STPA Intro

Dr. John Thomas

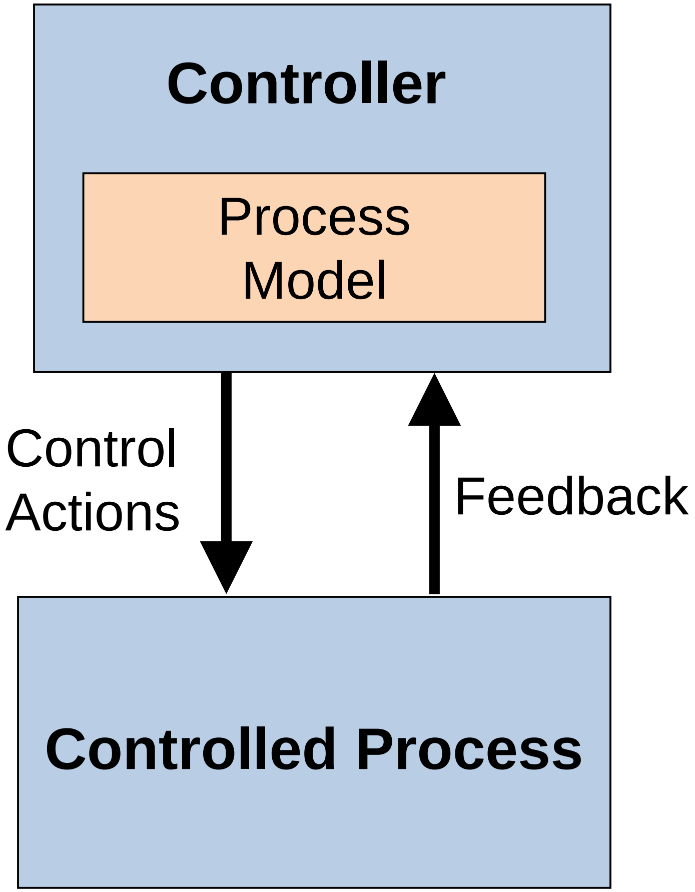
Any questions? Email me! JThomas4@mit.edu

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

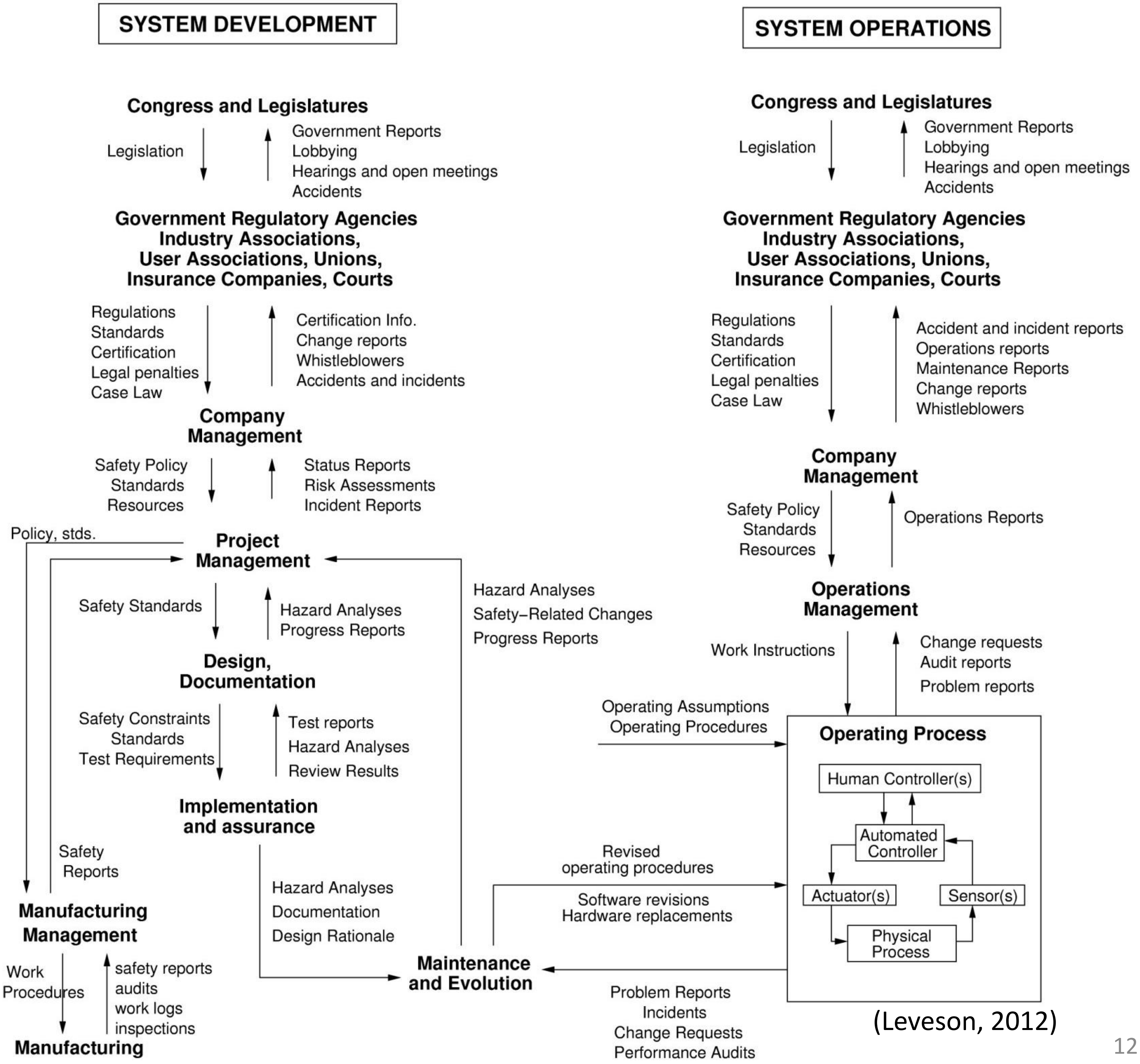


- Controllers use a **<u>process model</u>** to determine control actions
  - Accidents often occur when the process model is incorrect
- A good model of both software and human behavior in accidents
- Four types of **<u>unsafe control actions</u>**:
  1) Control commands required for safety are not 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

Can capture software errors, human errors, flawed requirements,…

Example Safety Control Structure

Control



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

(Leveson, 2012)

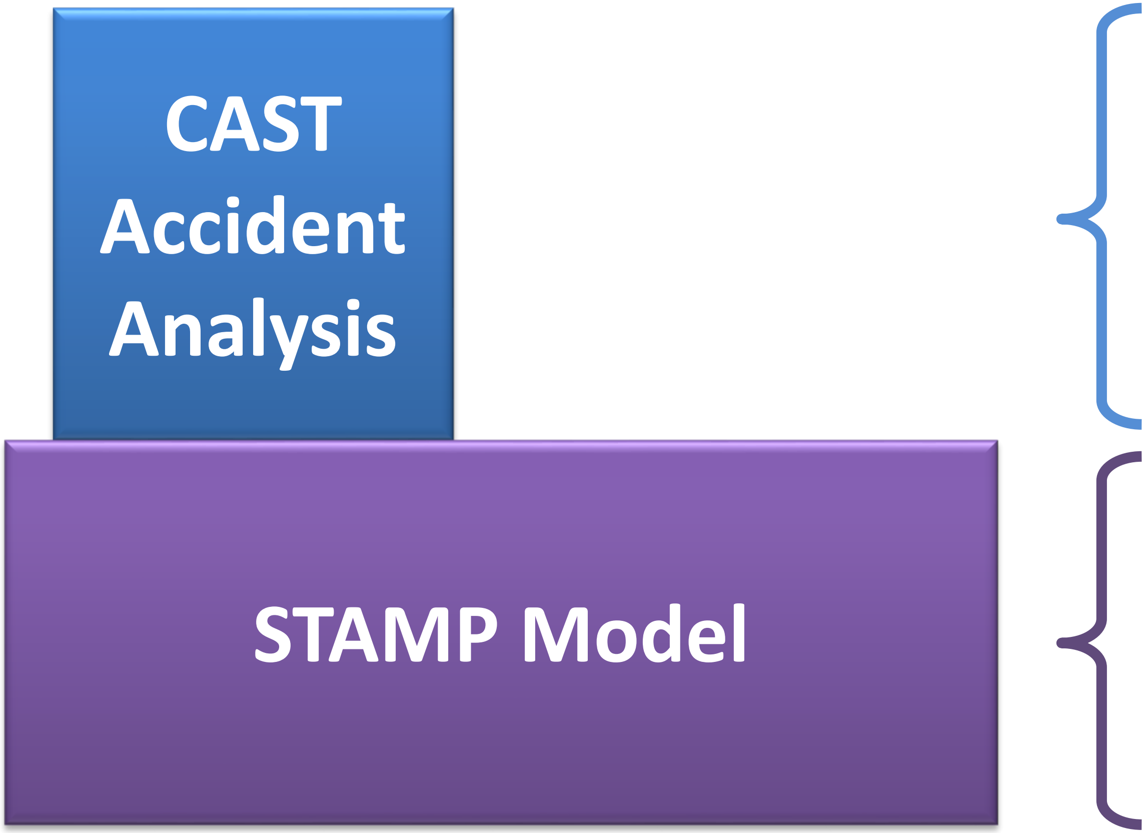
STAMP and STPA

STAMP Model

(Leveson, 2012)

