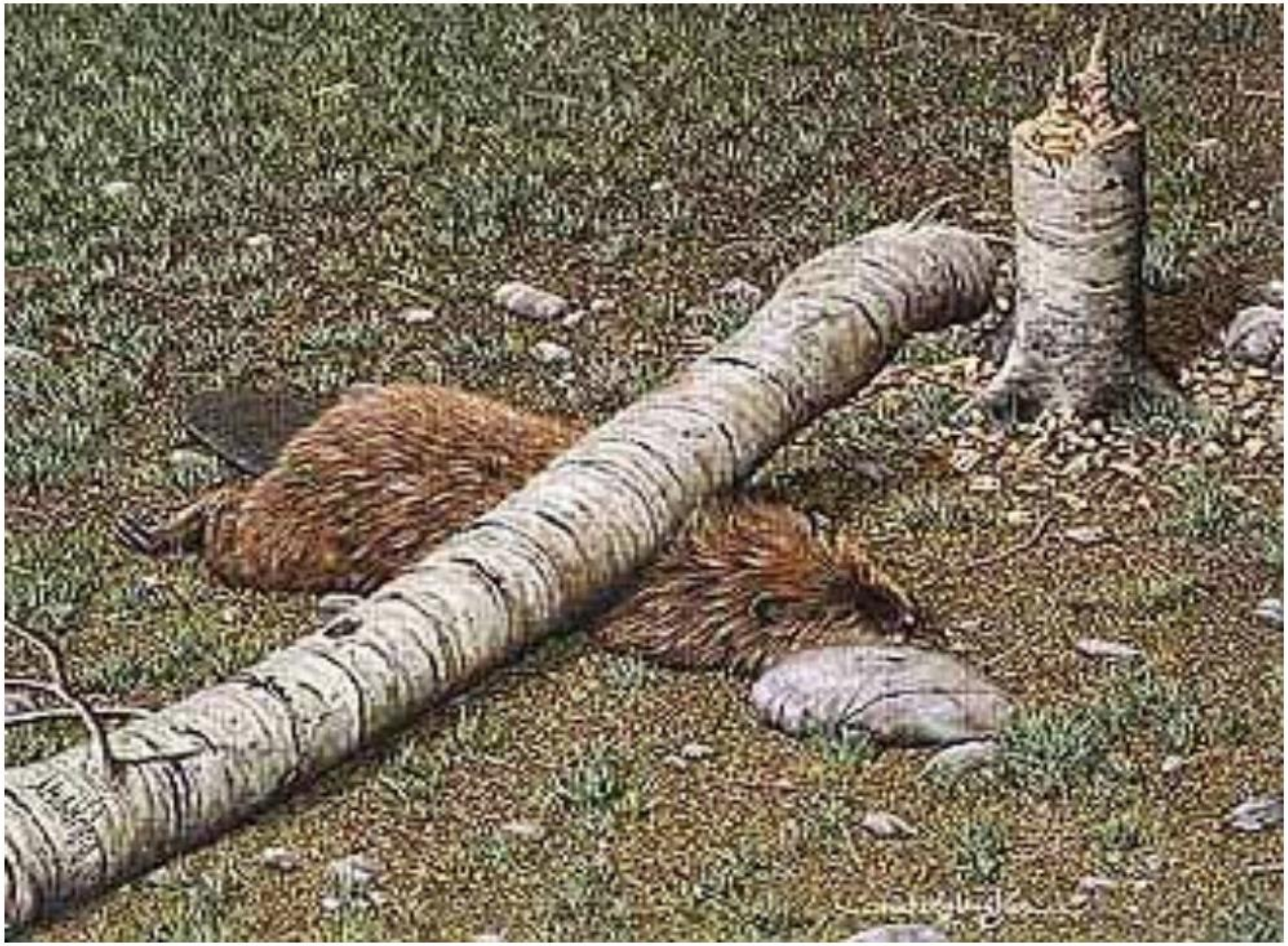
Engineering a Safer and More Secure World

Nancy Leveson

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



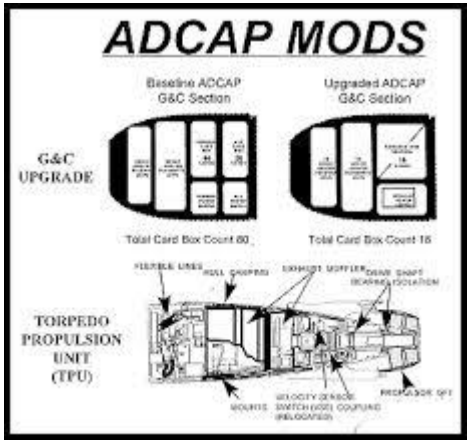
Goal for Session: Answer the Following Questions:

- Why do we need something new?
- What is STAMP and how does it differ from what people do now?
- What kinds of tools have been built on STAMP?
- Does it work?

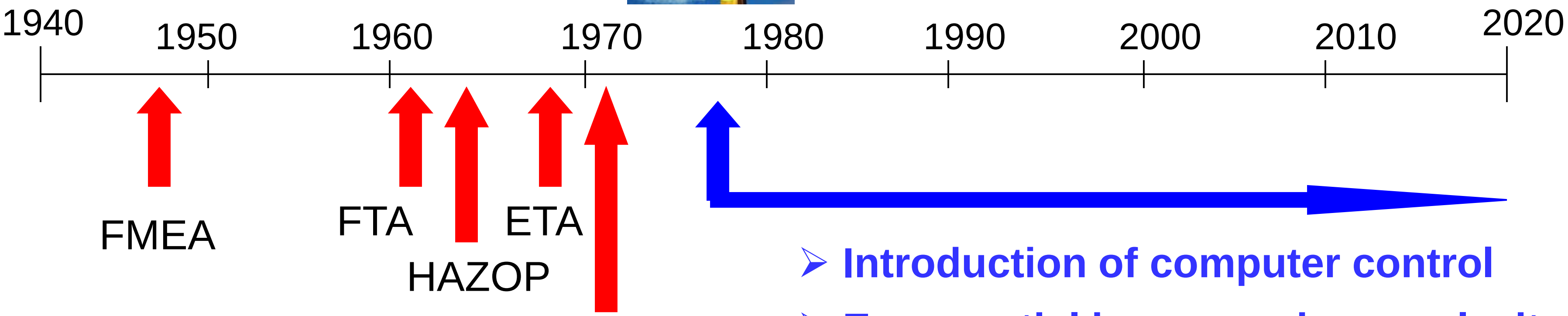
General Definition of “Safety”

- 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)
- System goals vs. constraints (limits on how can achieve the goals)
- Safety: Absence of losses

Why do we need something new?


ADCAP MODS
Baseline ADCAP G&C Section
Upgraded ADCAP G&C Section
G&C UPGRADE
Total Card Box Count 60
Total Card Box Count 16
FLEXIBLE LINES
HULL DAMPING
EXHAUST MUFFLER
DRIVE SHAFT BEARING ISOLATION
TORPEDO PROPULSION UNIT (TPU)
MOUNTS
VELOCITY SENSOR SWITCH (VSS) (RELOCATION)
COUPLING
PROPULSOR SFT

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



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

We Need Something New

- New levels of complexity do not fit into a reliability-oriented approach to safety.
- Two approaches being taken now:

Pretend there is no problem

Shoehorn new technology and new levels of complexity into old methods

Paradigm Change

- Does not imply what previously done is wrong and new approach correct
- Einstein:

“Progress in science (moving from one paradigm to another) is like climbing a mountain”

As move further up, can see farther than on lower points

Paradigm Change (2)

New perspective does not invalidate the old one, but extends and enriches our appreciation of the valleys below

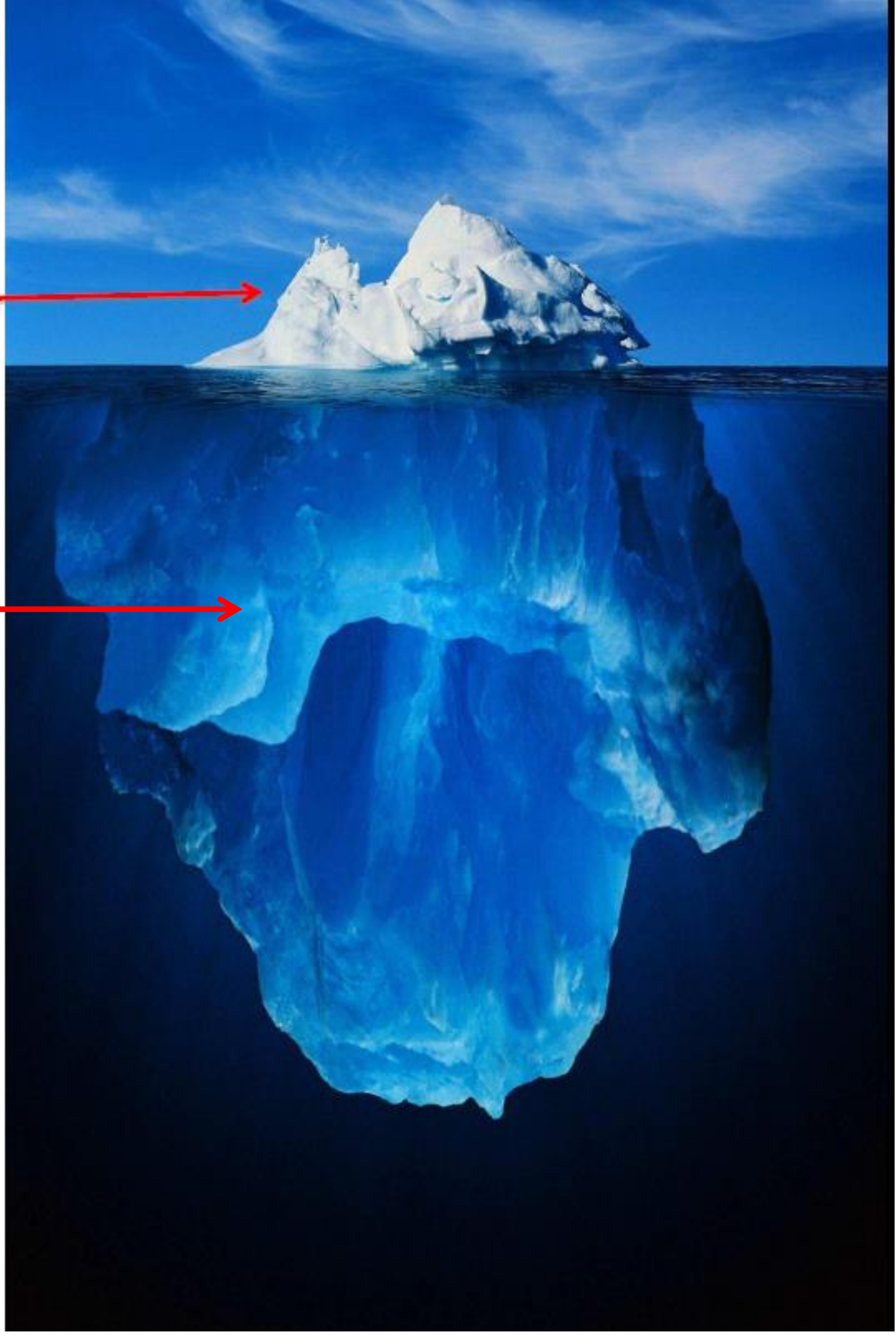
Value of new paradigm often depends on ability to accommodate successes and empirical observations made in old paradigm.

New paradigms offer a broader, rich perspective for interpreting previous answers.

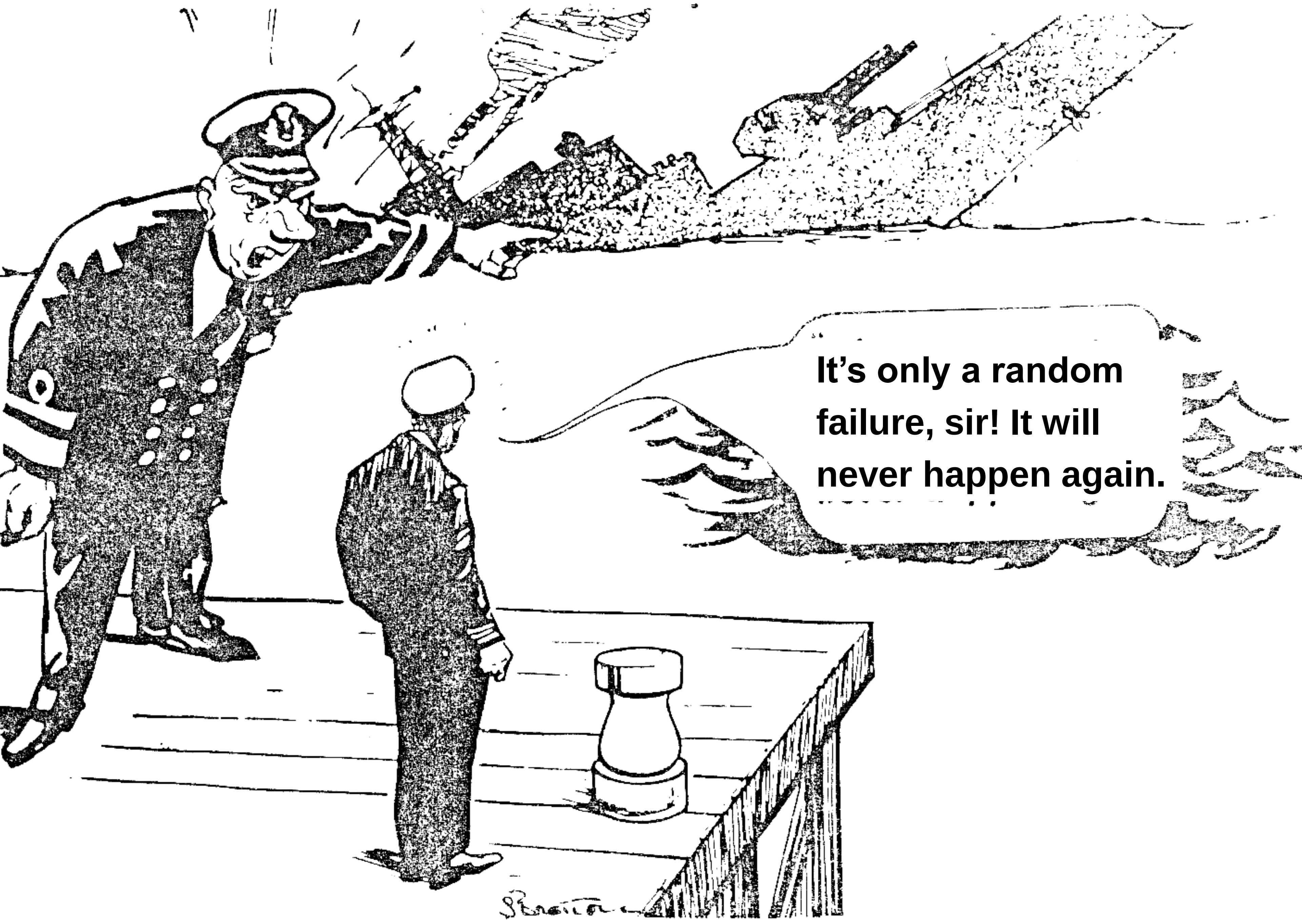
LEVERAGE

Event-based thinking

Systems Thinking
(STAMP)



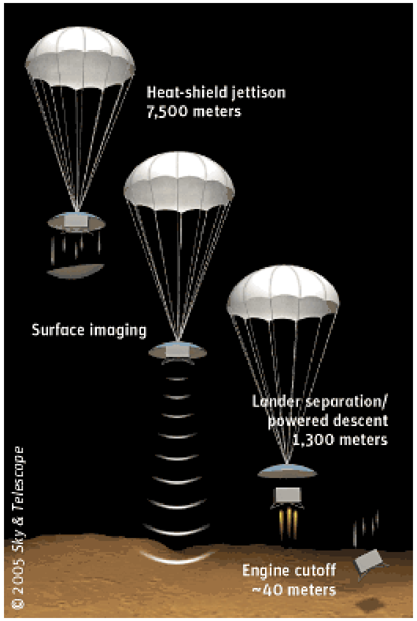
WYOUNG@MIT.EDU


It’s only a random failure, sir! It will never happen again.

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.

