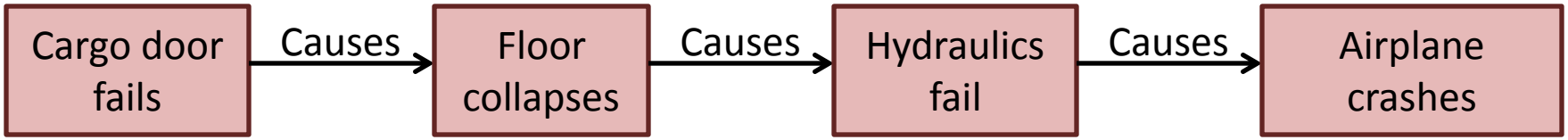
Systems Theoretic Process Analysis (STPA) Tutorial

Dr. John Thomas
Massachusetts Institute of Technology

Domino “Chain of events” Model

DC-10:



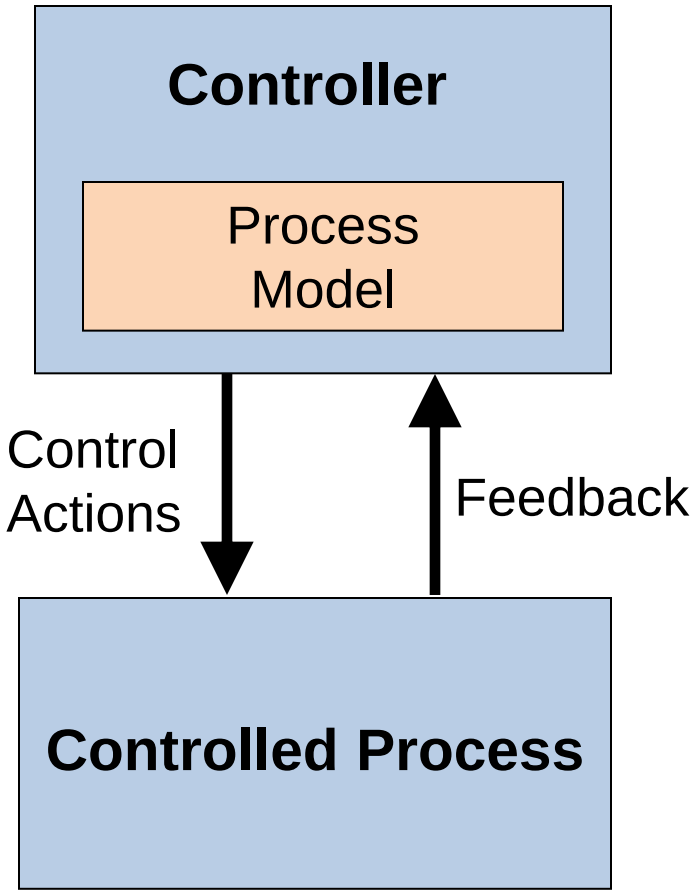
Event-based

Systems approach to safety engineering (STAMP)

STAMP Model

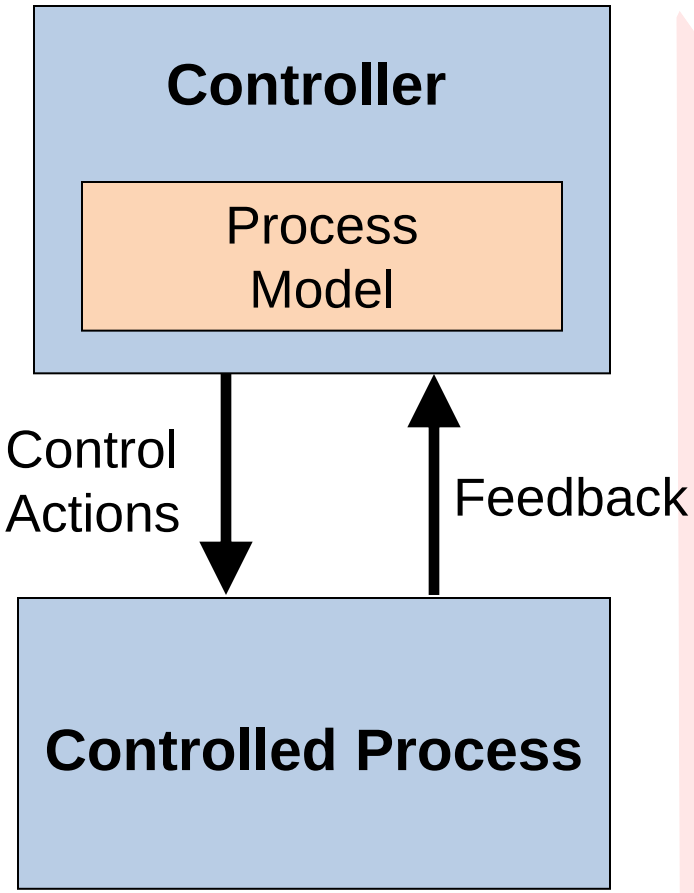
- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not a failure problem
- Prevent accidents by enforcing constraints on component behavior and **interactions**
- Captures more causes of accidents:
  - Component failure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

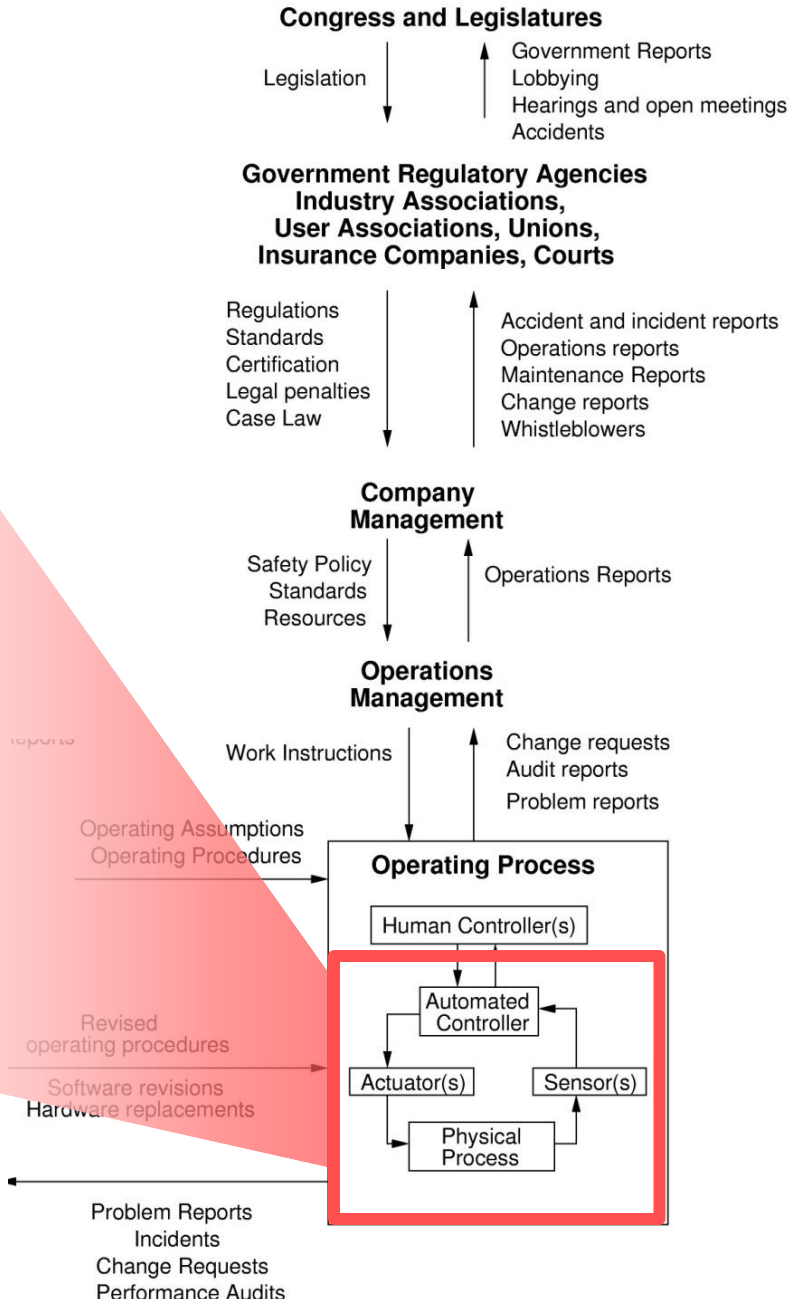
STAMP



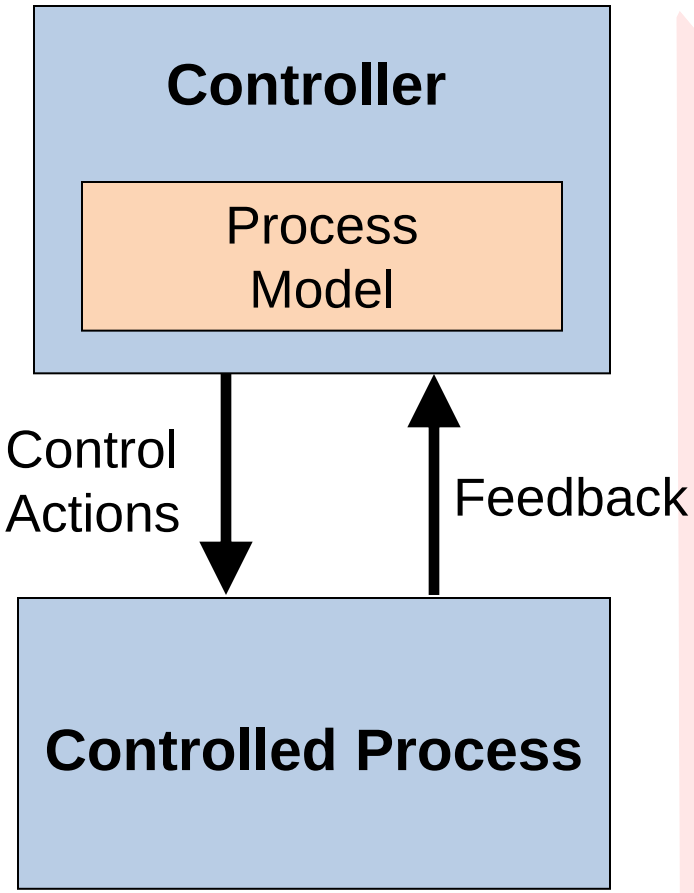
Tends to be a better model of software and human behavior than a failure-based model

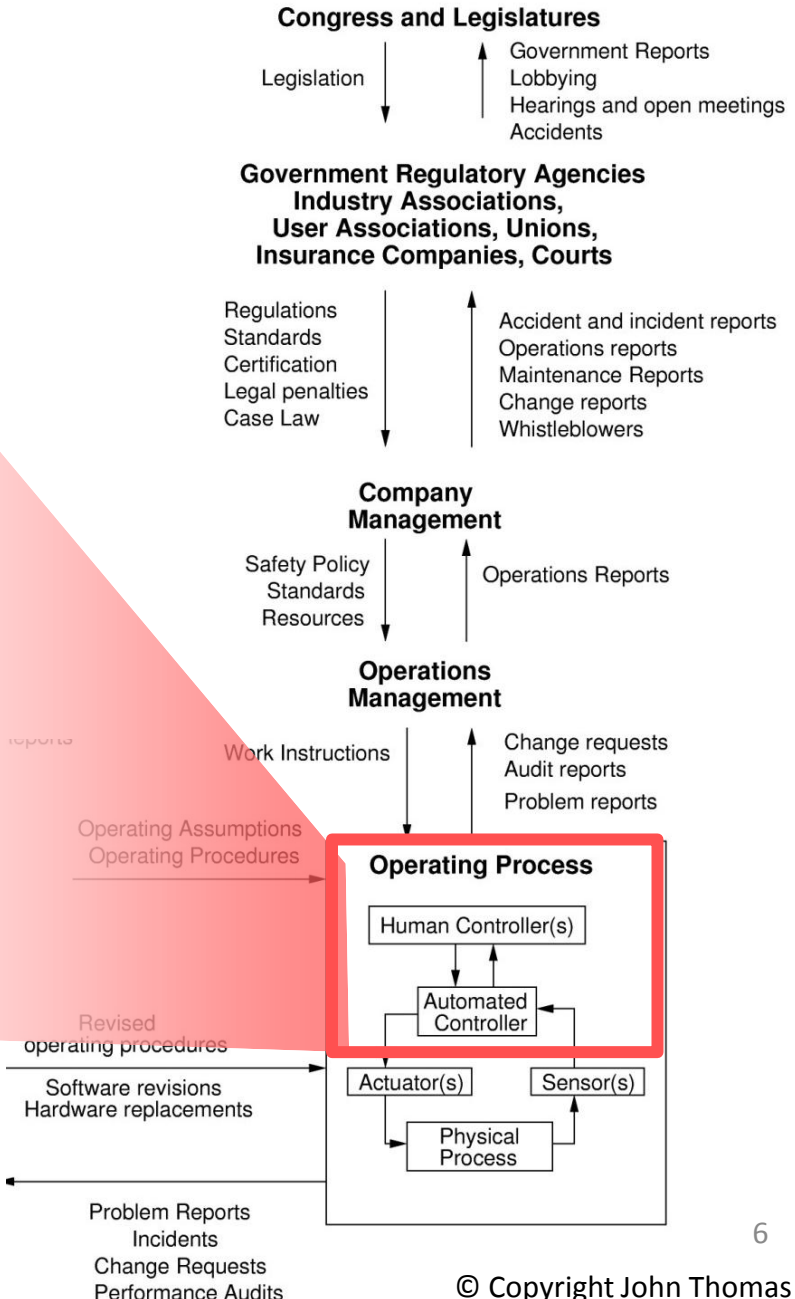
STAMP


Controller
Process Model
Control Actions
Feedback
Controlled Process

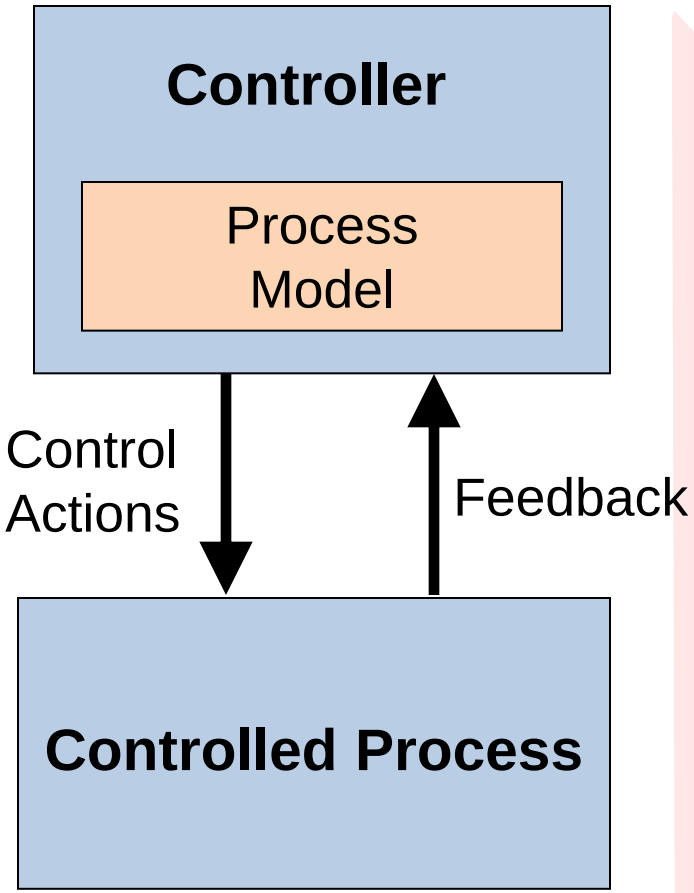

Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Legal penalties
Case Law
Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers
Company Management
Safety Policy
Standards
Resources
Operations Reports
Operations Management
Work Instructions
Change requests
Audit reports
Problem reports
Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated Controller
Actuator(s)
Sensor(s)
Physical Process
Revised operating procedures
Software revisions
Hardware replacements
Problem Reports
Incidents
Change Requests
Performance Audits

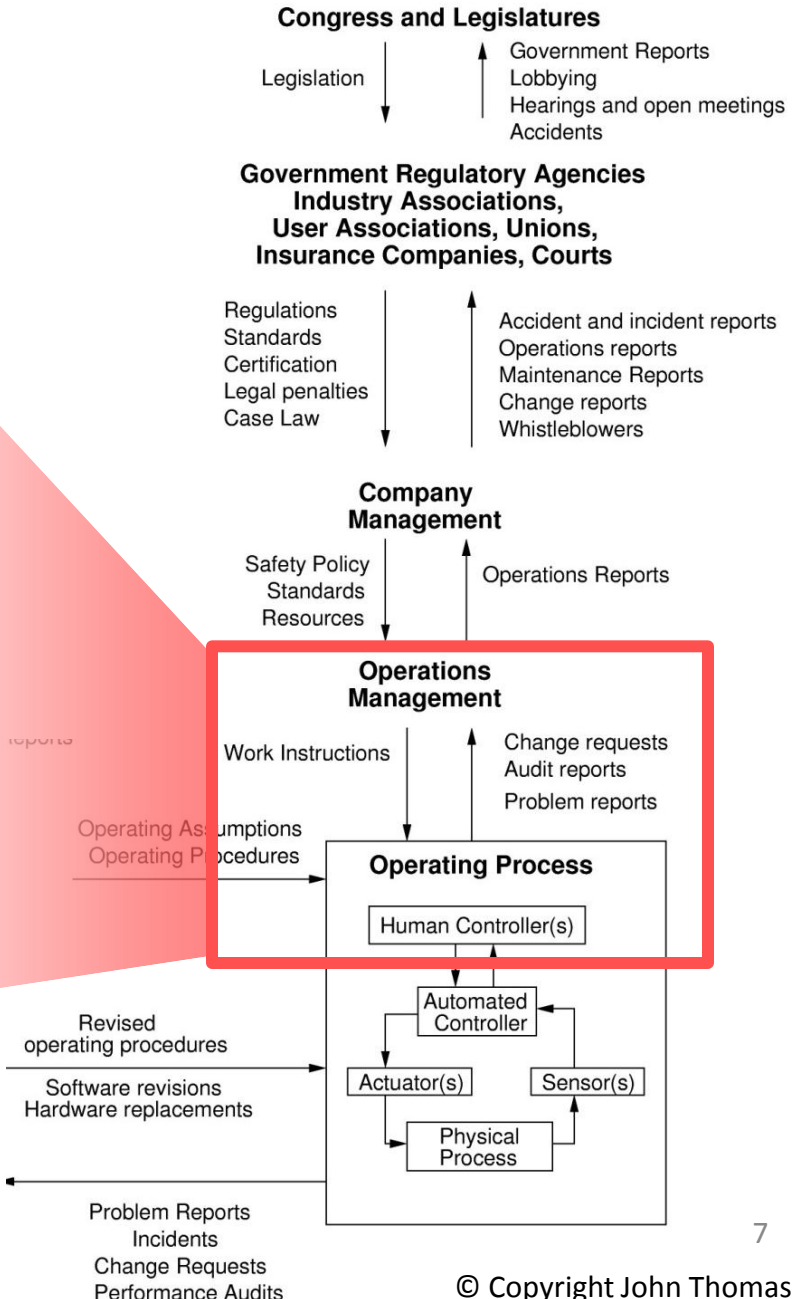
STAMP



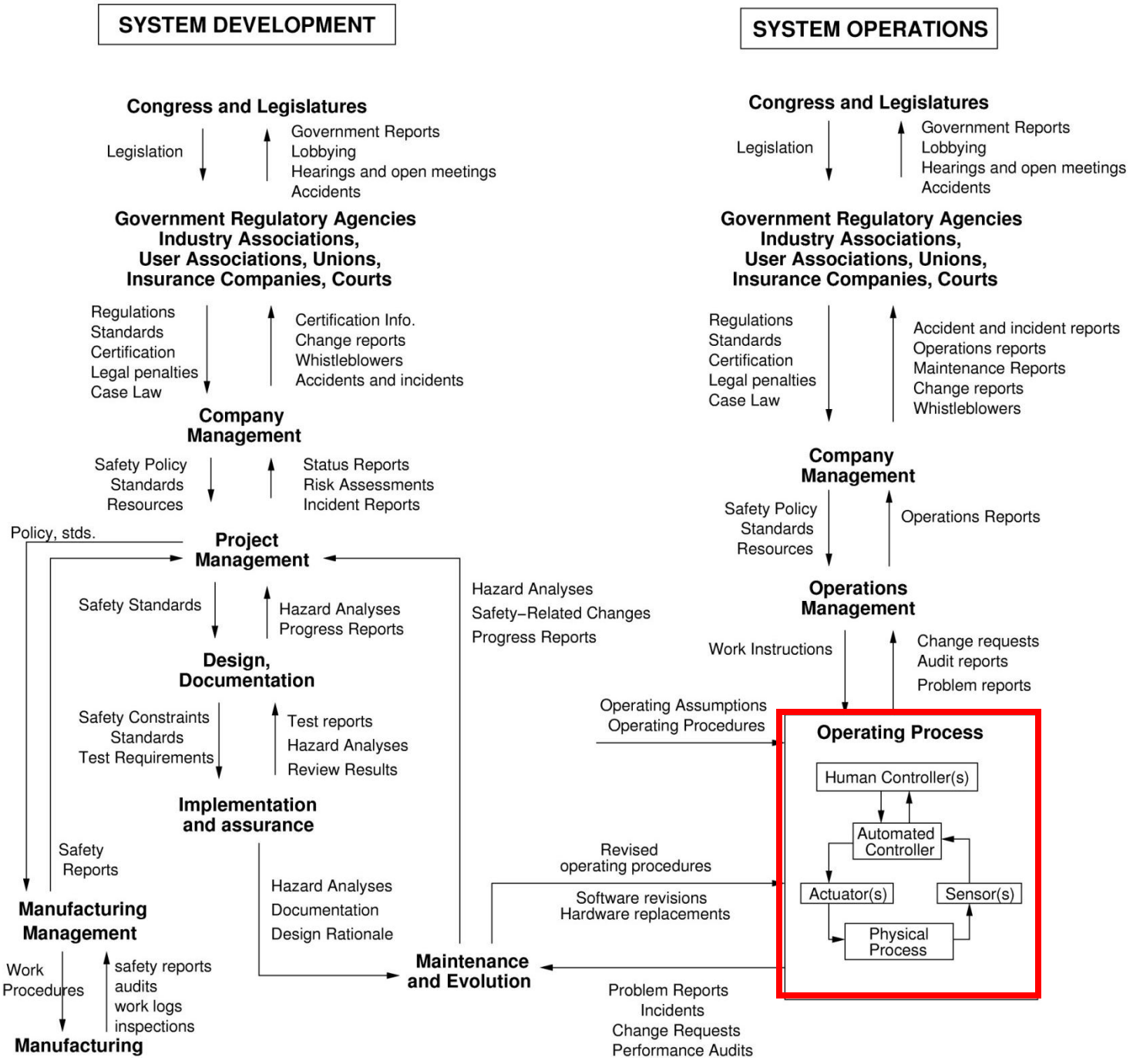


STAMP





Example Safety Control Structure

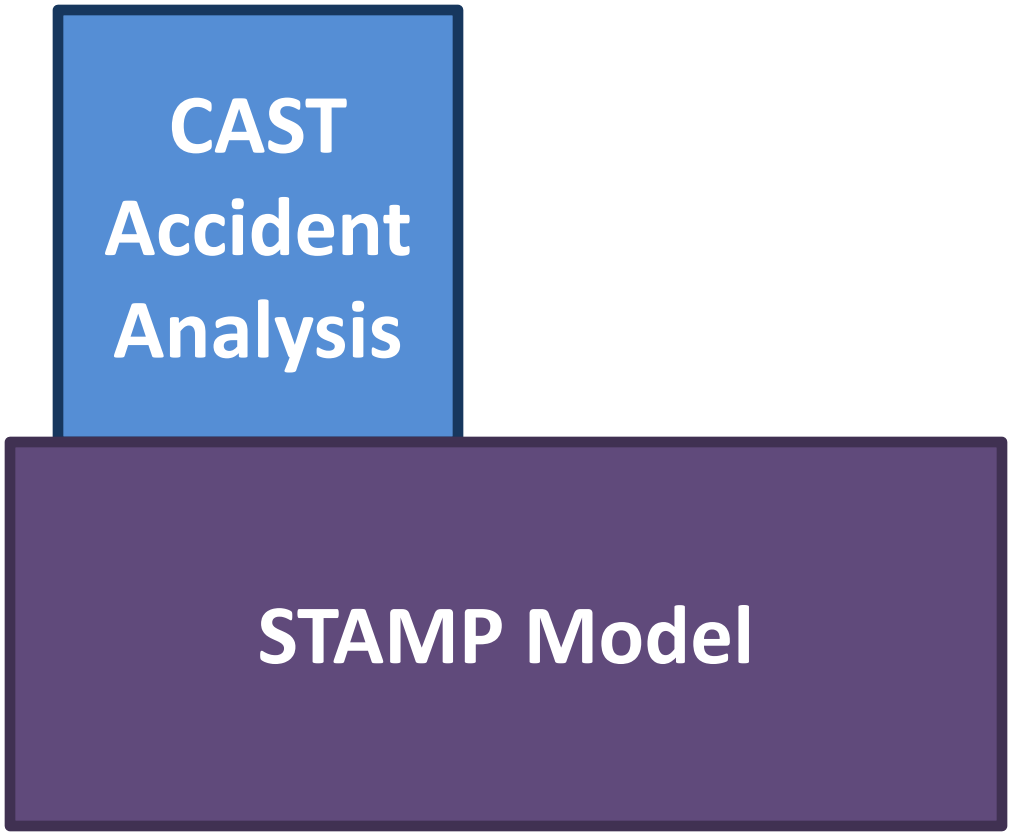


STAMP and STPA

STAMP Model

Accidents are caused by inadequate control

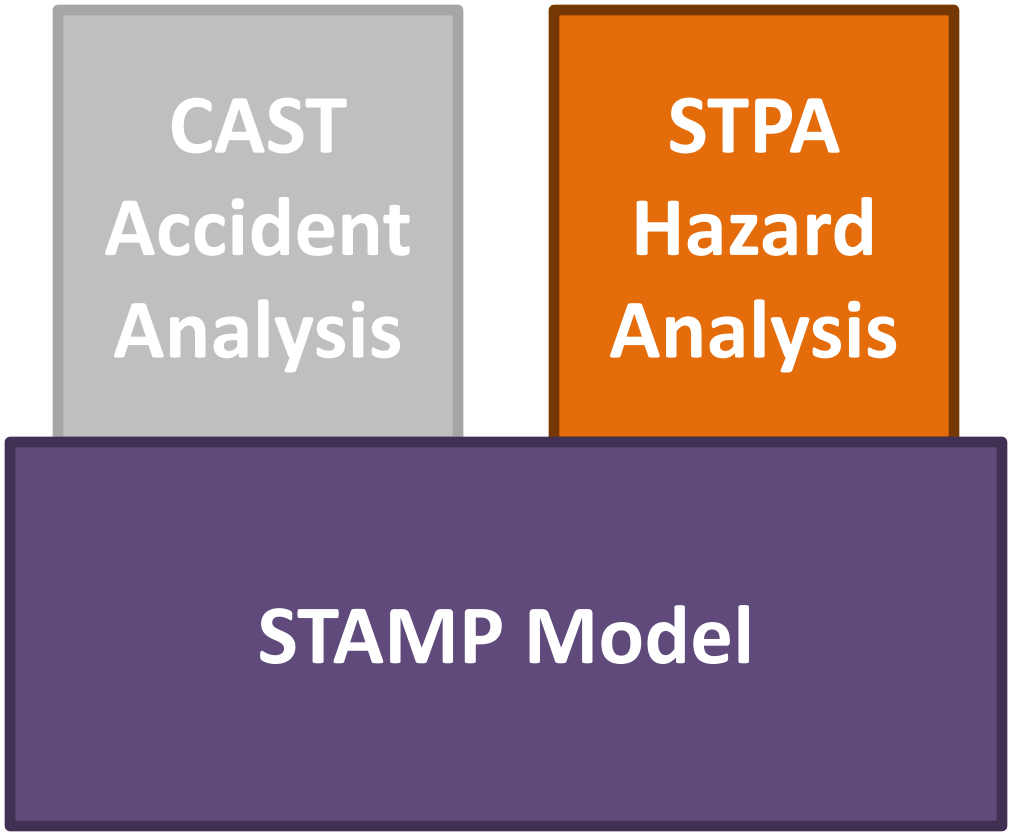
STAMP and STPA



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**
  10:30am – 3pm
  Pfaffenwaldring 7, Room 7.01
- STPA in automotive domain tutorial
  10:30am – 3pm
  Universitätsstr. 38 ,Room: 0.447
- STPA security tutorial (STPA-Sec)
  10:30am – 3pm
  Universitätsstr. 38 ,Room: 0.457

