Systems Theoretic Process Analysis (STPA)

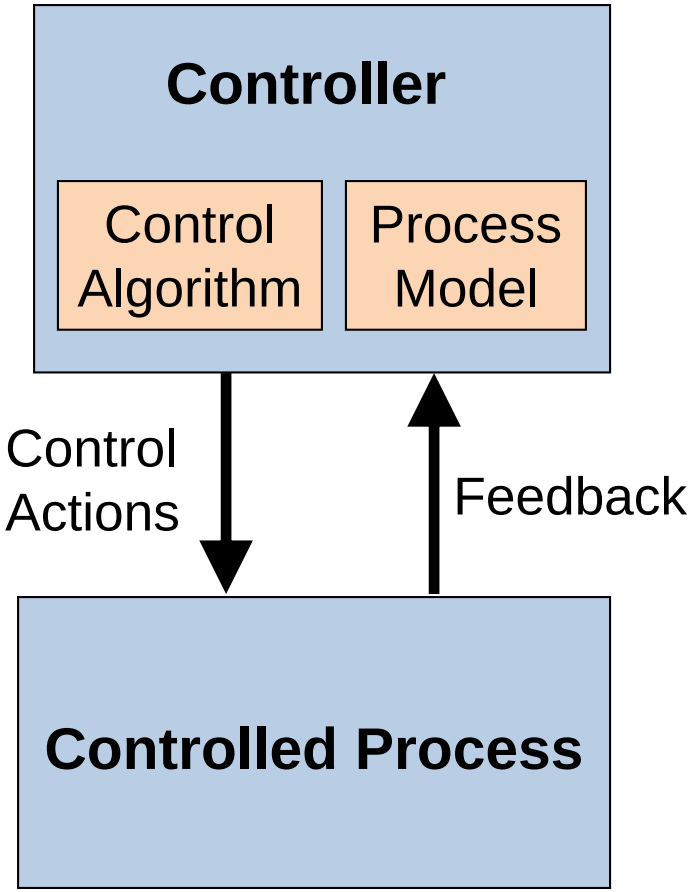
Systems approach to safety engineering (STAMP)

STAMP Model

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

(Leveson, 2012)

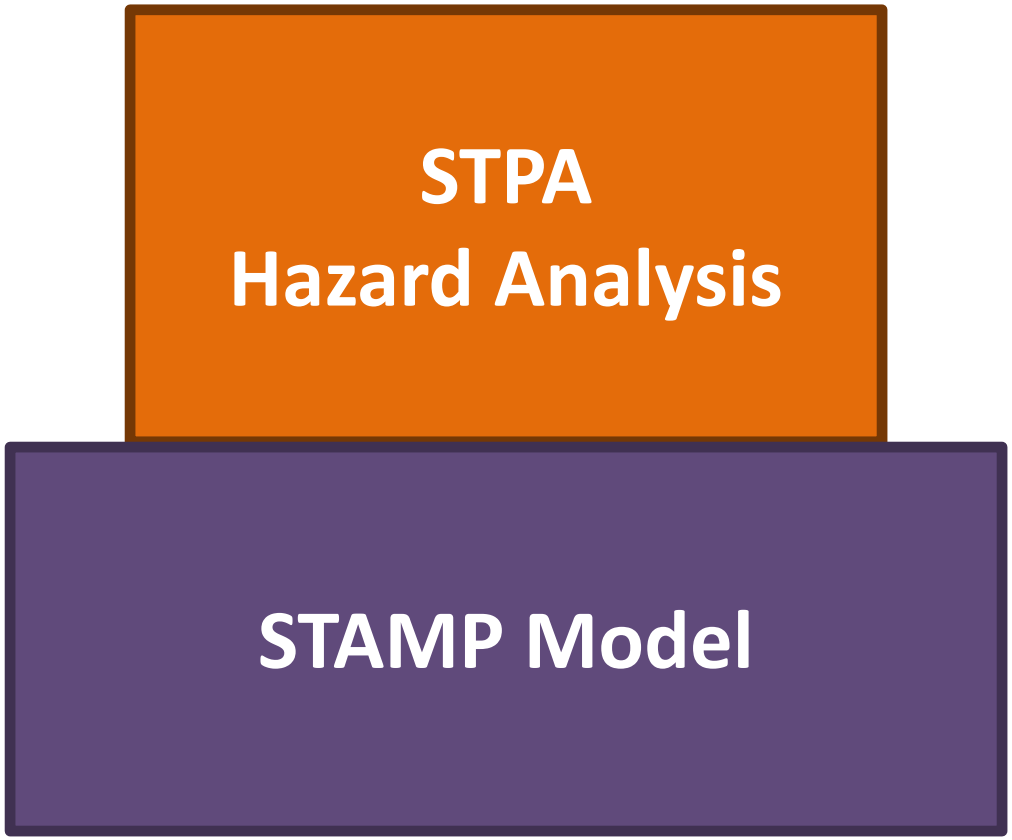
STAMP: basic control loop



- Controllers use a **process model** to determine control actions
  - Accidents often occur when the process model is incorrect
- A good model of both software and human behavior in accidents
- Four types of **unsafe 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

(Leveson, 2012)

STAMP and STPA



How do we find inadequate control in a design?

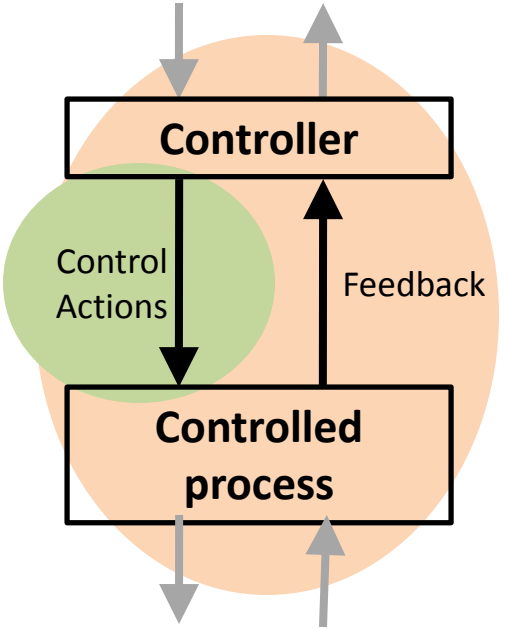
Accidents are caused by inadequate control

STPA
(System-Theoretic Process Analysis)

STPA Hazard Analysis

STAMP Model

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



Can capture requirements flaws, software errors, human errors

(Leveson, 2012)

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

- System 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**
- System 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
  - Something we want to **prevent**

System Accident	System Hazard
People die from exposure to toxic chemicals	Toxic chemicals from the plant are in the atmosphere

Definitions

- System 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**
- System 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
  - Something we want to **prevent**

System 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

Definitions

- System 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.

Broad view of safety

"Accident" is anything that is unacceptable, that must be prevented.

Not limited to loss of life or human injury!

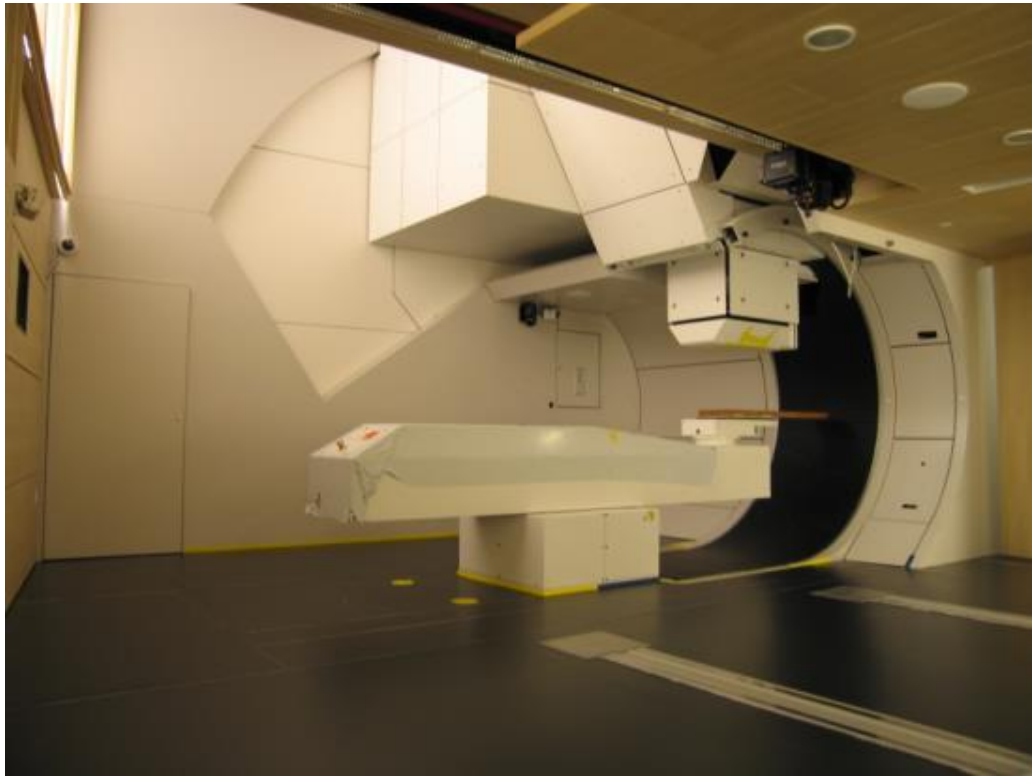
People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

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

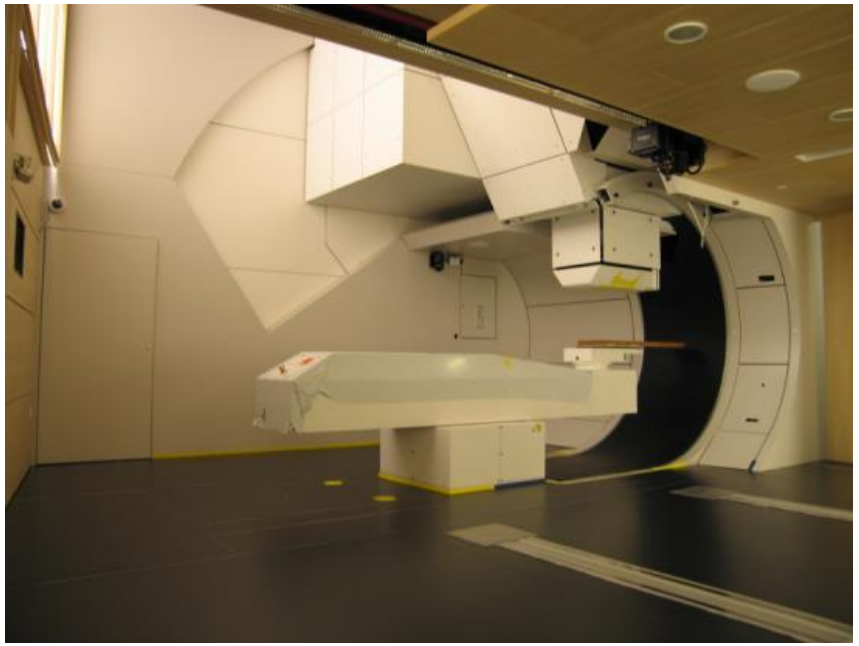
Proton Radiation Therapy System
Paul Scherrer Institute, Switzerland



- Accidents?
- Hazards?

Proton Therapy Machine (Antoine)

- Accidents
  - ACC1. Patient injury or death
  - ACC2. Ineffective treatment
  - ACC3. Loss to non-patient quality of life (esp. personnel)
  - ACC4. Facility or equipment damage
- Hazards
  - ?



Antoine PhD Thesis, 2012

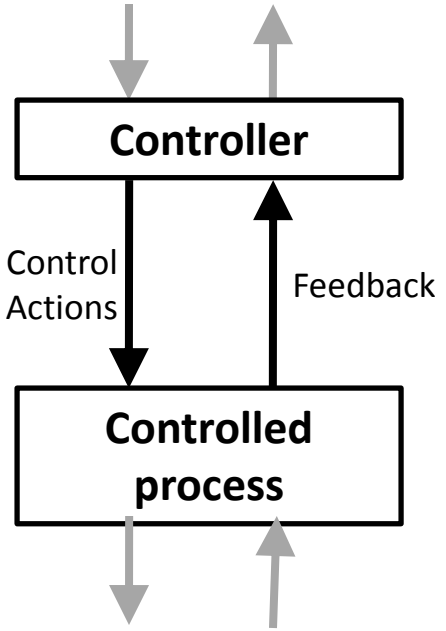
Proton Therapy Machine (Antoine)

- Accidents
  - ACC1. Patient injury or death
  - ACC2. Ineffective treatment
  - ACC3. Loss to non-patient quality of life (esp. personnel)
  - ACC4. Facility or equipment damage
- Hazards
  - H-R1. Patient tissues receive more dose than clinically desirable
  - H-R2. Patient tumor receives less dose than clinically desirable
  - H-R3. Non-patient (esp. personnel) is unnecessarily exposed to radiation
  - H-R4. Equipment is subject to unnecessary stress

Antoine PhD Thesis, 2012

STPA
(System-Theoretic Process Analysis)

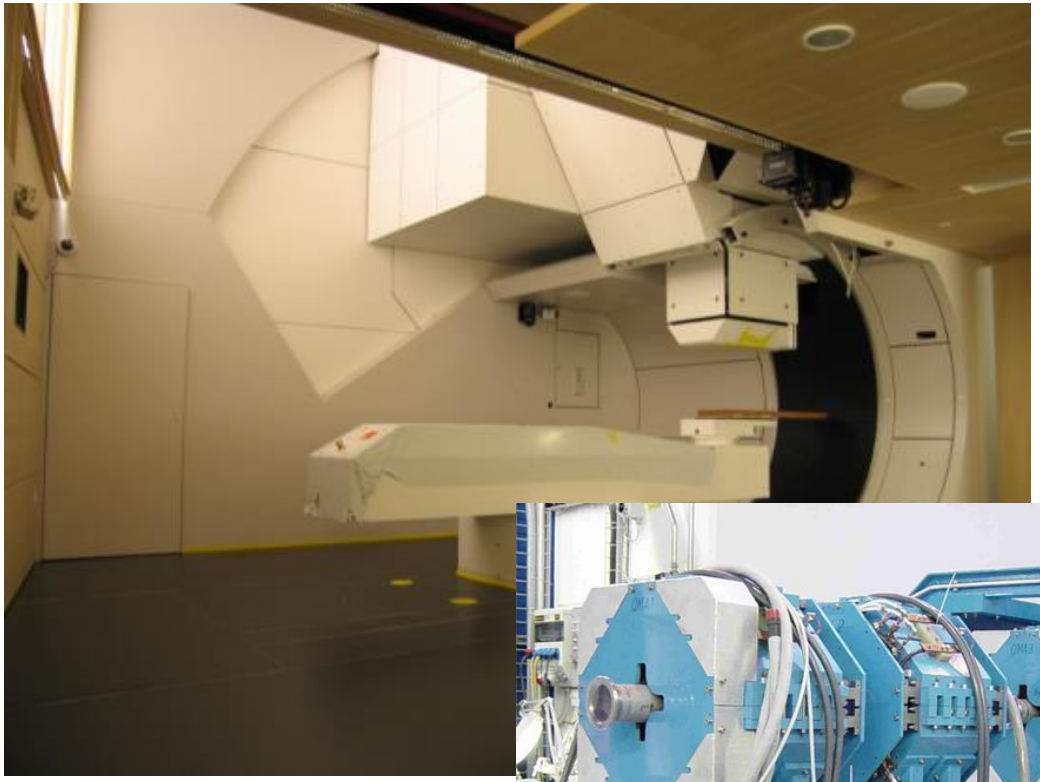
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



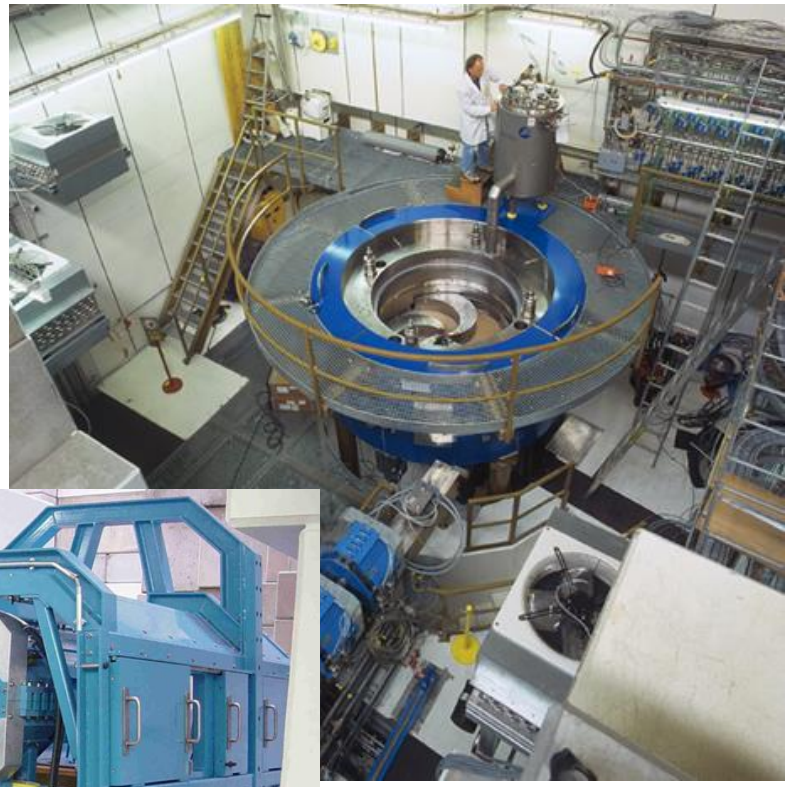
(Leveson, 2012)

Control Structure Examples

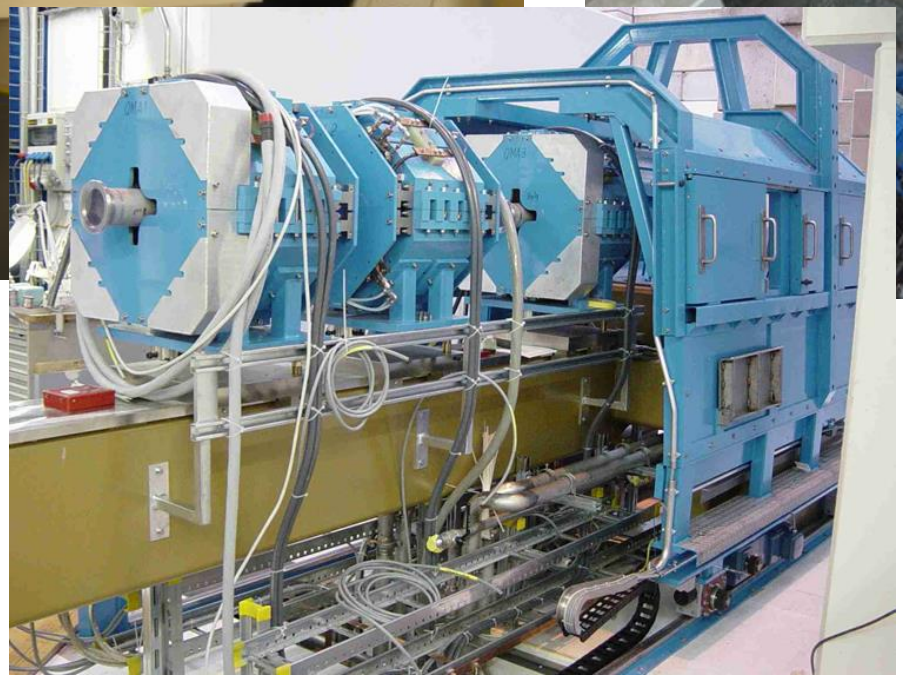
Proton Therapy Machine
High-level Control Structure



