Reliability and System Risk Analysis Workshop

Dr. John Thomas

Today’s Agenda

- Intro to human issues
- Intro to software issues
- STAMP accident model
- System Theoretic Hazard Analysis (STPA)
  - Intro
  - Examples
  - Exercise

DC-10 Cargo Door

- Incident in 1972
  - AA Flight 96
  - Cargo door blew out during flight
  - Part of the floor collapsed
  - Severed all control cables and hydraulics (which ran along the floor)
  - Pilot Bryce McCormick had previously decided to train himself to fly with only the engines
  - Pilot landed successfully, nobody died
- See video
  - http://www.youtube.com/watch?v=FJhsBAnZJ0M

DC-10: The “root” cause

- What do you think was the “root” cause?

Root Cause Seduction

- Accidents always complex, but often blamed on “sharp end” factors

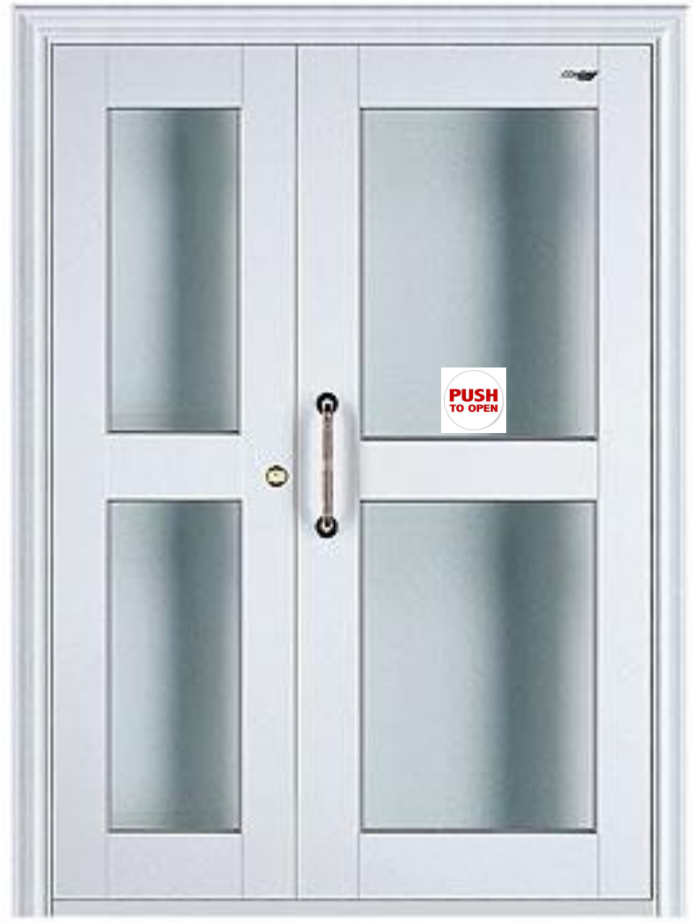
- Cannot prevent them unless understand ALL the factors that contributed

- Always additional factors (sometimes never identified)
  - Equipment design
  - Procedures
  - Management decisions
  - Etc.

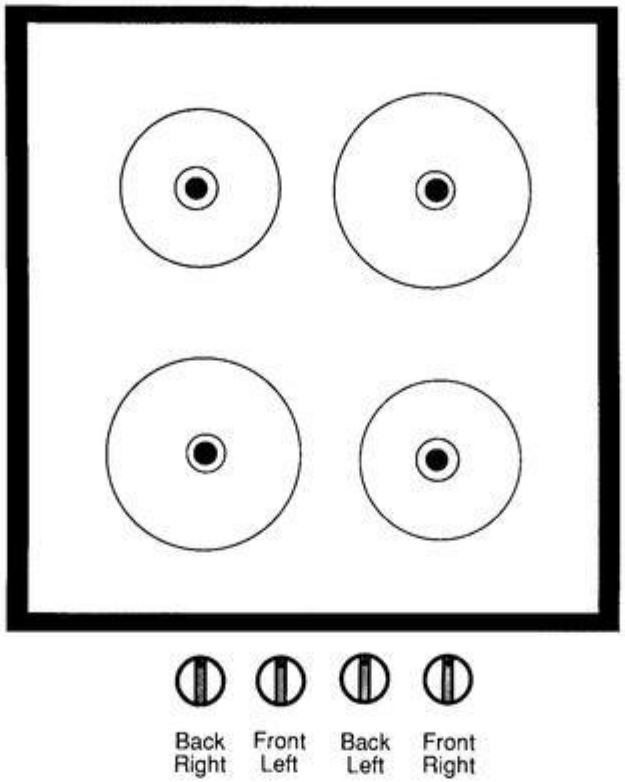
Root Cause Seduction

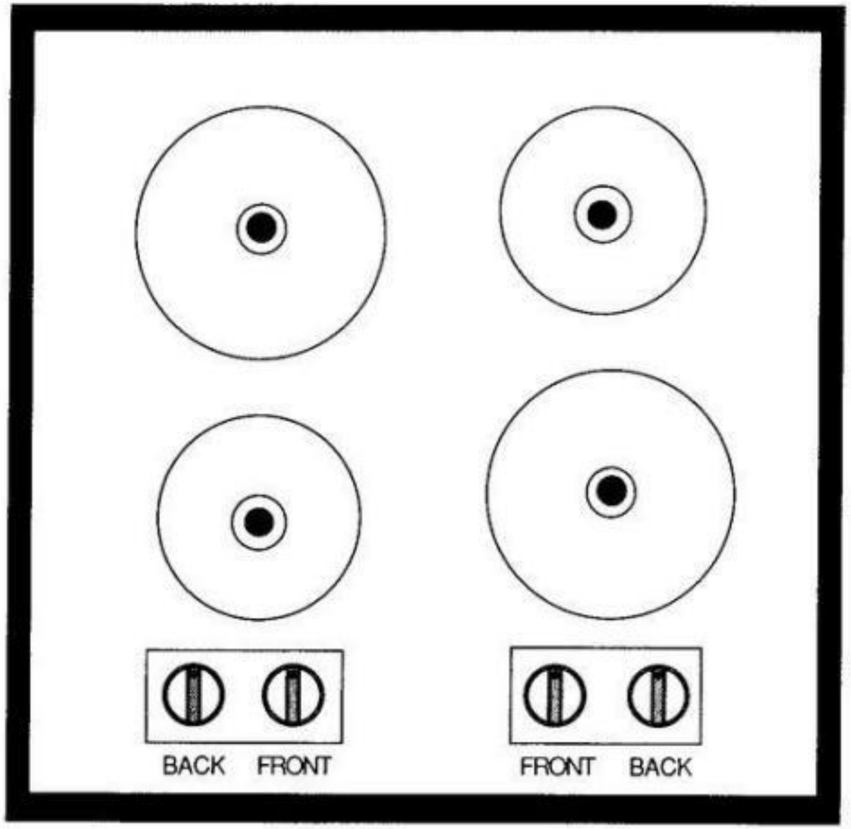
- Assuming there is a root cause gives us an illusion of control.
  - Usually focus on operator error or component failures
  - Ignore systemic and management factors
  - Leads to a sophisticated “whack a mole” game
    - Fix symptoms but not process that led to those symptoms
    - In continual fire-fighting mode
    - Having the same accident over and over

Poor design or human error?



Most stove tops

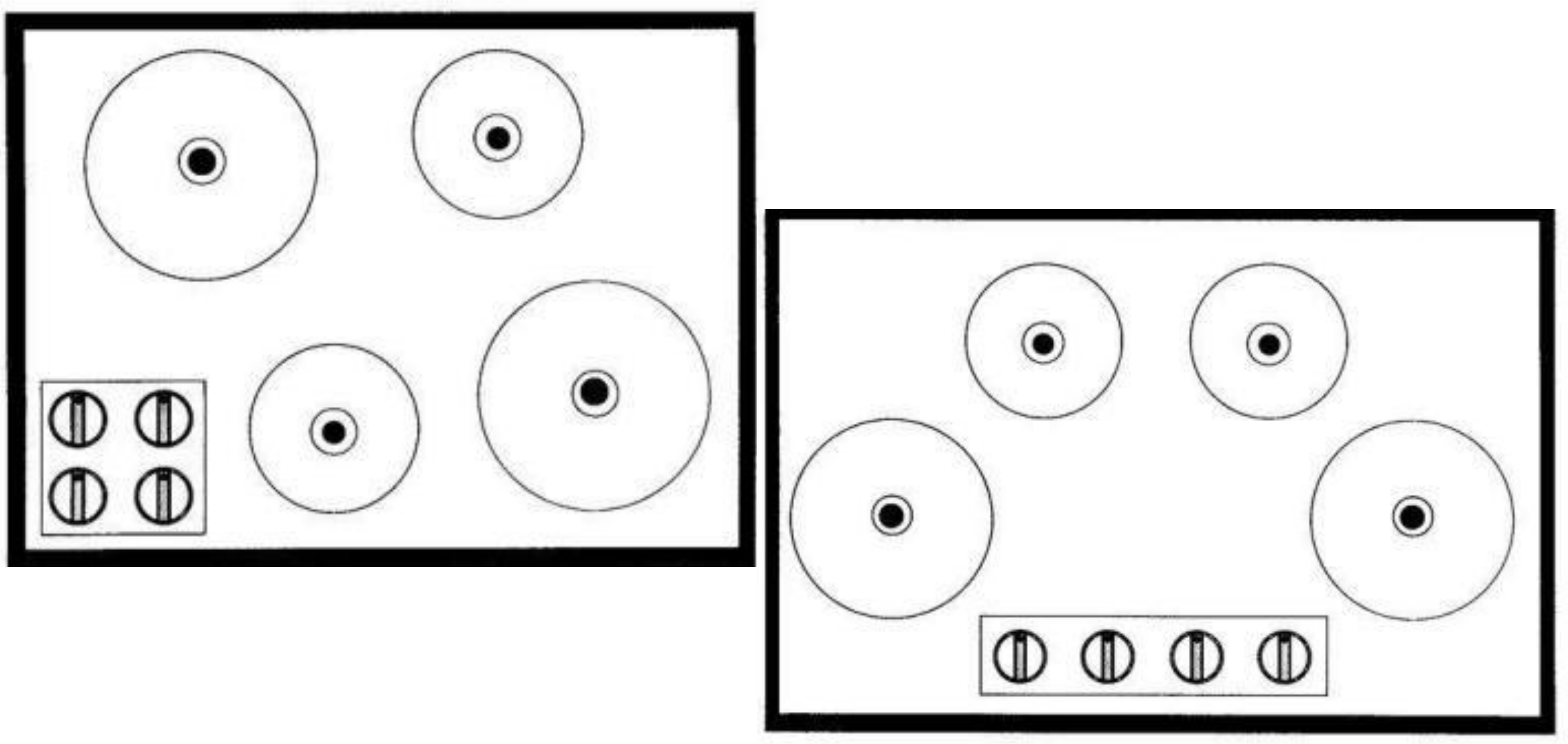




Is this a design problem or just human error?

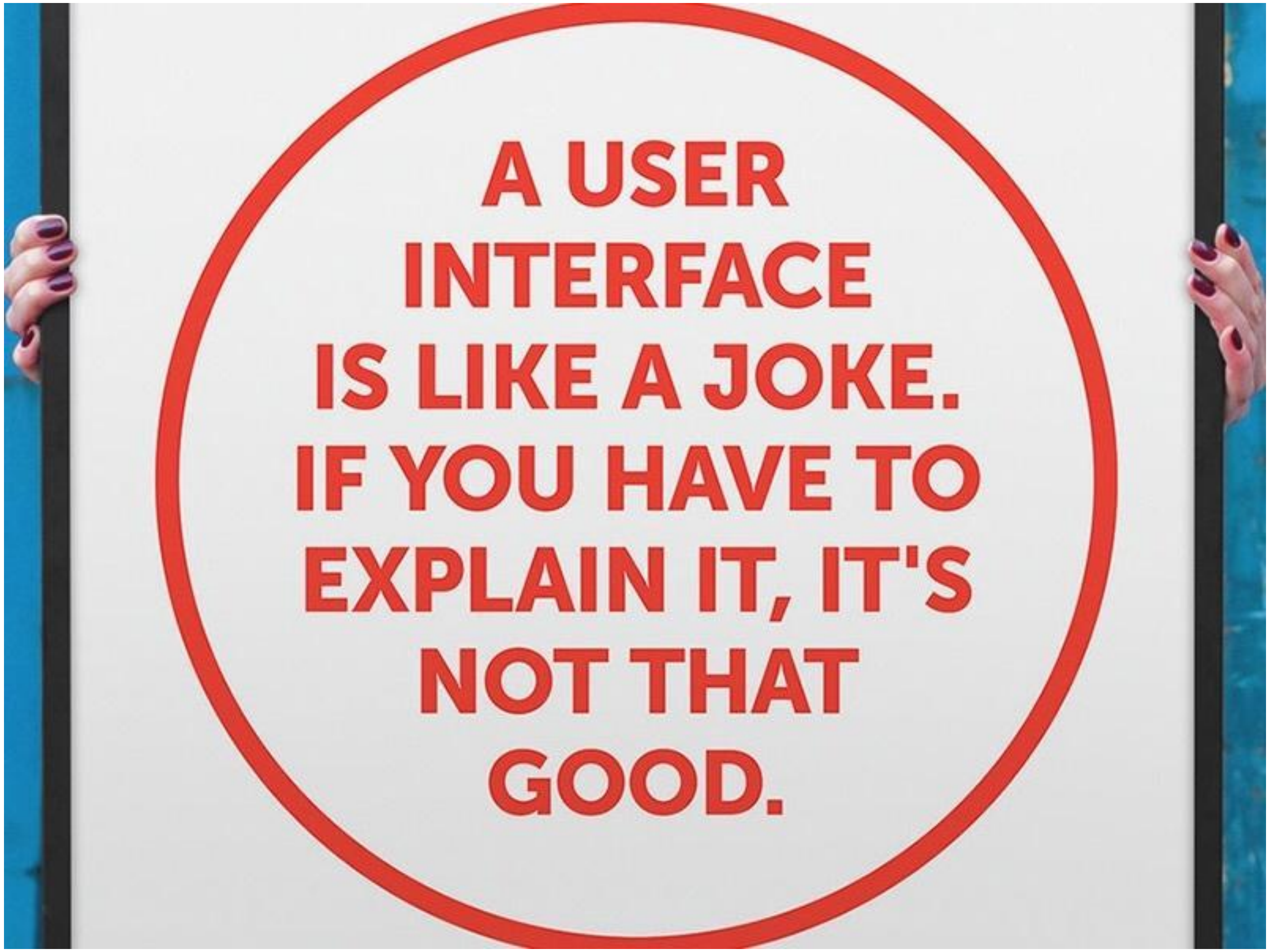
*Image from D. Norman, 1988

Natural Mapping



The right design will reduce human error

*Image from D. Norman, 1988



A USER INTERFACE IS LIKE A JOKE. IF YOU HAVE TO EXPLAIN IT, IT'S NOT THAT GOOD.

Using labels

- "If a design depends upon labels, it may be faulty. Labels are important and often necessary, but the appropriate use of natural mappings can minimize the need for them. Wherever labels seem necessary, consider another design."
  - Don Norman, The Design of Everyday Things

Human Error: Old View

- Human error is cause of incidents and accidents
- So do something about human involved (suspend, retrain, admonish)
- Or do something about humans in general
  - Marginalize them by putting in more automation
  - Rigidify their work by creating more rules and procedures

Human Error: New View

- Human error is a symptom, not a cause
- All behavior affected by context (system) in which occurs
- To do something about error, must look at system in which people work:
  - Design of equipment
  - Usefulness of procedures
  - Existence of goal conflicts and production pressures

(Sidney Dekker, Nancy Leveson, Jens Rasmussen, David Woods, etc.)

Norman

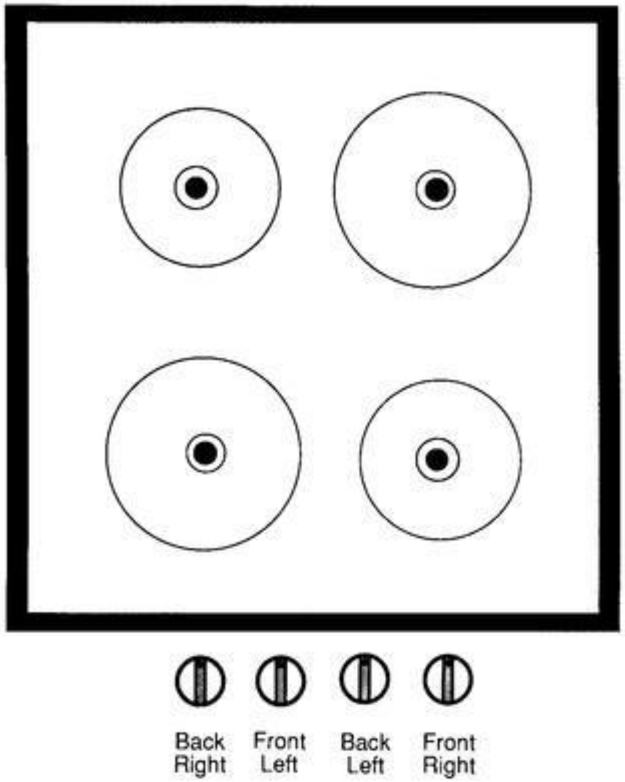
- “The Design of Everyday Things”
- Talks about designing things to minimize human error

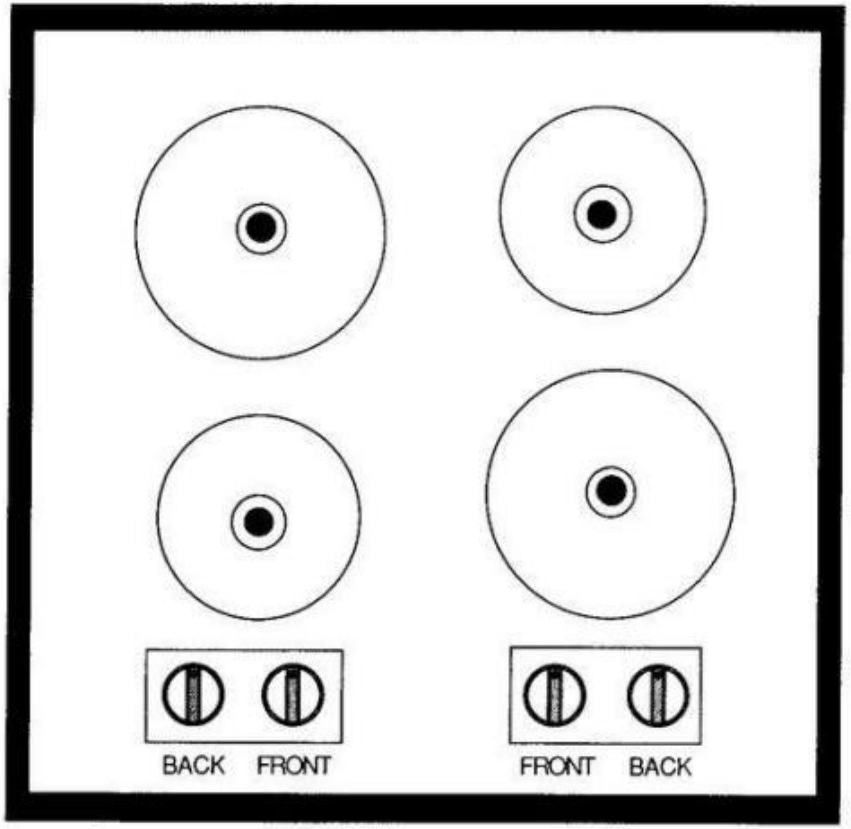
“Of course, people do make errors. Complex devices will always require some instruction, and someone using them without instruction should expect to make errors and to be confused. But designers should take special pains to make errors as cost-free as possible.”

Norman

- “The Design of Everyday Things”
- Talks about designing things to minimize human error

- “If an error is possible, someone will make it. The designer must assume that all possible errors will occur and design so as to minimize the chance of the error in the first place, or its effects once it gets made. Errors should be easy to detect, they should have minimal consequences, and, if possible, their effects should be reversible.”





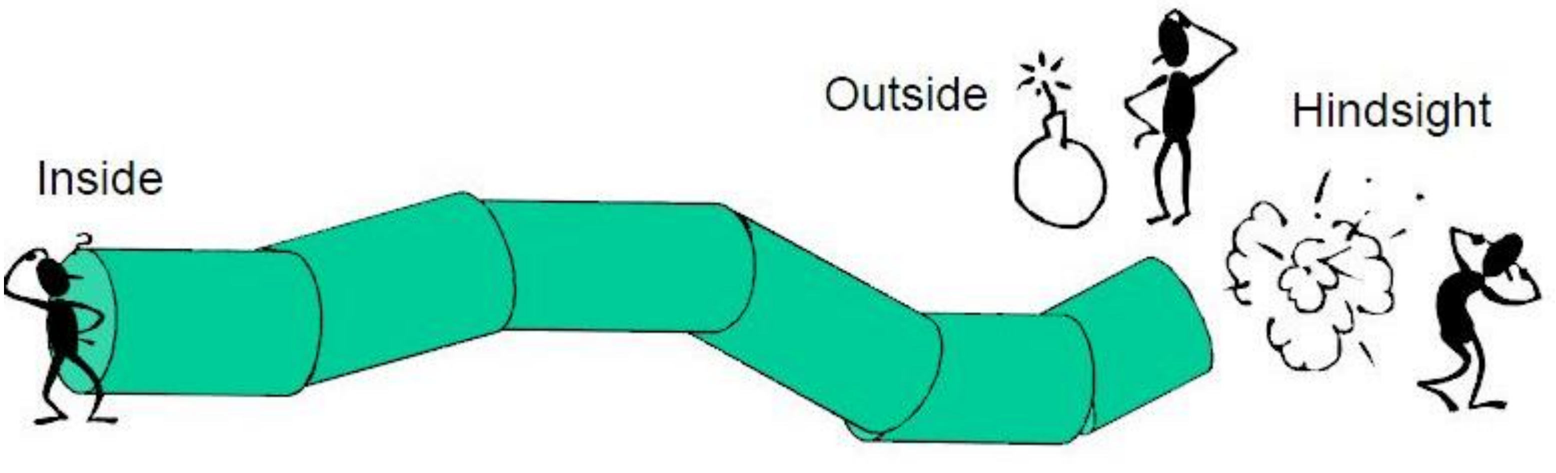
Make errors:

- Immediately detectable
- Minimal consequences
- Immediately reversible

*Image from D. Norman, 1988

Hindsight bias

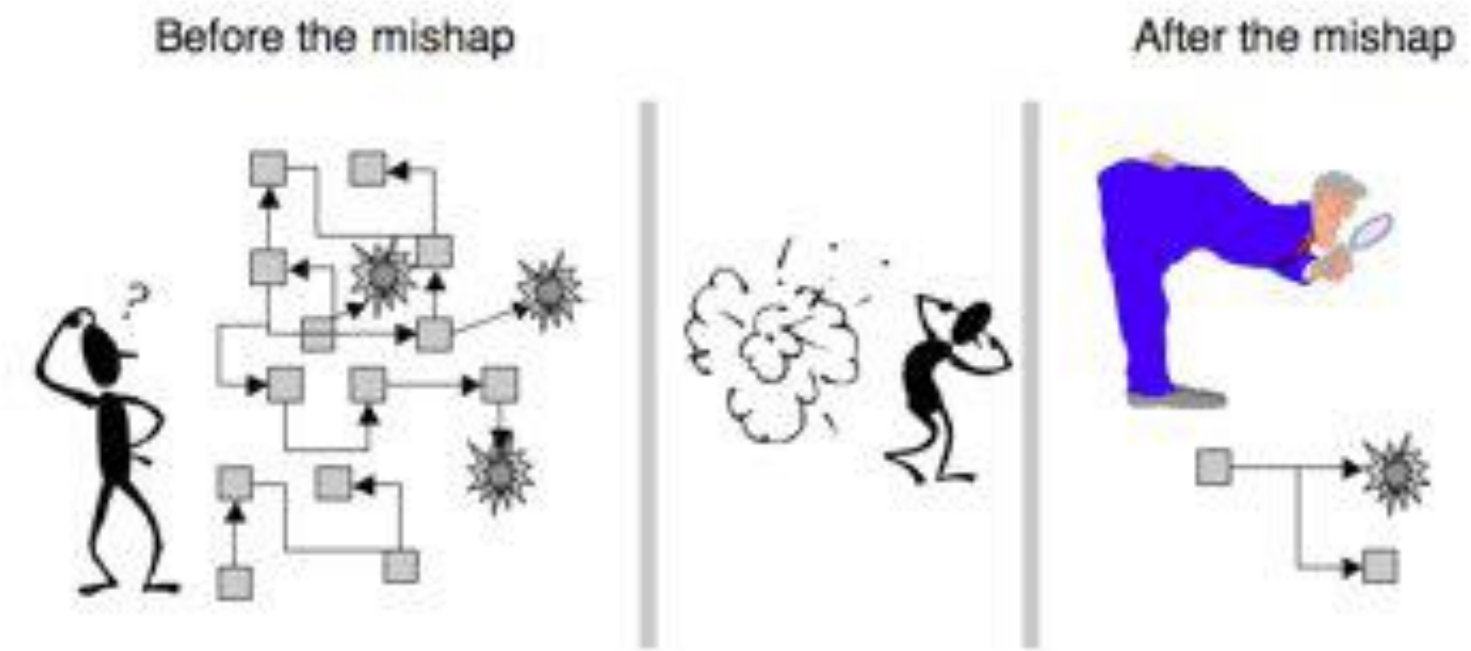
- In hindsight, the important factors are obvious
  - Easy to identify and disregard everything else
  - Easy to see where people went wrong, what they should have done or avoided
  - Easy to judge about missing a piece of information that turned out to be critical
  - Easy to see what people should have seen or avoided
- Makes human behavior seem strange, inexplicable
  - "Why in the world would they do that?"
  - Indicates a *lack of understanding*



Sidney Dekker

Hindsight bias

- Need to understand the operator's point of view
  - What information was actually presented?
  - What did the operator actually believe?
  - Why did that action seem reasonable to him at the time?



(Sidney Dekker, 2009)

"should have, could have, would have"

Sidney Dekker
Field Guide to Understanding Human Error

“The very use of the word ‘failure’ (for example: ‘the crew failed to recognize a mode change’) indicates that you are still on the outside of the tunnel, looking back and looking down. You are handing down a judgment from outside the situation. You are not providing an explanation from people’s point of view within.

Sidney Dekker
Field Guide to Understanding Human Error

“The word failure implies an alternative pathway, one which the people in question did not take (for example, recognizing the mode change). Laying out this pathway is counterfactual, as explained above. By saying that people ‘failed’ to take this pathway—in hindsight the right one—you judge their behavior according to a standard you can impose only with your broader knowledge of the mishap, its outcome and the circumstances surrounding it. You have not explained a thing yet. You have not shed light on how things looked on the inside of the situation; why people did what they did given their circumstances.”

Hindsight Bias

- Almost impossible to go back and understand how world looked to somebody not having knowledge of outcome
  - Oversimplify causality because start from outcome and reason backward
  - Overestimate likelihood of the outcome and people’s ability to foresee it because already know outcome
  - Overrate rule or procedure “violations”
  - Misjudge prominence or relevance of data presented to people at the time
  - Match outcomes with actions that went before it: if outcome bad, actions leading to it must have been bad too (missed opportunities, bad assessments, wrong decisions, and misperceptions)

Overcoming Hindsight Bias

- Assume nobody comes to work to do a bad job.
  - Simply finding and highlighting people's mistakes explains nothing.
  - Saying what did not do or what should have done does not explain why they did what they did.
- Need to understand why it made sense for people to do what they did
- Some factors that affect behavior
  - Goals person pursuing at time and whether may have conflicted with each other (e.g., safety vs. efficiency, production vs. protection)
  - Unwritten rules or norms
  - Information availability vs. information observability
  - Attentional demands
  - Organizational context

Incident analysis

- Very easy to blame sharp-end factors
  - Human error
  - Component failure / component reliability

- Very easy to fix only sharp-end problems, ignore rest

- Need systematic incident analysis method to identify deeper issues

Today’s Agenda

- Intro to software issues
- Intro to software issues
- STAMP accident model
- System Theoretic Hazard Analysis (STPA)
  - Intro
  - Examples
  - Exercise

Hypothetical Example:

- You are designing Version 2 of an expendable launch system. The purpose of the system is to deliver payloads (e.g. communication satellites) to low Earth orbit.
  - Version 1 is working well and can handle payloads up to 4800kg.
  - Version 2 is being developed to deliver heavier payloads up to 5900kg.
  - You are a safety engineer – your job is to make sure the vehicle is safe (low risk of being lost)
  - Today you are checking the inertial reference system (IRS) for any safety problems.
  - The system engineers explains: “We really just copied the same IRS software from Version 1, which has been thoroughly tested many times in the real world with no problems..“

Is the IRS component safe?

Real example: Ariane 5

- The Inertial Reference Software was copied from Ariane 4
- Never encountered a problem on Ariane 4
- Ariane 4 had lower horizontal velocity
- The spacecraft veered off course, destroyed. $370M

Safety depends on the context and the environment!

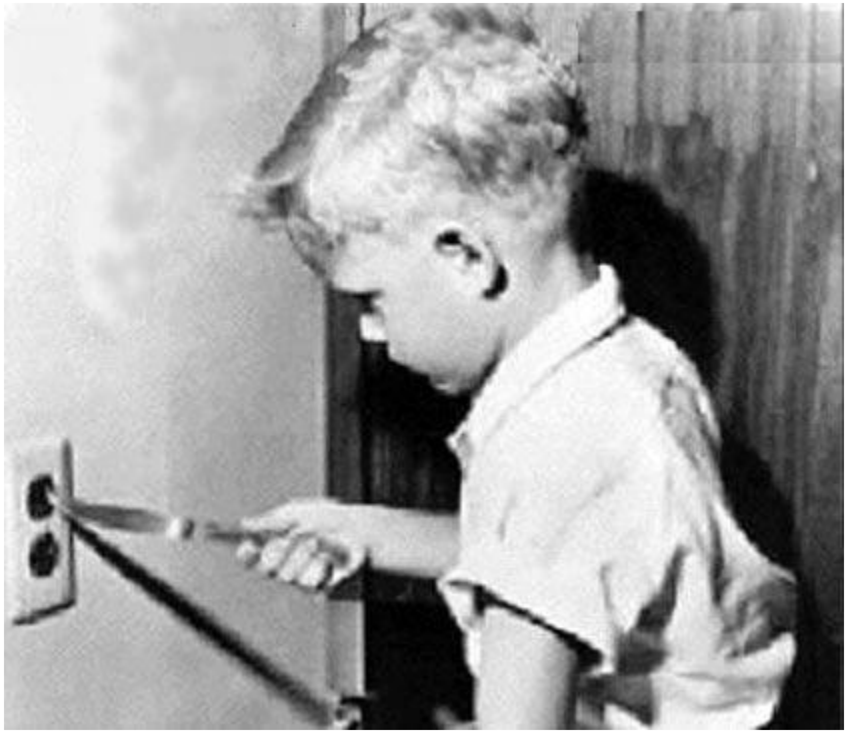
Safety as a component property

Safe or unsafe?