Accident with No Component Failures



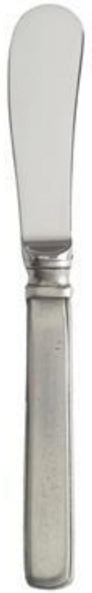
- Mars Polar Lander
  - Have to slow down spacecraft to land safely
  - Use Martian atmosphere, parachute, descent engines (controlled by software)
  - Software knows landed because of sensitive sensors on landing legs. Cut off engines when determine have landed.
  - But “noise” (false signals) by sensors 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

Warsaw A320 Accident

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

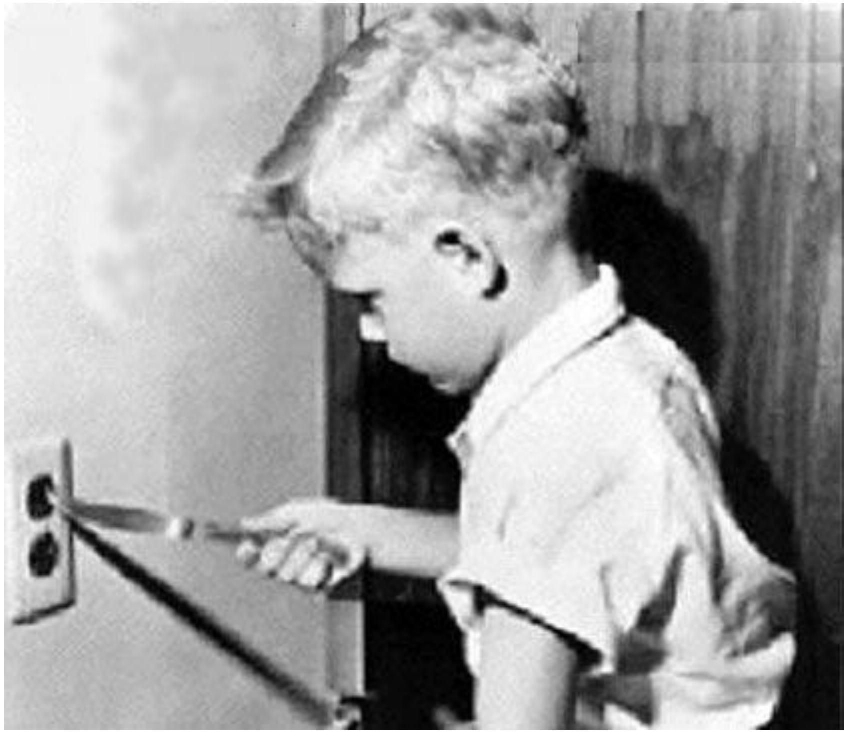
Washington State Ferry Problem

- 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.
- Rental cars could not be driven off ferries when got to port



Safe or Unsafe?

Safety Depends on Context

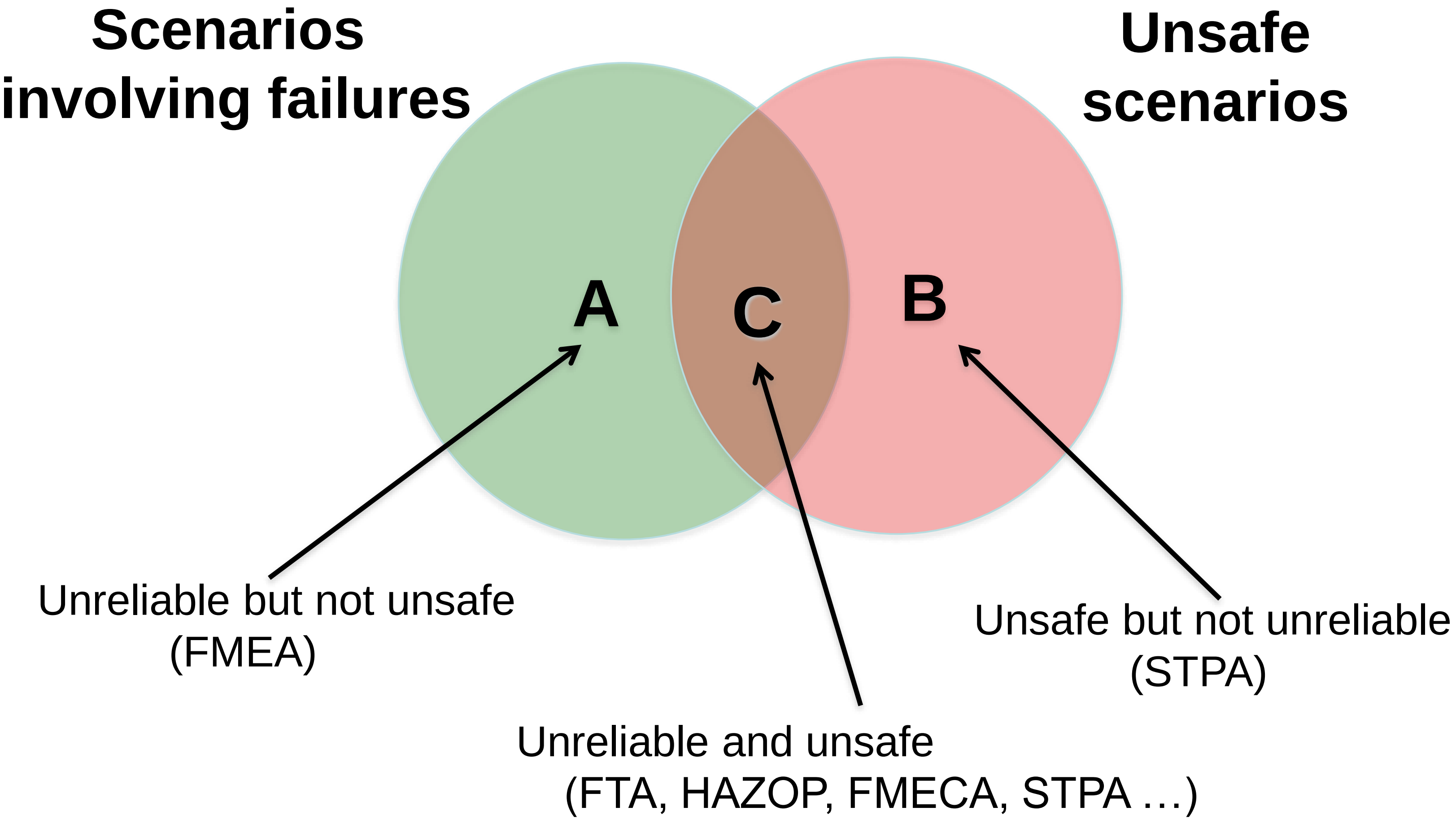


Two Types of Accidents

- **Component Failure Accidents**
  - Single or multiple component failures
  - Usually assume random failure

- **Component Interaction Accidents**
  - Arise in interactions among components
  - Related to complexity (coupling) in our system designs, which leads to system design and system engineering errors
  - No components may have “failed”
  - Exacerbated by introduction of computers and software but the problem is system design errors
    - Software allows almost unlimited complexity in our designs

Confusing Safety and Reliability



Unreliable but not unsafe
(FMEA)

Unsafe but not unreliable
(STPA)

Unreliable and unsafe
(FTA, HAZOP, FMECA, STPA …)

Preventing Component or Functional Failures is Not Enough

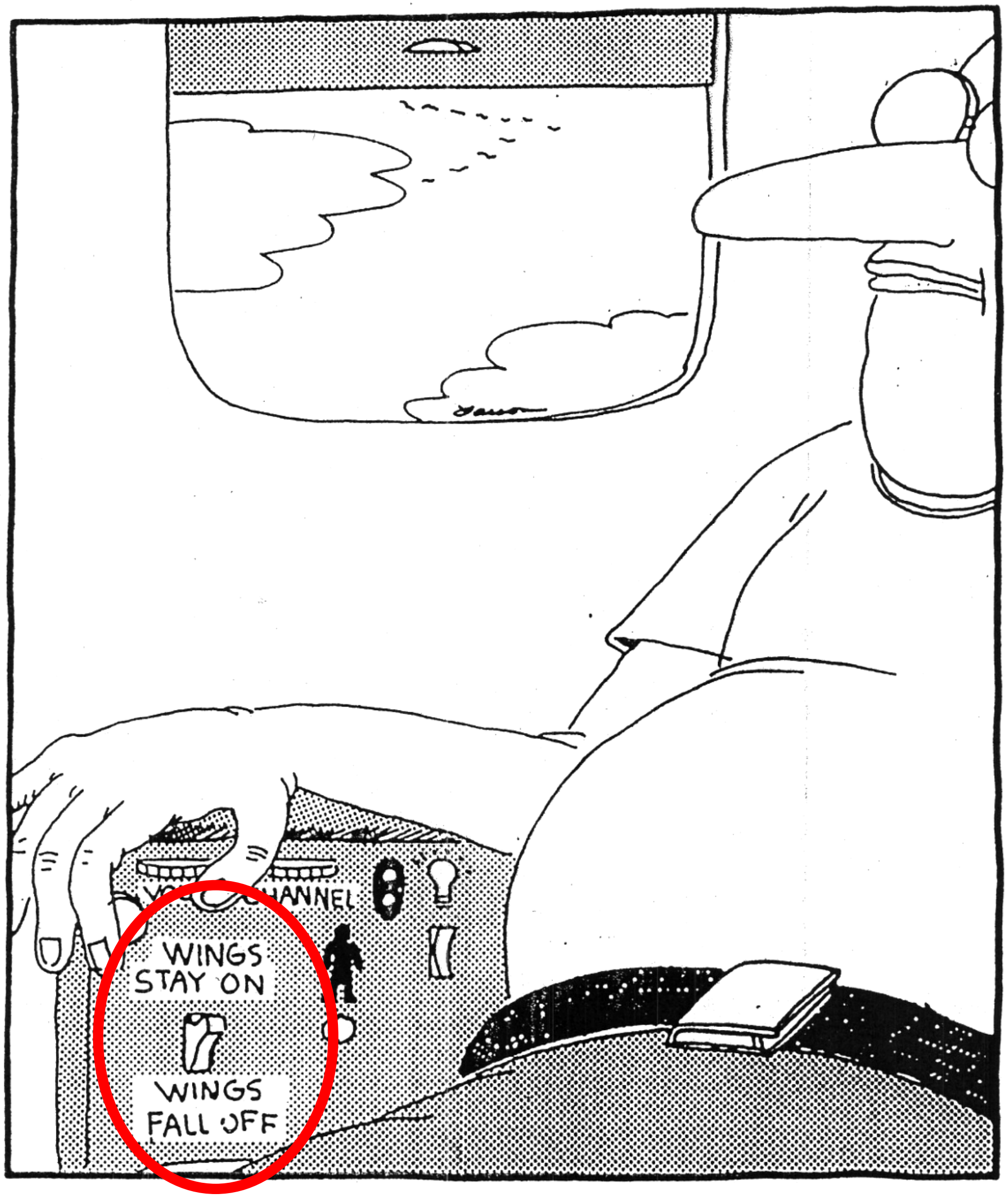
Software changes the role of humans in systems

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

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.

Another Accident Involving Thrust Reversers

- 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

- 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

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**

Human factors concentrates on the “screen out”

Hardware/Software engineering concentrates on the “screen in”

Not enough attention on integrated system as a whole

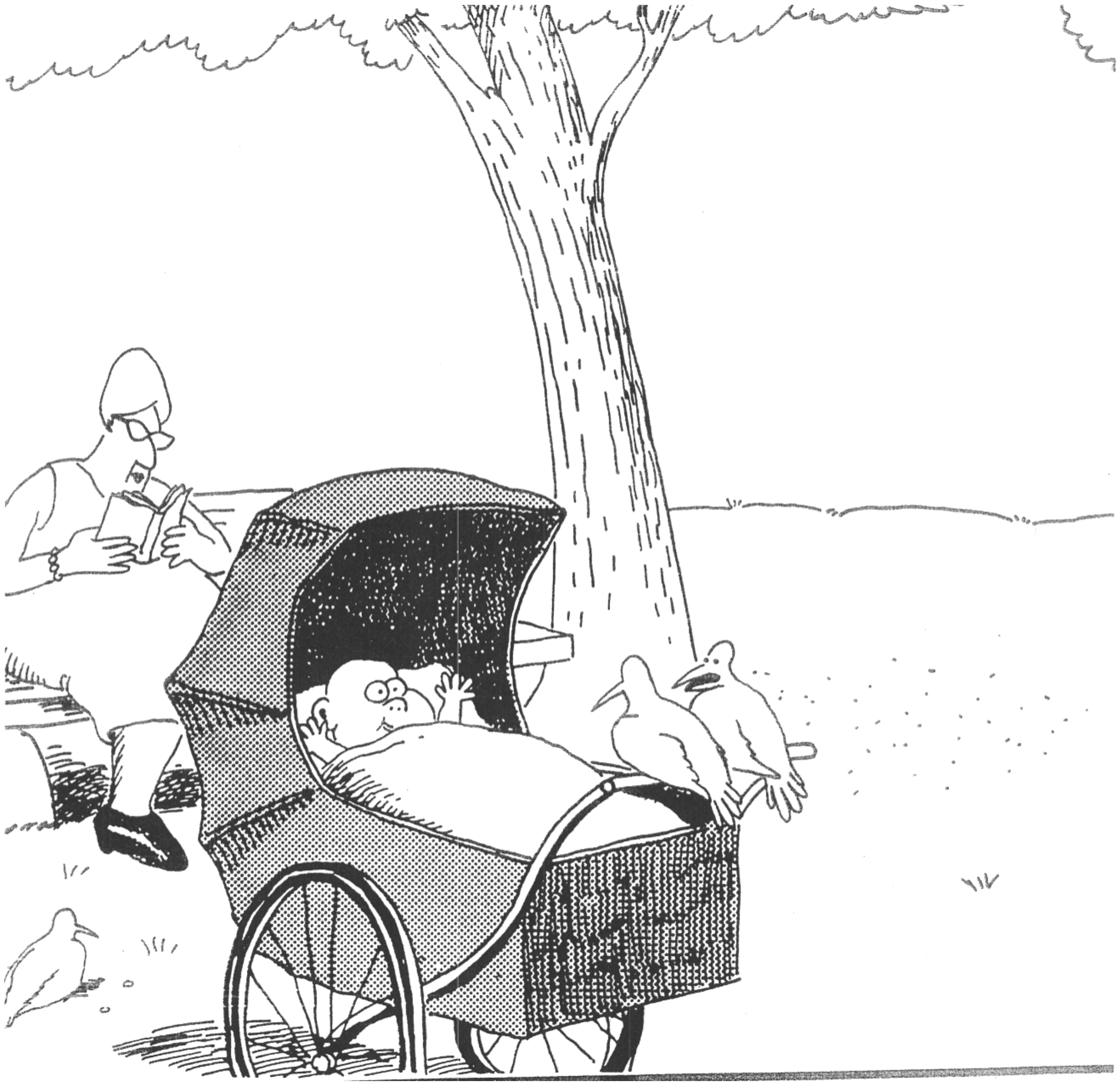
www.shutterstock.com · 116515978

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

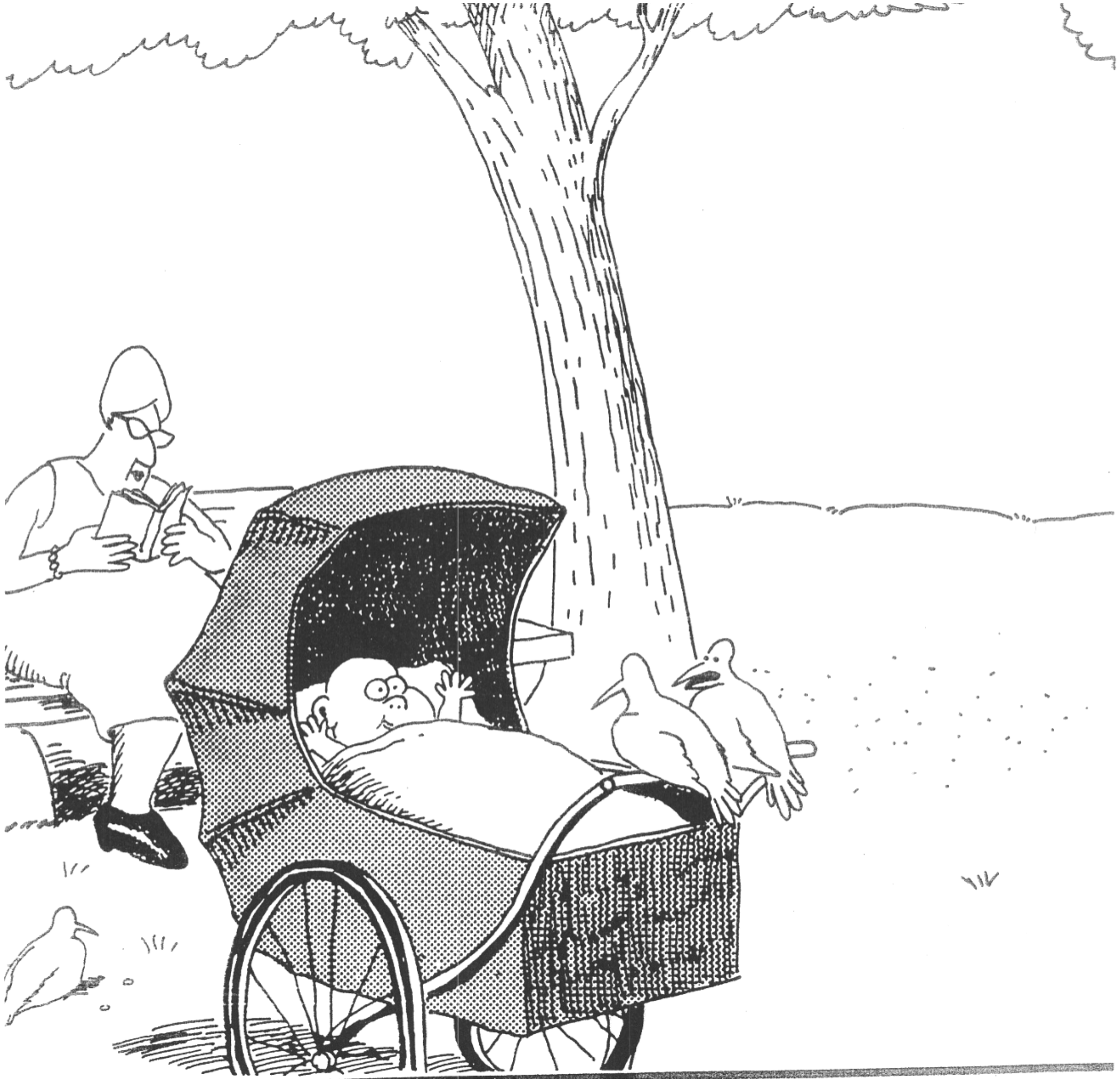
Summary of the Problem:

