Massachusetts
Institute of
Technology

Introduction to STPA

Anticipating & Preventing Loss Scenarios in Complex Systems

Dr. John Thomas

Engineering Systems Lab

MIT

Any questions? Email me! JThomas4@mit.edu

Tutorial Objective

- These short tutorials are **not training classes**
- We cannot cover everything in these tutorial sessions. The objective is just to introduce some of the core concepts and help new attendees follow the presentations to come. These short tutorials are subsets of larger training classes.
- As with most techniques, training and practice with a qualified instructor are needed to apply these techniques and become proficient.

STPA analyzes a control structure

What is a control structure?

Enabling abstraction

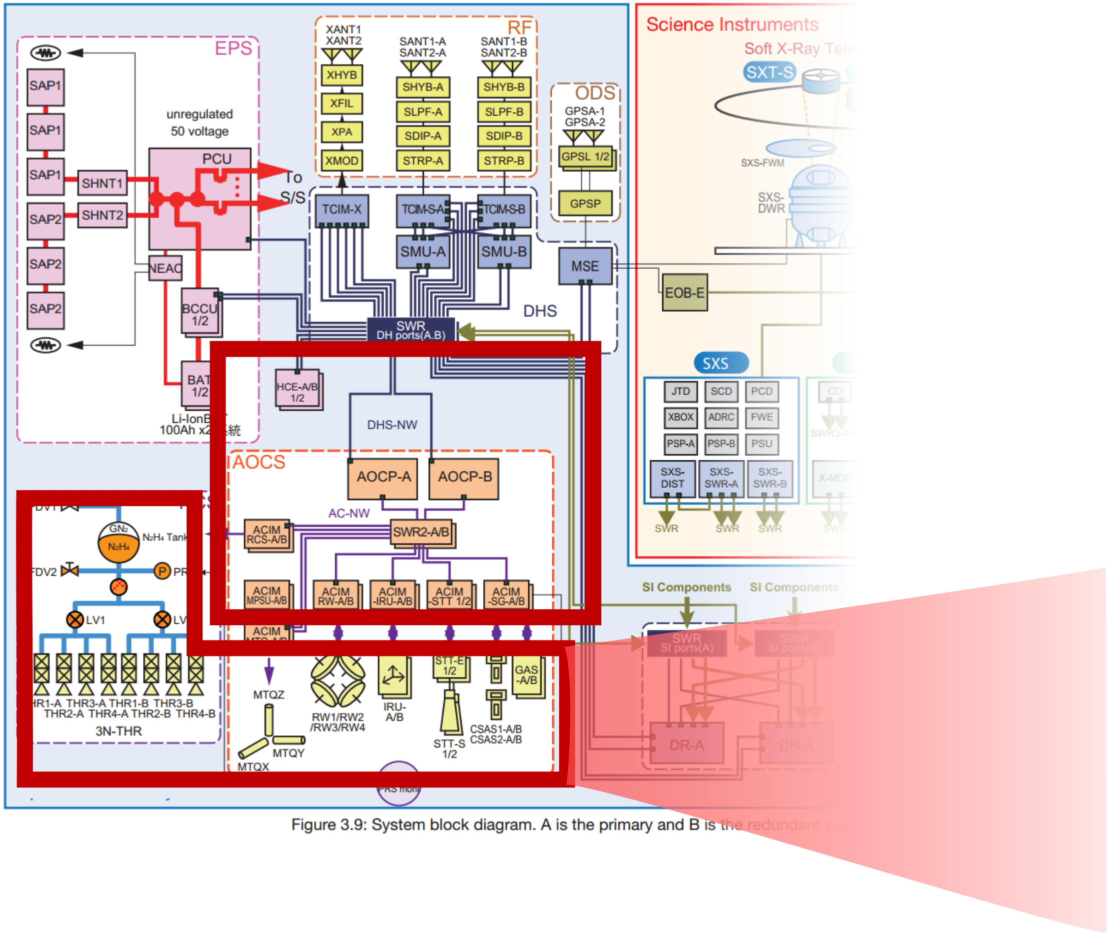
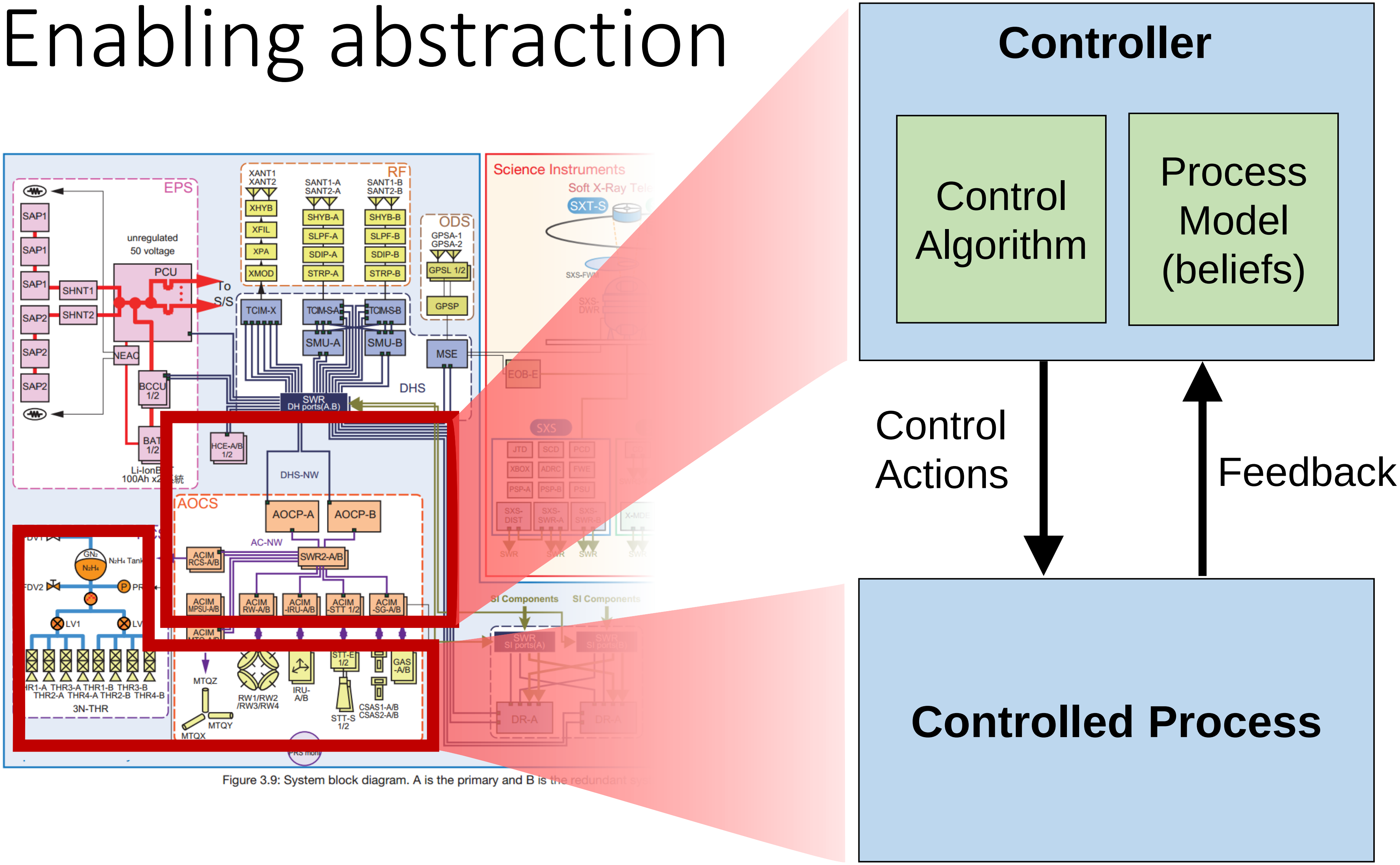


Figure 3.9: System block diagram. A is the primary and B is the redundant sy

Controlled Process

Thomas, 2017

Enabling abstraction



Controller

Control Algorithm

Process Model (beliefs)

Control Actions

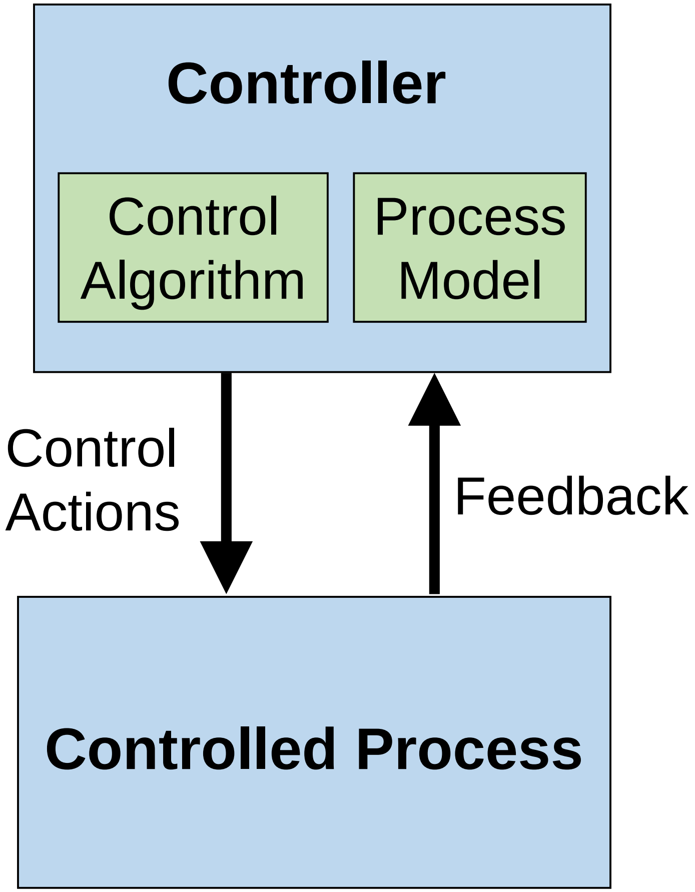
Feedback

Controlled Process

Figure 3.9: System block diagram. A is the primary and B is the redundant sy

Thomas, 2017

Basic control loop



- **Control actions** are provided to affect a controlled process
- **Feedback** may be used to monitor the process
- **Process model** (beliefs) formed based on feedback and other information
- **Control algorithm** determines appropriate control actions given current beliefs

(Leveson, 2012)

Enabling abstraction

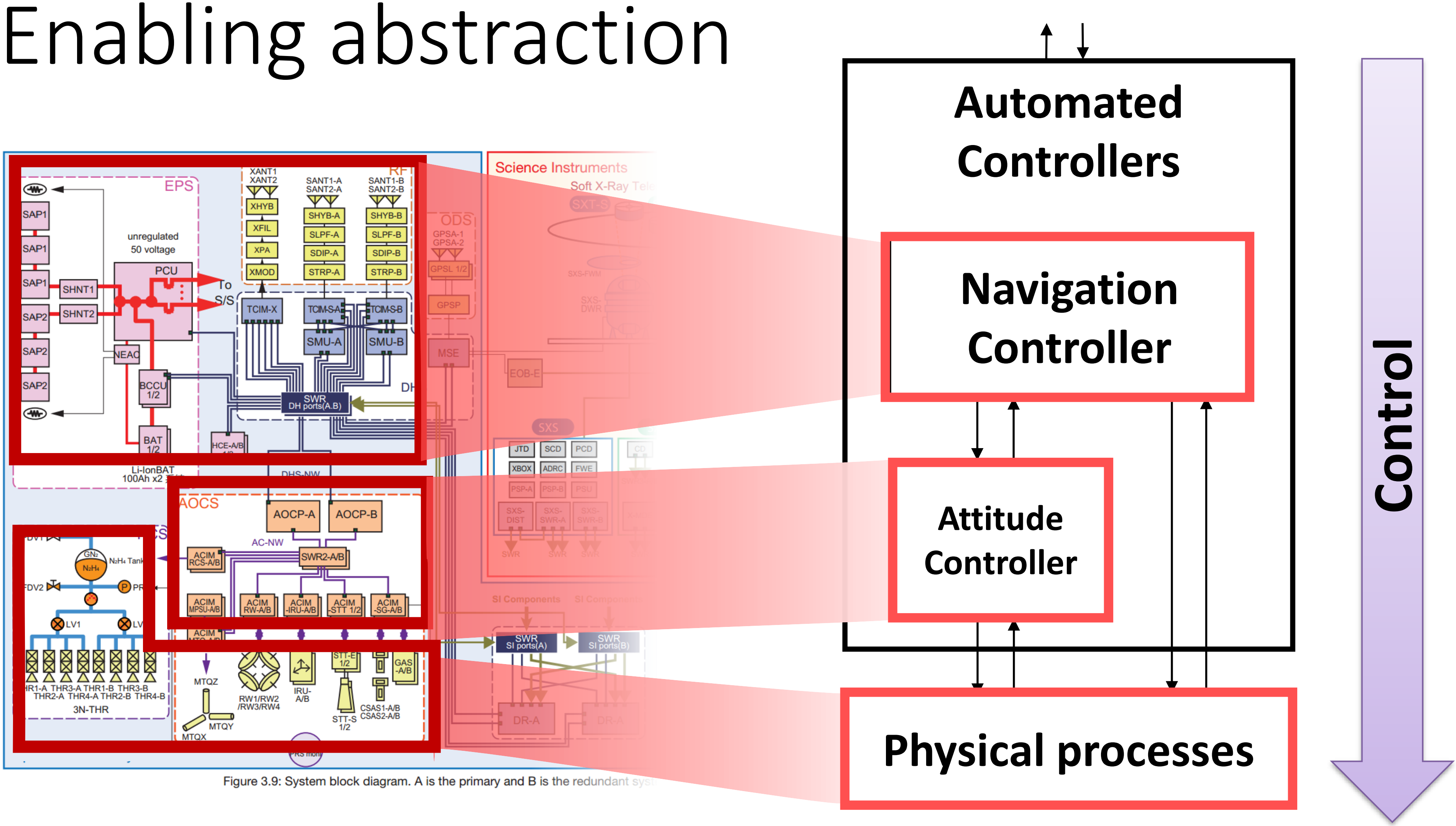


Figure 3.9: System block diagram. A is the primary and B is the redundant sys

Automated Controllers

Navigation Controller

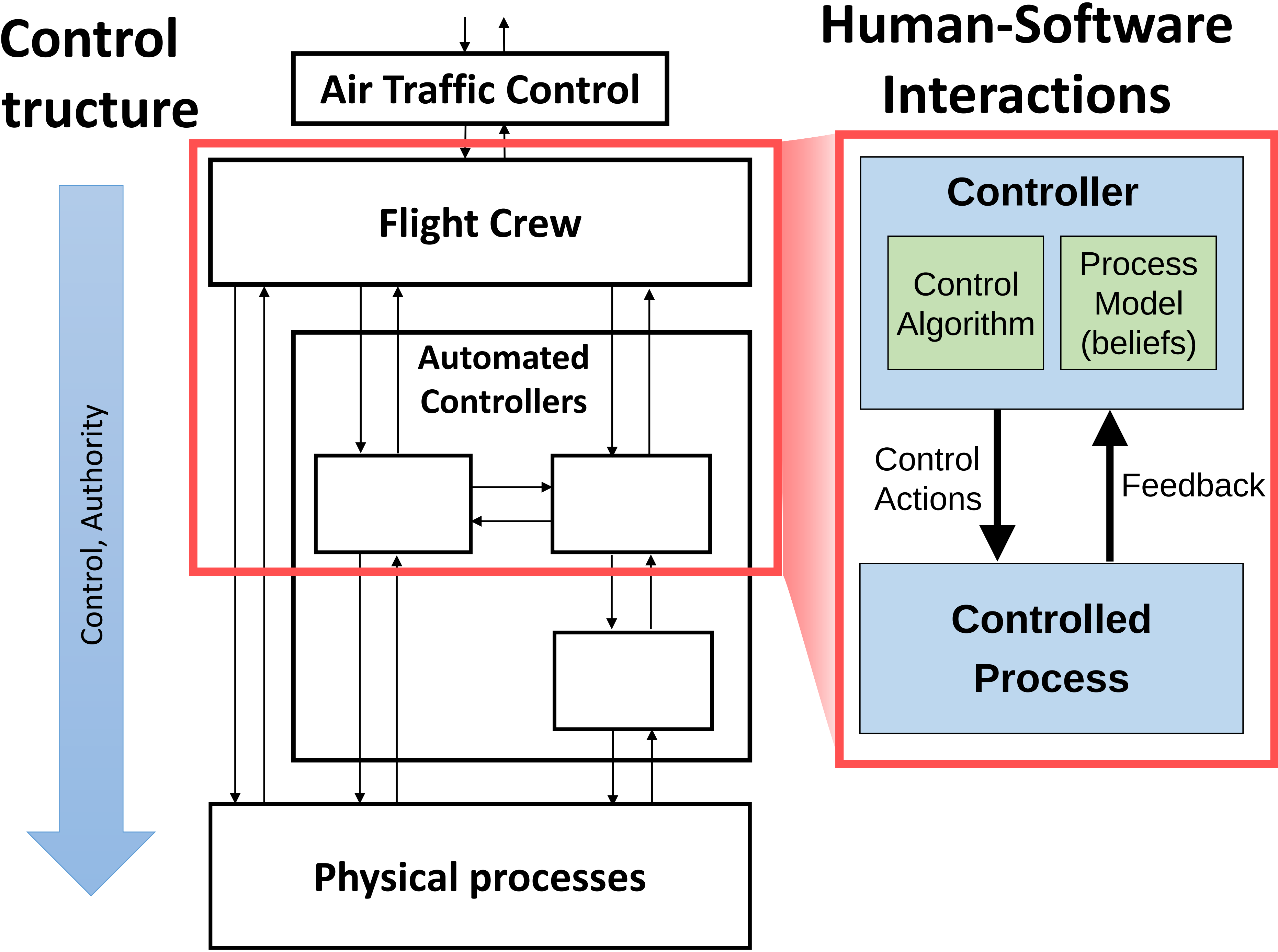
Attitude Controller

Physical processes

Control

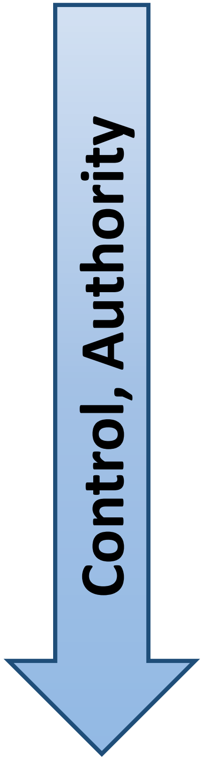
Control structure

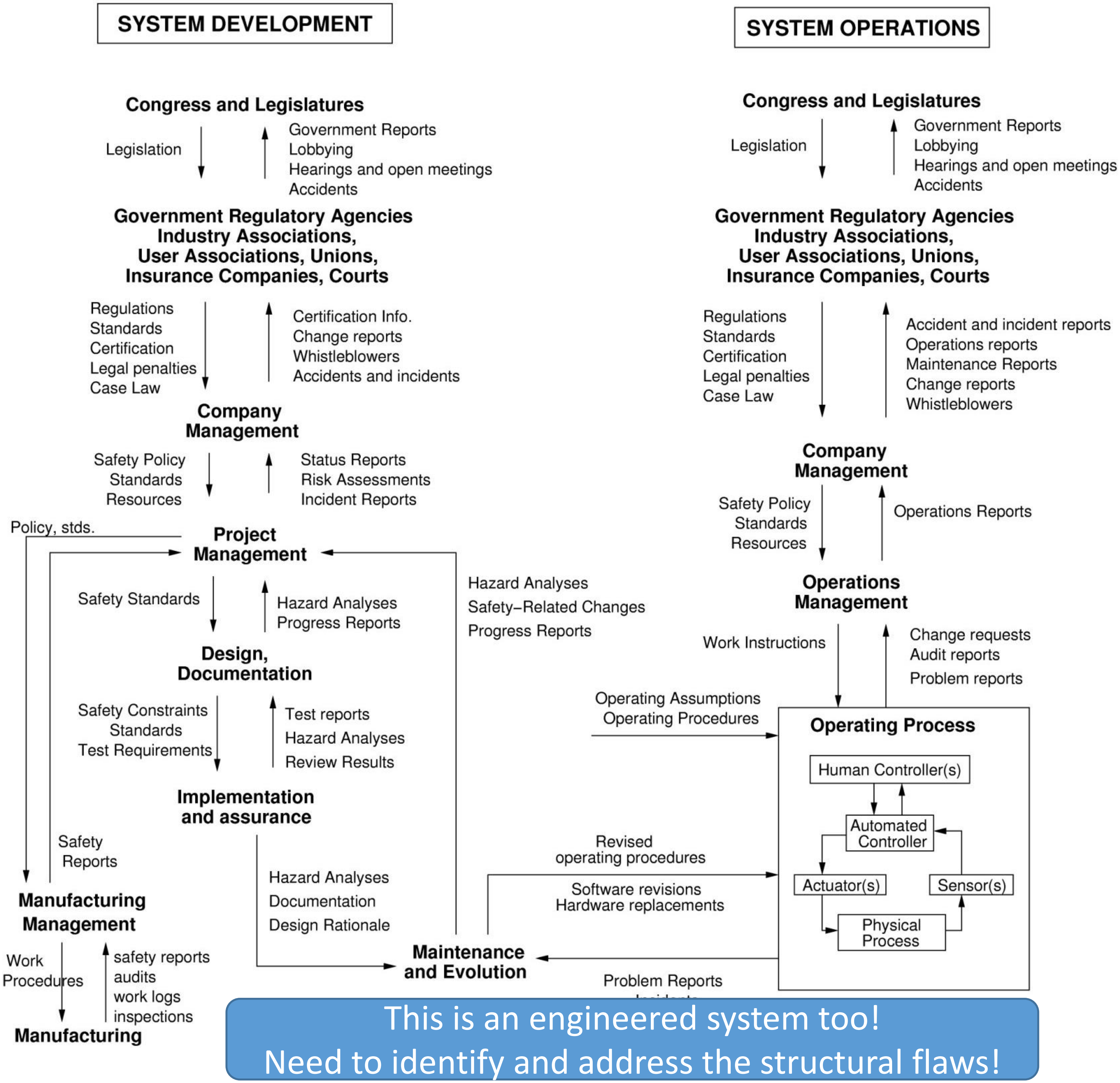
Human-Software Interactions



(Thomas, 2017)

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

This is an engineered system too!
Need to identify and address the structural flaws!

(Leveson, 2012)

Common sentiment: “But that’s too simplistic!”

Bubble Sort: Assembly

```
bs proc
   push bp
   mov bp, sp
   mov si, [bp + 4]
   mov cx, 18
   outer_loop:
        mov si, [bp + 4]
        mov bx, cx
        mov cx, 18
        inner_loop:
            mov al, [si]
            mov ah, 0h
            mov dl, [si + 1]
            mov dh, 0h
            cmp dl, al
            ja finish:
            ;sw
            mov [si + 1], al
            mov [si], dl
            finish:
            inc si
            loop inner_loop
            mov cx, bx
```

```
   loop outer_loop
   mov sp, bp
   pop bp
   retn 2
bs end
sw proc
    push bp
    mov bp, sp
    mov bx, [bp + 4]
    mov al, [bx]
    mov di, [bp + 6]
    mov cl, [di]
    mov [di], al
    mov [bx], cl
    mov sp, bp
    pop bp
    retn 4
sw end
```

Bubble Sort: JAVA

```
void bubbleSort(int arr[]) {
  int n = arr.length;
  for (int i = 0; i < n-1; i++) {
    for (int j = 0; j < n-i-1; j++) {
      if (arr[j] > arr[j+1]) {
        int temp = arr[j];
        arr[j] = arr[j+1];
        arr[j+1] = temp;
      }
    }
  }
}
```

Is complexity really the goal?
Simple is a good thing!

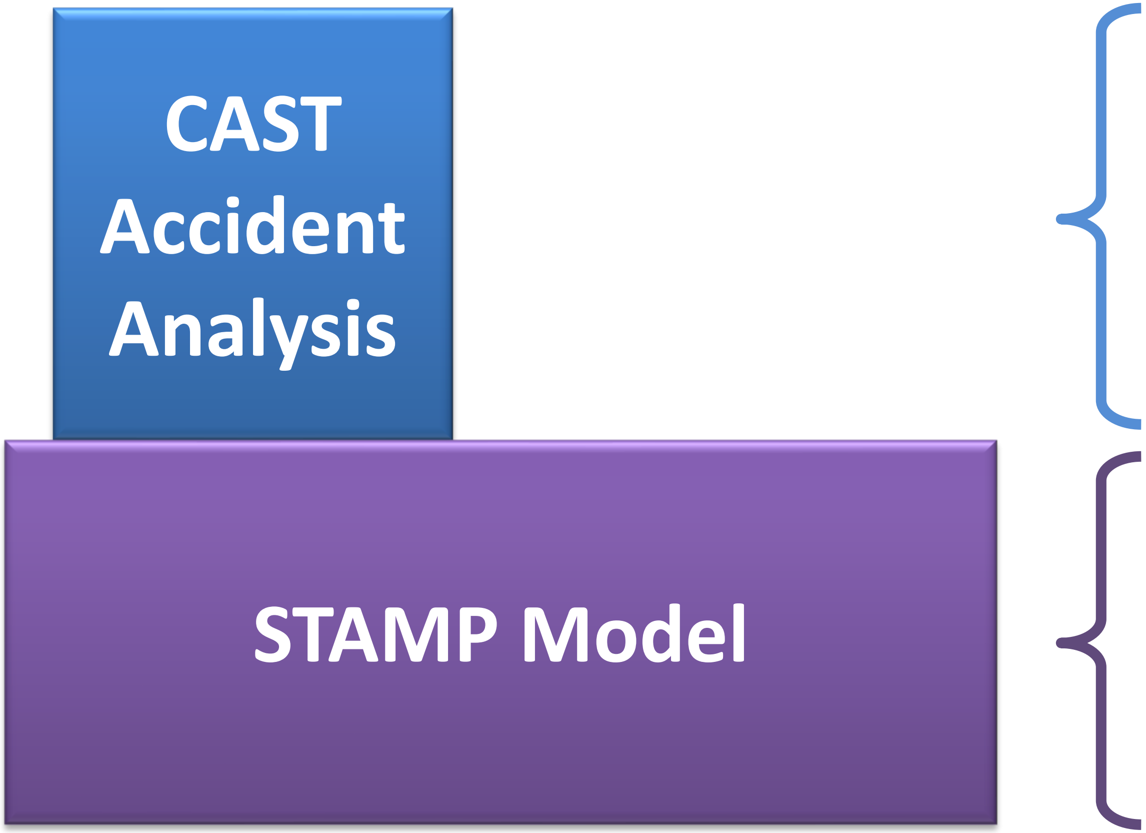
STAMP and STPA

STAMP Model

Accidents are caused by inadequate control

(Leveson, 2012)

STAMP and STPA



CAST Accident Analysis

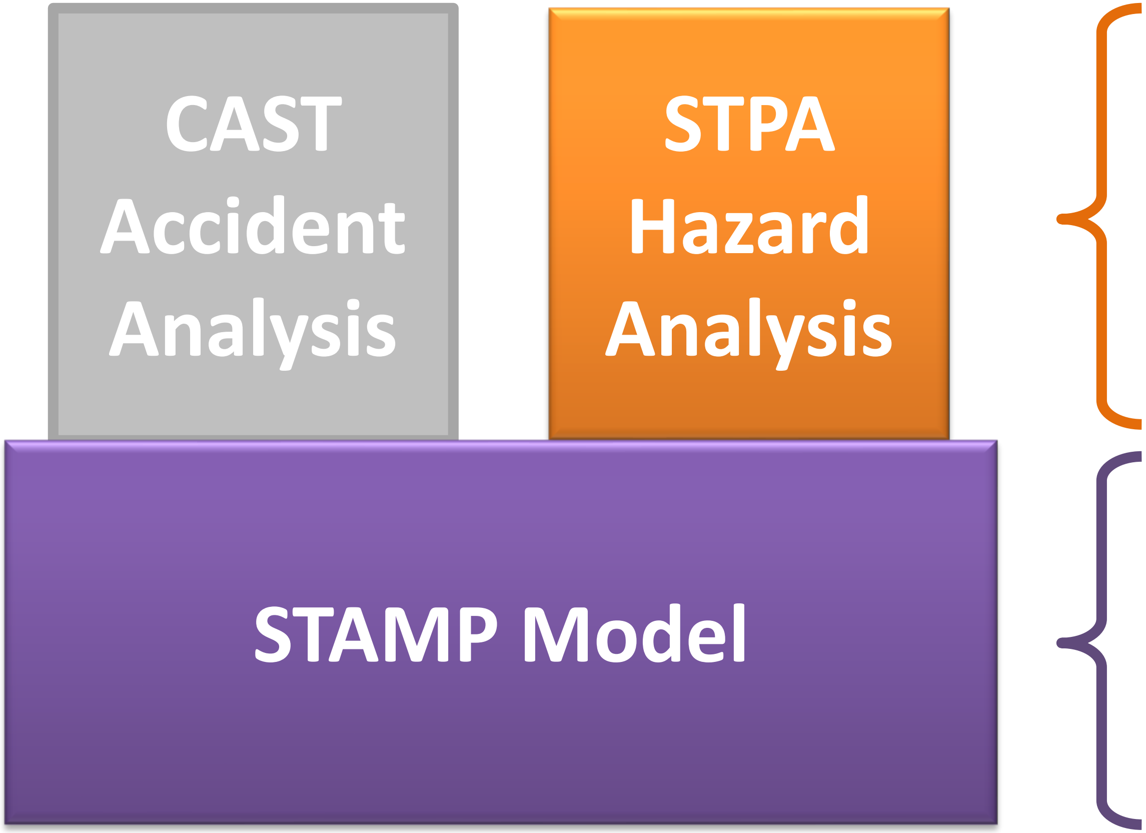
STAMP Model

How do we find inadequate control that caused a previous accident?

Accidents are caused by inadequate control

(Leveson, 2012)

STAMP and STPA



CAST Accident Analysis

STPA Hazard Analysis

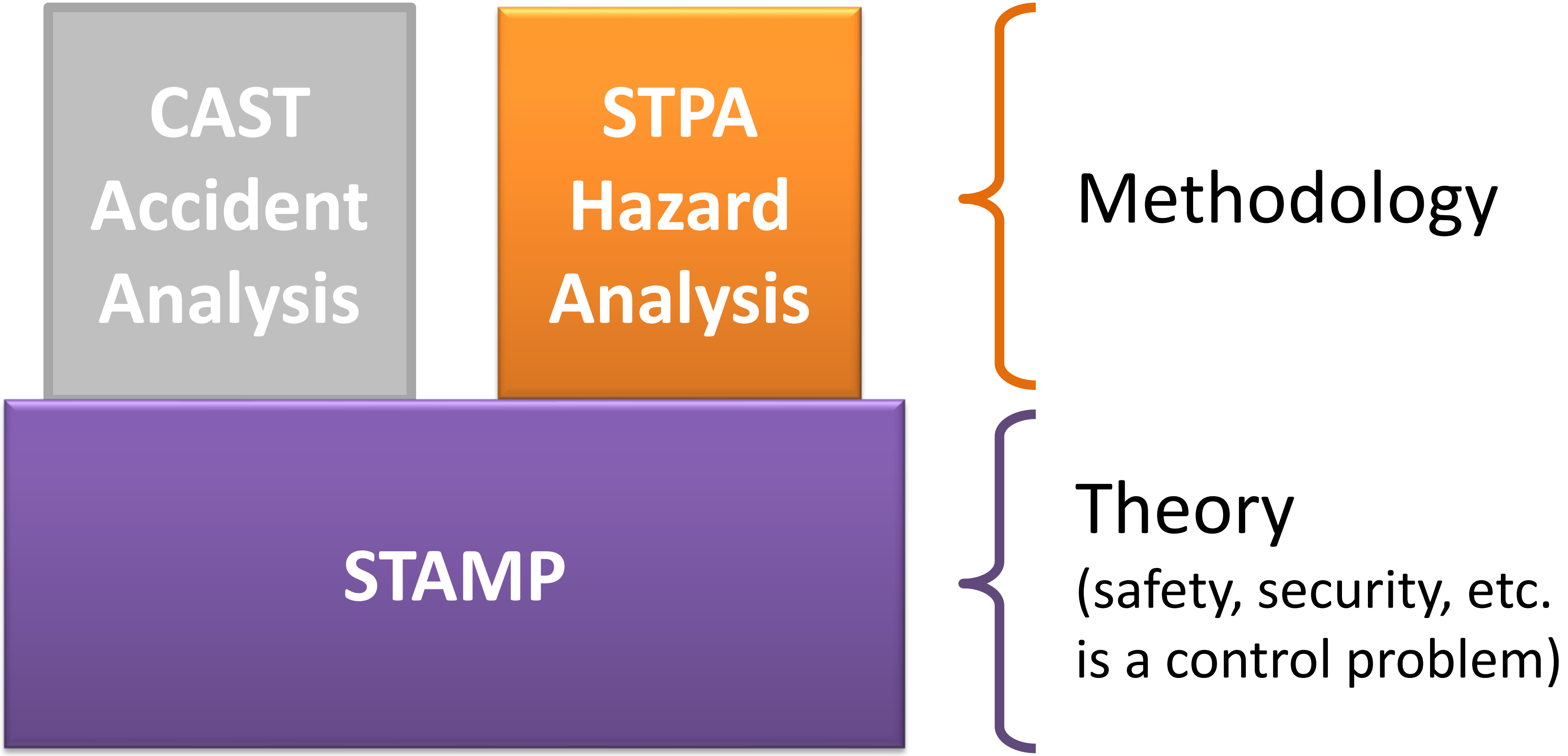
STAMP Model

How do we find inadequate controls in a system?

