

STAMP/STPA

Beginner Introduction

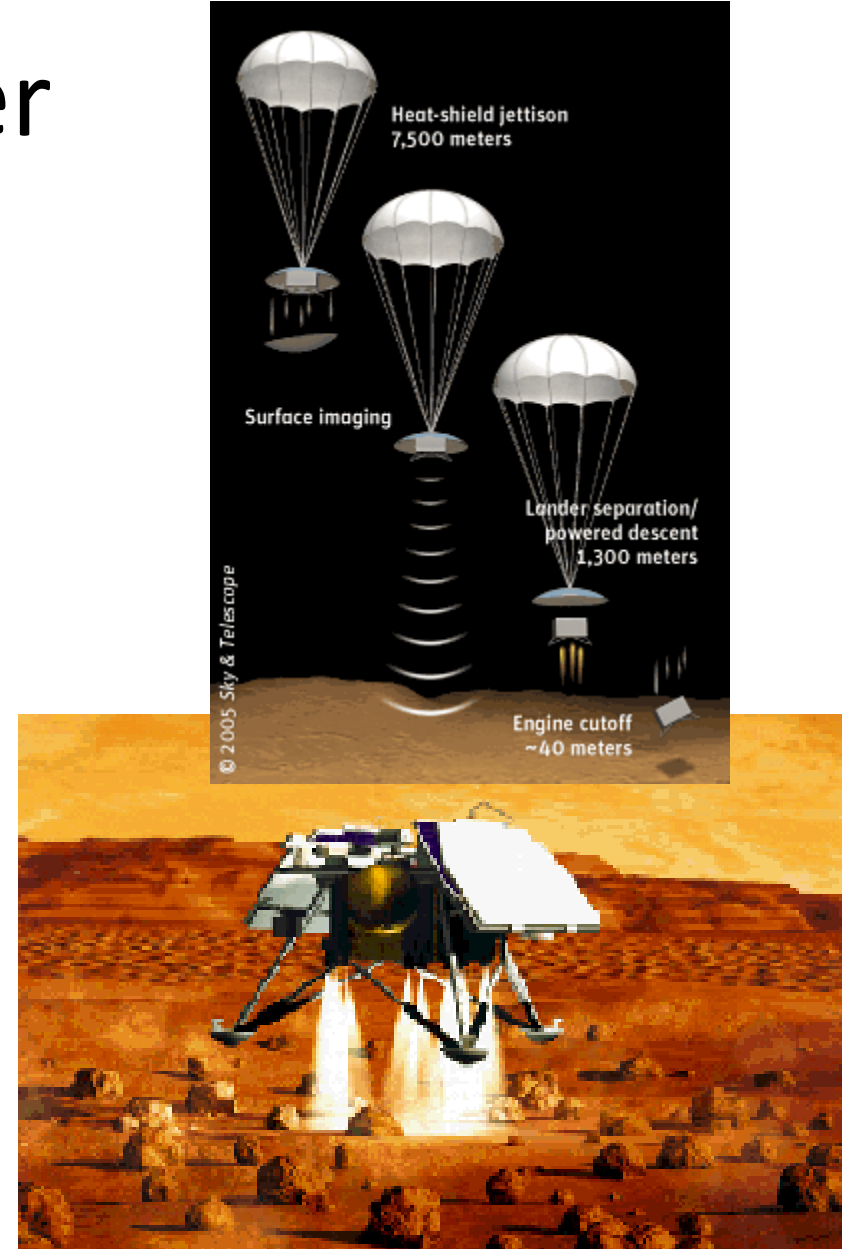
Dr. John Thomas
System Engineering Research Laboratory
Massachusetts Institute of Technology

Agenda

- Beginner Introduction
 - What problems are we solving?
 - How does STAMP/STPA solve those problems?
 - Simple STAMP/STPA examples
- Intermediate tutorial
 - Guided exercise: Apply STPA to a real system
- Research presentation
 - Recent STPA research results

Mars Polar Lander

- During the descent to Mars, the legs were deployed at an altitude of 40 meters.
- Touchdown sensors (on the legs) sent a momentary signal
- The software responded as it was required to: by shutting down the descent engines.
- The vehicle free-fell and was destroyed upon hitting the surface at 50 mph.



**No component failed!
All components performed exactly as designed!**

Boeing 787 Lithium Battery Fires

- 2013 – 2014
- Reliability analysis predicted 10 million flight hours between battery failures
 - Two fires caused by battery failures in 52,000 flight hours
 - Does not include 3 other less-reported incidents of smoke in battery compartment

Just a simple component failure?



Boeing 787 Lithium Battery Fires

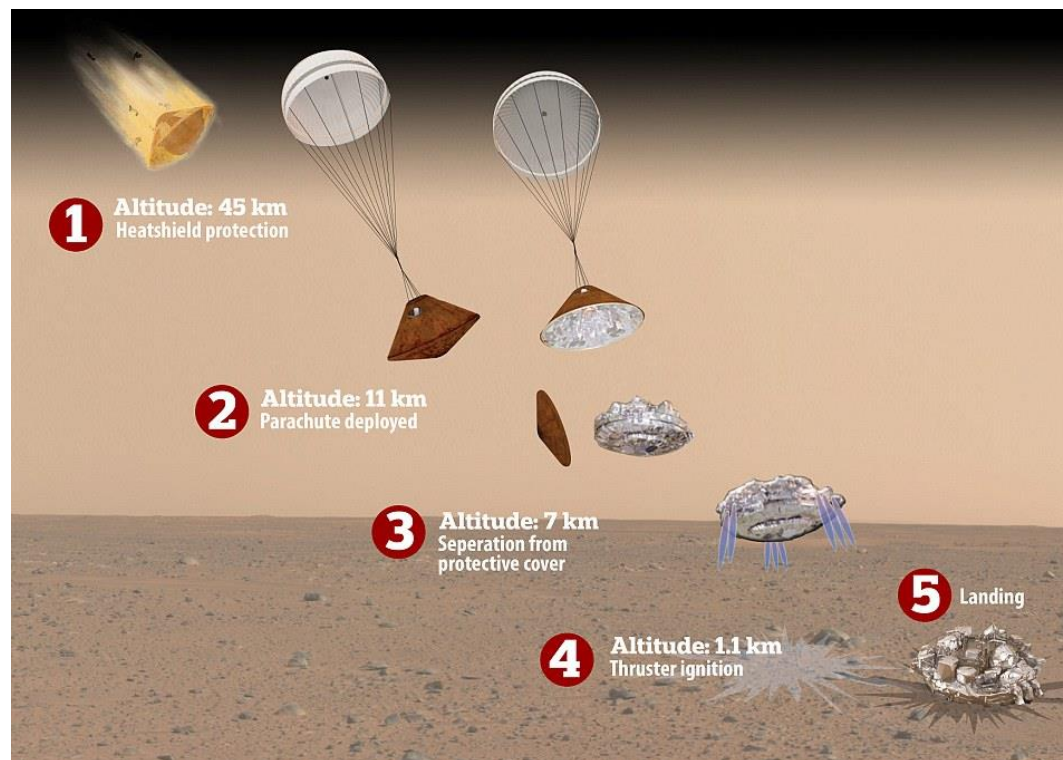
- A module monitors for smoke in the battery bay, controls fans and ducts to exhaust smoke overboard.
- Power unit experienced low battery voltage, shut down various electronics including ventilation.
- Smoke could not be redirected outside cabin



**All software requirements were satisfied!
The requirements were inadequate**

Schiaparelli Lander (2016)

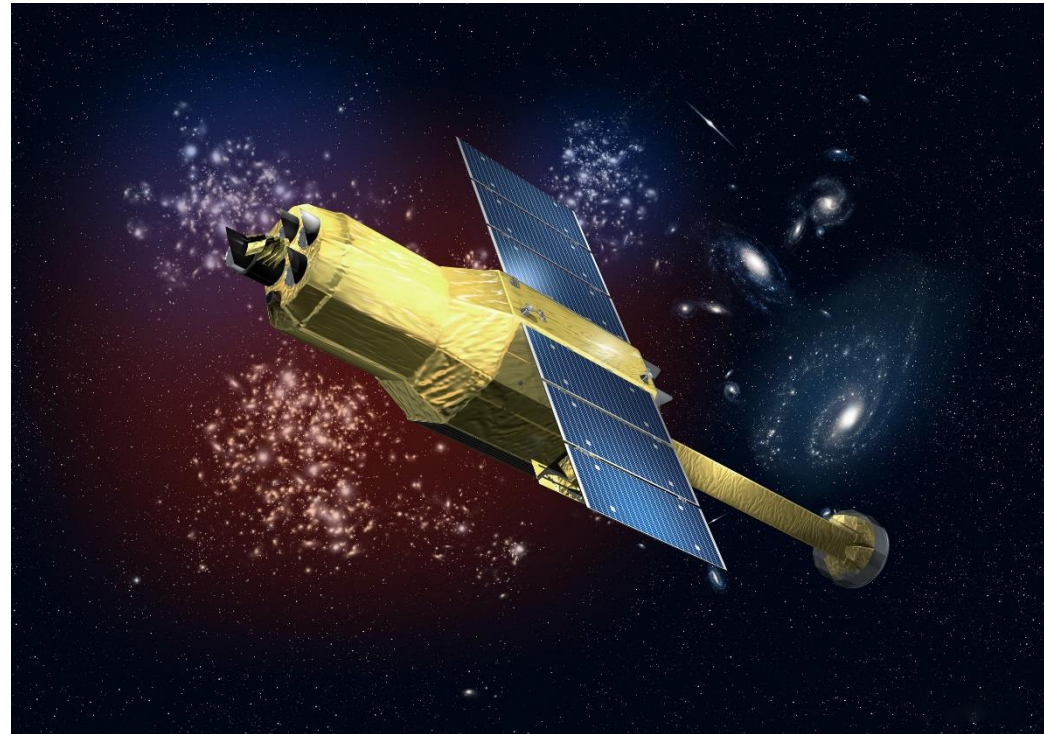
- 11km: Parachute deployed
- 3.7km: IMU saturated
 - Negative altitude calculated
 - Parachute jettisoned
 - Thrusters off
- Impact at 300 km/h (186 mph)
 - Designed to withstand 10 km/h



All components operated as designed!
No component failure!

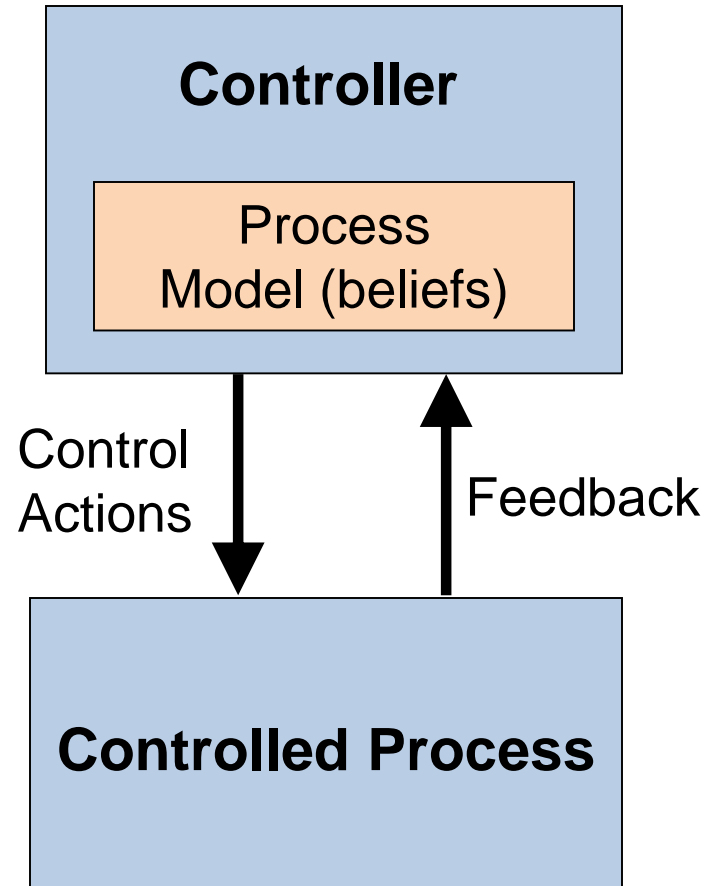
HITOMI Satellite (2016)

- Unable to detect bright stars for reference
- Parameters for Safe Hold Mode were incorrect
- Investigative subcommittee
 - Need for “approach to examine the overall design of the spacecraft”
- JAXA
 - “We were unable to let go of our usual methods”



All components operated as designed!
Not a simple component failure!

Basic Control Theory



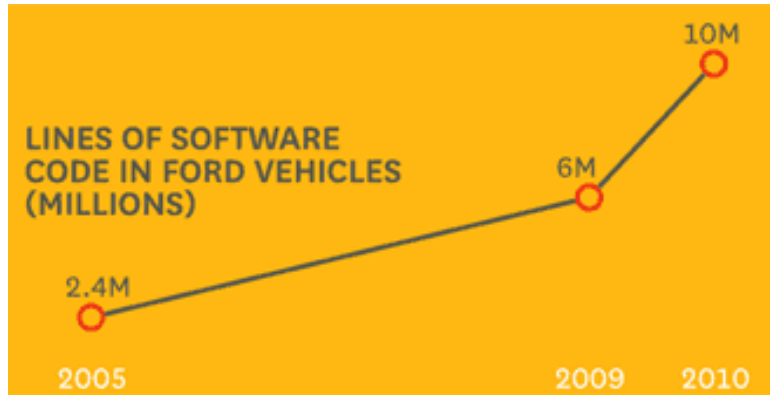
- Provides another way to think about accidents
- Forms foundation for STAMP/STPA