Accidents are caused by inadequate control

STAMP and STPA



CAST Accident Analysis

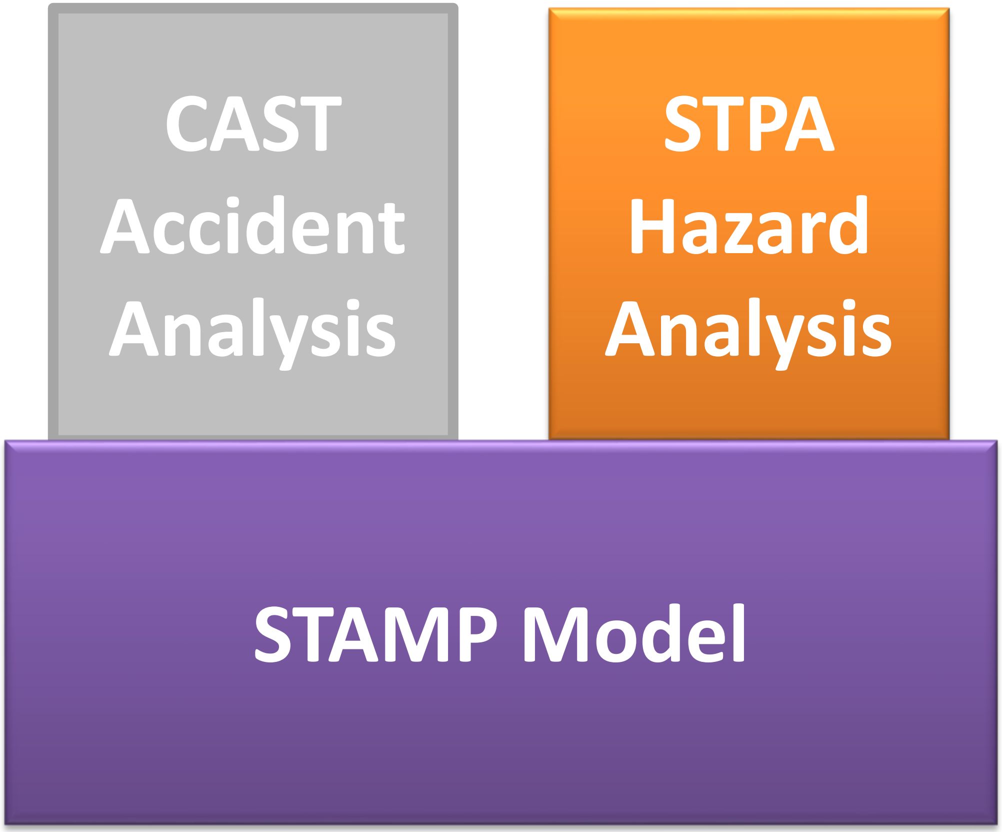
STAMP Model

How do we find inadequate control that caused the accident?

Accidents are caused by inadequate control

(Leveson, 2012)

STAMP and STPA



CAST
Accident
Analysis

STPA
Hazard
Analysis

STAMP Model

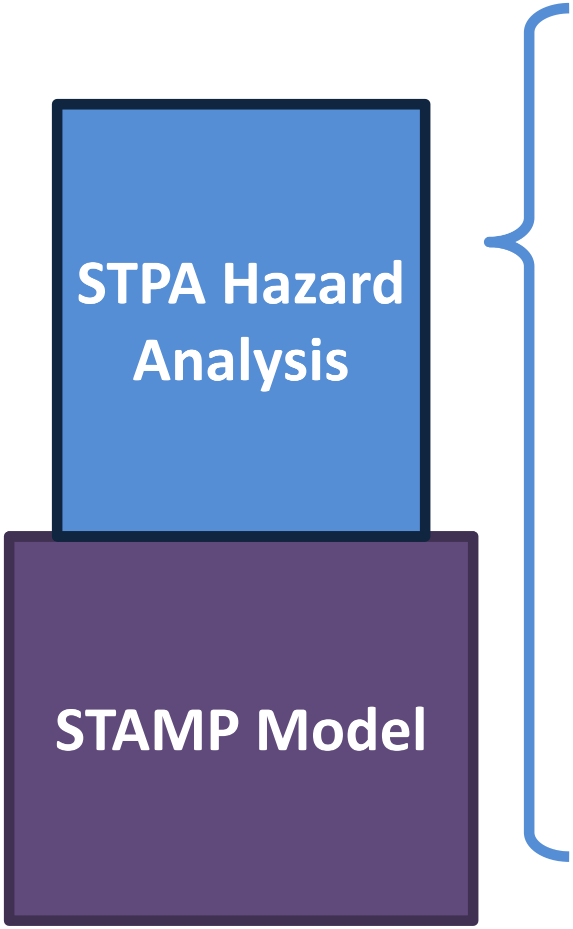
How do we find inadequate control in a design?

Accidents are caused by inadequate control

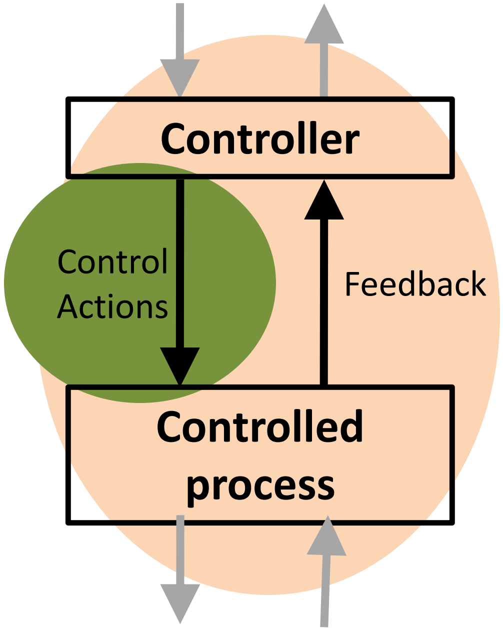
(Leveson, 2012)

STPA:
Systems Theoretic Process Analysis

STPA
(System-Theoretic Process Analysis)



- System engineering foundation
  - Define accidents, system hazards
  - Control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



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

- Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors **outside our control**
- Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

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

System Safety Constraints

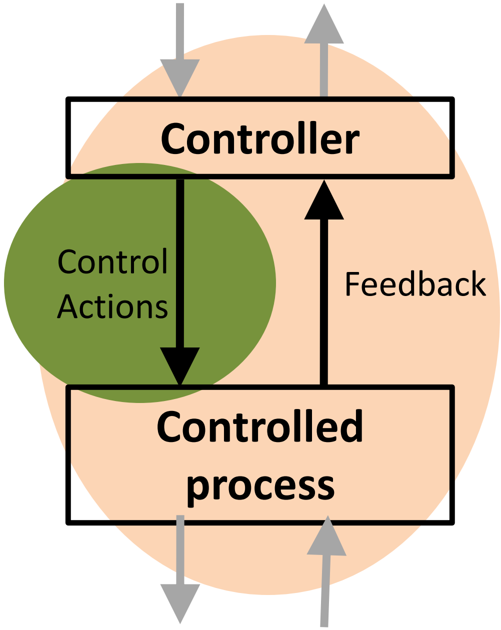
System Hazard		System Safety Constraint
Toxic chemicals from the plant are in the atmosphere	→	Toxic plant chemicals must not be released into the atmosphere
Nuclear power plant radioactive materials are not contained	→	Radioactive materials must not be released
Vehicles do not maintain safe distance 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

Aviation Examples

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

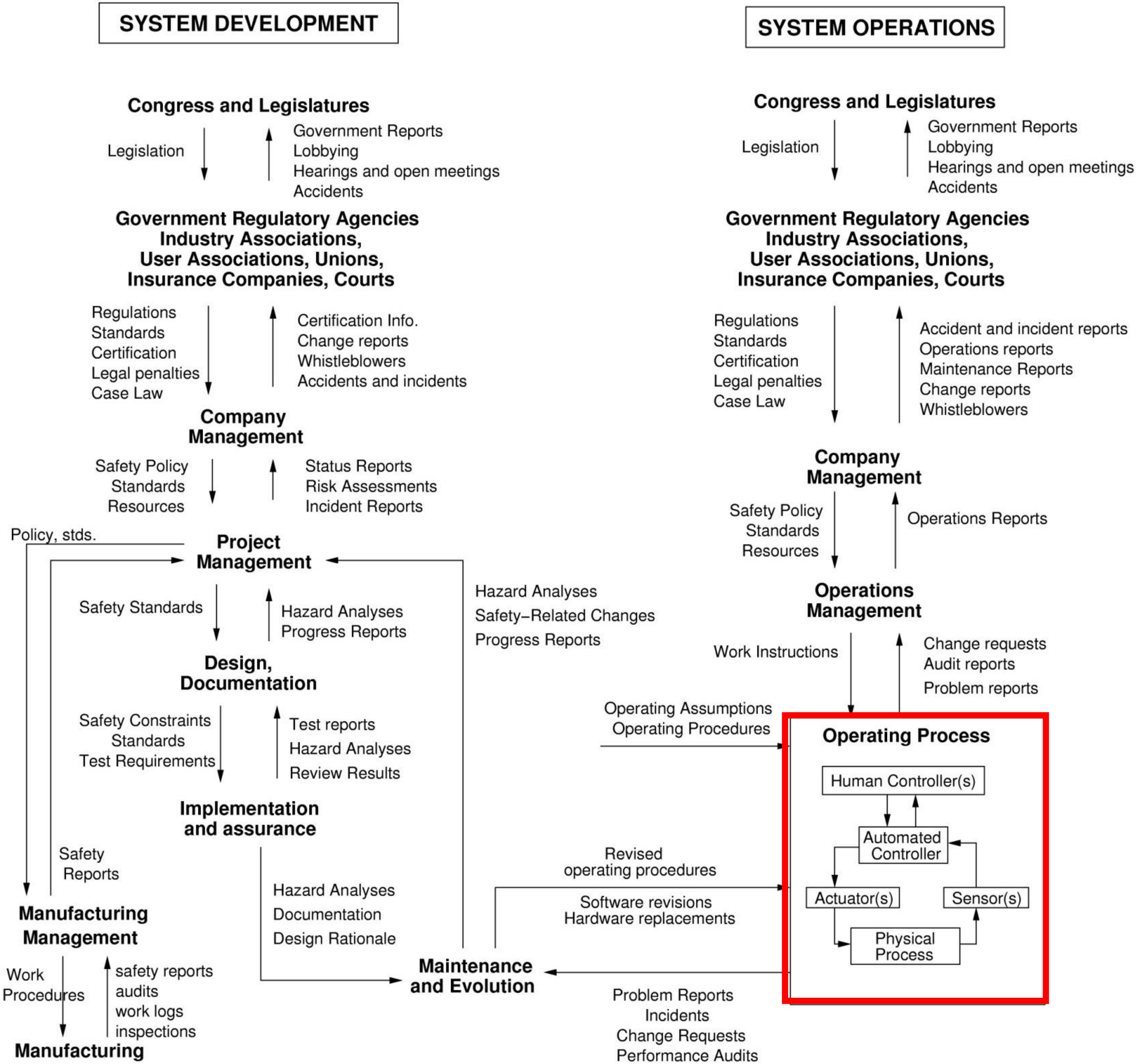
STPA
(System-Theoretic Process Analysis)