Gantry

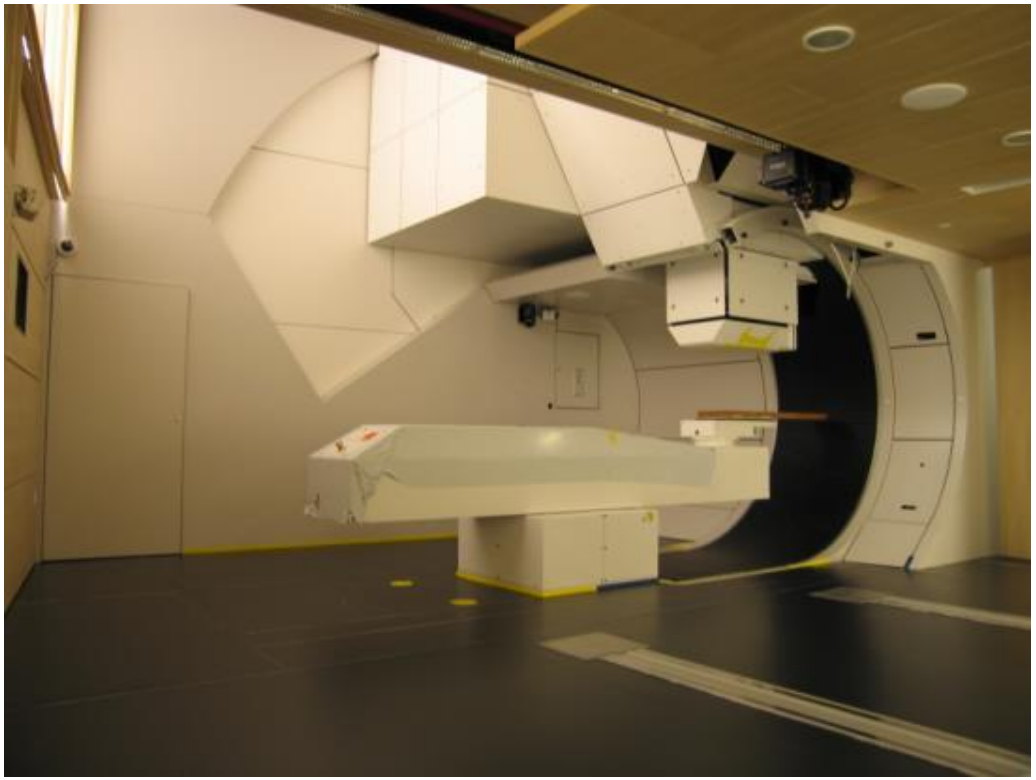


Cyclotron



Beam path and
control elements

Proton Therapy Machine
High-level Control Structure



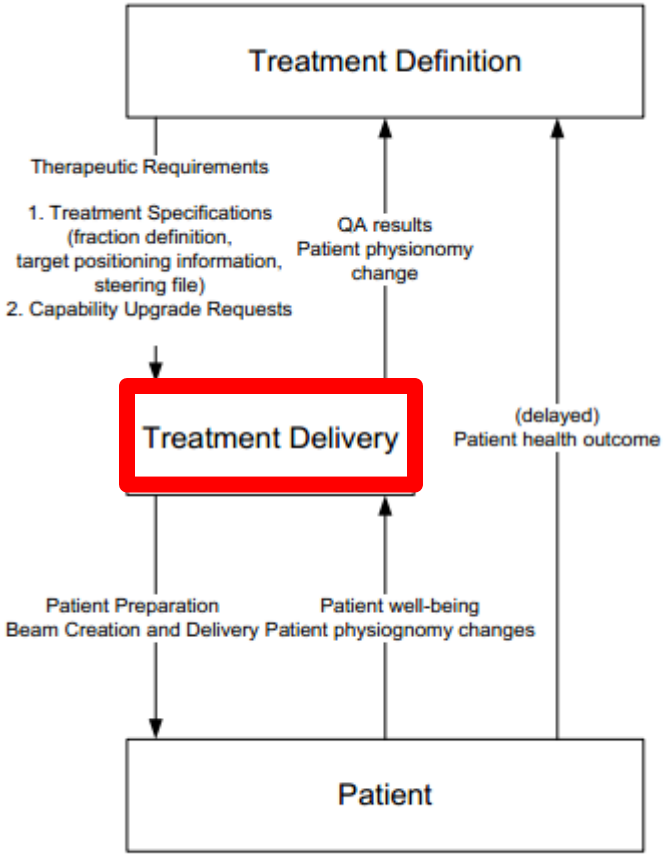


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Antoine PhD Thesis, 2012

Proton Therapy Machine Control Structure

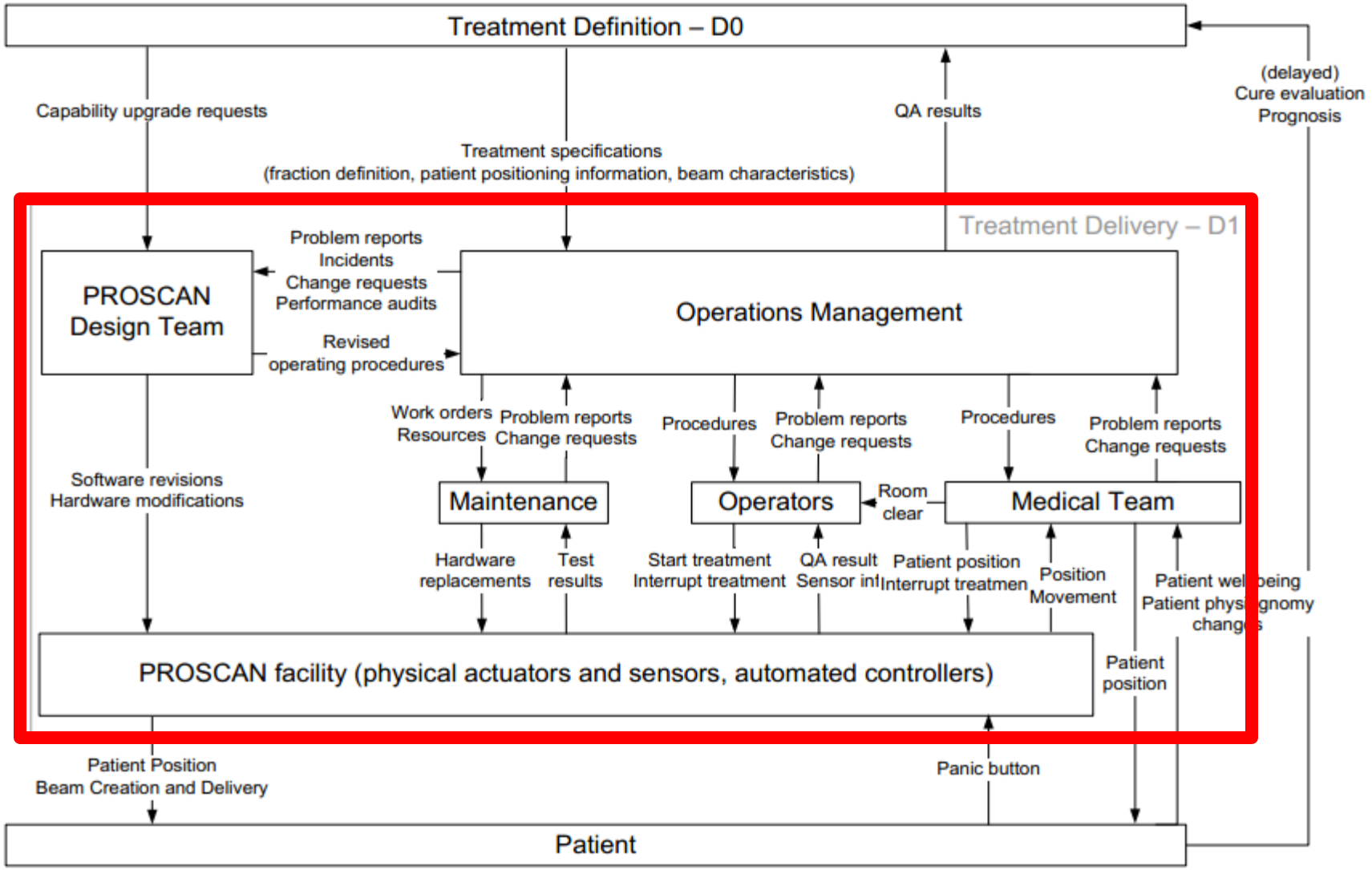
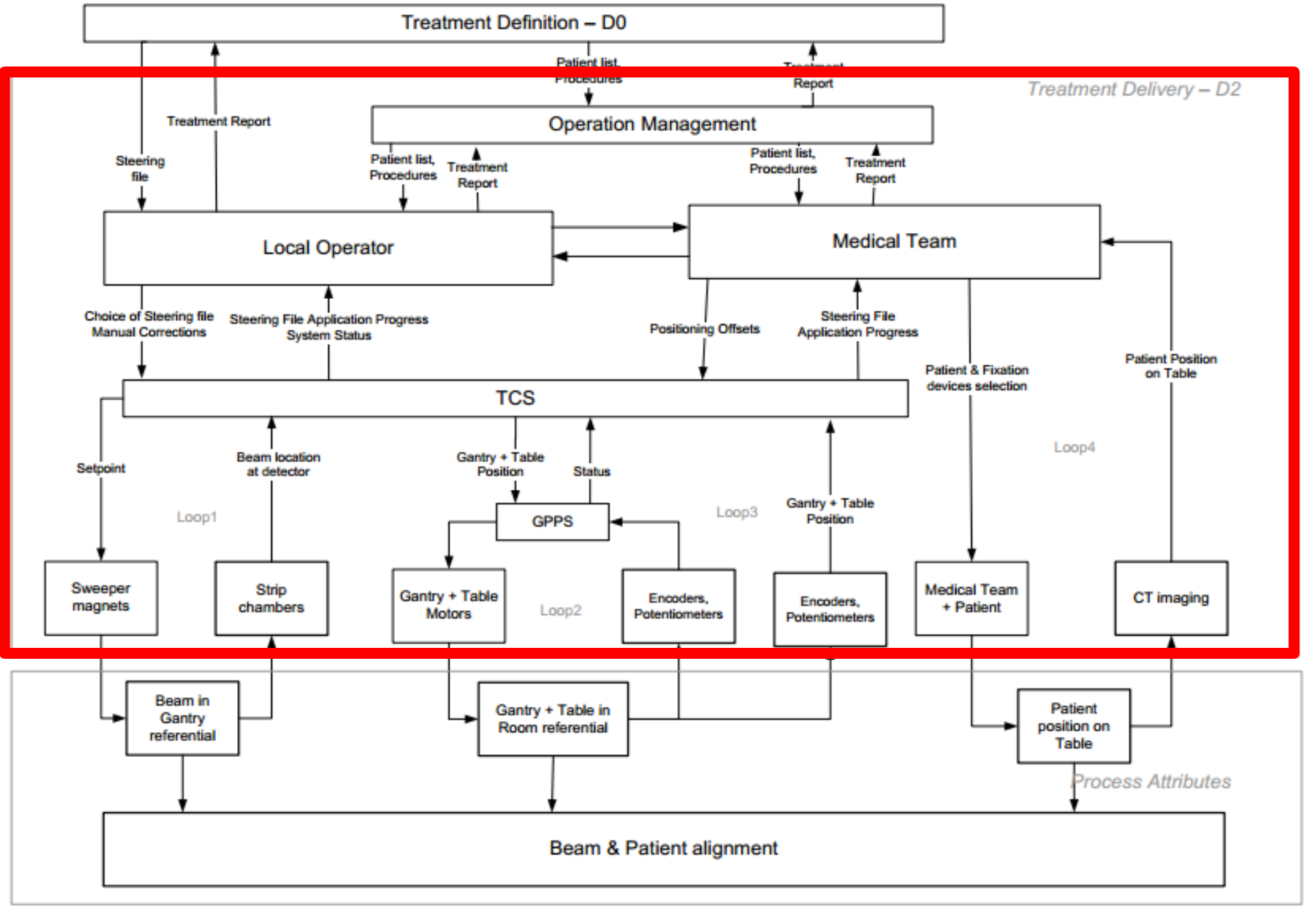


Figure 13 - Zooming into the Treatment Delivery group (D1)

Proton Therapy Machine Detailed Control Structure



Adaptive Cruise Control

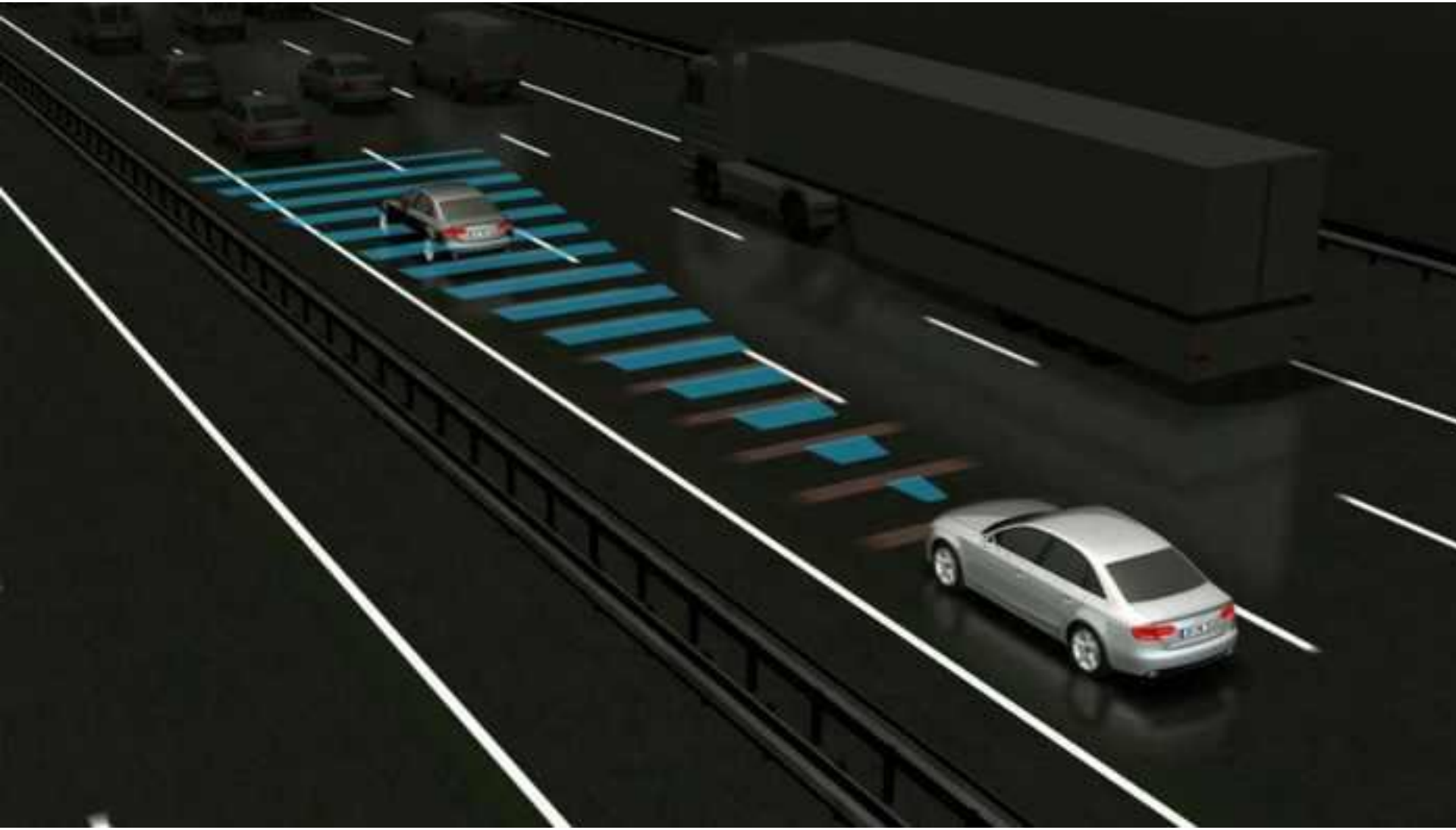
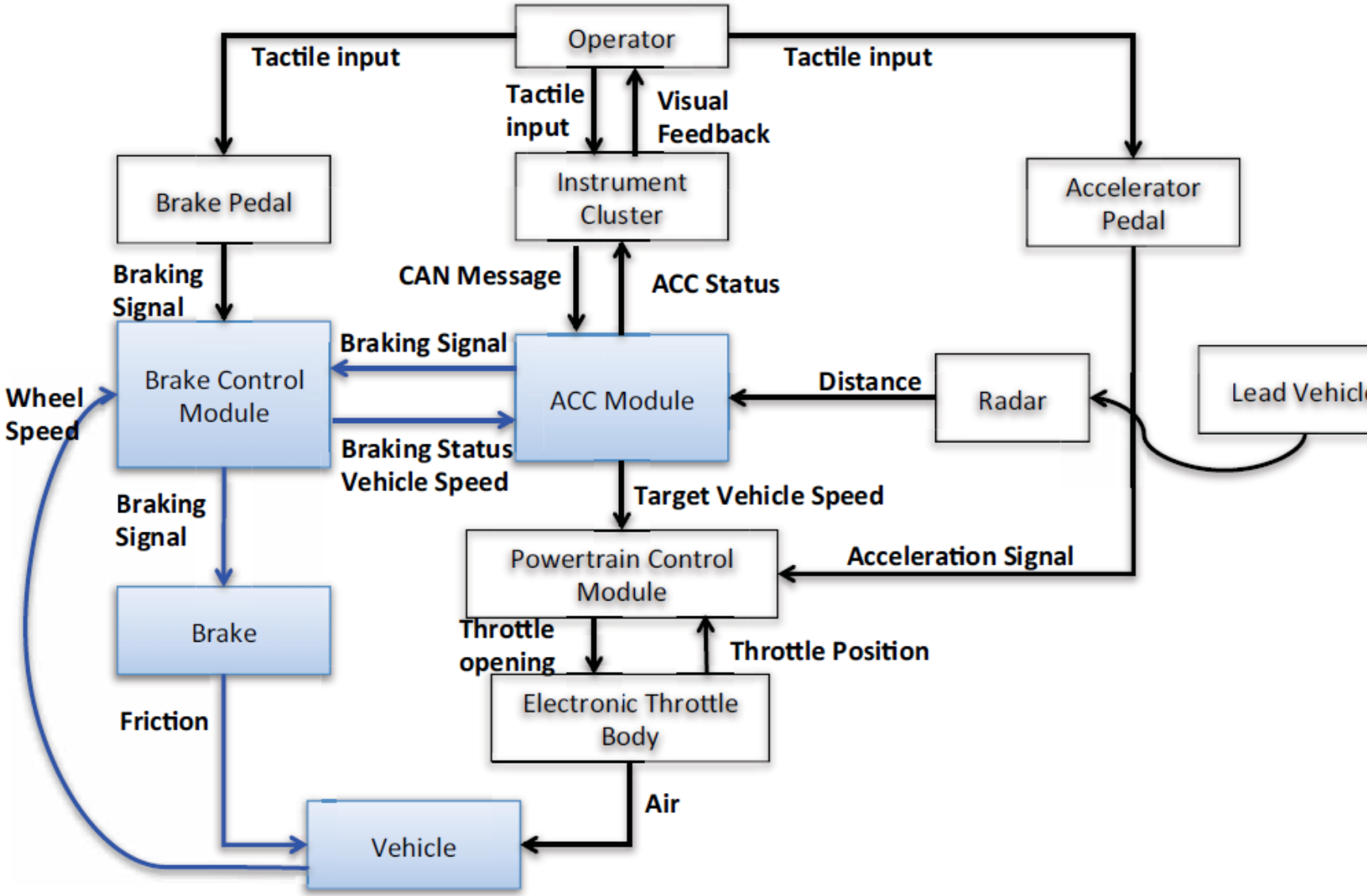
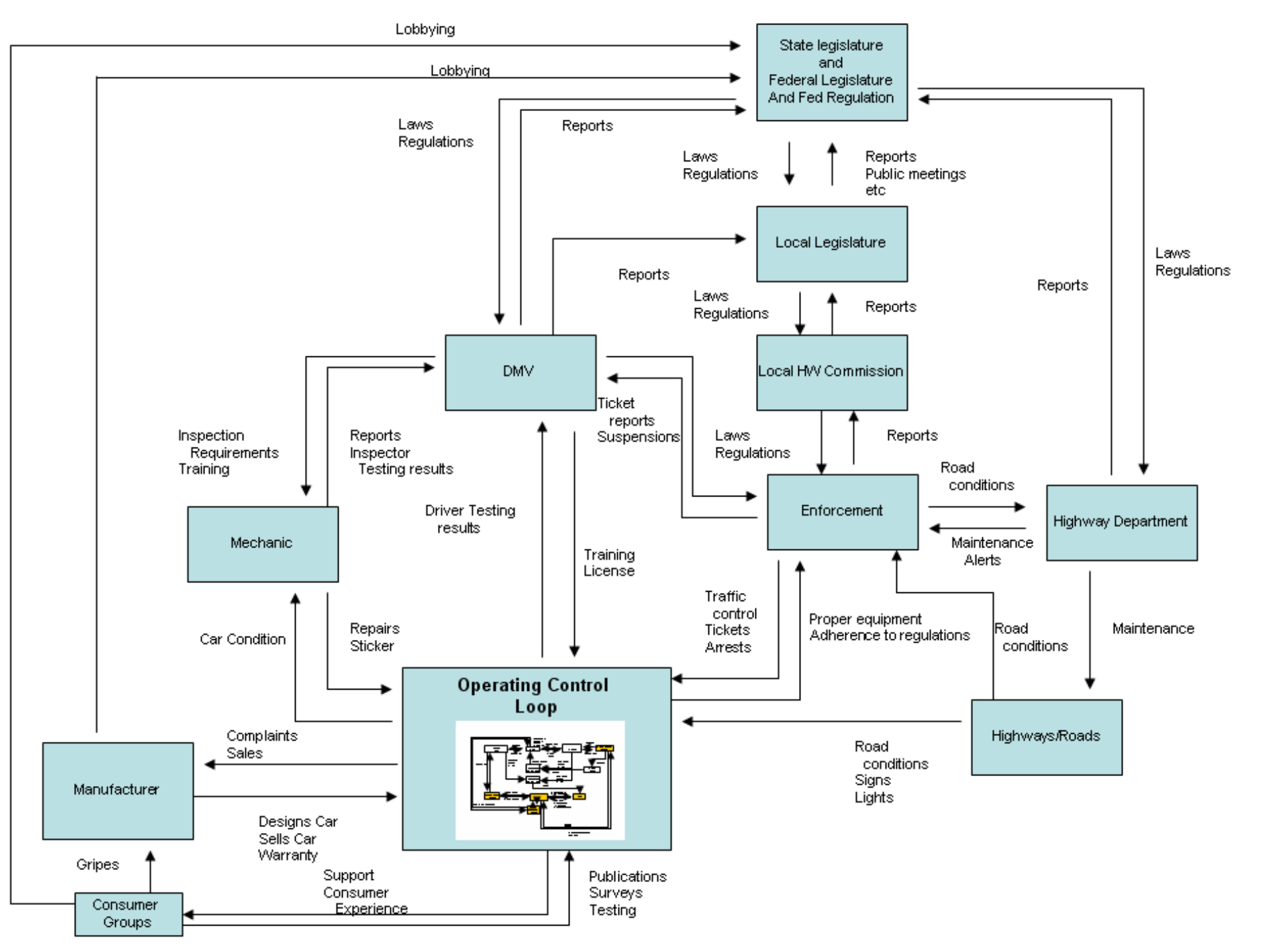