*Image: bluecashewkitchen.com

Safety is not a component property

- Safety is an emergent property of the system
  - Depends on context and environment!



Individual components are not inherently safe or unsafe

Toyota

- **2004:** Push-button ignition
- **2004:** Dealerships offer over-sized floor mats
- **2004-2009**
  - 102 incidents of stuck accelerators
  - Speeds exceed 100 mph despite stomping on the brake
  - 30 crashes
  - 20 injuries
- **2009, Aug**:
  - Car accelerates to 120 mph
  - Passenger calls 911, reports stuck accelerator
  - Car crashes killing 4 people
- **2010, Jul:**
  - Toyota: “Pedal Misapplication”, driver error
  - Investigated of 2,000 cases of unintended acceleration

How did you determine the software was flawed?

Implications for analysis

- Safety is not a property of the software / human
- Outward-looking analysis
  - Must emphasize interactions between software and it's environment
  - Must emphasize interactions between humans and their environment
  - Identify necessary behavior
  - Get the right requirements first
- Then use verification to ensure requirements are met
  - Simulation, testing, analysis, etc.

Toyota: Would redundancy help?

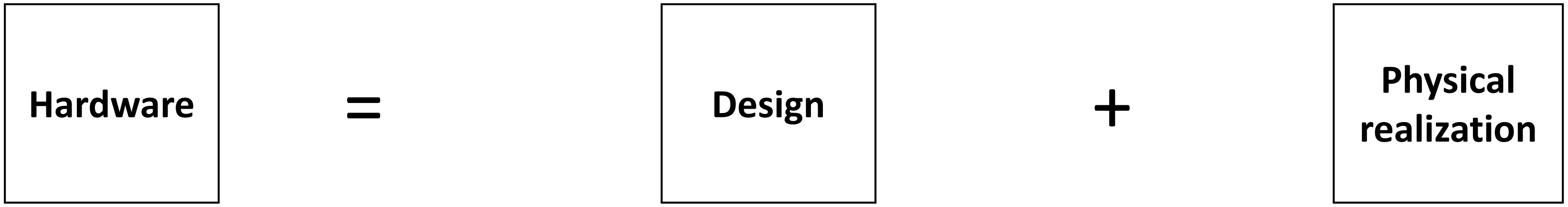
- **2004:** Push-button ignition
- **2004:** Dealerships offer over-sized floor mats
- **2004-2009**
  - 102 incidents of stuck accelerators
  - Speeds exceed 100 mph despite stomping on the brake
  - 30 crashes
  - 20 injuries
- **2009, Aug**:
  - Car accelerates to 120 mph
  - Passenger calls 911, reports stuck accelerator
  - Car crashes killing 4 people
- **2010, Jul:**
  - Toyota: “Pedal Misapplication”, driver error
  - Investigated of 2,000 cases of unintended acceleration

Did the push button “fail”?

Software

- Fundamentally different from other components
  - Software always does exactly what you tell it to do
- What does this say about standard engineering approaches?
  - Increasing component reliability
  - Preventing failures through redundancy
  - Reuse of designs

Hardware Problem Types



Hardware = **Design** + **Physical realization**

Essentially an idea, a plan in someone’s mind.

Example: Use a hall effect sensor to detect when spacecraft has landed

The physical system constructed according to the design

Example: light bulb might wear out over time, eventually fail

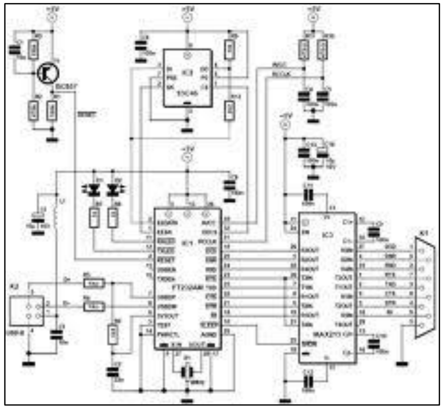
Hardware Composition

Design errors

Hardware failures

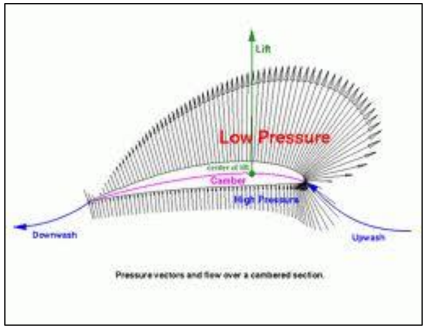
Hardware = Design + Physical realization

Electronic Module =



+

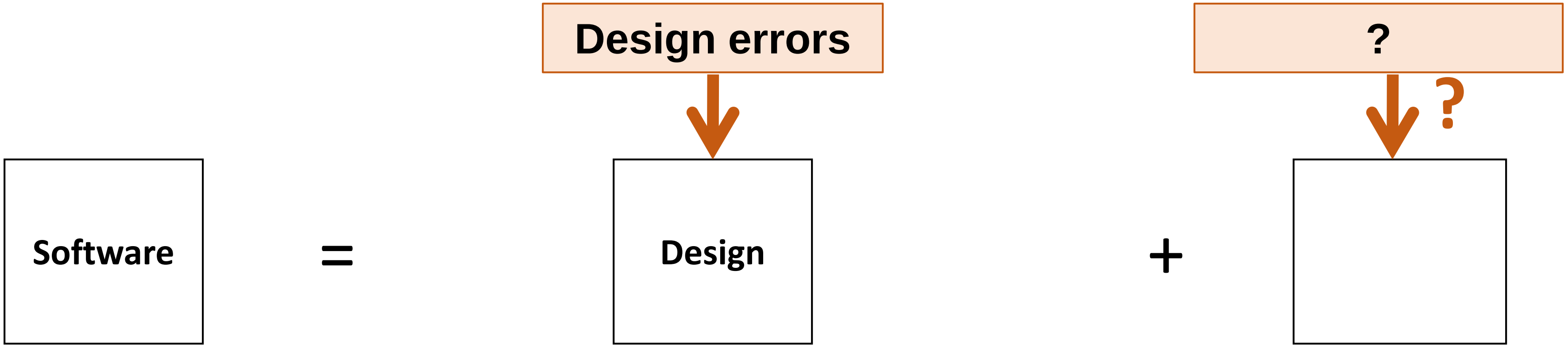
Wing =



+

Which type does redundancy address?

Software Composition



Design errors

?

?

Software = Design +

Chemical reactor program =

```
Open catalyst valve
Open cooling valve
If any fault is detected then
     halt all actions
```

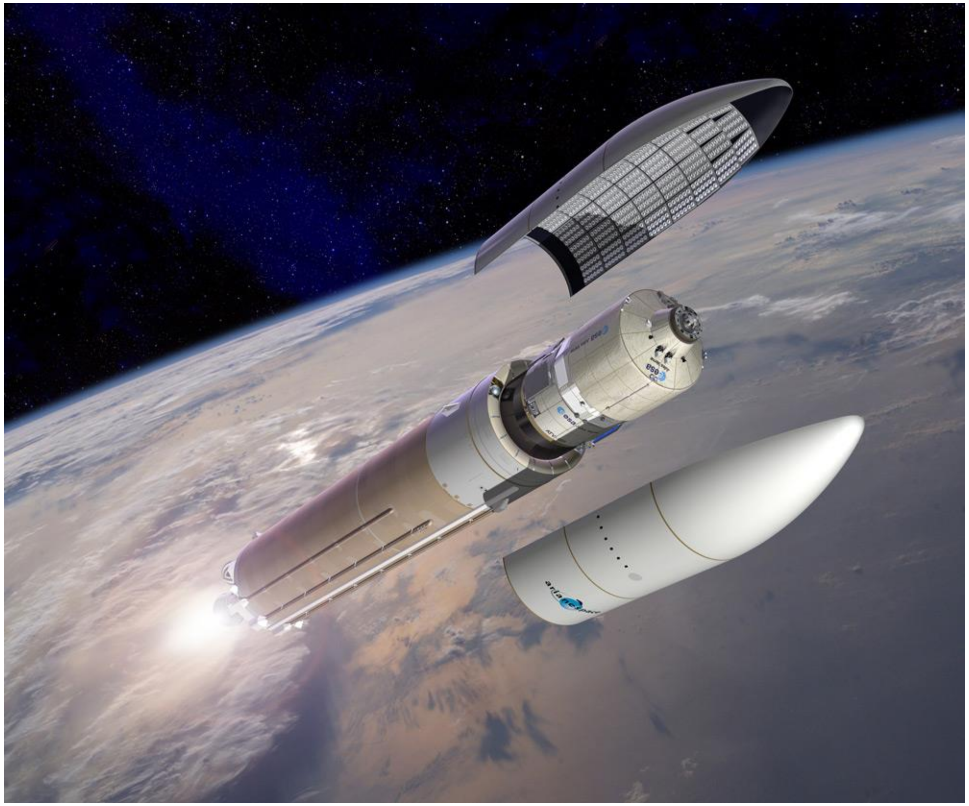
Autopilot program =

```
If airspeed < X then
     increase engine throttle
If airspeed > Y then
     decrease engine throttle
```

Which does redundancy address?

Making Software Redundant

- Ariane 5 had two redundant Inertial Reference Systems
  - Identical hardware
  - Identical software
- Software halted
  - Occurred in both systems at the same time
- $370M vehicle destroyed



Solutions for component failures may not work for software!

Mars Polar Lander

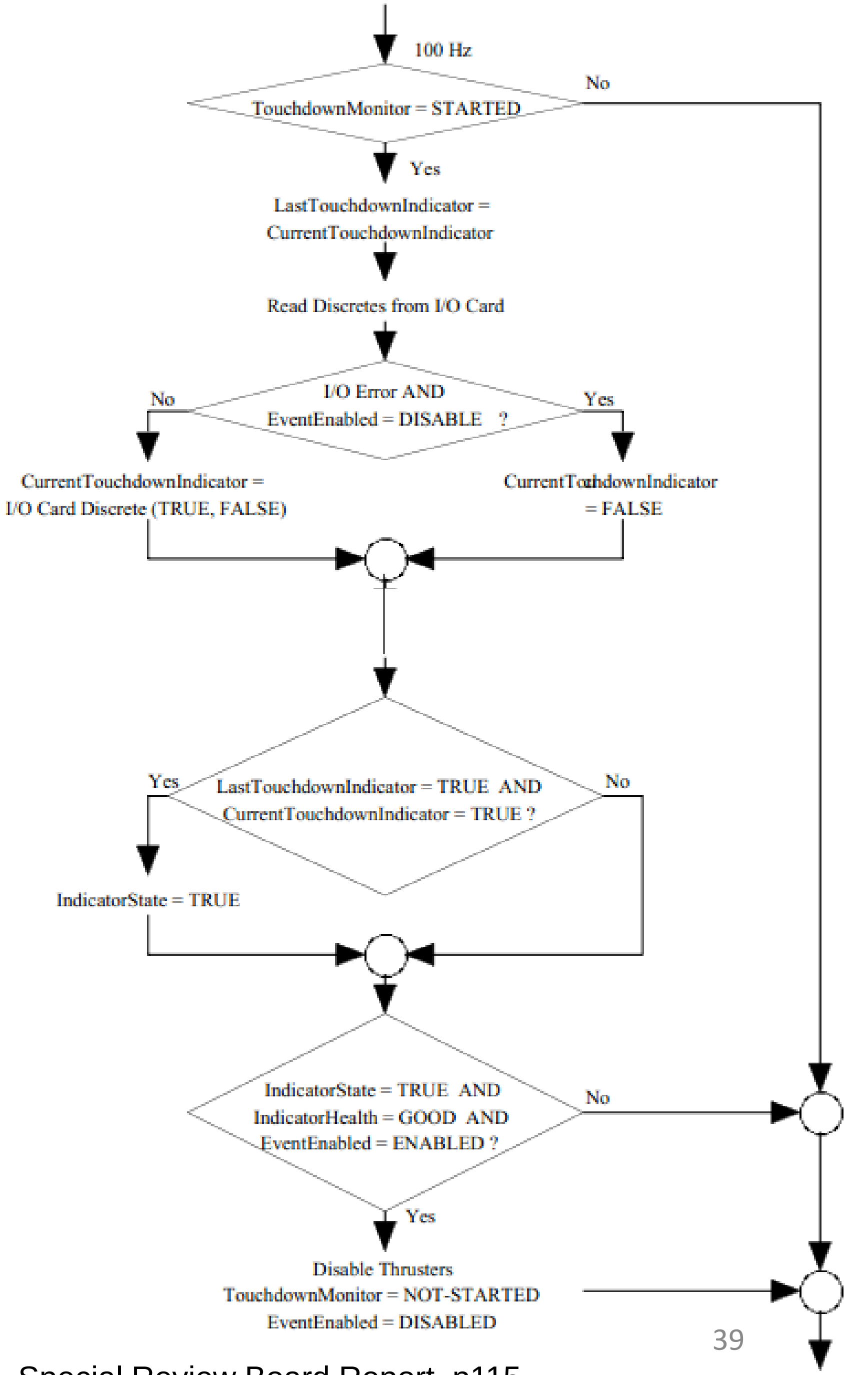
- During the descent to Mars, the legs were deployed
- Touchdown sensors (on the footpads) sent a momentary signal
- The software responded as it was designed to: by shutting down the descent engines
- The vehicle free-fell and was destroyed upon hitting the surface

No single component failed
All components performed as designed

What was the software problem?

- Didn’t “wear out” like valves or light bulbs

- Software performed exactly as designed

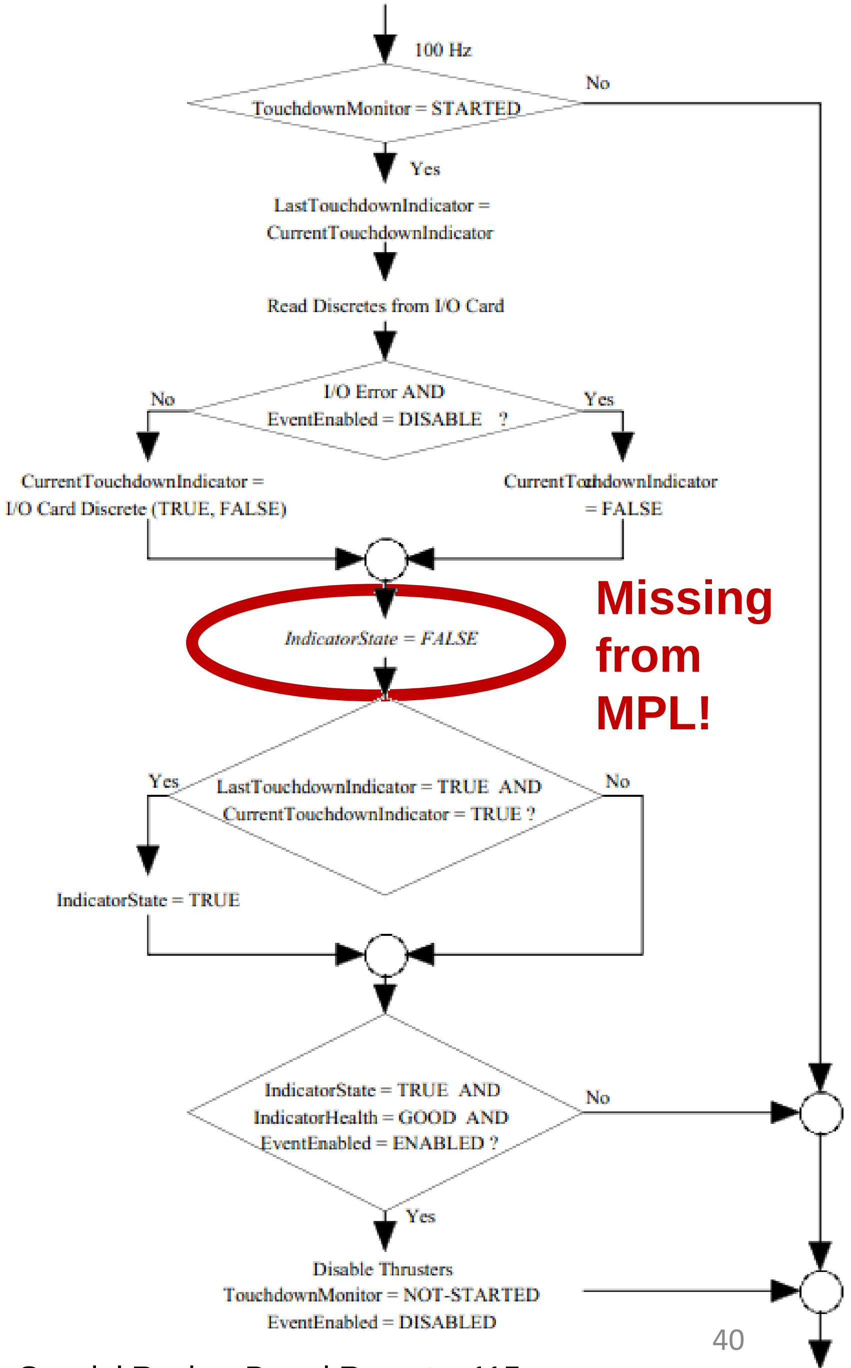


100 Hz
TouchdownMonitor = STARTED
No
Yes
LastTouchdownIndicator = CurrentTouchdownIndicator
Read Discretes from I/O Card
I/O Error AND EventEnabled = DISABLE ?
No
Yes
CurrentTouchdownIndicator = I/O Card Discrete (TRUE, FALSE)
CurrentTouchdownIndicator = FALSE
LastTouchdownIndicator = TRUE AND CurrentTouchdownIndicator = TRUE ?
Yes
No
IndicatorState = TRUE
IndicatorState = TRUE AND IndicatorHealth = GOOD AND EventEnabled = ENABLED ?
No
Yes
Disable Thrusters
TouchdownMonitor = NOT-STARTED
EventEnabled = DISABLED

JPL Special Review Board Report, p115

What was the software problem?

- Didn’t “wear out” like valves or light bulbs
- Software performed exactly as designed
  - The *design* was flawed
- “Curse of Software”
  - Always does what it is told

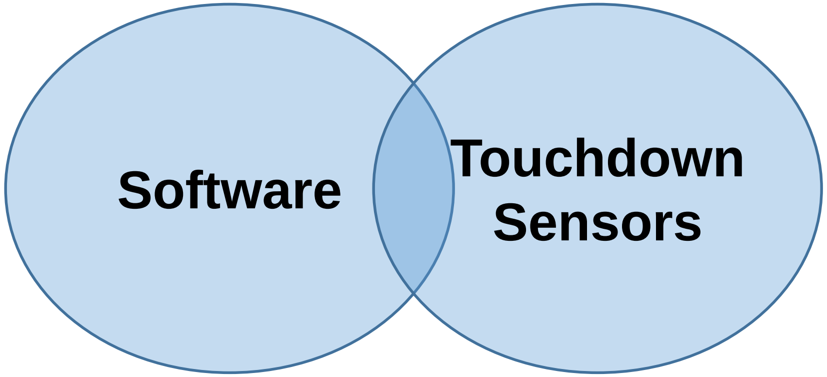

100 Hz
TouchdownMonitor = STARTED
No
Yes
LastTouchdownIndicator = CurrentTouchdownIndicator
Read Discretes from I/O Card
I/O Error AND EventEnabled = DISABLE ?
No
Yes
CurrentTouchdownIndicator = I/O Card Discrete (TRUE, FALSE)
CurrentTouchdownIndicator = FALSE
IndicatorState = FALSE
Yes
LastTouchdownIndicator = TRUE AND CurrentTouchdownIndicator = TRUE ?
No
IndicatorState = TRUE
IndicatorState = TRUE AND IndicatorHealth = GOOD AND EventEnabled = ENABLED ?
No
Yes
Disable Thrusters
TouchdownMonitor = NOT-STARTED
EventEnabled = DISABLED

Missing from MPL!

JPL Special Review Board Report, p115

Several Contributing Factors

- Touchdown sensor design
- Software implementation



Hard to see the problem by looking at any one part

Redundancy won’t help

Software Redundancy

- Space Shuttle had multiple redundant computers
- Backup Flight System (BFS) independent from Primary Avionics System Software (PASS)
  - Different software code
  - Different requirements
  - Different programmers
  - Different contractors
  - Different development environments
  - Different configuration management systems

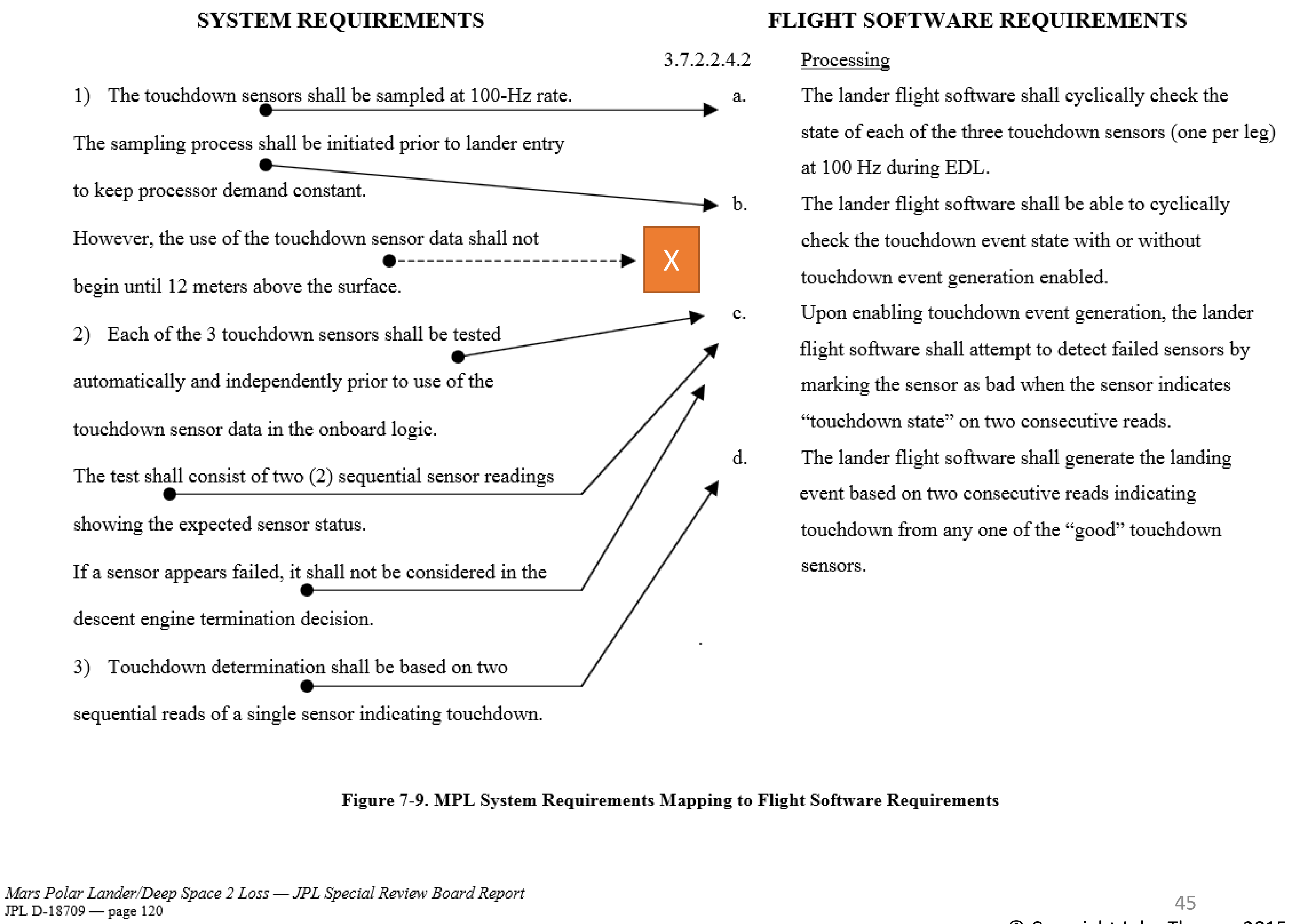
Software Redundancy

- STS-1 launch scrubbed at T-17 minutes
  - Backup computer could not synchronize with primary computers
  - Some computers began processing information earlier than it should have
  - Software was based on an incorrect assumption about scheduling

Redundancy can introduce new problems!

MPL Software

- Software engineers didn’t make a mistake
- All software requirements were met
- The requirements were incomplete!



SYSTEM REQUIREMENTS

1) The touchdown sensors shall be sampled at 100-Hz rate.

The sampling process shall be initiated prior to lander entry to keep processor demand constant.

However, the use of the touchdown sensor data shall not begin until 12 meters above the surface.

2) Each of the 3 touchdown sensors shall be tested automatically and independently prior to use of the touchdown sensor data in the onboard logic.

The test shall consist of two (2) sequential sensor readings showing the expected sensor status.

If a sensor appears failed, it shall not be considered in the descent engine termination decision.

3) Touchdown determination shall be based on two sequential reads of a single sensor indicating touchdown.

FLIGHT SOFTWARE REQUIREMENTS

3.7.2.2.4.2 Processing

a. The lander flight software shall cyclically check the state of each of the three touchdown sensors (one per leg) at 100 Hz during EDL.

b. The lander flight software shall be able to cyclically check the touchdown event state with or without touchdown event generation enabled.

c. Upon enabling touchdown event generation, the lander flight software shall attempt to detect failed sensors by marking the sensor as bad when the sensor indicates "touchdown state" on two consecutive reads.

d. The lander flight software shall generate the landing event based on two consecutive reads indicating touchdown from any one of the "good" touchdown sensors.

Figure 7-9. MPL System Requirements Mapping to Flight Software Requirements

It all comes back to humans!

- To understand why the software was wrong, we need to understand something about the people (and processes) that created it.

- Not necessarily true for hardware failures (e.g. pipes rusting, light bulbs burning out, brake pads wearing out, etc.)

Quote

- “The hardest single part of building a software system is deciding precisely what to build.”

  -- Fred Brooks, *The Mythical Man-Month*

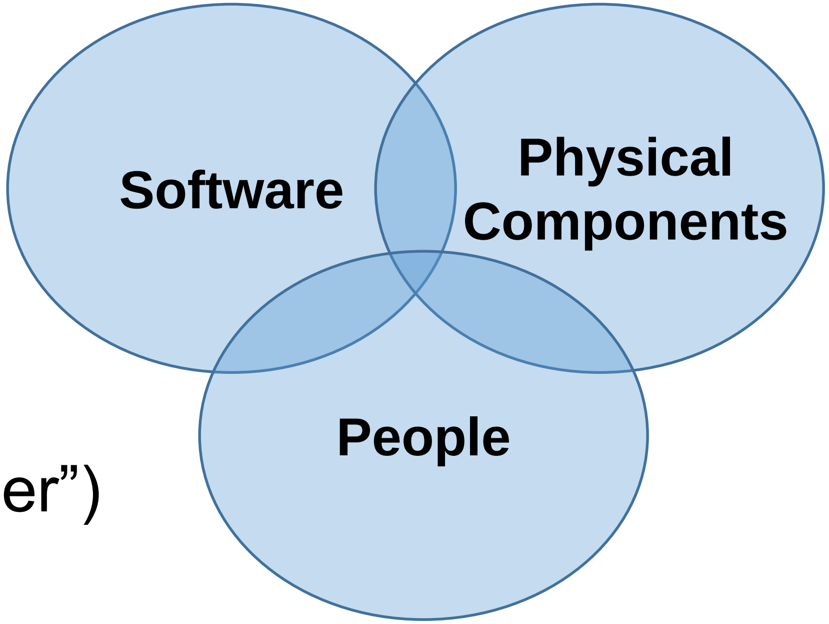
Why didn’t software testing uncover the problem?

- Software tests were based on software requirements
- Most tests were not done in vacuum/thermal chamber
- Some tests had wiring problems
- Etc.

Systems View

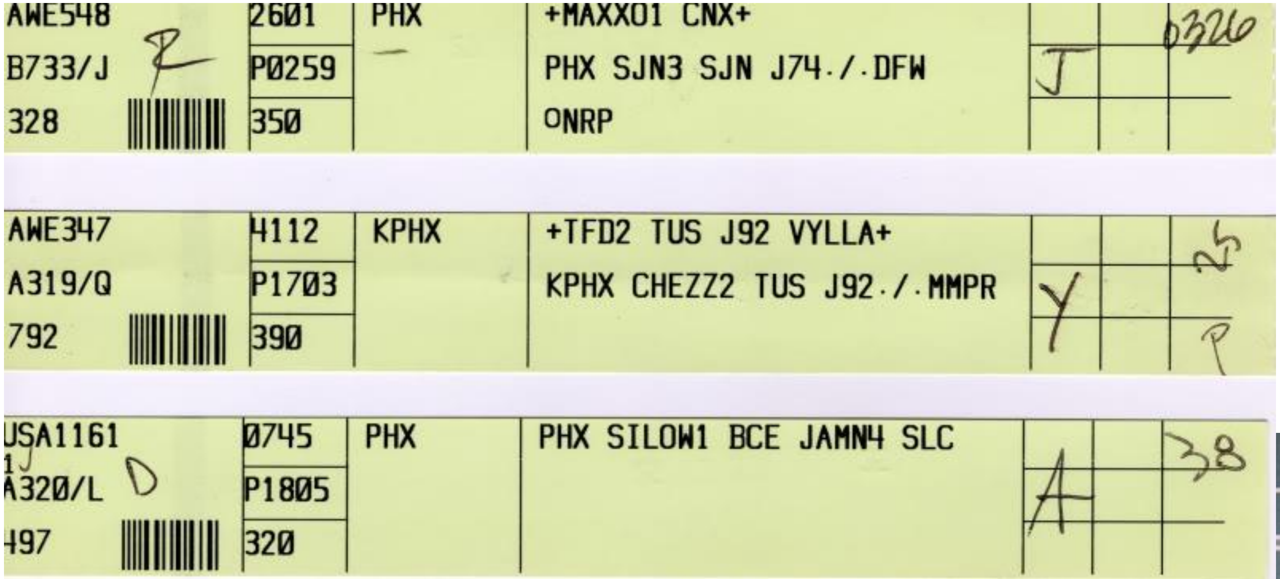
Many different factors were involved:

- Touchdown sensors
- Software implementation
- Software requirements
- Testing
- Engineering reviews
- Communication
- Time pressure
- Culture (“Faster, Better, Cheaper”)
- Etc.



