Combined AAvPA and PACDEFF International Symposium 2018

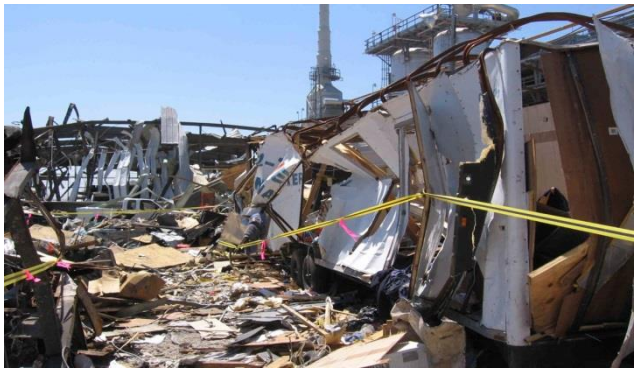


A Systems Approach to Human Factors Engineering

Nancy Leveson

Aeronautics and Astronautics
MIT





- You've carefully thought out all the angles
- You've done it a thousand times
- It comes naturally to you
- You know what you're doing, it's what you've been trained to do your whole life.
- Nothing could possibly go wrong, right?

Think Again.

The Problem

- Complexity is reaching a new level (tipping point) in modern systems
  - Old approaches becoming less effective
  - New causes of mishaps appearing (especially related to use of software and autonomy)
  - Human errors are changing
- Traditional analysis approaches do not provide the information necessary to prevent losses in these systems
- Engineers, psychologists, and human factors experts will need to work together.
  - But no common language
  - Need new approaches, new standards that design safety into systems from the beginning, including human operator requirements

General Definition of "Safety"

- Accident = 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.
  - Includes inadvertent and intentional losses (security)
- System goals vs. constraints (limits on how can achieve the goals)
- Safety: Absence of losses

Our current tools are all 40-65 years old but our technology is very different today

1940 1950 1960 1970 1980 1990 2000 2010 2020

FMEA

FTA

HAZOP

ETA

Bow Tie
(CCA)
FTA + ETA

- Introduction of computer control
- Exponential increases in complexity
- New technology
- Changes in human roles

Assumes accidents caused by component failures

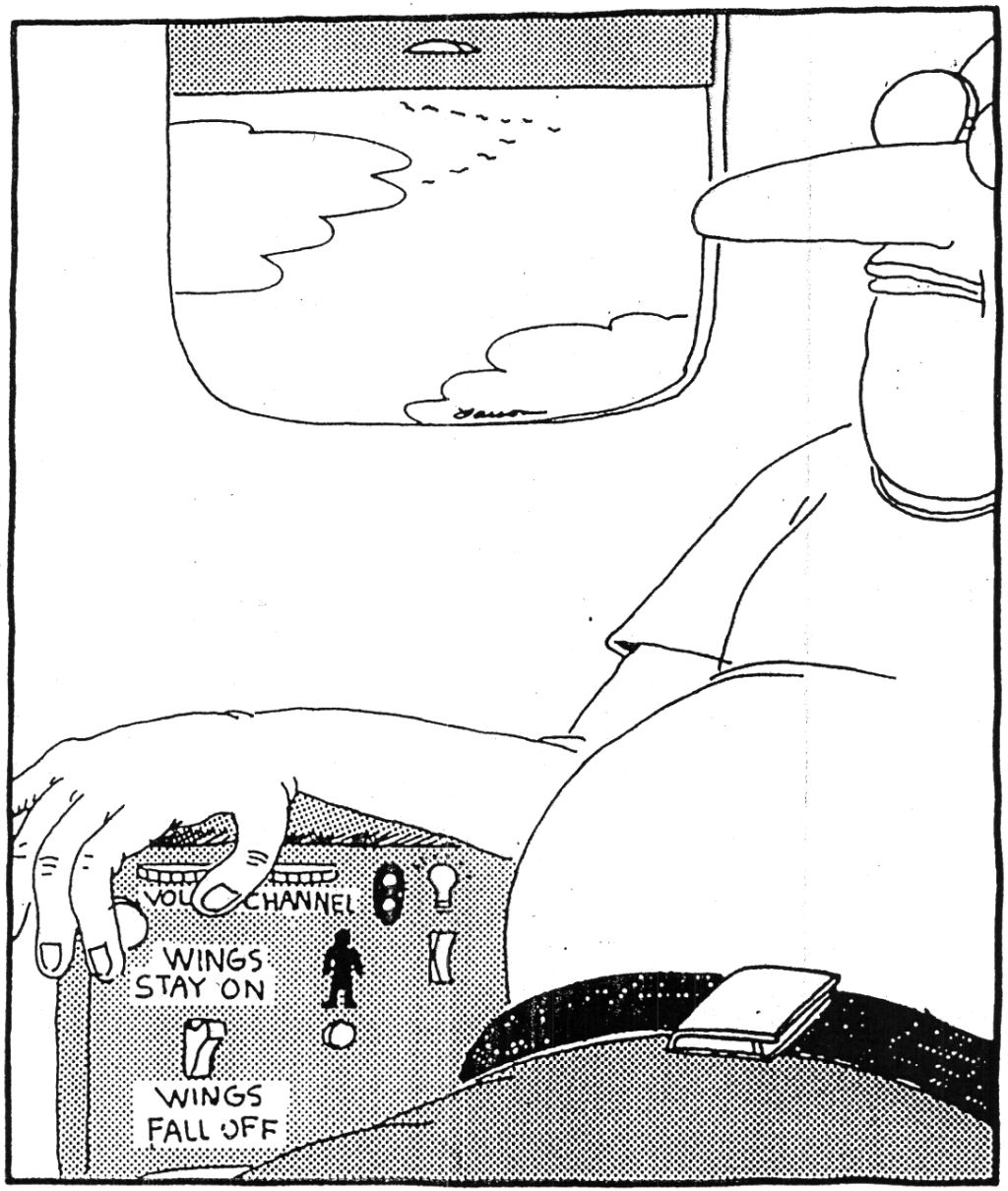
Software changes the role of humans in systems

Typical assumption is that operator error is cause of most incidents and accidents

- So do something about operator involved (admonish, fire, retrain them)
- Or do something about operators in general
  - Marginalize them by putting in more automation
  - Rigidify their work by creating more rules and procedures

"Cause" from the American Airlines B-757 accident report (in Cali, Columbia):

> "Failure of the flight crew to revert to basic radio navigation at the time when the FMS-assisted navigation became confusing and demanded an excessive workload in a critical phase of flight."



Fumbling for his recline button Ted unwittingly instigates a disaster

The New Systems View of Operator Error

- Operator error is a symptom, not a cause
- All behavior affected by context (system) in which occurs
  - Role of operators is changing in software-intensive systems as is the errors they make
  - Designing systems in which operator error inevitable and then blame accidents on operators rather than designers
- To do something about operator error, must look at system in which people work:
  - Design of equipment
  - Usefulness of procedures
  - Existence of goal conflicts and production pressures
- **Human error is a symptom of a system that needs to be redesigned**

Warsaw A320 Accident

- Software protects against activating thrust reversers when airborne
- Hydroplaning and other factors made the software not think the plane had landed
- Pilots could not activate the thrust reversers and ran off end of runway into a small hill.

Another Accident Involving Thrust Reversers

- Tu-204, Moscow, 2012
- Red Wings Airlines Flight 9268
- The soft 1.12g touchdown made runway contact a little later than usual.
- With the crosswind, this meant weight-on-wheels switches did not activate and the thrust-reverse system would not deploy.

An Accident Involving Thrust Reversers (2)

- Pilots believe the thrust reversers are deploying like they always do. With the limited runway space, they quickly engage high engine power to stop quicker. Instead this accelerated the Tu-204 forwards, eventually colliding with a highway embankment.

Another Accident Involving Thrust Reversers (2)

- Pilots believe the thrust reversers are deploying like they always do. With the limited runway space, they quickly engage high engine power to stop quicker. Instead this accelerates the Tu-204 forwards, eventually colliding with a highway embankment.

In complex systems, human and technical considerations cannot be isolated

Human factors concentrates on the “screen out”

Hardware/software engineering concentrates on the “screen in”

Not enough attention on integrated system as a whole

(e.g, mode confusion, situation awareness errors, inconsistent behavior, etc.

We Need Something New

- New levels of complexity, software, human factors do not fit into a reliability-oriented world.
- Two approaches being taken now:

Pretend there is no problem

Shoehorn new technology and new levels of complexity into old methods

Human Factors and Aircraft Risk Assessment Today (SAE ARP 4761)

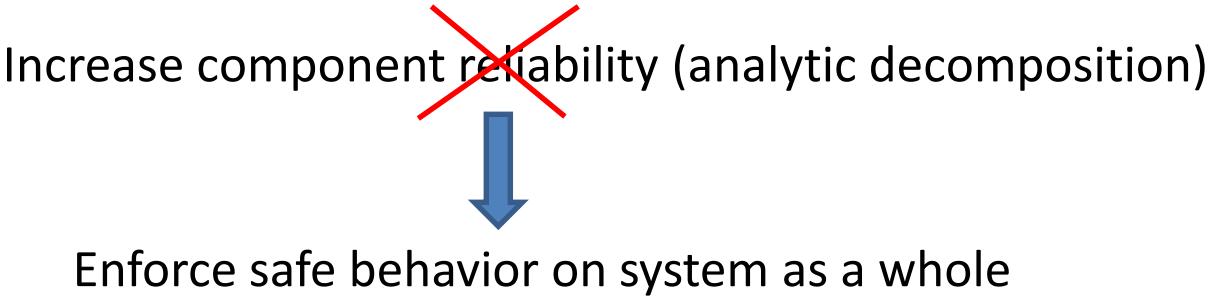
- FHA (Fault Tree analysis or FMEA or …)
  - Hardware and functions only
  - Based on probabilistic analysis
- Software handled separately
- Human factors handled separately

From SAE ARP 4761

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification
Decelerate Aircraft on the Ground	Loss of Deceleration Capability	Landing/ RTO/ Taxi		
	…	…	…	
	c. Unannunciated loss of deceleration capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resulting In low speed contact with terminal, aircraft, or vehicles	Major
	d. Annunciated loss of deceleration capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs	No Safety Effect

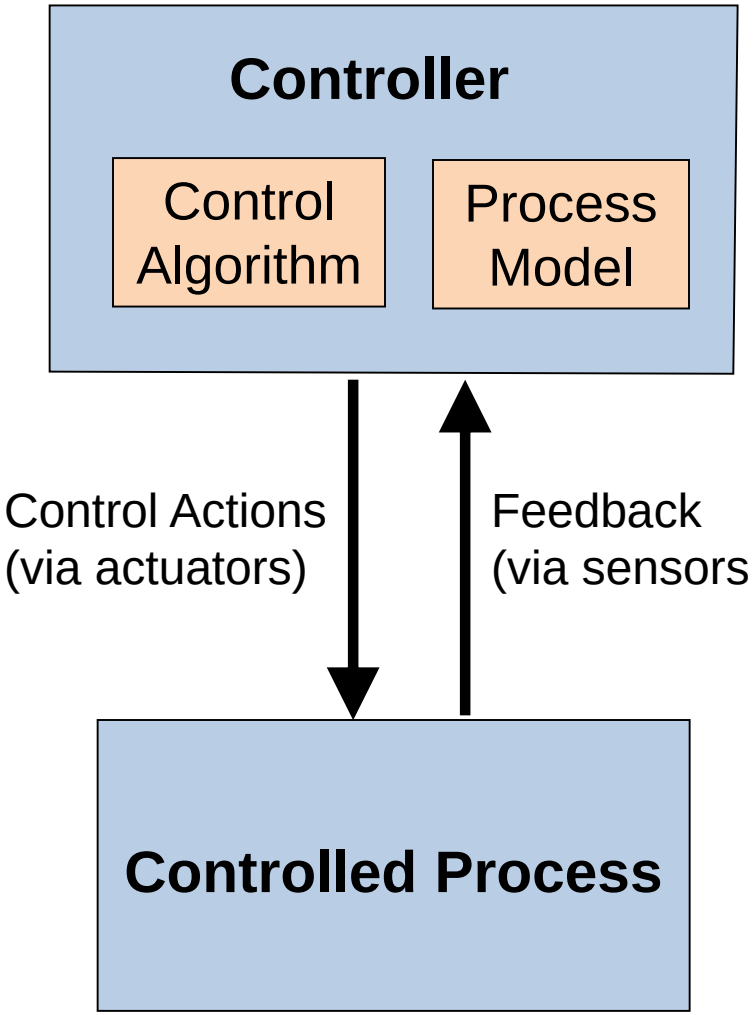
A Possible Solution

- Perform analysis on models that include humans, software, hardware
- Stop confusing component reliability and safety



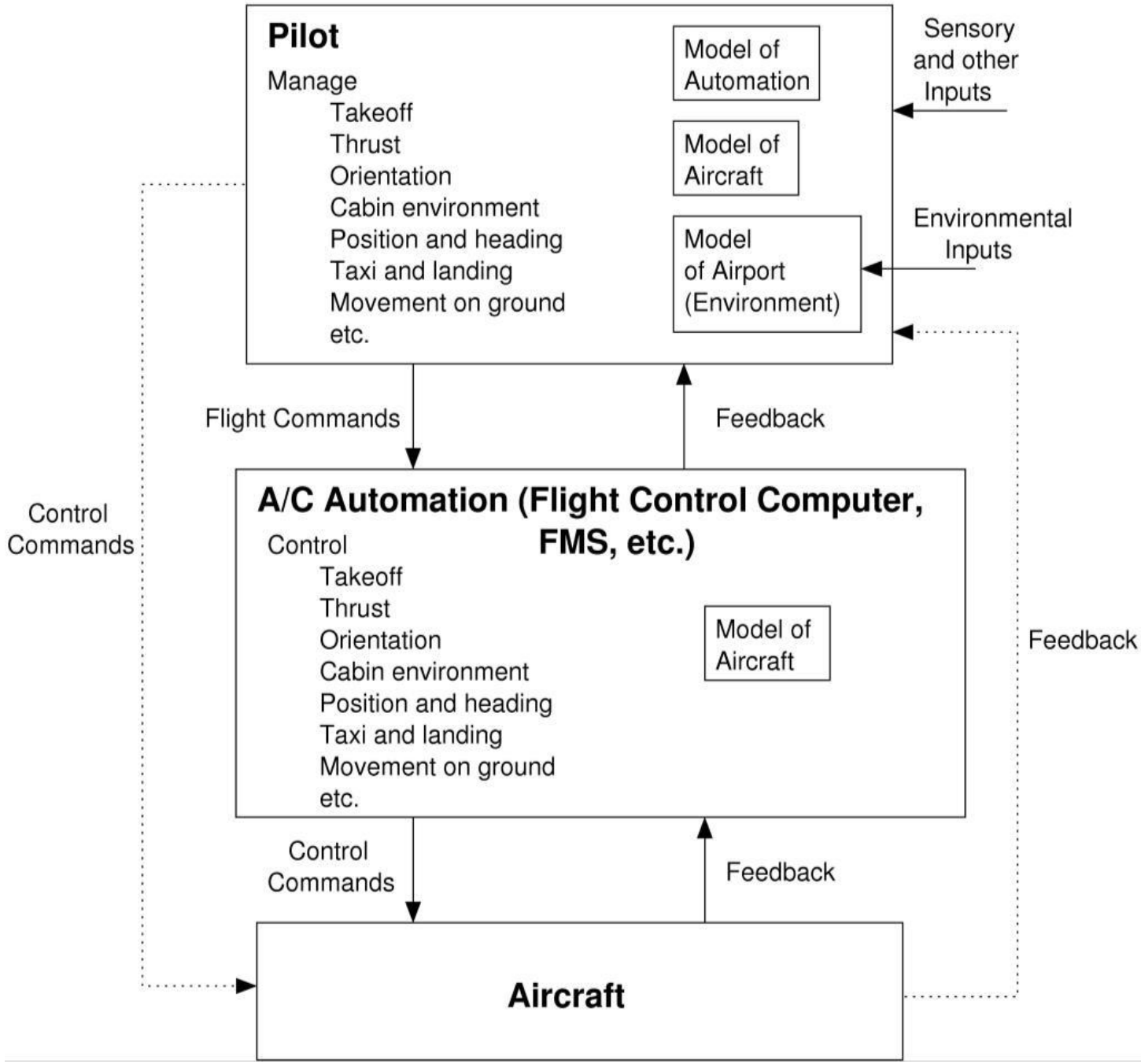
- Acknowledge increased complexity and other changes in engineering today
  - Accidents no longer can be understood as a chain of failure events
  - Need a holistic view of systemic factors in accidents

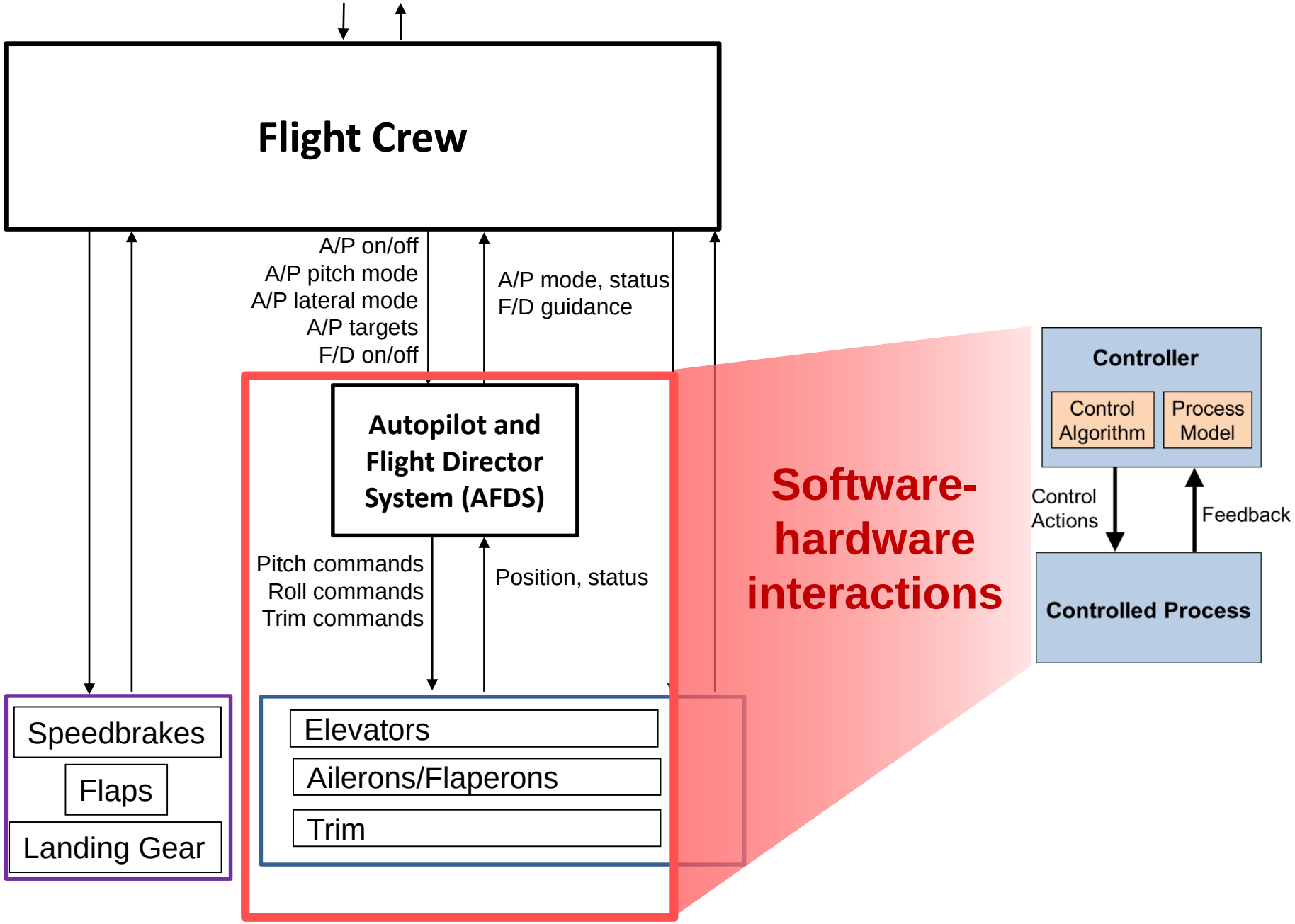
Models Constructed from Feedback Control Loops