- We need models and tools that handle:
  - Hardware and hardware failures
  - Software (particularly requirements)
  - Human factors
  - Interactions among system components
  - System design errors
  - Management, regulation, policy
  - Environmental factors
  - “Unknown unknowns”

And the interactions among all these things



It’s still hungry … and I’ve been stuffing worms into it all day.



It’s still hungry … and I’ve been stuffing worms into it all day.

We Need New Tools for the New Problems

What is STAMP and how does it differ from what people do now?

The Problem is Complexity

Ways to Cope with Complexity

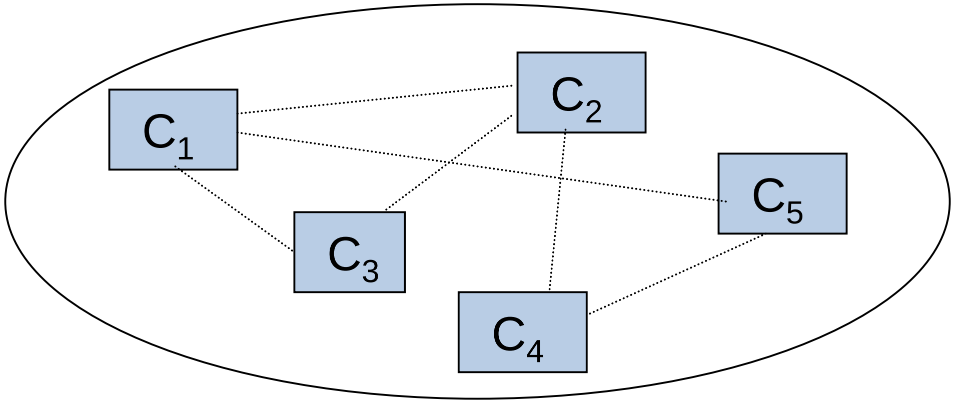
- Analytic Decomposition
- Statistics
- Systems Theory

Traditional Approach to Coping with Complexity

Analytic Decomposition ("Divide and Conquer")

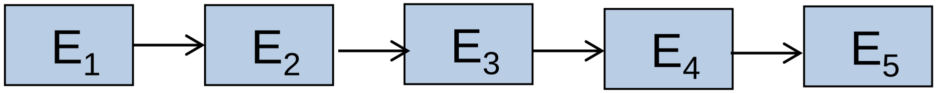
1. Divide system into separate parts

<u>Physical/Functional</u>: Separate into distinct components



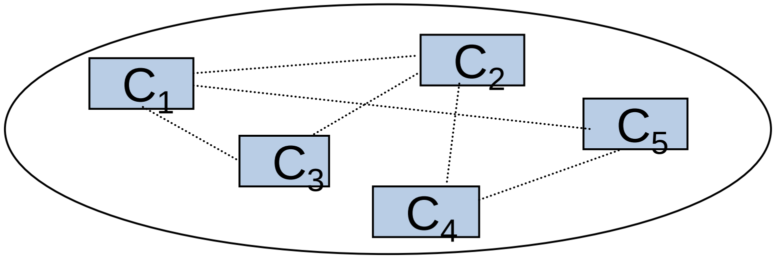
Components interact
In direct ways

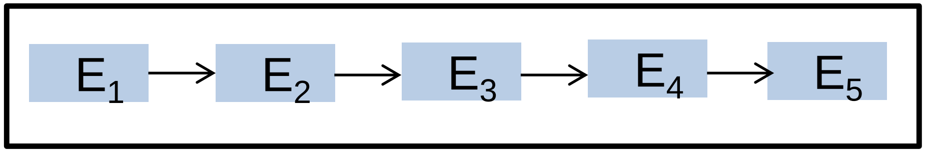
<u>Behavior</u>: Separate into events over time



Each event is the direct
result of the preceding event

Analytic Decomposition (2)





2. Analyze/examine pieces separately and combine results

- Assumes such separation does not distort phenomenon
  - ✓ Each component or subsystem operates independently
  - ✓ Components act the same when examined singly as when playing their part in the whole
  - ✓ Components/events not subject to feedback loops and non-linear interactions
  - ✓ Interactions can be examined pairwise

Bottom Line

- These assumptions are no longer true in our
  - Tightly coupled
  - Software intensive
  - Highly automated
  - Connected

  engineered systems

- Need a new theoretical basis
  - *System theory* can provide it

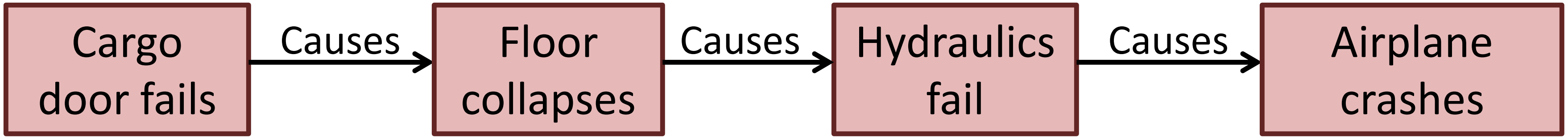
Traditional Approach to Safety Engineering

- Assume accidents caused by chains of failure events
- Forms the basis for most safety engineering and reliability engineering analysis:

  FTA, PRA, FMEA/FMECA, Event Trees, FHA, etc.
- Evaluate reliability of components separately and later combine analysis results into a system reliability value (assumes randomness, do software and humans behave this way?)
- Design (concentrate on dealing with component failure):
  - Redundancy and barriers (to prevent failure propagation),
  - High component integrity and overdesign,
  - Fail-safe design,
  - (humans) Operational procedures, checklists, training, ….

Domino “Chain of events” Model

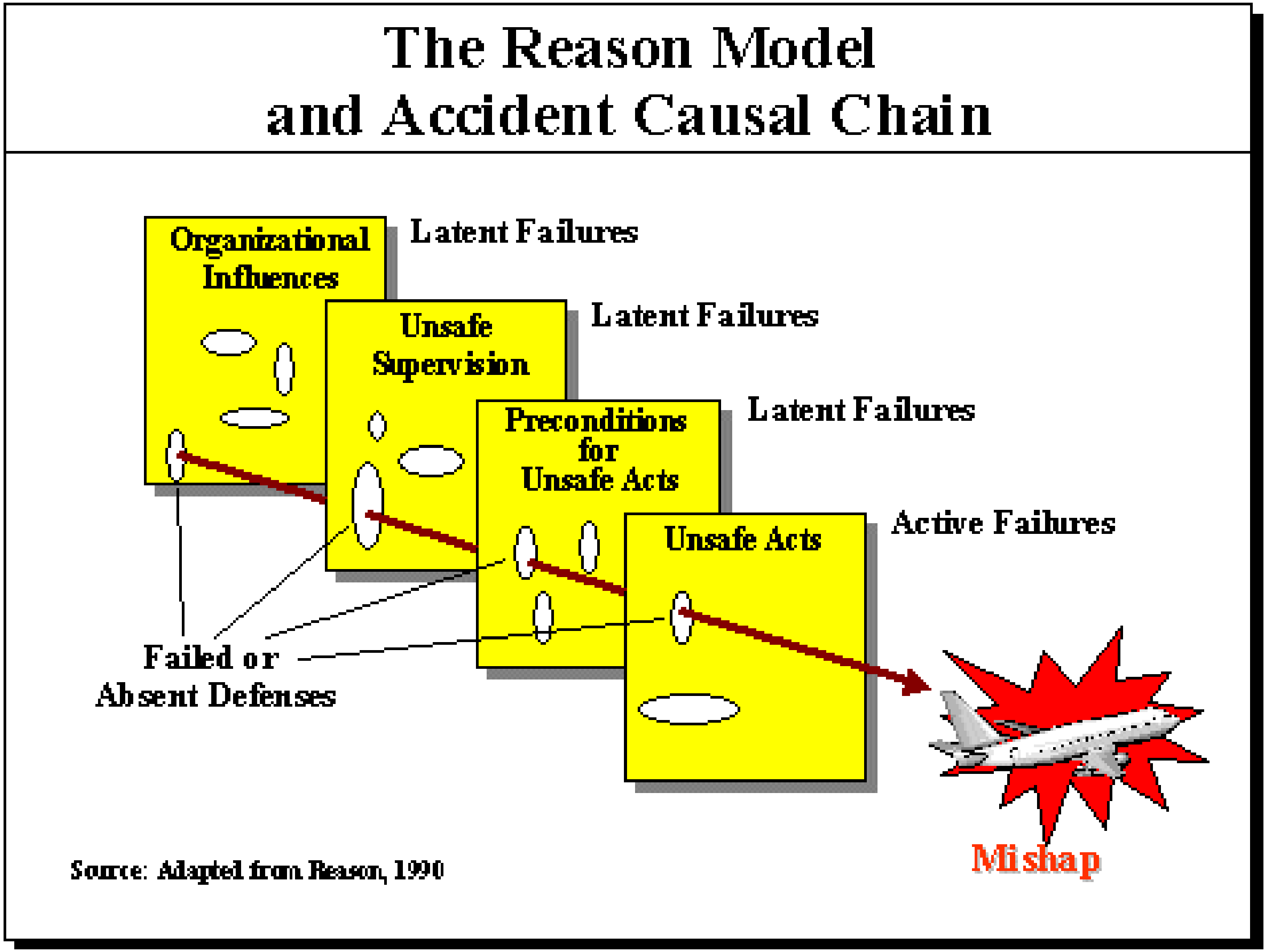
DC-10:



Cargo door fails → Causes → Floor collapses → Causes → Hydraulics fail → Causes → Airplane crashes

Chain of Failure Events

Reason Swiss Cheese (1990)

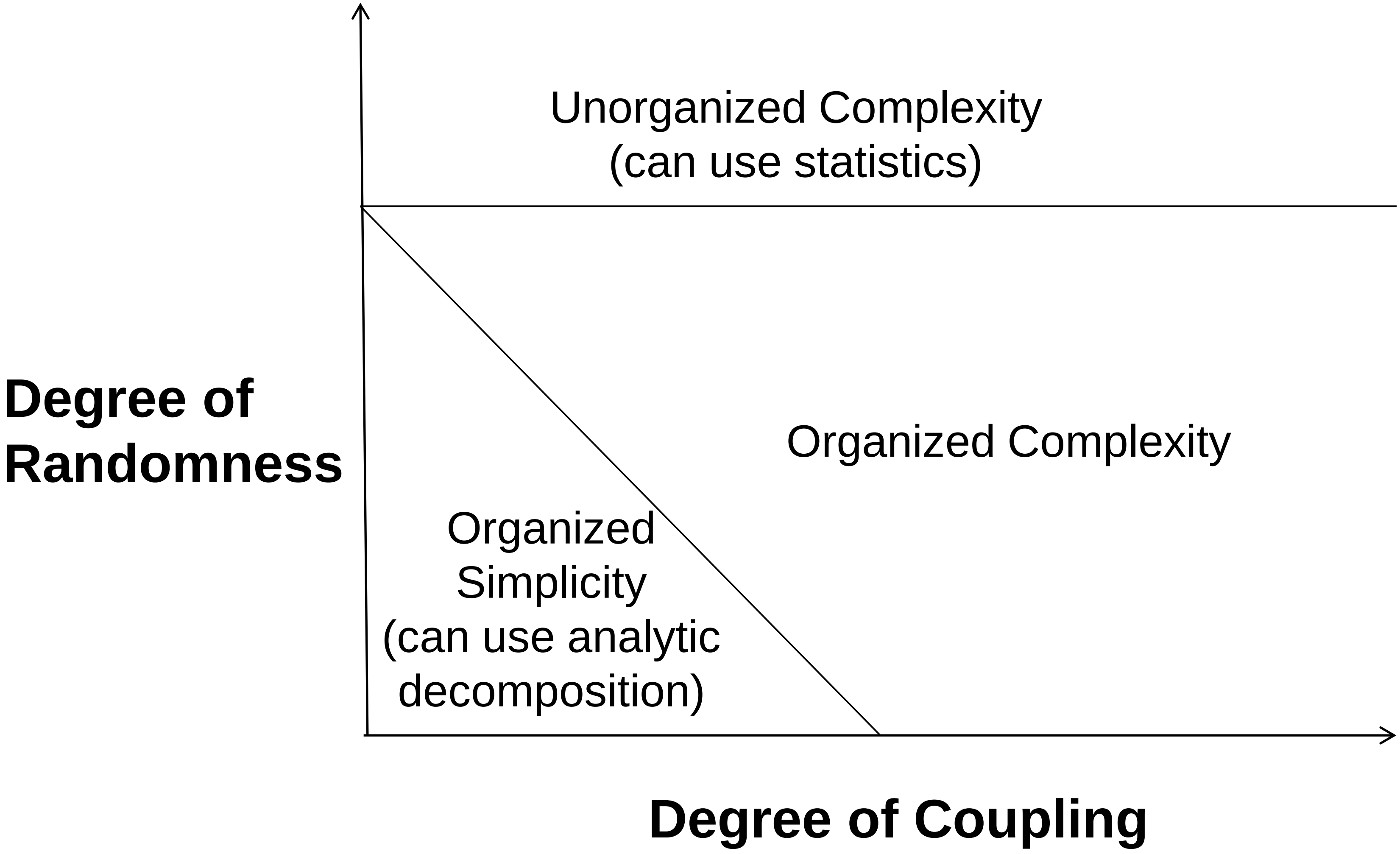


The Reason Model and Accident Causal Chain

Source: Adapted from Reason, 1990

Standard Safety Approach does not Handle

- Component interaction accidents
- Systemic factors (affecting all components and barriers)
- Software and software requirements errors
- Human behavior (in a non-superficial way)
- System design errors
- Indirect or non-linear interactions and complexity
- Culture and management
- Migration of systems toward greater risk over time (e.g., in search for greater efficiency and productivity)



[Credit to Gerald Weinberg]

Here comes the paradigm change!