- System engineering foundation
  - ✓ Define accidents, system hazards
  - Control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



Control Structure Examples

Example 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

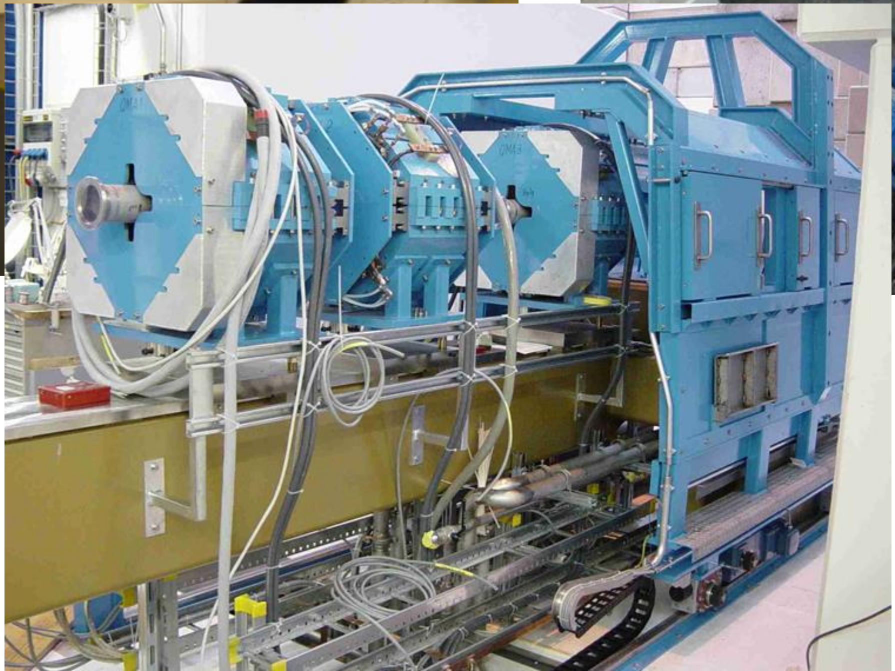
Problem Reports
Incidents
Change Requests
Performance Audits

(Leveson, 2012)

Proton Therapy Machine High-level Control Structure

Gantry

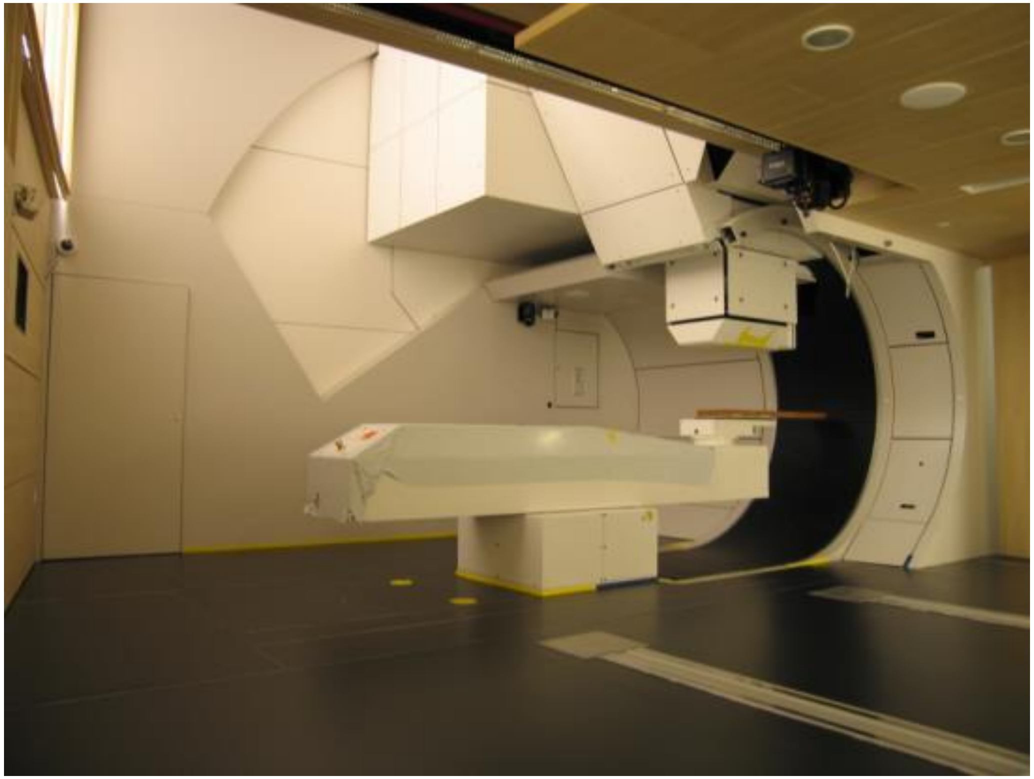
Cyclotron



Beam path and control elements

©

Proton Therapy Machine High-level Control Structure



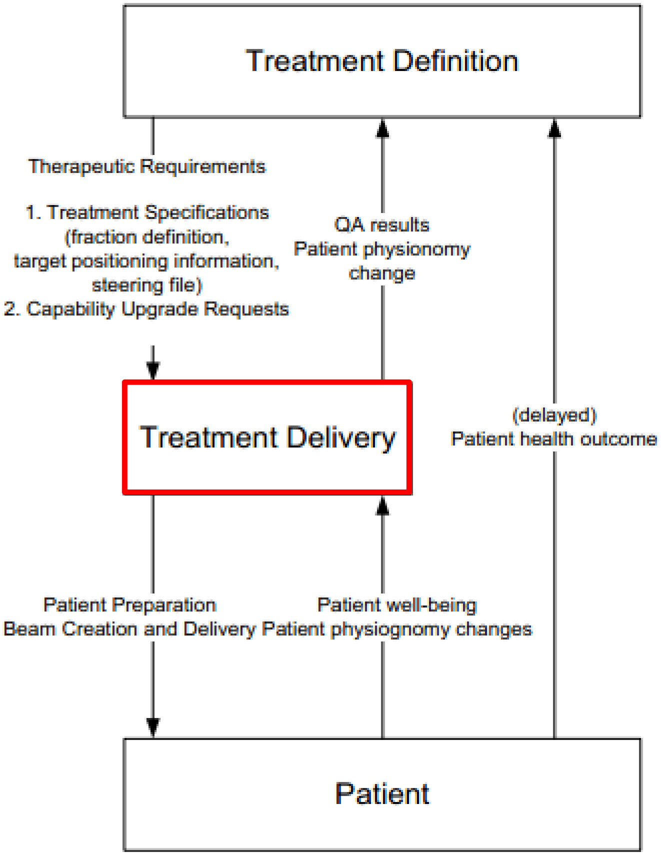
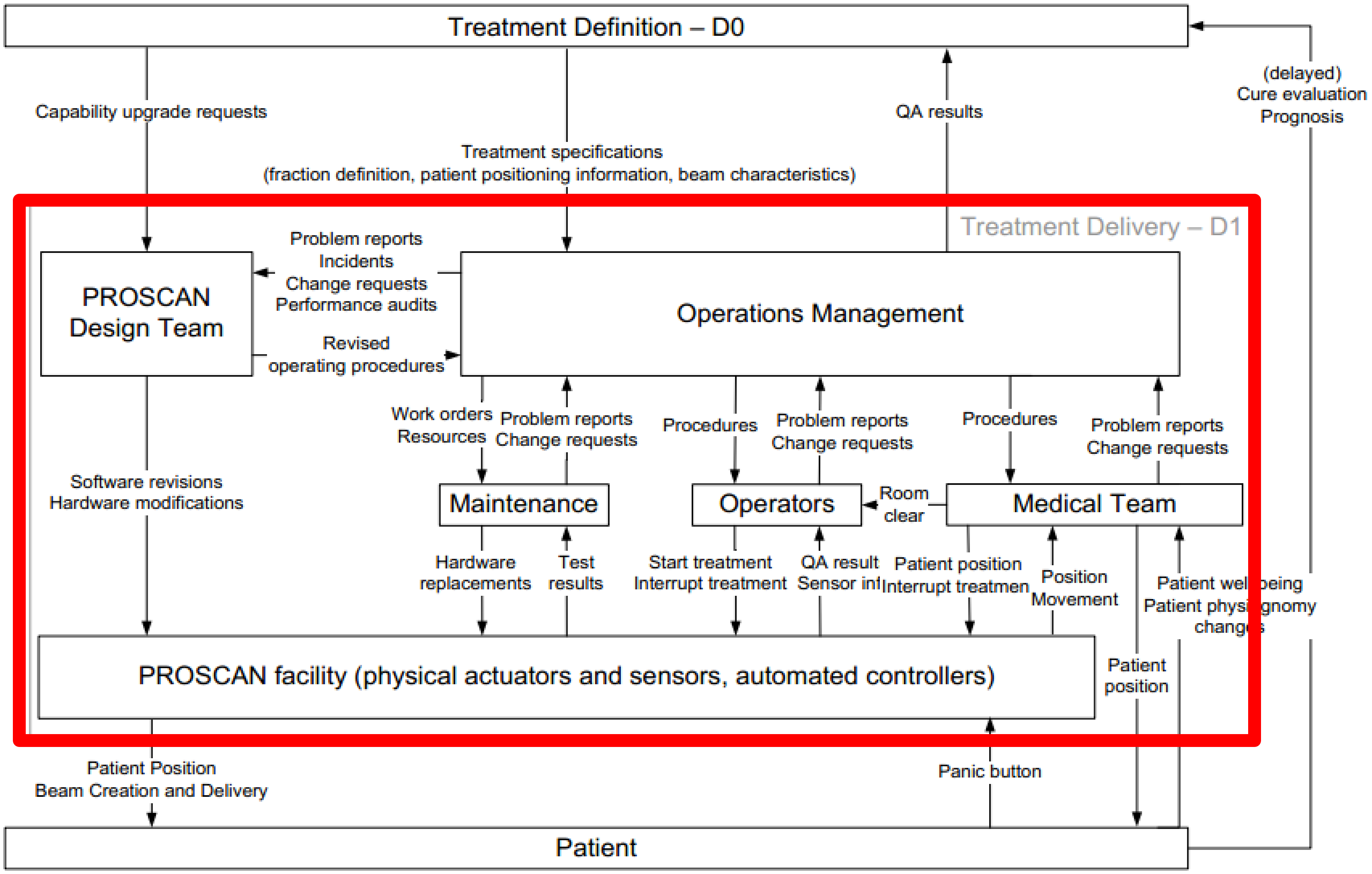

