Massachusetts Institute of Technology

System-Theoretic Process Analysis (STPA)

Primer and Mini-Tutorial

Dr. John Thomas
Director, Engineering Systems Lab
MIT

Any questions? Email me! JThomas4@mit.edu

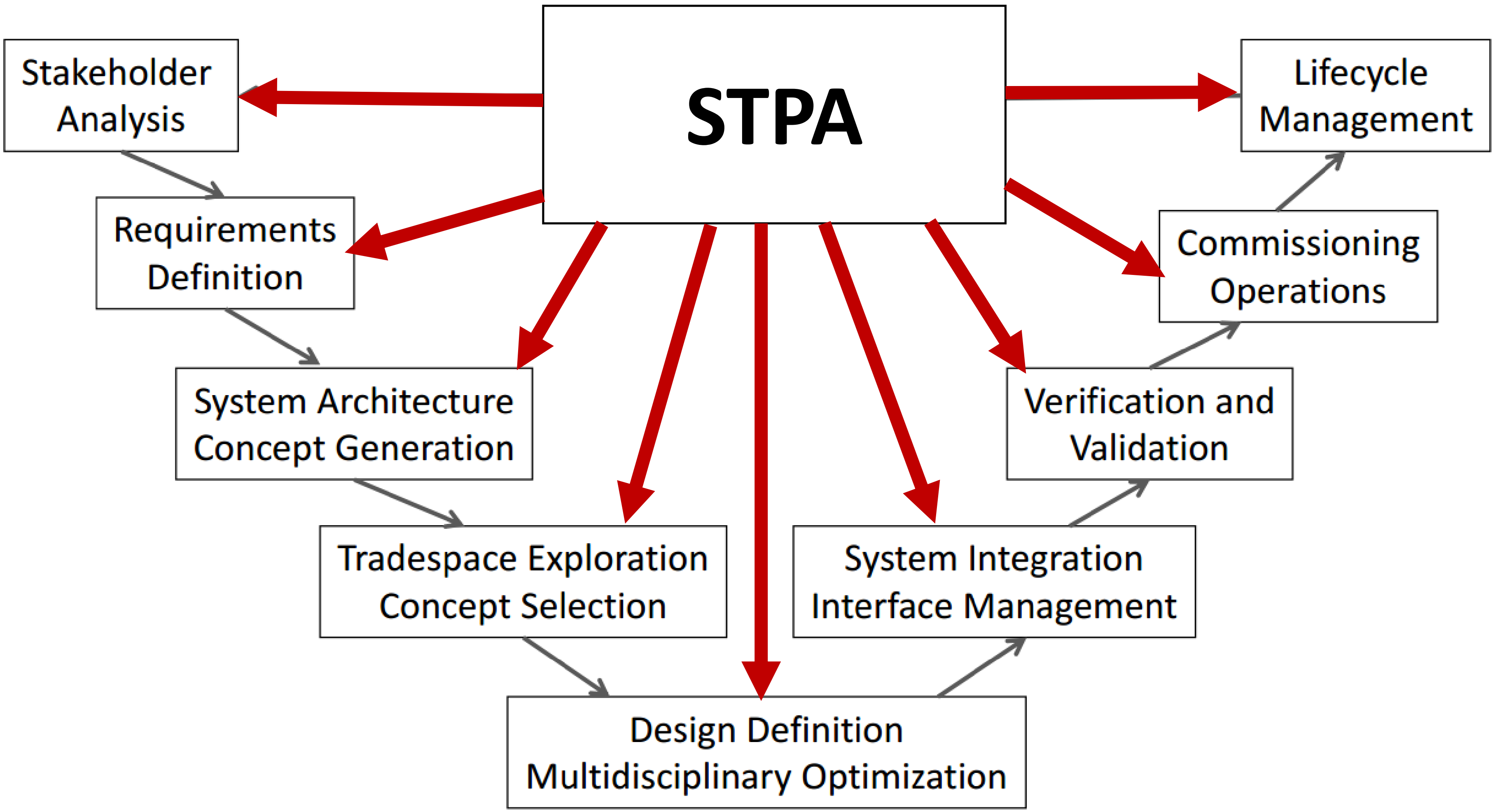
System-Theoretic Process Analysis (STPA)

STPA can support all phases of Systems Engineering

STPA is used to anticipate and prevent hazards caused by:
- Software, computers, and automation
- Human operator error/confusion
- Unexpected interactions between systems and functions
- System design errors
- Flawed assumptions
- Missing or incorrect requirements

The famous “V-Model” of Systems Engineering

16.842 Fundamentals of Systems Engineering



Many opportunities to address safety throughout!

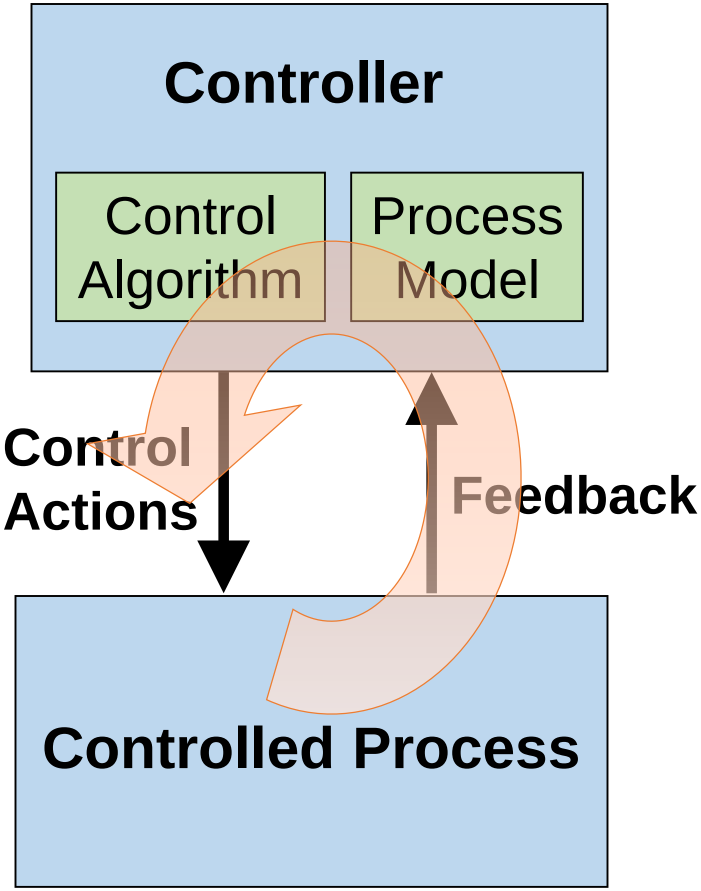
Bombardier crash

- Bombardier Learjet 60 Accident
  - September 19, 2008
  - Columbia Metropolitan Airport, South Carolina
- Aircraft was destroyed during rejected takeoff
- Computer ignored pilot commands for reverse thrusters
  - The tire explosion damaged landing gear sensors
  - Computer believed aircraft in flight
  - Computer <u>increased thrust</u> instead
- Aircraft destroyed

The control system operated exactly as designed!

This accident is complex, many factors! See report for more info.

Basic control loop



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

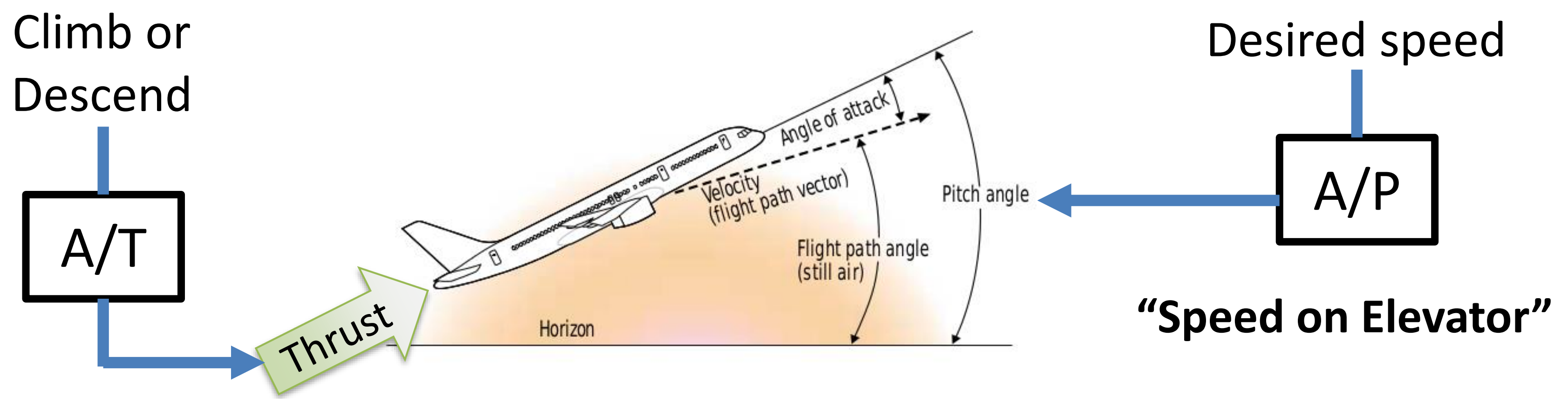
Asiana 214 crash: B777

- Aircraft begins to overshoot glideslope on descent
- PF disconnects A/P, moves thrust levers to idle
- A/T automatically switches to HOLD mode
- PF calls out for F/Ds off (SOP). PM replies “okay”.
- 500ft altitude: aircraft reaches desired glideslope path and speed
- Aircraft crosses below glideslope. PF pitches up to slow descent. A/T does not “wake-up” to increase throttle—throttle stays at idle.
- With aircraft below glideslope, crew initiates go-around. Aircraft collides with sea wall.

Thomas and Malmquist, 2018

This accident is complex, oversimplified here! See paper for more analysis.

Autopilot (A/P) and Autothrottle (A/T) Pairing



A/T will remain in HOLD mode until one of the following conditions is met:

- The airplane reaches the MCP target altitude
- The pilot engages a new AFDS pitch mode or new A/T mode
- The A/T arm switches are turned off
- The thrust is manually commanded to increase past the thrust limit
- The A/P is disconnected, and both F/D switches are turned off

Asiana 214 crash: B777

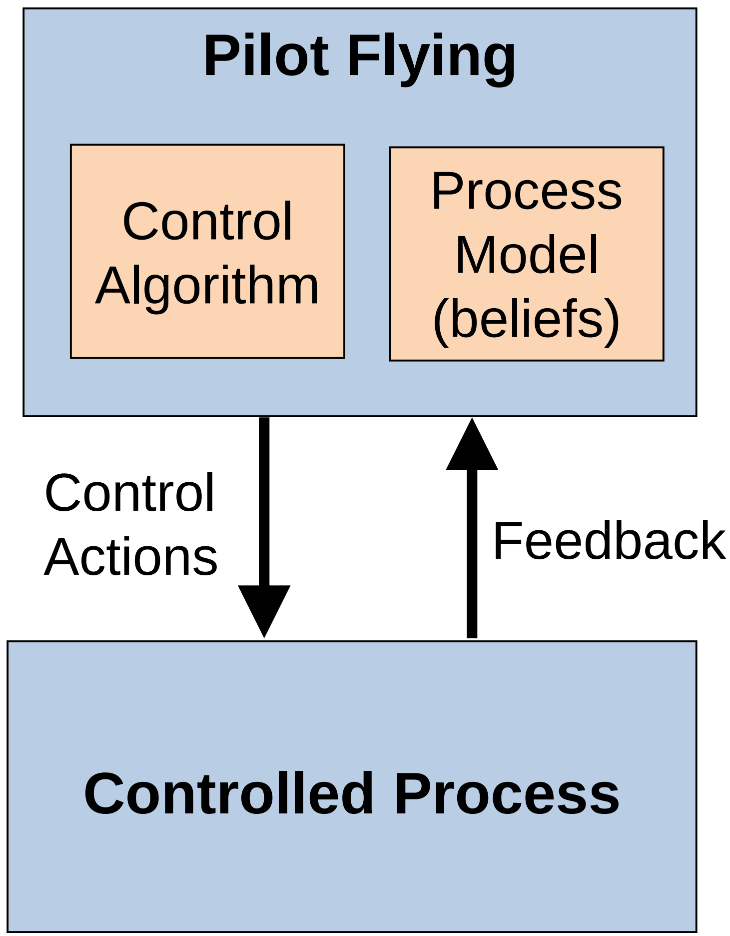
- Aircraft begins to overshoot glideslope on descent
- PF disconnects A/P, moves thrust levers to idle
- A/T automatically switches to HOLD mode
- PF calls out for F/Ds off (SOP). PM replies "okay".
- 500ft altitude: aircraft reaches desired glideslope path and speed
- Aircraft crosses below glideslope. PF pitches up to slow descent. A/T does not "wake-up" to increase throttle—throttle stays at idle.
- With aircraft below glideslope, crew initiates go-around. Aircraft collides with sea wall.

But PM F/D was not turned off!

Thomas and Malmquist, 2018

This accident is complex, oversimplified here! See paper for more analysis.

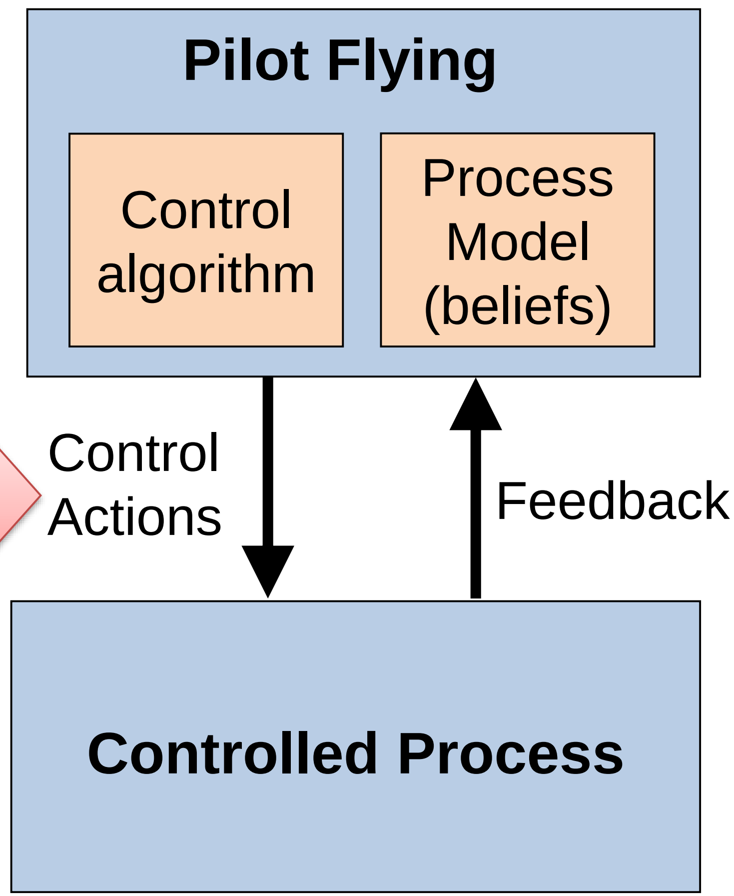
Basic Control Loop



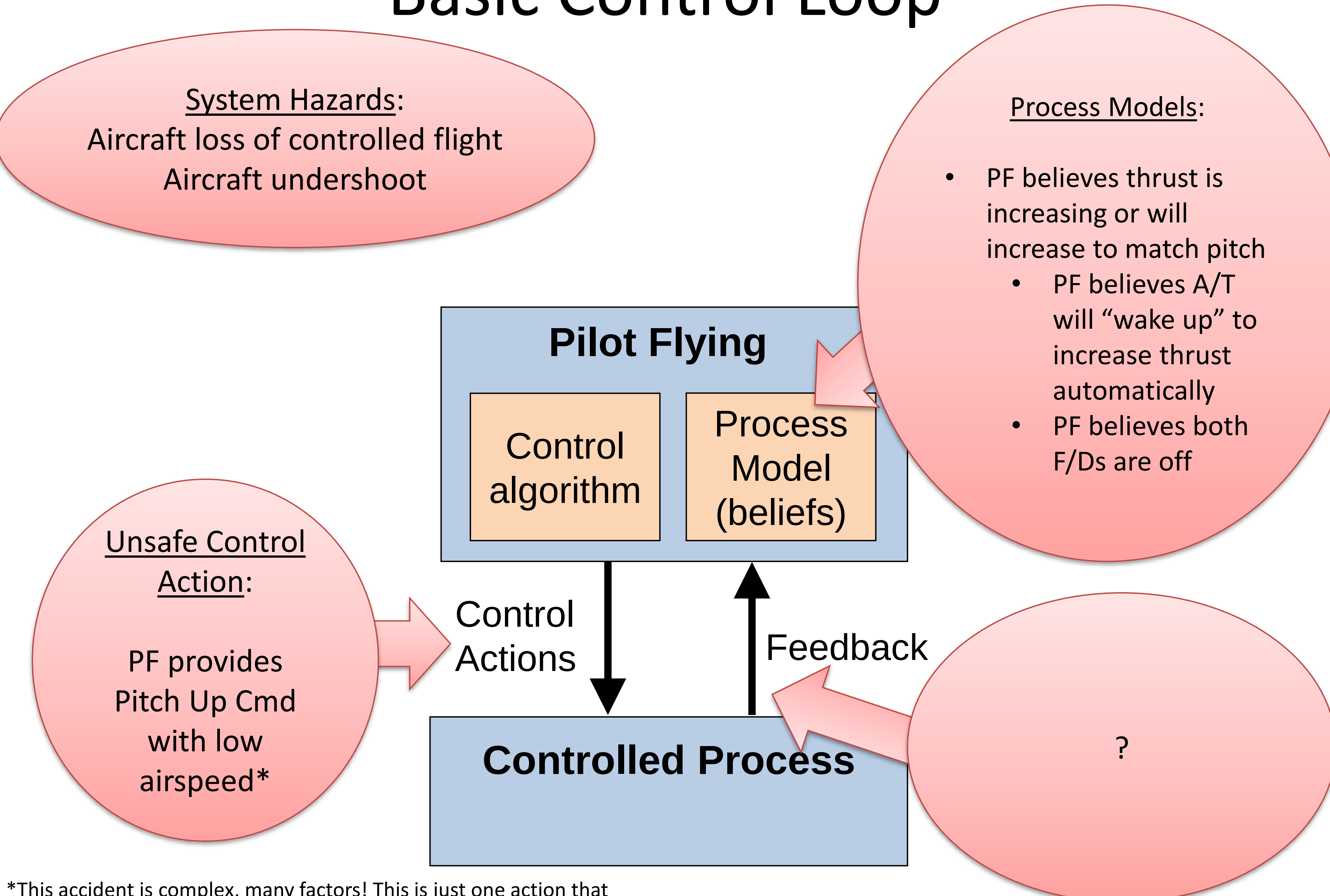
Basic Control Loop

<u>System Hazards</u>:
Aircraft loss of controlled flight
Aircraft undershoot

<u>Control Actions</u>
- Pitch up/down
- Throttle
- Roll
- Etc.

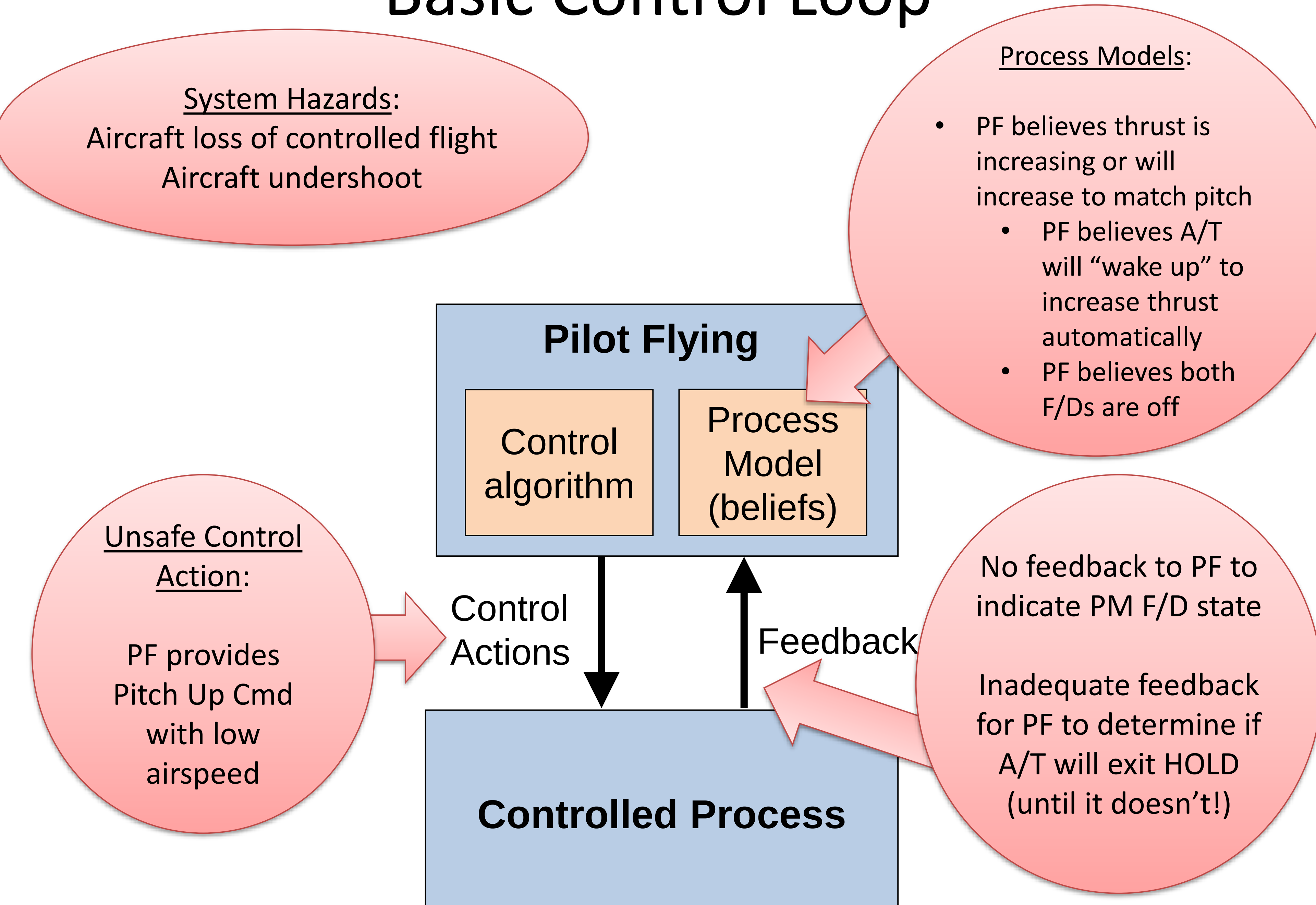


Basic Control Loop



*This accident is complex, many factors! This is just one action that happened in final seconds before crash. See paper for more analysis.

Basic Control Loop



Challenge: Complexity!

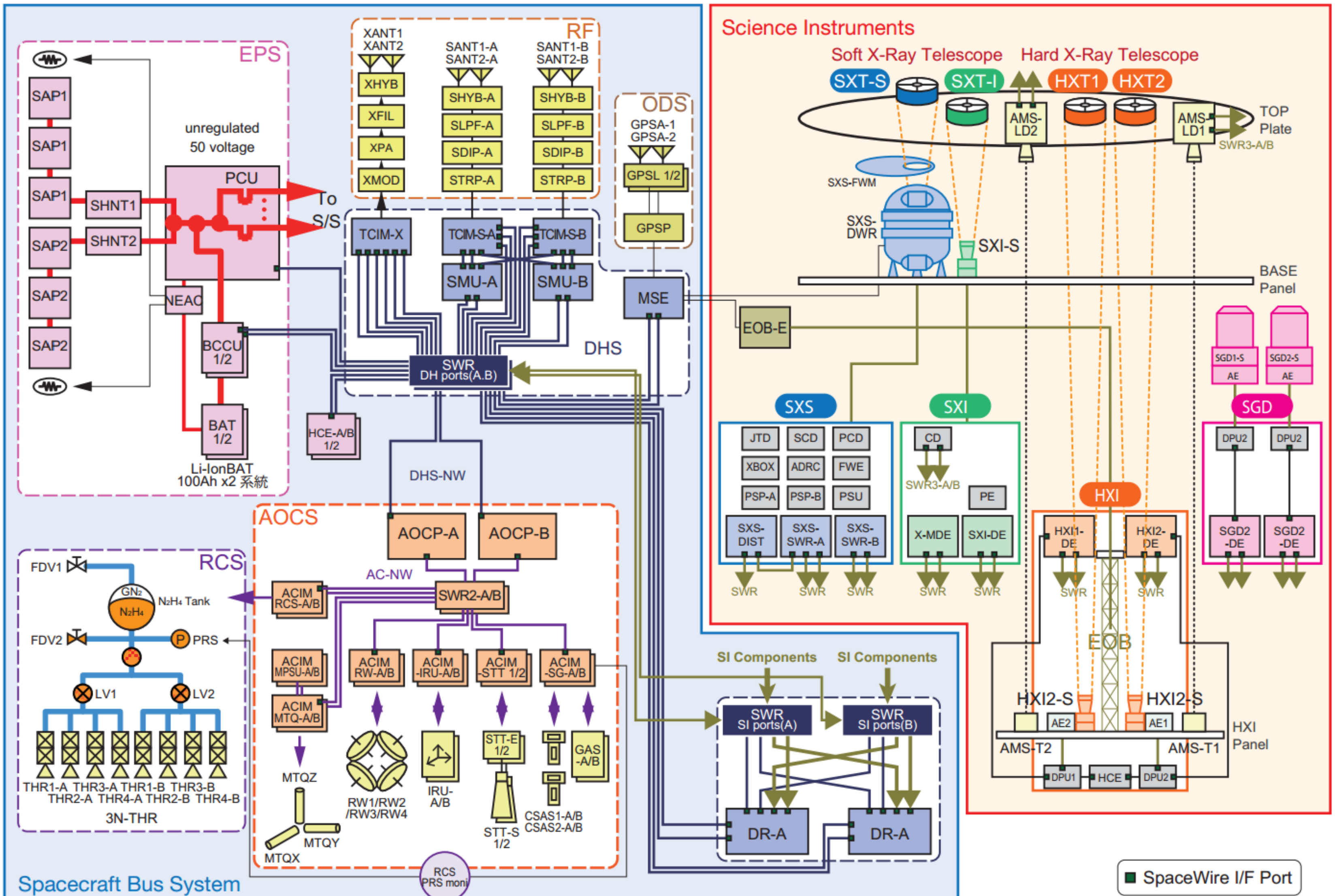


Figure 3.9: System block diagram. A is the primary and B is the redundant system.

Brute force approach

Need better ways to manage complexity!

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

How to manage complexity?