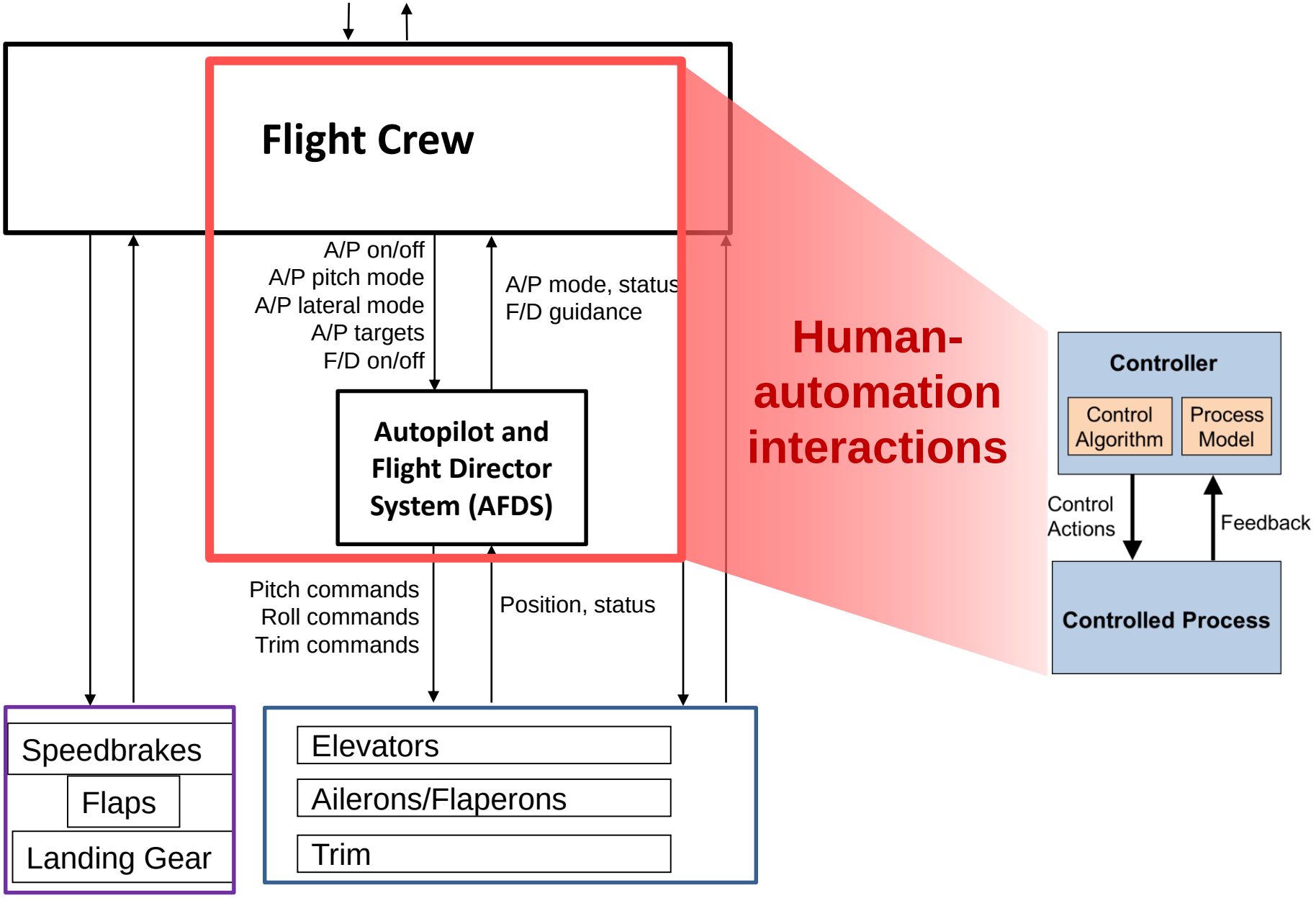
- Controllers use a **process model** to determine control actions
- Software/human related accidents often occur when the process model is incorrect
- Captures software errors, human errors, flawed requirements …

Treat safety as a control problem, not a failure problem

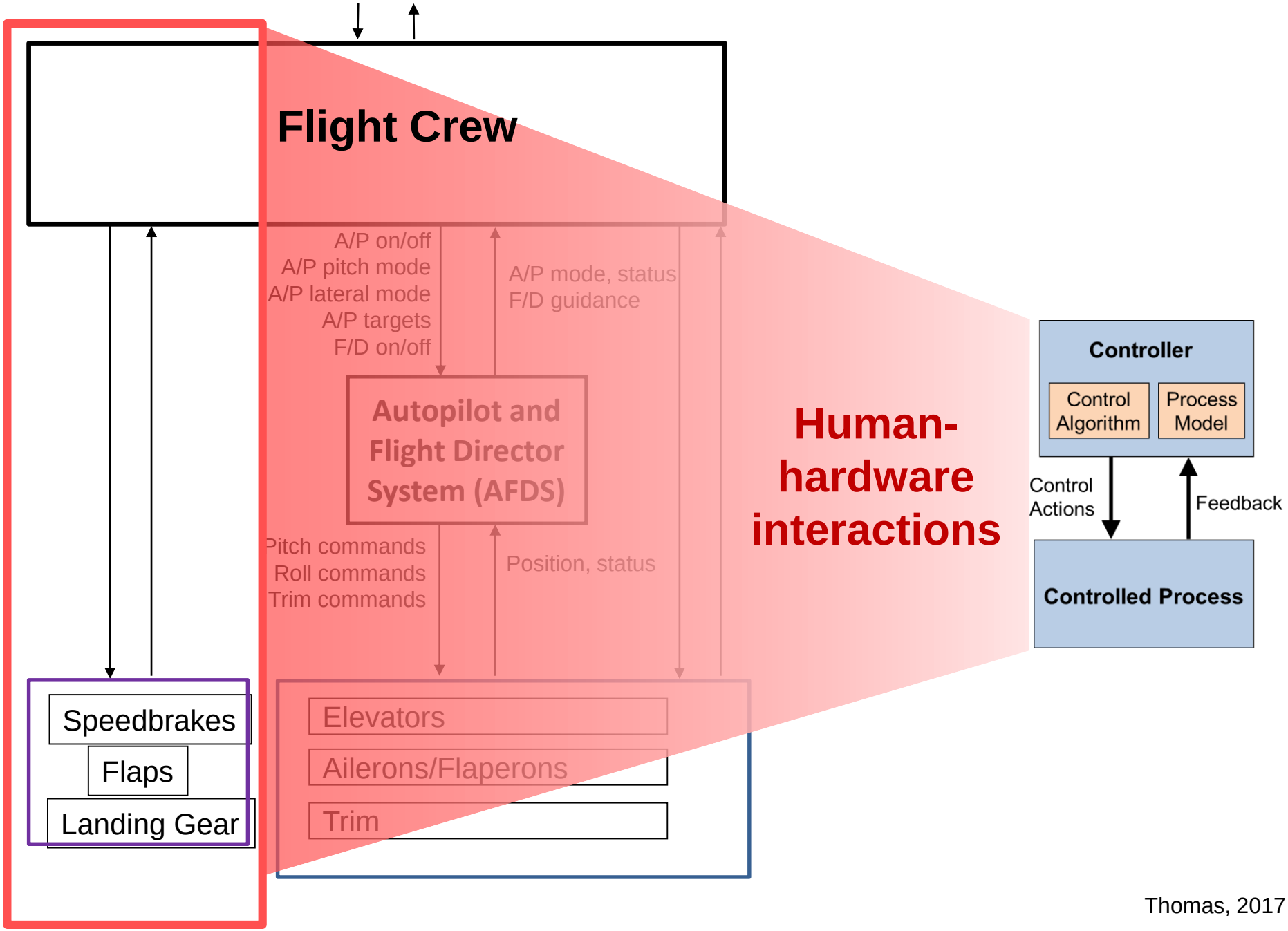

Pilot
Manage
Takeoff
Thrust
Orientation
Cabin environment
Position and heading
Taxi and landing
Movement on ground
etc.
Model of Automation
Model of Aircraft
Model of Airport (Environment)
Sensory and other Inputs
Environmental Inputs
Flight Commands
Feedback
A/C Automation (Flight Control Computer, FMS, etc.)
Control
Takeoff
Thrust
Orientation
Cabin environment
Position and heading
Taxi and landing
Movement on ground
etc.
Model of Aircraft
Control Commands
Feedback
Control Commands
Feedback
Aircraft


Flight Crew
A/P on/off
A/P pitch mode
A/P lateral mode
A/P targets
F/D on/off
A/P mode, status
F/D guidance
Autopilot and Flight Director System (AFDS)
Pitch commands
Roll commands
Trim commands
Position, status
Speedbrakes
Flaps
Landing Gear
Elevators
Ailerons/Flaperons
Trim
Software-hardware interactions
Controller
Control Algorithm
Process Model
Control Actions
Feedback
Controlled Process

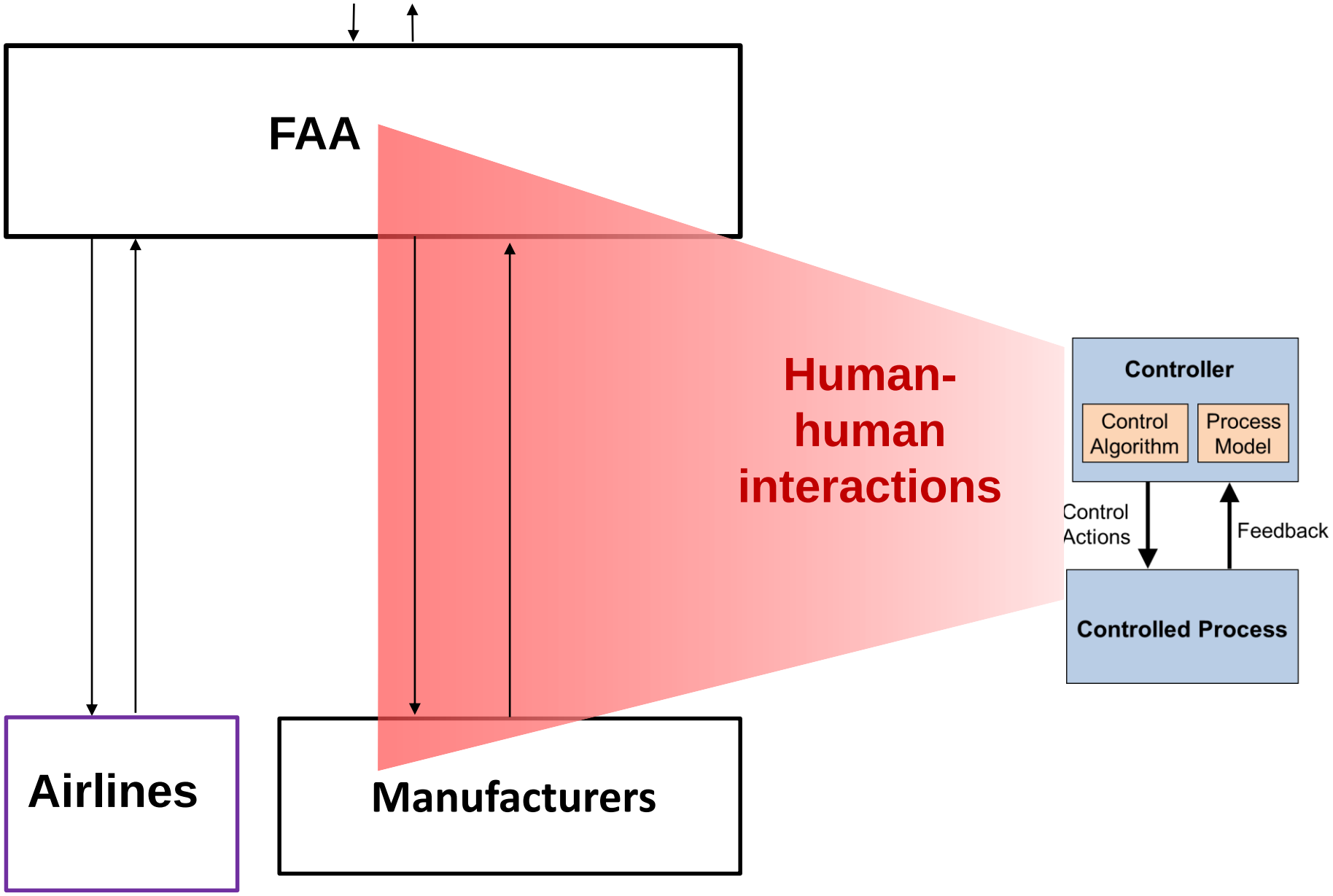
Thomas, 2017


Flight Crew
A/P on/off
A/P pitch mode
A/P lateral mode
A/P targets
F/D on/off
A/P mode, status
F/D guidance
Autopilot and Flight Director System (AFDS)
Pitch commands
Roll commands
Trim commands
Position, status
Speedbrakes
Flaps
Landing Gear
Elevators
Ailerons/Flaperons
Trim
Human-automation interactions
Controller
Control Algorithm
Process Model
Control Actions
Feedback
Controlled Process

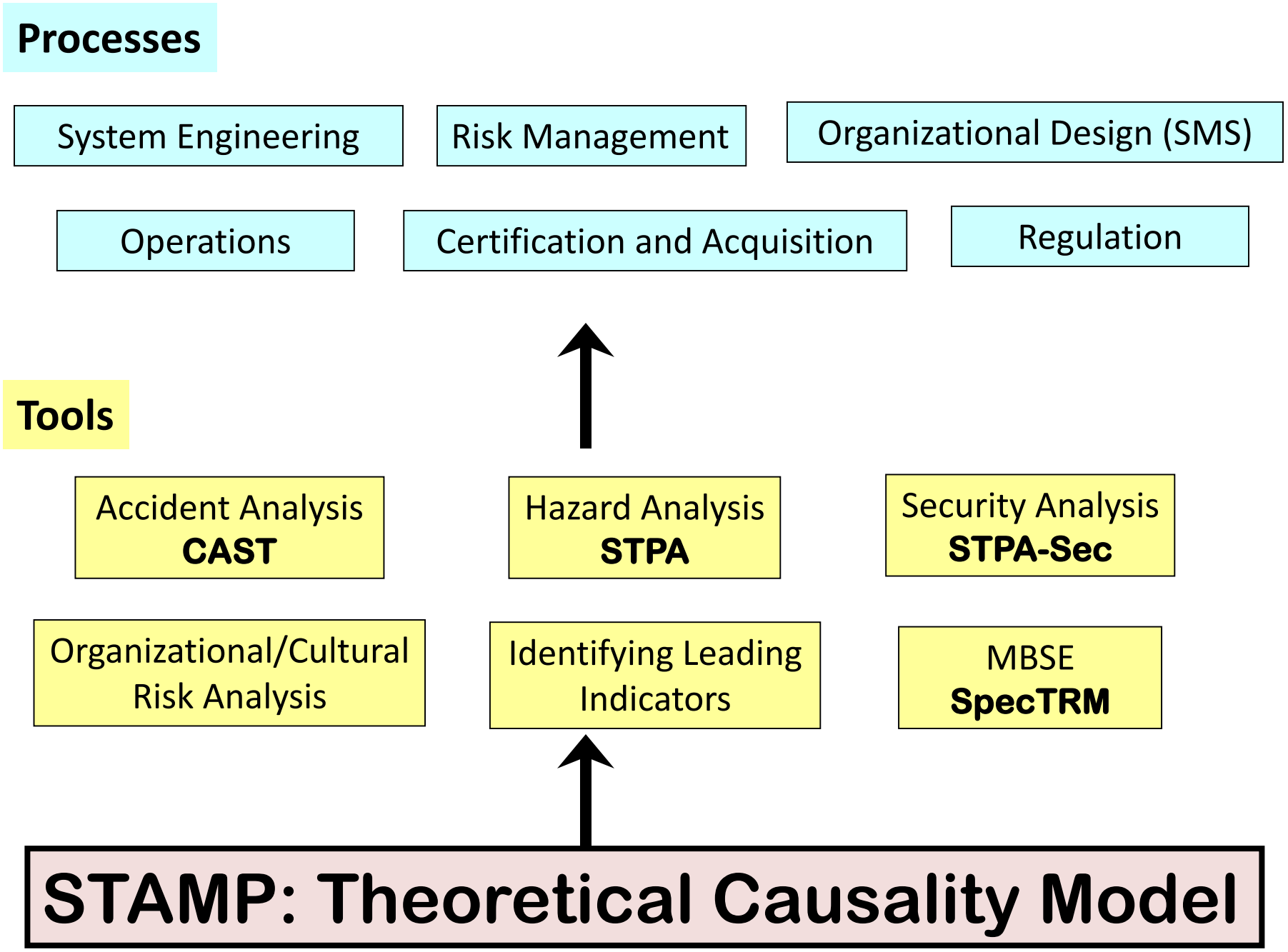
Thomas, 2017


Flight Crew
A/P on/off
A/P pitch mode
A/P lateral mode
A/P targets
F/D on/off
A/P mode, status
F/D guidance
Autopilot and Flight Director System (AFDS)
Pitch commands
Roll commands
Trim commands
Position, status
Speedbrakes
Flaps
Landing Gear
Elevators
Ailerons/Flaperons
Trim
Human-hardware interactions
Controller
Control Algorithm
Process Model
Control Actions
Feedback
Controlled Process

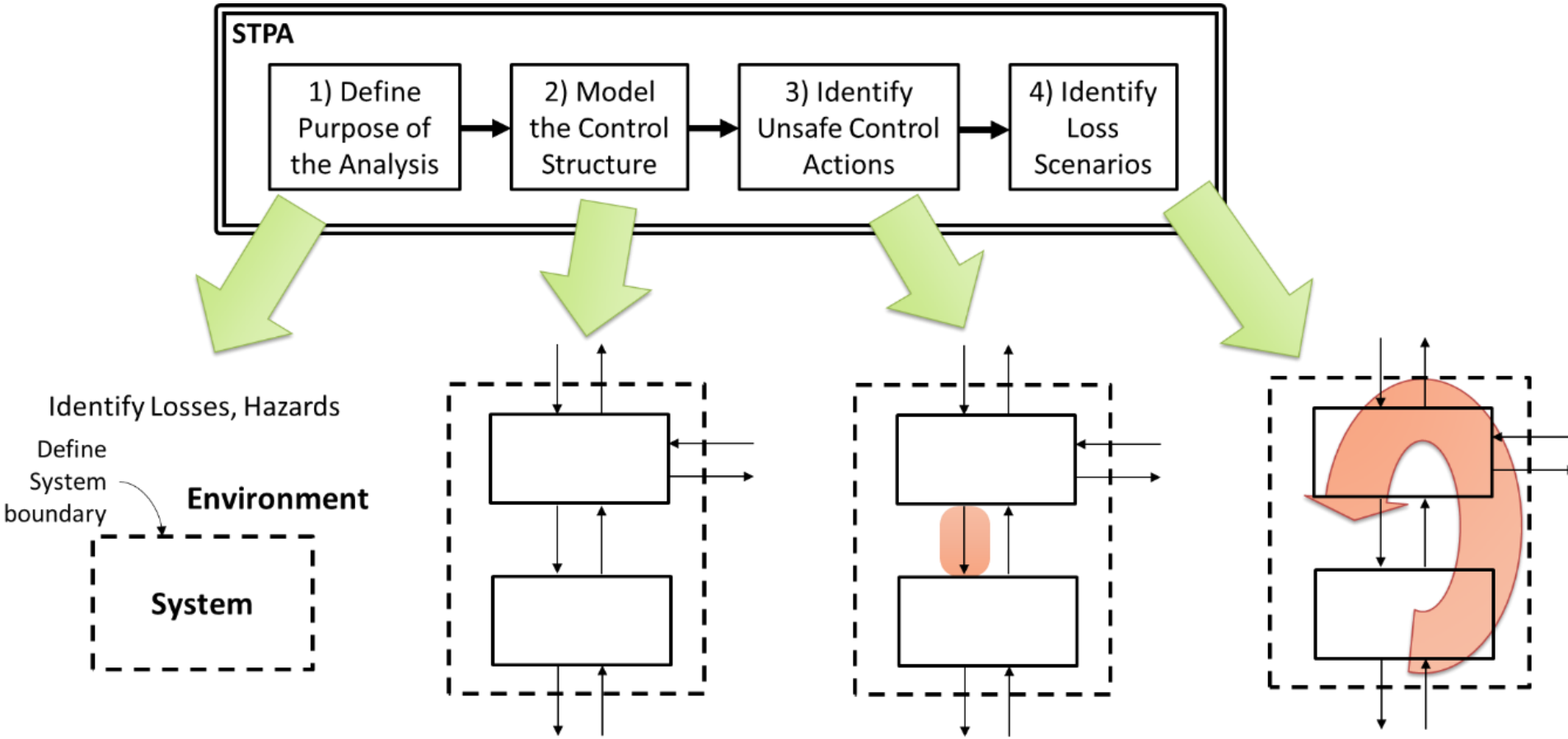
Thomas, 2017


FAA
Human-human interactions
Controller
Control Algorithm
Process Model
Control Actions
Feedback
Controlled Process
Airlines
Manufacturers

Thomas, 2017


Processes
System Engineering
Risk Management
Organizational Design (SMS)
Operations
Certification and Acquisition
Regulation
Tools
Accident Analysis
CAST
Hazard Analysis
STPA
Security Analysis
STPA-Sec
Organizational/Cultural
Risk Analysis
Identifying Leading
Indicators
MBSE
SpecTRM
STAMP: Theoretical Causality Model

STPA (System Theoretic Process Analysis)



Establish Analysis Goals (Stakeholders)

- **Identify losses to be considered**

  L1. Death or serious injury to aircraft passengers or people in the area of the aircraft

  L2. “Unacceptable” damage to the aircraft or objects outside the aircraft

  L3: Financial losses resulting from delayed operations

  L4: Reduced profit due to damage to aircraft or airline reputation

- **Identify System-Level Hazards**

  H1: Insufficient thrust to maintain controlled flight

  H2: Loss of airframe integrity

  H3: Controlled flight into terrain

  H4: An aircraft on the ground comes too close to moving or stationary objects or inadvertently leaves the taxiway

  H5: etc.