Treatment Definition
Therapeutic Requirements
1. Treatment Specifications (fraction definition, target positioning information, steering file)
2. Capability Upgrade Requests
QA results
Patient physionomy change
Treatment Delivery
(delayed) Patient health outcome
Patient Preparation
Beam Creation and Delivery
Patient well-being
Patient physiognomy changes
Patient

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

Antoine PhD Thesis, 2012

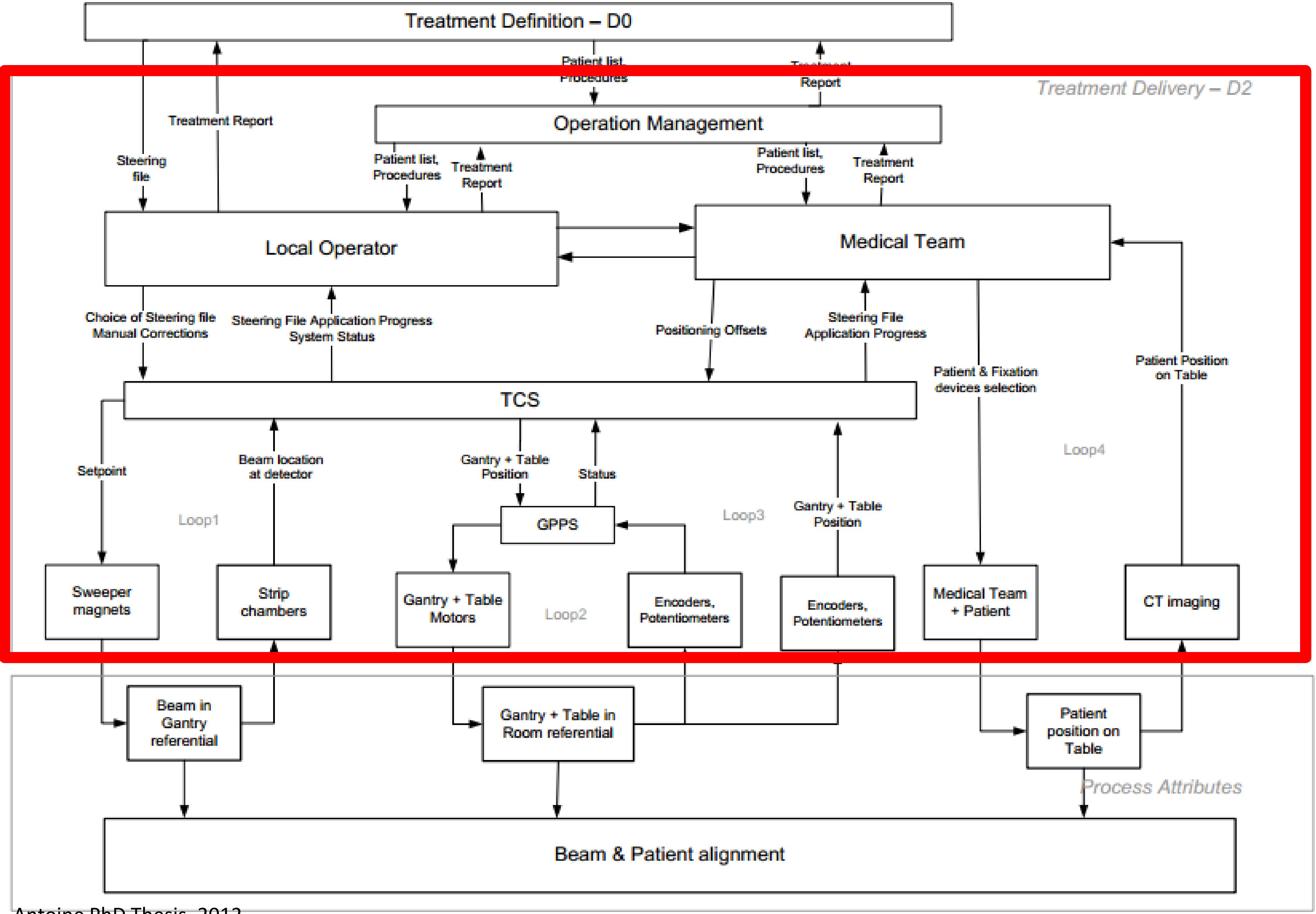
Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