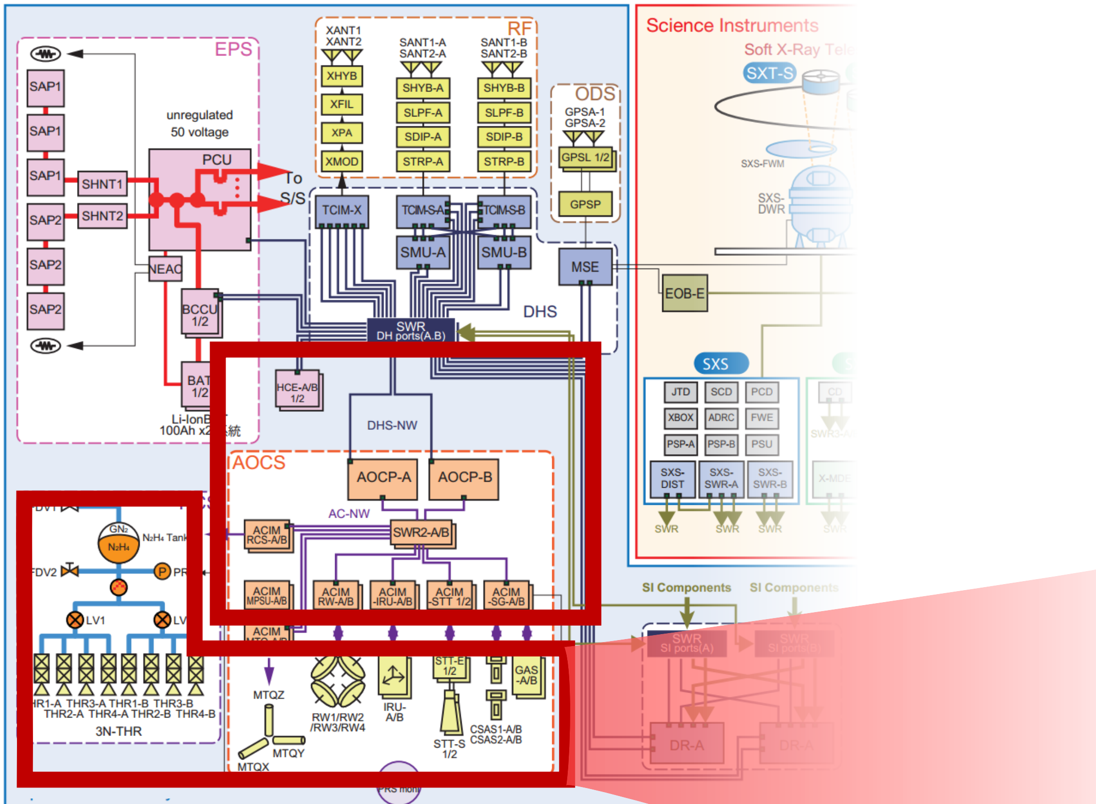
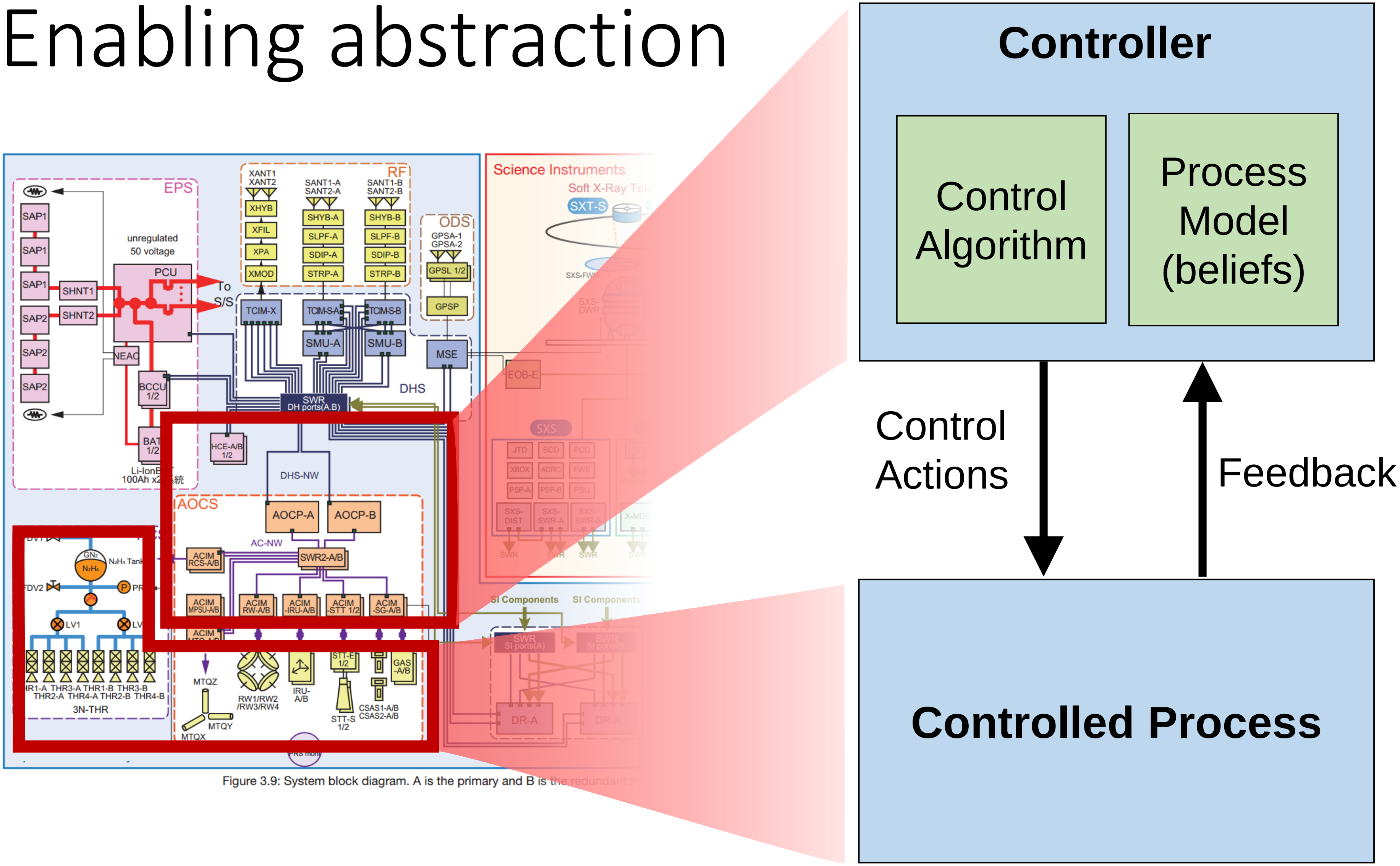


Figure 3.9: System block diagram. A is the primary and B is the redundant sy

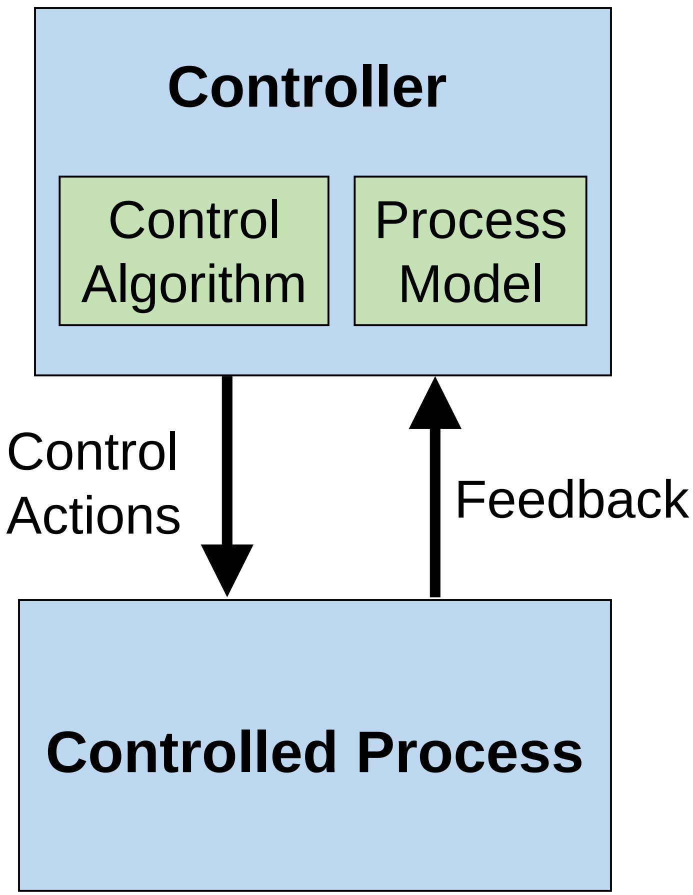
Controlled Process

Thomas, 2017

Enabling abstraction

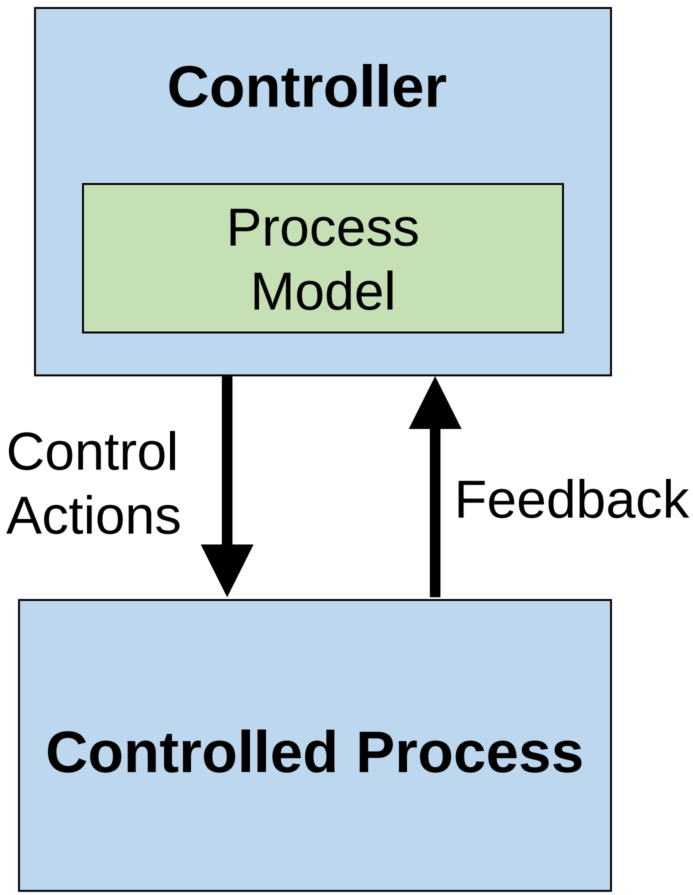


Basic control loop



- **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

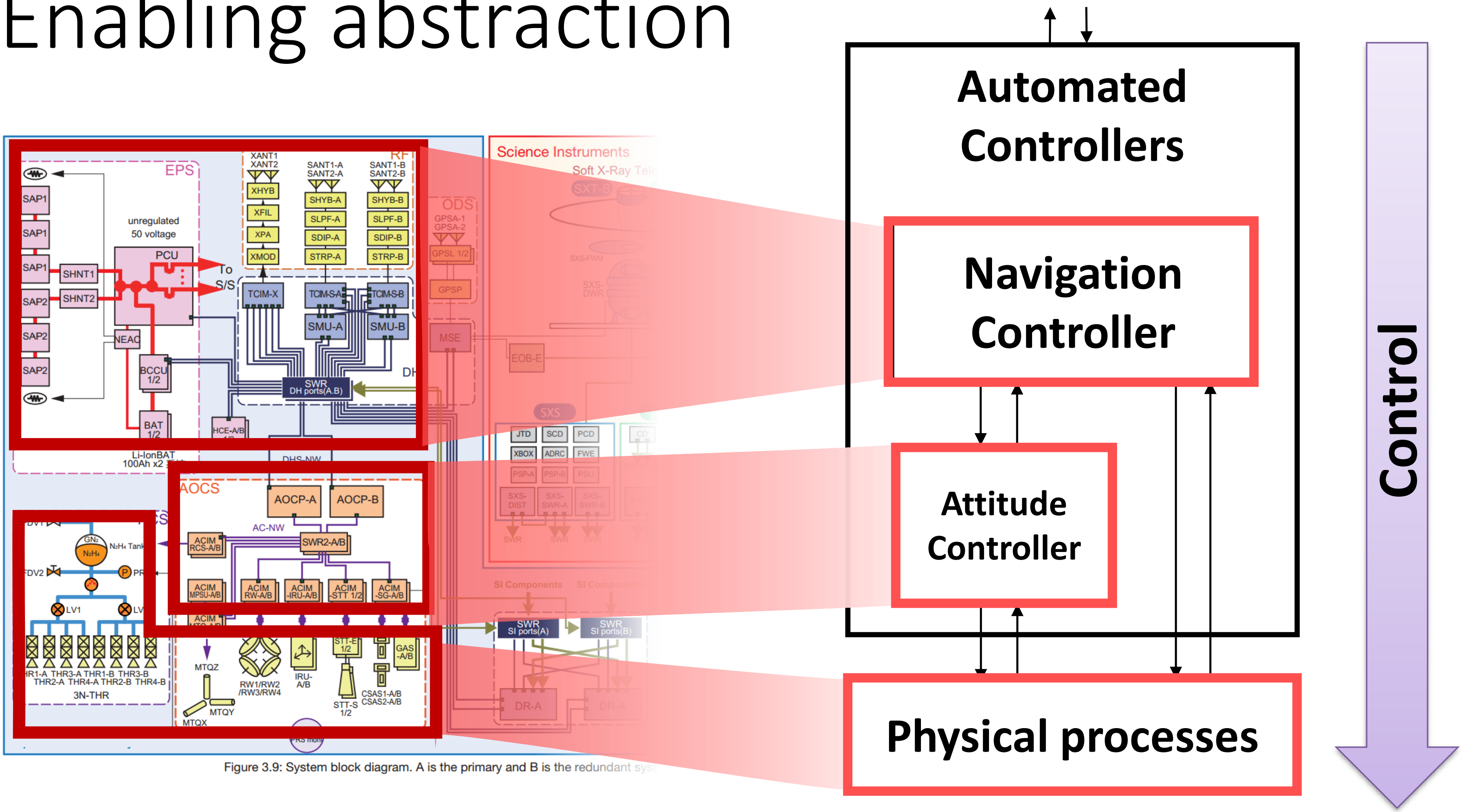
Controller Process Model



- Controllers use a **<u>process model</u>** to determine control actions
- Process model contains:
  - Current system state
  - Ways the process can change state
  - Required relationship among system variables
- Process model is updated through various forms of feedback

(Leveson, 2012)

Enabling abstraction



Thomas, 2017

Enabling abstraction

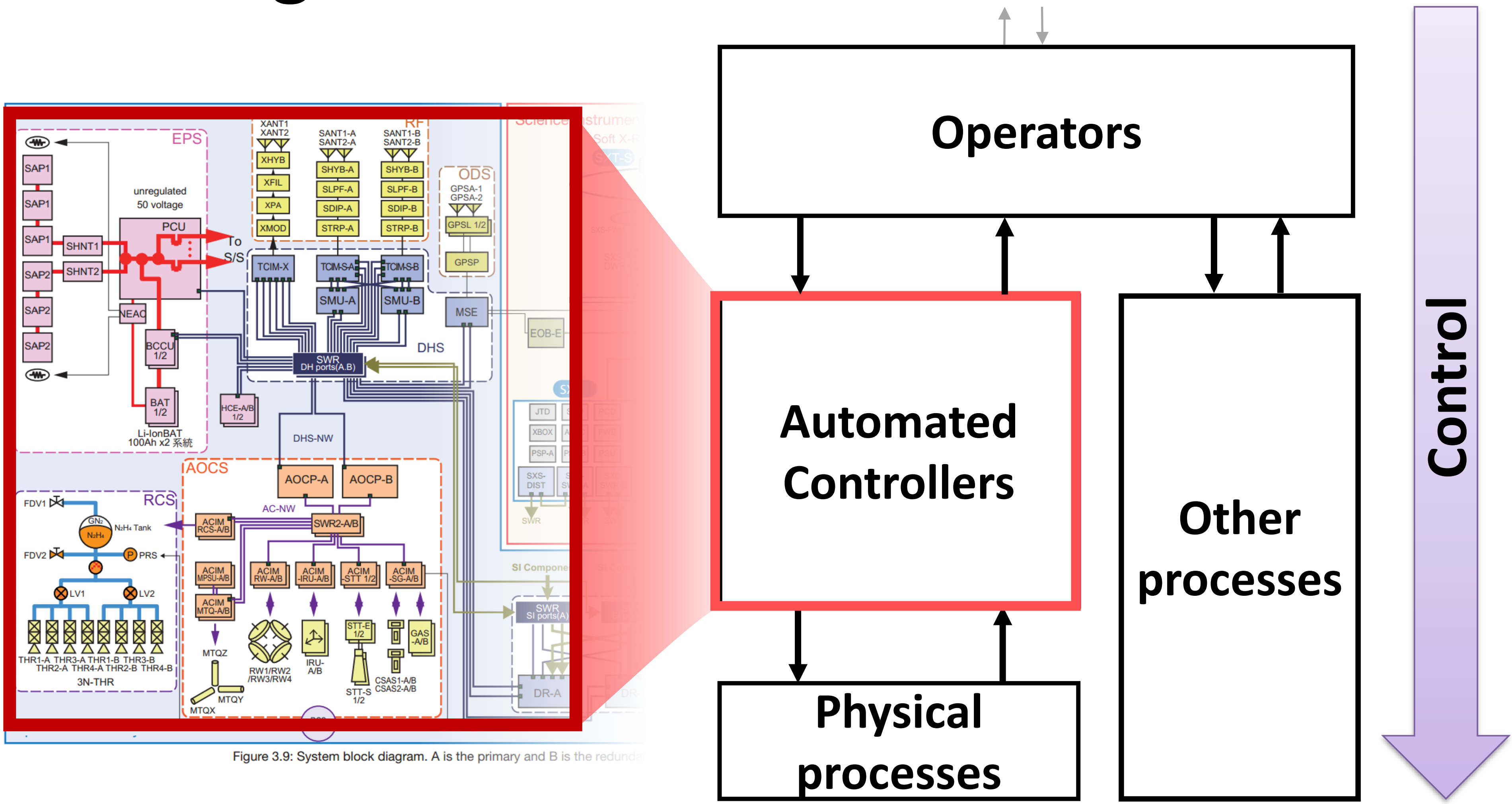


Figure 3.9: System block diagram. A is the primary and B is the redund

Thomas, 2017

Enabling abstraction

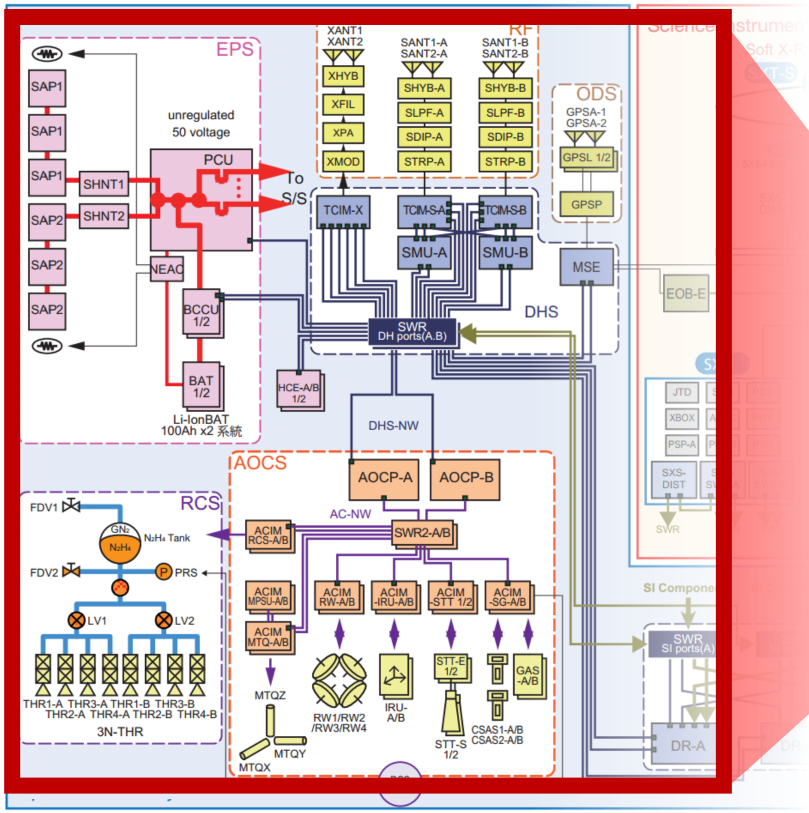
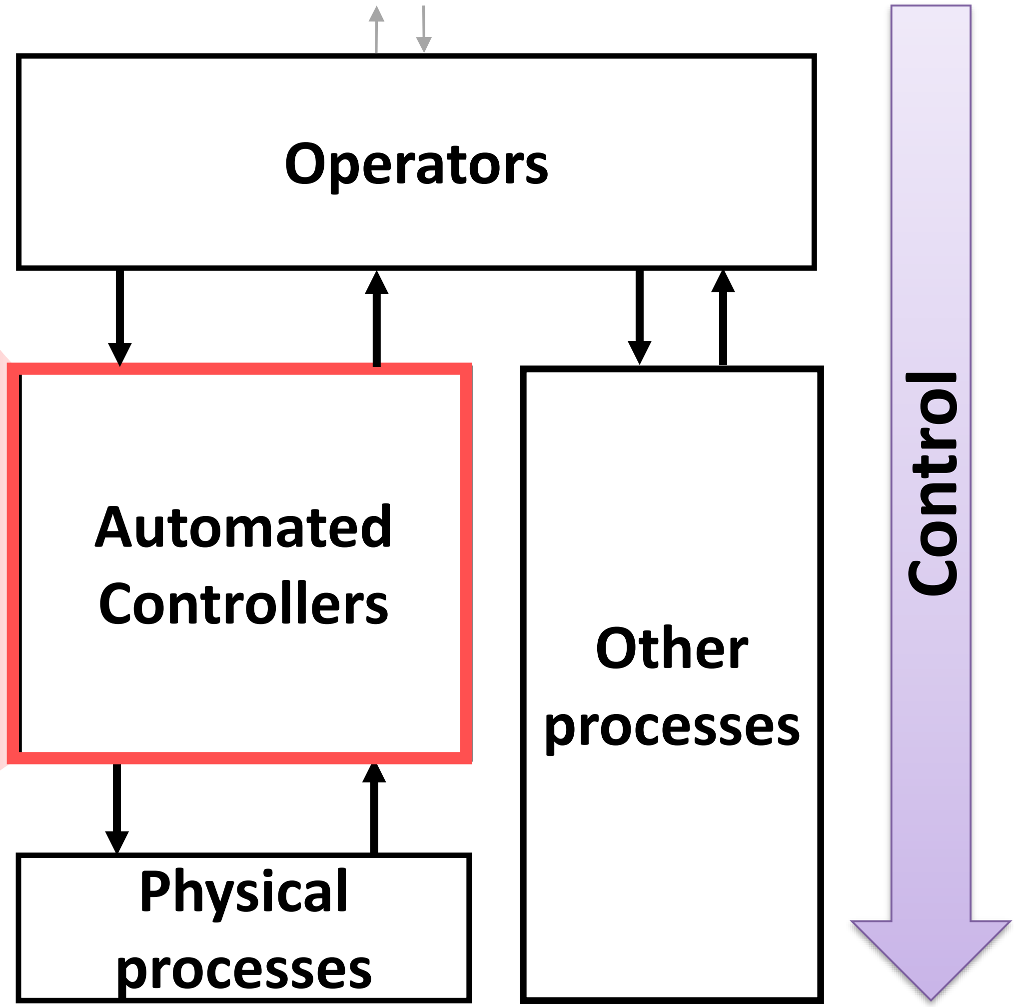


