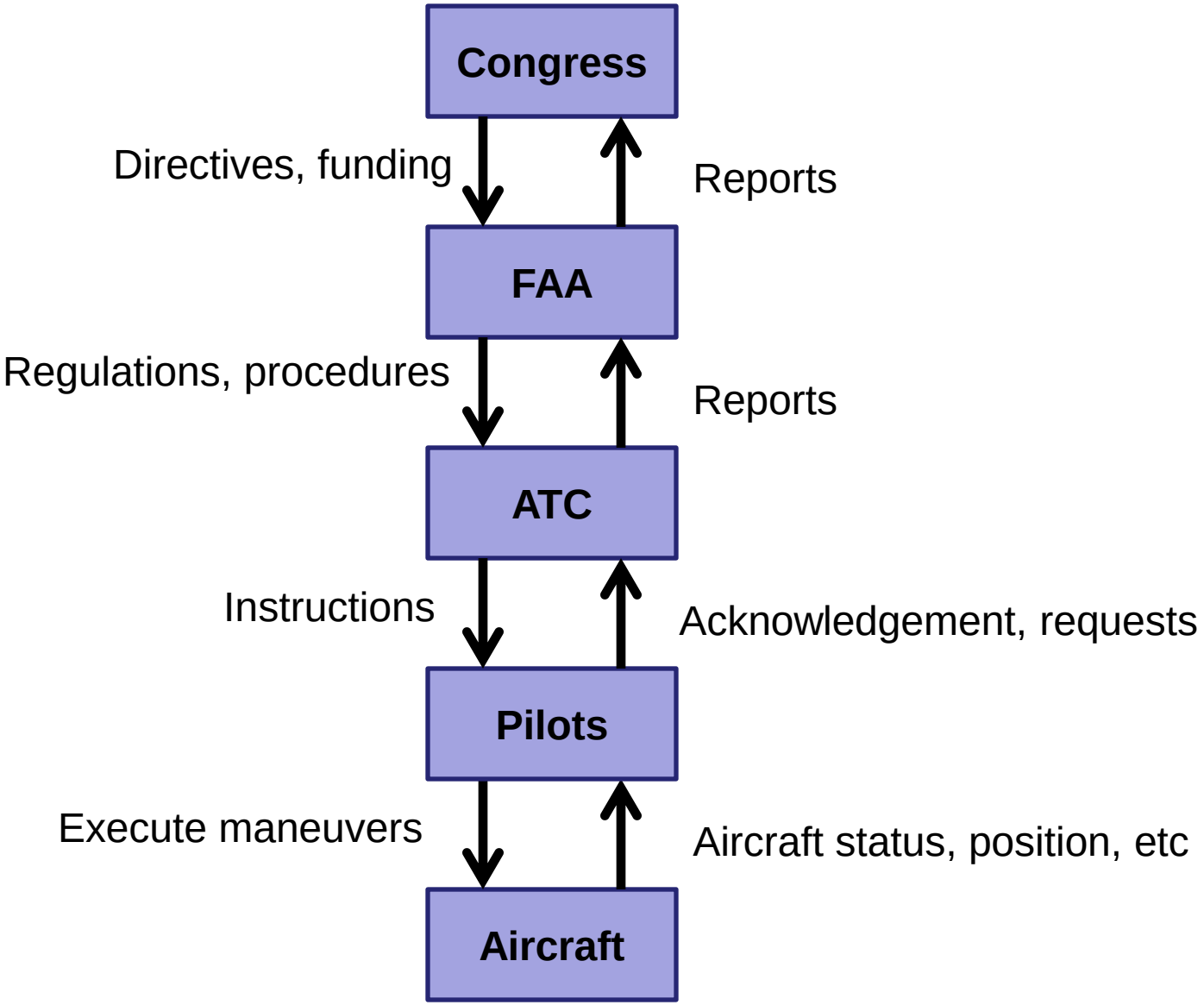


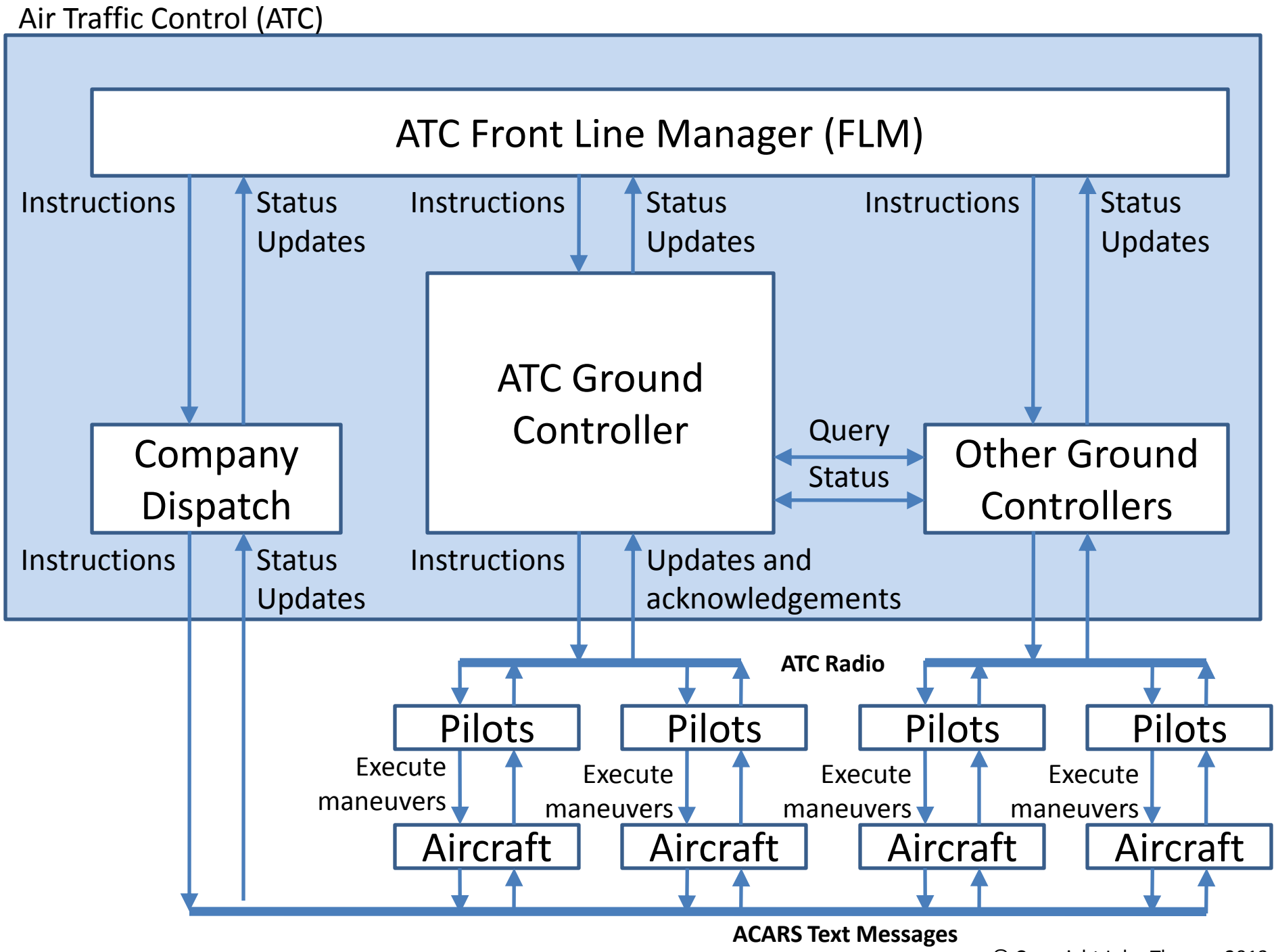
STPA Analysis

- More complex control structure



Example High-level control structure

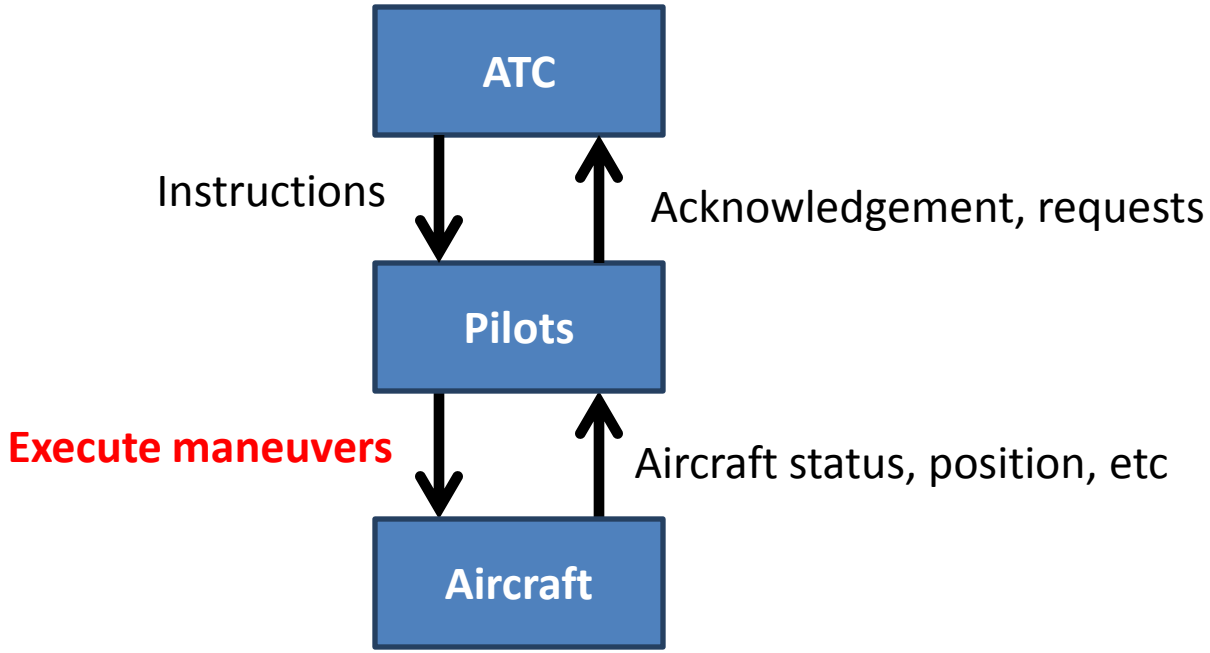




STPA Exercise

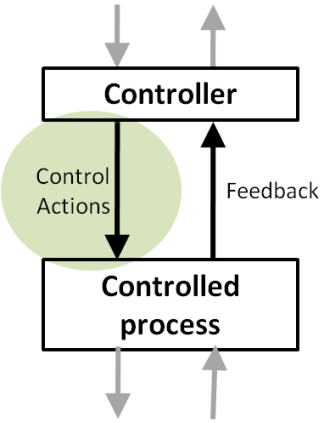
- ✓ Identify accidents and hazards
- ✓ Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not providing causes hazard, Providing causes hazard, Wrong timing, Stopped too soon
 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

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		

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)