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

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

Chemical Plant

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

Chemical Plant

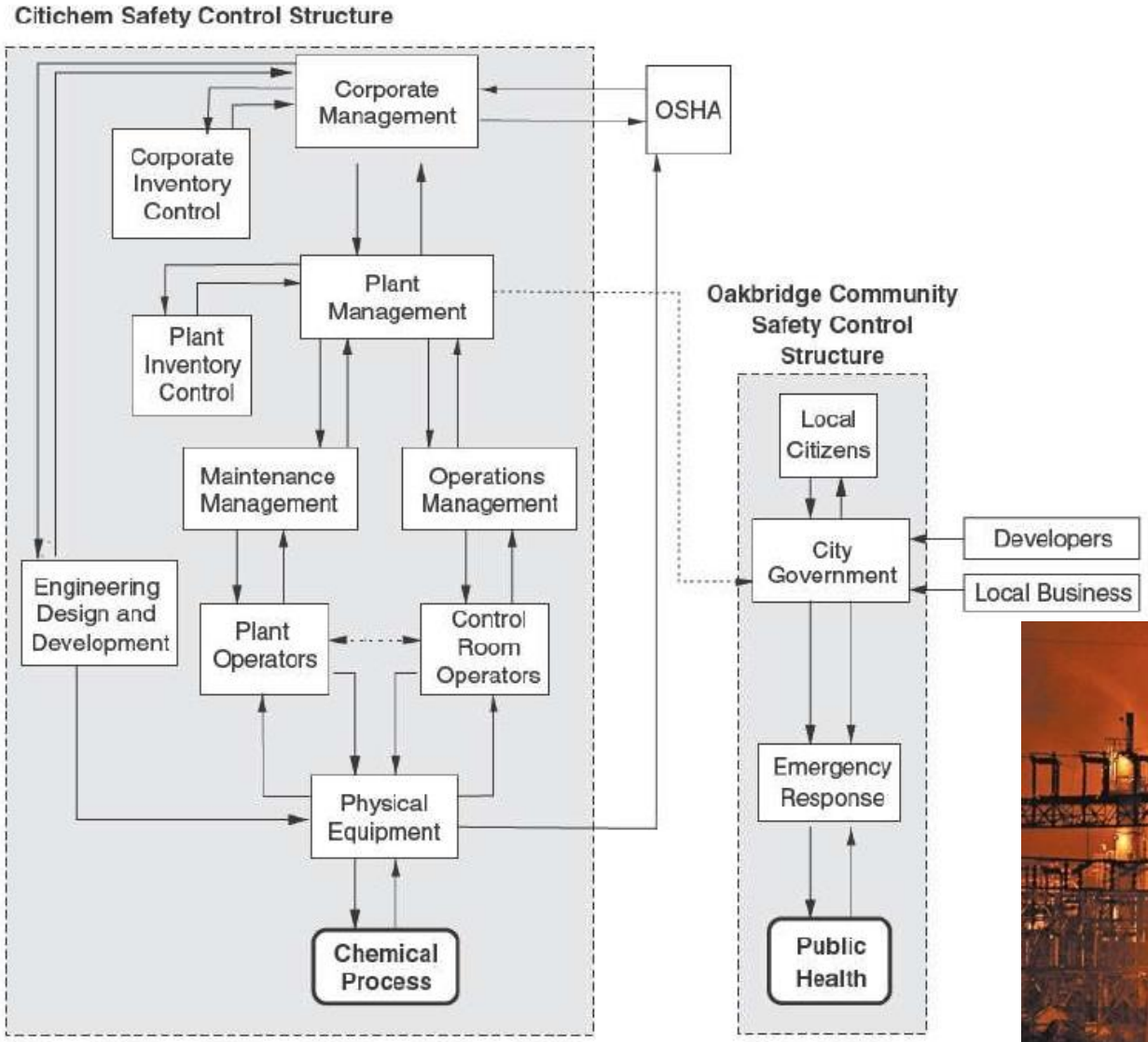


Image from:
http://www.cbgnetwork.org/2608.html

ESW p354

U.S. pharmaceutical safety control structure

Congress

FDA

Pharmaceutical Companies

Doctors

Patients

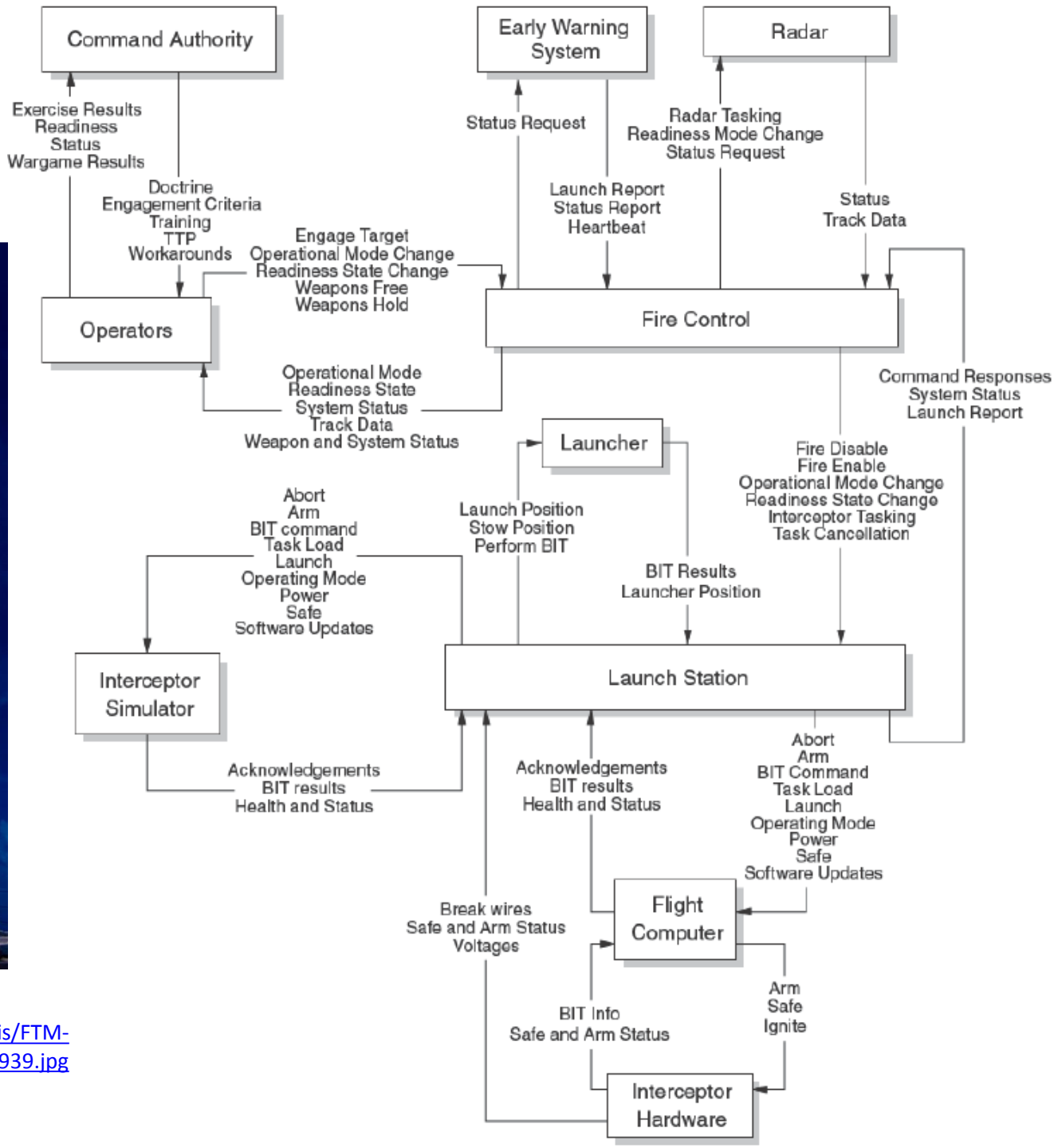
Image from: http://www.kleantreatmentcenter.com/wp-content/uploads/2012/07/vioxx.jpeg

Public group pressures
Industry group pressures
Political pressures mandate (e.g., FDAAA)
Congress
Reports
Dept. of Health and Human Services
Budget allocation
Budget needs
Budget allocation
Reports, priorities
FDA
FDA Commissioner
CDER Director
FDA/CDER Office of New Drugs
Division of Drug Marketing, Advertising and Communications
FDA/CDER Office of Surveillance and Epidemiology
Federal agencies in charge of funding
Editors/reviewers of scientific journals
Reviewers
Editorial constituency
Academically-affiliated researchers
Non-industry-funded researchers
FDA advisory committees
Industry-funded researchers
Content
Funding decisions
Membership decisions
Recommendations
User fees
Warning letters
Adverse events
New drug approval
New drug applications
Pharmaceutical companies
Pharmaceutical company investors/ shareholders
Pharmaceutical business leaders
Pharmaceutical trade associations
Pharmaceutical sales/marketing representatives
Pharmaceutical researchers/ scientists
Res/consult funds/agenda
Outputs of research/advising
Content
Inclusion on formulary
Price
Funds
Detailing, advertising and access to drugs
Adverse events
Payment, reimbursement, policy, formularies
Payers
Case reports
Budget allocation
Patient advocacy groups
Healthcare providers/prescribers
New information about existing drugs
Prescriptions
Symptoms, perceived benefits and side effects
Patients
Patient
Reimbursement
Claim
Patient's medical insurance
Insurance policy
Direct to consumer advertising
Legend
Information channels
Control channels

Ballistic Missile Defense System

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

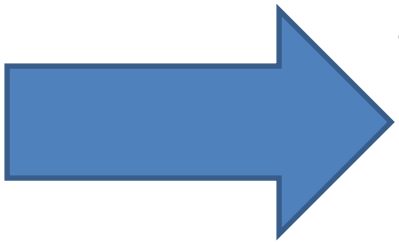
Safeware Corporation



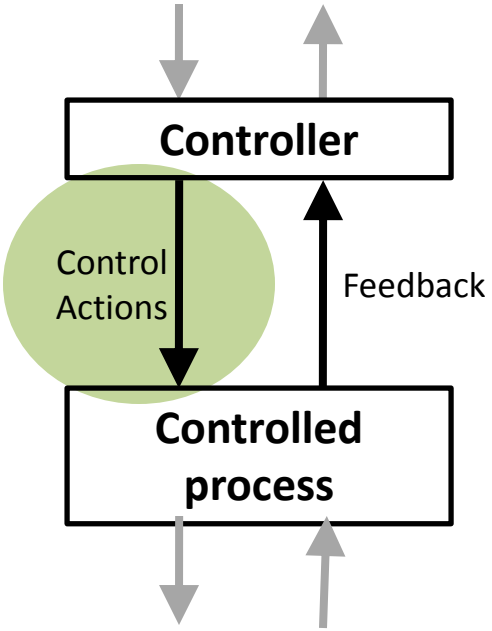
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards

- Draw the control structure

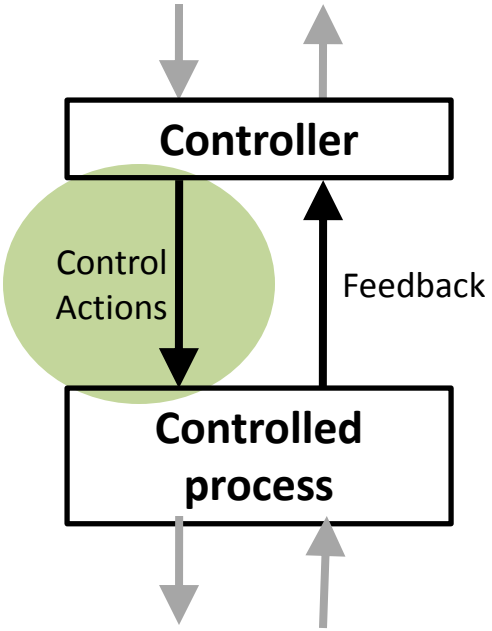


- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(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 (A)				

(Leveson, 2012)

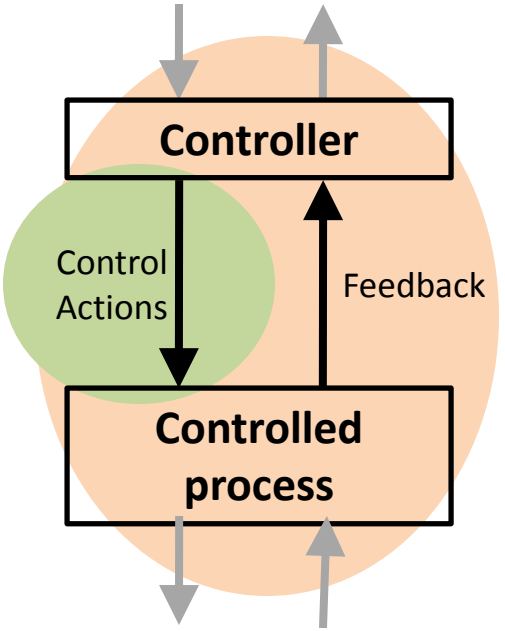
Step 1: Identify Unsafe Control Actions

(a more rigorous approach, will discuss later)

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

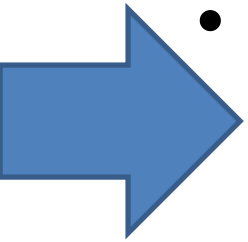
STPA
(System-Theoretic Process Analysis)

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



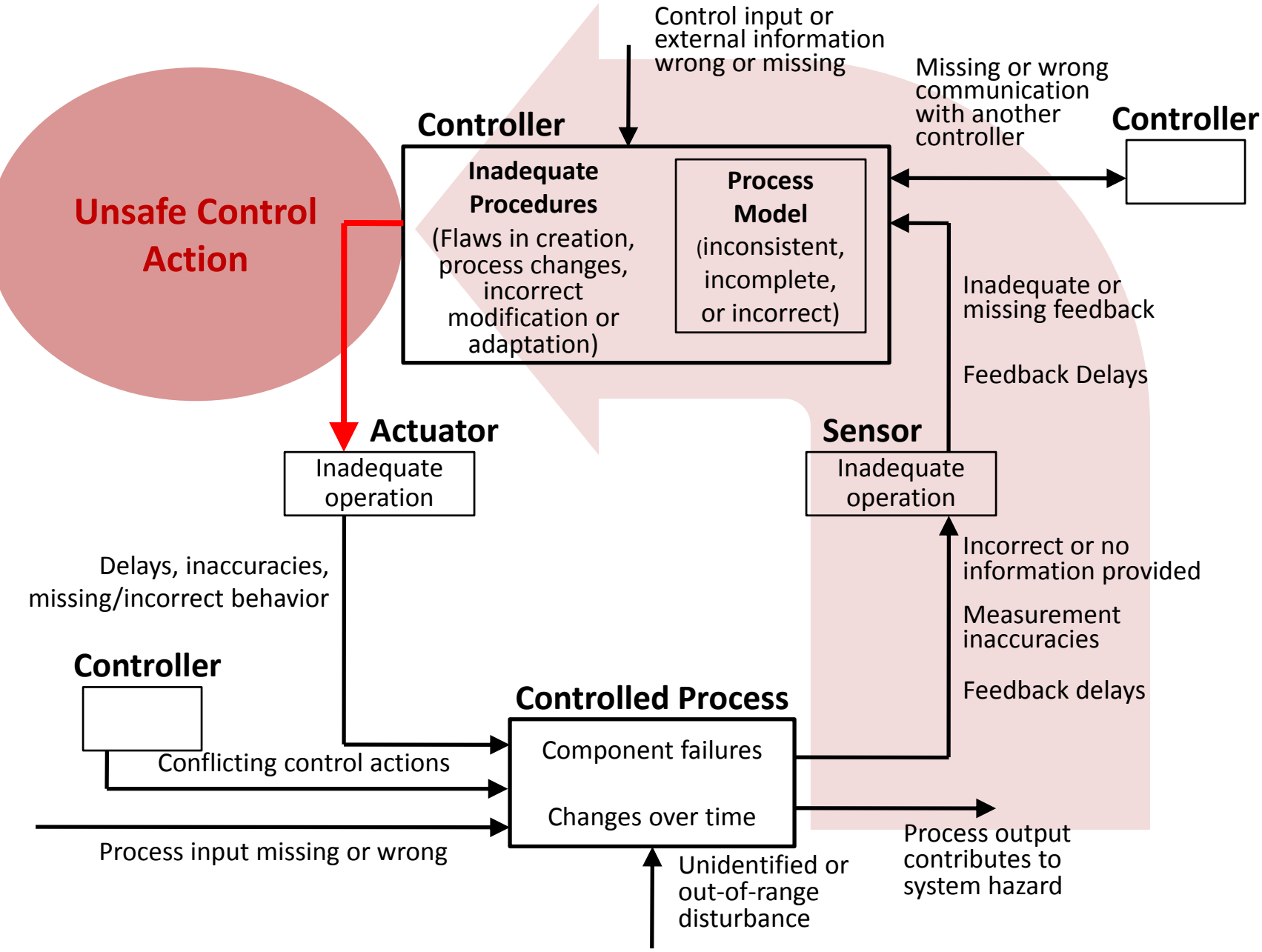
(Leveson, 2012)

STPA Step 2: Causal Factors and Scenarios



- Select an Unsafe Control Action
  A. Identify what could cause the unsafe control action
     - Develop causal accident scenarios
  B. Identify how control actions may not be followed or executed properly
     - Develop causal accident scenarios

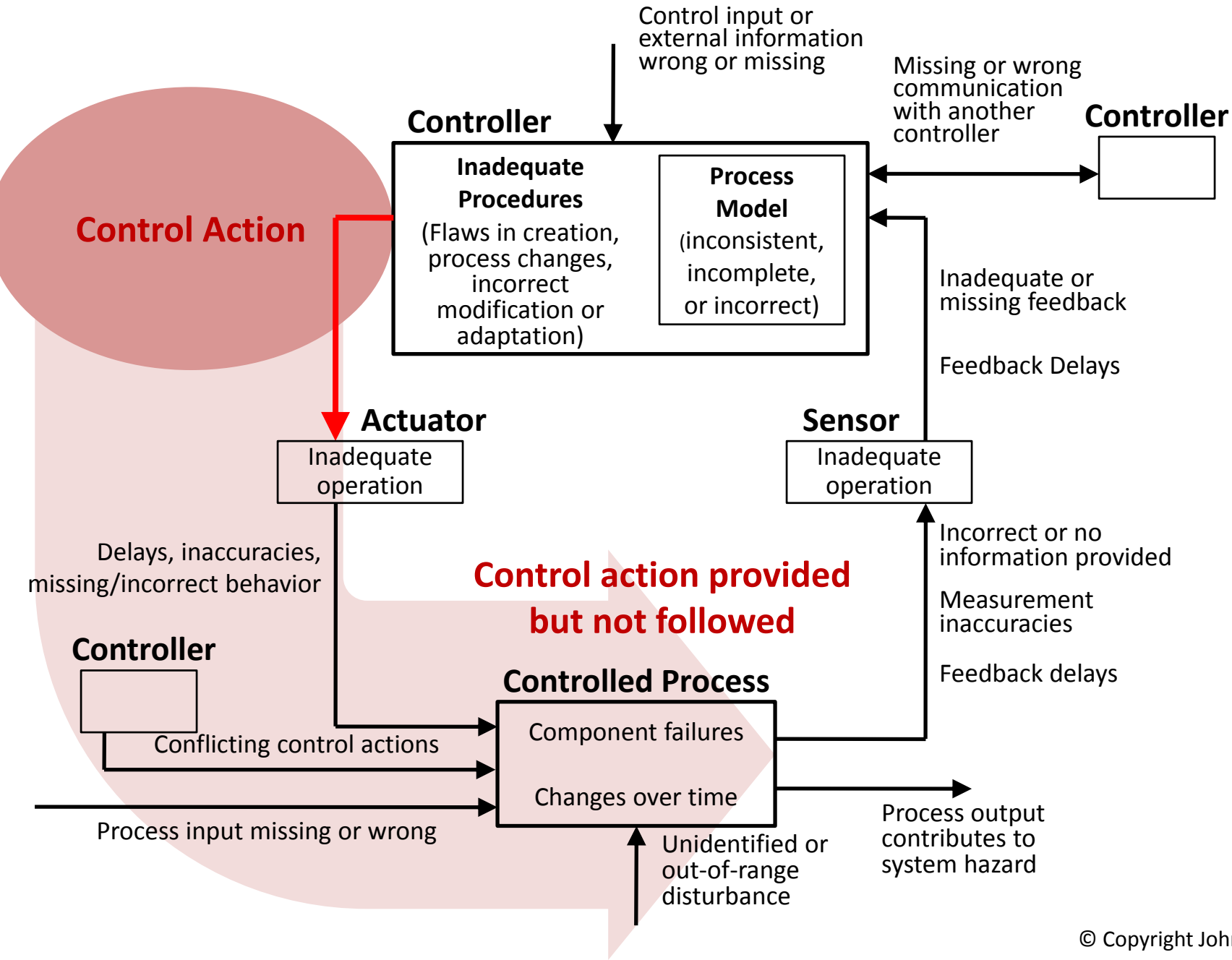
Step 2A: Potential causes of UCAs



STPA Step 2: Causal Factors and Scenarios

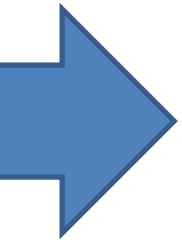
- Select an Unsafe Control Action
  A. Identify what could cause the unsafe control action
     - Develop causal accident scenarios
  B. Identify how control actions may not be followed or executed properly
     - Develop causal accident scenarios

Step 2B: Potential control actions not followed



STPA Step 2: Causal Factors and Scenarios

- Select an Unsafe Control Action
  A. Identify what could cause the unsafe control action
     - Develop causal accident scenarios
  B. Identify how control actions may not be followed or executed properly
     - Develop causal accident scenarios



- Identify controls and mitigations for the accident scenarios

Example Controls for Causal Scenarios

- **Scenario 1** – Operator provides Start Treatment command when there is no patient on the table or patient is not ready. Operator was not in the room when the command was issued, as required by other safety constraints. Operator was expecting patient to have been positioned, but table positioning was delayed compared to plan (e.g. because of delays in patient preparation or patient transfer to treatment area; because of unexpected delays in beam availability or technical issues being processed by other personnel without proper communication with the operator).