Accidents are caused by inadequate control

(Leveson, 2012)

STAMP and STPA



CAST Accident Analysis

STPA Hazard Analysis

STAMP

Methodology

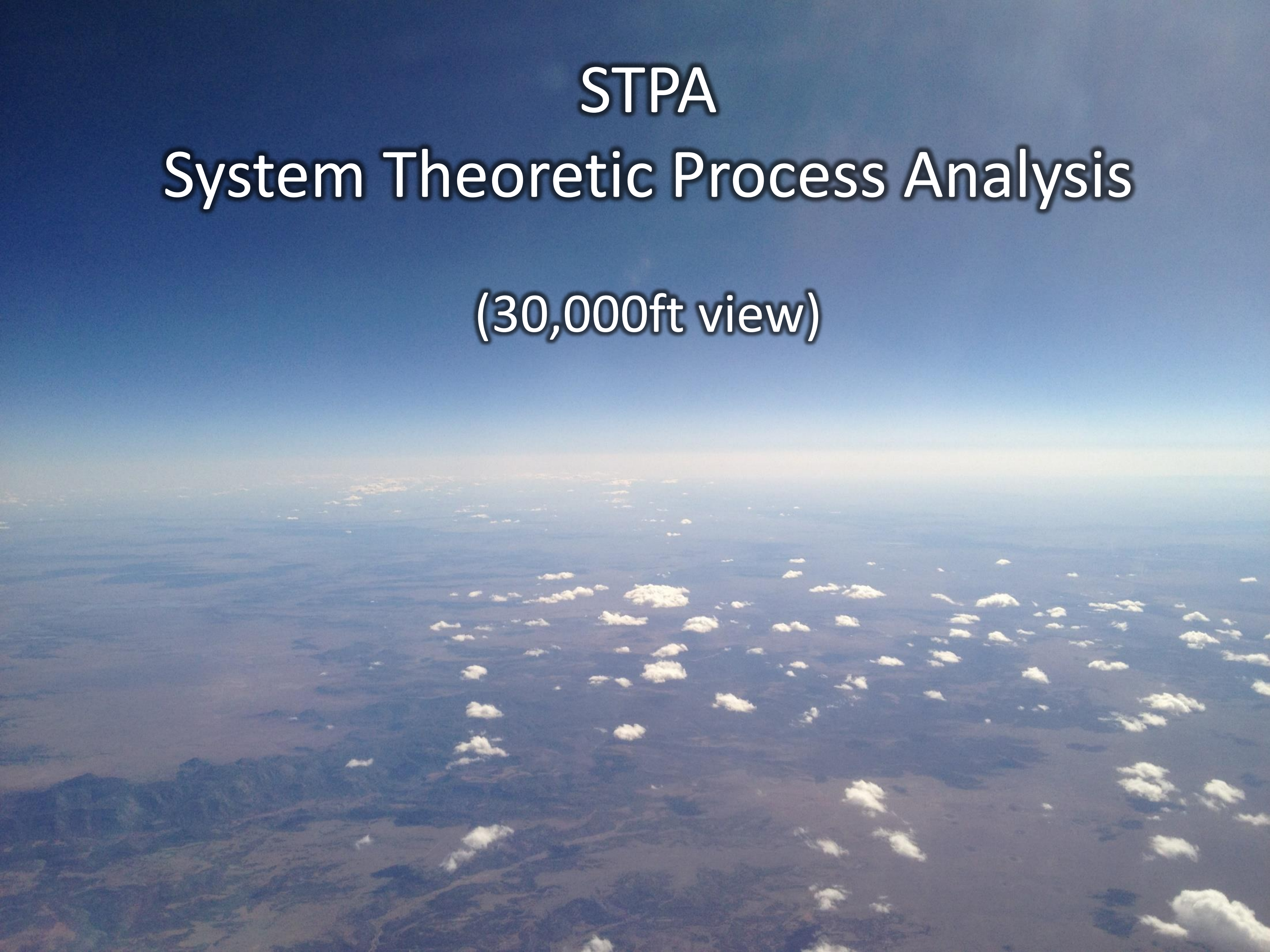
Theory

(safety, security, etc. is a control problem)

(Leveson, 2012)

STPA
System Theoretic Process Analysis

(30,000ft view)



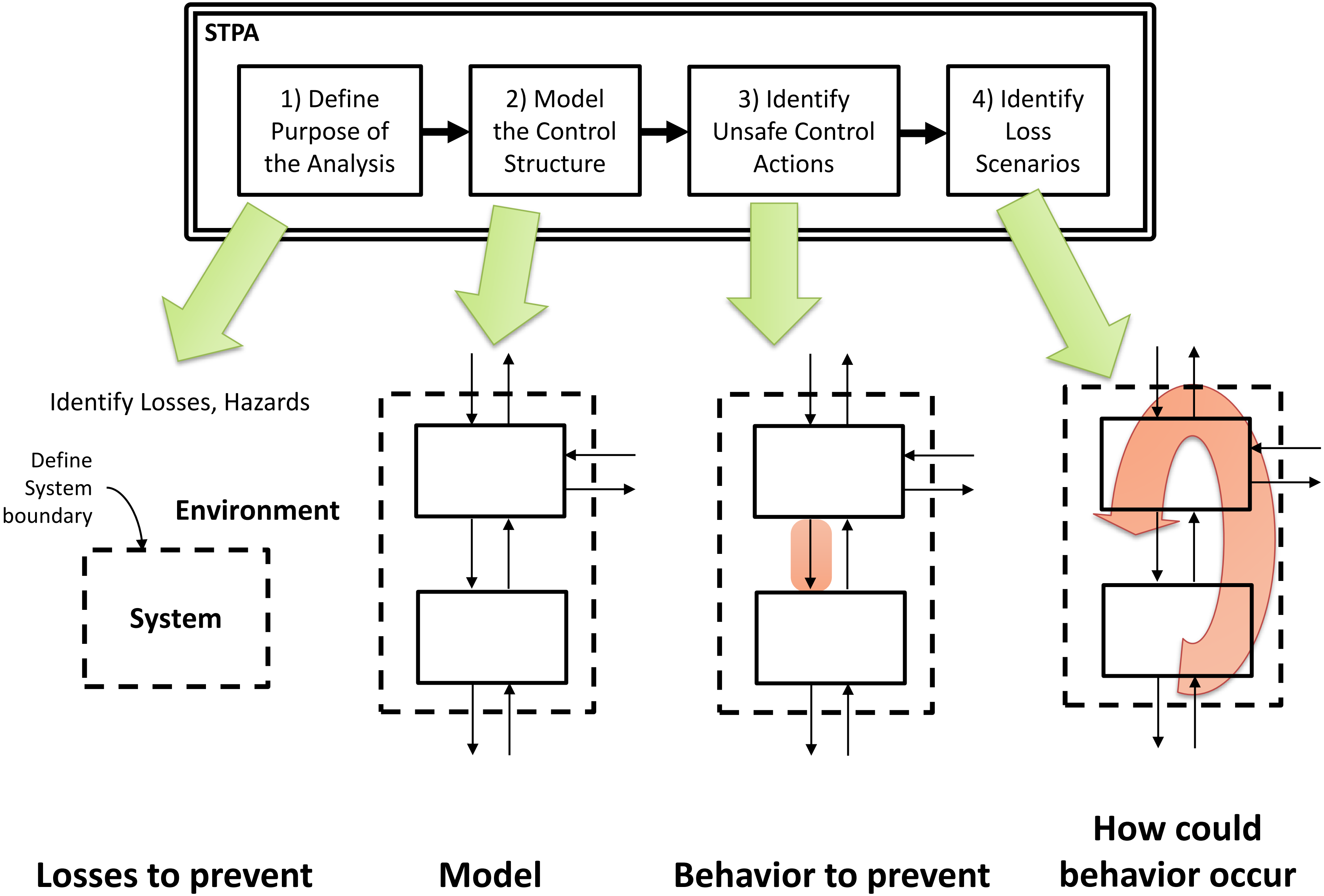
System-Theoretic Process Analysis (STPA)

STPA is a technique for development and safety assessment

STPA can help anticipate hazardous scenarios caused by:

- Software, computers, and automation
- Human error/confusion
- System design errors
- Flawed assumptions
- Missing design requirements
- Interactions between systems

Thomas, 2013



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

Losses to prevent

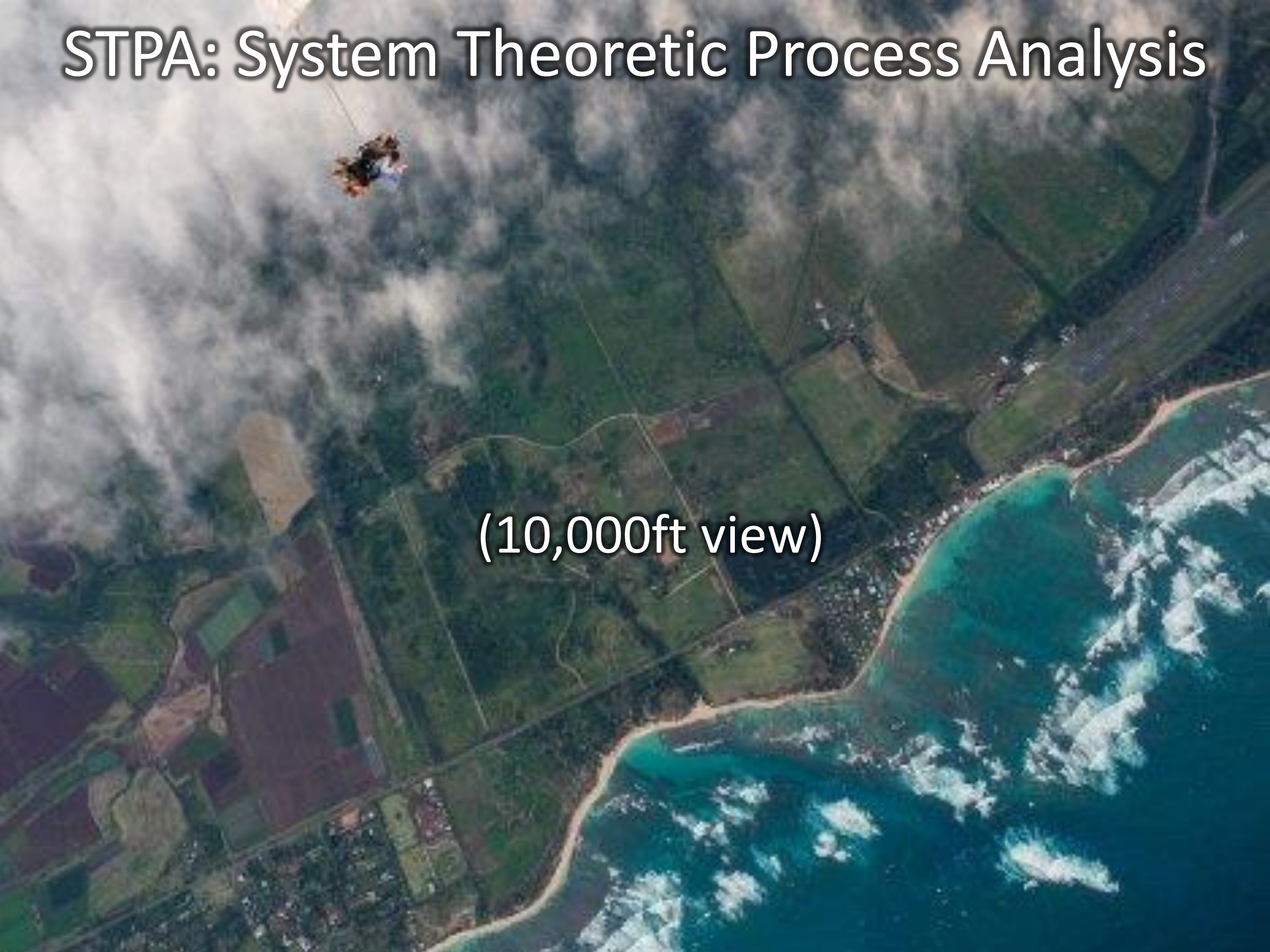
Model

Behavior to prevent

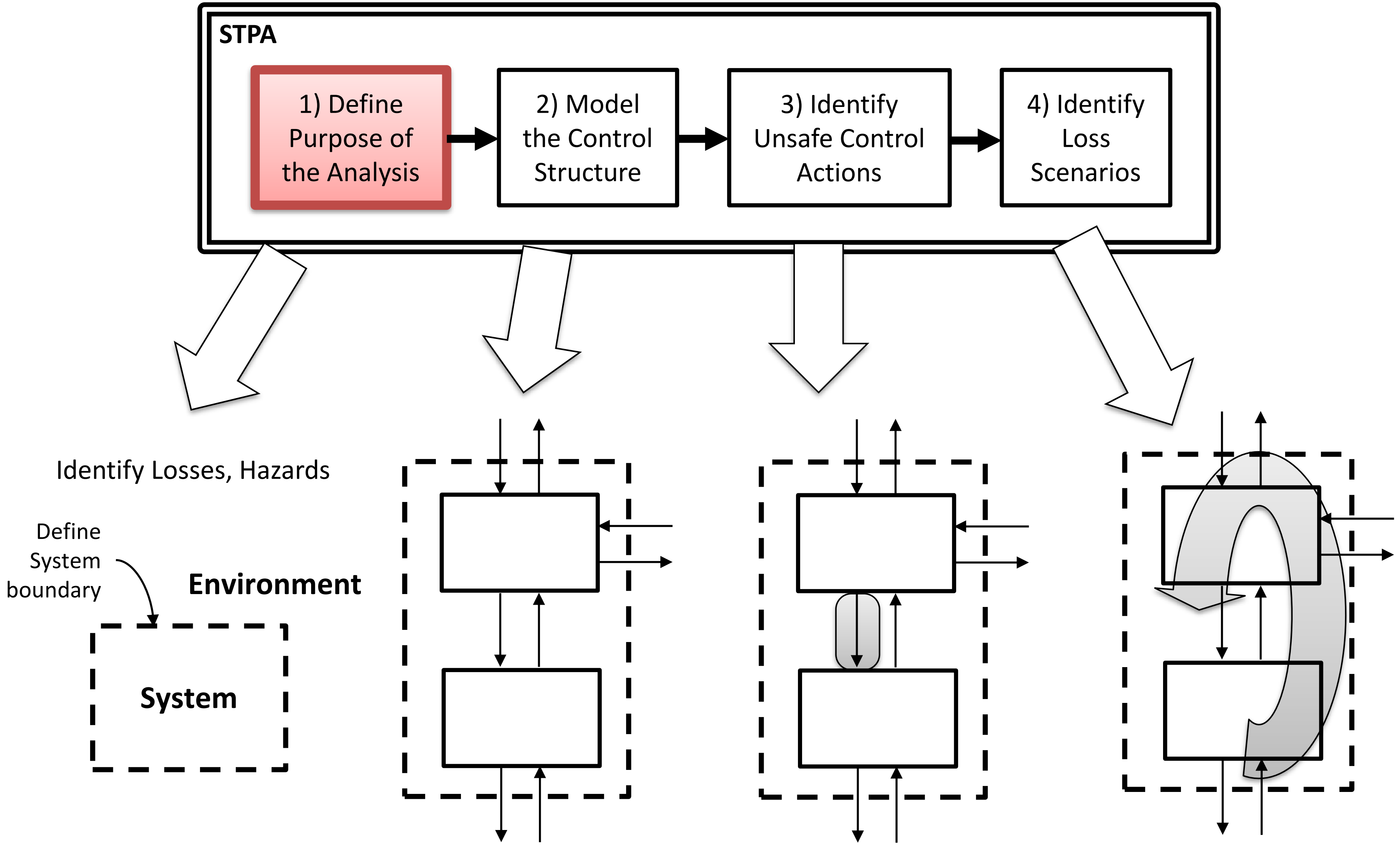
How could behavior occur

(Leveson and Thomas, 2018)

STPA: System Theoretic Process Analysis



(10,000ft view)



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

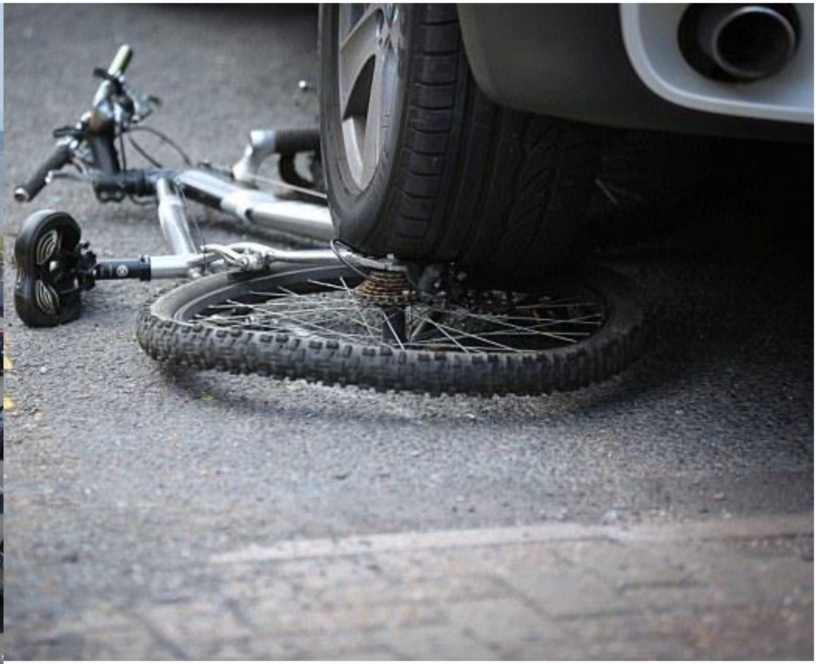
(Leveson and Thomas, 2018)

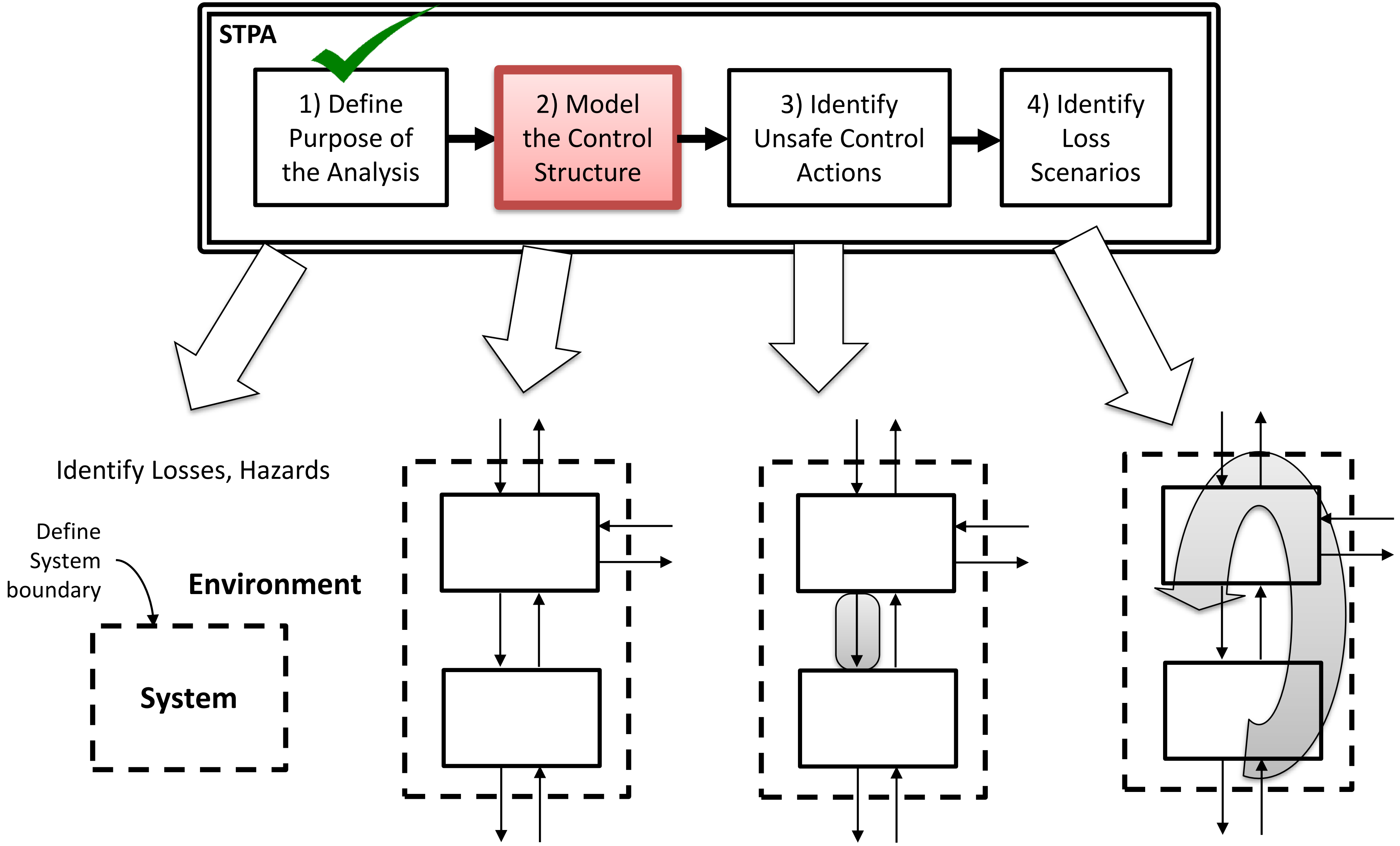
Automotive Example

- Losses
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the vehicle or objects outside the vehicle

Automotive Example

- Losses
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the vehicle or objects outside the vehicle
  - L-3: Loss of mission (transportation)
  - L-4: Loss of customer satisfaction




STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

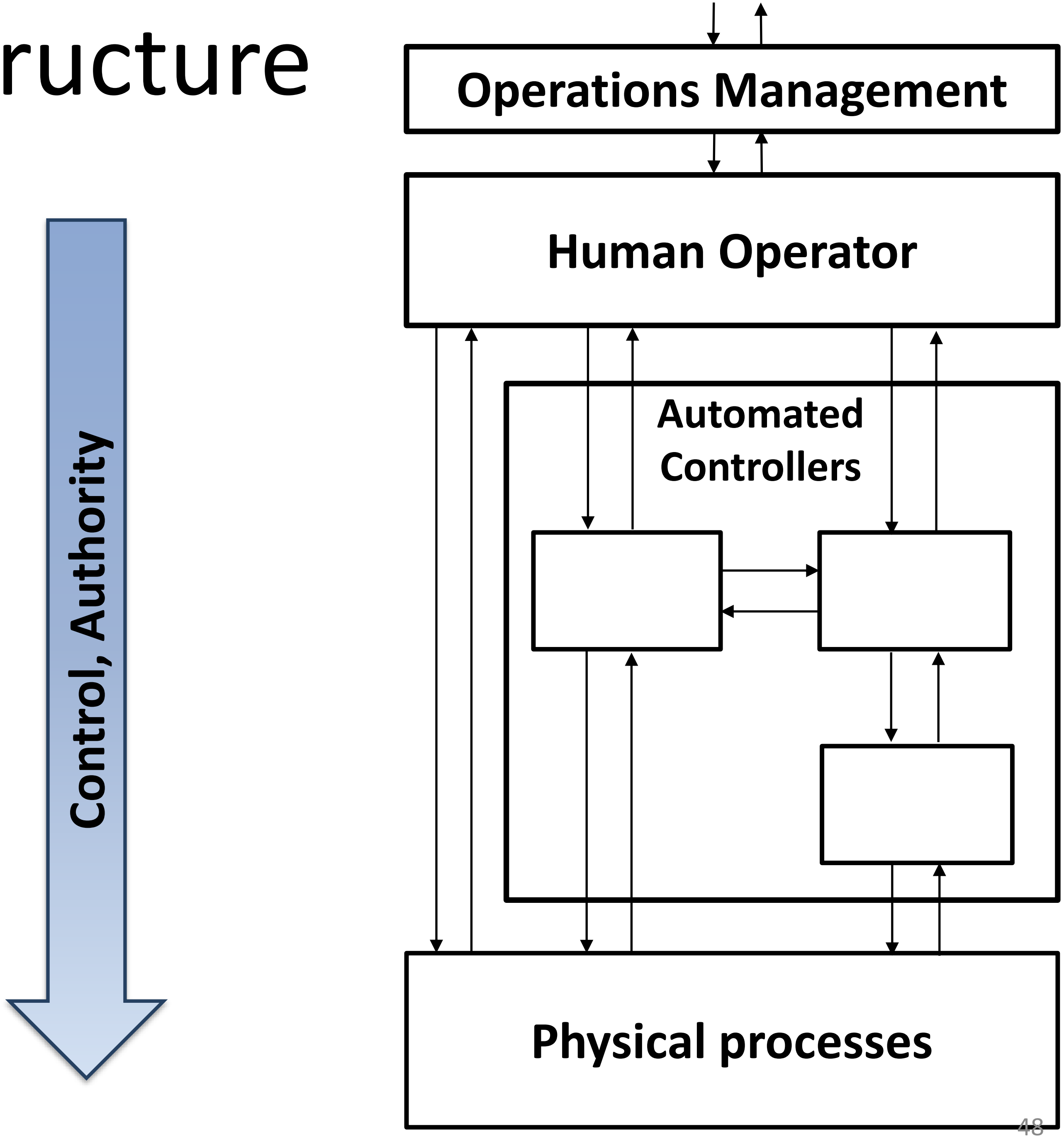
Define System boundary

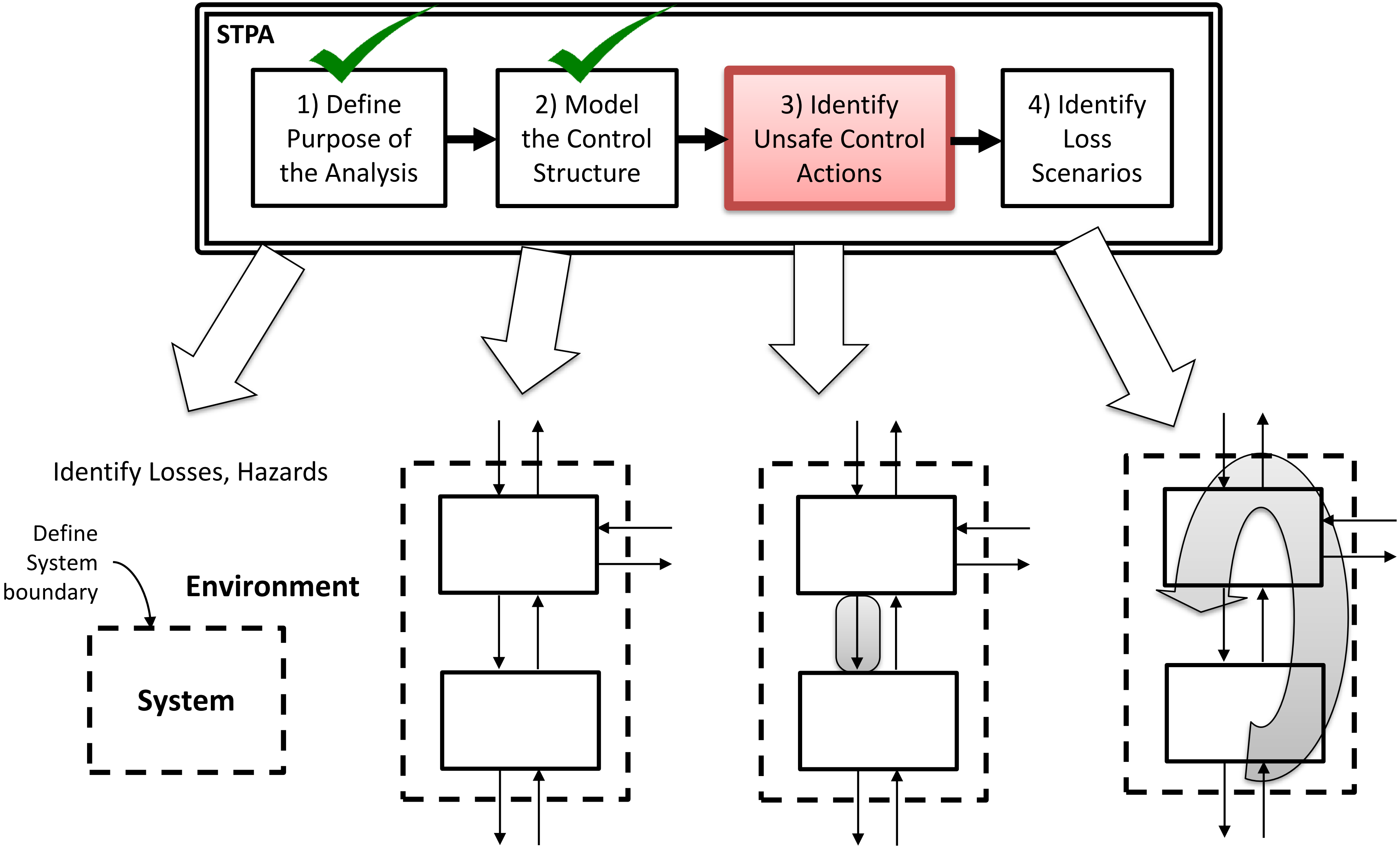
Environment

System

(Leveson and Thomas, 2018)

Control structure





STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

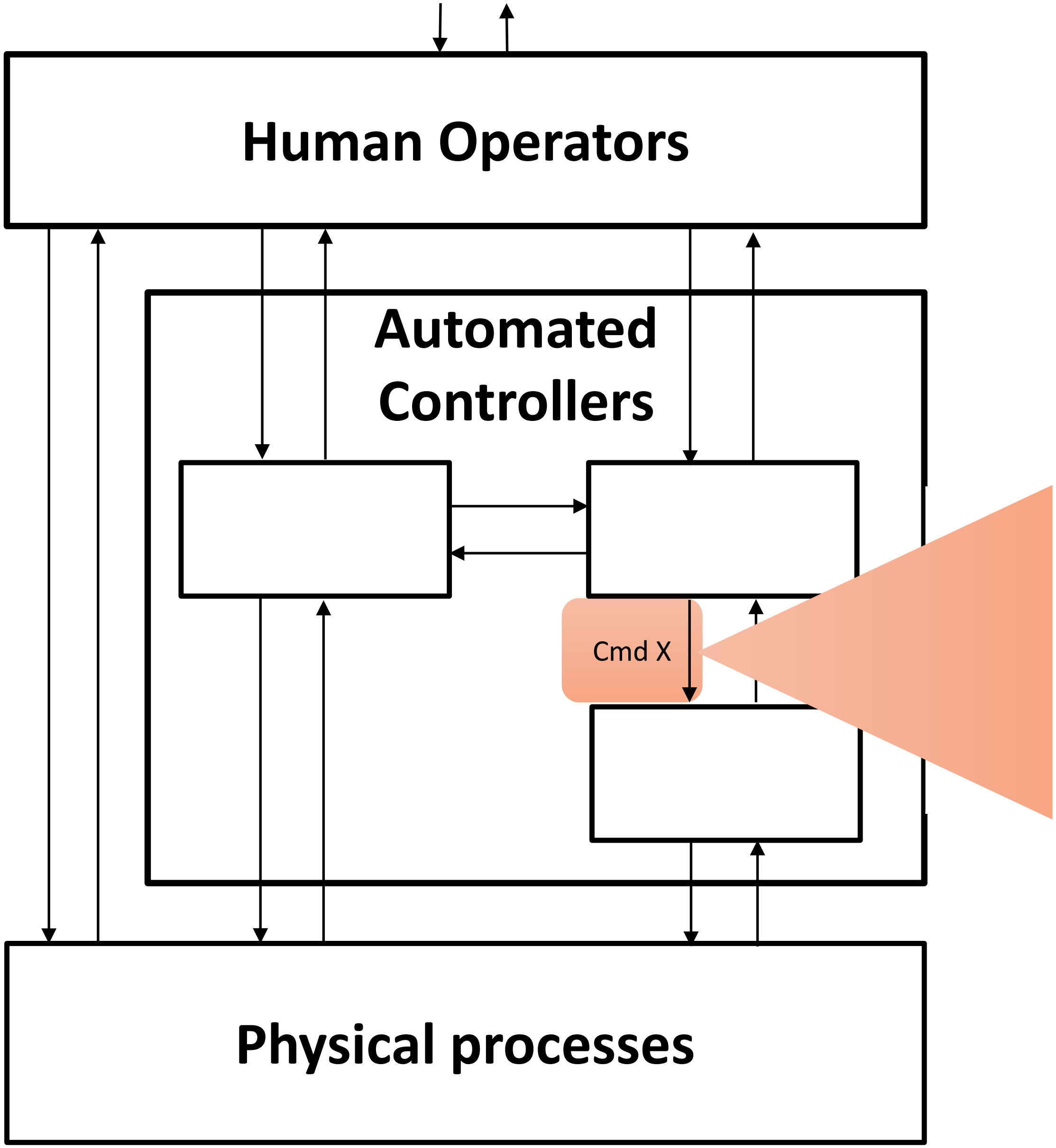
Define System boundary

Environment

System

(Leveson and Thomas, 2018)

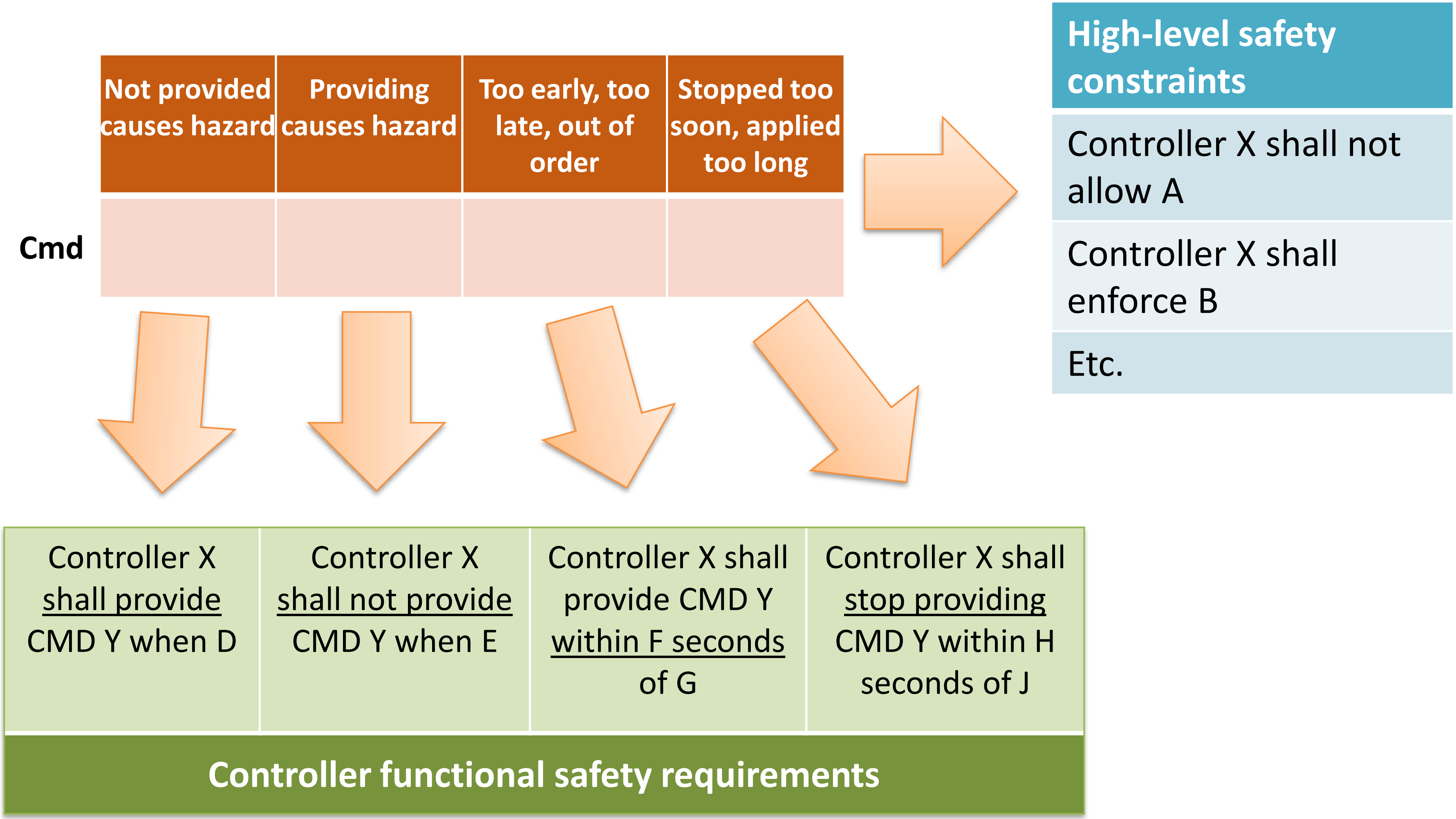
STPA: Identify Unsafe Control Actions (UCA)



Not provided causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long

(Thomas, 2017)

Generating constraints and requirements



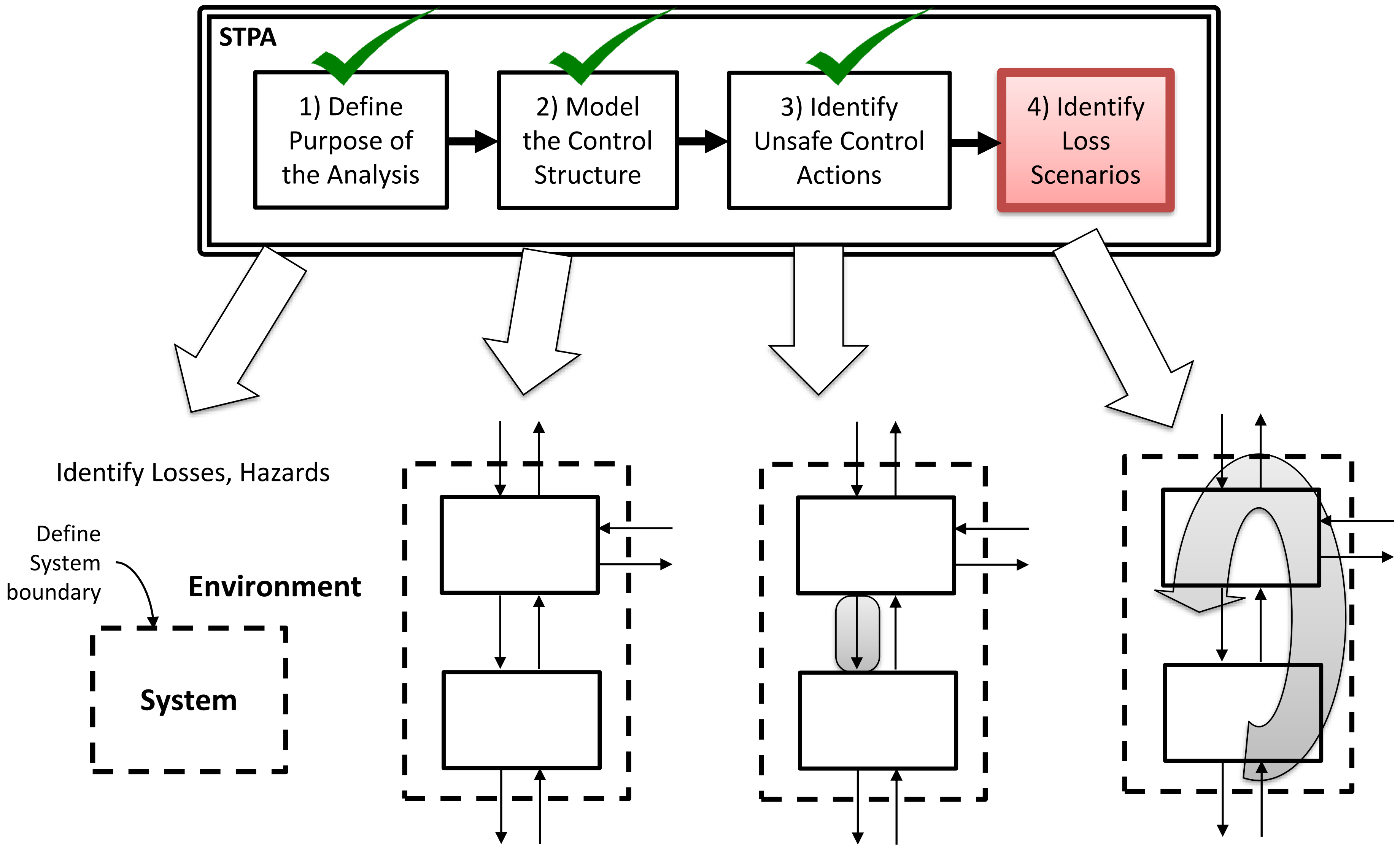
	Not provided causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Cmd				

High-level safety constraints
Controller X shall not allow A
Controller X shall enforce B
Etc.