Figure 3.9: System block diagram. A is the primary and B is the redund

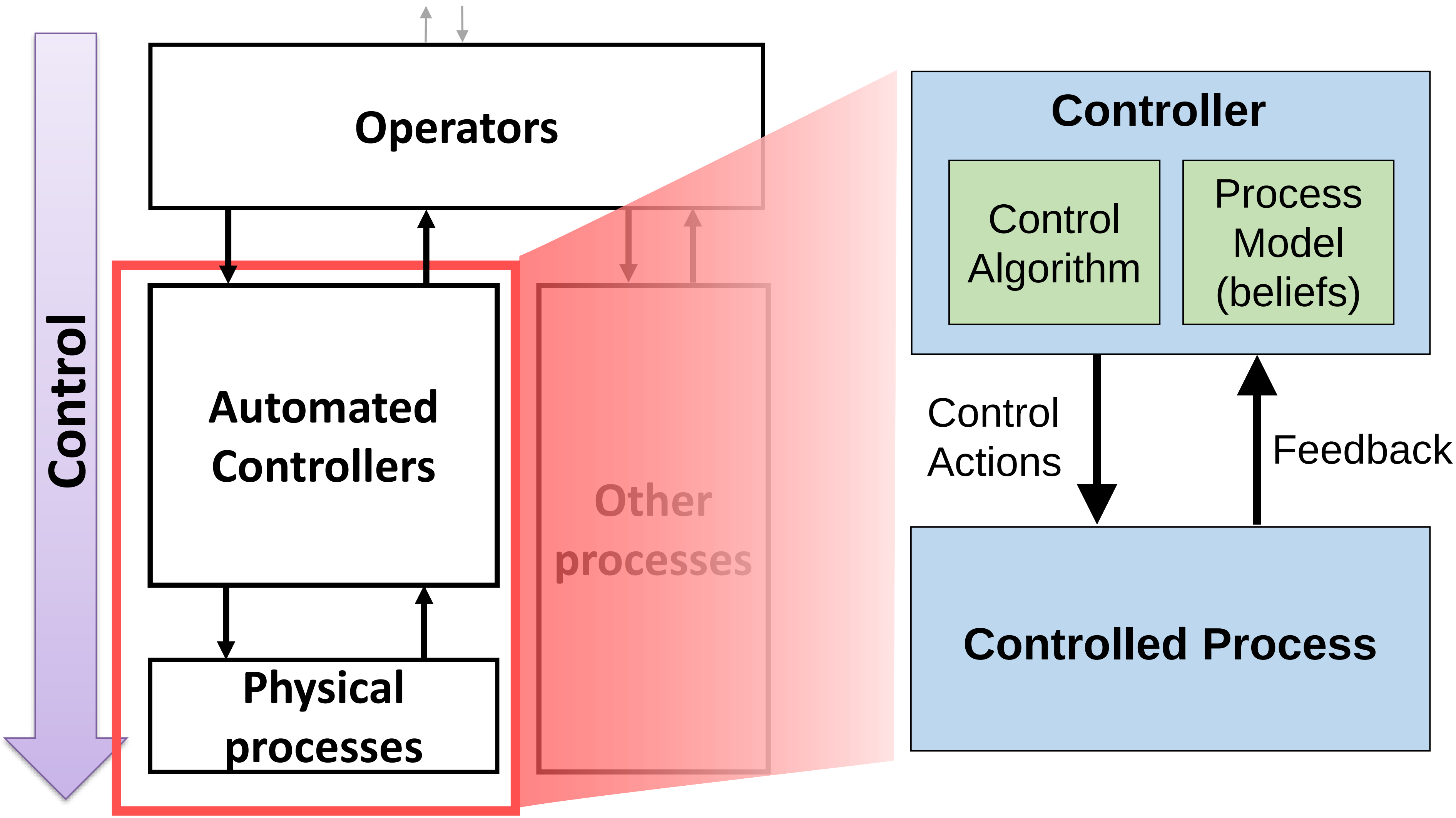


Component view

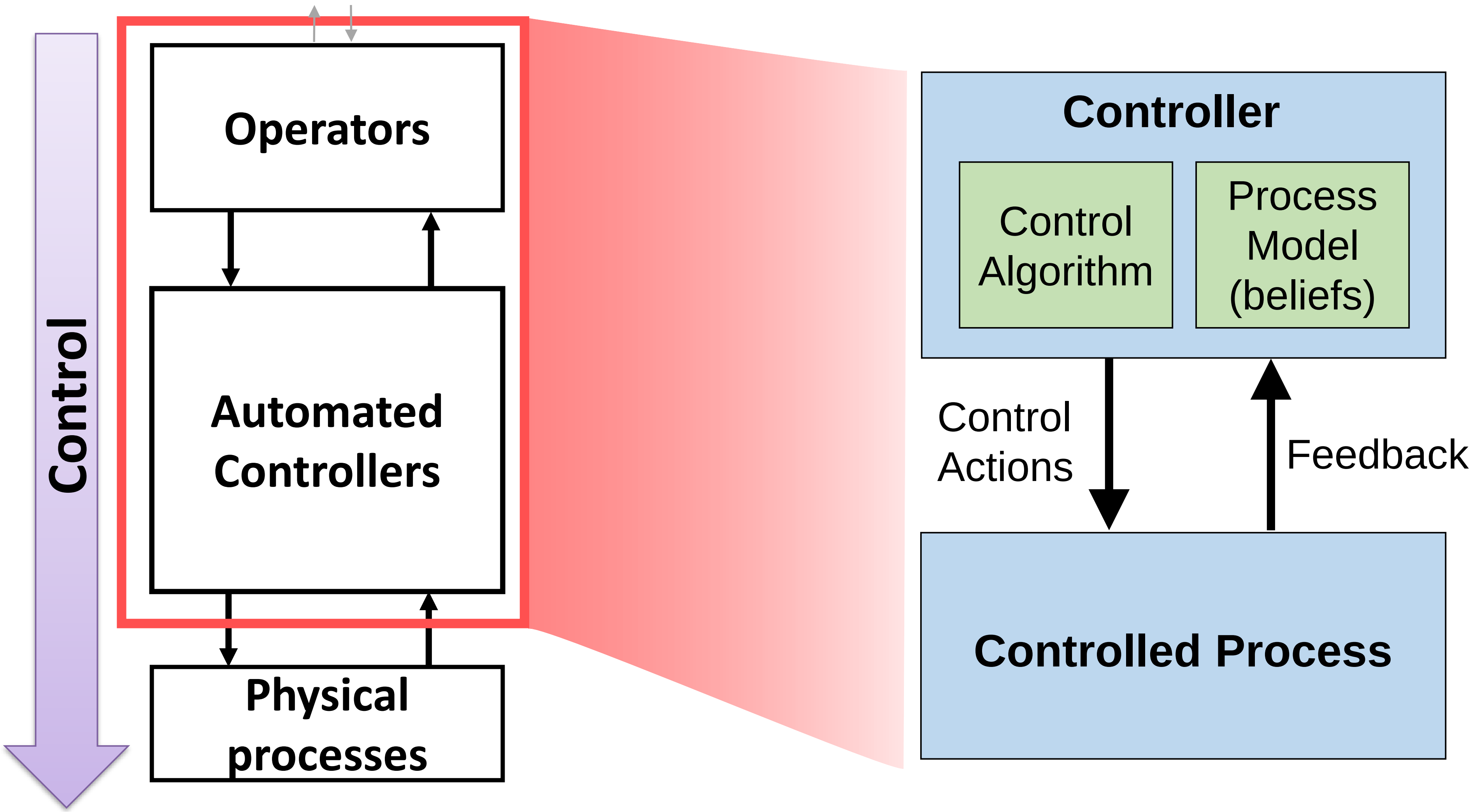
Systems view

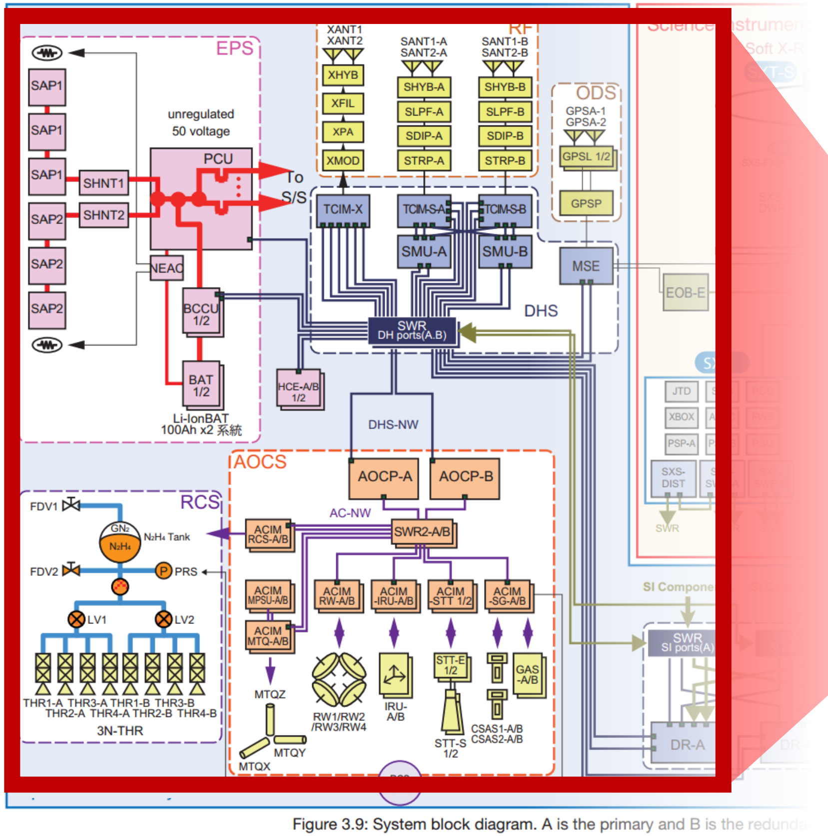
Thomas, 2017

Basic Control Structure

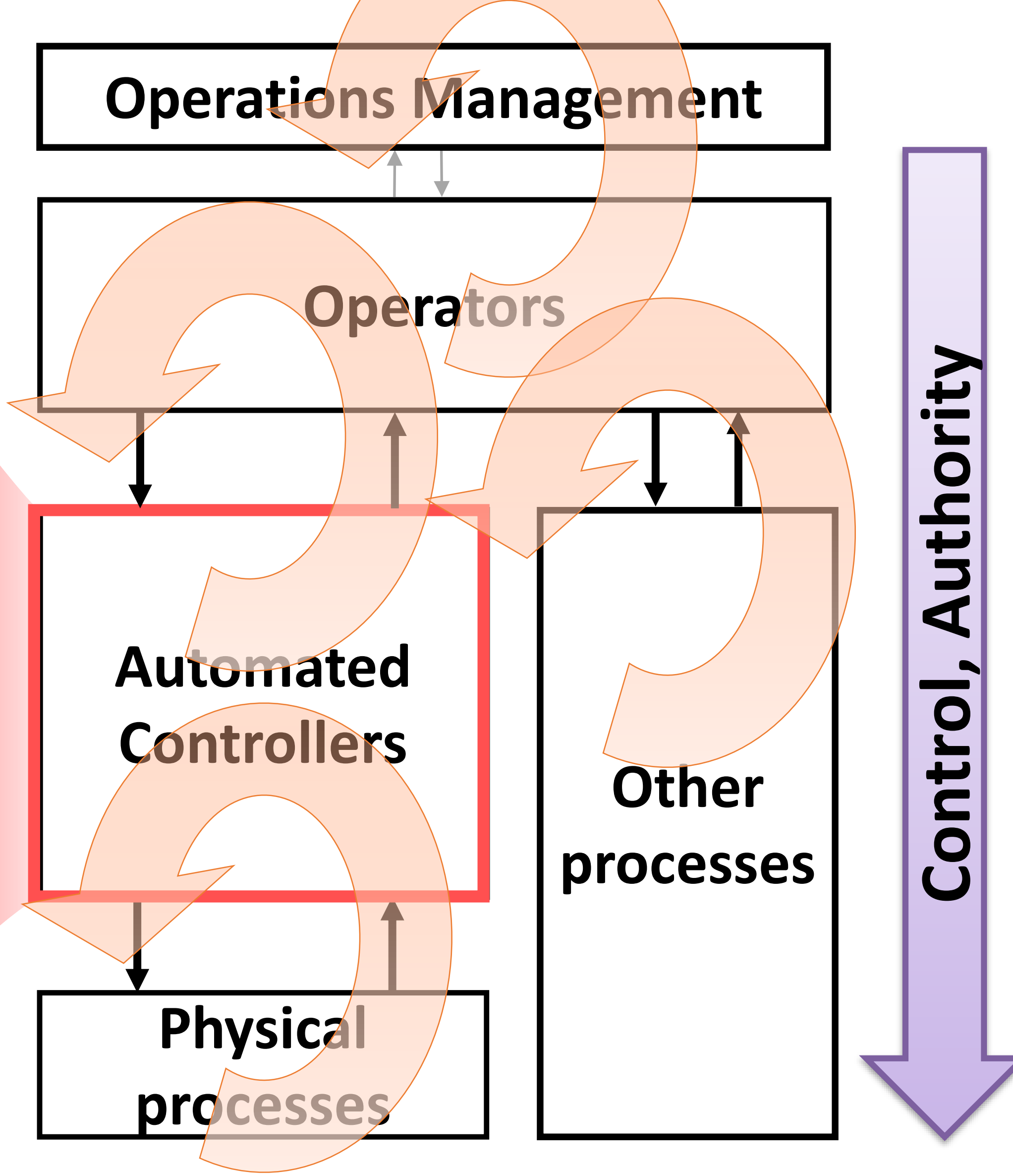


Basic Control Structure



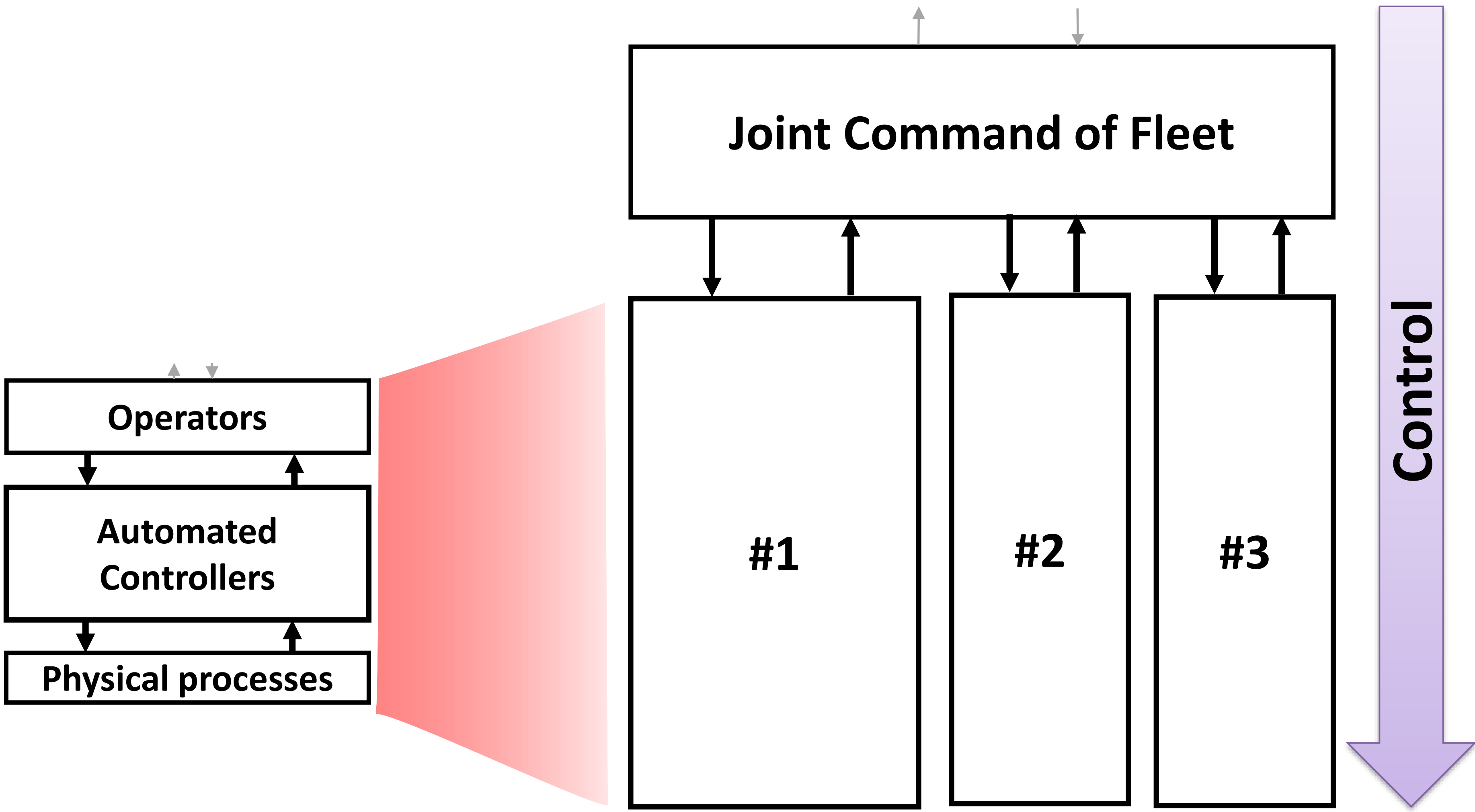


Component view



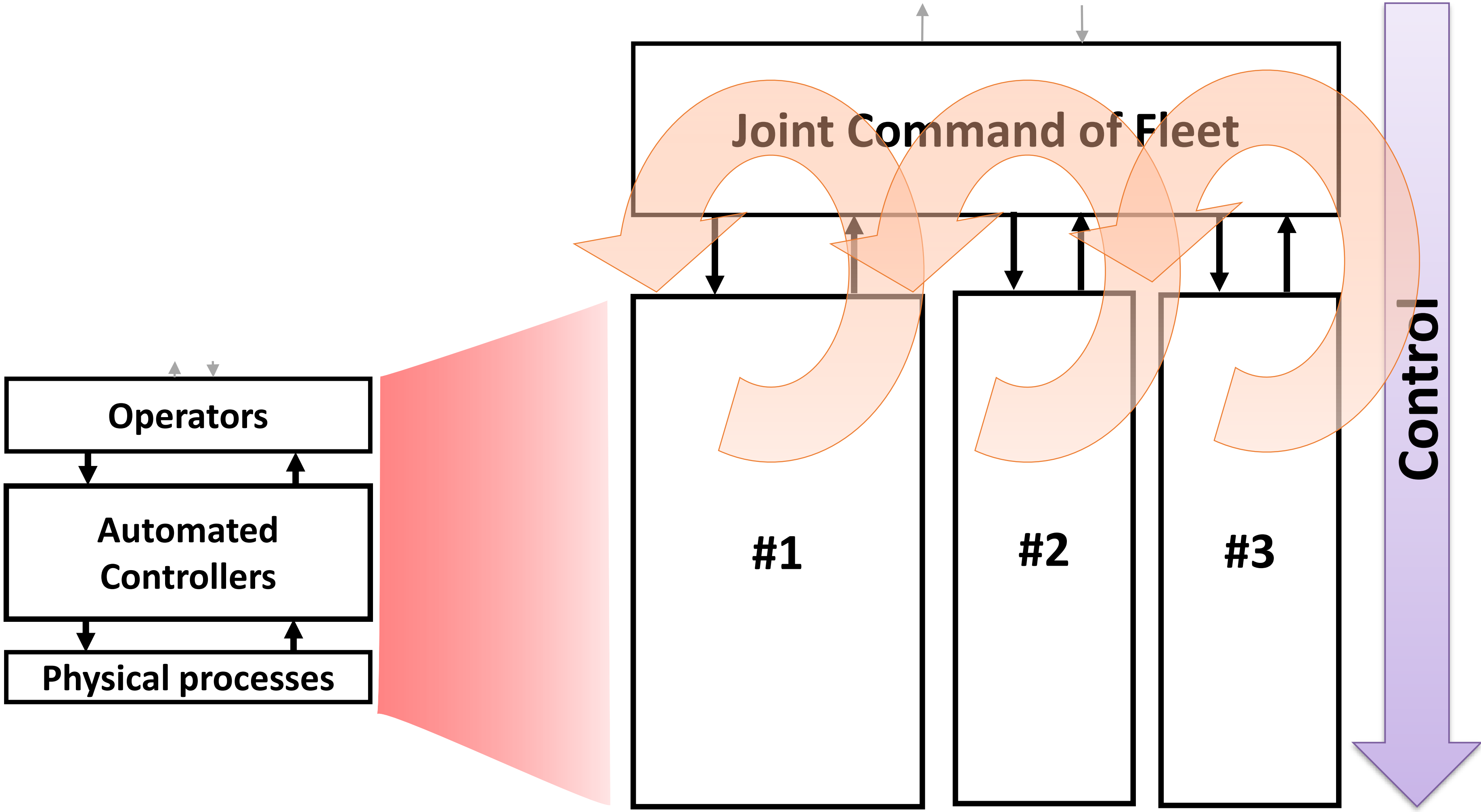
Systems view

Enabling abstraction



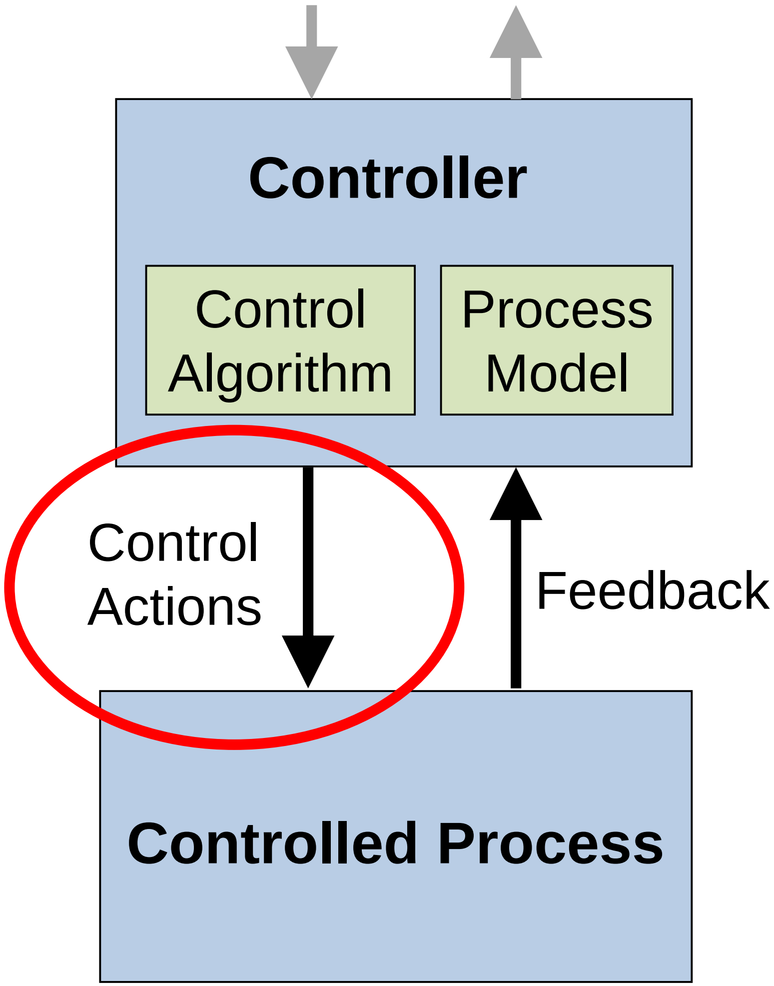
Thomas, 2018

Enabling abstraction



Thomas, 2018

Unsafe Control Actions

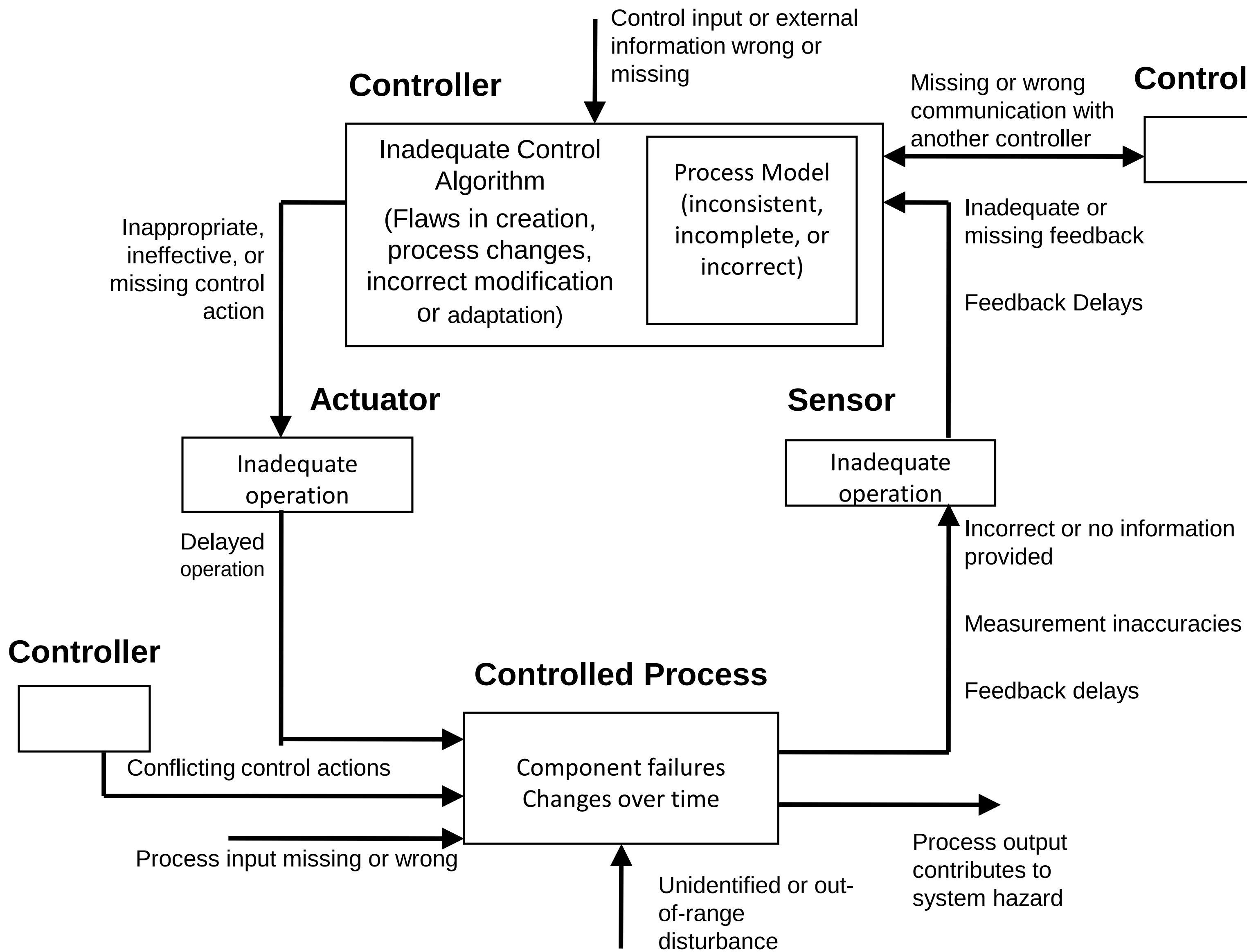


Four types of **unsafe control actions**:

1) Control actions required for safety are not given
2) Unsafe ones are given
3) Potentially safe control actions but given too early, too late
4) Control action stops too soon or applied too long

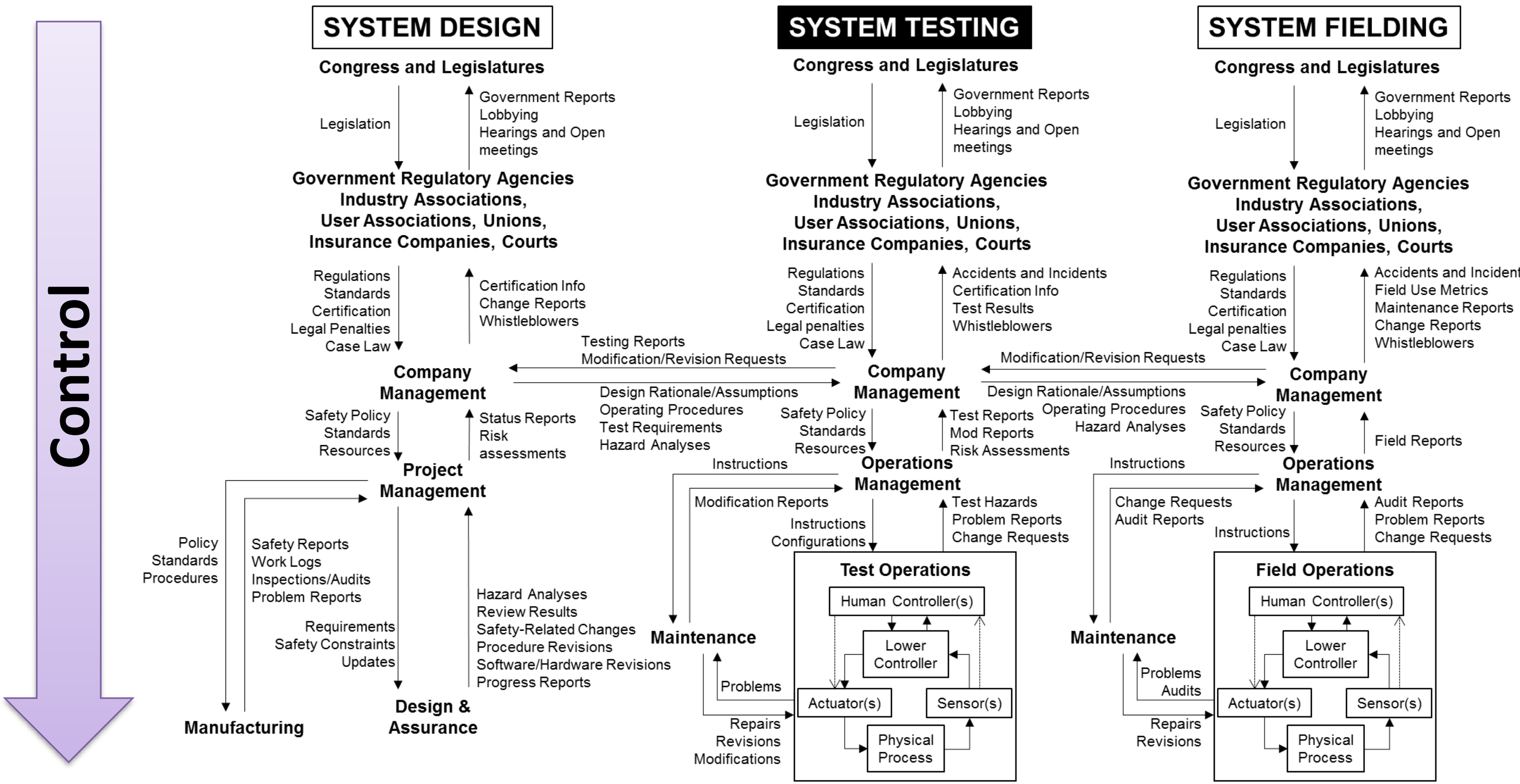
(Leveson and Thomas, 2018)

Some Factors in Causal Scenarios



(Leveson, 2012)