Hard to see the problem by looking at any one part

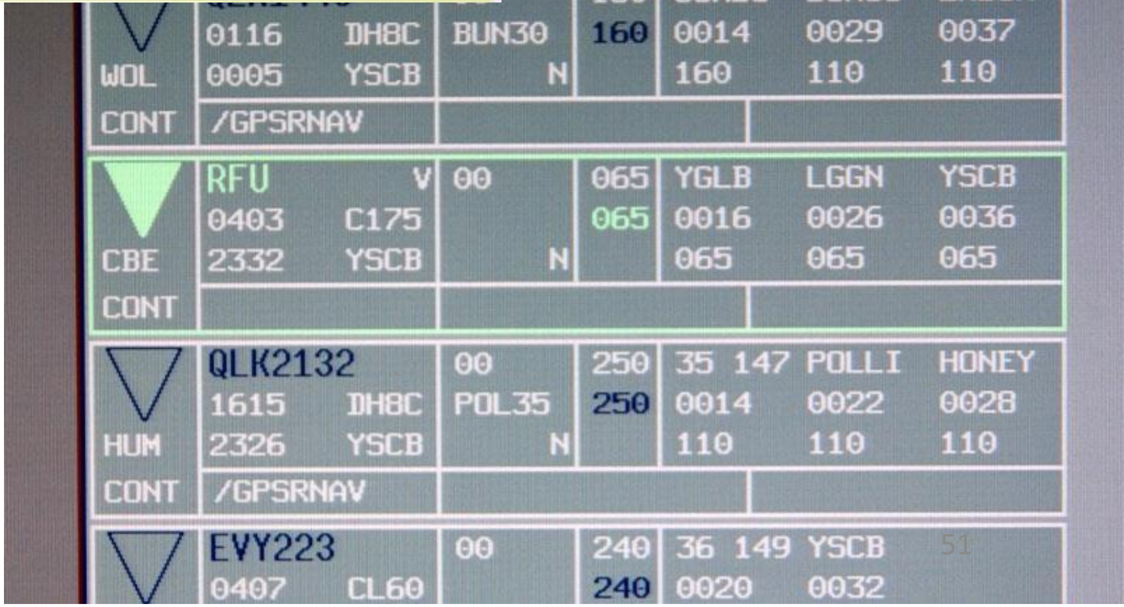
Air Traffic Control Flight Strips



```
AWE548        2601   PHX    +MAXX01 CNX+                          0326
B733/J   R    P0259  —      PHX SJN3 SJN J74./.DFW           J
328           350           ONRP

AWE347        4112   KPHX   +TFD2 TUS J92 VYLLA+                  25
A319/Q        P1703         KPHX CHEZZ2 TUS J92./.MMPR       Y
792           390                                                 P

USA1161       0745   PHX    PHX SILOW1 BCE JAMN4 SLC              38
1J
A320/L   D    P1805                                          A
497           320
```



```
                  N        100   100   100

      QLK...           160  CORDO BUNGO ENDOR
      0116   DH8C BUN30 160  0014  0029  0037
WOL   0005   YSCB     N      160   110   110
CONT  /GPSRNAV

      RFU       V 00    065  YGLB  LGGN  YSCB
      0403   C175       065  0016  0026  0036
CBE   2332   YSCB     N      065   065   065
CONT

      QLK2132     00    250  35 147 POLLI HONEY
      1615   DH8C POL35 250  0014  0022  0028
HUM   2326   YSCB     N      110   110   110
CONT  /GPSRNAV

      EVY223      00    240  36 149 YSCB
      0407   CL60       240  0020  0032
```

Implications for analysis

- Safety is not a property of the software / human
- Outward-looking analysis
  - Must emphasize interactions between software and it’s environment
  - Must emphasize interactions between humans and their environment
  - Get the right requirements first

- Then use verification to ensure requirements are met
  - Simulation, testing, analysis, etc.

Today’s Agenda

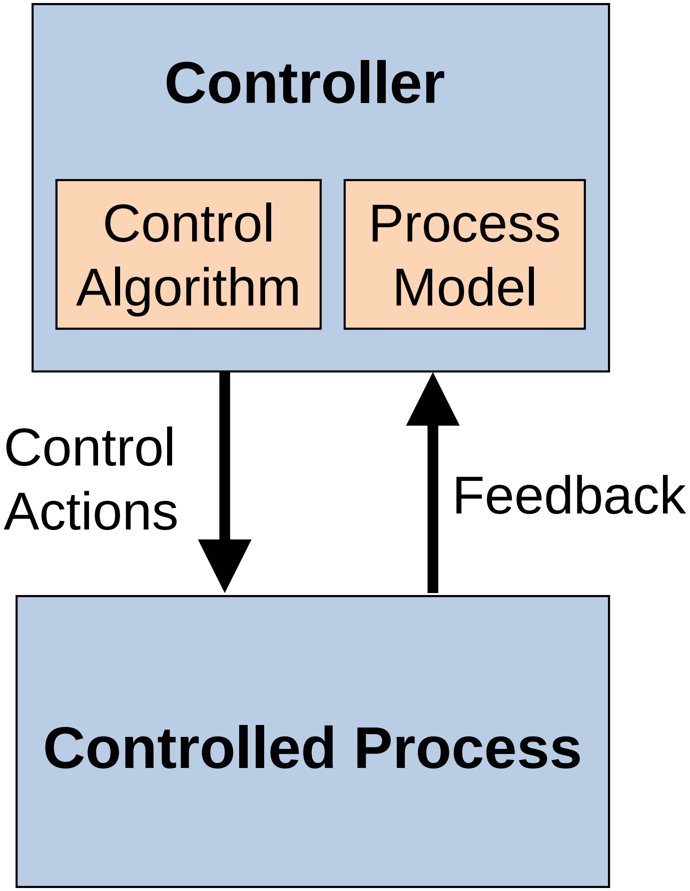
- Intro to software issues
- Intro to human issues
- STAMP accident model
- System Theoretic Hazard Analysis (STPA)
  - Intro
  - Examples
  - Exercise

Systems approach to safety engineering (STAMP)

STAMP Model

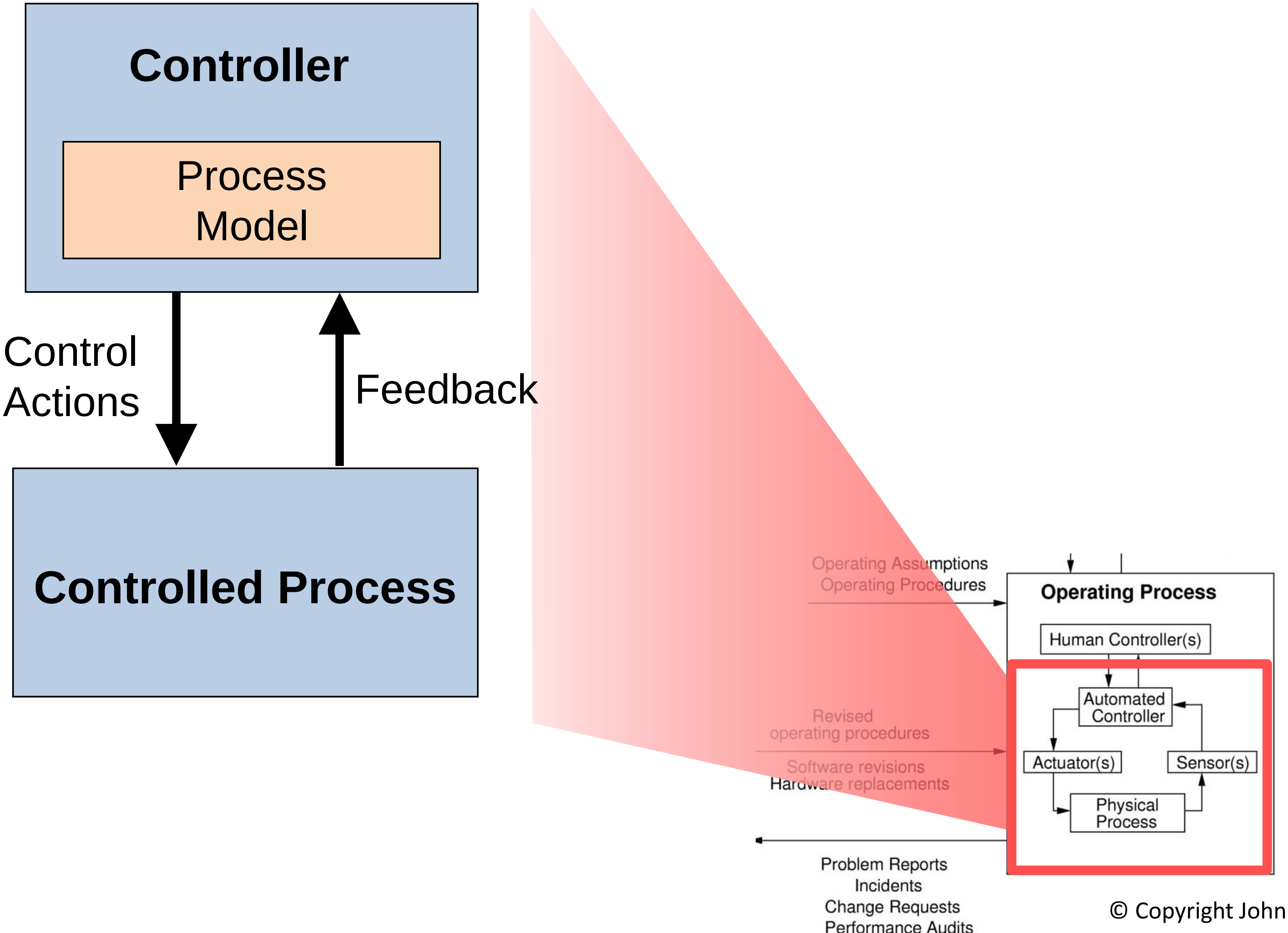
- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not just a failure problem
- Prevent accidents by enforcing constraints on component behavior and **interactions**
- Captures more causes of accidents:
  - Component failure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

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

STAMP



Controller

Process Model

Control Actions

Feedback

Controlled Process

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

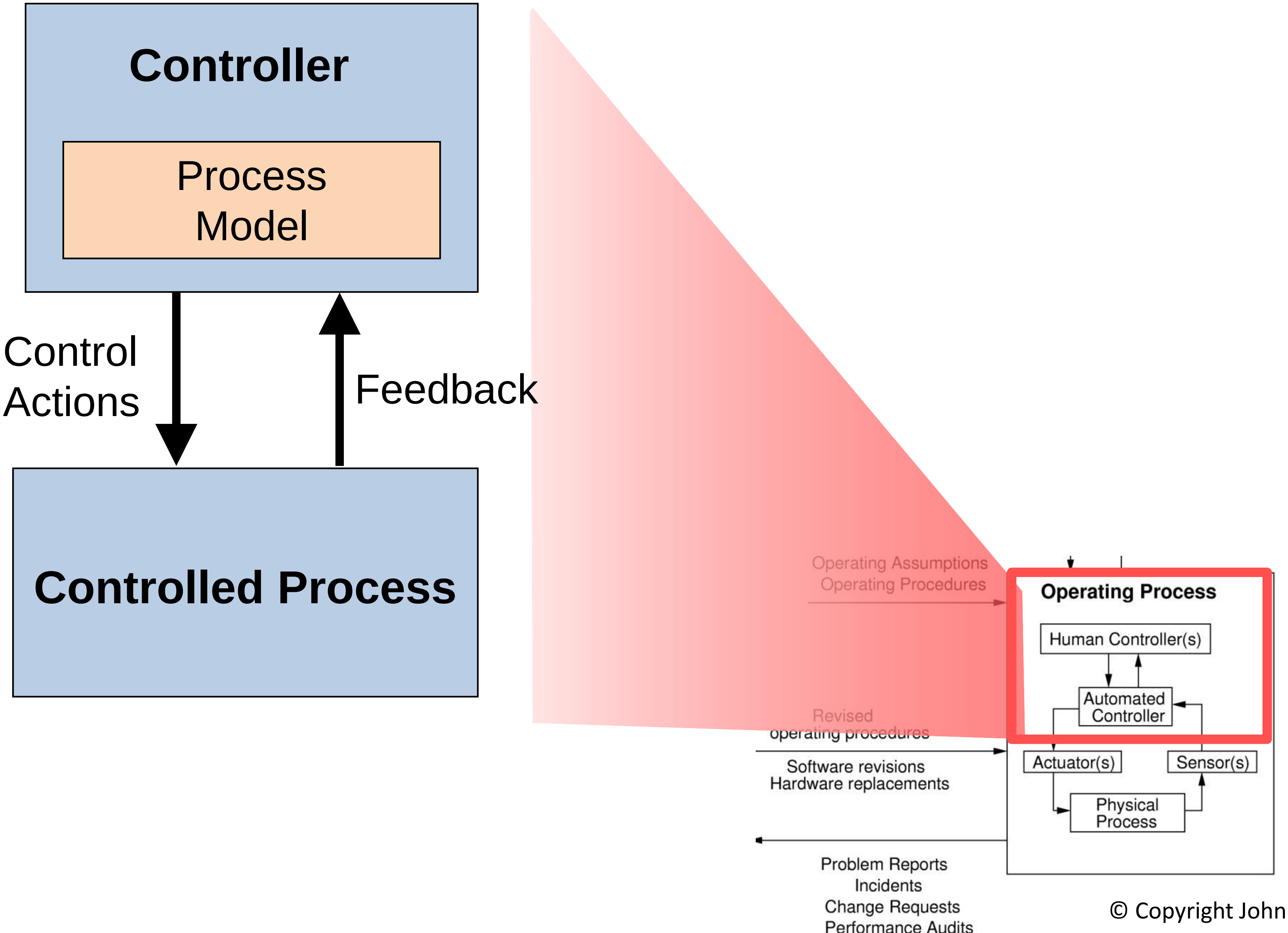
Physical Process

Revised
operating procedures

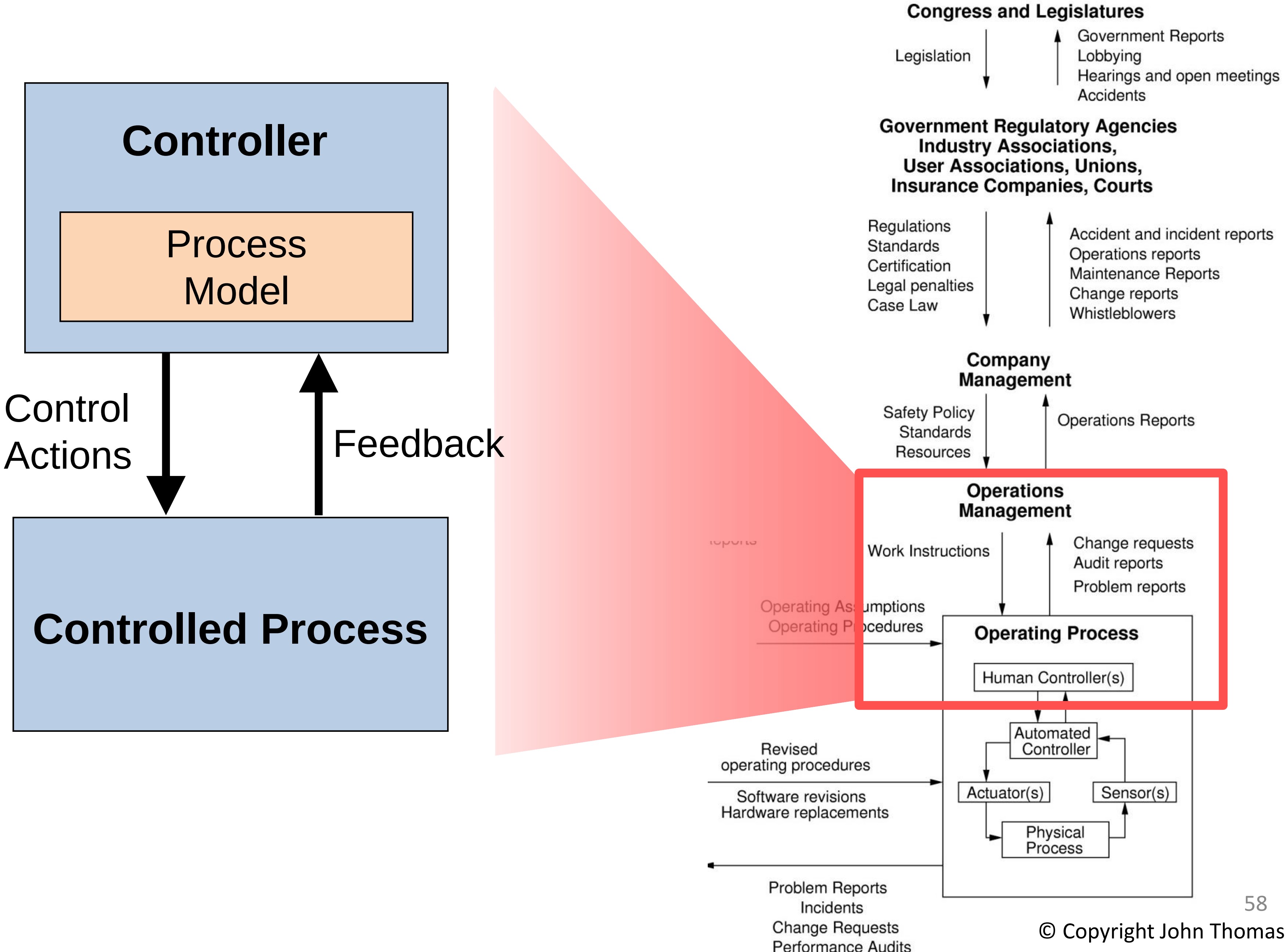
Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

STAMP


Controller
Process Model
Control Actions
Feedback
Controlled Process
Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated Controller
Revised operating procedures
Software revisions
Hardware replacements
Actuator(s)
Sensor(s)
Physical Process
Problem Reports
Incidents
Change Requests
Performance Audits

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

reports

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

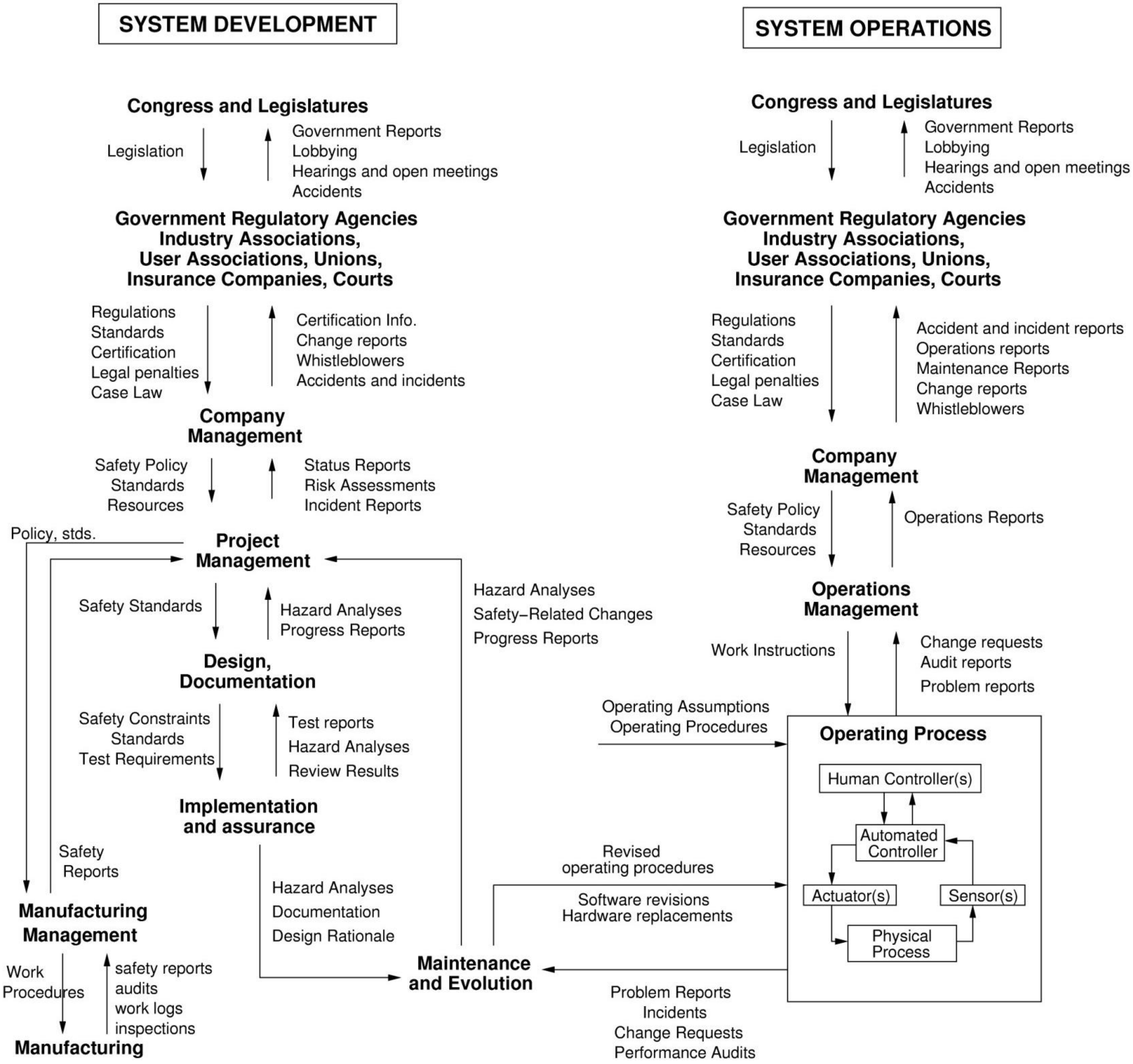
Physical Process

Revised operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

Example Safety Control Structure



SYSTEM DEVELOPMENT

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

Certification Info.
Change reports
Whistleblowers
Accidents and incidents

Company Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, stds.

Project Management

Safety Standards

Hazard Analyses
Progress Reports

Hazard Analyses
Safety–Related Changes
Progress Reports

Design, Documentation

Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation and assurance

Safety Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing Management

Work Procedures

safety reports
audits
work logs
inspections

Manufacturing

Maintenance and Evolution

SYSTEM OPERATIONS

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

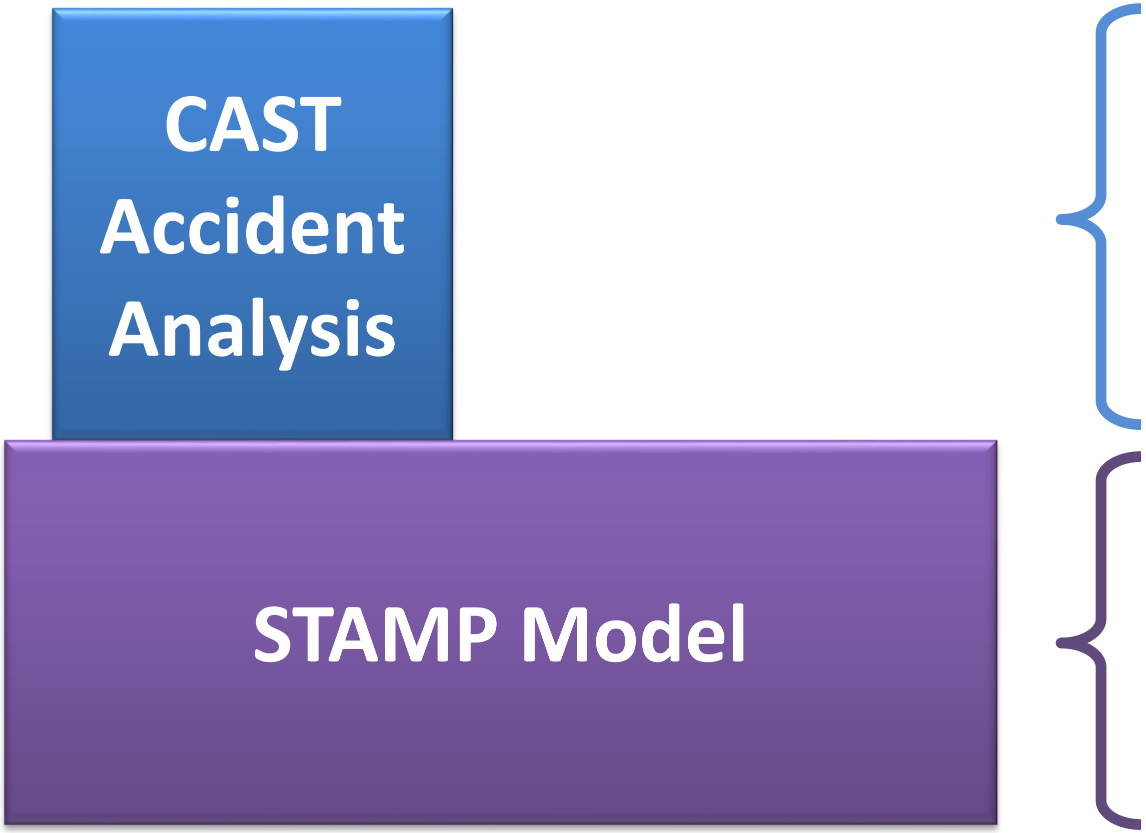
Problem Reports
Incidents
Change Requests
Performance Audits

STAMP and STPA

STAMP Model

Accidents are caused by inadequate control

STAMP and STPA



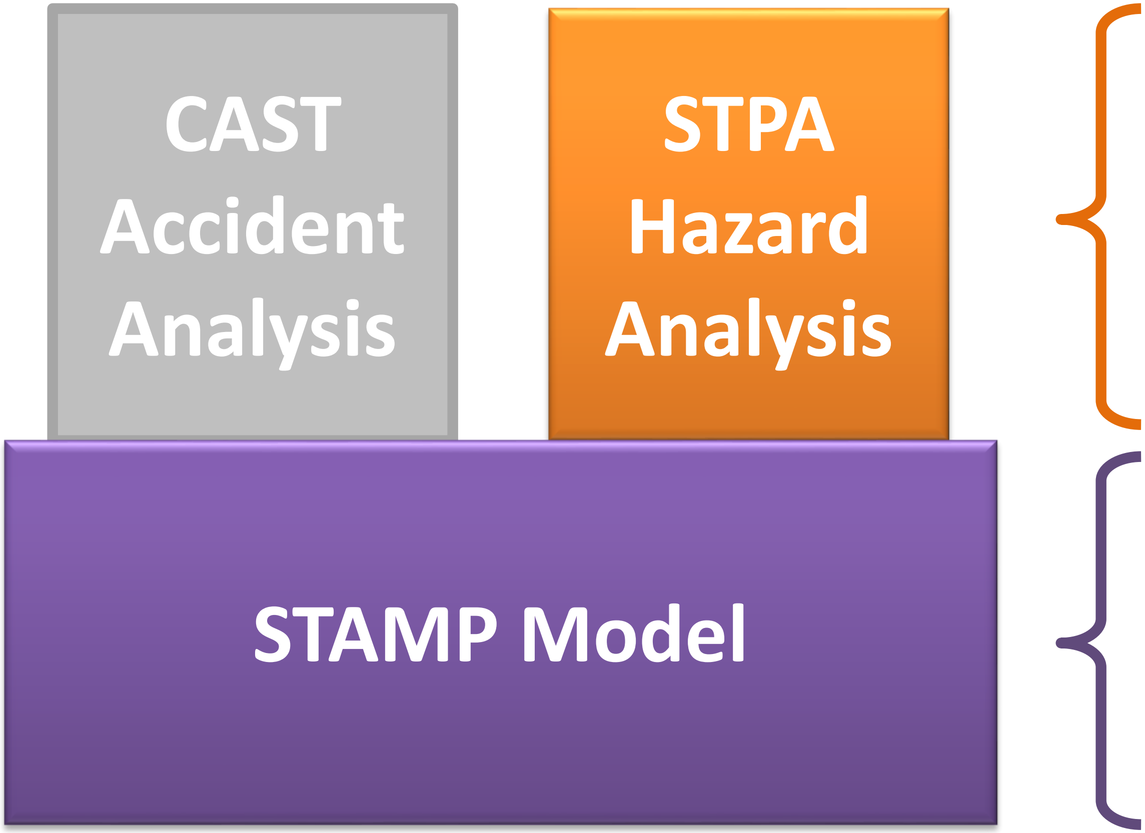
CAST Accident Analysis

STAMP Model

How do we find inadequate control that caused the accident?

Accidents are caused by inadequate control

STAMP and STPA



CAST
Accident
Analysis

STPA
Hazard
Analysis

STAMP Model

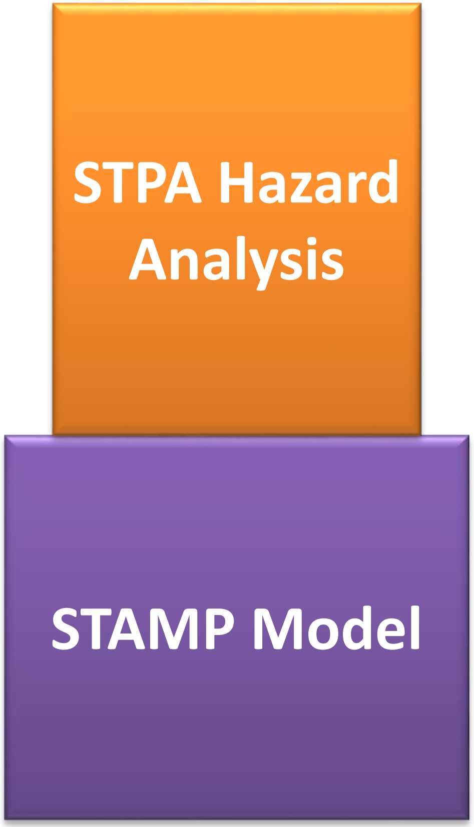
How do we find inadequate control in a design?

