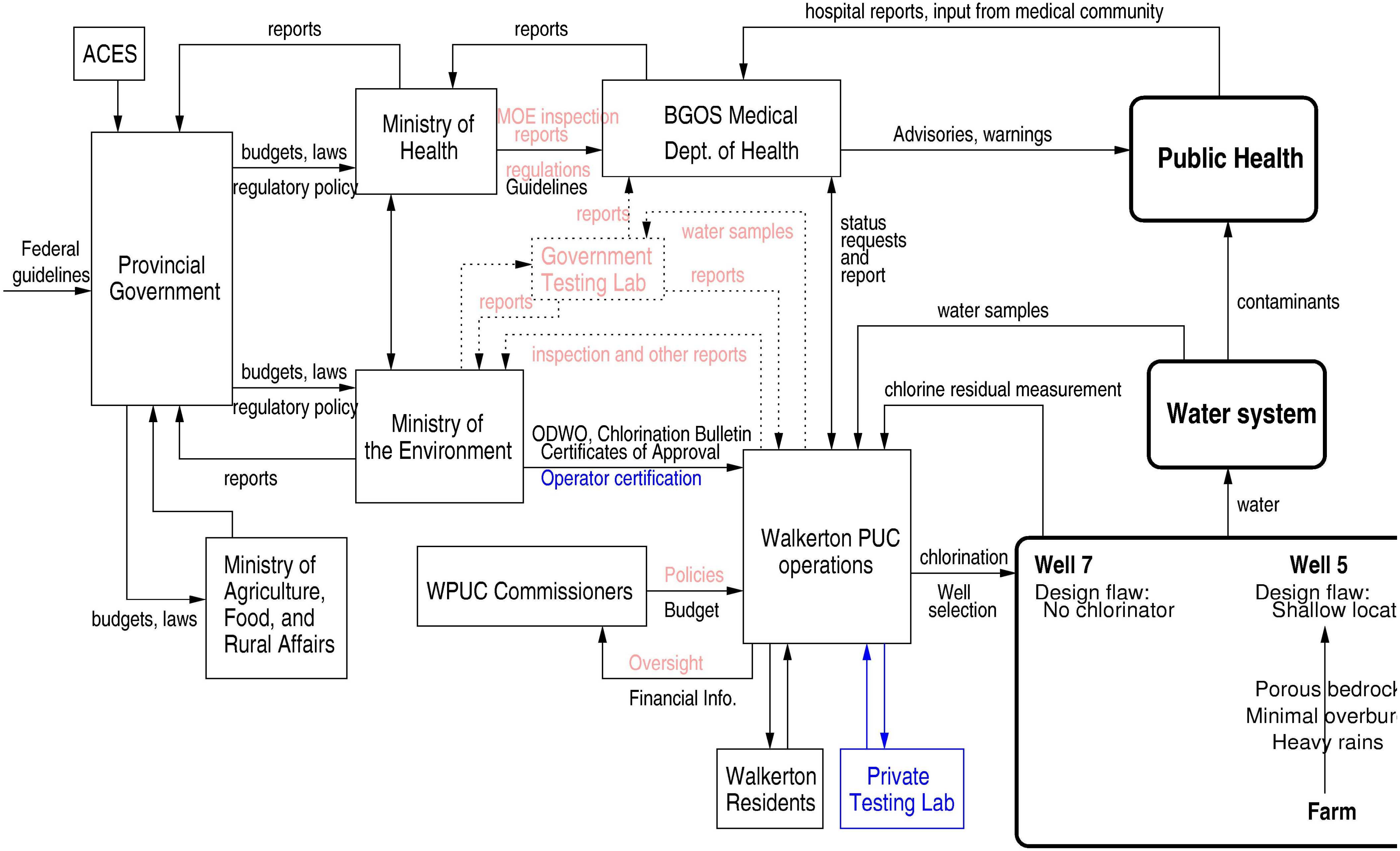
STPA: A New Hazard Analysis Technique

(System-Theoretic Process Analysis)

Summary: Accident Causality in STAMP

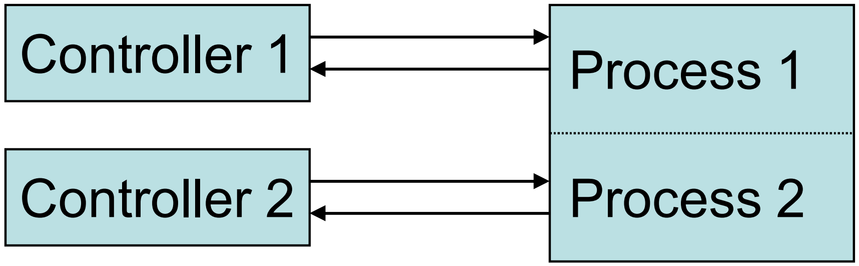
- Accidents occur when
  - Control structure or control actions do not enforce safety constraints
    - Unhandled environmental disturbances or conditions
    - Unhandled or uncontrolled component failures
    - Dysfunctional (unsafe) interactions among components
  - Control structure degrades over time (asynchronous evolution)
  - Control actions inadequately coordinated among multiple controllers


ACES
reports
reports
hospital reports, input from medical community
Ministry of Health
MOE inspection reports
BGOS Medical Dept. of Health
Advisories, warnings
Public Health
budgets, laws
regulatory policy
regulations
Guidelines
reports
water samples
Federal guidelines
Provincial Government
Government Testing Lab
status requests and report
reports
reports
contaminants
water samples
inspection and other reports
budgets, laws
regulatory policy
chlorine residual measurement
Water system
Ministry of the Environment
ODWO, Chlorination Bulletin
Certificates of Approval
Operator certification
reports
water
Walkerton PUC operations
chlorination
Well selection
Well 7
Design flaw:
No chlorinator
Well 5
Design flaw:
Shallow locat
Ministry of Agriculture, Food, and Rural Affairs
WPUC Commissioners
Policies
Budget
budgets, laws
Oversight
Financial Info.
Porous bedrock
Minimal overbur
Heavy rains
Walkerton Residents
Private Testing Lab
Farm