Controller X shall provide CMD Y when D	Controller X shall not provide CMD Y when E	Controller X shall provide CMD Y within F seconds of G	Controller X shall stop providing CMD Y within H seconds of J

Controller functional safety requirements

(Thomas, 2017)



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

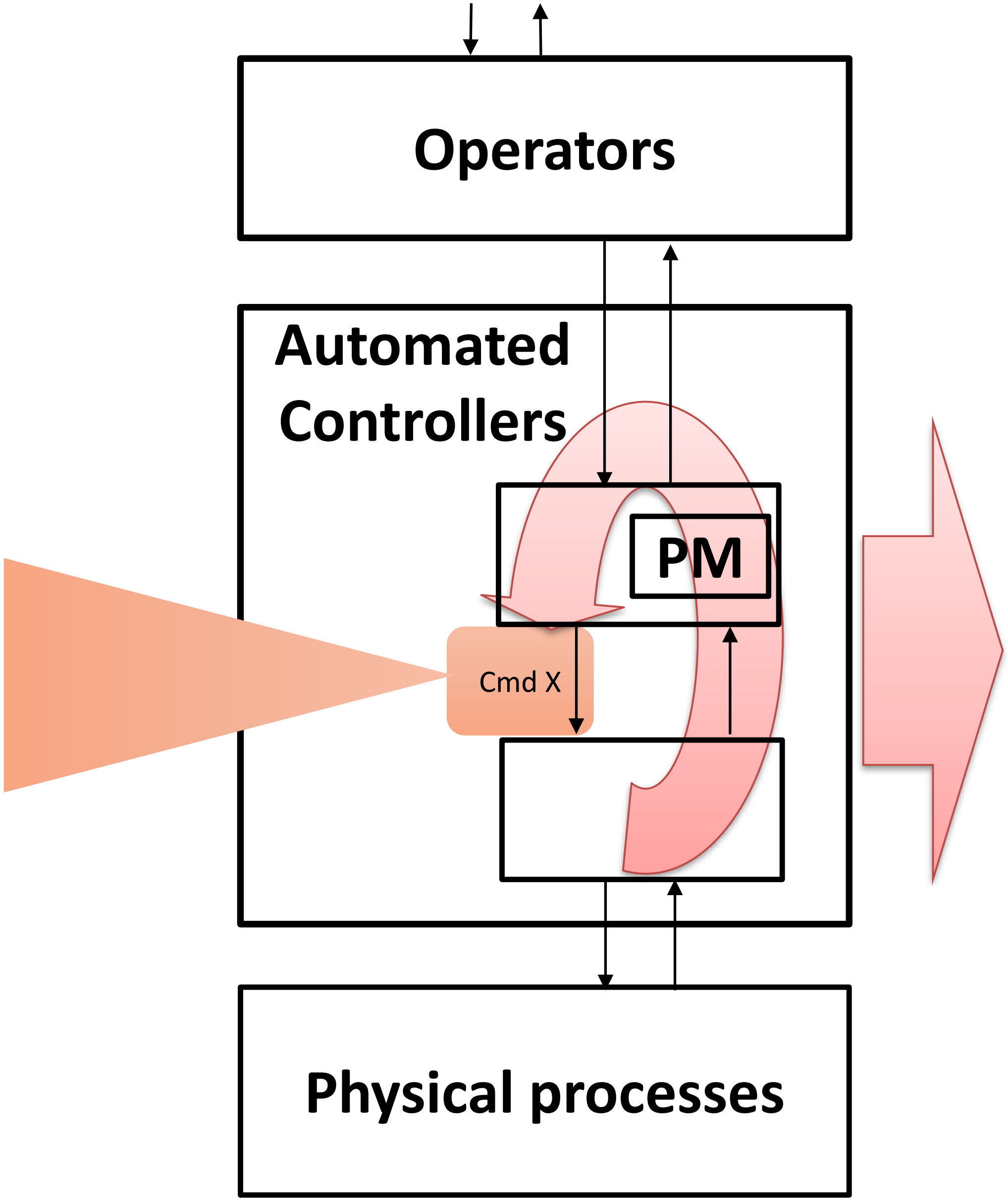
Environment

System

(Leveson and Thomas, 2018)

Identify loss scenarios

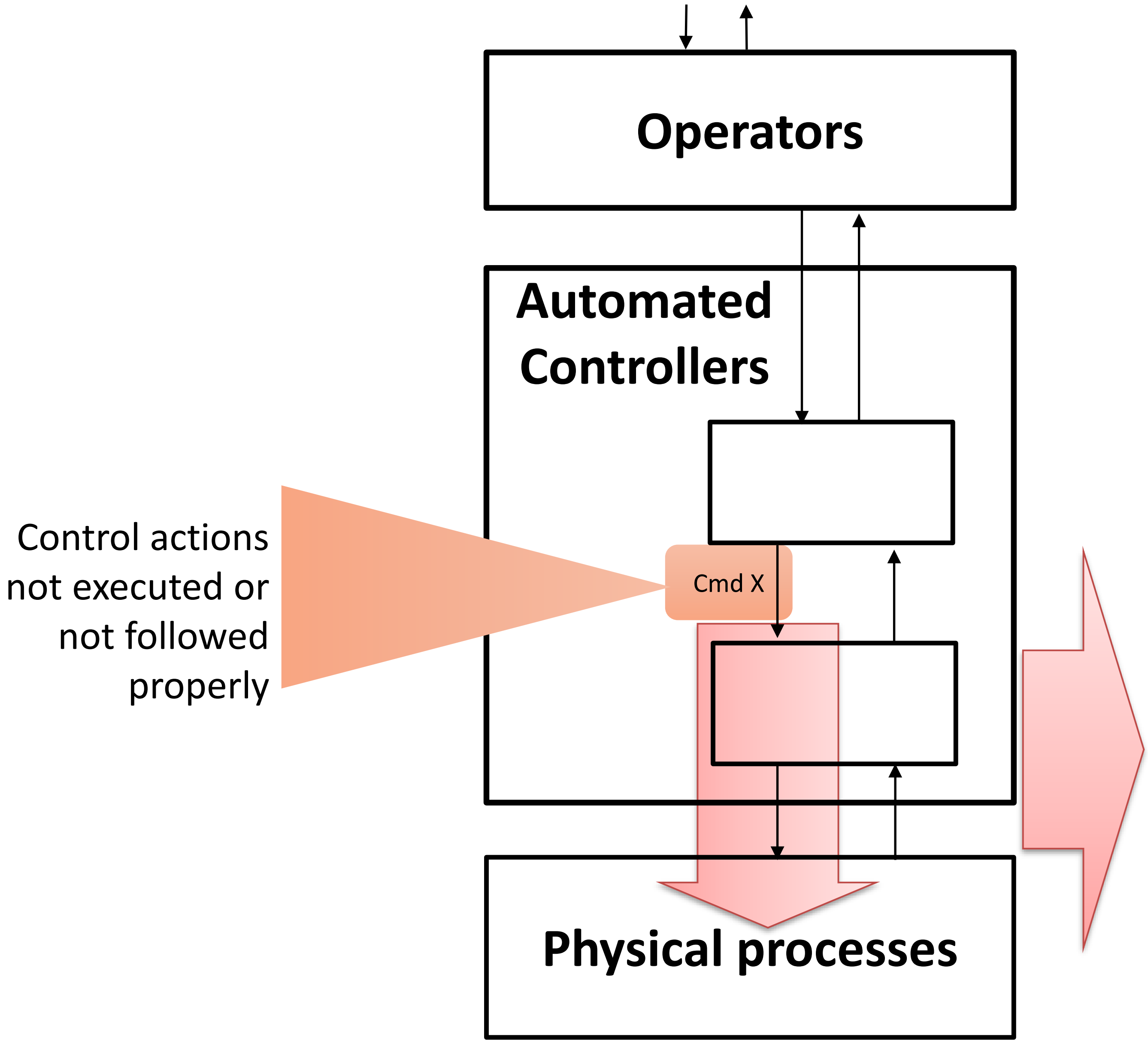
What could cause Unsafe Control Actions?



Scenarios
Controller incorrectly believes X because …
Controller control algorithm does not enforce Y because …
Incorrect feedback Z received because …
Sensor failure causes…
Etc.

(John Thomas, 2017)

Identify loss scenarios



Operators

Automated Controllers

Control actions not executed or not followed properly

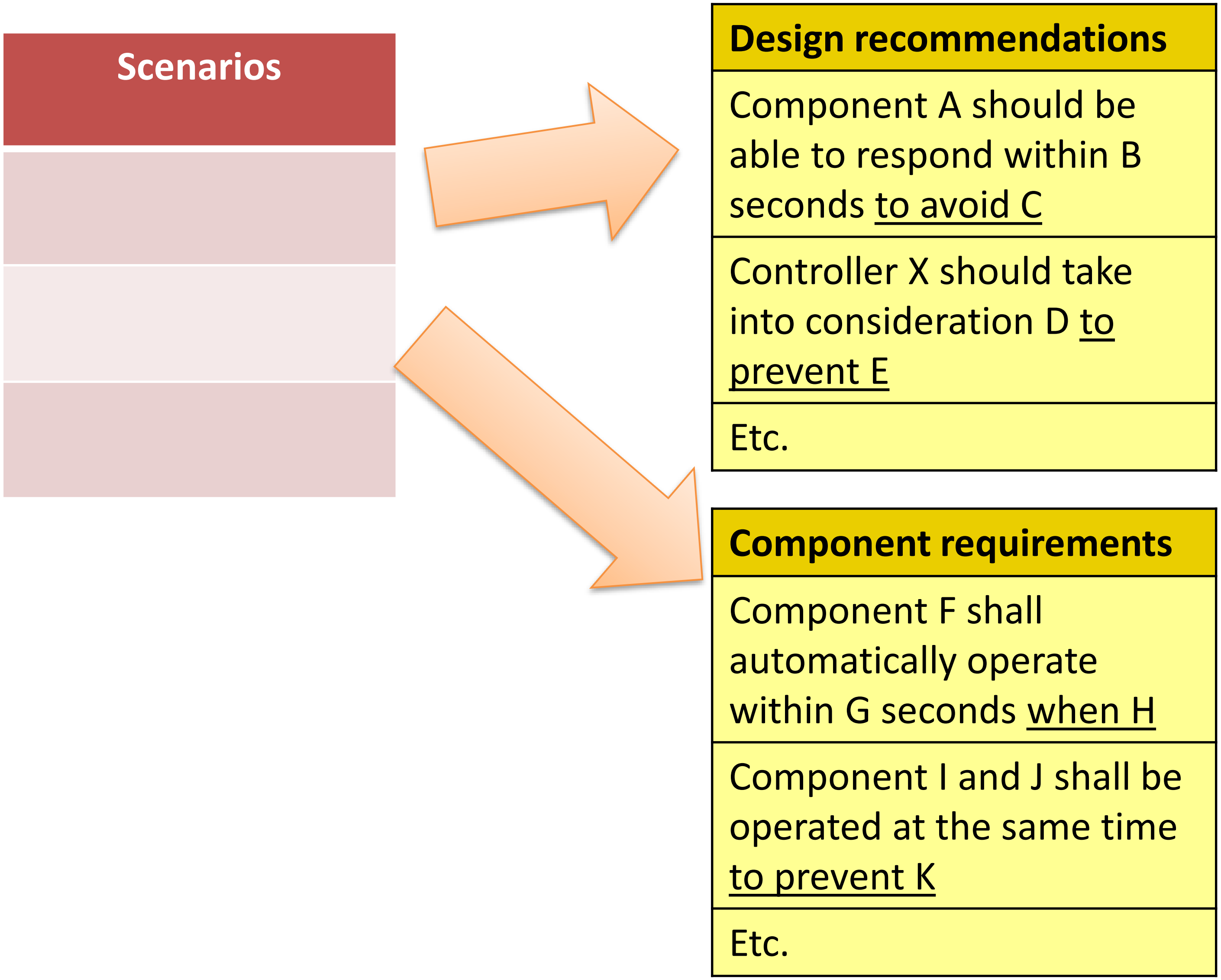
Cmd X

Physical processes

Scenarios
Cmd sent but not received because…
Cmd received but ignored because…
Actuator failure causes…

(Thomas, 2017)

Design recommendations and component requirements



Scenarios

Design recommendations
Component A should be able to respond within B seconds to avoid C
Controller X should take into consideration D to prevent E
Etc.

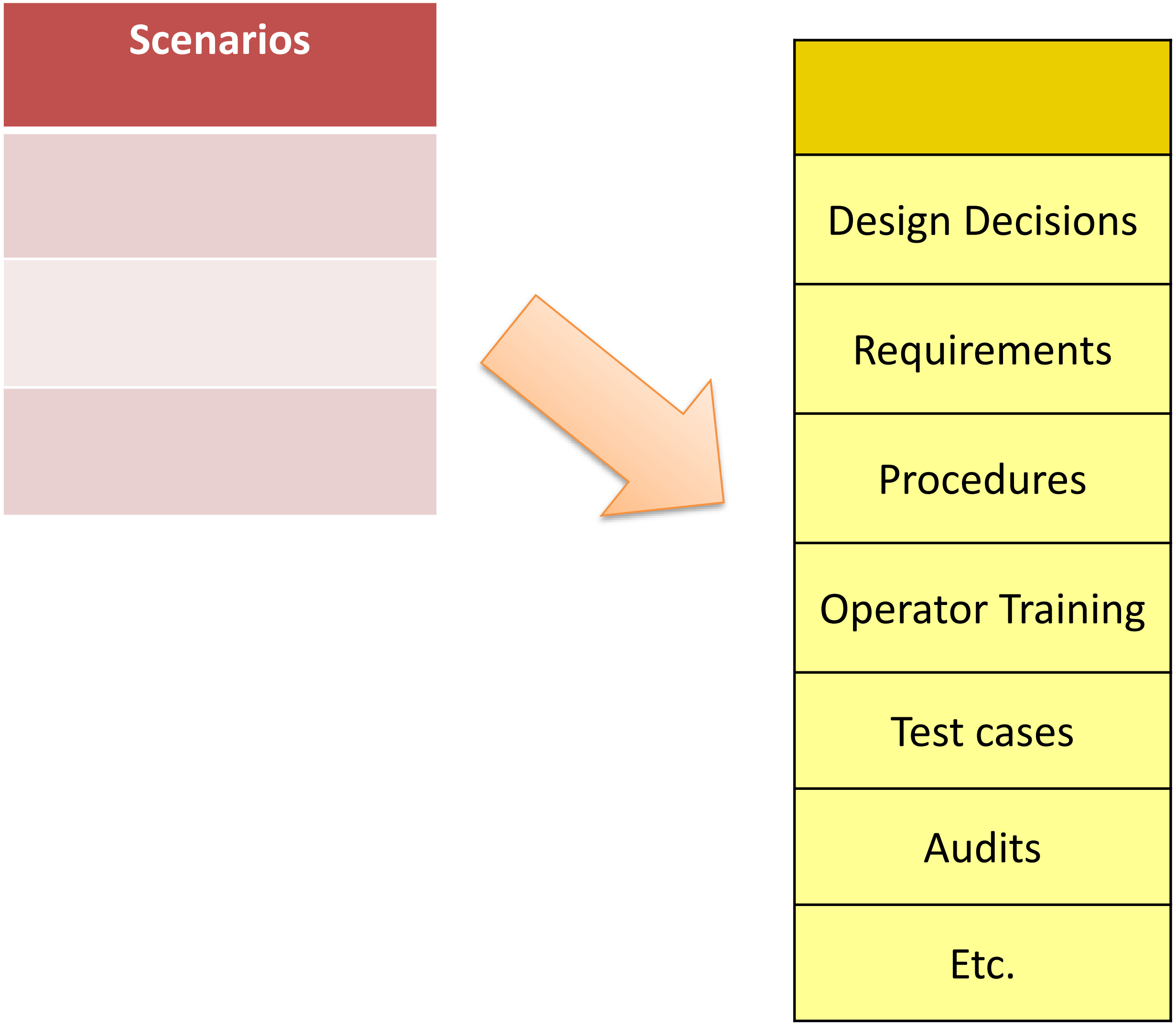
Component requirements
Component F shall automatically operate within G seconds when H
Component I and J shall be operated at the same time to prevent K
Etc.

Rationale and assumptions identified

Every recommendation and requirement is traceable

(Thomas, 2017)

Design decisions, requirements, training, test cases, audits, etc.



Scenarios

Design Decisions

Requirements

Procedures

Operator Training

Test cases

Audits

Etc.

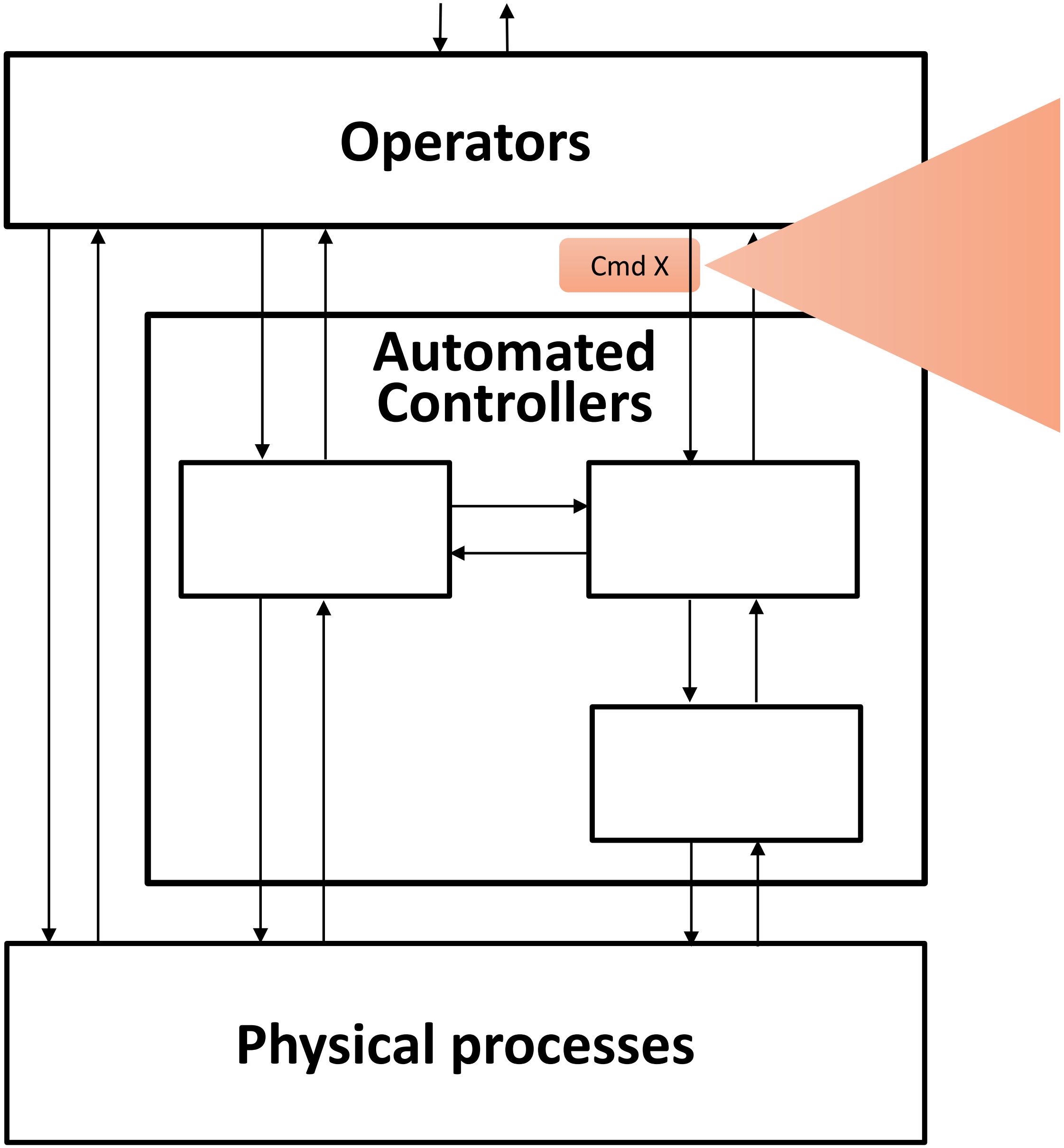
Rationale and assumptions identified

Every recommendation and decision is traceable

(Thomas, 2017)

What about human interactions?

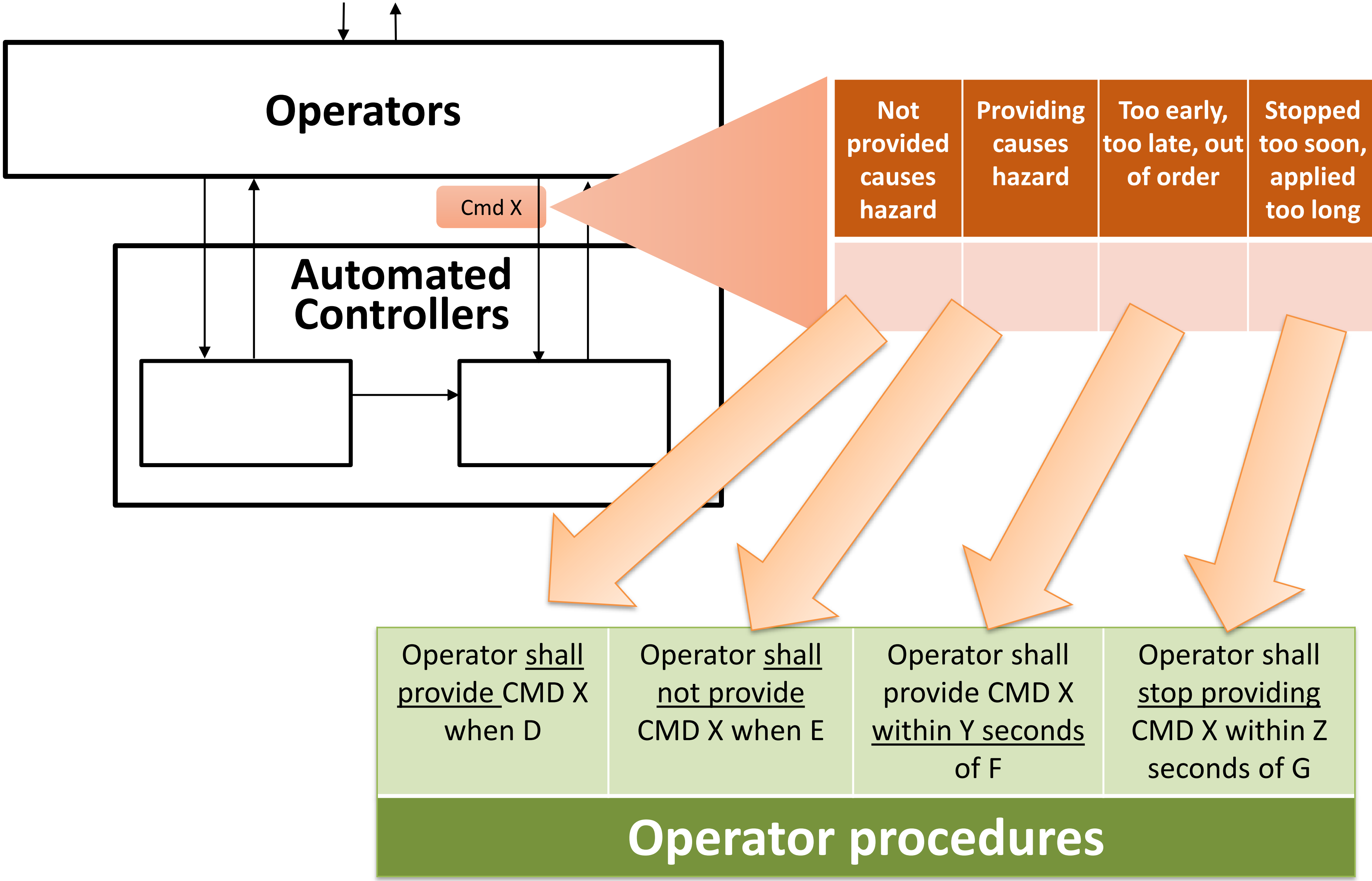
Unsafe Control Actions (UCA)



Not provided causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long

(Thomas, 2017)

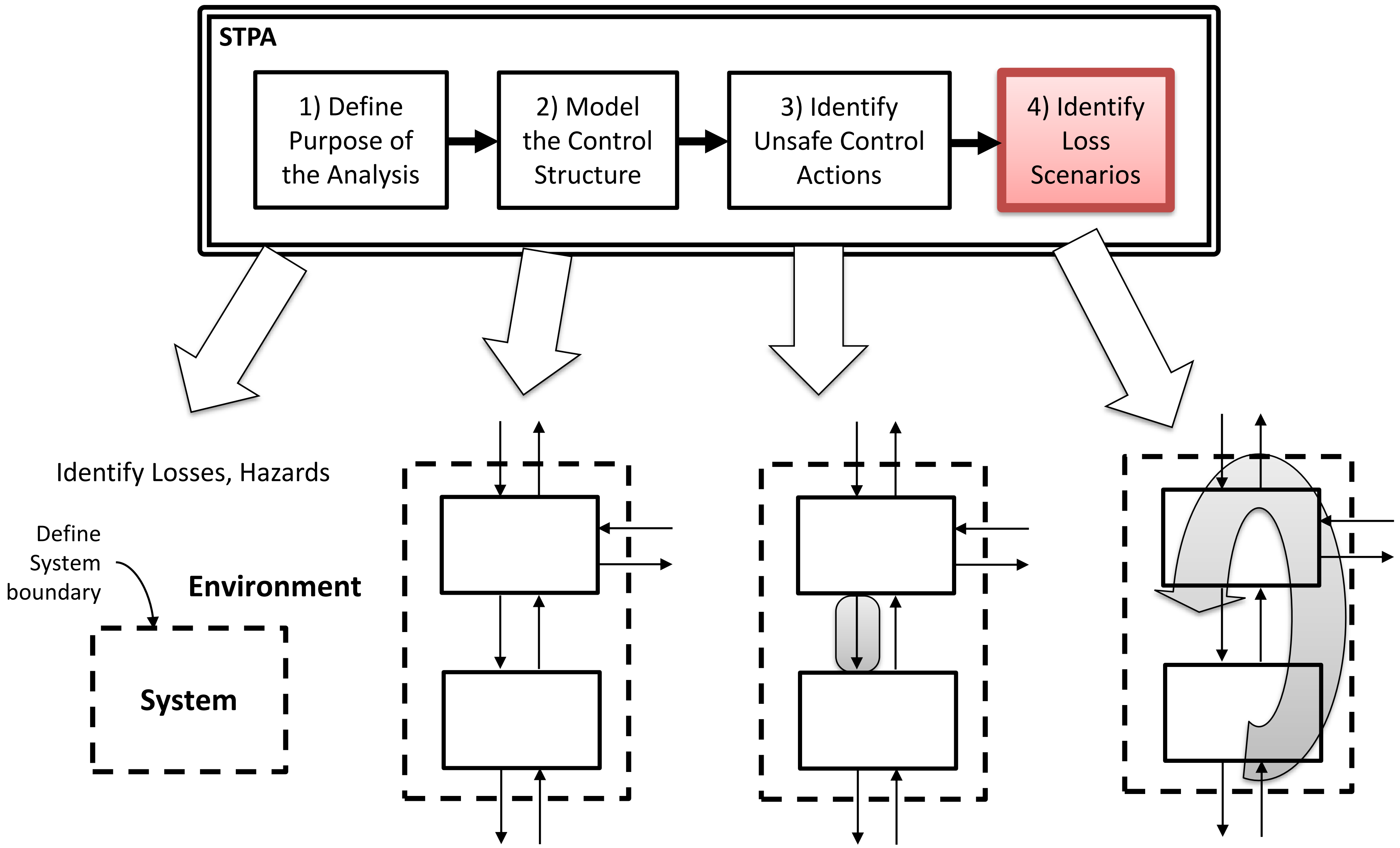
Generating & validating operator procedures



Not provided causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long

Operator shall provide CMD X when D	Operator shall not provide CMD X when E	Operator shall provide CMD X within Y seconds of F	Operator shall stop providing CMD X within Z seconds of G
Operator procedures			

(John Thomas, 2017)



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

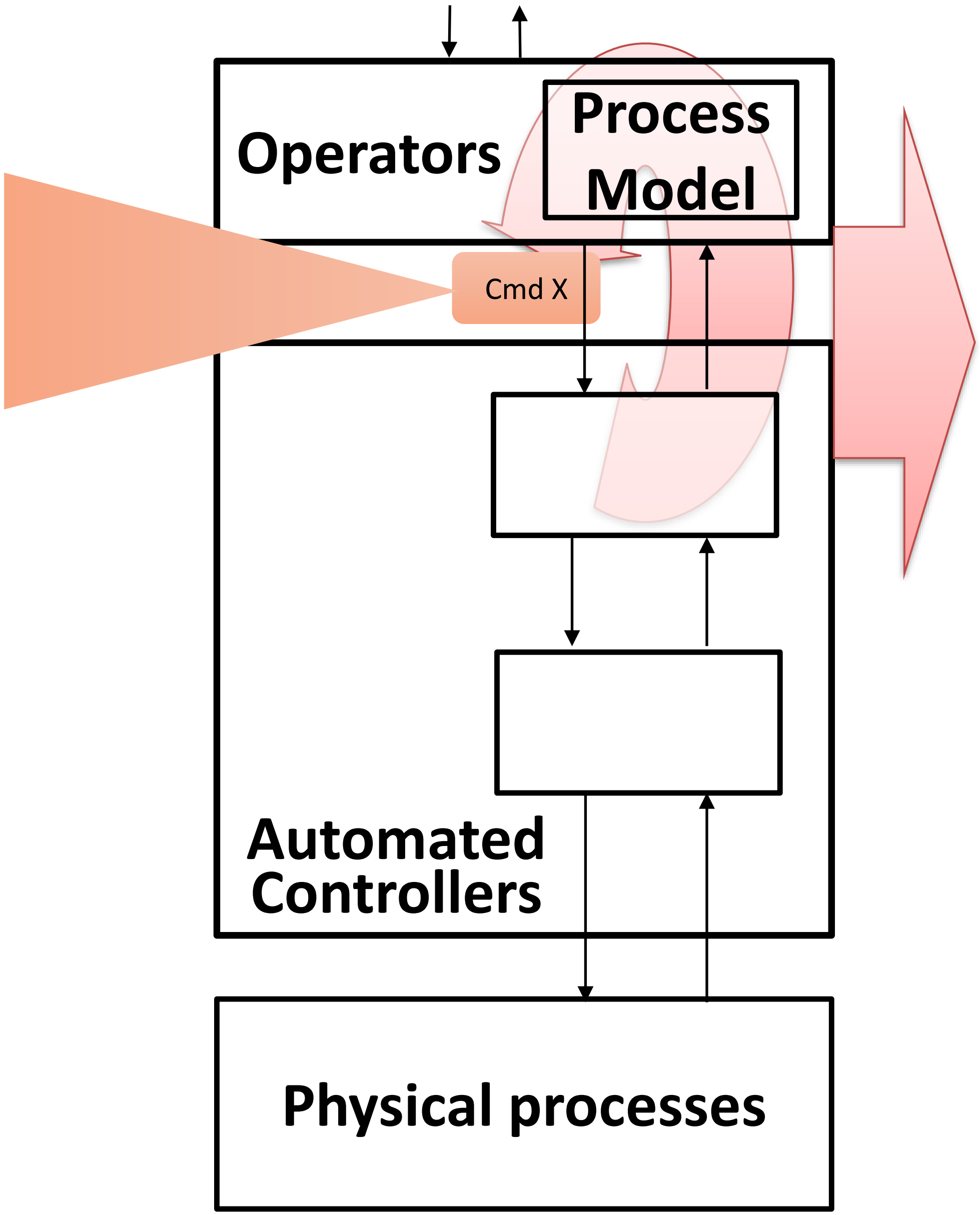
Environment

System

(Leveson and Thomas, 2018)

Identify loss scenarios

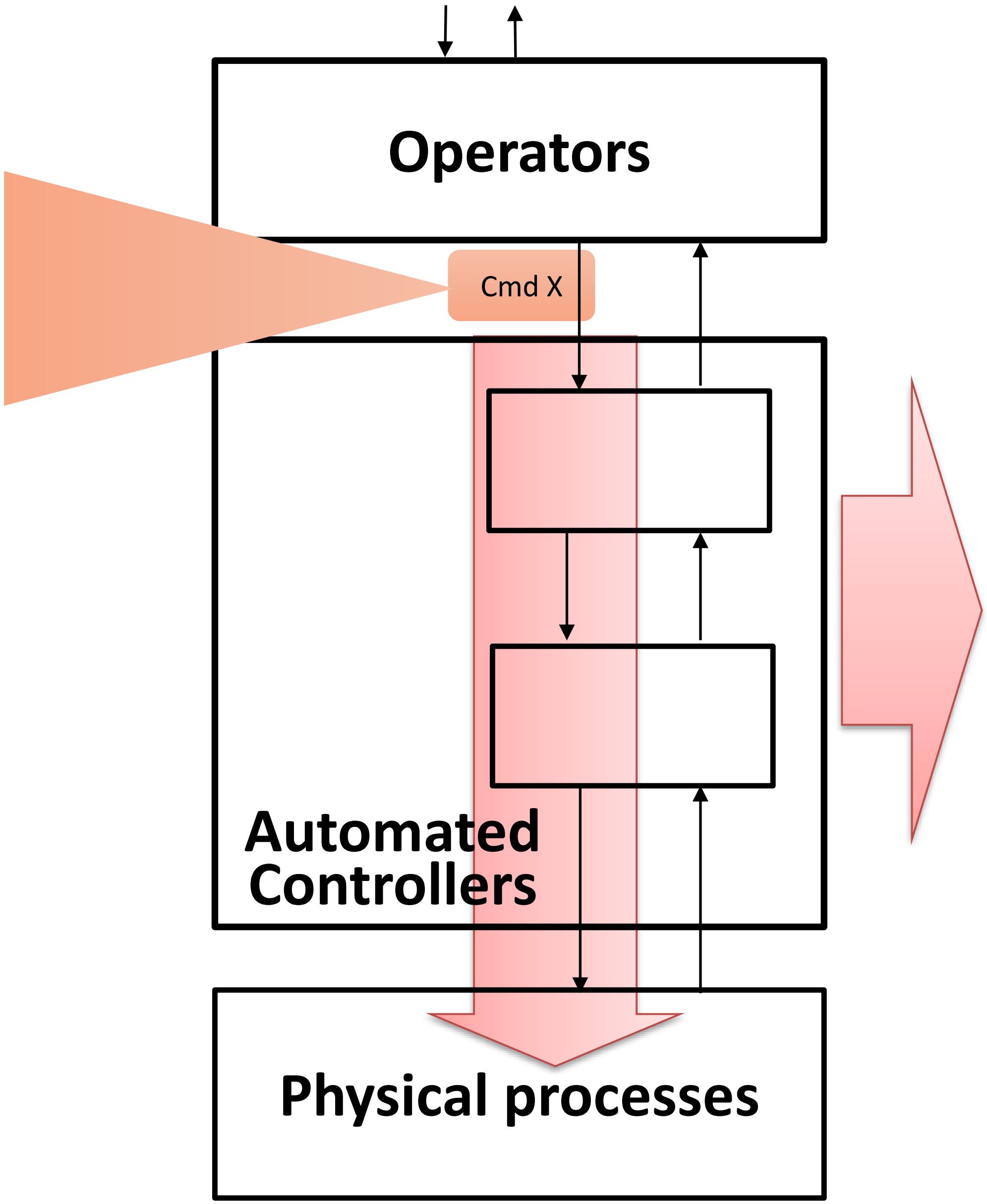
What could cause Unsafe Control Actions?



Scenarios
Op responded to failure in A by …
Op incorrectly believes X because …
Op does not perform Y because …
Op received incorrect feedback Z because …
Etc.

(John Thomas, 2017)

Identify loss scenarios

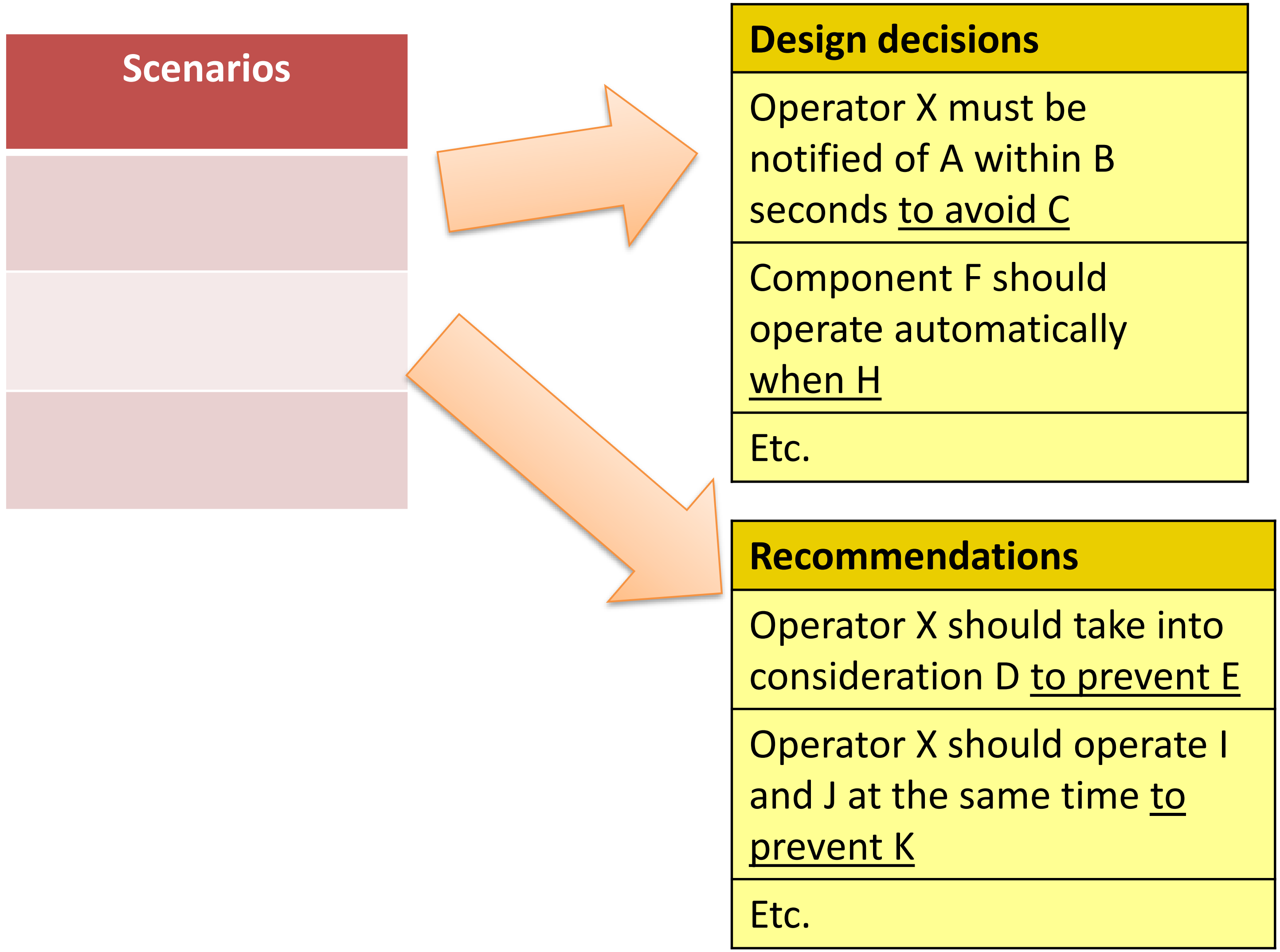


Control actions not executed or not followed properly

Scenarios
Op cmd sent but not received because…
Op cmd received but ignored because…
Actuator failure causes…

(Thomas, 2017)

Design decisions and recommendations



Scenarios

Design decisions
Operator X must be notified of A within B seconds to avoid C
Component F should operate automatically when H
Etc.

