

Applying Systems Thinking to Safety Requirements

Nancy Leveson

MIT



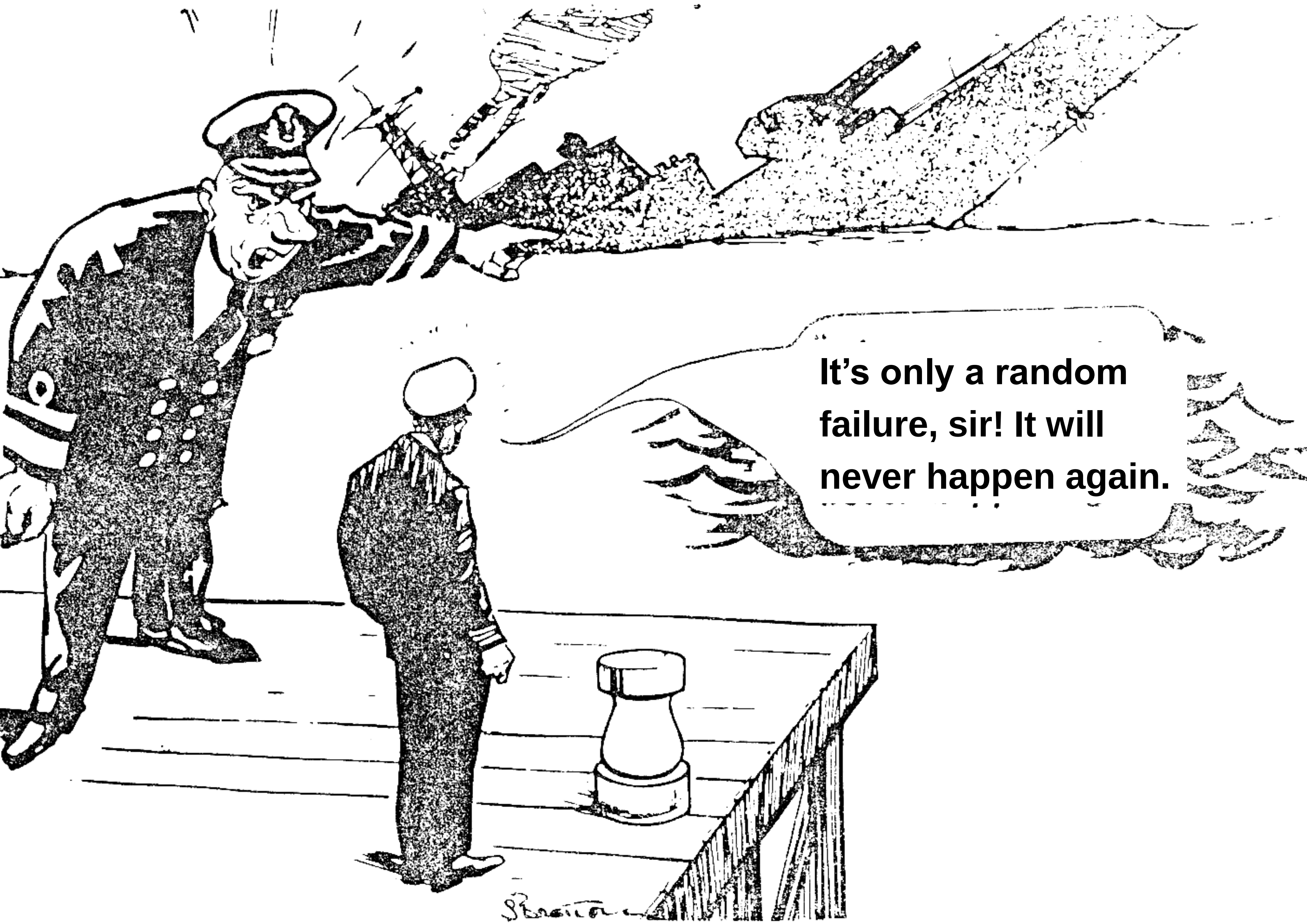
Traditional Approach to Safety

- Traditionally view safety as a failure problem
  - Chain of directly related failure events leads to loss
  - Analysis technique assume this model of causation to identify scenarios (chains of failure events)
    - FTA, Event Trees, FMEA, HAZOP, PRA, etc.
  - Establish barriers between events or try to prevent individual component failures