- **Controls:**
  - Provide operator with direct visual feedback to the gantry coupling point, and require check that patient has been positioned before starting treatment (M1).
  - Provide a physical interlock that prevents beam-on unless table positioned according to plan

Antoine PhD Thesis, 2012

Example Controls for Causal Scenarios

- **Scenario 2 –** Operator provides start treatment command when there is no patient. The operator was asked to turn the beam on outside of a treatment sequence (e.g. because the design team wants to troubleshoot a problem, or for experimental purposes) but inadvertently starts treatment and does not realize that the facility proceeds with reading the treatment plan and records the dose as being administered.

- **Controls:**
  - Reduce the likelihood that non-treatment activities have access to treatment-related input by creating a non-treatment mode to be used for QA and experiments, during which facility does not read treatment plans that may have been previously been loaded (M2);
  - Make procedures (including button design if pushing a button is what starts treatment) to start treatment sufficiently different from non-treatment beam on procedures that the confusion is unlikely.

Antoine PhD Thesis, 2012

Example Controls for Causal Scenarios Command not followed

- **Scenario 3 –** The operator provides the Start Treatment command, but it does not execute properly because the proper steering file failed to load (either because operator did not load it, or previous plan was not erased from system memory and overwriting is not possible) or the system uses a previously loaded one by default.

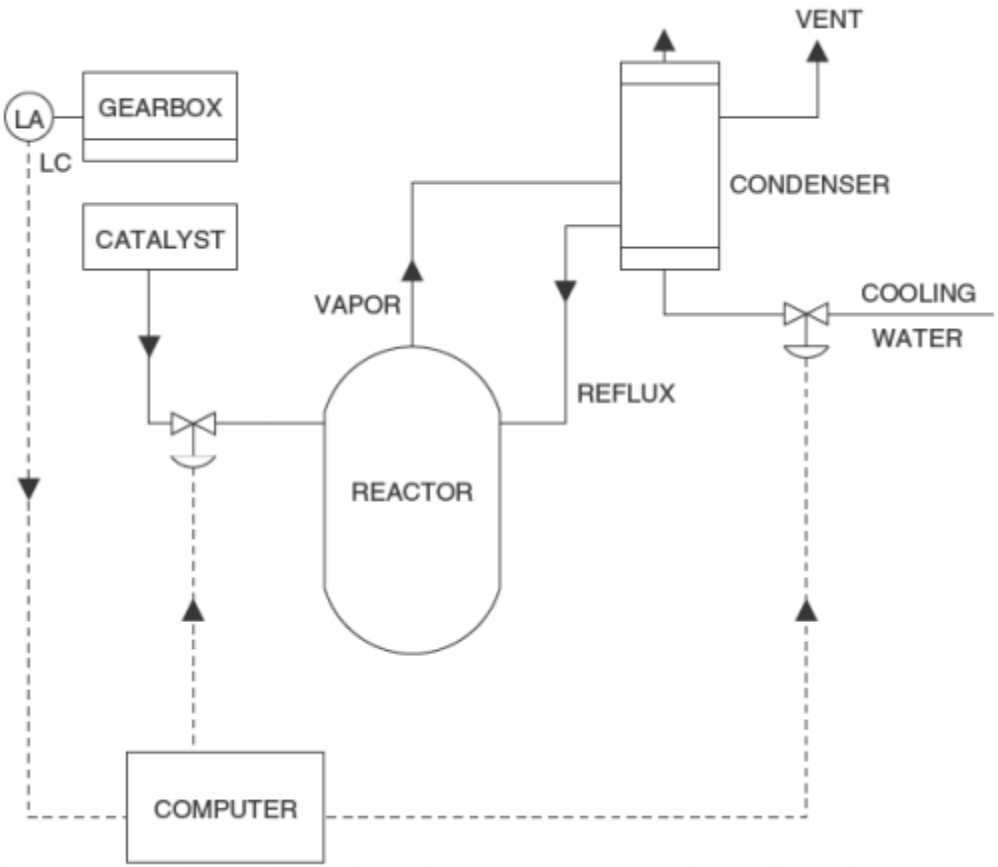
- **Controls:**
  - When fraction delivery is completed, the used steering file could for example be automatically dumped out of the system's memory (M4).
  - Do not allow a Start Treatment command if the steering file does not load properly
  - Provide additional checks to ensure the steering file matches the current patient (e.g. barcode wrist bands, physiological attributes, etc.)

Antoine PhD Thesis, 2012

Chemical Reactor Example

Chemical Reactor Design

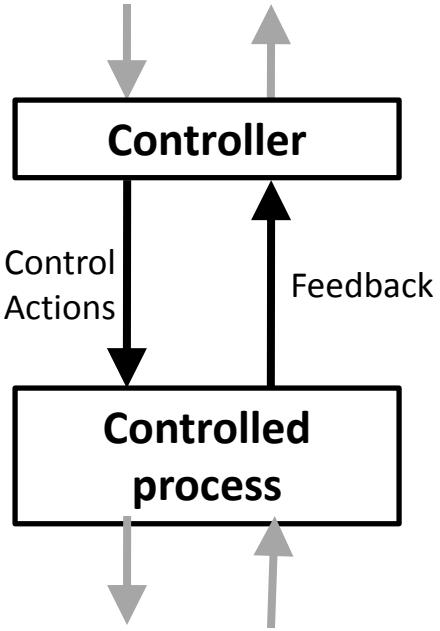
- Toxic catalyst flows into reactor
- Chemical reaction creates heat, pressure
- Water and condenser provide cooling



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

STPA
(System-Theoretic Process Analysis)

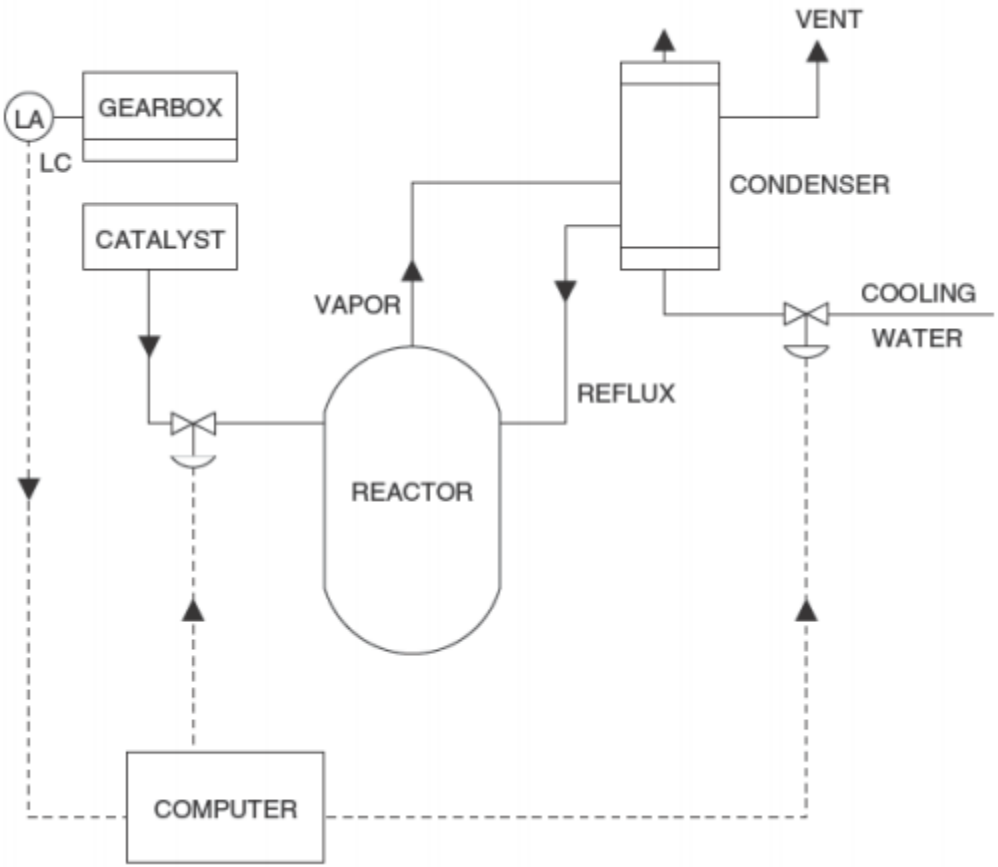
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

Chemical Reactor Design

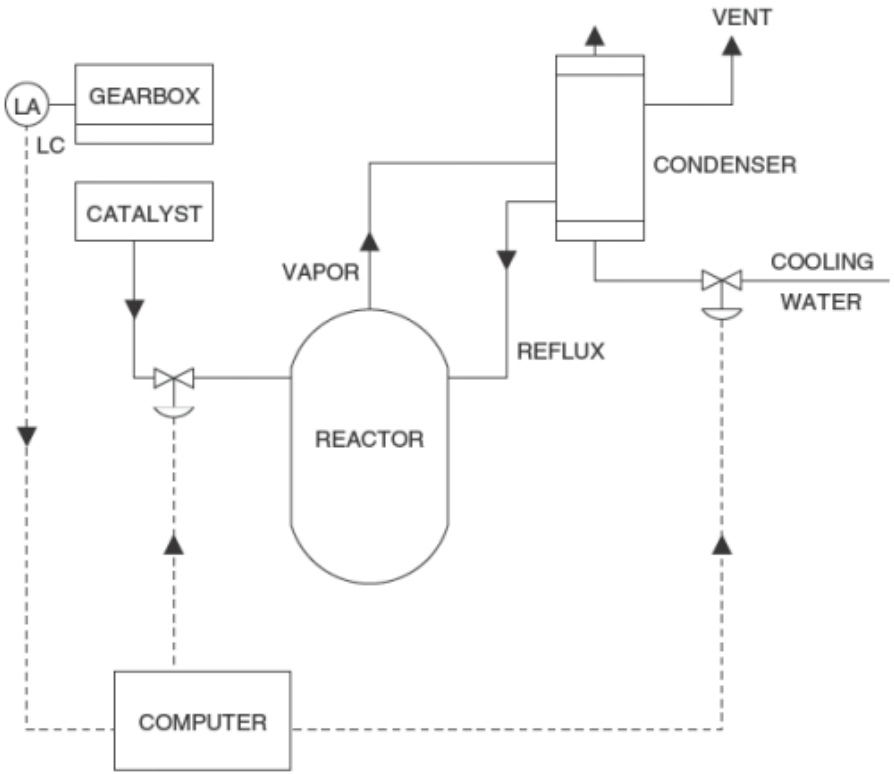
- Toxic catalyst flows into reactor
- Chemical reaction creates heat, pressure
- Water and condenser provide cooling

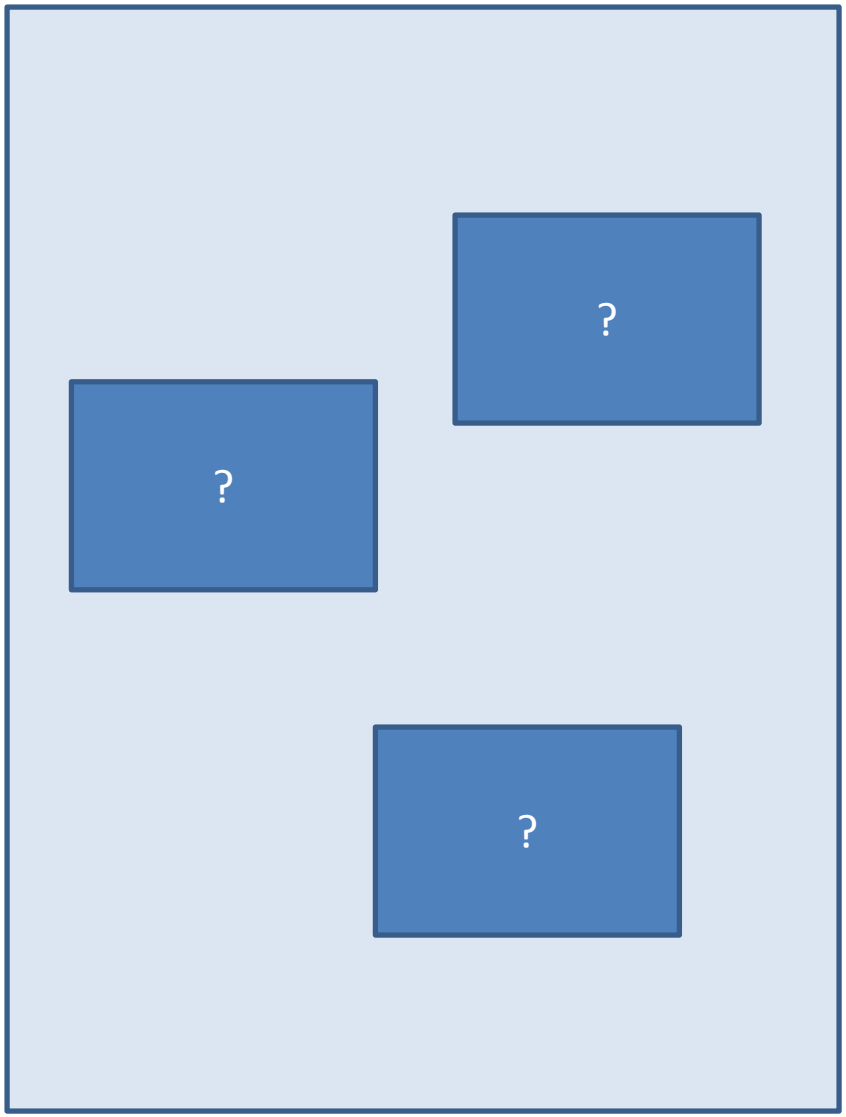


Create Control Structure

STPA Analysis

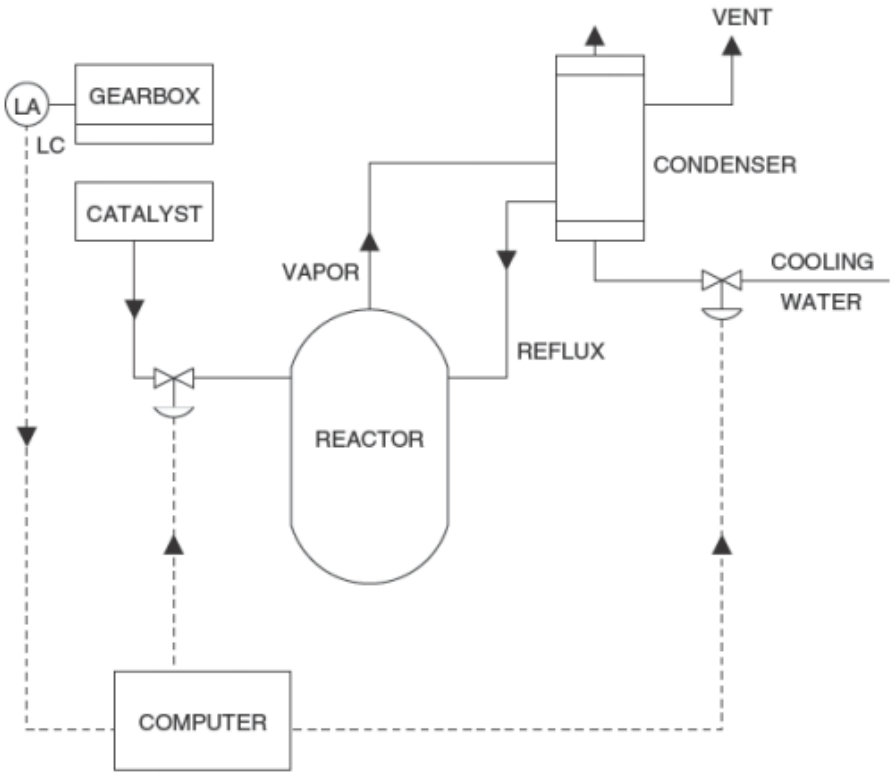
- High-level (simple) Control Structure
  - What are the main parts?