Example Generic Control Structure with System Testing



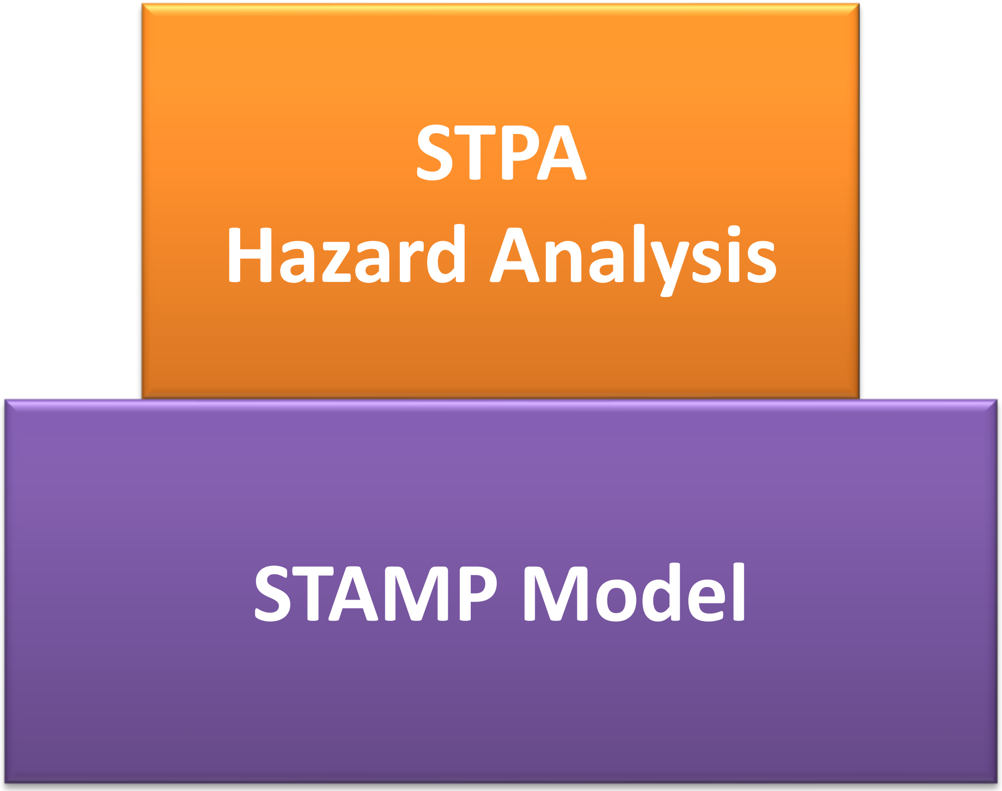
STAMP and STPA

STAMP Model

Losses are caused by inadequate control

(Leveson and Thomas, 2018)

STAMP and STPA

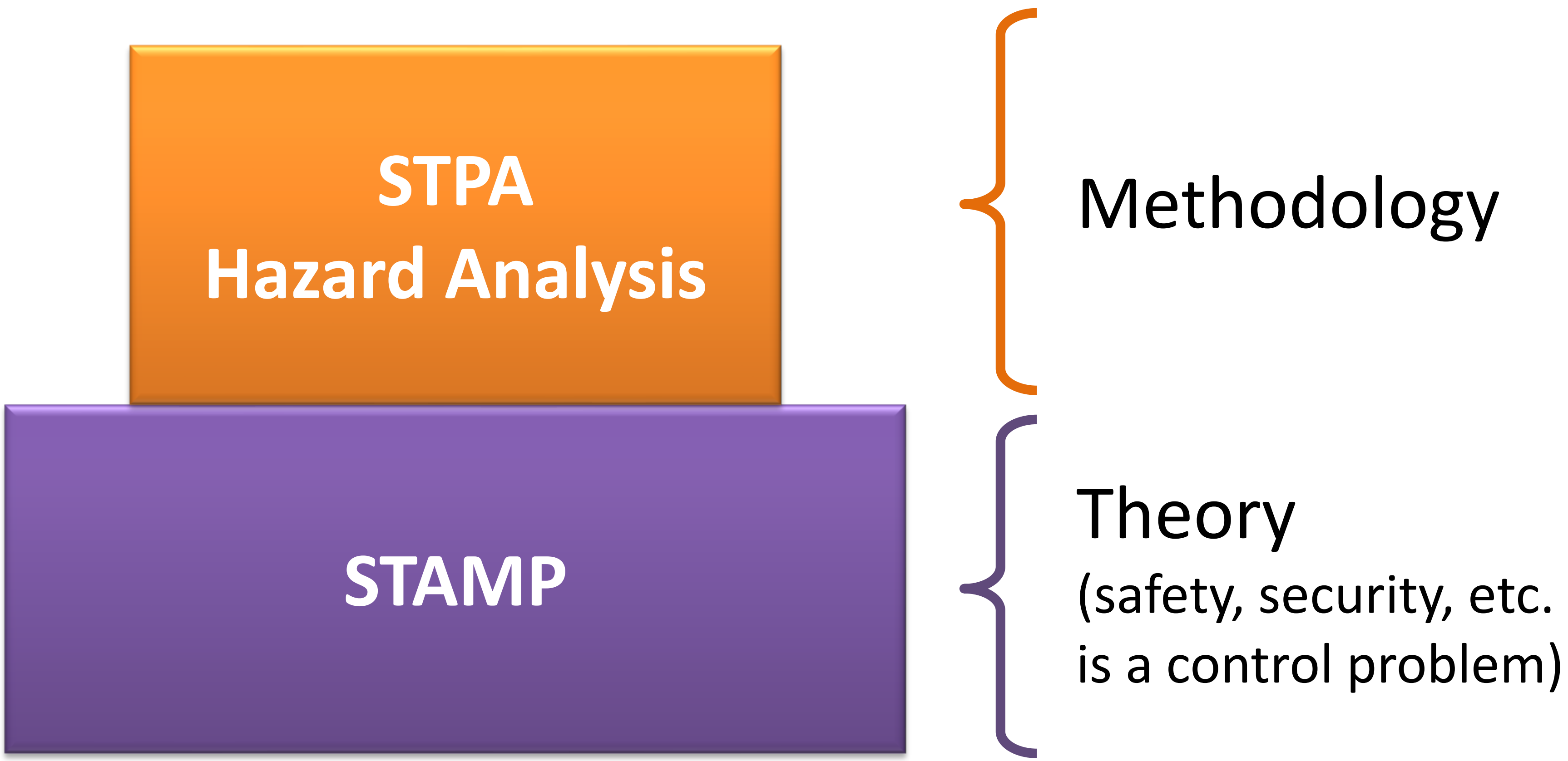


How do we anticipate & prevent inadequate control?

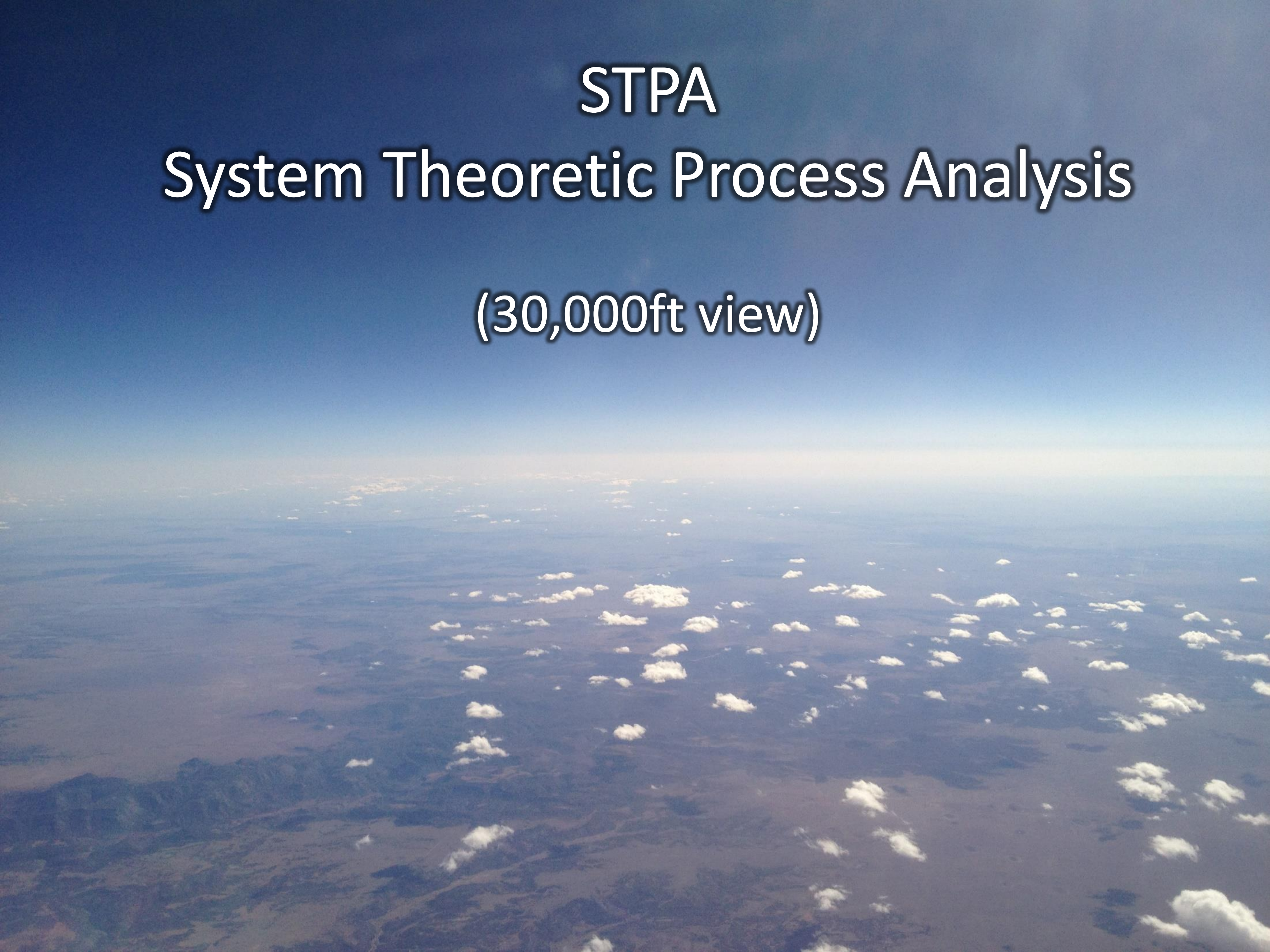
Losses are caused by inadequate control

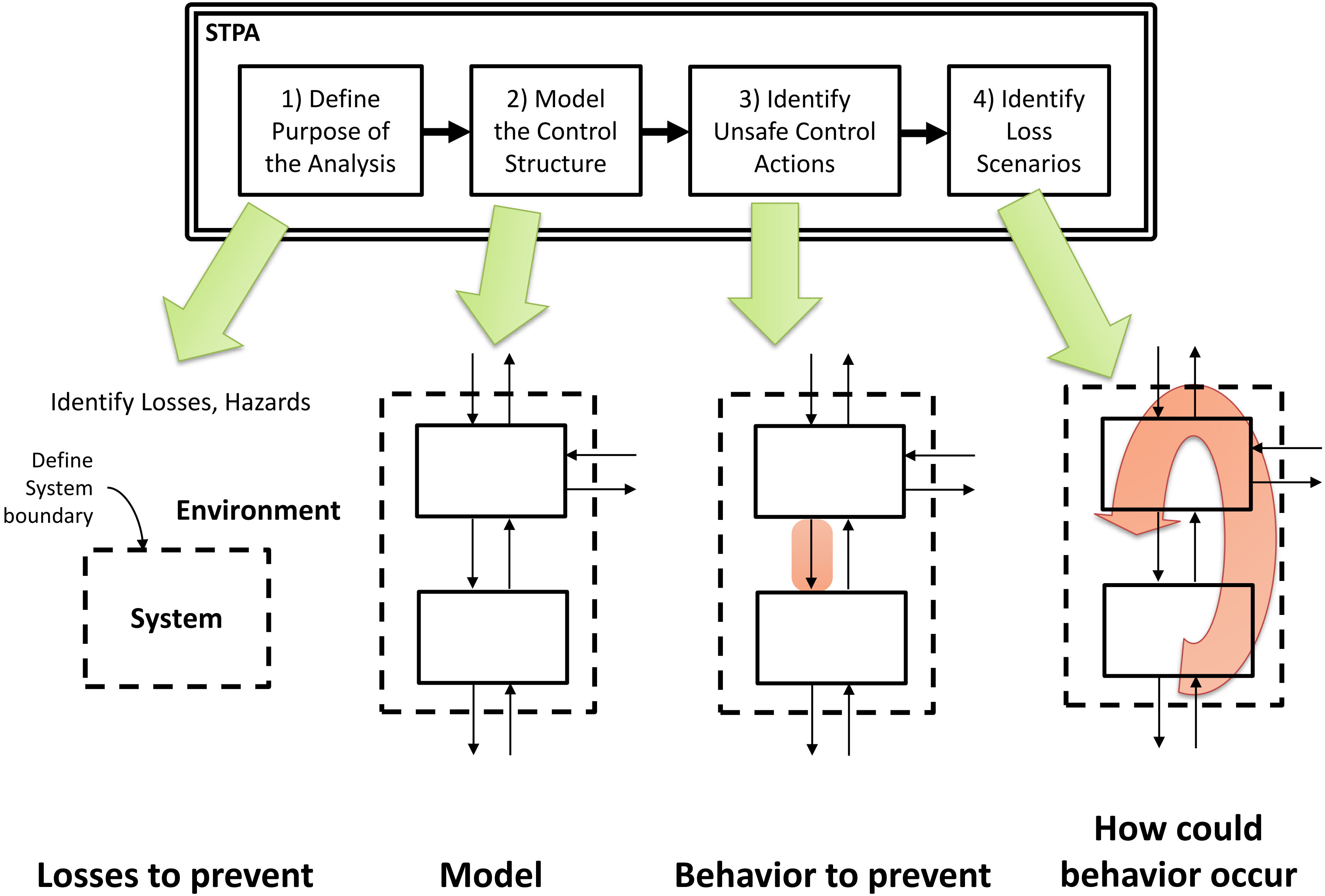
(Leveson and Thomas, 2018)

STAMP and STPA



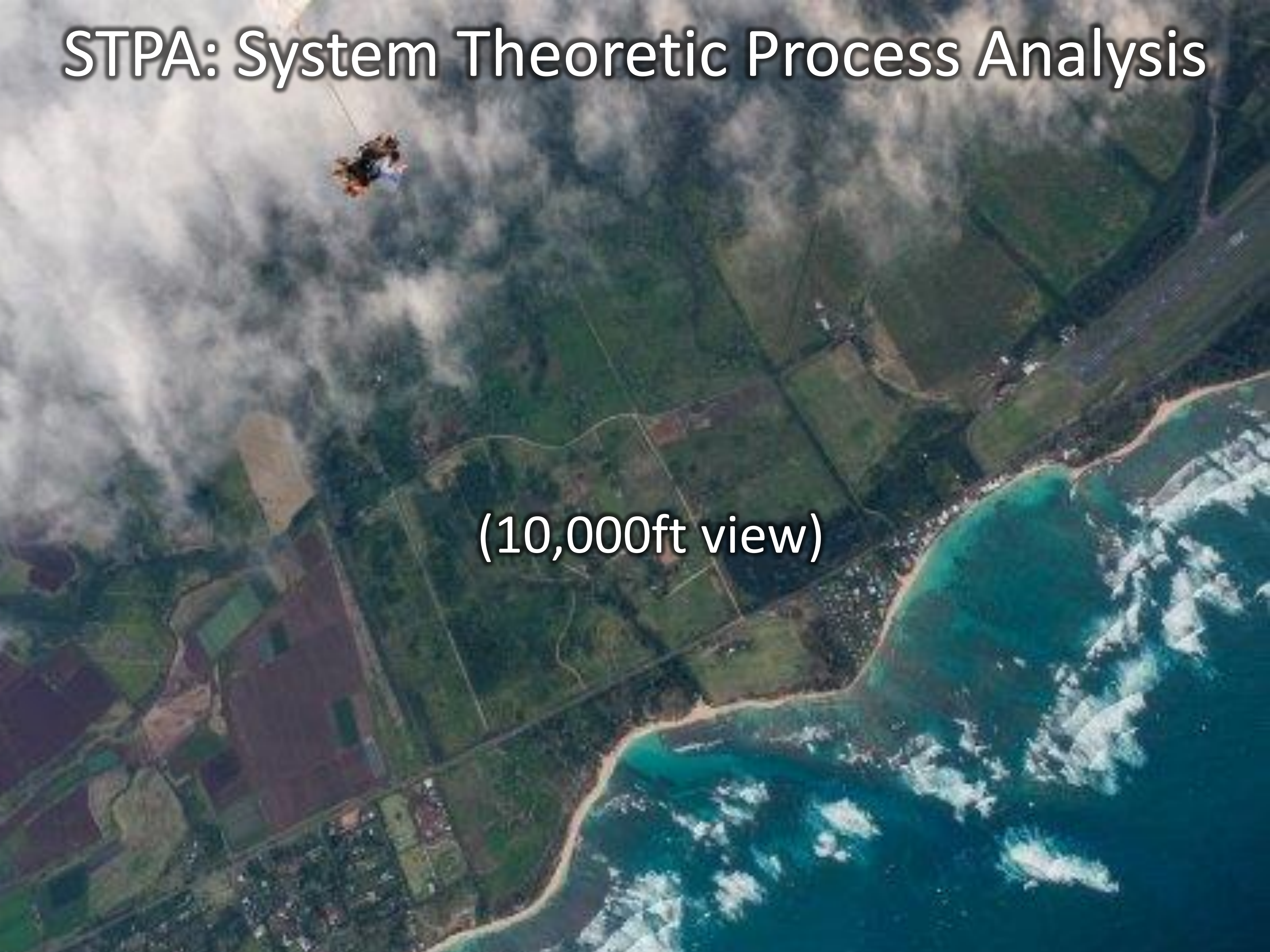
(Leveson and Thomas, 2018)


STPA
System Theoretic Process Analysis
(30,000ft view)

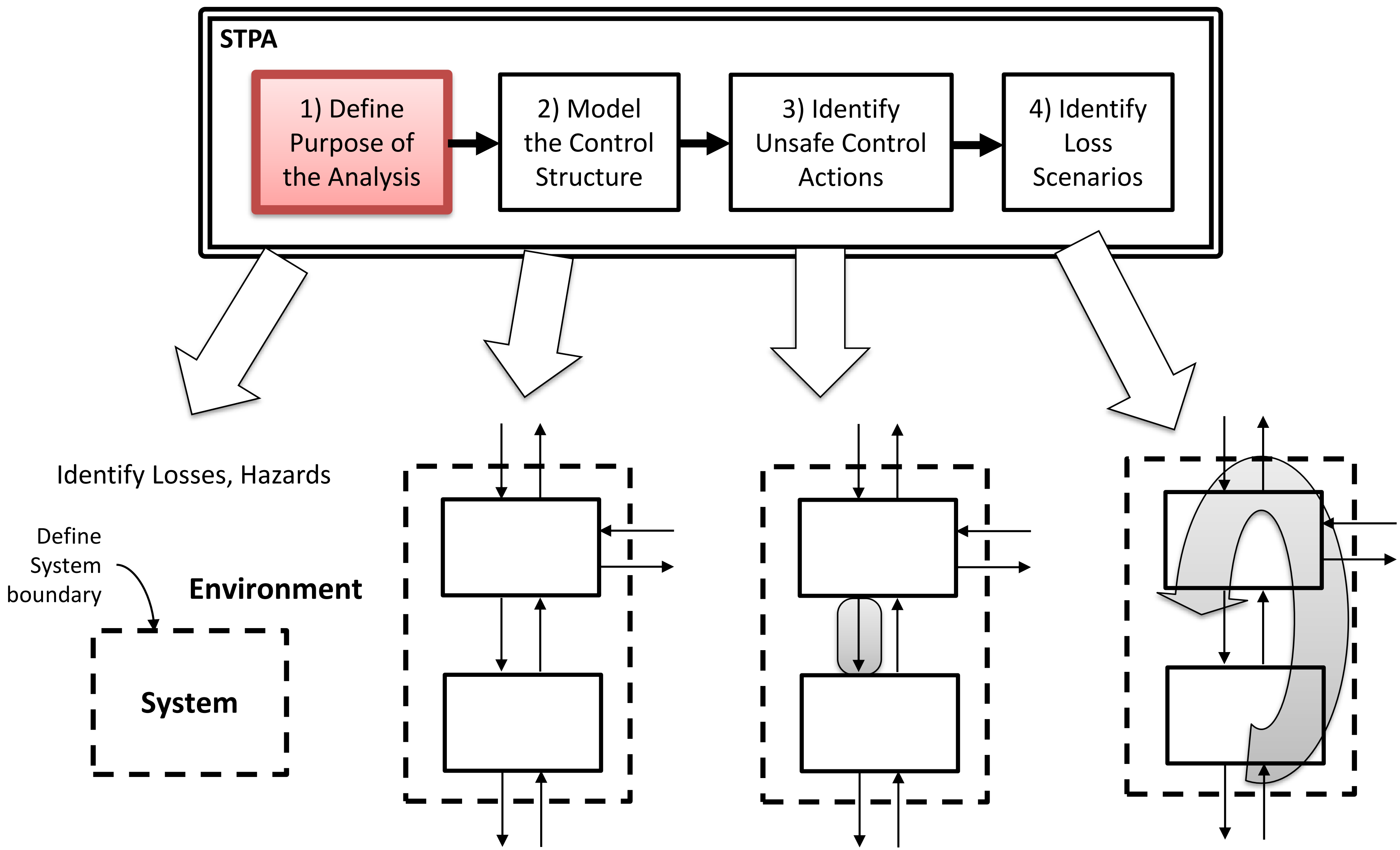


(Leveson and Thomas, 2018)

STPA: System Theoretic Process Analysis



(10,000ft view)



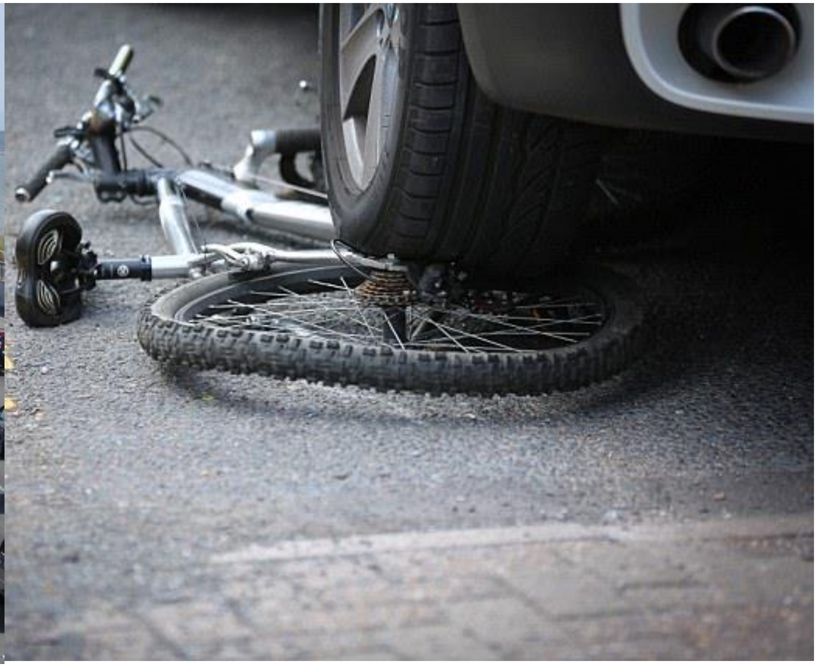
(Leveson and Thomas, 2018)

Definitions

- Accident = Mishap = Loss
  - Any undesired and unplanned event that results in a loss
  - e.g., loss of human life or injury, property damage, environmental pollution, mission loss, negative business impact (damage to reputation, etc.), product launch delay, legal entanglements, etc. [MIL-STD-882]
  - Includes inadvertent and intentional losses (security)

Automotive Example

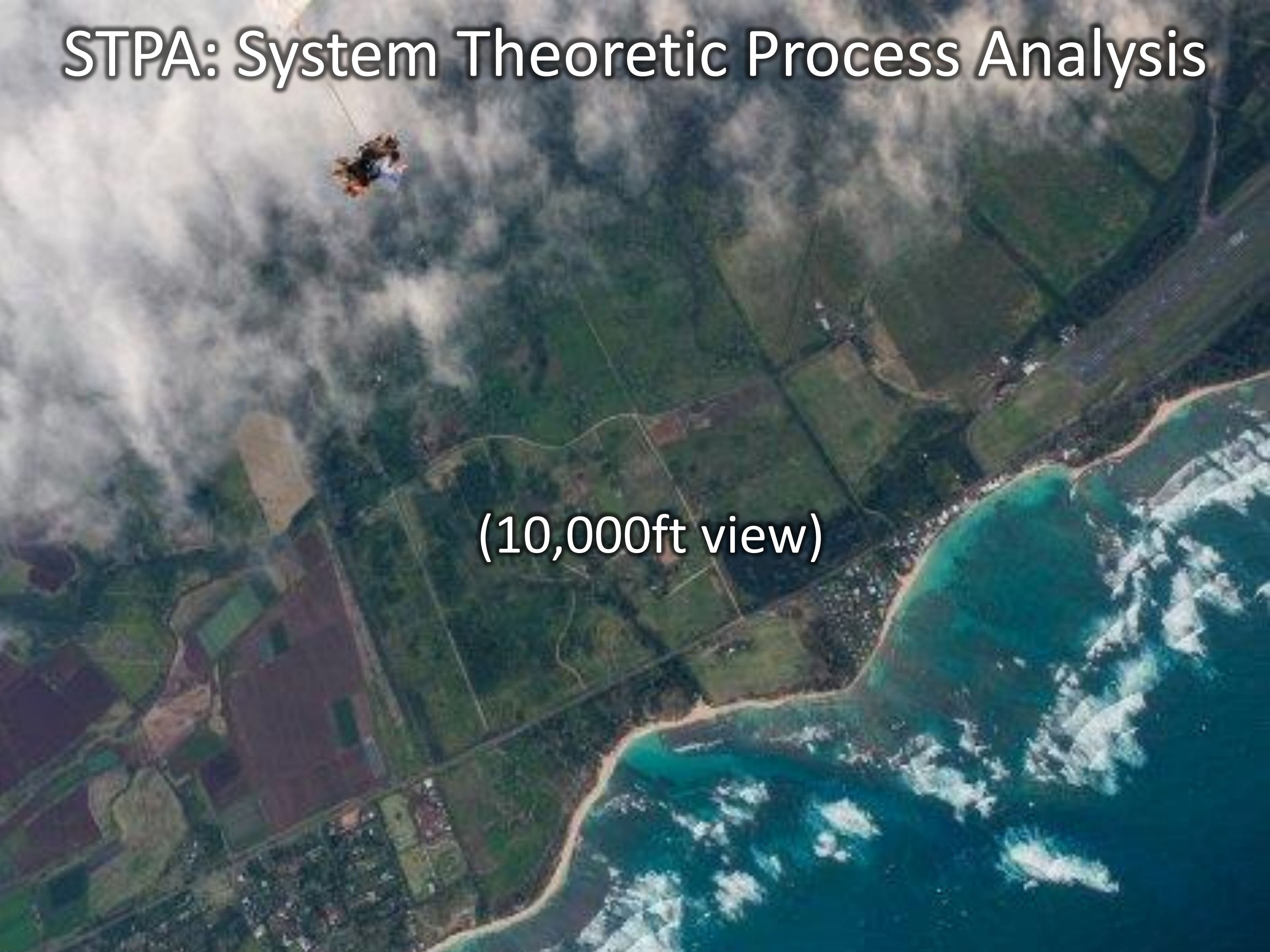
- Losses (Accidents)
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the vehicle or objects outside the vehicle
  - L-3: Loss of mission (transportation)
  - L-4: Loss of customer satisfaction