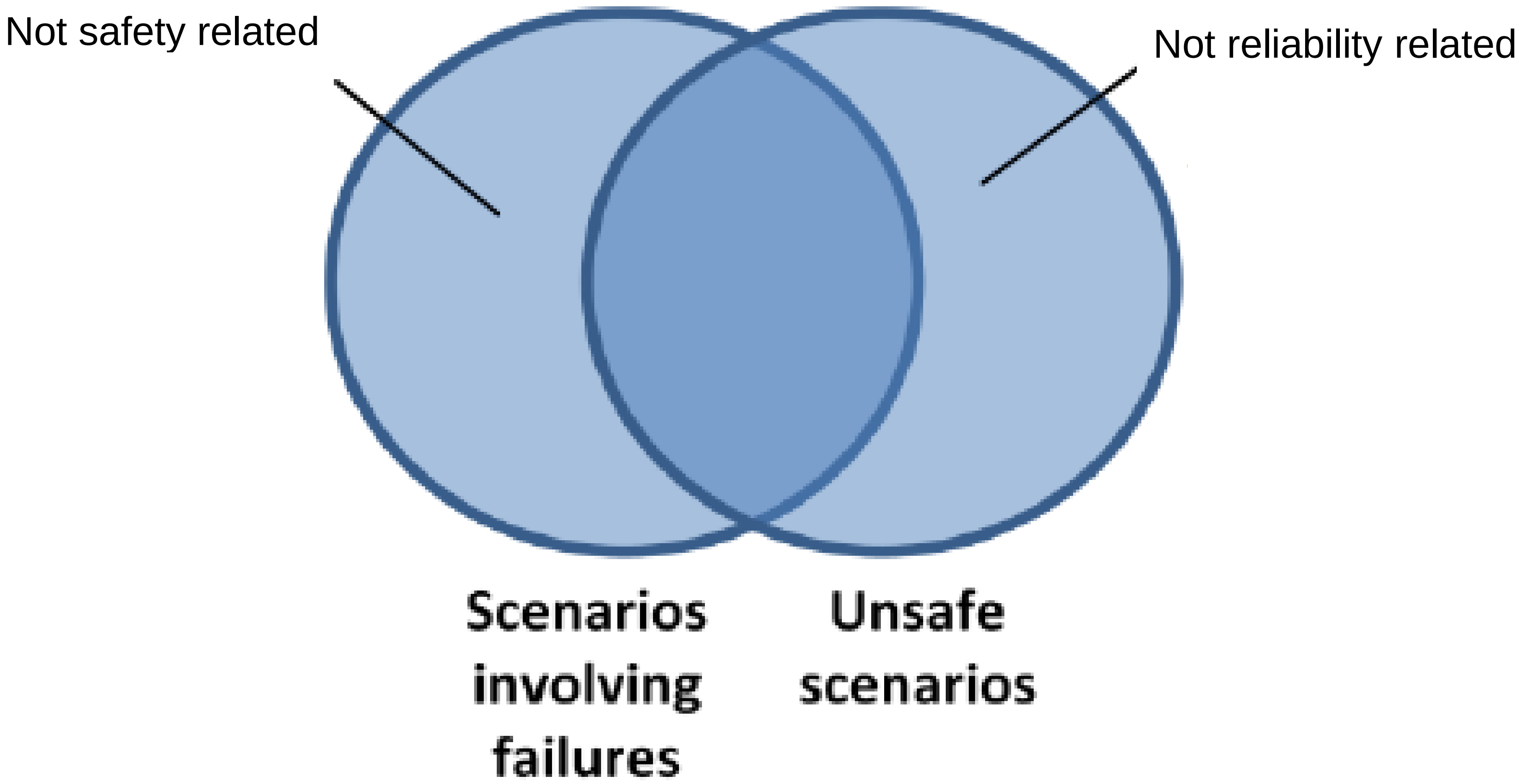
    e.g., redundancy, overdesign, safety margins, interlocks, fail-safe design, training for operators

System Safety Requirements

- Often specified in terms of system or component reliability
- Examples:
  - Inadvertent wheel braking of all wheels during takeoff roll after V1 shall be less than 5E-9 per flight.
  - The likelihood that the ITP Equipment provides an undetected erroneous Ground Speed Differential to the flight crew shall be less than 1E-3 per flight hour.
- But no way to verify that these requirements have been met except after a loss
  - e.g., 787 Lithium-ion battery fires (required to be 1E-9 or once in 10,000,000 flight hours) occurred twice in first 50,000 flight hours