Problems with Software

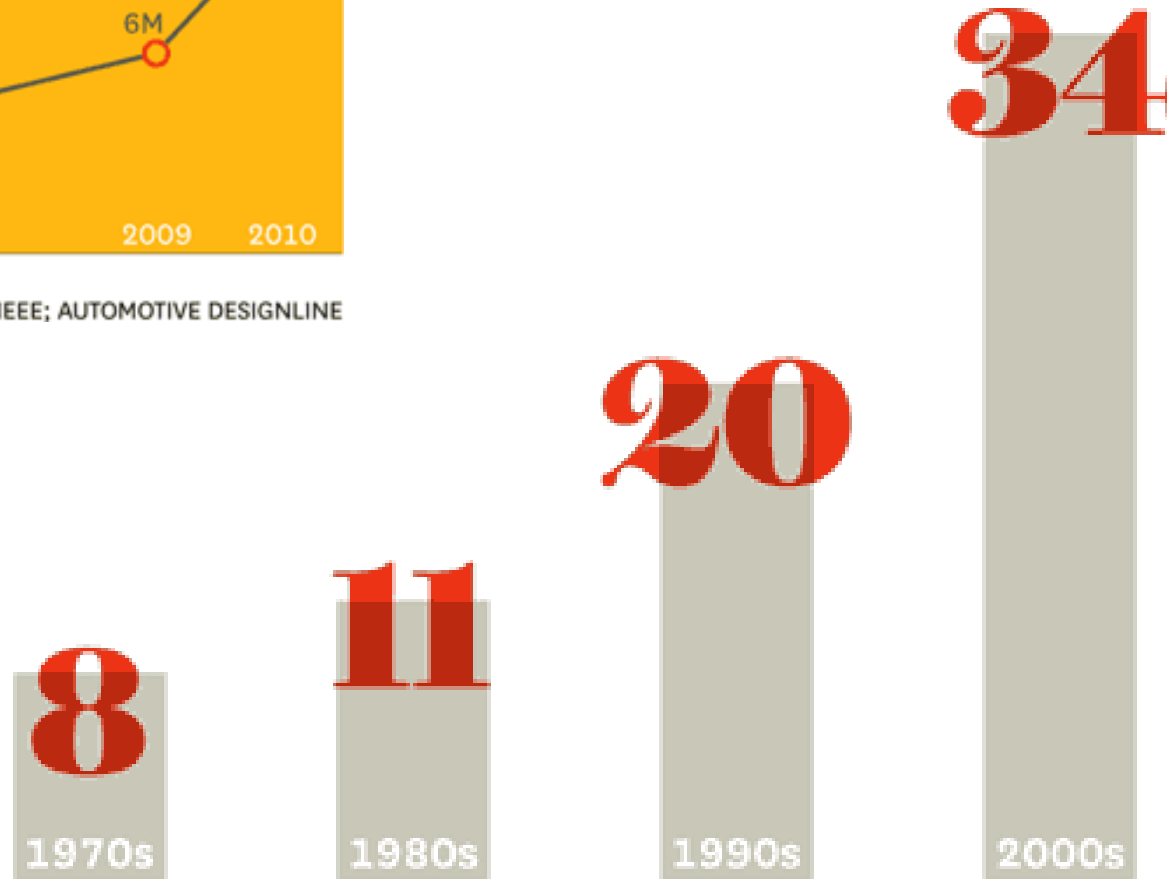
Quote

- “The hardest single part of building a software system is deciding precisely what to build.”
-- Fred Brooks, *The Mythical Man-Month*

Automotive recalls rapidly increasing!



SOURCES IEEE; AUTOMOTIVE DESIGNLINE



SOURCES BLOOMBERG; NHTSA

2013 Ford Fusion / Escape

- Engine fires
 - 13 reports of engine fire
 - Short time frame
 - (~Sept - Dec)
- Owners asked to “park their vehicles until further notice”
- 99,153 brand new vehicles affected

YAHOO!
AUTOS

Search Autos

Ford tells 89,000 Escape, Fusion owners to park cars because of engine fire risk



By Justin Hyde
November 30, 2012 6:03 PM
Motoramic



In a recall with few precedents, Ford warned today that 89,193 owners of brand new 2013 Ford Escape SUVs and Ford Fusions with 1.6-liter turbocharged engines should park their vehicles until further notice due to risk of engine fires -- and gave no estimate of when it would have a repair.

*Images from:

<https://autos.yahoo.com/blogs/motoramic/ford-tells-89-000-escape-fusion-owners-park-230316605.html>

<http://gearheads.org/stop-driving-your-ford-escape/>

The Problem

- Ford press release:
 - “The original cooling system design was not able to address a loss of coolant system pressure under certain operating conditions, which could lead to a vehicle fire while the engine was running.”
- Ford VP:
 - “We had a sequence of events that caused the cooling system software to restrict coolant flow,” he says. Most of the time, that would not be a problem and is the intended behavior. But in rare cases the coolant pressure coupled with other conditions may cause the coolant to boil. When the coolant boils, the engine may go into extreme overheating causing more boiling and rapid pressure increase. This caused coolant leaks near the hot exhaust that led to an engine fire.
 - Ford has seen 12 fires in Escapes and one in a Fusion.

Quotes from:

<http://corporate.ford.com/news-center/press-releases-detail/pr-ford-produces-fix-in-voluntary-37491>

<http://www.usatoday.com/story/money/cars/2012/12/10/ford-recall-escape-fusion-ecoboost/1759063/>

Quote

- “Almost all software-related accidents can be traced back to flaws in the requirements specification”

-- *Prof. Nancy Leveson, MIT*

These problems can pass every component and subsystem test, every simulation, and every verification effort!

Toyota to pay \$1.2B settlement in vehicle acceleration lawsuit

By [Bob Fredericks](#) and Post Wires

March 19, 2014 | 9:19am



Toyota Unintended Acceleration

- **2004-2009:** 102 incidents



Toyota Unintended Acceleration

- **2004:** Push-button ignition
- **2004-2009**
 - 102 incidents of uncontrolled acceleration
 - Speeds exceed 100 mph despite stomping on the brake
 - 30 crashes
 - 20 injuries
- **Today**
 - Software fixes for pushbutton ignition, pedals



**Pushbutton was reliable, Software was reliable.
All component requirements were met.
Overall system unsafe, unexpected!**

Toyota Unintended Acceleration

- **2004:** Push-button ignition
- **2004-2009**
 - 102 incidents of uncontrolled acceleration
 - Speeds exceed 100 mph despite stomping on the brake
 - 30 crashes
 - 20 injuries
- **Today**
 - Software fixes for pushbutton ignition, pedals



How can we be sure the requirements are right?
How can we integrate human and technical
considerations?

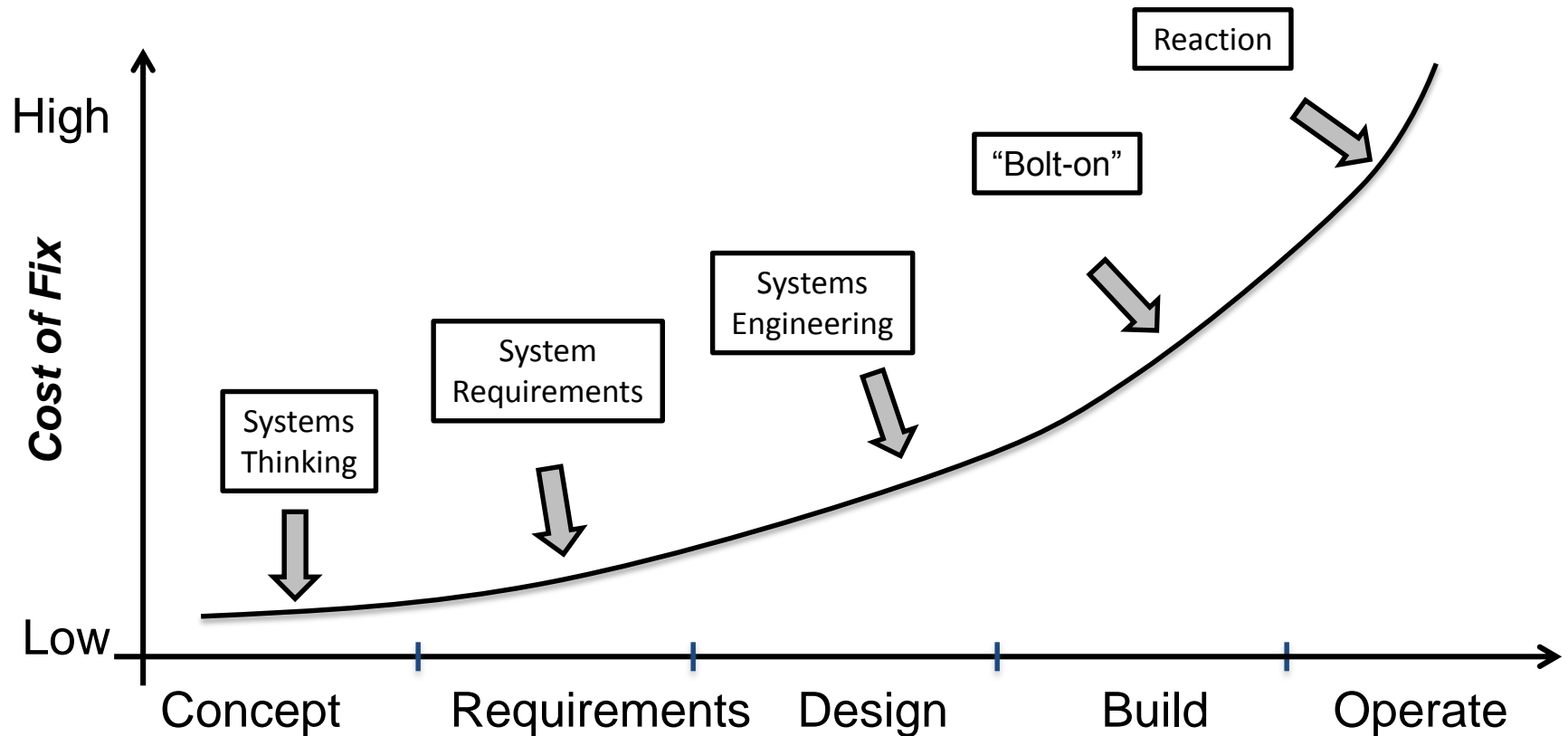
Honda Odyssey

- 344,000 minivans recalled
- Stability control software problem
- In certain circumstances, an error in the software can prevent the system from calibrating correctly, leading to pressure building up in the braking system, the National Highway Traffic Safety Administration said.
- If pressure builds to a certain point, "the vehicle may suddenly and unexpectedly brake hard, and without illuminating the brake lights, increasing the risk of a crash from behind," the NHTSA said.
- 2007-2008 models affected
 - Problem discovered in 2013



These problems made it through all existing processes: design reviews, testing, etc.

Addressing potential issues



Need to address issues early

Early decisions have biggest impact

Illustration courtesy Bill Young

Human Interactions

China Airlines 006

- Autopilot compensates for single engine malfunction
- Autopilot reaches max limits, aircraft turns slightly
- Pilots not notified Autopilot at its limits
- Pilots notice slight turn, disengage autopilot for manual control
 - Aircraft immediately nosedives



Pilot error or
“Clumsy automation”?

Operator Error: Old View

- Human error is cause of most incidents and accidents
- So do something about human involved
 - Fire them
 - Retrain them
 - Admonish them
 - Rigidify their work with more rules and procedures
- Or do something about humans in general
 - Marginalize them by putting in more automation

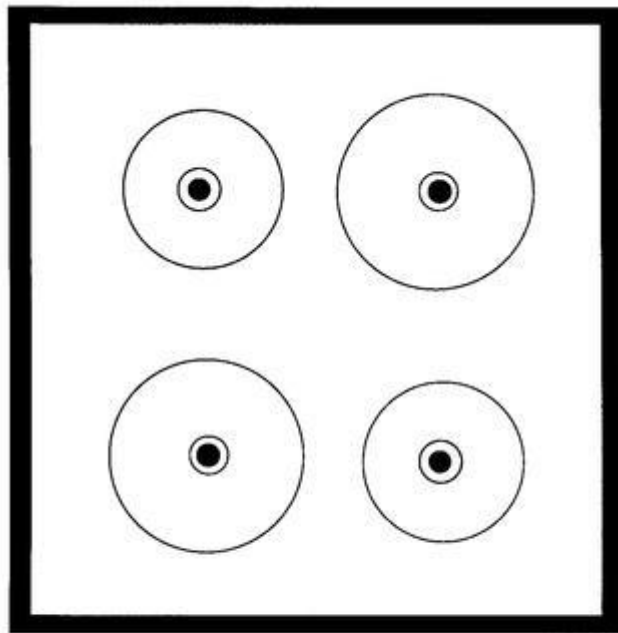
Operator Error: **Systems View**

(Dekker, Rasmussen, Leveson, Woods, etc.)

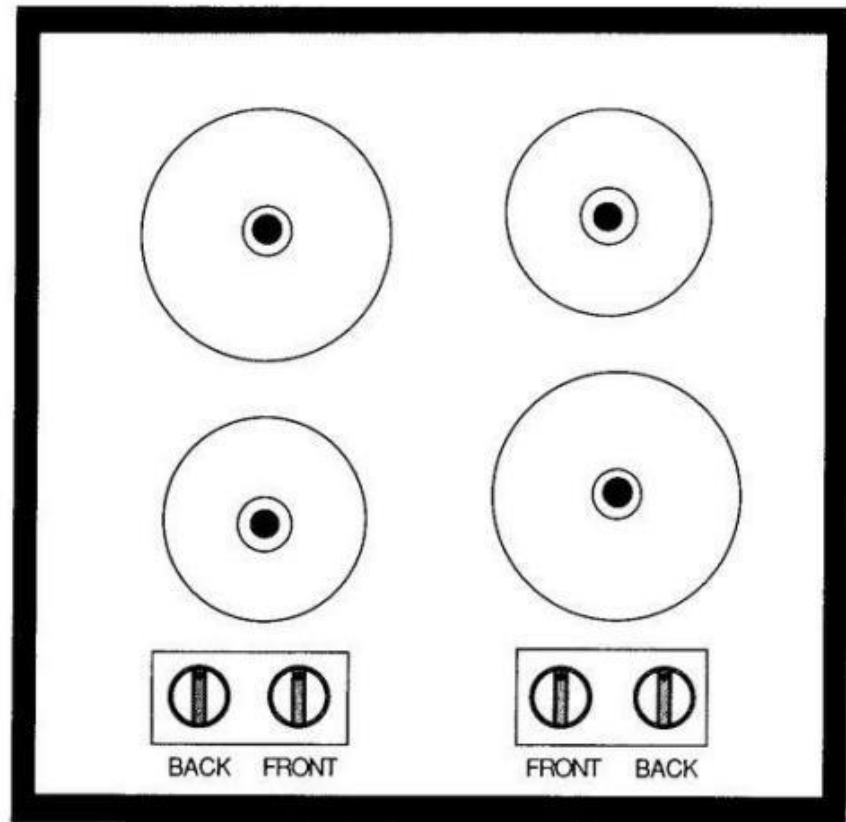
- Human error is a symptom, not a cause
- All behavior affected by context (system) in which it occurs
 - To understand human error, look at the system
 - System designs can make human error inevitable
 - **When bad systems cause operator error, can we really blame the operators rather than designers?**
- To do something about operator error, look at:
 - Unintuitive equipment and system designs
 - Usefulness of procedures
 - Existence of goal conflicts and production pressures