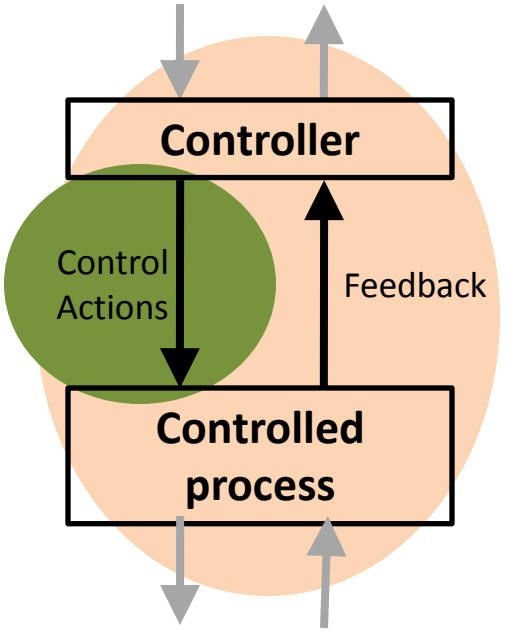
STPA Hazard Analysis

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



(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	System Hazard
People die from exposure to toxic chemicals	Toxic chemicals from the plant are in the atmosphere
People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

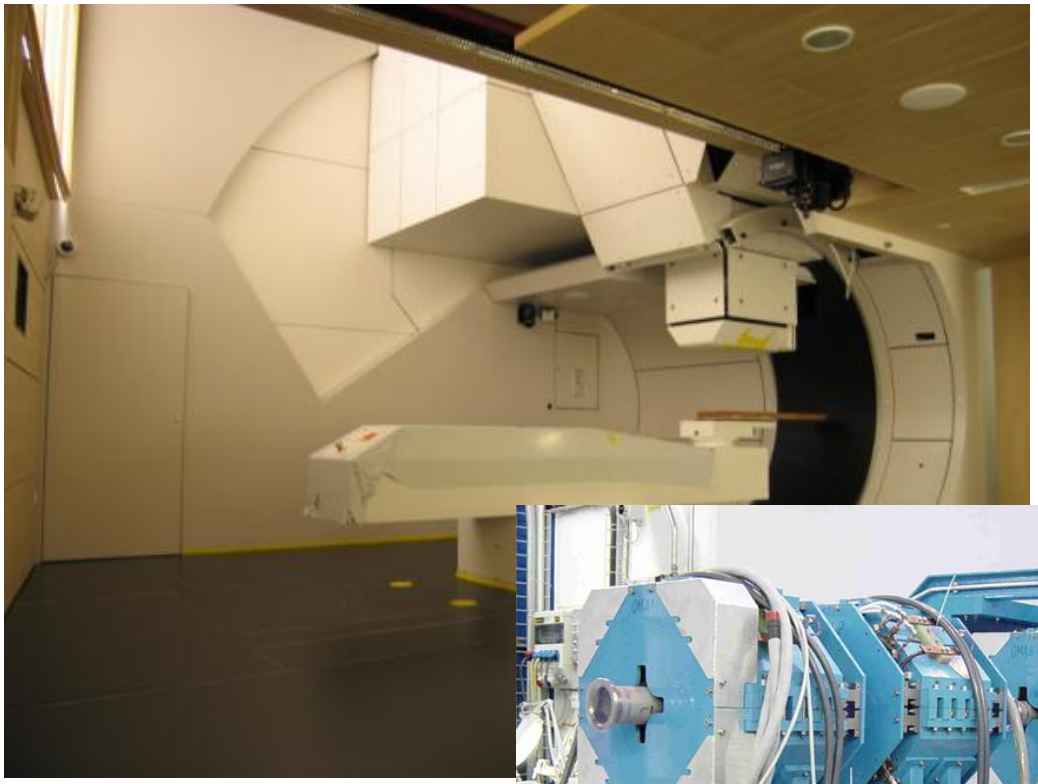
System Safety Constraints

System Hazard	System Safety Constraint
Toxic chemicals from the plant are in the atmosphere	Toxic plant chemicals must not be released into the atmosphere
Nuclear power plant radioactive materials are not contained	Radioactive materials must note be released
Vehicles do not maintain safe distance from each other	Vehicles must always maintain safe distances from each other
Food products for sale contain pathogens	Food products with pathogens must not be sold

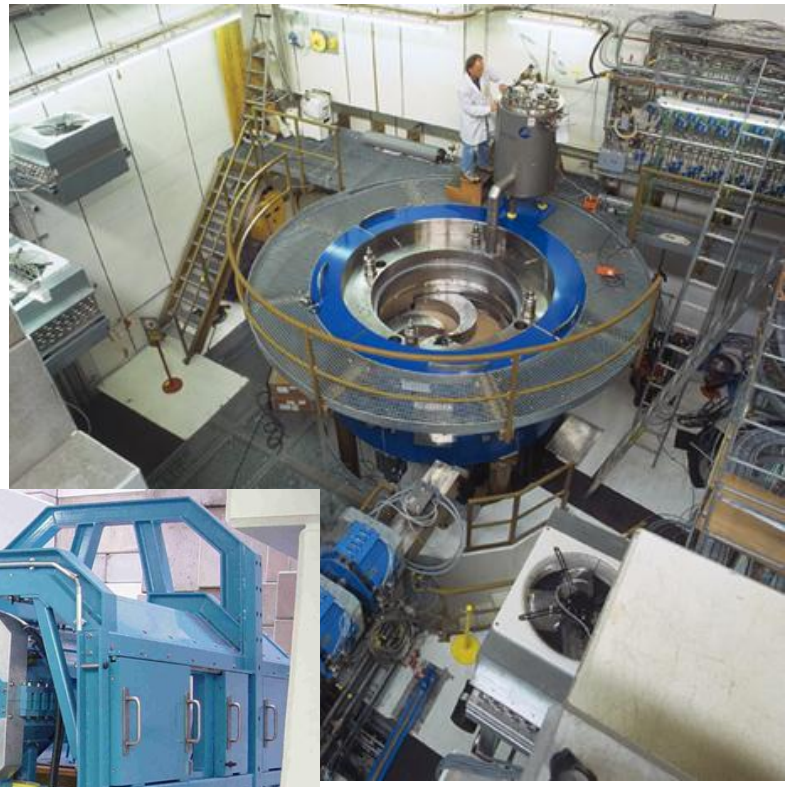
Additional hazards / constraints can be found in ESW p355

Control Structure Examples

Proton Therapy Machine
High-level Control Structure



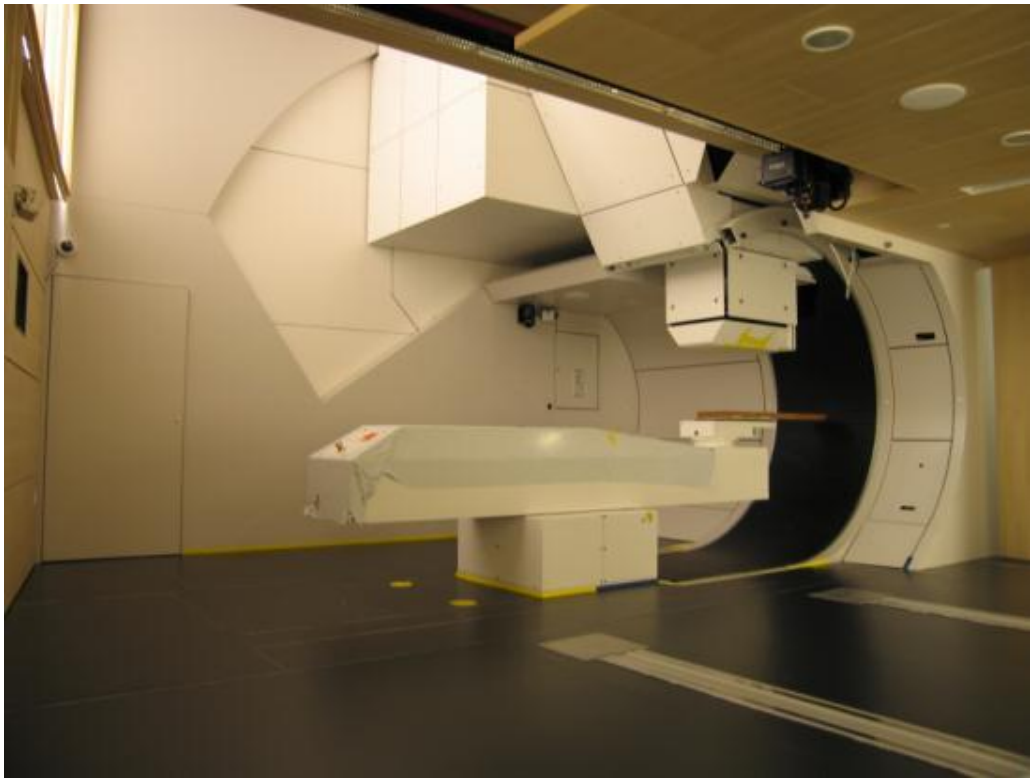
Gantry



Cyclotron

Beam path and
control elements

Proton Therapy Machine
High-level Control Structure



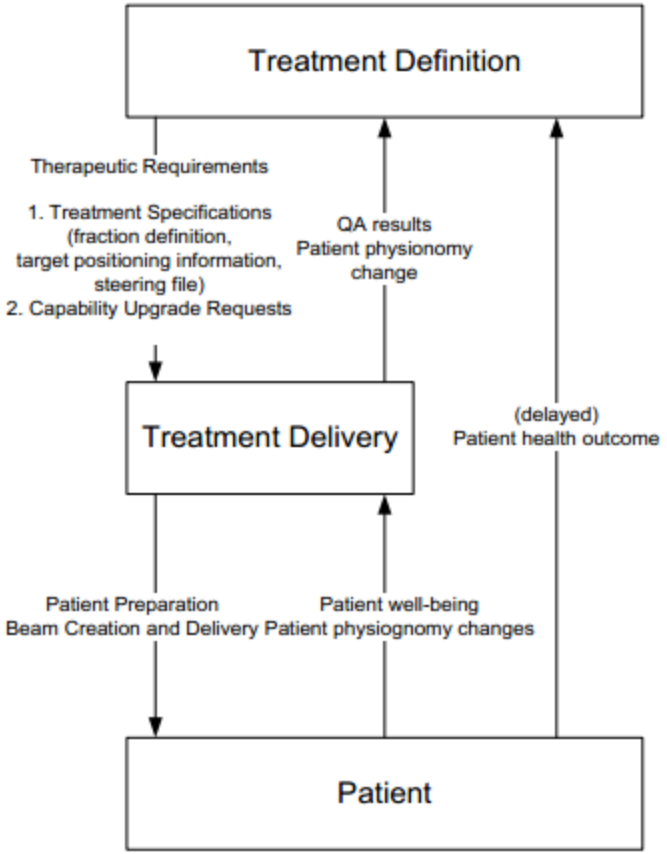
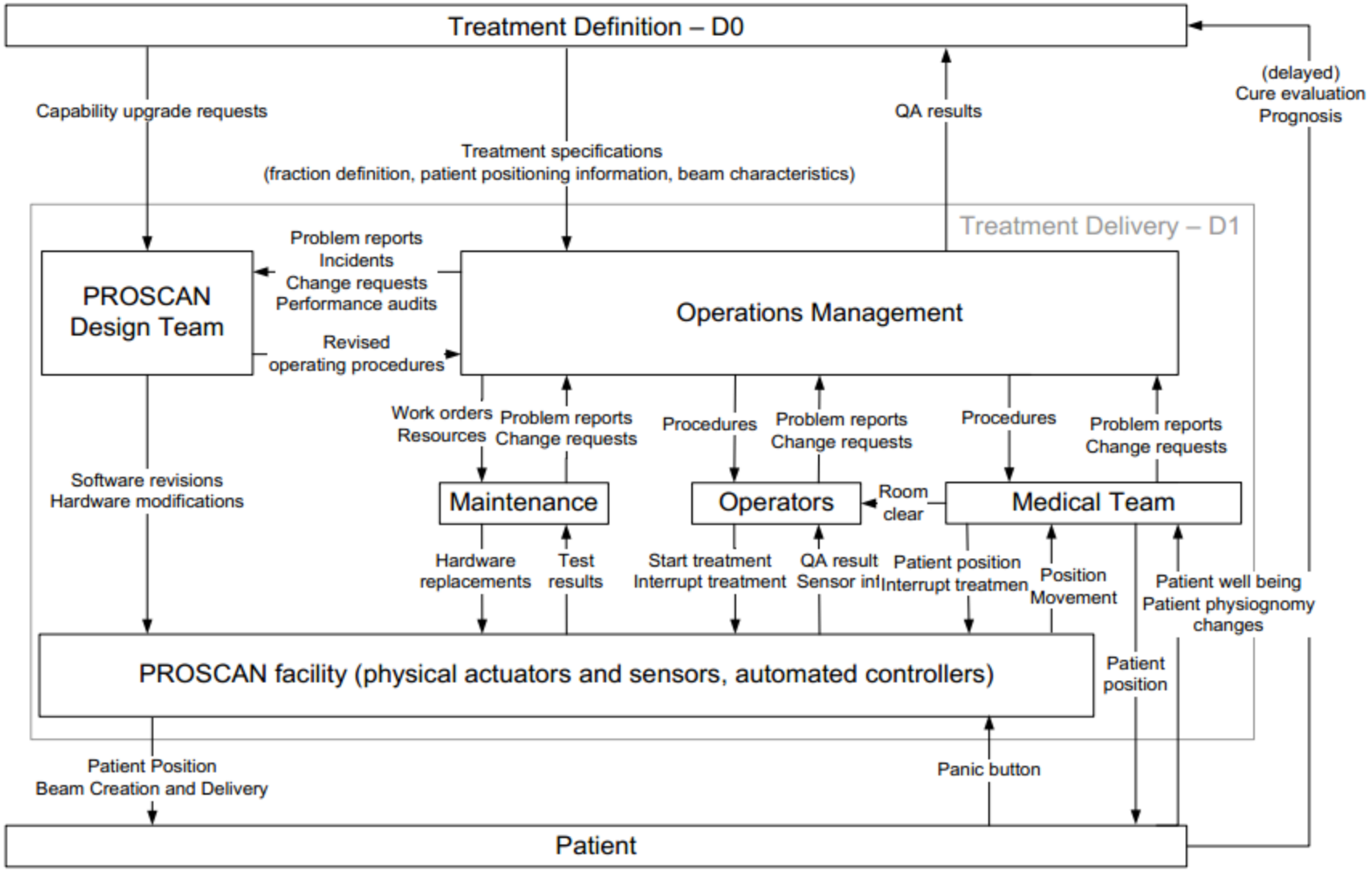