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

Proton Therapy Machine Detailed Control Structure

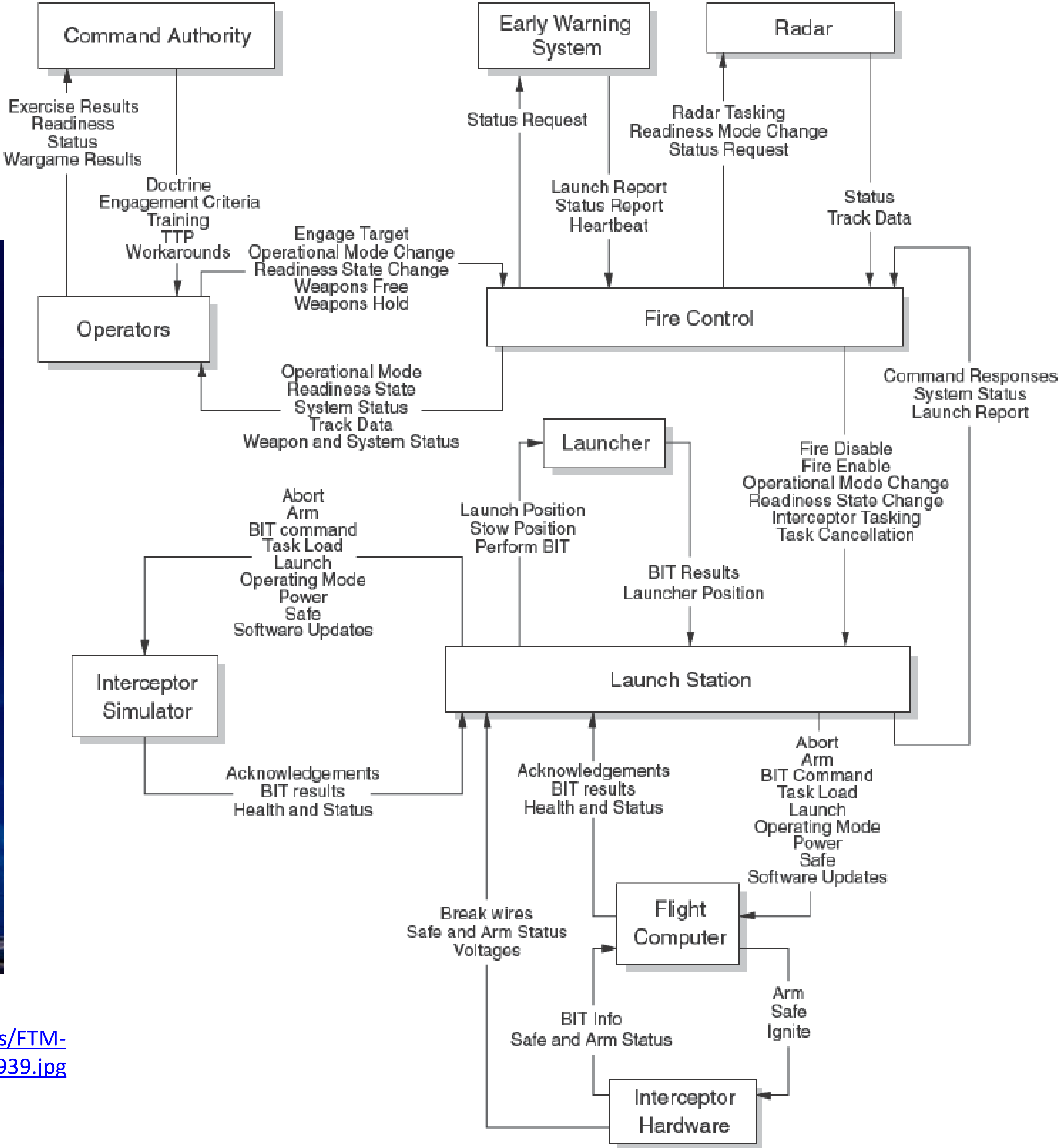


Antoine PhD Thesis, 2012

Ballistic Missile Defense System

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

Safeware Corporation



Adaptive Cruise Control

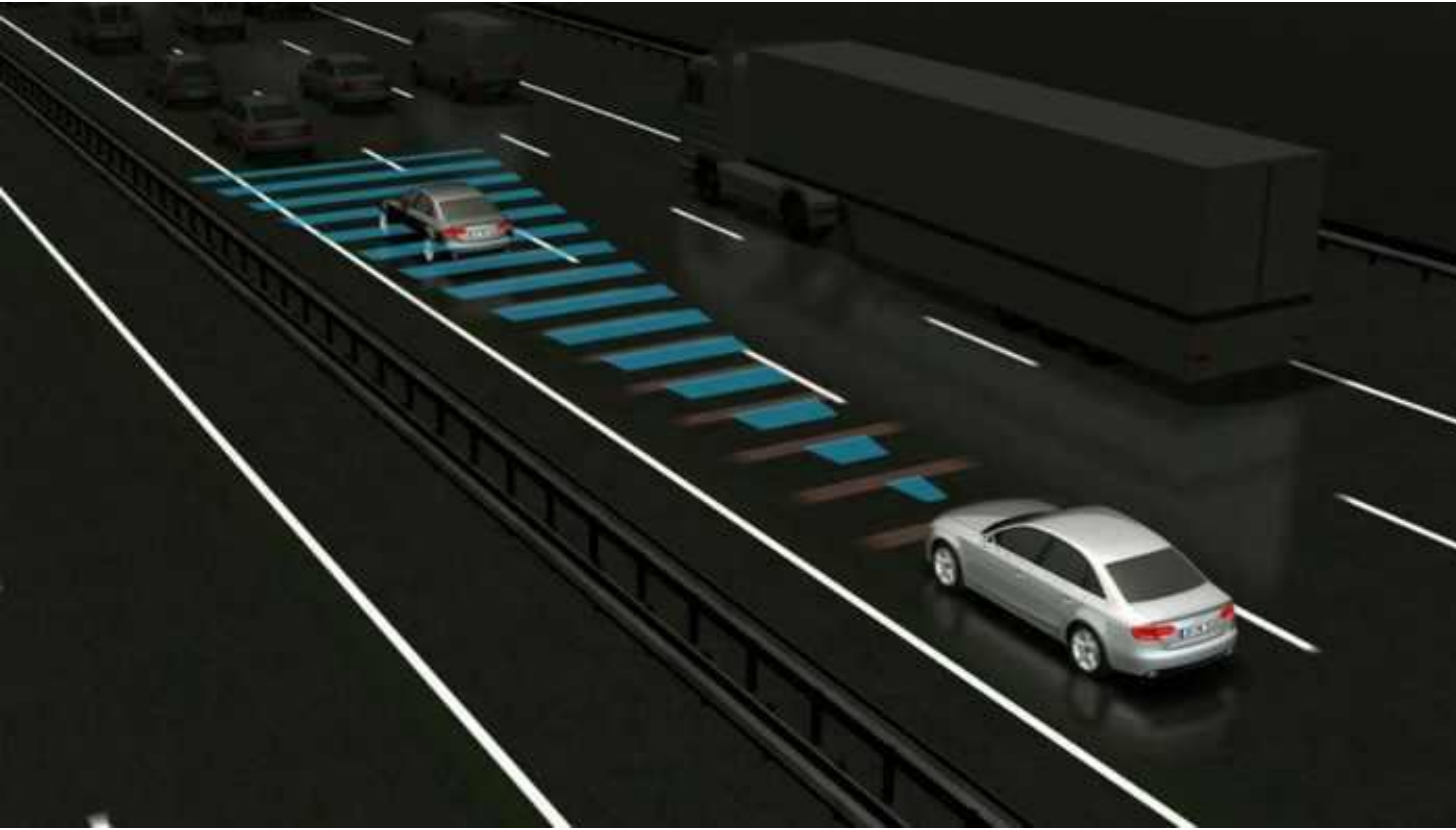
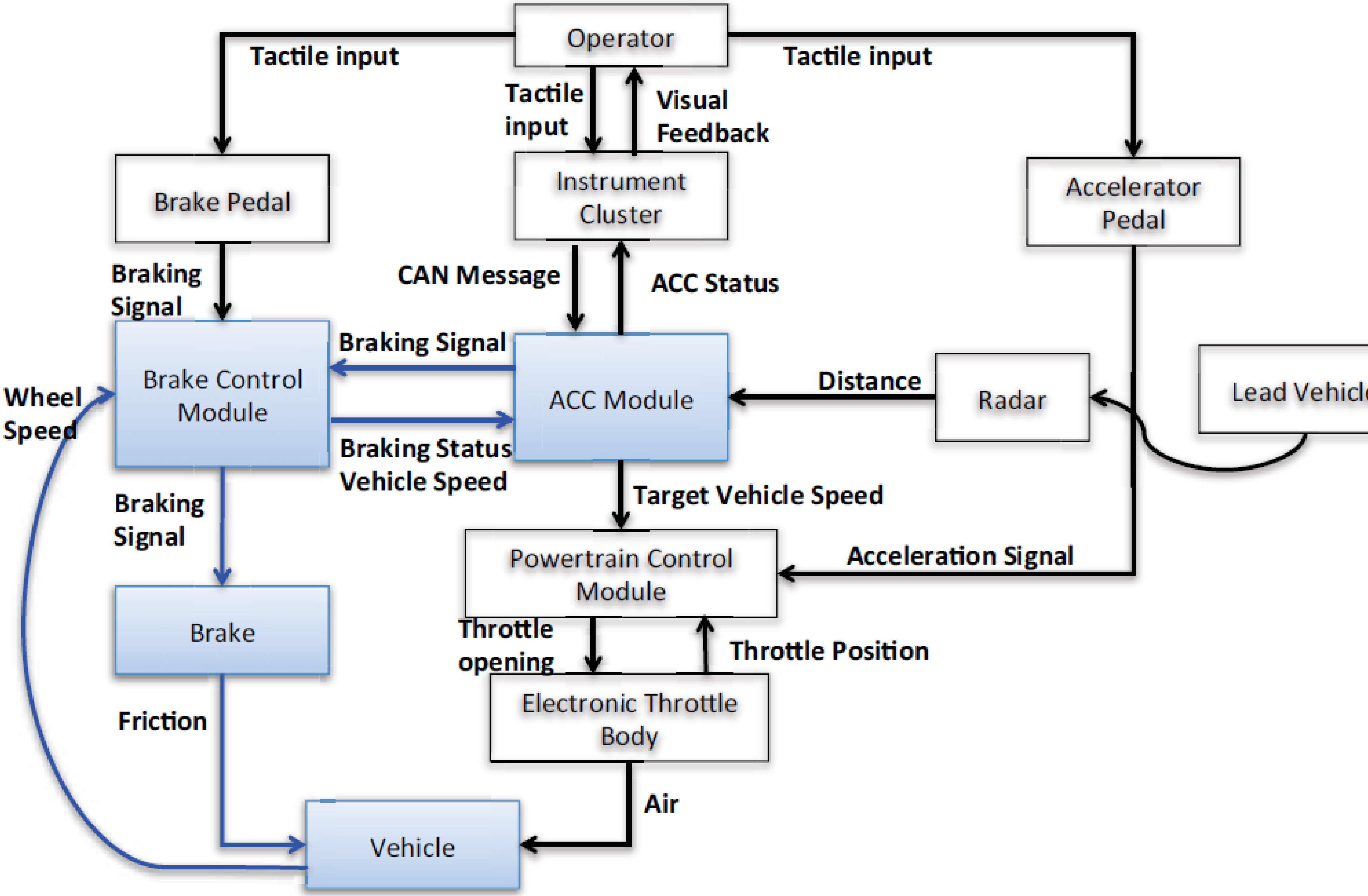
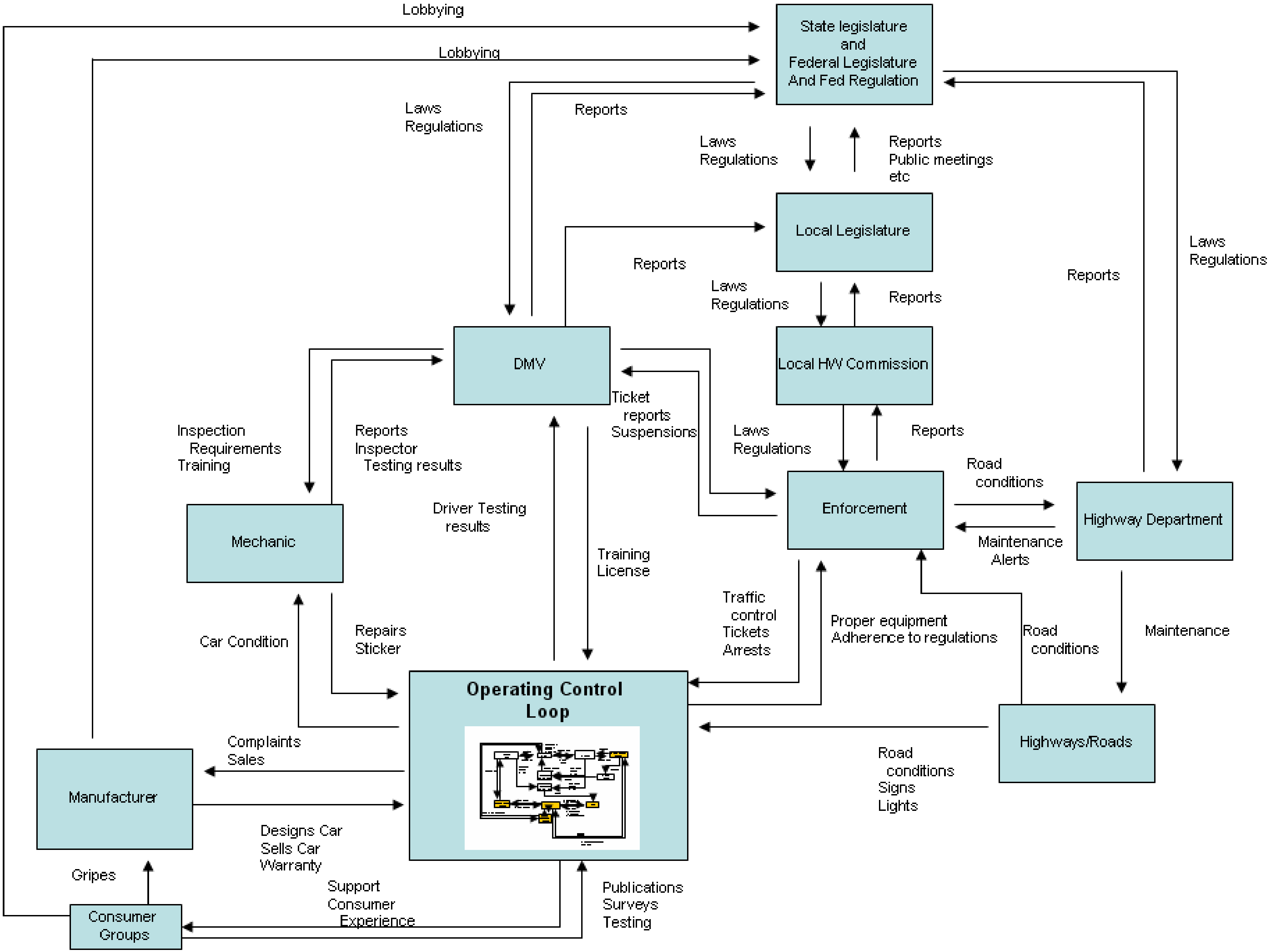