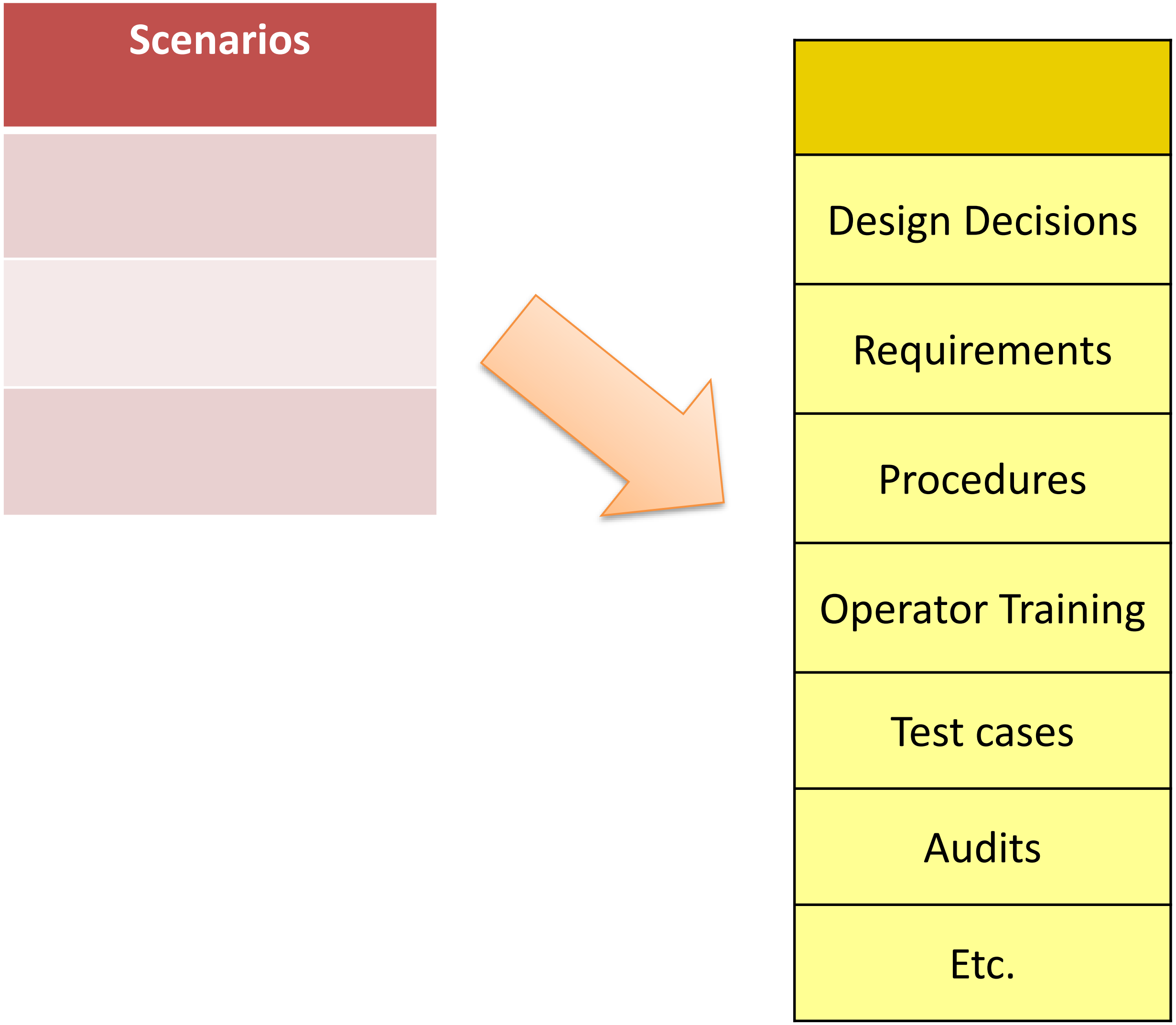
Rationale and assumptions identified

Recommendations
Operator X should take into consideration D to prevent E
Operator X should operate I and J at the same time to prevent K
Etc.

Every recommendation and decision is traceable

(Thomas, 2017)

Design decisions, requirements, training, test cases, audits, etc.

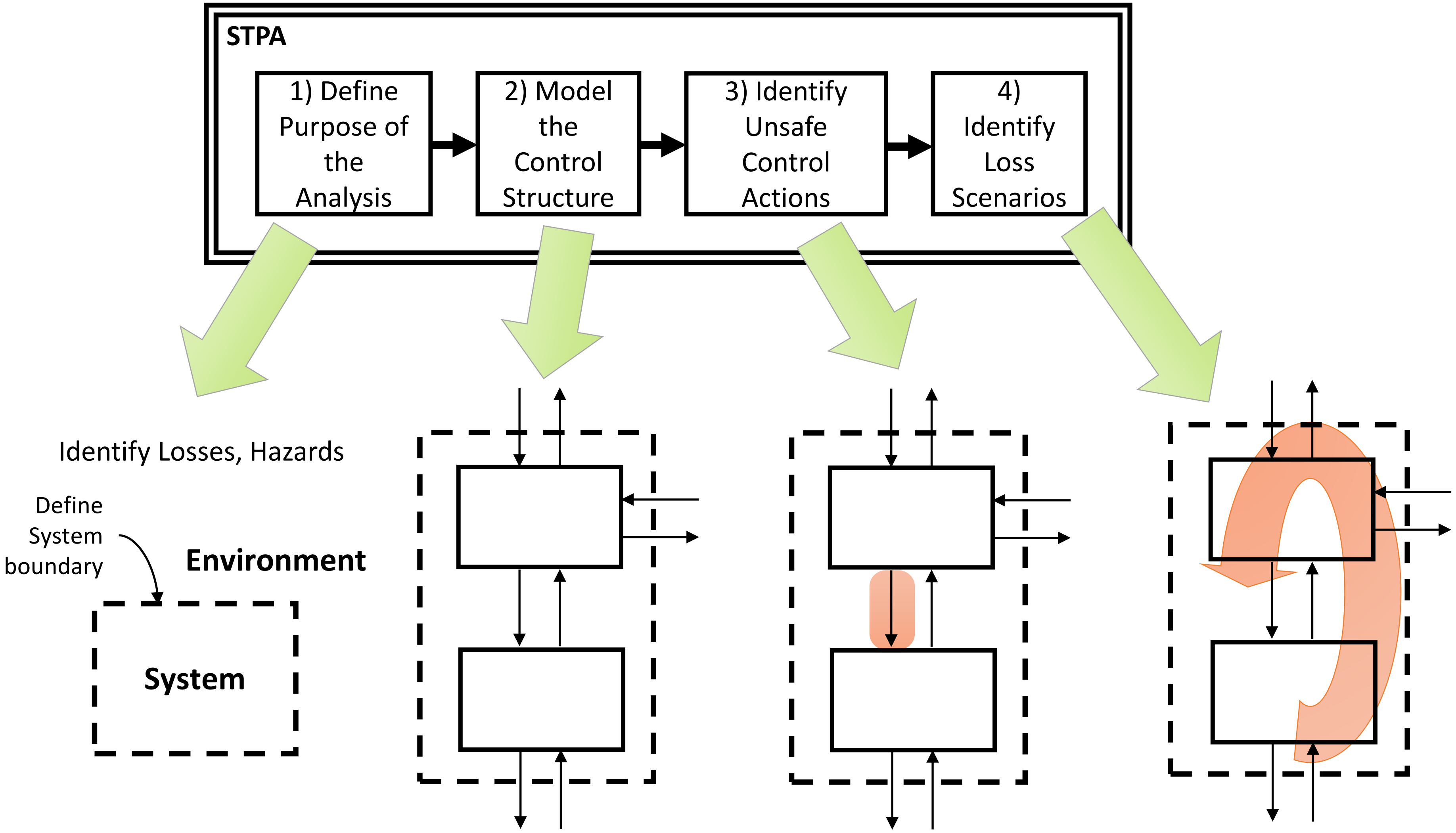


Rationale and assumptions identified

Every recommendation and decision is traceable

(Thomas, 2017)

STPA Overview



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

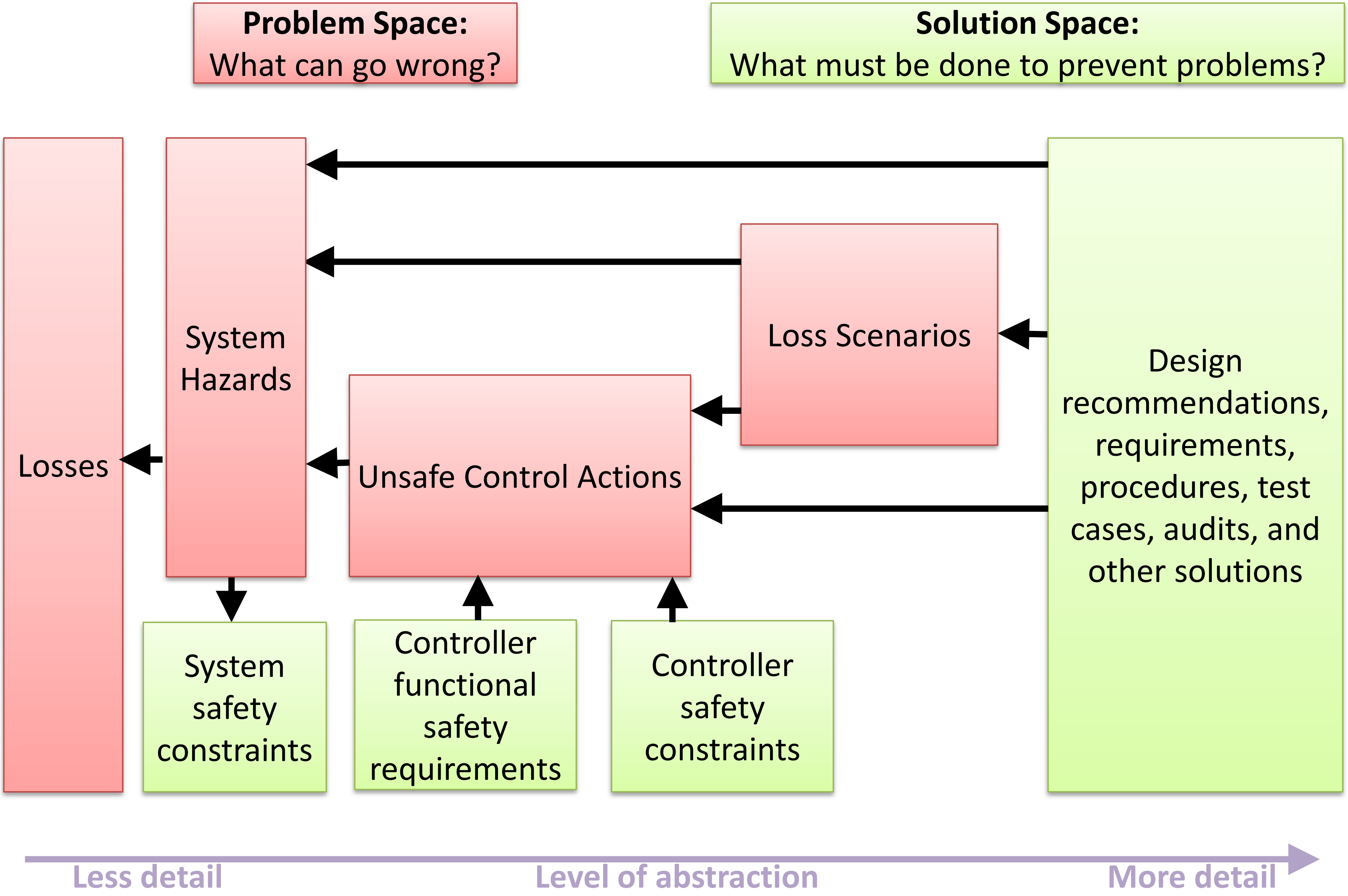
Define System boundary

Environment

System

(Leveson and Thomas, 2018)

STPA: Traceability is maintained throughout

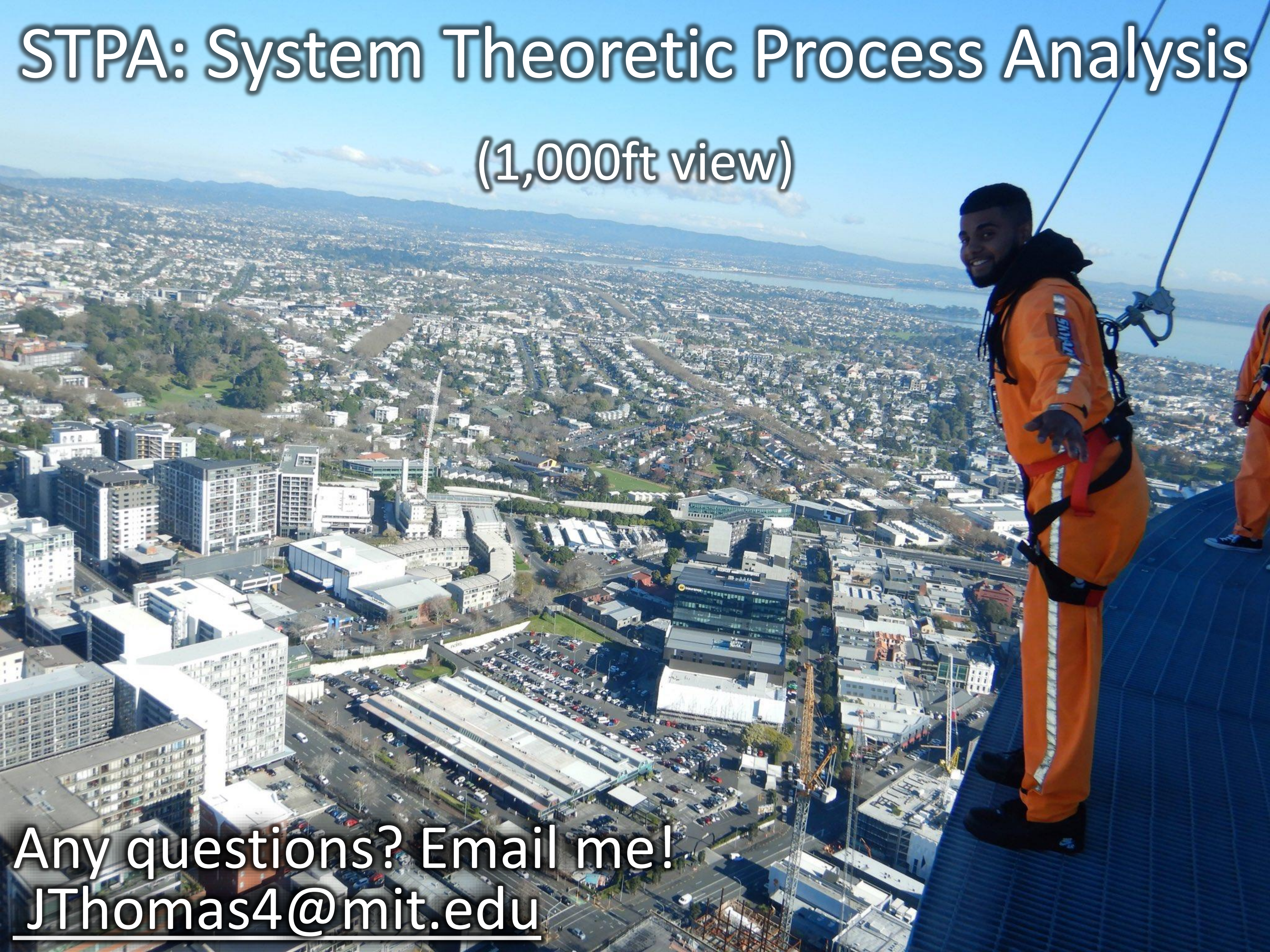


Problem Space:
What can go wrong?
Solution Space:
What must be done to prevent problems?
Losses
System Hazards
Loss Scenarios
Unsafe Control Actions
Design recommendations, requirements, procedures, test cases, audits, and other solutions
System safety constraints
Controller functional safety requirements
Controller safety constraints
Less detail
Level of abstraction
More detail

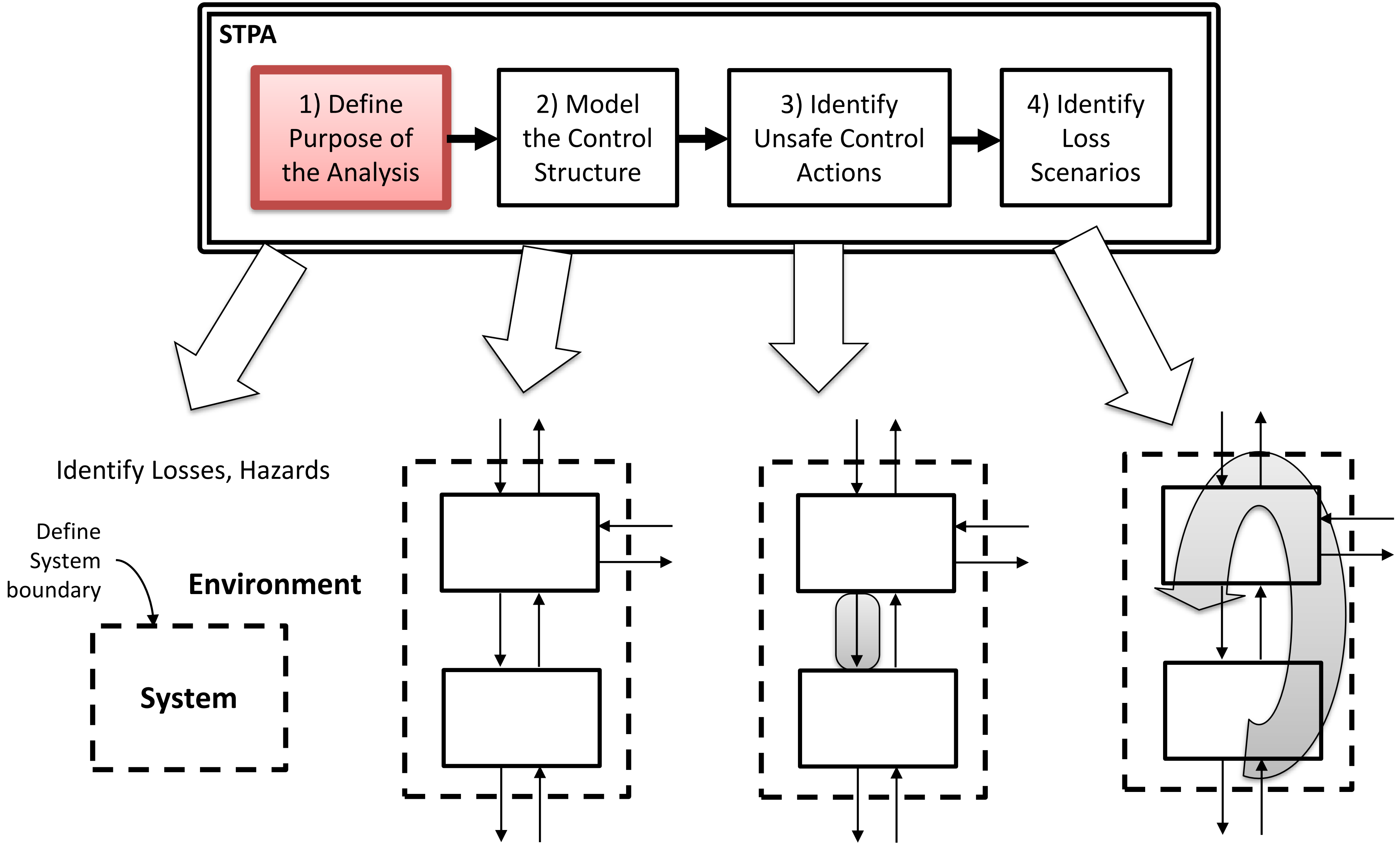
(Thomas, 2017)

STPA: System Theoretic Process Analysis

(1,000ft view)



Any questions? Email me!
JThomas4@mit.edu



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

(Leveson and Thomas, 2018)

Medical Example

Losses (Accidents)

- **L1:** Loss of life or serious injury to patient
- **L2:** Patient’s pain is not relieved (mission loss)

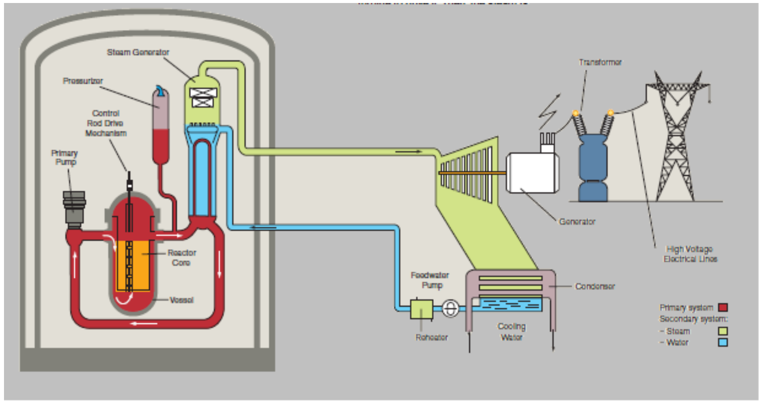
Patient-controlled Analgesia (PCA)

(Thomas, 2017)

Nuclear Power Plant

Losses

- L-1: Loss of life or injury
- L-2: Equipment damage
- L-3: Environmental contamination
- L-4: Loss of power generation (mission loss)



Safety or Security?

(Thomas, 2014)

Military applications

Losses

- L-1: Loss of life or injury to non-hostile forces
- L-2: Loss of mission (e.g. surveillance, attack, etc.)
- L-3: Loss of sensitive information
- L-4: Loss of or unintended damage to assets/equipment

MQ-9 Reaper

Future Attack Reconnaissance Aircraft

Safety or Security?

(Thomas, 2014)

Definitions

- Accident = Mishap = Loss
  - Any unacceptable loss
  - E.g. loss of human life or human injury, property damage, environmental pollution, mission loss, customer satisfaction, 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

Loss	System Hazard
Loss of human life or injury	**Chemical plant** releases toxic chemicals into the atmosphere
Loss of human life or injury	**Nuclear power plant** releases radioactive materials into environment
Loss of human life or injury	**Vehicles** do not maintain safe distance from each other
Loss of human life or injury	**Food products** for sale contain pathogens

Definitions

- Loss
  - Any unacceptable loss
  - E.g. loss of human life or human injury, property damage, environmental pollution, mission loss, customer satisfaction, etc.
  - May involve environmental factors **<u>outside our control</u>**
- System Hazard

Broad view of safety

“Loss” is anything that is unacceptable, that must be prevented.

Not limited to loss of life or human injury!

Loss of human life or injury	Vehicles do not maintain safe distance from each other
Loss of human life or injury	Food products for sale contain pathogens

Example System: Aviation

Loss: Loss of life or injury

System Hazard?

Loss: Loss of life or injury

System Hazard: <u>**Aircraft**</u> violates minimum separation

L-1: Loss of life or injury

H-1: **Aircraft** violates minimum separation [L-1]

<Hazard specification> = <System> & <Unsafe Condition> & <Link to Losses>

E.g. H-1 = Aircraft violate minimum separation standards in flight [L-1, L-2, L-4, L-5]

*The ordering of these elements in a hazard specification may vary

Example accidents and hazards

- A-1. Loss of life or serious injury to people
- A-2. Damage to the aircraft or objects outside the aircraft

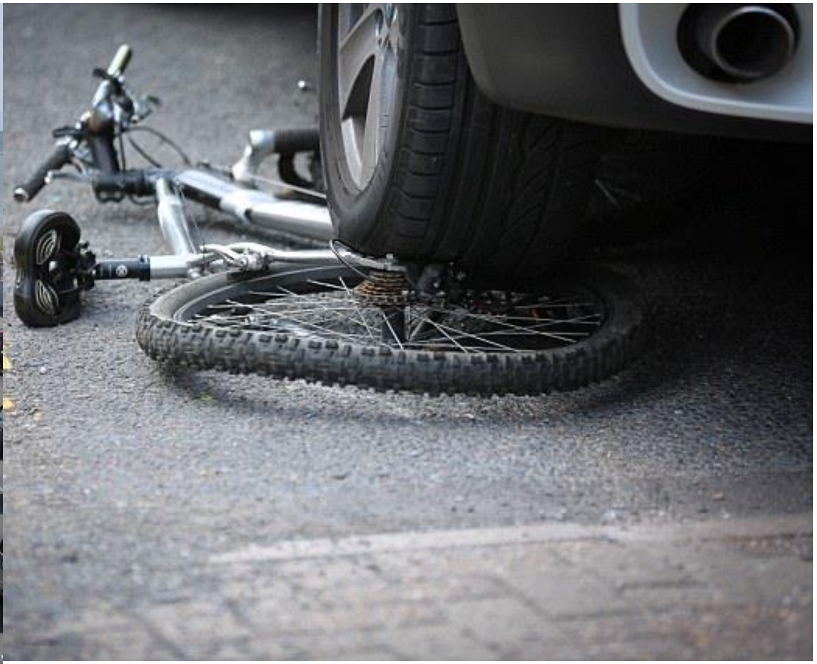
- Example Aircraft-level Hazards:
  - H-1: **Aircraft** violate minimum separation standards in flight
  - H-2: Controlled flight of **aircraft** into terrain
  - H-3: Loss of **aircraft** control
  - H-4: **Aircraft** airframe integrity is degraded
  - H-5: **Aircraft** environment is harmful to human health
    - E.g. exceeds limits for temperature, oxygen, attitude, rate of movement, etc.

Ask: What system-level states/conditions lead to losses?

(Thomas, 2017)

Automotive Example

- Losses
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the vehicle or objects outside the vehicle
  - L-3: Loss of mission (transportation)
  - L-4: Loss of customer satisfaction



Automotive Example

- Losses
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the vehicle or objects outside the vehicle

- System Hazards
  - H-1: **Vehicle** does not maintain safe distance from nearby objects
  - H-2: **Vehicle** enters dangerous area/region
  - H-3: **Vehicle** exceeds safe operating envelope for environment (speed, lateral/longitudinal forces)
  - H-4: **Vehicle** occupants exposed to harmful effects and/or health hazards
    - (e.g. fire, excessive temperature, inability to escape, door closes on passengers, etc.)

PCA pump: example losses and hazards

Losses (Accidents)

- **L1:** Loss of life or serious injury to patient
- **L2:** Patient's pain is not relieved
- **L3:** Loss of protected patient or proprietary hospital information
- **L4:** Financial loss or loss of hospital reputation

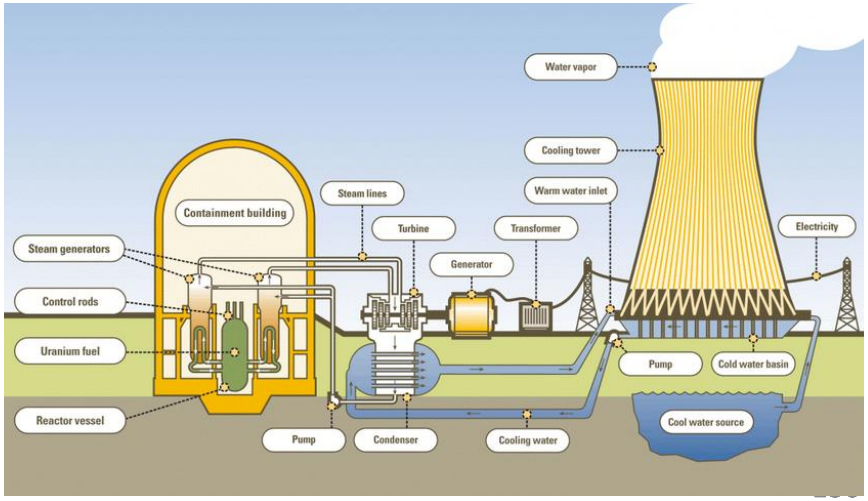
System Hazards

- **H1**: Patient has opioid overdose **[L1, L4]**
- **H2:** Patient has opioid under-dose **[L2]**
- **H3:** Patient info disclosed to unauthorized parties **[L3, L4]**

(Thomas, 2017)

Nuclear Example

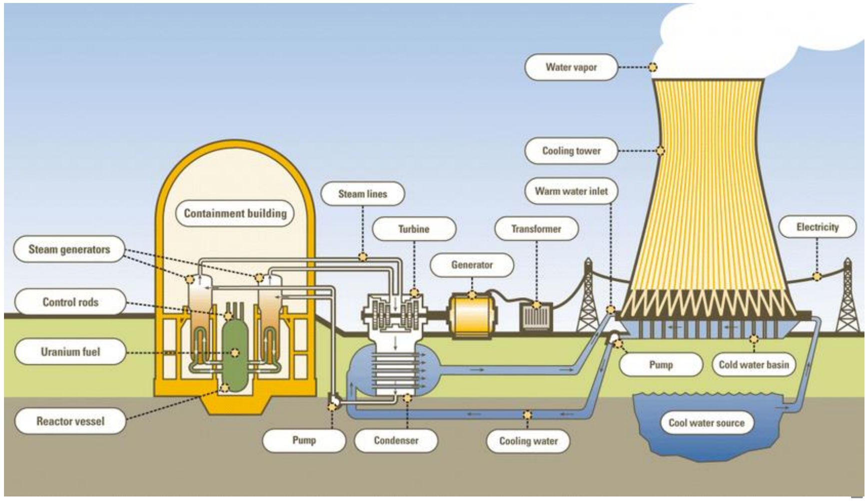
- What are stakeholder losses?
  - L-1: Loss of life or injury/health
  - L-2: Environmental loss (release)
  - L-3: Loss of/damage to plant
  - L-4: Loss of generation



Nuclear Example

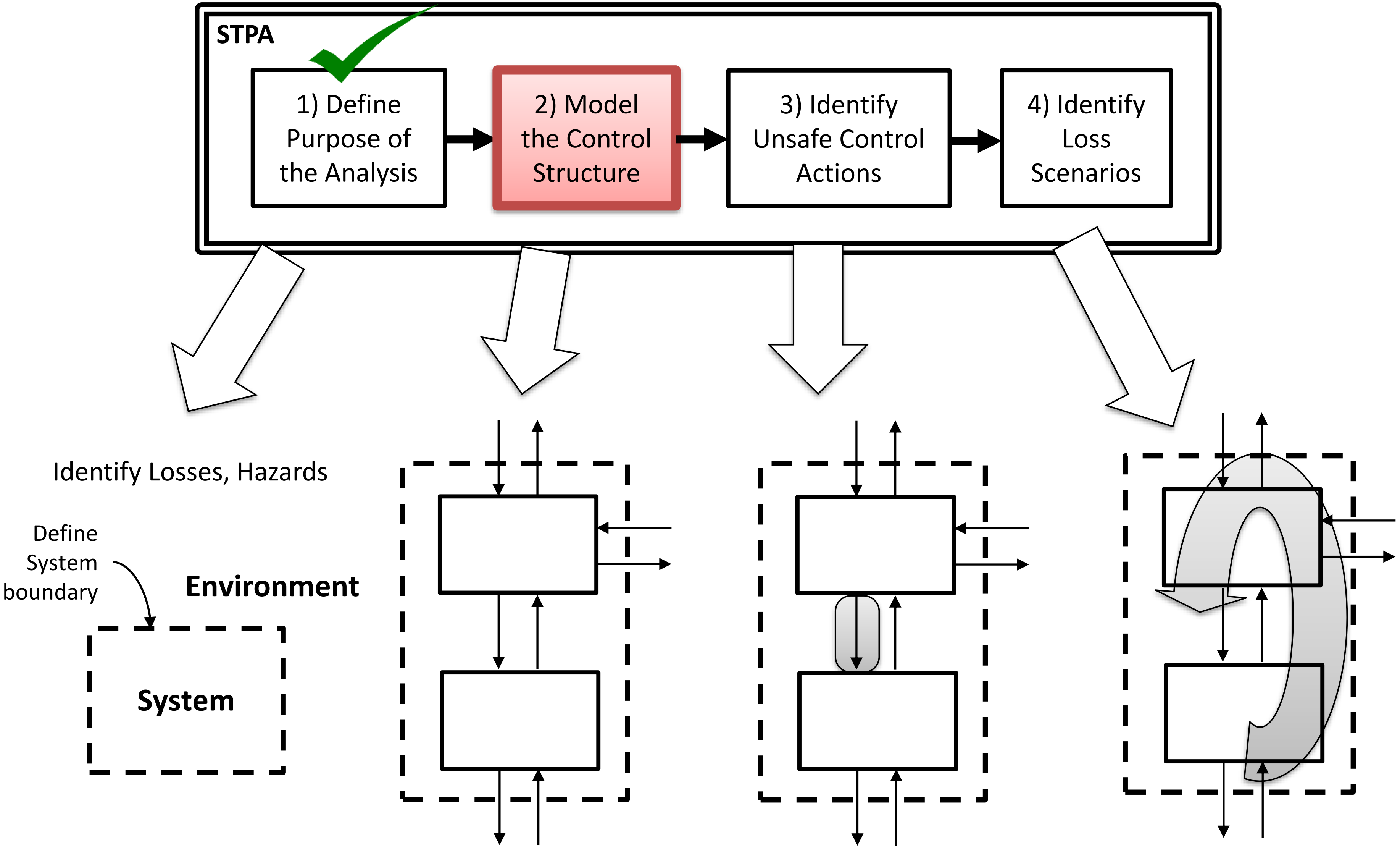
- What are stakeholder losses?
  - L-1: Loss of life or injury/health
  - L-2: Environmental loss (release)
  - L-3: Loss of/damage to plant
  - L-4: Loss of generation

- What are the system-level (plant-level) hazards?
  - H-1: Plant releases radioactive material [L-1, L-2, L-3, L-4]
  - H-2: Plant is operated outside limits [L-2, L-3, L-4]
  - H-3: Plant is shut down [L-4]



System Safety Constraints / Requirements

System Hazard	System Requirement
H-1: Vehicle does not maintain safe distance from nearby objects [L-1]	R-1: Vehicle must maintain safe distance from nearby objects [H-1]
H-2: Chemical plant releases toxic chemicals into the atmosphere [L-2]	R-2: Chemical plant must not release toxic chemicals into the atmosphere [H-2]
H-3: Nuclear power plant releases radioactive materials into environment [L-3]	R-3: Nuclear power plant must not release radioactive materials into environment [H-3]
H-4: Vehicles do not maintain safe distance from each other [L-4]	R-4: Vehicles must always maintain safe distances from each other [H-4]
H-5: Food products for sale contain pathogens [L-5]	R-5: Food products with pathogens must not be sold [H-5]



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

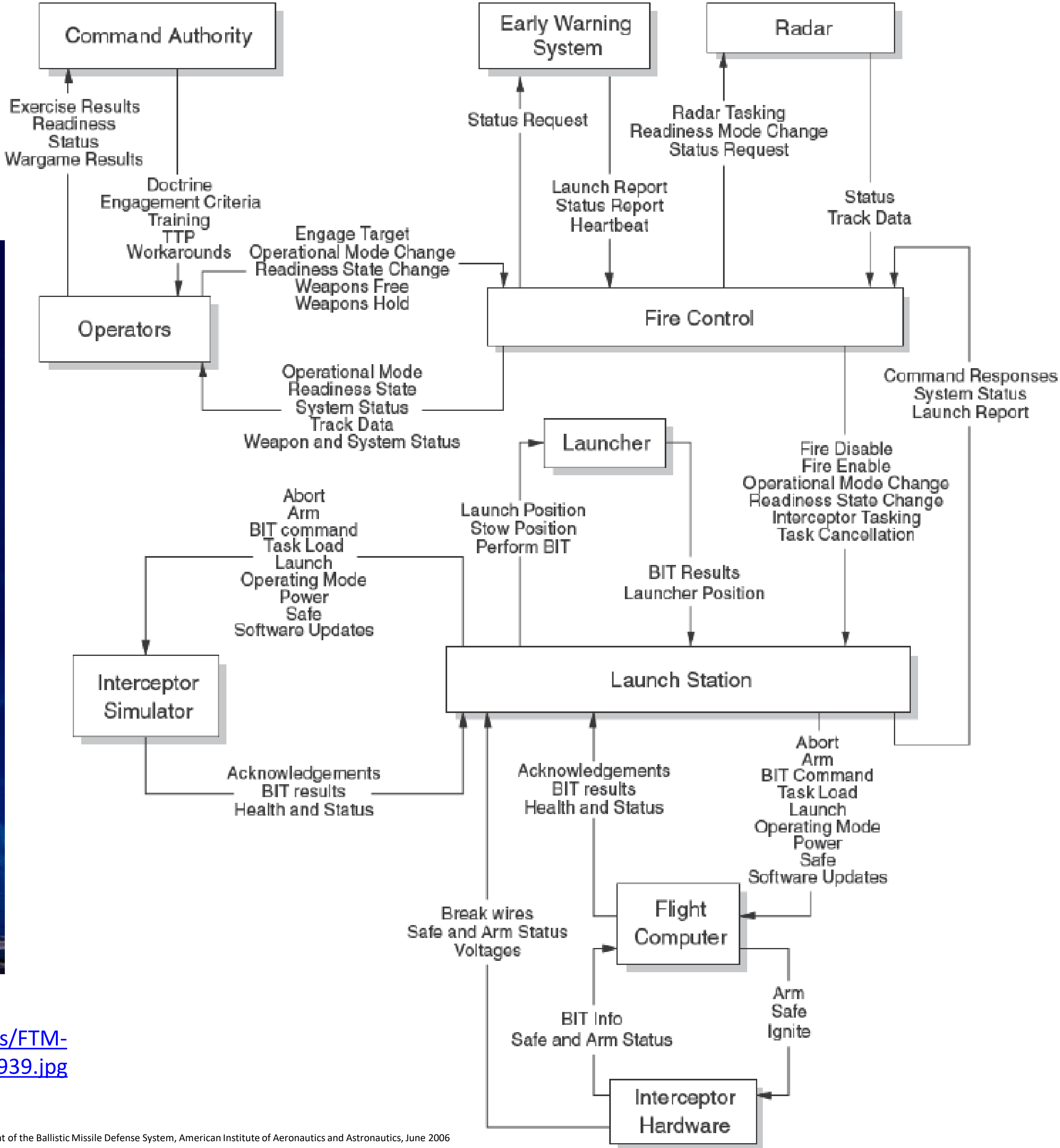
Environment

System

(Leveson and Thomas, 2018)