Accidents are caused by inadequate control

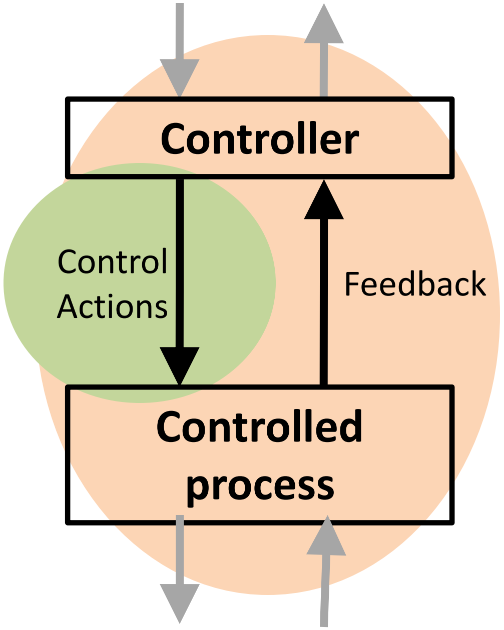
Today’s Agenda

- Intro to software issues
- Intro to human issues
- STAMP accident model
- System Theoretic Hazard Analysis (STPA)
  - Intro
  - Examples
  - Exercise

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



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 from Engineering a Safer World

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!

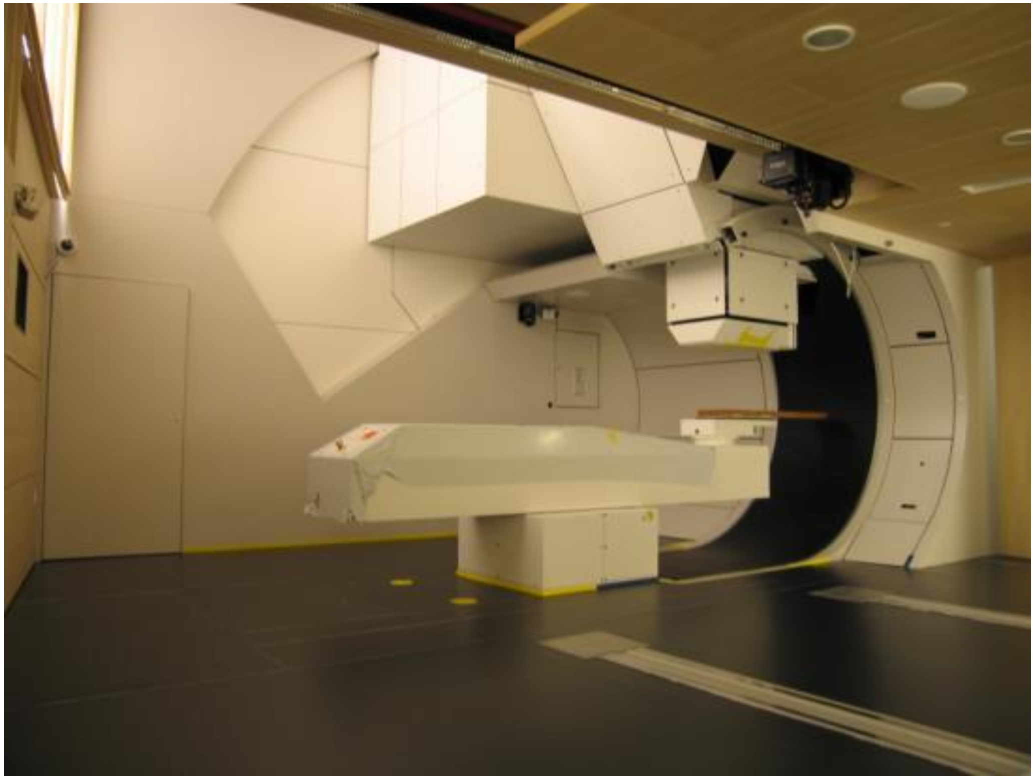
People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

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

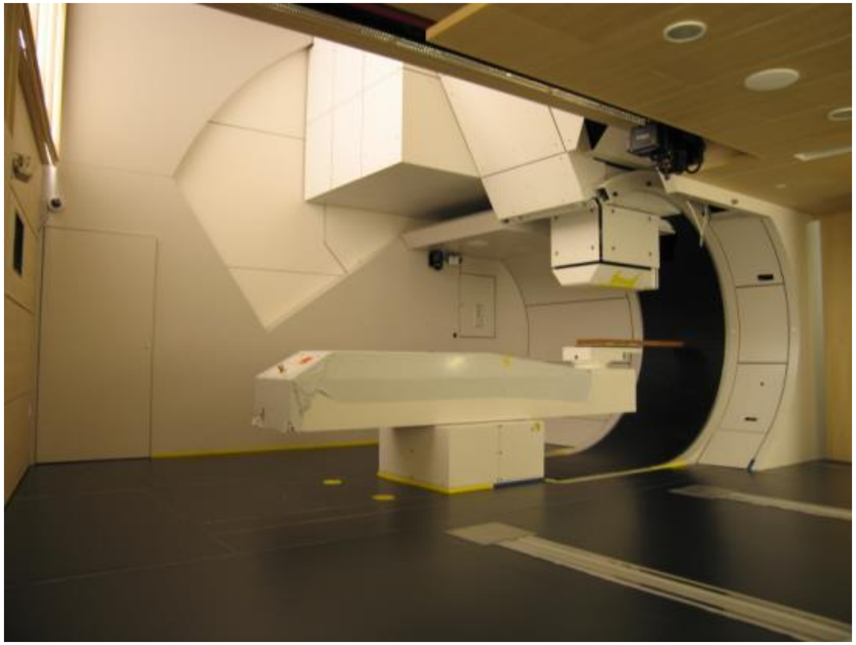
Proton Radiation Therapy System
Paul Scherrer Institute, Switzerland



- 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

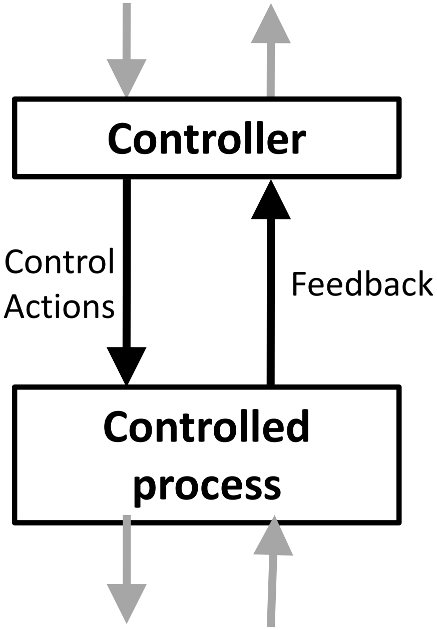
Proton Therapy Machine (Antoine)

- 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)

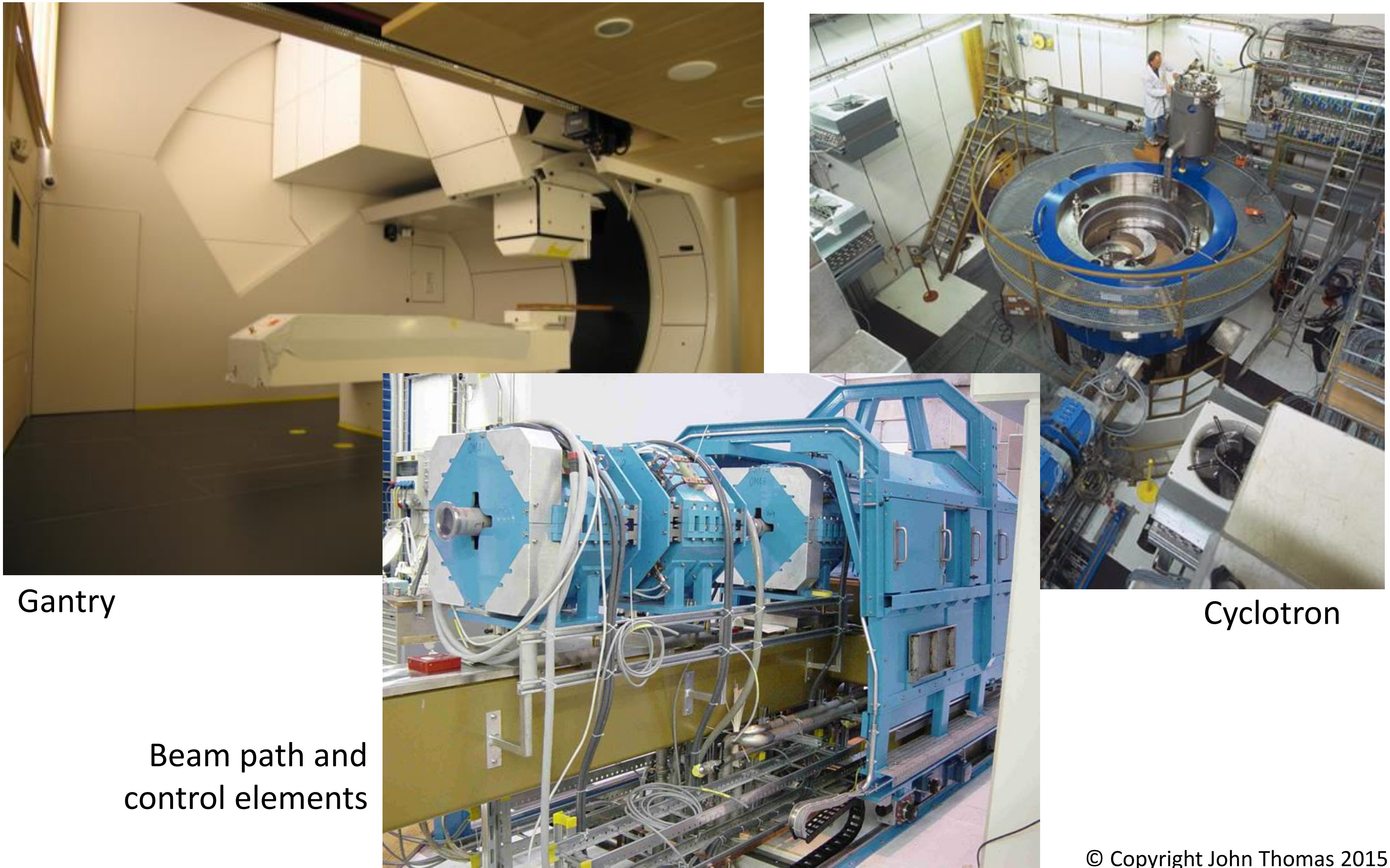
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

Control Structure Examples

Proton Therapy Machine
High-level Control Structure

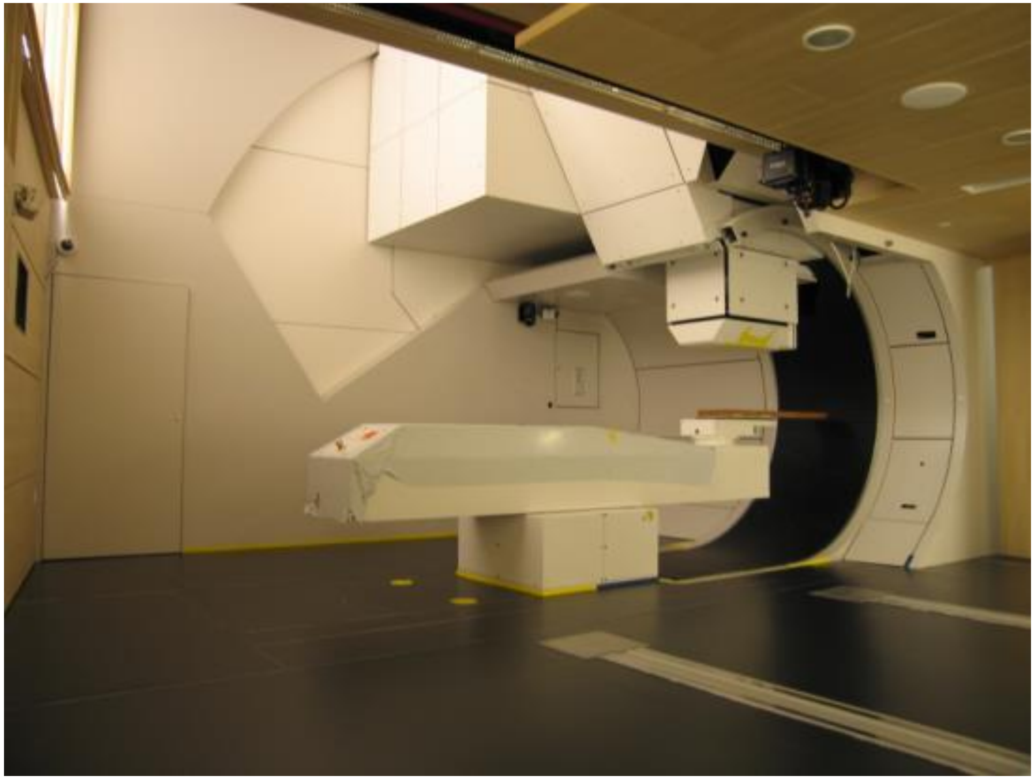


Gantry

Cyclotron

Beam path and
control elements

Proton Therapy Machine
High-level Control Structure



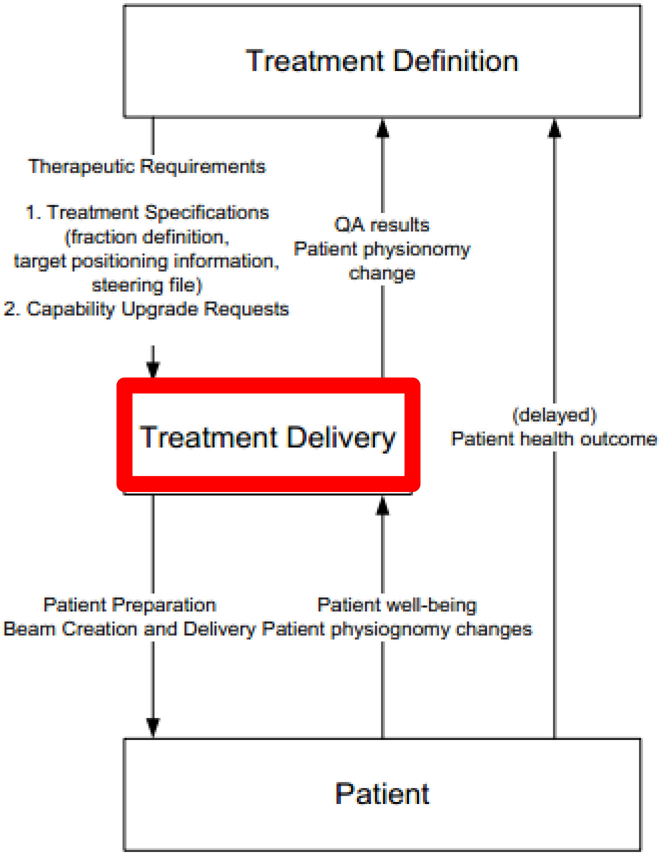


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Antoine PhD Thesis, 2012

Proton Therapy Machine Control Structure

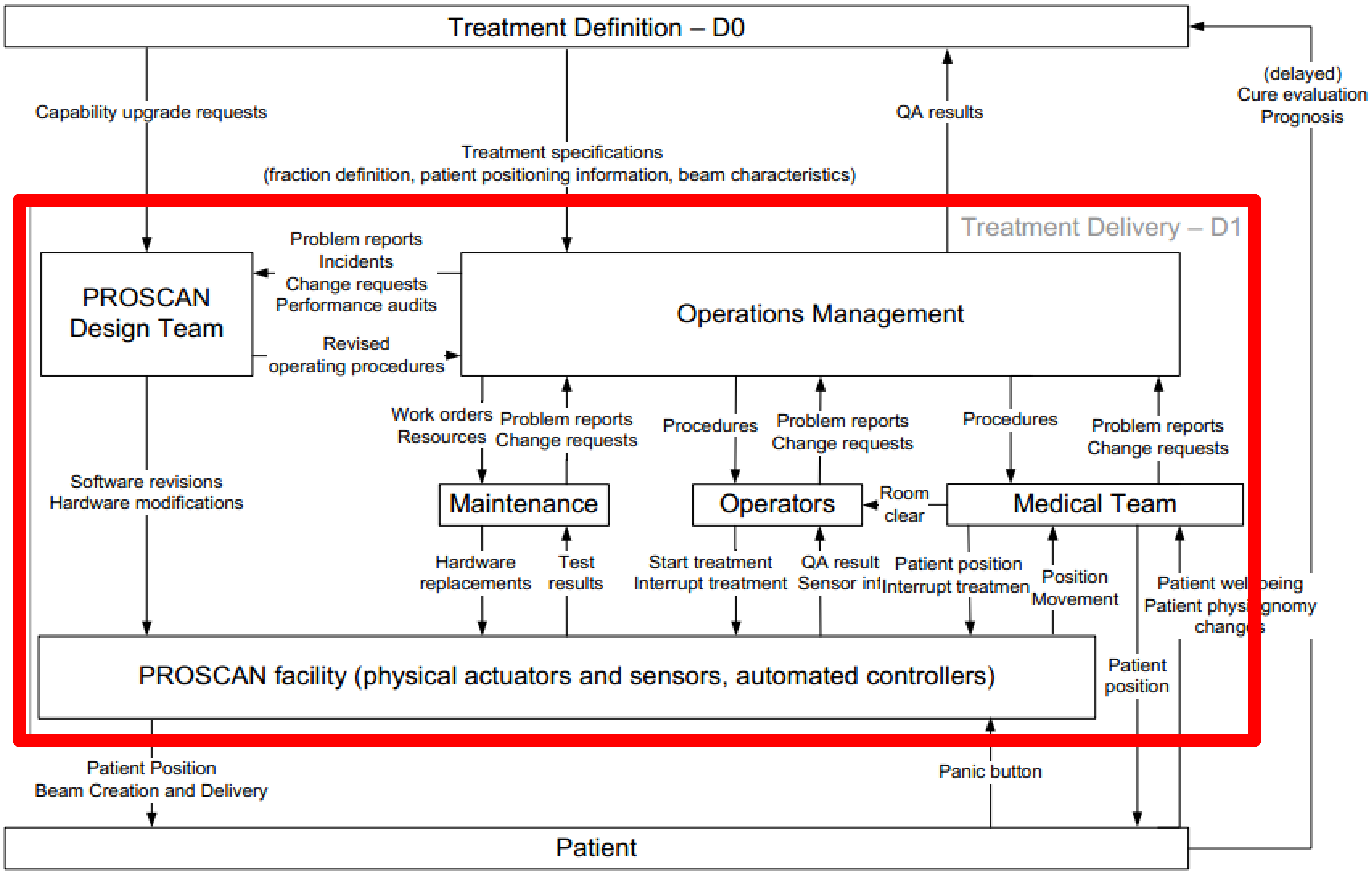
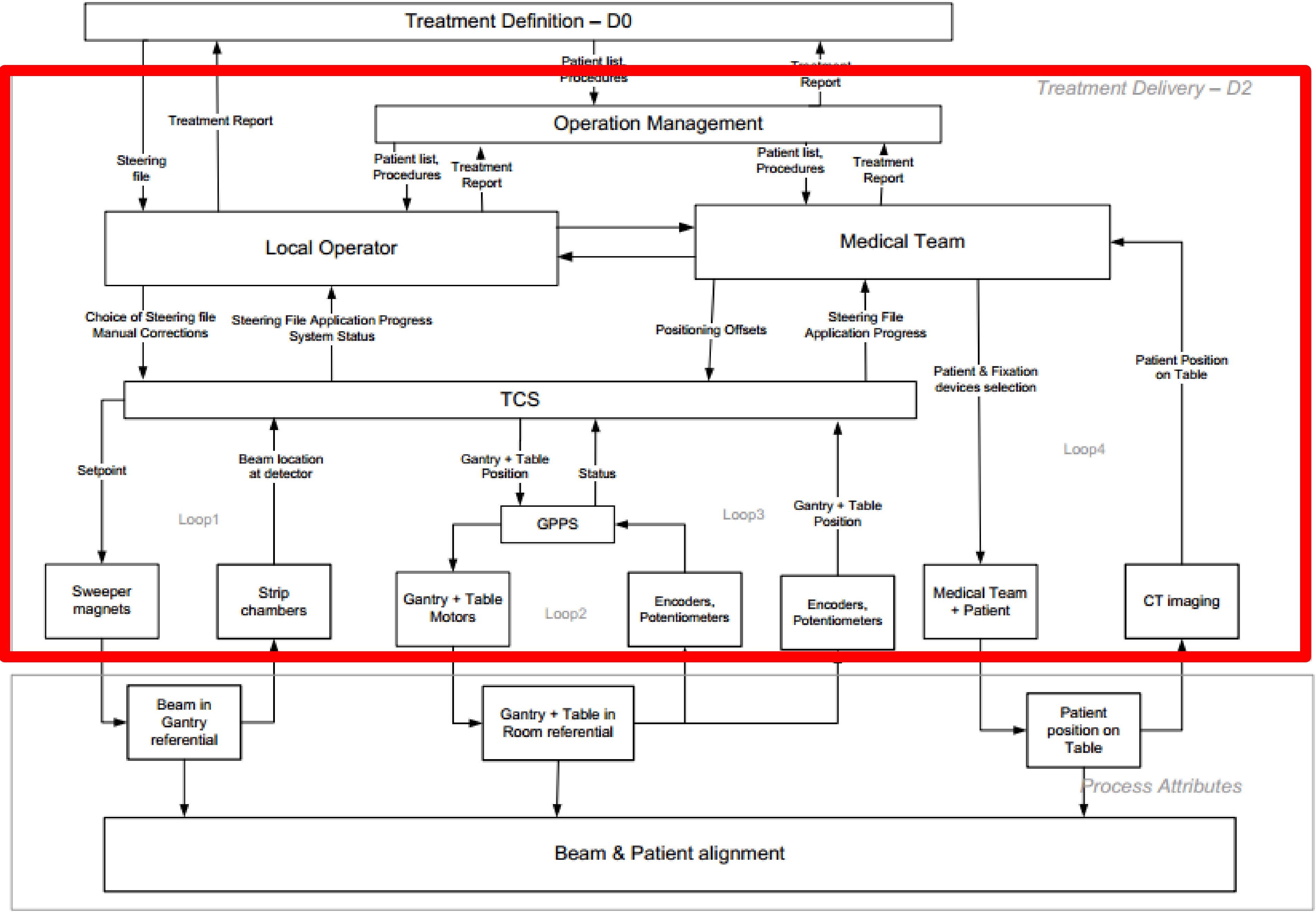


Figure 13 - Zooming into the Treatment Delivery group (D1)

Proton Therapy Machine Detailed Control Structure



Adaptive Cruise Control

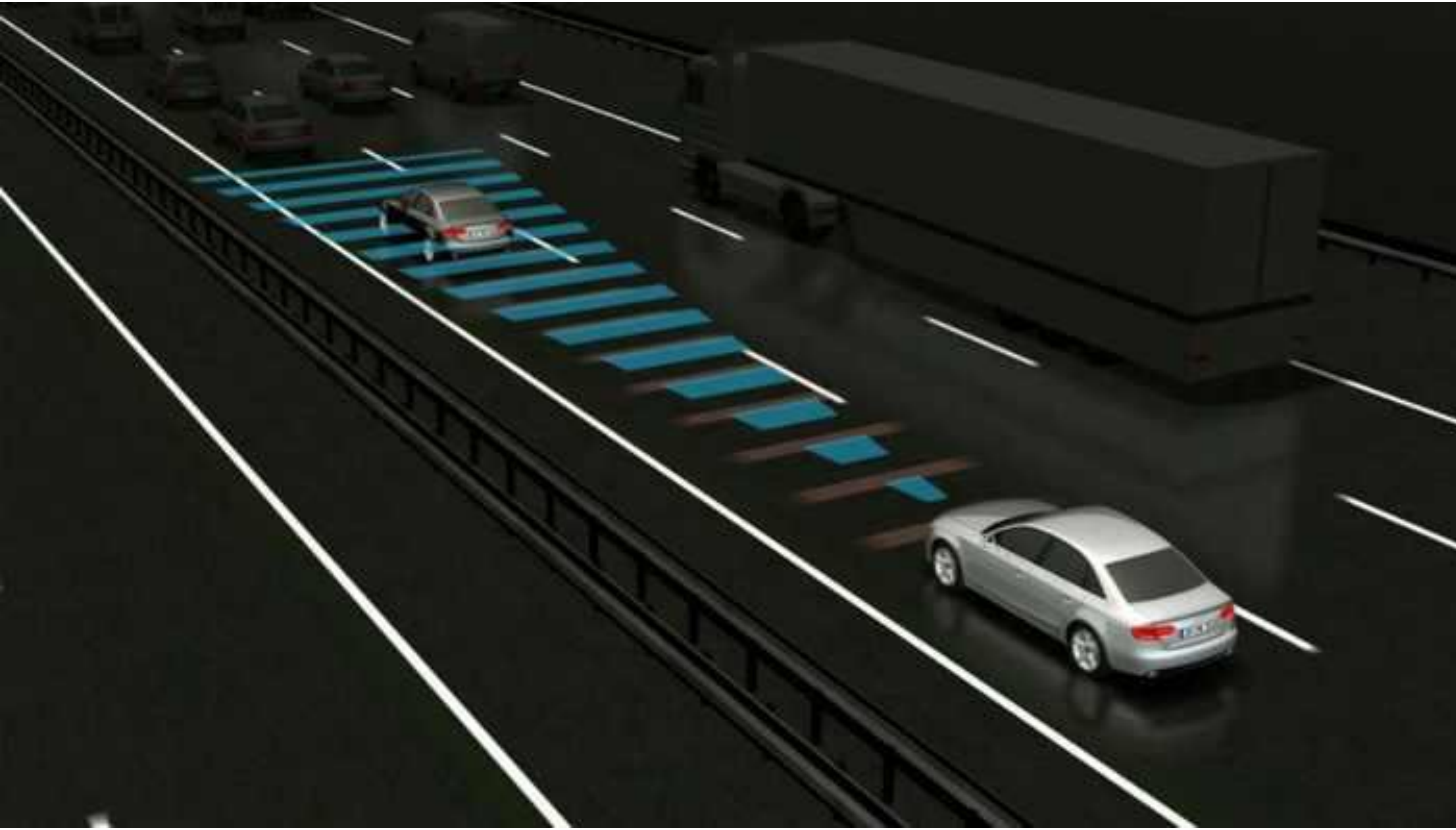
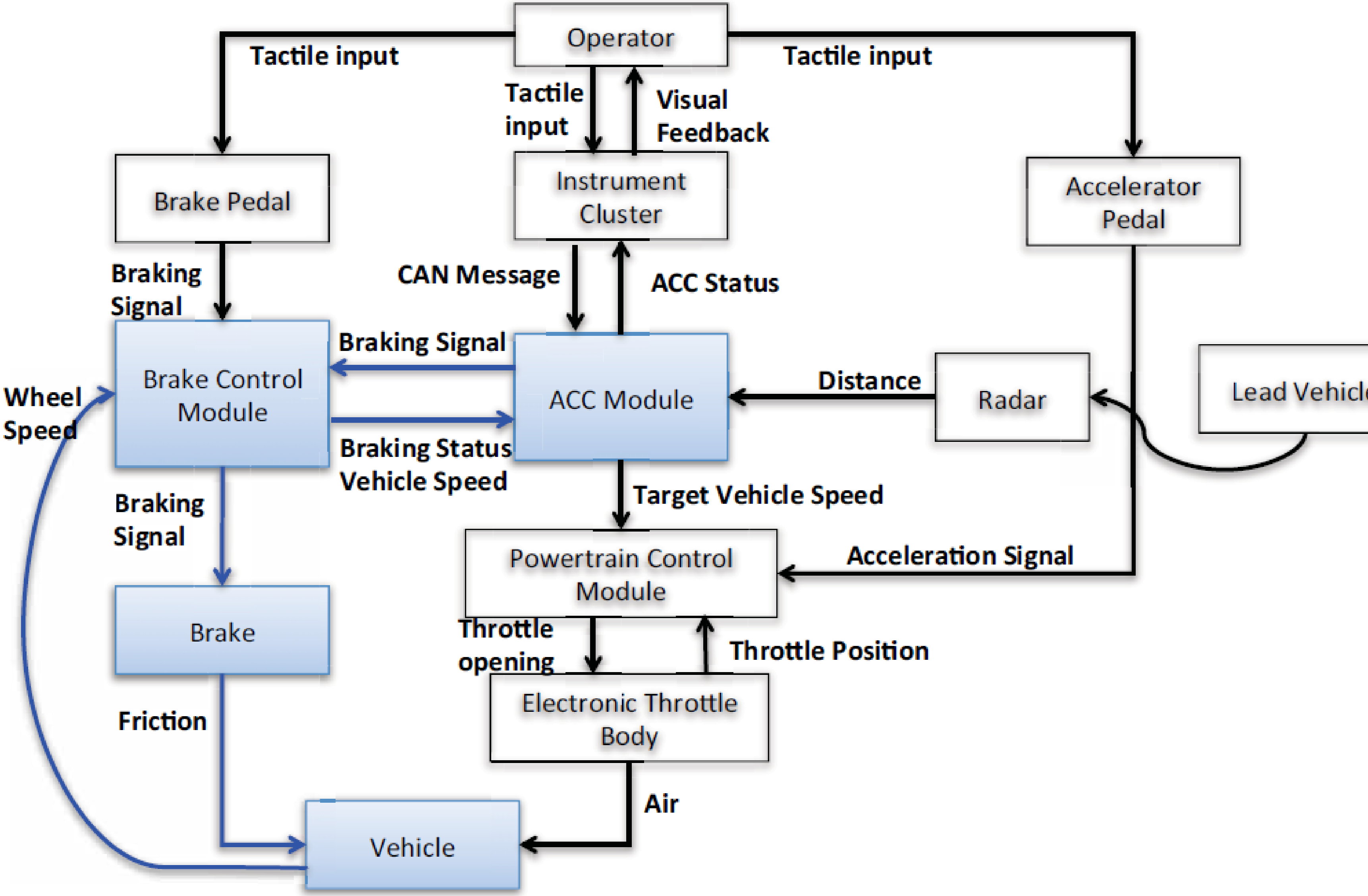
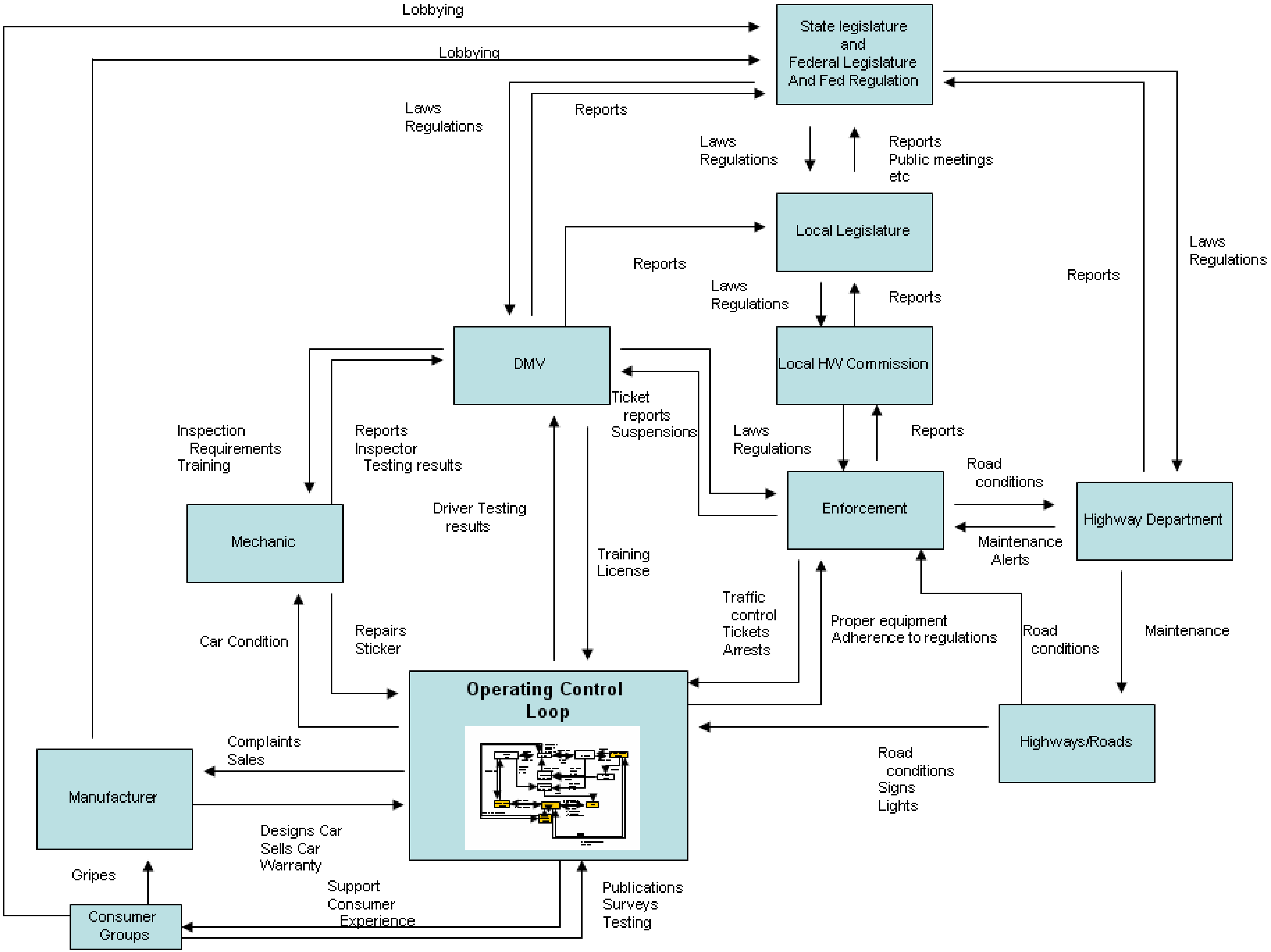