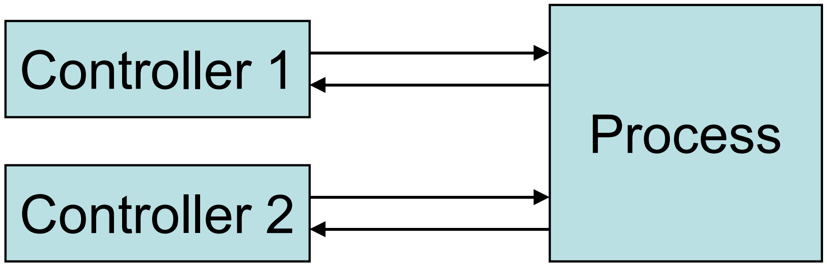
A Third Source of Risk

- Control actions inadequately coordinated among multiple controllers

Boundary areas



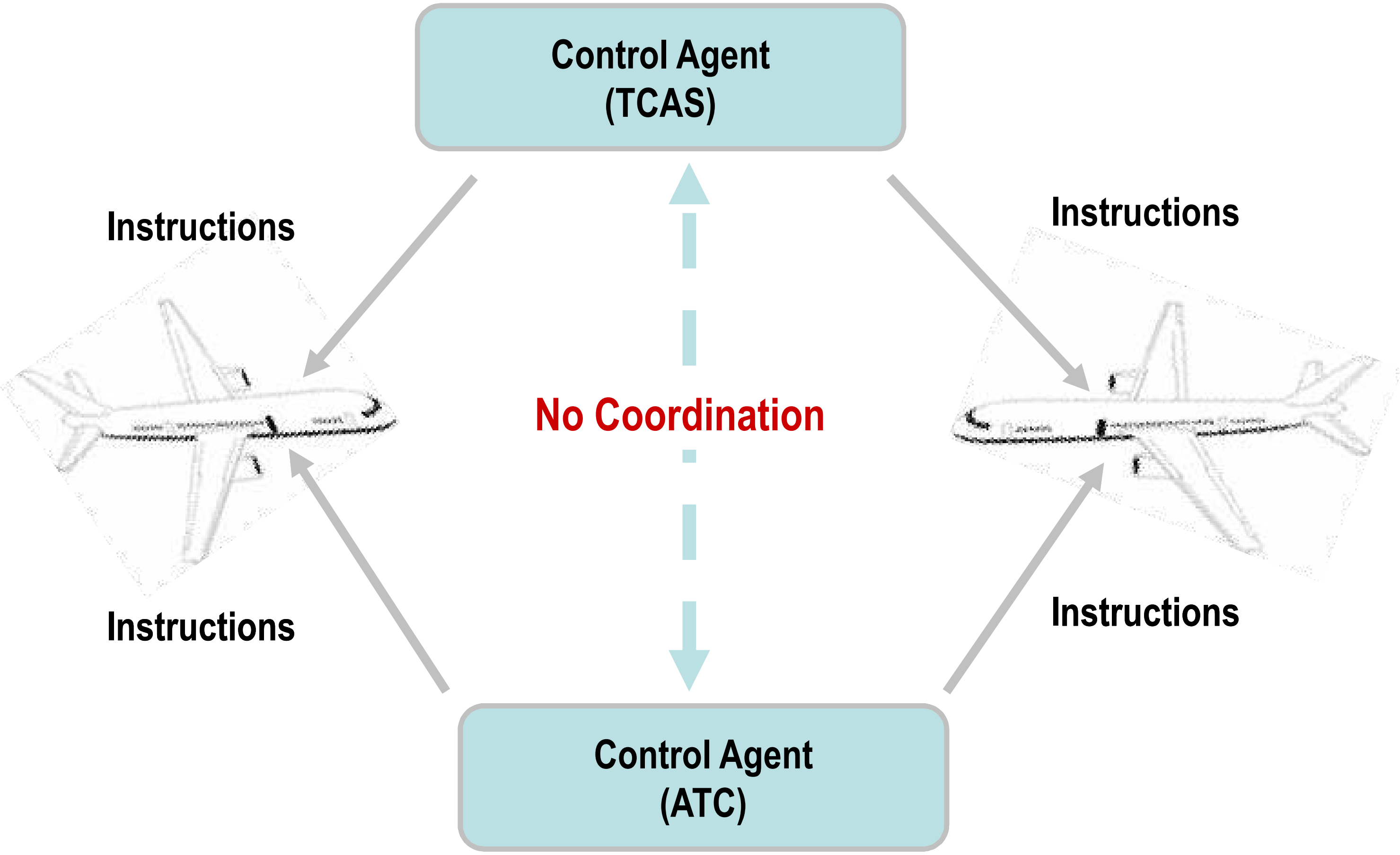
Overlap areas (side effects of decisions and control actions)



Uncoordinated “Control Agents”

“UNSAFE STATE”

BOTH TCAS and ATC provide uncoordinated & independent instructions



Control Agent
(TCAS)

Instructions

Instructions

No Coordination

Instructions

Instructions

Control Agent
(ATC)