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

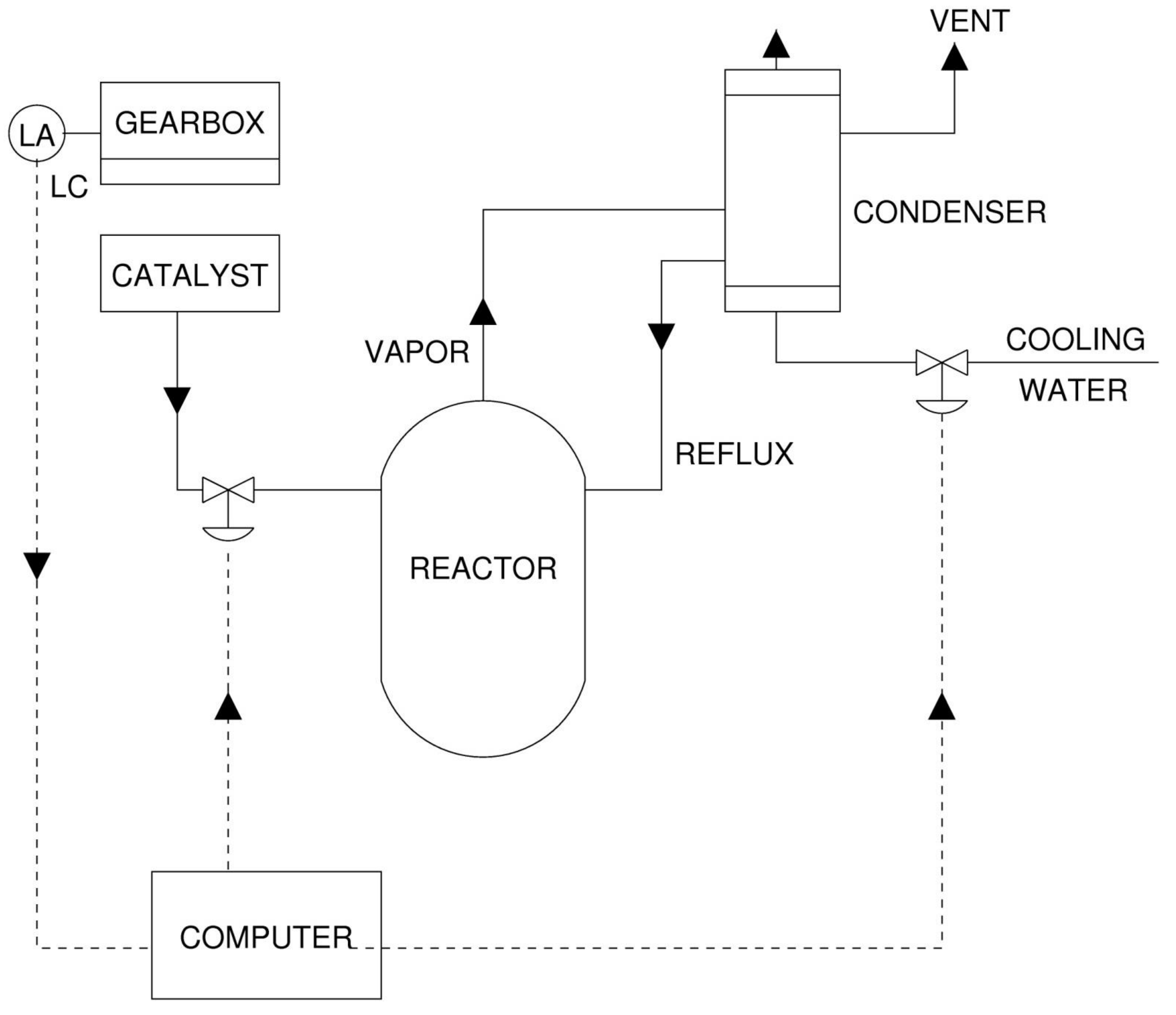
Confusing Safety and Reliability



Limitations of Traditional Approach

- Systems are becoming more complex
  - Accidents often result from interactions among components, not just component failures
  - Too complex to anticipate all potential interactions
    - By designers
    - By operators
  - Indirect and non-linear interactions
- Omits or oversimplifies important factors
  - Human error
  - New technology, particularly software
  - Culture and management
  - Evolution and adaptation

Accident with No Component Failures



Types of Accidents

- Component Failure Accidents
  - Single or multiple component failures
  - Usually assume random failure
- Component Interaction Accidents
  - Arise in interactions among components
  - Complexity getting to point where cannot anticipate or guard against all potential interactions
  - Exacerbated by introduction of computers and software but software is not the problem, complexity is

Software-Related Accidents

- Are usually caused by flawed requirements
  - Incomplete or wrong assumptions about operation of controlled system or required operation of computer
  - Unhandled controlled-system states and environmental conditions