Human error is a symptom of the system and its design

Most stove tops

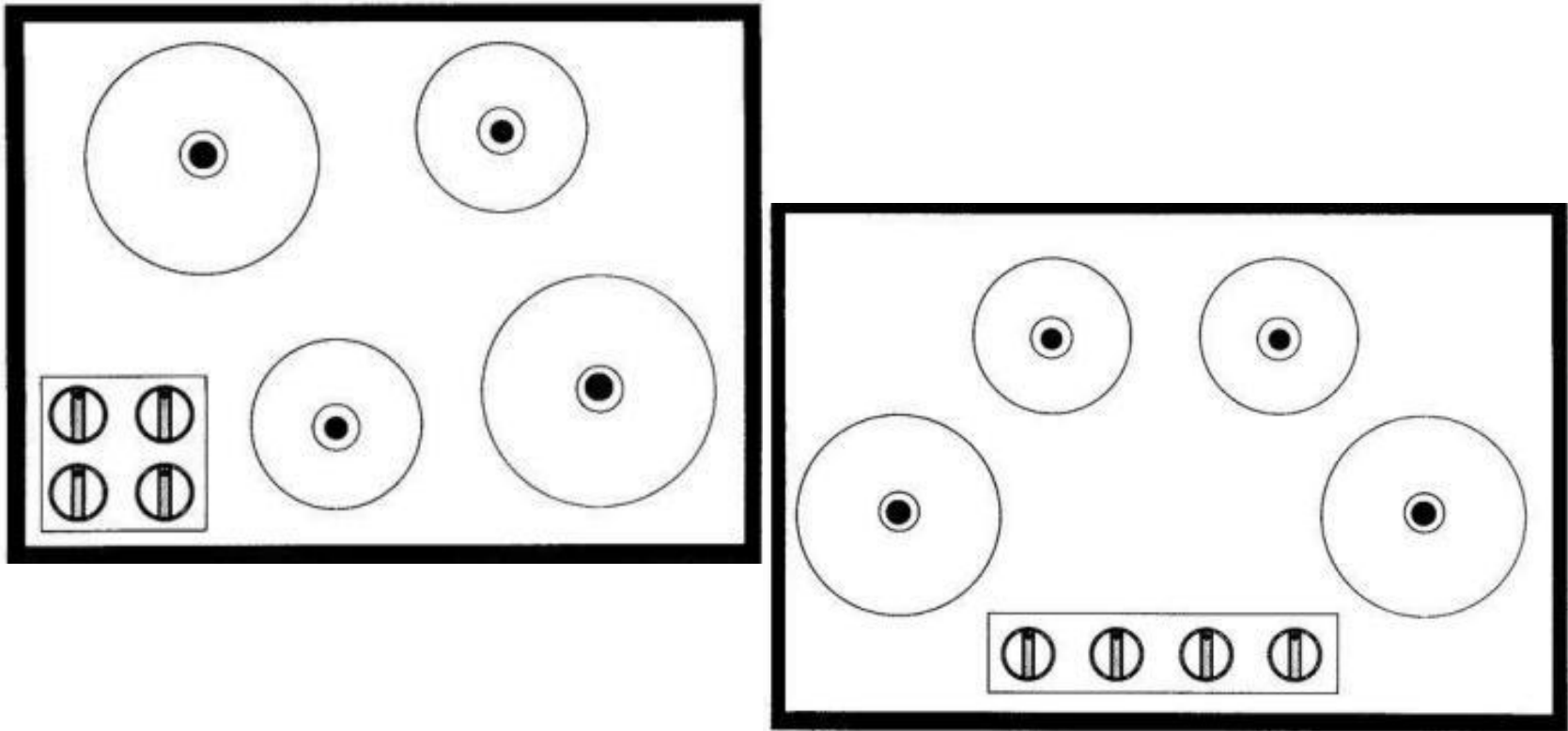


Back Right Front Left
Back Left Front Right



Is this a design problem or just human error?

Natural Mapping



The right design will reduce human error

Toyota Unintended Acceleration

- **2004:** Push-button ignition
- **2004-2009**
 - 102 incidents of uncontrolled acceleration
 - Speeds exceed 100 mph despite stomping on the brake
 - 30 crashes
 - 20 injuries
- **Today**
 - Software fixes for pushbutton ignition, pedals



Software design problem or driver error?

Tesla Summon



Tesla:

- "the incident occurred as a result of the driver not being properly attentive..."
- Drivers must agree to legal terms on their touch screen before the feature is allowed

This feature will park Model S while the driver is outside the vehicle. Please note that the vehicle may not detect certain obstacles, including those that are very narrow (e.g., bikes), lower than the fascia, or hanging from the ceiling. As such, Summon requires that you continually monitor your vehicle's movement and surroundings while it is in progress and that you remain prepared to stop the vehicle at any time using your key fob or mobile app or by pressing any door handle. You must maintain control and responsibility for your vehicle when using this feature and should only use it on private property. "

OK

CANCEL



STAMP: System Theoretic Accident Model and Processes

Foundation of STPA

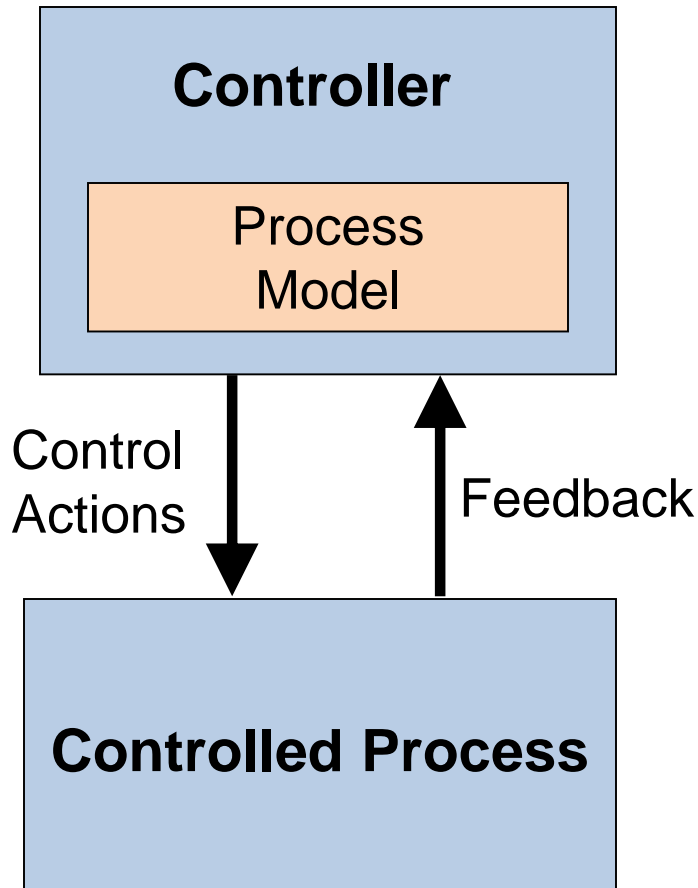
Systems approach to safety engineering (STAMP)



STAMP Model

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

Basic STAMP

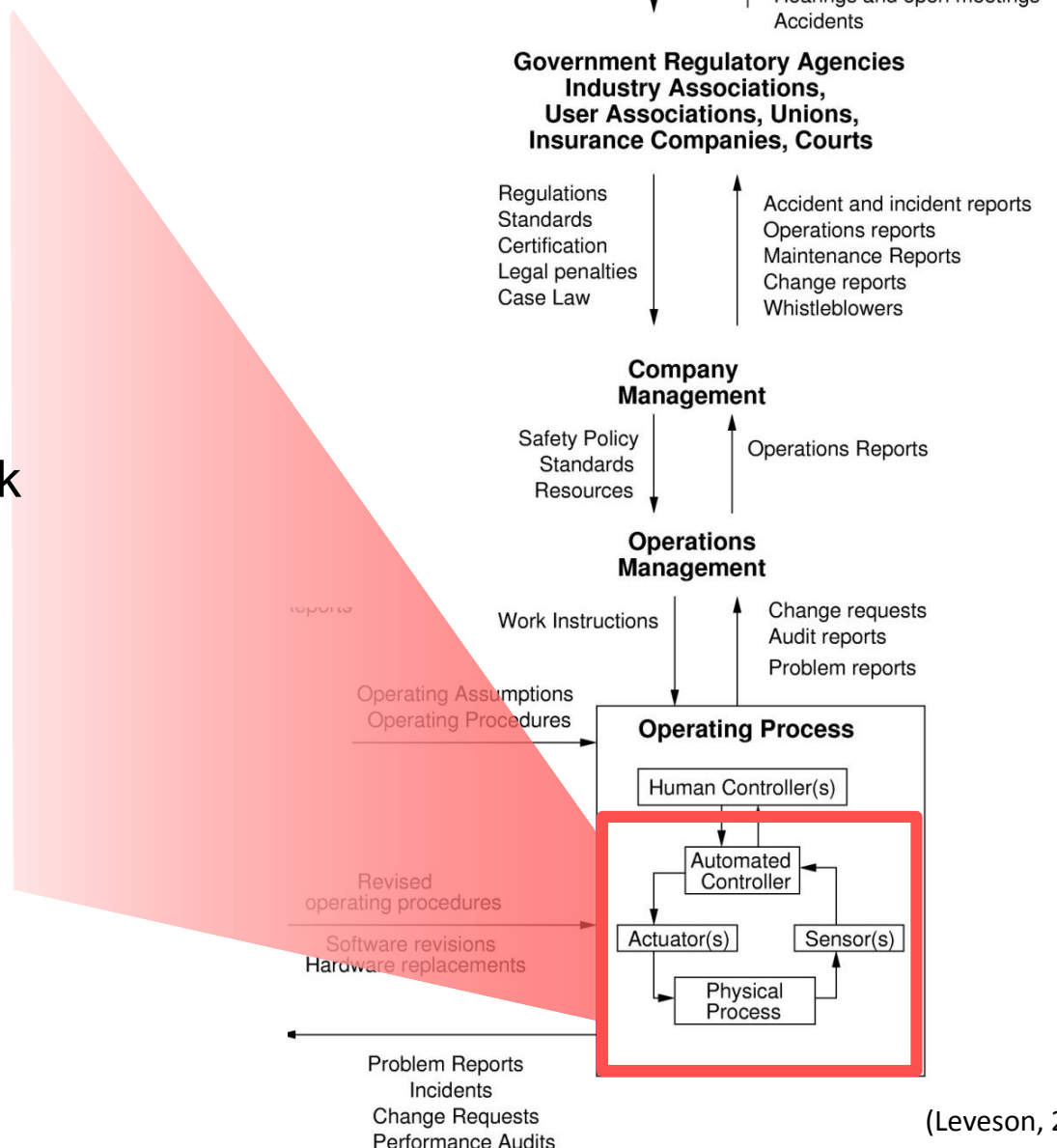
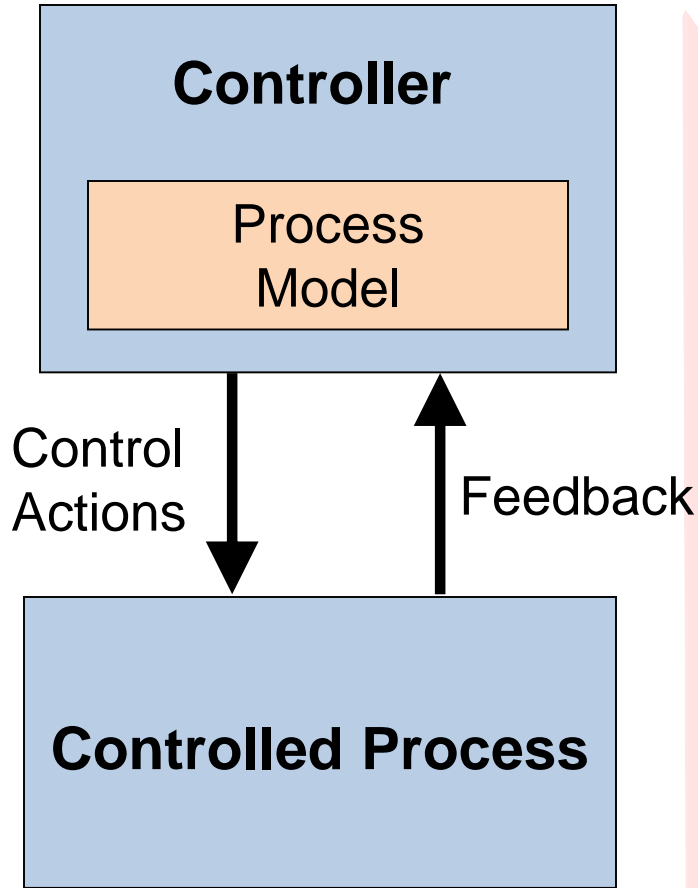


- Controllers use a **process model** to determine control actions
- Unanticipated behavior often occurs when the process model is incorrect
- Four types of **inadequate control actions**:
 - 1) Control commands are not given
 - 2) Inadequate commands are given
 - 3) Potentially correct commands but too early, too late
 - 4) Control action stops too soon or applied too long