Systems Theory

- Developed for systems that are
  - Too complex for complete analysis
    - Separation into (interacting) subsystems distorts the results
    - The most important properties are emergent
  - Too organized for statistics
    - Too much underlying structure that distorts the statistics
    - New technology and designs have no historical information
- First used on ICBM systems of 1950s/1960s

System Theory was created to provide a more powerful way to deal with complexity

Systems Theory (2)

- Focuses on systems taken as a whole, not on parts taken separately

- Emergent properties
  - Some properties can only be treated adequately in their entirety, taking into account all social and technical aspects

    "The whole is greater than the sum of the parts"

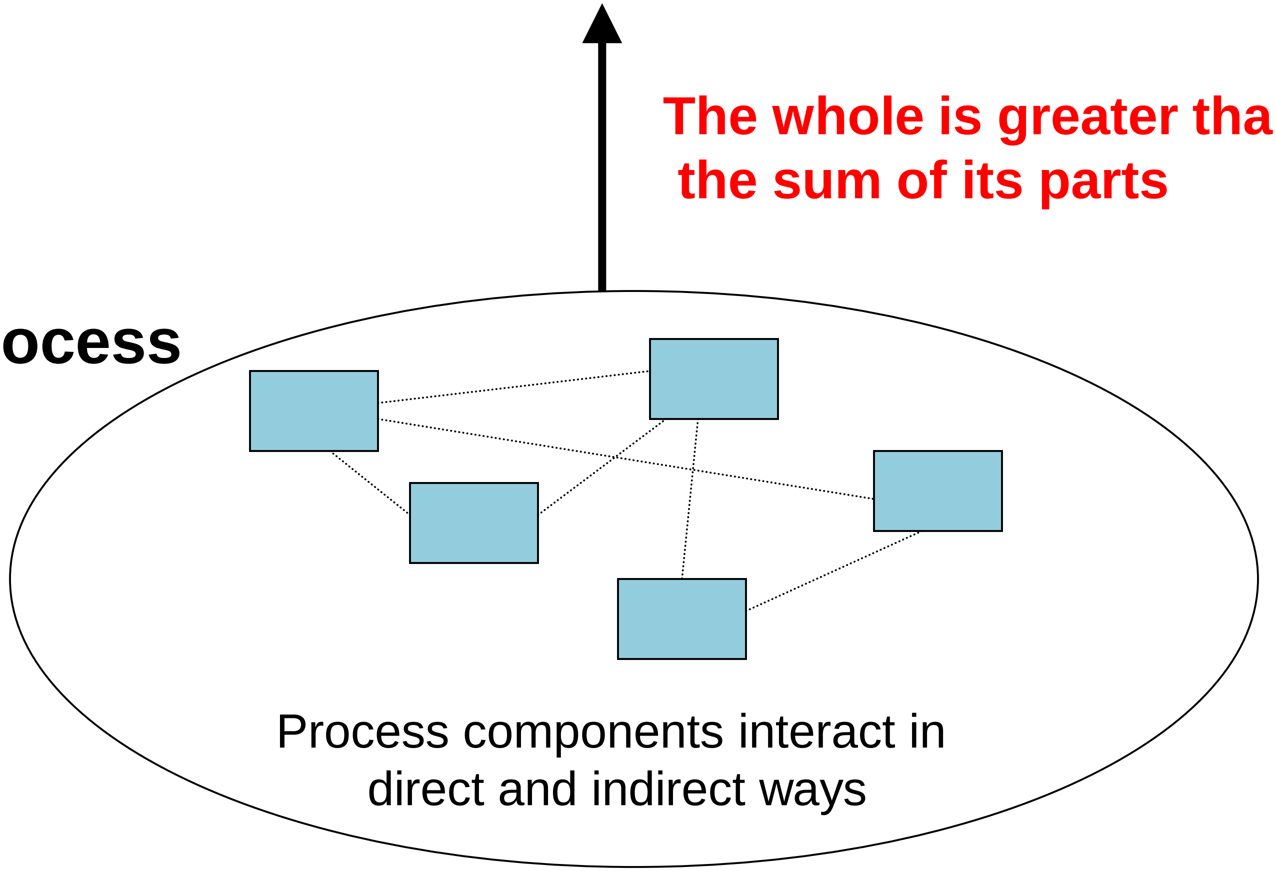
  - These properties arise from relationships among the parts of the system

    How they interact and fit together

System Theory

Emergent properties

(arise from complex interactions)



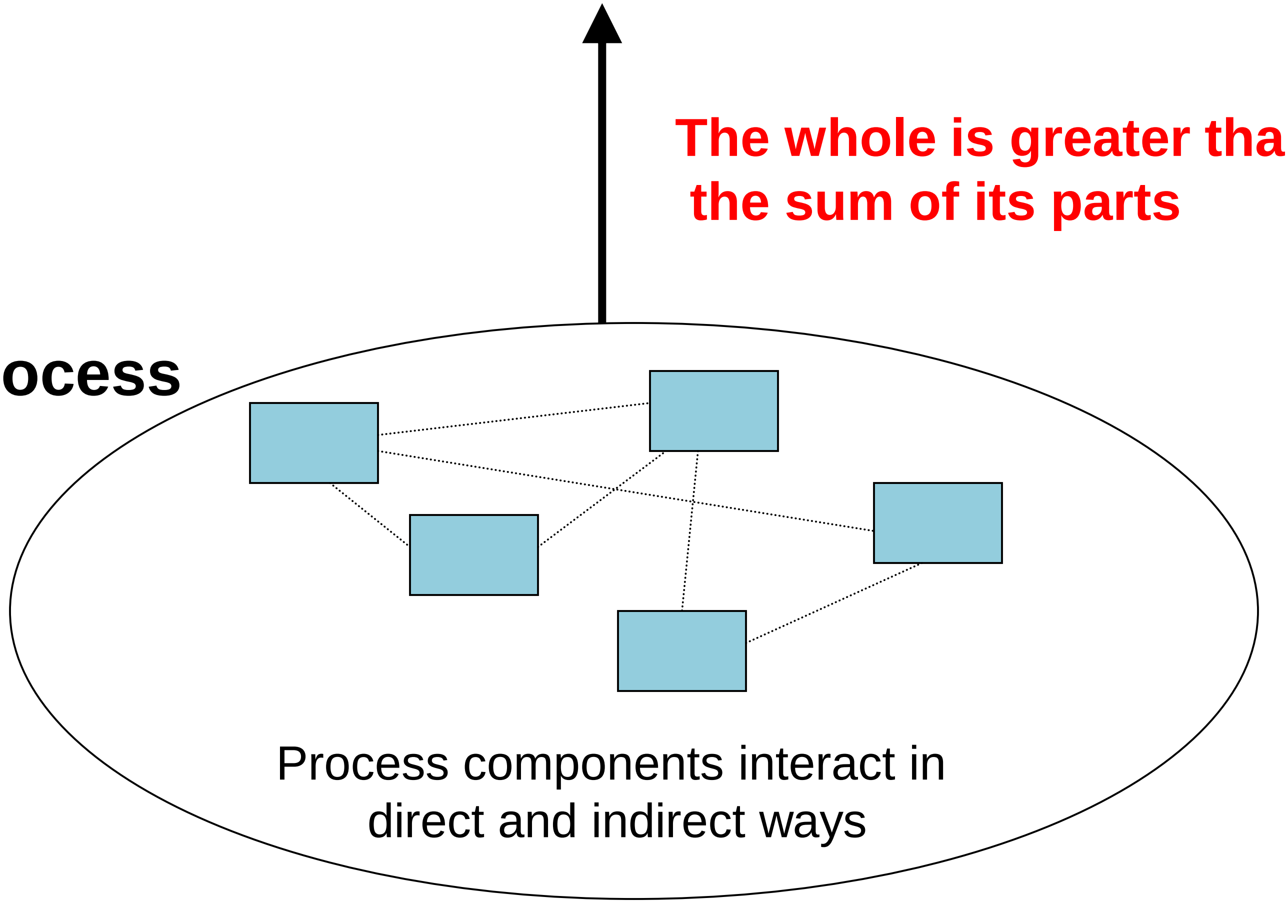
The whole is greater than the sum of its parts

Process

Process components interact in direct and indirect ways

Emergent properties

(arise from complex interactions)



The whole is greater than the sum of its parts

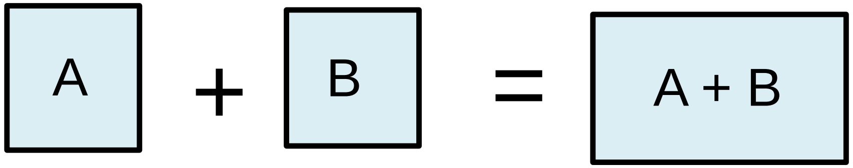
Process

Process components interact in direct and indirect ways

Safety and security are emergent properties

Cannot simply compose systems into a “system of systems”

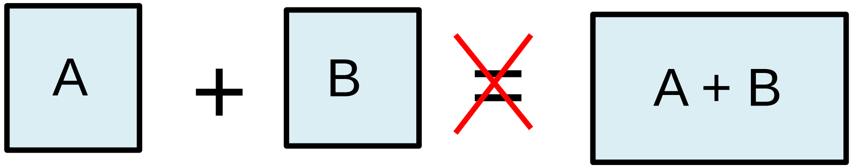
- Assumption



A + B = A + B

Cannot simply compose systems into a “system of systems”

- Assumption

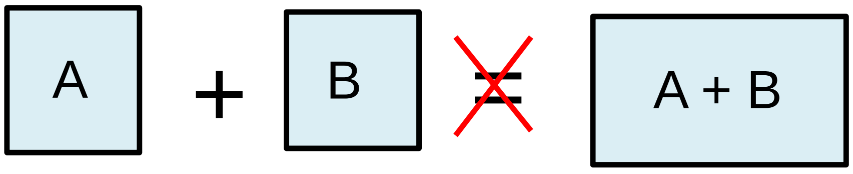


A + B ≠ A + B

but **not true**

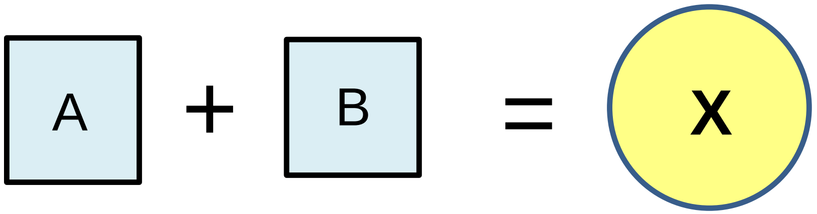
Cannot simply compose systems into a “system of systems”

- Assumption

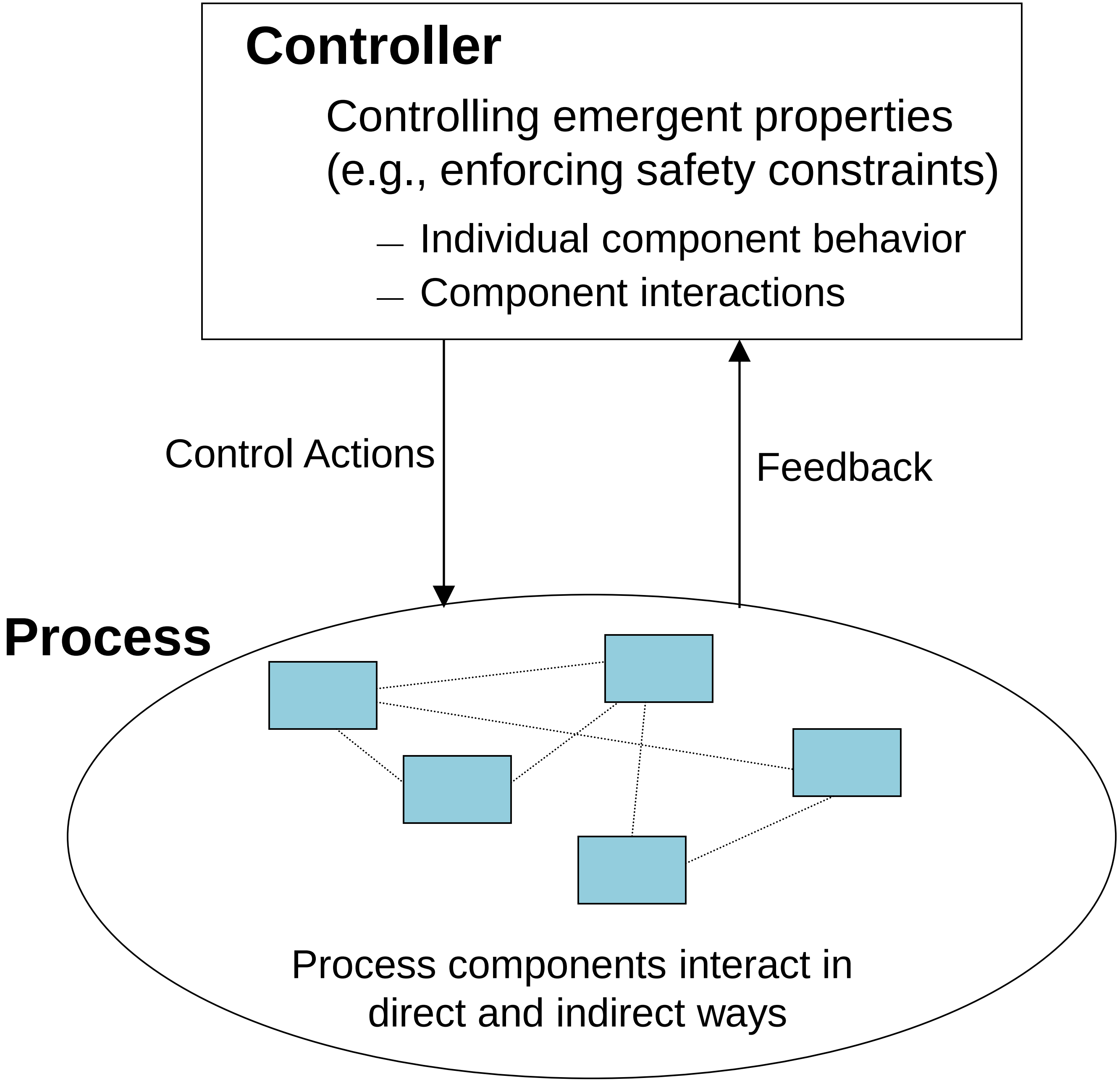


but **not true**

- In reality



Putting two systems together gives you a new and different system with different emergent properties



Controller

Controlling emergent properties
(e.g., enforcing safety constraints)

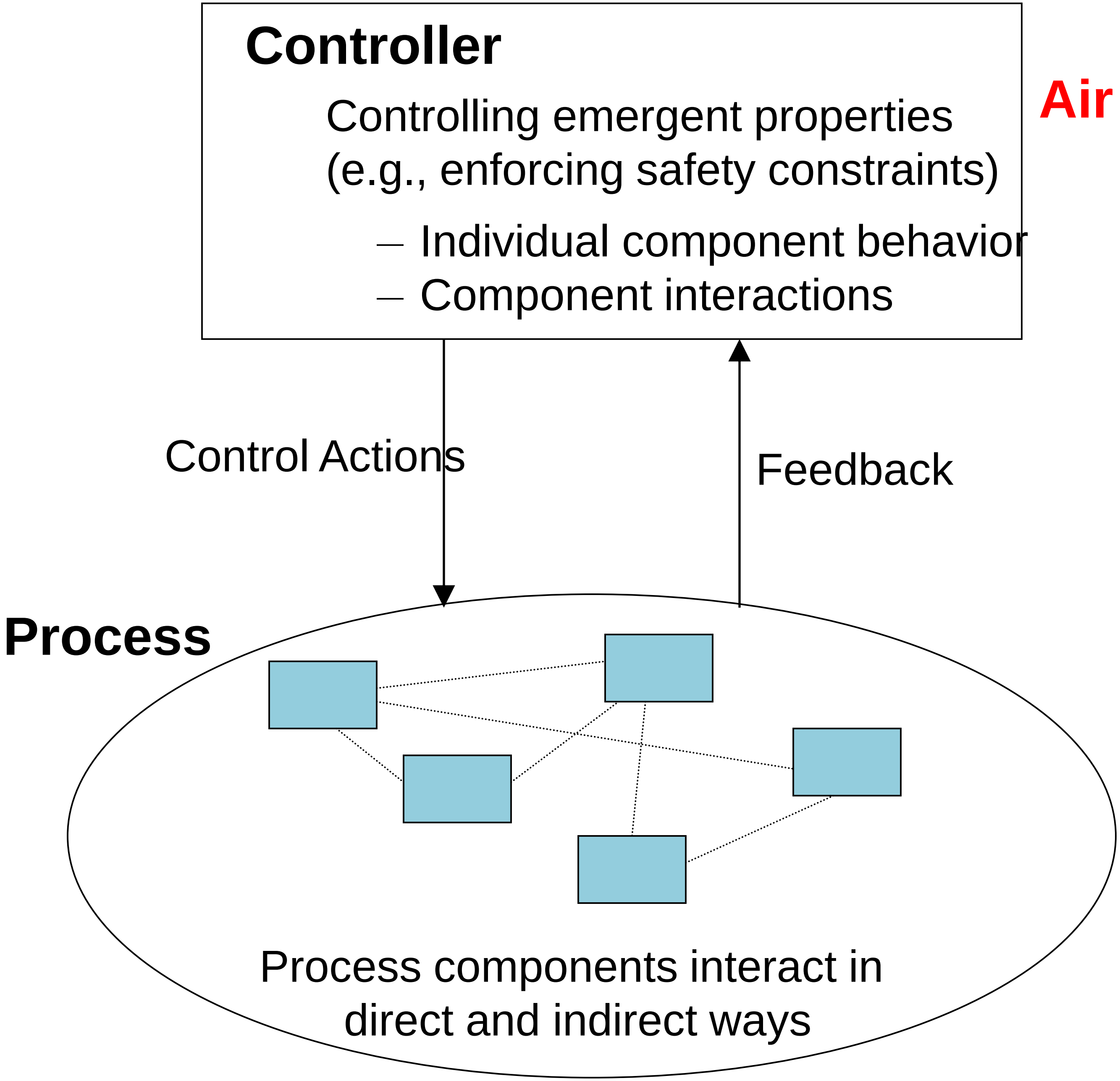
- Individual component behavior
- Component interactions