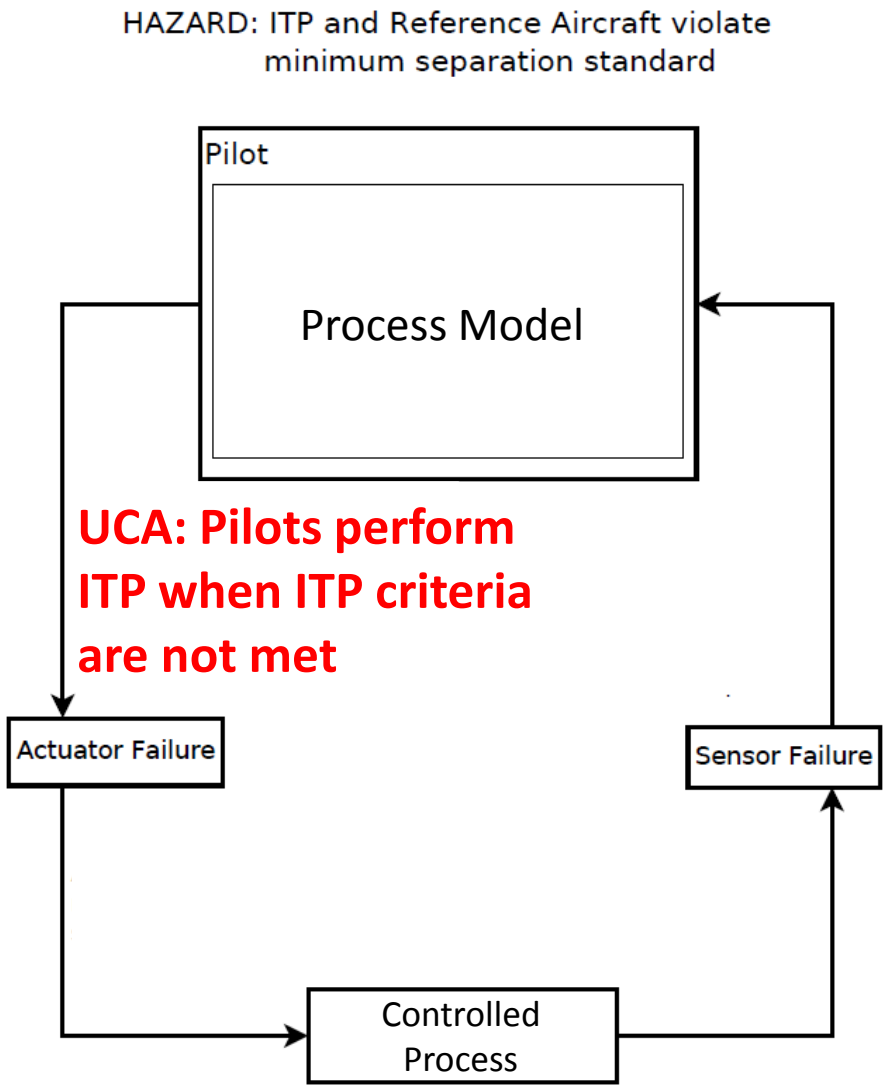
Defining Safety Constraints

Unsafe Control Action	Safety Constraint
Pilot 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

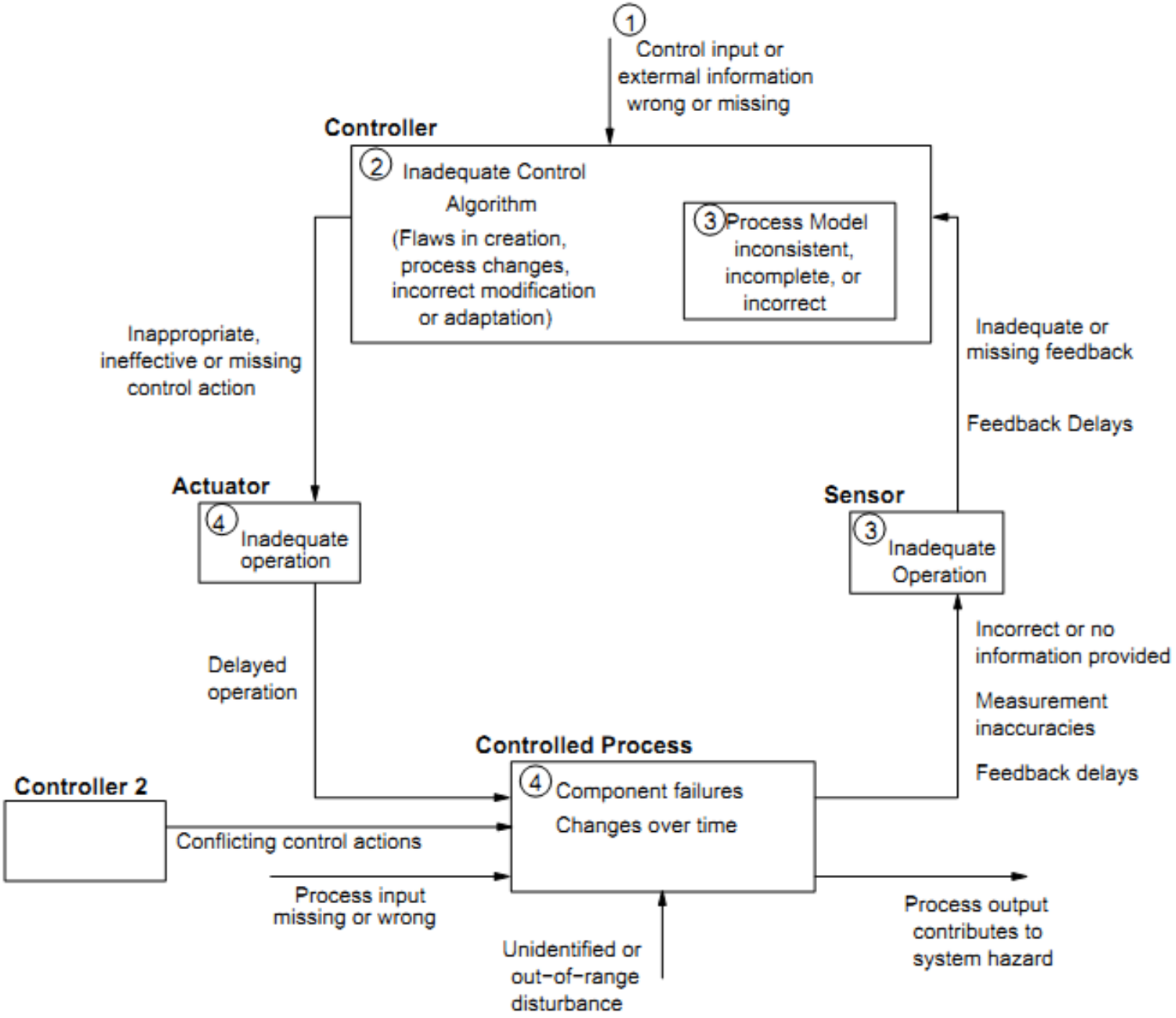
- ✓ Identify accidents and hazards
- ✓ Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- ✓ Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not providing causes hazard, Providing causes hazard, Wrong timing, Stopped too soon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