Hazard Analysis

- Investigating an accident before it occurs.
- Goal:
  - Identify potential causes of accidents (scenarios that can lead to losses)
  - So can be eliminated or controlled in design or operations before losses occur.
- Used for:
  - Developing requirements and design constraints
  - Validating requirements and design for safety
  - Preparing operational procedures and instructions
  - Test planning and evaluation
  - Management planning

System-Theoretic Process Analysis (STPA)

- Supports a safety-driven design process where
  - Hazard analysis influences and shapes early design decisions
  - Hazard analysis iterated and refined as design evolves
- Also supports accident analysis and risk analysis/hazard analysis of existing systems
- Goals (same as any hazard analysis)
  - Identify safety constraints/requirements necessary to ensure acceptable risk
  - Accumulate information about how hazards can be violated (scenarios), which is used to eliminate, reduce and control hazards in system design, development, manufacturing, and operations

STPA

- Used to assist in defining scenarios in which the safety constraints could be violated.
- The same goal as fault trees or any other hazard analysis approach) but
  - Looks at more than component failures
  - More support provided in the analysis
  - Finds more types of accident scenarios
- Starts from basic control structure and assigned responsibilities for safety-critical actions.

STPA on Social Systems

- We have applied STPA to social (organizational) systems
  - NASA Shuttle operations management structure
  - Effect of policy changes following the Vioxx events
  - Accident analysis and system redesign for food safety

But will concentrate in the following on the physical system

Steps in STPA

- Establish fundamentals
  - Define “accident” for your system
  - Define hazards
  - Rewrite hazards as constraints on system design
  - Draw preliminary (high-level) safety control structure
- Identify potentially unsafe control actions (safety requirements and constraints)
- Determine how each potentially hazardous control action could occur

Steps in STPA

- Define accidents
- Define system hazards associated with accidents
- Translate system hazards into high-level safety requirements (constraints)
- Construct high-level control structure including
  - Responsibilities of components
  - Preliminary process model
- Refine high-level safety constraints into detailed safety requirements on components and scenarios for losses
- Use results to create or improve system design

Defining Accidents

Accident: An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.

Incident: An event that involves no loss (or only minor loss) but with the potential for loss under different circumstances.

- Loss can include human injury, property damage, environmental pollution (damage), mission loss, etc.
- Could prioritize or assign varying levels of severity

Accidents or Unacceptable Losses for Explorer Spacecraft

ACC1. Humans and/or human assets on earth are killed/damaged. (↑PC1), (↓H5)

ACC2. Humans and/or human assets off of the earth are killed/damaged. (↑PC1)(↓H6)

ACC3. Organisms on any of the moons of the outer planet (if they exist) are killed or mutated by biological agents of Earth Origin. (↓H4)

ACC4. The scientific data corresponding to the mission goals are not collected. (↑G1, G2, G3, G4, G5, G6, G7), (↓H1)

Accidents (con't)

ACC5. The scientific data is rendered unusable (e.g., deleted, corrupted, not returned at required time) before it can be fully investigated. (↑G1, G2, G3, G4, G5, G6, G7), (↓H2,↓H3)

ACC6 Organisms of Earth origin are mistaken for organisms indigenous to any of the moons of the outer planet in future missions to study the outer planet's moon. (↓H4)

ACC7. An incident during this mission directly causes another mission to fail to collect, return, and/or use the scientific data corresponding to its mission goals. (↑PC1)(↓H7)

Exercise

- Select an application from your industry or company
- Define accidents in this system.

Defining "Hazards"

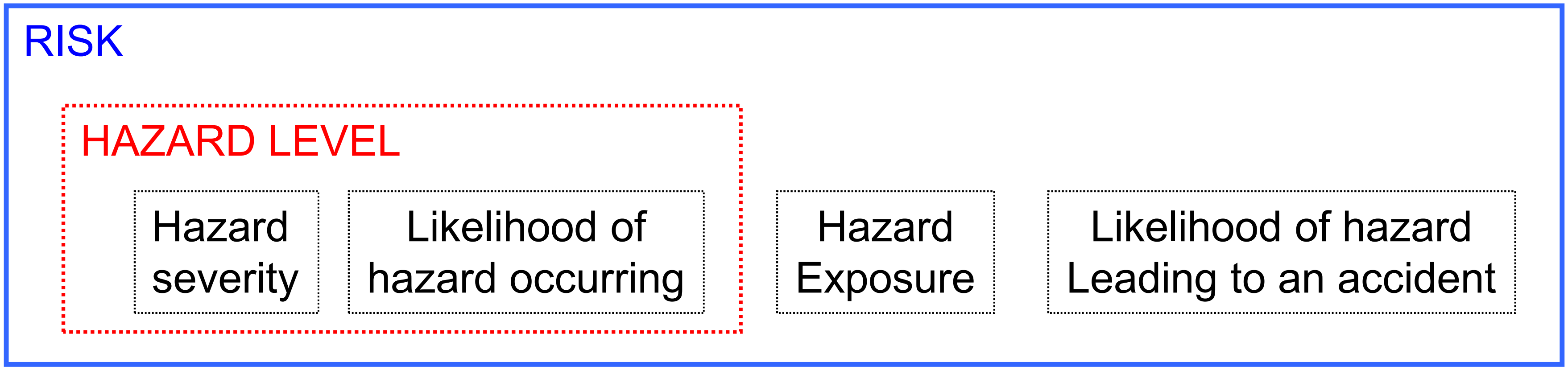
Hazard: A state or set of conditions that, together with other (worst case) conditions in the environment, will lead to an accident (loss event).

Note that a hazard is NOT equal to a failure.