Deceleration Hazards (H4)

H4-1: Inadequate aircraft deceleration upon landing, rejected takeoff, or taxiing

H4-2: Deceleration after the V1 point during takeoff

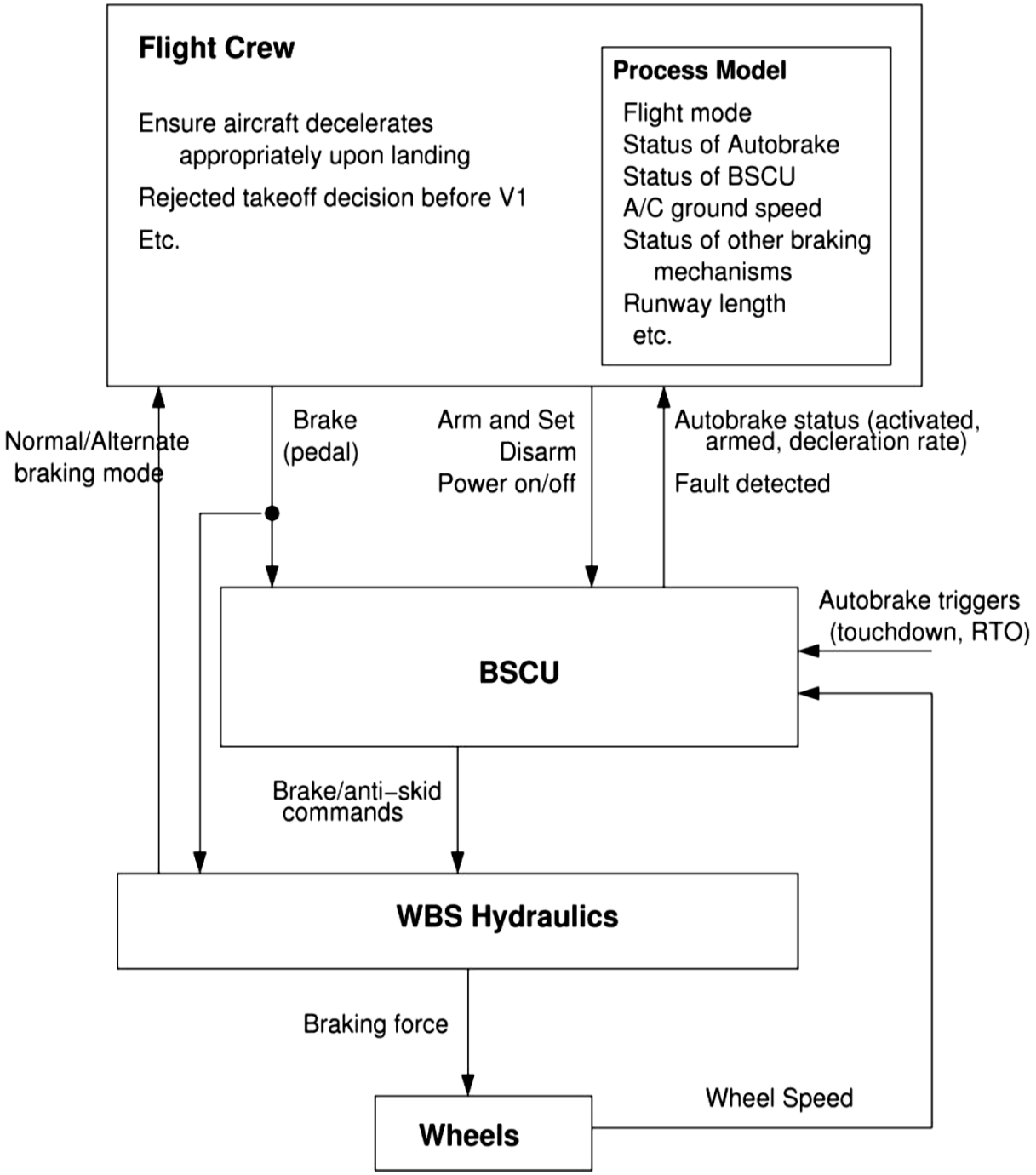
H4-3: Aircraft motion when the aircraft is parked

H4-4: Unintentional aircraft directional control (differential braking)

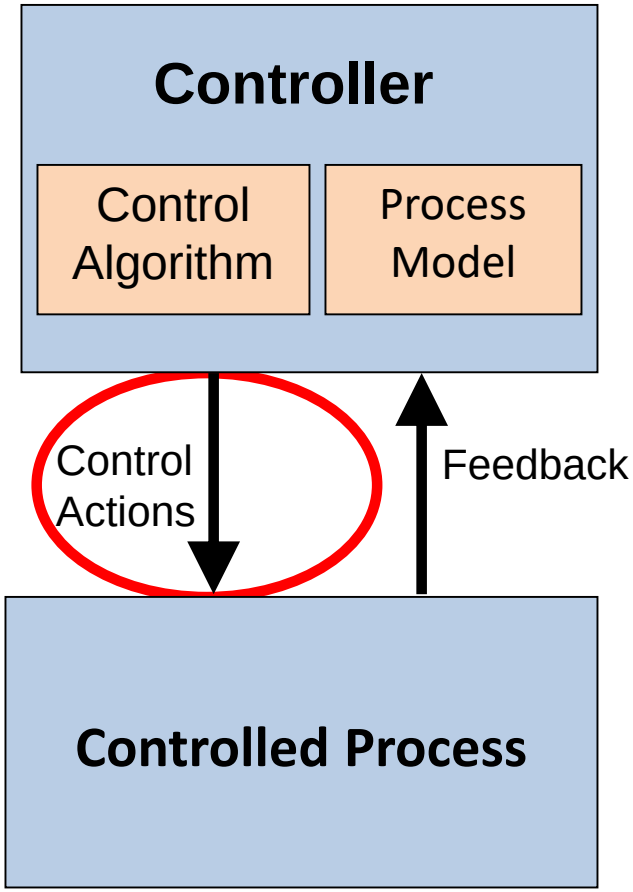
H4-5: Aircraft maneuvers out of safe regions (taxiways, runways, terminal gates, ramps, etc.)

H4-6: Main gear wheel rotation is not stopped when (continues after) the landing gear is retracted

Wheel Braking System Control Structure



Unsafe Control Actions



Four types of unsafe control actions

1) Control commands required for safety are not given
2) Unsafe commands are given
3) Potentially safe commands but given too early, too late, or in wrong order
4) Control action stops too soon or applied too long (continuous control)

Analysis:

1. Identify potential unsafe control actions
2. Identify why they might be given
3. If safe ones provided, then why not followed?

Unsafe Control Actions for Crew (Context Table)

Control Action By Flight Crew:	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
CREW.1 Manual braking via brake pedals	CREW.1a1 Crew does not provide manual braking during landing, RTO, or taxiing **when Autobrake is not providing braking (or insufficient braking),** leading to overshoot [H4-1, H4-5]	CREW.1b1 Manual braking provided with **insufficient pedal pressure,** resulting inadequate deceleration during landing [H4-1, H4-5]	CREW.1c1 Manual braking applied **before touchdown** causes wheel lockup, loss of control, tire burst [H4-1, H4-5]	CREW.1d1 Manual braking command is **stopped before safe taxi speed (TBD) is reached,** resulting in overspeed or overshoot [H4-1, H4-5]

Unsafe Control Actions by Autobraking

Control Action by BSCU	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
BSCU.1 Brake command	BSCU.1a1 Brake command not provided **during RTO (to V1)**, resulting in inability to stop within available runway length [H4-1, H4-5]	BSCU.1b1 Braking commanded excessively **during landing roll**, resulting in rapid deceleration, loss of control, occupant injury [H4-1, H4-5]	BSCU.1c1 Braking commanded **before touchdown**, resulting in tire burst, loss of control, injury, other damage [H4-1, H4-5]	BSCU.1d1 Brake command stops **during landing roll before taxi speed attained**, causing reduced deceleration [H4-1, H4-5]

Generate Potential Causal Scenarios

BSCU.1a2: Brake command not provided during landing roll, resulting in insufficient deceleration and potential overshoot

Scenario 1: Autobrake believes the desired deceleration rate has already been achieved or exceeded (incorrect process model). The reasons Autobrake may have this process model flaw include:

- If wheel speed feedback influences the deceleration rate determined by the Autobrake controller, inadequate wheel speed feedback may cause this scenario. Rapid pulses in the feedback (e.g. wet runway, brakes pulsed by anti-skid) could make the actual aircraft speed difficult to detect and an incorrect aircraft speed might be assumed.
- Inadequate external speed/deceleration feedback could explain the incorrect Autobrake process model (e.g. inertial reference drift, calibration issues, sensor failure, etc.)
- [Security related scenarios, e.g., intruder changes process model]

Possible Requirement for S1: Provide additional feedback to Autobrake to detect aircraft deceleration rate in the event of wheel slipping (e.g. fusion of multiple sensors)

UNSAFE CONTROL ACTION – CREW.1a1: Crew does not provide manual braking when there is no Autobraking and braking is necessary to prevent H4-1 and H4-5.

Scenario 1: Crew incorrectly believes that the Autobrake is armed and expect the Autobrake to engage (process model flaw)

Reasons that their process model could be flawed include:

- The crew previously armed Autobrake and does not know it later became unavailable

AND/OR

- The crew is notified that the Autobrake controller is still armed and ready, because the Autobrake controller does not detect when the BSCU has detected a fault. When the BSCU detects a fault it closes the green shut-off valve (making Autobrake commands ineffective), but the Autobrake system does not know about it or knows and does not notify the crew.

AND/OR

- The crew cannot process feedback due to multiple messages, conflicting messages, alarm fatigue, etc.
- …

Possible new requirements for S1: The BSCU hydraulic controller must provide feedback to the Autobrake when it has detected a fault and the Autobrake must disengage (and provide feedback to crew).

Other requirements may be generated from a human factors analysis of the ability of the crew to process the feedback under various worst-case conditions.

STPA Extension to (Better) Handle Human Factors

Megan France

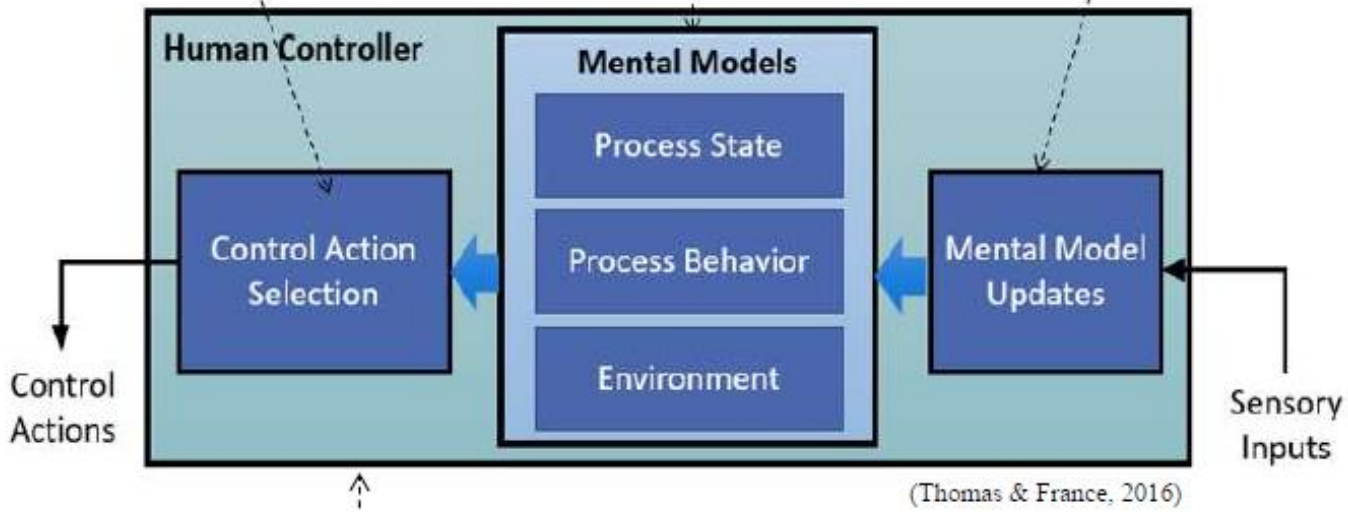
Dr. John Thomas

A NEW MODEL FOR HUMAN CONTROLLERS

Captures the controller's goals and how decisions are made based on the mental models

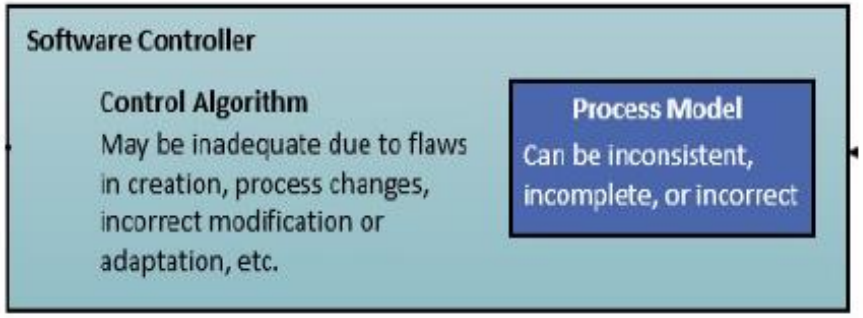
Captures specific types of flaws in the way the human controller conceptualizes the system and environment

Captures the influence of human experiences, and expectations on the processing of sensory input

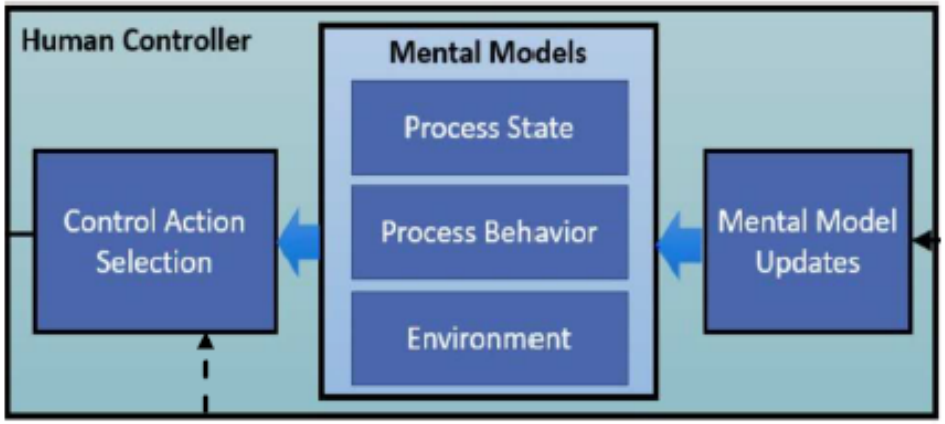


(Thomas & France, 2016)

Provides an alternative to the existing controller model which is better suited for software controllers



CONTROL ACTION SELECTION



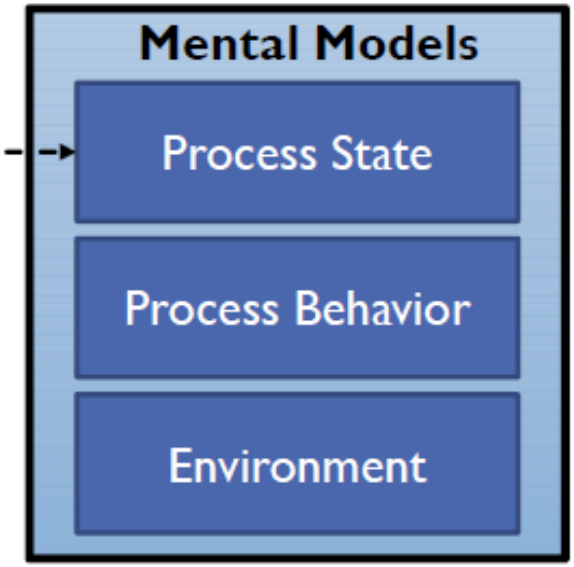
How did the operator choose which control action to perform?

Control Action Selection

- What were the operator's goals?
- What alternatives was the operator choosing between?
- How automatic or novel was the behavior?
- How might the operator's mental models affect their decision?
- What external factors (*eg. time pressure*) might affect their decision?

MENTAL MODELS

"Small-scale models of external reality"
– Kenneth Craik, 1943



Mental models are ***partial representations.***

- *Information may be purposefully omitted*
- *"Unknowns" may be known or unknown*
- *Information may be incorrect or outdated*

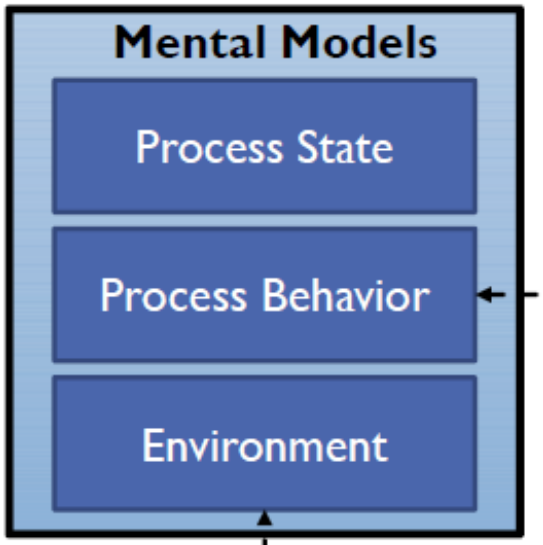
What does the operator believe about the system?

Mental Model of Process State

- Beliefs about modes and mode changes
- Believes about the current process stage, for processes with multiple stages
- Beliefs about system variables (eg. true/false)

MENTAL MODELS

What does the operator believe about the system?