STPA Analysis: Causal Factors

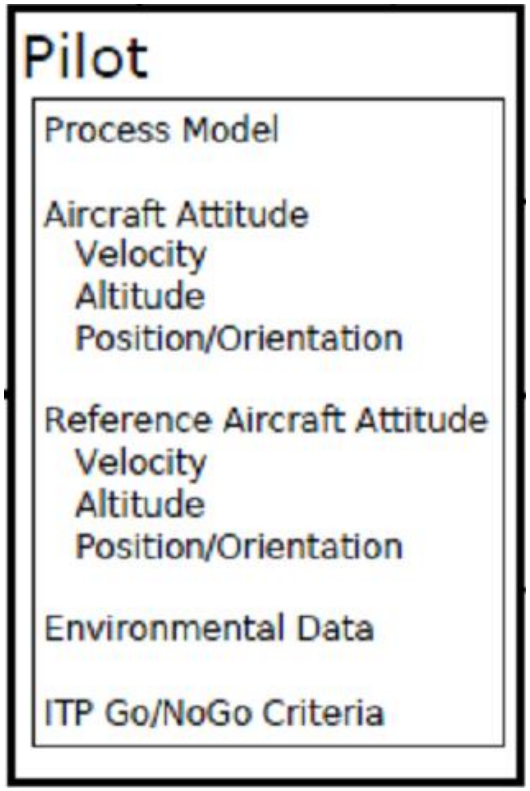


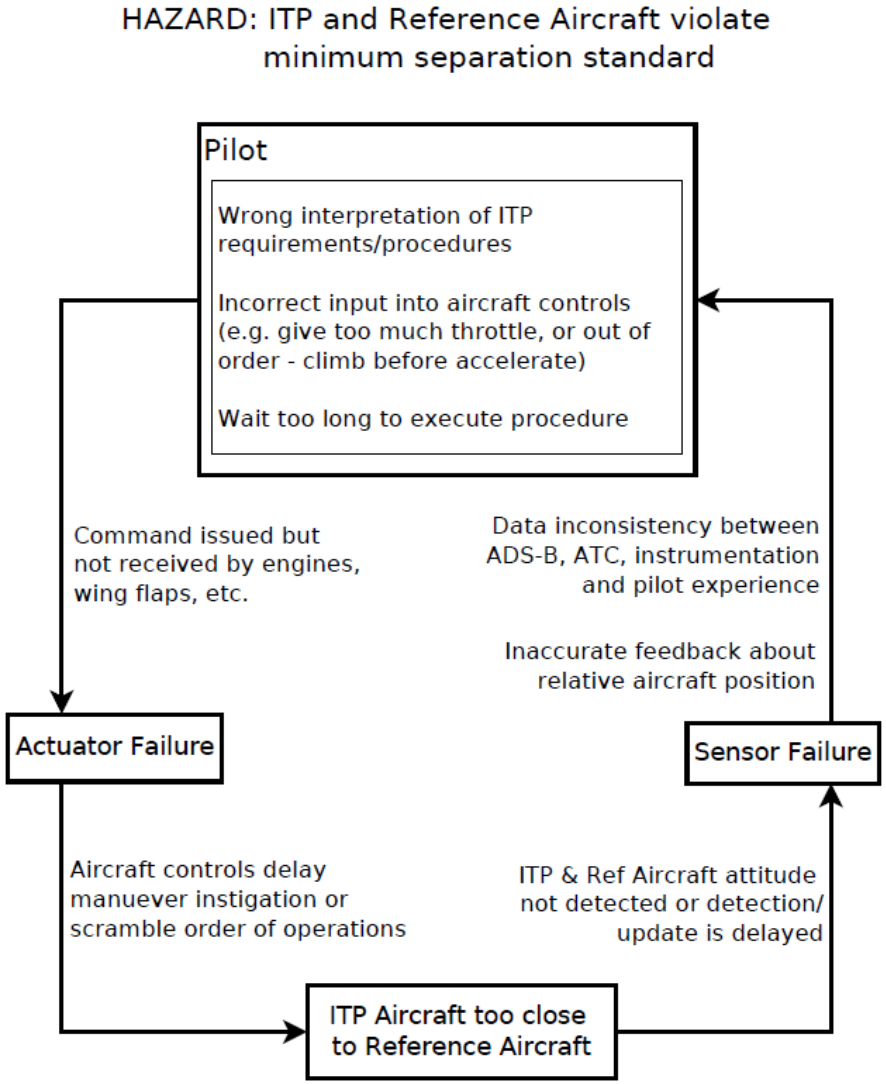
- How could this action be caused by:
  - Process model
  - Feedback
  - Sensors
  - Etc?
- Also consider control action not followed