"Distinguishing hazards from failures is implicit in understanding the difference between safety and reliability engineering." (C.O. Miller)

Hazard Level: A combination of severity (worst potential damage in case of an accident) and likelihood of occurrence of the hazard.

Risk: The hazard level combined with the likelihood of the hazard leading to an accident plus exposure (or duration) of the hazard.



RISK

HAZARD LEVEL

Hazard severity

Likelihood of hazard occurring

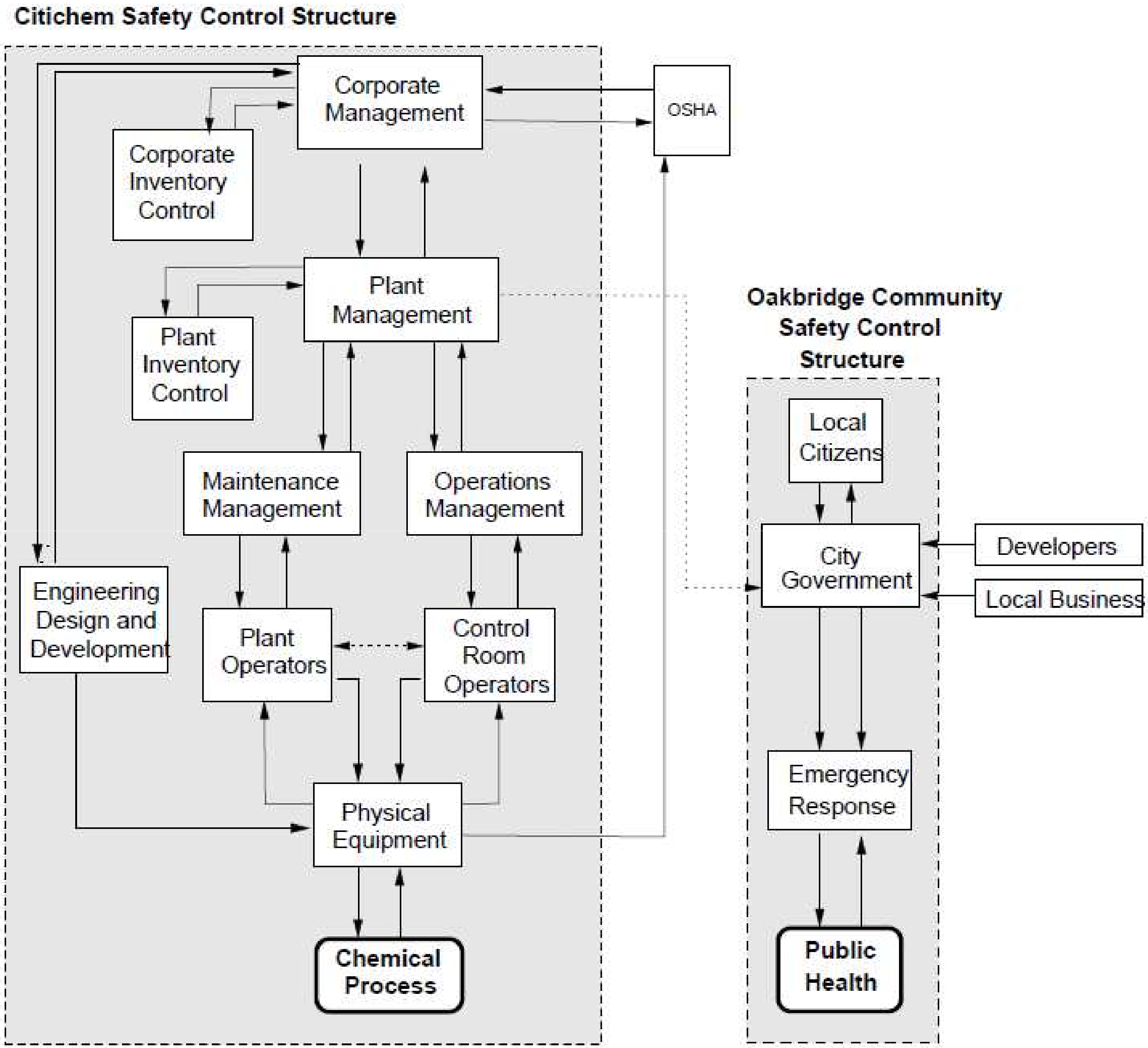
Hazard Exposure

Likelihood of hazard Leading to an accident

Safety: Freedom from accidents or losses.

Identifying Hazards

- Must be within system but that depends on where draw system boundaries
  - Choose hazards within design space
  - Example: release of chemicals from plant
- Each part of socio-technical system responsible for different parts of accident process and perhaps different hazards
- Define small set of high-level hazards first
- Then can translate hazards into safety constraints and requirements and refine them.


Citichem Safety Control Structure
Corporate Management
OSHA
Corporate Inventory Control
Plant Management
Plant Inventory Control
Maintenance Management
Operations Management
Engineering Design and Development
Plant Operators
Control Room Operators
Physical Equipment
Chemical Process
Oakbridge Community Safety Control Structure
Local Citizens
City Government
Developers
Local Business
Emergency Response
Public Health

Hazards for Explorer Spacecraft

H1. Inability of Mission to collect data. (↑ACC4)

H2. Inability of Mission to return collected data. (↑ACC5)

H3. Inability of Mission scientific investigators to use returned data. (↑ACC5)

H4. Contamination of Outer Planet Moon with biological agents of Earth origin on mission hardware. (↑ACC3)

H5. Exposure of Earth life or human assets on Earth to toxic, radioactive, or energetic elements of mission hardware. (↑ACC1)

H6. Exposure of Earth life or human assets off Earth to toxic, radioactive, or energetic elements of mission hardware. (↑ACC2)