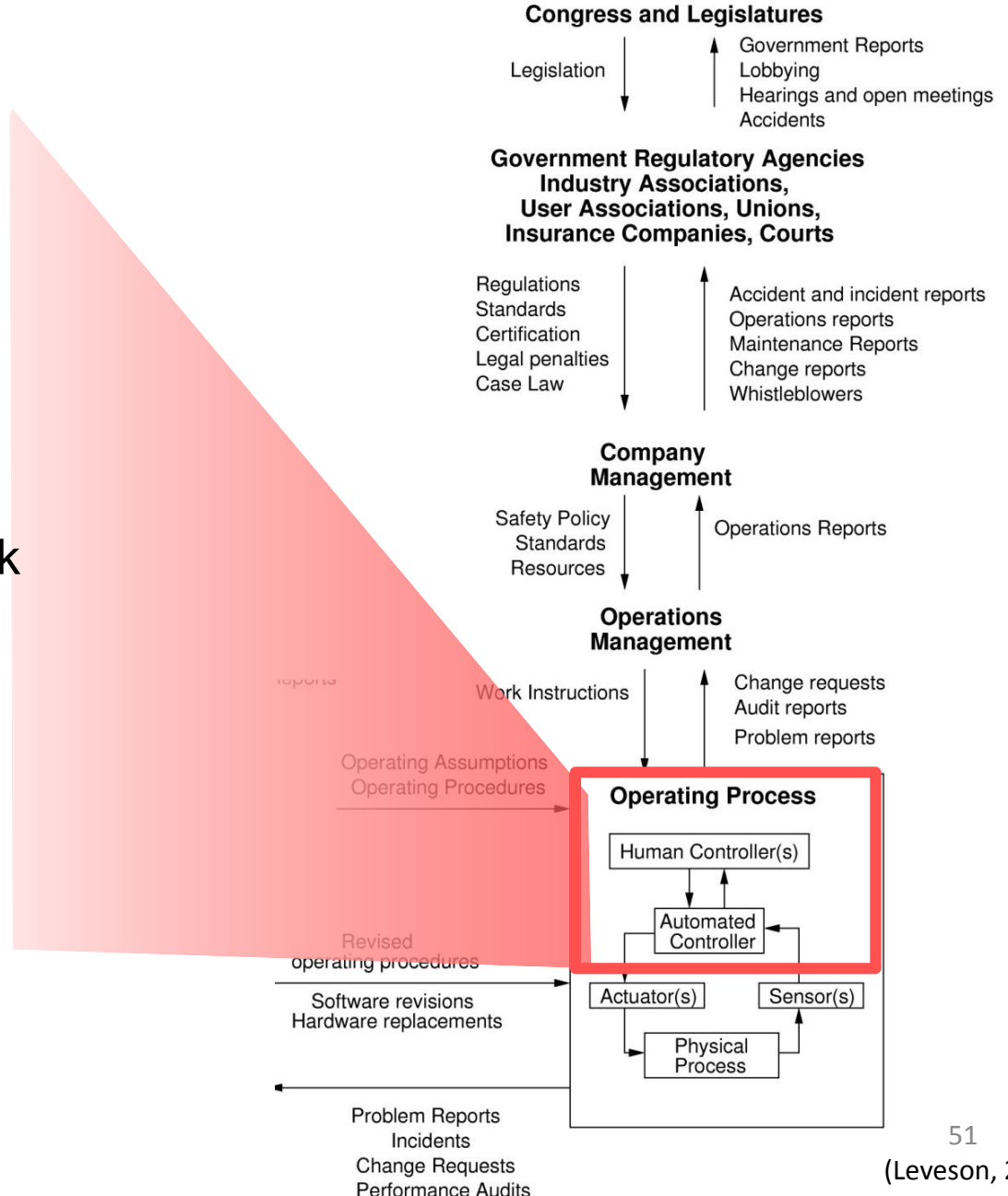
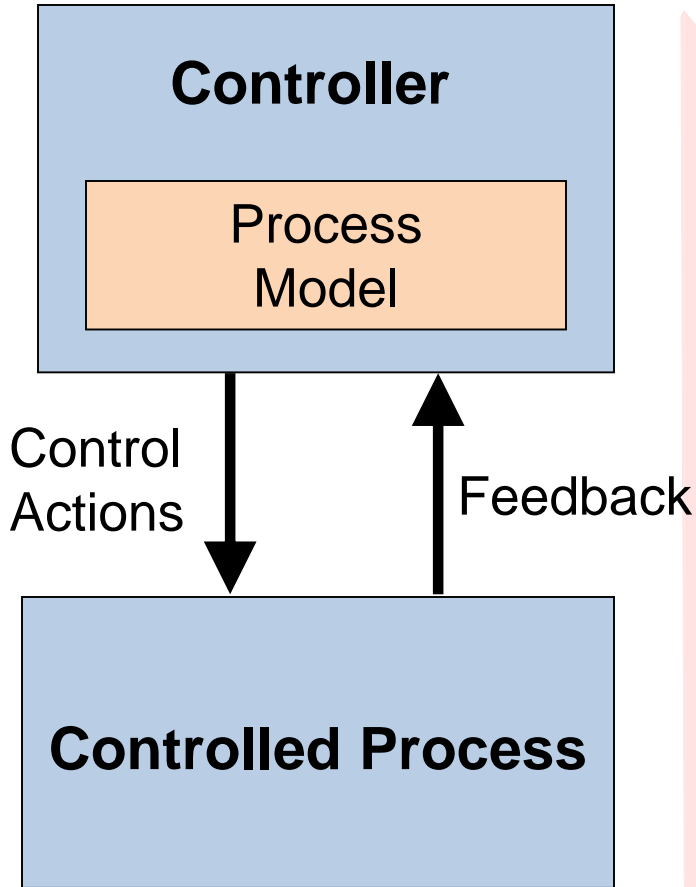
Tends to be a good model of both software and human behavior
Explains software errors, human errors, interaction accidents,⁴⁹...

(Leveson, 2012)

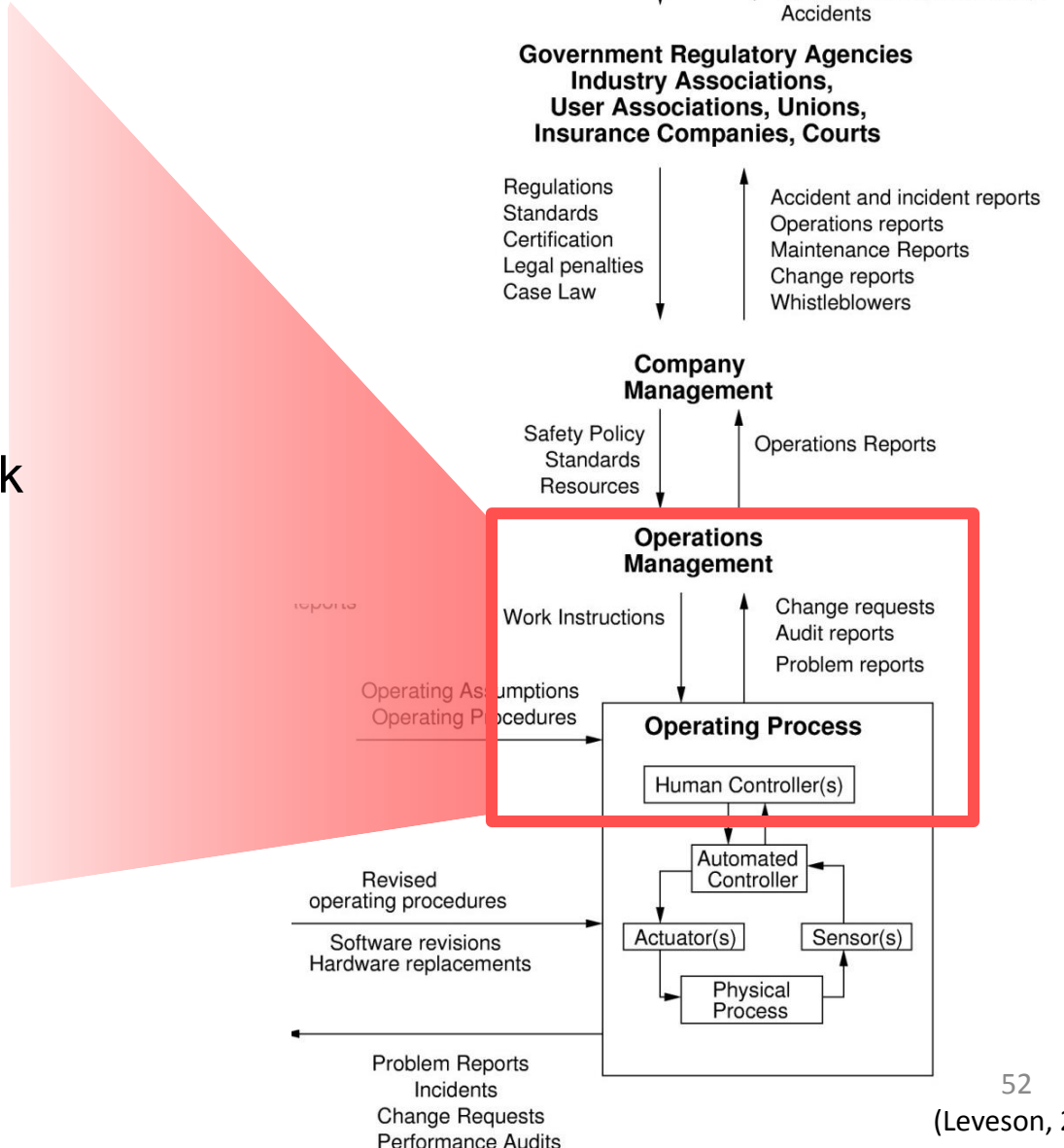
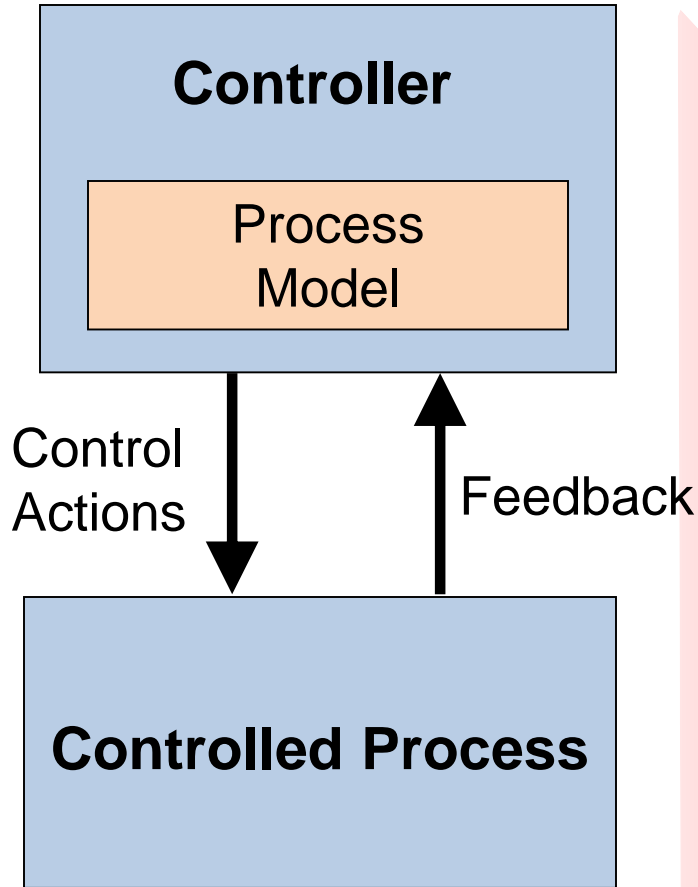
Basic STAMP



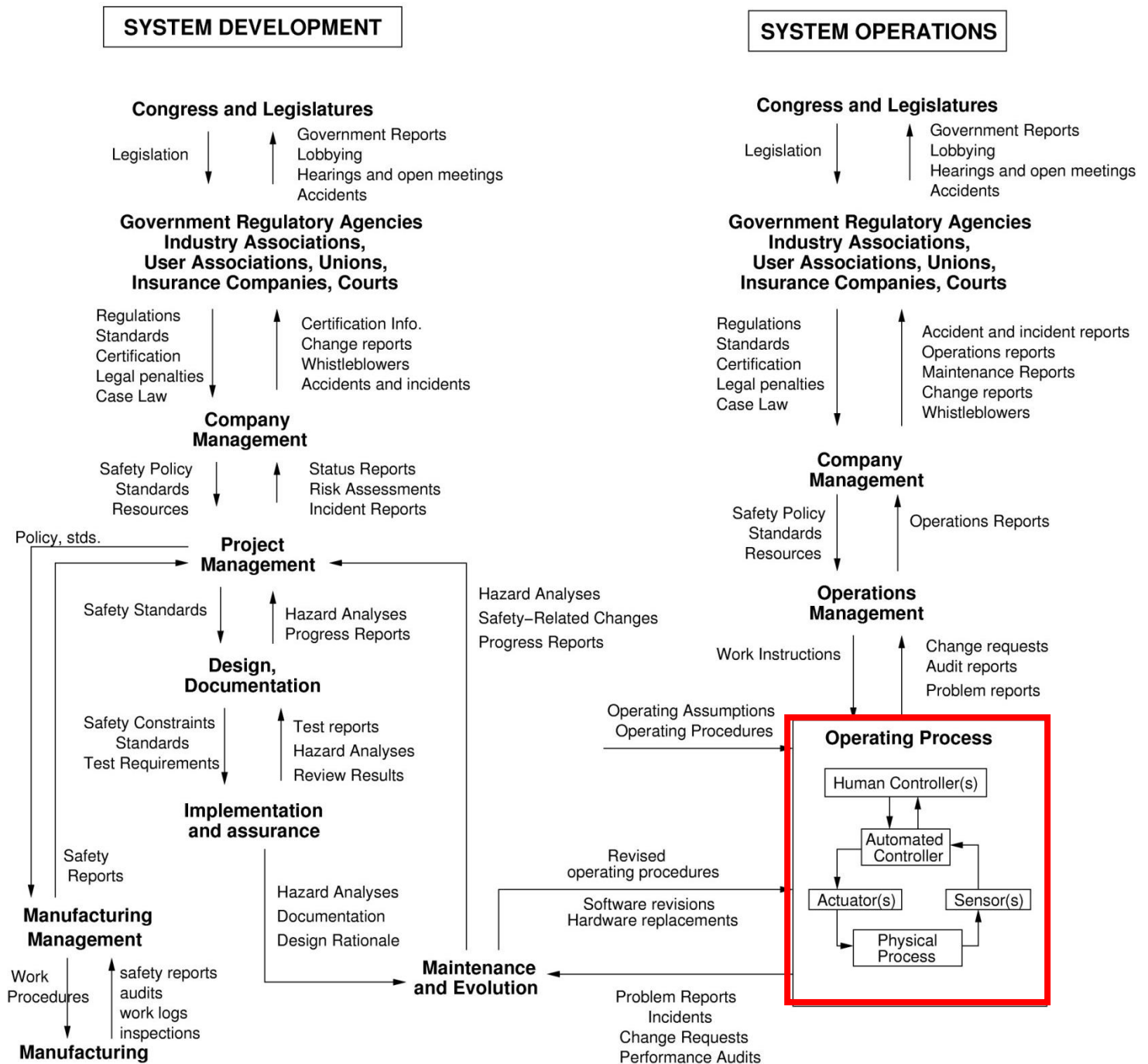
Basic STAMP



Basic STAMP



Example Control Structure



(Leveson, 2012)

STAMP and STPA

STAMP Model

Accidents are
caused by
inadequate control

STAMP and STPA

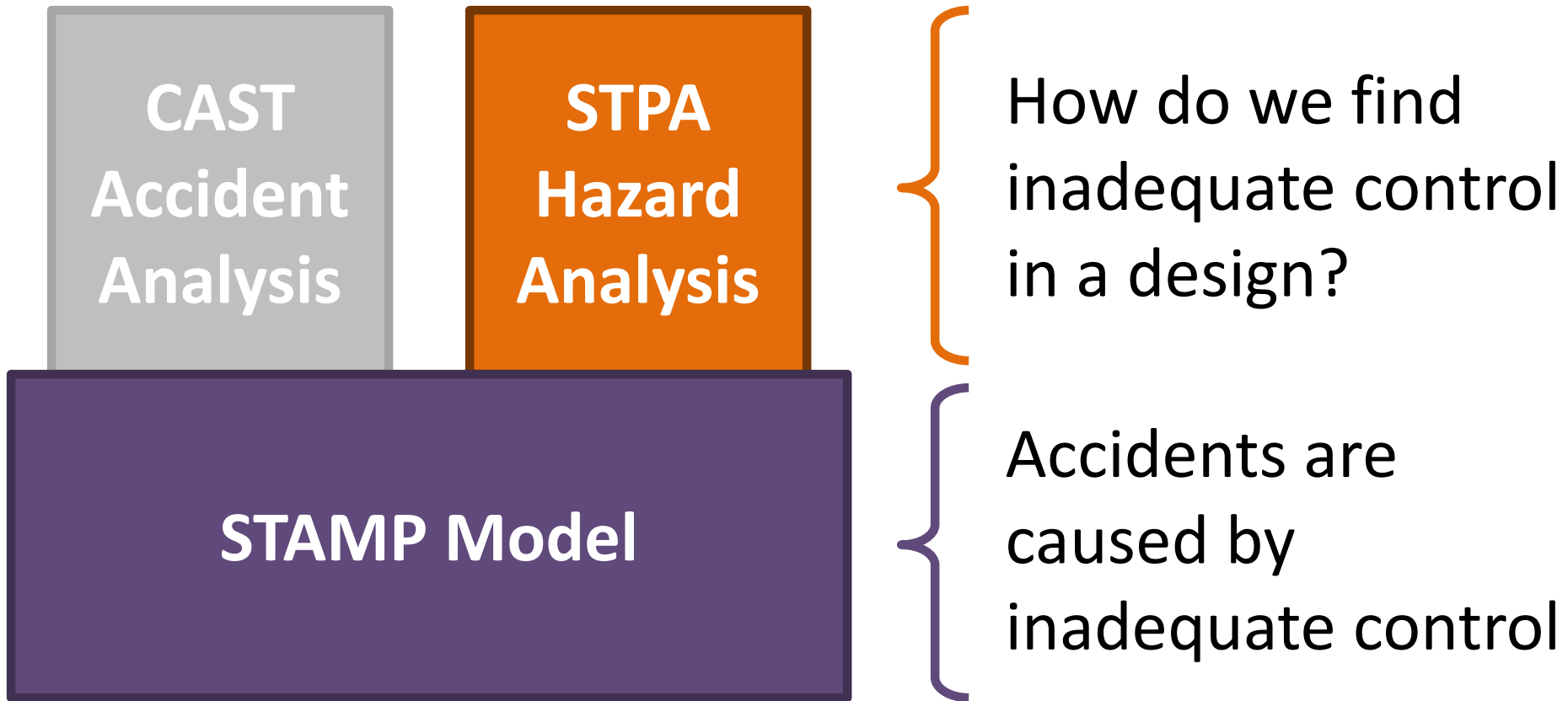
**CAST
Accident
Analysis**

STAMP Model

How do we find inadequate control that caused an accident?