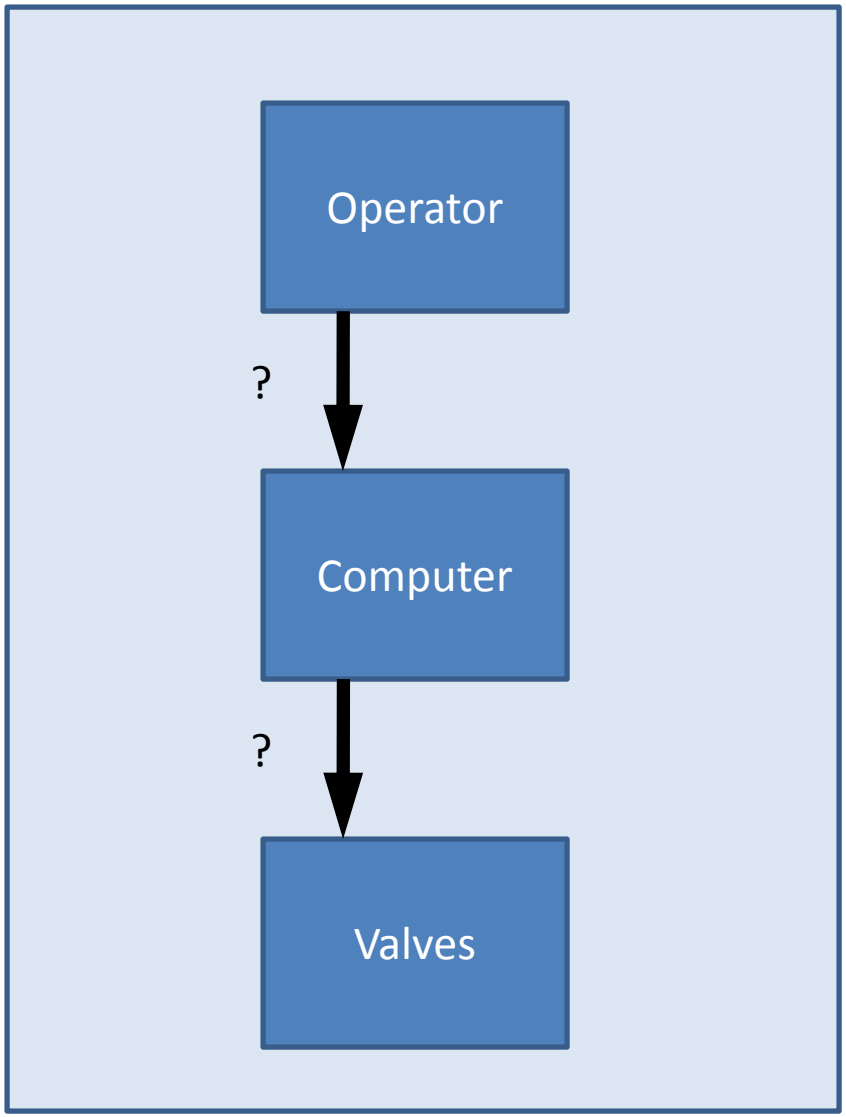




STPA Analysis

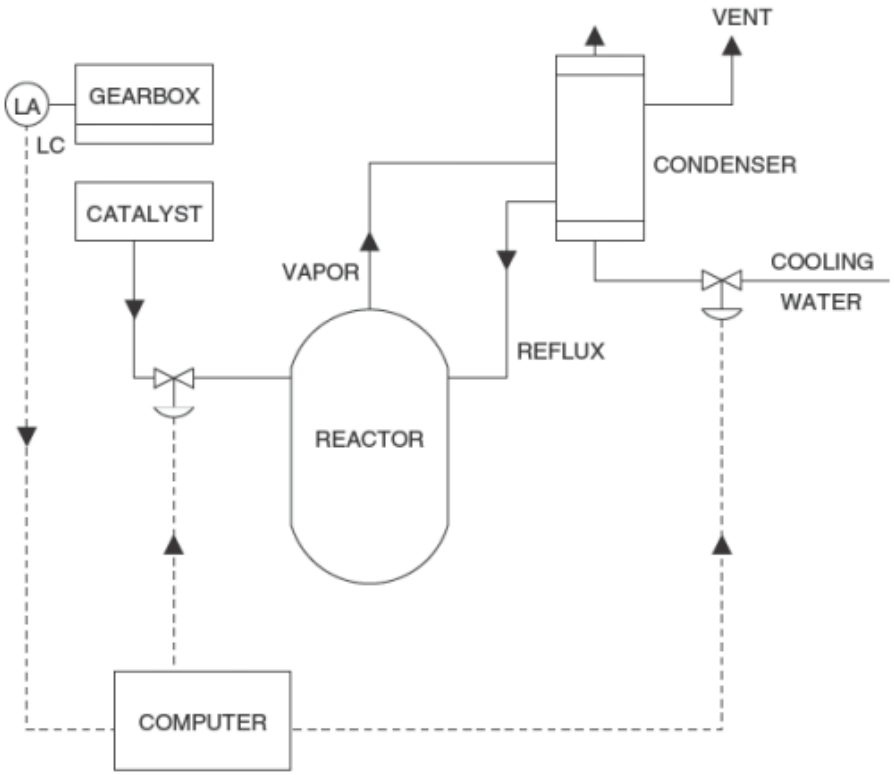
- High-level (simple) Control Structure
  - What commands are sent?

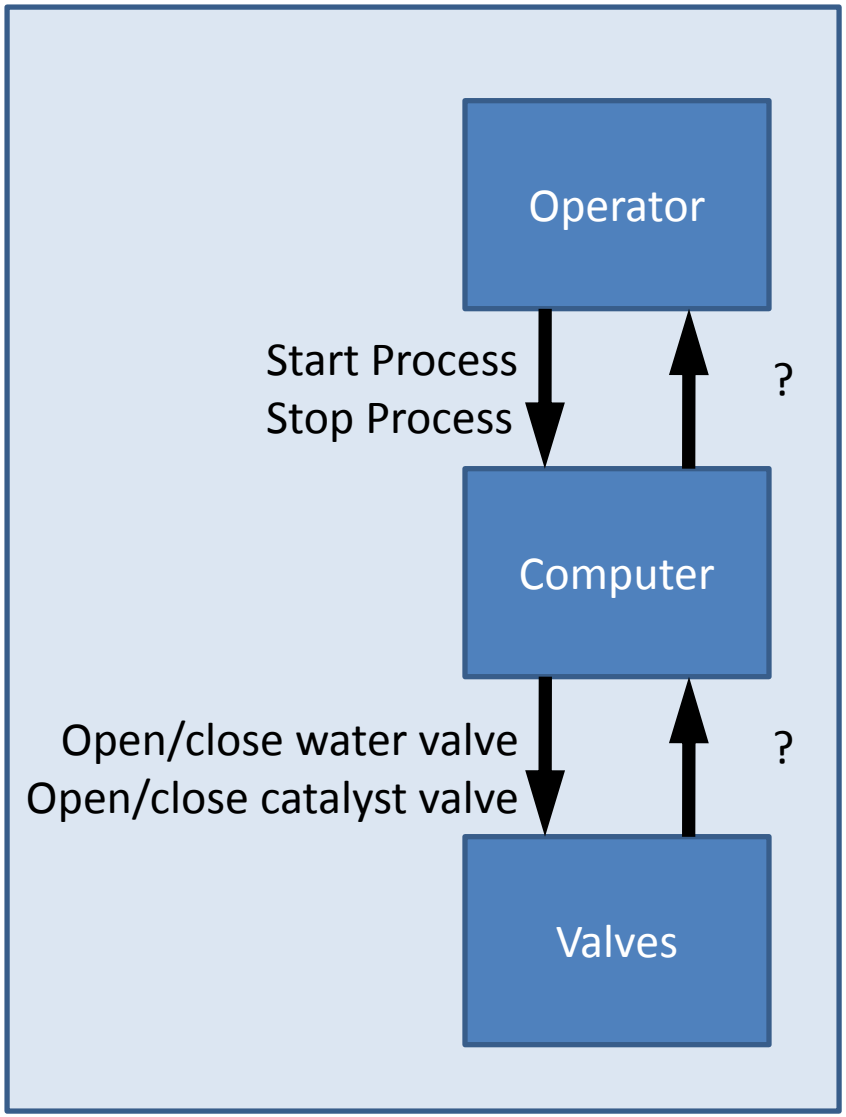




STPA Analysis

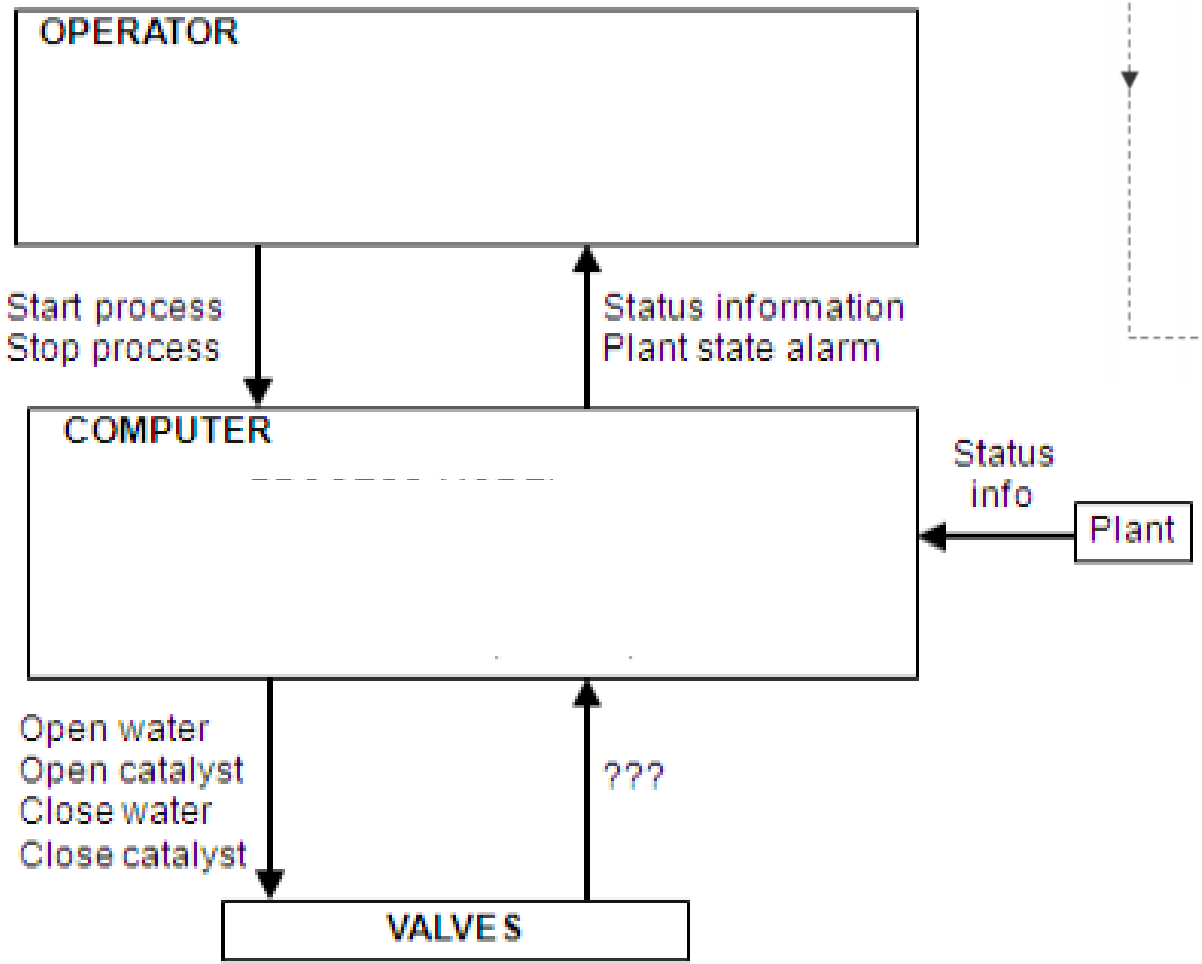
- High-level (simple) Control Structure
  - What feedback is received?

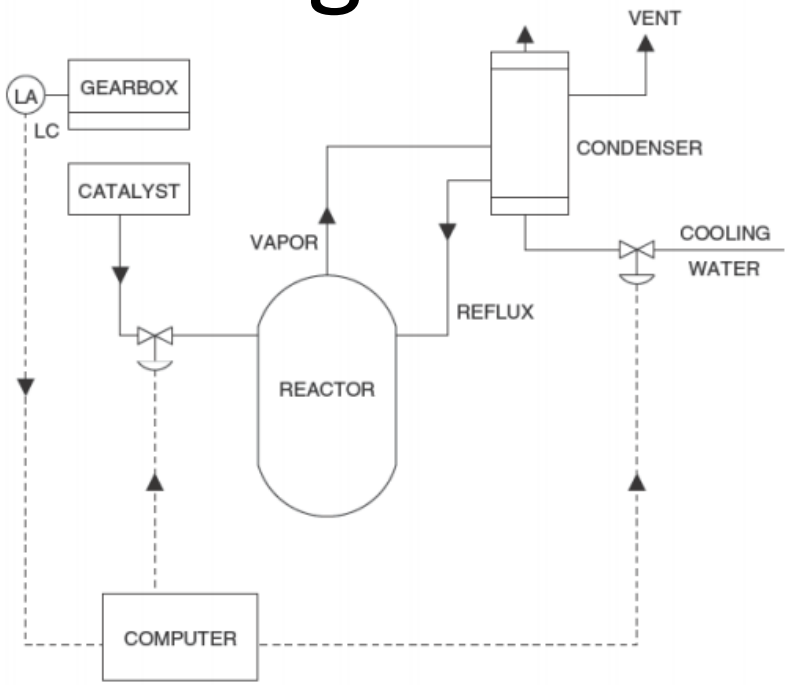




Chemical Reactor Design

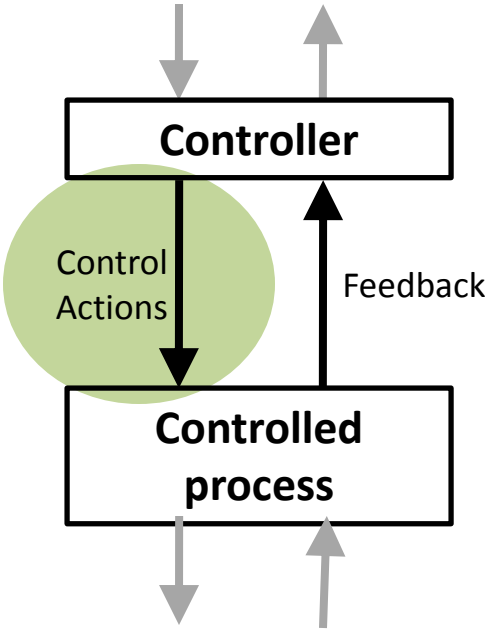
Control Structure:





STPA
(System-Theoretic Process Analysis)

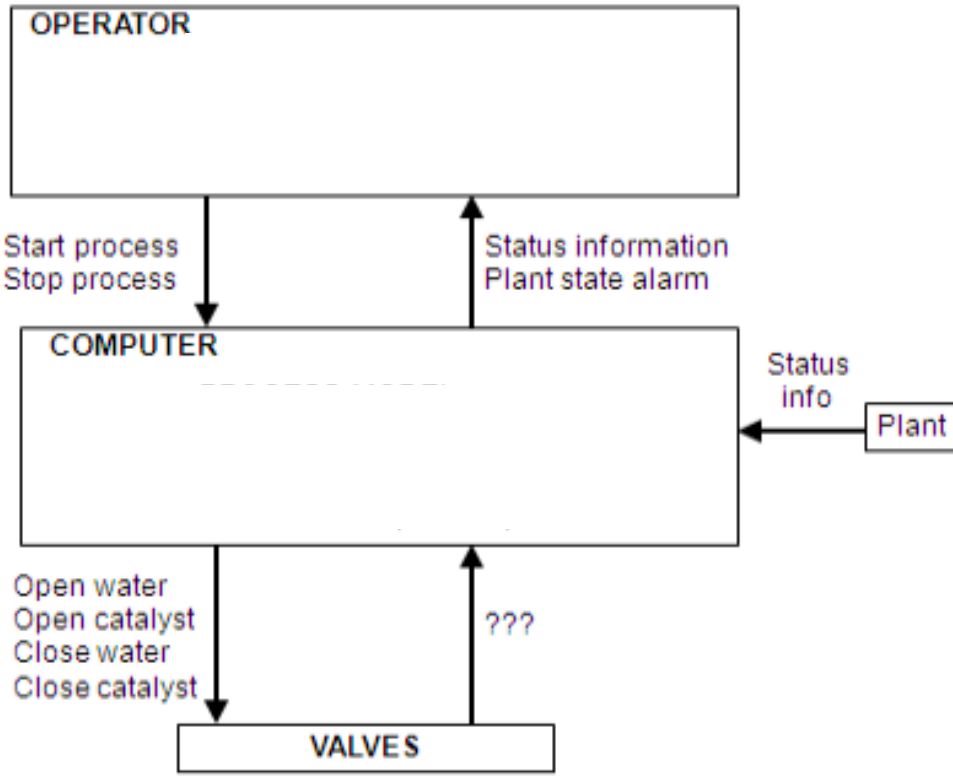
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

Chemical Reactor: Unsafe Control Actions

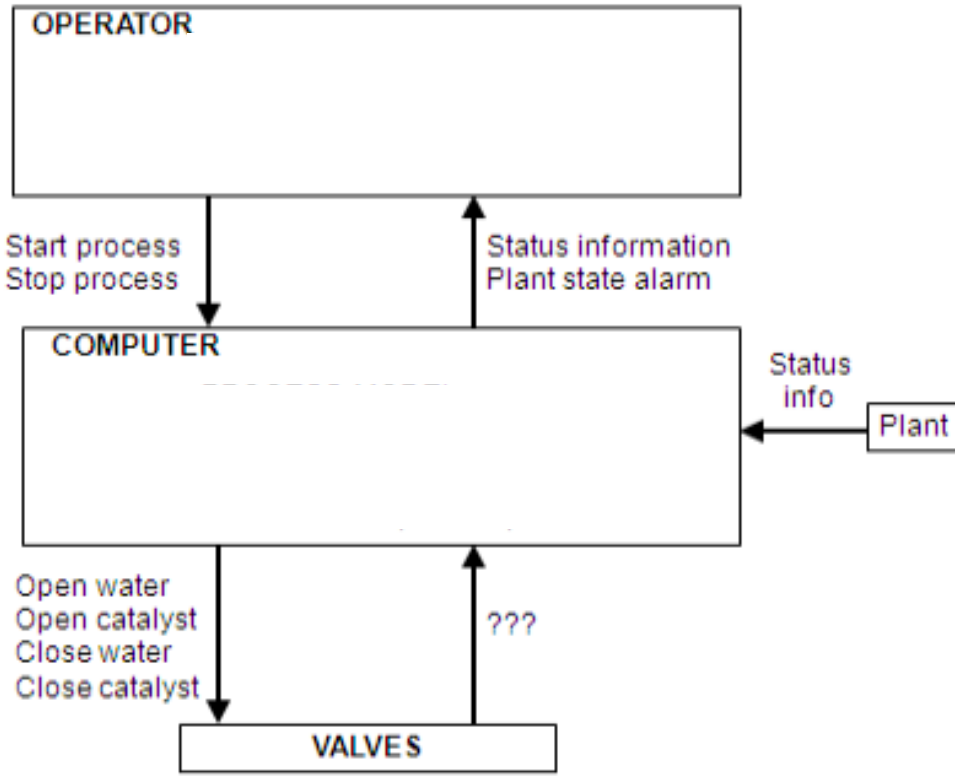
Control Structure:



	?	?	?	?
Close Water Valve				

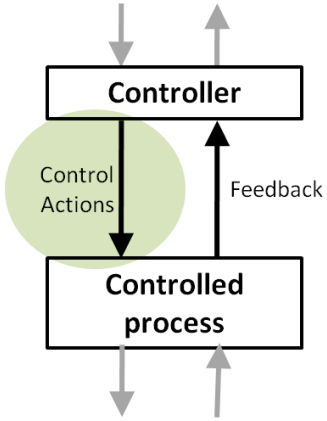
Chemical Reactor: Unsafe Control Actions

Control Structure:



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve	?	**Computer provides Close Water cmd while catalyst open**	?	?

Structure of an Unsafe Control Action



Example:

"Computer provides close water valve command when catalyst open"

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)

Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve		Computer closes water valve while catalyst open	Computer closes water valve before catalyst closes	
Open Water Valve	Computer does not open water valve when catalyst open		Computer opens water valve more than X seconds after open catalyst	Computer stops opening water valve before it is fully opened
Open Catalyst Valve		Computer opens catalyst valve when water valve not open	Computer opens catalyst more than X seconds before open water	
Close Catalyst Valve	Computer does not close catalyst when water closed		Computer closes catalyst more than X seconds after close water	Computer stops closing catalyst before it is fully closed

Safety Constraints

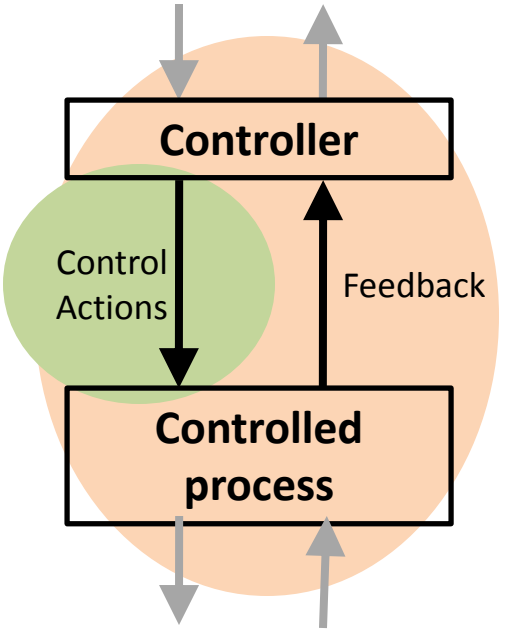
Unsafe Control Action	Safety Constraint
Computer does not open water valve when catalyst valve open	Computer must open water valve whenever catalyst valve is open
Computer opens water valve more than X seconds after catalyst valve open	Computer must open water valve within X seconds of catalyst valve open
Computer closes water valve while catalyst valve open	Computer must not close water valve while catalyst valve open
Computer closes water valve before catalyst valve closes	Computer must not close water valve before catalyst valve closes
Computer opens catalyst valve when water valve not open	Computer must not open catalyst valve when water valve not open
Etc.	Etc.