Ballistic Missile Defense System

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



Command Authority

Exercise Results
Readiness
Status
Wargame Results

Doctrine
Engagement Criteria
Training
TTP
Workarounds

Operators

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

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

Early Warning System

Status Request

Launch Report
Status Report
Heartbeat

Radar

Radar Tasking
Readiness Mode Change
Status Request

Status
Track Data

Fire Control

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

Acknowledgements
BIT results
Health and Status

Launch Station

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

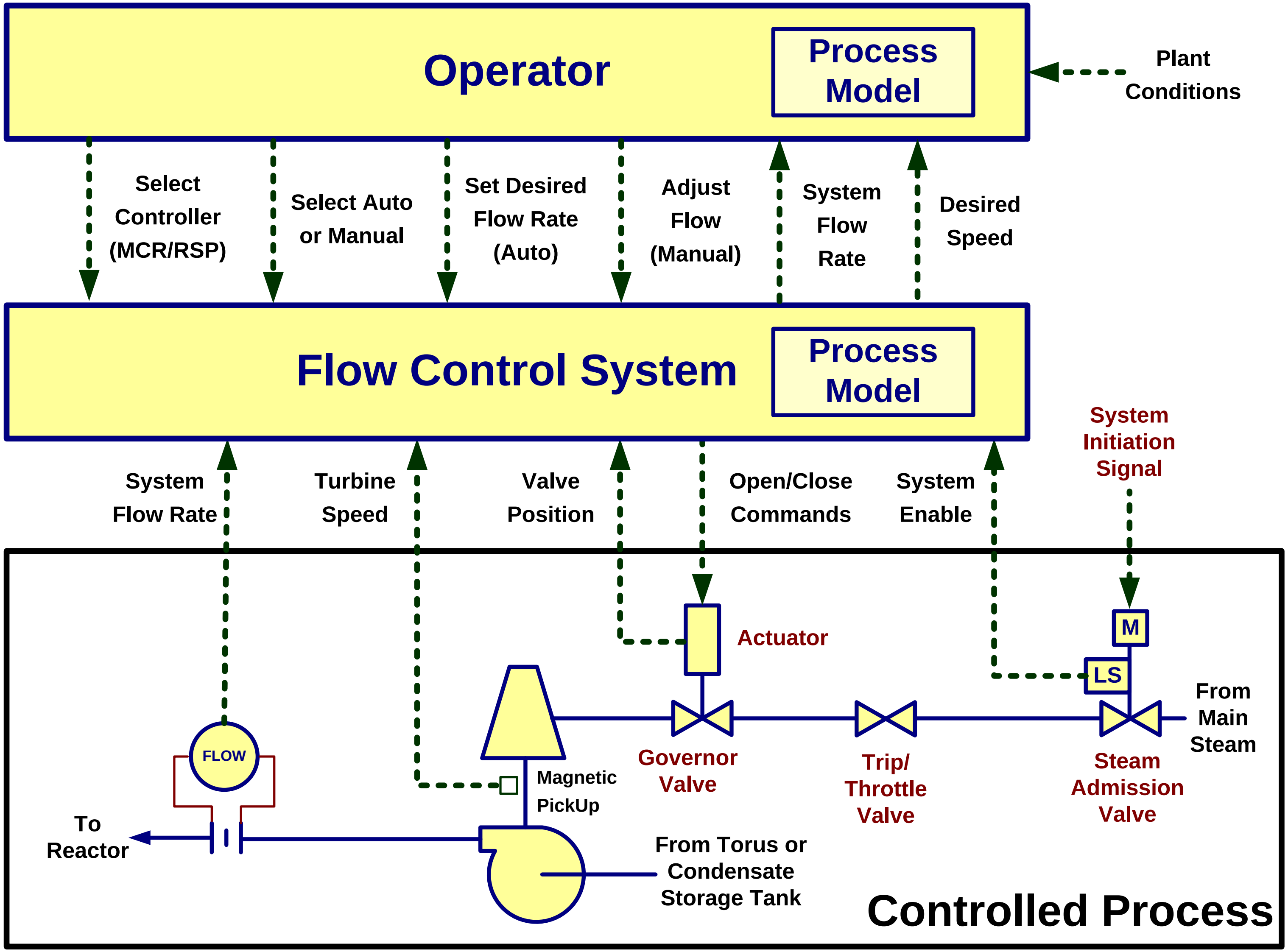
BIT Info
Safe and Arm Status

Arm
Safe
Ignite

Interceptor Hardware

Pereira, Lee, Howard, A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System, American Institute of Aeronautics and Astronautics, June 2006

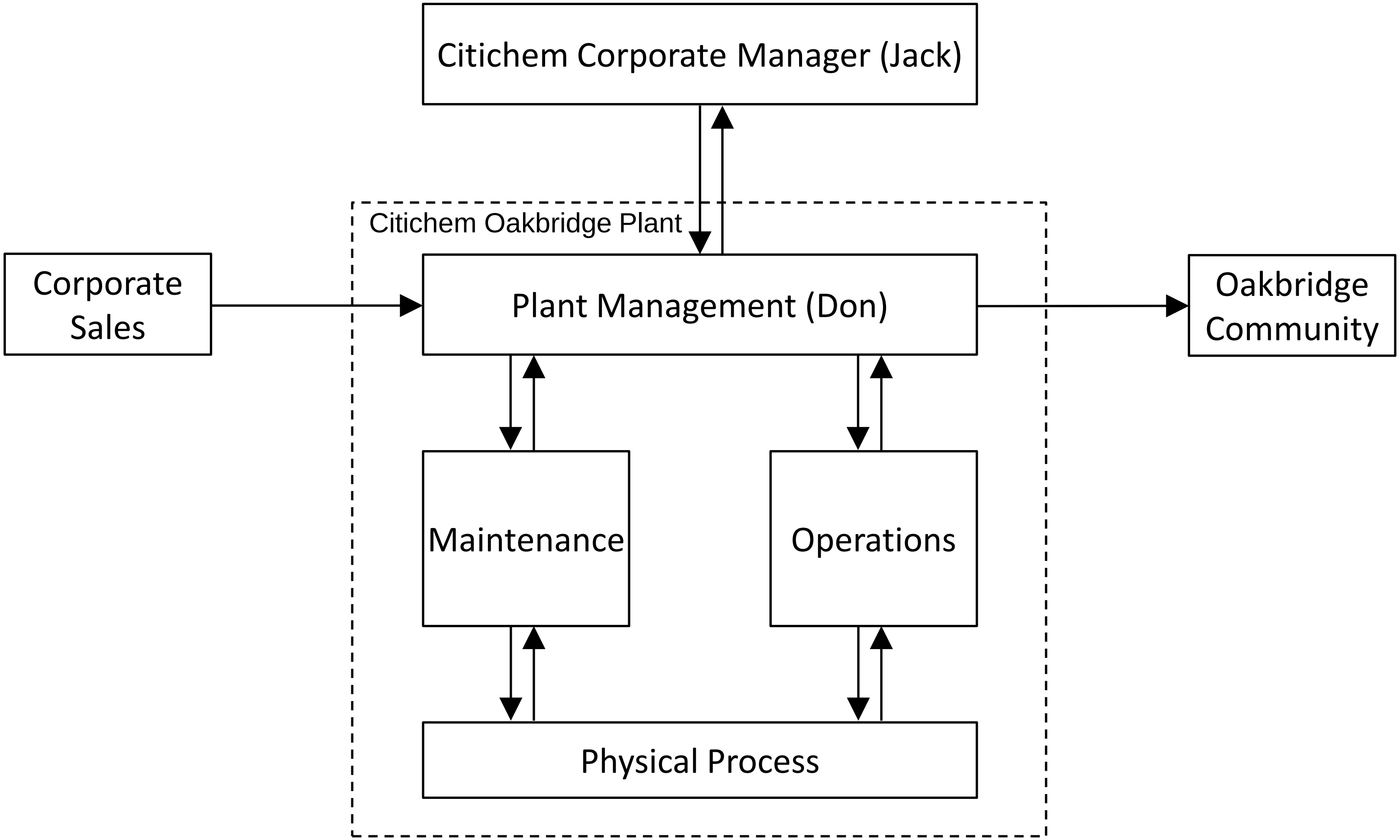
Control Structure



Chemical Plant

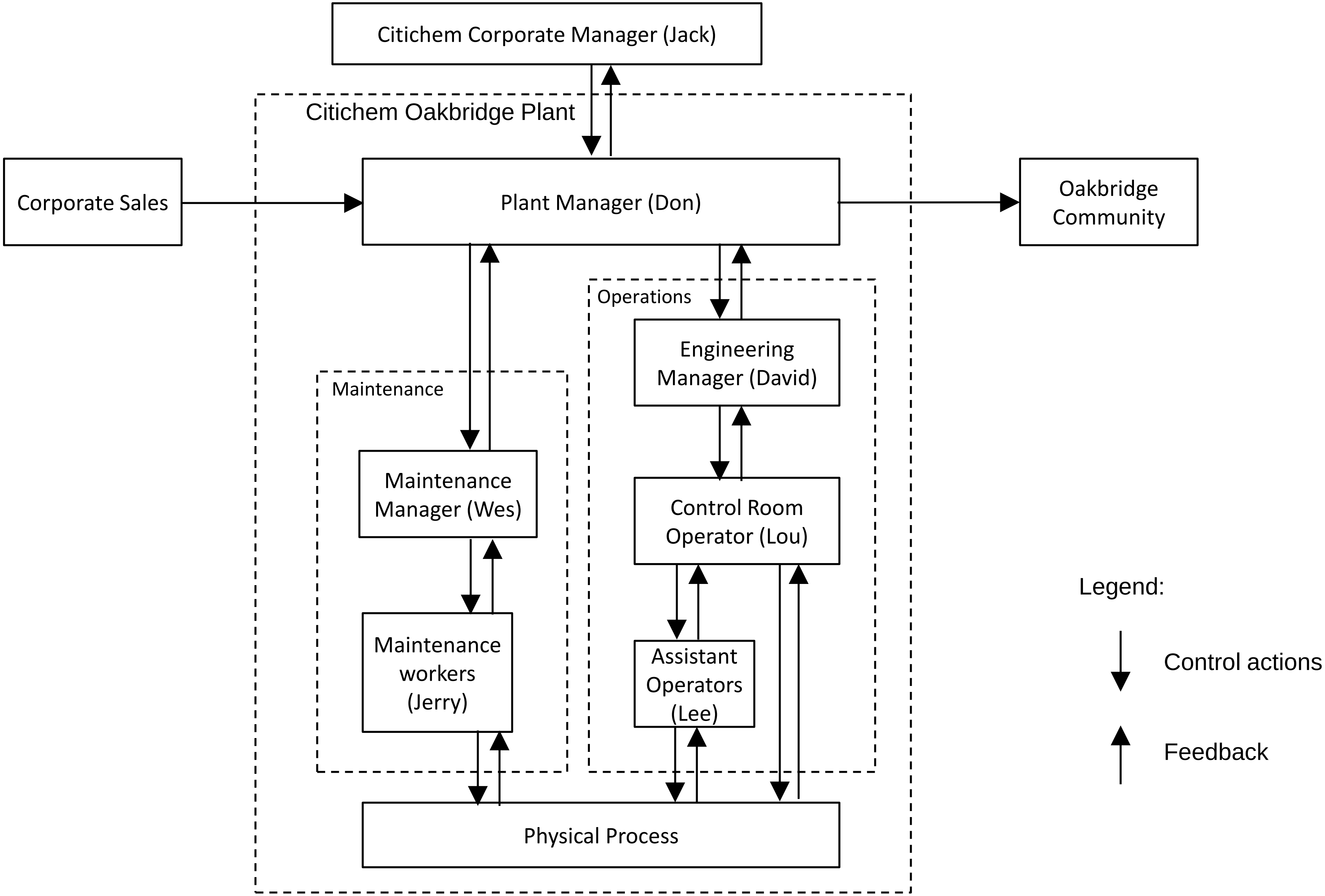
Image from: http://www.cbgnetwork.org/2608.html

Initial High-level Control Structure



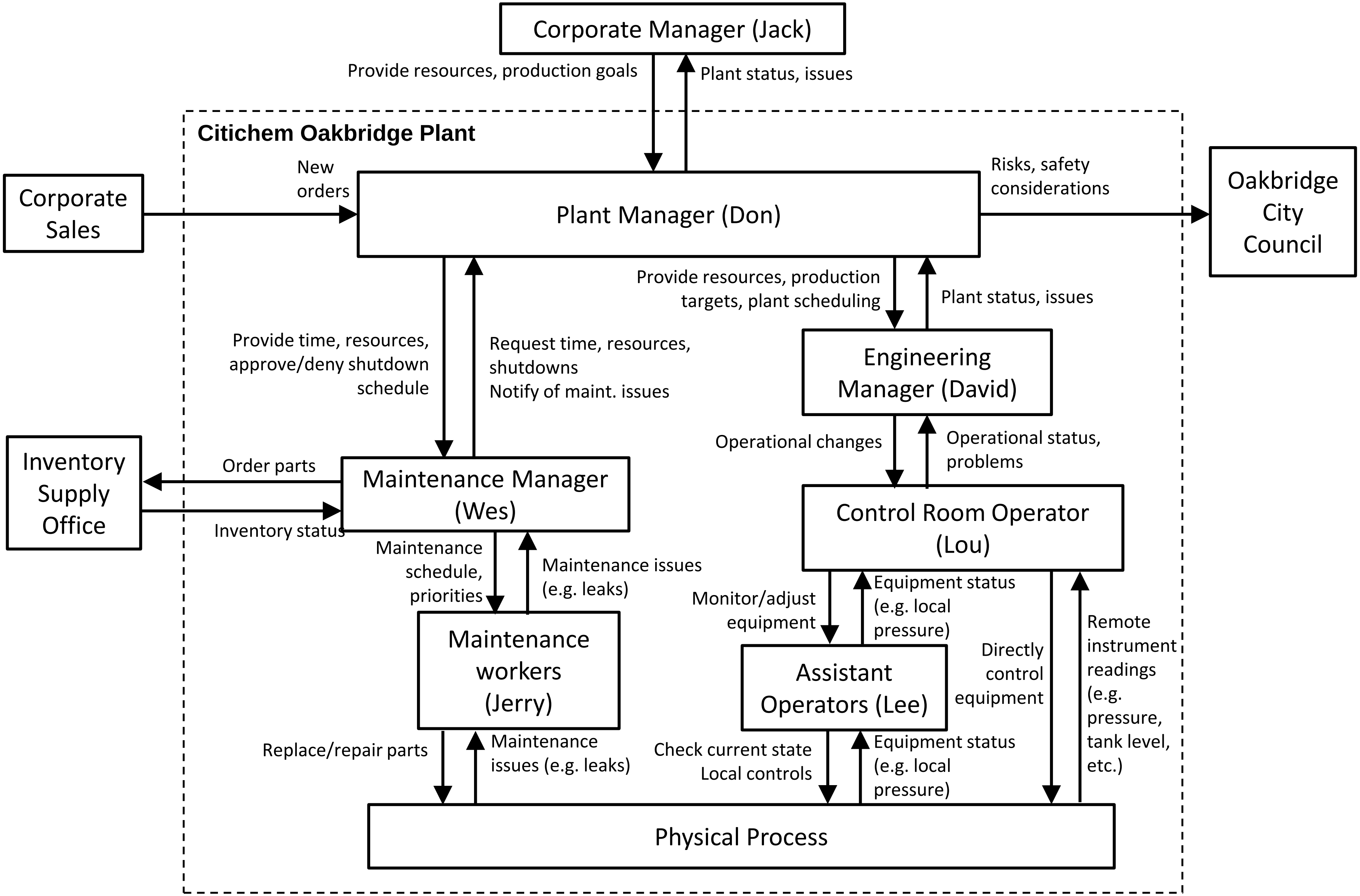
We can start with a very abstract high-level control structure like this. Now we need to define the initial system boundary. For the purpose of this exercise, suppose we have ability to get information about, and fix problems in, the Oakbridge plant. Let's "zoom in" on that piece.

Oakbridge Plant Control Structure


Citichem Corporate Manager (Jack)
Citichem Oakbridge Plant
Corporate Sales
Plant Manager (Don)
Oakbridge Community
Operations
Engineering Manager (David)
Maintenance
Maintenance Manager (Wes)
Control Room Operator (Lou)
Maintenance workers (Jerry)
Assistant Operators (Lee)
Physical Process
Legend:
Control actions
Feedback

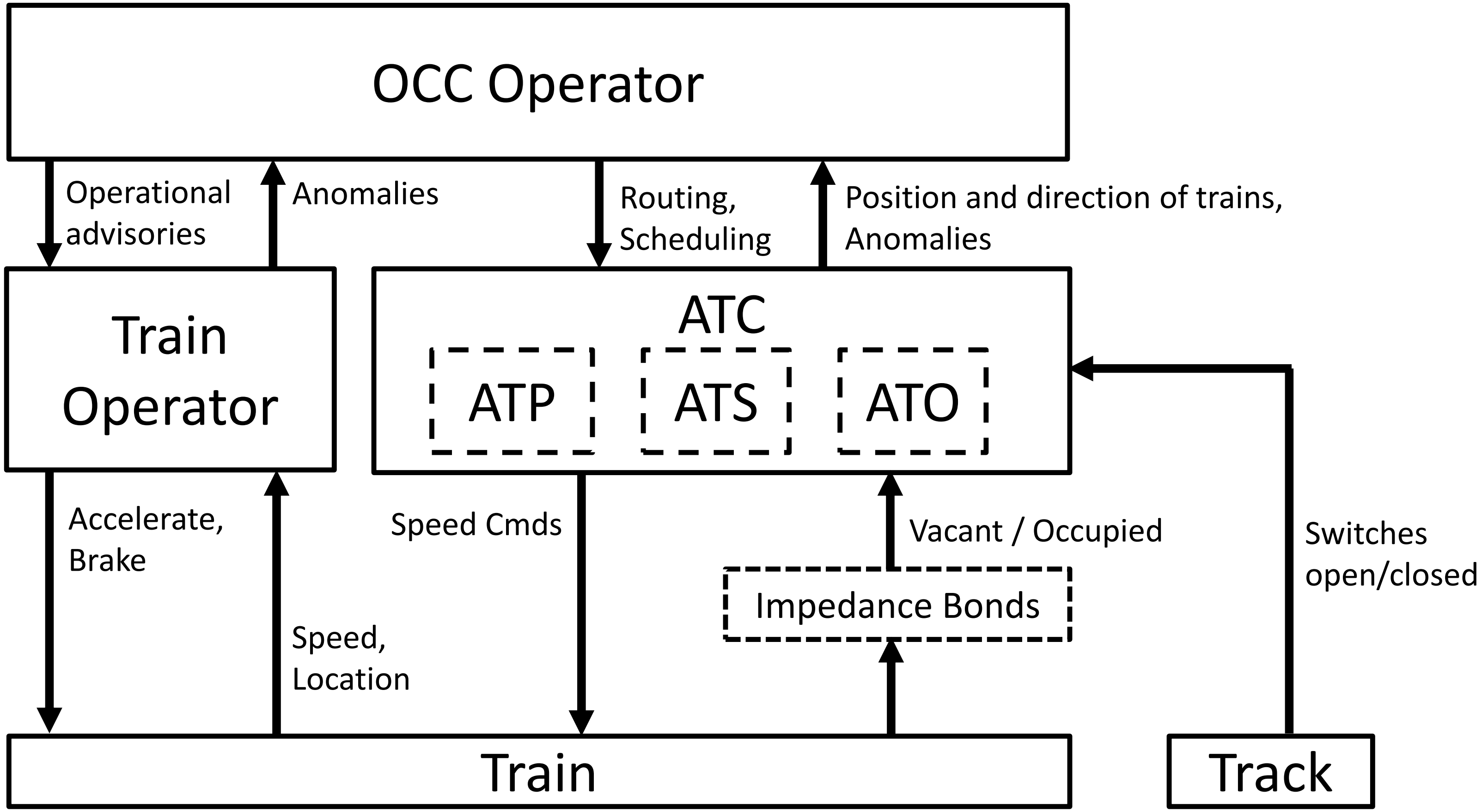
Thomas, Leveson, Stringfellow, 2009

Example of more refined control structure


Corporate Manager (Jack)
Provide resources, production goals
Plant status, issues
Citichem Oakbridge Plant
Corporate Sales
New orders
Plant Manager (Don)
Risks, safety considerations
Oakbridge City Council
Provide resources, production targets, plant scheduling
Plant status, issues
Engineering Manager (David)
Provide time, resources, approve/deny shutdown schedule
Request time, resources, shutdowns
Notify of maint. issues
Operational changes
Operational status, problems
Inventory Supply Office
Order parts
Inventory status
Maintenance Manager (Wes)
Control Room Operator (Lou)
Maintenance schedule, priorities
Maintenance issues (e.g. leaks)
Monitor/adjust equipment
Equipment status (e.g. local pressure)
Maintenance workers (Jerry)
Assistant Operators (Lee)
Directly control equipment
Remote instrument readings (e.g. pressure, tank level, etc.)
Replace/repair parts
Maintenance issues (e.g. leaks)
Check current state
Local controls
Equipment status (e.g. local pressure)
Physical Process

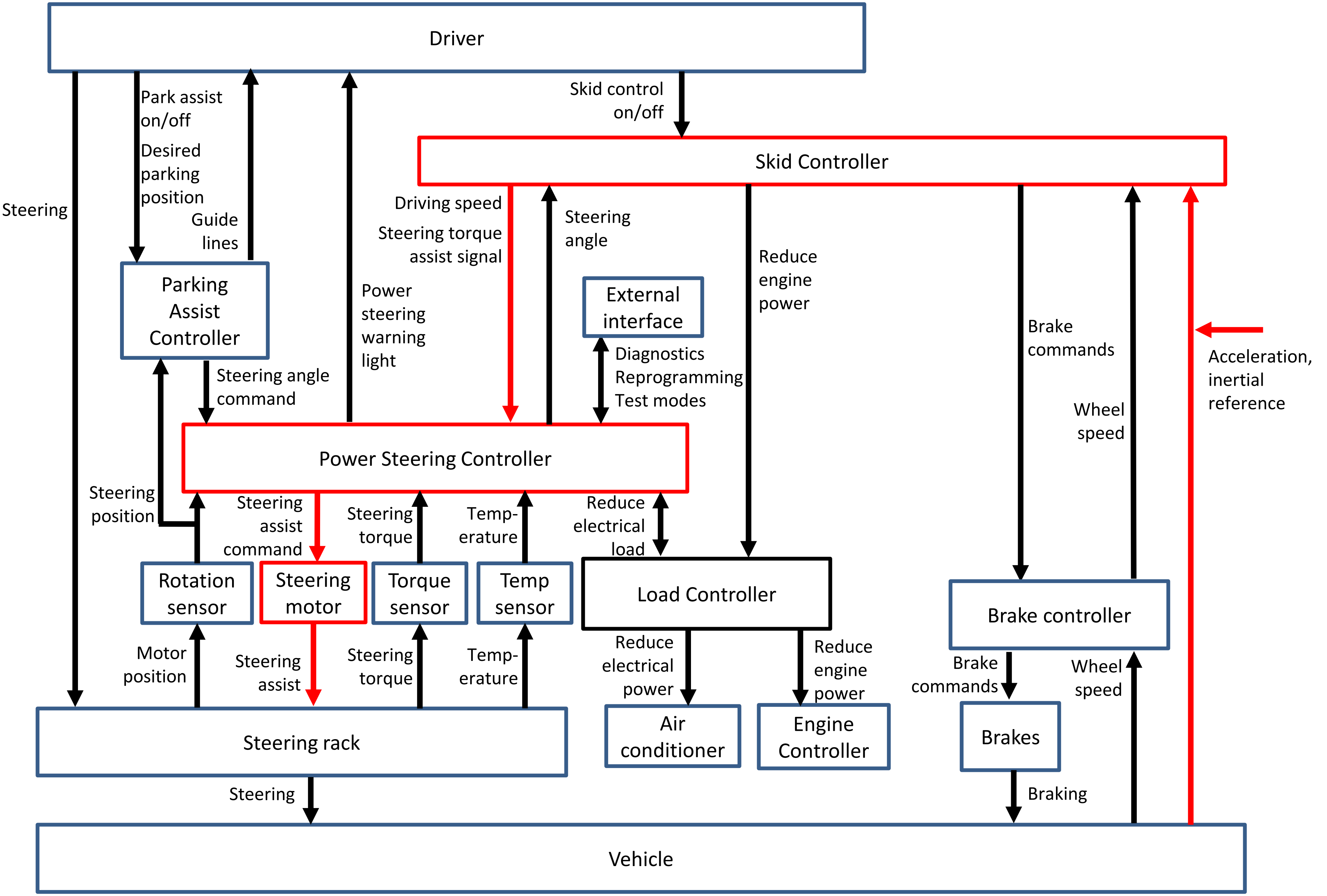
Thomas, Leveson, Stringfellow, 2009

Simplified Control Structure



Thomas, 2019

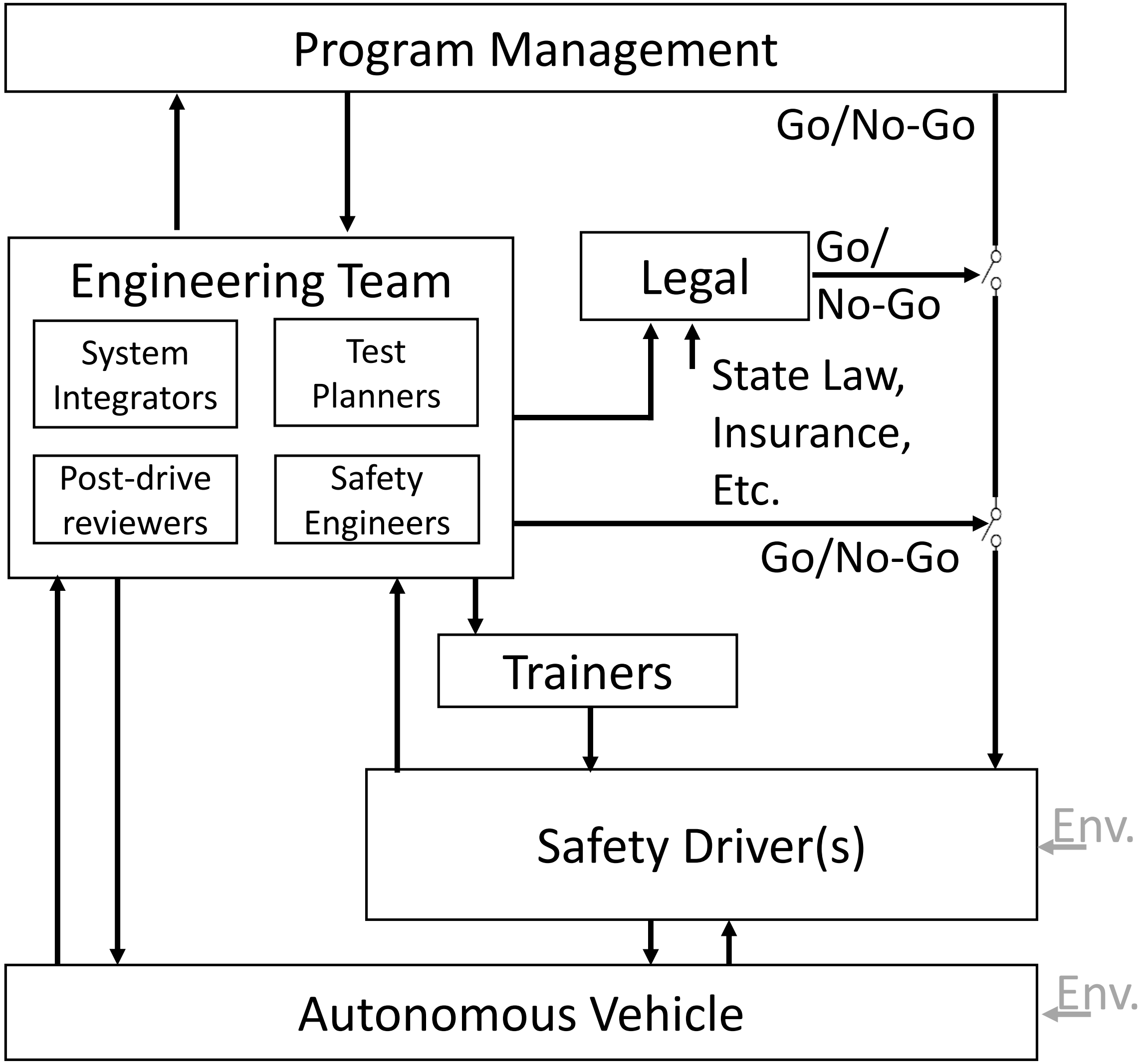
Electric Power Steering: Control Structure