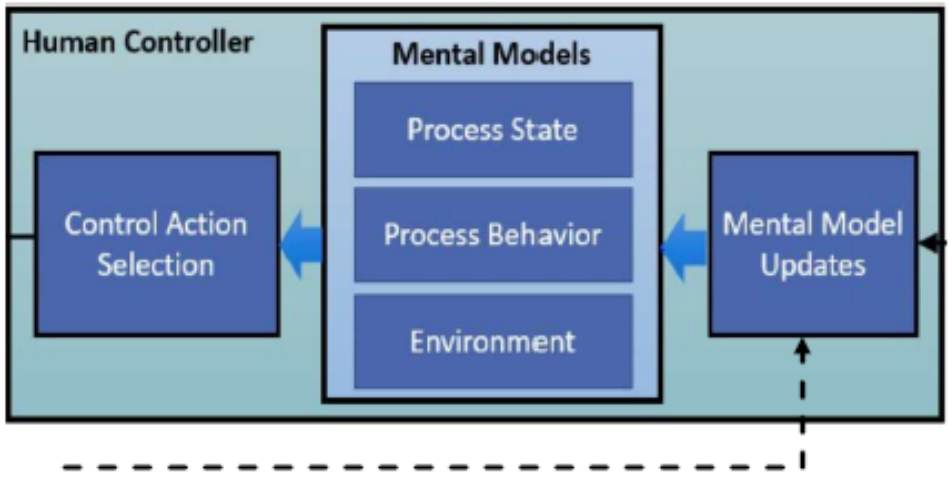
Mental Model of Process Behavior

- Beliefs about what the system can do
- Beliefs about how the system will behave in a particular mode or stage of operation
- Beliefs about if-then relationships between operator input and system output

Mental Model of the Environment

- Changes in environmental conditions
- Familiar or unfamiliar environments
- State and behavior of other controllers
- Social and organizational relationships

MENTAL MODEL UPDATES

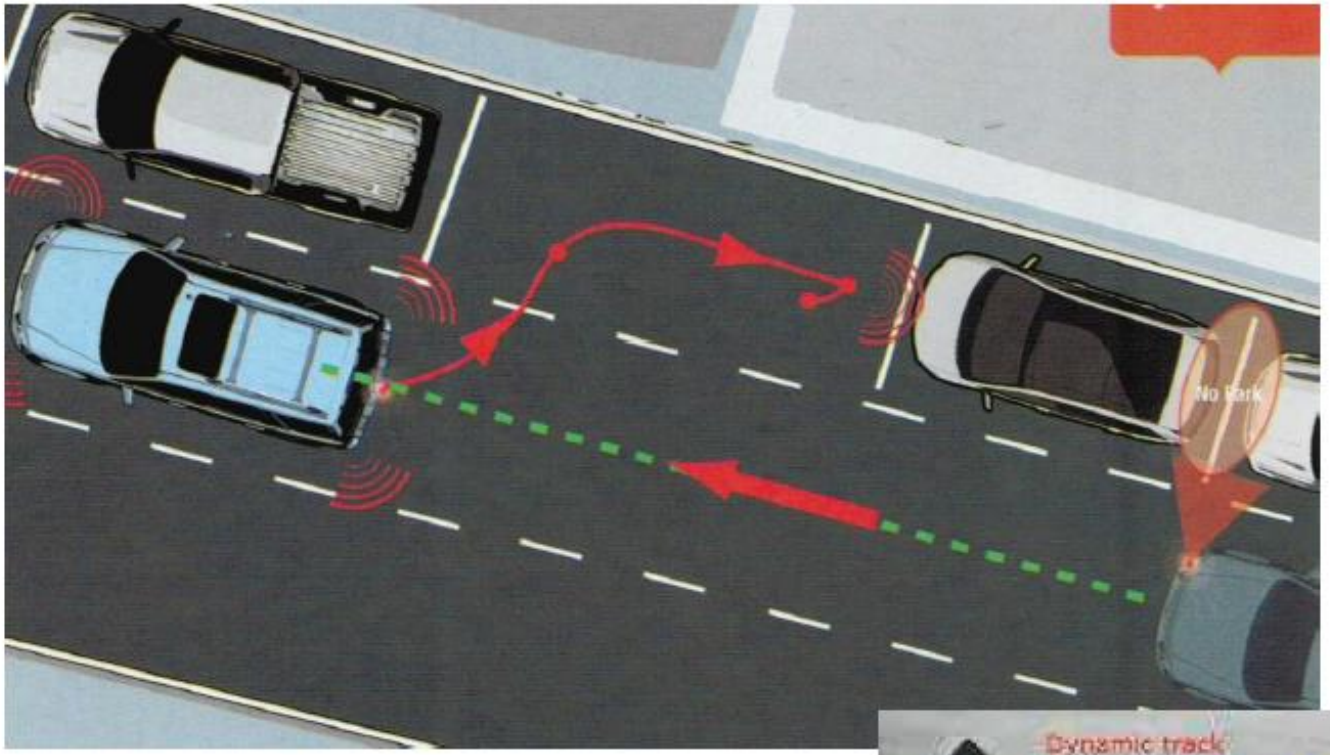


How did the operator come to have their current beliefs?

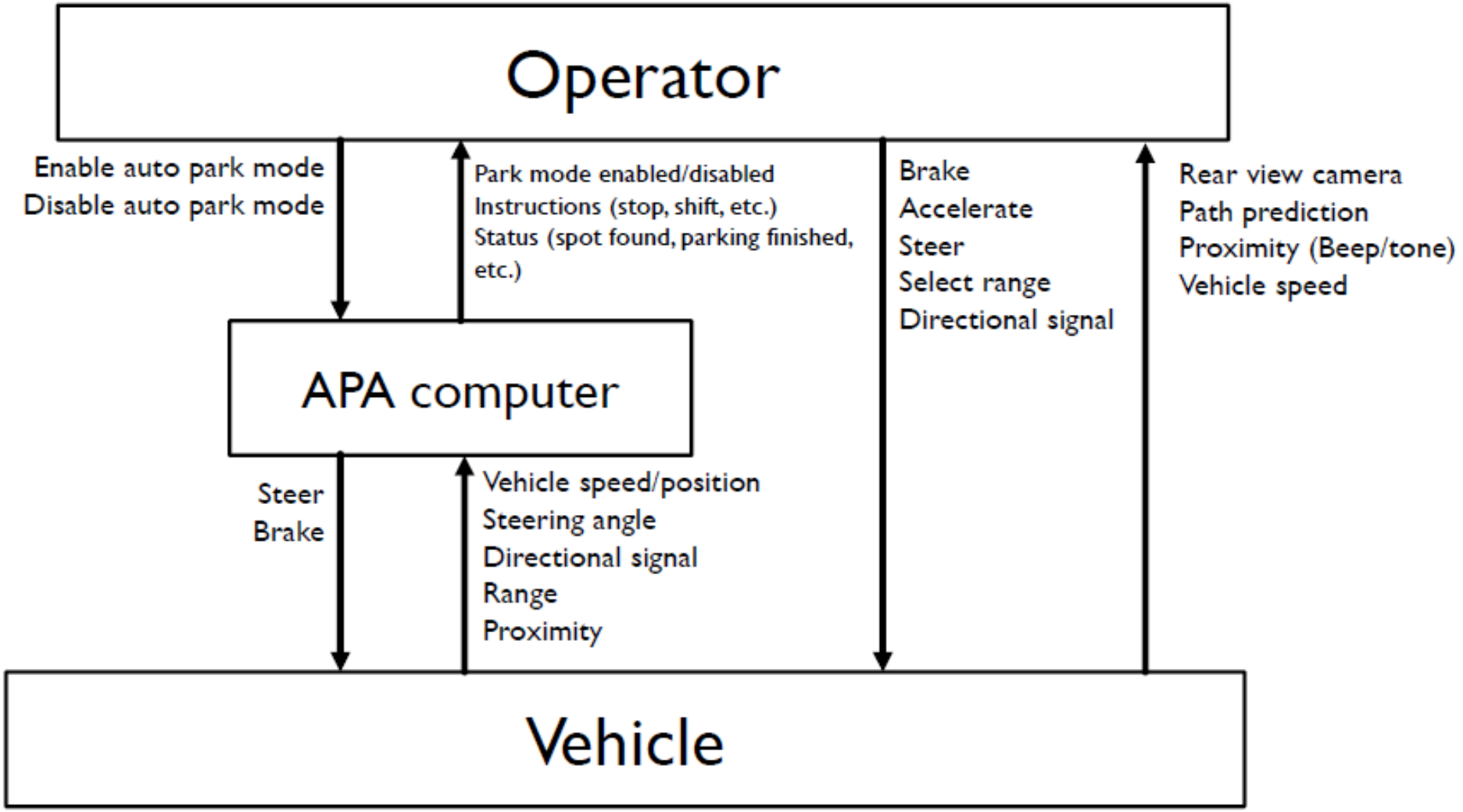
Mental Model Updates (and Initial Formation!)

- Consider initial formation of mental model vs. later updates
- Consider non-feedback inputs such as training programs and documentation
- Consider whether input/feedback was observed (*salience, expectations*)
- Consider whether input/feedback was correctly perceived & interpreted

AUTOMATED PARKING



HIGH-LEVEL CONTROL STRUCTURE



Key Assumptions about System Design

- The automation is capable of steering, braking, shifting gears, and accelerating
- The driver is expected to monitor the system to respond to unexpected events and obstacles
- The driver may temporarily override the APA computer's actions by braking or accelerating for short periods of time
- Automation is fully disabled if driver
  - Grabs the wheel
  - Accelerates above a given maximum speed
  - Brakes for more than 2 seconds
  - Or presses the APA button

UNSAFE CONTROL ACTIONS

Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/ Order**	**Stopped Too Soon / Applied Too Long**
Brake (Driver)	UCA 2b-33: Driver does not brake when APA is disabled and the vehicle is on a collision path. [H-1] UCA 2b-34: Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle. [H-1]	UCA 2b-35: Driver provides insufficient brake command when APA computer does not react appropriately to the obstacle. [H-1] UCA 2b-36: Driver provides too much brake when doing so puts other traffic on collision course or causes passenger injury. [H-2]	UCA 2b-37: Driver waits too long to brake after the automation does not react appropriately to an obstacle. [H-1] UCA 2b-38: Driver brakes too early before braking is needed, putting the vehicle on a collision path. [H-1]	UCA 2b-39: Driver continues override braking for too long and disables automation when doing so puts the vehicle on a collision path. [H-1] UCA 2b-40: Driver does not brake for long enough to avoid collision when automation is not reacting appropriately to an obstacle. [H-1]

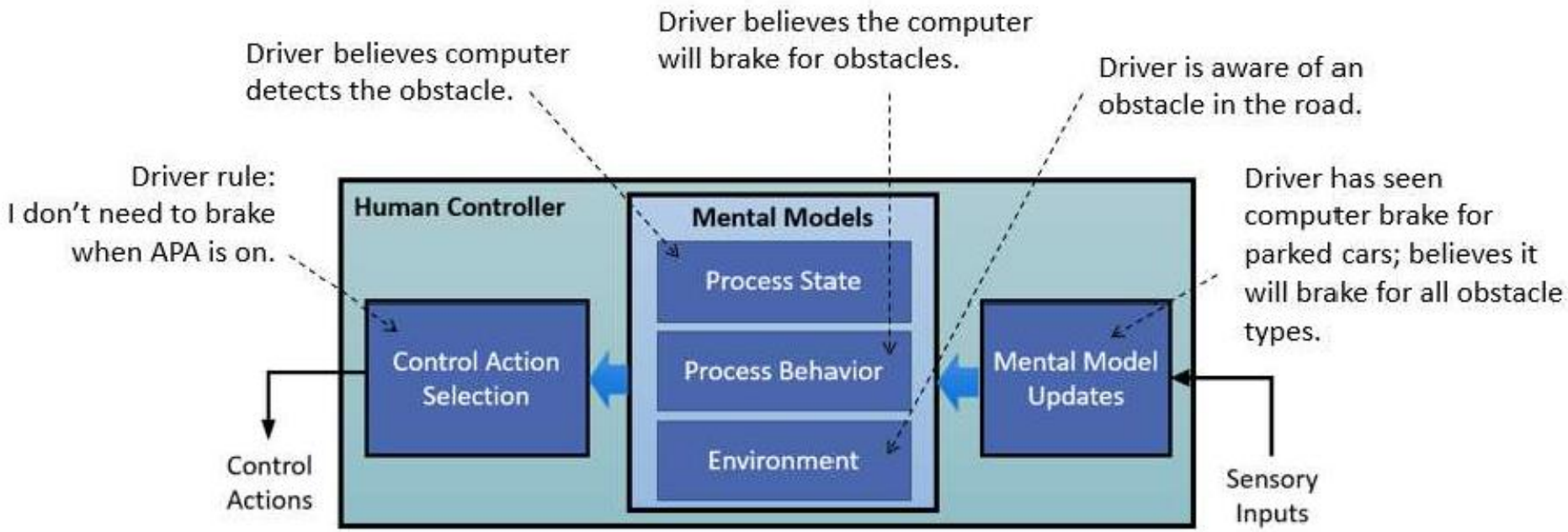
CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.

Scenario: The driver does not brake for the obstacle because the driver incorrectly believes that the computer detects and will brake for the obstacle ahead. This belief stems from past experience in which she has seen the computer apply the brakes to avoid hitting other parked vehicles. She does not receive any feedback that the computer is unaware of the obstacle.

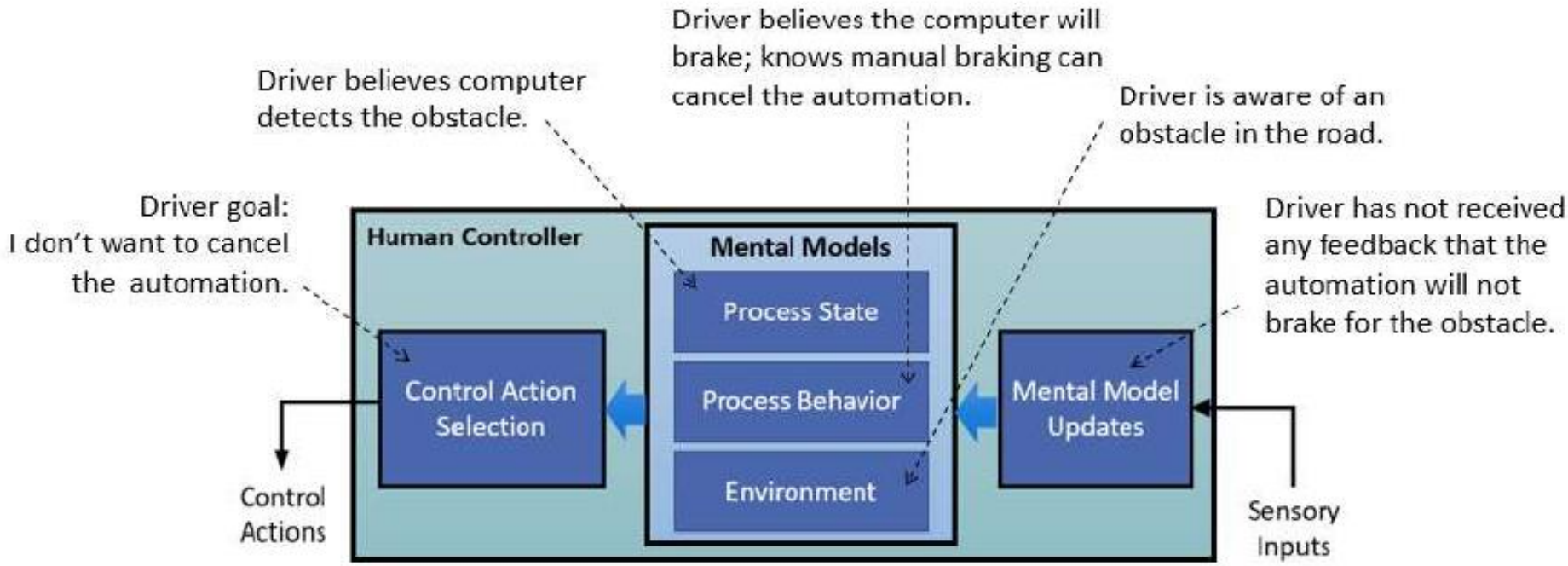
CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.



CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.



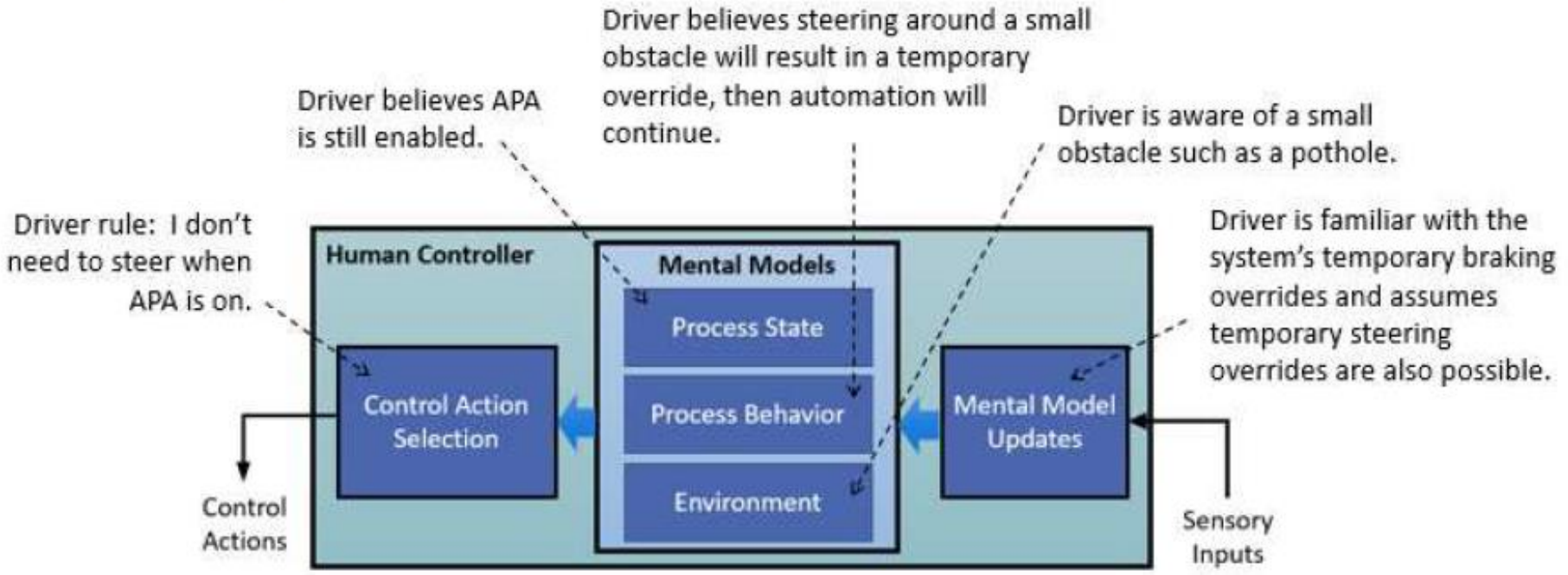
CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver stops providing steering commands after initially disabling the automation.

Scenario: The driver acts on the assumption that he does not need to steer when autopark is enabled, and he incorrectly believes it is still enabled because he did not notice or understand the indicator that it disabled. He had grabbed the steering wheel to swerve around a small obstacle and incorrectly assumed this would result in a temporary override because he knows that braking can cause temporary overrides and assumes steering can do the same.

CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver stops providing steering commands after initially disabling the automation.



STARTING POINTS FOR SOLUTIONS

Scenario details:

- The driver is concerned that braking would cancel the automation and require her to restart the parking maneuver.
- The driver incorrectly believes that the computer detects and will brake for the obstacle ahead. She does not receive any feedback that the computer is unaware of the obstacle.

Some possible solutions:

- Make it easy to resume auto parking with minimal steps for the driver.
- Provide feedback about automation's status (obstacles detected or not) and next actions in the form of a prominent display.
- Consider whether it is appropriate to require driver monitoring of the system or whether automation should be designed to handle such events.

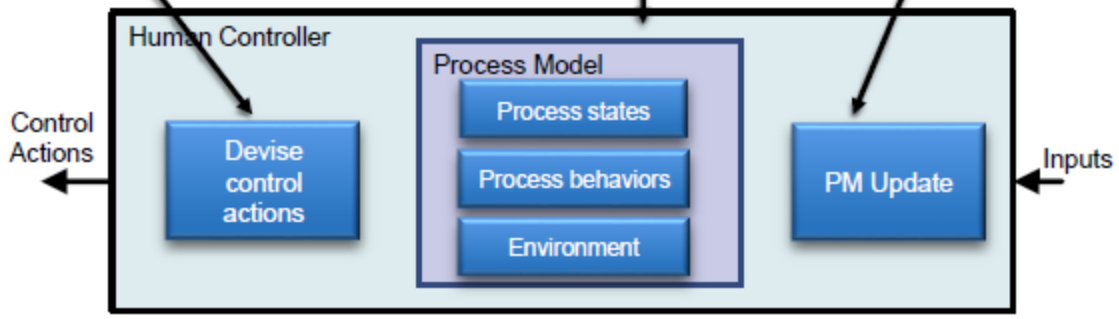
SUMMARY OF NEW MODEL BENEFITS

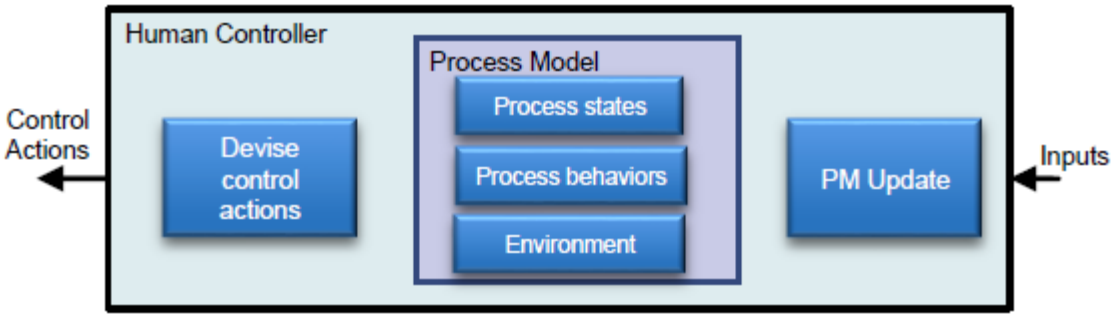
The new model scenarios incorporate additional context to explain ***why*** the driver may have certain beliefs and how those beliefs influence the driver's control actions.