Control Actions

Feedback

Process

Process components interact in
direct and indirect ways



Controller

Controlling emergent properties (e.g., enforcing safety constraints)

- Individual component behavior
- Component interactions

Control Actions

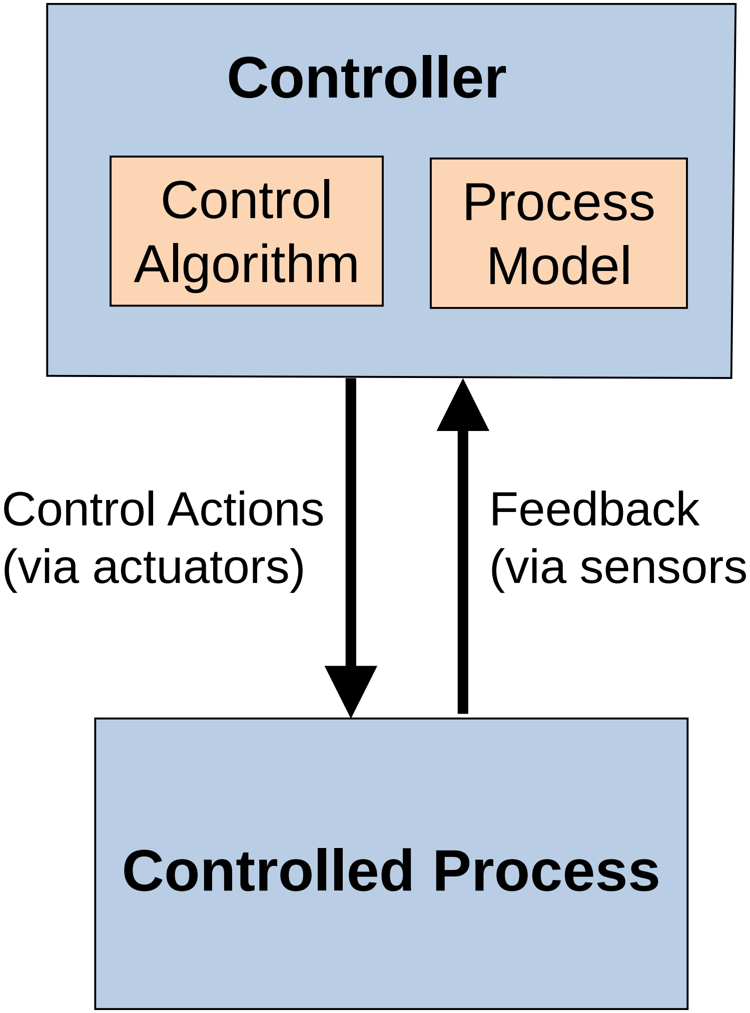
Feedback

Process

Process components interact in direct and indirect ways

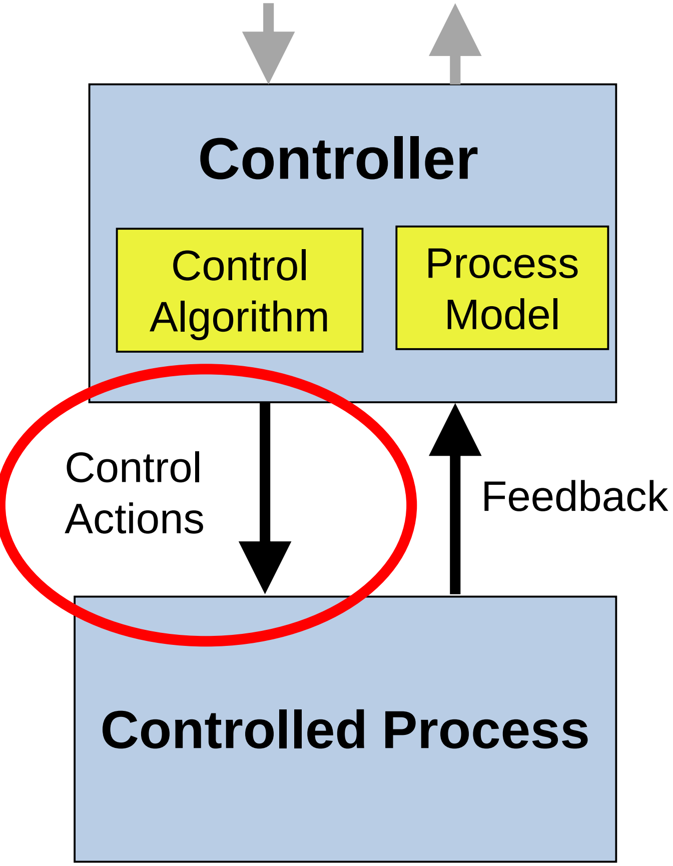
Air Traffic Control:
Safety
Throughput

Role of Process Models in Control



- 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 …

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
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?

Integrated Approach to Safety and Security

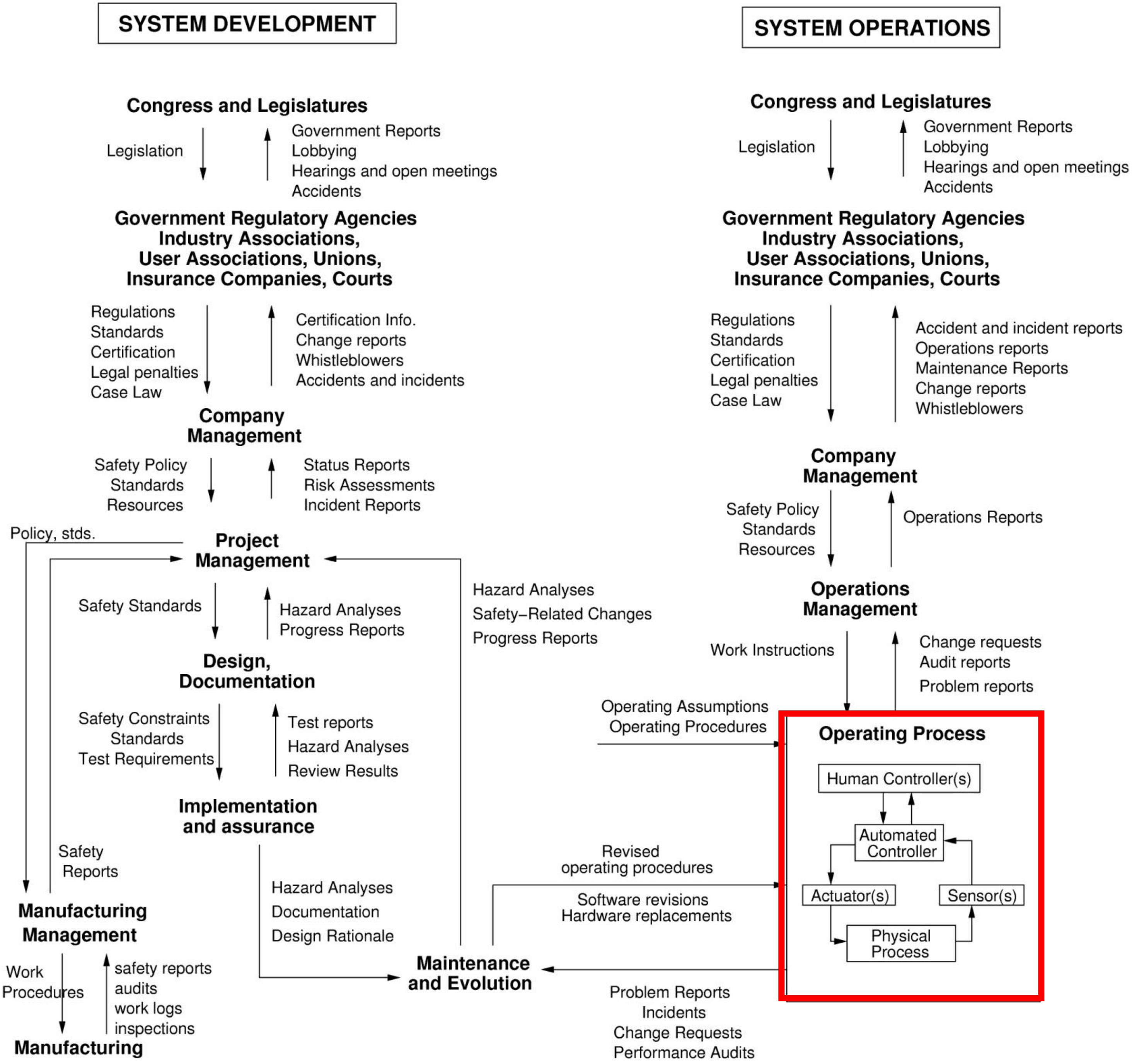
- Both concerned with losses (intentional or unintentional)
  - Ensure that critical functions and services are maintained
  - New paradigm for safety will work for security too
    - May have to add new causes, but rest of process is the same
  - A top-down, system engineering approach to designing safety and security into systems

Example: Stuxnet

- Loss: Damage to reactor (in this case centrifuges)
- Hazard/Vulnerability: Centrifuges are damaged by spinning too fast
- Constraint to be Enforced: Centrifuges must never spin above maximum speed
- Hazardous 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
    - Could be inadvertent or deliberate
- Potential controls:
  - Mechanical limiters (interlock), Analog RPM gauge

Focus on preventing hazardous state
(not keeping intruders out)

Example Safety Control Structure (SMS)



SYSTEM DEVELOPMENT

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Certification Info.
Change reports
Whistleblowers
Accidents and incidents

Company Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, stds.

Project Management

Safety Standards

Hazard Analyses
Progress Reports

Hazard Analyses
Safety–Related Changes
Progress Reports

Design, Documentation

Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation and assurance

Safety Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing Management

Work Procedures

safety reports
audits
work logs
inspections

Manufacturing

Maintenance and Evolution

SYSTEM OPERATIONS

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers

Company Management

Safety Policy
Standards
Resources

Operations Reports

Operations Management

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

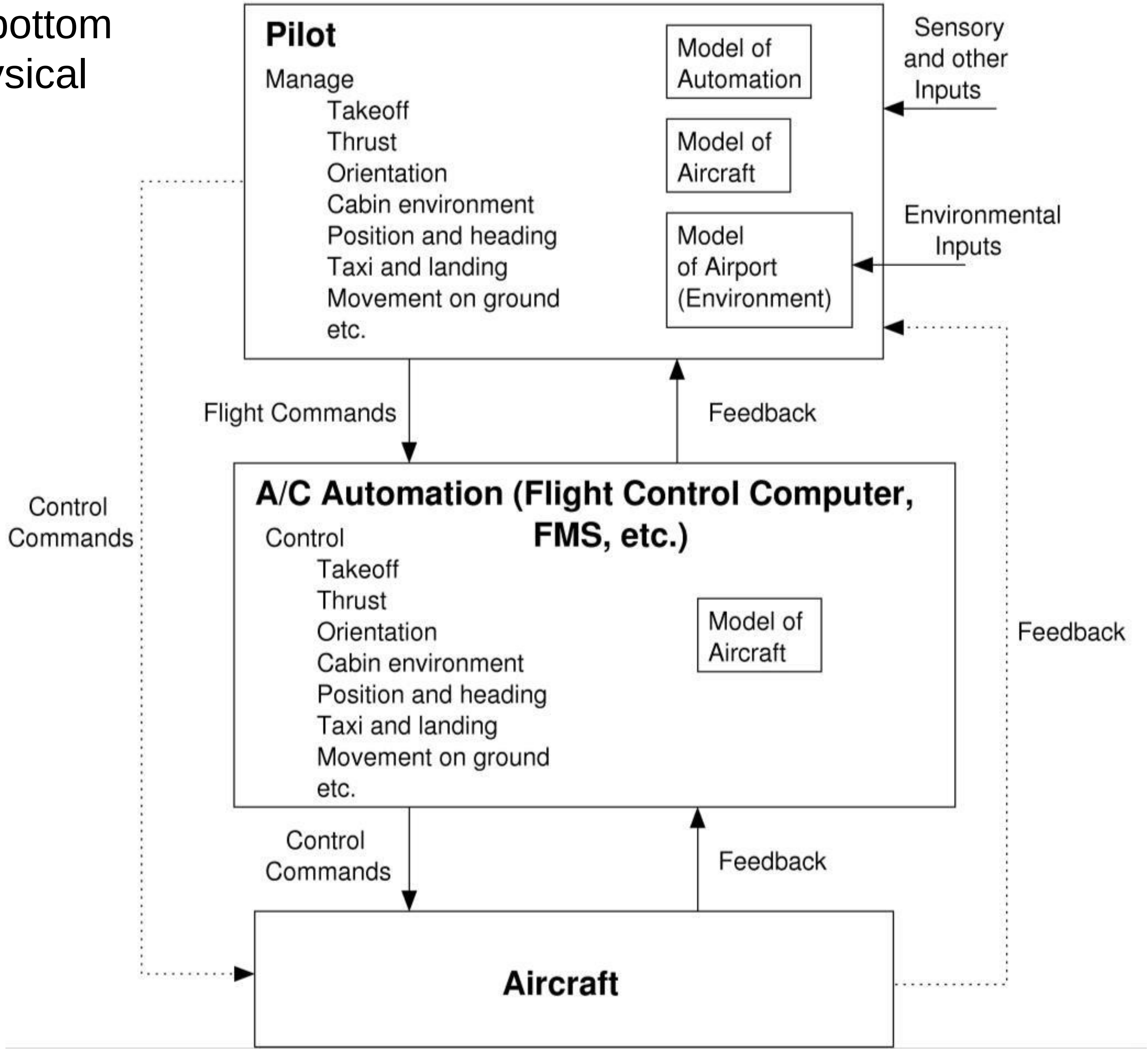
Physical Process

Revised operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

[Box on bottom right, physical process]



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)

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

Aircraft

Controls/Controllers Enforce Safety Constraints

- Power must never be on when access door open
- Two aircraft/automobiles must not violate minimum separation
- Aircraft must maintain sufficient lift to remain airborne
- Integrity of hull must be maintained on a submarine
- Toxic chemicals/radiation must not be released from plant
- Workers must not be exposed to workplace hazards
- Public health system must prevent exposure of public to contaminated water and food products
- Pressure in a offshore well must be controlled

These are the High-Level Functional Safety/Security Requirements to Address During Design

A Broad View of “Control”

Component failures and unsafe interactions may be “controlled” through design

(e.g., redundancy, interlocks, fail-safe design)

or through process

- Manufacturing processes and procedures
- Maintenance processes
- Operations

or through social controls

- Governmental or regulatory
- Culture
- Insurance
- Law and the courts
- Individual self-interest (incentive structure)

STAMP

(System-Theoretic Accident Model and Processes)

- A new, more powerful accident/loss causality model
- Based on systems theory, not reliability theory
- Defines accidents/losses as a dynamic control problem (vs. a failure problem)
- Applies to VERY complex systems
- Includes
  - Scenarios from traditional hazard analysis methods (failure events)
  - Component interaction accidents
  - Software and system design errors
  - Human errors
  - Entire socio-technical system (not just technical part)

Safety as a Dynamic Control Problem (STAMP)