Thomas, 2016

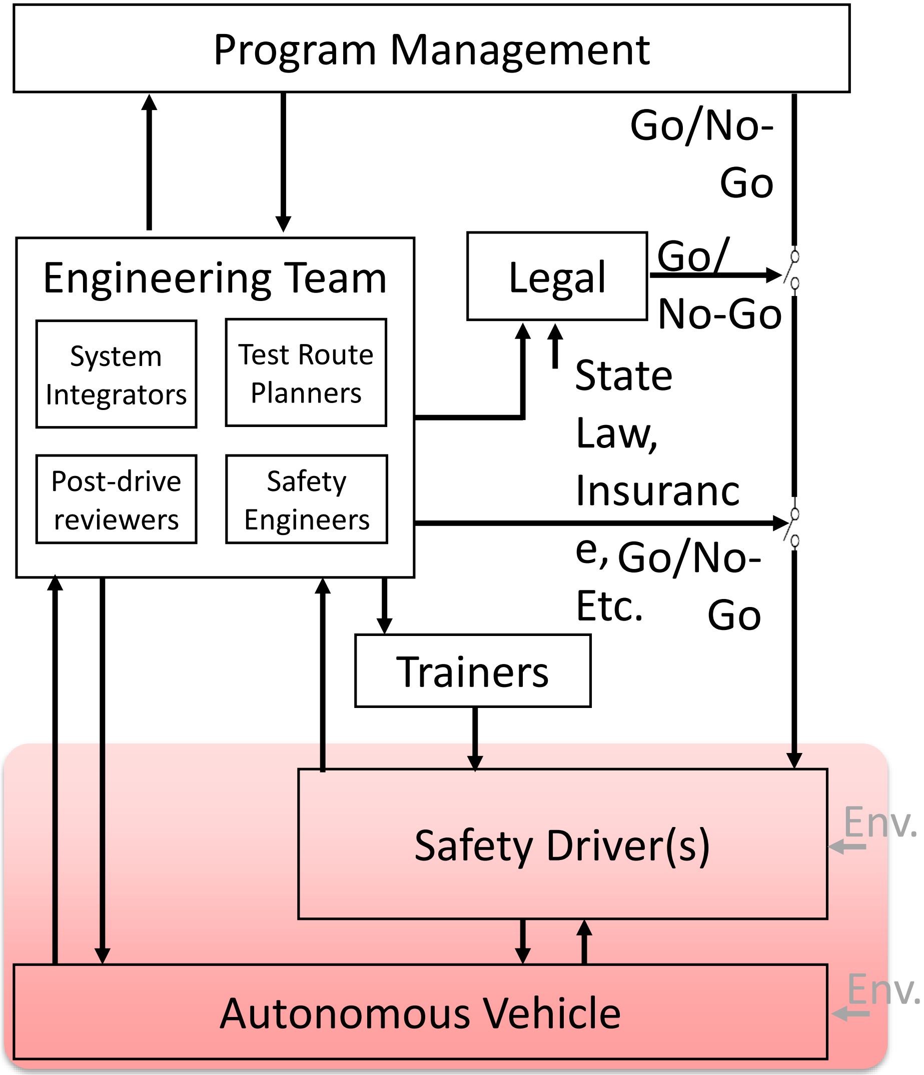
Autonomous Vehicles

Level 1 control structure

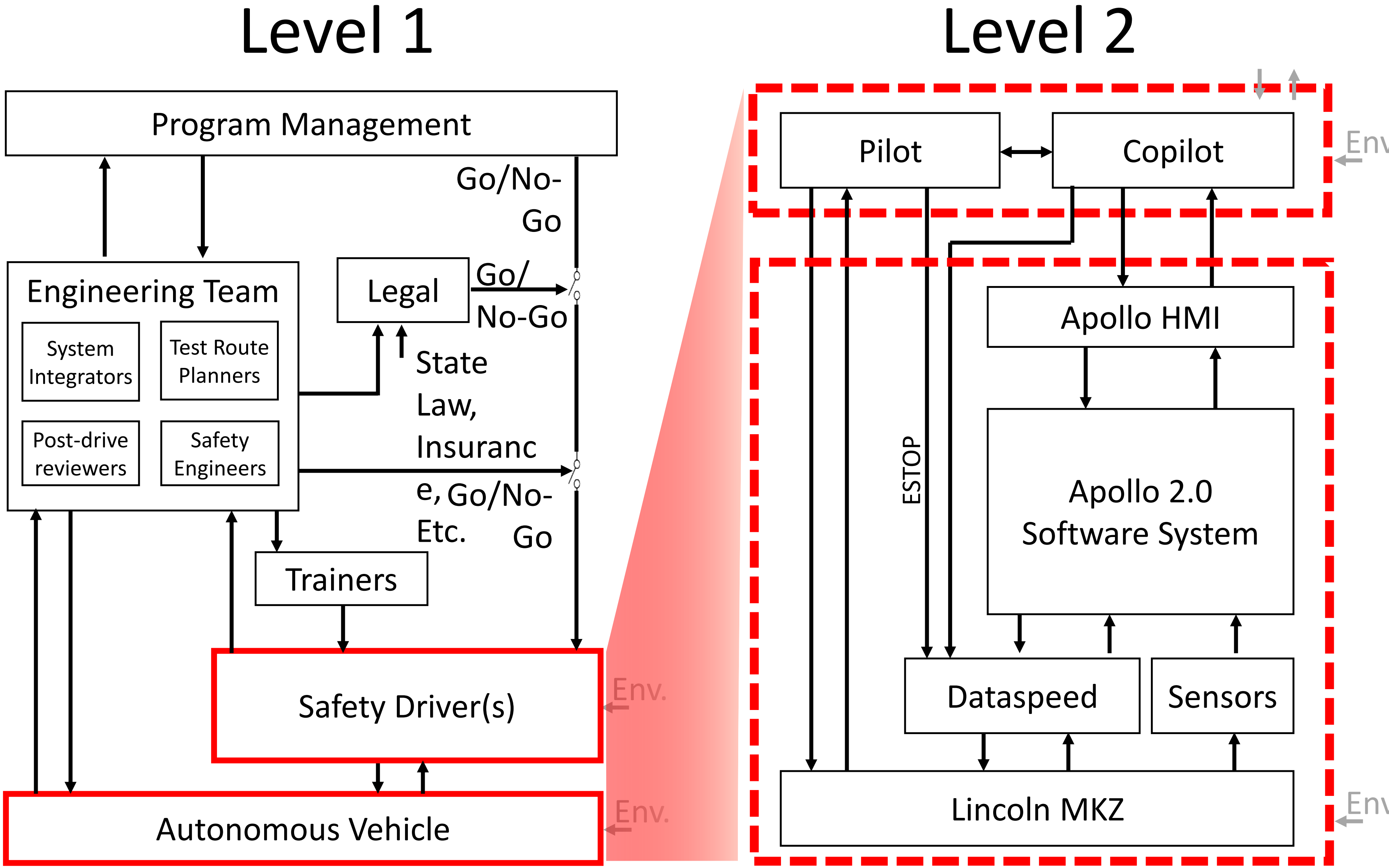


Control Structure Refinement

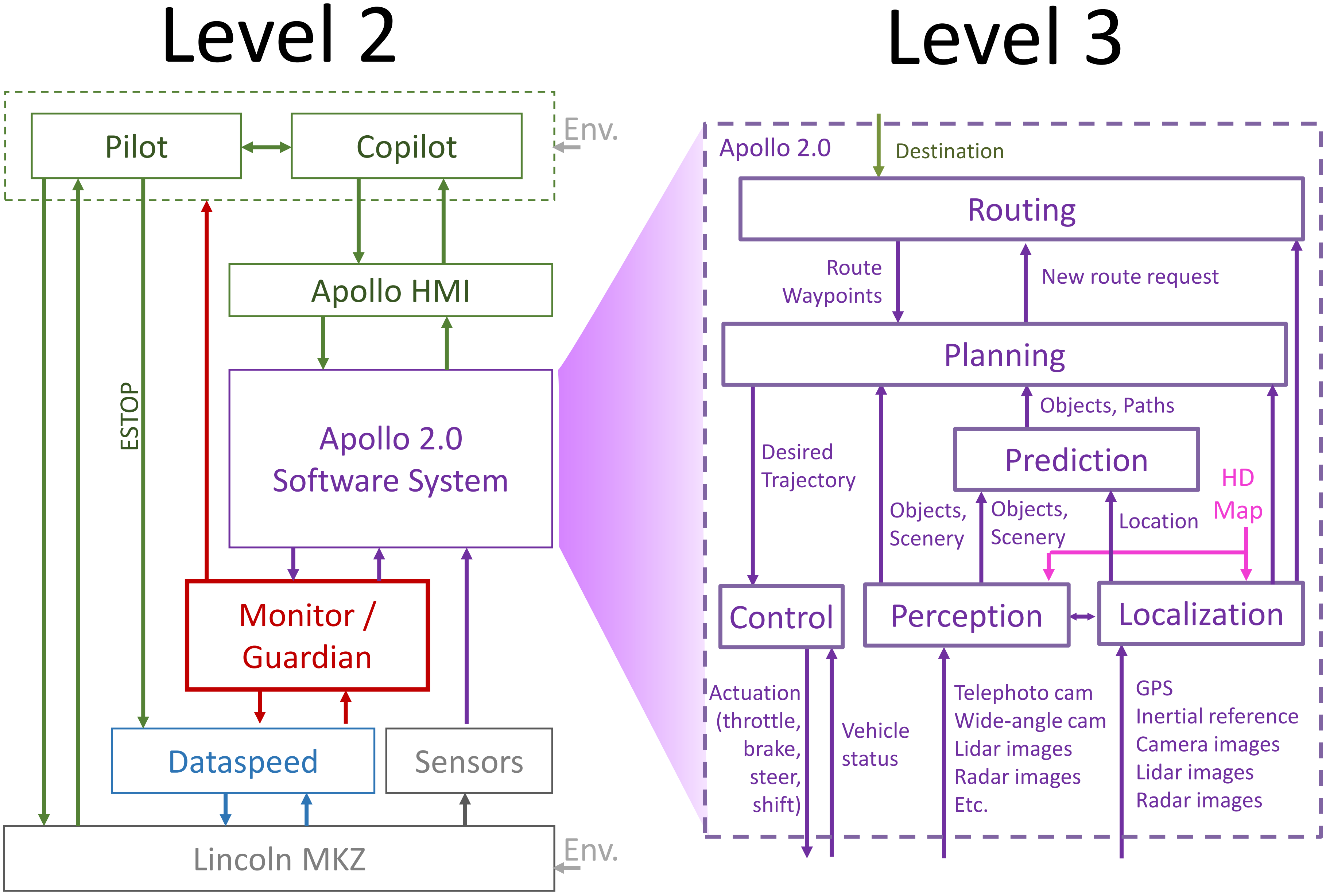
Level 1



Control Structure Refinement

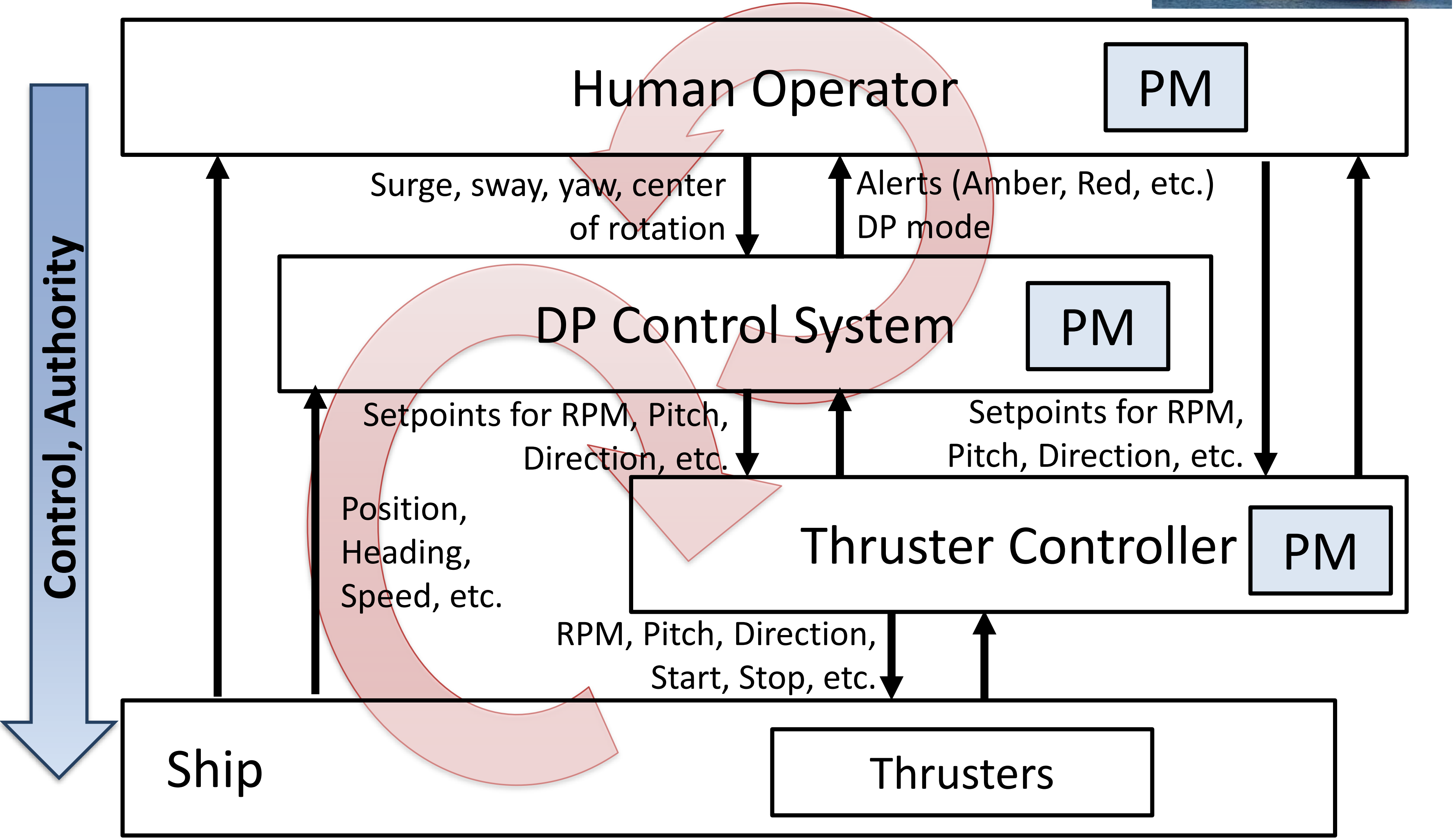


Control Structure Refinement



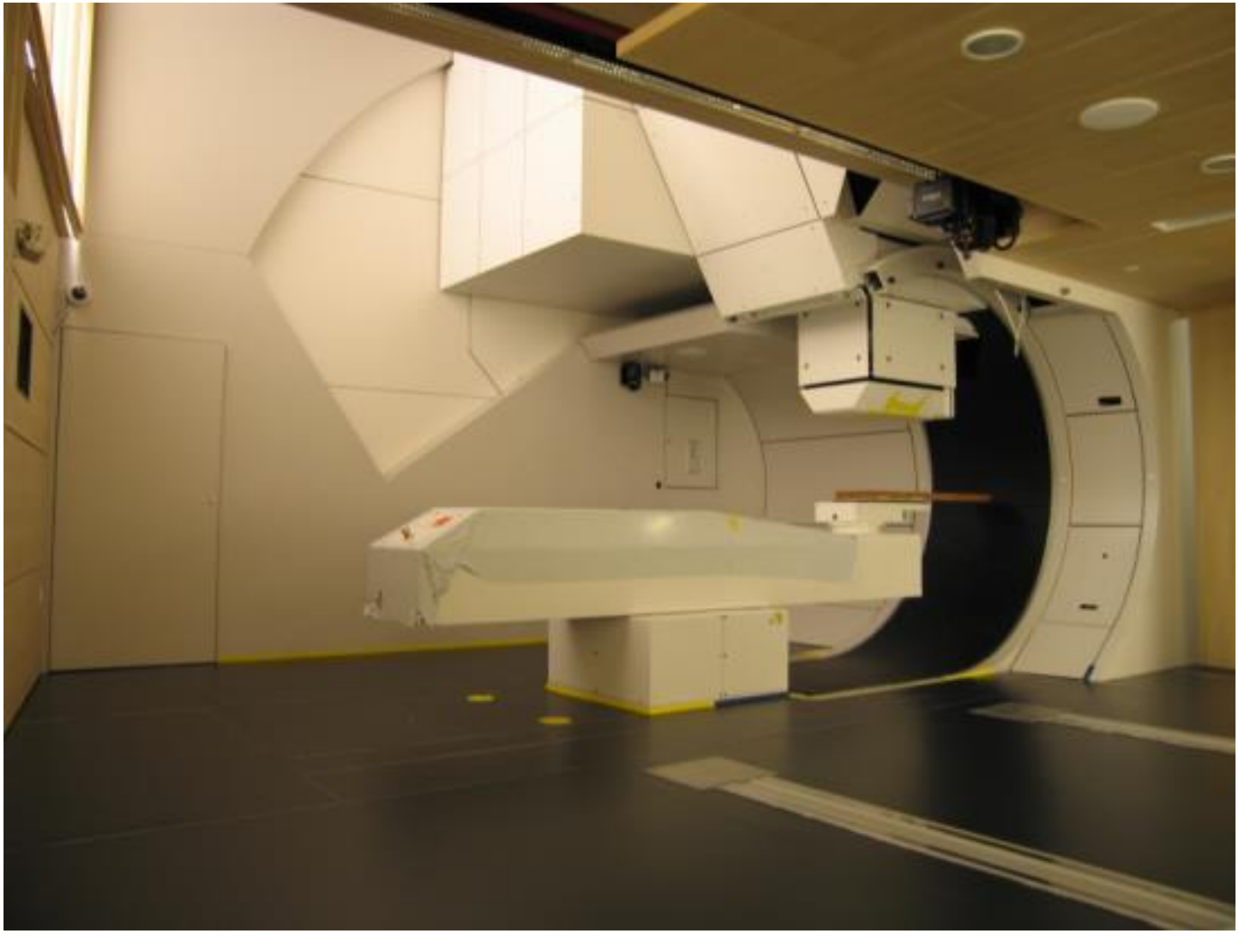
Thomas, 2019

STPA Control Structure (simplified)


Control, Authority
Human Operator
PM
Surge, sway, yaw, center of rotation
Alerts (Amber, Red, etc.)
DP mode
DP Control System
PM
Setpoints for RPM, Pitch, Direction, etc.
Setpoints for RPM, Pitch, Direction, etc.
Position, Heading, Speed, etc.
Thruster Controller
PM
RPM, Pitch, Direction, Start, Stop, etc.
Ship
Thrusters

Adapted from B. Abrecht, 2015; R. Puisa, 2019

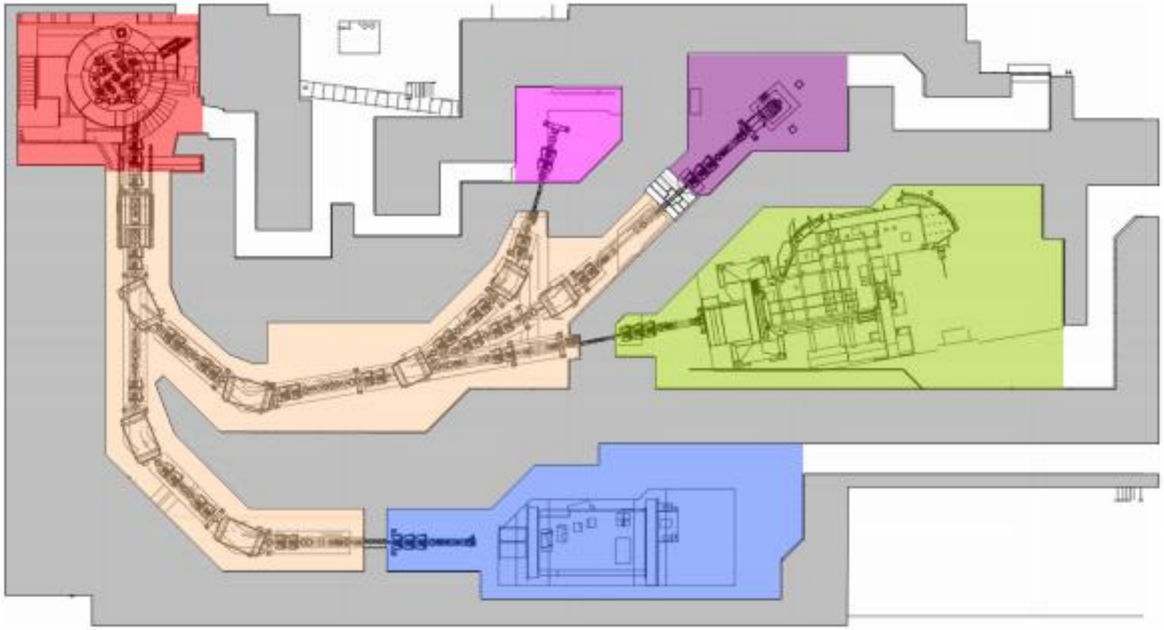
Proton Therapy Machine
High-level Control Structure



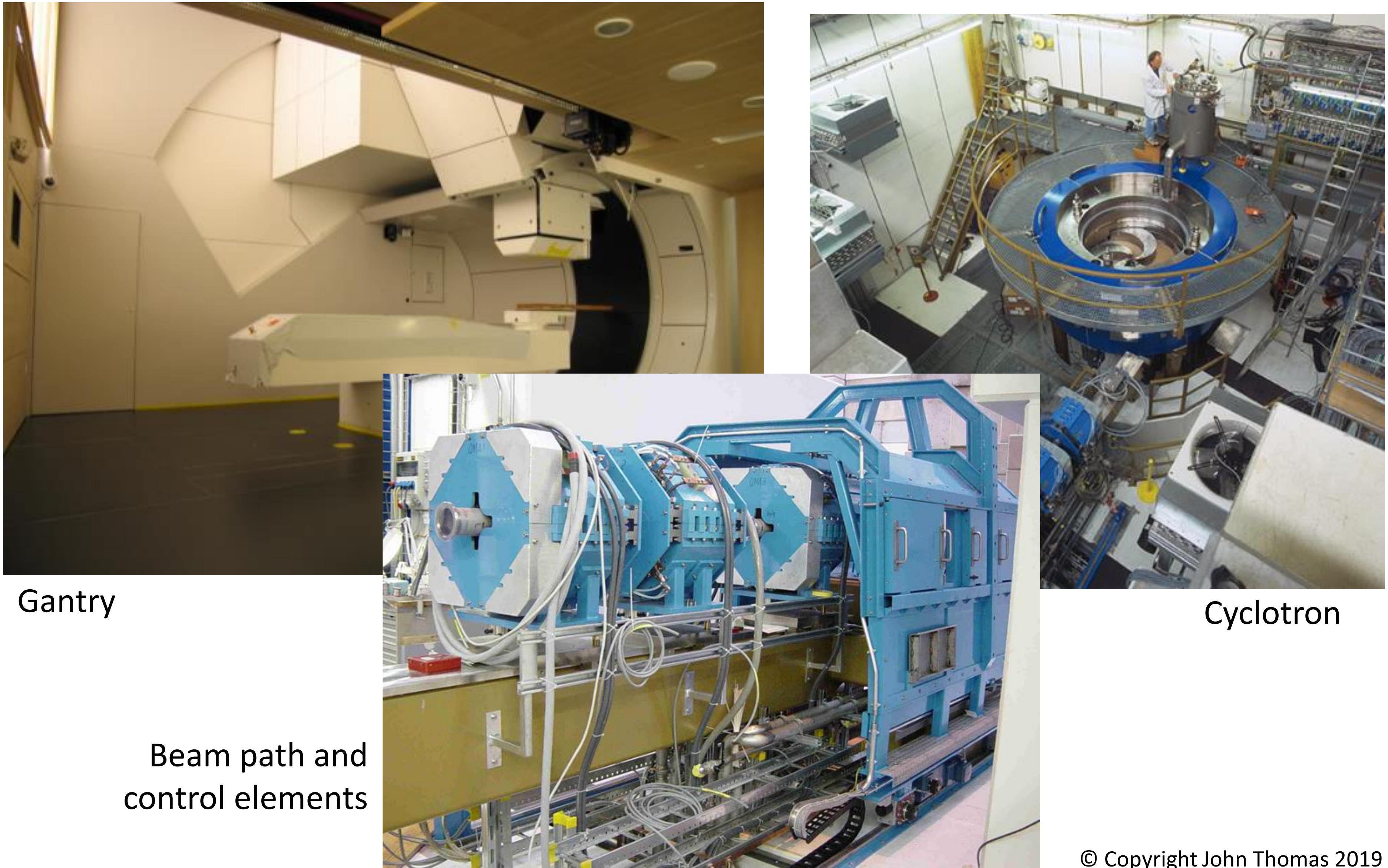
Proton Radiation Therapy System
Paul Scherrer Institute, Switzerland

Proton Radiation Therapy System
Paul Scherrer Institute, Switzerland

- 🟥 250 MeV Proton accelerator (superconducting cyclotron)
- 🟧 Beamlines to 4 user areas
- 🟪 OPTIS
- 🟦 Gantry 1
- 🟩 Gantry 2
- 🟪 Experimental area



Proton Therapy Machine High-level Control Structure

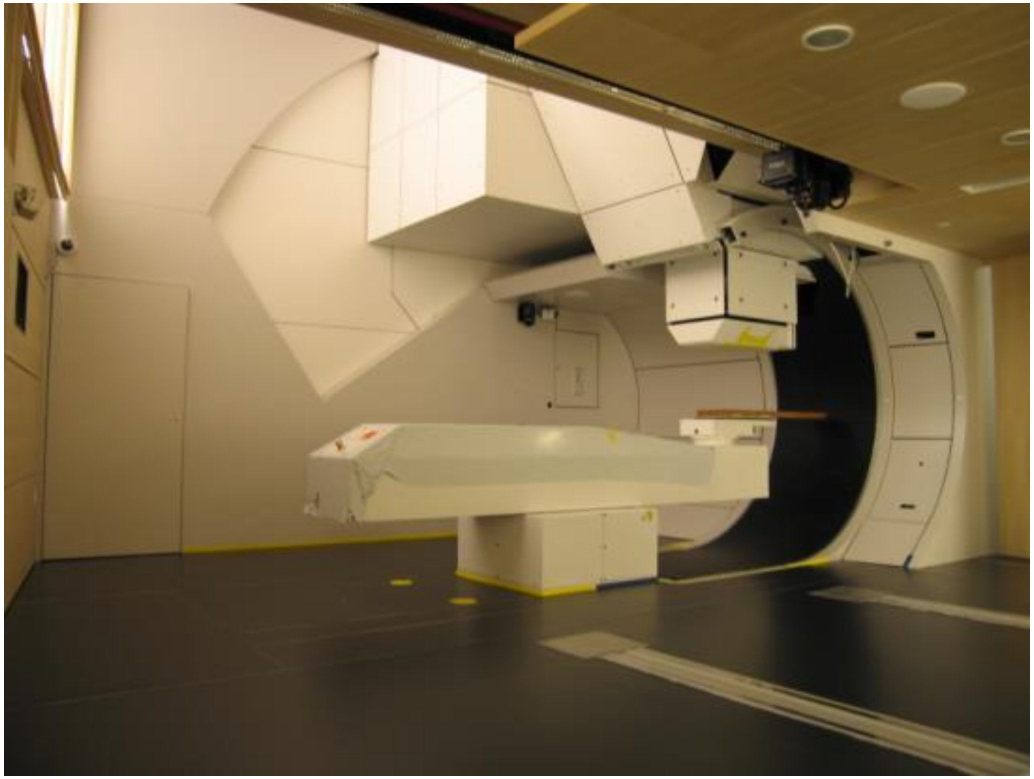


Gantry

Cyclotron

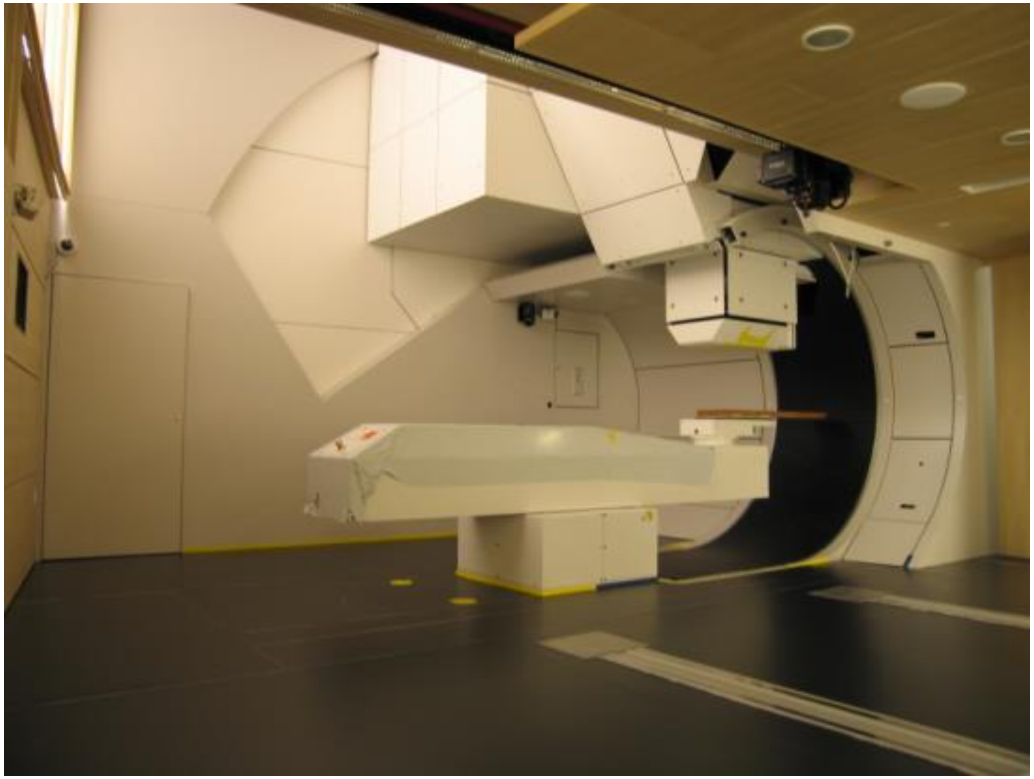
Beam path and control elements

Proton Therapy Machine
High-level Control Structure



- How big do you think the control structure is?

Proton Therapy Machine
High-level Control Structure



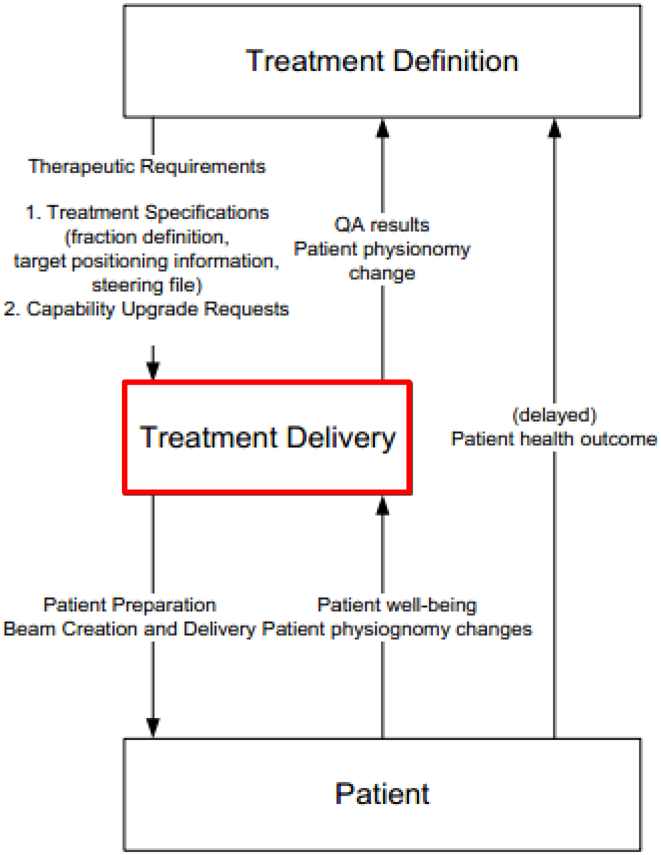
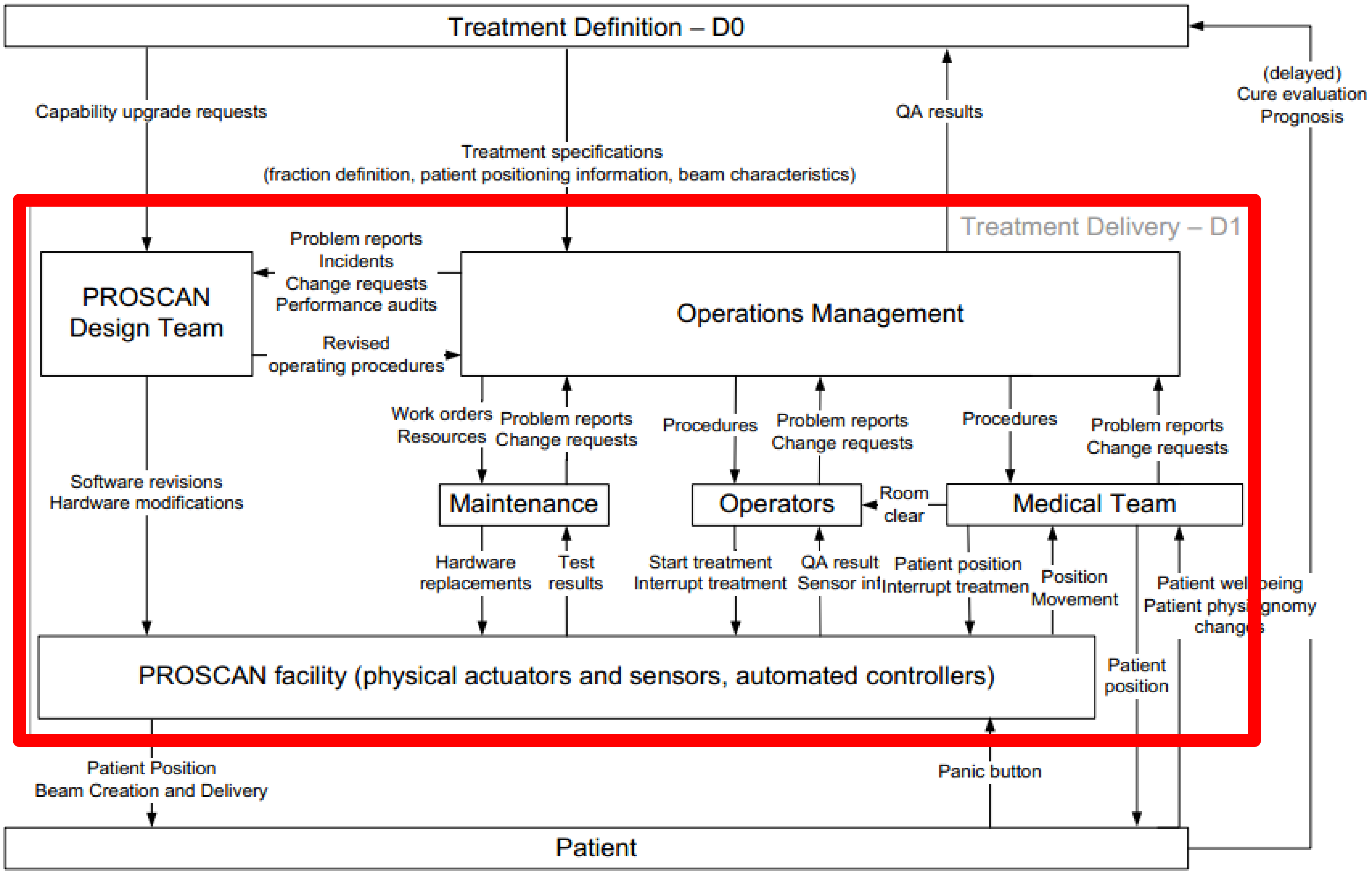


Figure 11 - High-level functional description of the PROSCAN facility (D0)

Antoine PhD Thesis, 2012

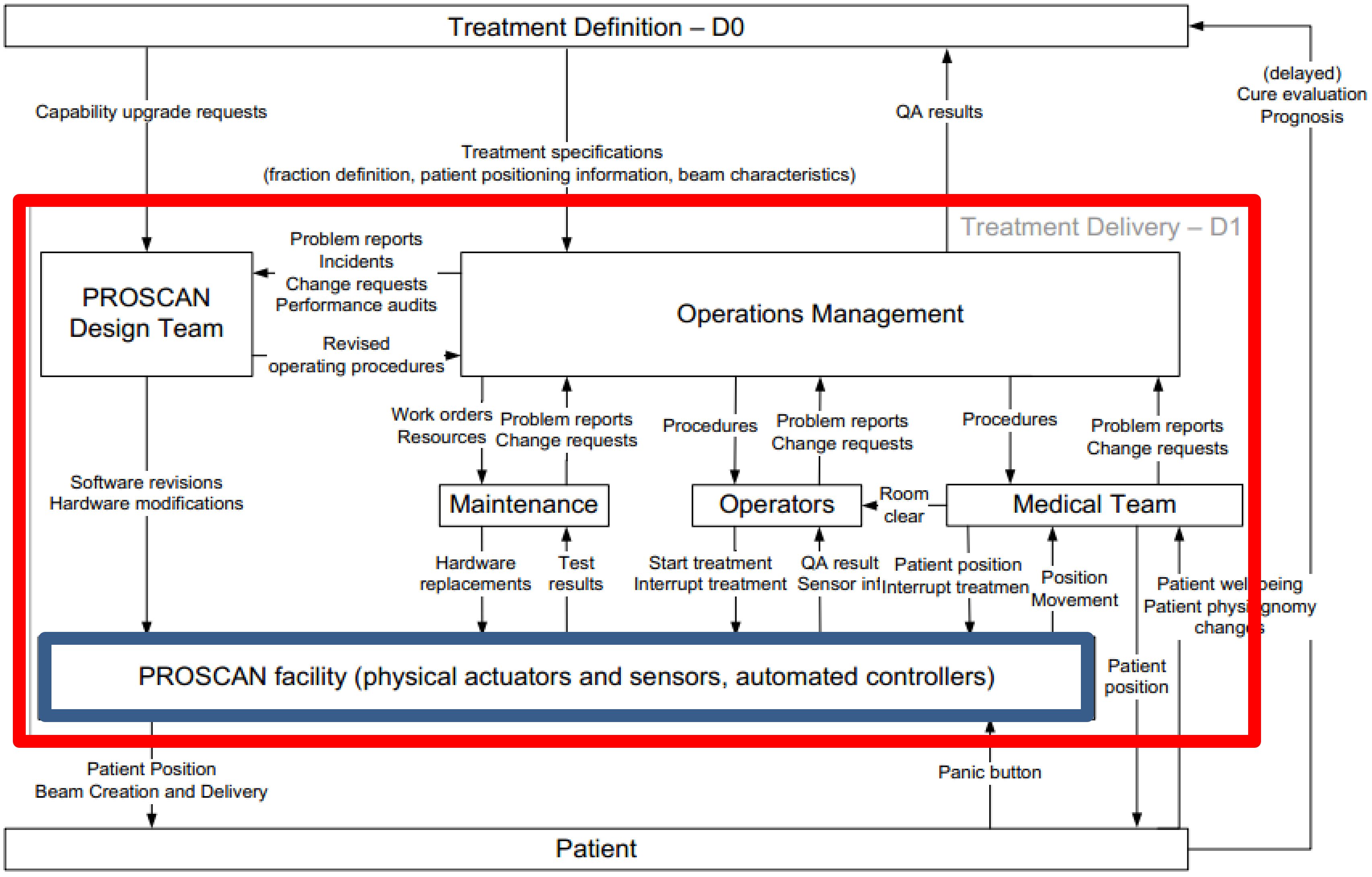
Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

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

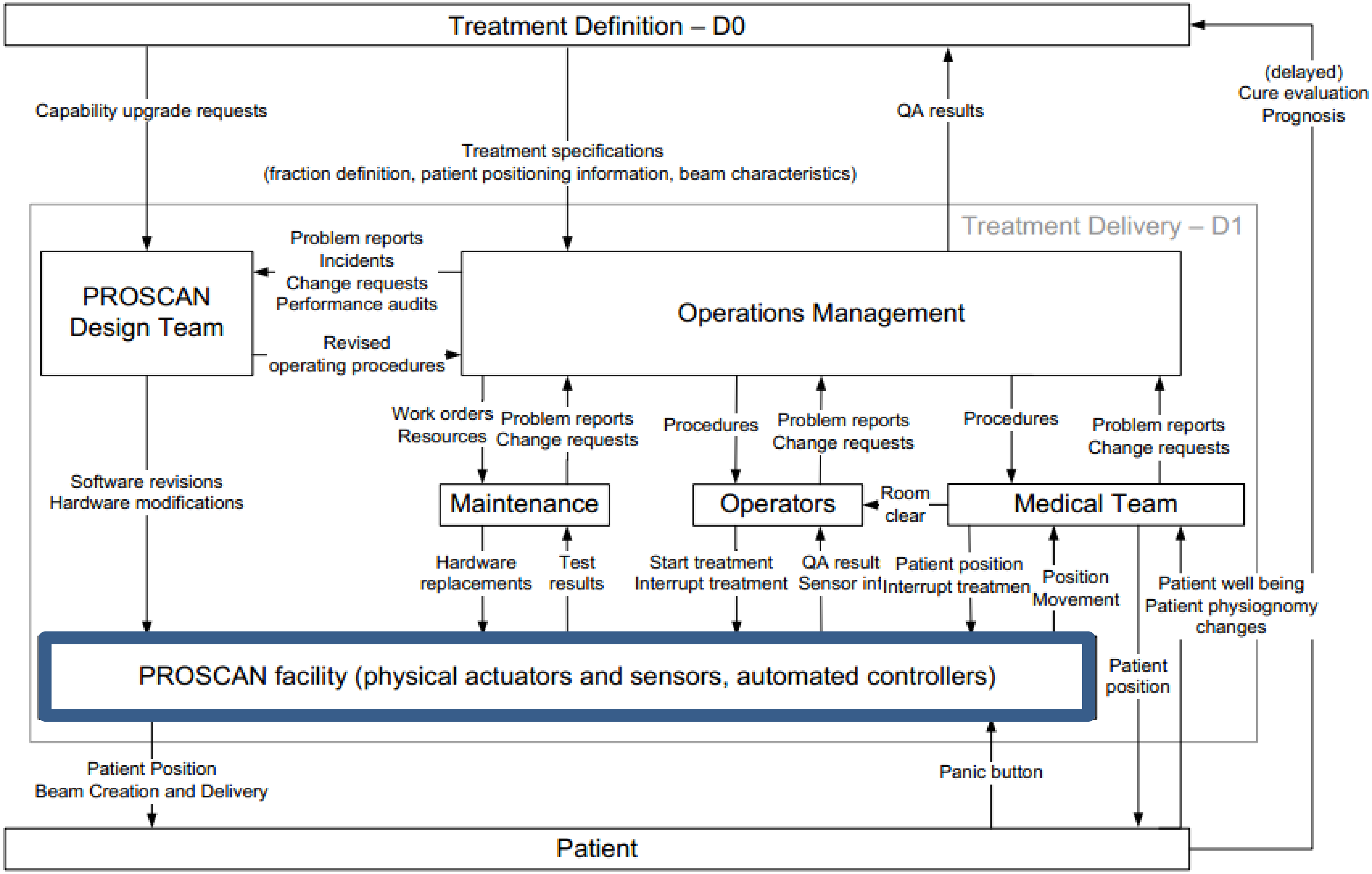
Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