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

Example: ACC – BCM Control Loop



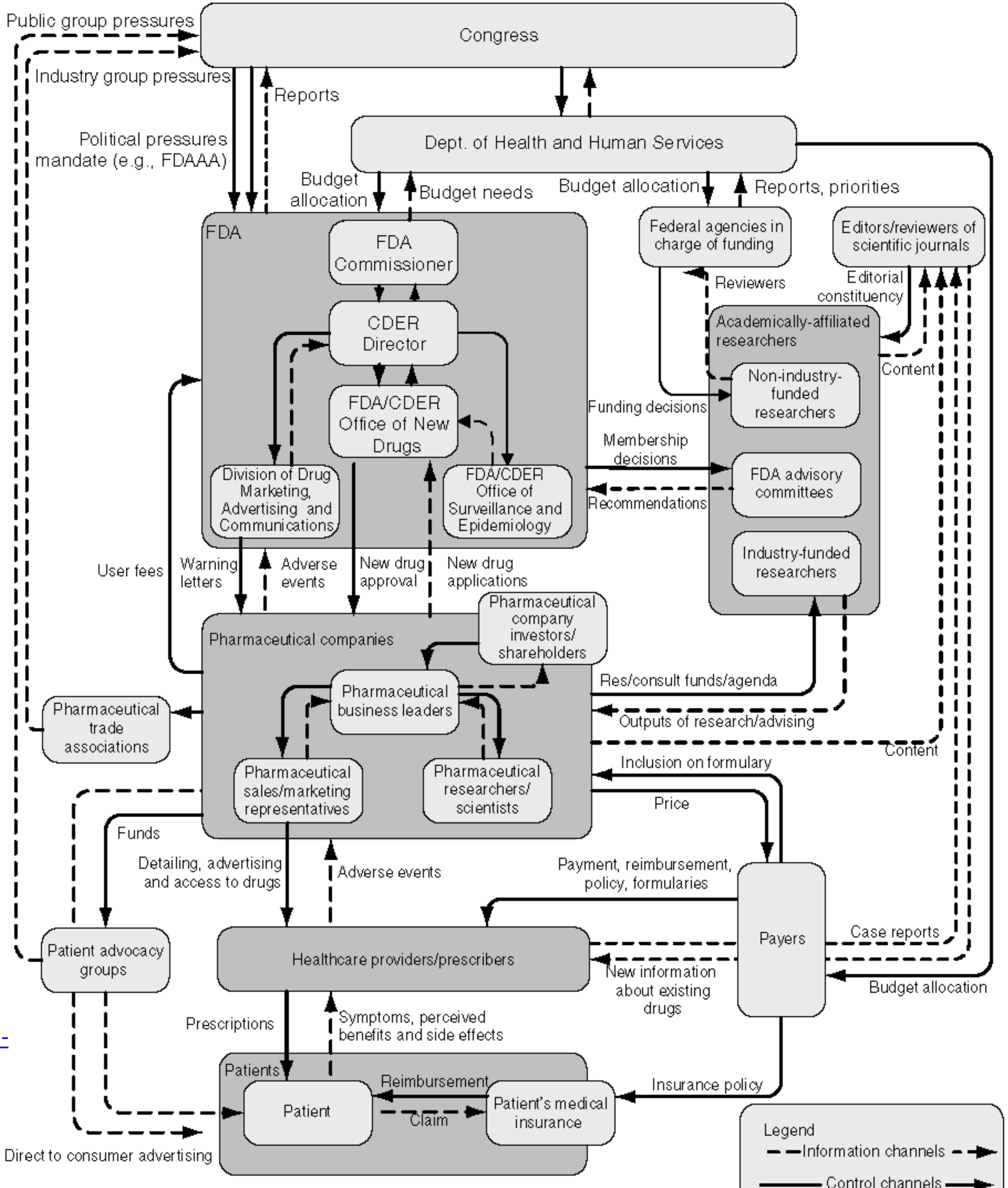
Qi Hommes


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

U.S. pharmaceutical safety control structure

(a purely human/organizational system)

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


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
Non-industry-funded researchers
Content
Funding decisions
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
Outputs of research/advising
Content
Pharmaceutical trade associations
Pharmaceutical sales/marketing representatives
Pharmaceutical researchers/ scientists
Inclusion on formulary
Price
Funds
Detailing, advertising and access to drugs
Adverse events
Payment, reimbursement, policy, formularies
Payers
Patient advocacy groups
Healthcare providers/prescribers
Case reports
New information about existing drugs
Budget allocation
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

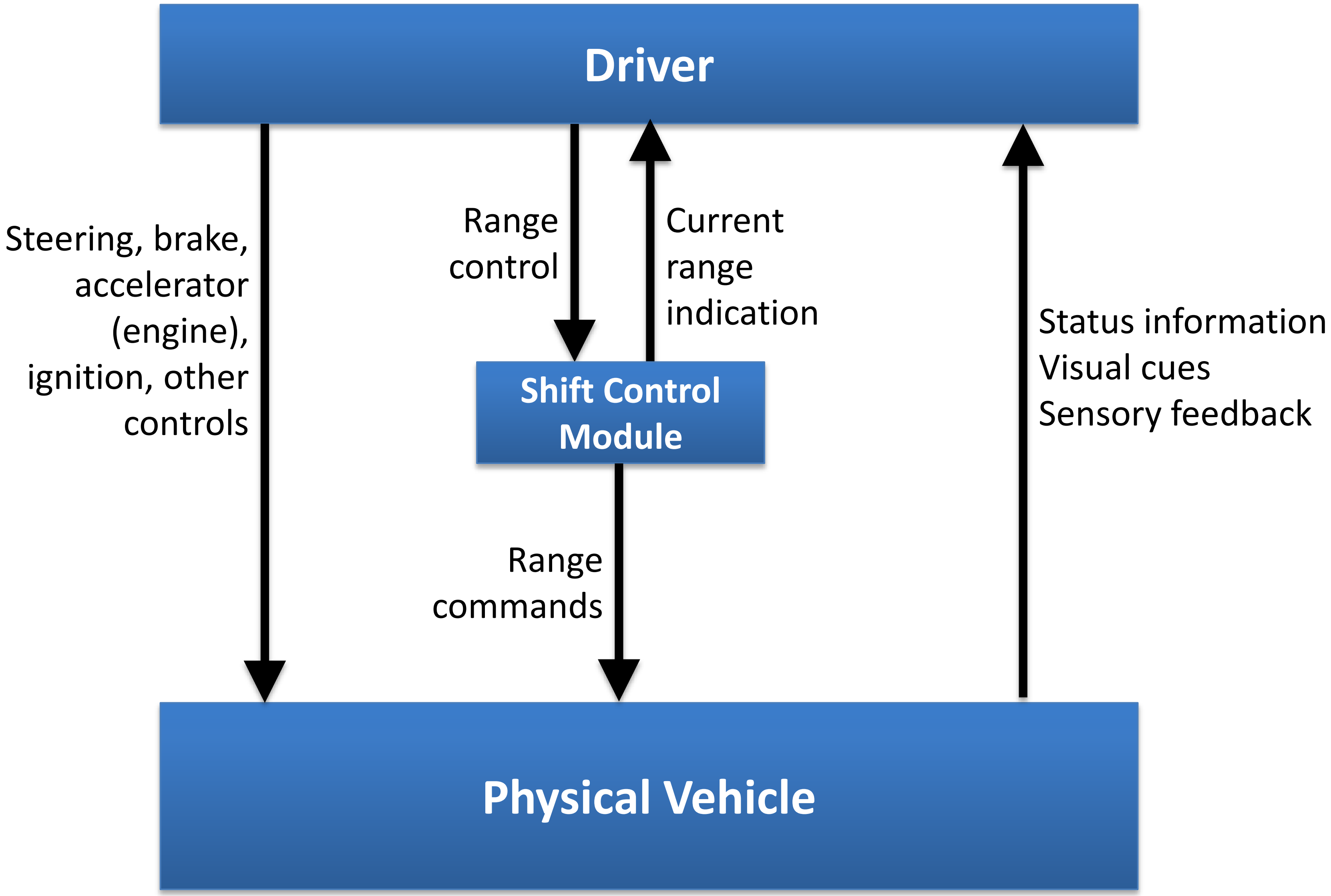
Leveson, Couturier, Thomas, Dierks, Wierz, Psaty, Finkelstein, Applying System Engineering to Pharmaceutical Safety

Automotive Shift By Wire

- The shift-by-wire concept replaces mechanical cables between the shifter and the transmission with an electronic lever, a computer, and electronic actuators. The computer senses the shift lever position and commands the actuator to achieve the appropriate transmission range.

Your turn:
Control structure?