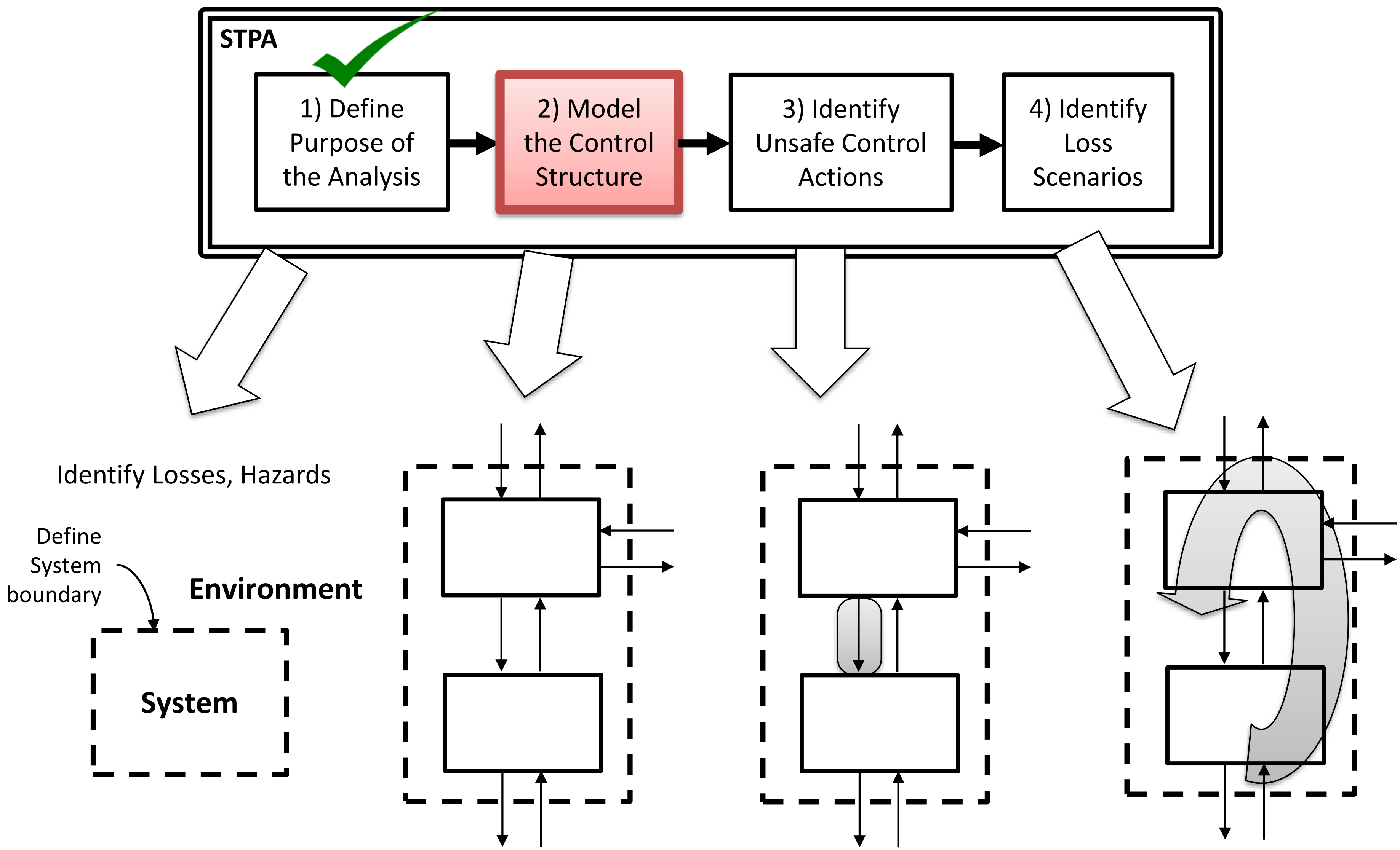
Aviation Example

- Losses
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the aircraft or objects outside the aircraft
  - L-3: Loss of mission (transportation)
  - L-4: Loss of performance / efficiency

STPA: System Theoretic Process Analysis

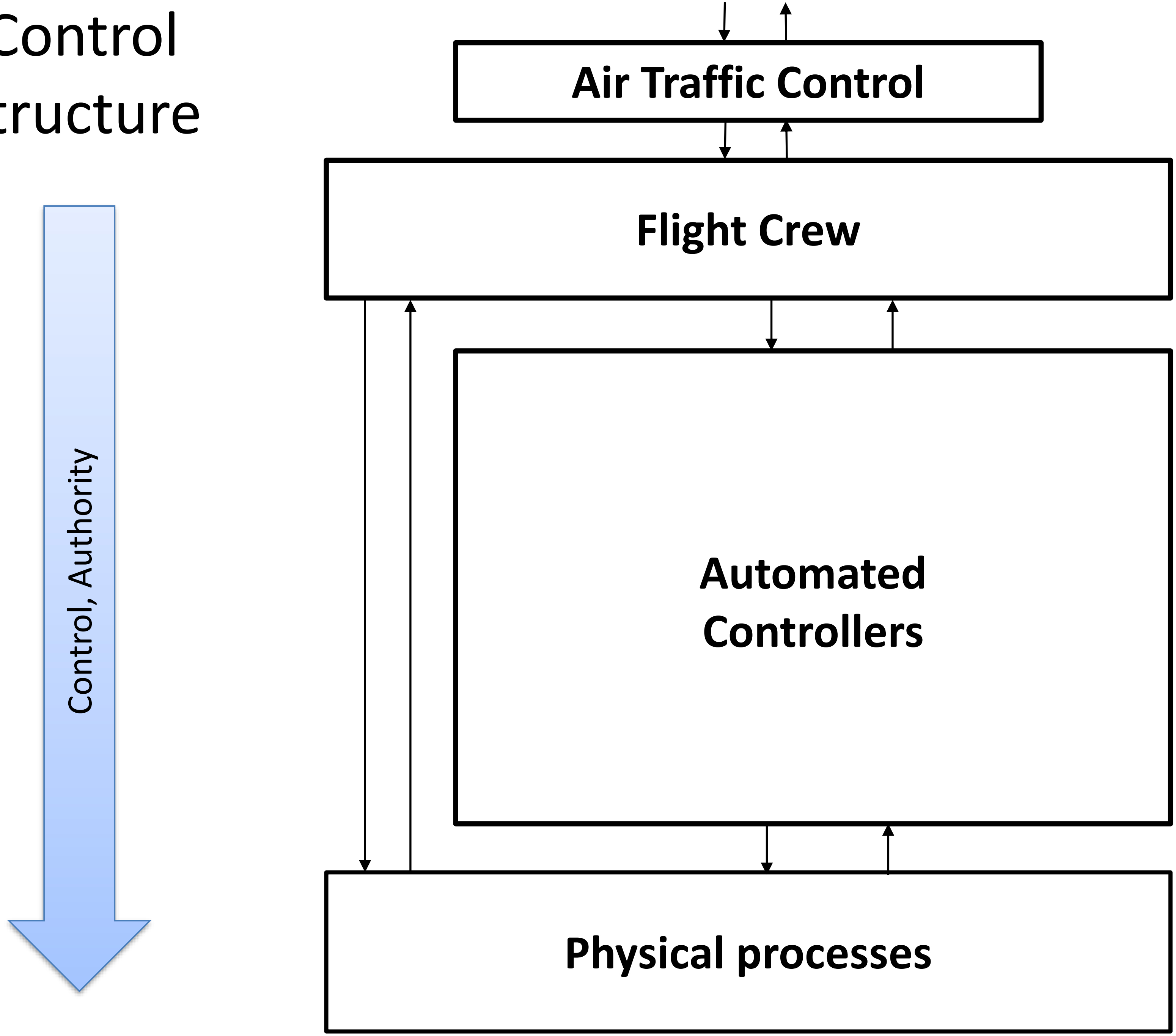


(10,000ft view)



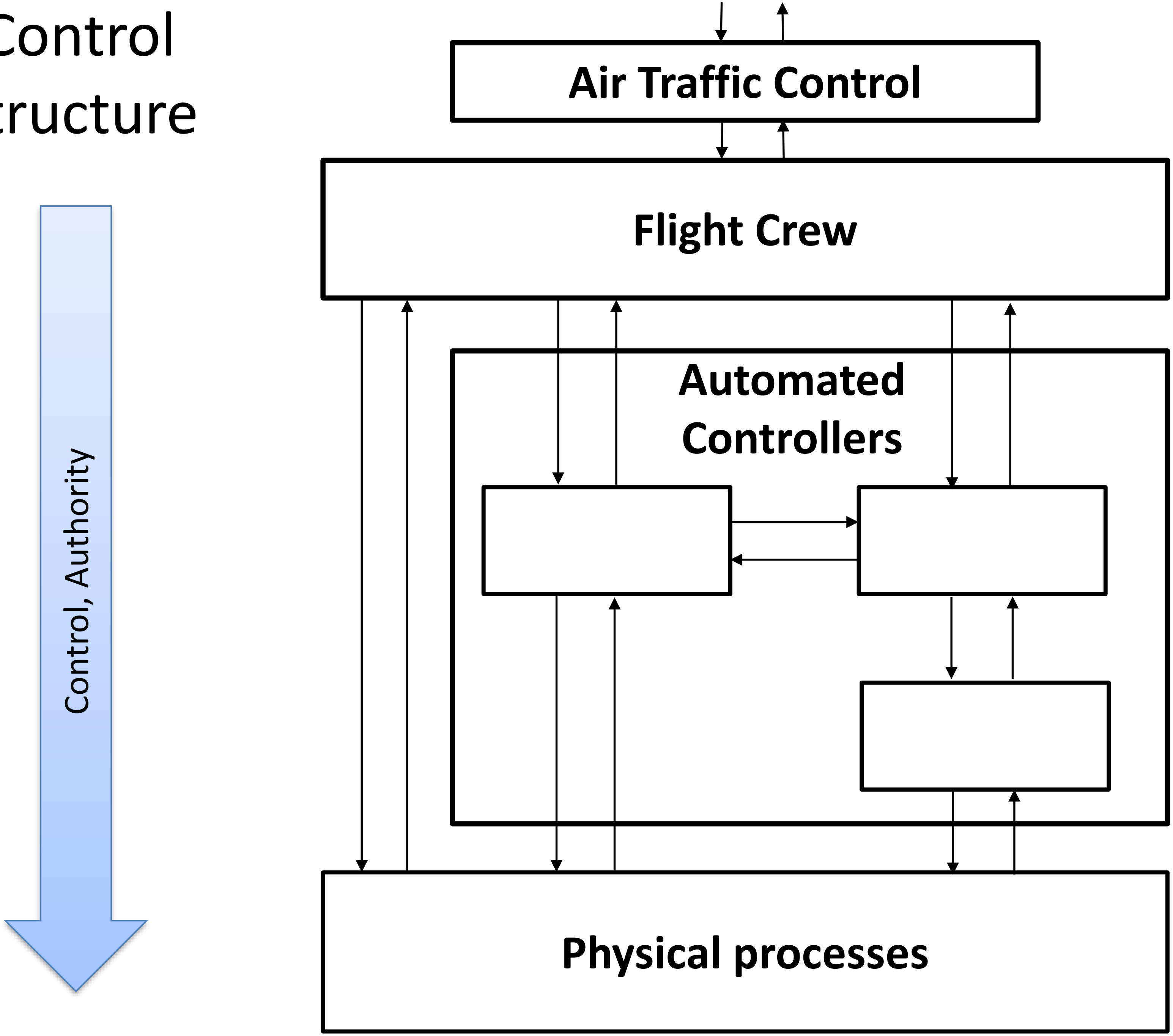
(Leveson and Thomas, 2018)

Control structure



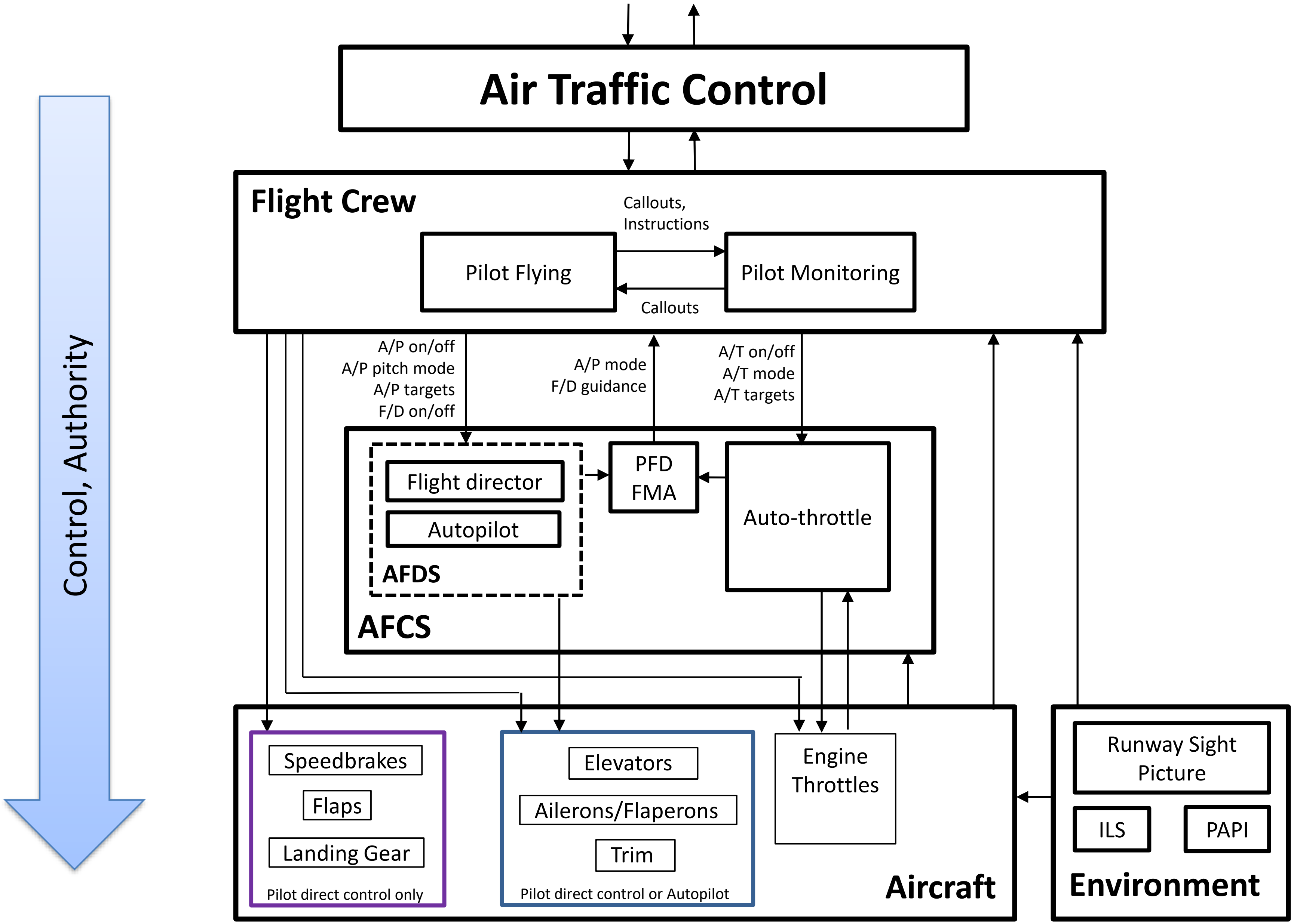
(Thomas, 2017)

Control structure

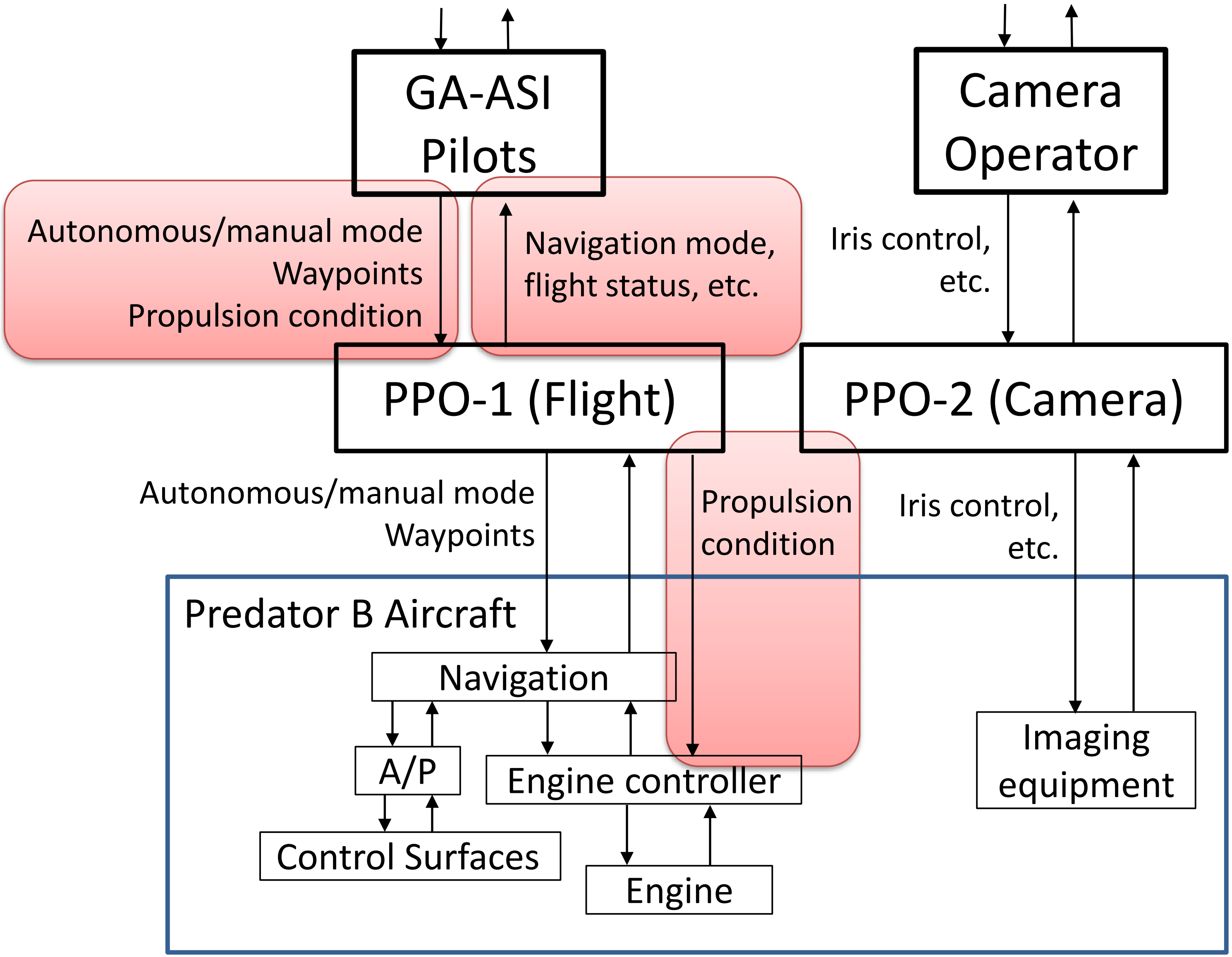


(Thomas, 2017)

Control Structure



Unmanned Predator-B Crash (US CBP)

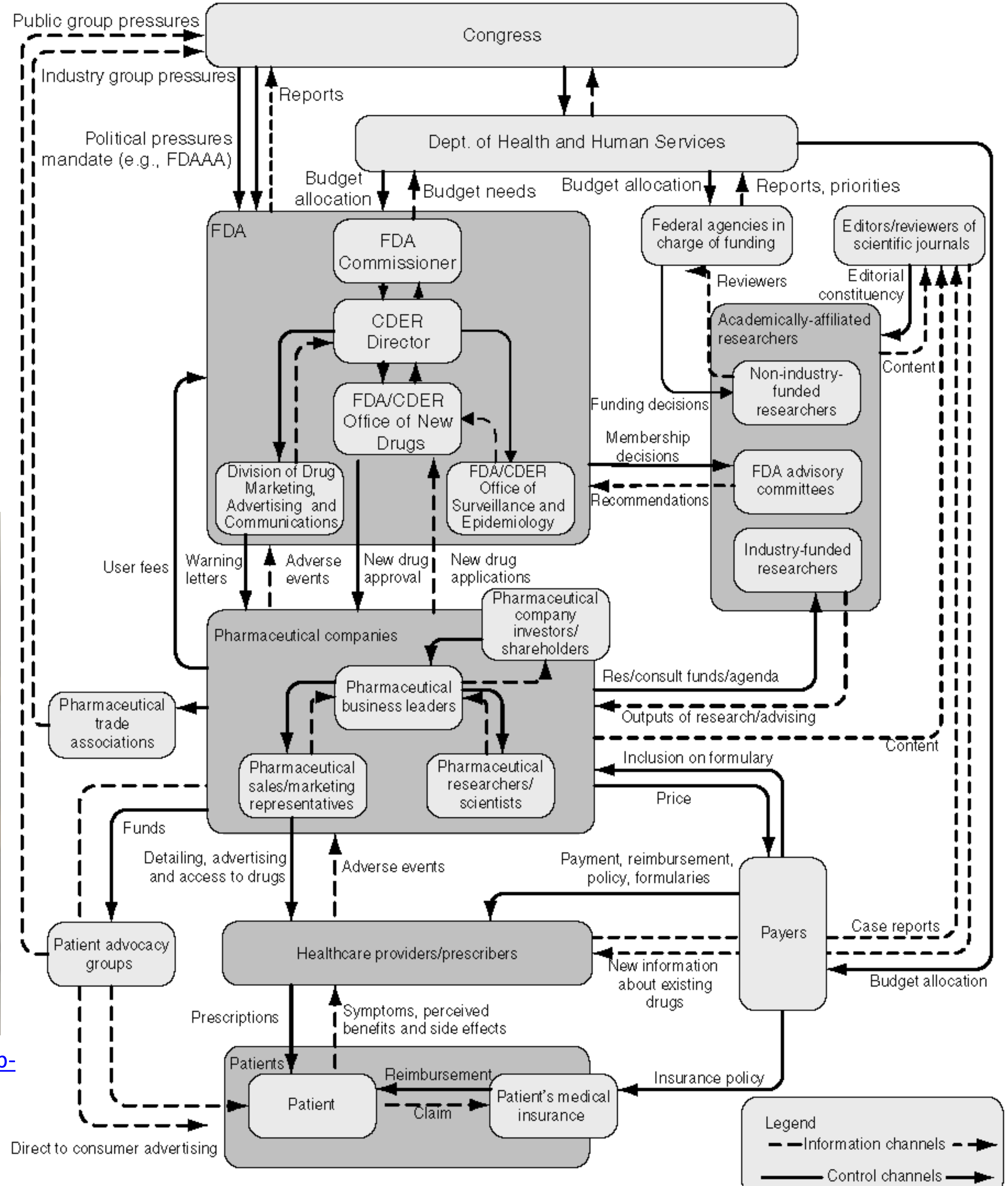


Thomas, 2017

U.S. pharmaceutical safety control structure

(a purely human/organizational system)

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



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

Adaptive Cruise Control

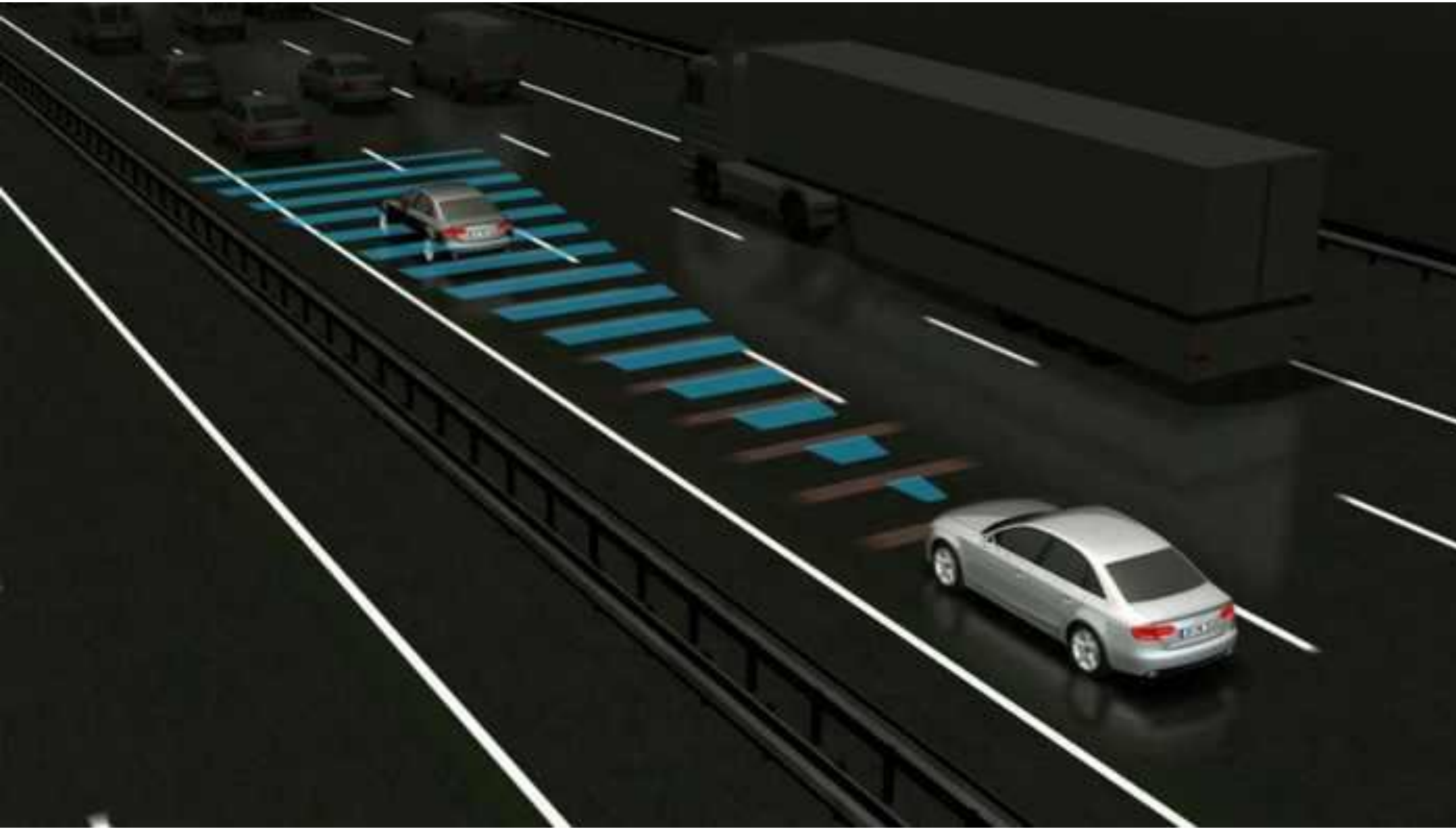
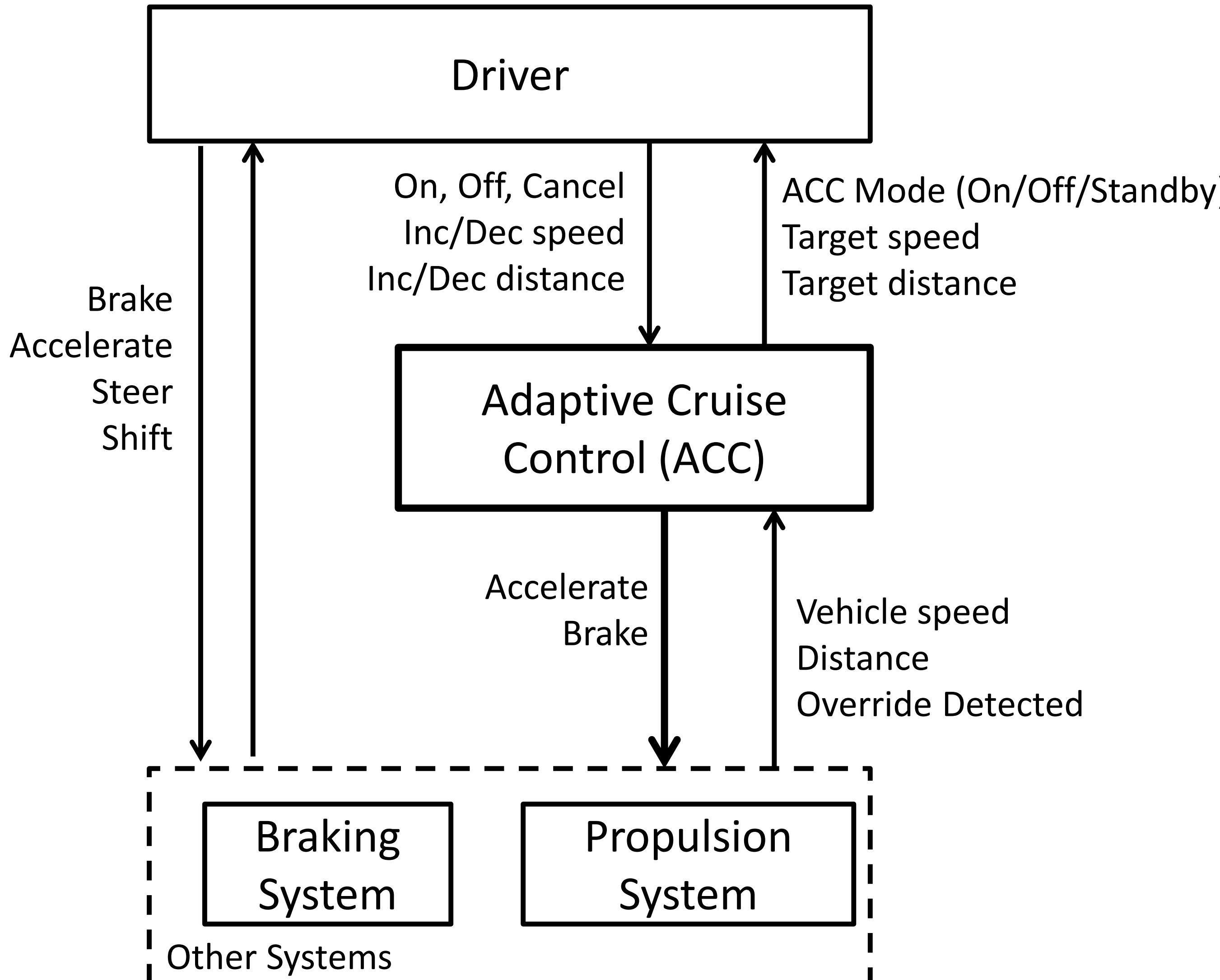