Hint: Causal Factors



STPA Analysis: Causal Factors



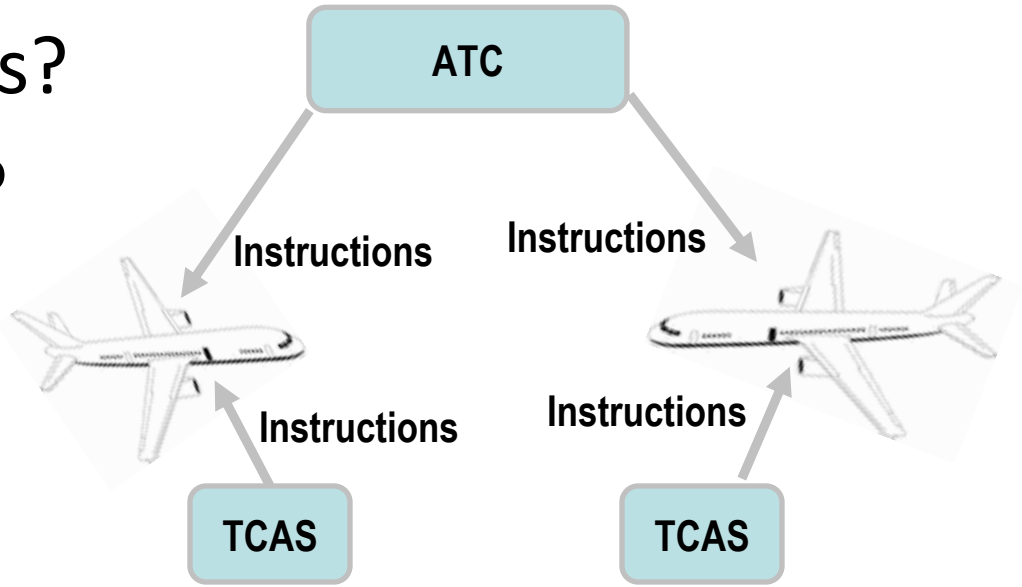


Traffic Collision Avoidance System (TCAS)

Traffic Collision Avoidance System (TCAS)

- Monitors airspace around aircraft
- Can provide advisories to warn pilot of potential collision

- System-level Accidents?
- System-level Hazards?



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

Traffic Collision Avoidance System (TCAS)

- Aircraft Accident: Two or more aircraft collide
- Aircraft Hazard: Near Mid Air Collision (NMAC)
- TCAS Hazard: TCAS causes or does not prevent NMAC

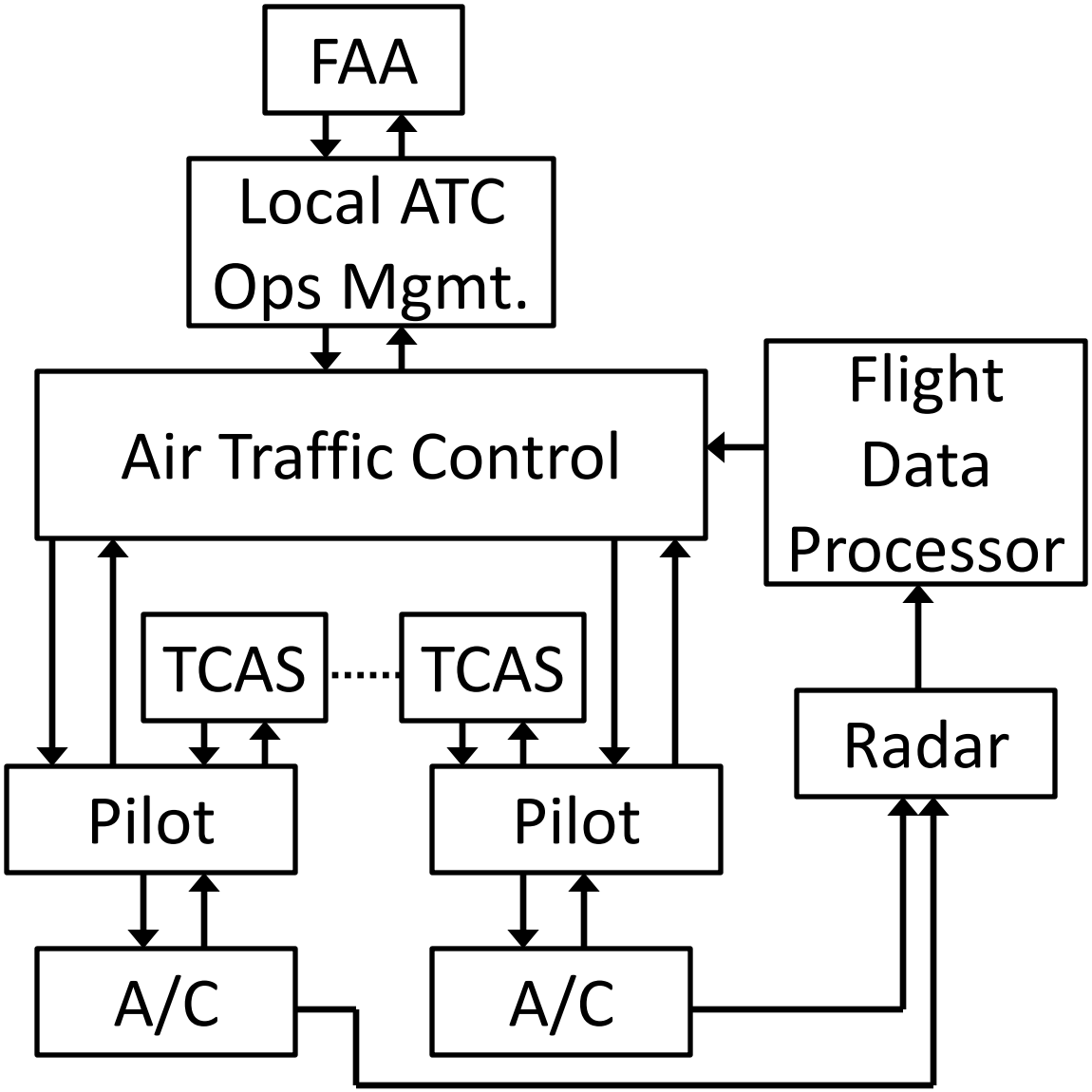
Traffic Collision Avoidance System (TCAS)