Control structure: Initial Concept



Driver

Steering, brake, accelerator (engine), ignition, other controls

Range control

Current range indication

Status information
Visual cues
Sensory feedback

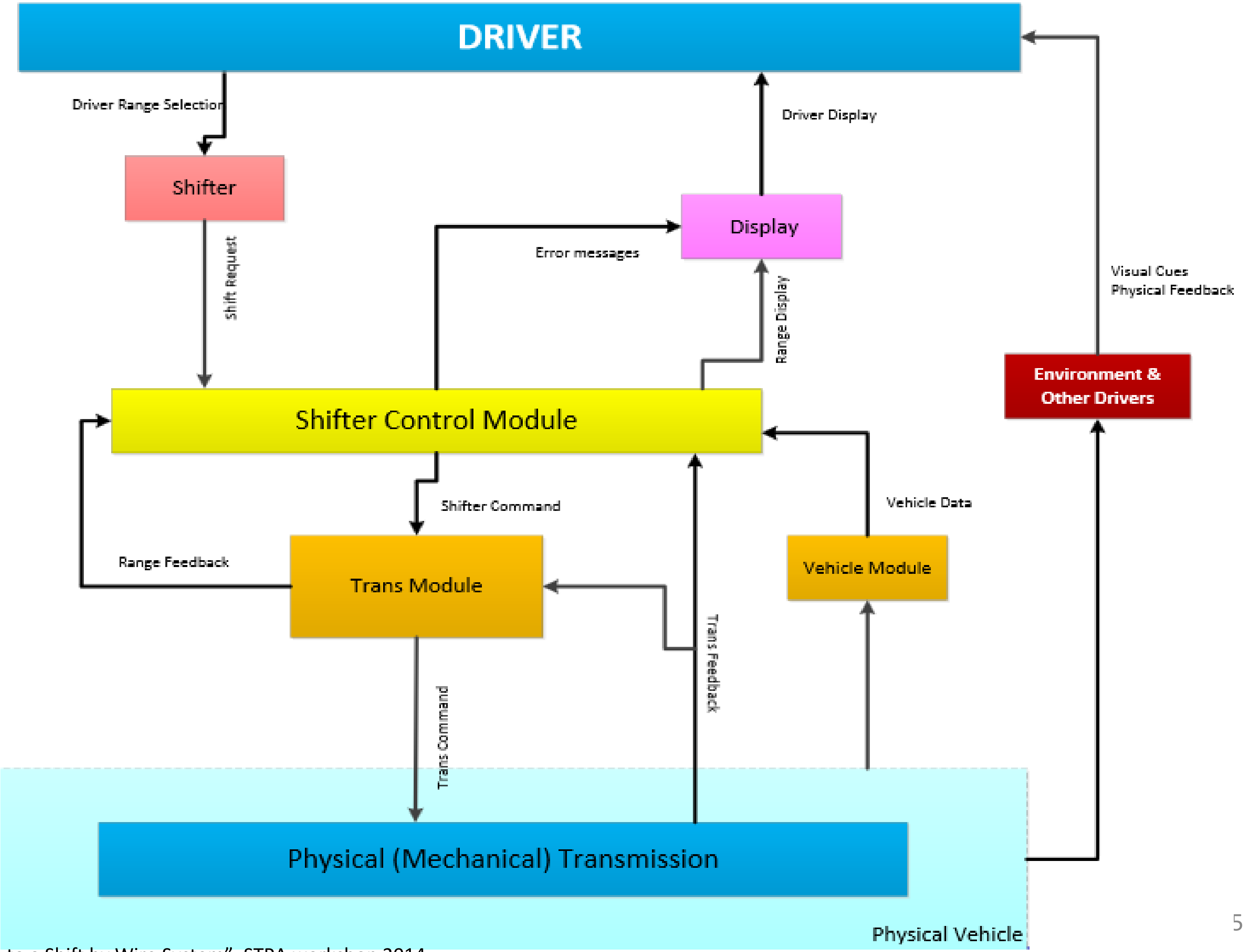
Shift Control Module

Range commands

Physical Vehicle

*Similar for both mechanical/electrical implementations

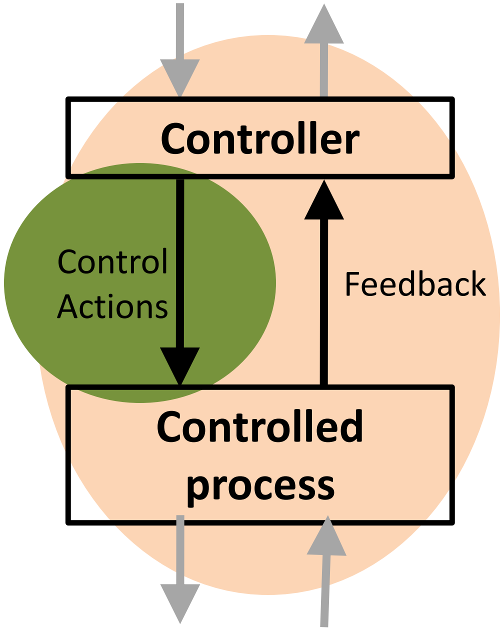
Control Structure: Refined



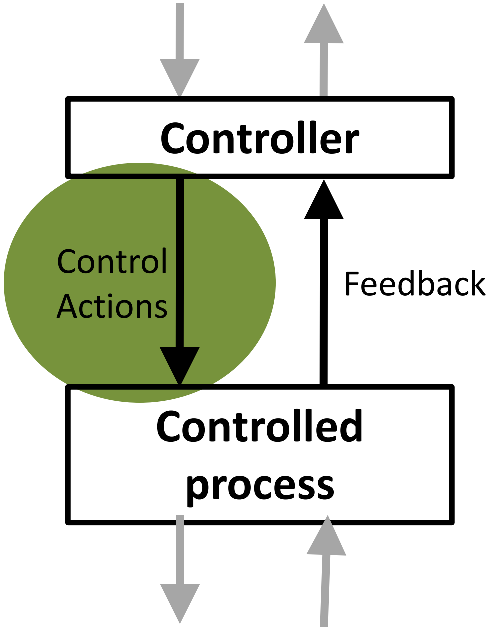
"Application of STPA to a Shift by Wire System", STPA workshop 2014

STPA
(System-Theoretic Process Analysis)

- ✓ System engineering foundation
  - Define accidents, hazards, constraints
  - Control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



STPA Step 1: Unsafe Control Actions (UCA)

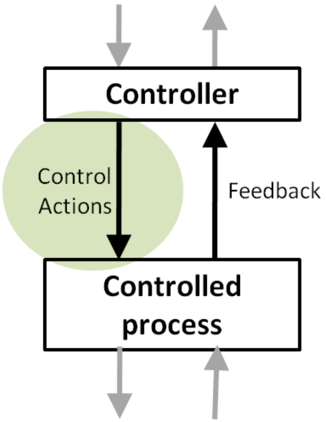


4 ways unsafe control may occur:

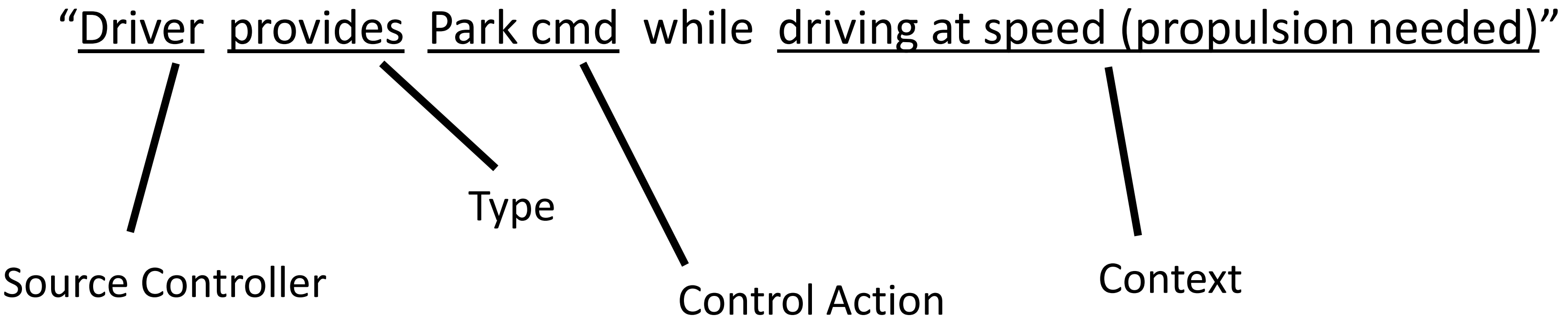
- A control action required for safety is not provided or is not followed
- An unsafe control action is provided that leads to a hazard
- A potentially safe control action provided too late, too early, or out of sequence
- A safe control action is stopped too soon or applied too long (for a continuous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

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Shifter Command	?	?	?	?