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Antoine PhD Thesis, 2012

Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

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

Chemical Plant

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

Chemical Plant

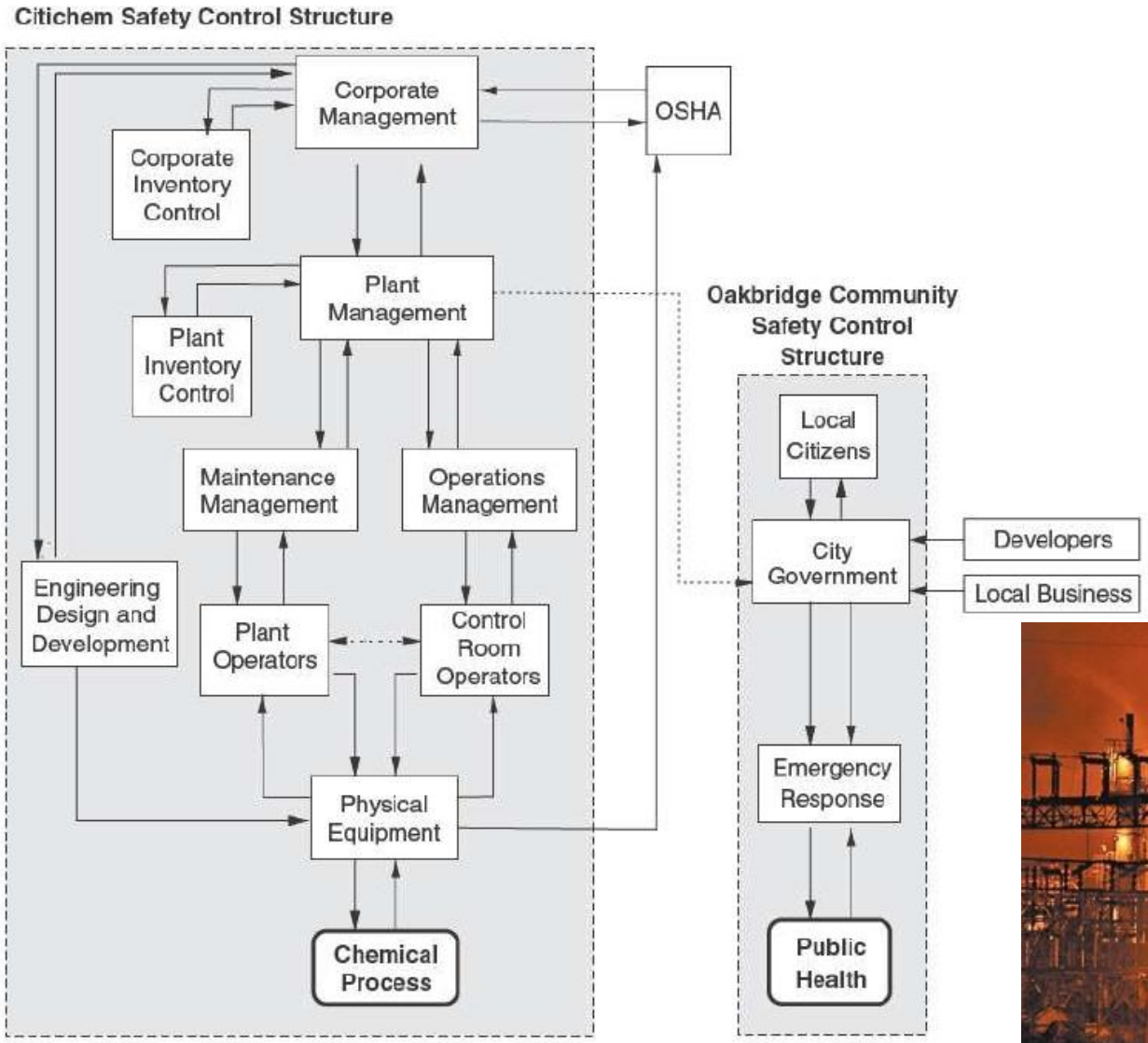


Image from:
http://www.cbgnetwork.org/2608.html

ESW p354

Adaptive Cruise Control

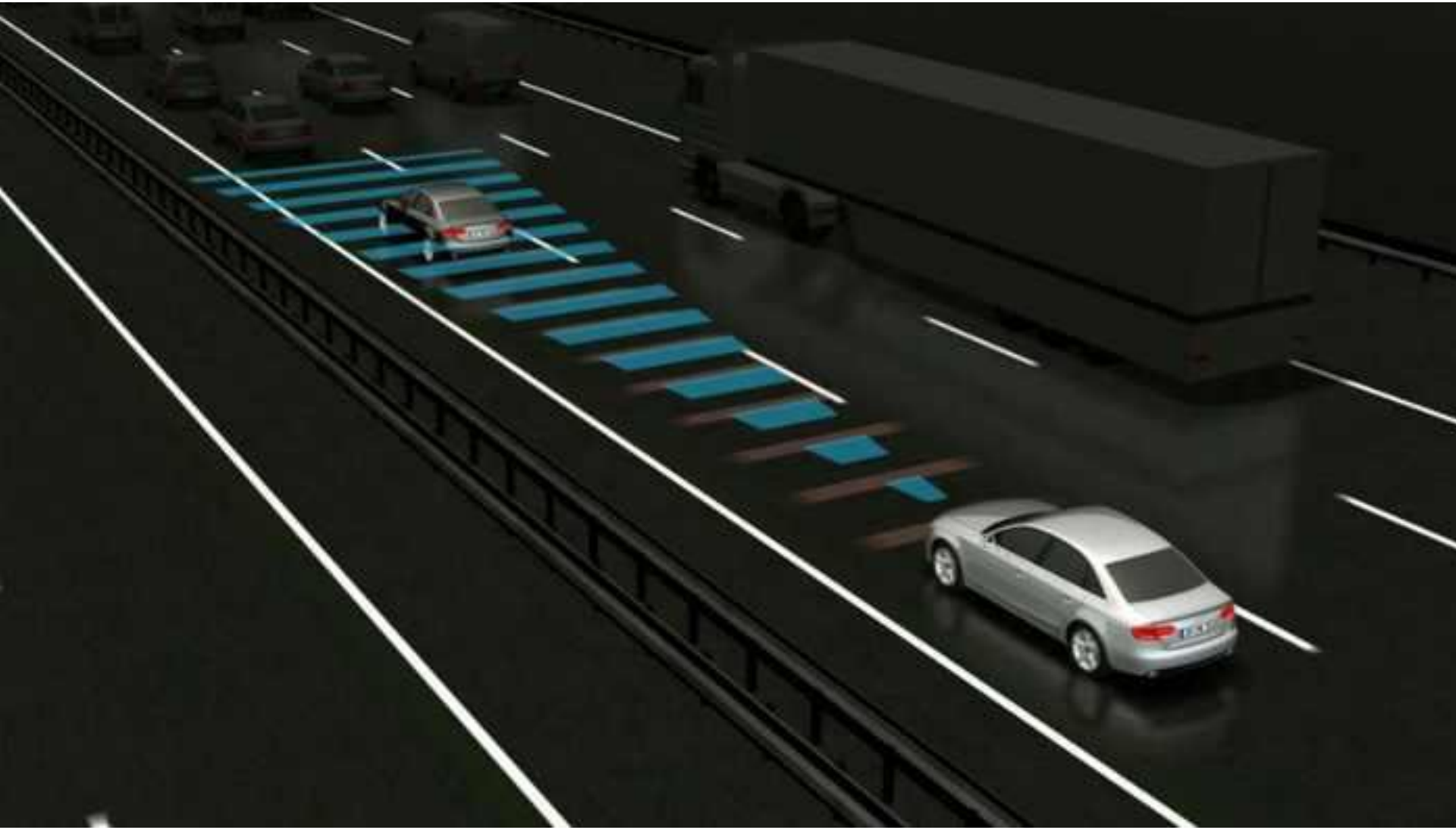
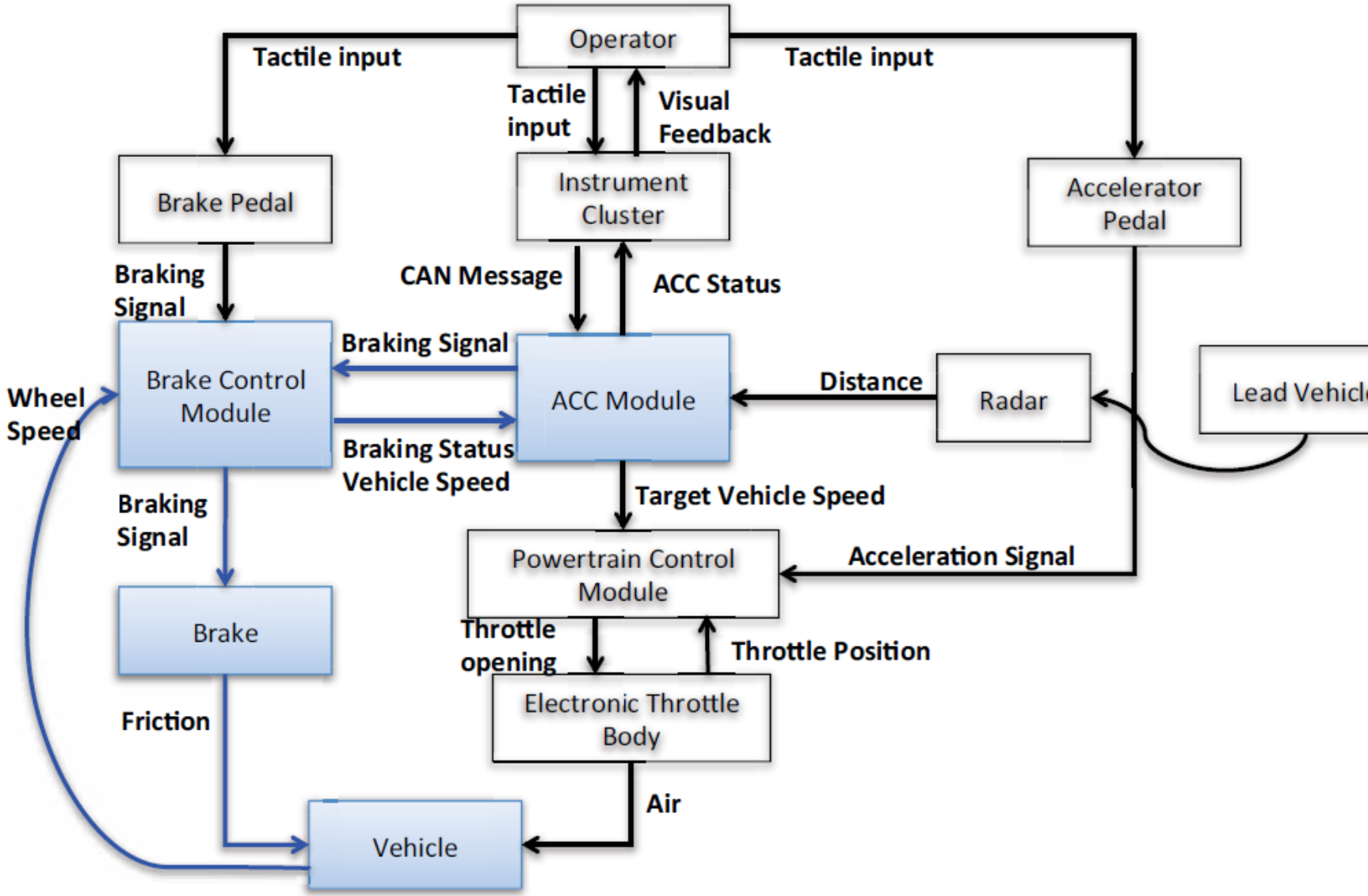
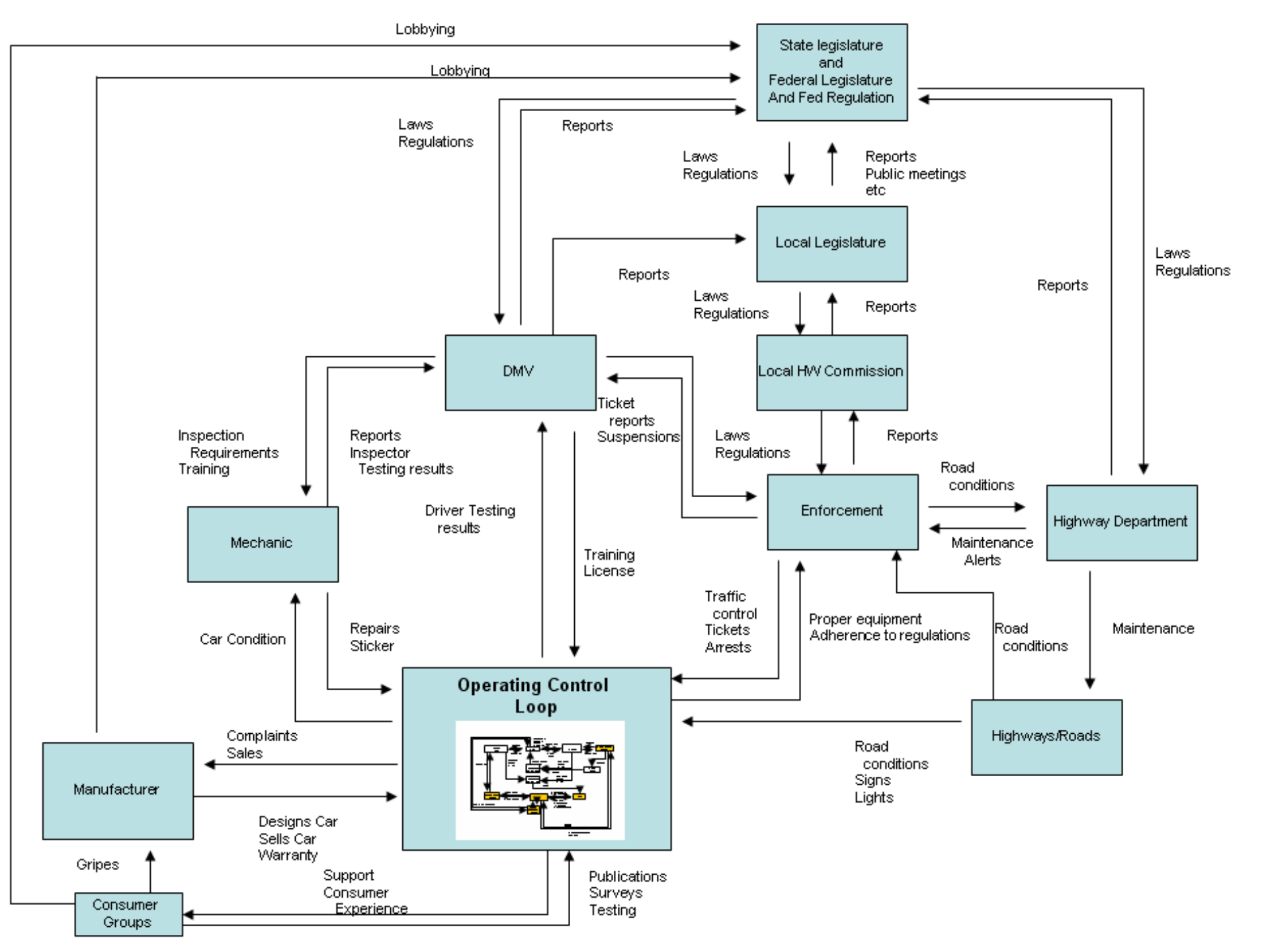


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

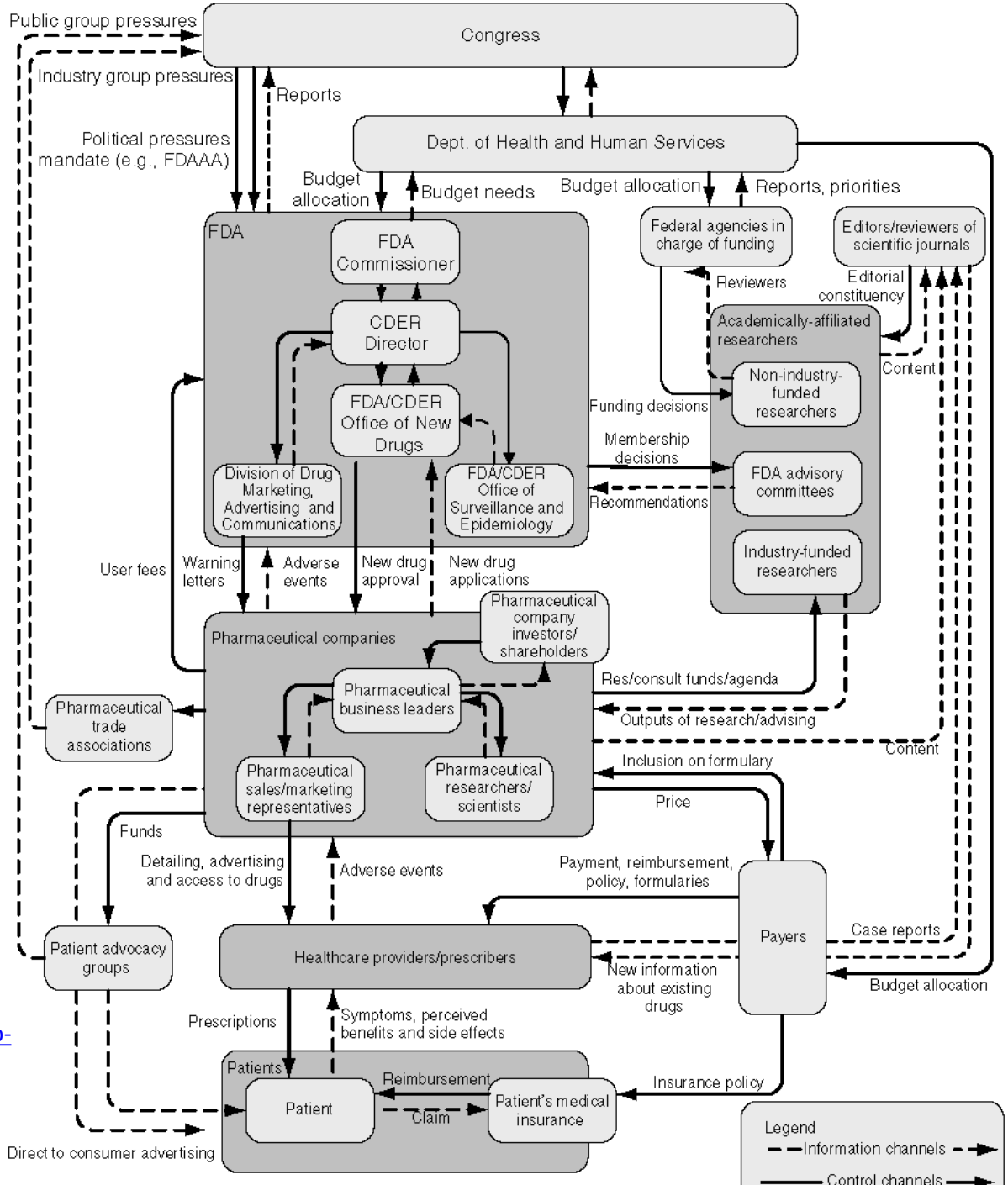
Example: ACC – BCM Control Loop




Lobbying
Lobbying
State legislature and Federal Legislature And Fed Regulation
Laws Regulations
Reports
Laws Regulations
Reports Public meetings etc
Local Legislature
Reports
Laws Regulations
Reports
Reports
Laws Regulations
DMV
Local HV Commission
Ticket reports Suspensions
Laws Regulations
Reports
Inspection Requirements Training
Reports Inspector Testing results
Road conditions
Enforcement
Highway Department
Driver Testing results
Mechanic
Training License
Maintenance Alerts
Traffic control Tickets Arrests
Proper equipment Adherence to regulations
Road conditions
Maintenance
Car Condition
Repairs Sticker
Operating Control Loop
Complaints Sales
Highways/Roads
Road conditions Signs Lights
Manufacturer
Designs Car Sells Car Warranty
Gripes
Support Consumer Experience
Publications Surveys Testing
Consumer Groups

U.S. pharmaceutical safety control structure

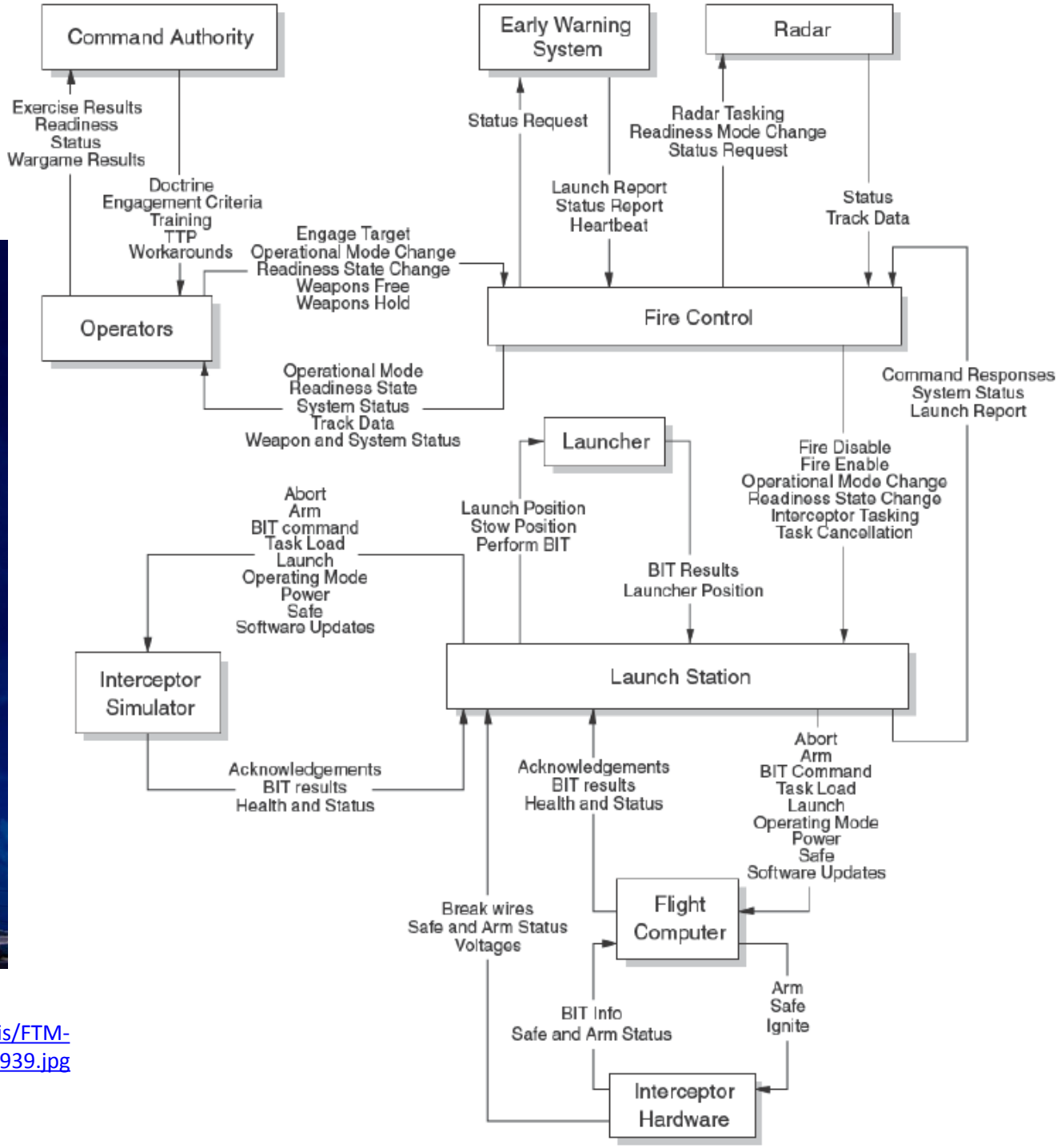
Image from: http://www.kleantreatmentcenter.com/wp-content/uploads/2012/07/vioxx.jpeg



Ballistic Missile Defense System

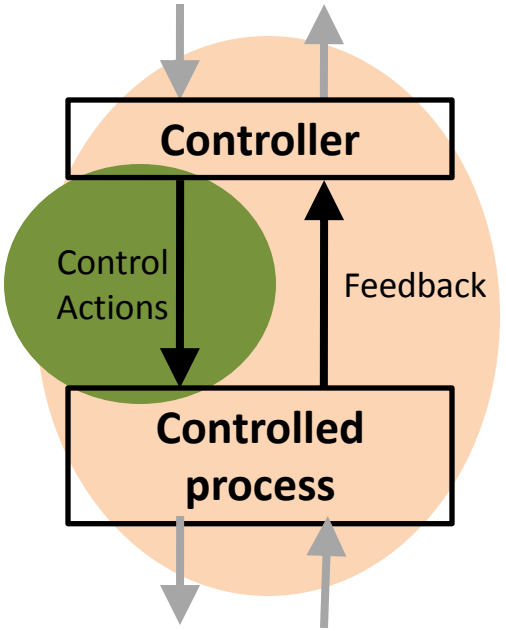
Image from:
http://www.mda.mil/global/images/system/aegis/FTM-21_Missile%201_Bulkhead%20Center14_BN4H0939.jpg

Safeware Corporation



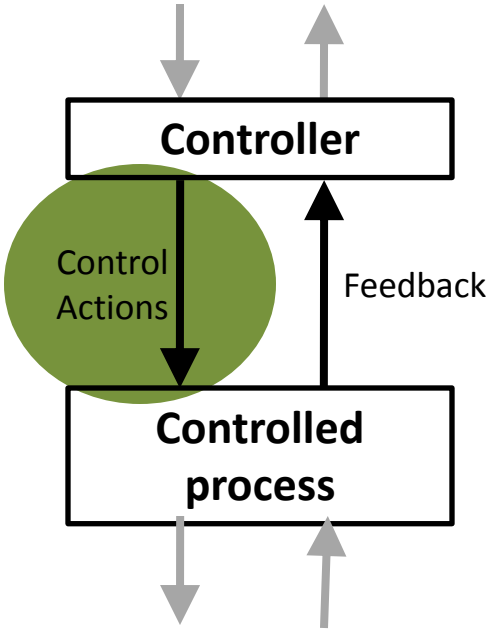
STPA
(System-Theoretic Process Analysis)

- 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)



4 ways unsafe control may occur:

- A control action required for safety is not provided or is not followed
- An unsafe control action is provided that leads to a hazard
- A potentially safe control action provided too late, too early, or out of sequence
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action)

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

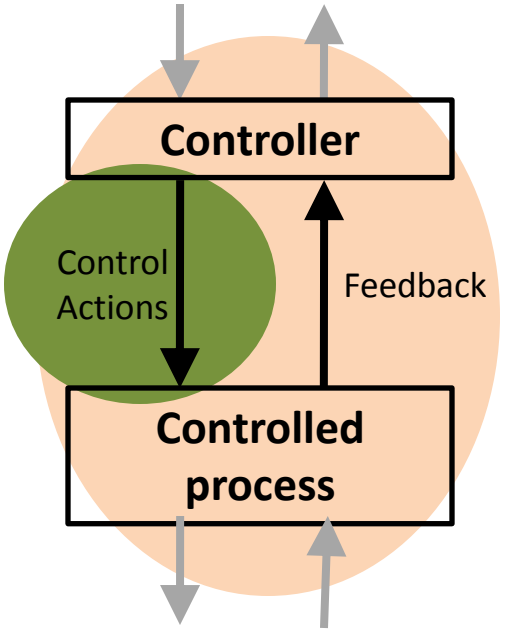
Step 1: Identify Unsafe Control Actions

(a more rigorous approach)

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

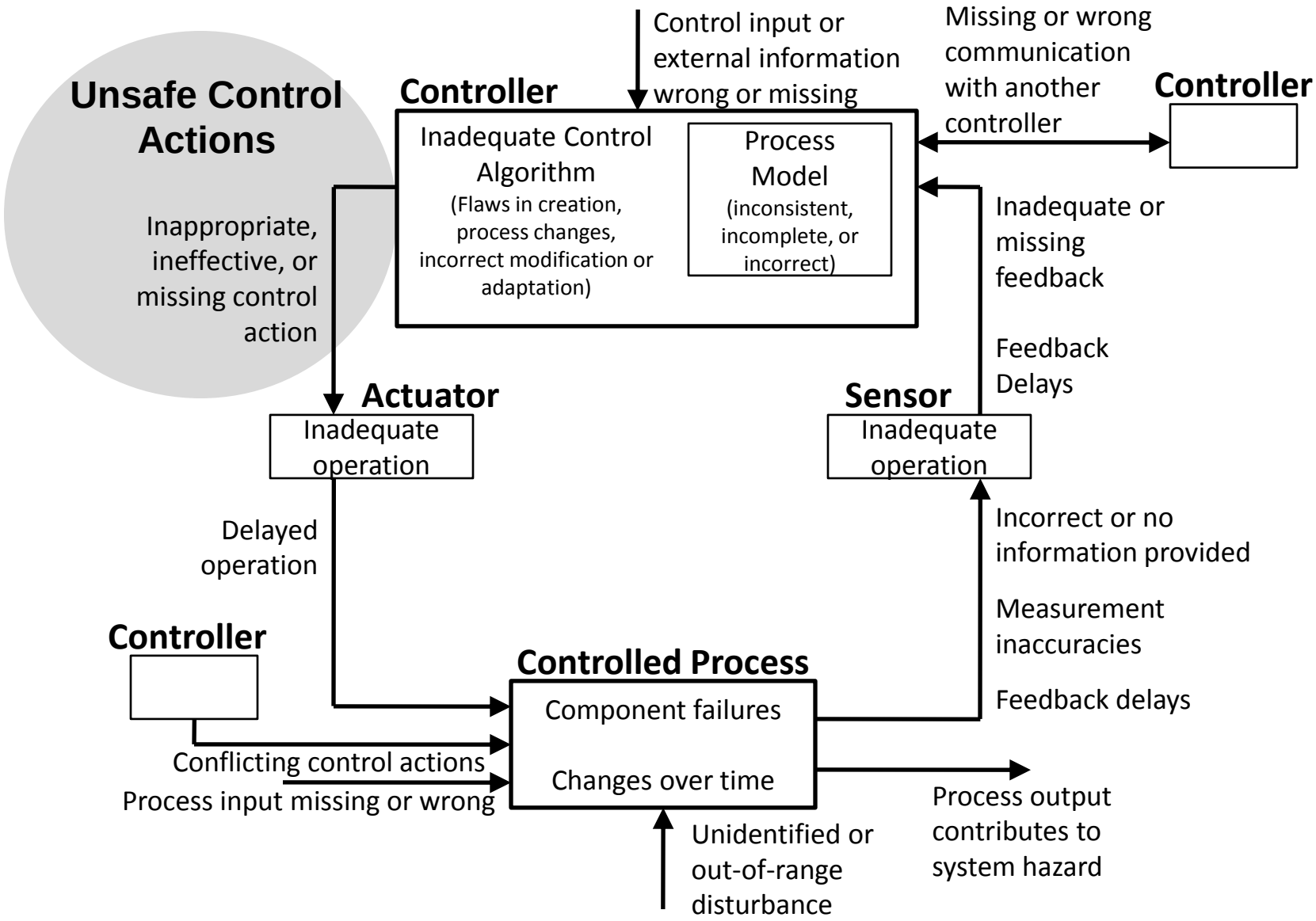
STPA
(System-Theoretic Process Analysis)

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



(Leveson, 2012)

STPA Step 2: Identify Control Flaws



STPA Examples

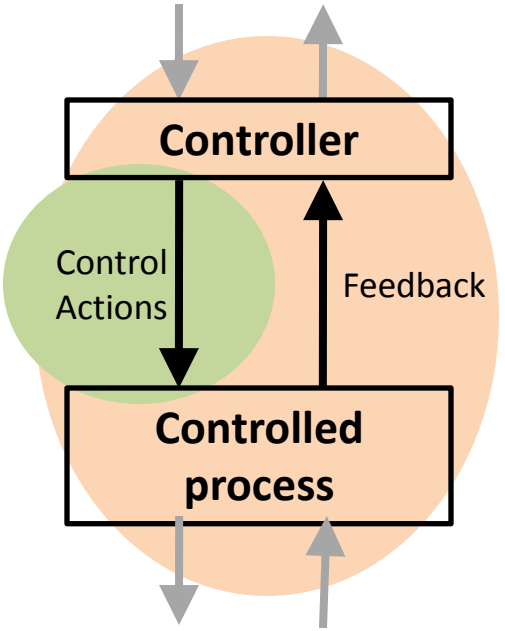
Nextgen In-Trail Procedure (ITP) Exercise

a new in-trail procedure
for trans-oceanic flights

STPA Process

Establish foundation for analysis

- Define accidents
- Define system hazards
- Rewrite hazards as safety constraints
- Draw safety control structure



- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal factors

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

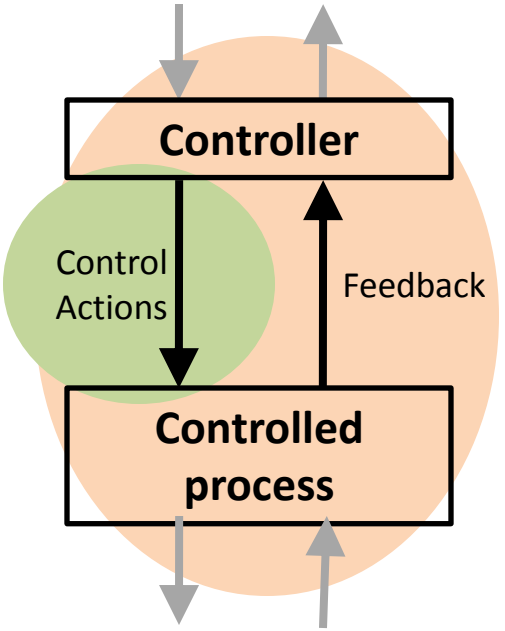
- System-level Accident (loss)
  - Two aircraft collide
  - Aircraft crashes into terrain / ocean
- System-level Hazards
  - Two aircraft violate minimum separation
  - Aircraft enters unsafe atmospheric region
  - Aircraft enters uncontrolled state
  - Aircraft enters unsafe attitude
  - Aircraft enters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

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 Process

- Establish foundation for analysis
  - ✓ Define accidents
  - ✓ Define system hazards
  - → Rewrite hazards as safety constraints
  - – Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal factors