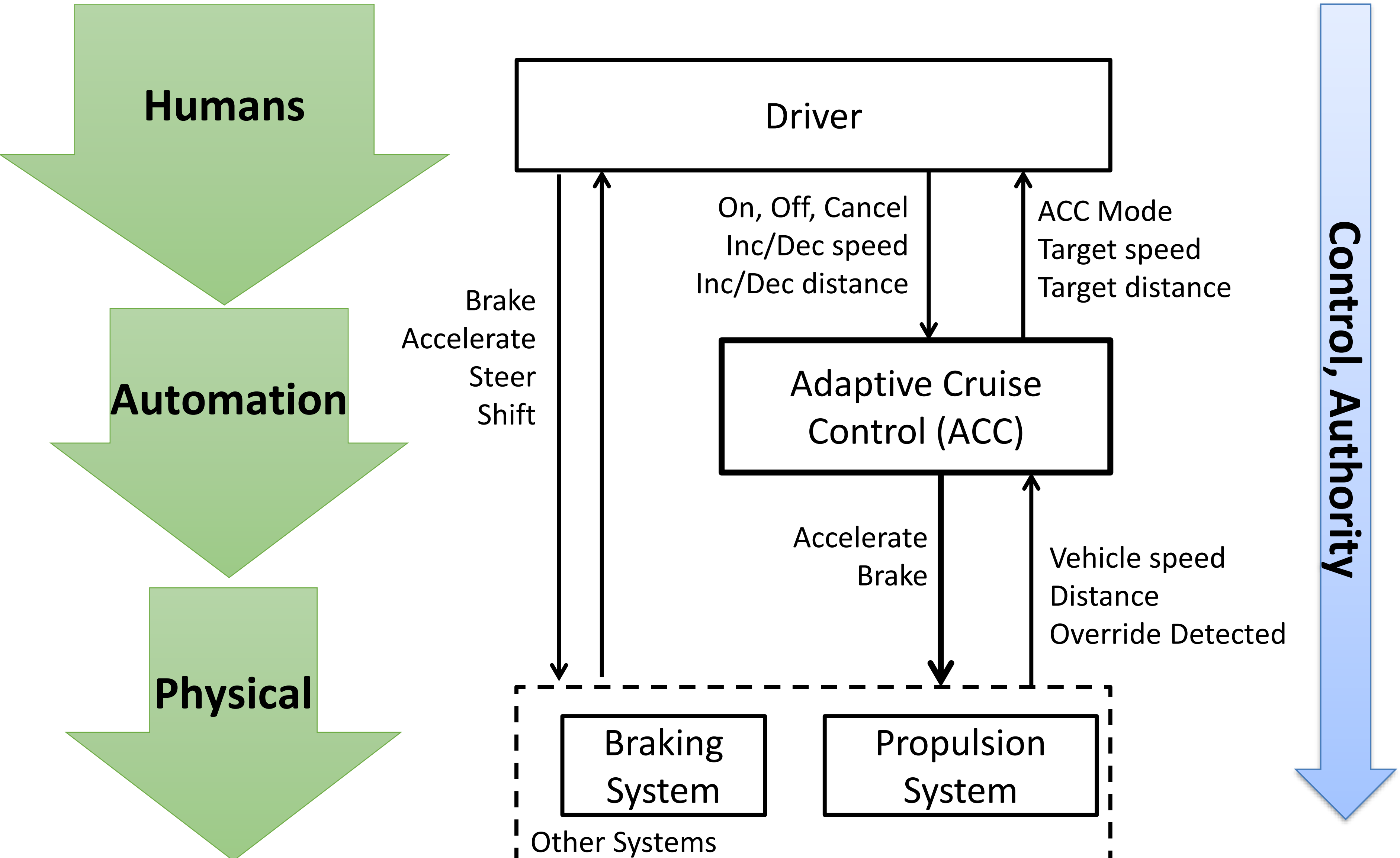
Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

Adaptive Cruise Control (ACC) Control Structure



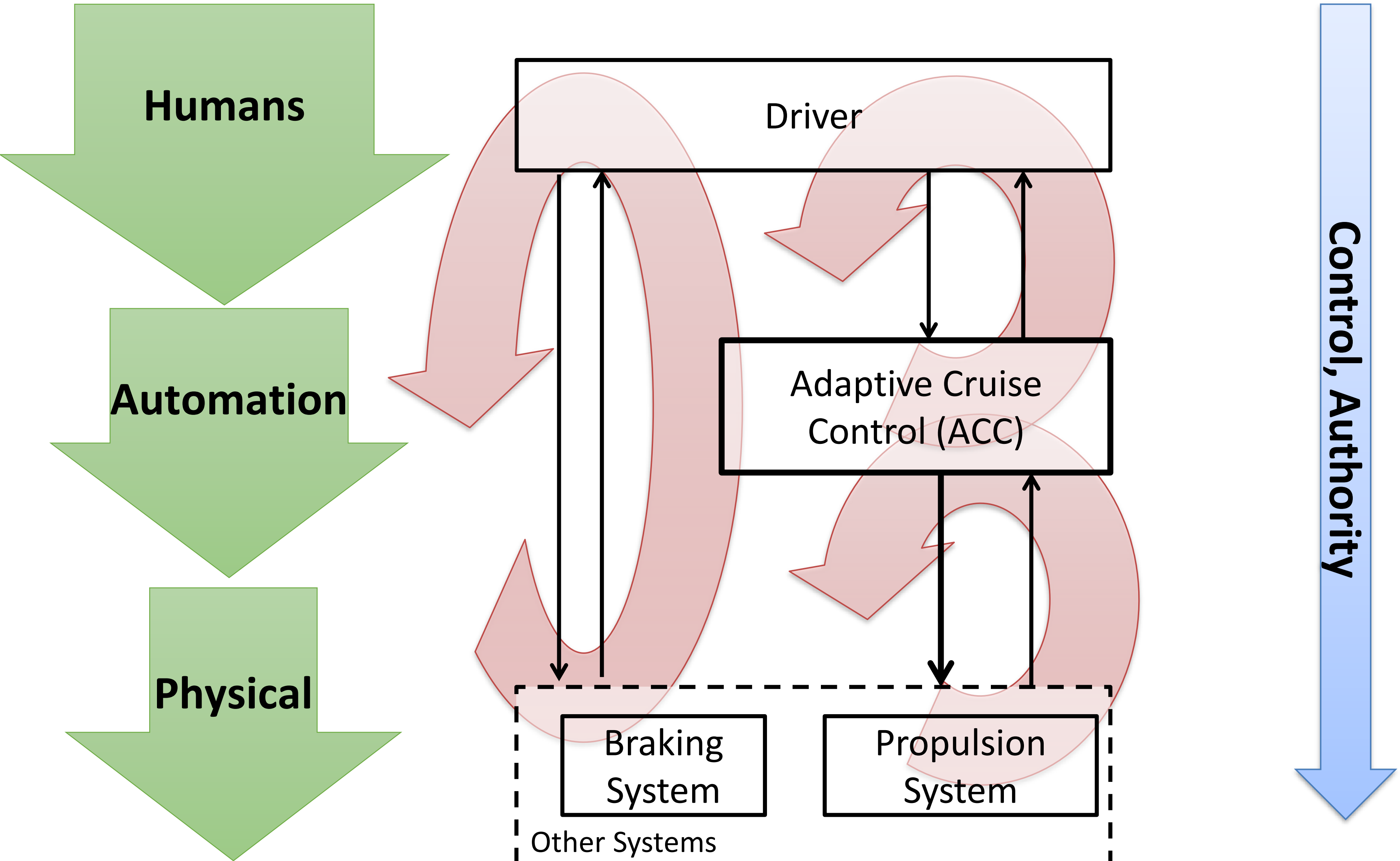
Thomas, 2017

Adaptive Cruise Control (ACC) Control Structure



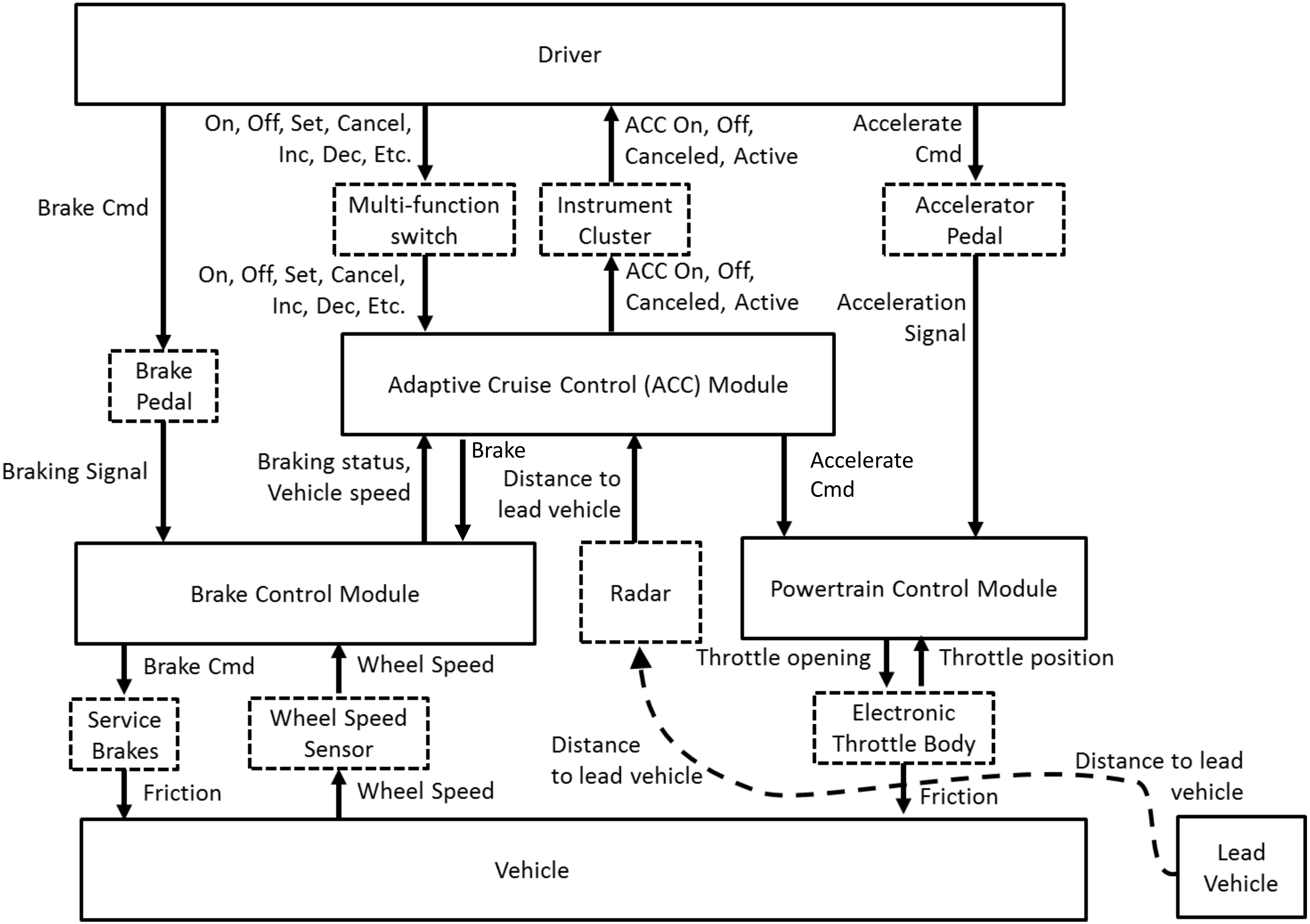
Thomas, 2017

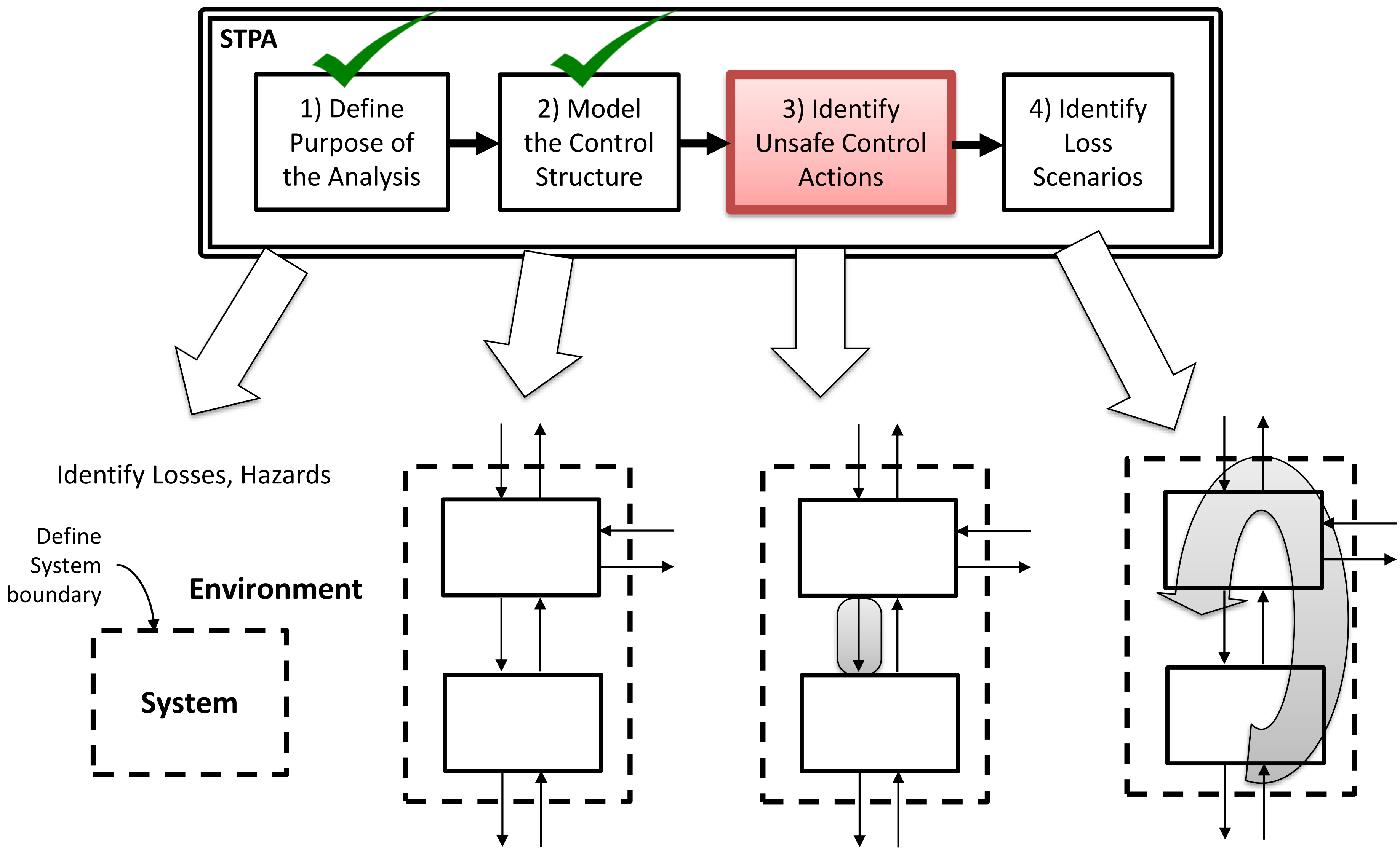
Adaptive Cruise Control (ACC) Control Structure



Thomas, 2017

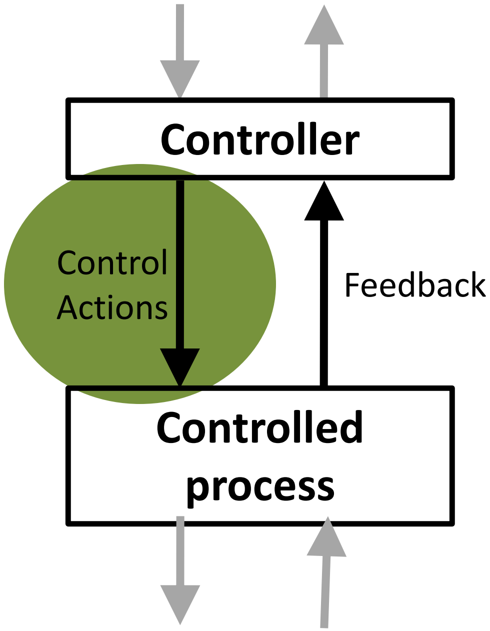
Refined Control Structure





(Leveson and Thomas, 2018)

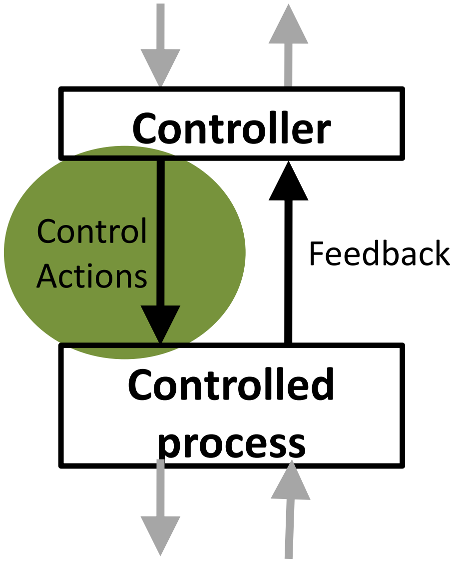
Identifying Unsafe Control Actions (UCA)



4 ways unsafe control may occur:

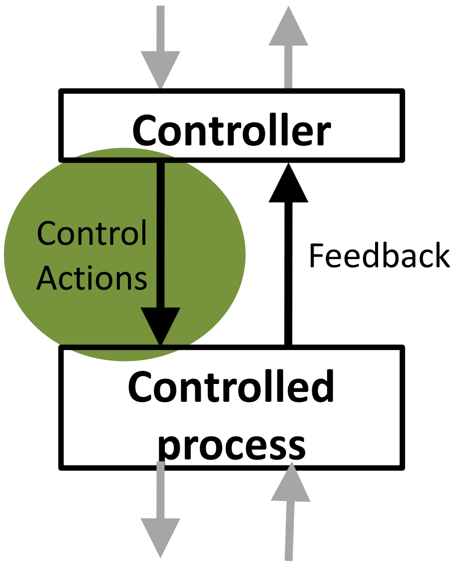
Brake Command				

Identifying Unsafe Control Actions (UCA)



	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)

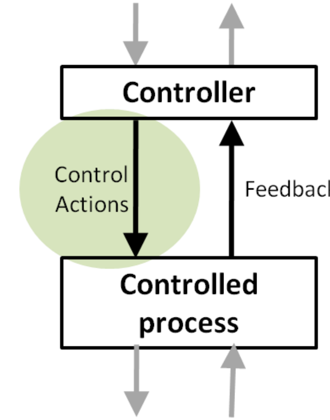


Example:
"Driver does not provide Brake cmd when forward collision imminent"

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	?	?	?	?

Structure of an Unsafe Control Action



Example:

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

Source Controller

Type

Control Action

Context

Four parts of an unsafe control action

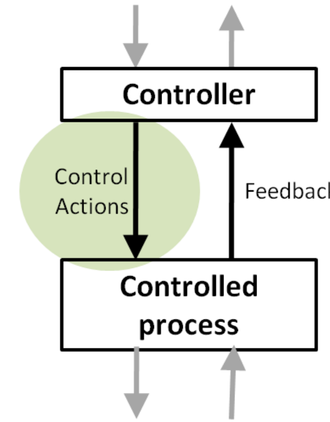
– Source Controller: the controller that can provide the control action
– Type: whether the control action provided, not provided, etc.
– Control Action: the controller's command that was provided / missing
– Context: conditions for the hazard to occur
  - (system or environmental state in which command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

Thomas, 2017

Component Safety Constraints

Unsafe Control Action	Component Safety Constraint
UCA-1: Computer provides Shift-to-Park cmd while vehicle is moving [H-3]	SC-1: Computer shall not provide Shift-to-Park cmd while vehicle is moving [UCA-1]

Structure of an Unsafe Control Action



Example:

"<u>Driver</u> <u>provides</u> <u>Park cmd</u> while <u>vehicle is moving</u>"

Source Controller

Type

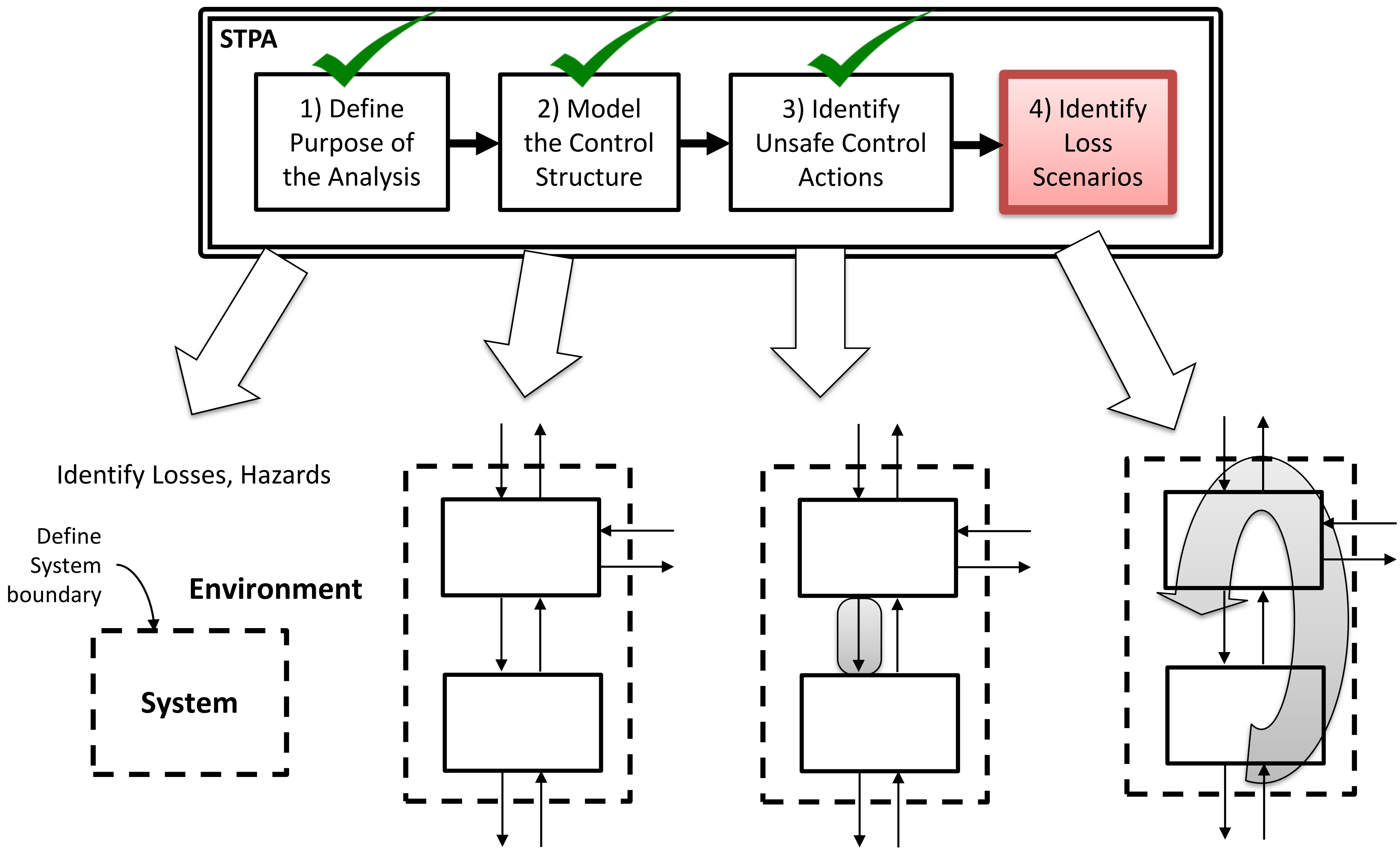
Control Action

Context

Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action 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)