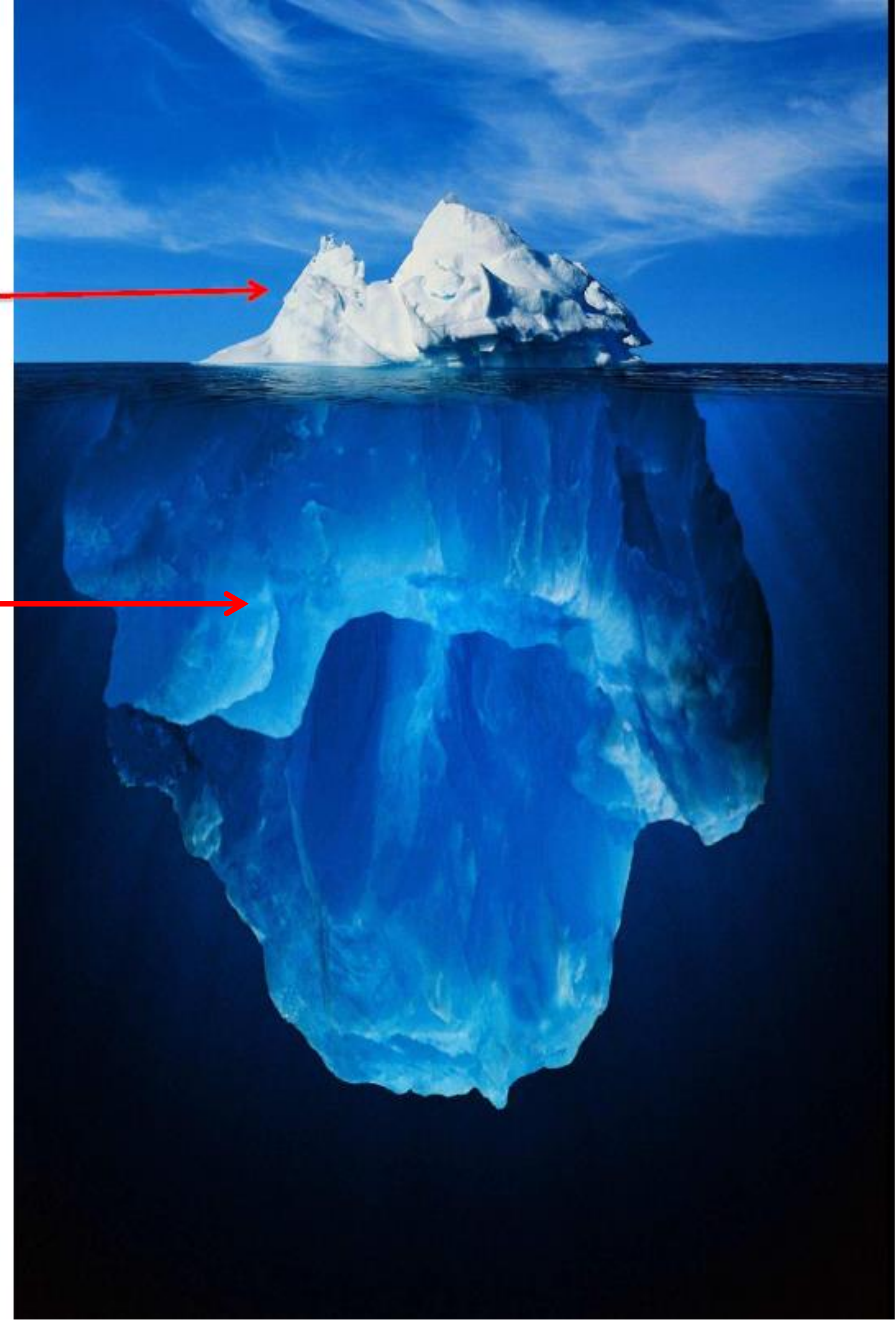
- Merely trying to get the software “correct” or to make it reliable will not make it safer under these conditions.

Software-Related Accidents (2)

- Software may be highly reliable and “correct” and still be unsafe:
  - Correctly implements requirements but specified behavior unsafe from a system perspective.
  - Requirements do not specify some particular behavior required for system safety (incomplete)
  - Software has unintended (and unsafe) behavior beyond what is specified in requirements.

What do we need to do?

- Generate system safety requirements from hazard analysis
  - Expand our accident causation models
  - Create new hazard analysis techniques that
    - Work early in concept development and requirements specification stages
    - Consider more than component failures



WYOUNG@MIT.EDU

STAMP: An Expanded Accident Causality Model

- Accidents involve a complex, dynamic "process"
  - Not simply chains of failure events
  - Arise in interactions among humans, machines and the environment
- Treat safety as a dynamic control problem
  - Safety requires enforcing a set of constraints on system behavior
  - Accidents occur when interactions among system components violate those constraints
  - Safety becomes a control problem rather than just a reliability problem

Safety as a Dynamic Control Problem

- Examples
  - O-ring did not control propellant gas release by sealing gap in field joint of Challenger Space Shuttle
  - Software did not adequately control descent speed of Mars Polar Lander
  - At Texas City, did not control the level of liquids in the ISOM tower
  - In DWH, did not control the pressure in the well
  - Financial system did not adequately control the use of financial instruments

Safety as a Dynamic Control Problem (2)