Captures goals and prioritization; how UCAs are selected based on PM

Captures specific types of flaws which may call for different solutions

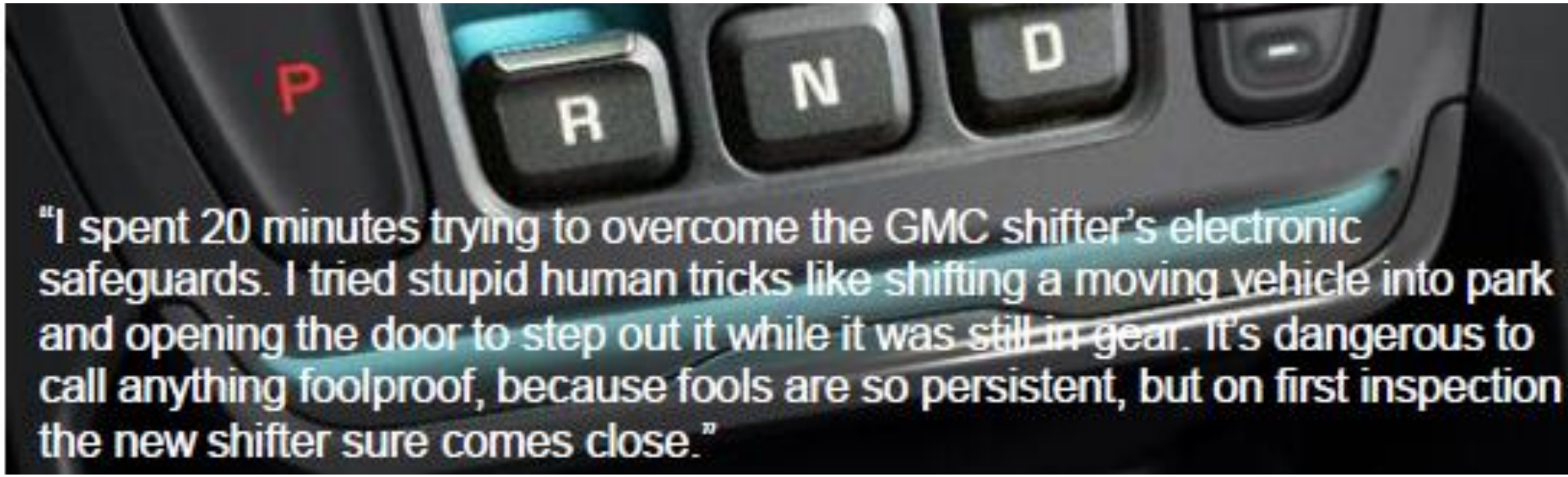
Captures influence of past experience and expectations on processing of inputs





- Adds more sophisticated human error analysis to STPA
- Suggests engineering solutions; does not just identify problems
- Can be used earlier in design process than detailed simulations and prototypes
- **Provides a "common language" for engineers to collaborate across domains**

STPA Integrated into GM Concept Development Phase (slide from Mark Vernacchia, GM)



Mark Phelan, Detroit Free Press, Auto Critic, July 1, 2017

Examples of Uses Beyond Traditional System Safety

- Airline operations (leading indicators of increasing risk)
- Workplace safety
- Design of safety management systems
- Cybersecurity
- Quality
- Production engineering
- Organizational culture
- Banking and finance
- Criminal law

Is it Practical?

- STPA has been or is being used in a large variety of industries
  - Automobiles (>80% use)
  - Aircraft and Spacecraft (extensive use and growing)
  - Air Traffic Control
  - UAVs (RPAs)
  - Defense systems
  - Medical Devices and Hospital Safety
  - Chemical plants
  - Oil and Gas
  - Nuclear and Electric Power
  - Robotic Manufacturing / Workplace Safety
  - Pharmaceuticals
  - etc.
- International standards in development or STPA already included (already satisfies MIL-STD-882)

Evaluations and Estimates of ROI

- Hundreds of evaluations and comparison with traditional approaches used now
  - Controlled scientific and empirical (in industry)
  - All show STPA is better (identifies more critical requirements or design flaws)
  - All (that measured) show STPA requires orders of magnitude fewer resources than traditional techniques
- ROI estimates only beginning but one large defense industry contractor claims they are seeing 15-20% return on investment (wrt whole contract, not just hazard analysis) when using STPA

To Make Progress We Need to:

- Develop and use different approaches that match the world of engineering today
- Consider the entire sociotechnical system
- Focus on building safety/security in rather than assuring/measuring it after the design is completed

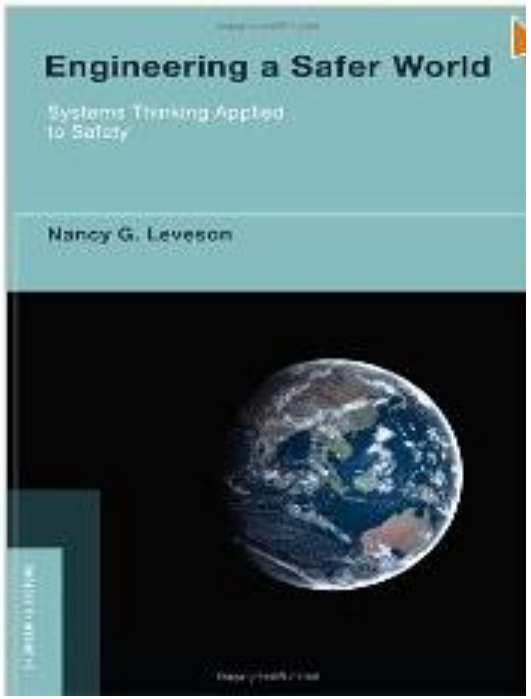
"The best way to predict the future is to create it."

Abraham Lincoln

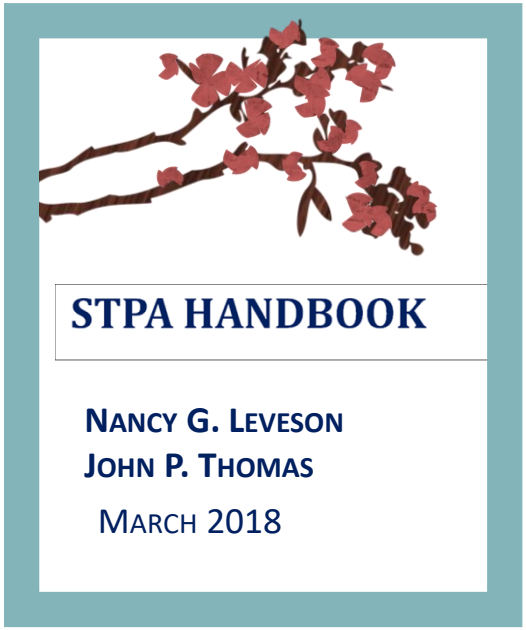
- Develop and use new approaches to certification, regulation, risk management, and risk assessment

MIT STAMP/STPA Workshop

- 327 people from 32 countries registered last year
- Industry, academia, government
- Just about every safety-critical industry represented



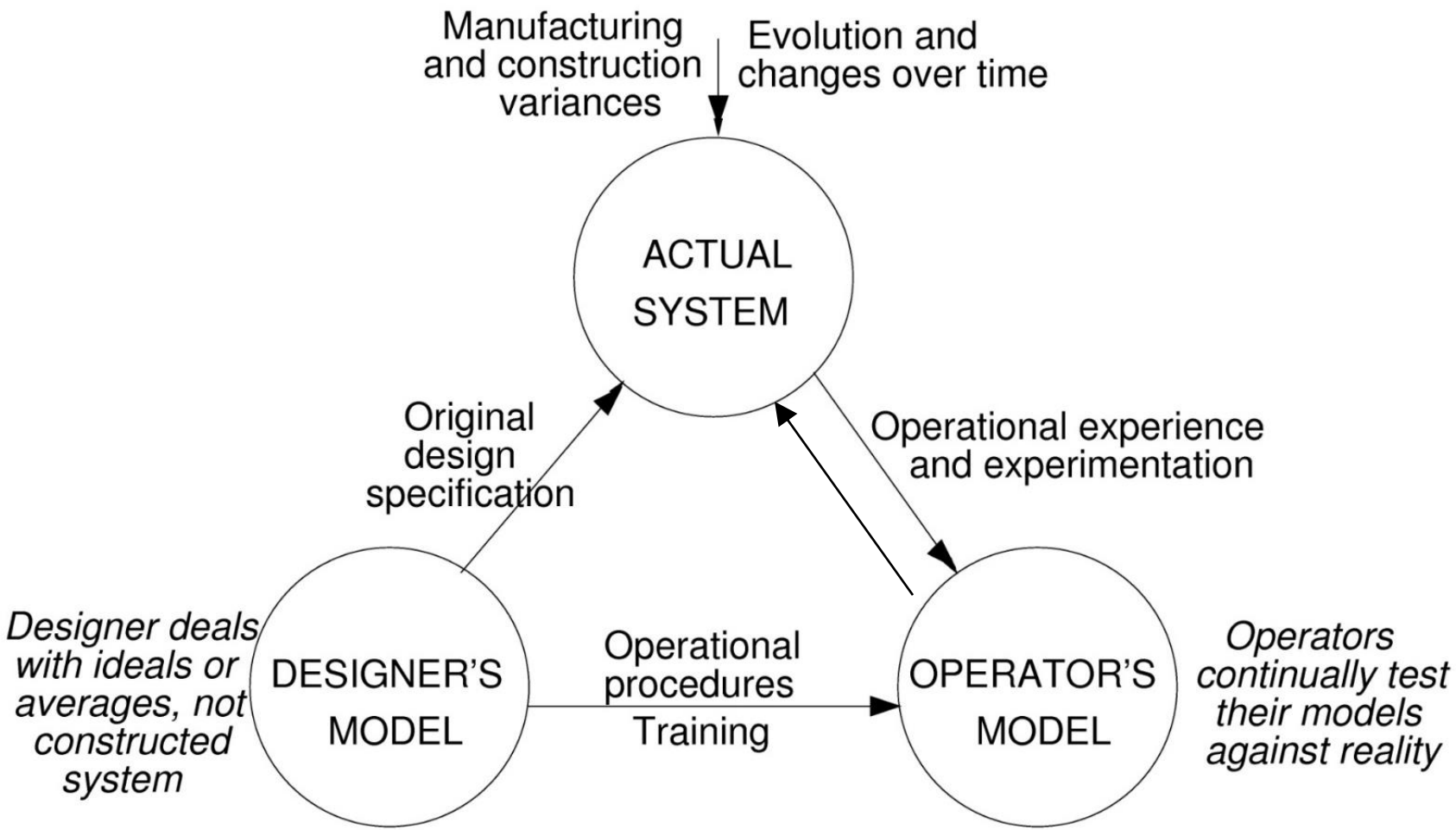
MIT Press, 2012



http://psas.scripts.mit.edu

QUESTIONS?

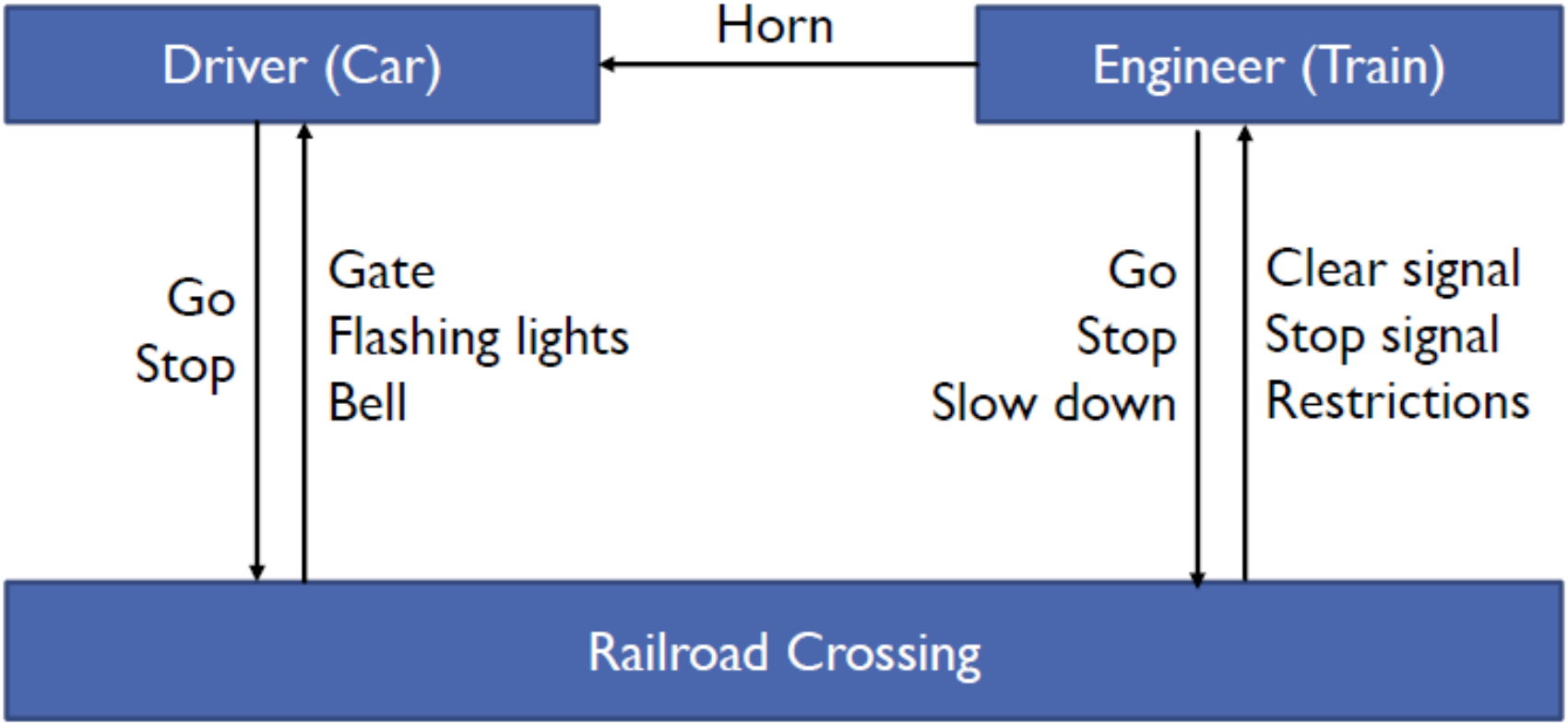
Operator “Error” Not Just a Random Failure



RAILROAD CROSSING EXAMPLE

Accidents	A1: A car and train collide at a railroad crossing.
Hazards	H1: A car is stopped in the path of a train. H2: A car is moving in front of the path of a train.

SAFETY CONTROL STRUCTURE [SIMPLIFIED]



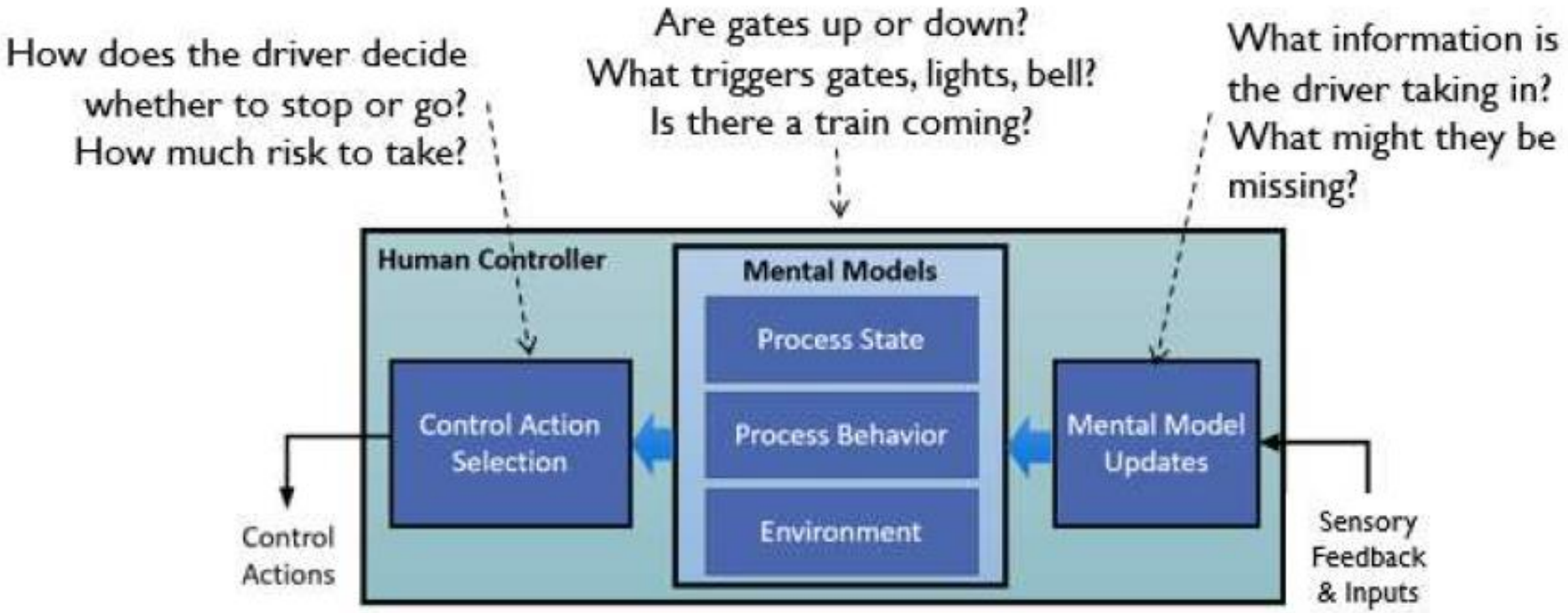
DRIVER UNSAFE CONTROL ACTIONS

Control Action	Applying causes Hazard	Not applying causes hazard	Wrong timing or order	Stopped too soon or applied too long
Stop	**UCA-1:** Driver stops over the tracks when a train is approaching. [H1]	**UCA-2:** Driver does not stop before the crossing when a train is approaching. [H2]	-	-

Reminder-
H1: A car is stopped in the path of a train.
H2: A car is moving in front of the path of a train.