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

Example: ACC – BCM Control Loop



Qi Hommes


Lobbying
Lobbying
State legislature and Federal Legislature And Fed Regulation
Laws Regulations
Reports
Laws Regulations
Reports Public meetings etc
Laws Regulations
Reports
Local Legislature
Laws Regulations
Reports
Local HW Commission
Reports
DMV
Ticket reports Suspensions
Laws Regulations
Reports
Inspection Requirements Training
Reports Inspector Testing results
Road conditions
Enforcement
Highway Department
Maintenance Alerts
Driver Testing results
Mechanic
Training License
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

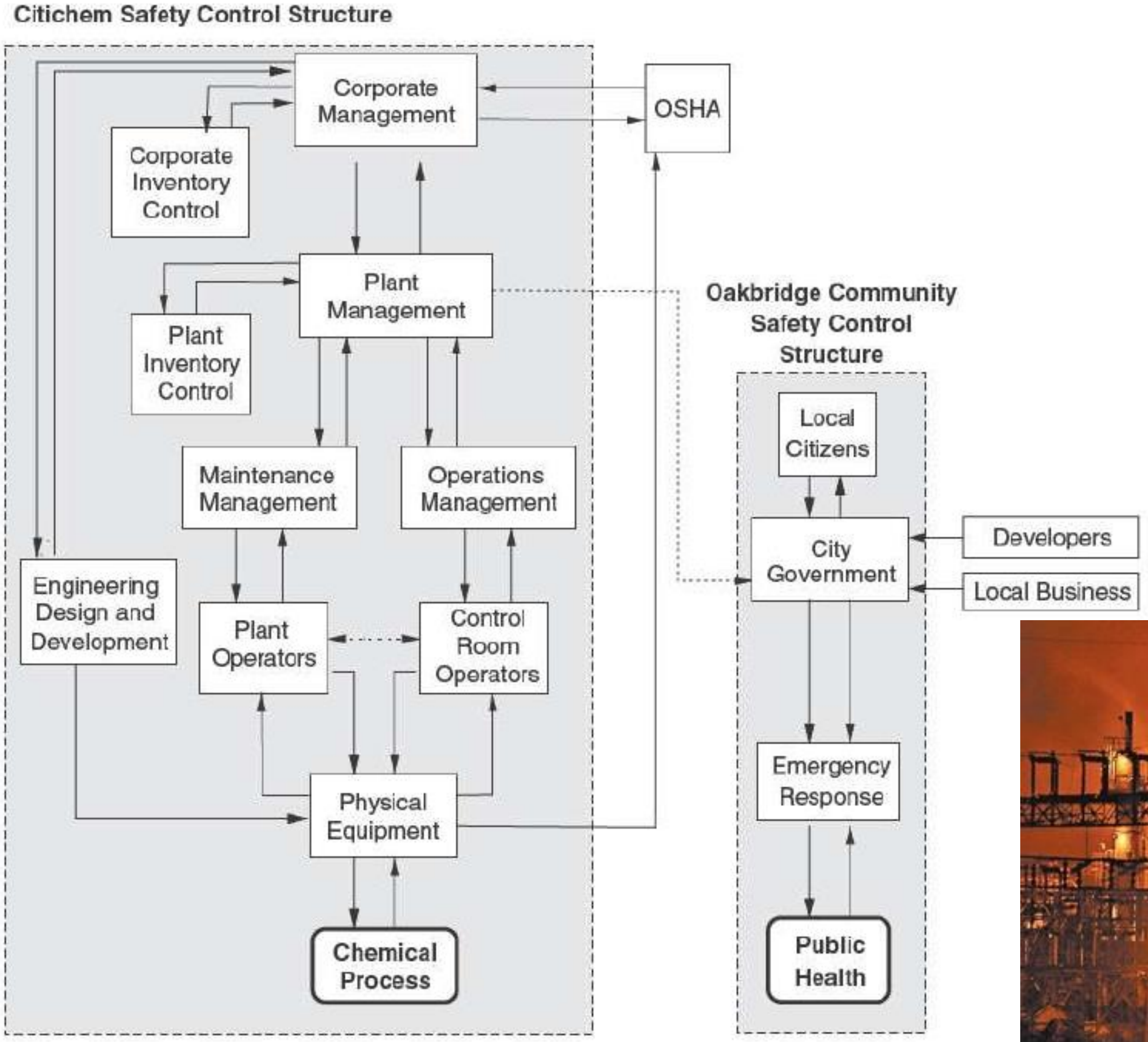


Image from:
http://www.cbgnetwork.org/2608.html

ESW p354

U.S. pharmaceutical safety control structure

Congress

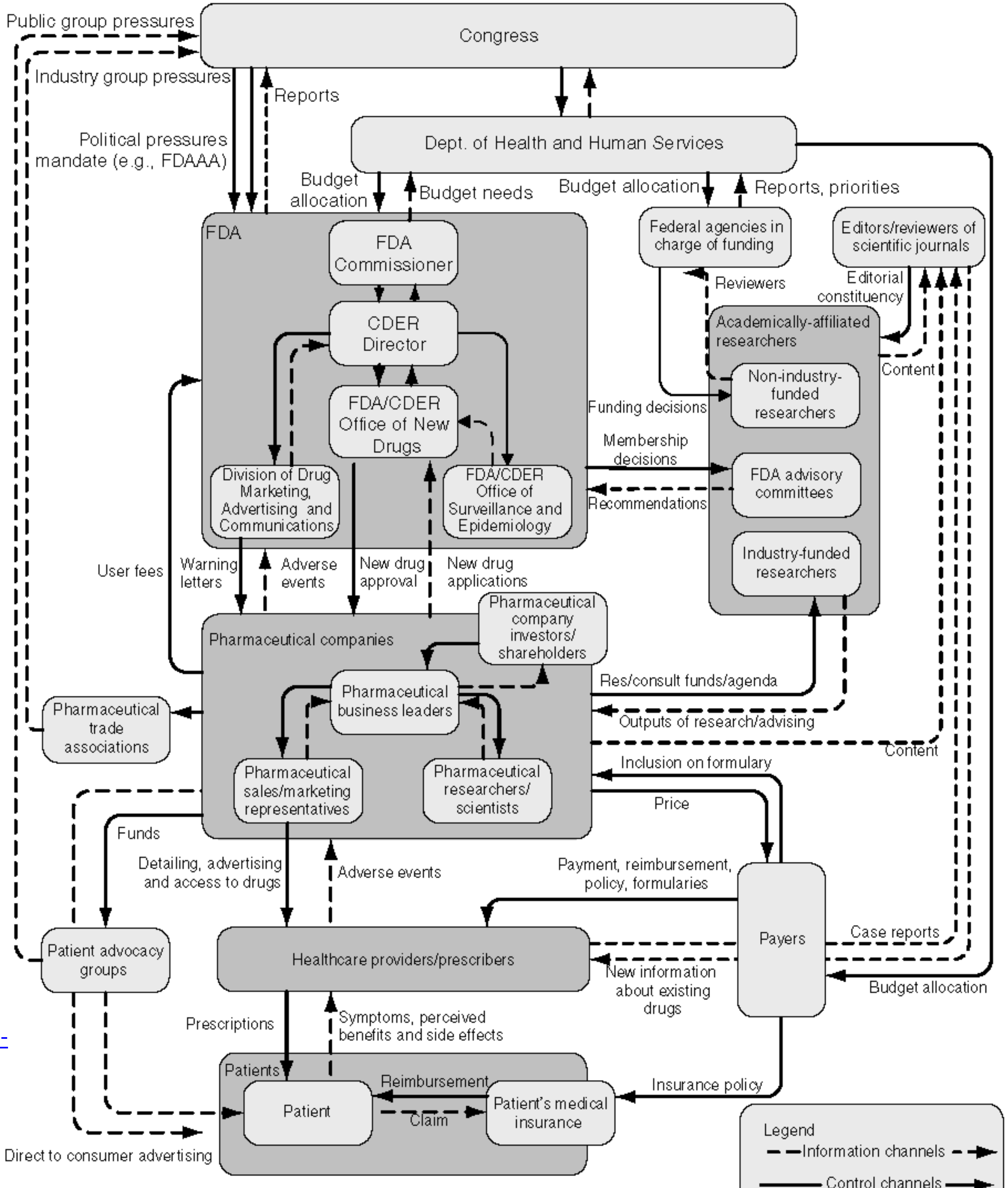
FDA

Pharmaceutical Companies

Doctors

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

Patients

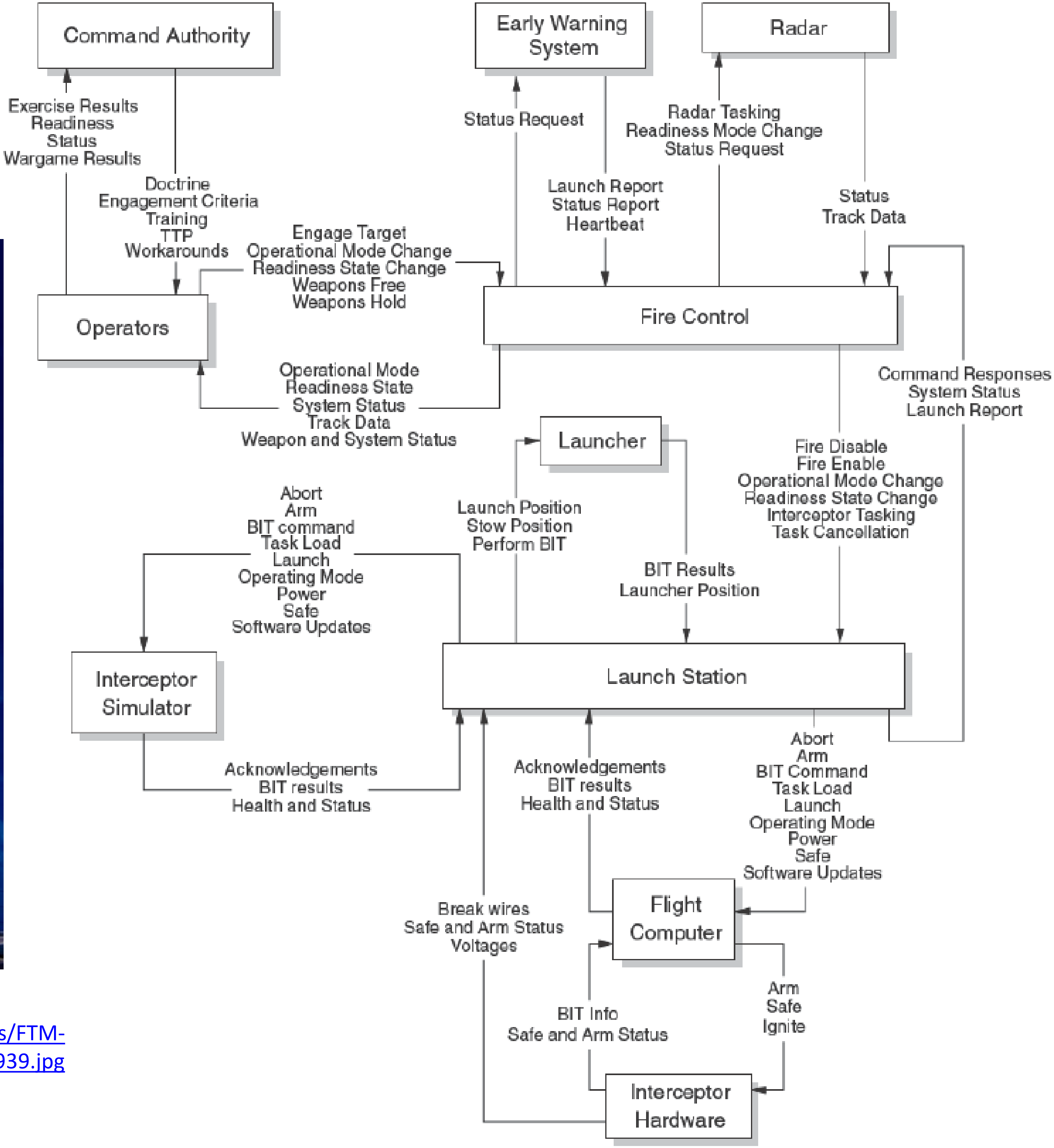


Public group pressures
Congress
Industry group pressures
Reports
Political pressures mandate (e.g., FDAAA)
Dept. of Health and Human Services
Budget allocation
Budget needs
Budget allocation
Reports, priorities
FDA
FDA Commissioner
CDER Director
FDA/CDER Office of New Drugs
Division of Drug Marketing, 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
Content
Funding decisions
Non-industry-funded researchers
Membership decisions
FDA advisory committees
Recommendations
Industry-funded researchers
User fees
Warning letters
Adverse events
New drug approval
New drug applications
Pharmaceutical companies
Pharmaceutical company investors/shareholders
Pharmaceutical business leaders
Res/consult funds/agenda
Pharmaceutical trade associations
Outputs of research/advising
Content
Pharmaceutical sales/marketing representatives
Pharmaceutical researchers/scientists
Inclusion on formulary
Price
Funds
Detailing, advertising and access to drugs
Adverse events
Payment, reimbursement, policy, formularies
Patient advocacy groups
Healthcare providers/prescribers
Payers
Case reports
New information about existing drugs
Budget allocation
Prescriptions
Symptoms, perceived benefits and side effects
Patients
Reimbursement
Patient
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



Command Authority

Early Warning System

Radar

Exercise Results
Readiness
Status
Wargame Results

Doctrine
Engagement Criteria
Training
TTP
Workarounds

Status Request

Launch Report
Status Report
Heartbeat

Radar Tasking
Readiness Mode Change
Status Request

Status
Track Data

Engage Target
Operational Mode Change
Readiness State Change
Weapons Free
Weapons Hold

Operators

Fire Control

Operational Mode
Readiness State
System Status
Track Data
Weapon and System Status

Command Responses
System Status
Launch Report

Launcher

Launch Position
Stow Position
Perform BIT

BIT Results
Launcher Position

Fire Disable
Fire Enable
Operational Mode Change
Readiness State Change
Interceptor Tasking
Task Cancellation

Abort
Arm
BIT command
Task Load
Launch
Operating Mode
Power
Safe
Software Updates

Interceptor Simulator

Launch Station

Acknowledgements
BIT results
Health and Status

Acknowledgements
BIT results
Health and Status

Abort
Arm
BIT Command
Task Load
Launch
Operating Mode
Power
Safe
Software Updates

Break wires
Safe and Arm Status
Voltages

Flight Computer

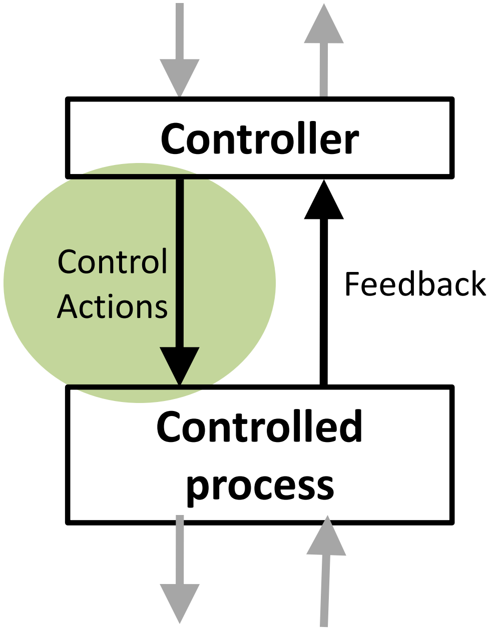
BIT Info
Safe and Arm Status

Arm
Safe
Ignite

Interceptor Hardware

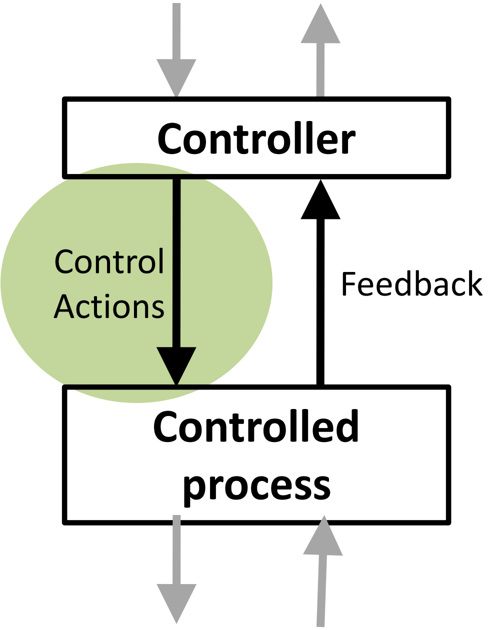
STPA
(System-Theoretic Process Analysis)

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



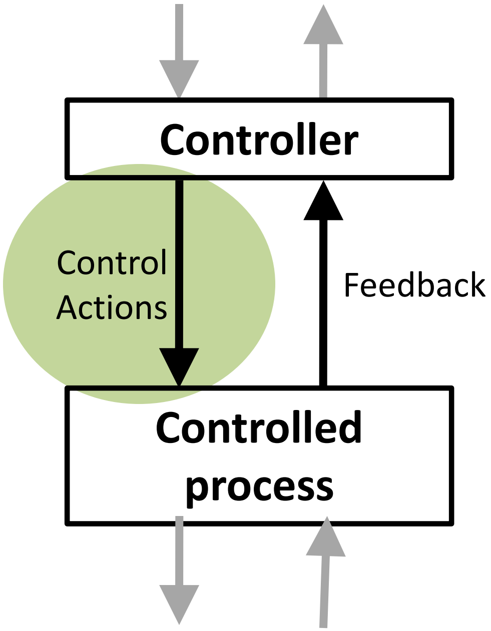
(Leveson, 2012)

STPA Step 1: Unsafe Control Actions (UCA)



Control Action (A)				

STPA Step 1: Unsafe Control Actions (UCA)

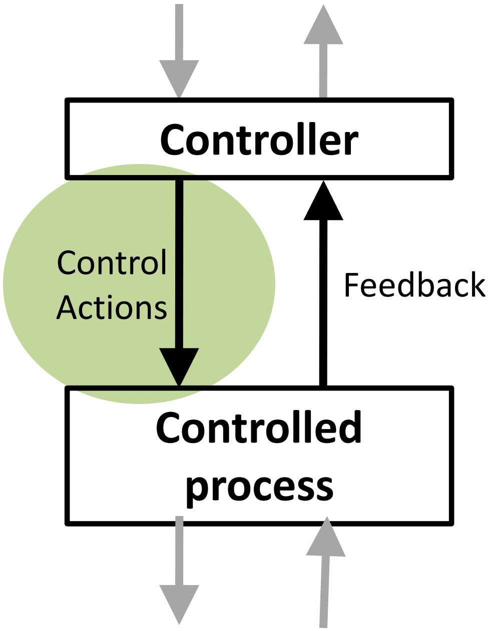


4 ways unsafe control may occur:

- 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)

Control Action (A)				

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)				

Proton Therapy Machine Control Structure

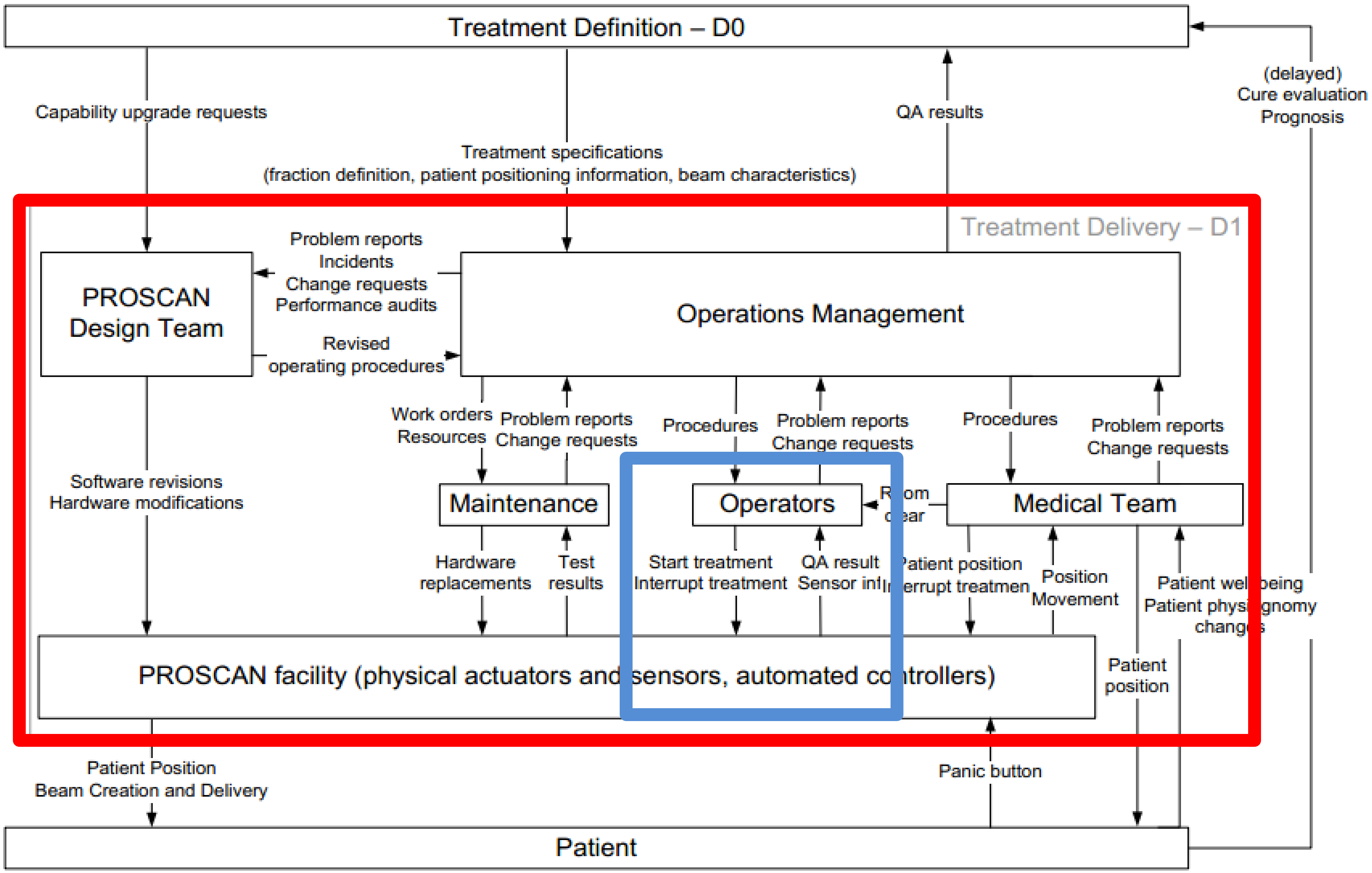
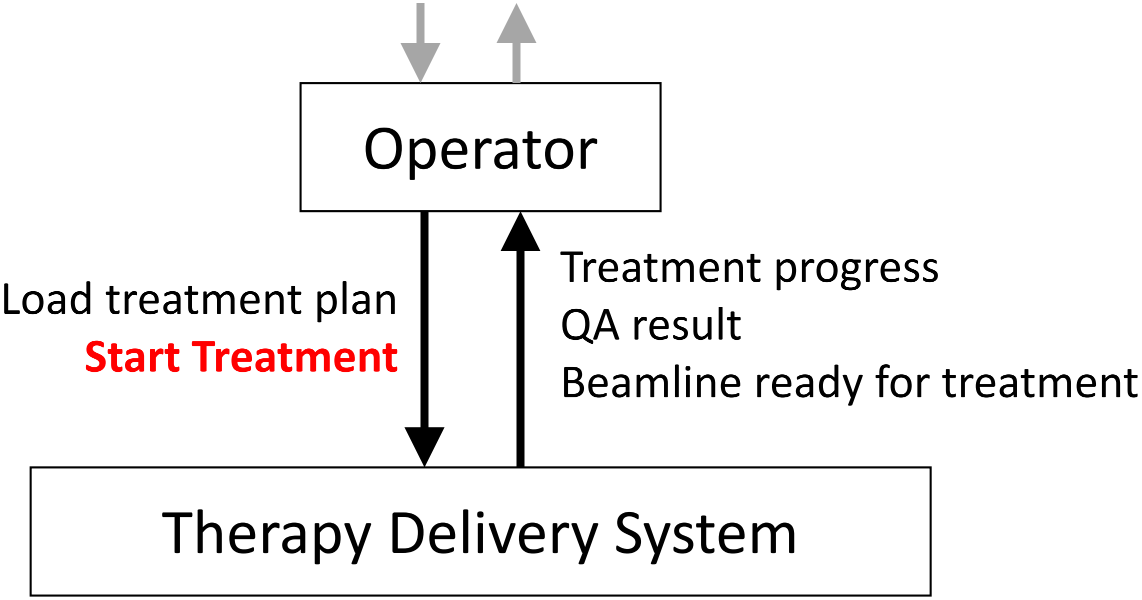


Figure 13 - Zooming into the Treatment Delivery group (D1)

Step 1: Identify Unsafe Control Actions



System Hazards

H-R1. Patient tissues receive more dose than clinically desirable

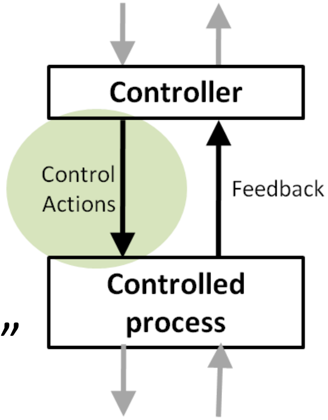
H-R2. Patient tumor receives less dose than clinically desirable

H-R3. Non-patient (esp. personnel) is unnecessarily exposed to radiation

H-R4. Equipment is subject to unnecessary stress

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early/too late, wrong order**	**Stopped too soon/ applied too long**
Start Treatment Command		Operator provides Start Treatment cmd while personnel is in room (↑H-R3)		

Structure of an Unsafe Control Action



Example:

"Operator provides start treatment cmd while personnel is in room"

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)