Structure of an Unsafe Control Action



Example:



"Driver provides Park cmd while driving at speed (propulsion needed)"

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)

(Thomas, 2013)

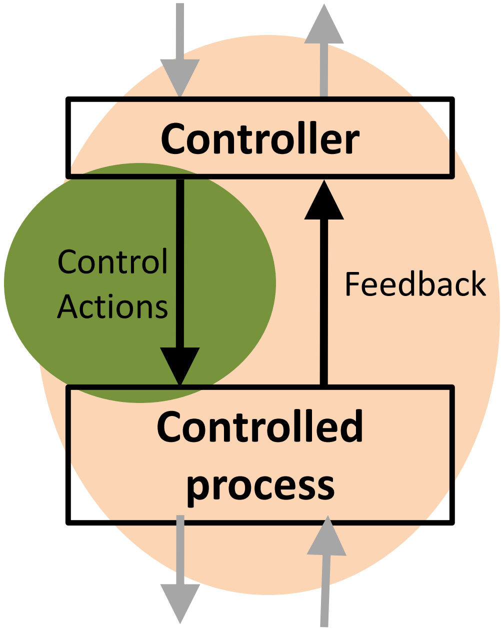
©

UCAs → Safety Constraints

Unsafe Control Action		Safety Constraint
	➡	
	➡	
	➡	
	➡	

STPA
(System-Theoretic Process Analysis)

- ✓ System engineering foundation
  - Define accidents, hazards, constraints
  - Control structure
- ✓ Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



©

STPA Step 2: Identify Causal Scenarios

- Select an Unsafe Control Action

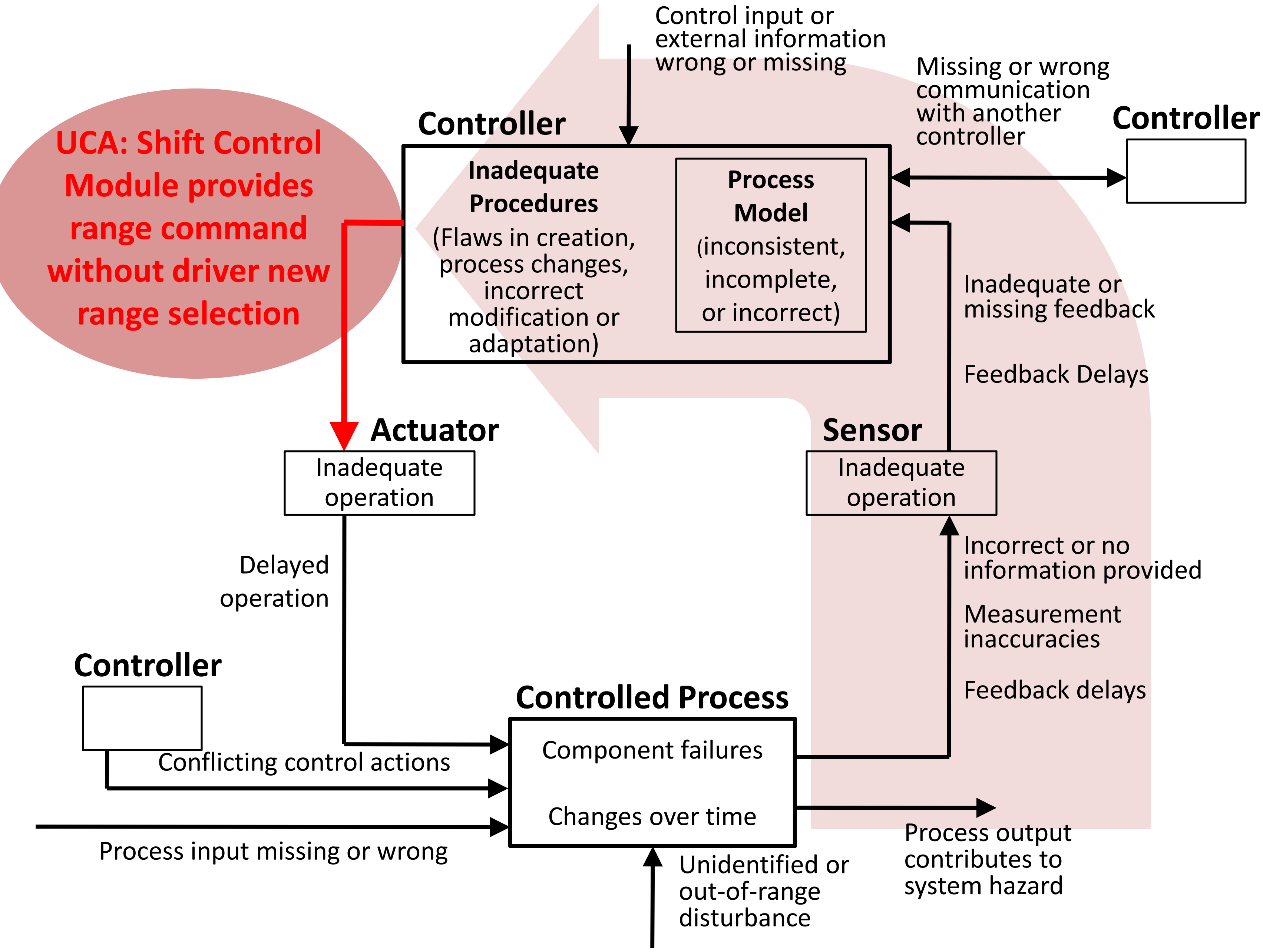
A. Identify what might cause it to happen

- Develop accident scenarios
- Identify controls and mitigations

B. Identify how control actions may not be followed or executed properly

- Develop causal accident scenarios
- Identify controls and mitigations

Step 2A: Potential causes of UCAs



UCA: Shift Control Module provides range command without driver new range selection

Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller
Inadequate Procedures
(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
Delayed operation
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

©

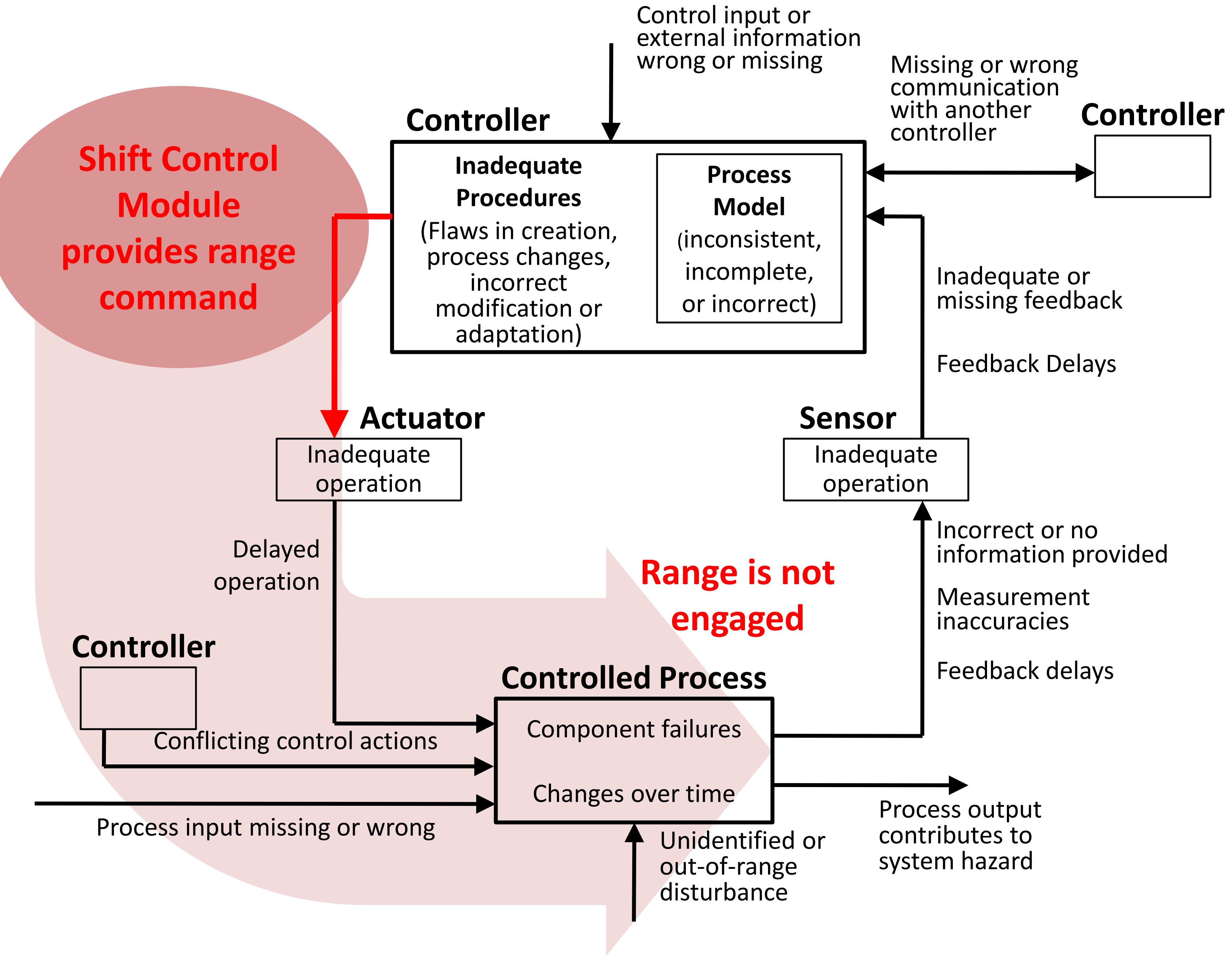
STPA Step 2: Identify Causal Scenarios

- Select an Unsafe Control Action

A. Identify what might cause it to happen
   - Develop accident scenarios
   - Identify controls and mitigations

B. Identify how control actions may not be followed or executed properly
   - Develop causal accident scenarios
   - Identify controls and mitigations

Step 2B: Potential control actions not followed


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Shift Control Module provides range command
Inadequate Procedures
(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
Delayed operation
Range is not engaged
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

©

How does STPA compare?

- MIT: TCAS
  - Existing high quality fault tree done by MITRE for FAA
  - MIT comparison: STPA captured everything in fault tree, plus more
- JAXA: HTV
  - Existing fault tree reviewed by NASA
  - JAXA comparison: STPA captured everything in fault tree, plus more
- EPRI: HPCI/RCIC
  - Existing fault tree & FMEA overlooked causes of real accident
  - EPRI comparison: Blind study, only STPA found actual accident scenario
- NRC: Power plant safety systems
  - Proposed design that successfully completed Final Safety Analysis Report
  - STPA found additional issues that had not been considered
- Safeware: U.S. Missile Defense Agency BMDS
  - Existing hazard analysis per U.S. military standards
  - Safeware comparison: STPA captured existing causes plus more
  - STPA took 2 people 3 months, MDA took 6 months to fix problems
- Automotive: EPS
  - Compare STPA results to FMECA using SAE J1739
- MIT: NextGen ITP
  - Existing fault tree & event tree analysis by RTCA
  - MIT comparison: STPA captured 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