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

Proton Therapy Machine Control Structure



Antoine PhD Thesis, 2012

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

Adaptive Cruise Control

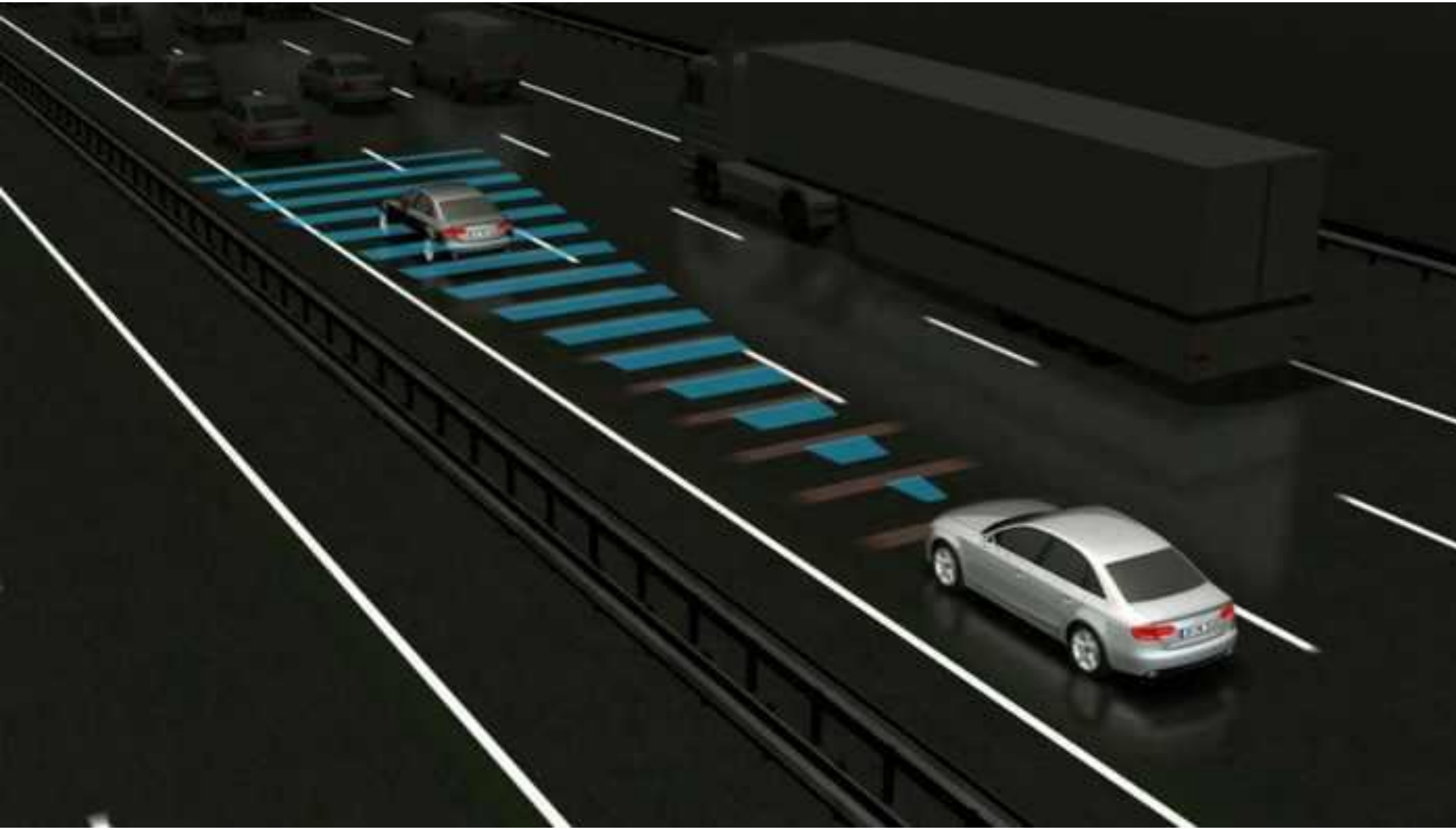
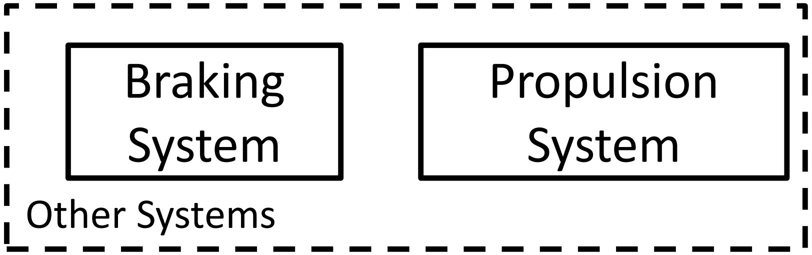


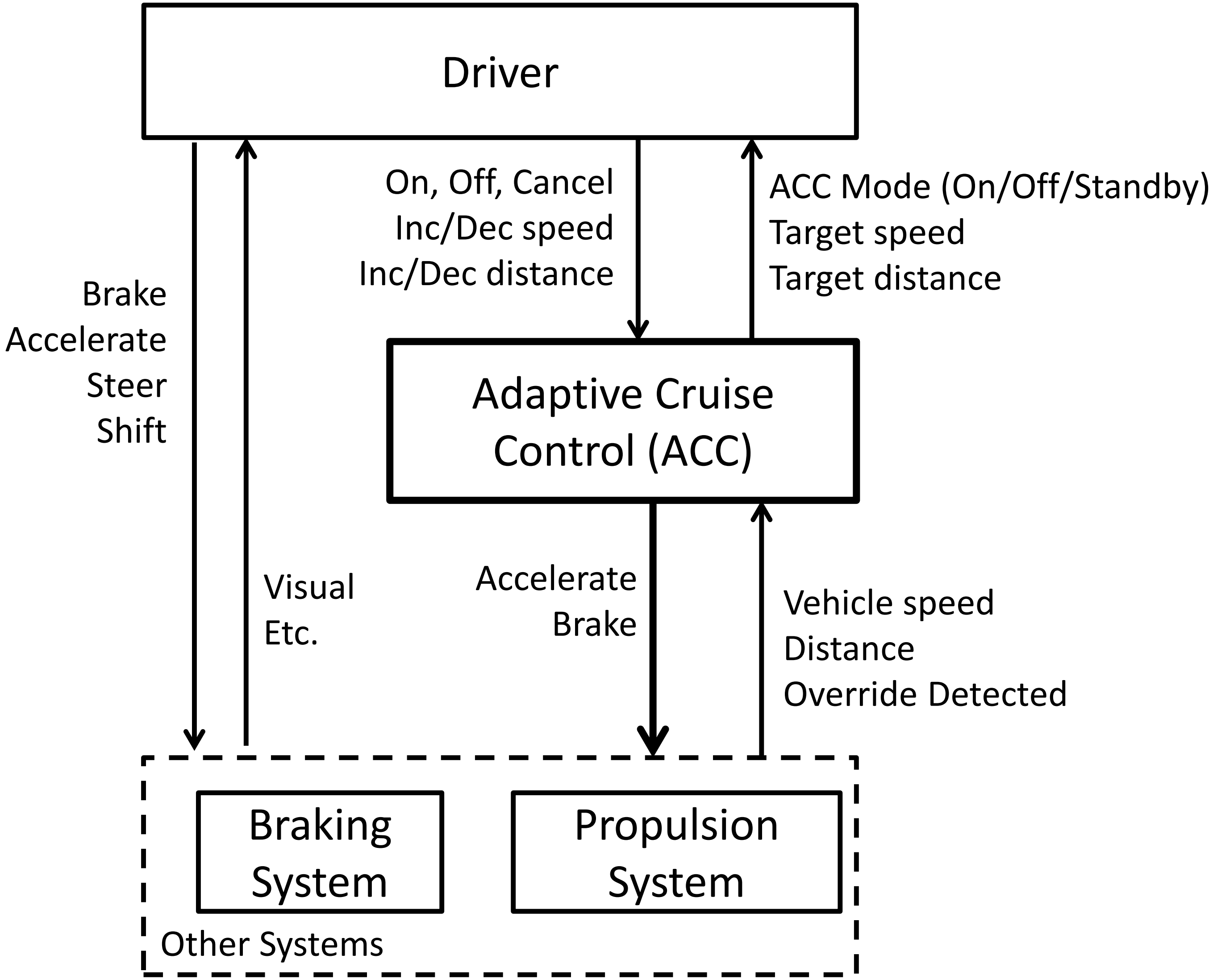
Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

Adaptive Cruise Control (ACC) Control Structure



Thomas, 2017

Adaptive Cruise Control (ACC) Control Structure



Driver

On, Off, Cancel
Inc/Dec speed
Inc/Dec distance

ACC Mode (On/Off/Standby)
Target speed
Target distance

Brake
Accelerate
Steer
Shift

Visual
Etc.

Adaptive Cruise Control (ACC)

Accelerate
Brake

Vehicle speed
Distance
Override Detected

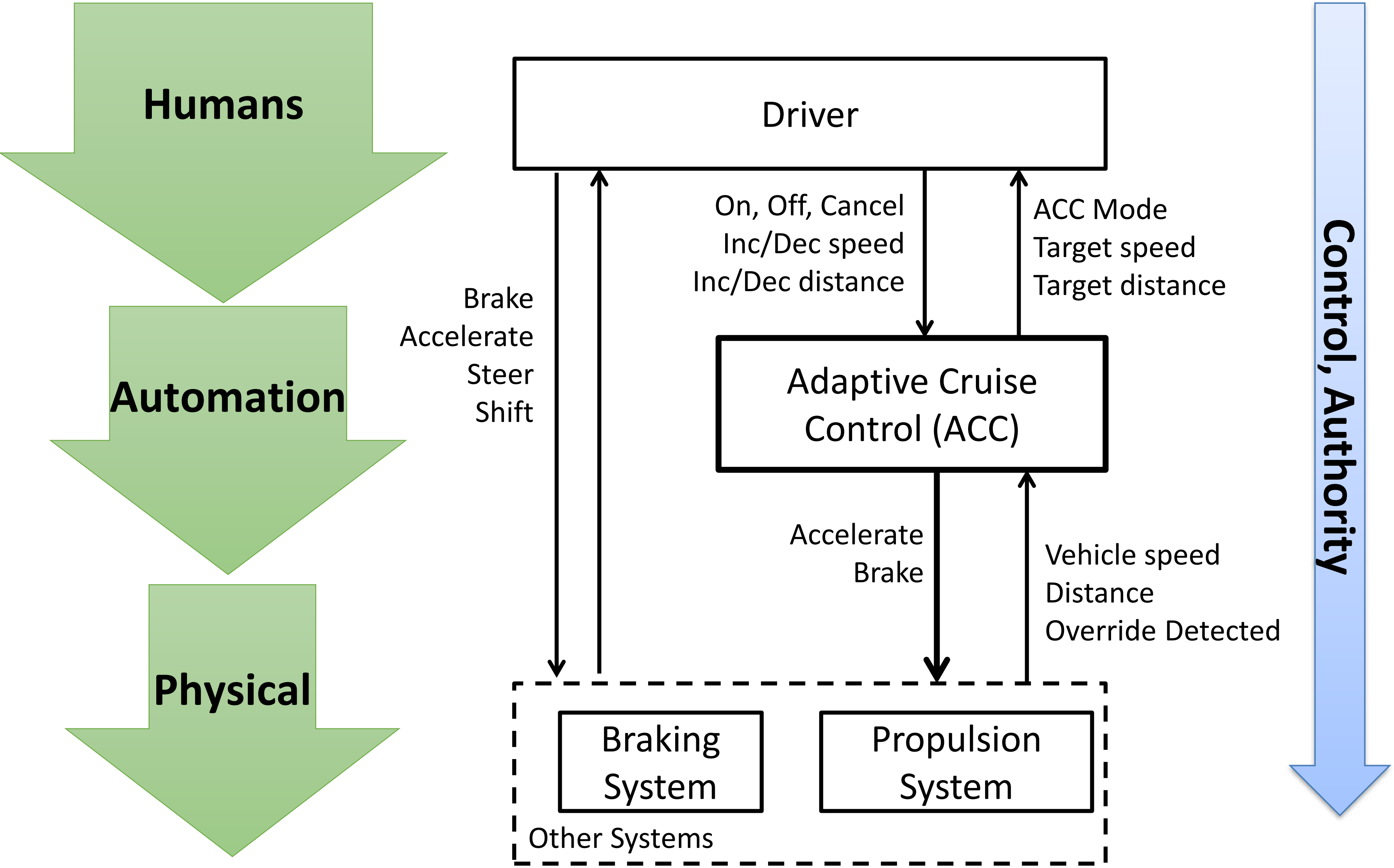
Braking System

Propulsion System

Other Systems

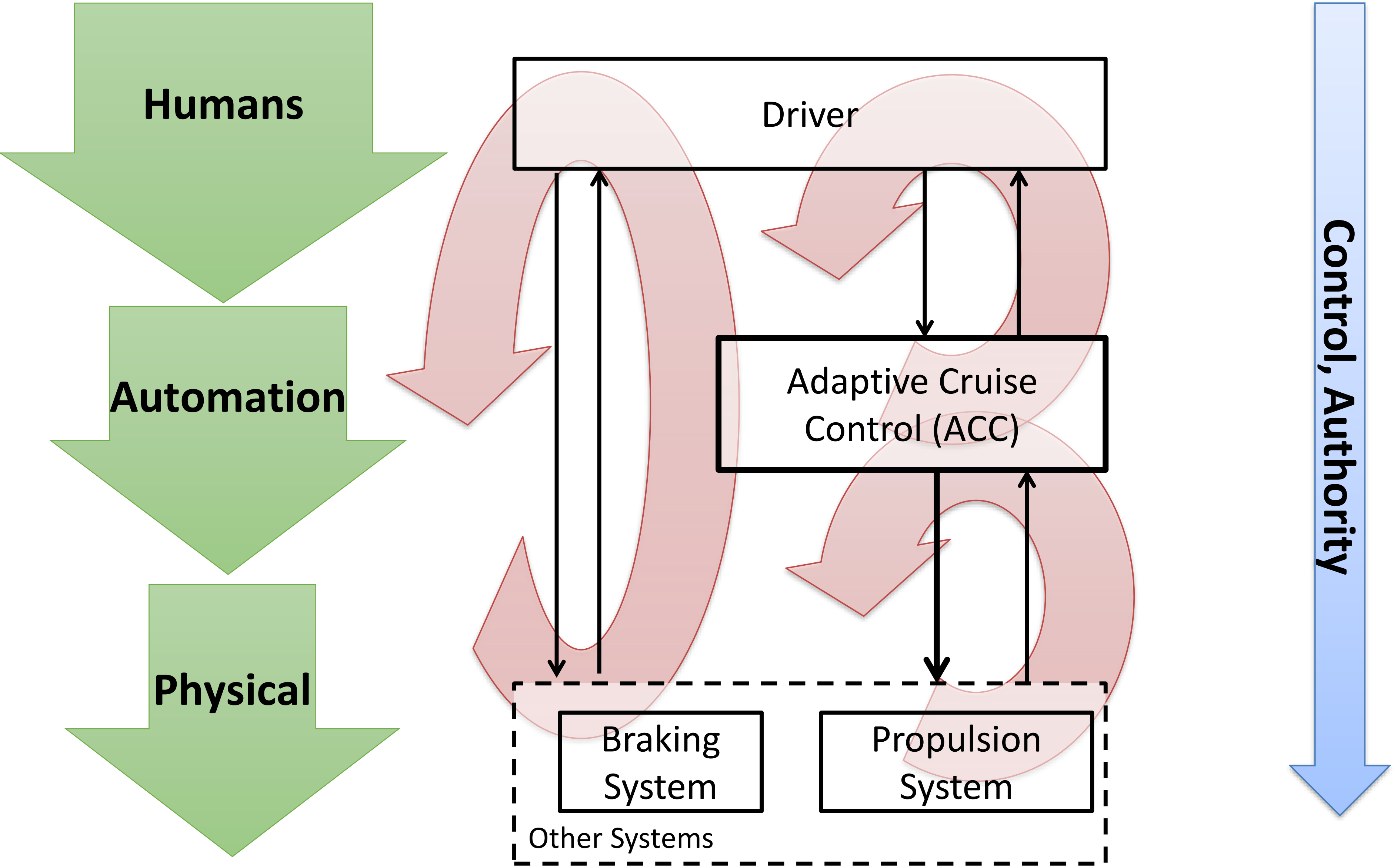
Thomas, 2017

Adaptive Cruise Control (ACC) Control Structure



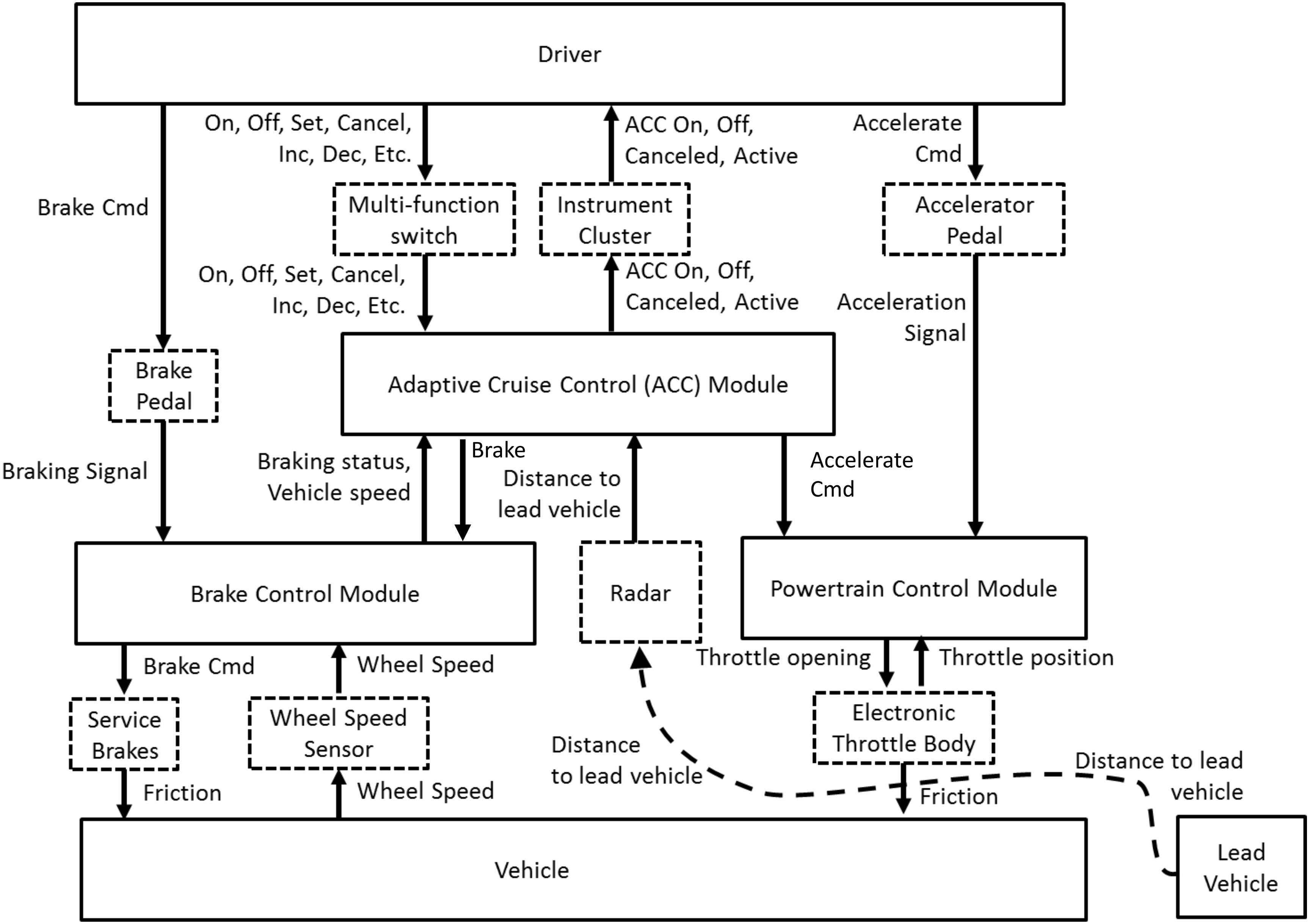
Thomas, 2017

Adaptive Cruise Control (ACC) Control Structure

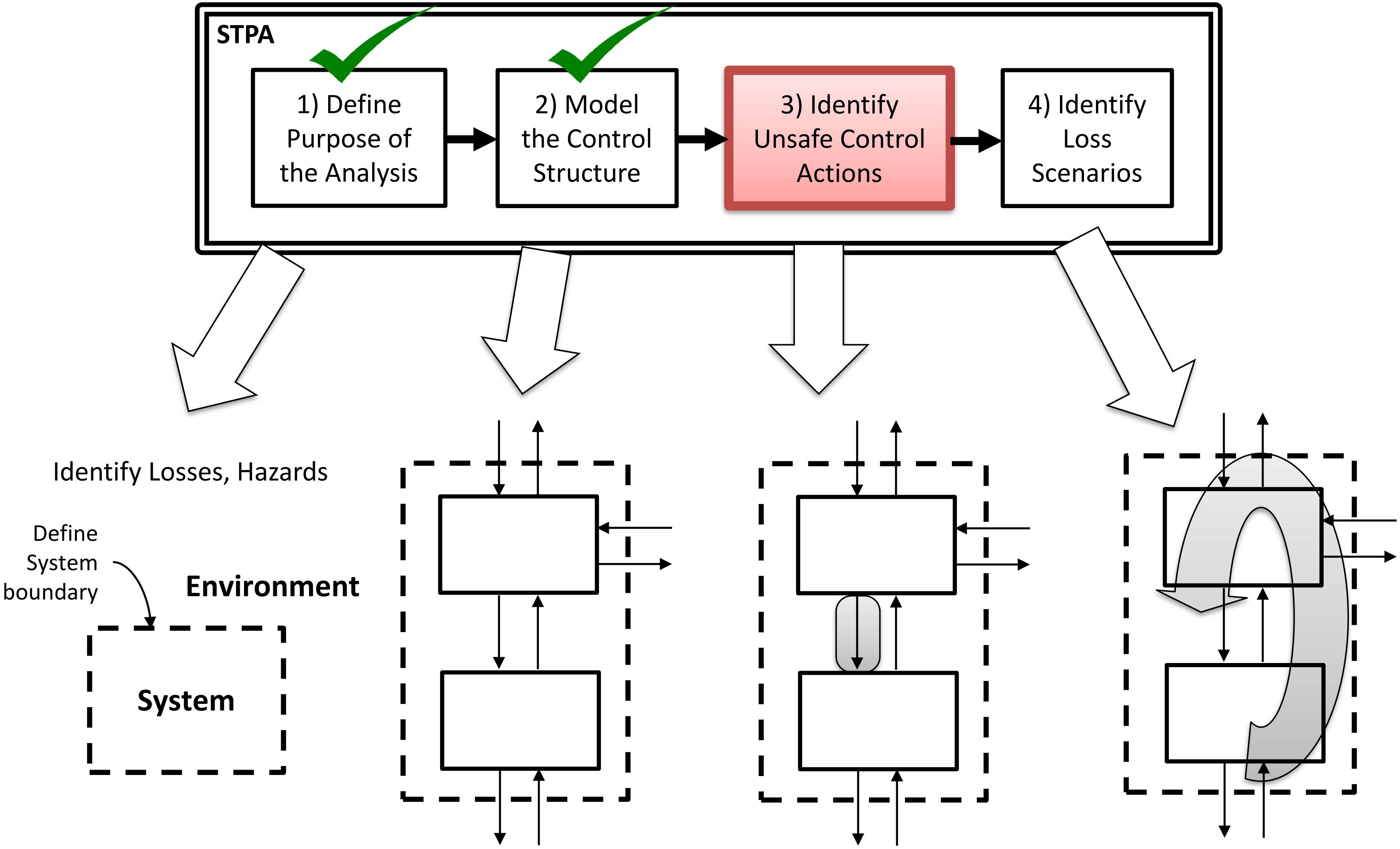


Thomas, 2017

Refined Control Structure



Thomas, 2017



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

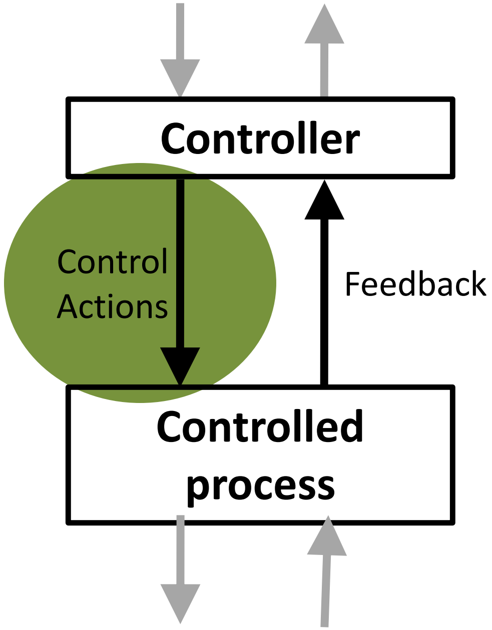
Define System boundary

Environment

System

(Leveson and Thomas, 2018)

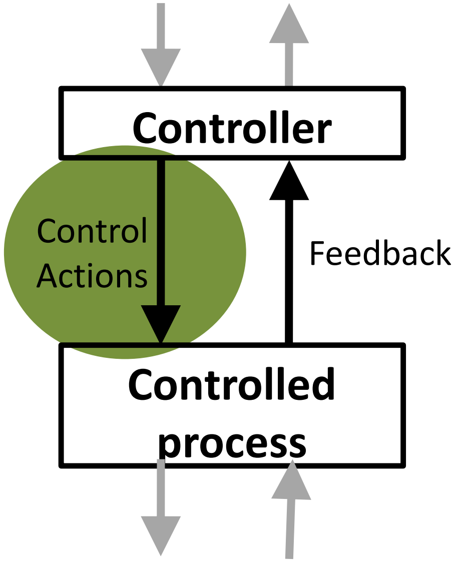
Identifying Unsafe Control Actions (UCA)



4 ways unsafe control may occur:

Brake Command				

Identifying Unsafe Control Actions (UCA)



Example:

"Driver does not provide Brake cmd while forward collision imminent"

Source Controller

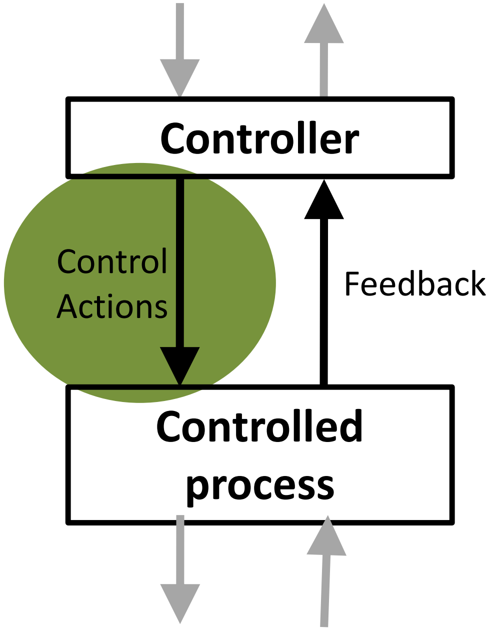
Type

Control Action

Context

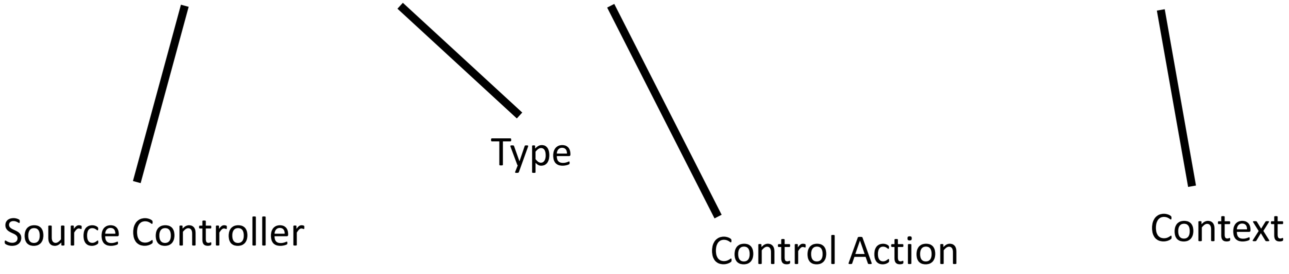
	Not providing causes hazard	Providing causes hazard	Too early, too late, Order	Stopped Too Soon / Applied too long
Brake Command	?	?	?	?

Identifying Unsafe Control Actions (UCA)



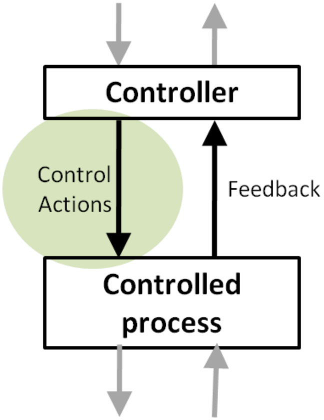
Example:

"Computer provides Shift-to-Park cmd while vehicle is moving"

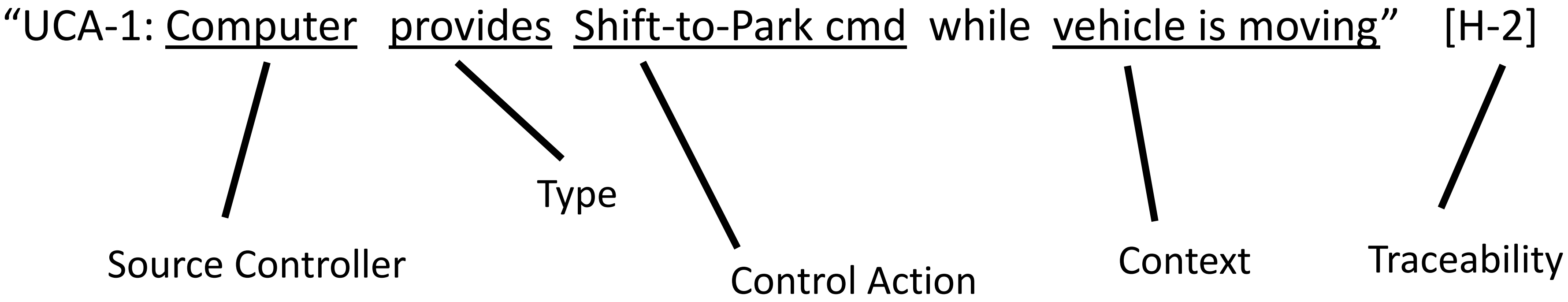


	Not providing causes hazard	Providing causes hazard	Too early, too late, Order	Stopped Too Soon / Applied too long
Brake Command	?	?	?	?

Structure of an Unsafe Control Action



Example:



“UCA-1: Computer provides Shift-to-Park cmd while vehicle is moving” [H-2]

Source Controller

Type

Control Action

Context

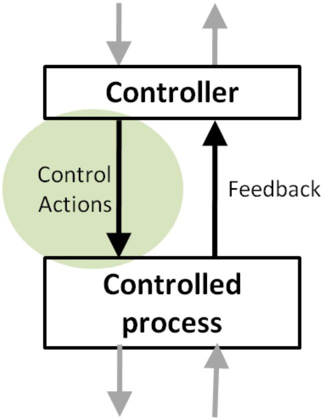
Traceability

Four parts of an unsafe control action

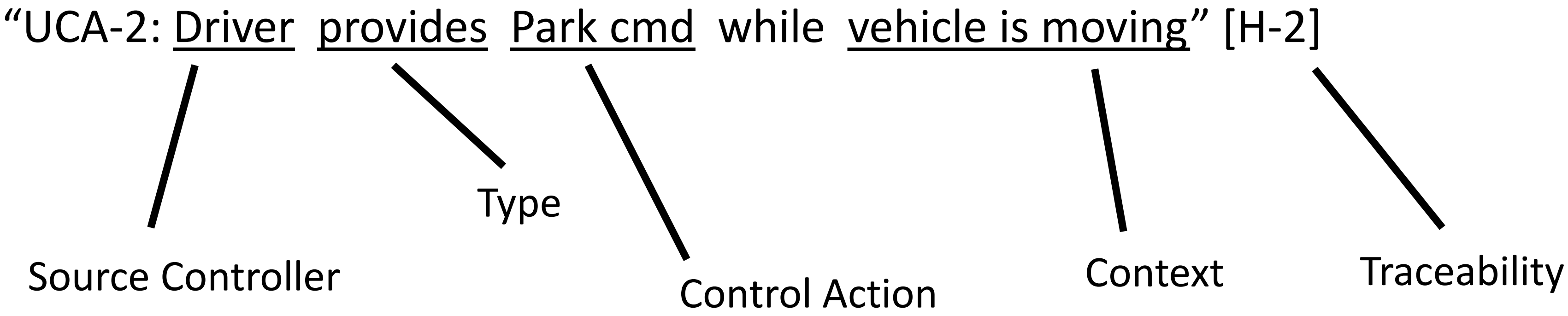
- Source Controller: the controller that can provide the control action
- Type: whether the control action provided, not provided, etc.
- Control Action: the controller’s command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)

Thomas, 2017

Structure of an Unsafe Control Action



Example:

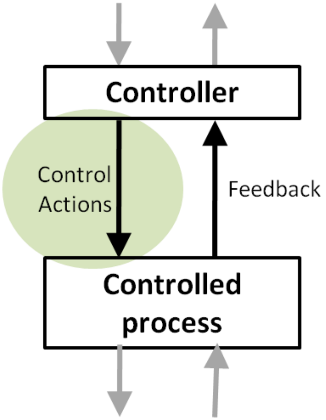

“UCA-2: Driver provides Park cmd while vehicle is moving” [H-2]

Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action provided, not provided, etc.
- 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)

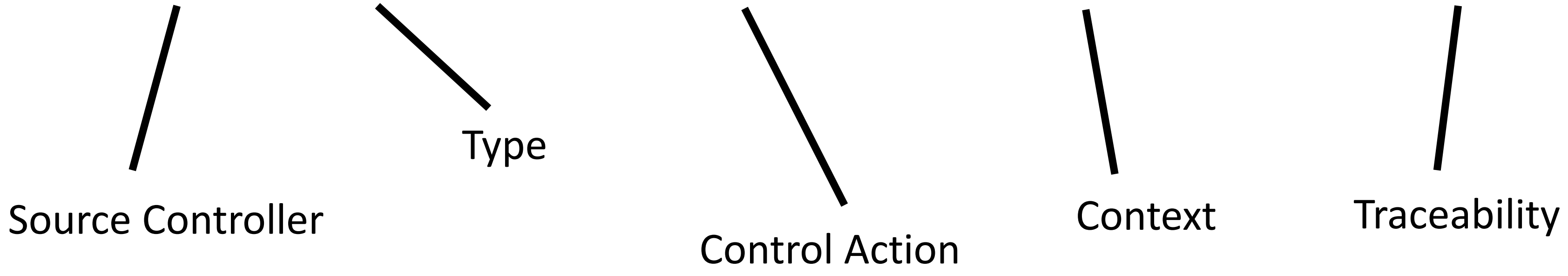
Thomas, 2017

Structure of an Unsafe Control Action



Example:

UCA-2: “Driver does not provide Park cmd before _______________” [H-2]

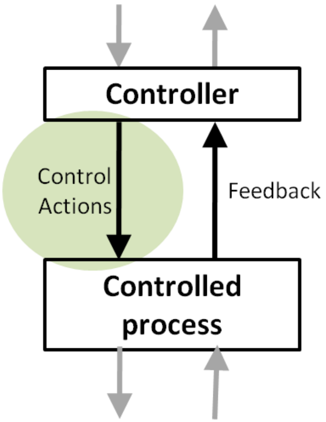


Four parts of an unsafe control action

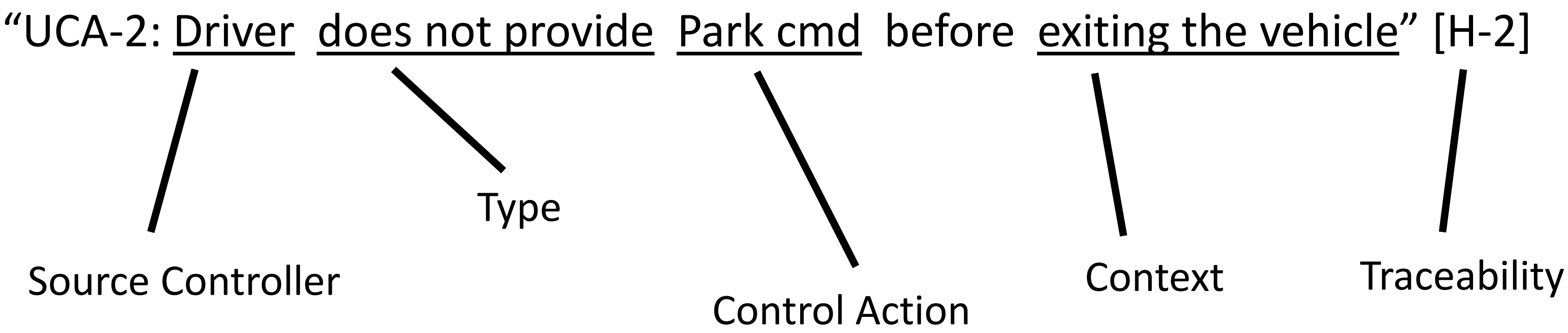
- Source Controller: the controller that can provide the control action
- Type: whether the control action provided, not provided, etc.
- Control Action: the controller’s command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)

Thomas, 2017

Structure of an Unsafe Control Action



Example:


“UCA-2: Driver does not provide Park cmd before exiting the vehicle” [H-2]