Unsafe control action summary

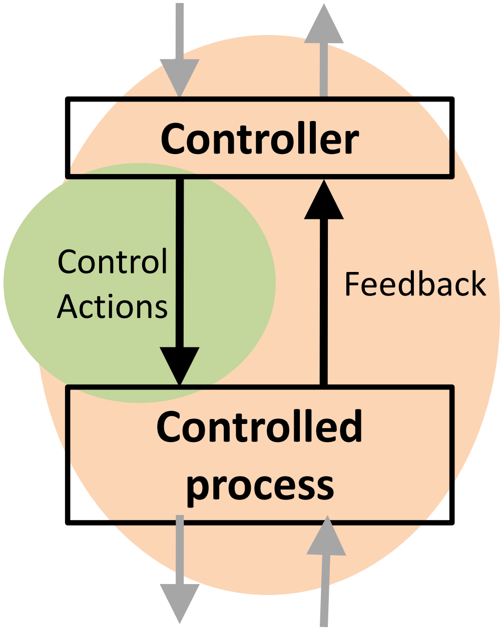
- UCA1. Treatment is started while personnel is in room (↑H-R3)
- UCA2. Treatment is started while patient is not ready to receive treatment (↑H-R1, H-R2
  - Note: This includes “wrong patient position”, “patient feeling unwell”, etc.
- UCA3. Treatment is started when there is no patient at the treatment point (↑H-R2)
- UCA4. Treatment is started with the wrong treatment plan (↑H-R1,H-R2)
- UCA5. Treatment is started without a treatment plan having been loaded (↑H-R1,H-R2)
- UCA6. Treatment is started while the beamline is not ready to receive the beam (↑H-R1, H-R4)
- UCA7. Treatment is started while not having mastership (↑H-R1, H-R2, H-R3)
- UCA8. Treatment is started while facility is in non-treatment mode (e.g. experiment or trouble shooting mode) (↑H-R1, H-R2)
- UCA9. Treatment start command is issued after treatment has already started (↑H-R1, H-R2)
- UCA10. Treatment start command is issued after treatment has been interrupted and without the interruption having adequately been recorded or accounted for (↑H-R1, H-R2)
- UCA11. Treatment does not start while everything else is otherwise ready (↑H-R1, H-R2)

Component Safety Constraints

Unsafe Control Action	Component Safety Constraint
Treatment is started while personnel is in room	Treatment must not be started while personnel are in the room
Treatment is started while the beamline is not ready to receive the beam	Treatment must not start before beamline is fully configured
Treatment is started when there is no patient at the treatment point	Treatment must not start until when patient is at the treatment point
Treatment is started without a treatment plan having been loaded	Treatment must not start until a new treatment plan has been loaded

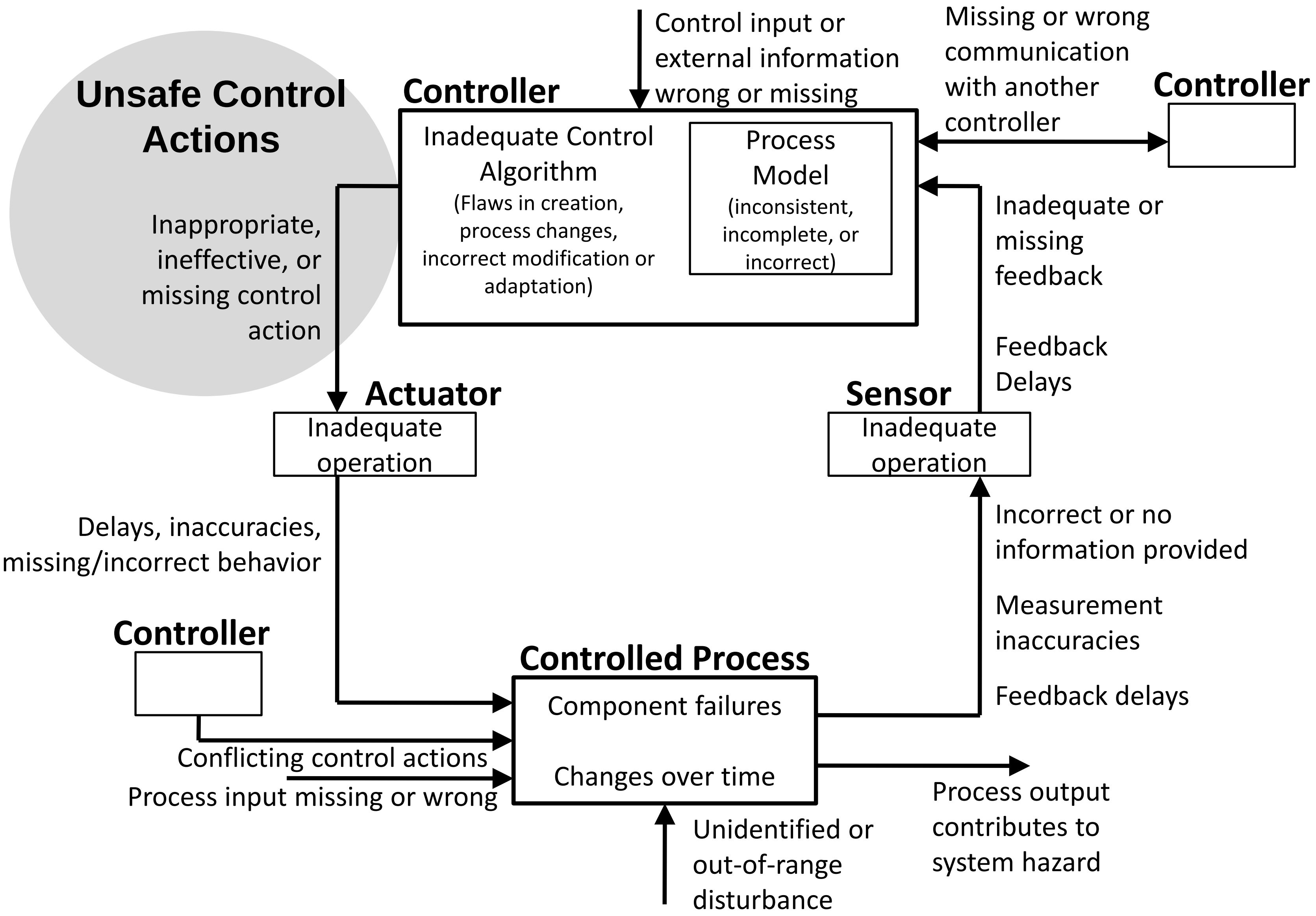
STPA
(System-Theoretic Process Analysis)

- ✓ 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



Unsafe Control Actions

Inappropriate, ineffective, or missing control action

Controller

Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

Process Model (inconsistent, incomplete, or incorrect)

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delays, inaccuracies, missing/incorrect behavior

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

Conflicting control actions

Process input missing or wrong

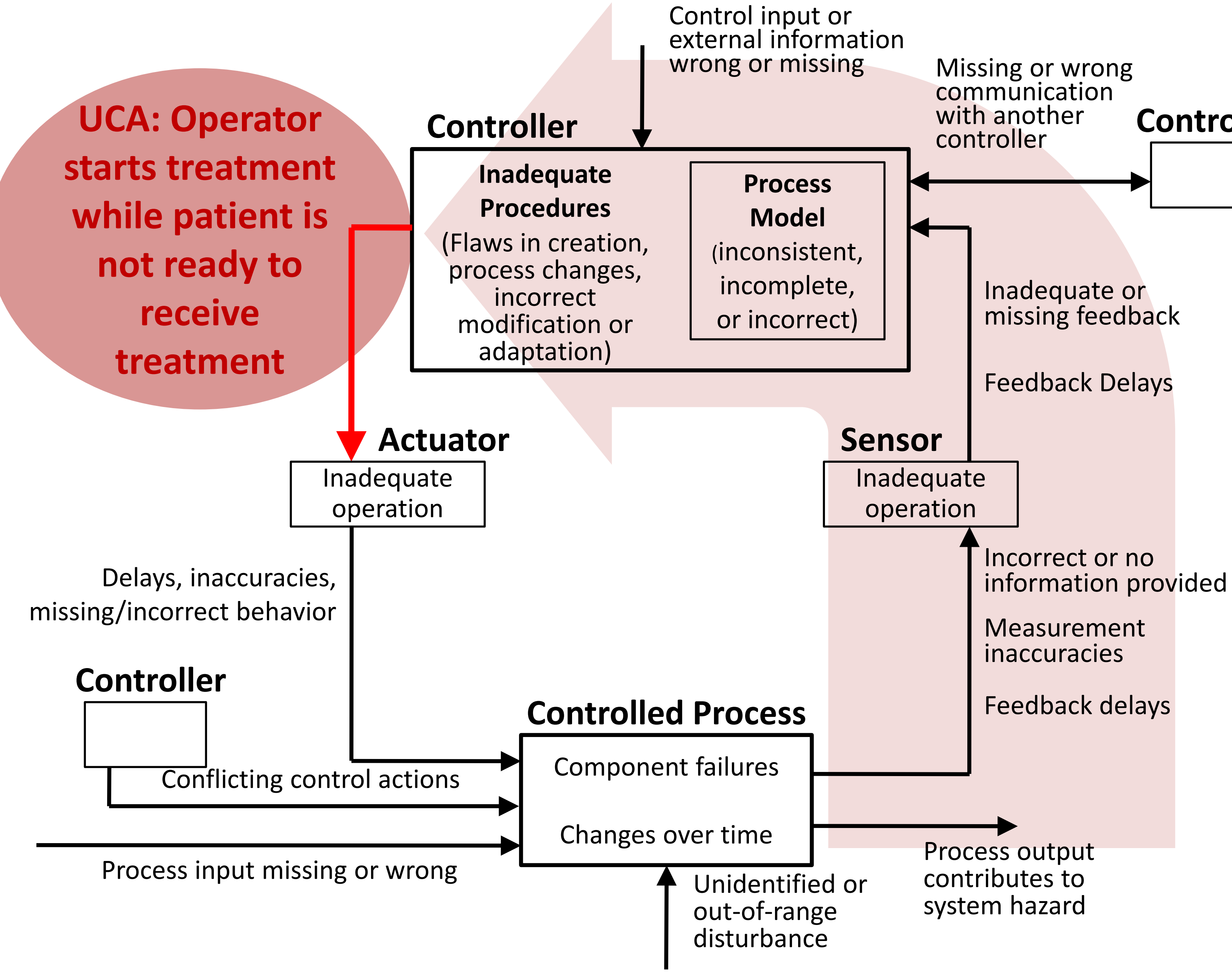
Unidentified or out-of-range disturbance

Process output contributes to system hazard

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



UCA: Operator starts treatment while patient is not ready to receive treatment

Controller

Inadequate Procedures

(Flaws in creation, process changes, incorrect modification or adaptation)

Process Model

(inconsistent, incomplete, or incorrect)

Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Delays, inaccuracies, missing/incorrect behavior

Controller

Conflicting control actions

Controlled Process

Component failures

Changes over time

Process input missing or wrong

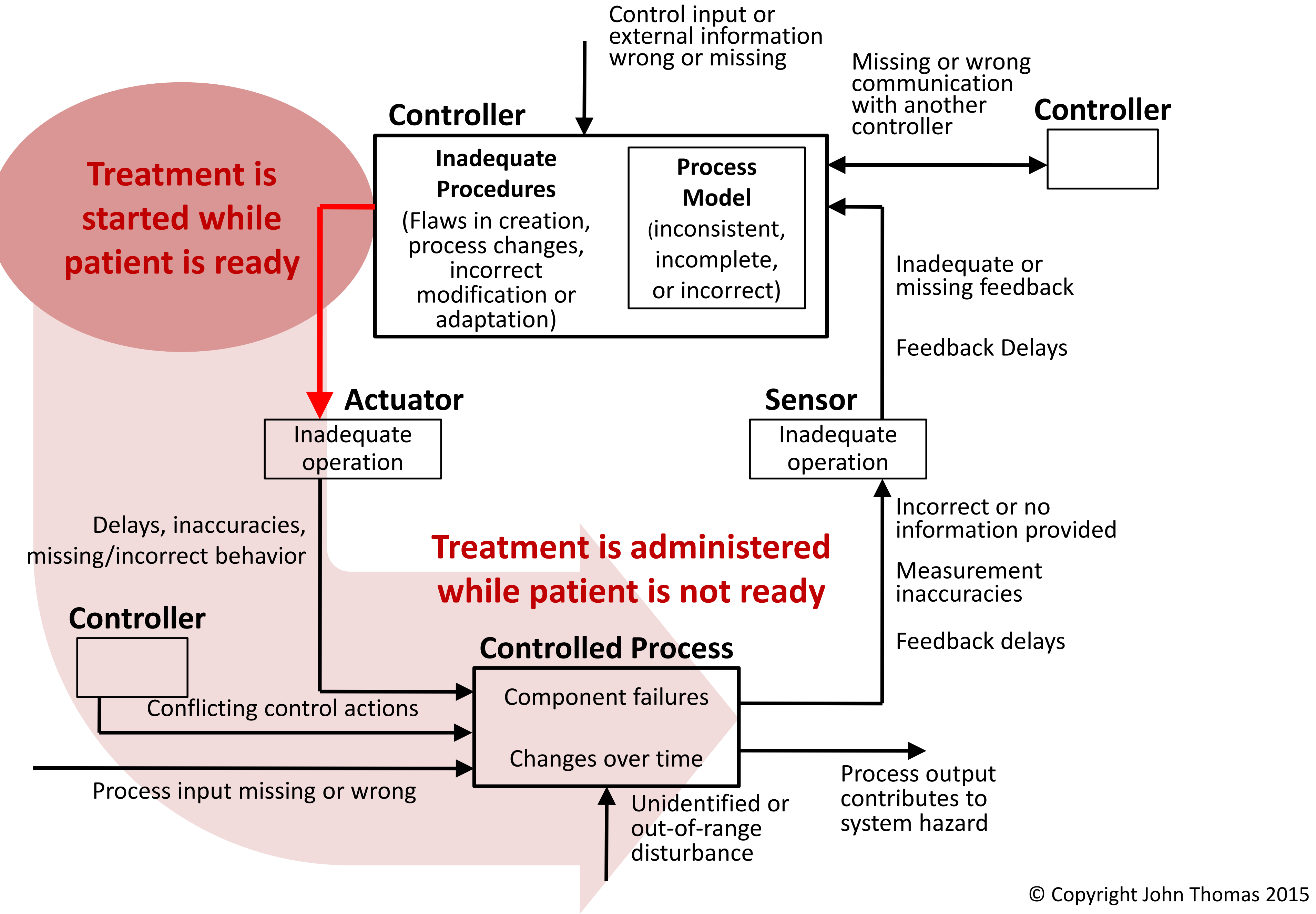
Unidentified or out-of-range disturbance

Process output contributes to system hazard

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


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Inadequate Procedures
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or incorrect)
Treatment is started while patient is ready
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delays, inaccuracies, missing/incorrect behavior
Treatment is administered while patient is not ready
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

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

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.

Example Controls for Causal Scenarios Command not followed

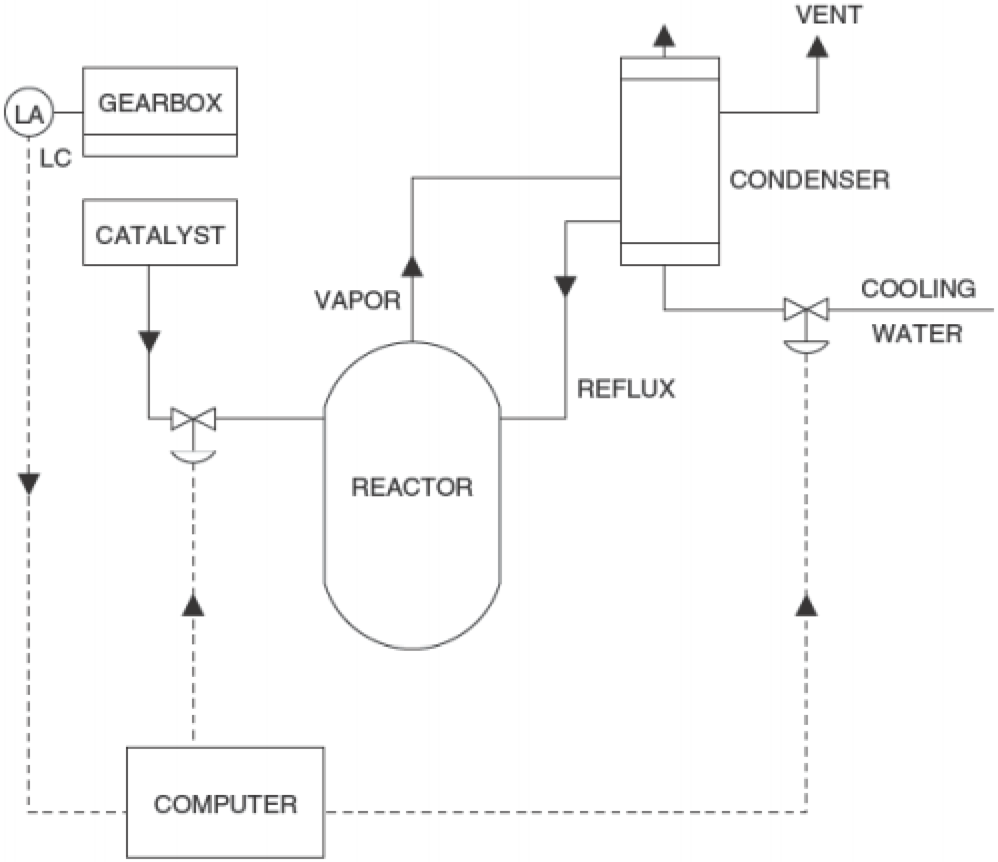
- **Scenario 3 –** The operator provides the Start Treatment command, but it does not execute properly because the proper steering file failed to load (either because operator did not load it, or previous plan was not erased from system memory and overwriting is not possible) or the system uses a previously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

Chemical Reactor Example

Chemical Reactor Design

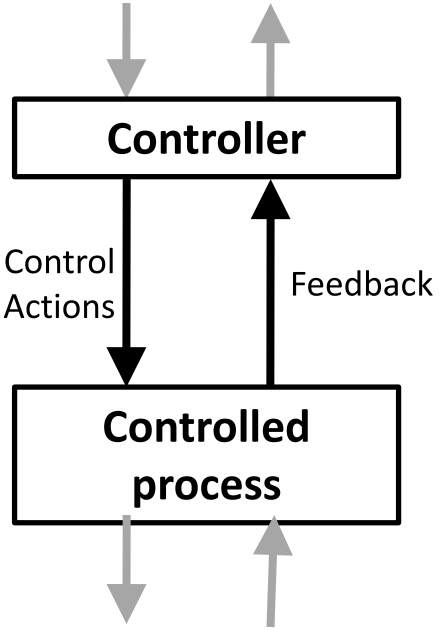
- Toxic catalyst flows into reactor
- Chemical reaction creates heat, pressure
- Water and condenser provide cooling



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

STPA
(System-Theoretic Process Analysis)

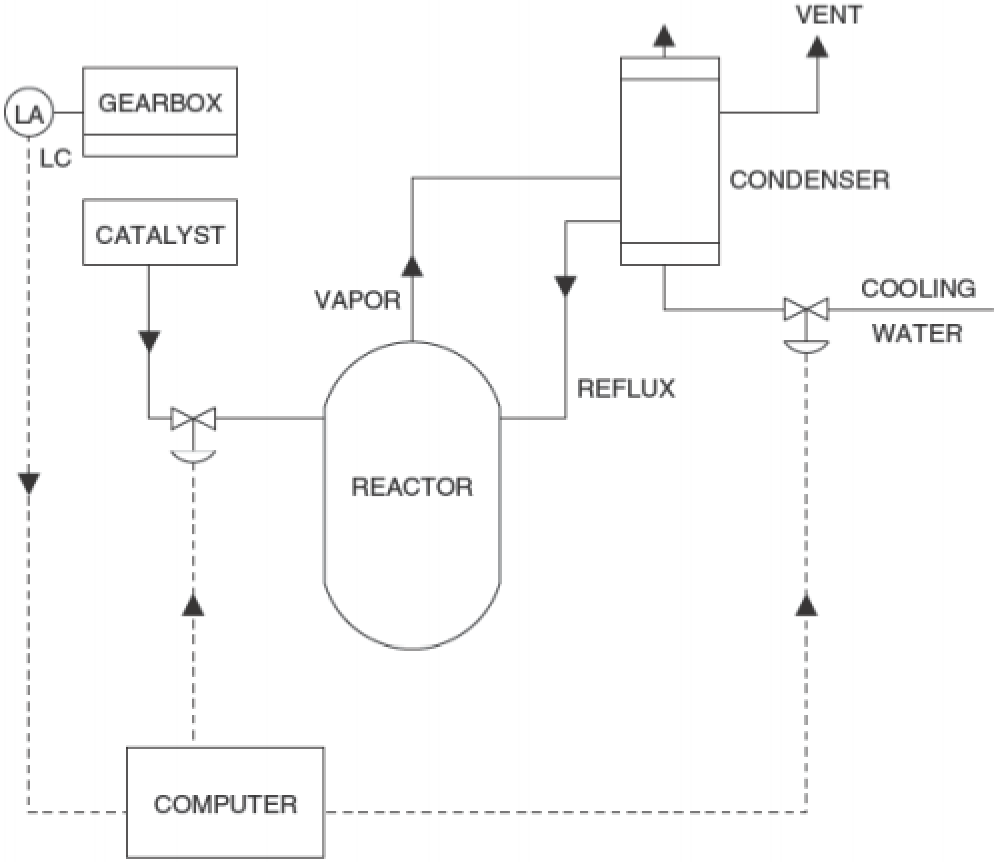
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

Chemical Reactor Design

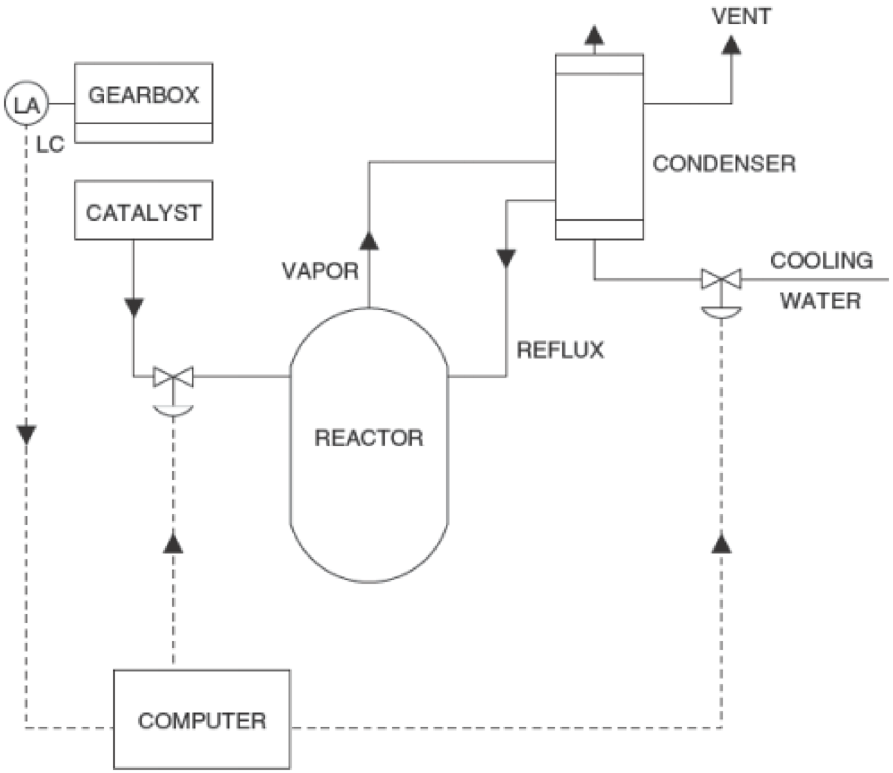
- Toxic catalyst flows into reactor
- Chemical reaction creates heat, pressure
- Water and condenser provide cooling

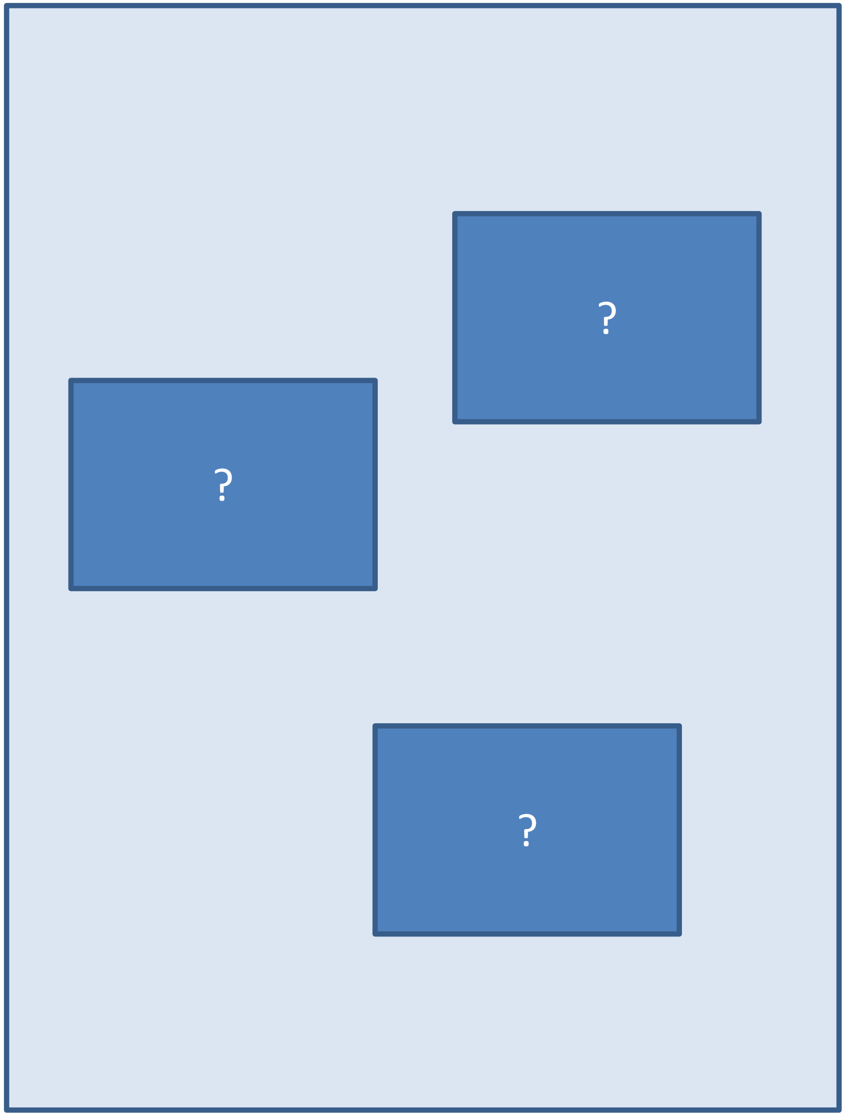


Create Control Structure

STPA Analysis

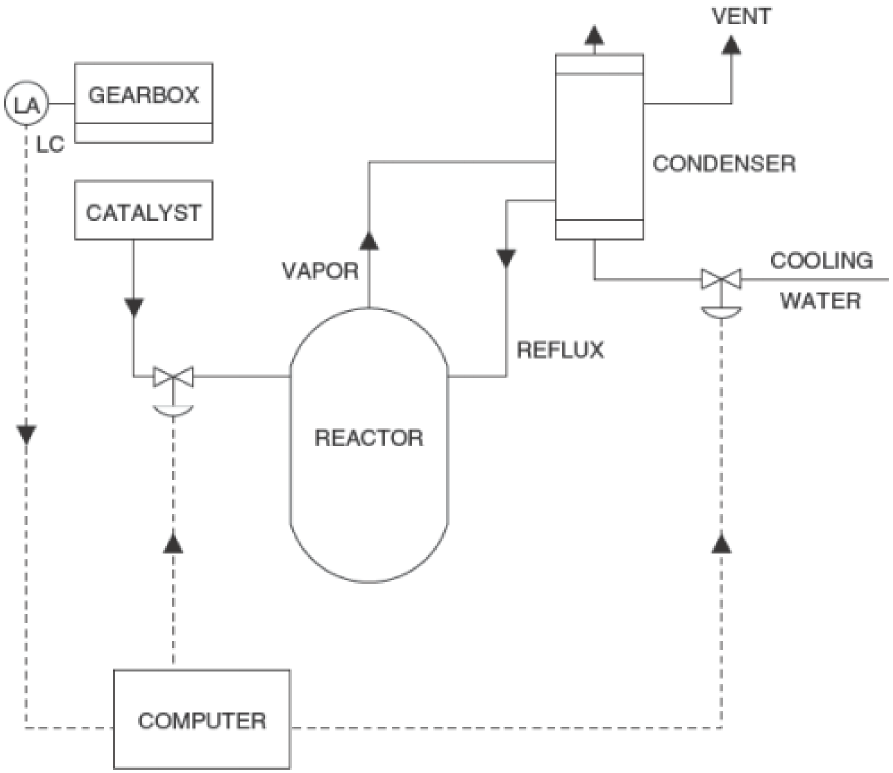
- High-level (simple) Control Structure
  - What are the main parts?