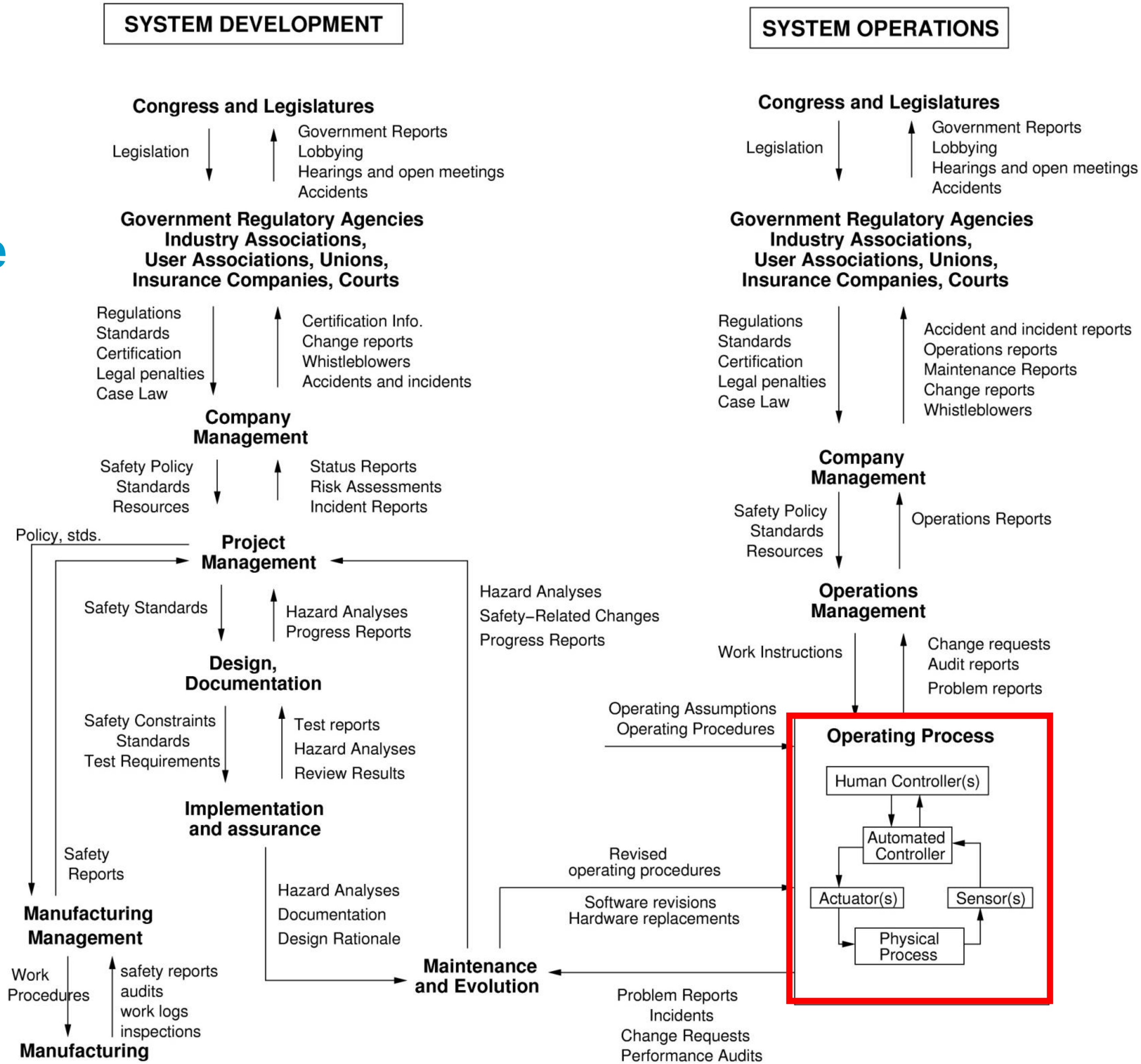
- A change in emphasis:

~~"prevent failures"~~

↓

"enforce safety constraints on system behavior"

Example Safety Control Structure



Safety as a Control Problem (3)

- **Goal: Design an effective control structure (safety management system) that eliminates or reduces adverse events**
  - Need clear definition of requirements at <u>all</u> levels of safety control structure
  - Entire control structure must together enforce the system safety property (constraints)
    - Physical design (inherent safety)
    - Operations
    - Management
    - Social interactions and culture
  - Need requirements at all levels, not just technical level

Processes

System Engineering (e.g., Specification, Safety-Guided Design, Design Principles)