Traceability

- Always provide traceability information between UCAs and the hazards they cause
  - Same for Safety Constraints
- Two ways:
  - Create one UCA table (or safety constraint list) per hazard, label each table with the hazard
  - Create one UCA table for all hazards, include traceability info at the end of each UCA
    - E.g. **Computer closes water valve while catalyst open [H-1]**

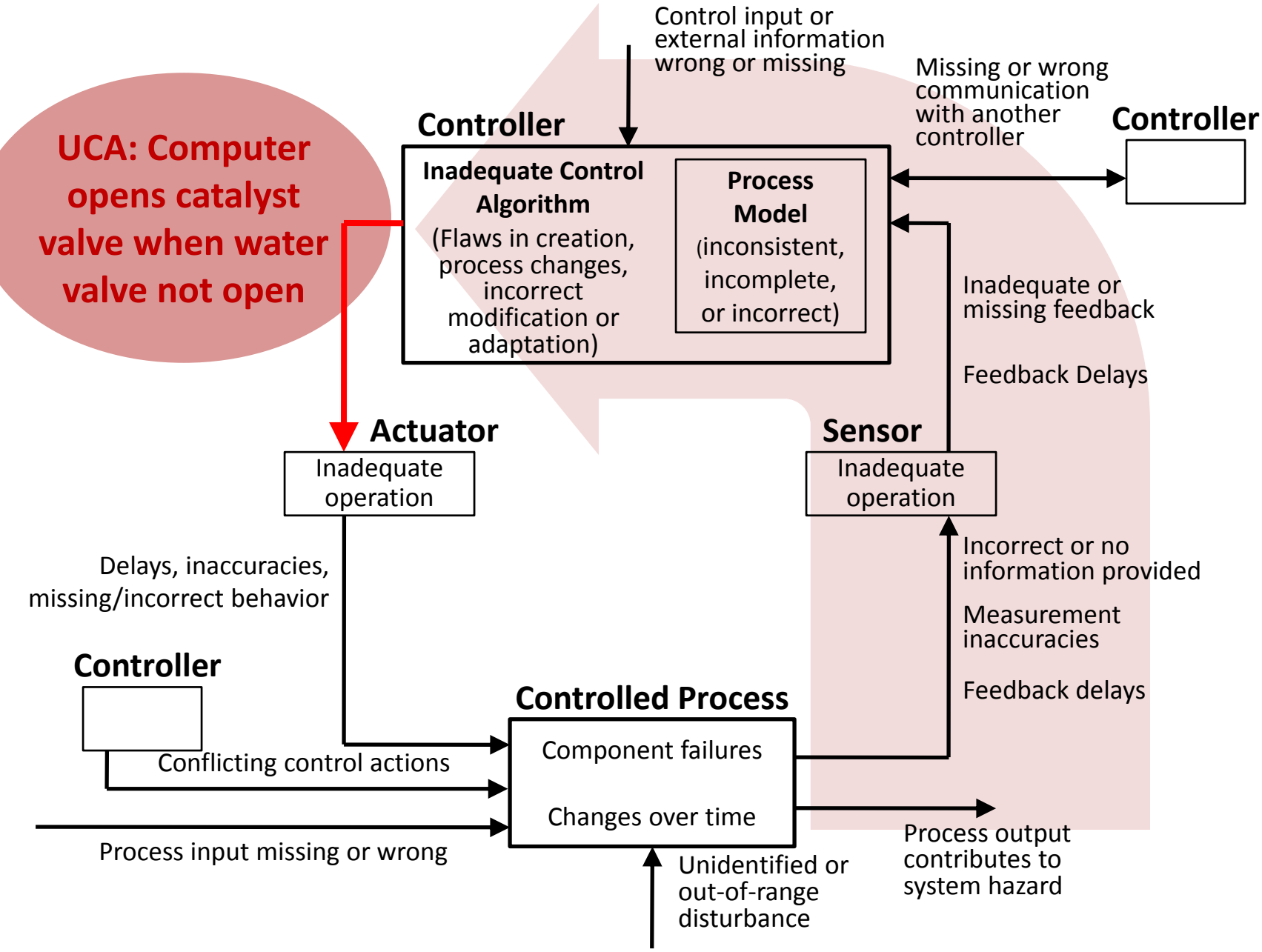
STPA
(System-Theoretic Process Analysis)

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

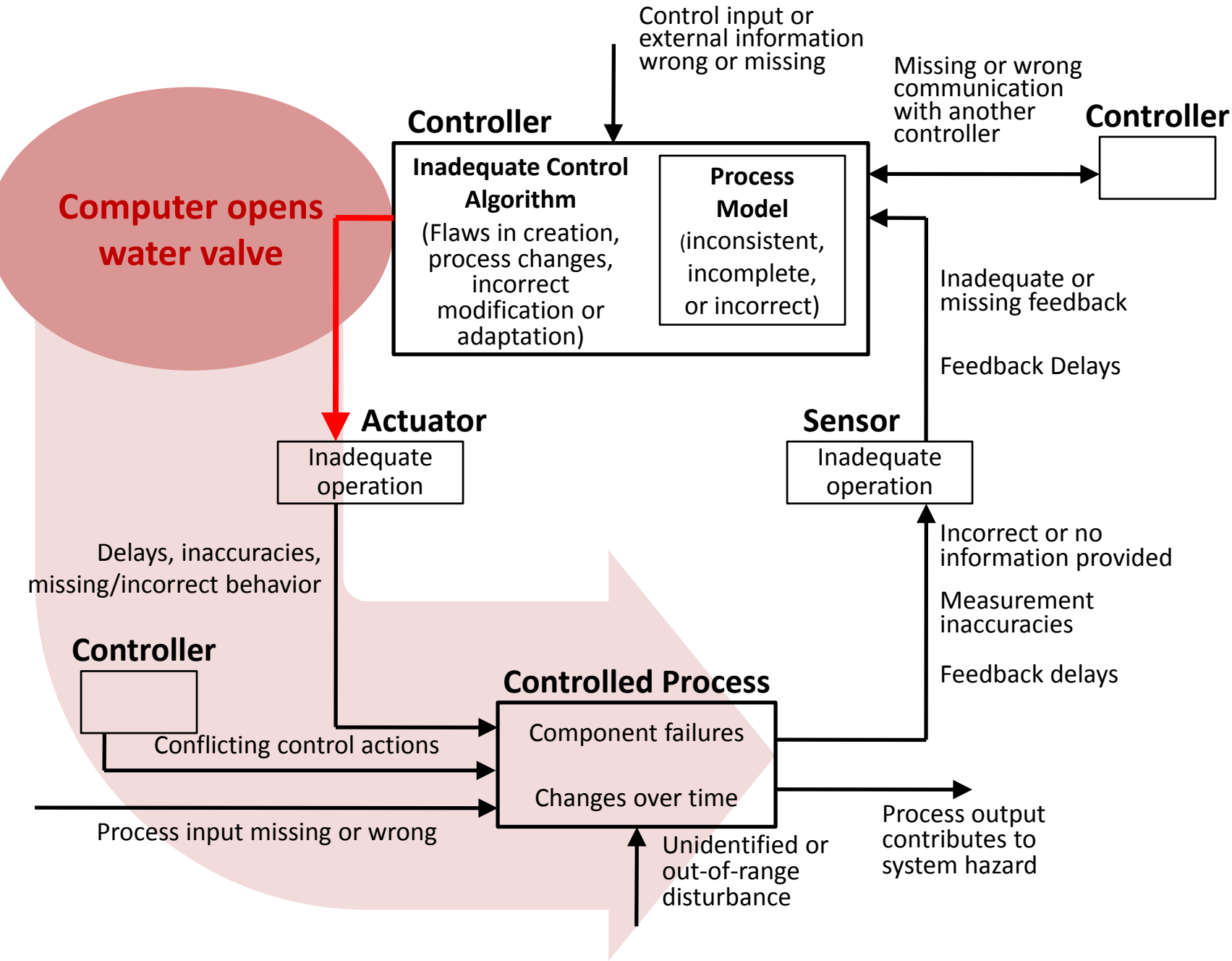


(Leveson, 2012)

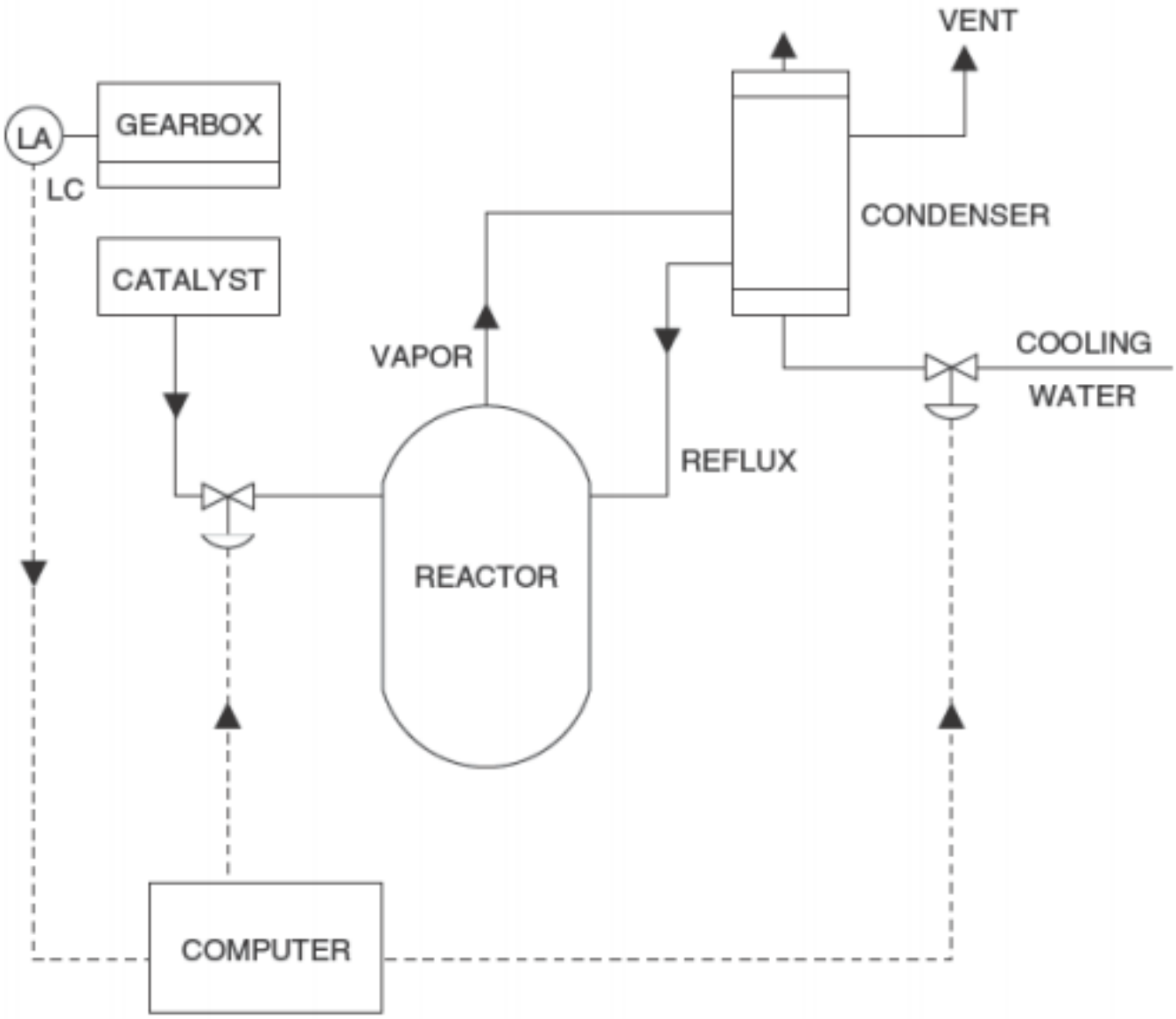
Step 2: Potential causes of UCAs



Step 2: Potential control actions not followed



Chemical Reactor: Real accident

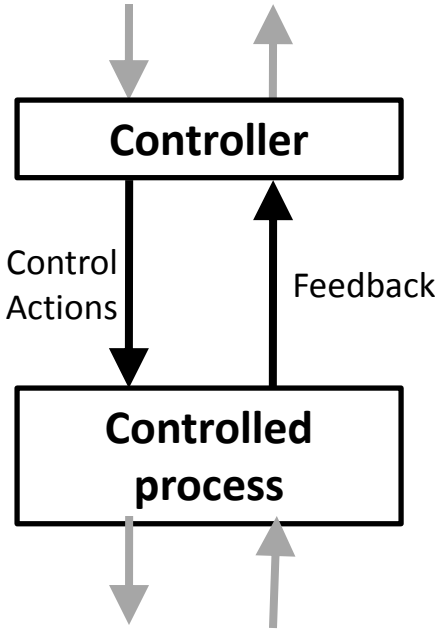


ITP Exercise

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)

System-level Accident (Loss): Aircraft crashes

System-level Hazard: Two aircraft violate minimum separation

Aviation Examples

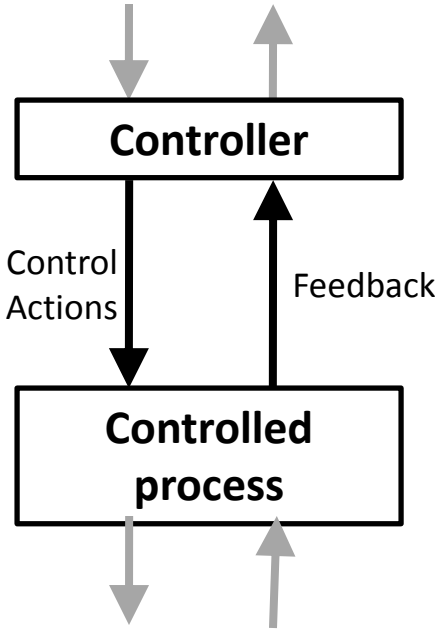
- System-level Accident (loss)
  - A-1: Two aircraft collide
  - A-2: Aircraft crashes into terrain / ocean
- System-level Hazards
  - H-1: Two aircraft violate minimum separation
  - H-2: Aircraft enters unsafe atmospheric region
  - H-3: Aircraft enters uncontrolled state
  - H-4: Aircraft enters unsafe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

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: ?

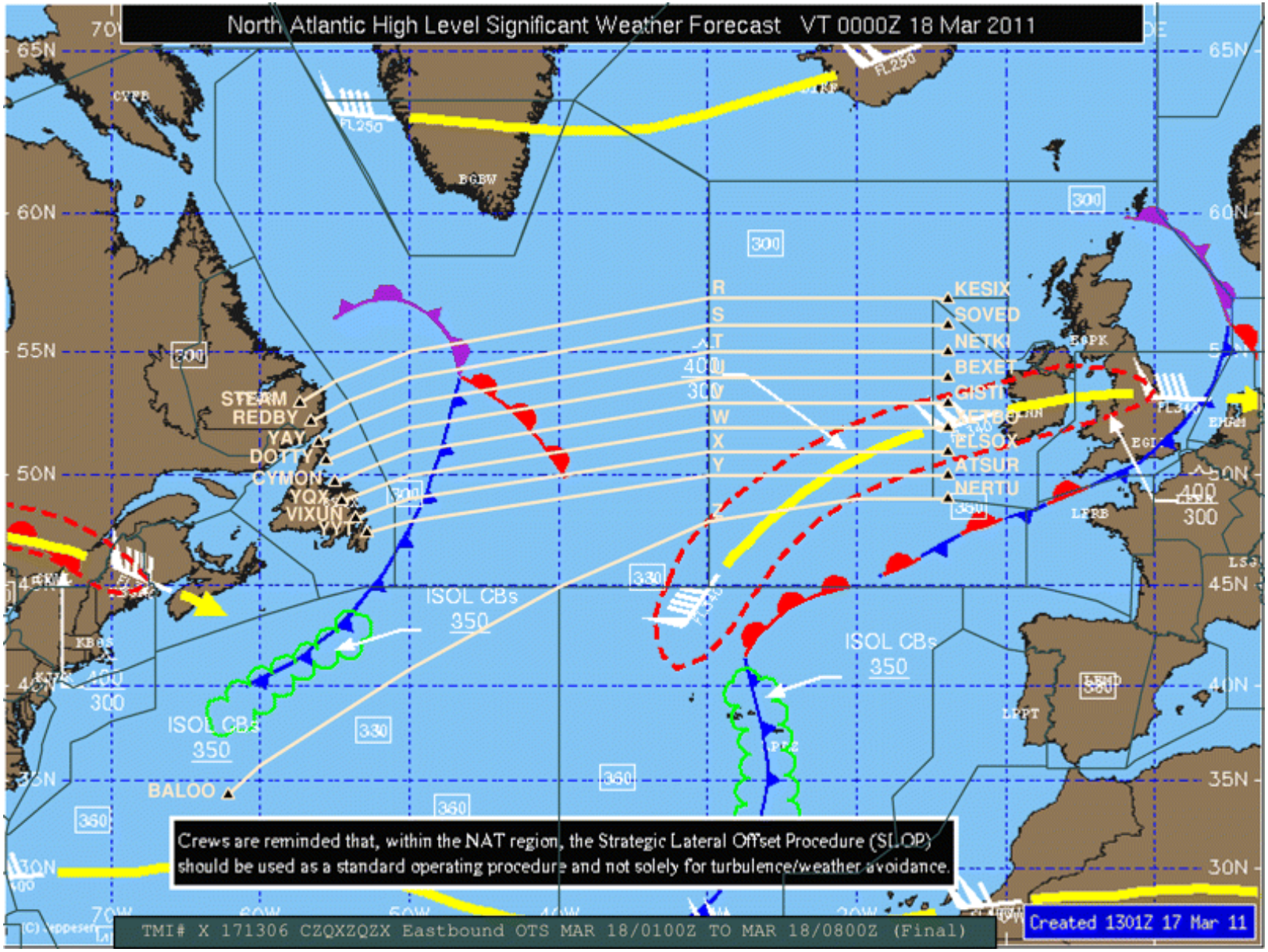
STPA
(System-Theoretic Process Analysis)

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



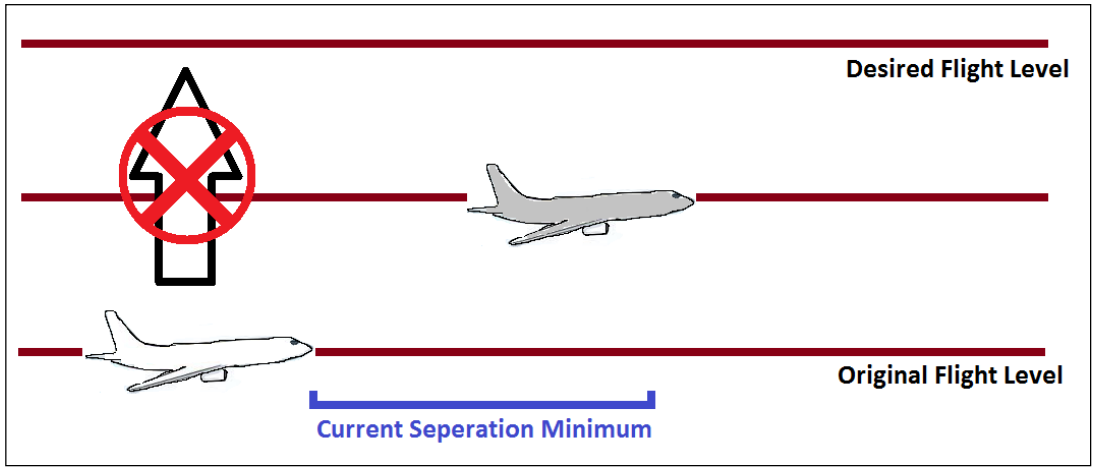
(Leveson, 2012)

North Atlantic Tracks



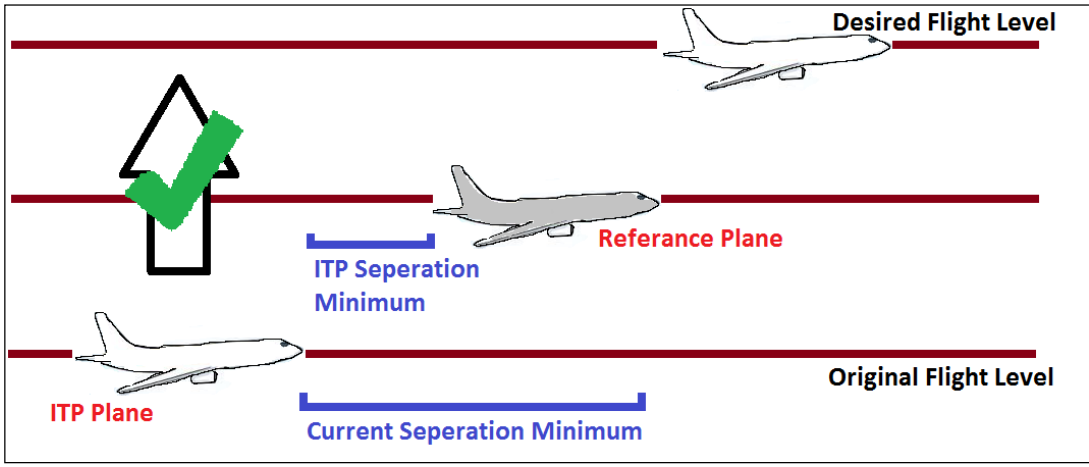
STPA application:
NextGen In-Trail Procedure (ITP)