- Hazards result from lack of enforcement of safety constraints in system design and operations

- Goal is to control the behavior of the components and systems as a whole to ensure safety constraints are enforced in the operating system

- A change in emphasis:

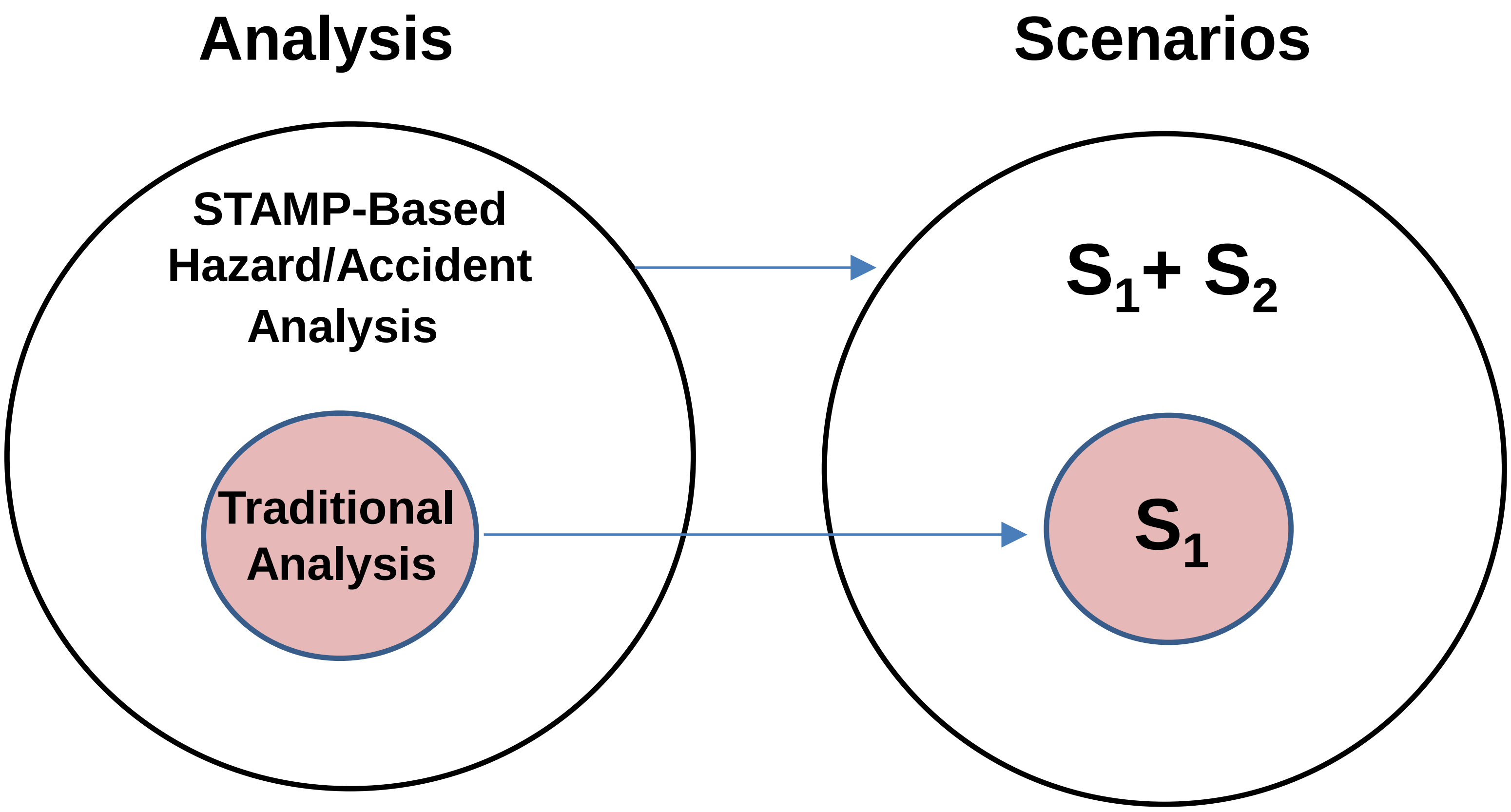
~~Increase component reliability (prevent failures)~~

⬇

Enforce safety/security constraints on system behavior

(note that enforcing constraints might require preventing failures or handling them but includes more than that)

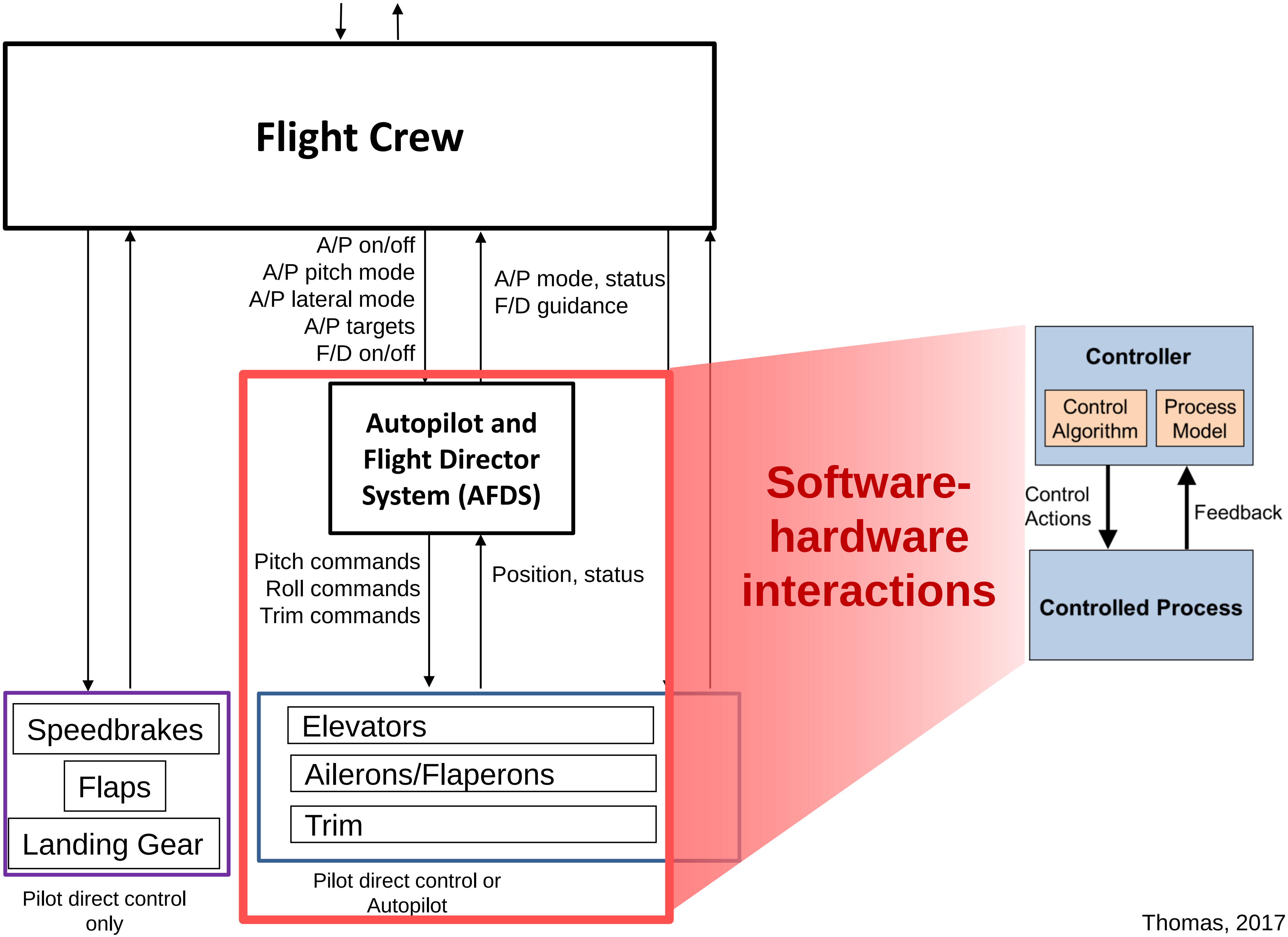
STAMP-Based vs. Traditional Analysis



Safety as a Control Problem

Goal: Design an effective control structure that eliminates or reduces adverse events.

- Need clear definition of expectations, responsibilities, authority, and accountability at all levels of safety control structure
- Need appropriate feedback
- Entire control structure must together enforce the system safety property (constraints)
  - Physical design (inherent safety)
  - Operations
  - Management
  - Social interactions and culture