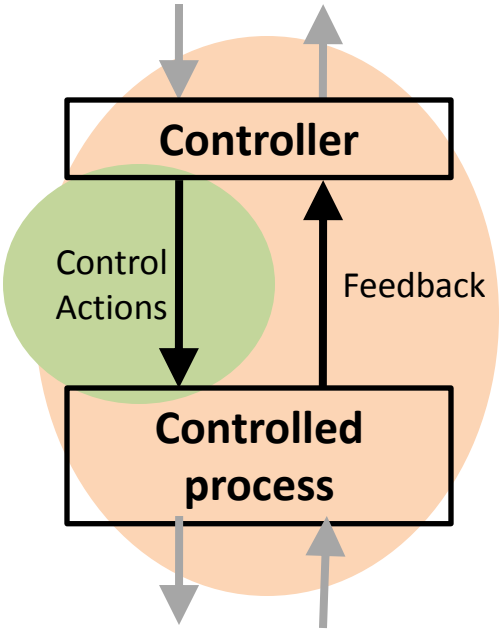


System Safety Constraints

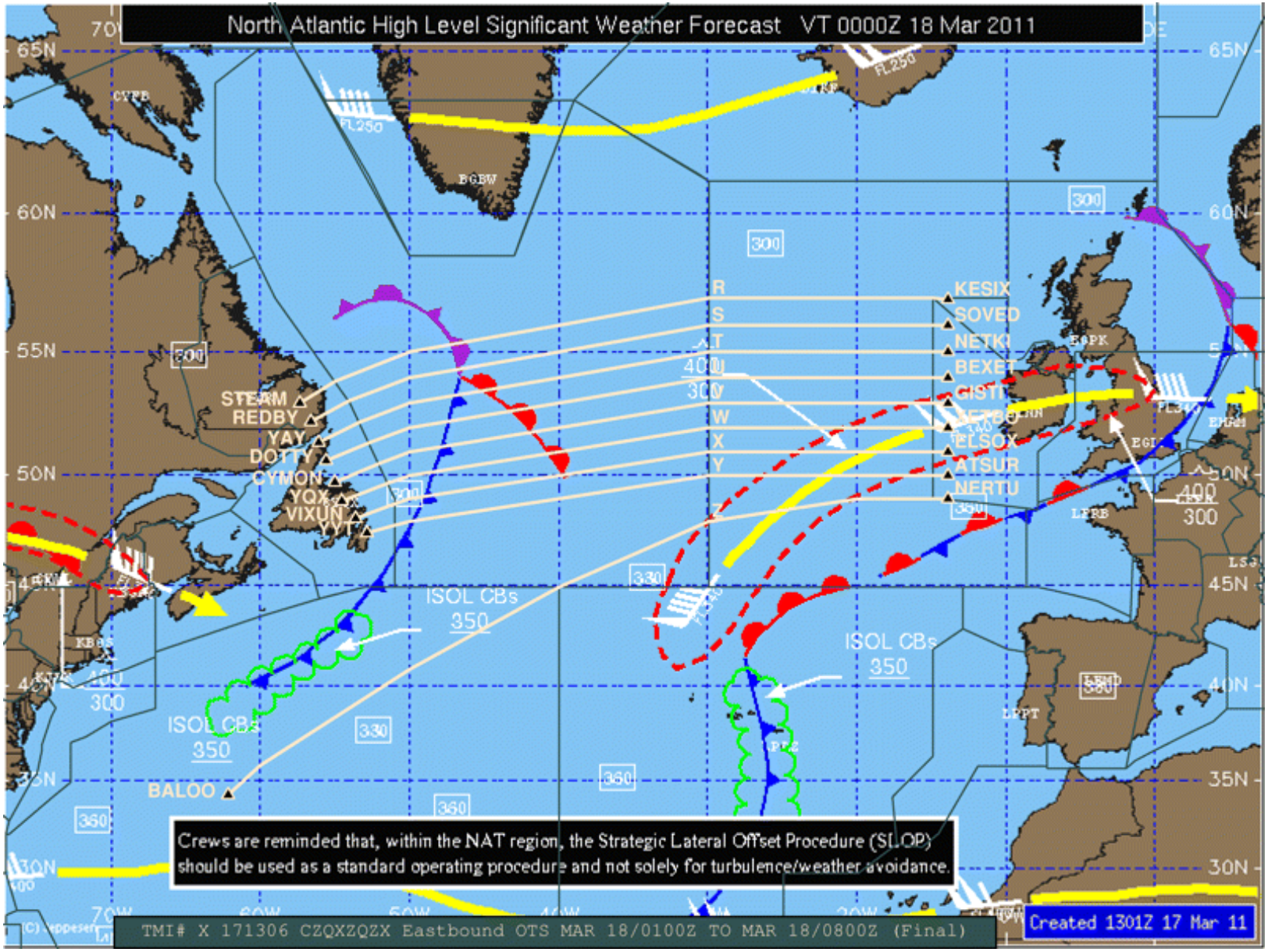
System Hazard	System Safety Constraint
H-1: Two aircraft violate minimum separation	SC-1: ?
H-2: Aircraft enters unsafe atmospheric region	SC-2: ?
H-3: Aircraft enters uncontrolled state	SC-3: ?
H-4: Aircraft enters unsafe attitude	SC-4: ?
H-5: Aircraft enters prohibited area	SC-5: ?

STPA Process

- Establish foundation for analysis
  - ✓ Define accidents
  - ✓ Define system hazards
  - ✓ Rewrite hazards as safety constraints
  - Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal factors

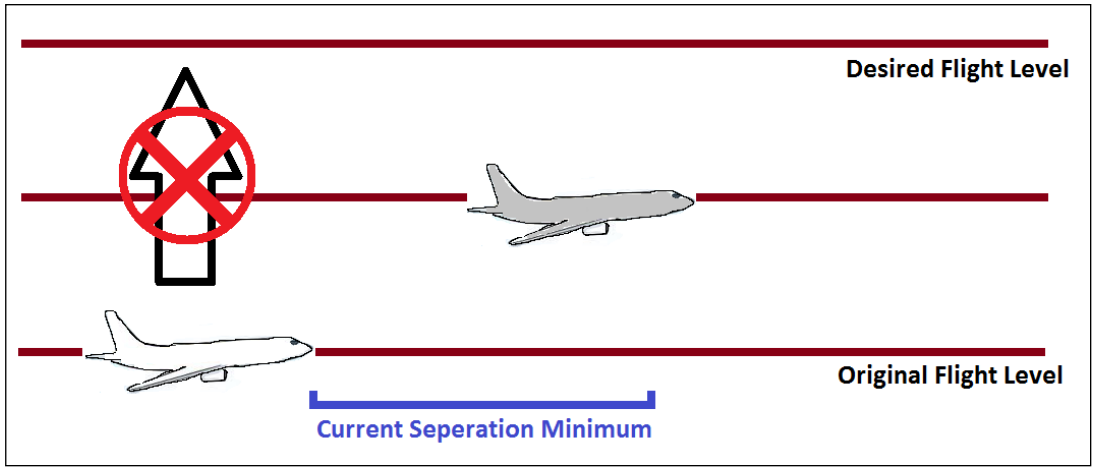


North Atlantic Tracks



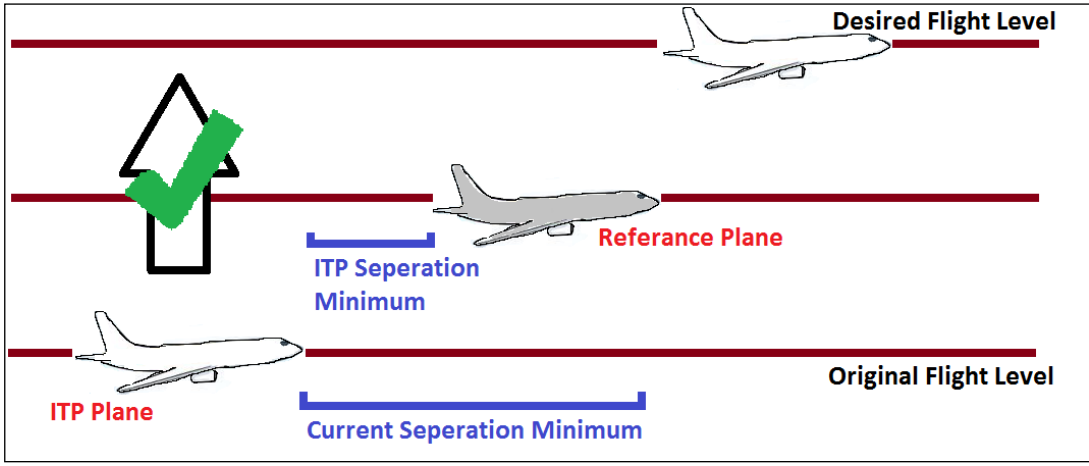
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



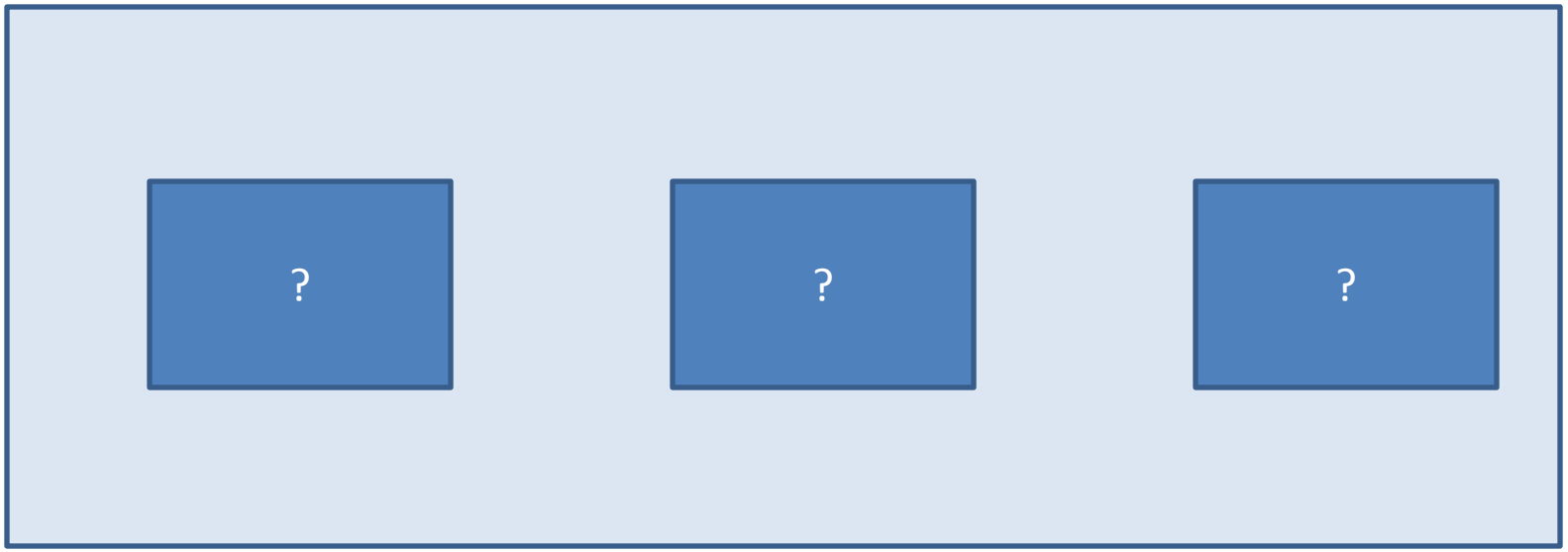
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



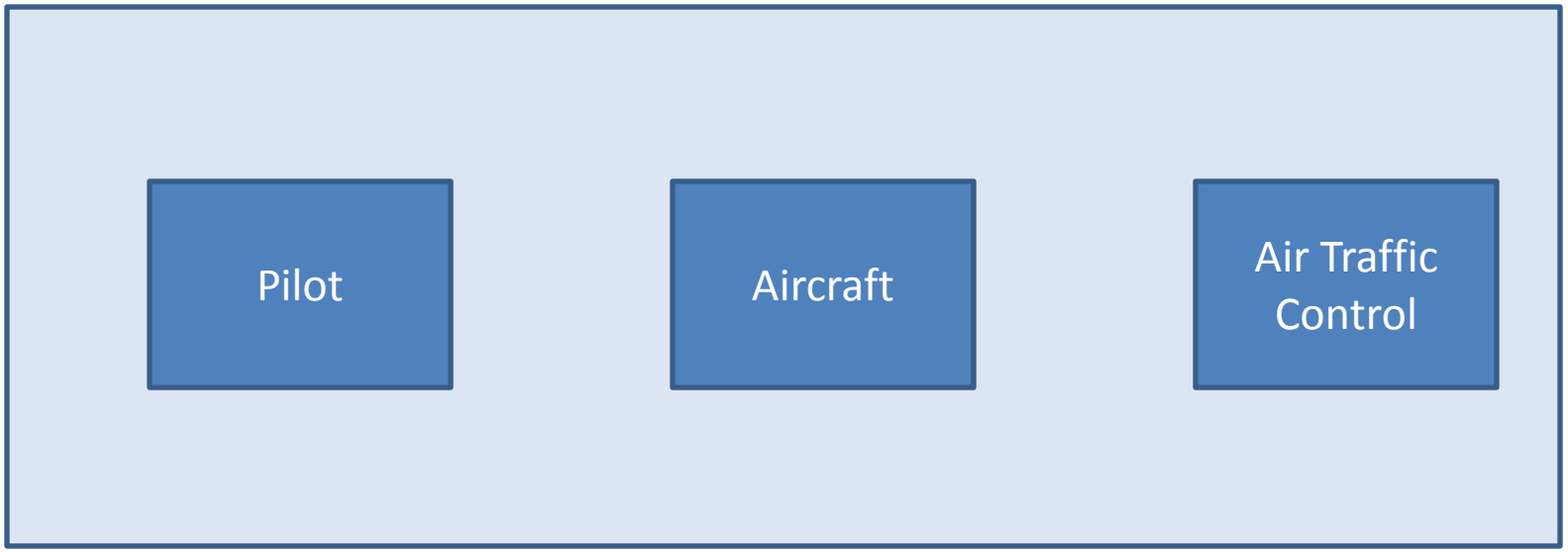
Draw the Functional Control Structure

- High-level Control Structure
  - What are the major components and controllers of the system?



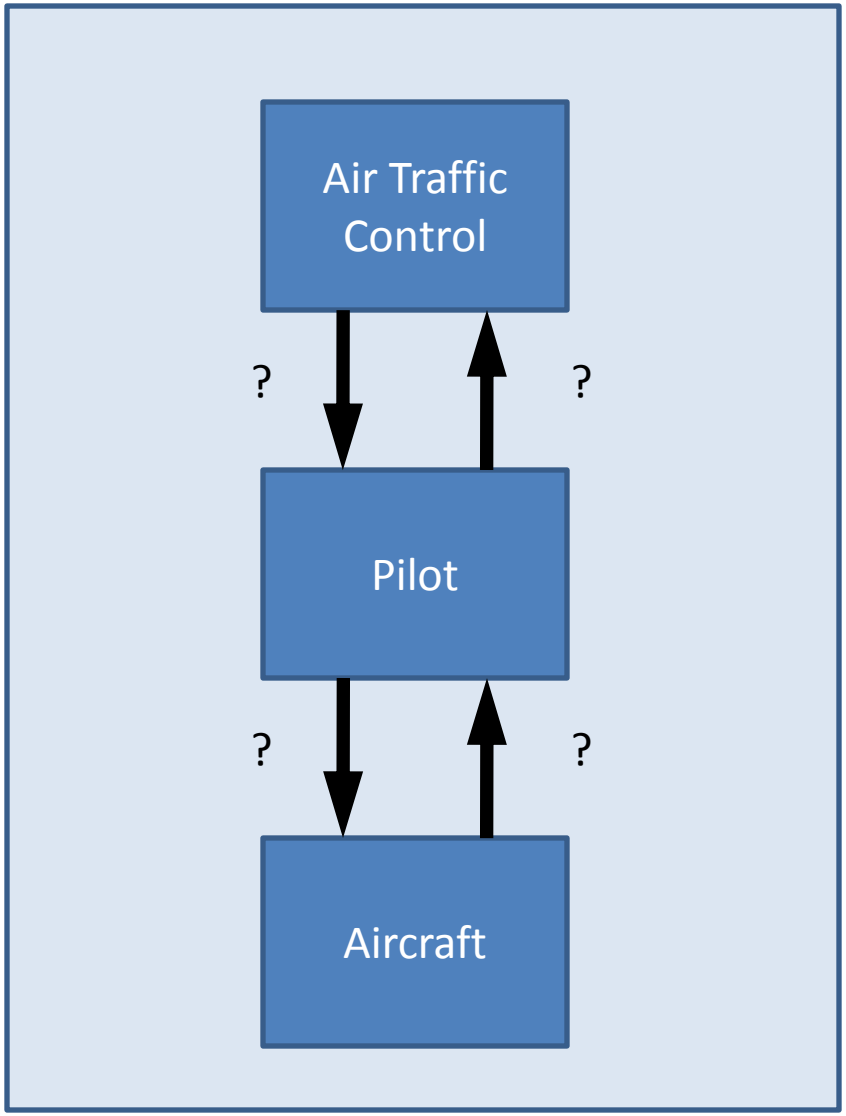
Draw the Functional Control Structure

- High-level Control Structure
  - Who controls who or what?



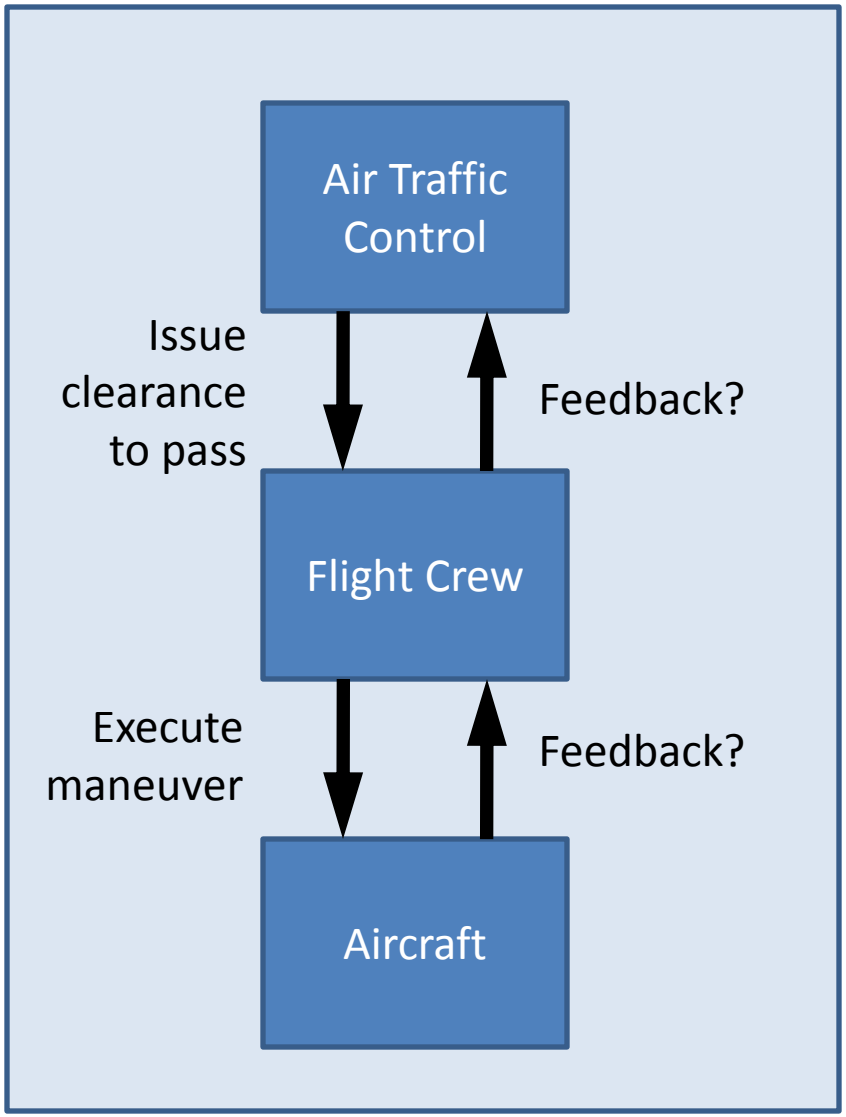
Draw the Functional Control Structure

- High-level Control Structure
  - What control actions can be sent?



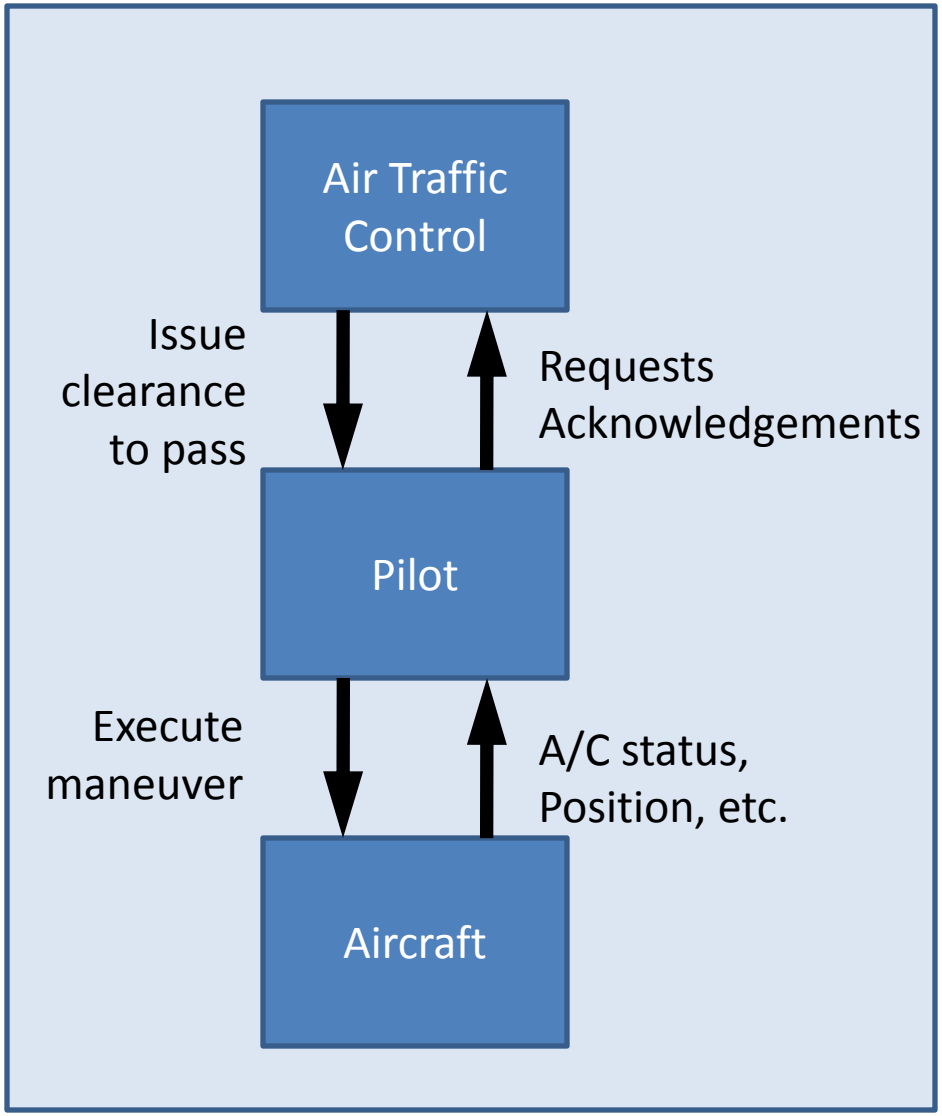
Draw the Functional Control Structure

- High-level Control Structure
  - How do controllers make those decisions?
  - What feedback is sent?