Current State



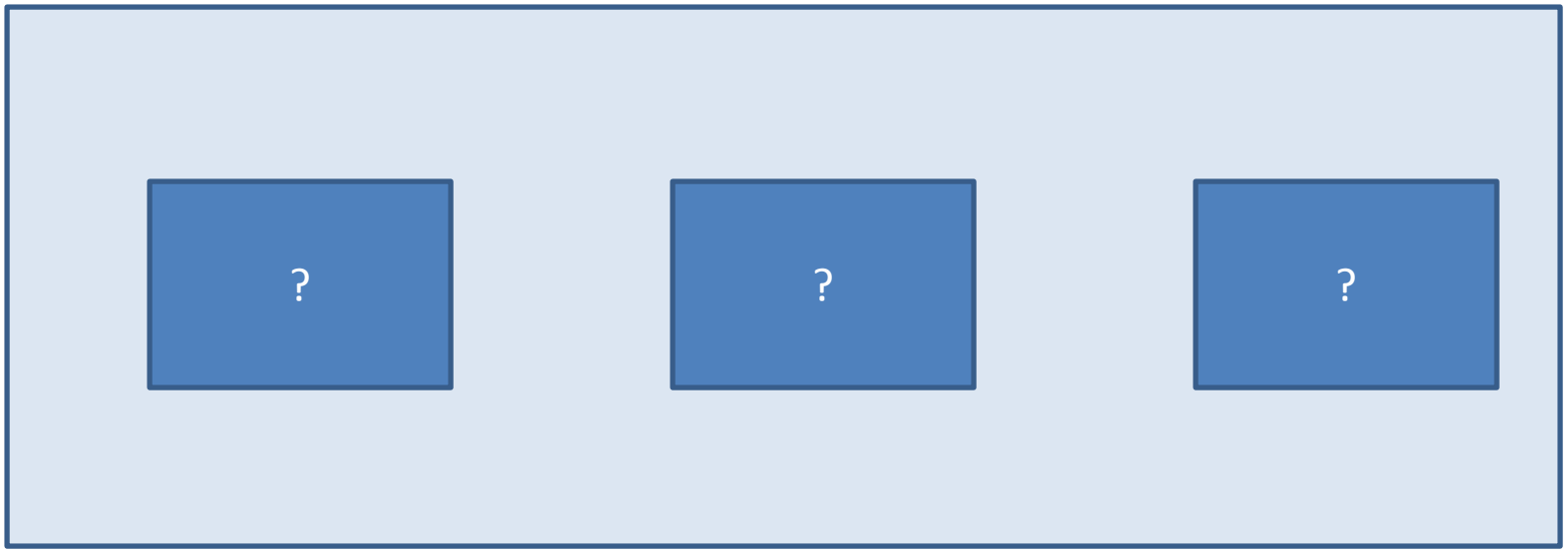
- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change