- Monitors airspace around aircraft
- Can provide advisories to warn pilot of potential collision

Create control structure

Traffic Collision Avoidance System (TCAS)

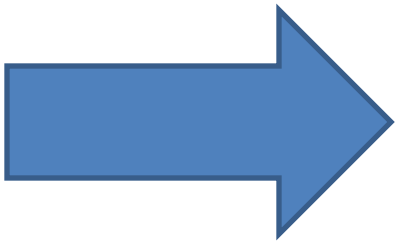
Example Control Structure:



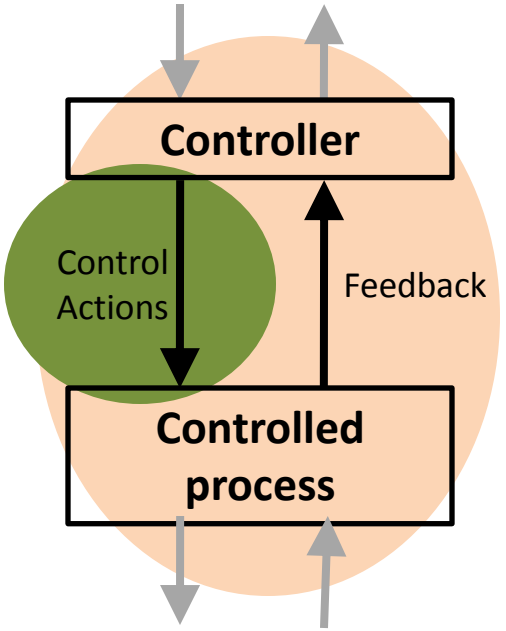
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards

- Construct the control structure



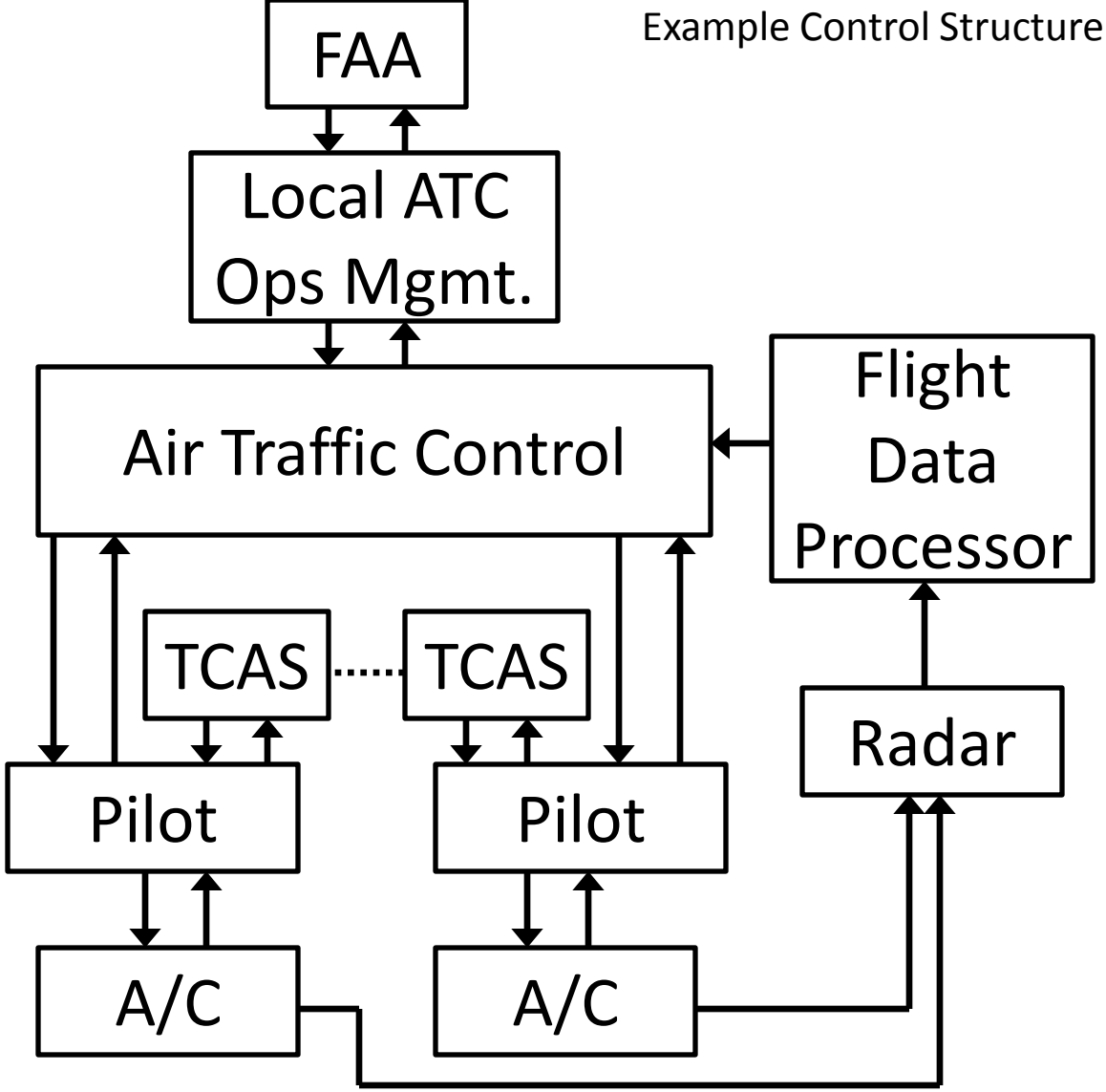
- **Step 1: Identify unsafe control actions**
- **Step 2: Identify causal factors and control flaws**