H7. Inability of other space exploration missions to use shared space exploration infrastructure to collect, return, or use data. (↑ACC5)

Hazards for TCAS II

TCAS Hazards:

1. Near mid-air collision (NMAC): Two controlled aircraft violate minimum separation standards)
2. Controlled maneuver into ground
3. Pilot loses control of aircraft
4. Interference with other safety-related aircraft systems
5. Interference with the ground-based ATC system
6. Interference with ATC safety-related advisory

Exercise Continued

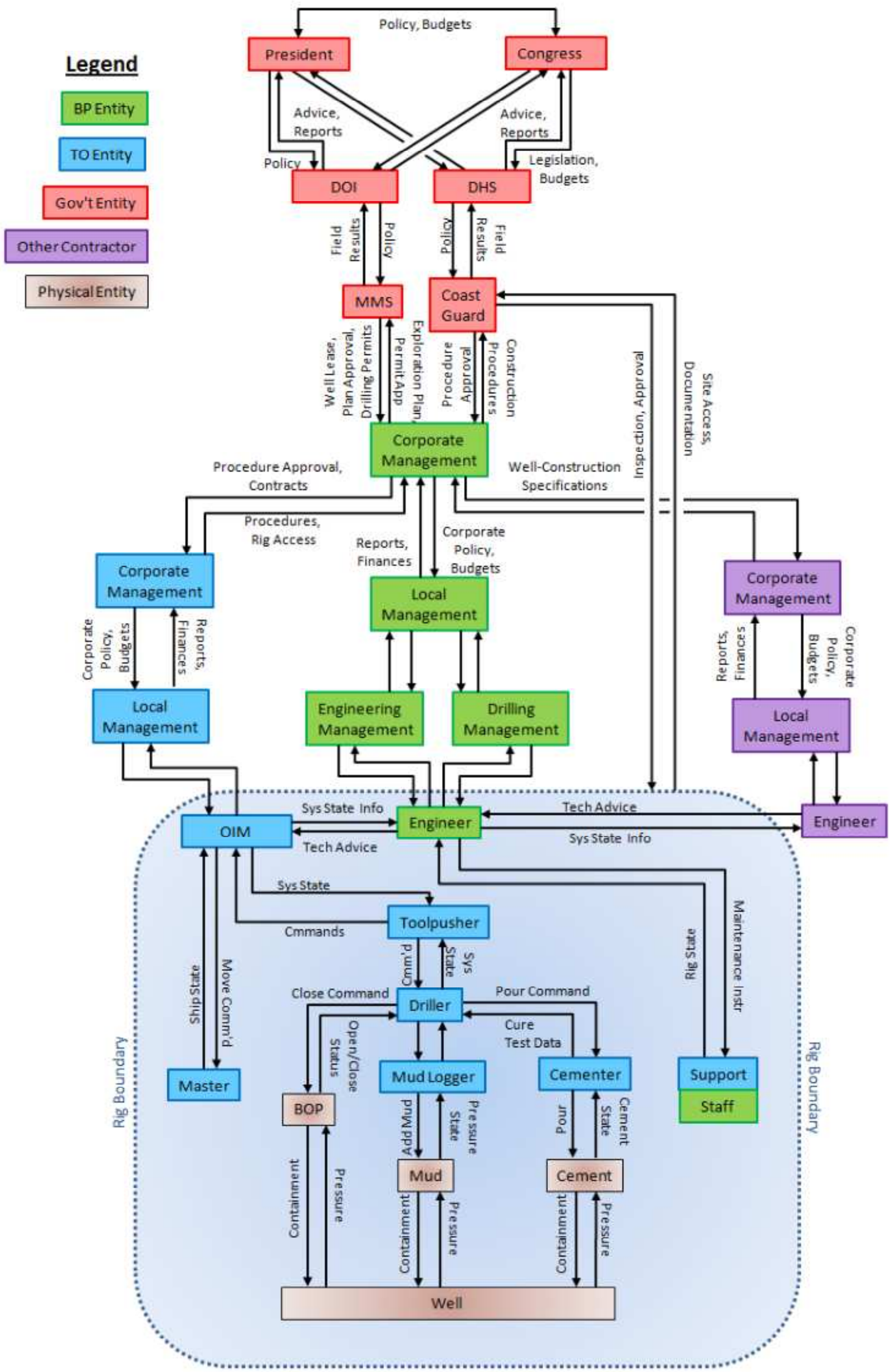
- Now identify the high-level hazards for your selected system
  - Be careful to identify only the high-level ones (will be very few)
  - Don’t include causes (e.g., operator error) or refine them at this point