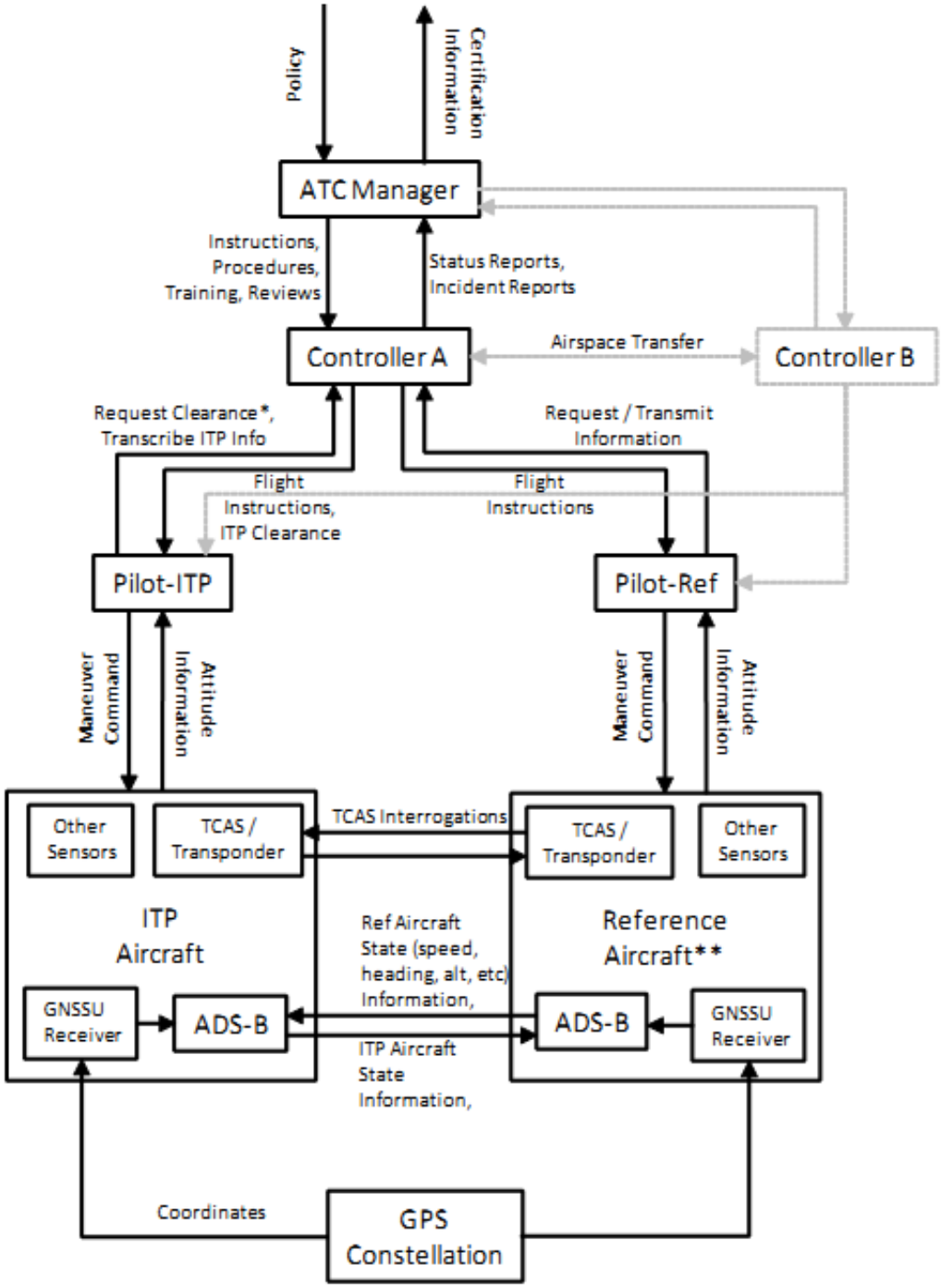


Draw the Functional Control Structure

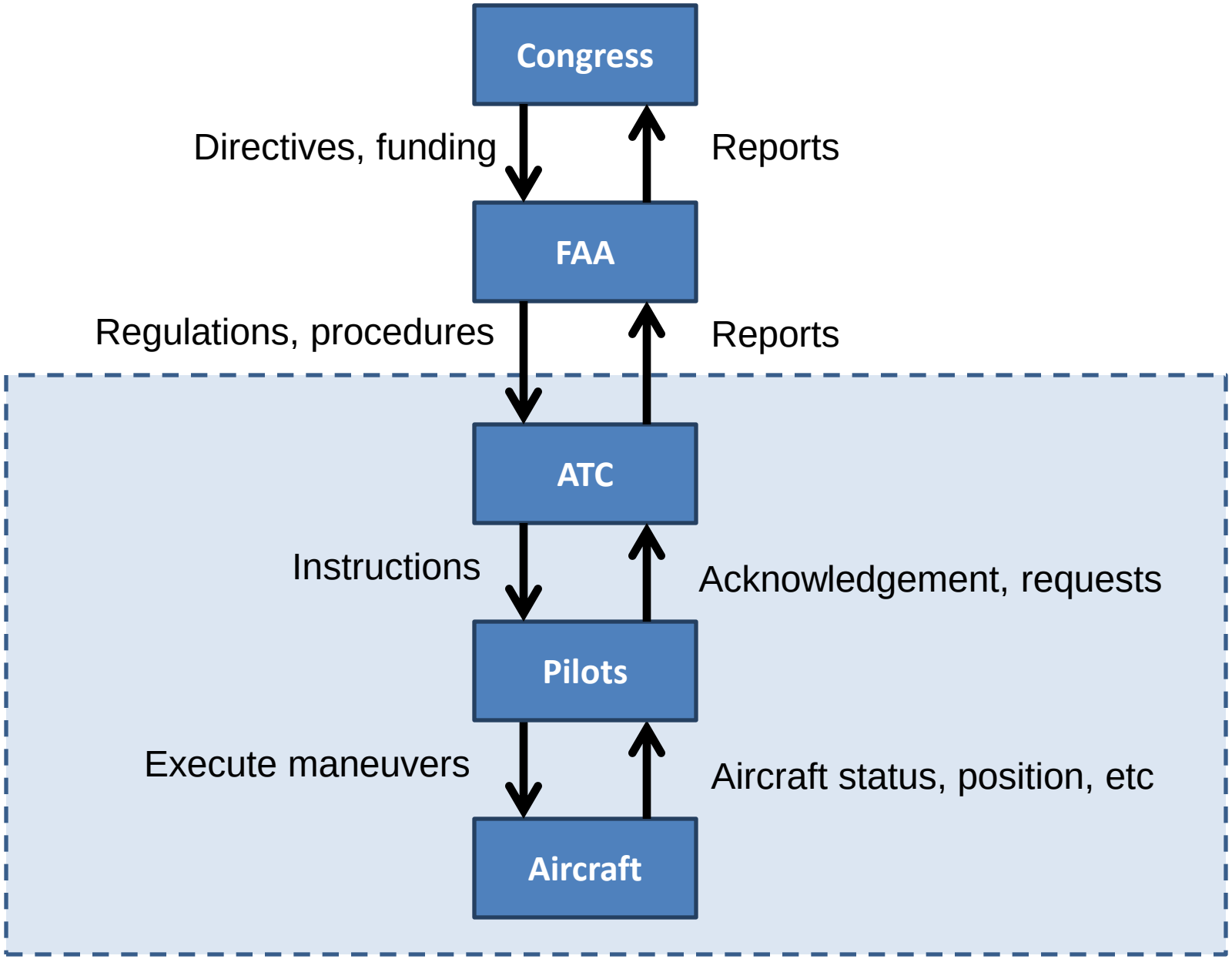
- High-level Control Structure

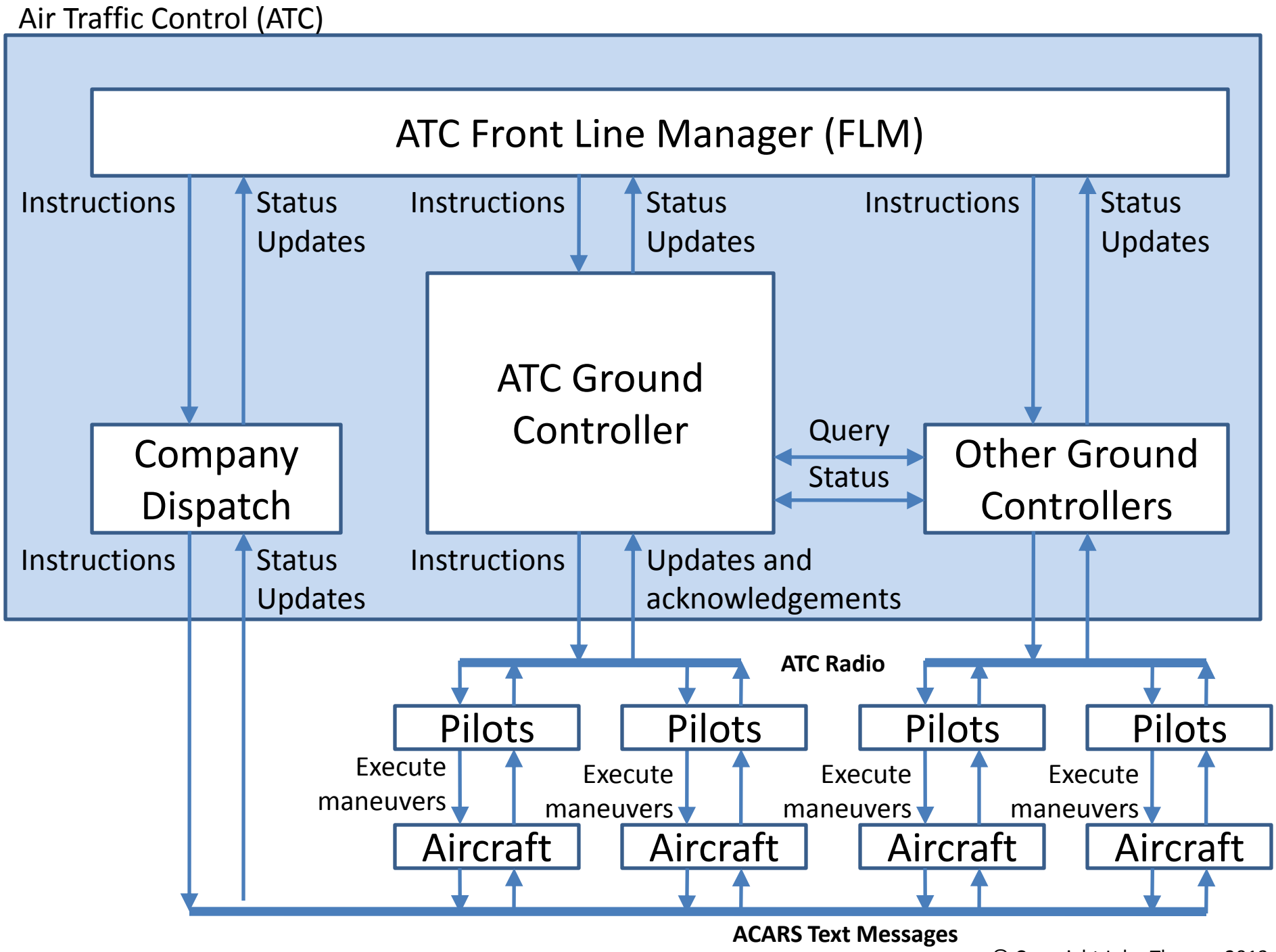


Adding Detail



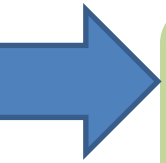
Adding Levels





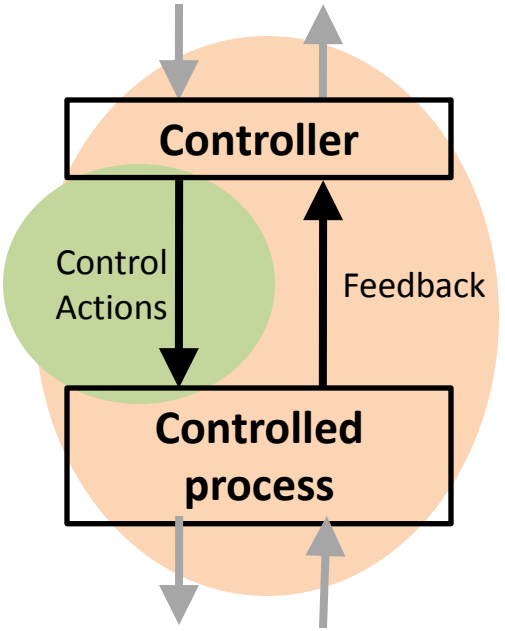
STPA Process

- Establish foundation for analysis
  - ✓ Define accidents
  - ✓ Define system hazards
  - ✓ Rewrite hazards as safety constraints
  - ✓ Draw safety control structure



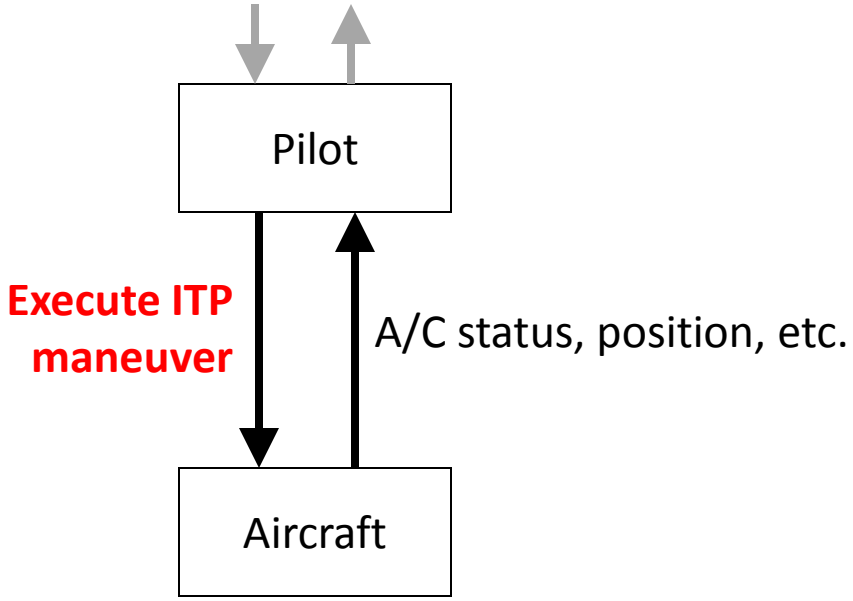
Step 1: Identify unsafe control actions and safety constraints

- Step 2: Identify causal factors



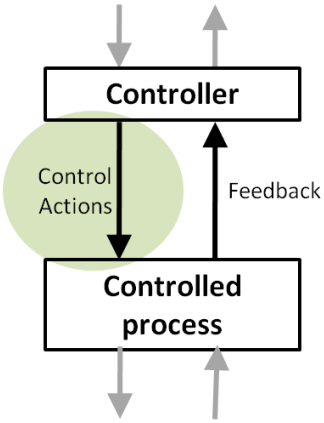
Step 1: Identify Unsafe Control Actions

Example: Let's start with the pilot



Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early/too late, wrong order**	**Stopped too soon/ applied too long**
Execute ITP Maneuver		Pilots provide ITP maneuver when it is not approved		

Structure of an Unsafe Control Action



Example:
"Pilots provide ITP maneuver when maneuver is not approved"

Source Controller

Type

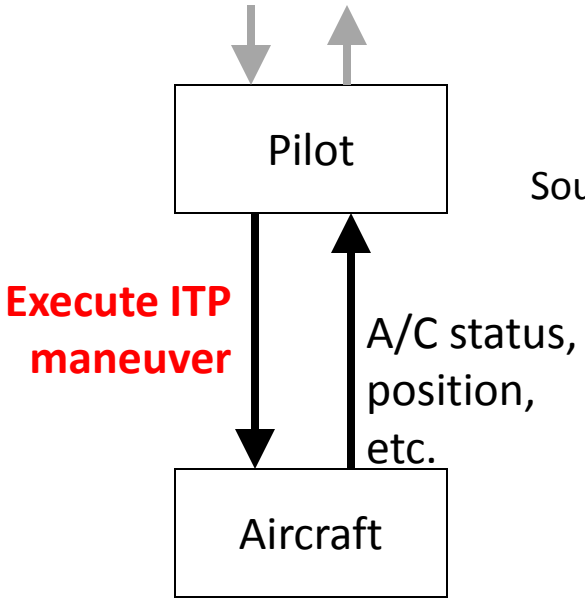
Control Action

Context

Four parts of an unsafe 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)

Step 1: Identify Unsafe Control Actions



Example:
"Pilots provide ITP maneuver when maneuver is not approved"

Source Controller

Type

Control Action

Context

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early/too late, wrong order**	**Stopped too soon/ applied too long**
Execute ITP Maneuver	?	Pilots provide ITP maneuver when it is not approved	?	?

Flight Crew Unsafe Control Actions

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order	Stopped too soon/ applied too long
Execute ITP		Pilots execute maneuver when not approved Pilots execute maneuver when ITP criteria are not satisfied Pilots execute maneuver with incorrect climb rate, final altitude, etc	Pilots execute maneuver too soon before approval Pilots execute maneuver too late after reassessment	Pilots stop maneuver before reaching designated altitude Pilots continue to climb/descend beyond designated altitude
Abnormal Termination of ITP	FC continues with maneuver in dangerous situation	FC aborts unnecessarily FC does not follow regional contingency procedures while aborting		

Controller Safety Constraints

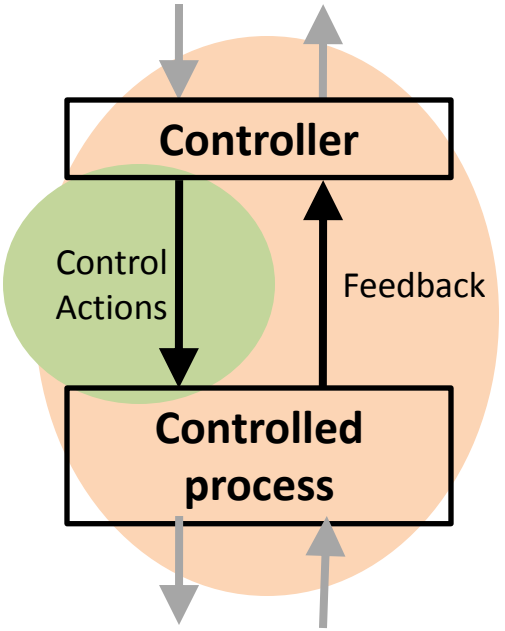
Unsafe Control Action	Safety Constraint
Pilots execute maneuver when not approved	Pilots must not execute maneuver when request has not been approved
Pilots execute maneuver when ITP criteria are not satisfied	?
Pilots execute maneuver with incorrect climb rate, final altitude, etc	?
Pilots execute maneuver too soon before approval	?
Pilots execute maneuver too late after reassessment	?
Pilots stop maneuver before reaching designated altitude	?
Pilots continue to climb/descend beyond designated altitude	?

Controller Safety Constraints

Unsafe Control Action	Safety Constraint
Pilots execute maneuver when not approved	Pilots must not execute maneuver when request has not been approved
Pilots execute maneuver when ITP criteria are not satisfied	Pilots must not execute maneuver when ITP criteria are not satisfied
Pilots execute maneuver with incorrect climb rate, final altitude, etc	Pilots must not execute maneuver with incorrect climb rate, final altitude, etc.
Pilots execute maneuver too soon before approval	Pilots must not begin to execute maneuver before approval
Pilots execute maneuver too late after reassessment	Pilots must execute maneuver within X minutes of reassessment
Pilots stop maneuver before reaching designated altitude	Pilots must not stop maneuver before reaching designated altitude (except in emergency temination)
Pilots continue to climb/descend beyond designated altitude	Pilots must not climb/descent beyond designated altitude

STPA Process

- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure



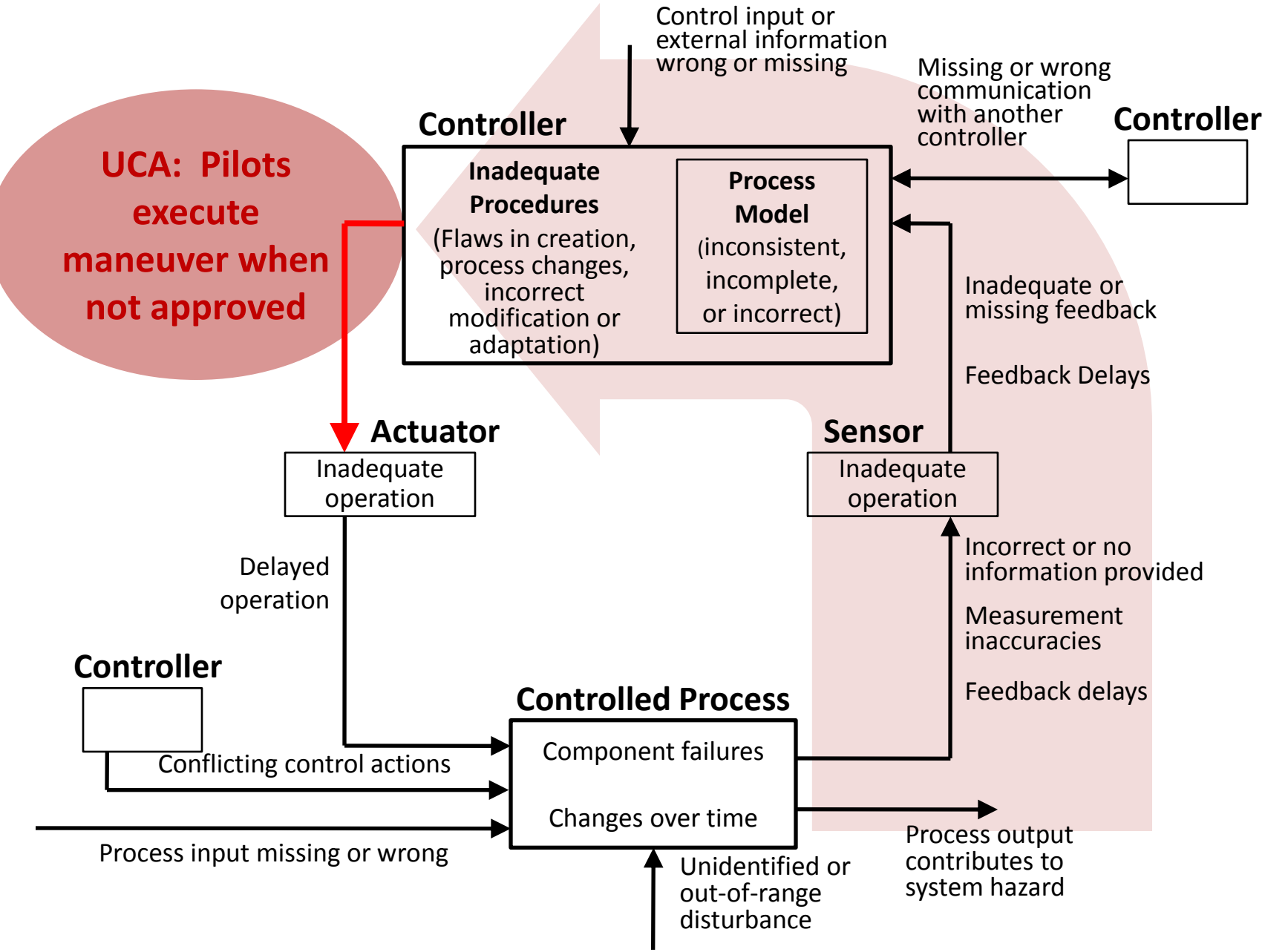
Step 1: Identify unsafe control actions and safety constraints

Step 2: Identify causal factors

STPA Step 2: Identify Causal Factors

- Select an Unsafe Control Action
- Identify potential causal factors explaining how it could happen

Step 2: Potential causes of UCAs



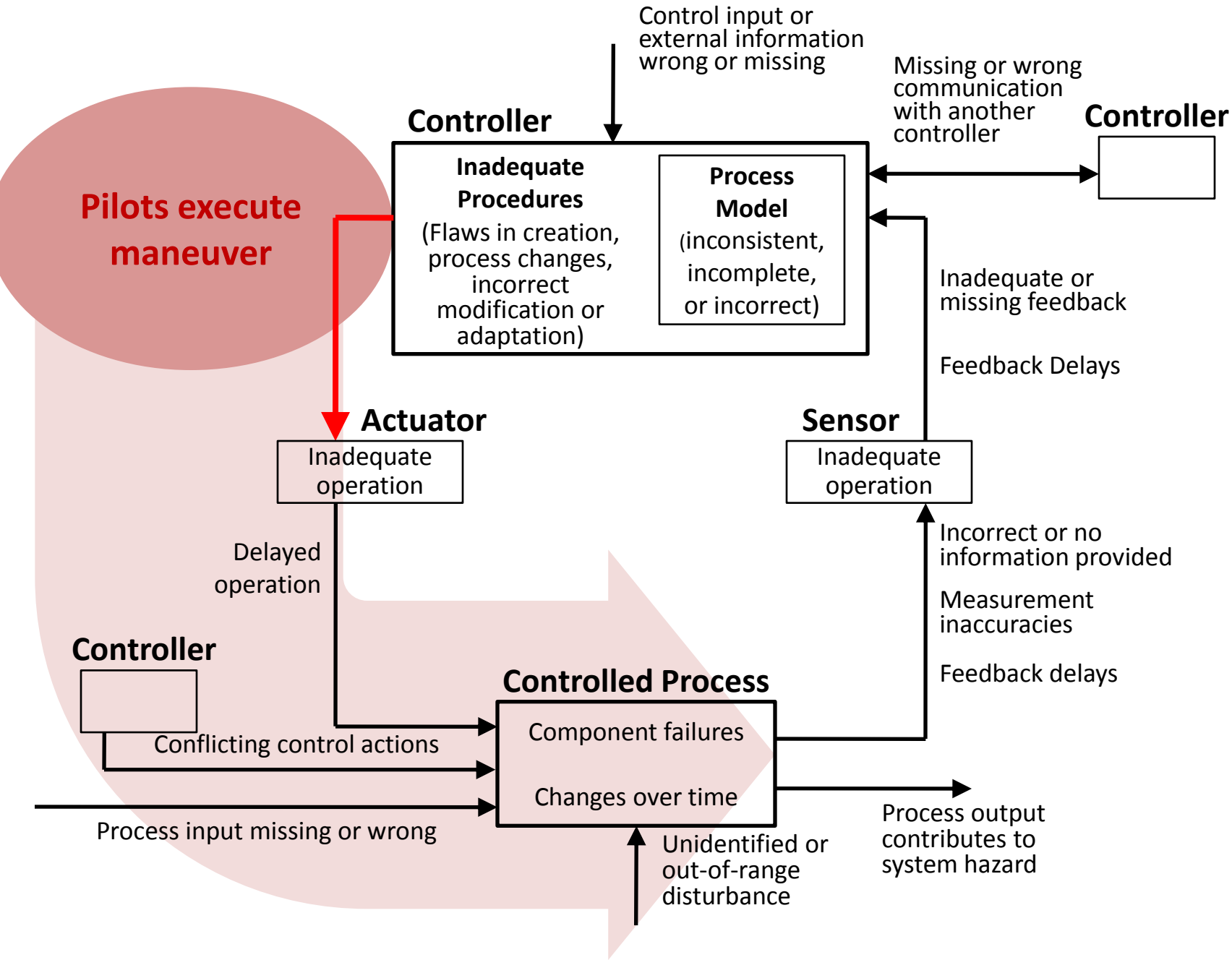
STPA Step 2: Identify Causal Factors

- ✓ Select an Unsafe Control Action
- ✓ Identify potential causal factors explaining how it could happen
- → Identify how control actions may be provided but not followed