(Leveson, 2012)

TCAS

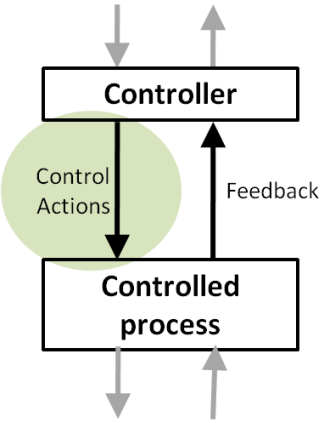
Example Control Structure



Identify Unsafe Control Actions

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Resolution Advisory (RA)	**TCAS does not provide an RA when collision imminent**			

Structure of a Hazardous Control Action



Example:
"TCAS does not provide RA when collision imminent"

Source Controller (SC)

Type (T)

Control Action (CA)

Context (Co)

Four parts of a hazardous control action

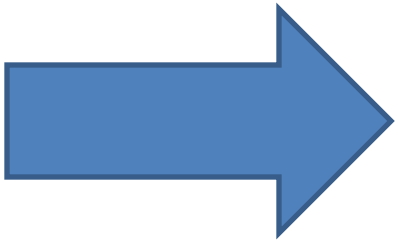
- Source Controller: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command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

STPA
(System-Theoretic Process Analysis)

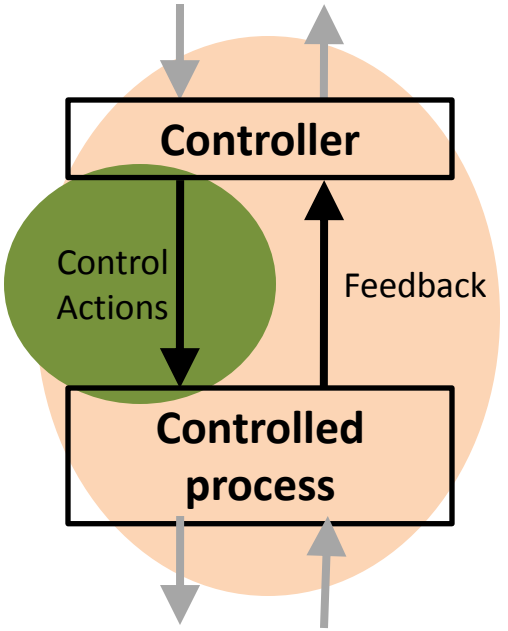
- Identify accidents and hazards

- Construct the control structure

- Step 1: Identify unsafe control actions



- Step 2: Identify causal factors and control flaws



(Leveson, 2012)