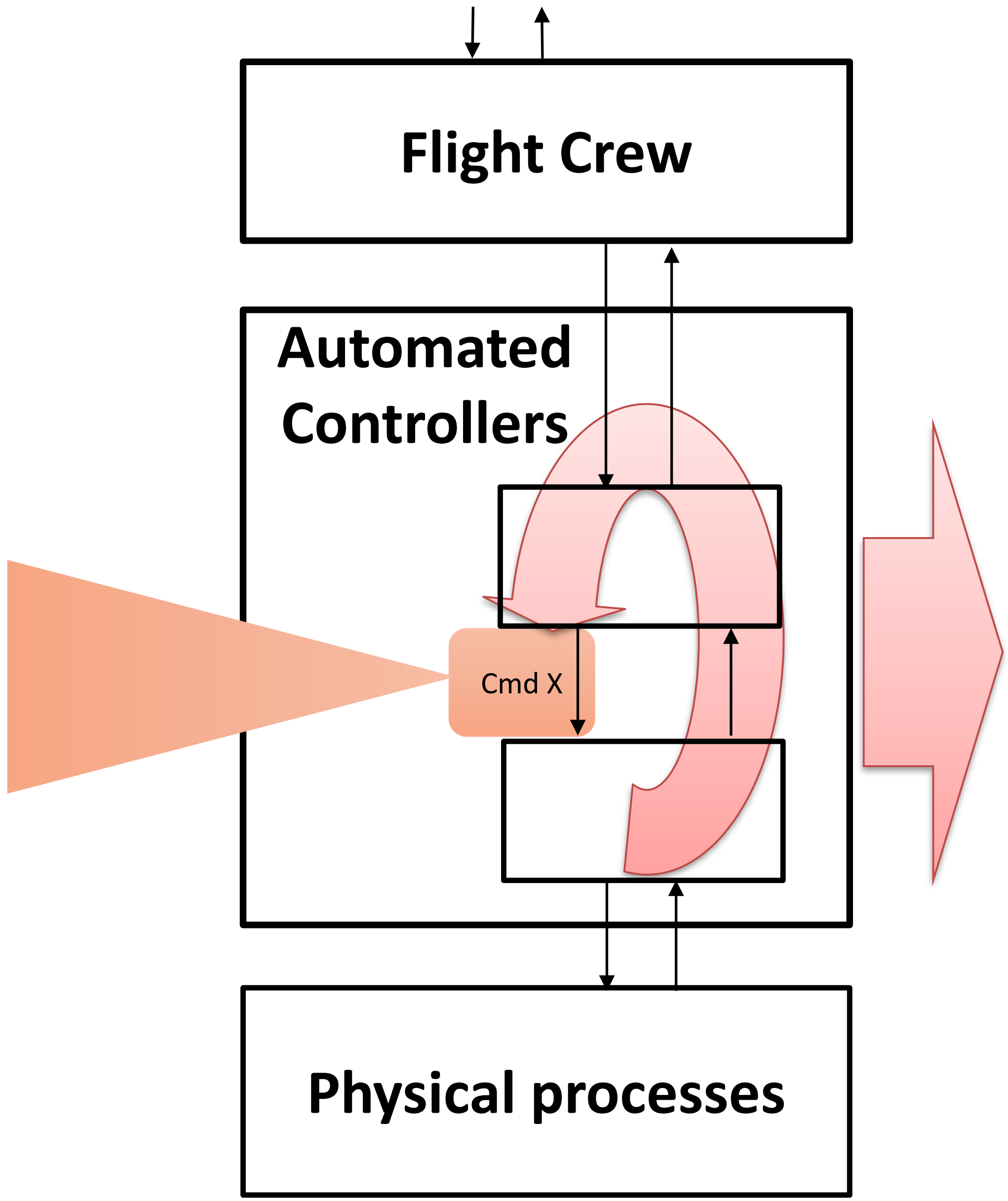
Thomas, 2017



(Leveson and Thomas, 2018)

Identify loss scenarios

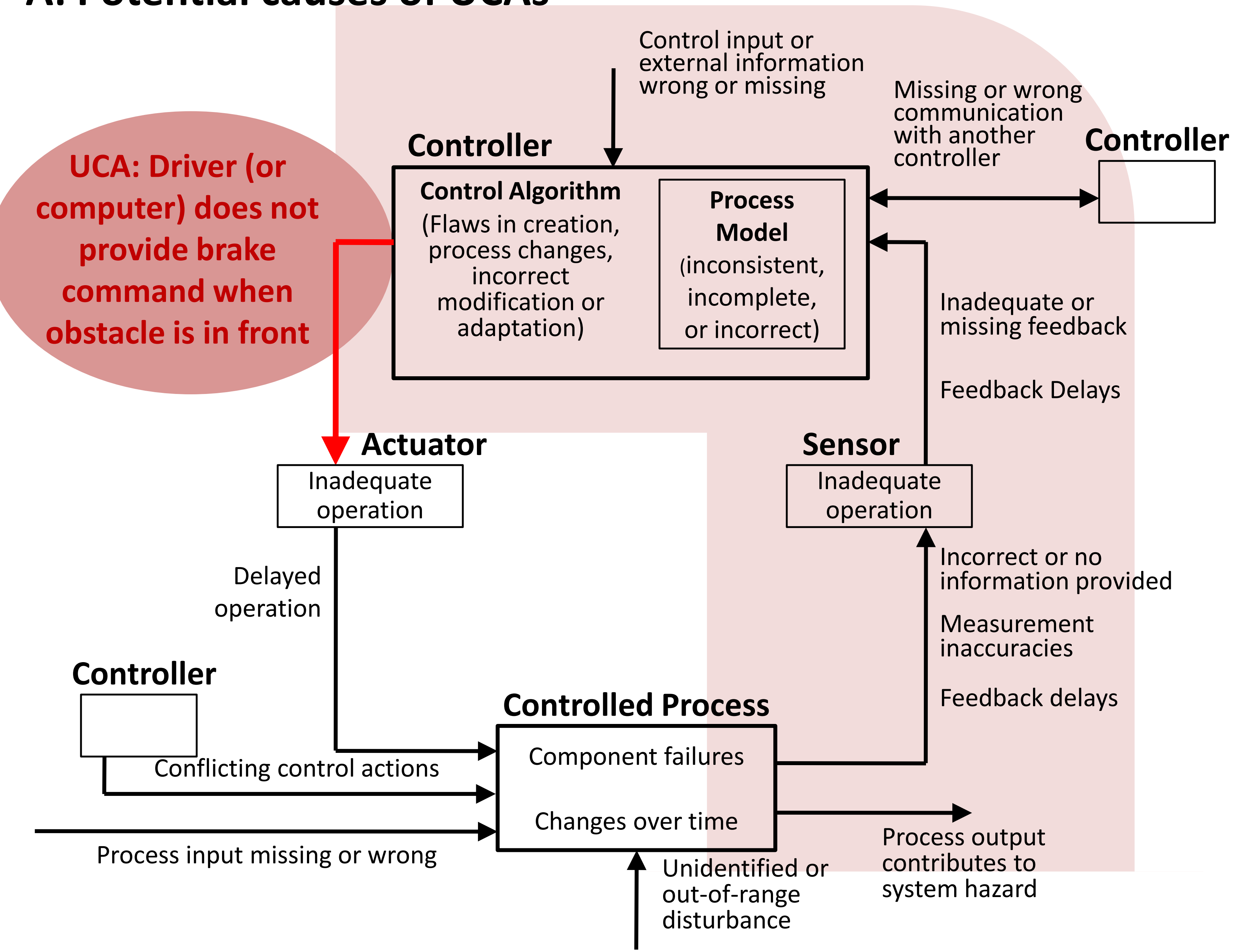
What could cause Unsafe Control Actions?



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)

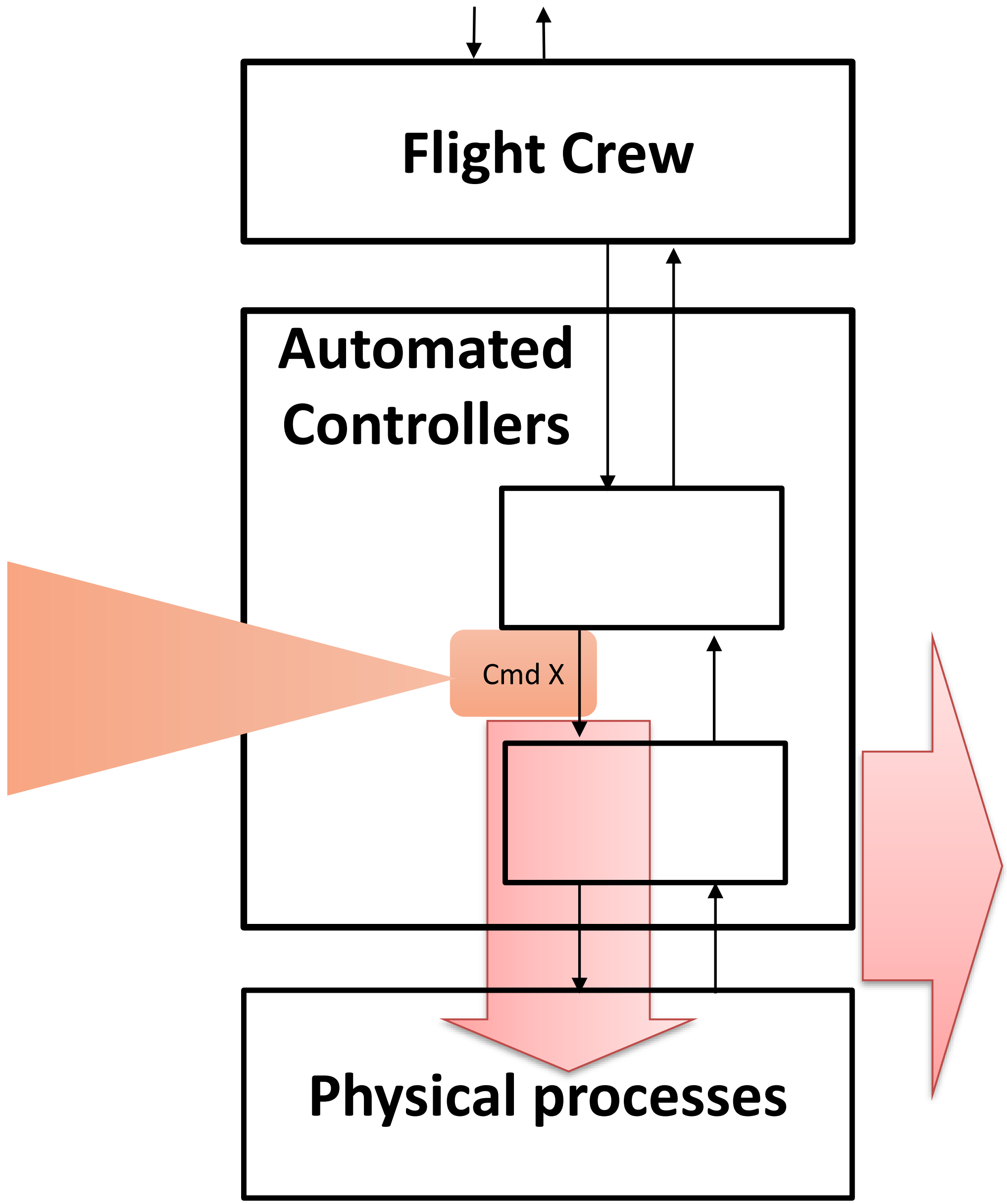
A: Potential causes of UCAs



Thomas, 2017

Identify loss scenarios

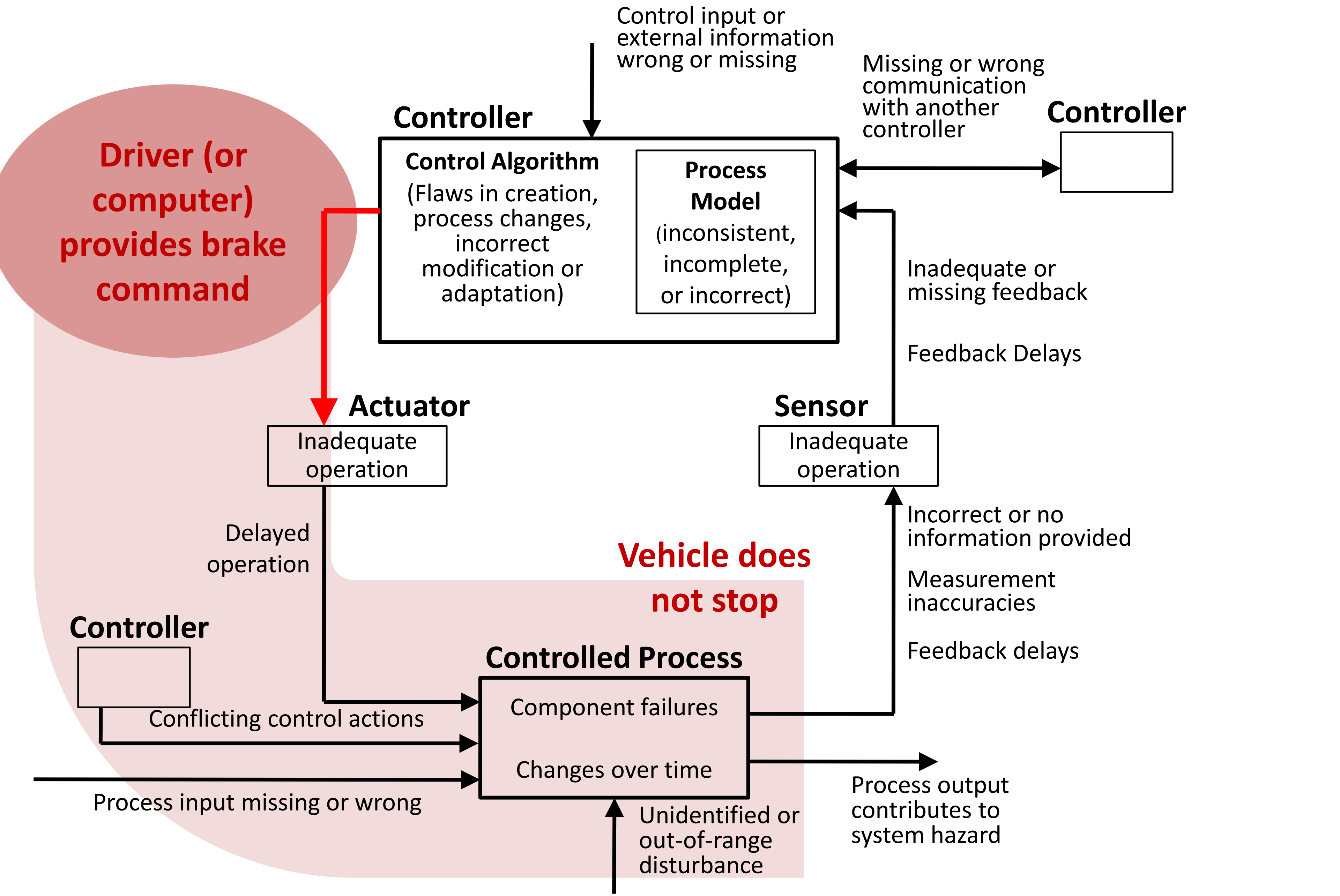
Control actions not executed or not followed properly



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

(Thomas, 2017)

B: Potential control actions not followed



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.

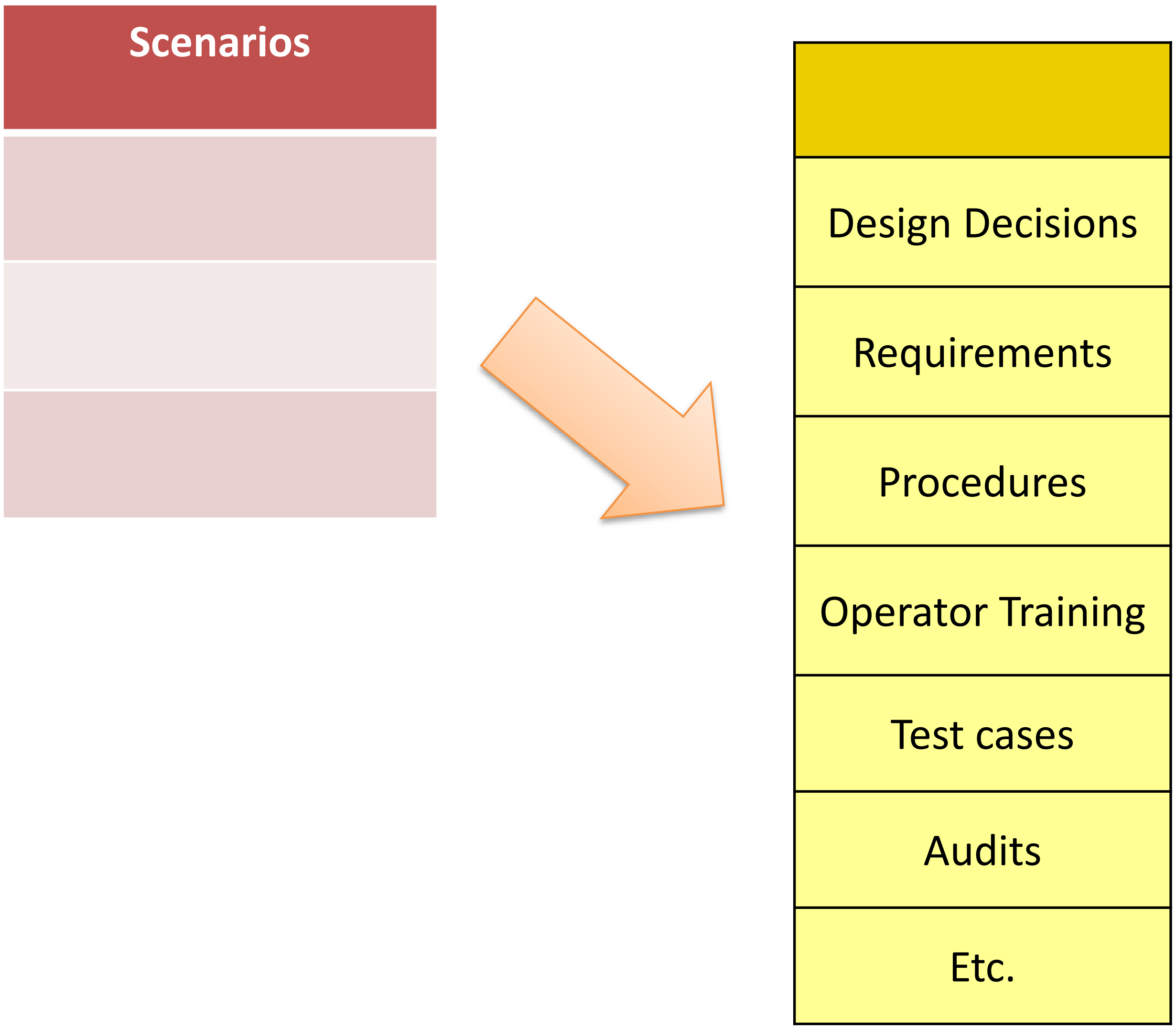
Rationale and assumptions identified

Recommendations
Crew must take into consideration D to prevent E
Crew 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.

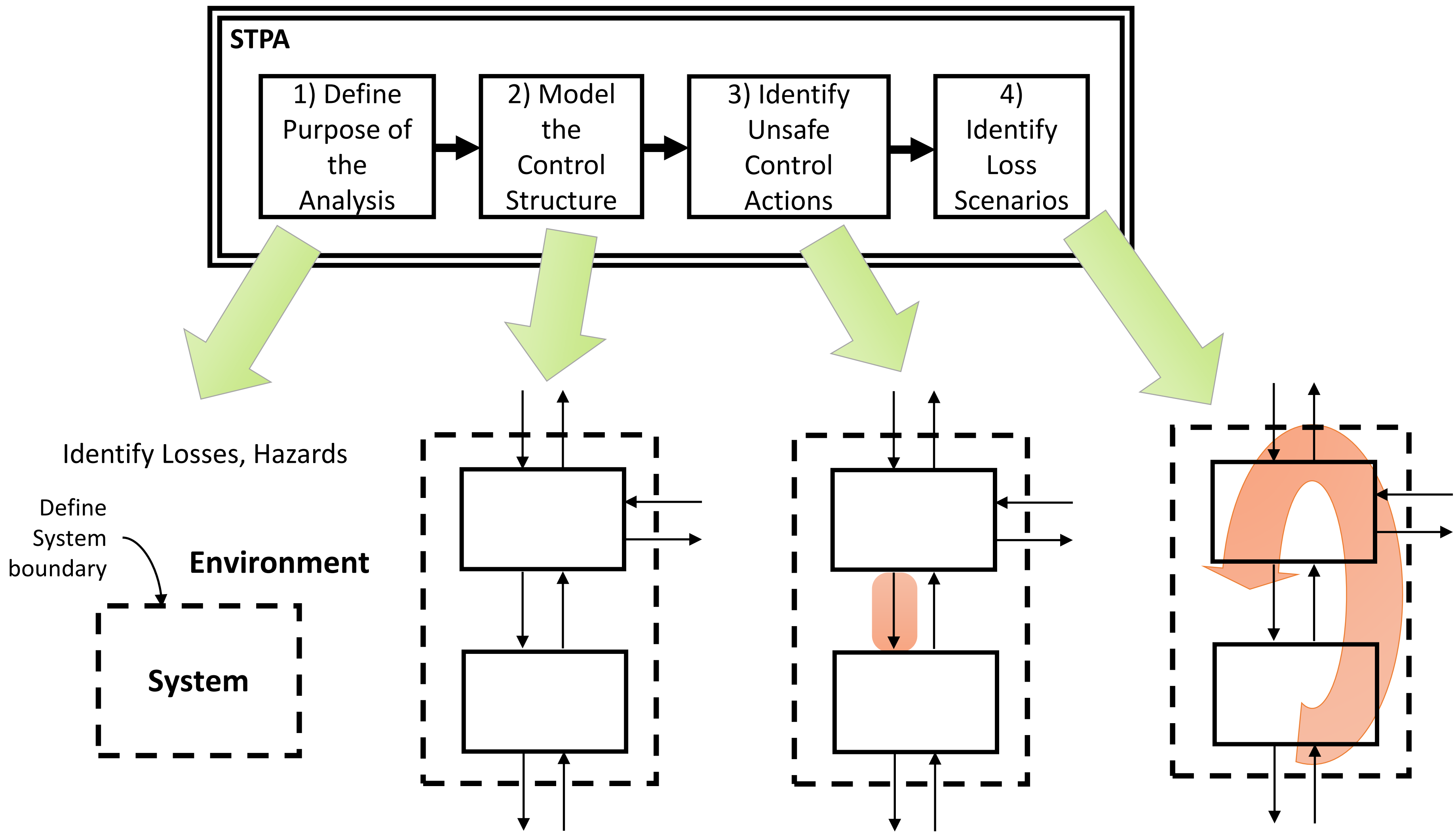


Rationale and assumptions identified

Every recommendation and decision is traceable

(Thomas, 2017)

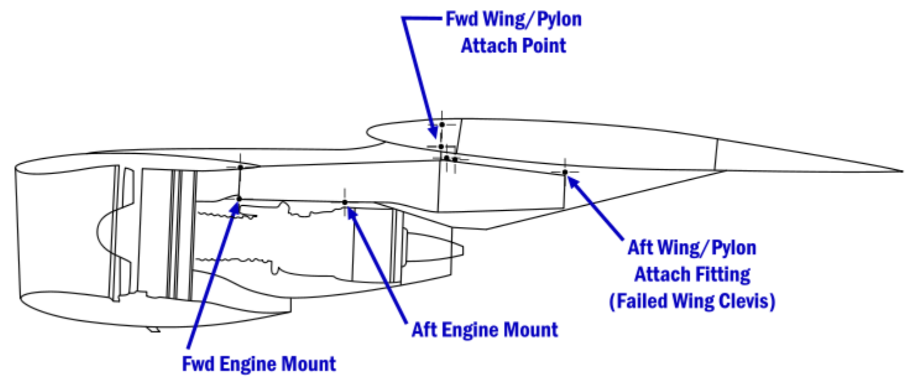
STPA Overview



Very short example: DC-10 engine out

American Airlines 191: DC-10

- Left engine (#1) separates from aircraft on takeoff
- Pilot follows standard procedure for engine out. Raises nose to 14°, slows to takeoff safety airspeed (V_2) of 153 knots
    - This the specified speed at which the aircraft can safely climb after sustaining an engine failure
- Aircraft suddenly rolls left 120° (uncommanded), crashes
- Killed all 271 people on board. Deadliest aviation accident on US soil to this day.
- Post-accident simulator recreations done with 12 other pilots. None could prevent the crash.



John Thomas, 2019

American Airlines 191: DC-10

- Left engine (#1) separates from aircraft on takeoff
- Pilot follows standard procedure for engine out. Raises nose to 14°, slows to takeoff safety airspeed (V_2) of 153 knots
  - This the specified speed at which the aircraft can safely climb after sustaining an engine failure
- Aircraft suddenly rolls left 120° (uncommanded), crashes
- Killed all 271 people on board. Deadliest aviation accident on US soil to this day.
- Post-accident simulator recreations done with 12 other pilots. None could prevent the crash.

- Damaged hydraulic lines, left slats retracted
- Stall speed of left wing increased from 124 knots to 159 knots
- Cockpit indication incorrectly confirmed slats still in extended position (not visible from cockpit)
- Slat disagreement warning light inoperative (powered by #1 engine)
- Captain stick shaker inoperative (powered by #1 engine)
- First officer stick shaker never installed (offered as optional feature, not purchased by AA)

John Thomas, 2019

Using STPA to ask questions

System Hazard: Aircraft uncontrolled flight

Question: What Pilot control actions can cause aircraft to stall?

UCA: Pilot decreases speed below stall speed

Question: What Pilot beliefs would cause Pilot to decrease speed below stall speed?

- Incorrectly believes speed is higher than it is
- Incorrectly believes stall speed is lower than it is

Pilot

Control algorithm

Process Model (beliefs)

Control Actions

Feedback

Question: What Pilot inputs would cause Pilot to believe stall speed lower than it is?

- No stick shaker during stall
- No slat disagreement ind. during slat retract

Question: What process behavior would cause slats to retract without slat disagreement indication?