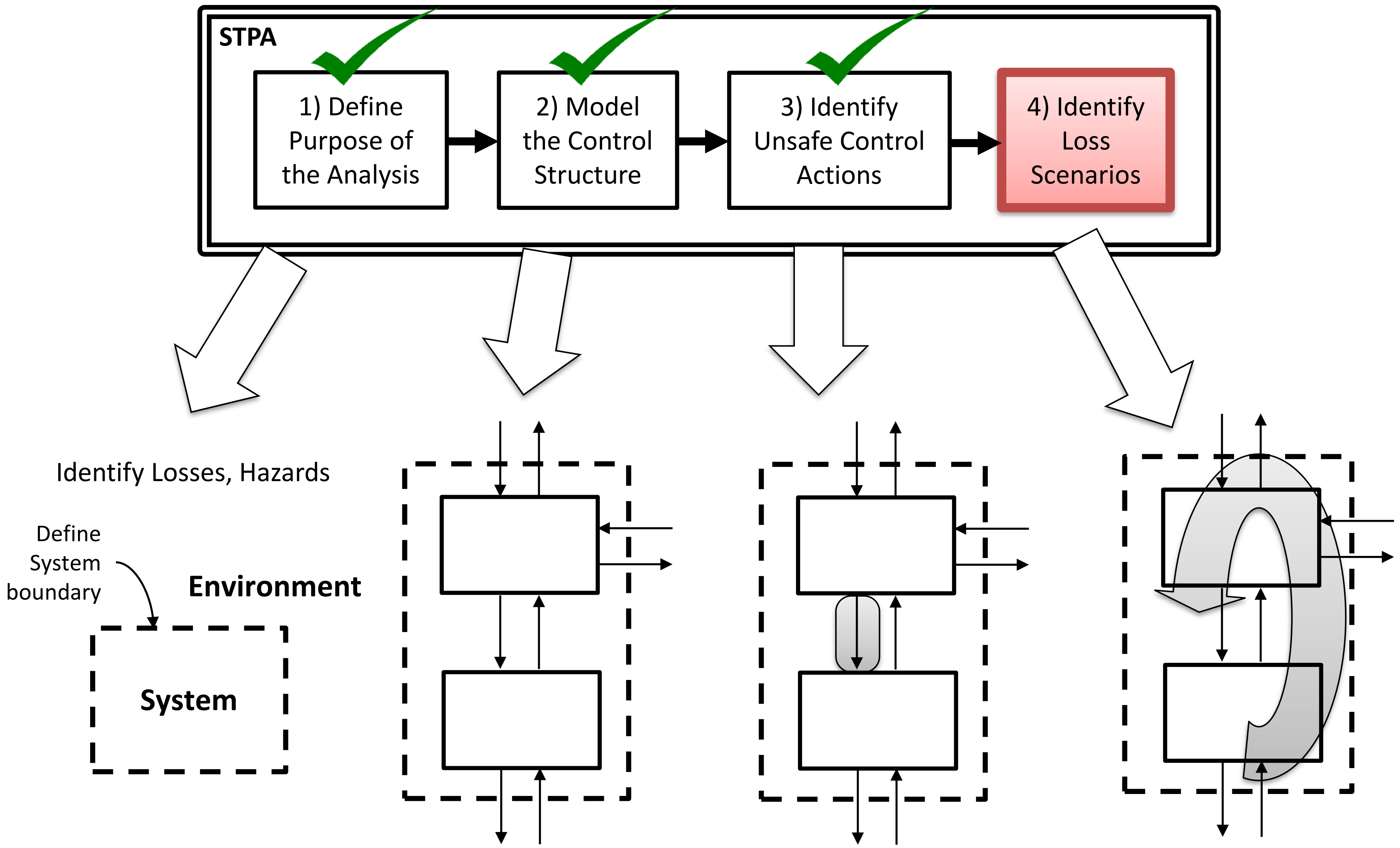
Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action provided, not provided, etc.
- 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, 2017

Component Safety Constraints

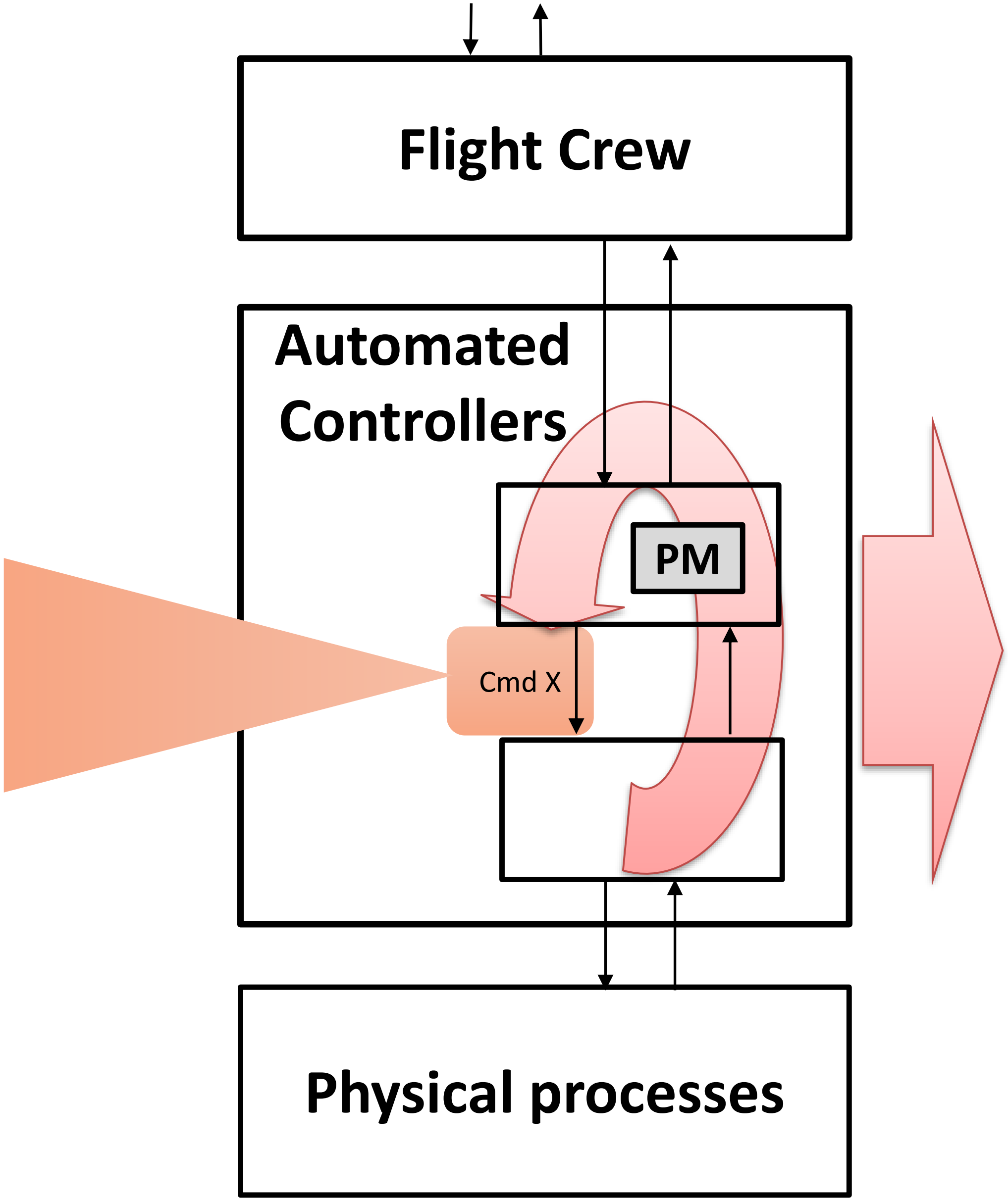
Unsafe Control Action		**Component Safety Constraint**
UCA-1: Driver does not provide Shift-to-Park cmd before exiting vehicle [H-3]	➡	SC-1: Driver shall provide Shift-to-Park cmd before exiting vehicle [UCA-1]
	➡	
	➡	
	➡	


STPA
✓
1) Define Purpose of the Analysis
✓
2) Model the Control Structure
✓
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

(Leveson and Thomas, 2018)

Identify loss scenarios

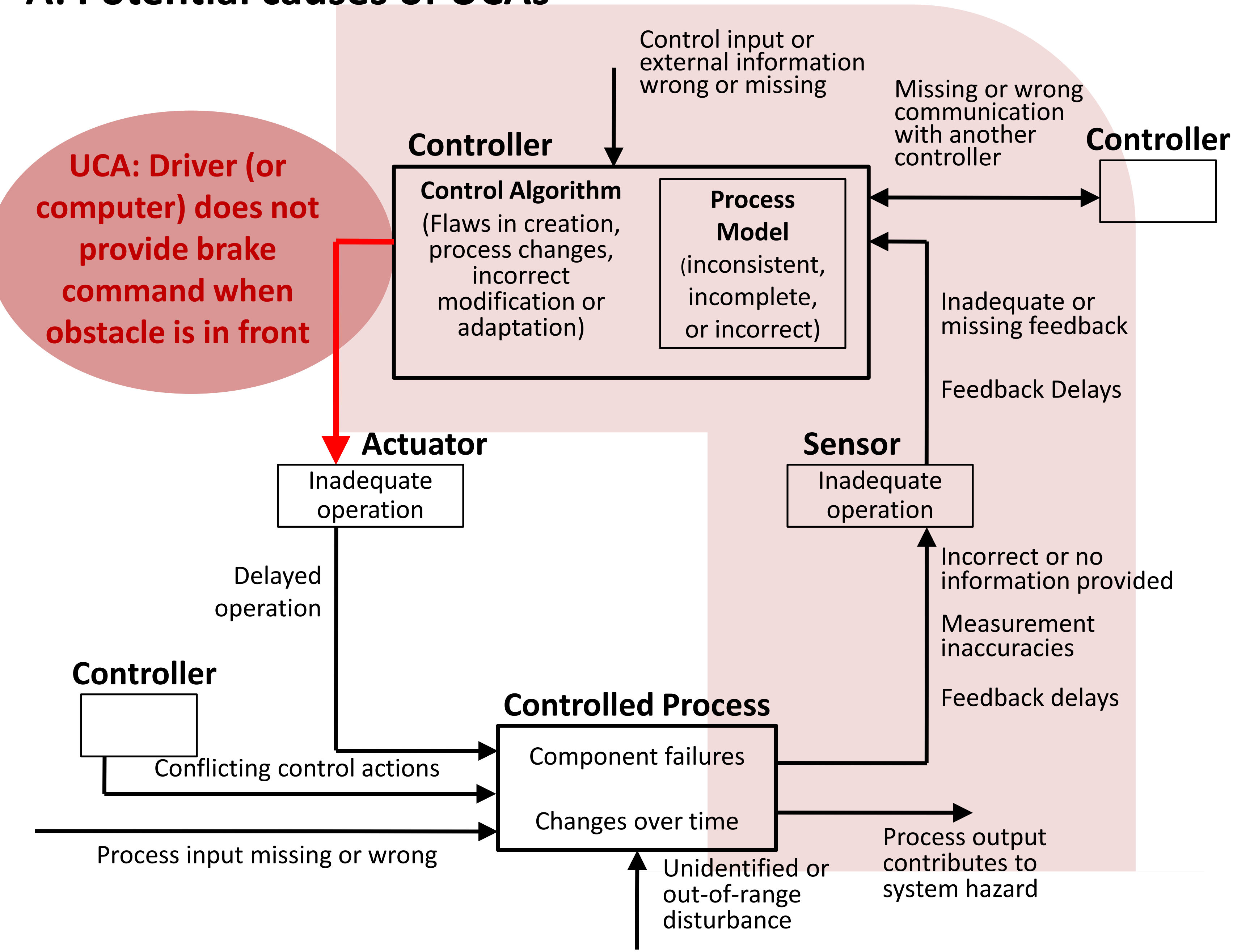
What could cause Unsafe Control Actions?



Scenarios
Controller incorrectly believes X because …
Controller control algorithm does not enforce Y because …
Incorrect feedback Z received because …
Sensor failure causes…
Etc.

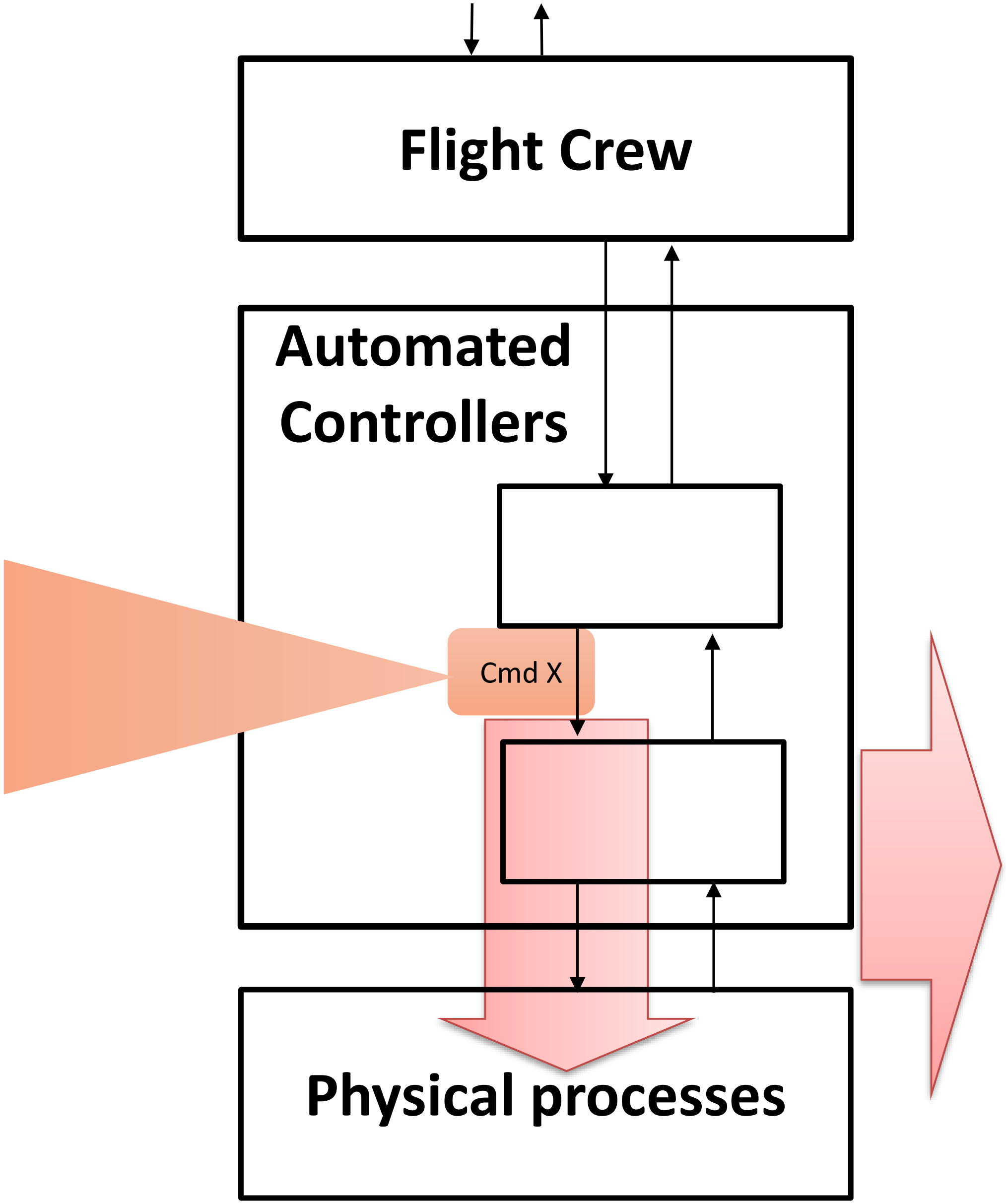
(Thomas, 2017)

A: Potential causes of UCAs


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
UCA: Driver (or computer) does not provide brake command when obstacle is in front
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
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

Thomas, 2017

Identify loss scenarios

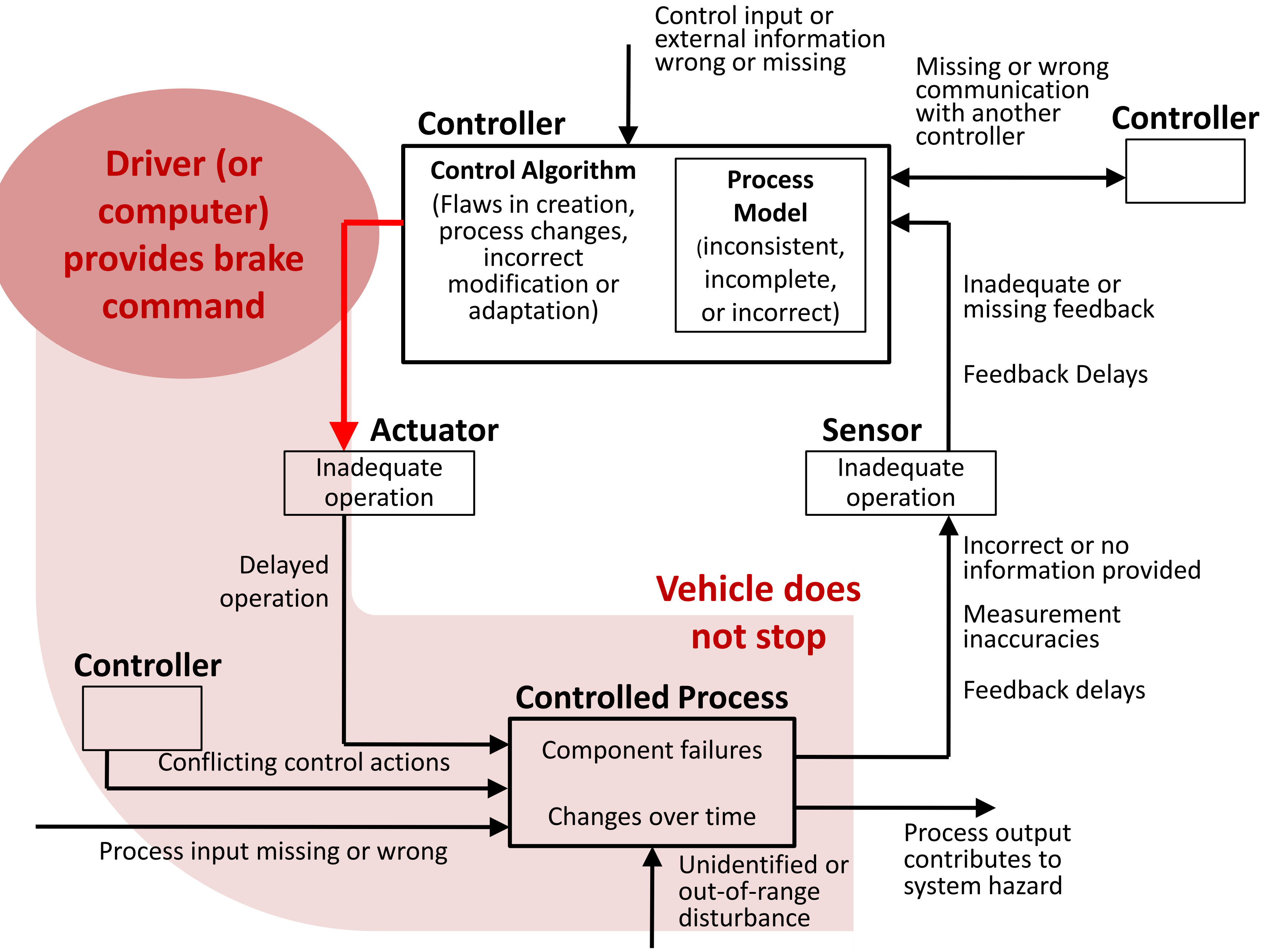


Control actions not executed or not followed properly

Scenarios
Cmd sent but not received because…
Cmd received but ignored because…
Actuator failure causes…

(Thomas, 2017)

B: Potential control actions not followed



Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Controller

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

Process Model (inconsistent, incomplete, or incorrect)

Driver (or computer) provides brake command

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delayed operation

Vehicle does not stop

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

Conflicting control actions

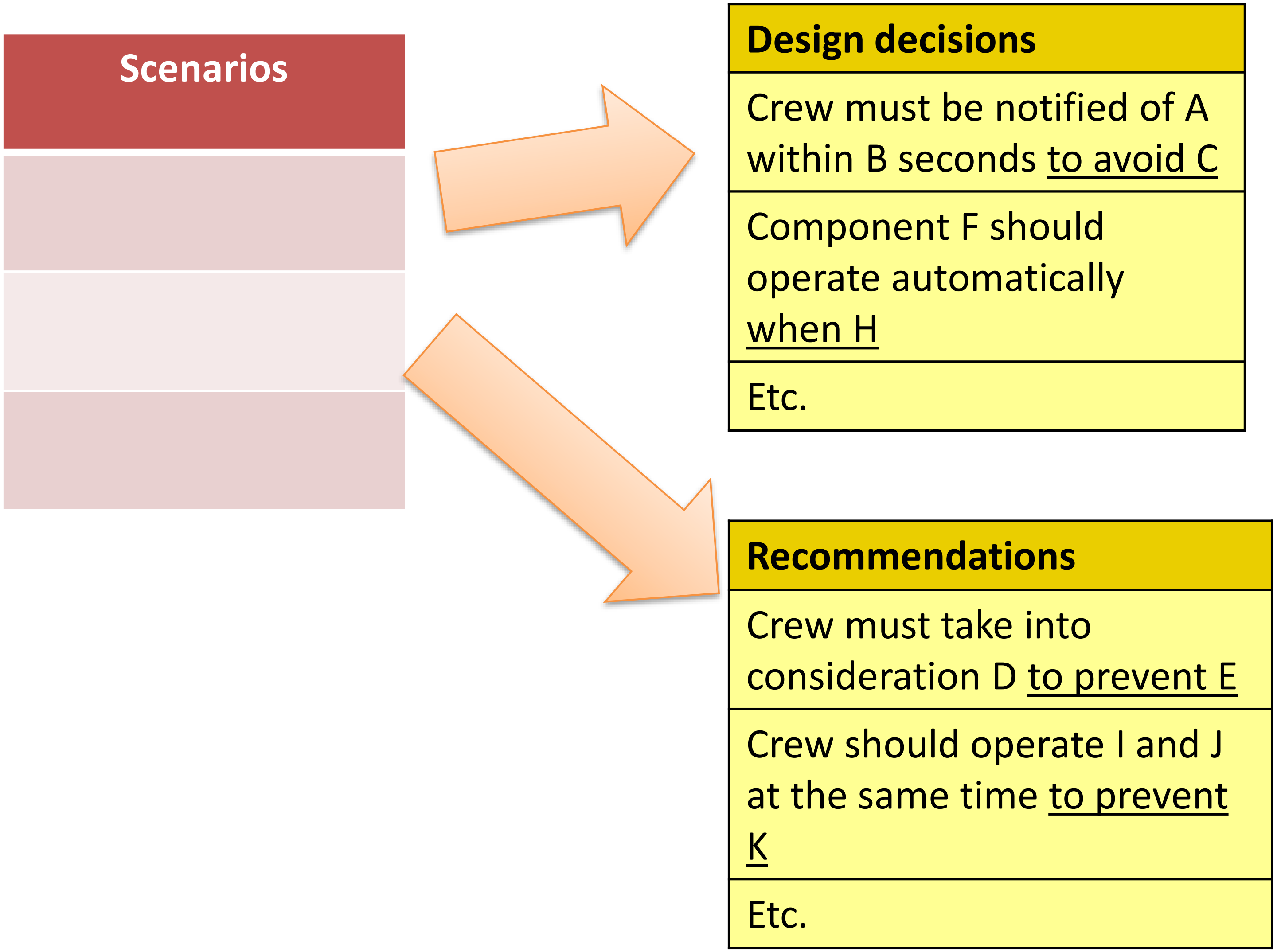
Process input missing or wrong

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Thomas, 2017

Design decisions and recommendations



Scenarios

Design decisions

Crew must be notified of A within B seconds to avoid C

Component F should operate automatically when H

Etc.

Recommendations

Crew must take into consideration D to prevent E

Crew should operate I and J at the same time to prevent K

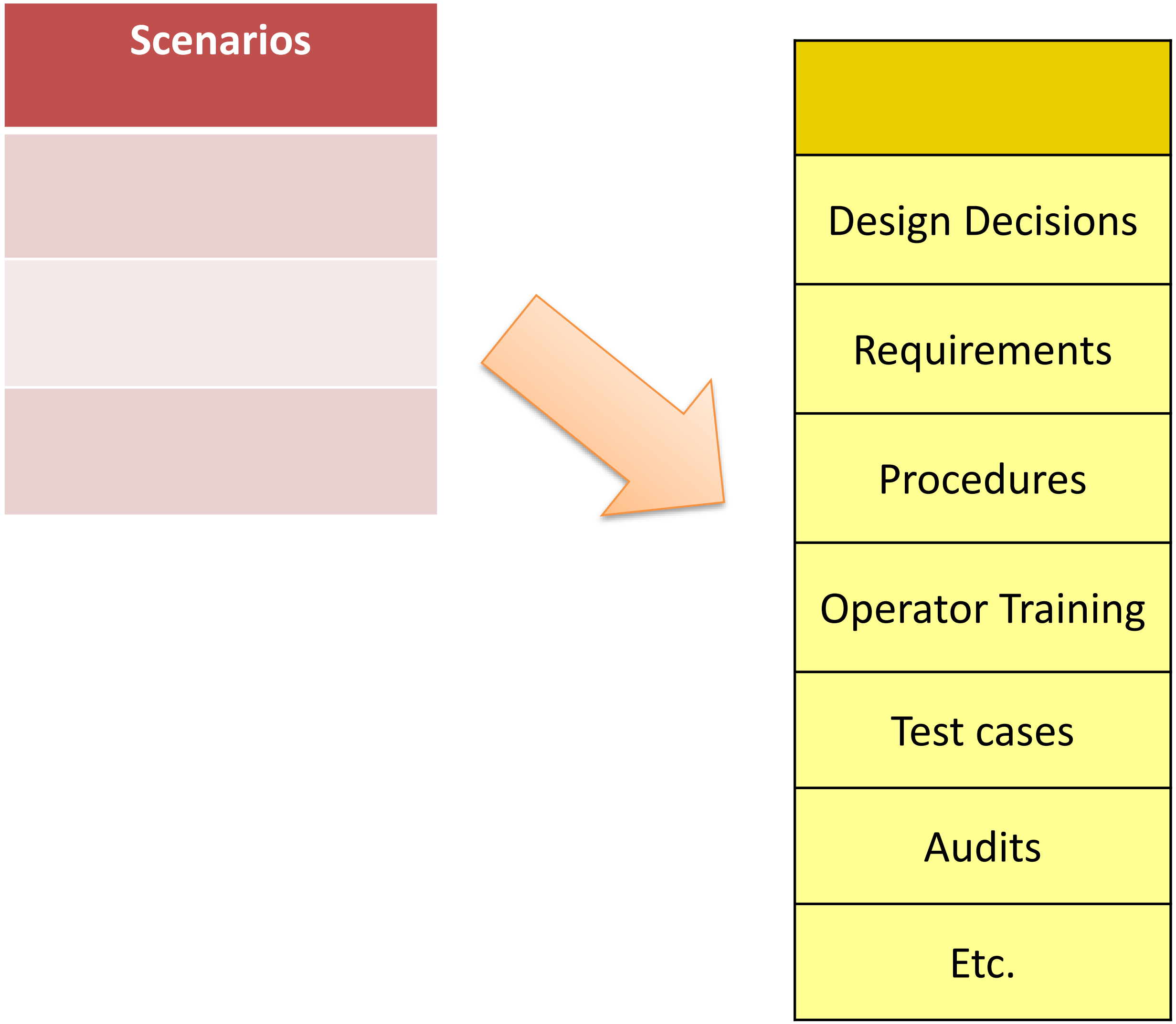
Etc.

Rationale and assumptions identified

Every recommendation and decision is traceable

(Thomas, 2017)

Design decisions, requirements, training, test cases, audits, etc.



Scenarios

Design Decisions

Requirements

Procedures

Operator Training

Test cases

Audits

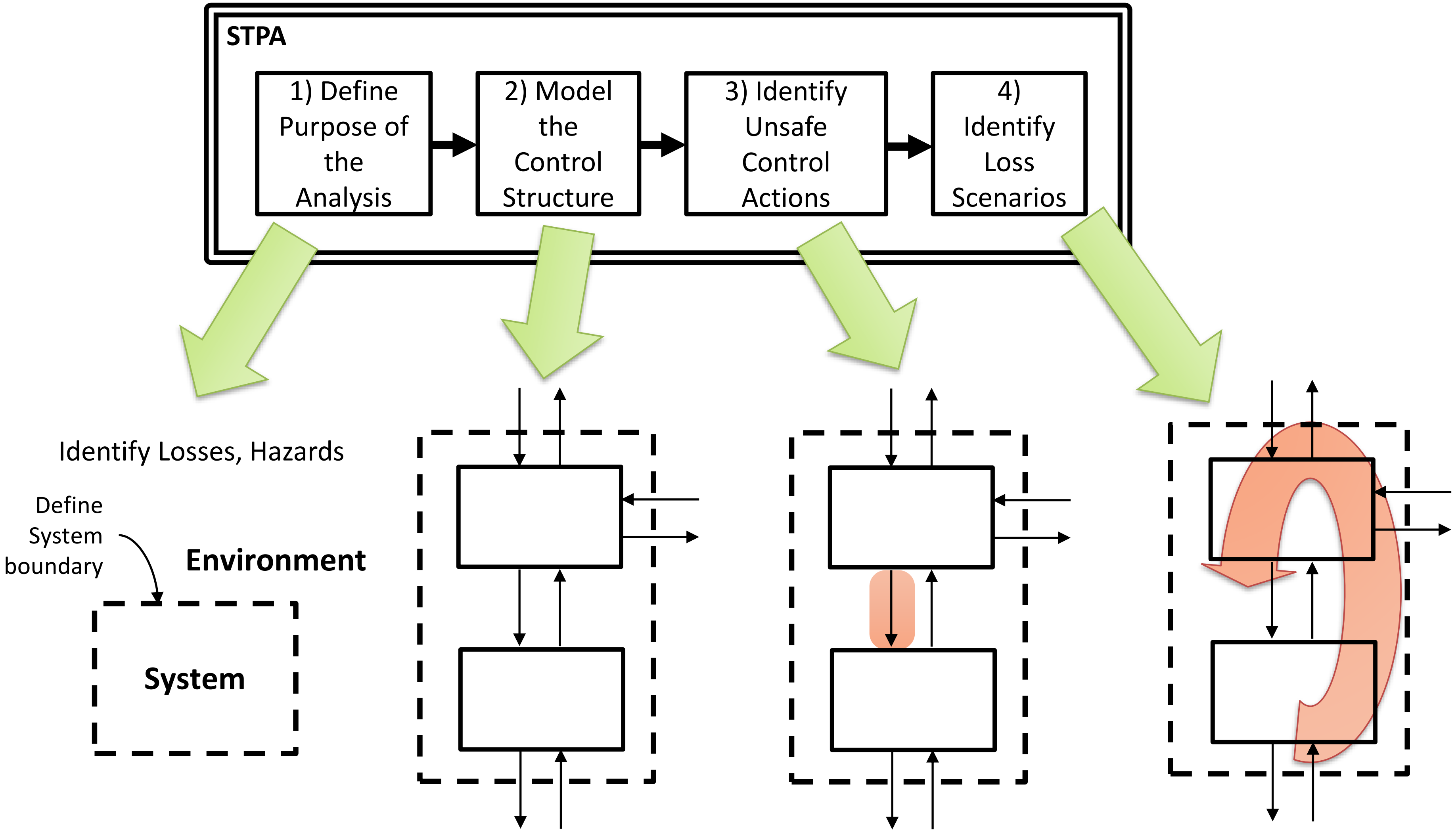
Etc.

Rationale and assumptions identified

Every recommendation and decision is traceable

(Thomas, 2017)

STPA Overview



STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

(Leveson and Thomas, 2018)

Summary

- Role of air/ground switch failure states was not fully recognized during the original design process
  - Inputs protecting against inadvertent activation had a common mode failure case
- Changed environment during flight at altitude allows Thrust Control Malfunction (TCM) detection
- STPA analysis identified
  - The inadequate operation of the air-ground switch
  - The TCM protection process output contributing the unsafe control action of inadvertent engine shutdown
  - Relative to the original design work STPA identified approximately 30 additional items that required review including several design changes
- Although a “novel” approach (STPA) applied techniques slightly different from the examples, the ability to explain the approach and understand the results drove consensus for the solutions
- Improved software now in customer's flight tests with no TCM functional issues. Aircraft level approval for both engines

STPA: The most popular approach you haven’t tried? [2019]

Countries:
Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Cyprus
Czech Republic
Denmark
England
Estonia
Finland
France
Germany
Greece
Hong Kong
Iceland
India
Ireland
Israel
Italy
Japan
Kenya
Korea
Kosovo
Kuwait
Malaysia
Mexico
Nepal
Netherlands
New Zealand
Nigeria
Norway
Pakistan
Poland
Portugal
Saudi Arabia
Scotland
Serbia
Singapore
South Korea
Spain
Sverige
Sweden
Switzerland
Taiwan
Thailand
Turkey
UK
United Arab
Emirates (UAE)
USA

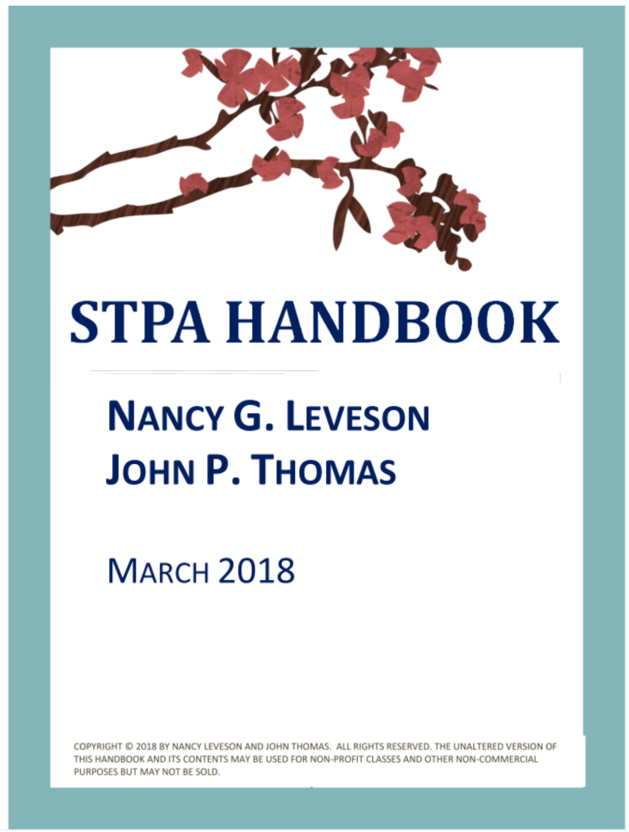
Industries:
Academia
Accelerator
Engineering
Accelerator-
based research
Accident
investigation
Aeronautics
Aerospace
Agriculture
Air Force
Air Traffic Control
Air
Transportation
Aircraft
Analytics and
Simulation
Automation
Automotive
Aviation
BioPharmaceutic
al
Chemical
Civil Engineering
Clinical Research
Cloud Computing
Collegiate Sports
Communication
Computer
Science
Computing
Construction
Consulting
Consumer Goods
Consumer
Products
Content Delivery
Network (CDN)
Critical
Infrastructure
Critical
Infrastructures
Cyber operations
Cybersecurity
Dam Safety
Decision Analysis
Defense
Disaster Risk
Management
Diving and
Hyperbarics
Education
Electric Power
Electrical &
Computer
Engineering
Elevator industry
Embedded
Software Testing
Energy
Engineering
Services
Enterprise
Software
Entertainment
Environmental
Ergonomics
Fertilizer
Manufacturing
FFRDC
Financial
Firefighting
Fitness
Food
Food processing
Gas
Government
Grid Energy
Storage
Ground Combat
Systems (Live
Fire)
Healthcare
Higher Education
Home Appliances
Hospitals
Human Factors
Hydropower
Industrial
Industrial
Automation
Industrial Control
Industrial
equipment
Information
security
Information
Technology (IT)
Infrastructure
Insurance
Internet
Internet of Things
(IoT)
IV&V
Labor
Labor
Organization
Labor Unions
Life sciences R&D
Logistics
Logistics and
Aviation
Manufacturing
Manufacturing
Process
Automation
Maritime
Medical
Medical Devices
Medicine
Metals
Military
Military
Acquisition
Military Aviation
Military Defense
Mining
National Security
Natural disasters
Naval
News
Non-profit R&D
Nuclear
Nuclear Energy
Nuclear
enginering
Nuclear Power
Nuclear Utility
Nuclear Weapon
Surety
Oil
Oil & gas
Open Standards
Open Systems
Oversight
Particle
Accelerators
Patient Safety
Petrochemical
Petroleum
Pipelines
Pharmaceutical
(clinical)
Pharmaceuticals
Power
PRA consultants
Private
Investigations
Process
Process industry
Processing
Public Sector
R&D
Rail Traffic
Control and
Safety
Railroads
Real estate
Refining
Regs
Research
Road Traffic
Management
Road transport
Robotics
Rotating
Equipment
Safety
Safety Assurance
Safety Consulting
Safety
engineering
Safety
Management
Satellite Operator
Security
Sediment
Management
Semiconductor
Ship Design
Shipbuidling
Shipping
Software
Space
Steel
Structural
engineering
Supply Chain
Management
Surface
Transportation
System
Engineering
System Safety
Systems
Engineering
Telecoms
Test and eval
Think tank
Trade Association
Traffic Control
and Safety
Training
Transportation
Turnaround &
Innovation
Consulting
University
Videographer
Web
development
Web provider
Web standards

STPA Common Mistakes

- Not adequately educated in STPA
  - A short tutorial is not enough!
  - Formal education is needed.
- Implementing STPA without an expert STPA facilitator
  - Example mistake: We already have a facilitator with decades of experience facilitating fault tree analysis. Just give us a couple days to “bring him up to speed on the STPA methodology”.
  - Lessons from HAZOP and PRA:
    - The expert facilitator role requires years of experience, not days/months.
    - “only 1/3 of people who are otherwise qualified by education, experience, etc. actually make good HAZOP leaders”
- Limiting STPA to a simple system or simple problem with obvious answers
- “It’s not rigorous enough” (a beginner)
- “It’s too rigorous” (also a beginner)

For more information

- Google: “STPA Handbook”
  - How-to guide for practitioners applying STPA
  - Free PDF download from MIT (see website below)
  - Same book used in our professional/industry STPA training classes
- Website: mit.edu/psas
- Questions? Email me! JThomas4@mit.edu



STPA HANDBOOK

NANCY G. LEVESON
JOHN P. THOMAS

MARCH 2018