DEVELOPING CAUSAL SCENARIOS

New model gives us additional information to consider…



DEVELOPING CAUSAL SCENARIOS

UCA-1: Driver stops over the tracks when a train is approaching. [H1]

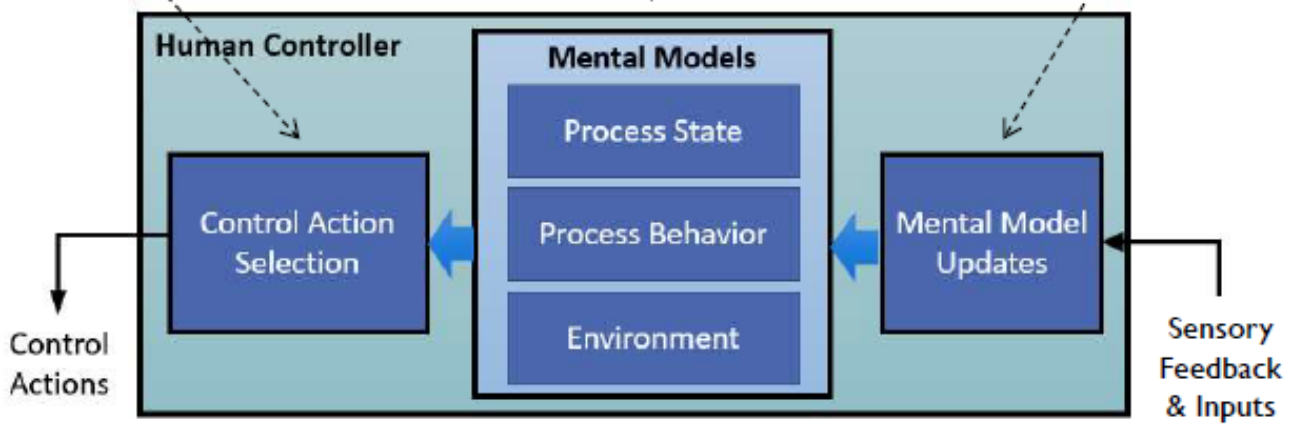
Driver incorrectly believes there is no train / it is safe to cross (PS),

Because a gate would come down if it were not safe (PB).

Driver is at an intersection in traffic (E).

Driver decides to cross intersection because he is in a hurry & believes it is safe (but gets stuck on track).

Driver is familiar with gated crossings & did not notice this crossing has no gate.



DEVELOPING CAUSAL SCENARIOS

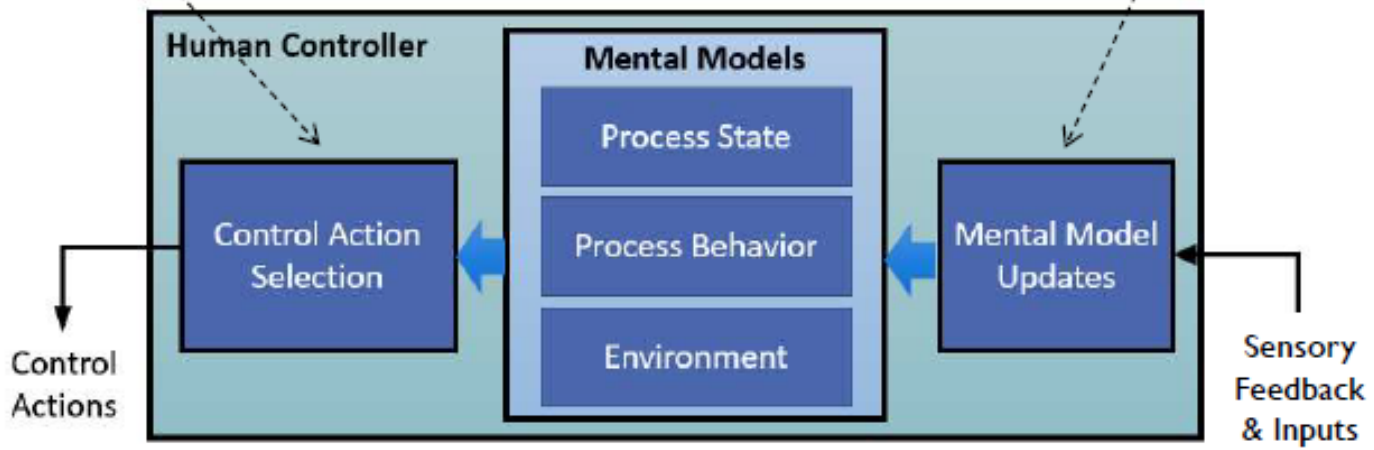
UCA-2: Driver does not stop before the crossing when a train is approaching. [H2]

Driver decides to go around the gate, believing the risk is low.

Driver knows that gates sometimes come down when there is no train (PB).

Driver believes there is no train (PS).

Driver has waited for gates in the past when no train was coming.



Definition of Hazard and Hazard Analysis

Hazard/vulnerability:

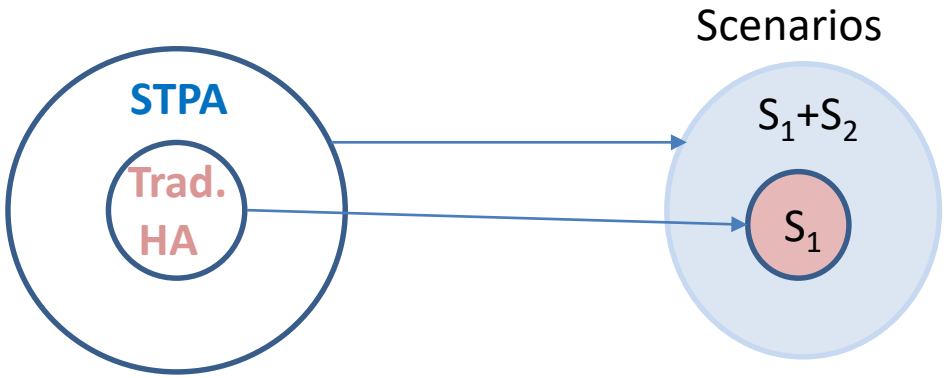
A system state or set of conditions that, together with some worst-case environmental conditions, will lead to a loss

Hazard Analysis:

Identifying operational scenarios that can lead to a hazard/vulnerability

Safety Engineering:

Eliminating or controlling hazard scenarios in the system design and operations



Washington State Ferry Problem

- Rental cars could not be driven off ferries when got to port
- Local rental car company installed a security device to prevent theft by disabling cars if car moved when engine stopped
- When ferry moved and cars not running, disabled them.

Integrated Approach to Safety and Security (Col. Bill Young)

- Safety: prevent losses due to unintentional actions by benevolent actors
- Security: prevent losses due to intentional actions by malevolent actors
- Common goal: loss prevention
  - Ensure that critical functions and services provided by networks and services are maintained
  - New paradigm for safety will work for security too
    - May have to add new causes, but rest of process is the same
  - A top-down, system engineering approach to designing security (and safety) into systems

Example: Stuxnet

- Loss: Damage to reactor (in this case, centrifuges)
- Hazard/vulnerability: Centrifuges damaged by spinning too fast
- Constraint to be enforced: Centrifuges must never spin above maximum speed
- Unsafe control action: Issuing *increase speed* command when already spinning at maximum speed
- One potential causal scenario
  - Incorrect process model: Thinks spinning at less than maximum speed
  - Does not matter whether deliberate or accidental
- Potential controls:
  - Mechanical limiter (interlock), analog RPM gauge

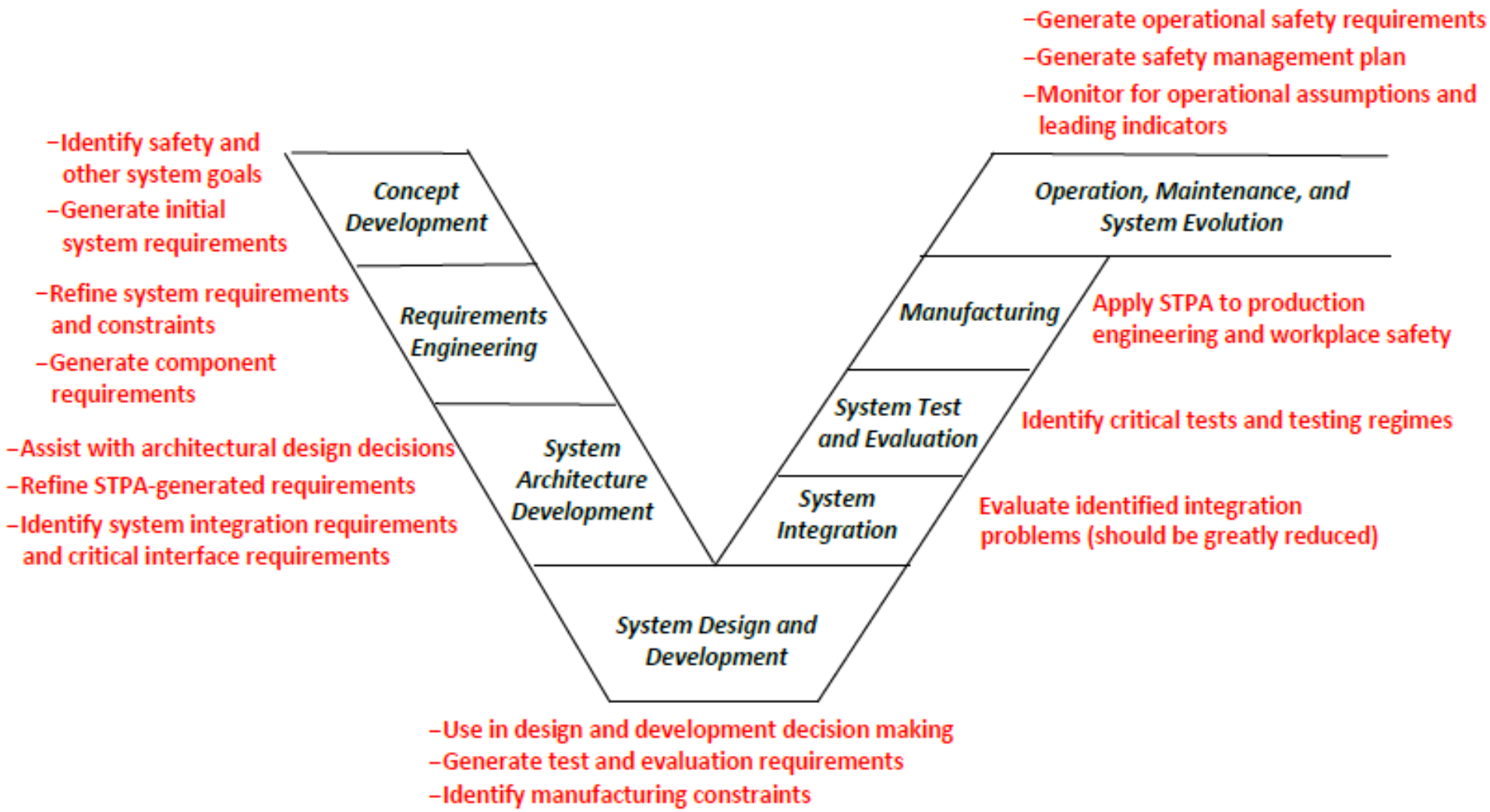
Focus on preventing hazardous state (not keeping intruders out)

Traditional Approach to Safety

- Traditionally view safety as a failure problem
  - Chain of directly related failure events leads to loss
  - Try to prevent component failures or establish barriers between events
- Limitations
  - Systems are becoming more complex
    - Accidents often result from interactions among components
    - Cannot anticipate all potential interactions
  - Omits or oversimplifies important factors
    - Human error
    - New technology (including software)
    - Culture and management
    - Evolution and adaptation

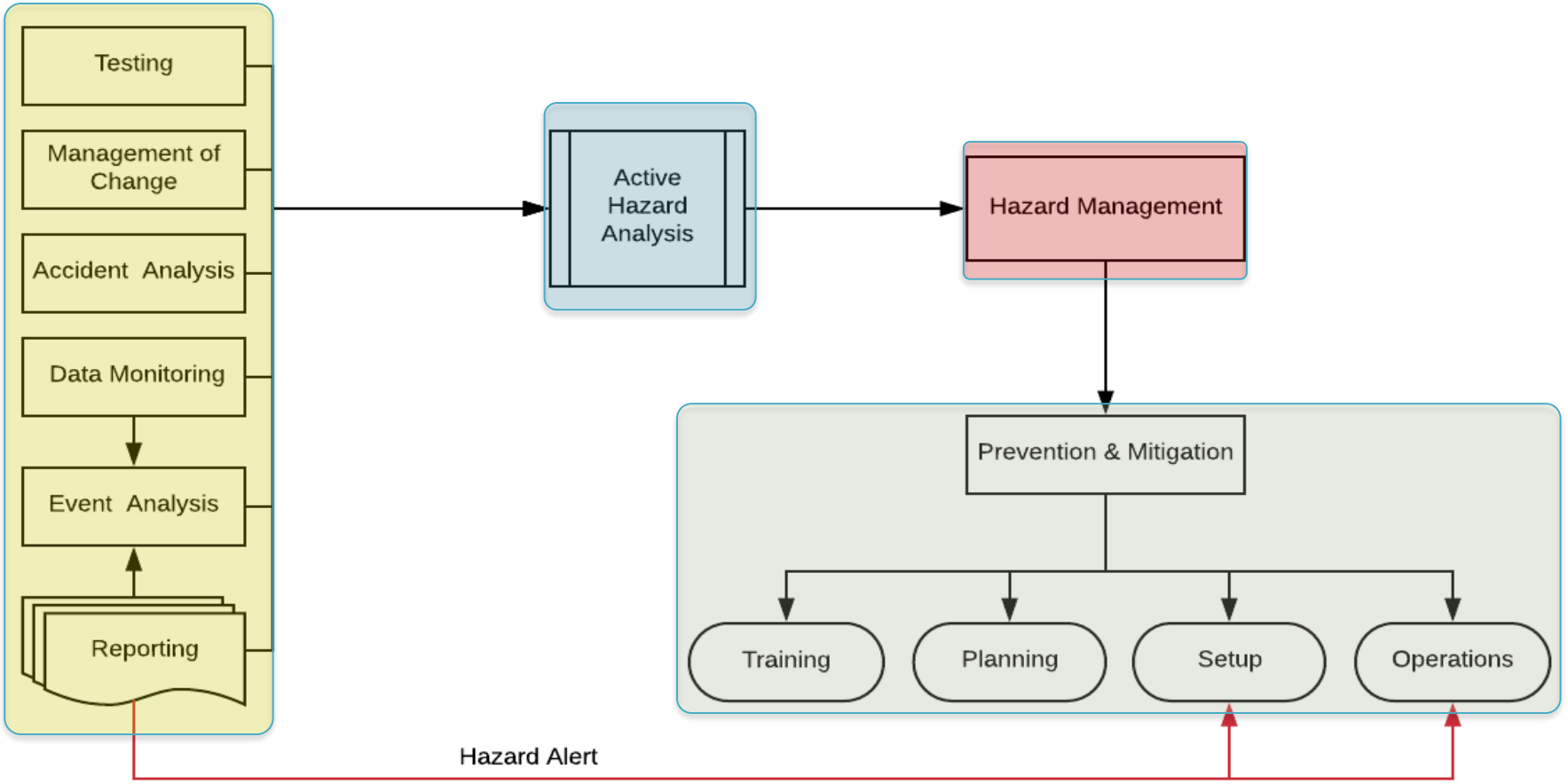
Accidents are <u>not</u> just the result of random failure

STPA can be used throughout product development and operations



Risk Management During Operations and Leading Indicators (Maj. Diogo Castilho)

- Systems and their environments are not static
- Goal is to detect when risk is increasing (leading indicators)

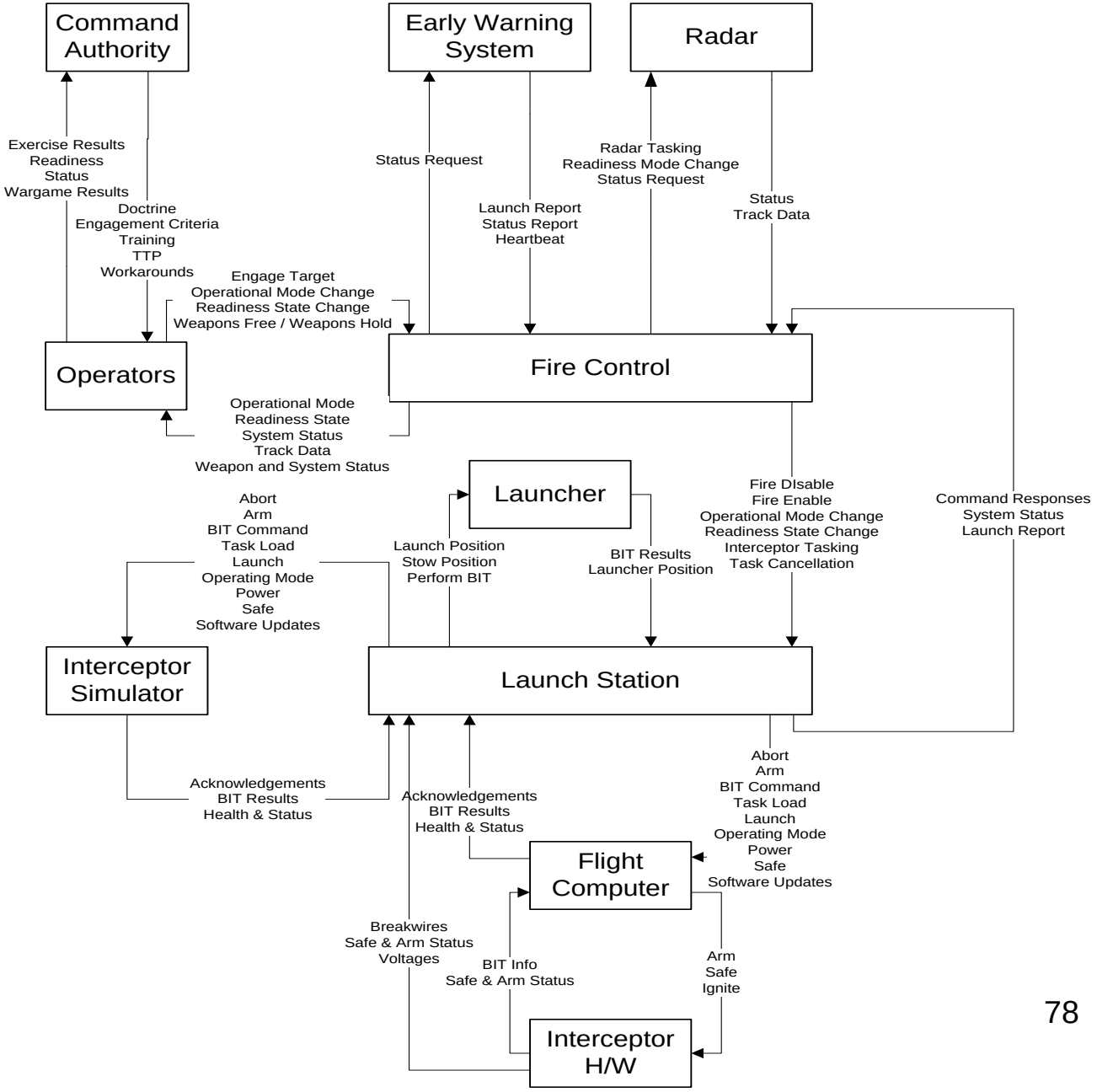


Ballistic Missile Defense System (MDA)

- Hazard was inadvertent launch
- Analyzed right before deployment and field testing (so done late)
  - 2 people, 5 months (unfamiliar with system)
  - Found so many paths to inadvertent launch that deployment delayed six months
- One of first uses of STPA on a real defense system (2005)

Sea-based sensors on the Aegis platform, upgraded early warning radars (UEWR), the Cobra Dane Upgrade (CDU), Ground-based Midcourse Defense (GMD) Fire Control and Communications (GFC/C), a Command and Control Battle Management and Communications (C2BMC) Element, and Ground-based interceptors (GBI). Future block upgrades were originally planned to introduce additional Elements into the BMDS, including Airborne Laser (ABL) and Terminal High Altitude Area Defense (THAAD).