Defining the High-Level Control Structure

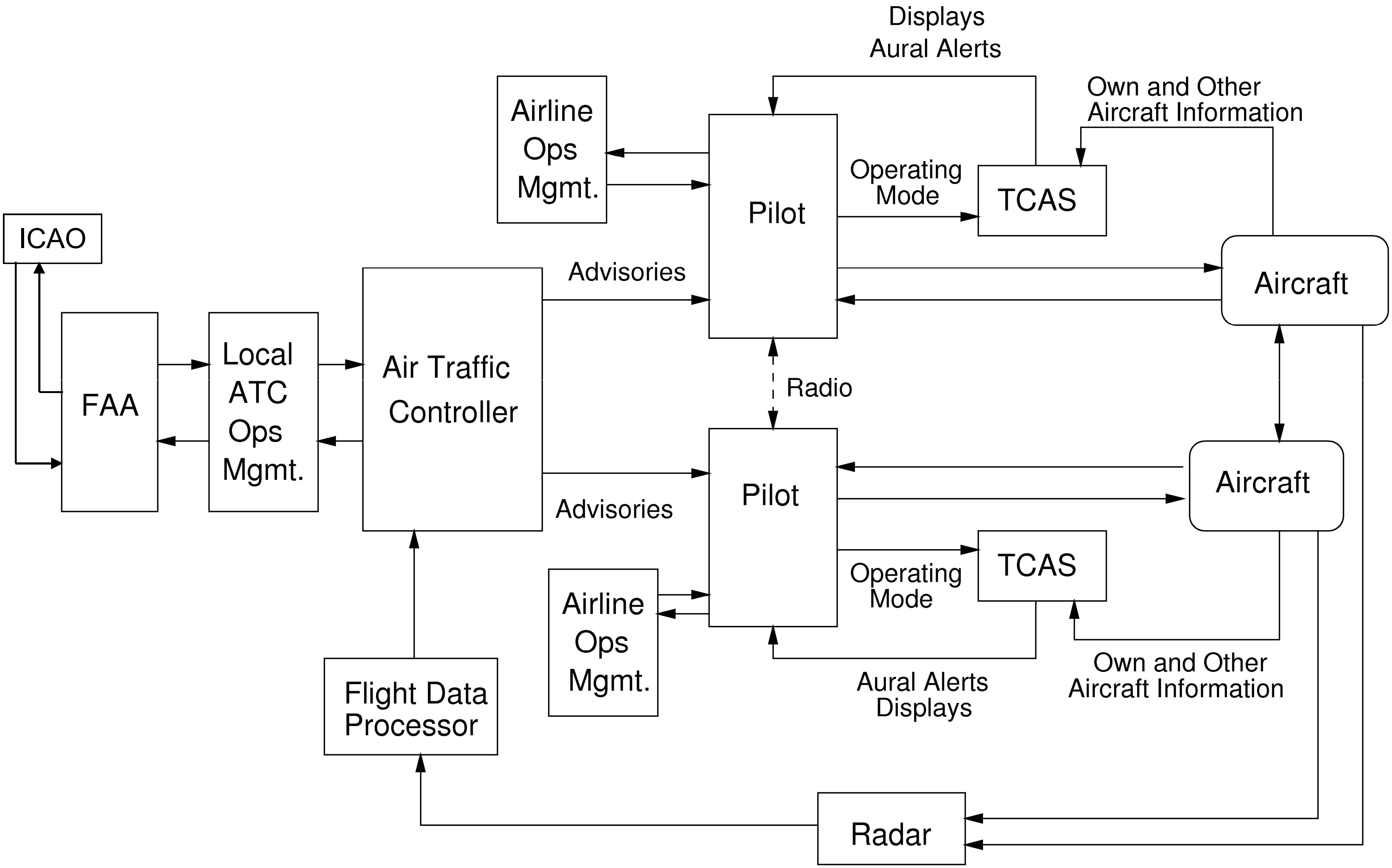
- Need the control structure not the physical structure
- Engineers more used to defining physical connections than logical connections
- Basically just functional decomposition of the system

Defining the Safety Control Structure

- High-level preliminary control structure is defined first
- Then refine as design process continues
- Need the control structure not the physical structure
  - Not the same as the physical structure
  - Basically the functional structure of the system
- Often useful to define levels or different views


Legend
BP Entity
TO Entity
Gov't Entity
Other Contractor
Physical Entity
Policy, Budgets
President
Congress
Advice, Reports
Advice, Reports
Policy
Legislation, Budgets
DOI
DHS
Field Results
Policy
Policy
Field Results
MMS
Coast Guard
Well Lease, Plan Approval, Drilling Permits
Permit App
Exploration Plan
Procedure Approval
Construction Procedures
Inspection, Approval
Site Access, Documentation
Corporate Management
Procedure Approval, Contracts
Well-Construction Specifications
Procedures, Rig Access
Reports, Finances
Corporate Policy, Budgets
Corporate Management
Local Management
Corporate Management
Corporate Policy, Budgets
Reports, Finances
Reports, Finances
Corporate Policy, Budgets
Local Management
Engineering Management
Drilling Management
Local Management
Sys State Info
Tech Advice
Engineer
OIM
Tech Advice
Sys State Info
Engineer
Sys State
Toolpusher
Cmmands
Comm'd
Sys State
Ship State
Move Comm'd
Rig State
Maintenance Instr
Close Command
Pour Command
Driller
Open/Close Status
Cure Test Data
Master
BOP
Mud Logger
Cementer
Support
Staff
Add Mud
Pressure State
Pour
Cement State
Mud
Cement
Containment
Pressure
Containment
Pressure
Containment
Pressure
Well
Rig Boundary
Rig Boundary

TCAS II Control Structure



Component Responsibilities

TCAS:

- Receive and update information about its own and other aircraft
- Analyze information received and provide pilot with
  - Information about where other aircraft in the vicinity are located
  - An escape maneuver to avoid potential NMAC threats

Pilot

- Maintain separation between own and other aircraft using visual scanning
- Monitor TCAS displays and implement TCAS escape maneuvers
- Follow ATC advisories

Air Traffic Controller

- Maintain separation between aircraft in controlled airspace by providing advisories (control action) for pilot to follow

Aircraft components (e.g., transponders, antennas)

- Execute control maneuvers
- Receive and send messages to/from aircraft
- Etc.