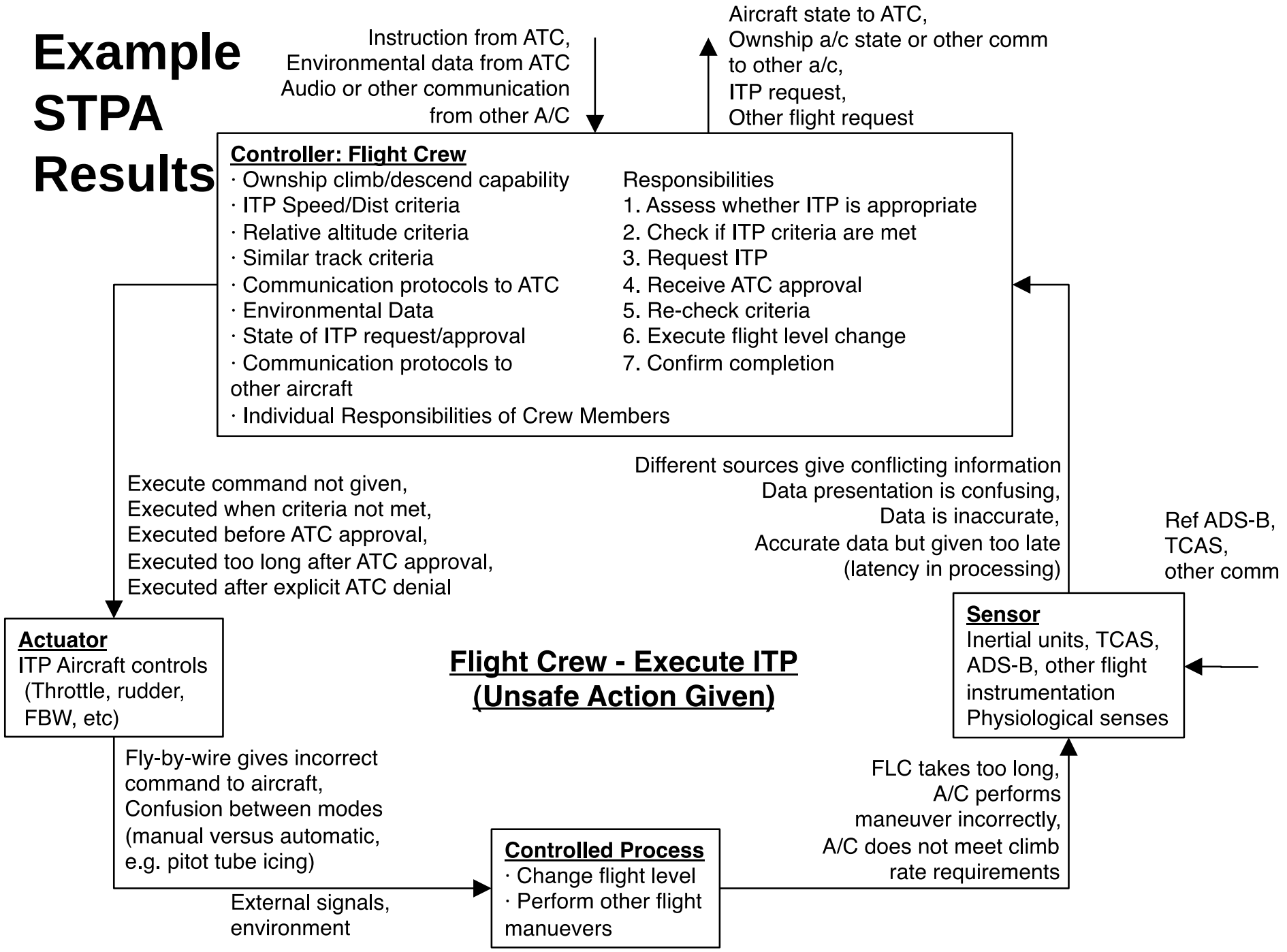
Recall the four ways unsafe control may occur:

- A control action required for safety is not provided **or is not followed**
- An unsafe control action is provided that leads to a hazard
- A potentially safe control action provided too late, too early, or out of sequence
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action)

Step 2: Potential control actions not followed



Example STPA Results



STPA Primer

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

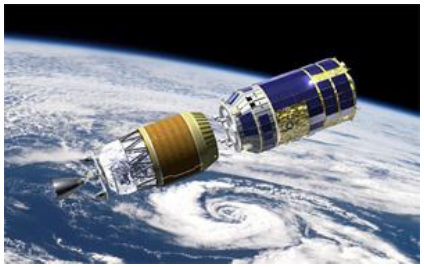
STAMP/STPA – Advanced Tutorial

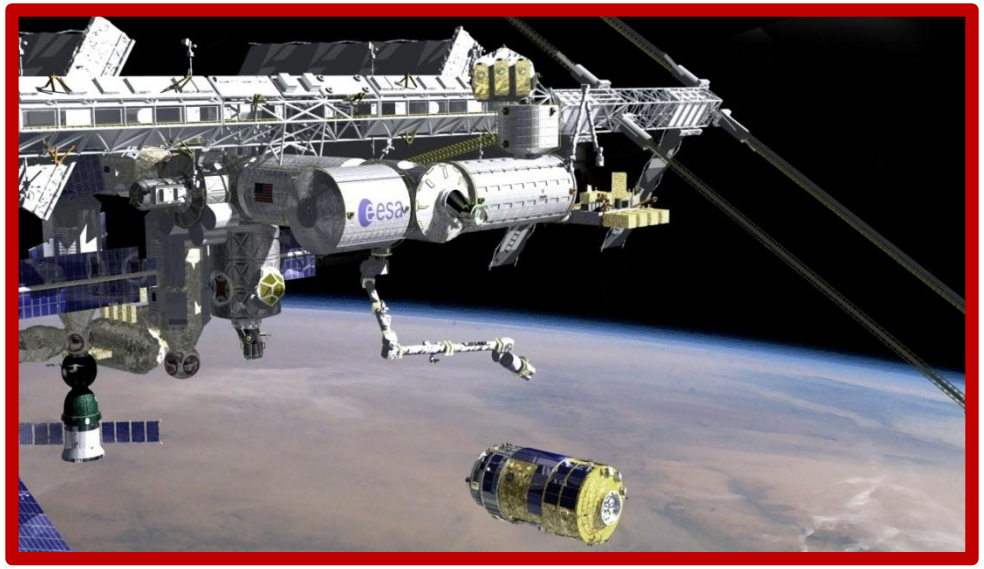
JAXA H-II Transfer Vehicle (HTV)

Takuto Ishimatsu

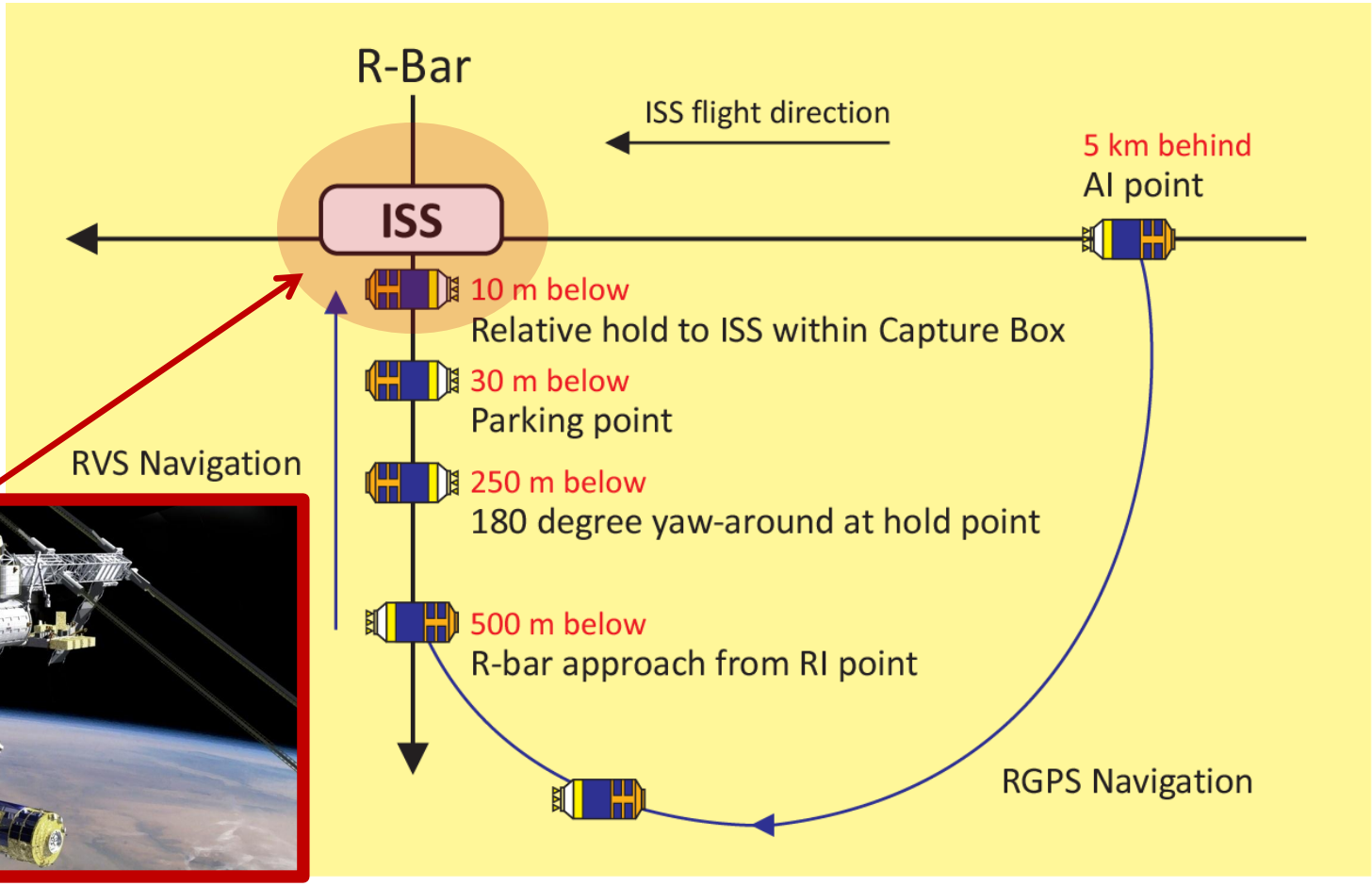
HTV: H-II Transfer Vehicle

- JAXA's unmanned cargo transfer spacecraft
  - Launched from the Tanegashima Space Center aboard the H-IIB rocket
  - Delivers supplies to the International Space Station (ISS)
  - HTV-1 (Sep '09) and HTV-2 (Jan '11) were completed successfully
  - **Proximity operations** involve the ISS (including crew) and NASA and JAXA ground stations





Capture Operation

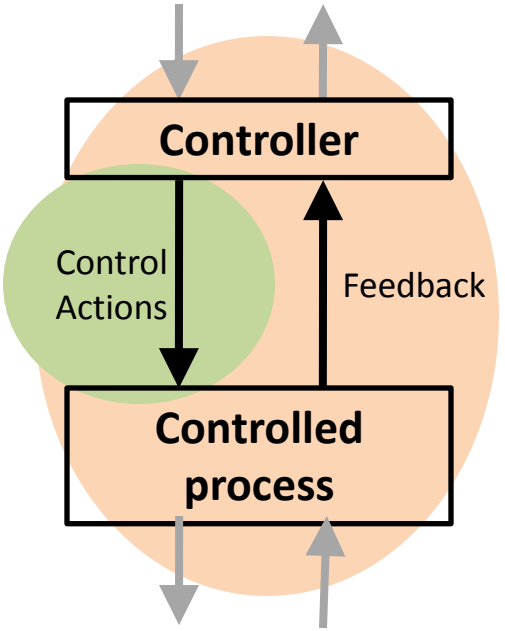


Basic Information

- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA/JAXA ground stations**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to HTV (by radio) to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** to ISS and ground stations (state vectors and flight mode)
    3. ISS crew manipulates SSRMS (robotic arm) to grapple HTV
  - If HTV drifts out of Capture Box before capture (since it is deactivated), either ISS crew or NASA/JAXA ground stations must activate HTV by sending ***Abort/Retreat/Hold*** commands
  - ISS crew and NASA/JAXA ground stations can communicate with each other using a **voice loop connection** through the entire operation

STPA Process

- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal scenarios

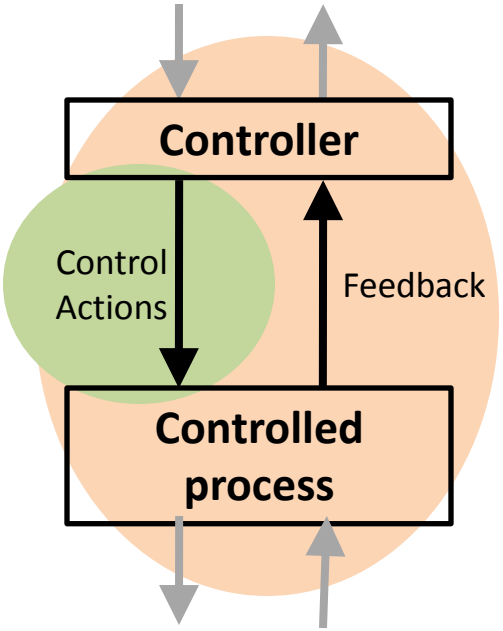


Accidents / Hazards

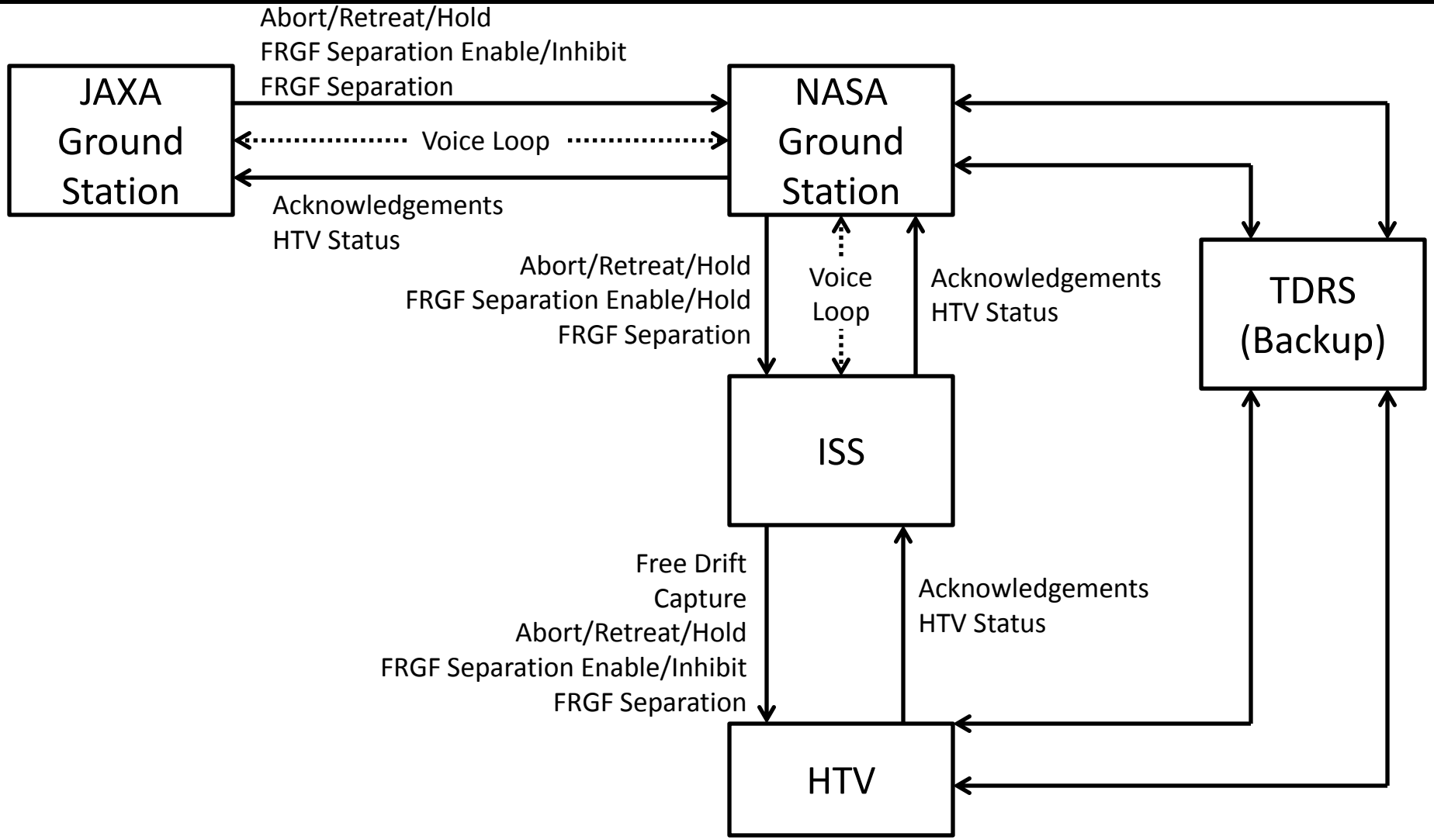
- Accidents
  - A-1: HTV collides with ISS
  - A-2: Loss of delivery mission
- System Hazards
  - ?
- System Safety Constraints
  - ?

STPA Process

- Establish foundation for analysis
  - ✓ Define accidents
  - ✓ Define system hazards
  - ✓ Rewrite hazards as safety constraints
  - Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal scenarios

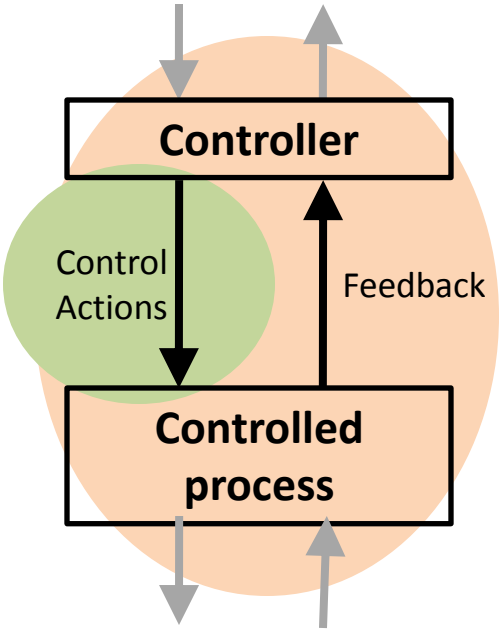


Control Structure



STPA Process

- Establish foundation for analysis
  - ✔ Define accidents
  - ✔ Define system hazards
  - ✔ Rewrite hazards as safety constraints
  - ✔ Draw safety control structure

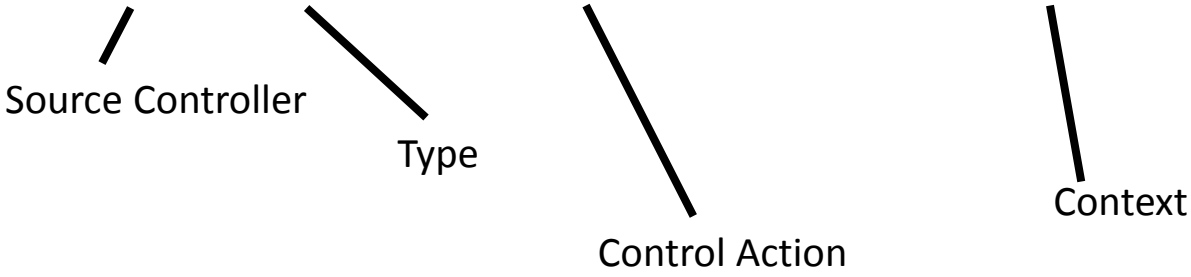


Step 1: Identify unsafe control actions and safety constraints

- Step 2: Identify causal scenarios

Unsafe Control Actions

Example:
"Pilots provide ITP maneuver when maneuver is not approved"



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Abort				
Free Drift				
Capture				

Actual Astronaut Control Interface

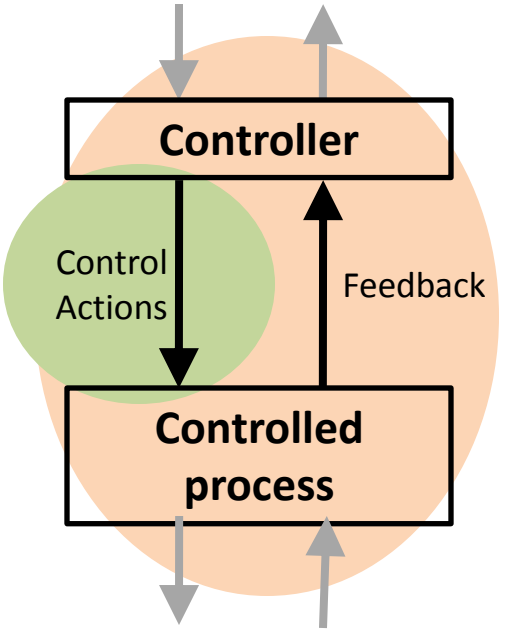
Step 1: Unsafe Control Actions

Unsafe control actions leading to Hazard H-2 (drift into ISS)

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
Free Drift (Deactivation)	[UCA4] HTV is not deactivated when ready for capture	[UCA5] HTV is deactivated when not appropriate (e.g., while still approaching ISS)	EARLY: [UCA6] HTV is deactivated while not ready for immediate capture LATE: [UCA7] HTV is not deactivated for a long time while FRGF separation is enabled	
Execute Capture	[UCA8] Capture is not executed while HTV is deactivated	[UCA9] Capture is attempted when HTV is not deactivated [UCA10] SSRMS hits HTV inadvertently	EARLY: [UCA11] Capture is executed before HTV is deactivated LATE: [UCA12] Capture is not executed within a certain amount of time	[UCA13] Capture operation is stopped halfway and not completed
Abort Retreat Hold	[UCA17] Abort/Retreat/Hold is not executed when necessary (e.g., when HTV is drifting to ISS while uncontrolled)	[UCA18] Abort/Retreat/Hold is executed when not appropriate (e.g. after successful capture)	LATE: [UCA19] Abort/Retreat/Hold is executed too late when immediately necessary (e.g., when HTV is drifting to ISS while uncontrolled)	

STPA Process

- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure



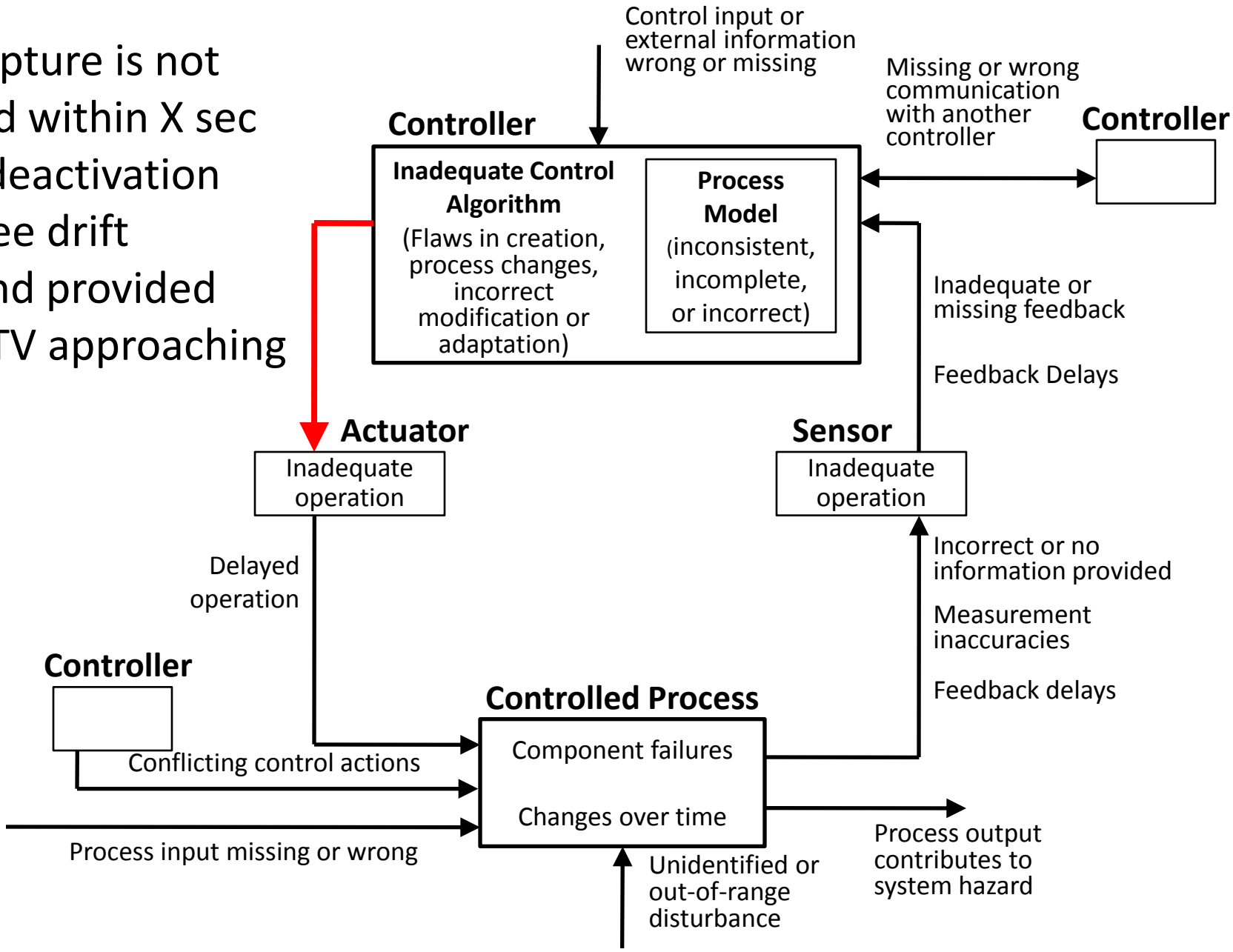
Step 1: Identify unsafe control actions and safety constraints

Step 2: Identify causal scenarios

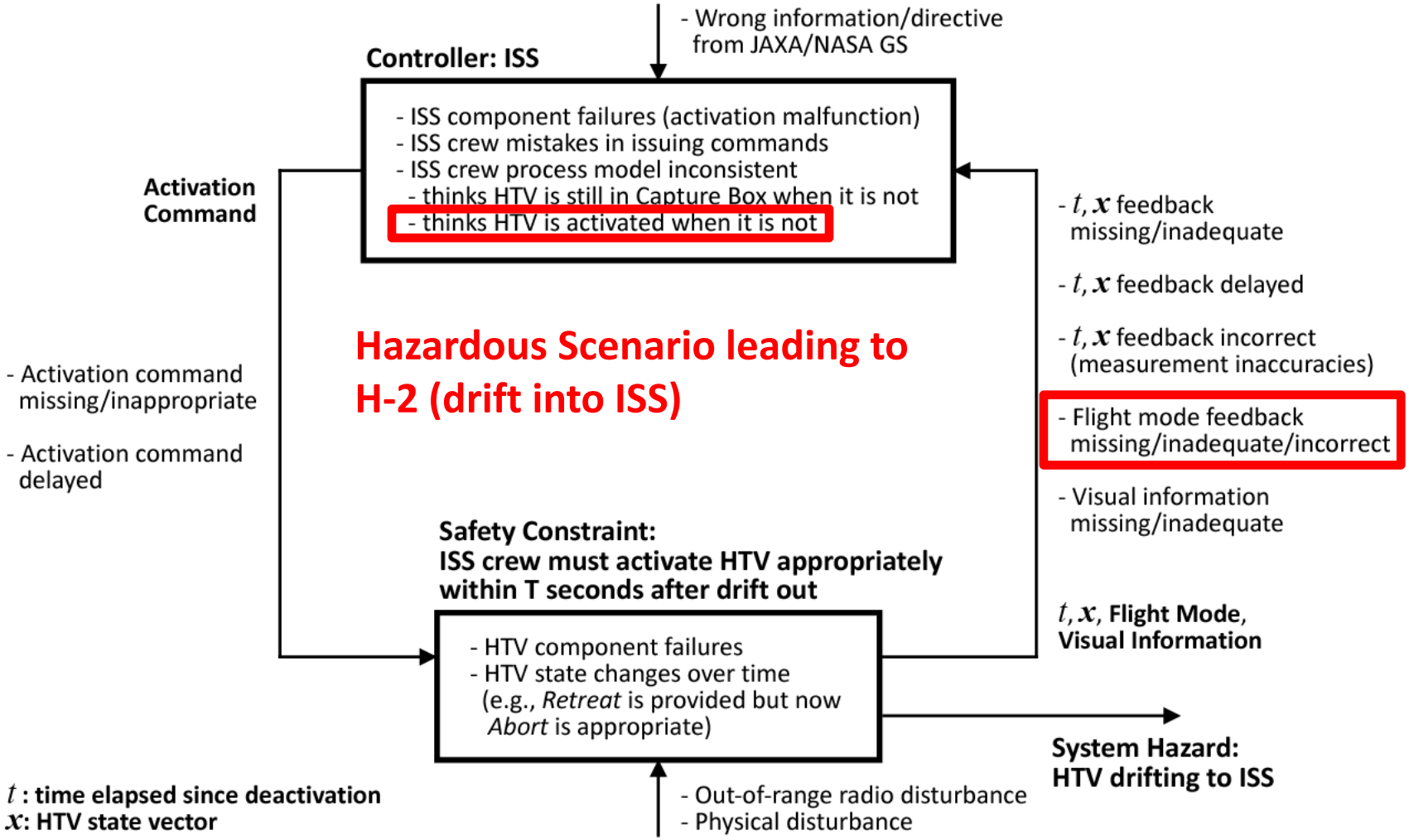
Step 2: Identify causal scenarios

UCA: Capture is not executed within X sec of HTV deactivation

UCA: Free drift command provided while HTV approaching ISS



Step 2: Causal Factors leading to H-2



Rigorous method for STPA Step 1

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?