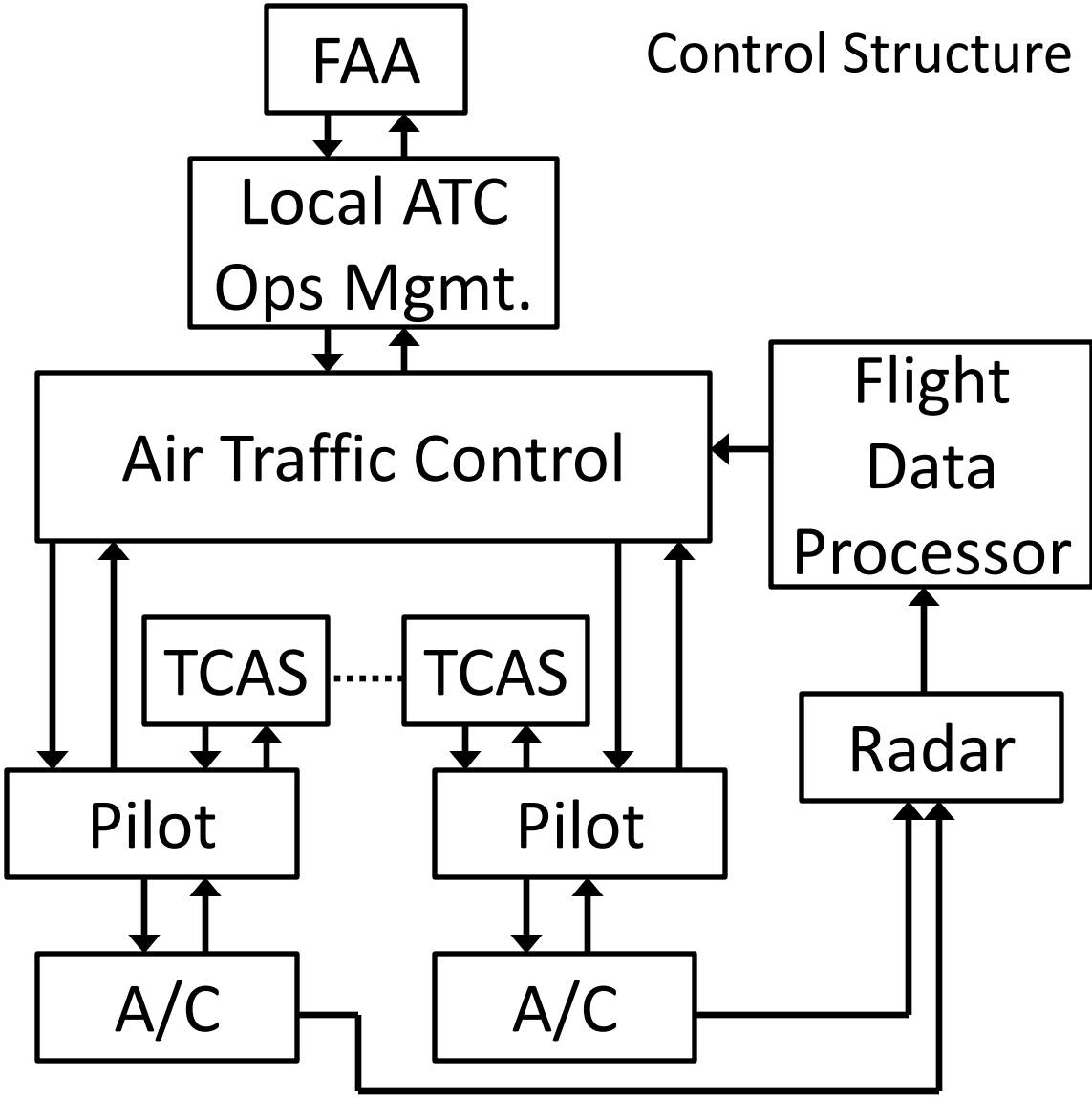
TCAS

Control Structure

UCA1: TCAS does not provide an RA when collision imminent

SC1: TCAS must always provide necessary RA to prevent imminent NMAC (<25 sec to collision)

- What might violate this safety constraint?
  - Process model flaws?
  - Control algorithm flaws?
  - Poor feedback?
  - Component failures?

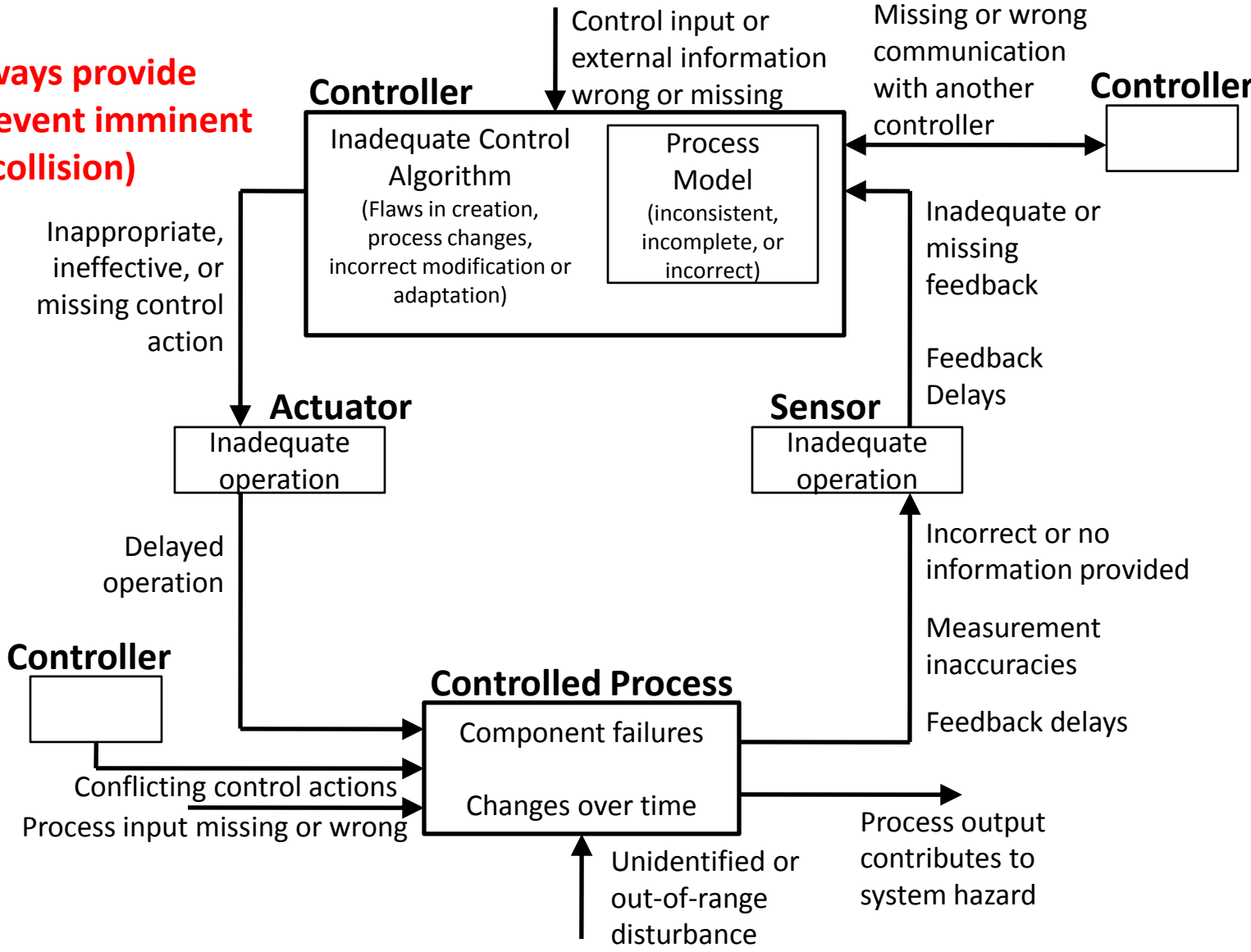


Identify Causal Factors

STPA Step 2: Identify Control Flaws

UCA1: TCAS does not provide an RA when collision imminent

SC1: TCAS must always provide necessary RA to prevent imminent NMAC (<25 sec to collision)



STPA Primer

- Written for industry to provide guidance in learning STPA
  - Not a book or academic paper
  - “living” document
  - Google “STPA Primer”

Group Exercise:
JAXA H-II Transfer Vehicle (HTV)