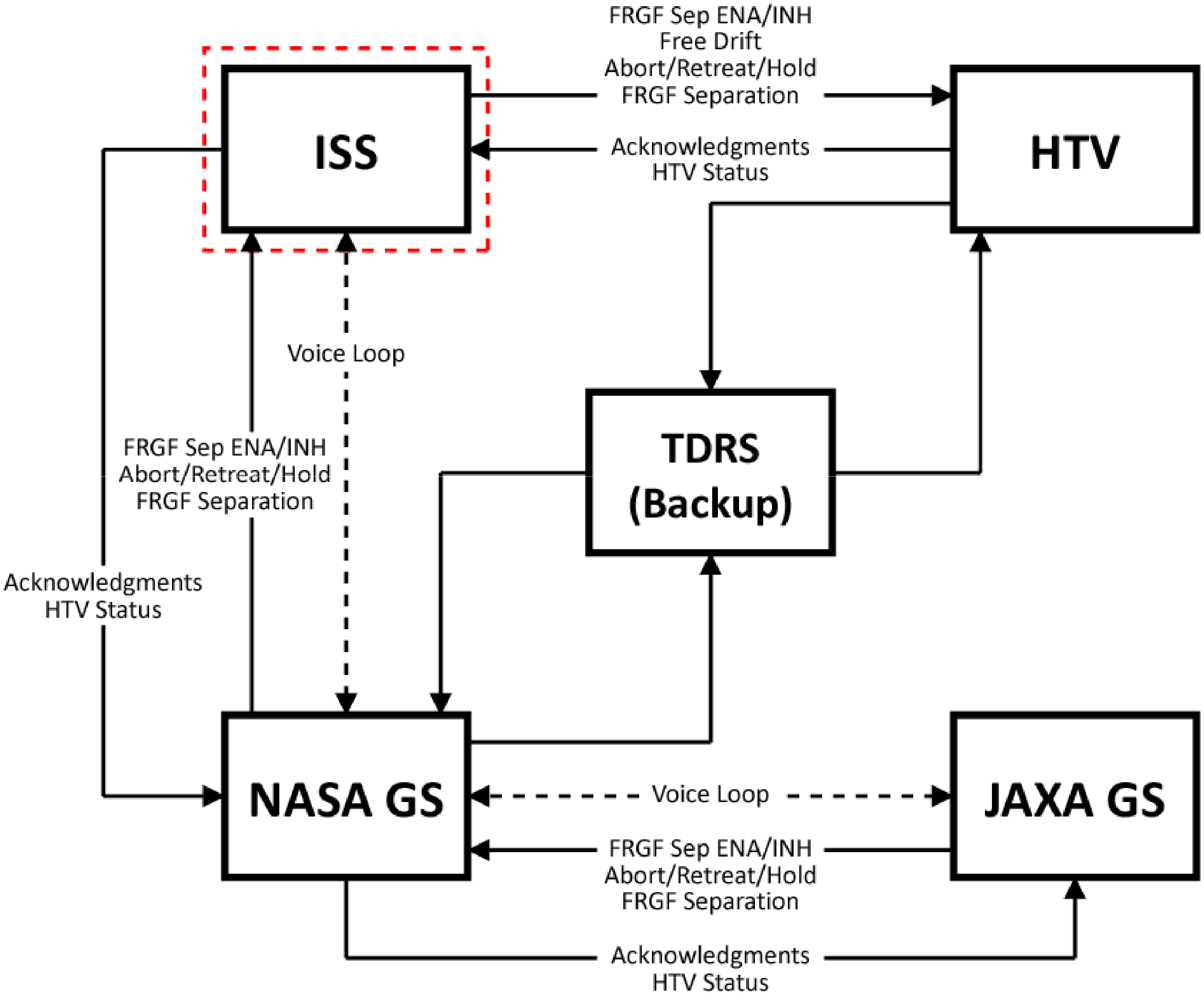
Airline Operations Management

- Provide procedures for using TCAS and following TCAS advisories
- Train pilots
- Audit pilot performance