Example: Train door controller

System Hazards

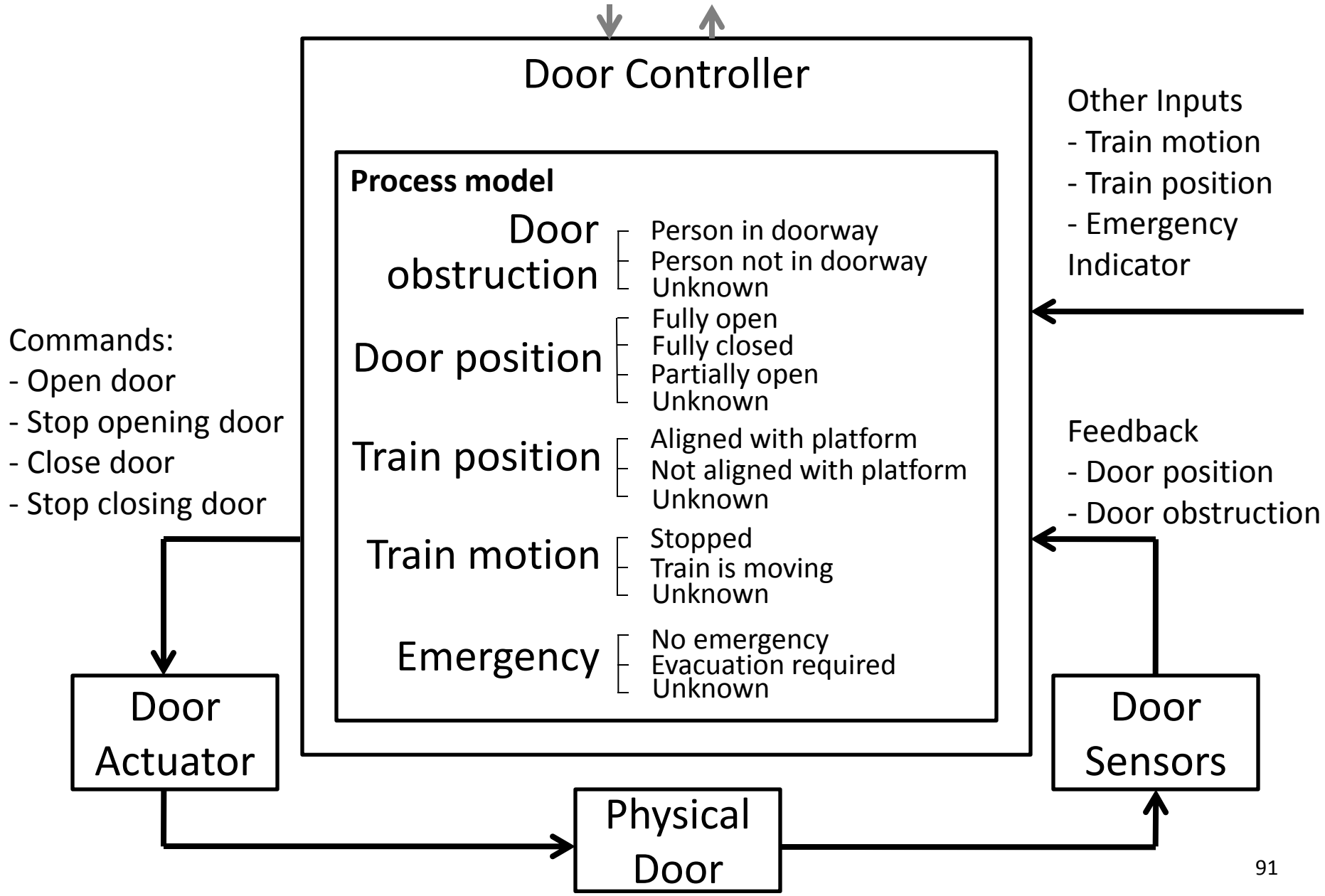
H-1: Doors close on a person in the doorway

H-2: Doors open when the train is moving or not at platform

H-3: Passengers/staff are unable to exit during an emergency

Image: http://upload.wikimedia.org/wikipedia/commons/f/fe/Mbta-redline-bombardier.jpg

Example: Control loop



1) Control action is provided

- Control action: *Door Open* command
- 1a) Define potential contexts (combinations of process model variables)

Control Action	Train Motion	Emergency	Train Position	Door Obstruction	Door Position
Door open command	Stopped	No	Aligned with platform	Not obstructed	Closed
Door open command	Stopped	No	Aligned with platform	Not obstructed	Open
Door open command	Stopped	Yes	Aligned with platform	Obstructed	Closed
…	…	…	…	…	…

1) Control action is provided

Control action: *Door Open* command

- 1a) Define potential contexts (combinations of process model variables)
- 1b) Determine whether the control action is hazardous in each context

Control Action	Train Motion	Emergency	Train Position	Door Obst. / Position	Hazardous?
Door open cmd when:	Moving	No	(doesn't matter)	(doesn't matter)	**Yes**
Door open cmd when:	Moving	Yes	(doesn't matter)	(doesn't matter)	**Yes***
Door open cmd when:	Stopped	Yes	(doesn't matter)	(doesn't matter)	**No**
Door open cmd when:	Stopped	No	Not at platform	(doesn't matter)	**Yes**
Door open cmd when:	Stopped	No	At platform	(doesn't matter)	**No**

*Design decision: In this situation, evacuate passengers to other cars. Meanwhile, stop the train and then open doors.

1) Control action is provided

Control action: *Door Open* command

- 1a) Define potential contexts (combinations of process model variables)
- 1b) Determine whether the control action is hazardous in each context
- 1c) Determine whether control action can still be hazardous if too early/too late

Control Action	Train Motion	Emergency	Train Position	Door Obst. / Position	Hazardous ?	Hazardous if provided too early?	Hazadous if provided too late?
Door open command	Moving	No	(doesn't matter)	(doesn't matter)	**Yes**	**Yes**	**Yes**
Door open command	Moving	Yes	(doesn't matter)	(doesn't matter)	**Yes***	**Yes***	**Yes***
Door open command	Stopped	Yes	(doesn't matter)	(doesn't matter)	**No**	**No**	**Yes**
Door open command	Stopped	No	Not at platform	(doesn't matter)	**Yes**	**Yes**	**Yes**
Door open command	Stopped	No	At platform	(doesn't matter)	**No**	**No**	**No**

2) Control action is not provided

Control action: *Door Open* command

- 2a) Identify process model variables
- 2b) Determine whether the absence of control action is hazardous in each context

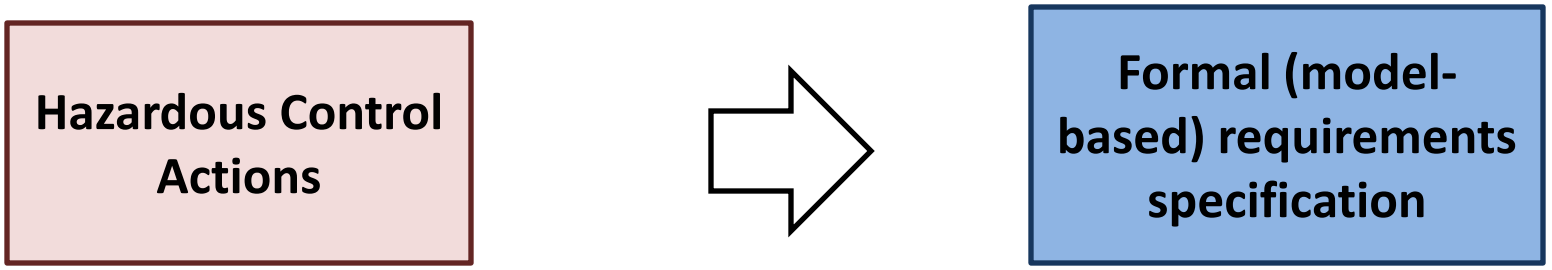
Control Action	Train Motion	Emergency	Train Position	Door Obst. / Pos.	Hazardous?
Door open command not provided	Stopped	Yes	(doesn't matter)	(doesn't matter)	**Yes**
Door open command not provided	Stopped	(doesn't matter)	(doesn't matter)	Closing on obstruction	**Yes**
Door open command not provided	(all others)				**No**

Resulting List of Hazardous Control Actions

Hazardous Control Actions
Door open command provided while train is moving and there is no emergency
Door open command provided too late while train is stopped and emergency exists
Door open command provided while train is stopped, no emergency, and not at platform
Door open command provided while train is moving and emergency exists
Door open command not provided while train is stopped and emergency exists
Door open command not provided while doors are closing on someone

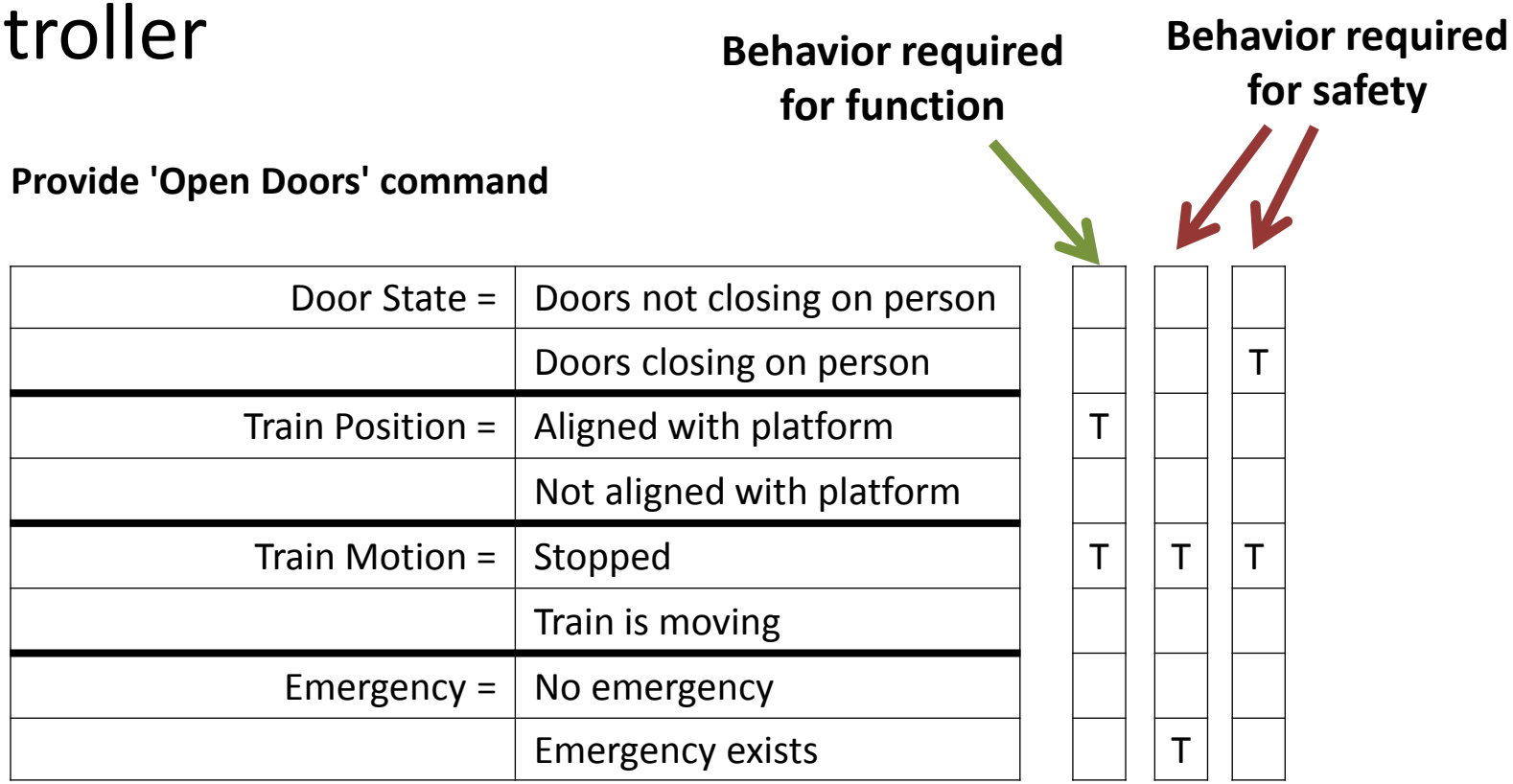
Parts of this can be automated!

Automatically generating safety requirements



Generating safety requirements

- Example: Generated black-box model for door controller

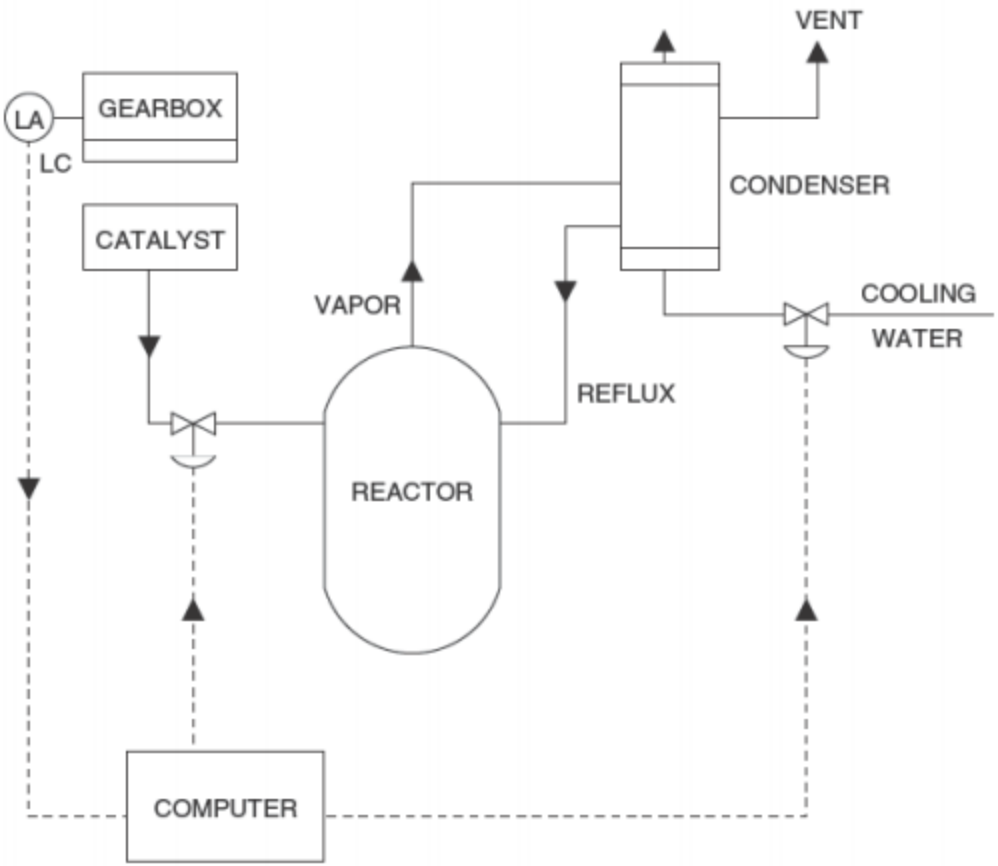


Method can help integrate safety requirements with functional requirements

Chemical Reactor

Chemical Reactor Design

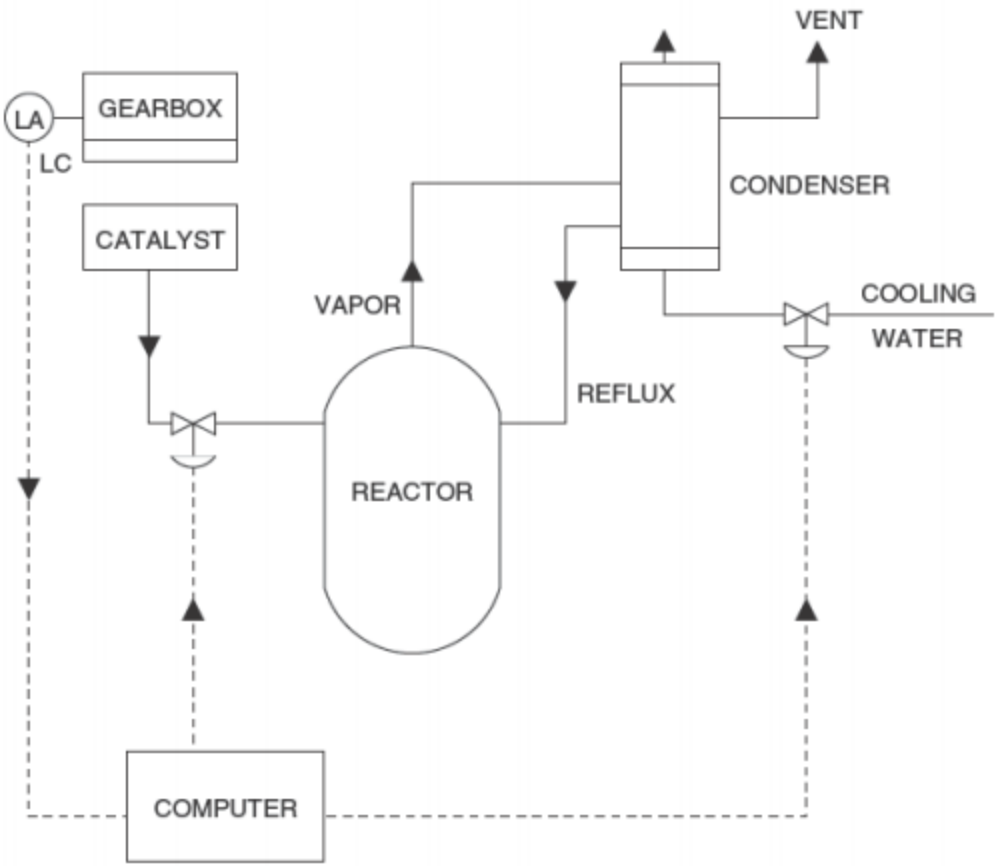
- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling



What are the accidents, system hazards, system safety constraints?

Chemical Reactor Design

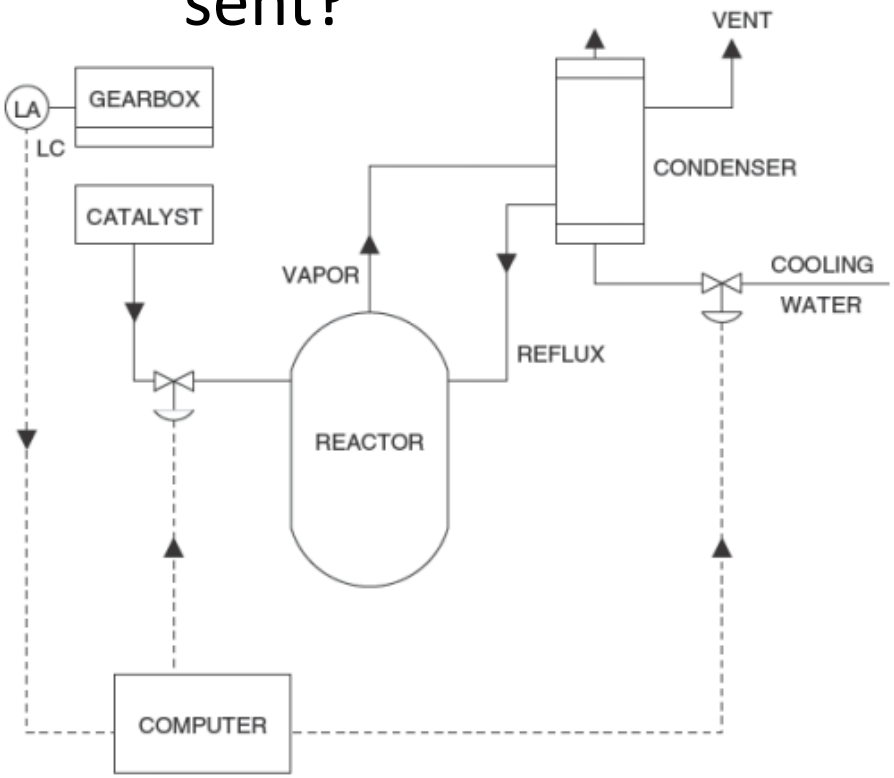
- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

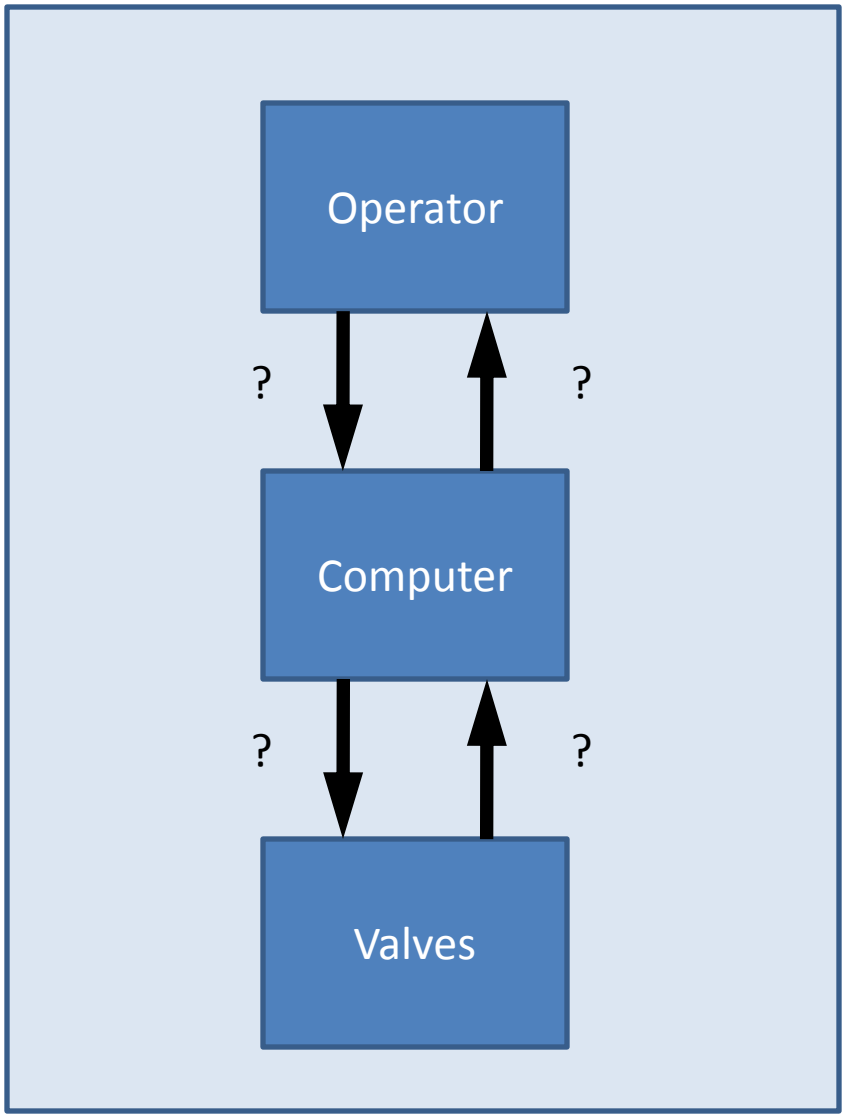


Create Control Structure

STPA Analysis

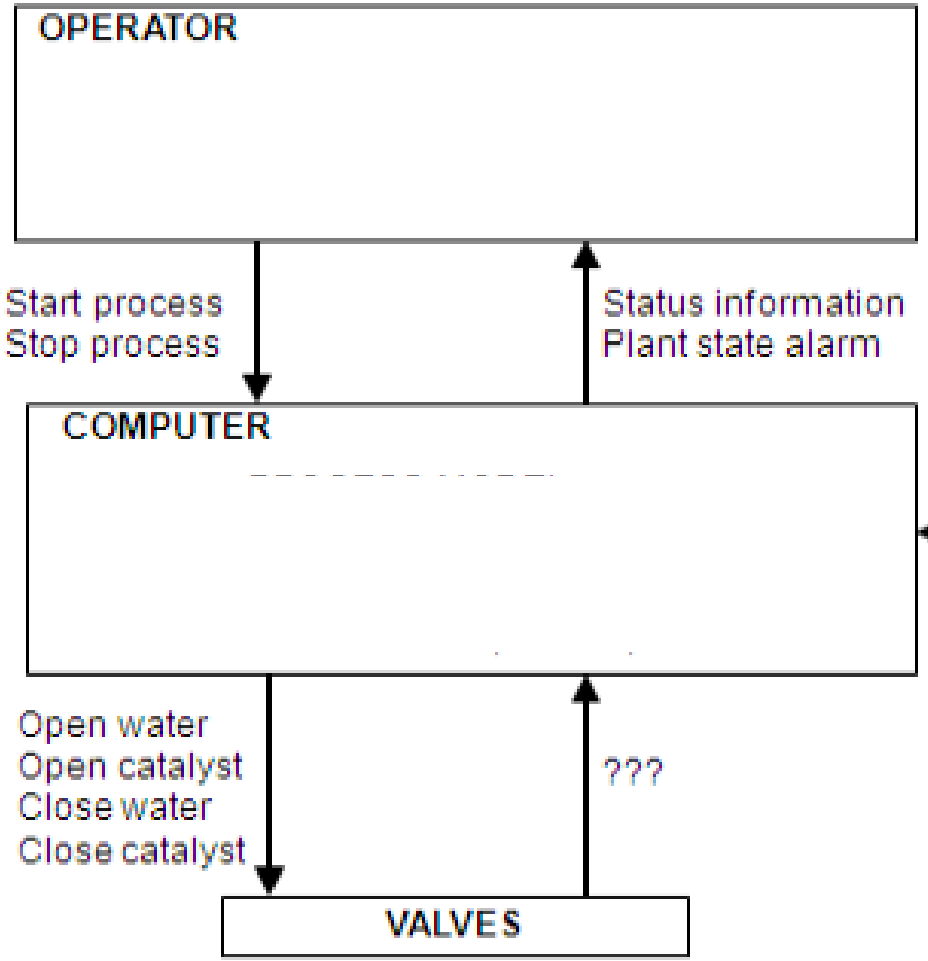
- High-level (simple) Control Structure
  - What commands are sent?