Risk Management

Operations

Management Principles/ Organizational Design

Regulation

Tools

Accident/Event Analysis **CAST**

Hazard Analysis **STPA**

Specification Tools **SpecTRM**

Organizational/Cultural Risk Analysis

Identifying Leading Indicators

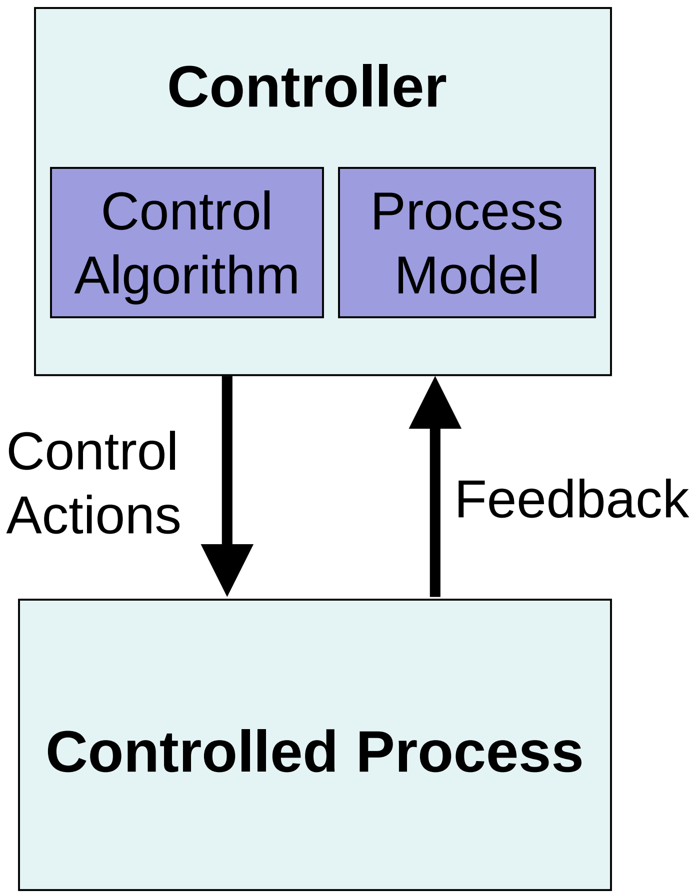
Security Analysis **STPA-sec**

STAMP: Theoretical Causality Model

STPA (System-Theoretic Process Analysis)

- Integrated into system engineering
  - Can be used from beginning of project
  - Safety-guided design
  - Guidance for evaluation and test
  - Incident/accident analysis
- Works on social and organizational aspects of systems
- Generates system and component safety requirements (safety constraints to be enforced)
- Identifies flaws in system design and scenarios leading to violation of a safety requirement (i.e., a hazard)
  - Use to generate more detailed requirements

Role of Process Models in Control



- Controllers use a **process model** to determine control actions
- Accidents often occur when the process model is incorrect
- Four types of hazardous control actions:
  - Control commands required for safety are not given
  - Unsafe ones are given
  - Potentially safe commands given too early, too late
  - Control stops too soon or applied too long

(Leveson, 2003); (Leveson, 2011)

STPA and Requirements

- STPA Step 1:
  - Identify unsafe control actions
  - Use four types of unsafe control actions
  - Generate high-level safety requirements
- STPA Step 2:
  - Identify detailed scenarios leading to unsafe control actions
  - Use generic causal factors for unsafe control actions
  - Generate detailed safety requirements

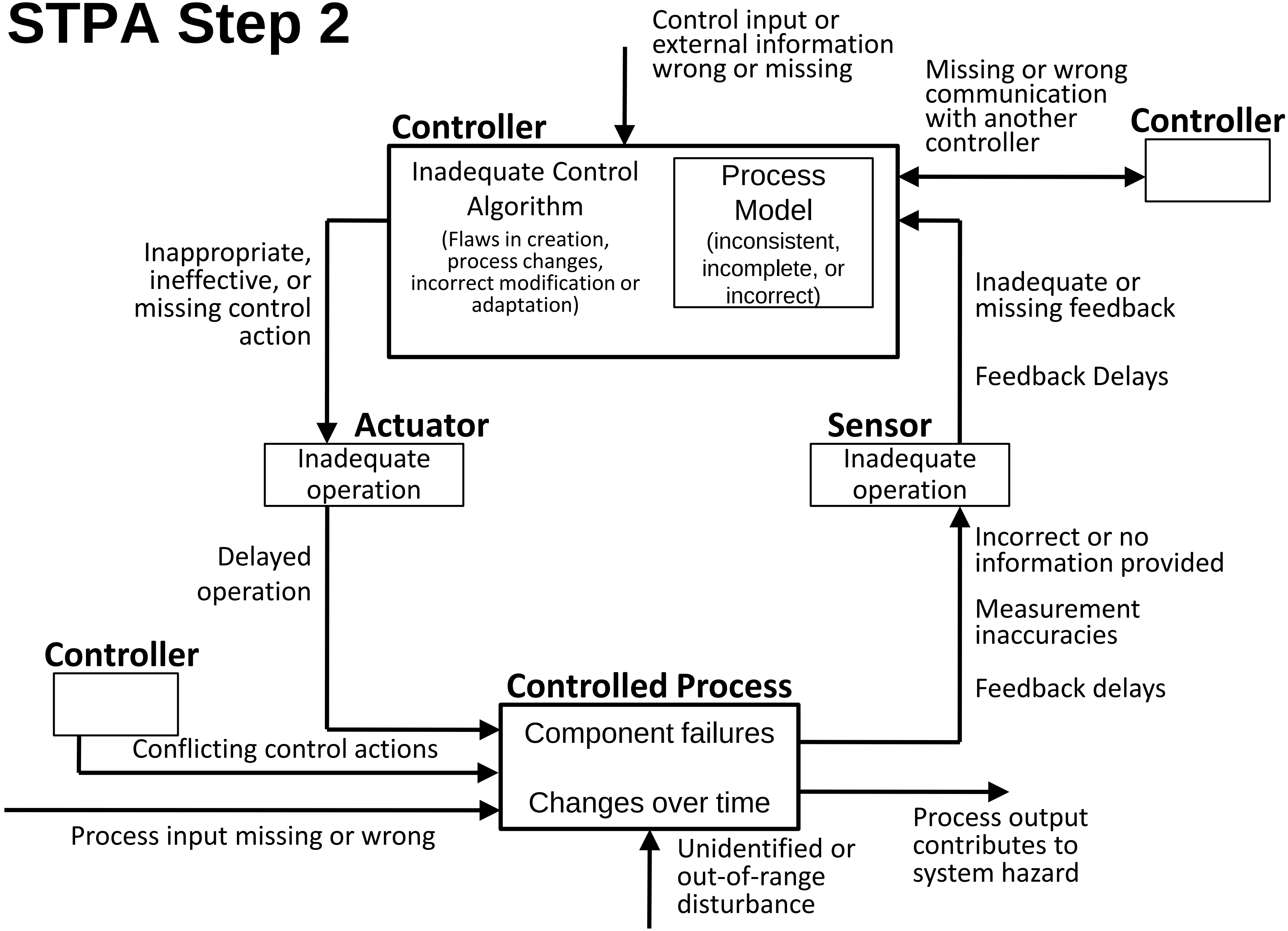
Hazard: Catalyst in reactor without reflux condenser operating (water flowing through it)