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

Pilot direct control only

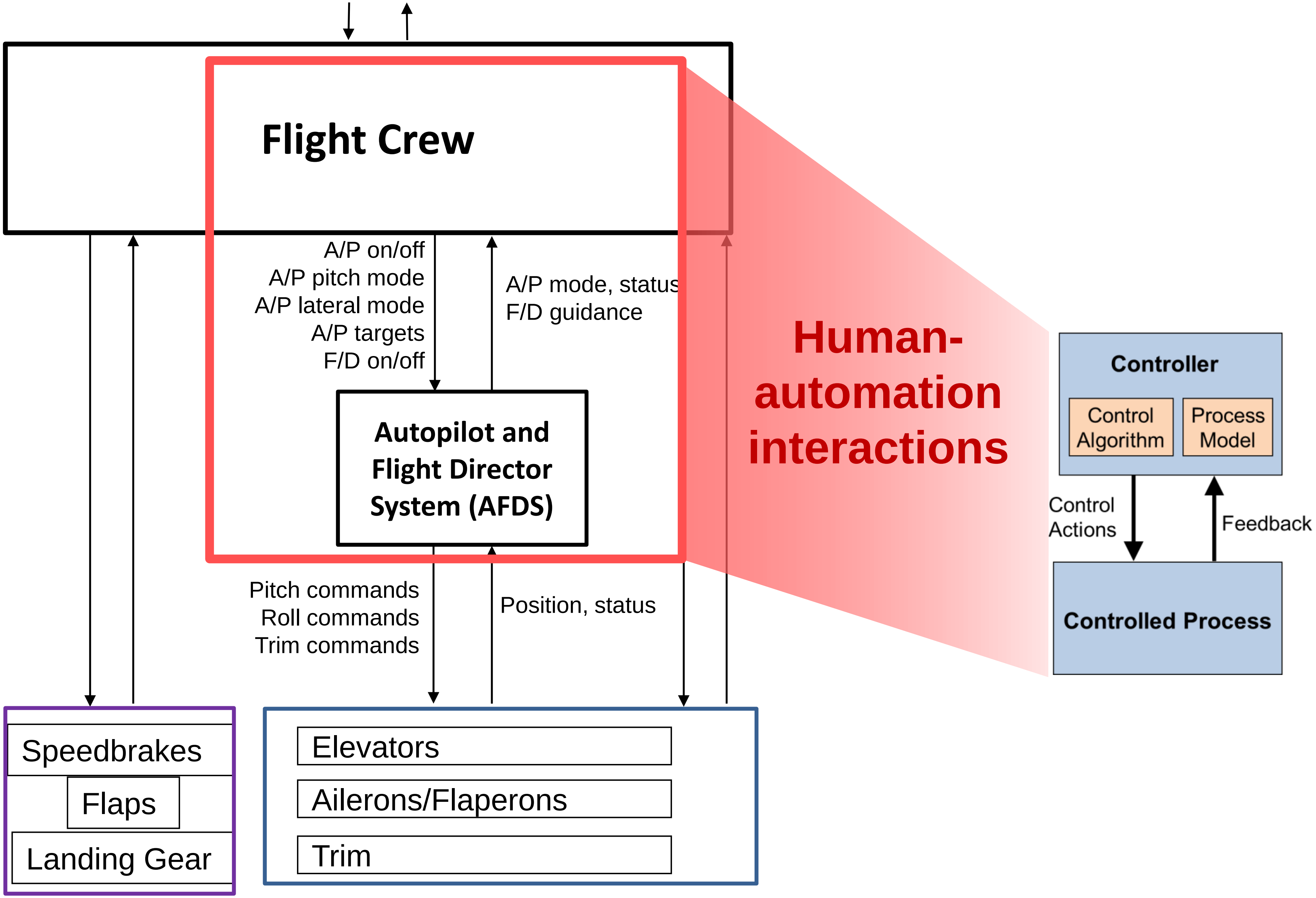
Elevators
Ailerons/Flaperons
Trim

Pilot direct control or Autopilot

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

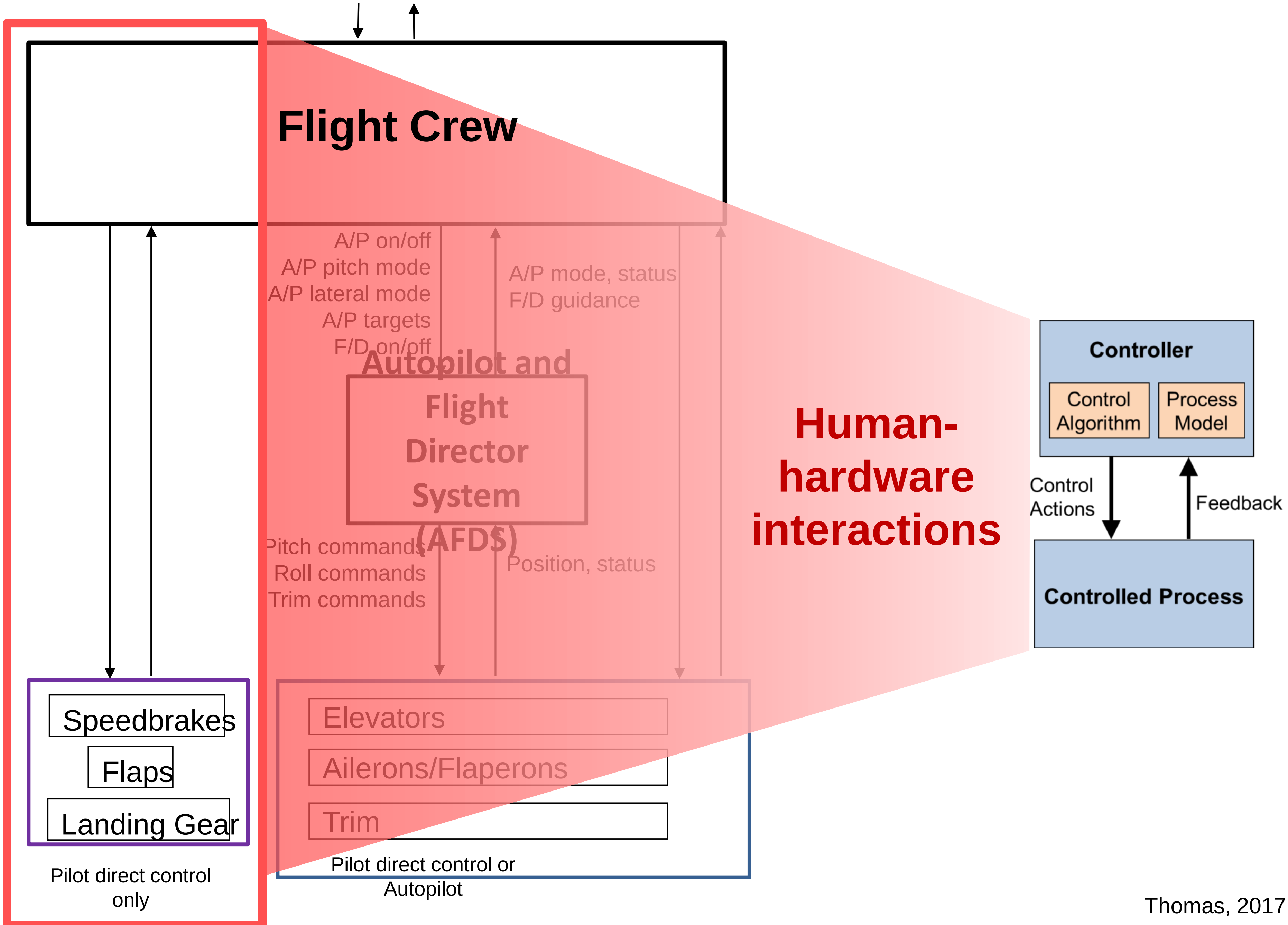
Feedback

Controlled Process

Pilot direct control only

Pilot direct control or Autopilot

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

Pilot direct control only

Elevators
Ailerons/Flaperons
Trim

Pilot direct control or Autopilot

Human-hardware interactions

Controller

Control Algorithm

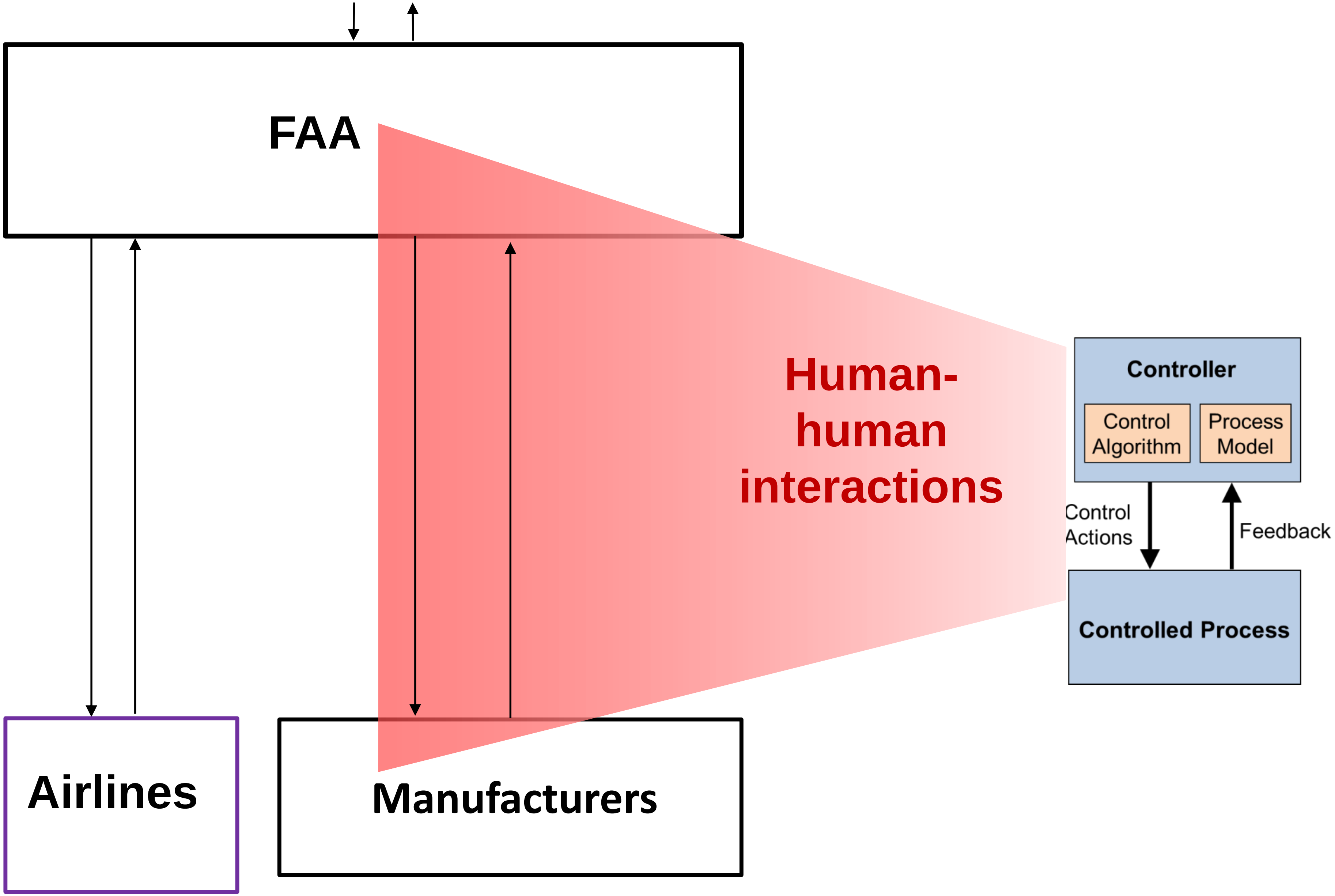
Process Model

Control Actions

Feedback

Controlled Process

Thomas, 2017



FAA

Airlines

Manufacturers

Human-human interactions

Controller

Control Algorithm

Process Model

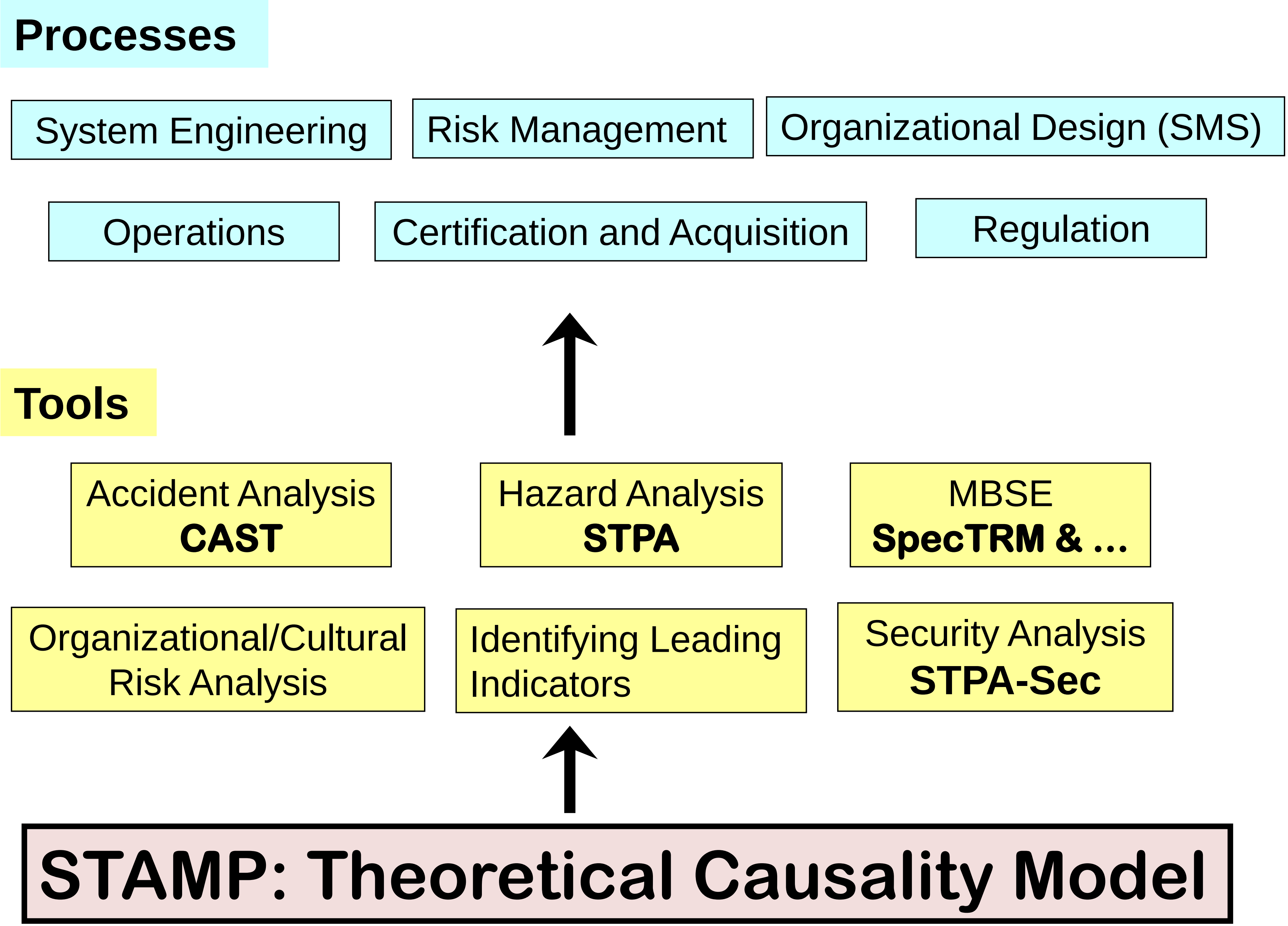
Control Actions

Feedback

Controlled Process

Thomas, 2017

What kinds of tools are available?



Processes

System Engineering

Risk Management

Organizational Design (SMS)

Operations

Certification and Acquisition

Regulation

Tools

Accident Analysis
CAST

Hazard Analysis
STPA

MBSE
SpecTRM & …

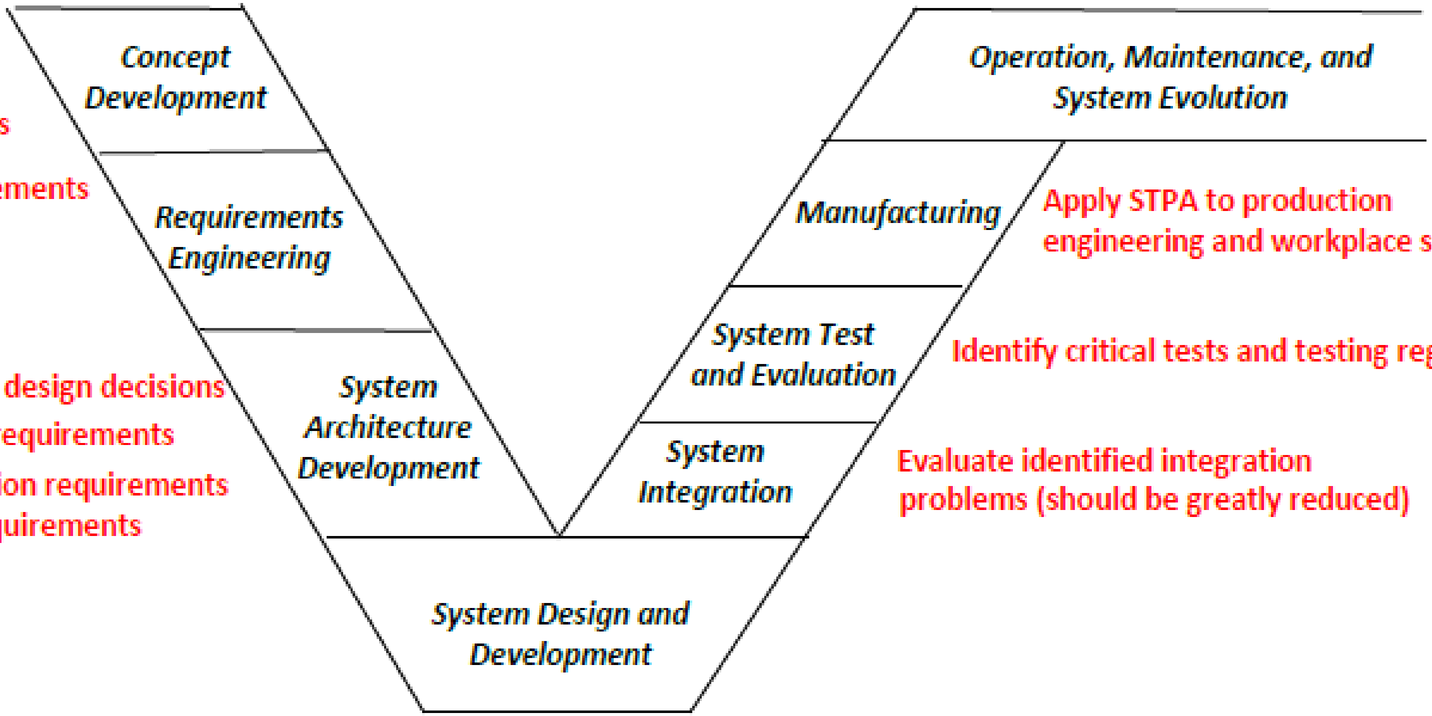
Organizational/Cultural
Risk Analysis

Identifying Leading
Indicators

Security Analysis
STPA-Sec

STAMP: Theoretical Causality Model

STPA can be used throughout product development and operations



Concept Development

- Identify safety and other system goals
- Generate initial system requirements

Requirements Engineering

- Refine system requirements and constraints
- Generate component requirements

System Architecture Development

- Assist with architectural design decisions
- Refine STPA-generated requirements
- Identify system integration requirements and critical interface requirements

System Design and Development

- Use in design and development decision making
- Generate test and evaluation requirements
- Identify manufacturing constraints

System Integration

Evaluate identified integration problems (should be greatly reduced)

System Test and Evaluation

Identify critical tests and testing regimes

Manufacturing

Apply STPA to production engineering and workplace safety

Operation, Maintenance, and System Evolution

- Generate operational safety requirements
- Generate safety management plan
- Monitor for operational assumptions and leading indicators

How is it being used?
Does it work?
Is it useful?

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 when using STPA

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).

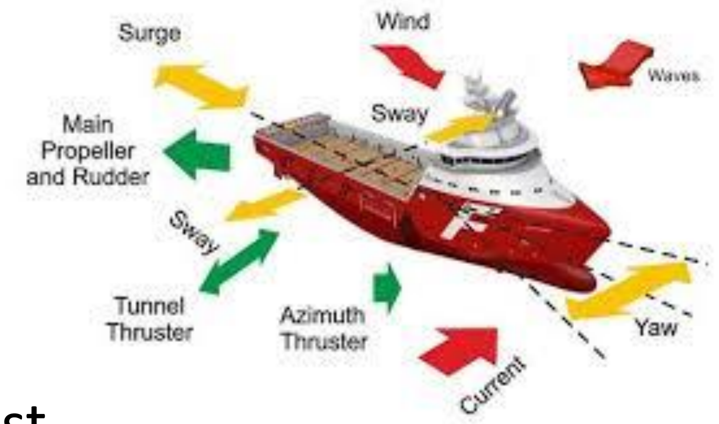
Future Vertical Lift for Army (Lt. David Horning)

- Both MIT and Boeing independently identified safety/security requirements early in concept development
- Used to evaluate the CONOPS
- Could it be used to create the CONOPS?

UH-60MU (Blackhawk)

- Analyzed Warning, Caution, and Advisory (WCA) system
- STPA results were compared with an independently conducted hazard analysis of the UH-60MU using traditional safety processes described in SAE ARP 4761 and MIL-STD-882E.
  - STPA found the same hazard causes as the traditional techniques and
  - Also identified things not found using traditional methods, including design flaws, human behavior, and component integration and interactions

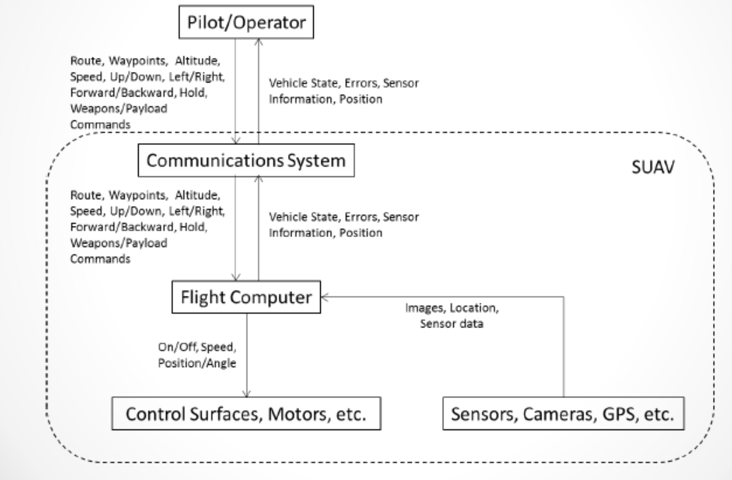
Navy Escort Vessels (Lt. Blake Abrecht)

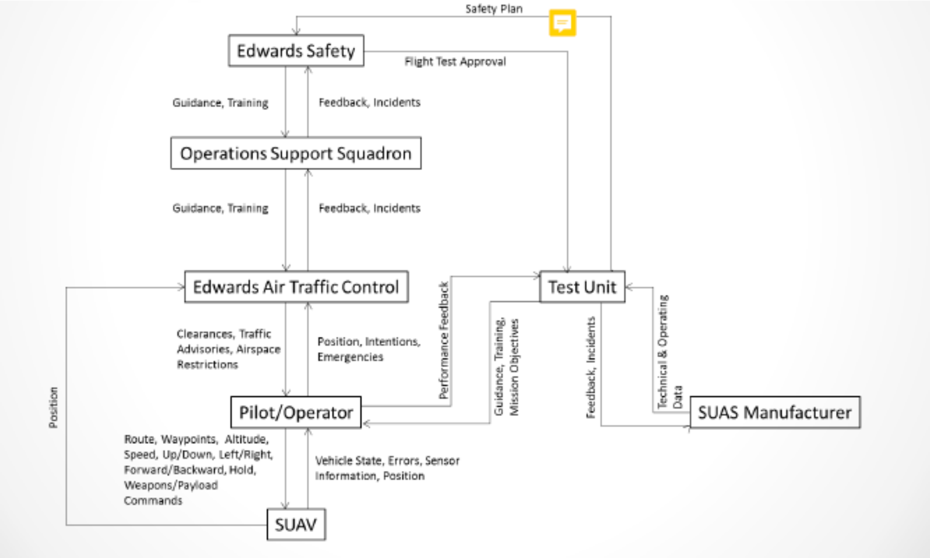


- Dynamic positioning system
- Ran into each other twice during test
- Performed a CAST analysis (on two incidents) and STPA on system as a whole
- STPA found scenarios not found by MIL-STD-882 analysis (fault trees and FMEA)
- Navy admiral rejected our findings saying “We’ve used PRA for 40 years and it works just fine”
- Put into operation and within 2 months ran into a submarine
- Scenario was one we had found