Accidents are caused by inadequate control

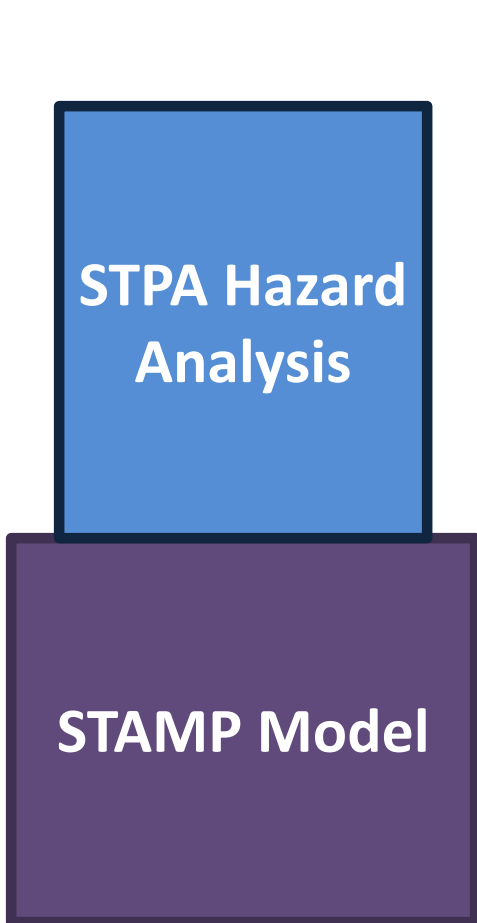
STAMP and STPA



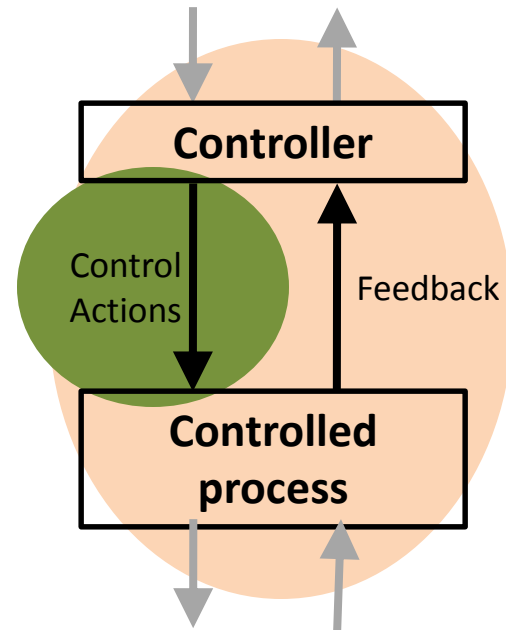
STPA: System Theoretic Process Analysis

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).

Example System: Aviation



System-level Accident (Loss): ?

Example System: Aviation



System-level Accident (Loss): Two aircraft collide



System-level Accident (Loss): Two aircraft collide
System-level Hazard: ?



System-level Accident (Loss): Aircraft crashes

System-level Hazard: Two aircraft violate minimum separation

Aviation Examples

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

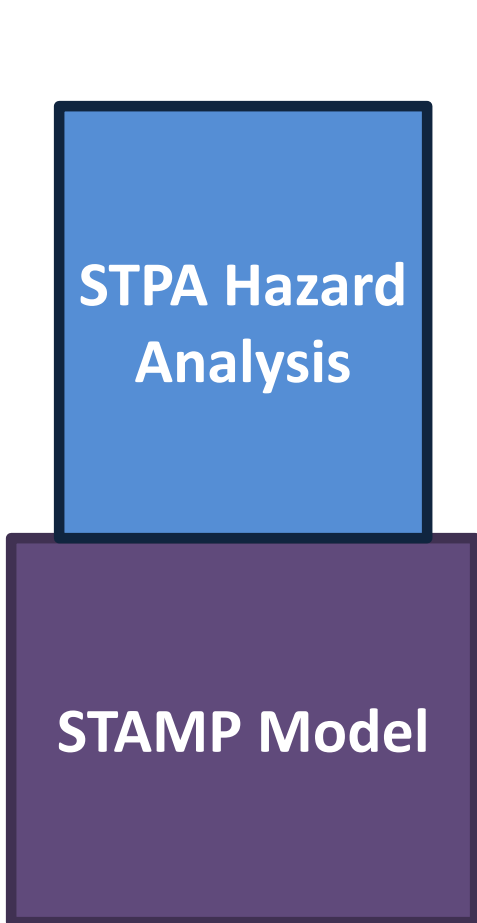
Example system: Automotive vehicles



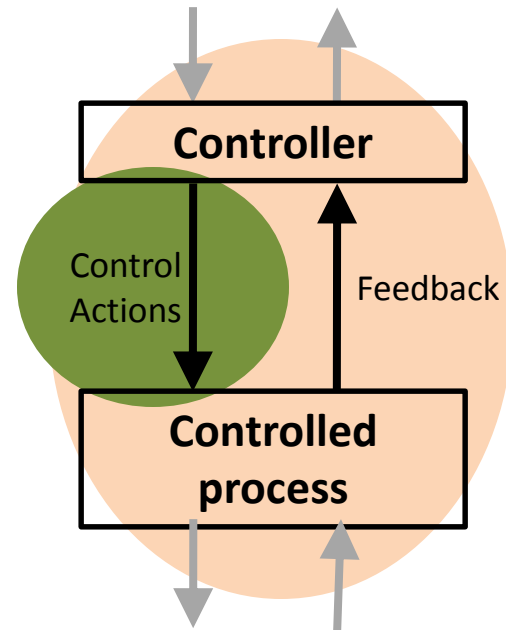
- Accidents and Hazards?

STPA

(System-Theoretic Process Analysis)

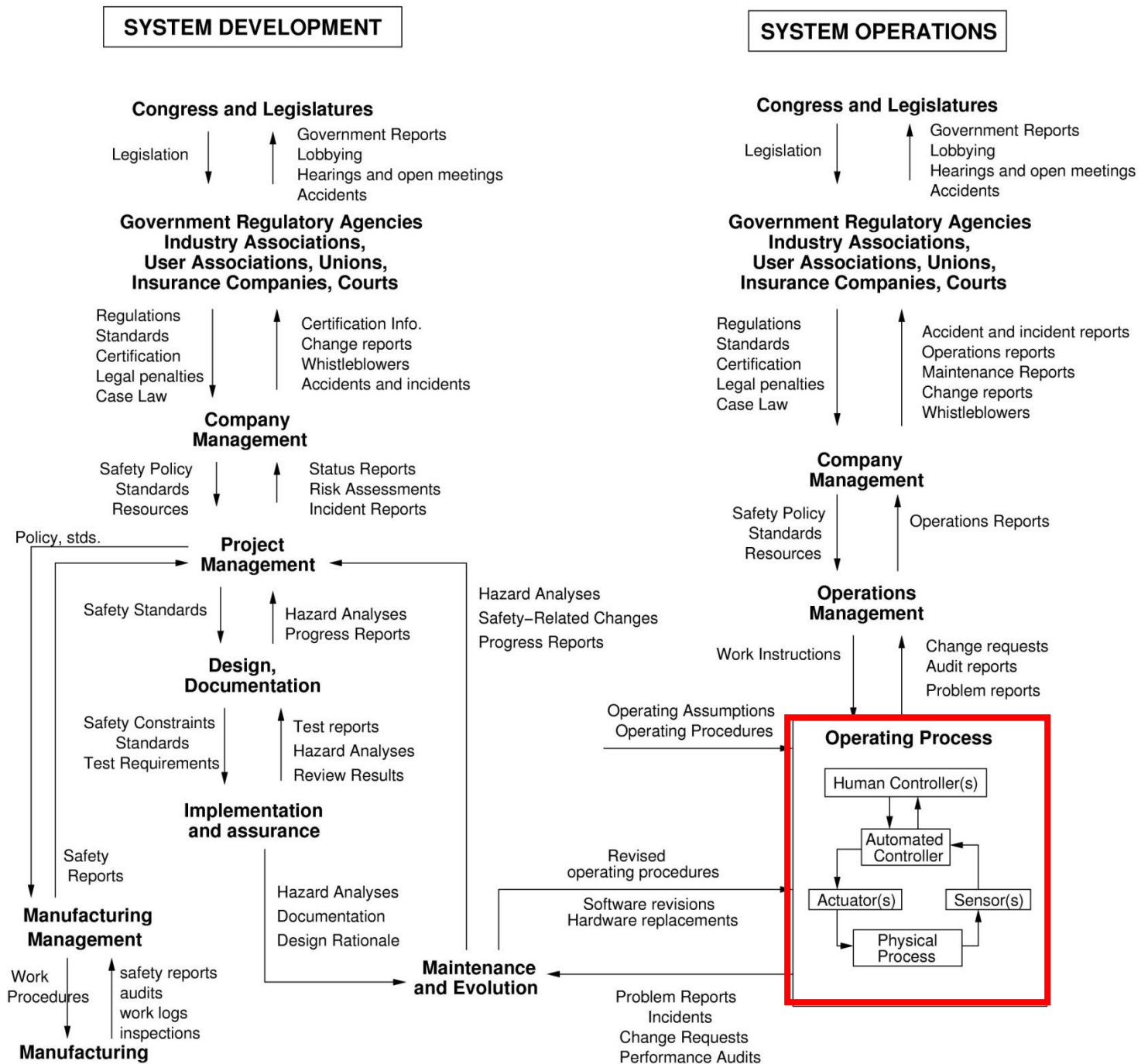


- System engineering foundation
 - Define accidents, system hazards
 - Control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



Control Structure Examples

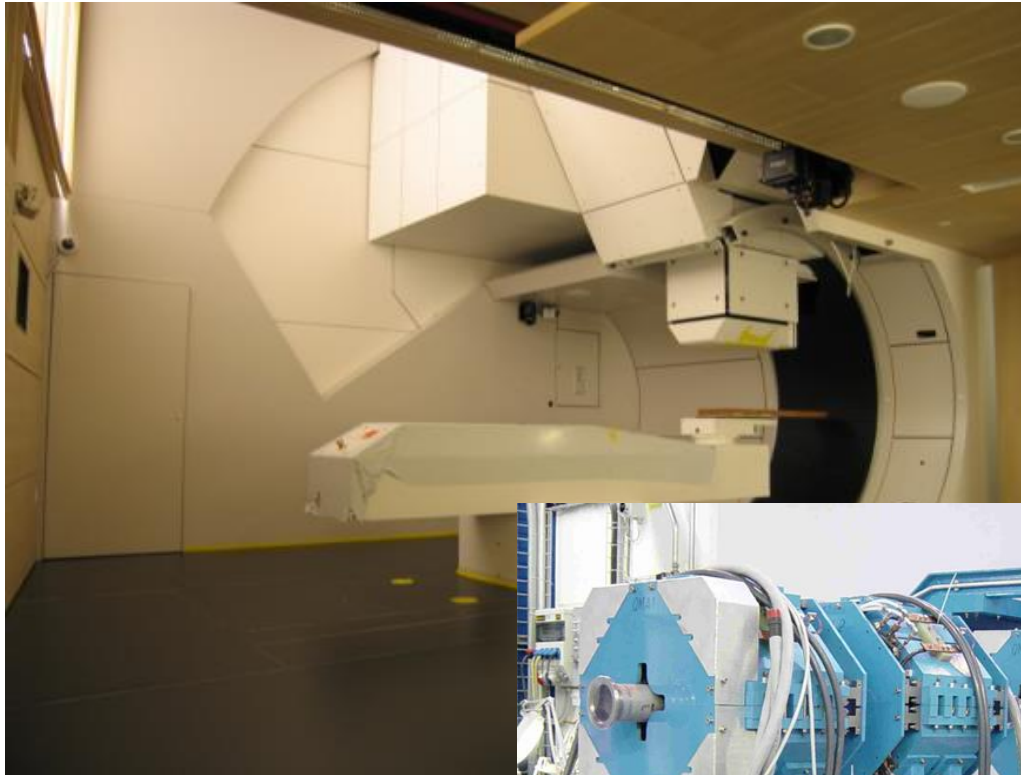
Example Control Structure



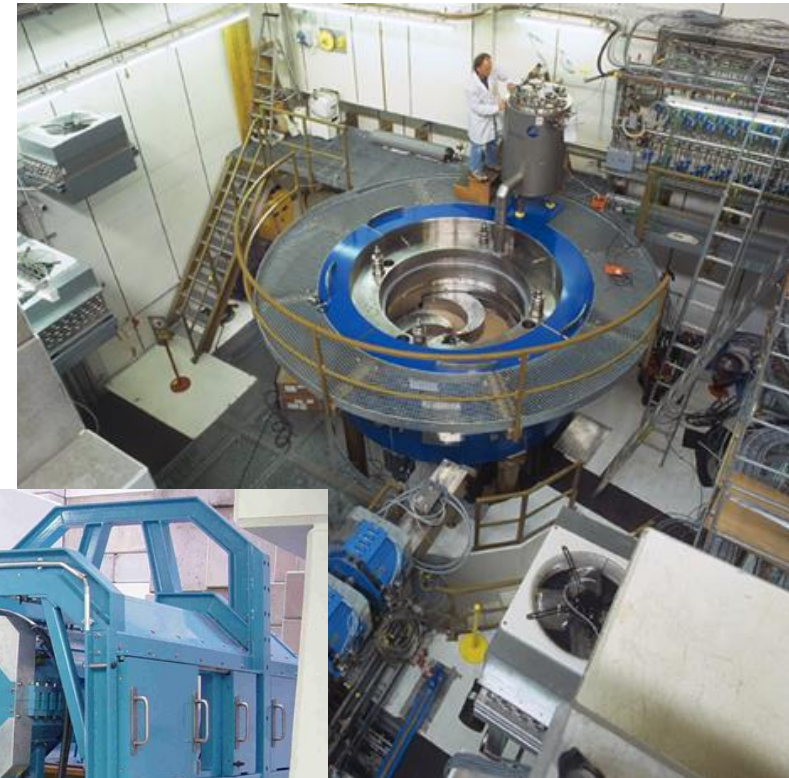
(Leveson, 2012)