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order	Stopped too soon/ applied too long
Open water	Not opened when catalyst open		Open water more than X seconds after open catalyst	Stop before fully opened
Close water		Close while catalyst open	Close water before catalyst closes	
Open catalyst		Open when water valve not open	Open catalyst more than X seconds before open water	
Close catalyst	Do not close when water closed		Close catalyst more than X seconds after close water	Stop before fully closed

Safety Requirements Generated from Table

- Water valve must always be fully open before catalyst valve is opened.
  - Water valve must never be opened (complete opening) more than X seconds after catalyst valve opens
- Catalyst valve must always be fully closed before water valve is closed.
  - Catalyst valve must never be closed more than X seconds after water valve has fully closed.

STPA Step 2


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or incorrect)
Inappropriate, ineffective, or missing control action
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Delayed operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Step 2: Identify Causes of Unsafe Control Actions

- Identify causes of giving unsafe control actions

  Open catalyst valve when water valve not open

  Consider how controller's process model could identify that water valve is open when it is not.

- Identify causes for a required control action (e.g., open water valve) being given by the software but not executed.
- Generate more detailed safety requirements from causes
- Design features (controls) to protect the system from the scenarios identified

Requirements on Entire Safety Management System

- Can also generate requirements for human operators and the safety management system (safety control structure) using STPA