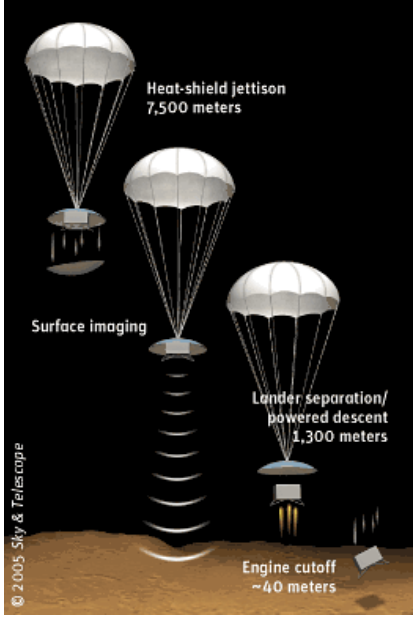
Control Structure for FMIS



Example Hazard Scenarios Found

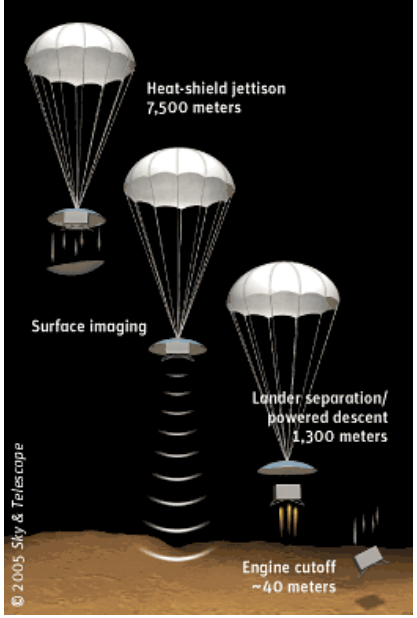
- Missing software and human operator requirements, for example:
  - Operator could input a legal (but unanticipated) instruction at same time that radars detect a potential (but not dangerous) threat
  - Could lead to software issuing an instruction to enable firing an interceptor at a non-threat
- Timing conditions that could lead to incorrectly launching an interceptor
- Situations in which simulator data could be taken as real data

Accident with No Component Failures



- Mars Polar Lander
  - Have to slow down spacecraft to land safely
  - Use Martian atmosphere, parachute, descent engines (controlled by software)
  - Software knows landed because of sensitive sensors on landing legs. Cuts off engines when determines have landed.
  - But “noise” (false signals) by sensors generated when landing legs extended. Not in software requirements.
  - Software not supposed to be operating at that time but software engineers decided to start early to even out the load on processor
  - Software thought spacecraft had landed and shut down descent engines while still 40 meters above surface

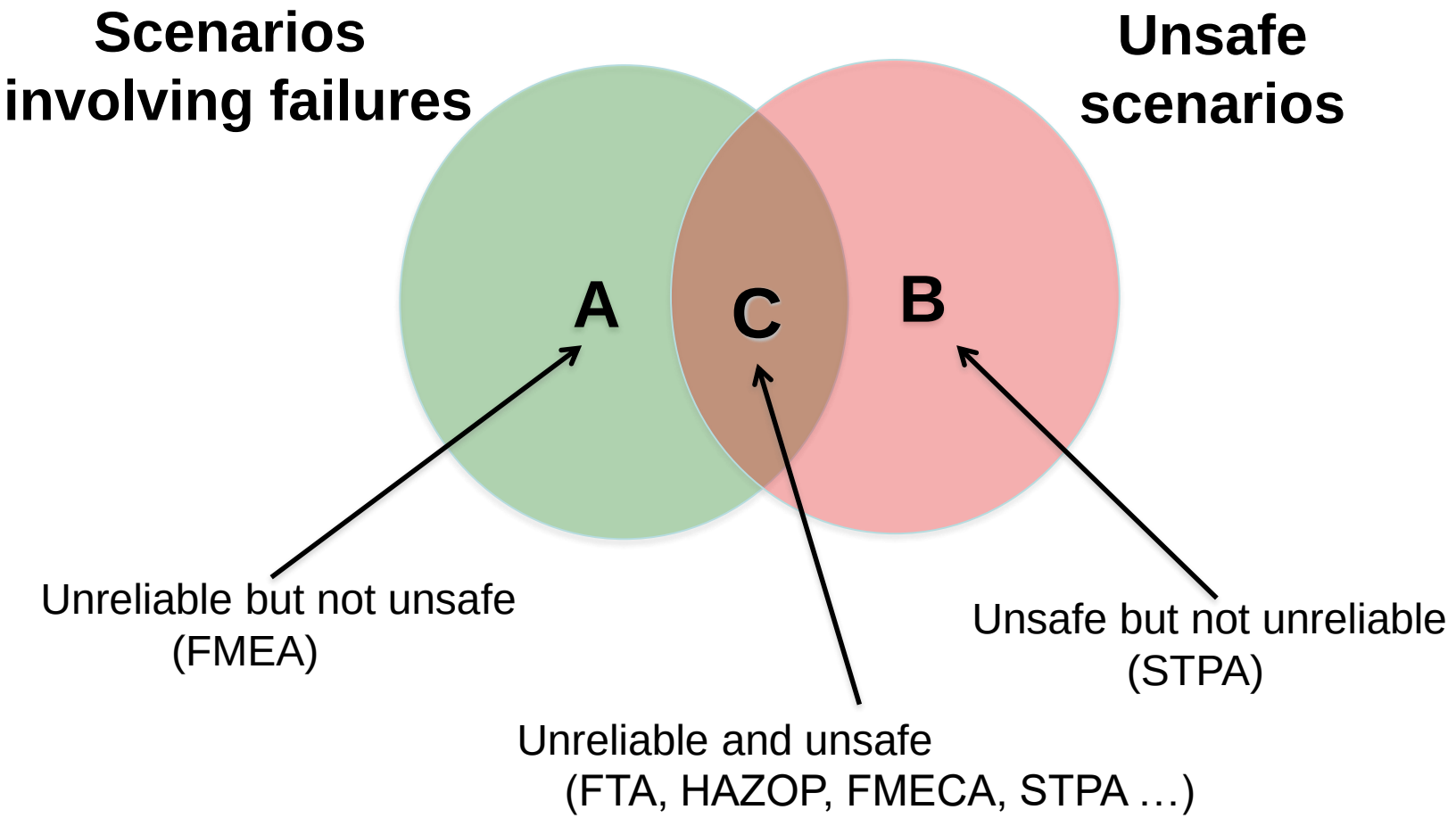
Accident with No Component Failures



- Mars Polar Lander
  - Have to slow down spacecraft to land safely
  - Use Martian atmosphere, parachute, descent engines (controlled by software)
  - Software knows landed because of sensitive sensors on landing legs. Cuts off engines when determines have landed.
  - But “noise” (false signals) by sensors generated when landing legs extended. Not in software requirements.
  - Software not supposed to be operating at that time but software engineers decided to start early to even out the load on processor
  - [illegible]nt

All software requirements were satisfied!
The requirements were unsafe

Confusing Safety and Reliability



Preventing Component or Functional Failures is Not Enough

High-Level Flight Crew Requirements

- FC-R1: Crew must not provide manual braking before touchdown [CREW.1c1]

  Rationale: *Could cause wheel lockup, loss of control, or tire burst*.

- FC-R2: Crew must not stop manual braking more than TBD seconds before safe taxi speed reached [CREW.1d1]

  Rationale: *Could result in overspeed or runway overshoot*.

- FC-R3: The crew must not power off the BSCU during autobraking [CREW.4b1]

  Rationale: *Autobraking will be disarmed*.

- etc.

Example BSCU Requirements

- BSCU-R1: A brake command must always be provided during RTO [BSCU.1a1]

  Rationale: Could result in not stopping within the available runway length

- BSCU-R2: Braking must never be commanded before touchdown [BSCU.1c1]

  Rationale: Could result in tire burst, loss of control, injury, or other damage

- BSCU-R3: Wheels must be locked after takeoff and before landing gear retraction [BSCU.1a4]

  Rationale: Could result in reduced handling margins from wheel rotation in flight.

- Etc.

Example Requirements for BSCU Hydraulic Controller

- HC-R1: The HC must not open the green hydraulics shutoff valve when there is a fault requiring alternate braking [HC.1b1]

  Rationale: *Both normal and alternate braking would be disabled.*

- HC-R2: The HC must pulse the anti-skid valve in the event of a skid [HC.2a1]

  Rationale: *Anti-skid capability is needed to avoid skidding and to achieve full stop in wet or icy conditions*.

- HC-R3: The HC must not provide a position command that opens the green meter valve when no brake command has been received [HC.3b1]

  Rationale: *Crew would be unaware that uncommanded braking was being applied*

- Etc.

Robots, piper

Cali American Airlines Crash

Identified causes:

- Flight crew's failure to adequately plan and execute the approach to runway 10 at Cali and their **inadequate use of automation**

- Failure of flight crew to discontinue the approach into Cali, despite **numerous cues** alerting them of the inadvisability of continuing the approach

- **Lack of situational awareness of the flight crew regarding vertical navigation, proximity to terrain, and the relative location of critical radio aids**

- **Failure of the flight crew to revert to basic radio navigation at the time when the FMS-assisted navigation became confusing and demanded an excessive workload in a critical phase of flight.**

Case Study of a New Semi-Automated Manufacturing Process

- Traditional assessment process led by a longstanding company expert
  - Task-Based Risk Assessment (TRA)
  - Robotics Industry Association

- STPA analysis led by a newly trained employee

Example TRA Form

Line No	Task Description	Hazards	Initial Risk				Risk Reduction Measures	Final Risk				
			Severity	Exposure	Avoidance	Risk Level		Severity	Exposure	Avoidance	SRP/CS of mitigation (if applicable)	Risk Level
			S1 - S3	E1 - E2	A1 - A3	Tbl 2		S1 - S3	E1 - E2	A1 - A3	Tbl 5	Tbl 2
1	Task 1	mechanical : unexpected start	S2	E2	A2	R1	Use of pendant & enabling devices, safety scanners, Safety PLC, Systems programming requiring operator confirmations, Training & Procedures	E1	A1	S2		R3B
2	Task 1	mechanical : Crushing, pinching, impact movement system	S2	E1	A1	R2B	Training and procedures; situational awareness	E1	A1	S2		R3B
3	Task 1	slips / trips / falls : trip	S1	E1	A1	R4	Housekeeping, caution and situational awareness	E1	A1	S1		R4
4	Task 2	ergonomics / human factors : lifting / bending / twisting	S1	E1	A2	R3B	Proper techniques; adherence to shop practices	E1	A1	S1		R4
5	Task 3	lasers : eye exposure	S1	E2	A1	R3A	Position the laser to a safe location or shut down when not in use. Class 2 laser. Limit access to the build area.	E1	A1	S1		R4

Examples of TRA Results (1)

- Unexpected movement was cause more than 70 times
  - Recommended standard shop practices, situational awareness, and standing clear of movement.
    - How does someone in the workplace stand clear of something that unexpectedly moves?
  - Safeguarding the space with a fence and using pendants and enabling devices if the users need to enter the space.
    - If don't know how or when system will move, how does controller in hand mitigate the risk?
    - If anything it makes the situation more hazardous by providing a false sense of security for the people nearest to the system and its associated hazards.

Examples of TRA Results (2)

- Another common one was safety components/systems not functioning properly, but then lists a safety system as the risk reduction method.
- Lots of recommendations for more rules, procedures, policies
- Large variability in estimates of severity, exposure, avoidance
- Process does not try to understand why hazards occur. So mitigations focus on controlling workers and not on controlling or changing system behavior.
- Assessment of human actions stops with what human did and not attempt to understand <u>why</u>.
  - Does not promote a safety-related discussion of human factors, roles of management, operations, processes, environment

STPA Analysis

- Starts by identifying hazards to be considered

H1: Exposure to uncontrolled energy (or energy at a level that could lead to a loss)

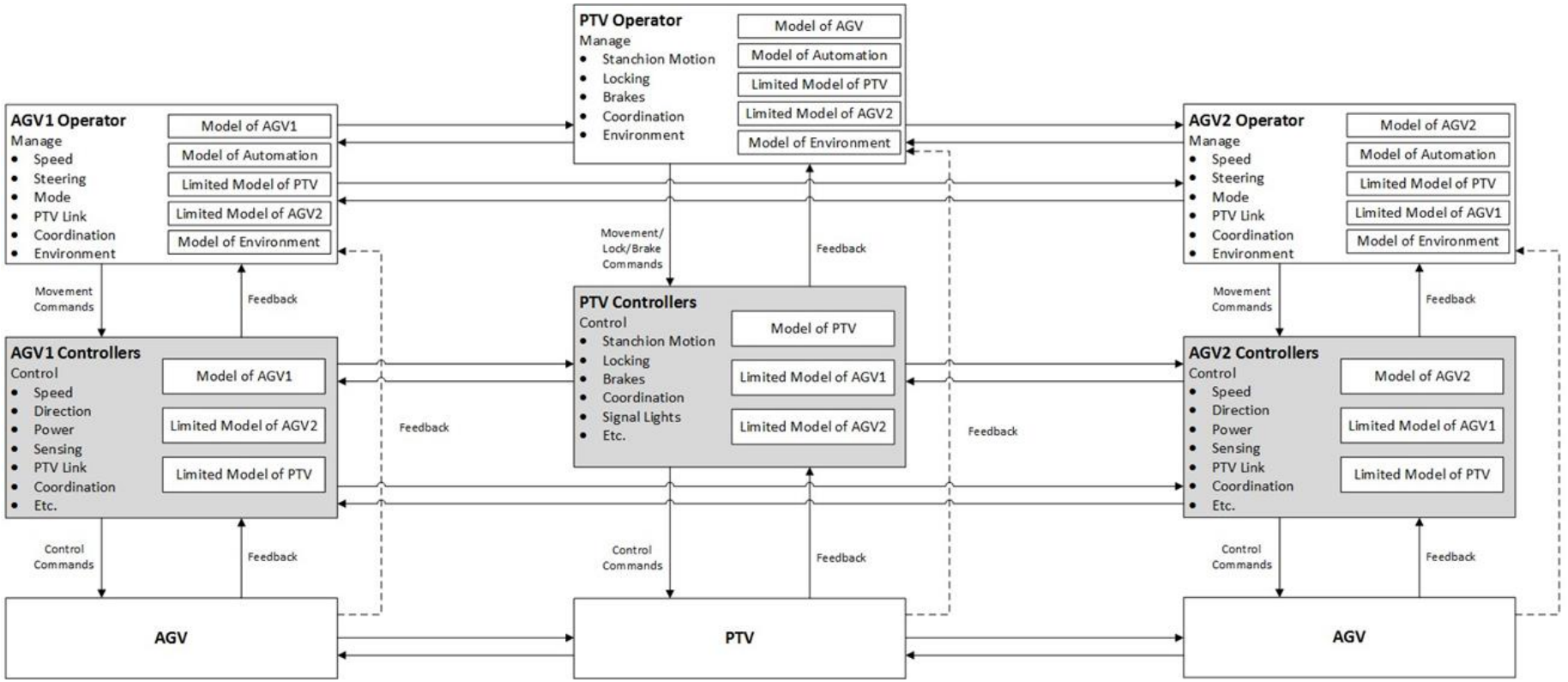
H2: Potentially injurious movement of the human body (or stress on the body) that could lead to injury

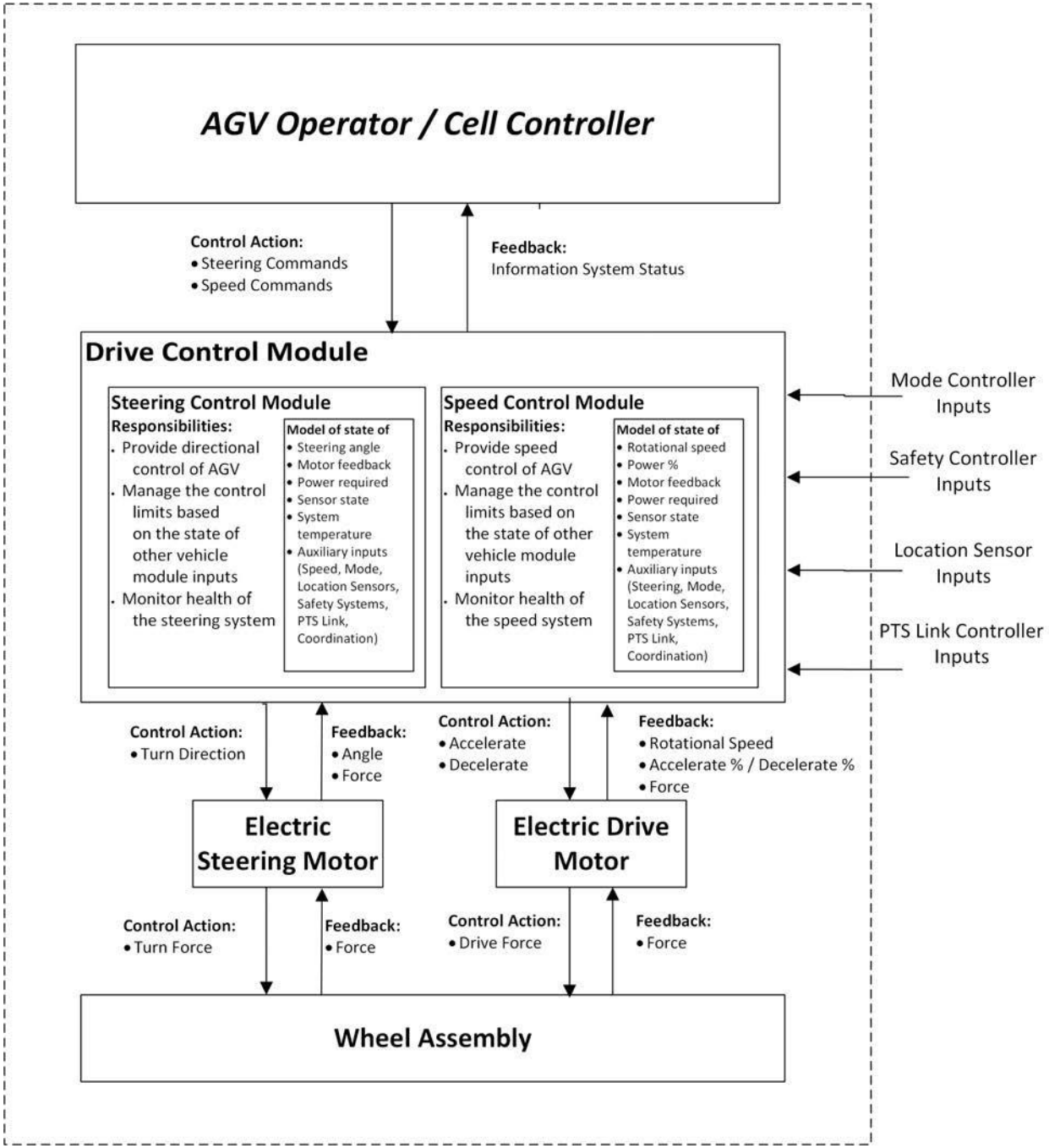
H3: Exposure to toxic materials above a safe level

H4: Exposure to noise levels that could affect hearing

H5: Extended exposure to an environment not providing basic human health requirements

Create the Control Structure Model




AGV Operator / Cell Controller
Control Action:
• Steering Commands
• Speed Commands
Feedback:
Information System Status
Drive Control Module
Steering Control Module
Responsibilities:
. Provide directional control of AGV
. Manage the control limits based on the state of other vehicle module inputs
. Monitor health of the steering system
Model of state of
• Steering angle
• Motor feedback
• Power required
• Sensor state
• System temperature
• Auxiliary inputs (Speed, Mode, Location Sensors, Safety Systems, PTS Link, Coordination)
Speed Control Module
Responsibilities:
. Provide speed control of AGV
. Manage the control limits based on the state of other vehicle module inputs
. Monitor health of the speed system
Model of state of
• Rotational speed
• Power %
• Motor feedback
• Power required
• Sensor state
• System temperature
• Auxiliary inputs (Steering, Mode, Location Sensors, Safety Systems, PTS Link, Coordination)
Mode Controller Inputs
Safety Controller Inputs
Location Sensor Inputs
PTS Link Controller Inputs
Control Action:
• Turn Direction
Feedback:
• Angle
• Force
Control Action:
• Accelerate
• Decelerate
Feedback:
• Rotational Speed
• Accelerate % / Decelerate %
• Force
Electric Steering Motor
Electric Drive Motor
Control Action:
• Turn Force
Feedback:
• Force
Control Action:
• Drive Force
Feedback:
• Force
Wheel Assembly

Identify Unsafe Control Actions

1. A control action required for safety is not provided or is not followed

2. An unsafe control action is provided that leads to a hazard

3. A potentially safe control action is provided too late, too early, or out of sequence

4. A safe control action is stopped too soon or applied too long (for continuous or nondiscrete control actions)

Control Action	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon / Applied Too Long
Operator provides drive commands to drive control module	**UCA1:** Drive control module commanded to drive when the movement will violate minimum separation with an object [H1.1]	**UCA3:** Drive control module not commanded to drive when the movement will prevent a violation of minimum separation with an object [H1.1]	**UCA4:** Drive control module commanded to drive before or after a safe path direction [H1.1]	**UCA7:** Drive control module commanded to drive too long when the movement violates minimum separation with an object [H1.1]
	UCA2: Drive control module commanded to drive when a human is handling components that will move [H1]		**UCA5:** Drive control module commanded to drive before a human stops handling components that will move [H1]	
			UCA6: Drive control module commanded to drive after a human starts handling components that will move [H1]	