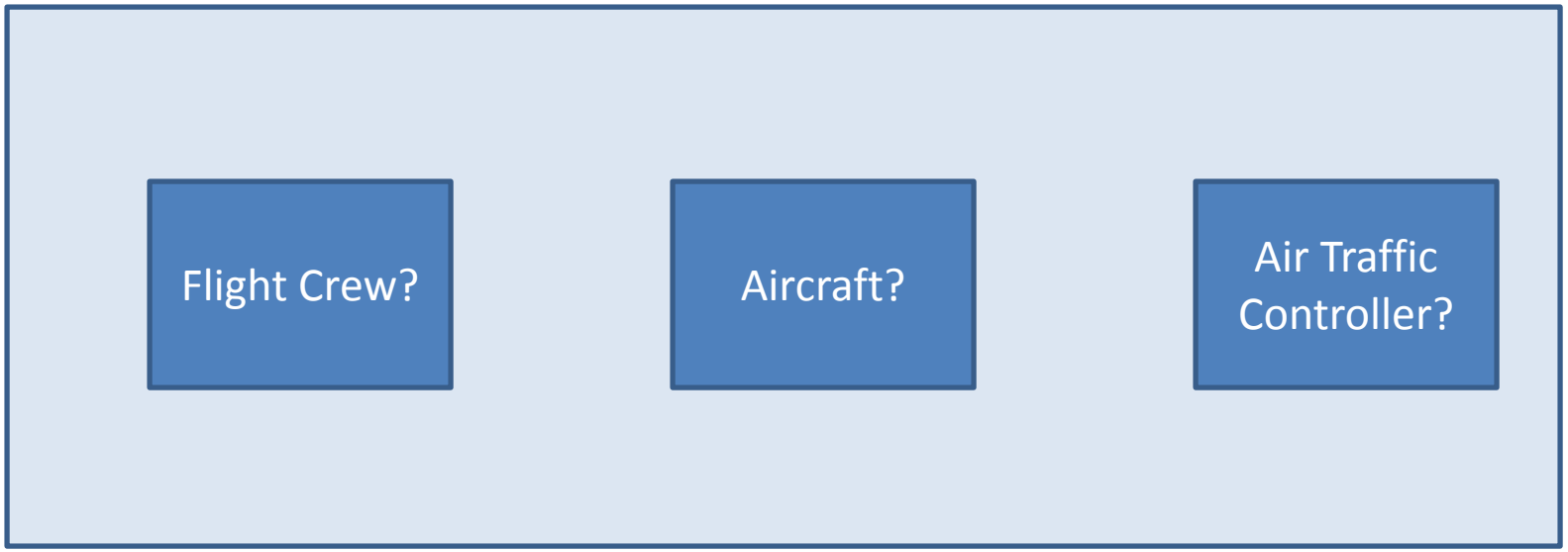
Draw the Functional Control Structure

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



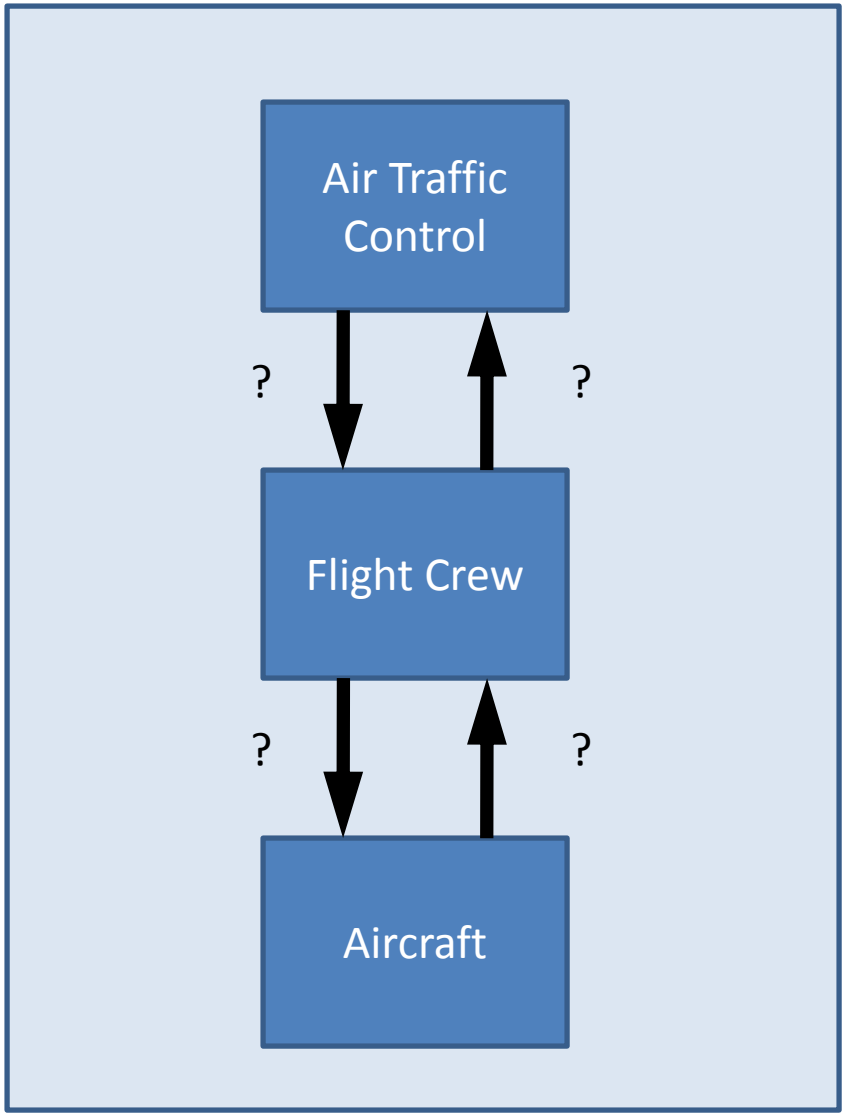
Draw the Functional Control Structure

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



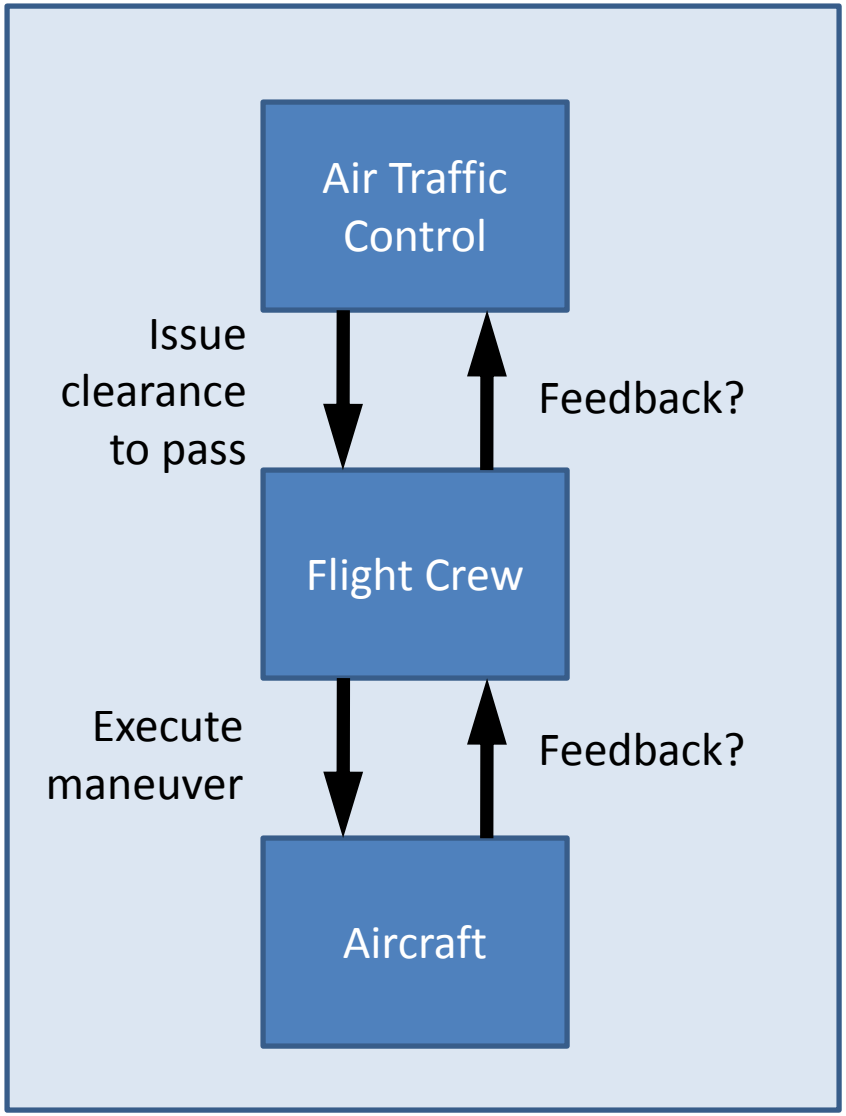
Draw the Functional Control Structure

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



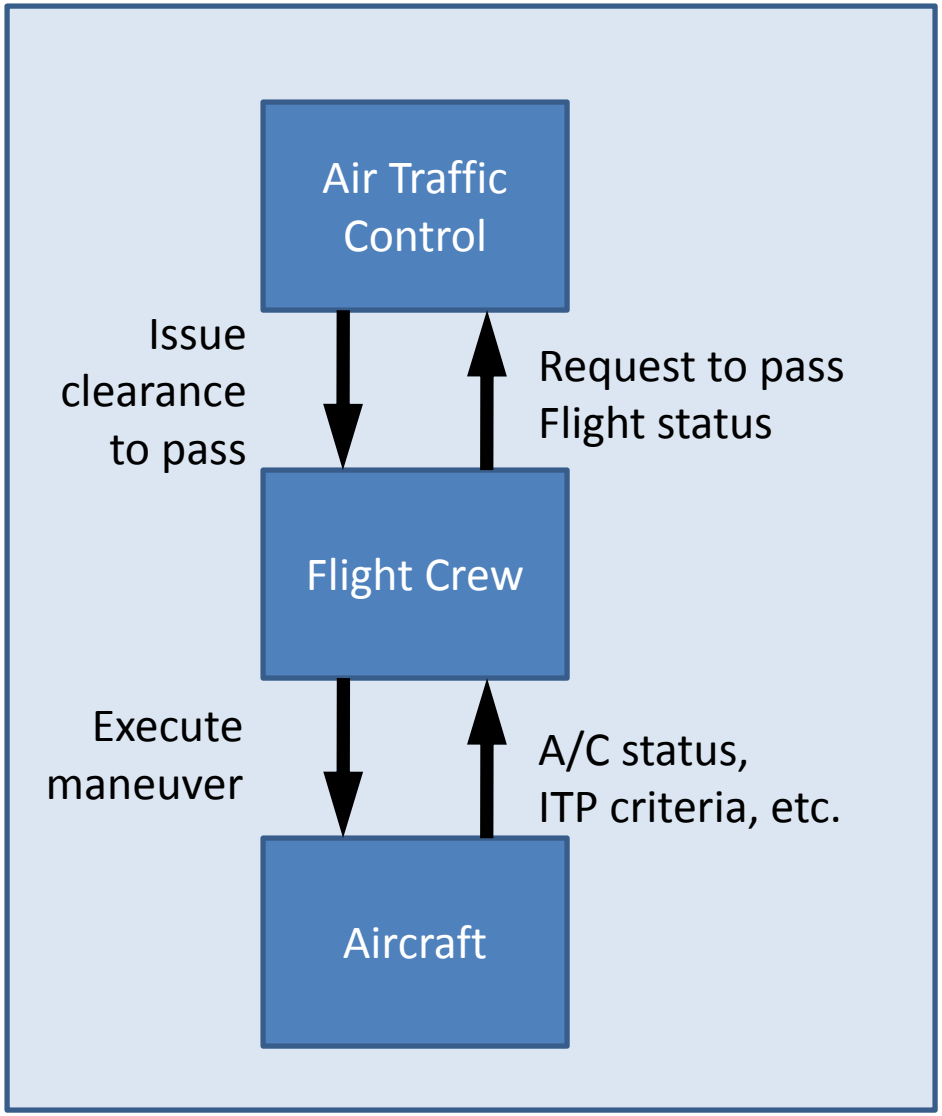
Draw the Functional Control Structure

- High-level (simple) Control Structure

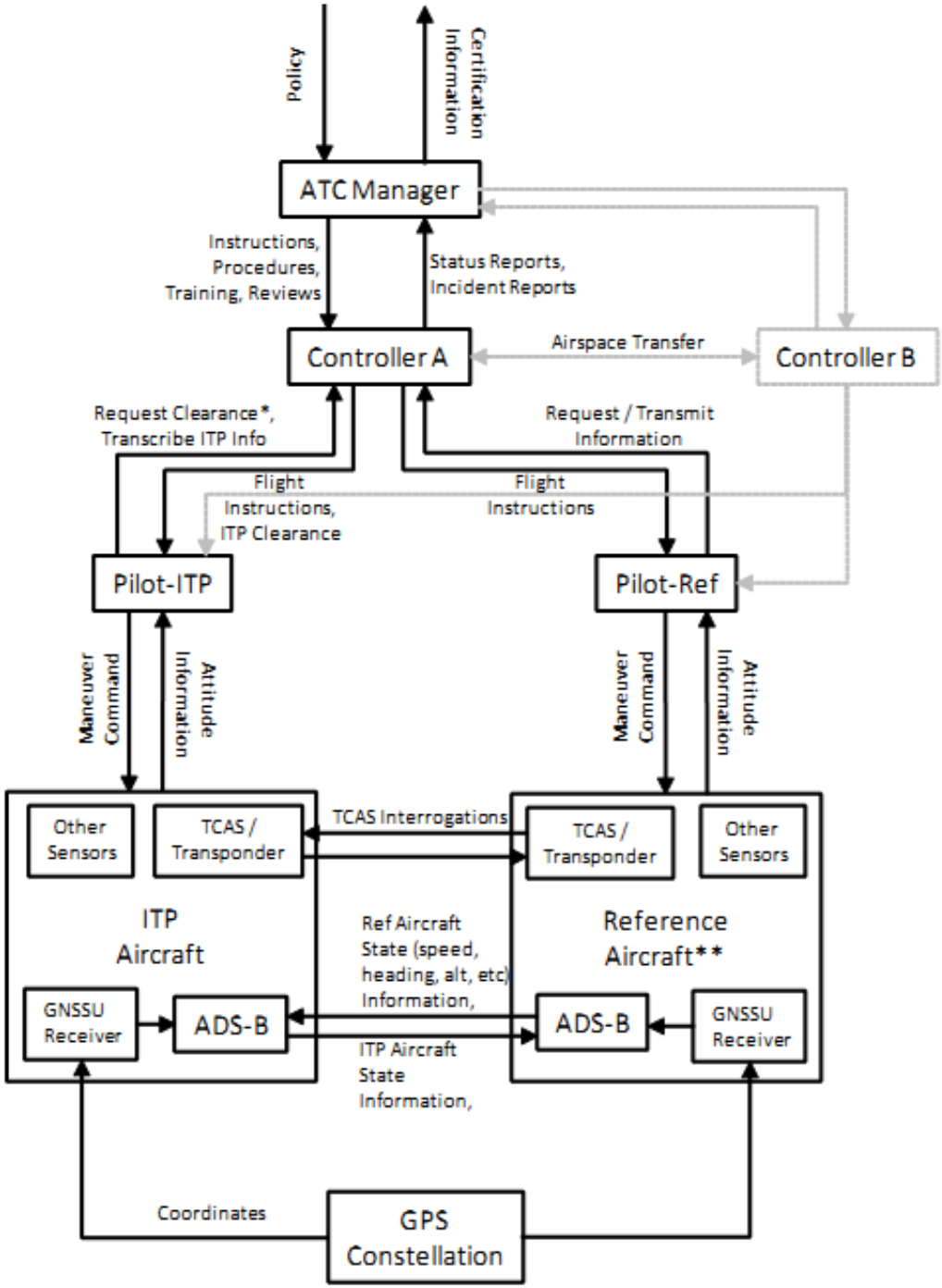


Draw the Functional Control Structure

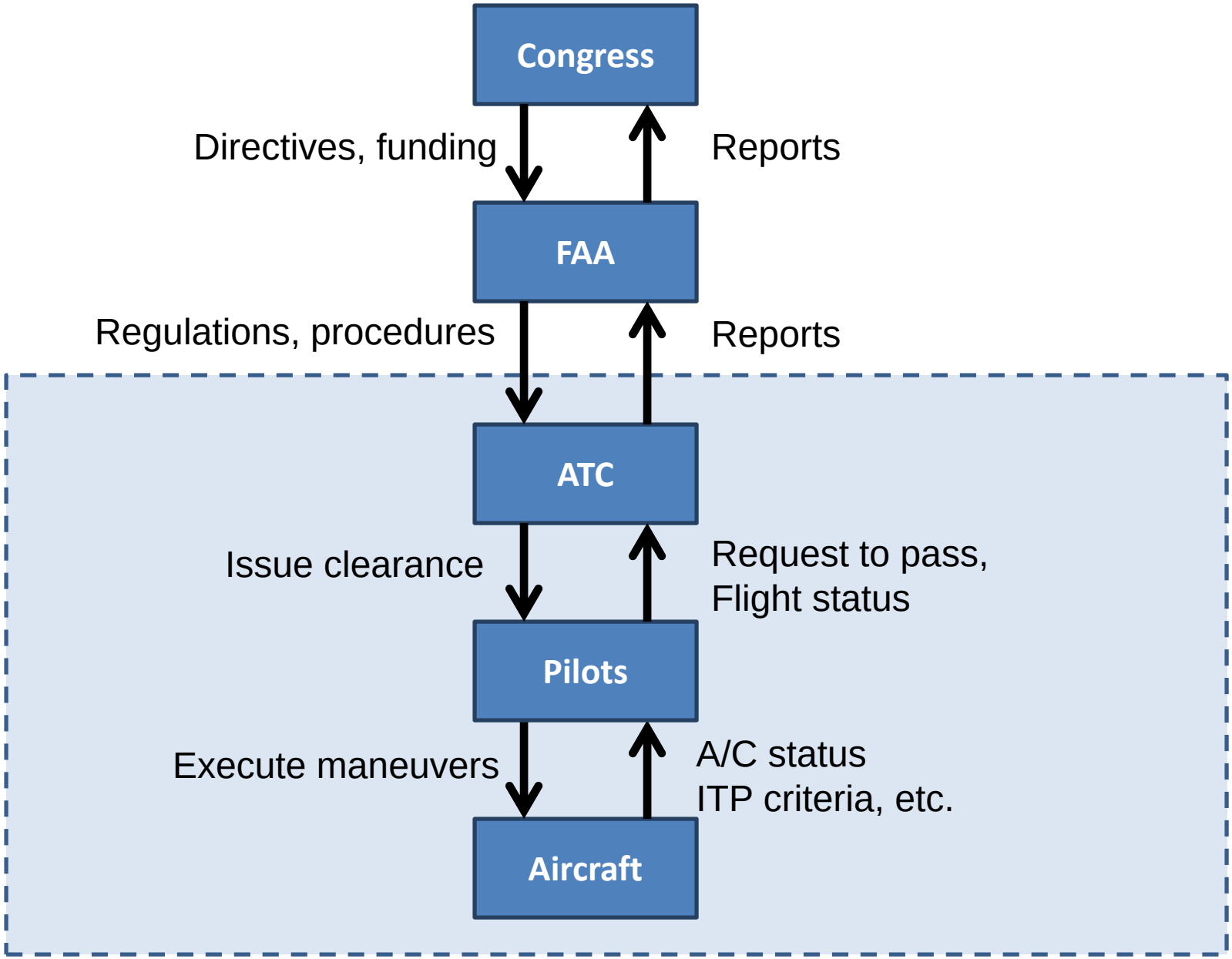
- High-level Control Structure

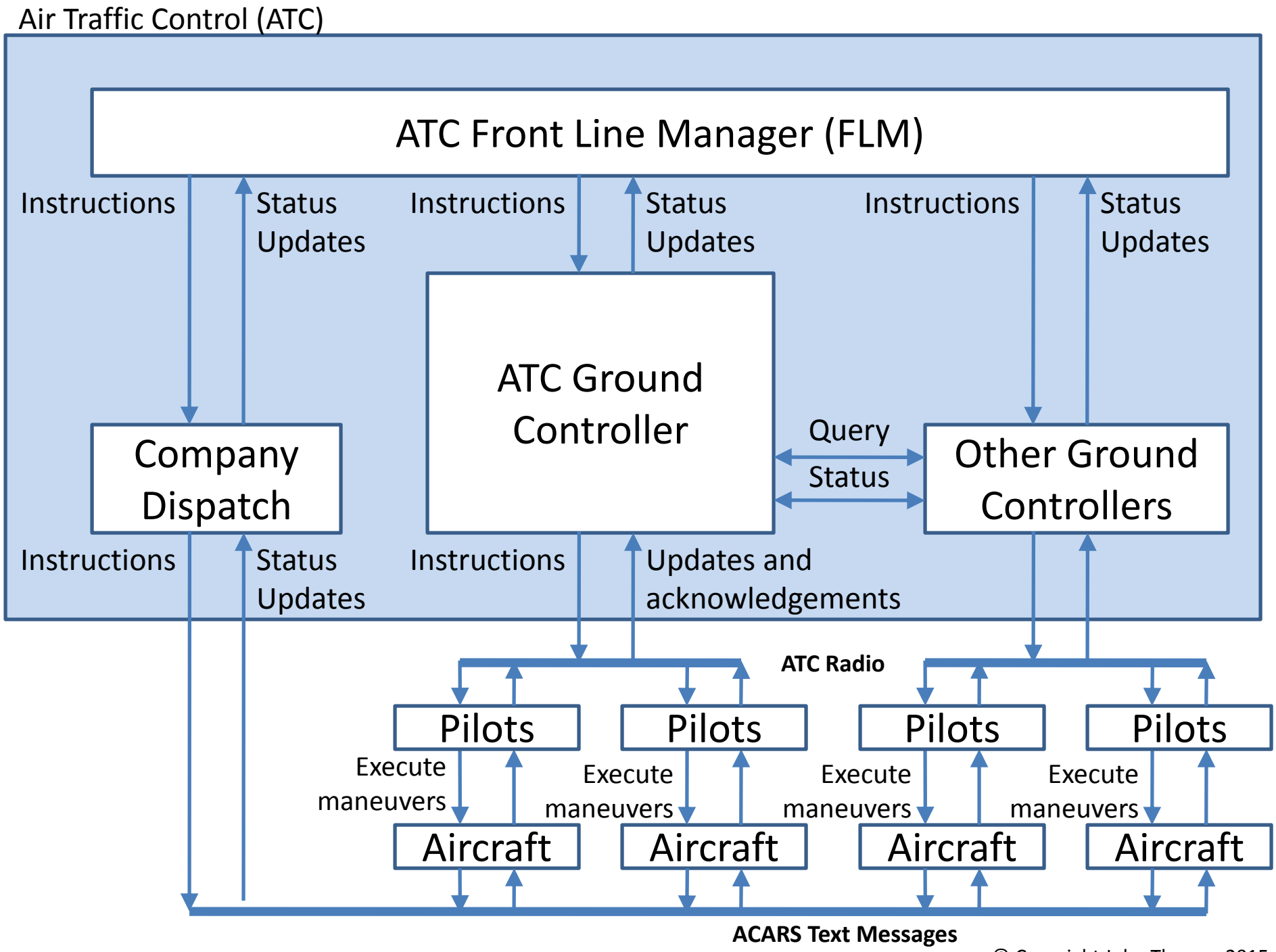


More complex control structure



Adding Levels





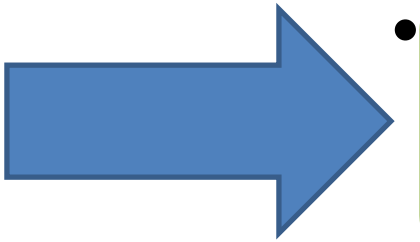
Pilot Responsibilities and Process Model

- Responsibilities:
  - Assess whether ITP maneuver is appropriate
  - Check if ITP criteria are met
  - Request ITP
  - Receive ITP approval
  - Recheck criteria
  - Execute flight level change
  - Confirm new flight level to ATC
- Process Model
  - Own ship climb/descend capability
  - ADS-B data for nearby aircraft (velocity, position, orientation)
  - ITP criteria (speed, distance, relative attitude, similar track, data quality)
  - State of ITP request/approval
  - etc.

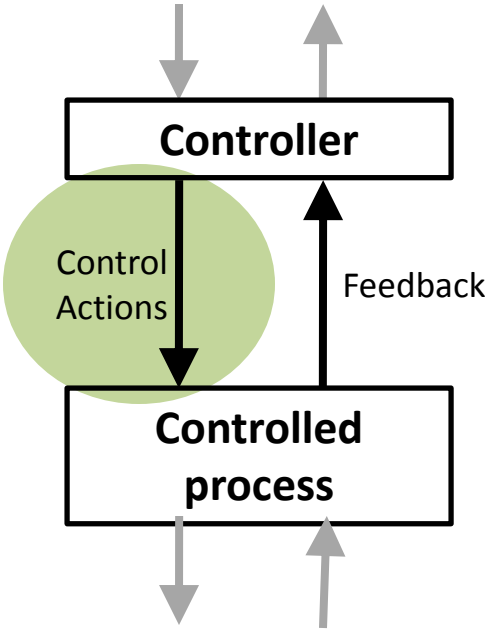
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards

- Draw the control structure



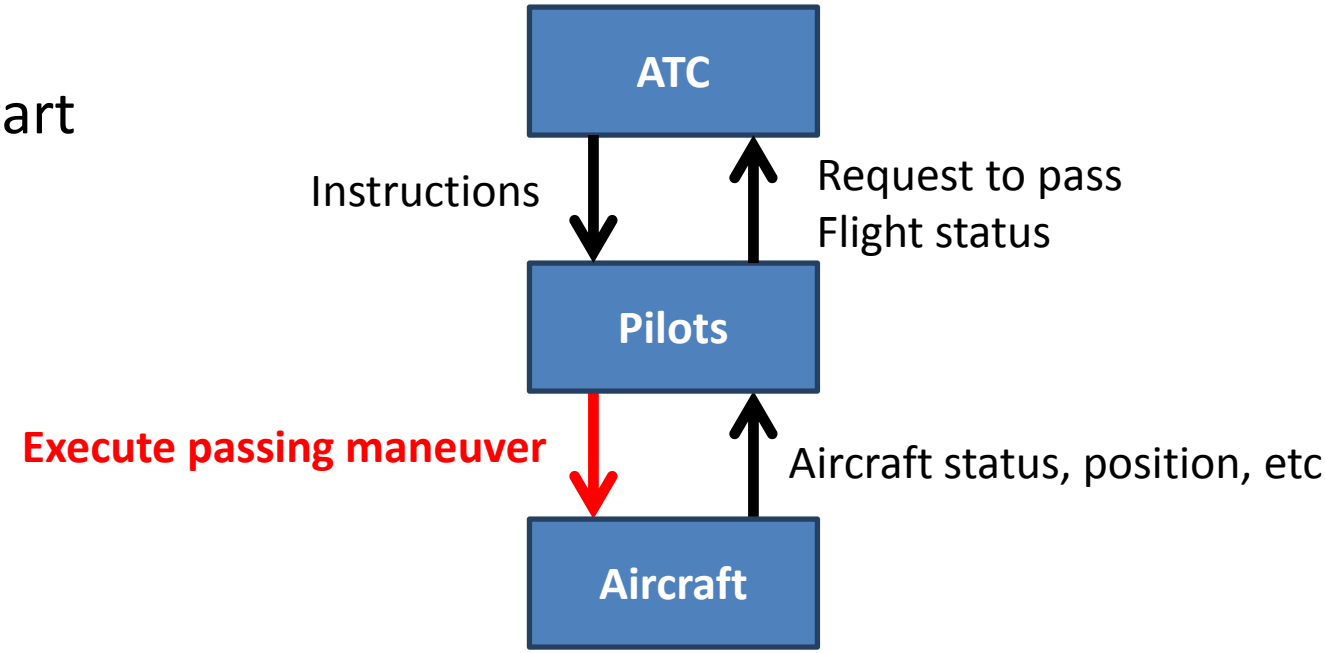
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

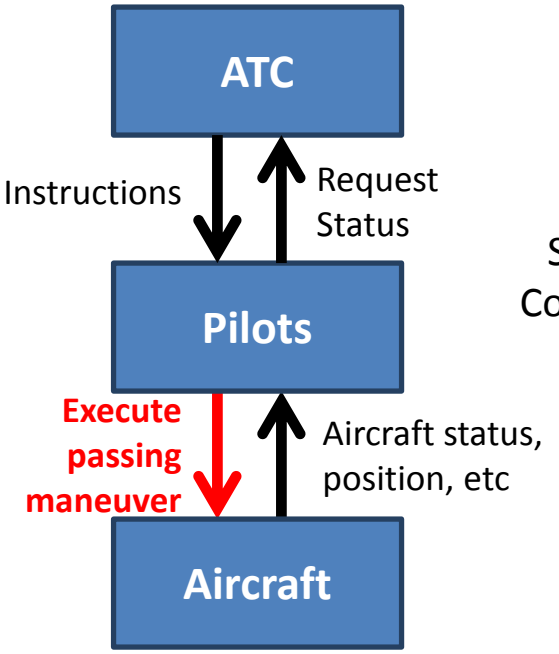
Identify Unsafe Control Actions

Example: Let's start with the pilot



Control Action	Not providing causes hazard	Providing Causes hazard	Incorrect Timing/ Order	Stopped Too Soon
Execute Passing Maneuver				

Identify Unsafe Control Actions



Example UCA:

"Pilots provide passing maneuver when maneuver is not approved"

- Pilots — Source Controller
- provide — Type
- passing maneuver — Control Action
- maneuver is not approved — Context

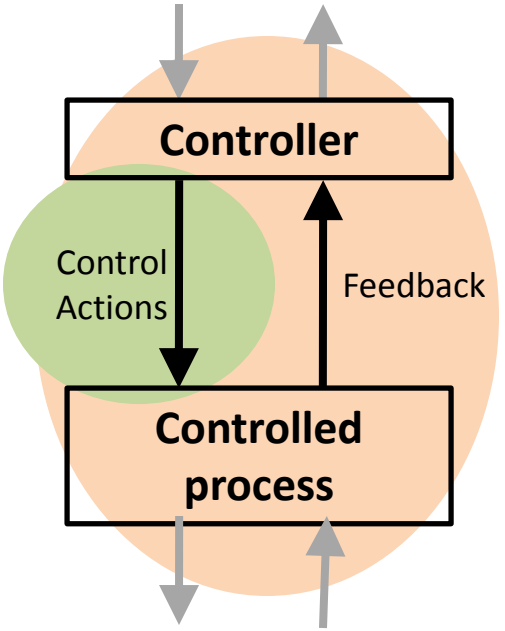
Control Action	Not providing causes hazard	Providing Causes hazard	Incorrect Timing/ Order	Stopped Too Soon
Execute Passing Maneuver	?	Pilots perform passing maneuver when it is not approved [H-1]	?	?

Controller Safety Constraints

Unsafe Control Action	Safety Constraint
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

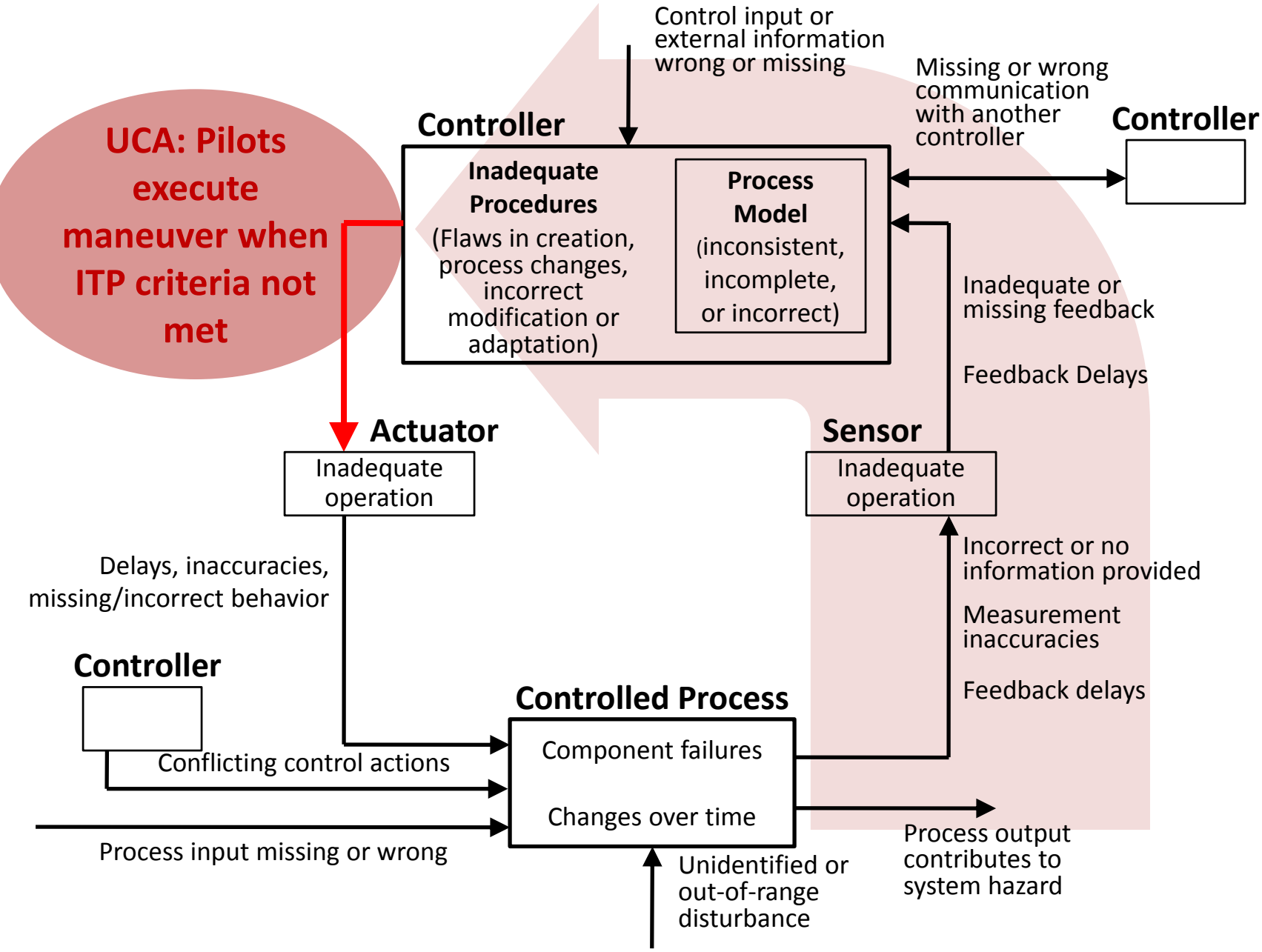
STPA
(System-Theoretic Process Analysis)

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



(Leveson, 2012)

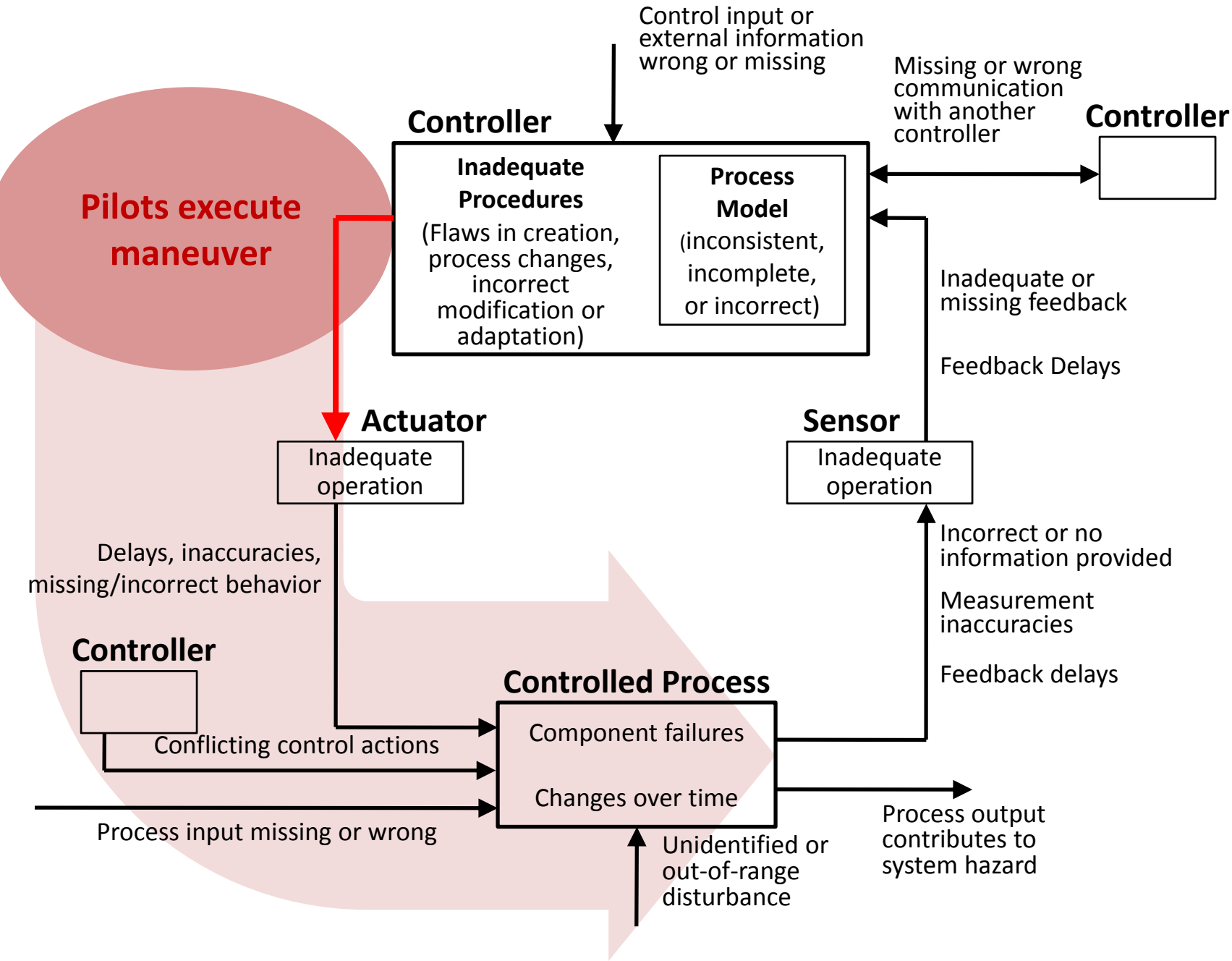
Step 2: Potential causes of UCAs



STPA Step 2: Causal Factors and Scenarios

- Select an Unsafe Control Action
  A. Identify what could cause the unsafe control action
     - Develop causal accident scenarios
  B. Identify how control actions may not be followed or executed properly
     - Develop causal accident scenarios

Step 2: Potential control actions not followed



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

For more information

- Google: “STPA Primer”
  - Written for industry to provide guidance in learning STPA
- Website: mit.edu/psas
  - Previous MIT STAMP workshop presentations
- Book
  - “Engineering a Safer World” by Nancy Leveson
- Sunnyday.mit.edu
  - Academic STAMP papers, examples