Proton Therapy Machine

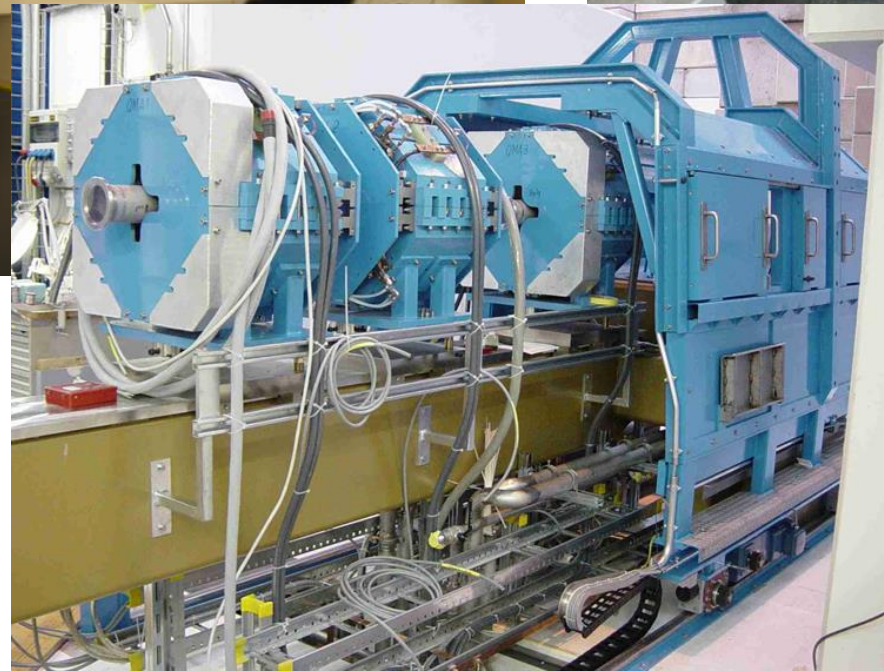
High-level Control Structure



Gantry



Cyclotron



Beam path and control elements

Proton Therapy Machine

High-level Control Structure

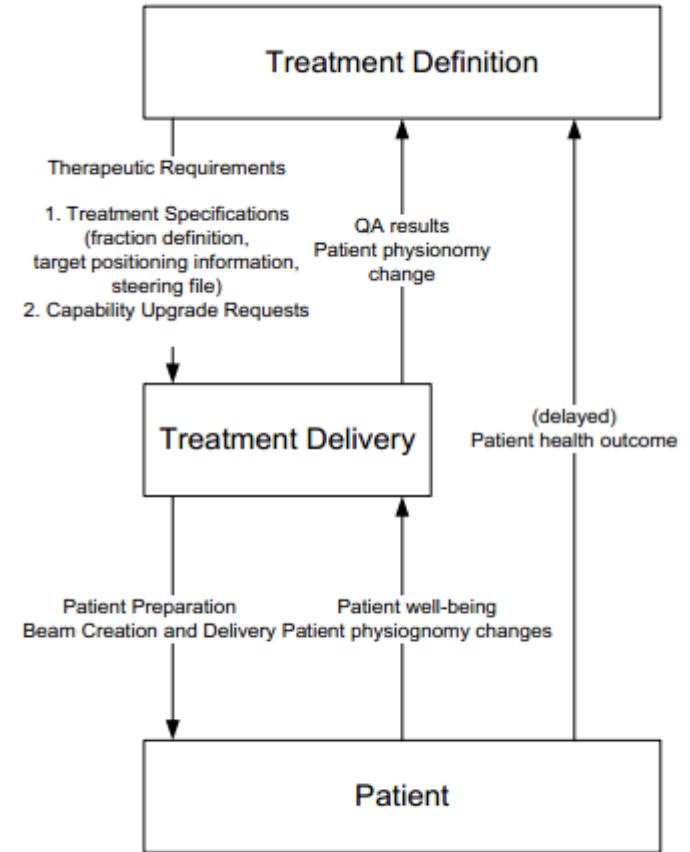
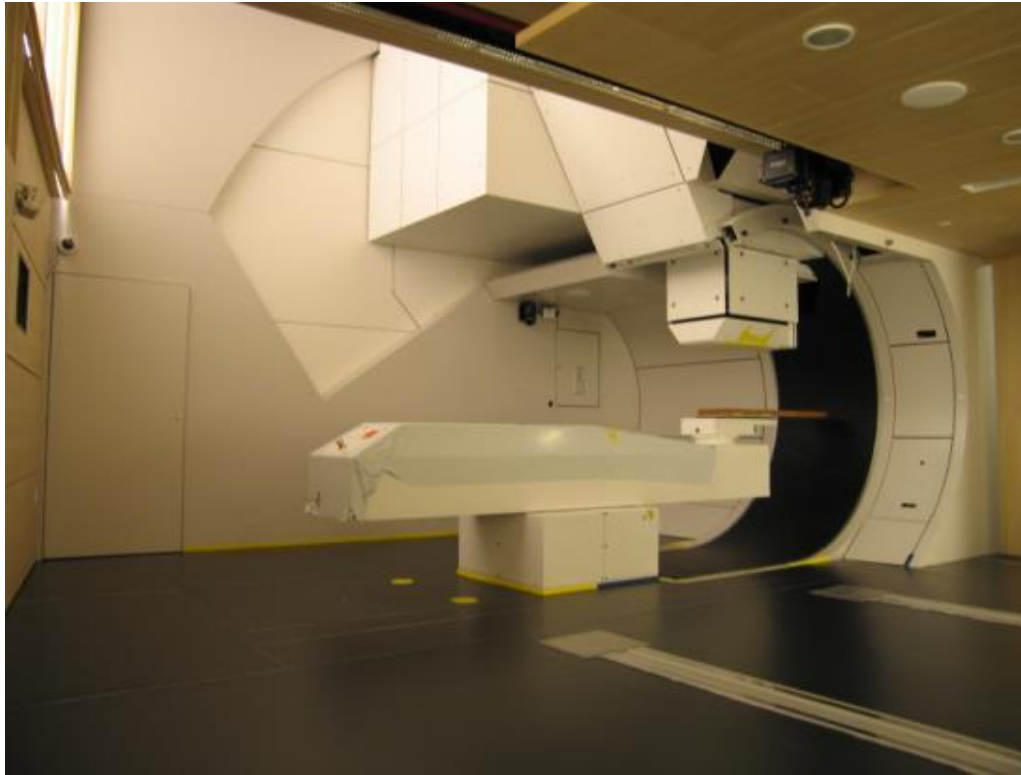
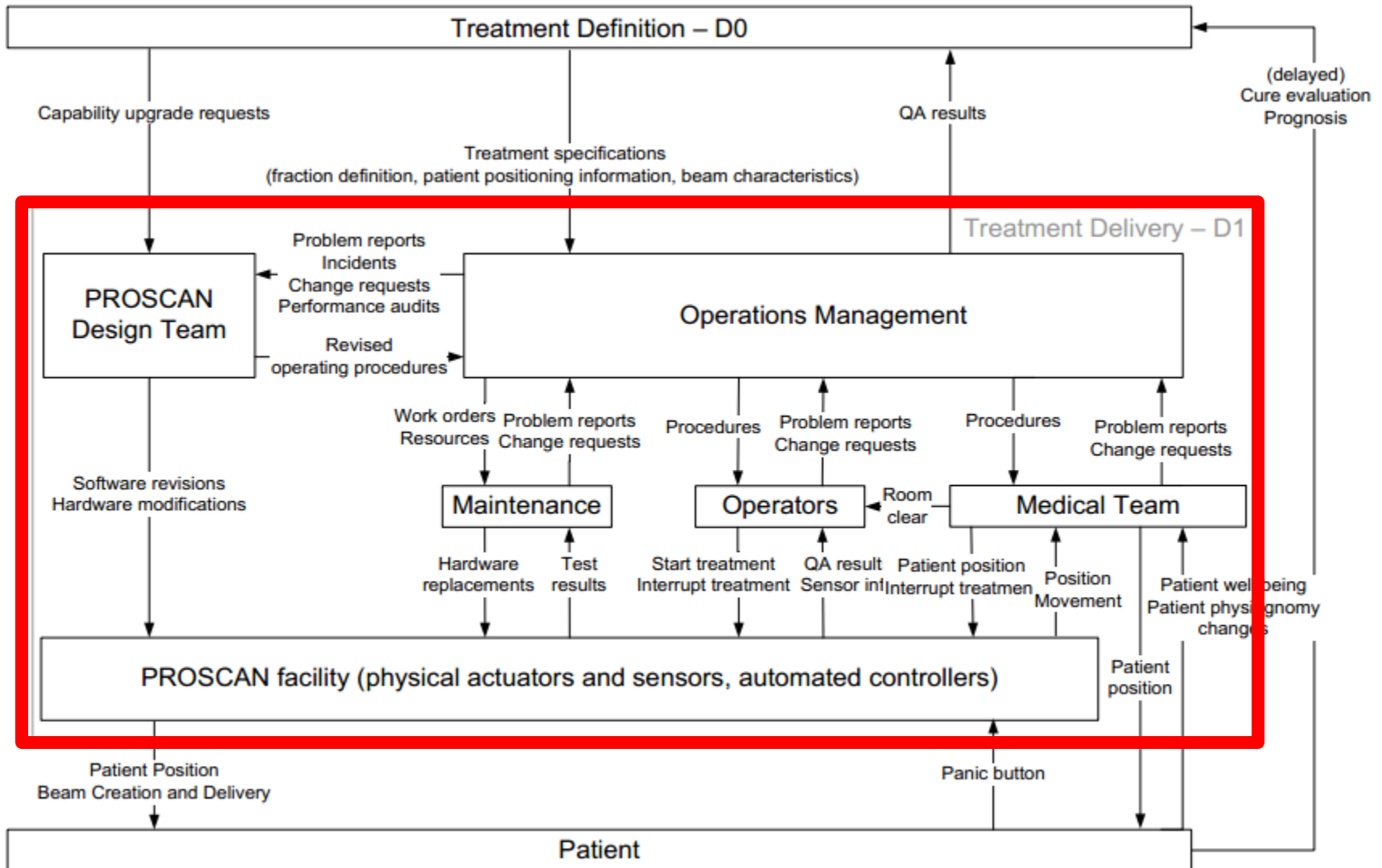


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Managing complexity

- Lesson from systems theory, cognitive science
- Human minds manage complexity through abstraction and hierarchy
- Use **top-down** process
 - Start at a high abstract level
 - Iterate to drill down into more detail
 - Build hierarchical models of the system