Identify Causal Scenarios

UCA1: Drive control module commanded to drive when the movement will violate minimum separation with an object. [H1]

- ***Causal Scenario 1:*** The operator does not see the object or misjudges the safe path.
  - Operator inattention due to task overload, changes to the environment, or other external factors.
  - Operating in cluttered/restrictive areas
  - Objects are blocked from view by other workers, the vehicle itself, or the spar load on the AGV/PTV/AGV combination

Identify Causal Scenarios (2)

UCA1: Drive control module commanded to drive when the movement will violate minimum separation with an object. [H1]

Causal Scenario 7: The operator drives the AGV into an obstacle that is not detected by the scanners. Possible causes include:

- The object is outside of the safety scanners field of view.
  - Obstacles in the factory are at the PTV or spar level.
  - PTV guide rails are above the AGV
  - AGV being used for unintended use, such as carrying objects that extend past the scanner FOV.
- The object is in the safety scanners field of view but below the detection threshold.
- The object enters the field of view and is impacted by the AGV at a rate faster than the scan and reaction rate of the vehicle.
- The scanner capabilities have degraded over time.
- The scanner fails into an unsafe state

Generate Recommendations

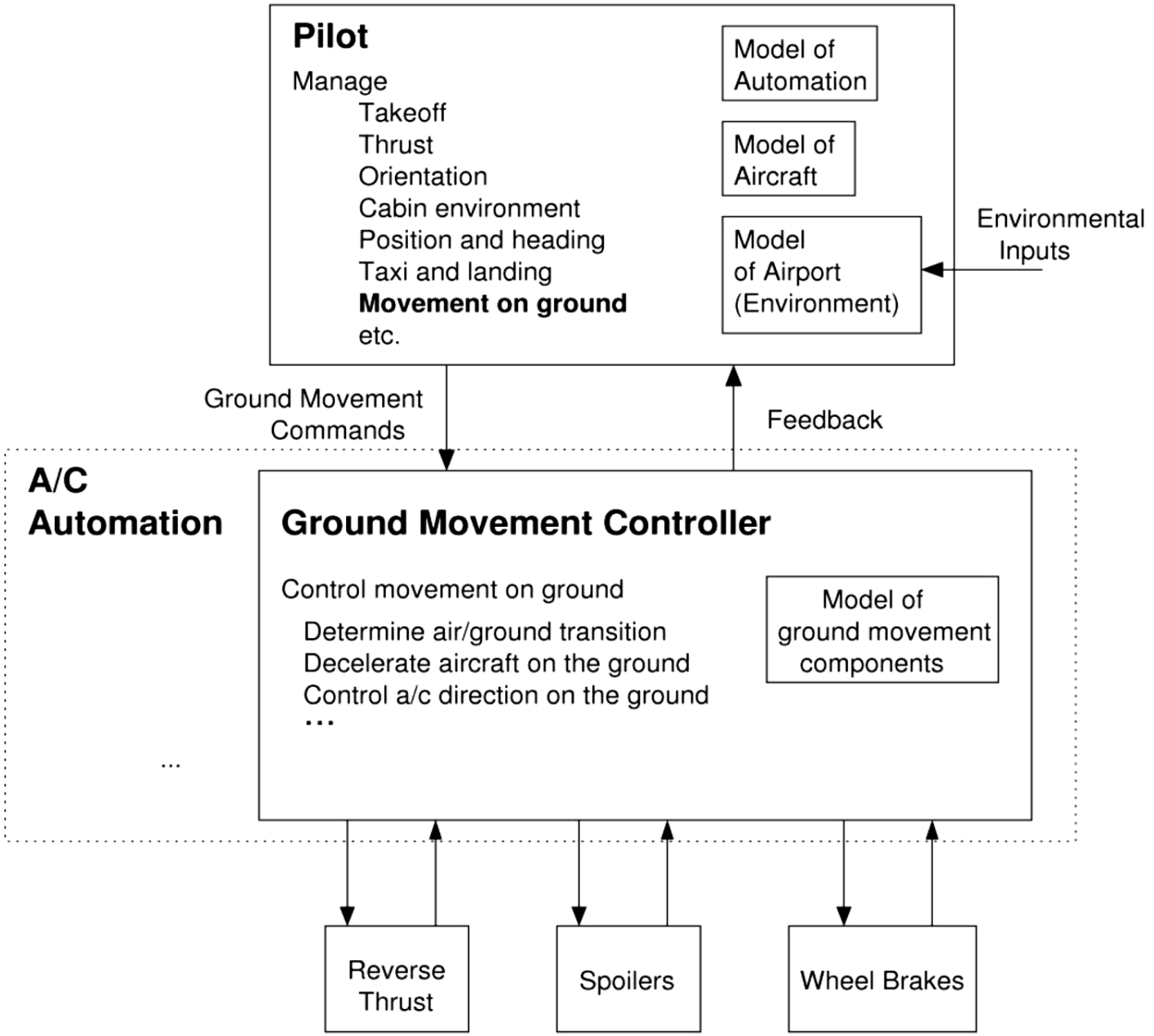
- New controls, redesign equipment, fault-tolerance, etc.

Most Preferred

Least Preferred

Risk Reduction Measures	Examples	Influence on Risk Factors	Classification	TRA	STPA
Elimination or Substitution	• Eliminate pinch points (increase clearance) • Intrinsically safe (energy containment) • Automated material handling (robots, conveyors, etc.) • Redesign the process to eliminate or reduce human interaction • Reduced energy • Substitute less hazardous chemicals	• Impact on overall risk (elimination) by affecting severity and probability of harm • May affect severity of harm, frequency of exposure to the hazard under consideration, and/or the possibility of avoiding or limiting harm depending on which method of substitution is applied.	Design Out	4%	14%
Guards, Safeguarding Devices, and Complementary Measures	• Barriers • Interlocks • Presence sensing devices (light curtains, safety mats, area scanners, etc.) • Two hand control and two-hand trip devices	• Greatest impact on the probability of harm (Occurrence of hazardous events under certain circumstance) • Minimal if any impact on severity of harm	Engineering Controls	34%	57%
Awareness Devices	• Lights, beacons, and strobes • Computer warnings • Signs and labels • Beepers, horns, and sirens	• Potential impact on the probability of harm (avoidance) • No impact on severity of harm	Administrative Controls	62%	29%
Training and Procedures	• Safe work procedures • Safety equipment inspections • Training • Lockout / Tagout / Verify	• Potential impact on the probability of harm (avoidance and/or exposure) • No impact on severity of harm			
Personal Protective Equipment (PPE)	• Safety glasses and face shields • Ear plugs • Gloves • Protective footwear • Respirators	• Potential impact on the probability of harm (avoidance) • No impact on severity of harm			

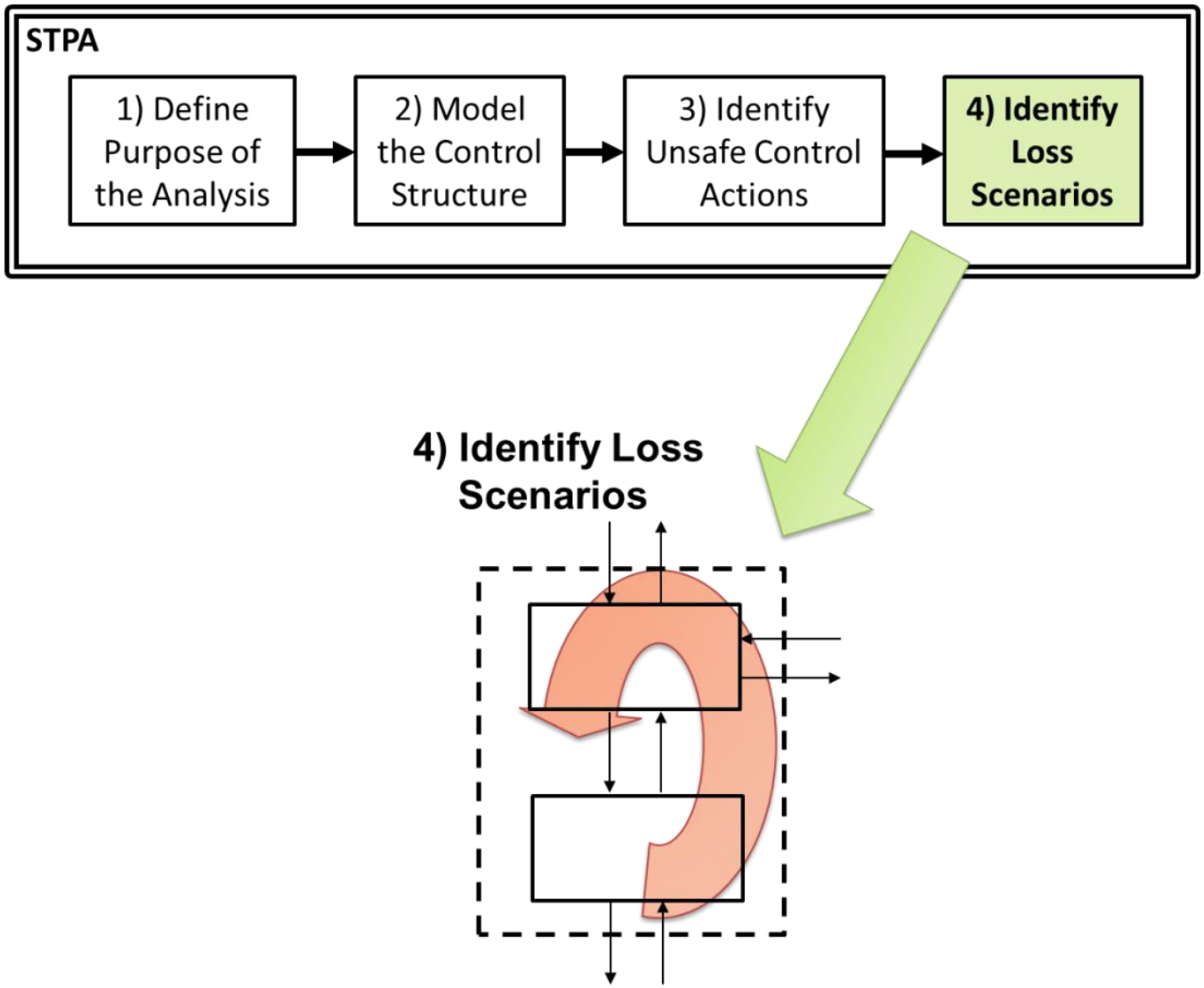
Criteria	TRA	STPA
Feasibility		
Compliant to Government Safety Regulations and Standards	G	G
Compliant to Industry Safety Regulations and Standards	G	G
Compliant to Company Safety Regulations and Standards	G	Y
Documented Analysis Process	G	G
Quality		
Includes hardware failure accidents	G	G
Includes technological factors in accidents beyond hardware failures, such as system design and requirements flaws (software and component interactions)	Y	G
Includes the role of management, operations, and procedures in accidents	R	G
Includes the role of the environment in accidents	R	G
Goes beyond specifying what humans did wrong to explain why they did what they did (includes sophisticated human factors in analysis)	R	G
Creates thorough understanding of the problem before implementing controls IAW the hierarchy of controls	R	G
Cost – Time required for case study assessment (approximate total personnel hours)	1000	300


Pilot
Manage
Takeoff
Thrust
Orientation
Cabin environment
Position and heading
Taxi and landing
Movement on ground
etc.
Model of Automation
Model of Aircraft
Model of Airport (Environment)
Environmental Inputs
Ground Movement Commands
Feedback
A/C Automation
Ground Movement Controller
Control movement on ground
Determine air/ground transition
Decelerate aircraft on the ground
Control a/c direction on the ground
...
Model of ground movement components
...
Reverse Thrust
Spoilers
Wheel Brakes

Examples of Requirements/Constraints Generated on the Interaction Between Deceleration Components

- **SC-BS-1**: Spoilers must deploy when the wheel brakes are activated manually or automatically above TBD speed.
- **SC-BS-2**: Wheel brakes must activate upon retraction of landing gear.
- **SC-BS-3**: Activation of ground spoilers must activate armed automatic braking (autobrake) system.
- **SC-BS-4**: Automatic braking system must not activate wheel brakes with forward thrust applied.
- **SC-BS-5**: Automatic spoiler system must retract the spoilers when forward thrust is applied.

Identifying Loss Scenarios



STPA-Generated Safety Requirements/Constraints

Unsafe Control Action	Description	Rationale
FC-R1	Crew must not provide manual braking before touchdown [CREW.1c1]	Could cause wheel lockup, loss of control, or tire burst
FC-R2	Crew must not stop manual braking more than TBD seconds before safe taxi speed reached [CREW.1d1]	Could result in overspeed or runway overshoot
FC-R3	The crew must not power off the BSCU during autobraking [CREW.4b1]	Autobraking will be disarmed
BSCU-R1	A brake command must always be provided during RTO [BSCU.1a1]	Could result in not stopping within the available runway length
BSCU-R2	Braking must never be commanded before touchdown [BSCU.1c1]	Could result in tire burst, loss of control, injury, or other damage
BSCU-R3	Wheels must be locked after takeoff and before landing gear retraction [BSCU.1a4]	Could result in reduced handling margins from wheel rotation in flight

A Systems Approach to Safety (and Security)

- Emphasizes building in safety rather than measuring it or adding it on to a nearly completed design
- Looks at system as a whole, not just components (a top-down holistic approach)
- Takes a larger view of causes than just failures
  - Accidents today are not just caused by component failures
  - Includes software and requirements flaws, human behavior, design flaws, etc.
- Goal is to use modeling and analysis to design and operate the system to be safe, not to predict the likelihood of a loss.
- Same analysis results can be used for cyber security

System Engineering Benefits

- Finds faulty underlying assumptions in concept development before flow downstream as anomalies (where more costly to change)
  - 70-80% of safety-critical decisions made during concept development
- Finds incomplete information, basis for further discussion with customer
- Both intended and unintended functionality are handled
- Includes software and operators in the analysis
  - Provides deeper insight into system vulnerabilities, particularly for cyber and human operator behavior.

System Engineering Benefits (2)

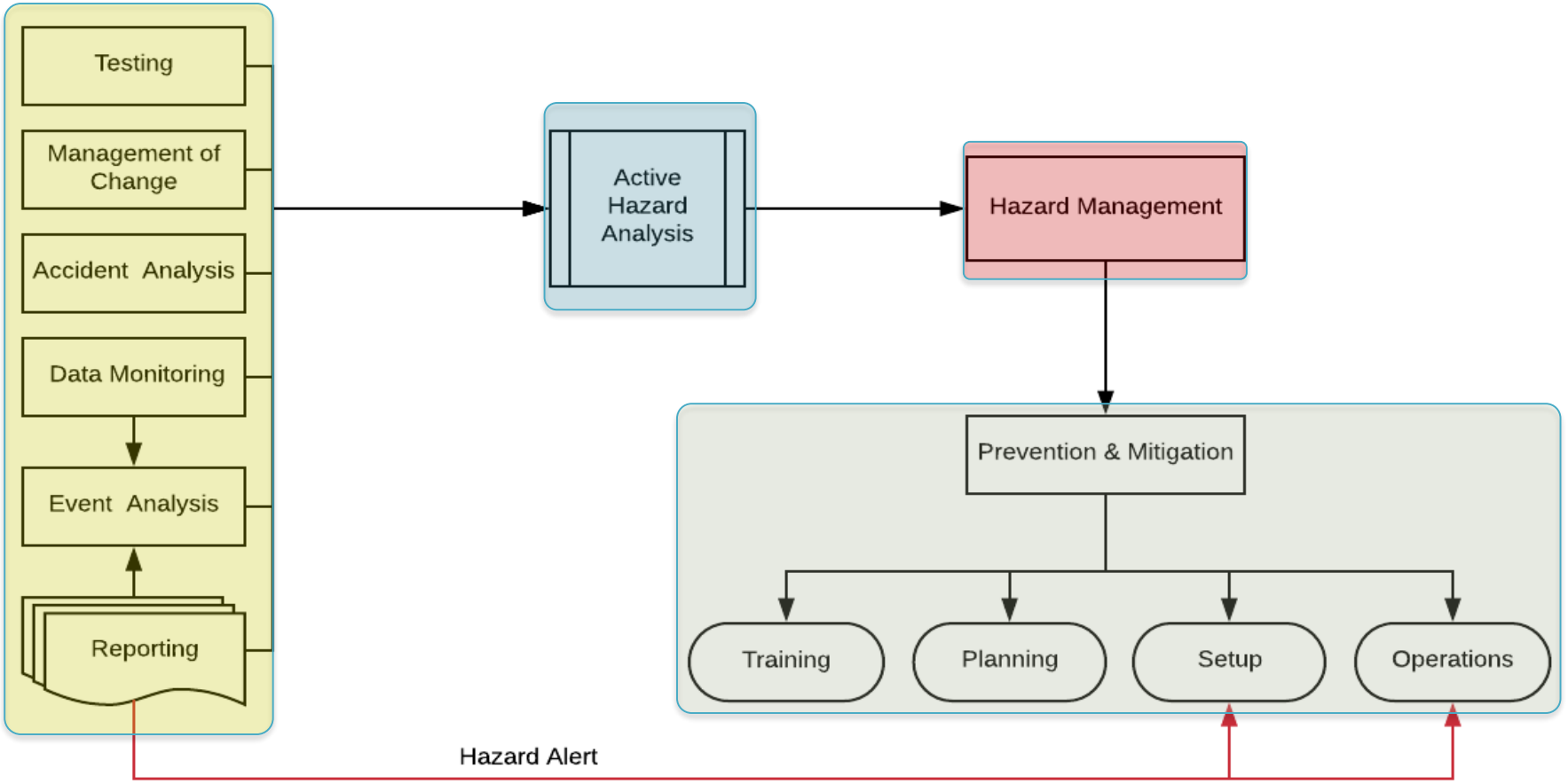
- Can analyze very complex systems.
  - ”Unknown unknowns” usually only found during ops can be identified early in development process
- Can be started early in concept analysis
  - Assists in identifying safety/security requirements before architecture or design exists
  - Then used to design safety and security into system, eliminating costly rework when design flaws found later.
  - As design is refined and more detailed design decisions are made, STPA analysis is refined to help make those decisions
- Complete traceability from requirements to system artifacts
  - Enhances maintainability and evolution

System Engineering Benefits (3)

- Models developed for the analysis provide documentation of system functionality (vs. physical or logical design)
  - Often missing or difficult to find in documentation for large, complex systems
- Easily integrated into system engineering process and model based system engineering.
  - Models are functional models rather than simply physical or logical models.

Risk Management During Operations and Leading Indicators (Maj. Diogo Castilho)

- Systems and their environments are not static
- Goal is to detect when risk is increasing (leading indicators)



What Failed Here?

- Navy aircraft were ferrying missiles from one location to another.
- One pilot executed a planned test by aiming at aircraft in front and firing a dummy missile.
- Nobody involved knew that the software was designed to substitute a different missile if the one that was commanded to be fired was not in a good position.
- In this case, there was an antenna between the dummy missile and the target so the software decided to fire a live missile located in a different (better) position instead.

Boeing 787 Lithium Battery Fires

Models predicted 787 battery thermal problems would occur once in 10 million flight hours…but two batteries overheated in just two weeks in 2013

Boeing 787 Lithium Battery Fires

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

All software requirements were satisfied!
The requirements were unsafe

High-Level (System) Requirements/Constraints

SC1: Forward motion must be retarded within TBD seconds of a braking command upon landing, rejected takeoff, or taxiing (H4-1).

SC2: The aircraft must not decelerate after V1 (H4-2).

SC3: Uncommanded movement must not occur when the aircraft is parked (H4-3).

SC4: Differential braking must not lead to loss of or unintended aircraft directional control (H4-4)

SC5: Aircraft must not unintentionally maneuver out of safe regions (taxiways, runways, terminal gates and ramps, etc.) (H4-5)

SC6: Main gear rotation must stop when the gear is retracted (H4-6)

STPA analysis will refine these into detailed requirements/constraints

- **On system**
- **On components (including humans)**

Human Factors in Airworthiness Certification

- Human factors considered but separately
- Misses interaction problems between human and automation (particularly software)
  - Trying to fix automation design deficiencies through interface design or training is not very effective
  - STPA also identifies feedback requirements (what and when)
- Probabilistic analysis for human errors makes little sense
  - Pilots doing complex cognitive processing
  - Human behavior always affected by context in which it occurs