Controlled Process

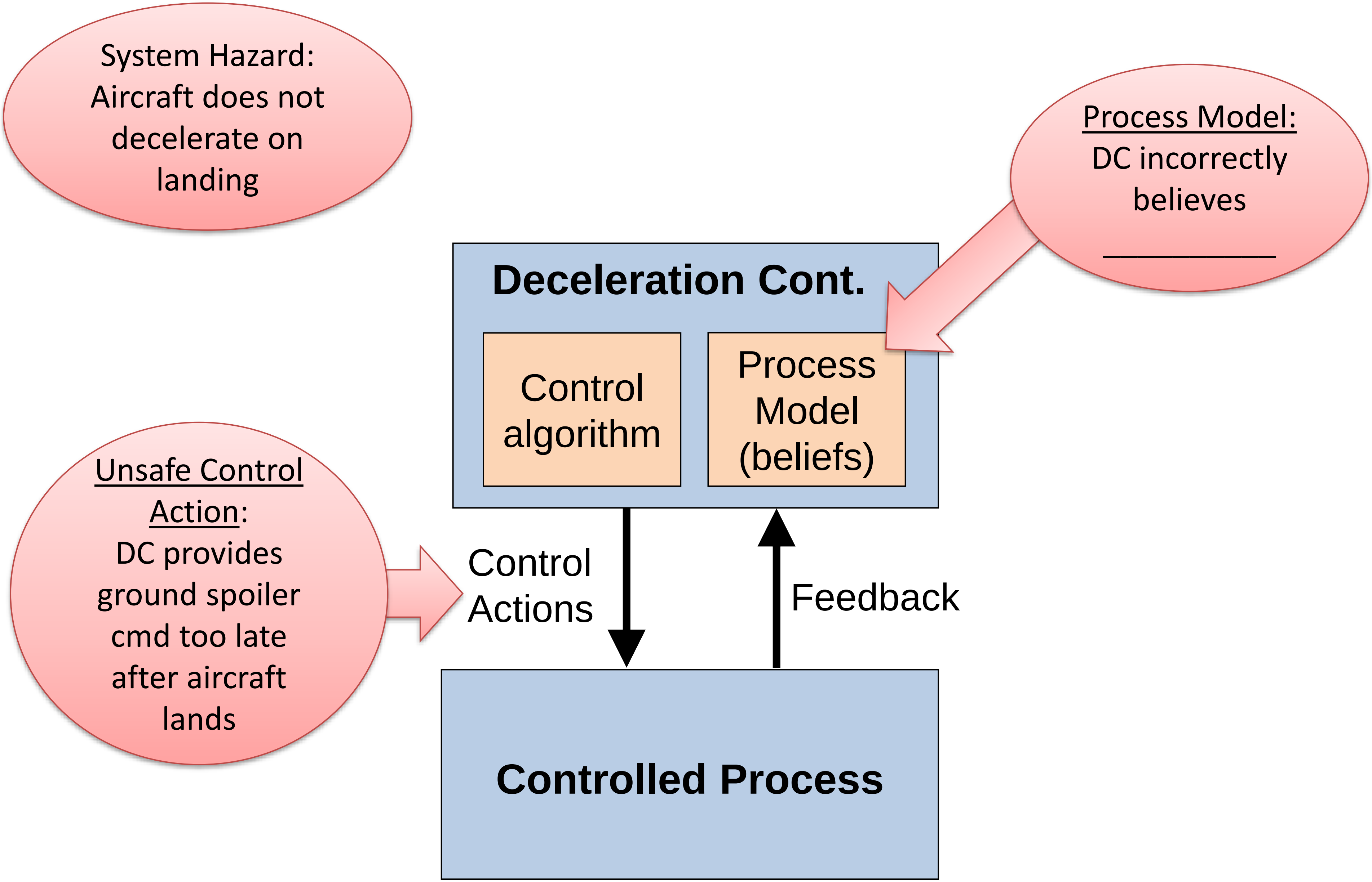
Loss #1 engine/power
Hydraulic rupture near slats

Very short exercise:
A320 Thrust Reversers

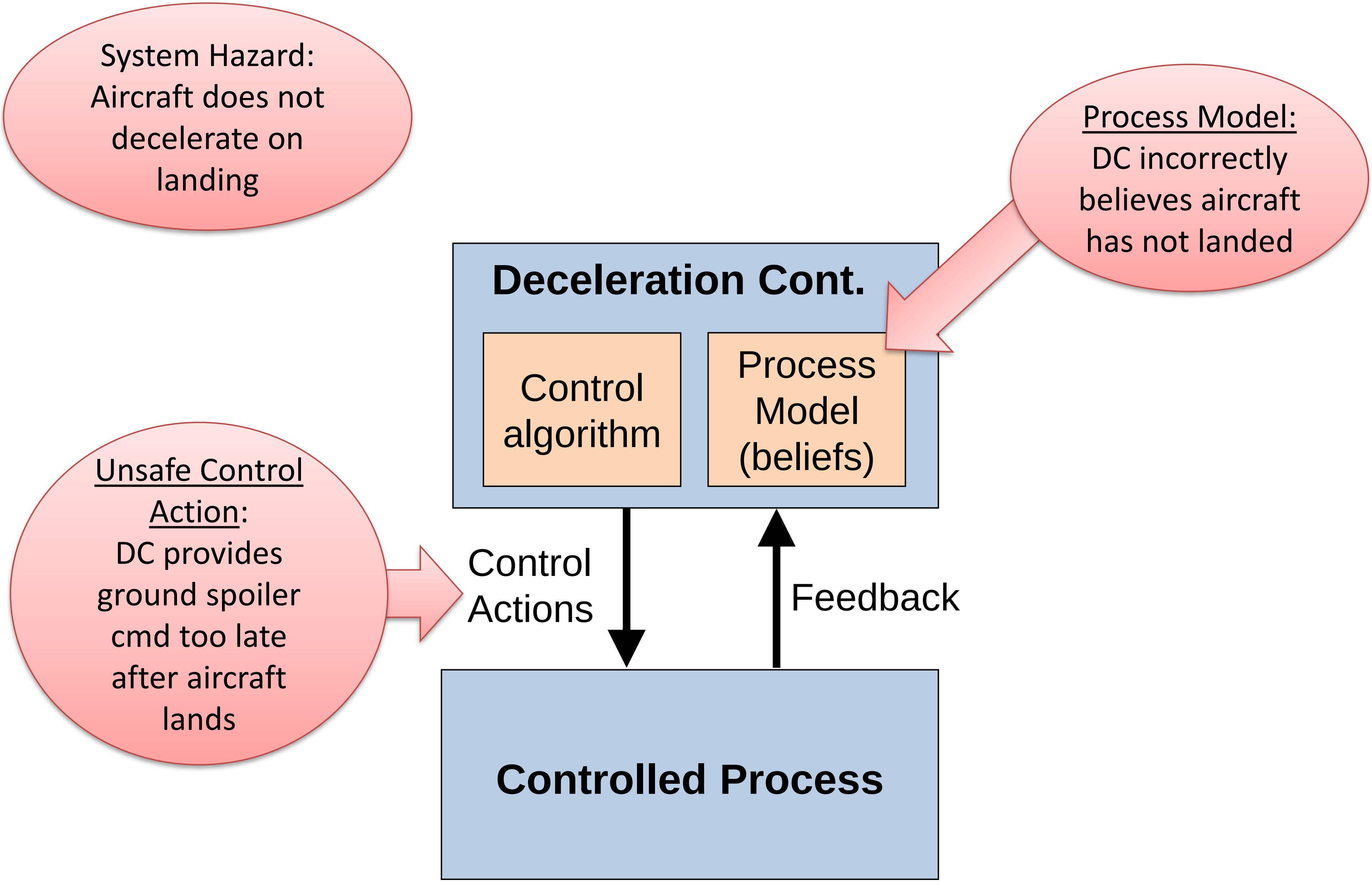
A320 Automation

- A320 automation protects against certain actions until aircraft has landed
- Deceleration on landing:
  - Thrust reversers not allowed until WoW sensed on both main landing gear struts
  - Ground spoilers not allowed until sufficient WoW or wheel speed
  - Wheel brakes triggered when sufficient wheel speed detected

Basic Control Loop



Basic Control Loop

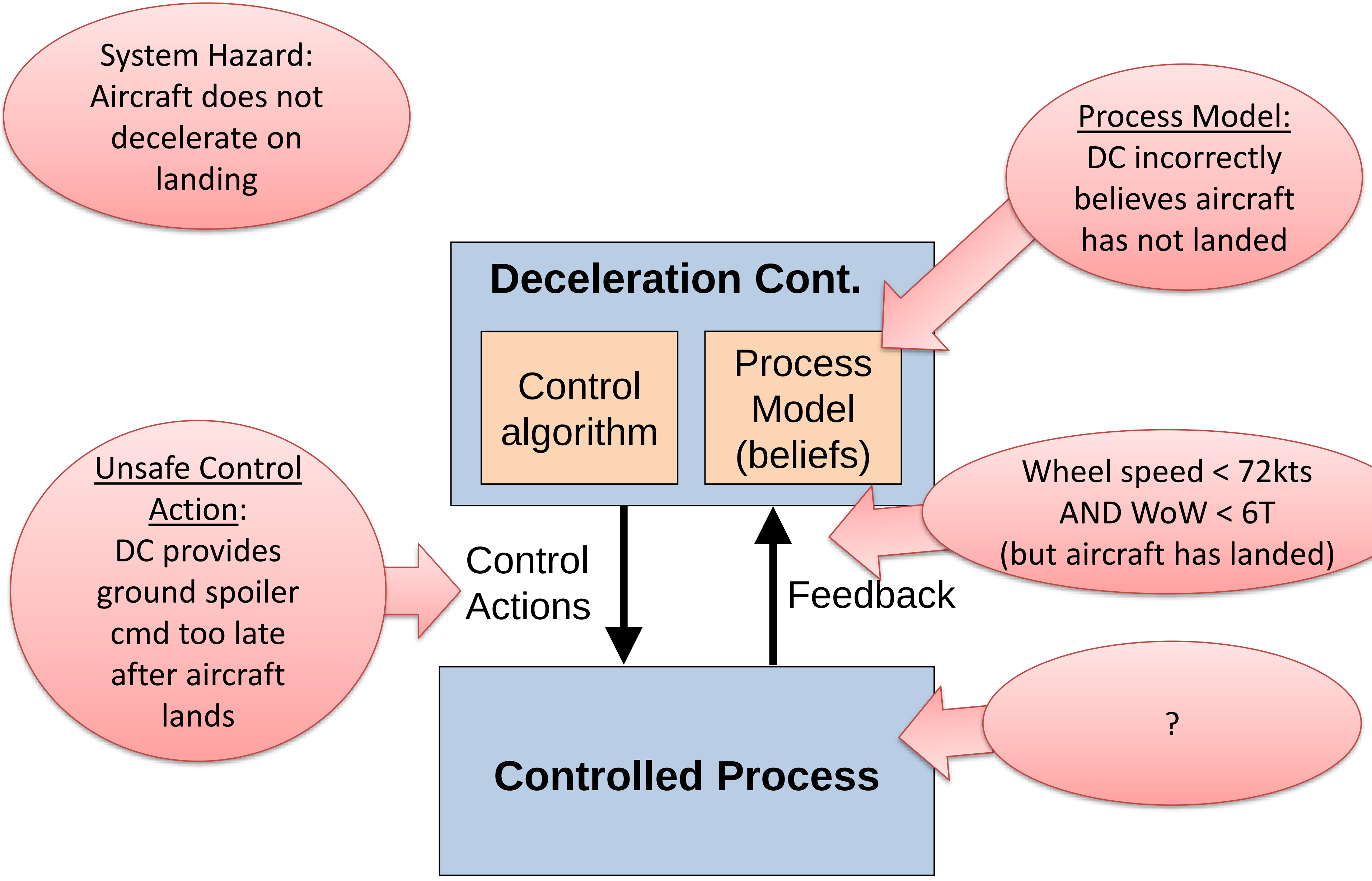


A320 Automation

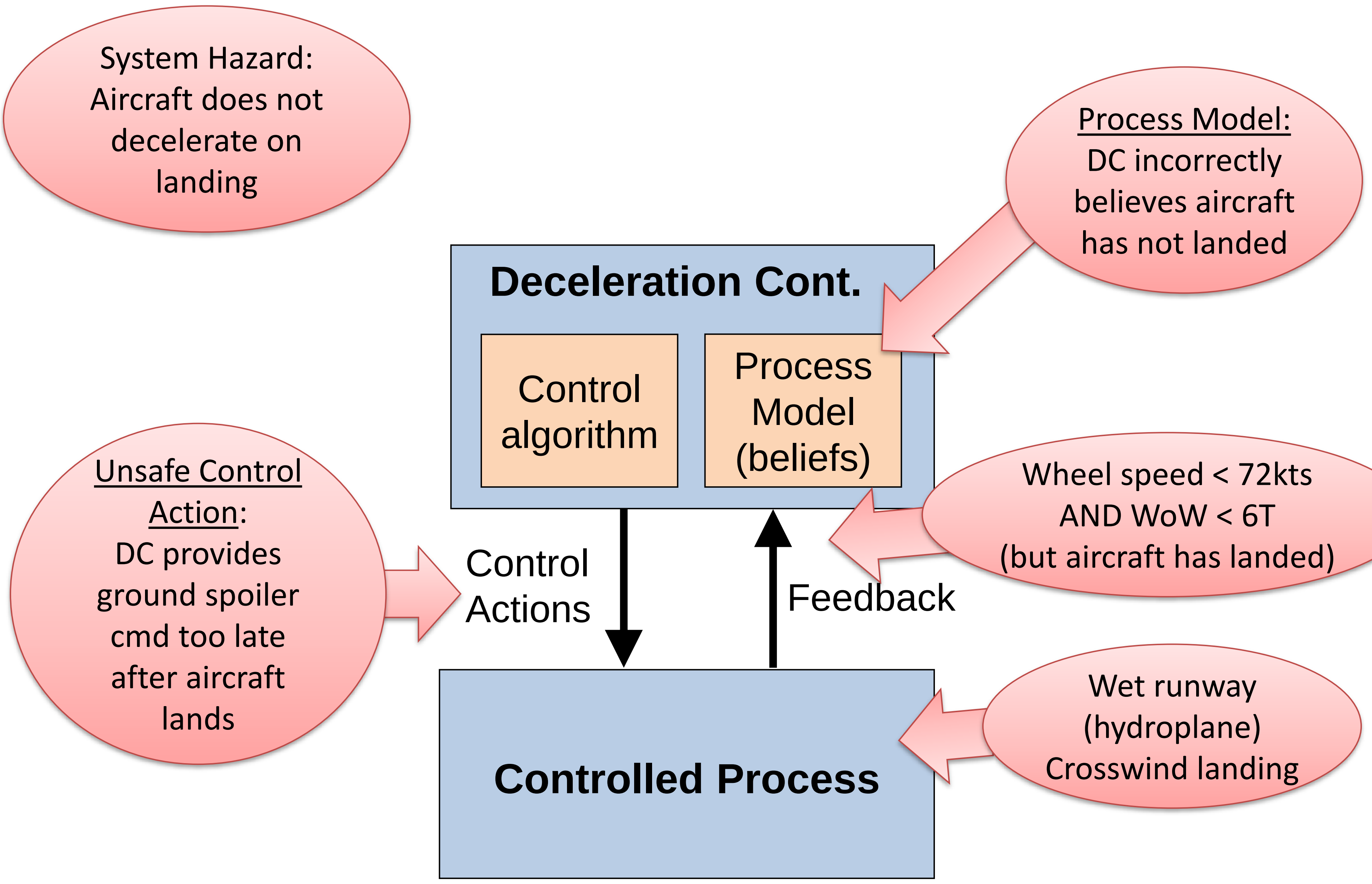
- Automation algorithm allows thrust reversers when:
  - At least 6.3 tons on each main landing gear strut
- Automation algorithm allows ground spoilers when:
  - At least 6.3 tons on each main landing gear strut

    OR
  - Wheel turning at least 72 knots
- Automation algorithm triggers wheel brake when:
  - Wheel turning at least 0.8 V_0 knots

Basic Control Loop



Basic Control Loop



Using STPA to ask questions

System Hazard: Aircraft does not decelerate on landing

Question: What DC control actions can cause aircraft to not decelerate on landing?

UCA: DC provides thrust reverse cmd too late after aircraft lands

Question: What DC beliefs would cause it to provide thrust reverse cmd too late?

PM: DC incorrectly believes aircraft has not landed

Deceleration Cont.

Control algorithm

Process Model (beliefs)

Question: What DC inputs would cause TRC to believe aircraft has not landed?

Wheel speed < 72kts
WoW < 6T
(but aircraft has landed)

Control Actions

Feedback

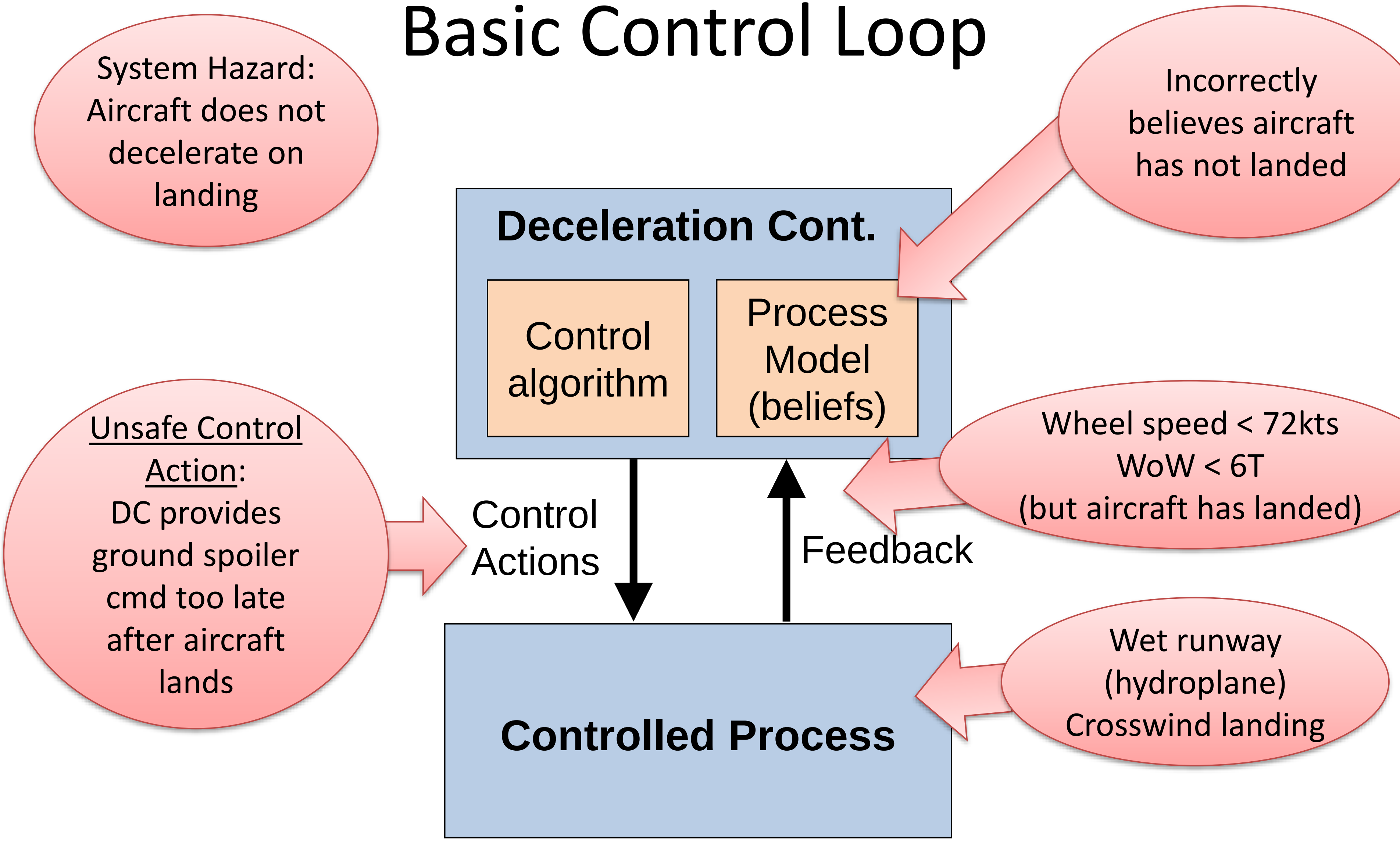
Question: What would cause WOW<6 and WS<72 when aircraft has really landed?

Controlled Process

Wet runway
(hydroplane)
Crosswind landing

John Thomas, 2019

Basic Control Loop



Could this be exploited by an adversary?

A320 Warsaw Crash

- Thrust reverser would not deploy on landing
- Automation prevented manual pilot override
- 9 seconds after touchdown, software allowed thrust reversers and spoilers to deploy
- 13 seconds after touchdown, software triggered wheel braking
- Plane overruns, crashes, catches fire

Sept 1993, Lufthansa 2904

Automation satisfied all component requirements! What went wrong?

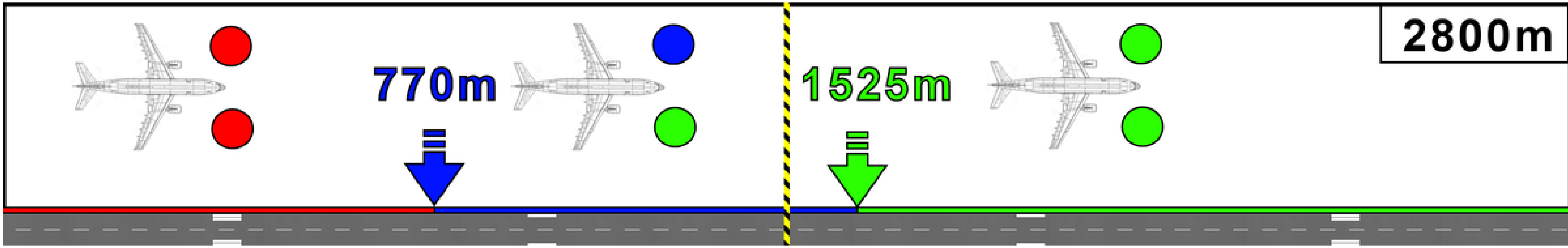
This accident is complex, many factors! See report for more info.

A320 Warsaw Crash

- Software algorithms to ensure aircraft has landed:
  - Must be 6.3 tons on each main landing gear strut
  - Wheel must be turning at least 72 knots
- Off-nominal landing conditions at Warsaw
  - Crosswind landing (one side first)
  - Wet runway: wheels hydroplane

Lufthansa 2904, Airbus A320

Each component operated without failure or deviation!



This accident is complex, many factors! See report for more info.

Wrap-up

STPA in Industry Standards

- ISO/PAS 21448: SOTIF: Safety of the Intended Functionality
  - STPA used assess safety of digital systems
- ASTM WK60748
  - "Standard Guide for Application of STPA to Aircraft"
- SAE AIR6913
  - "Using STPA during Development and Safety Assessment of Civil Aircraft"
- RTCA DO-356A
  - "Airworthiness Security Methods and Considerations"
  - STPA-sec used for cybersecurity of digital systems
- IEC 63187
  - "Functional safety - Framework for safety critical E/E/PE systems for defence industry applications"
- SAE J3187
  - "Recommended Practice for STPA in Automotive Safety Critical Systems"
- EPRI/Sandia
  - Recommending to use STPA for digital I&C

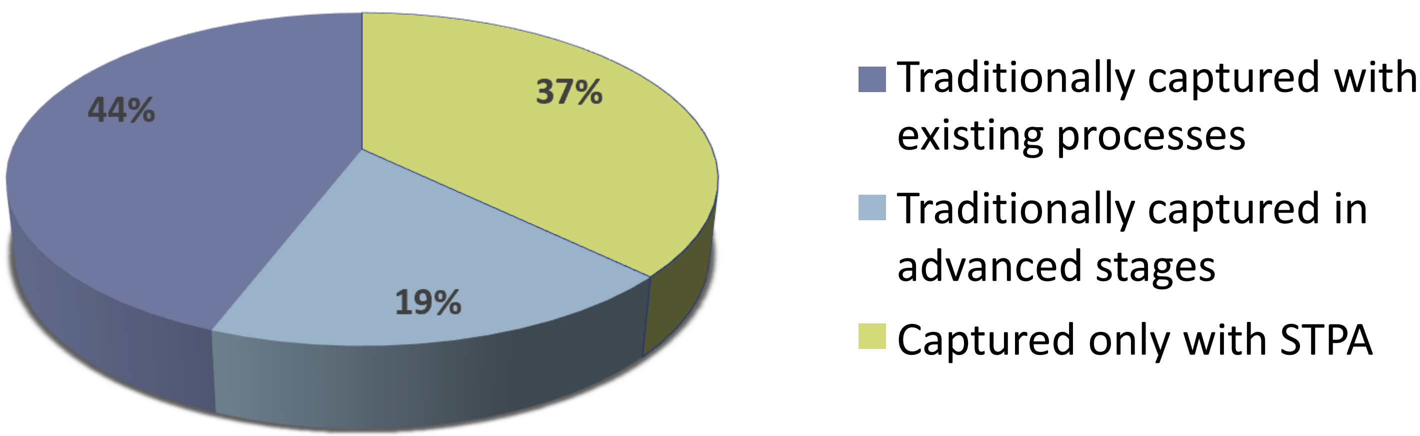
Regulatory Activity

- FAA internal certification training
- EASA application: means of compliance
- INTA (Spanish civil/military authority)
- CAAC / CAUC / MIT collaboration (Chinese authority)

Embraer STPA application

- 2016: Air Management System
  - Identified 200+ safety constraints (requirements) and 700+ design recommendations to eliminate or mitigate hazards (satisfy the safety constraints).

Embraer Aircraft Smoke Control System analysis



Boeing STPA-STAMP applications

- Future Vertical Lift (FVL) Mission system and Flight control system
- V-22 STPA New Production System requirements generation
- 777X St. Louis factory Automate Ground Vehicle (AGV) system
- 777 Wing body join STPA analysis (by MIT LGO graduate student)
- 777 Robotic system STPA
- Auburn Composite FAB center
- Boeing Radiation Effects Lab (BREL)
- Everett Delivery Center (control of aircraft hazardous energy (LOTO))
- BDS Commercial Crew (CCTS) Service Module Hot Fire Test
- Other development and cyber security projects with military customers
- Cathay Pacific has contributed their operational STPA analysis for flight deck development

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

Rolls-Royce

Sample of STPA use worldwide, all industries (incomplete, <10%)

STPA: The most popular approach you haven't tried?

Massachusetts Institute of Technology

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
BioPharmaceutical
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

Massachusetts Institute of Technology

STPA Common Mistakes

- Not getting properly educated in STPA
  - A short tutorial is not enough!

- 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”.

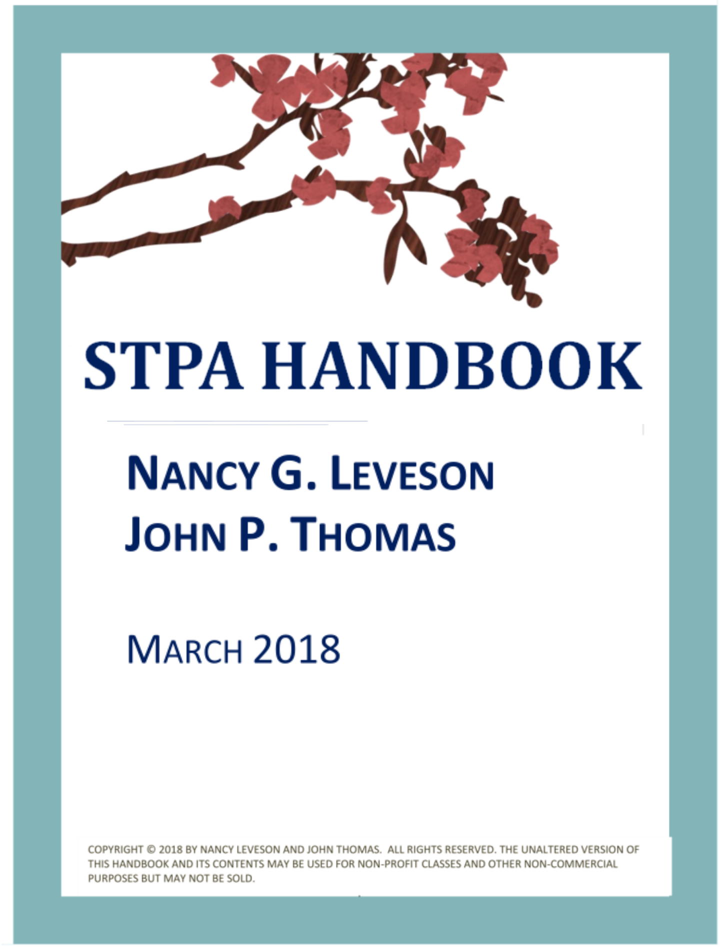
- Limiting STPA to a simple system or simple problem with obvious answers

For more information

- Google: “STPA Handbook”
  - How-to guide for practitioners applying STPA
- Website: mit.edu/psas

- Questions? Email me!

  JThomas4@mit.edu



LinkedIn

“John Thomas MIT”