Proton Therapy Machine Control Structure



Ballistic Missile Defense System

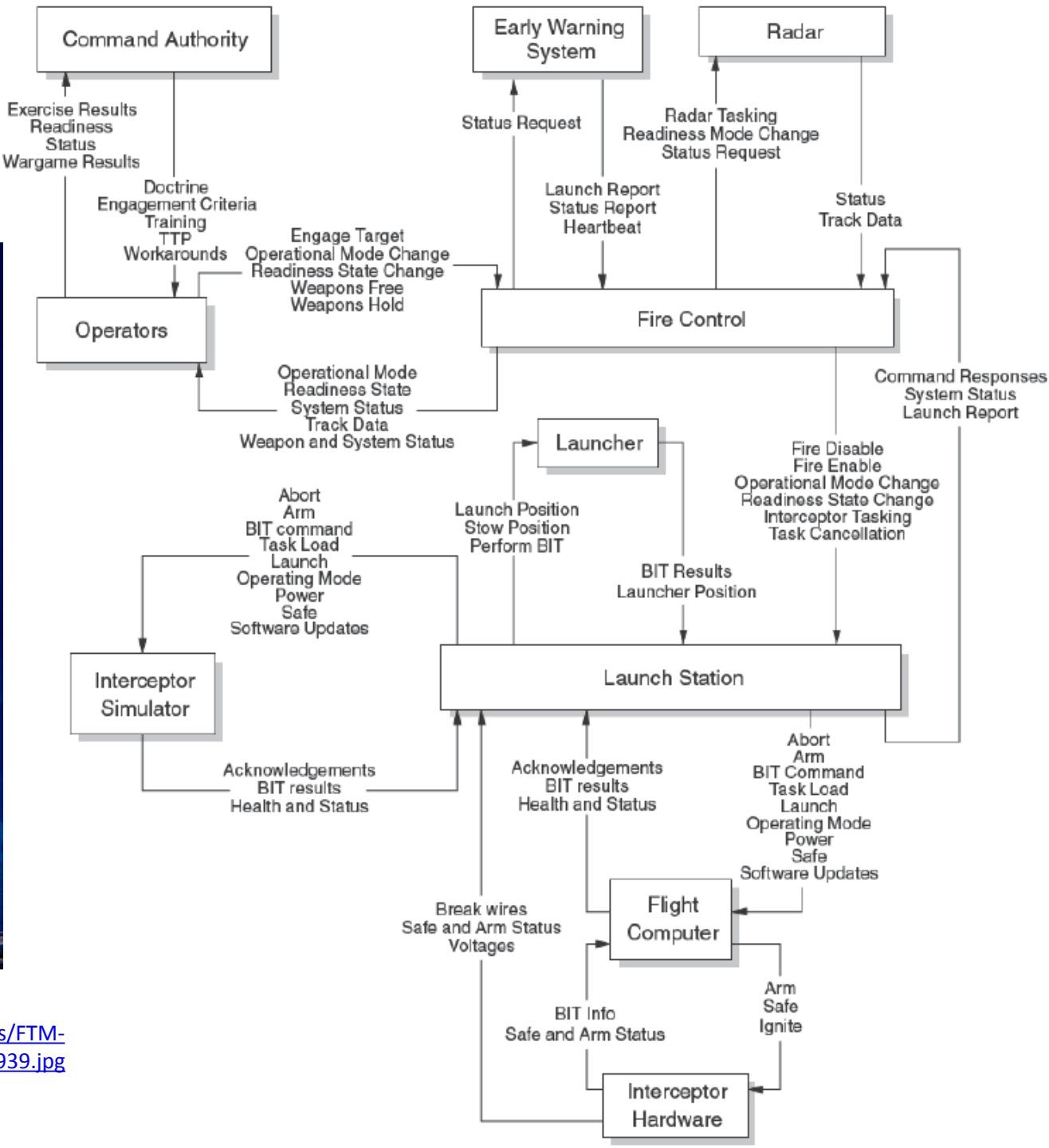
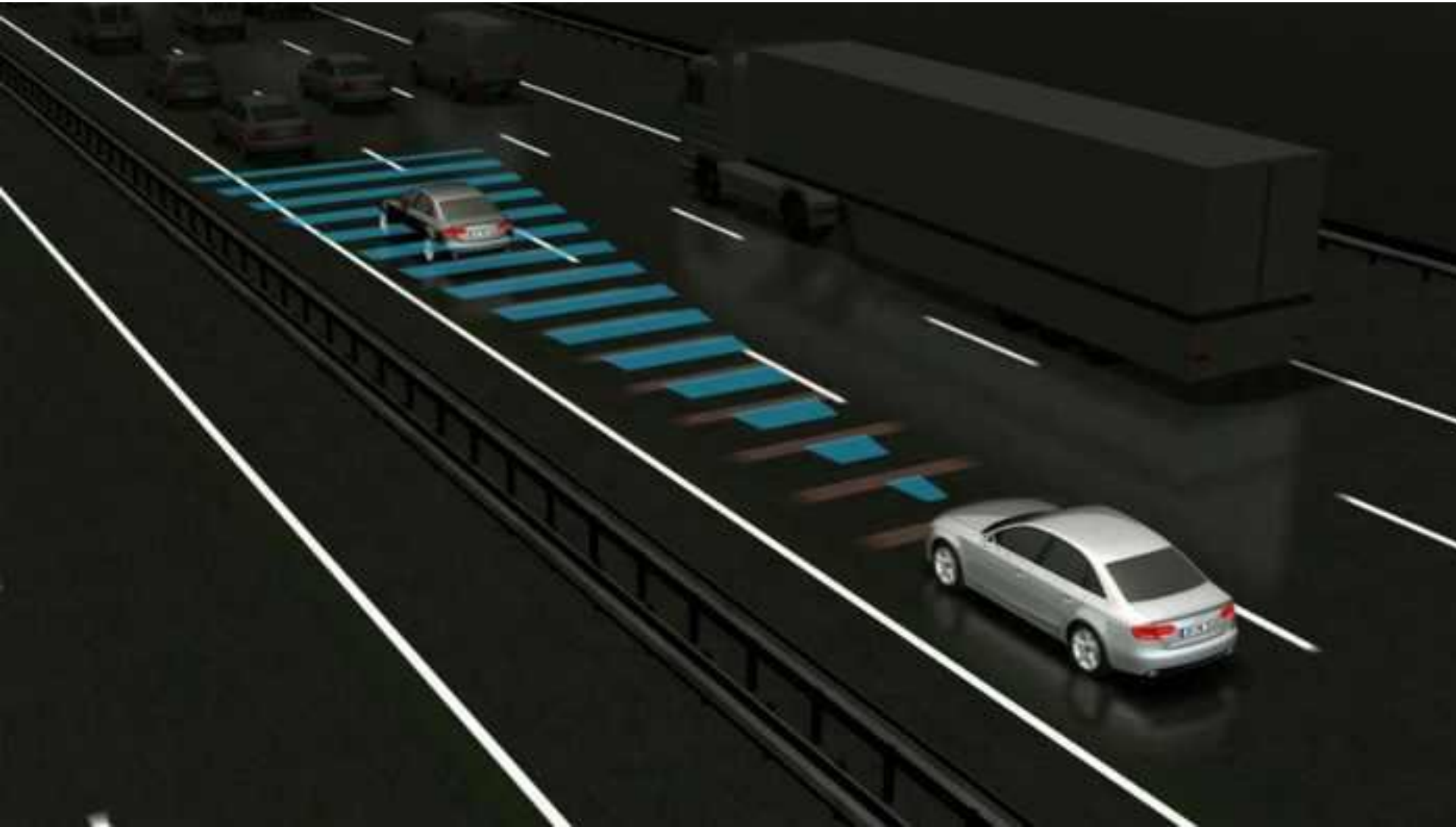
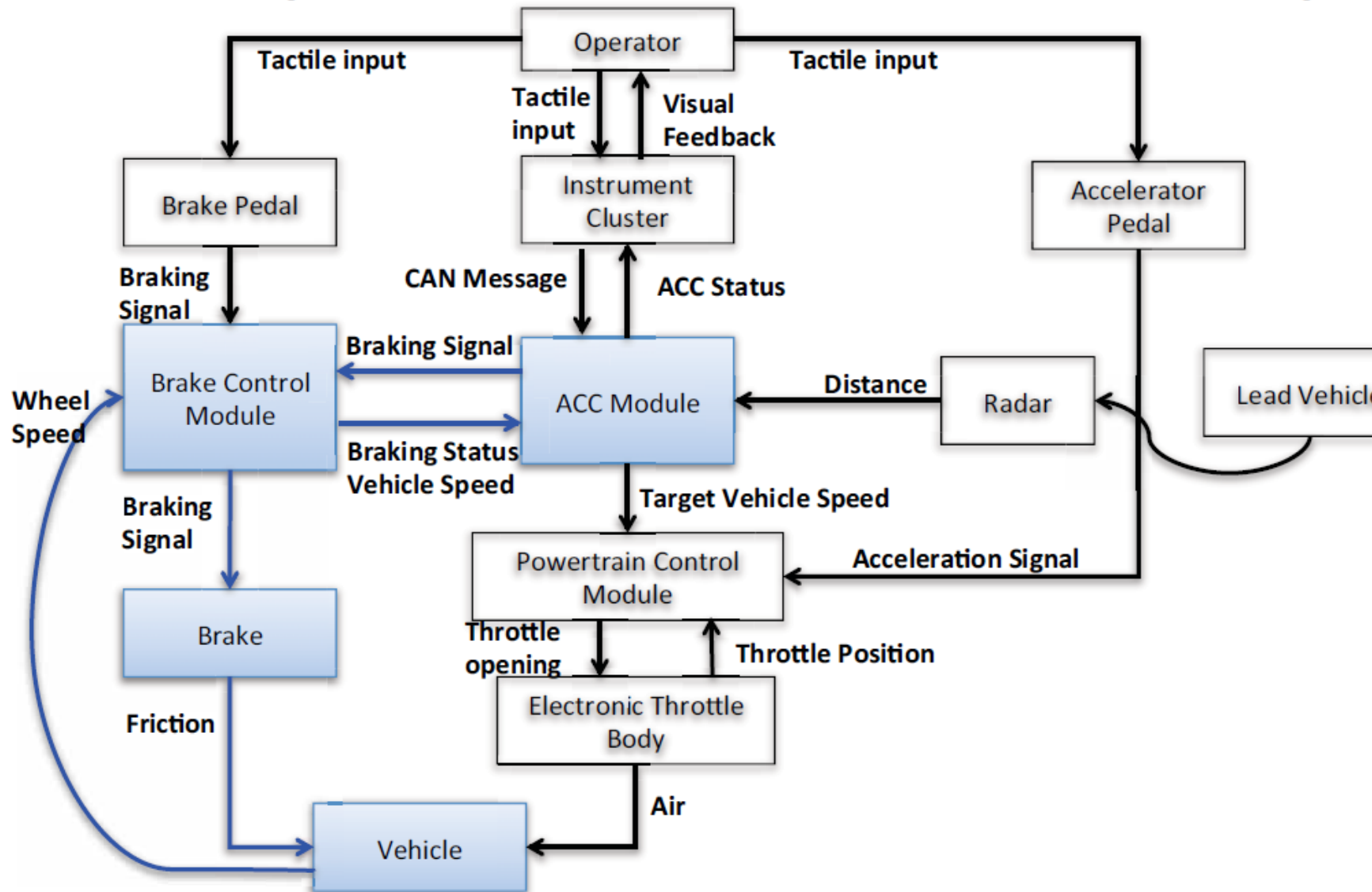


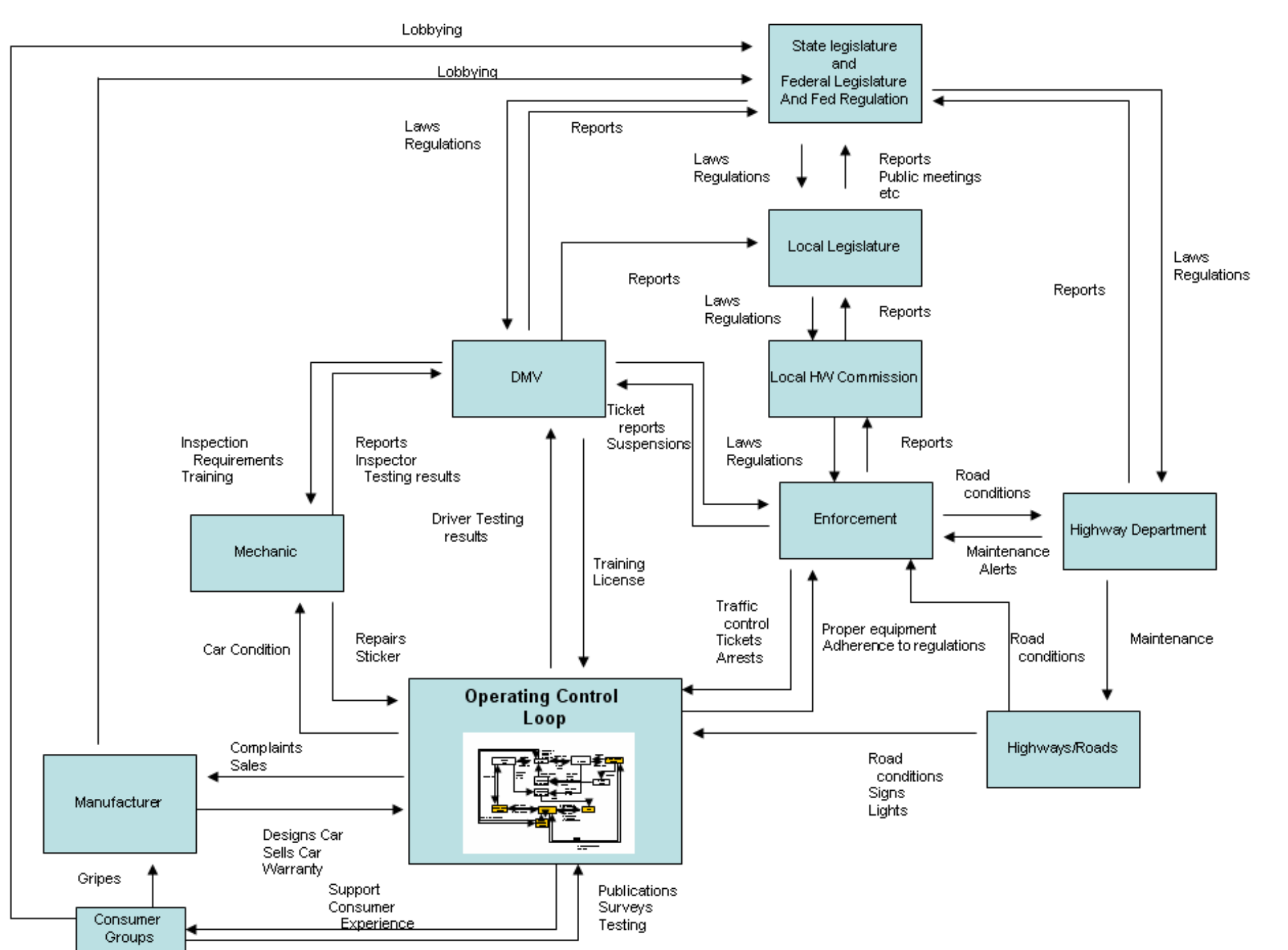
Image from:
http://www.mda.mil/global/images/system/aegis/FTM-21_Missile%20Bulkhead%20Center14_BN4H0939.jpg