STPA in Small Unmanned UAS testing at EDW (Lt. Sarah Folse and Maj. Sarah Summers)

- System safety requirements and recommendations to accommodate SUAS testing at EDW

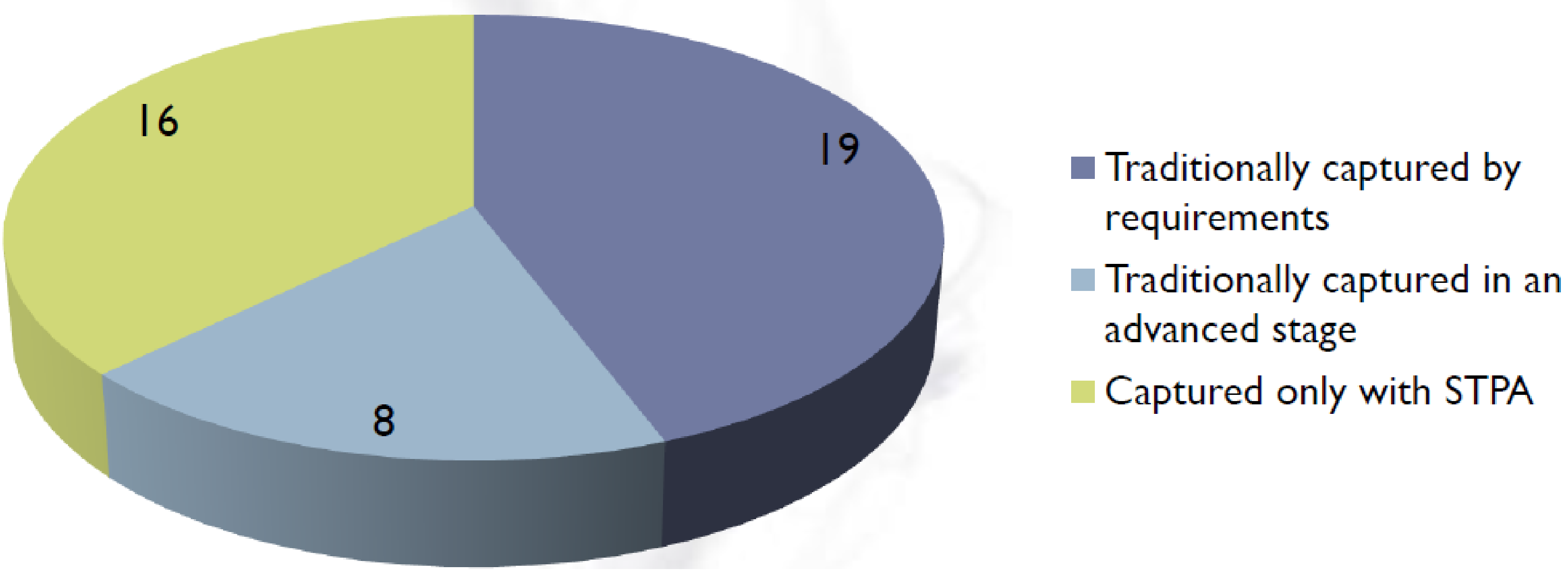

Pilot/Operator
Route, Waypoints, Altitude, Speed, Up/Down, Left/Right, Forward/Backward, Hold, Weapons/Payload Commands
Vehicle State, Errors, Sensor Information, Position
Communications System
SUAV
Route, Waypoints, Altitude, Speed, Up/Down, Left/Right, Forward/Backward, Hold, Weapons/Payload Commands
Vehicle State, Errors, Sensor Information, Position
Flight Computer
Images, Location, Sensor data
On/Off, Speed, Position/Angle
Control Surfaces, Motors, etc.
Sensors, Cameras, GPS, etc.


Safety Plan
Edwards Safety
Flight Test Approval
Guidance, Training
Feedback, Incidents
Operations Support Squadron
Guidance, Training
Feedback, Incidents
Edwards Air Traffic Control
Test Unit
Performance Feedback
Guidance, Training, Mission Objectives
Feedback, Incidents
Technical & Operating Data
Clearances, Traffic Advisories, Airspace Restrictions
Position, Intentions, Emergencies
Position
Pilot/Operator
SUAS Manufacturer
Route, Waypoints, Altitude, Speed, Up/Down, Left/Right, Forward/Backward, Hold, Weapons/Payload Commands
Vehicle State, Errors, Sensor Information, Position
SUAV

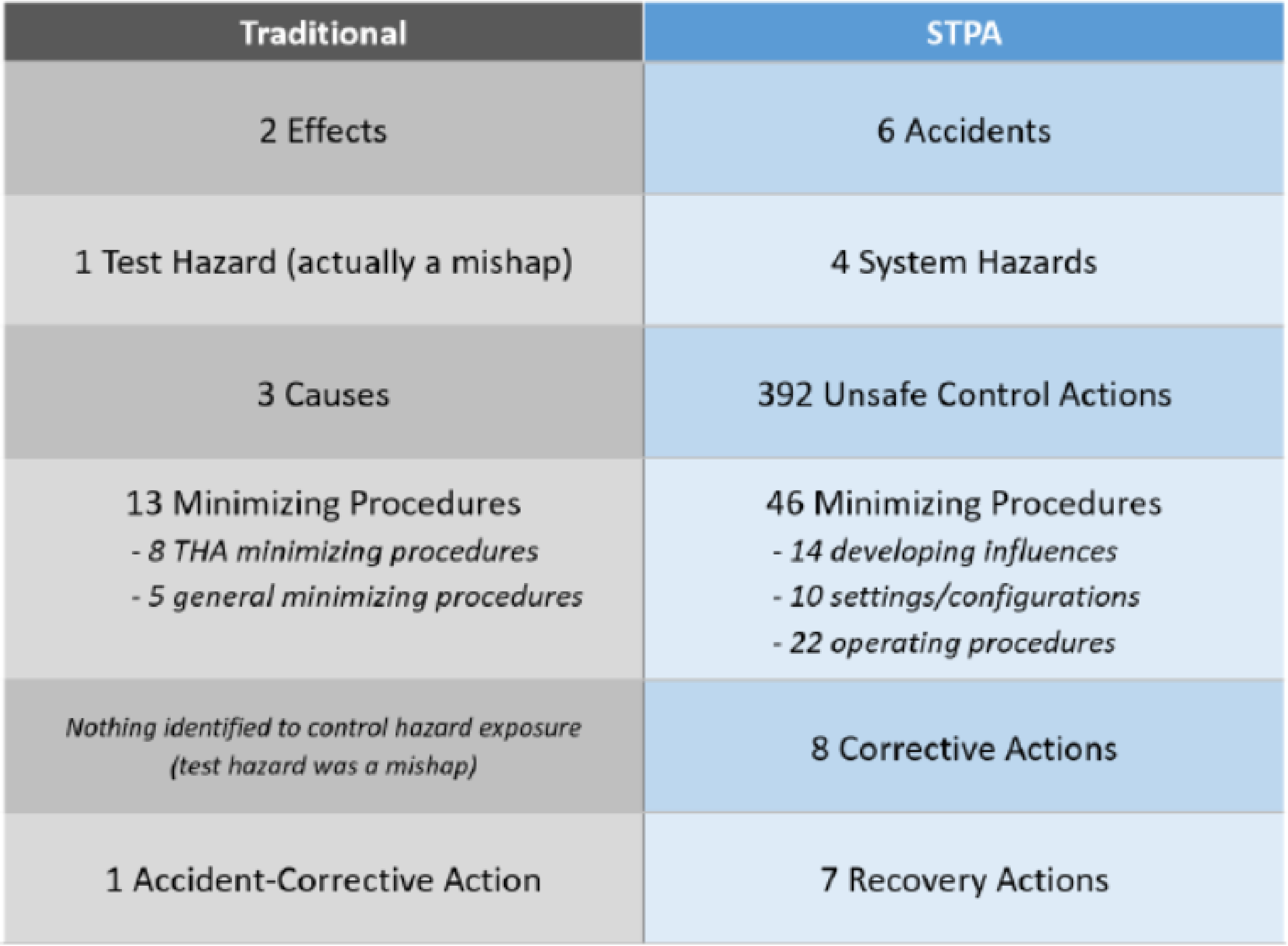
EPRI Nuclear Power Plant Controlled Experiment

- Compared FTA, FMEA, ETA, HAZOP and STPA
- Two graduate students spent 2 weeks on this
- Only STPA found accident that had occurred in plant but analysts did not know about

- Embraer Aircraft Smoke Control System requirements captured by STPA



U.S. Air Force Flight Test



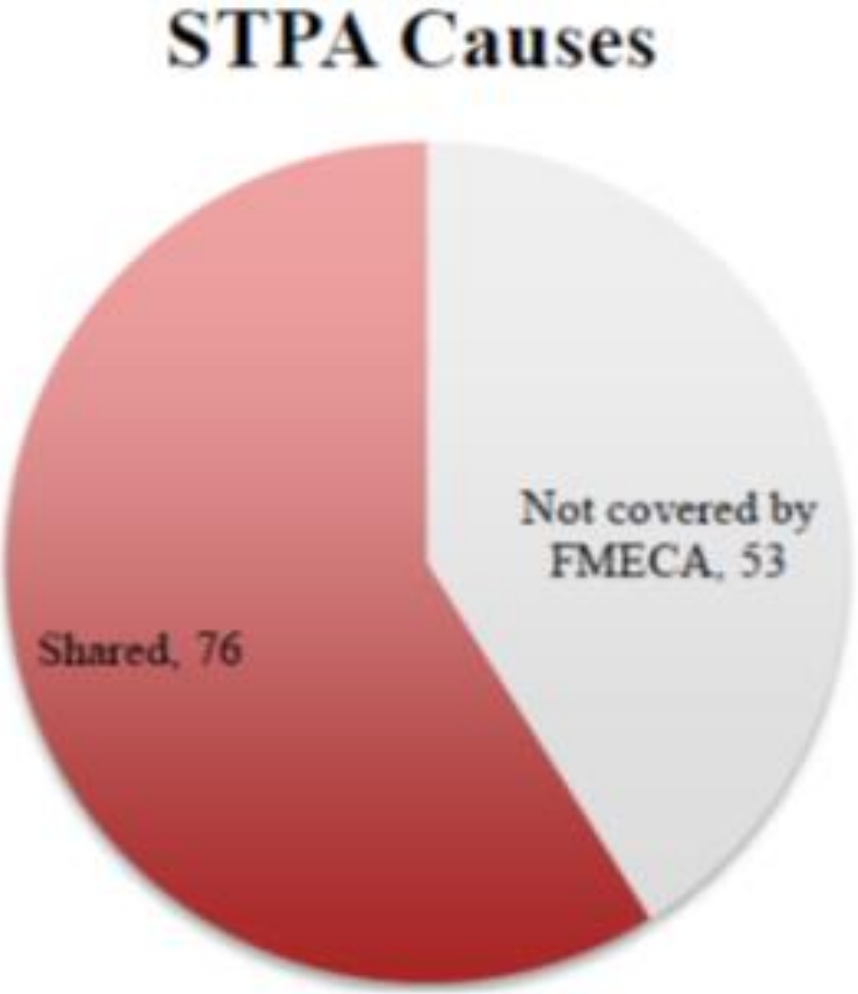
Traditional	STPA
2 Effects	6 Accidents
1 Test Hazard (actually a mishap)	4 System Hazards
3 Causes	392 Unsafe Control Actions
13 Minimizing Procedures *- 8 THA minimizing procedures* *- 5 general minimizing procedures*	46 Minimizing Procedures *- 14 developing influences* *- 10 settings/configurations* *- 22 operating procedures*
Nothing identified to control hazard exposure (test hazard was a mishap)	8 Corrective Actions
1 Accident-Corrective Action	7 Recovery Actions

- Range Extender System for Electric Vehicles (Valeo)
  - FTA/CPA took 3 times effort of STPA, found less

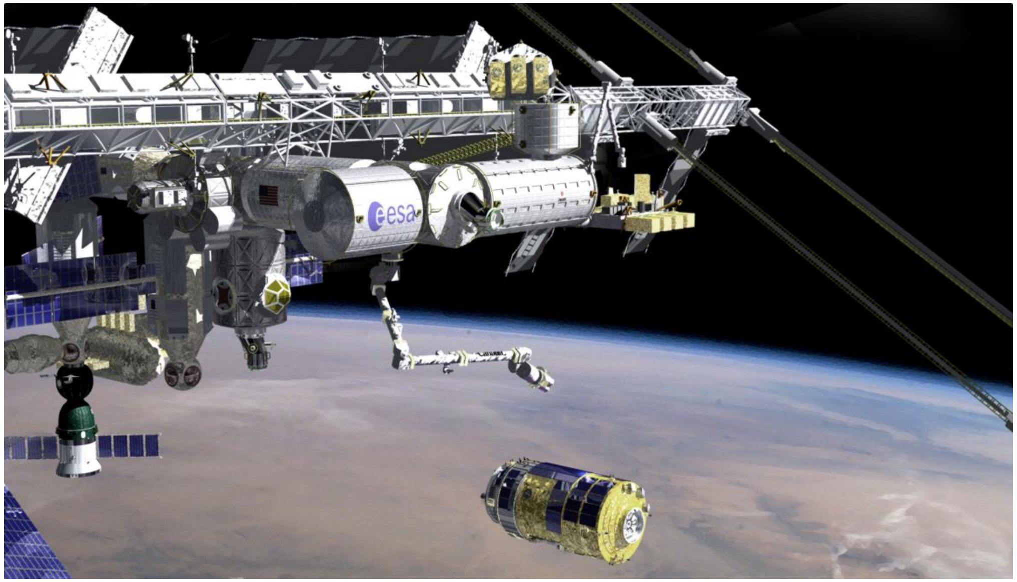
- Medical Device (Class A recall)

FMECA	STPA
70+ causes of accidents	175+ causes accidents (9 related to adverse event)
Team of experts	Single semi-expert
Time dedication: months/years)	Time: weeks/month
Identified only single fault causes	Identified complex causes of accidents

- Automotive Electric Power Steering System



- HTV Unmanned Japanese Spacecraft
  - STPA found all causes found by FTA plus a lot more



Other Uses

- Workplace safety
- Design for Safe Manufacturing/Assembly
- Production Engineering
- Organizational Analysis (e.g., system engineering process)

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/secure, not to predict the likelihood of a loss.

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

- Augments system engineering process and model based system engineering.
  - Models are functional models rather than simply physical or logical models.

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

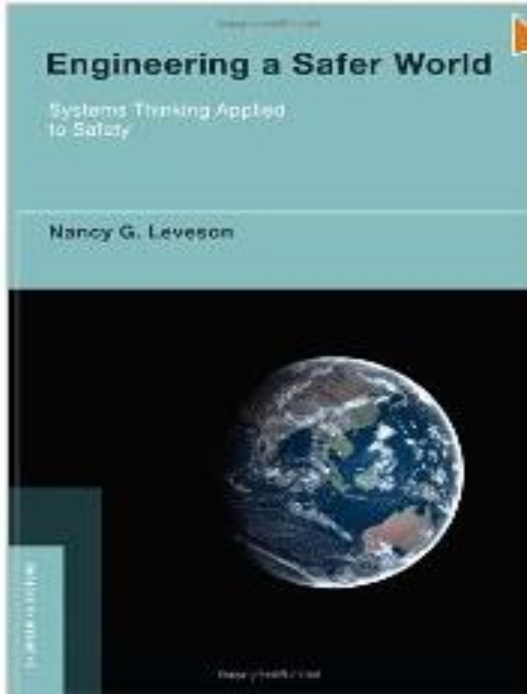
“The best way to predict the future is to create it.”

Abraham Lincoln

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

Nancy Leveson, *Engineering a Safer World:*

Systems Thinking Applied to Safety



MIT Press, January 2012