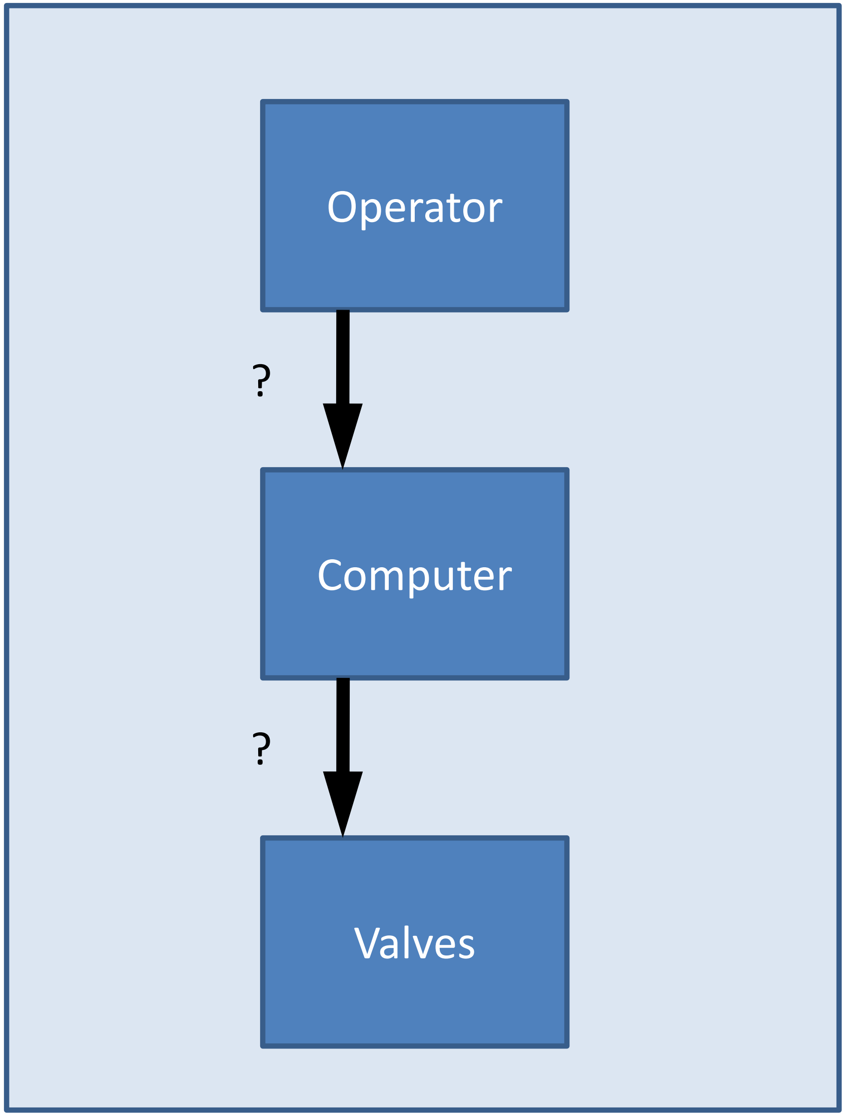




STPA Analysis

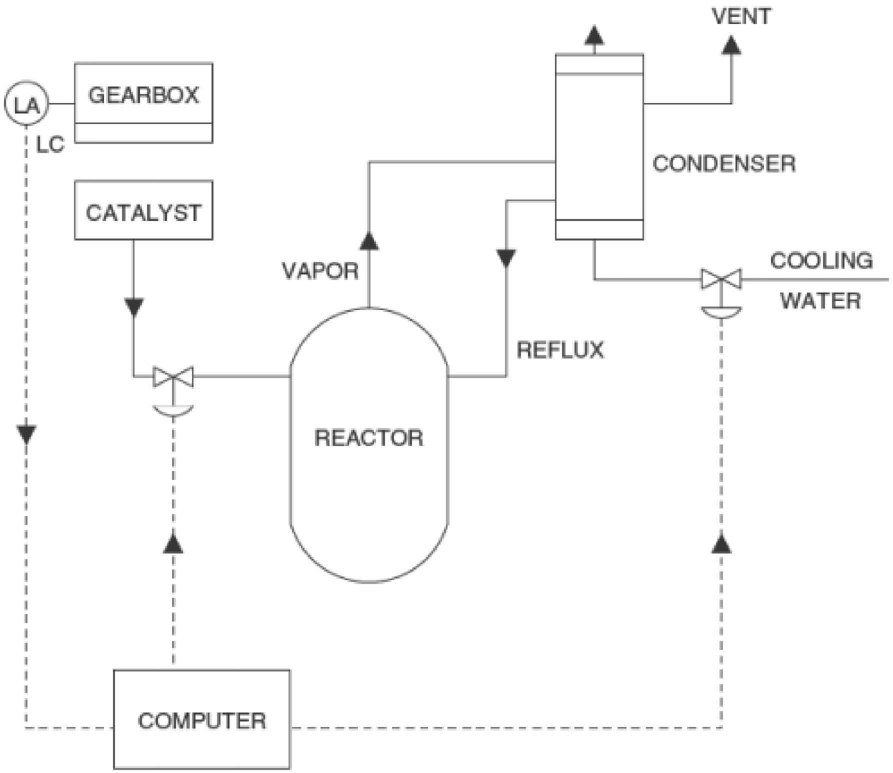
- High-level (simple) Control Structure
  - What commands are sent?

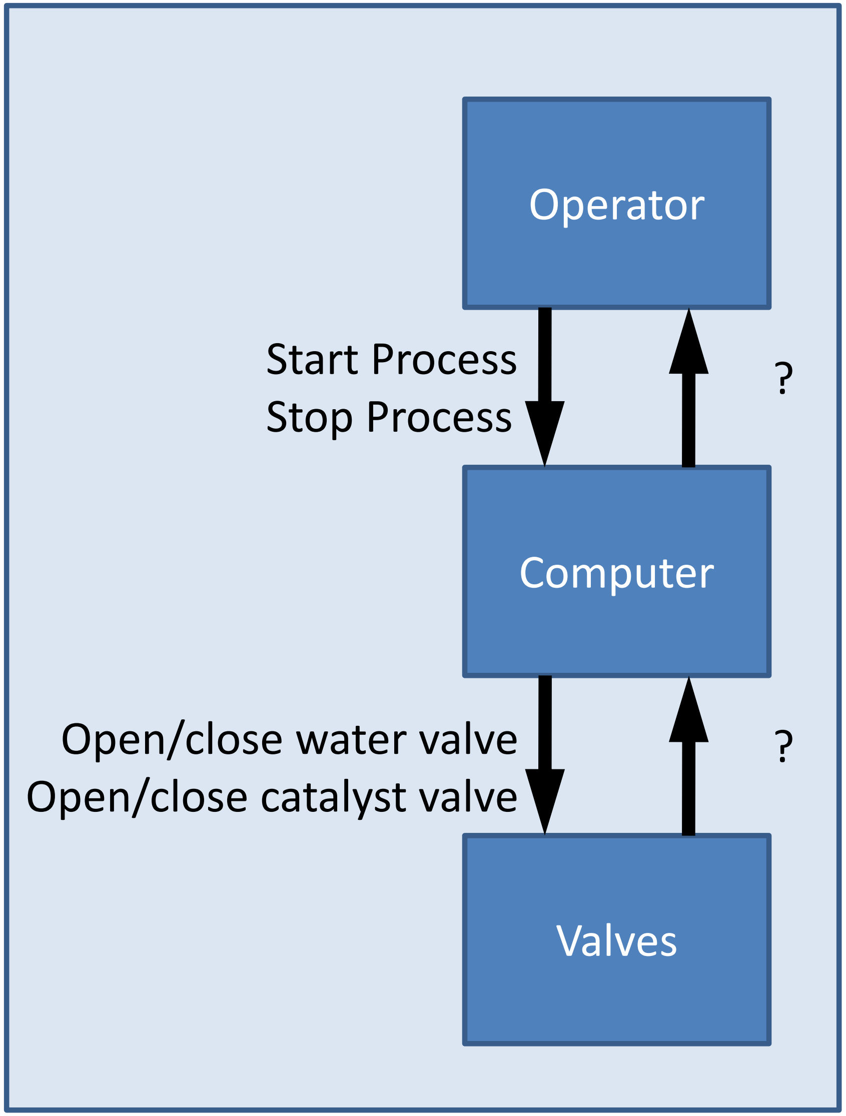




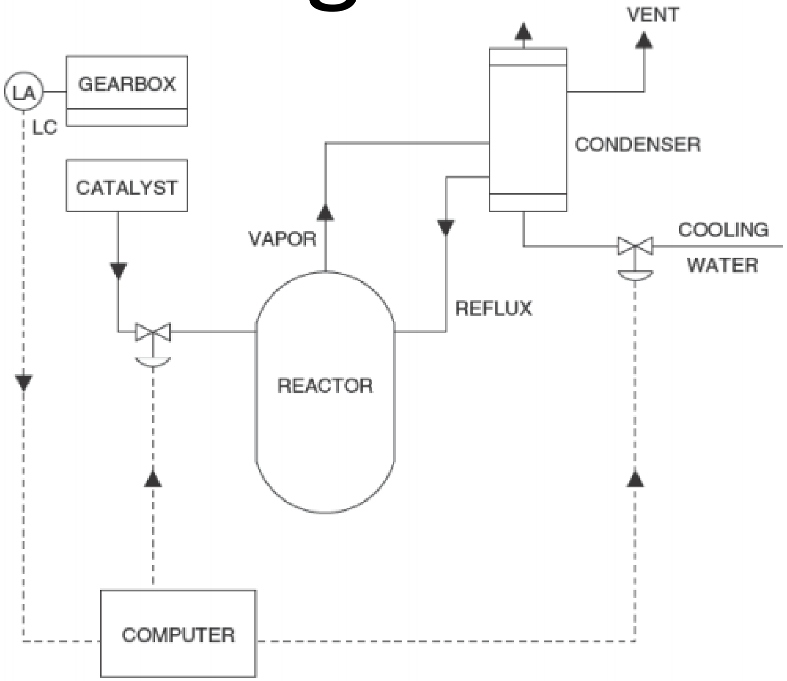
STPA Analysis

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

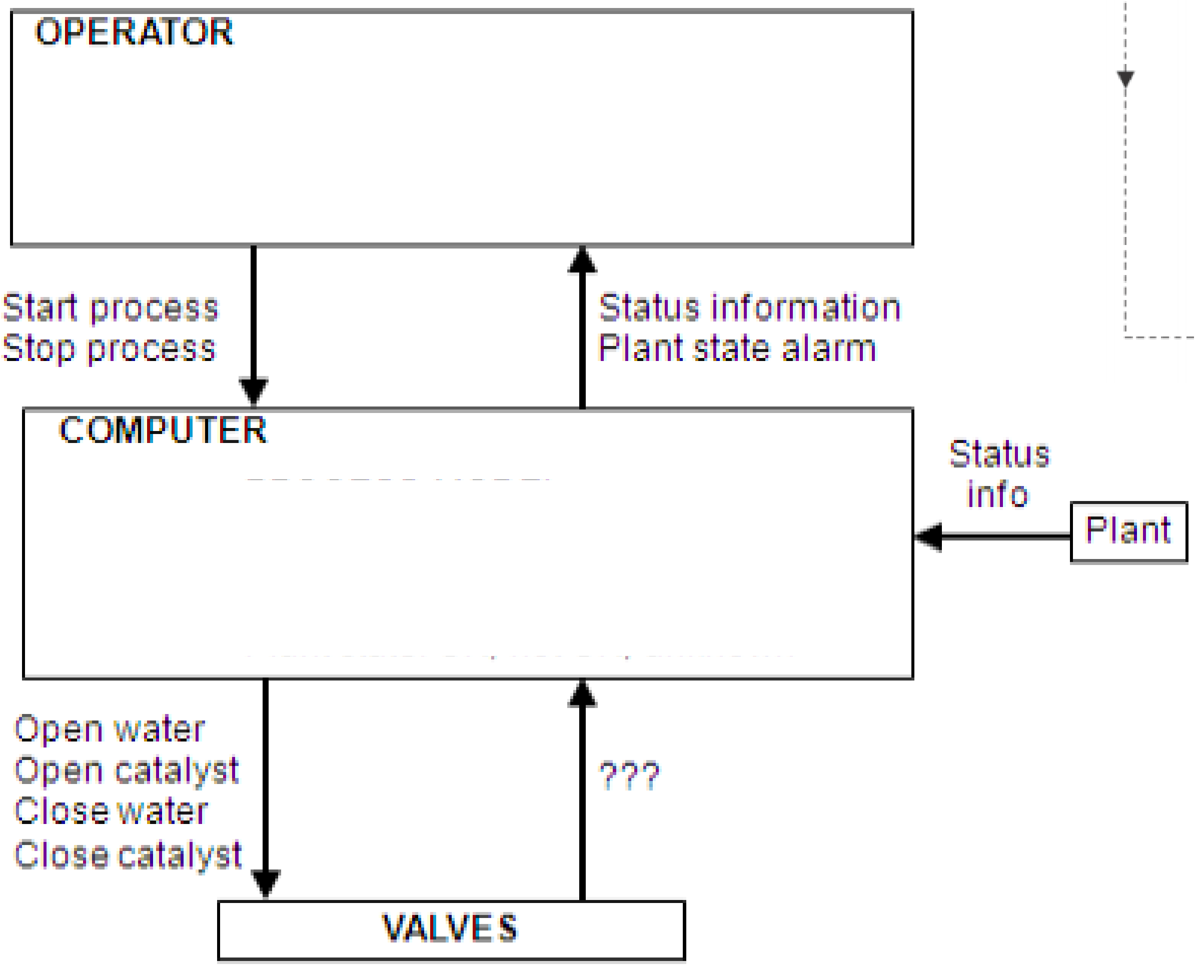




Chemical Reactor Design



Control Structure:



OPERATOR

Start process
Stop process

Status information
Plant state alarm

COMPUTER

Status info

Plant

Open water
Open catalyst
Close water
Close catalyst

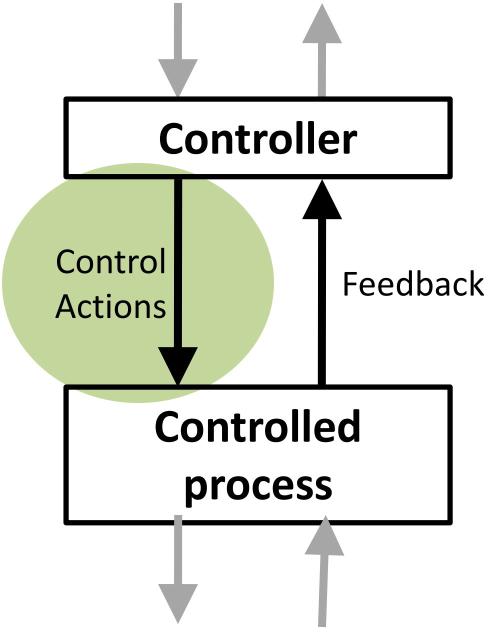
???

VALVES

© Copyright John thomas 2015

STPA
(System-Theoretic Process Analysis)

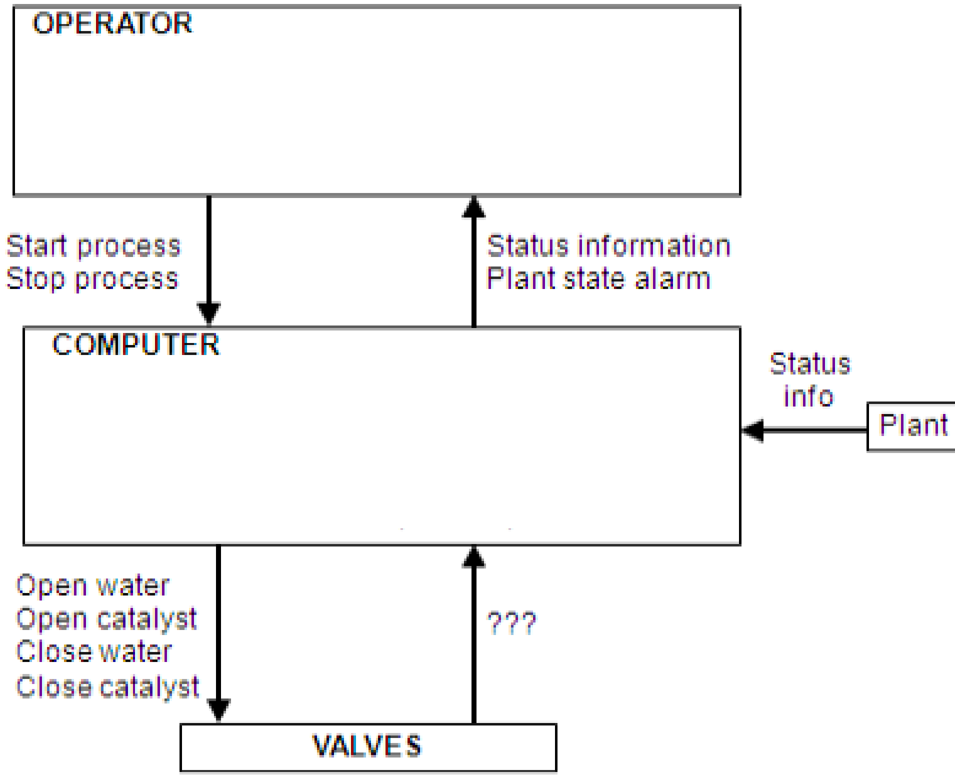
- ✓ Identify accidents and hazards
- ✓ Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



(Leveson, 2012)

Chemical Reactor: Unsafe Control Actions

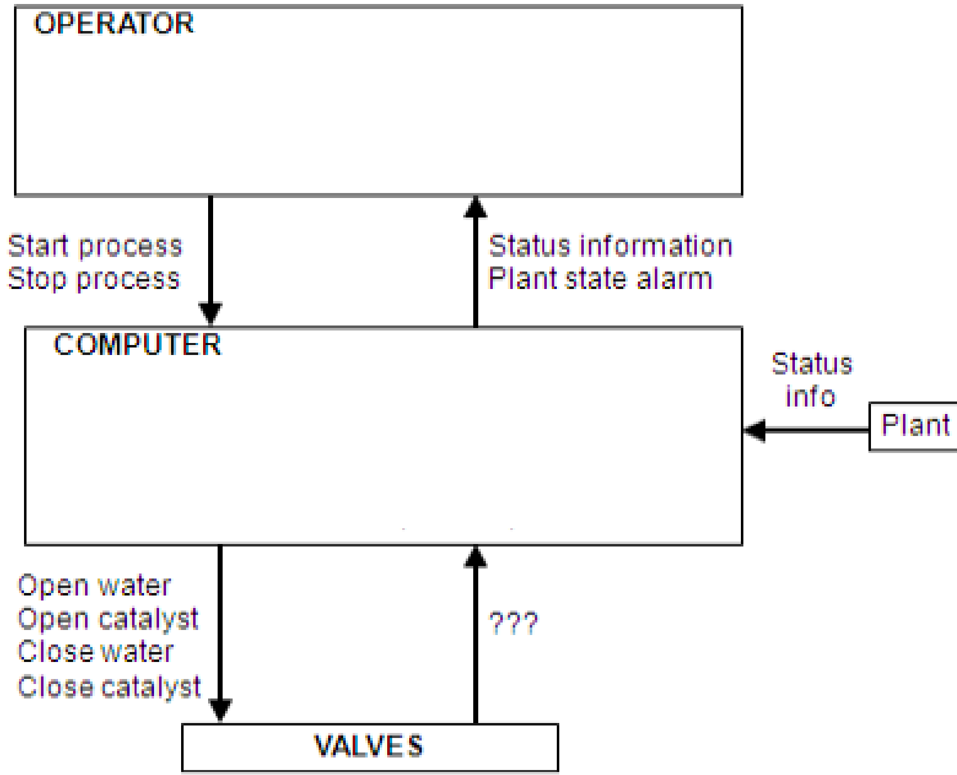
Control Structure:



	?	?	?	?
Close Water Valve				

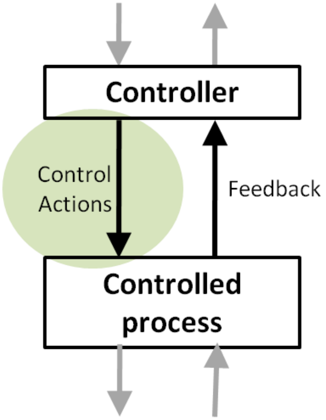
Chemical Reactor: Unsafe Control Actions

Control Structure:

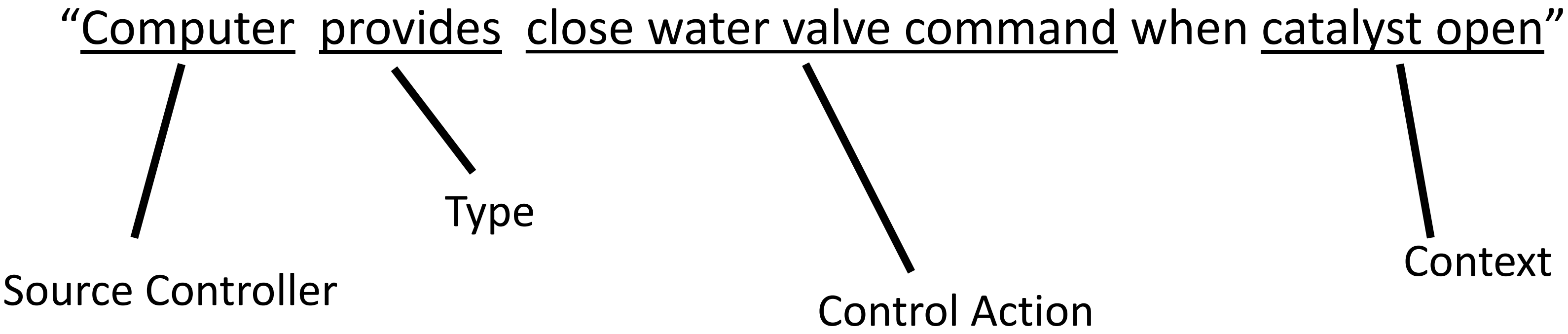


	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve	?	Computer provides Close Water cmd while catalyst open	?	?

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 provides Close Water cmd while catalyst open	Computer provides Close Water cmd before catalyst closes	
Open Water Valve				
Open Catalyst Valve				
Close Catalyst Valve				

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 closes water valve while catalyst valve open	?
Computer closes water valve before catalyst valve closes	?
Computer opens catalyst valve when water valve not open	?
Etc.	Etc.

Safety Constraints

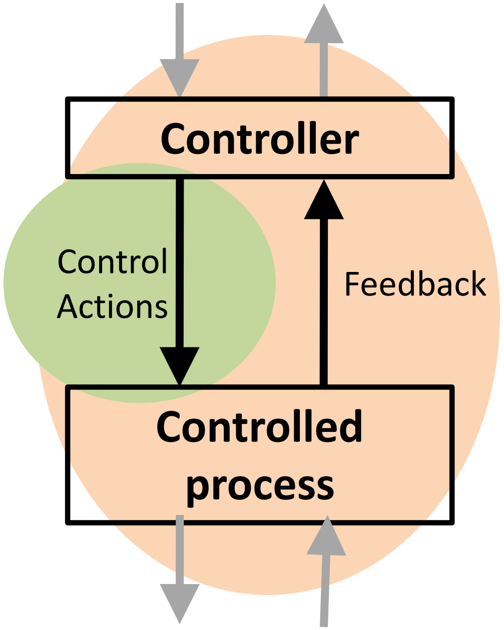
Unsafe Control Action	Safety Constraint
Computer does not open water valve when catalyst valve open	Computer must open water valve whenever catalyst valve is open
Computer opens water valve more than X seconds after catalyst valve open	Computer must open water valve within X seconds of catalyst valve 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]**

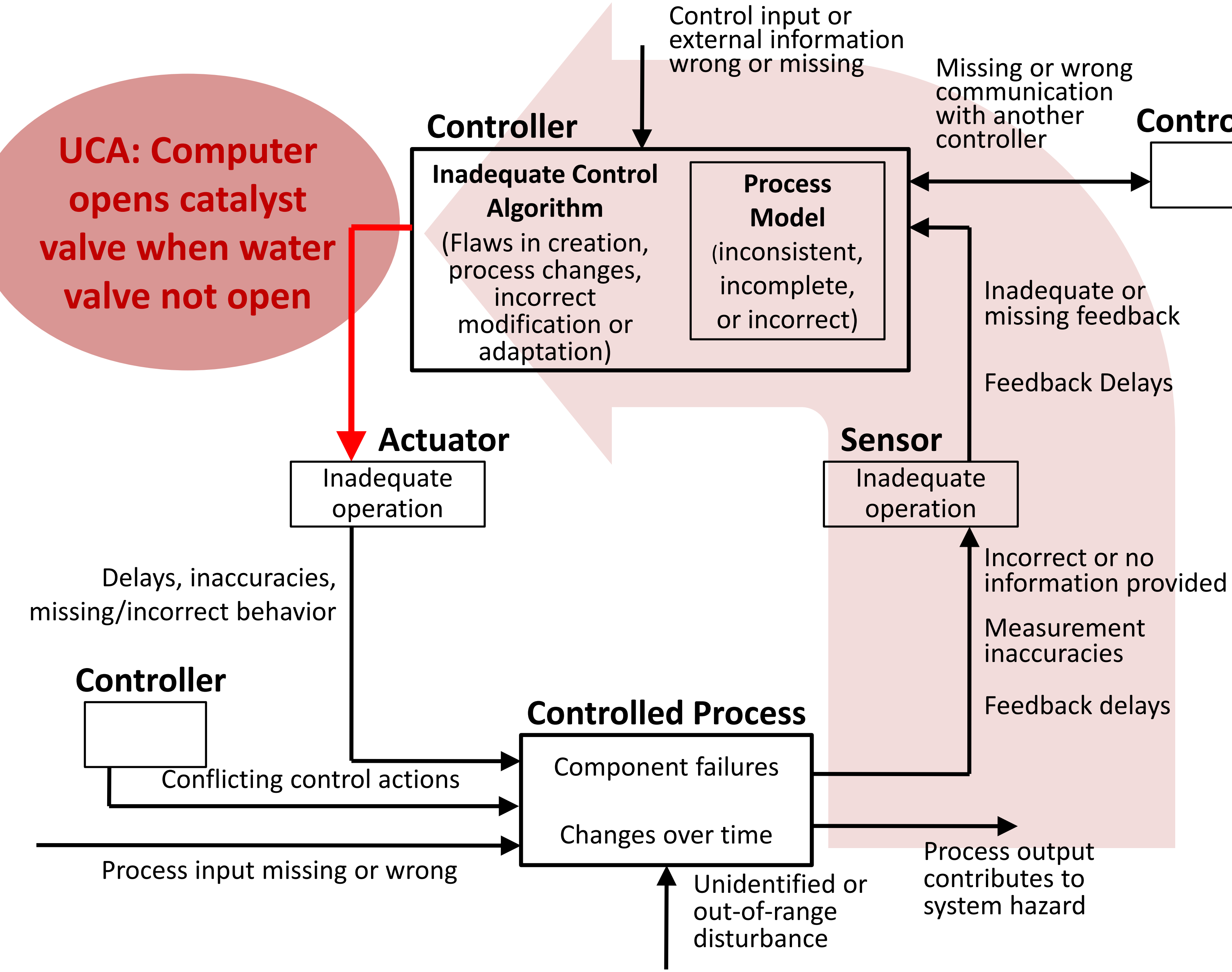
STPA
(System-Theoretic Process Analysis)

- ✓ 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



UCA: Computer opens catalyst valve when water valve not open

Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)

Process Model
(inconsistent, incomplete, or incorrect)

Controller

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delays, inaccuracies, missing/incorrect behavior

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

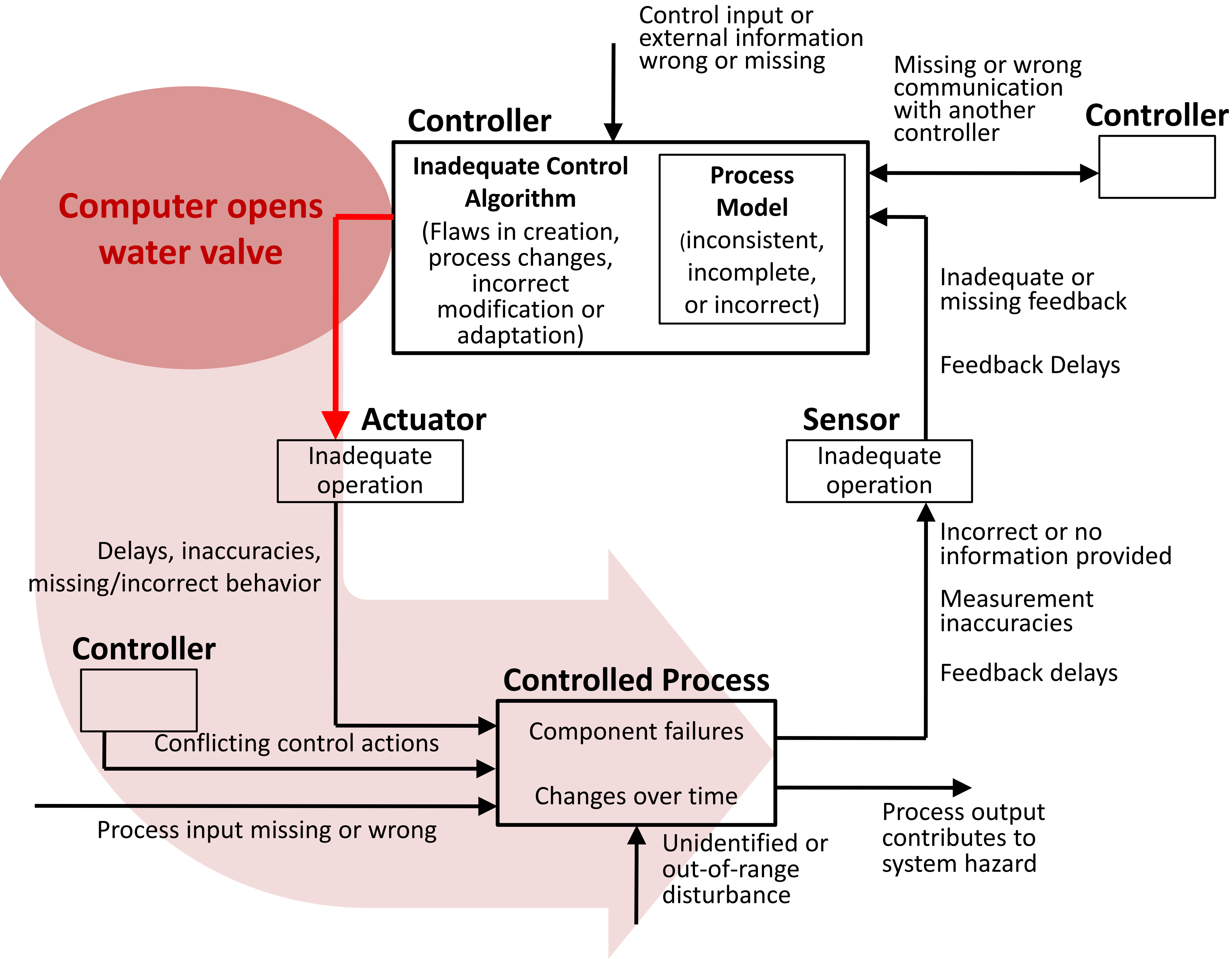
Conflicting control actions

Process input missing or wrong

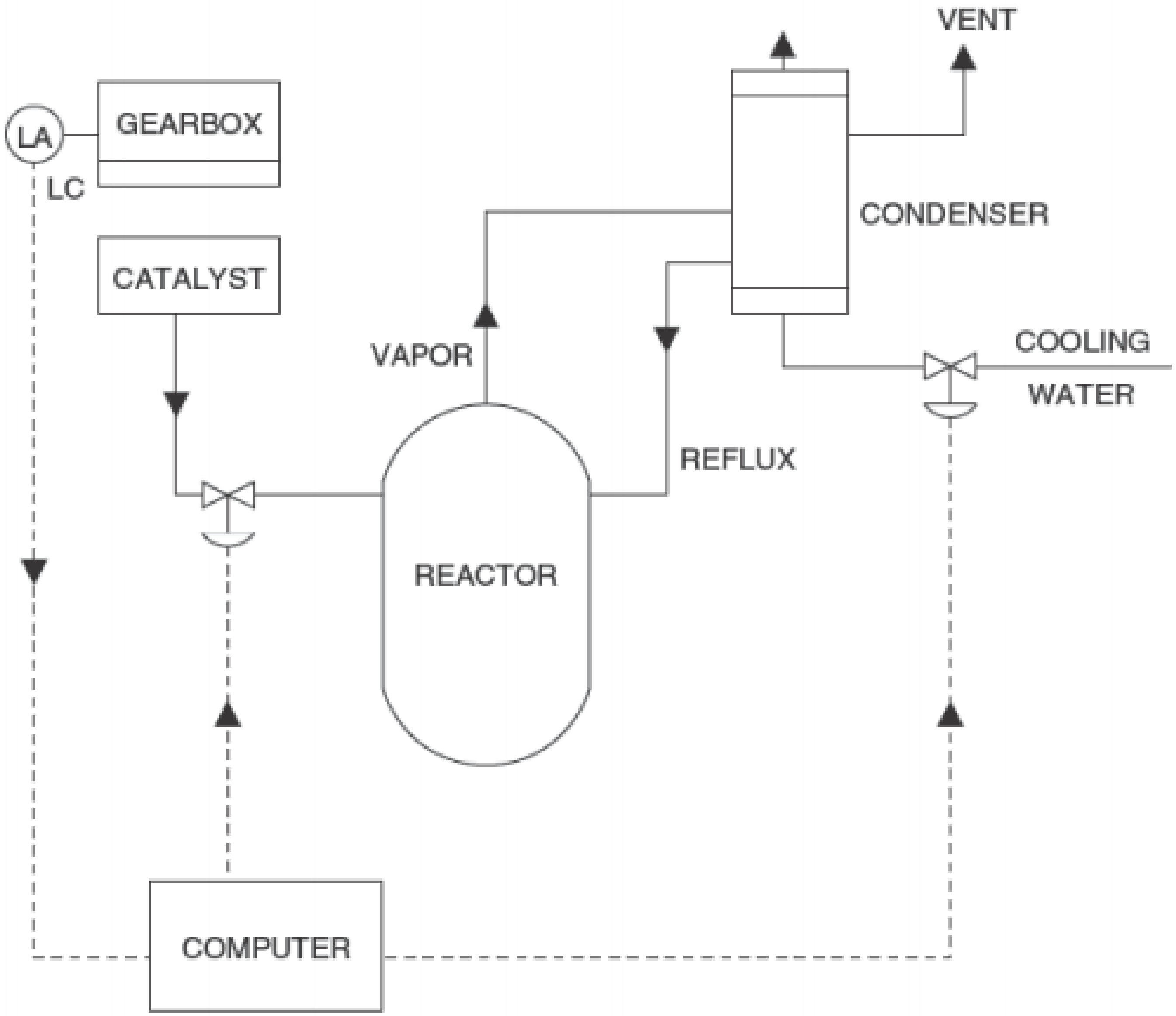
Unidentified or out-of-range disturbance