Adaptive Cruise Control



Example: ACC – BCM Control Loop





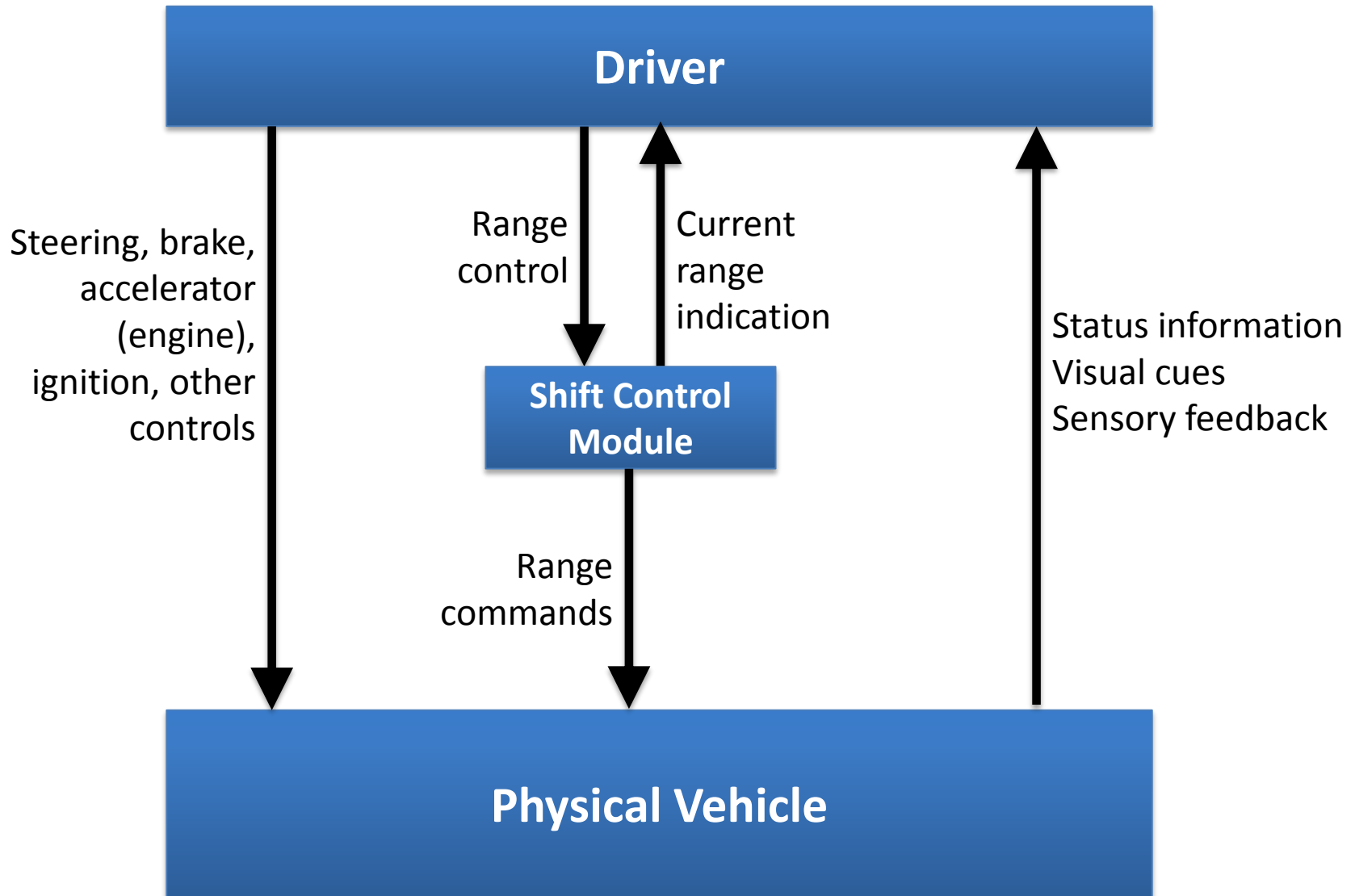
Automotive shift-by-wire



Automotive Shift by Wire

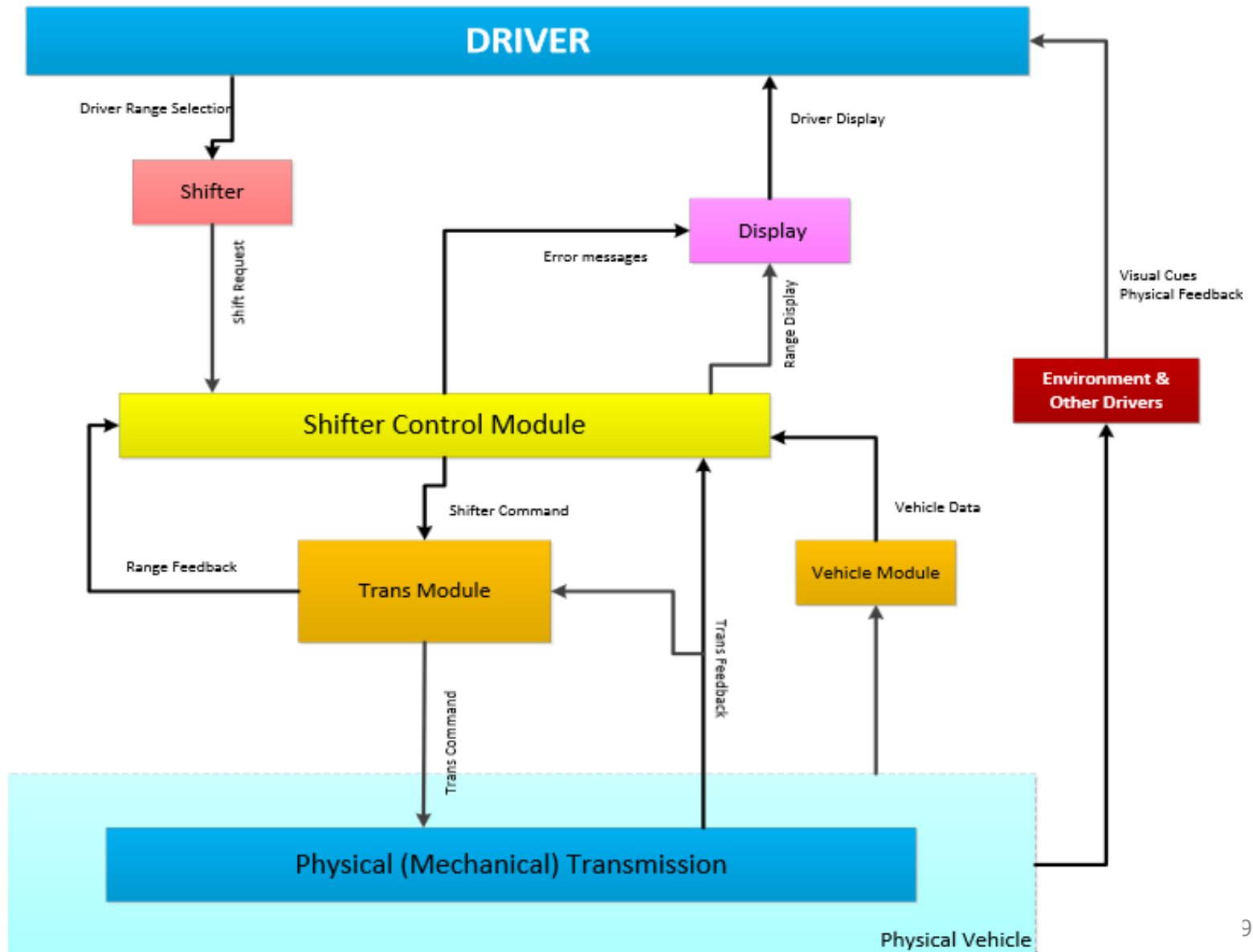
Your turn:
Control structure?

Control structure for vehicle



*Similar for both mechanical/electrical implementations

Automotive Shift by Wire

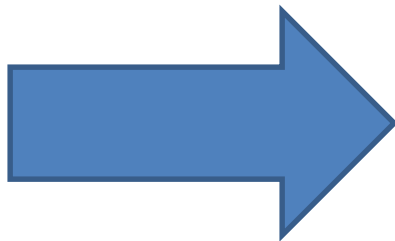


STPA

(System-Theoretic Process Analysis)

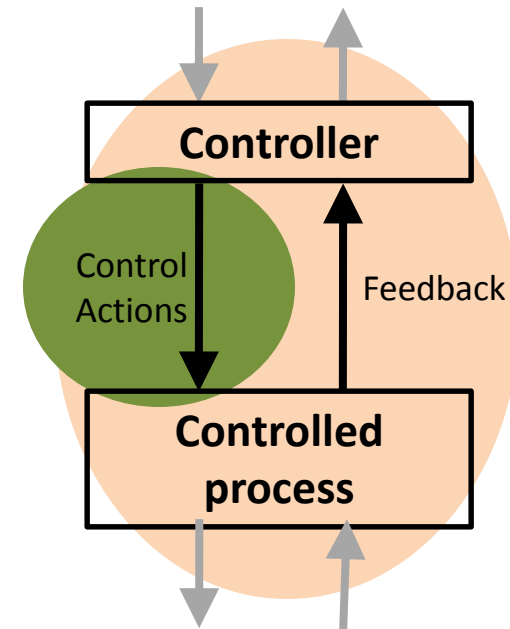


- System engineering foundation
 - Define accidents, system hazards
 - Control structure

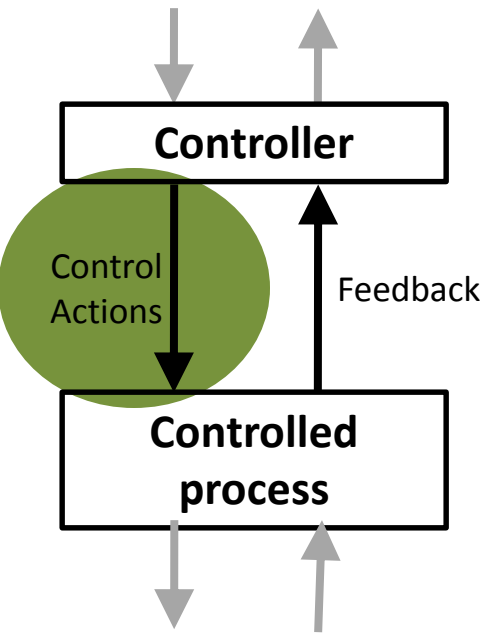


- Step 1: Identify unsafe control actions

- Step 2: Identify accident causal scenarios



STPA Step 1: Unsafe Control Actions (UCA)

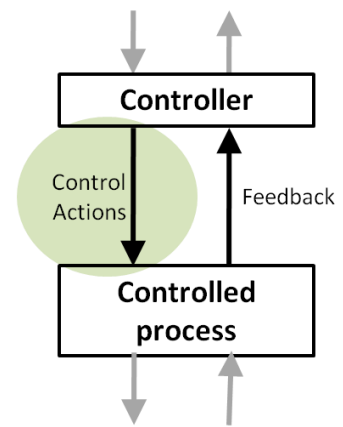


4 ways unsafe control may occur:

- 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:

“Computer provides open catalyst valve cmd while water valve is closed”

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)

UCAs → Safety Constraints

Unsafe Control Action

Safety Constraint



STPA

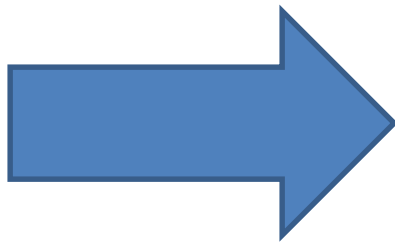
(System-Theoretic Process Analysis)



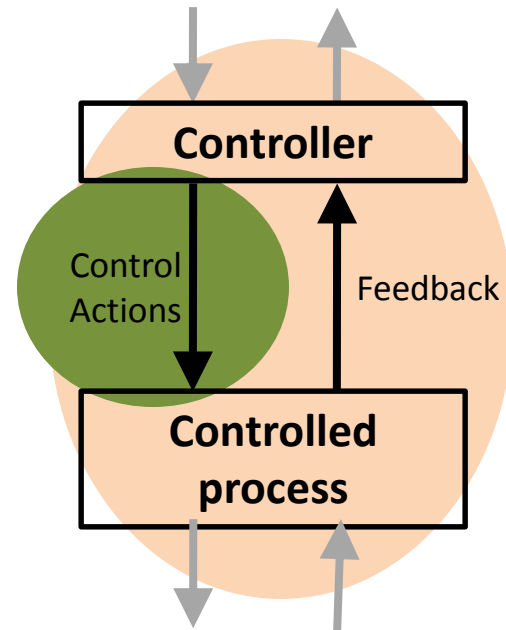
- System engineering foundation
 - Define accidents, system hazards
 - Control structure



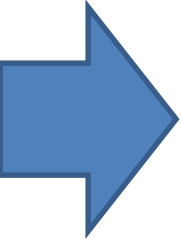
- Step 1: Identify unsafe control actions



- Step 2: Identify accident causal scenarios

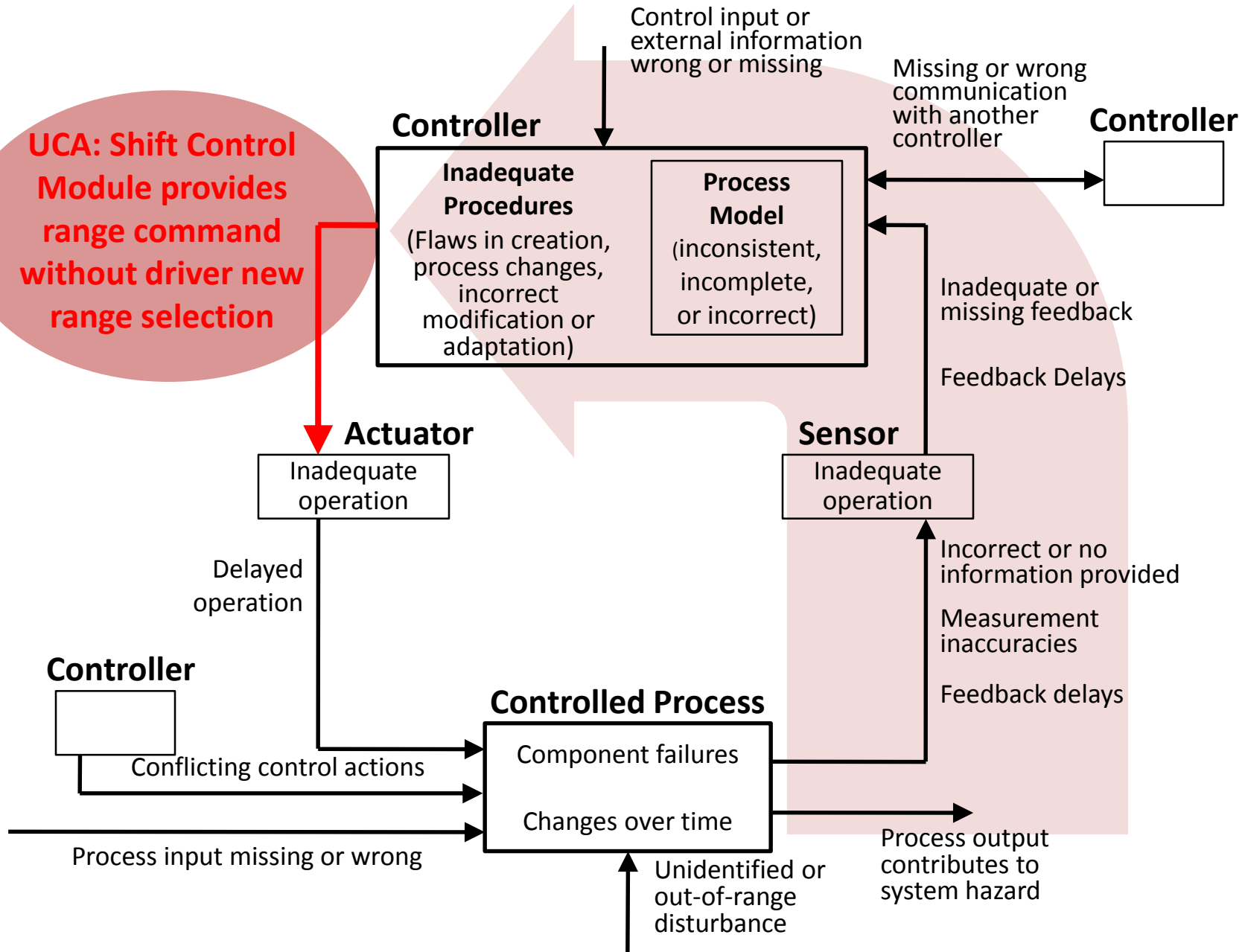


STPA Step 2: Identify Causal Factors

- 
- 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

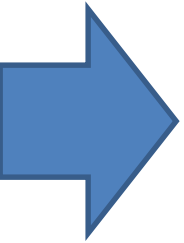
Step 2A: Potential causes of UCAs

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



STPA Step 2: Identify Causal Factors

- 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