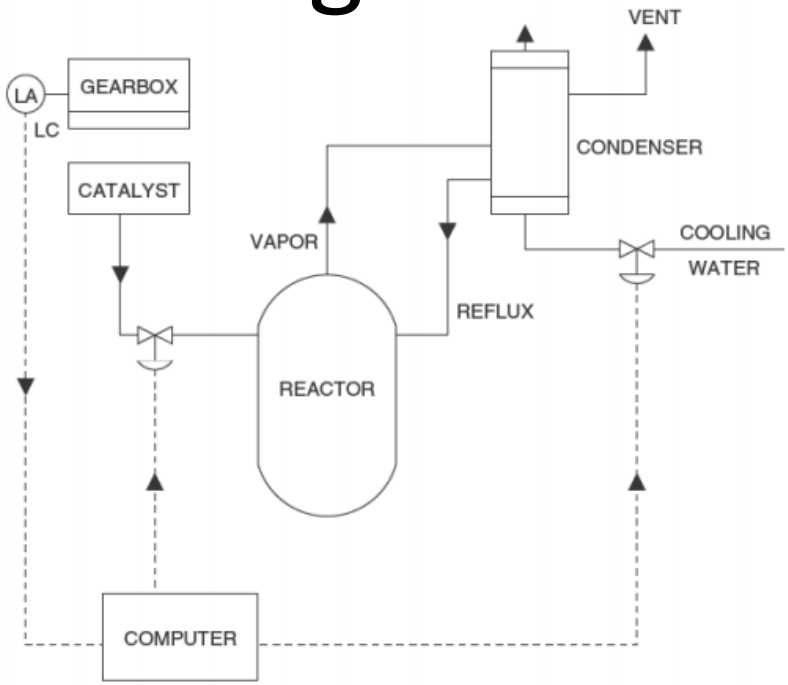




Chemical Reactor Design

Control Structure:

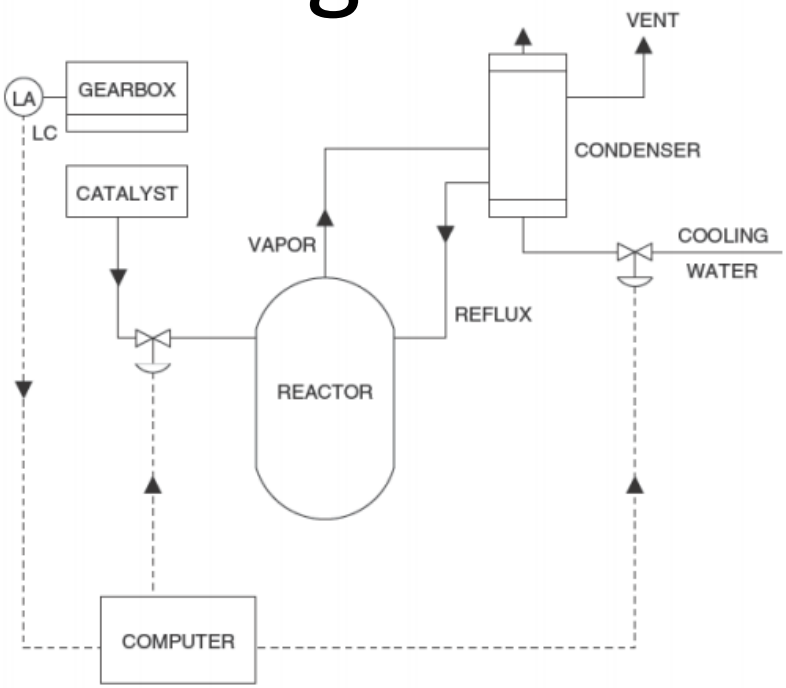


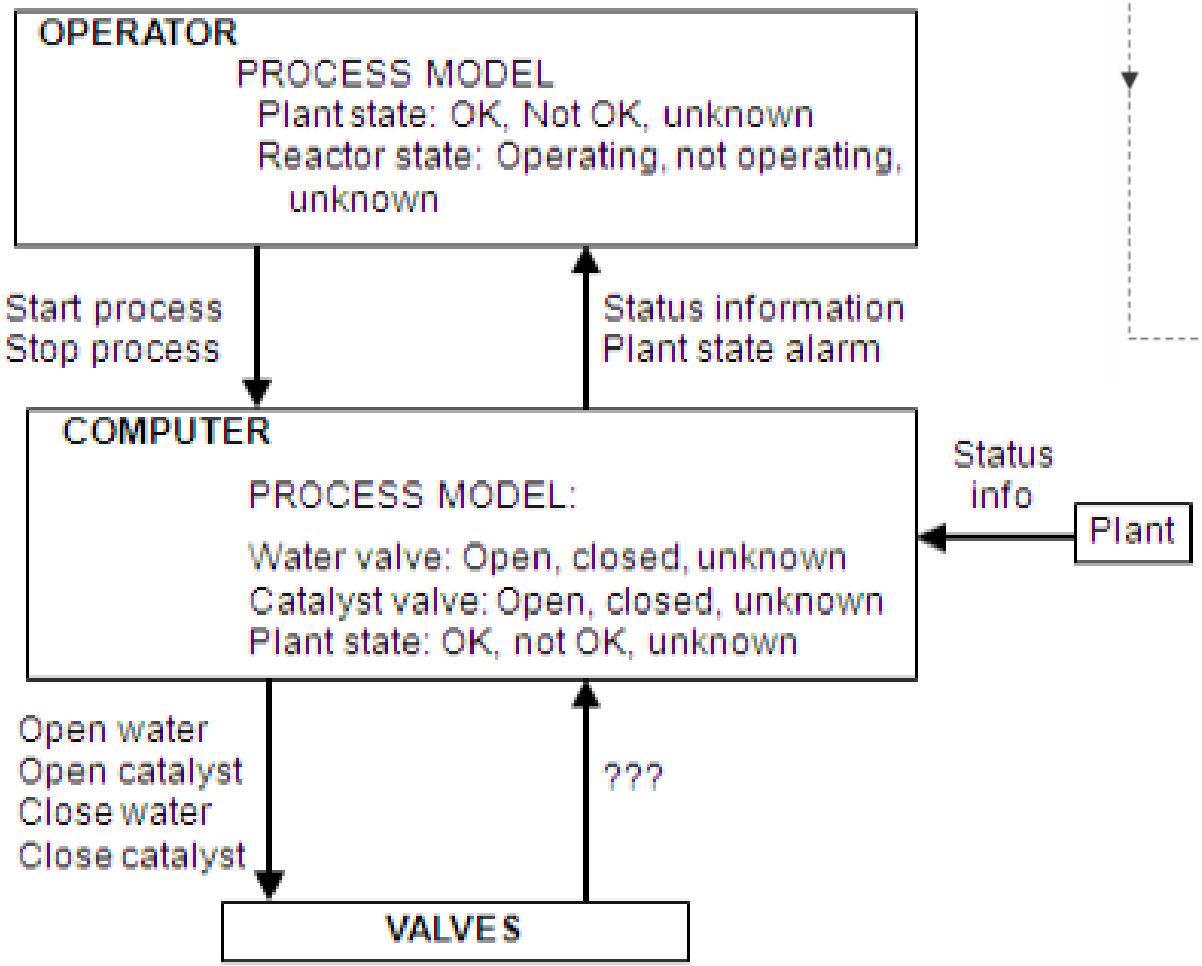


What are the process model variables?

Chemical Reactor Design

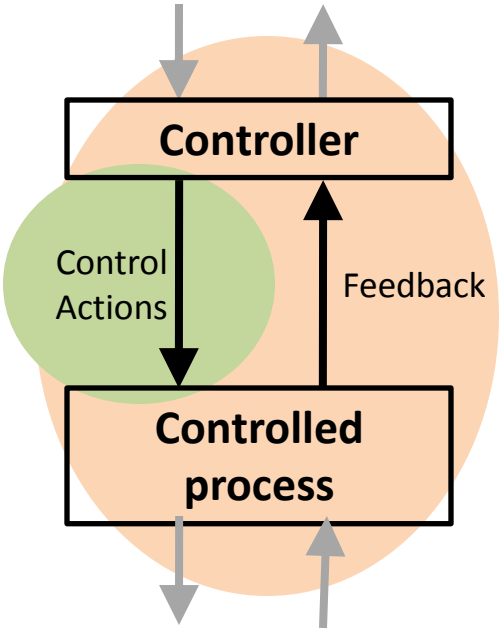
Control Structure:





STPA Process

- Establish foundation for analysis
  - ✔ Define accidents
  - ✔ Define system hazards
  - ✔ Rewrite hazards as safety constraints
  - ✔ Draw safety control structure

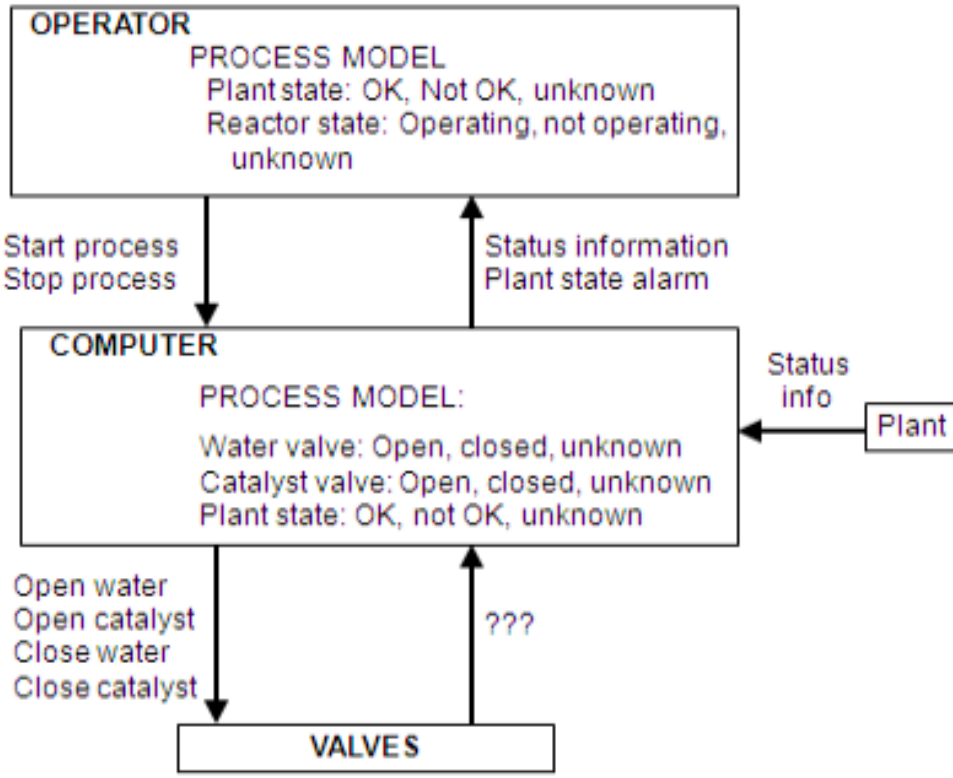


Step 1: Identify unsafe control actions and safety constraints

- Step 2: Identify causal scenarios

Chemical Reactor

Control Structure:



Identify Unsafe Control Actions

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Open Water Valve	**Computer does not open water valve when catalyst open**			

Rigorous UCA identification

Control Action	Water valve	Catalyst valve	Plant state	Hazardous if provided?	Hazardous if not provided?
Open water valve when:	Open	Open	OK	No	No
Open water valve when:	Open	Closed	OK	No	No
Open water valve when:	Closed	Open	OK	No	Yes
Open water valve when:	Closed	Closed	OK	No	No
Open water valve when:	Open	Open	Not OK	No	No
Open water valve when:	Open	Closed	Not OK	No	No
Open water valve when:	Closed	Open	Not OK	No	Yes
Open water valve when:	Closed	Closed	Not OK	No	No

Rigorous UCA identification

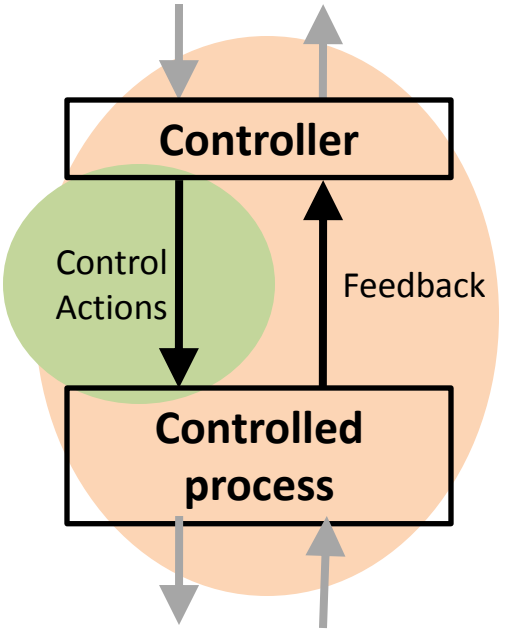
Control Action	Water valve	Catalyst valve	Plant state	Hazardous if provided?	Hazardous if not provided?
Open water valve when:	Open	Open	(doesn't matter)	**No**	**No**
Open water valve when:	(doesn't matter)	Closed	(doesn't matter)	**No**	**No**
Open water valve when:	Closed	Open	(doesn't matter)	**No**	**Yes**

UCA-1: Computer does not opens water valve when catalyst valve is open and water valve is closed

SC-1: Computer must open the water valve whenever the catalyst valve is open

STPA Process

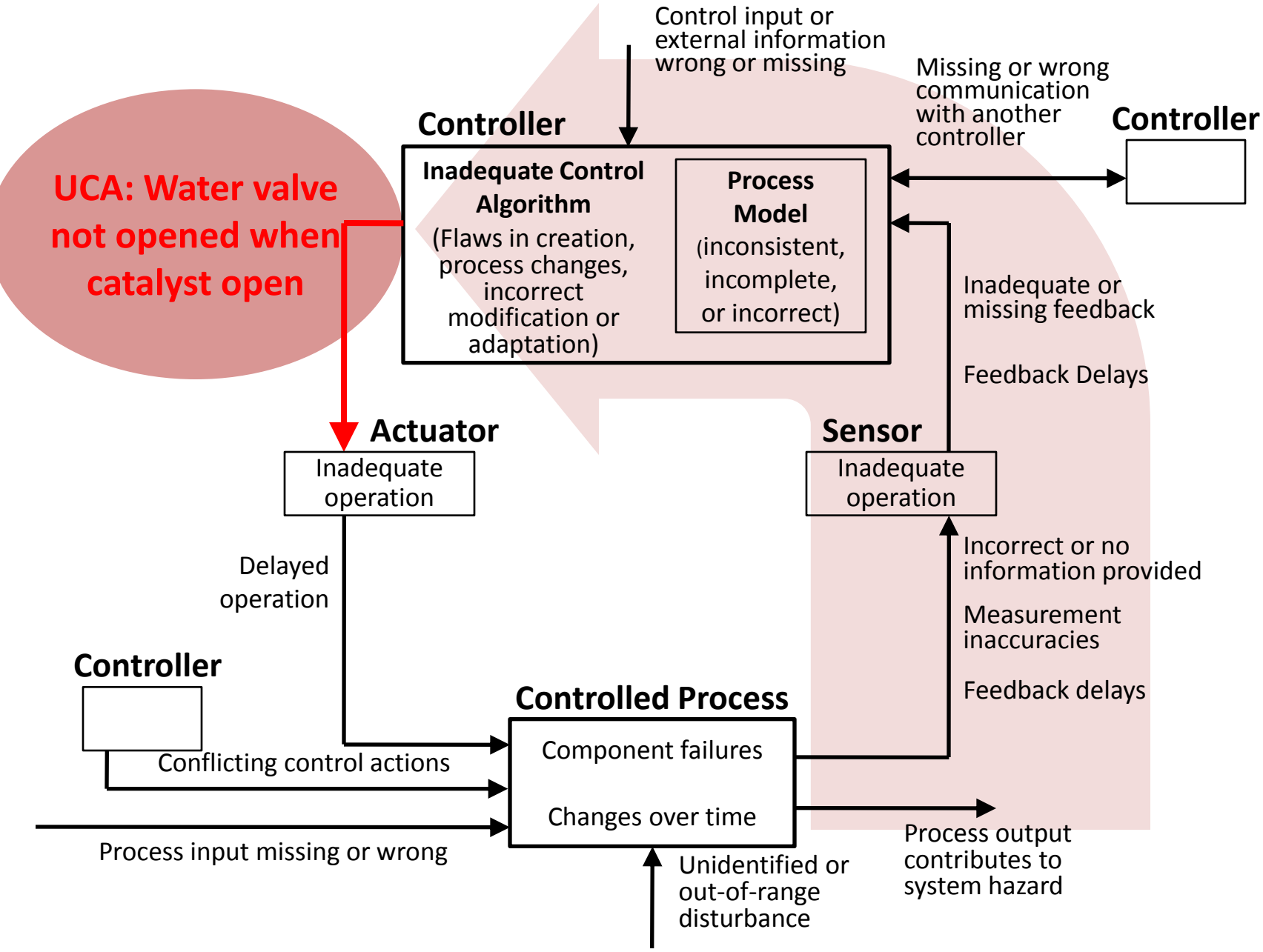
- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure



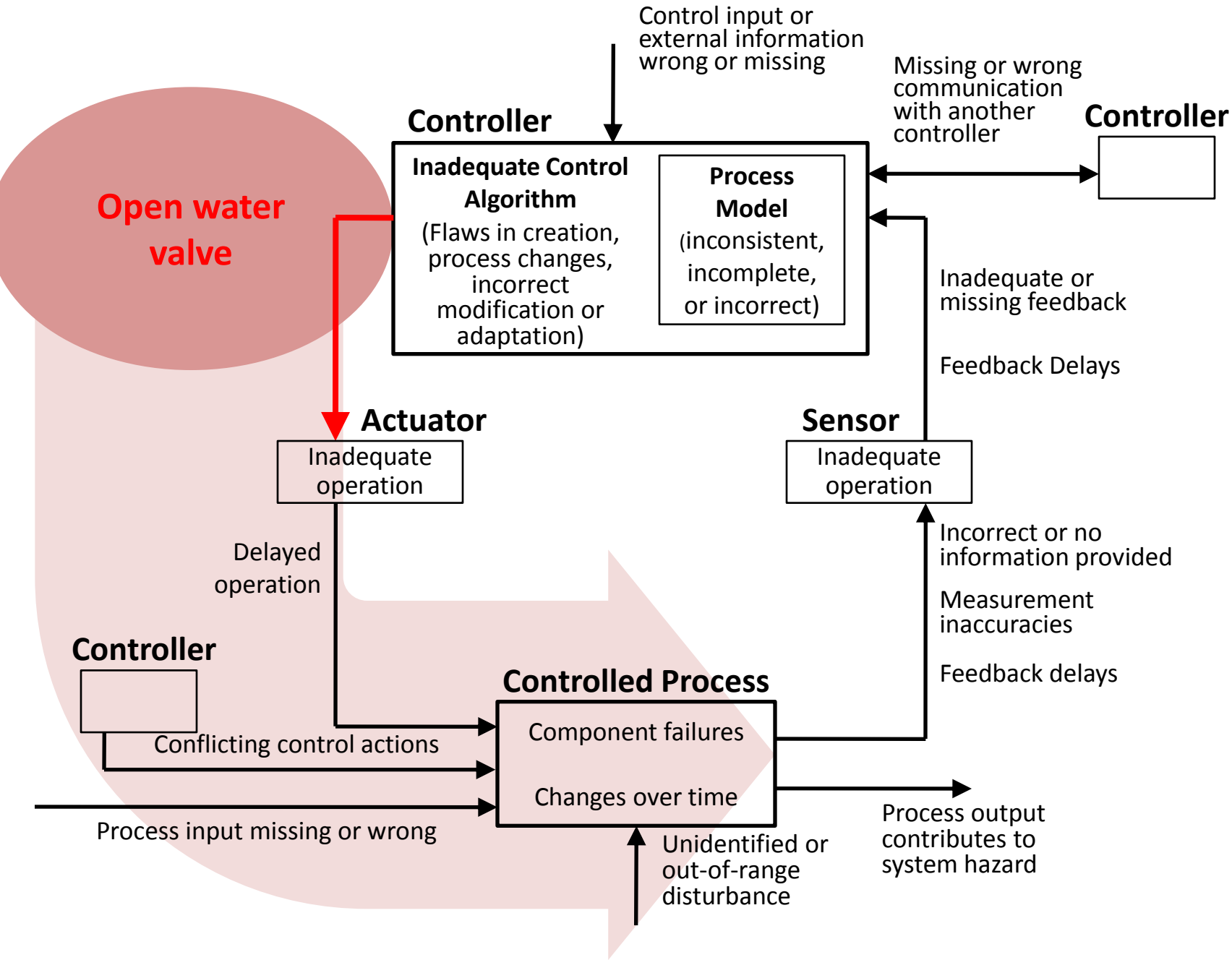
Step 1: Identify unsafe control actions and safety constraints

Step 2: Identify causal scenarios

Step 2: Potential causes of UCAs



Step 2: Potential control actions not followed



Additional Steps

Additional steps

- Use causal analysis to identify detailed safety design requirements and design options
- Iterate top-down
  - Refine into more detailed control structures
  - Refine safety constraints (requirements) into more detailed requirements for each component

See examples of these in my presentation tomorrow

Operations and Performance Monitoring

Consider how designed controls could degrade over time

Use STPA results to build in protection:

a) Planned performance audits where assumptions underlying the hazard analysis are the preconditions for the operational audits and controls

b) Management of change procedures

c) Incident/accident analysis

How does STPA compare?

- MIT: TCAS
  - Existing high quality fault tree done by MITRE for FAA
  - MIT comparison: STPA found everything in fault tree, plus more
- JAXA: HTV
  - Existing fault tree reviewed by NASA
  - JAXA comparison: STPA found everything in fault tree, plus more
- EPRI: HPCI/RCIC
  - Existing fault tree & FMEA overlooked causes of real accident
  - EPRI comparison: Blind study, only STPA found actual accident scenario
- Safeware: U.S. Missile Defense Agency BMDS
  - Existing hazard analysis per U.S. military standards
  - Safeware comparison: STPA found everything plus more
  - STPA took 2 people 3 months, MDA took 6 months to fix problems
- MIT: NextGen ITP
  - Existing fault tree & event tree analysis by RTCA
  - MIT comparison: STPA found everything in fault tree, plus more
- MIT: Blood gas analyzer
  - Existing FMEA found 75 accident causes
  - STPA by S.M. student found 175 accident causes
  - STPA took less effort, found 9 scenarios that led to FDA Class 1 recall

Applications

- Adaptive cruise control system
- Proton therapy machine
- Safety analysis of new missile defense system (MDA)
- Safety-driven design of new JPL outer planets explorer
- Safety analysis of the JAXA HTV (unmanned cargo spacecraft to ISS)
- Incorporating risk into early trade studies (NASA Constellation)
- Orion (Space Shuttle replacement)
- Safety of maglev trains (Japan Central Railway)
- NextGen (for NASA)
- Accident/incident analysis (aircraft, petrochemical plants, air traffic control, railway accident, …)

Additional info

- Google: “STPA Primer”
- MIT STAMP Conference in March
  - Google: “MIT STAMP Conference”
  - Website has past presentations
- Sunnyday.mit.edu
  - Additional STAMP papers, examples