Process output contributes to system hazard

Step 2: Potential control actions not followed


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Computer opens water valve
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or incorrect)
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delays, inaccuracies, missing/incorrect behavior
Controller
Conflicting control actions
Controlled Process
Component failures
Changes over time
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Chemical Reactor: Real accident



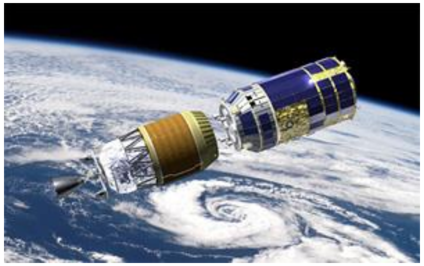
STAMP/STPA – Advanced Tutorial

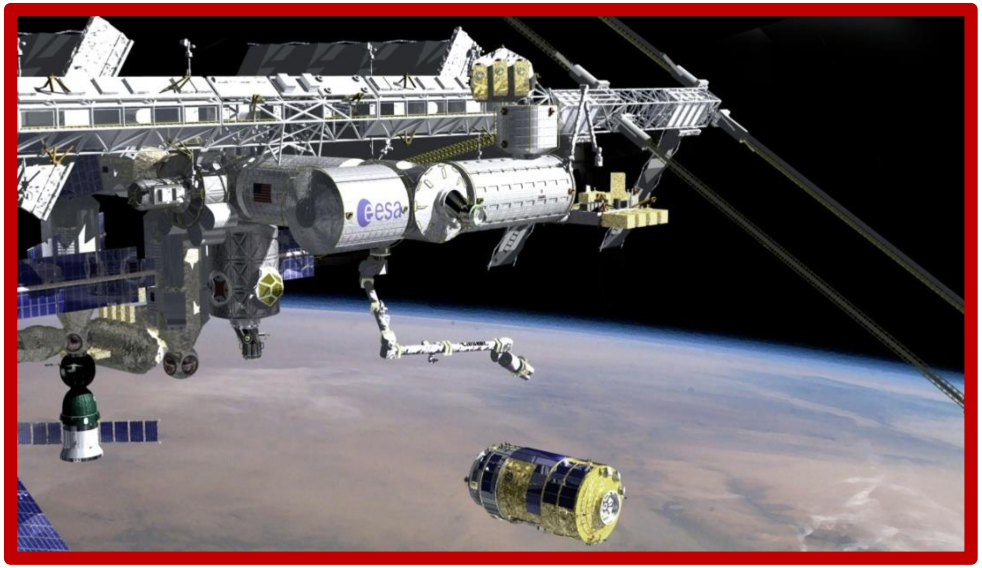
JAXA H-II Transfer Vehicle (HTV)

Takuto Ishimatsu

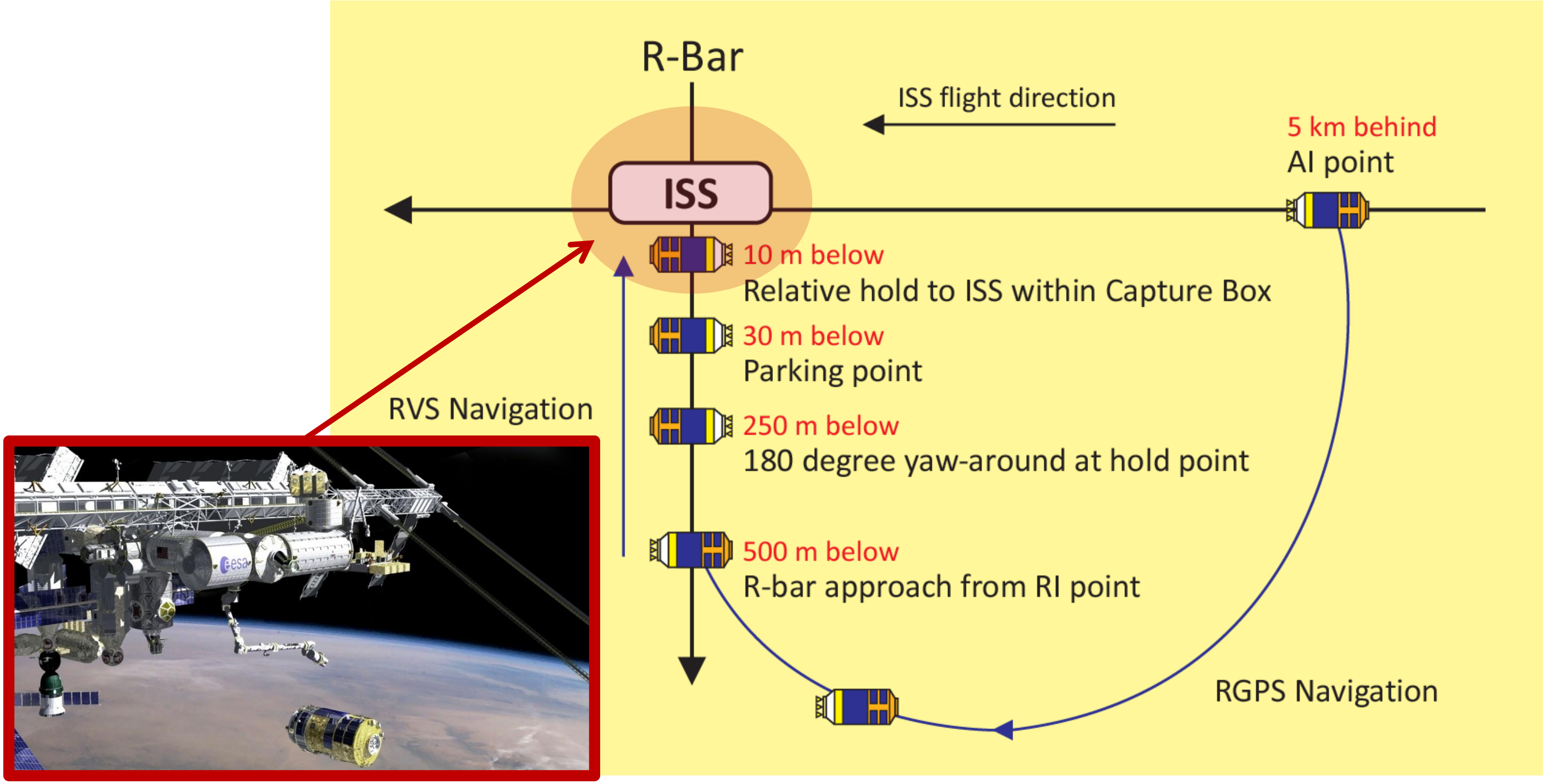
HTV: H-II Transfer Vehicle

- 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

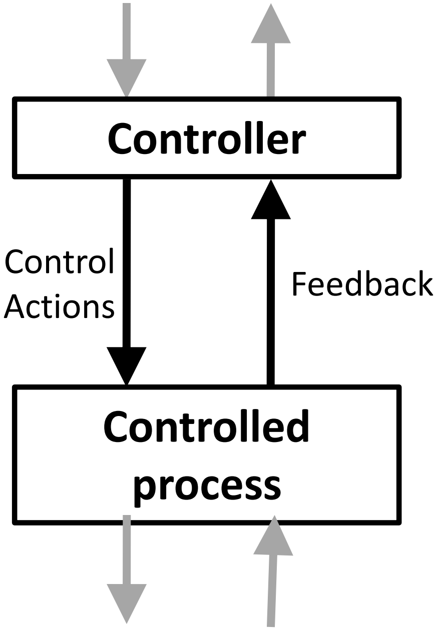


Basic Information

- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA ground station**
  - **JAXA ground station**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to deactivate HTV (by radio) to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (activated/deactivated mode, fault status) to ISS and ground stations
    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, NASA, or JAXA must activate HTV by sending ***Abort/Retreat/Hold*** commands to the HTV. Abort is final (HTV ignores all future commands).
  - ISS crew and NASA/JAXA ground stations can communicate with each other using a **voice loop connection** through the entire operation

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



Controller

Control Actions

Feedback

Controlled process

(Leveson, 2012)

Accidents / Hazards

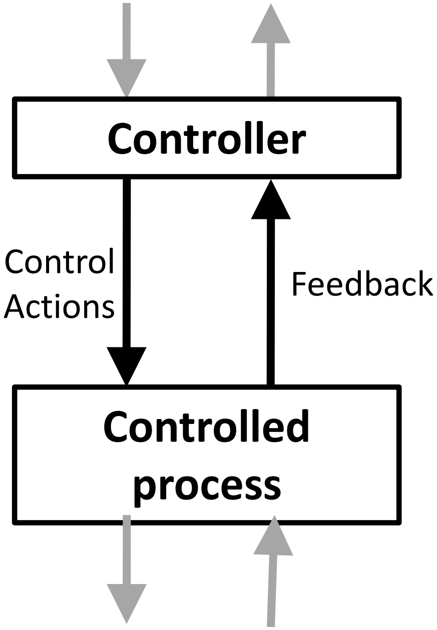
- Accidents
  - HTV collides with ISS
- Hazards
  - HTV too close to ISS (for given speed)

Accidents / Hazards

- Accidents
  - A-1: HTV collides with ISS
  - A-2: Loss of delivery mission
- Hazards
  - H-1: HTV too close to ISS (for given operational phase)
  - H-2: HTV trajectory makes delivery impossible
- 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



Controller

Control Actions

Feedback

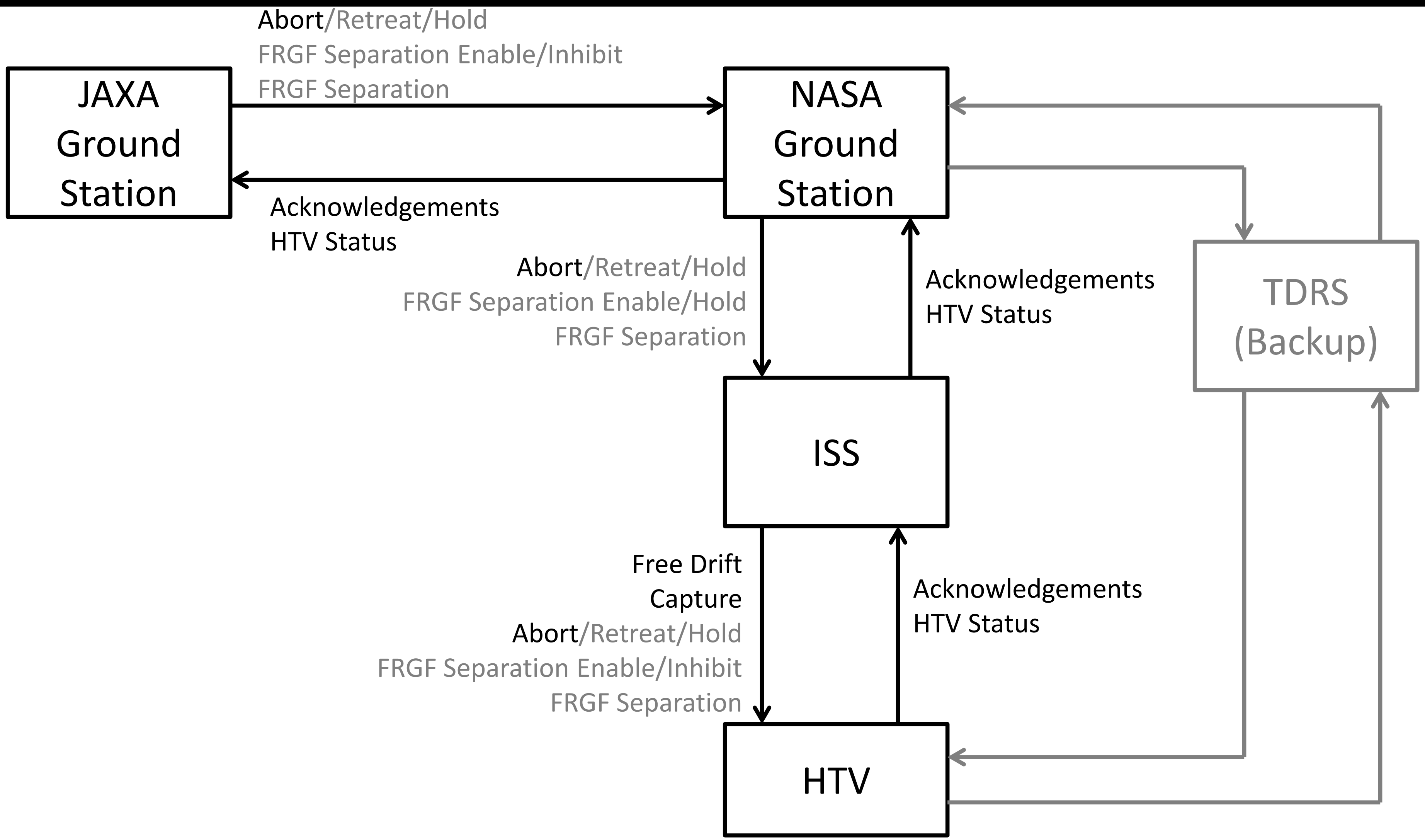
Controlled process

(Leveson, 2012)

Basic Information

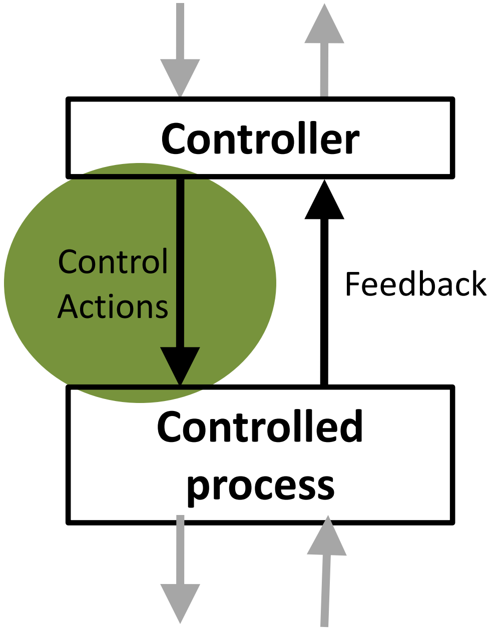
- Accident we want to prevent: **collision with ISS**
- Components in the system
  - **HTV**
  - **ISS (including crew)**
  - **NASA ground station**
  - **JAXA ground station**
- Capture operation
  - Once HTV reaches Capture Box (10 m below ISS),
    1. ISS crew sends a ***Free Drift*** command to deactivate HTV (by radio) to disable the thrusters in preparation for capture
    2. HTV sends back **HTV status** (activated/deactivated mode, fault status) to ISS and ground stations
    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, NASA, or JAXA must activate HTV by sending ***Abort/Retreat/Hold*** commands to the HTV. Abort is final (HTV ignores all future commands).
  - ISS crew and NASA/JAXA ground stations can communicate with each other using a **voice loop connection** through the entire operation

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)

STPA Step 1: Unsafe Control Actions

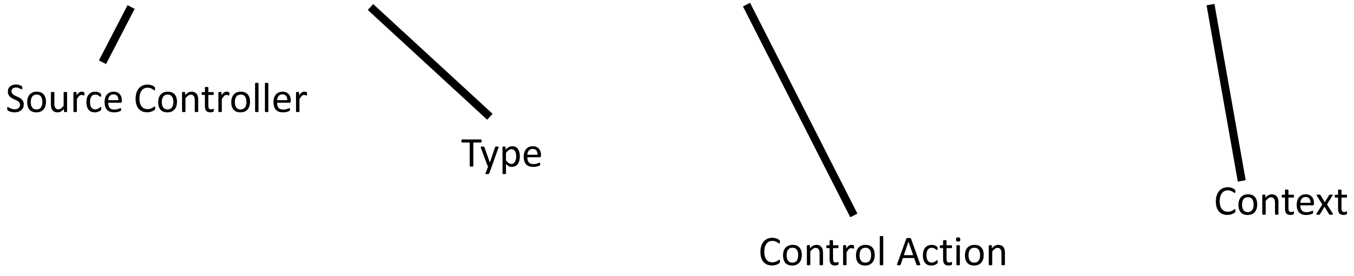
ISS Crew Actions

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

STPA Step 1: Unsafe Control Actions

Example:

"Computer provides open catalyst valve cmd while water valve is closed"



Source Controller

Type

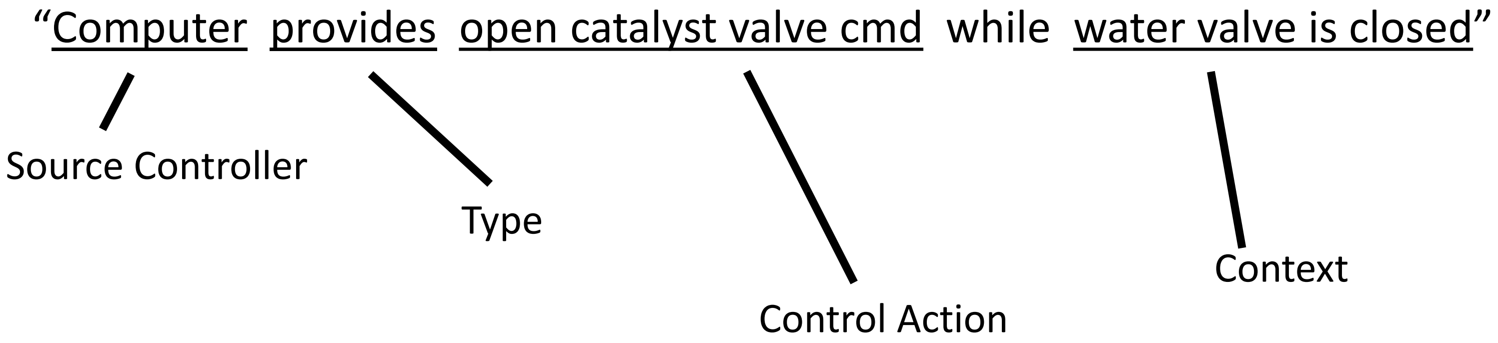
Control Action

Context

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

STPA Step 1: Unsafe Control Actions

Example:



"Computer provides open catalyst valve cmd while water valve is closed"

Source Controller

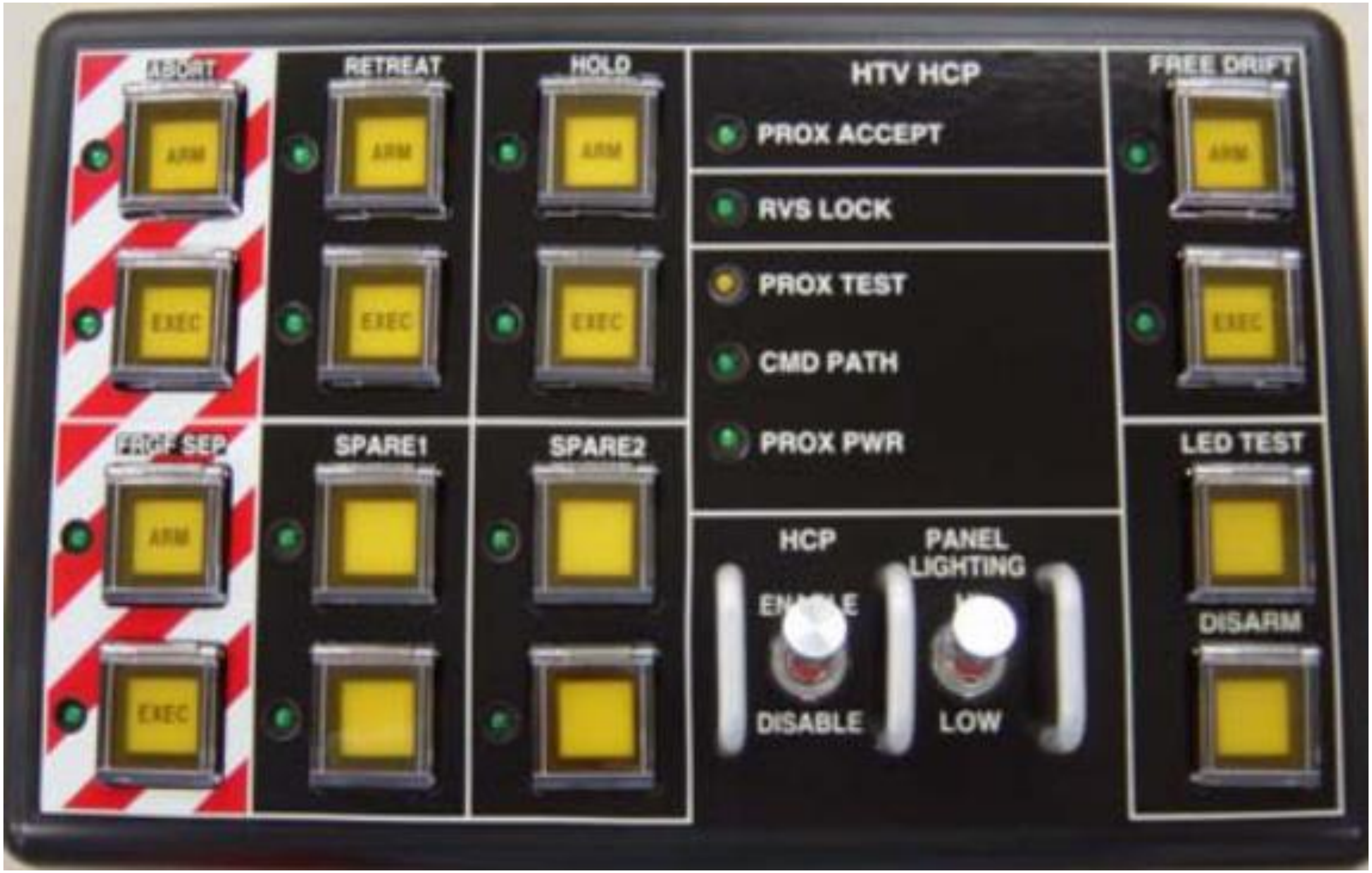
Type

Control Action

Context

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Abort	ISS crew does not provide abort when _______	ISS crew provides abort when _______	ISS crew provides abort too late after _______	
Free Drift				
Capture				

Actual Astronaut Control Interface



Step 1: Unsafe Control Actions

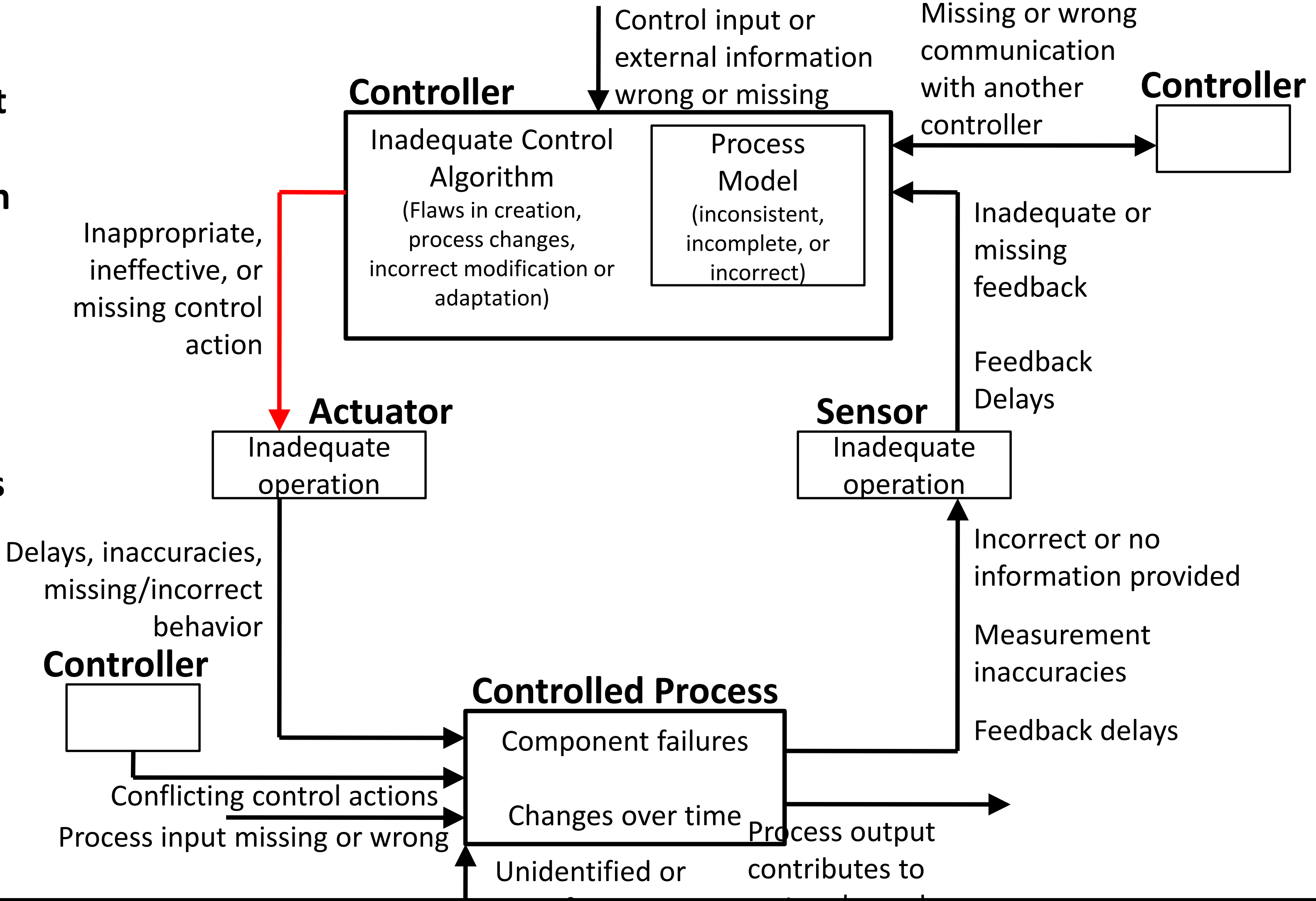
Unsafe control actions leading to Hazard H-1: HTV too close to ISS (for given operational phase)

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 Step 2: Accident Scenarios

UCA-1: ISS Crew does not perform capture within X sec of HTV deactivation [H-1, H-2]

UCA-2: ISS Crew provides free drift command while HTV approaching ISS [H-1, H-2]



Controller

Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

Process Model (inconsistent, incomplete, or incorrect)

Inappropriate, ineffective, or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delays, inaccuracies, missing/incorrect behavior

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

Conflicting control actions

Process input missing or wrong

Unidentified or

Process output contributes to

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: 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, …)

For more information

- Google: “STPA Primer”
  - Written for industry to provide guidance in learning STPA
  - Not a book or academic paper
  - “living” document
- Website: mit.edu/psas
  - Previous MIT STAMP workshop presentations
  - Industry-focused
- Sunnyday.mit.edu
  - Academic STAMP papers, examples