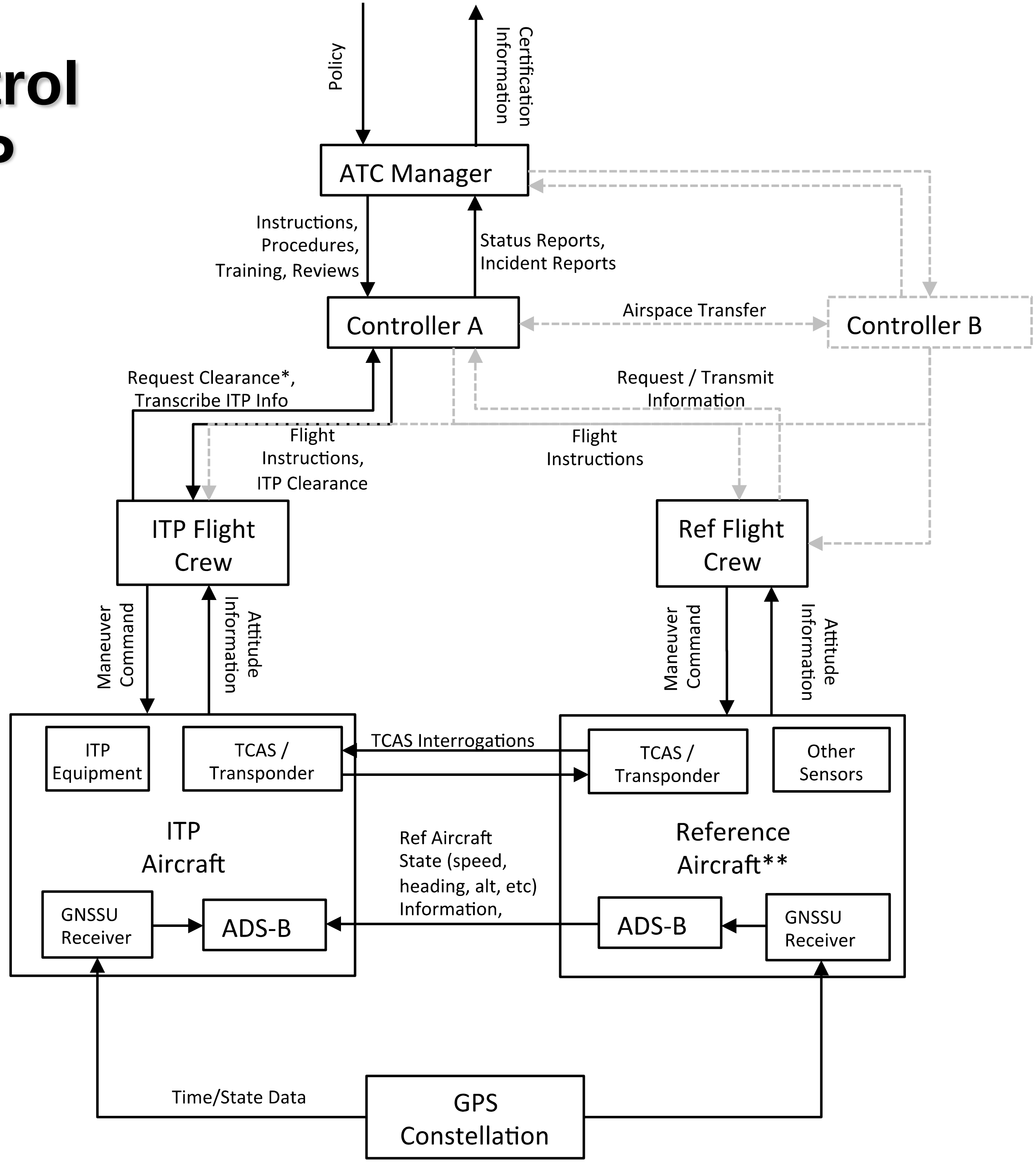
Examples:

  - NASA safety management after Columbia
  - Radiation therapy at UCSD and UCLA hospitals
  - CO_2 capture, transport, and storage (Samadi, Ecole des Mines)

STPA Use on Real Systems

- Hundreds of users around the world in almost all safety-critical industries
- In all evaluations and comparisons, STPA found more scenarios (paths) to accidents and less costly to perform
- In some cases, STPA found real accidents that traditional hazard analysis techniques missed

High-Level Control Structure for ITP



Potentially Hazardous Control Actions by the Flight Crew

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon/Applied Too Long
Execute ITP		ITP executed when not approved ITP executed when ITP criteria are not satisfied ITP executed with incorrect climb rate, final altitude, etc	ITP executed too soon before approval ITP executed too late after reassessment	ITP aircraft levels off above requested FL ITP aircraft levels off below requested FL
Abnormal Termination of ITP	FC continues with maneuver in dangerous situation	FC aborts unnecessarily FC does not follow regional contingency procedures while aborting		

High Level Constraints on Flight Crew

- The flight crew must not execute the ITP when it has not been approved by ATC.
- The flight crew must not execute an ITP when the ITP criteria are not satisfied.
- The flight crew must execute the ITP with correct climb rate, flight levels, Mach number, and other associated performance criteria.
- The flight crew must not continue the ITP maneuver when it would be dangerous to do so.
- The flight crew must not abort the ITP unnecessarily. (Rationale: An abort may violate separation minimums)
- When performing an abort, the flight crew must follow regional contingency procedures.
- The flight crew must not execute the ITP before approval by ATC.
- The flight crew must execute the ITP immediately when approved unless it would be dangerous to do so.
- The crew shall be given positive notification of arrival at the requested FL

Potentially Hazardous Control Actions for ATC

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon or Applied Too Long Causes Hazard
Approve ITP request		Approval given when criteria are not met Approval given to incorrect aircraft	Approval given too early Approval given too late	
Deny ITP request				
Abnormal Termination Instruction	Aircraft should abort but instruction not given	Abort instruction given when abort is not necessary	Abort instruction given too late	

High-Level Constraints on ATC

- Approval of an ITP request must be given only when the ITP criteria are met.
- Approval must be given to the requesting aircraft only.
- Approval must not be given too early or too late [needs to be clarified as to the actual time limits]
- An abnormal termination instruction must be given when continuing the ITP would be unsafe.
- An abnormal termination instruction must not be given when it is not required to maintain safety and would result in a loss of separation.
- An abnormal termination instruction must be given immediately if an abort is required.