Air Traffic Control Operations Management

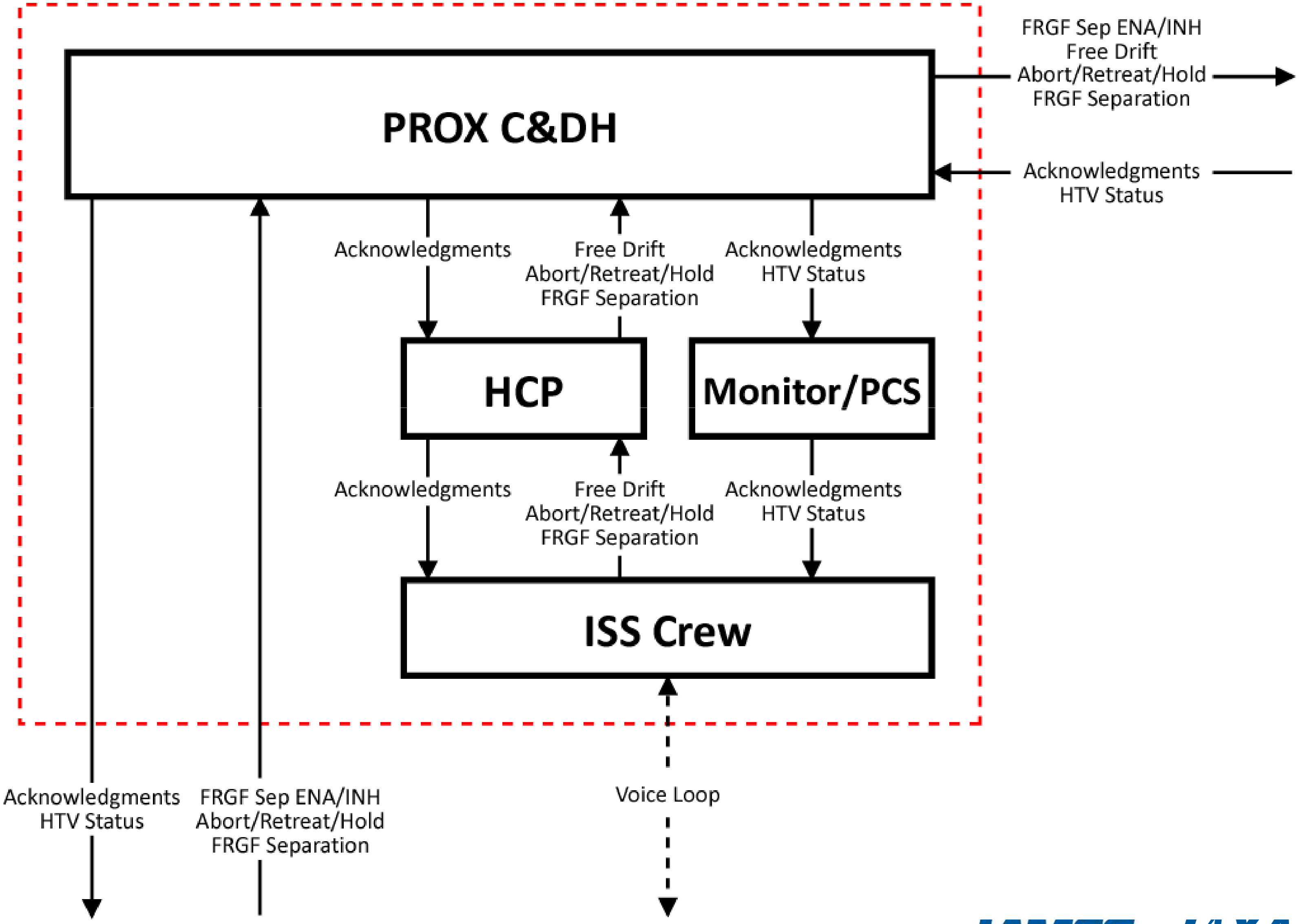
- Provide procedures
- Train controllers,
- Audit performance of controllers
- Audit performance of overall collision avoidance system

Control Structure Diagram – Level 0



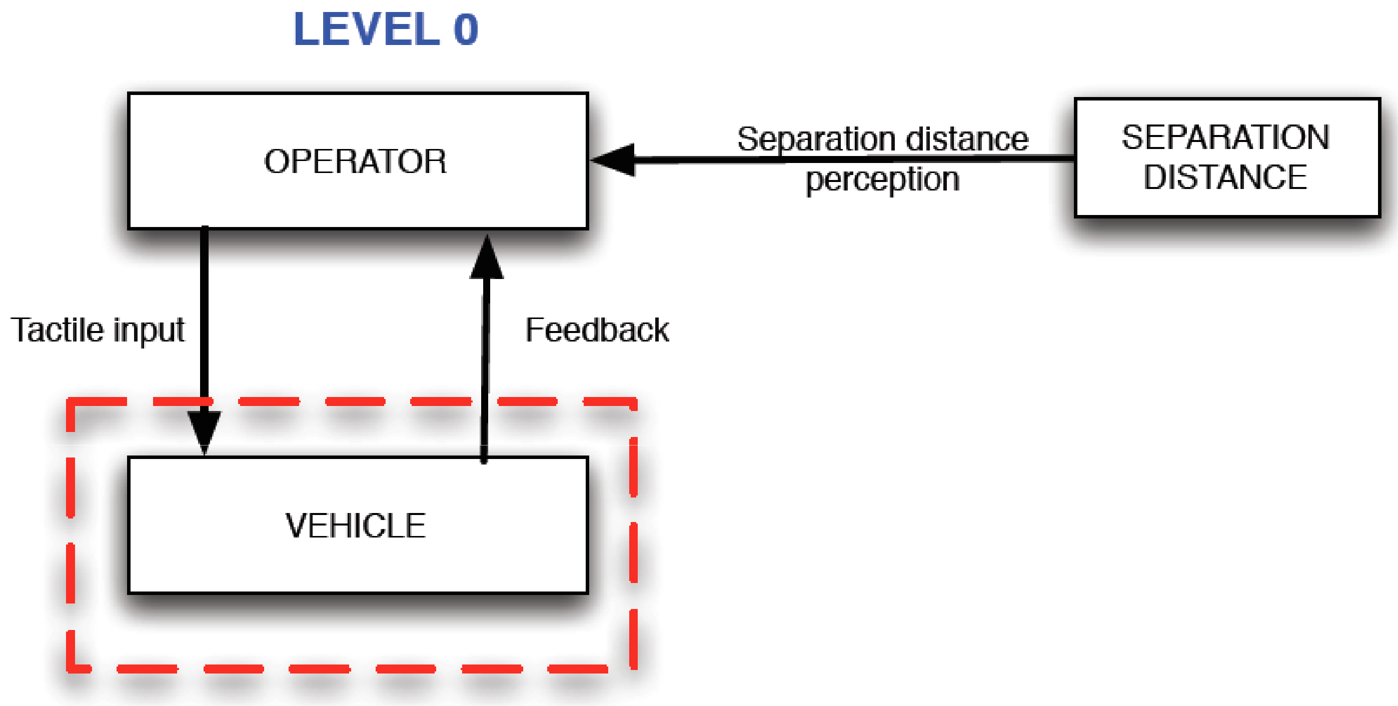
Japan Manned Space Systems Corporation JAMSS JAXA Japan Aerospace Exploration Agency

Control Structure Diagram – ISS Level 1



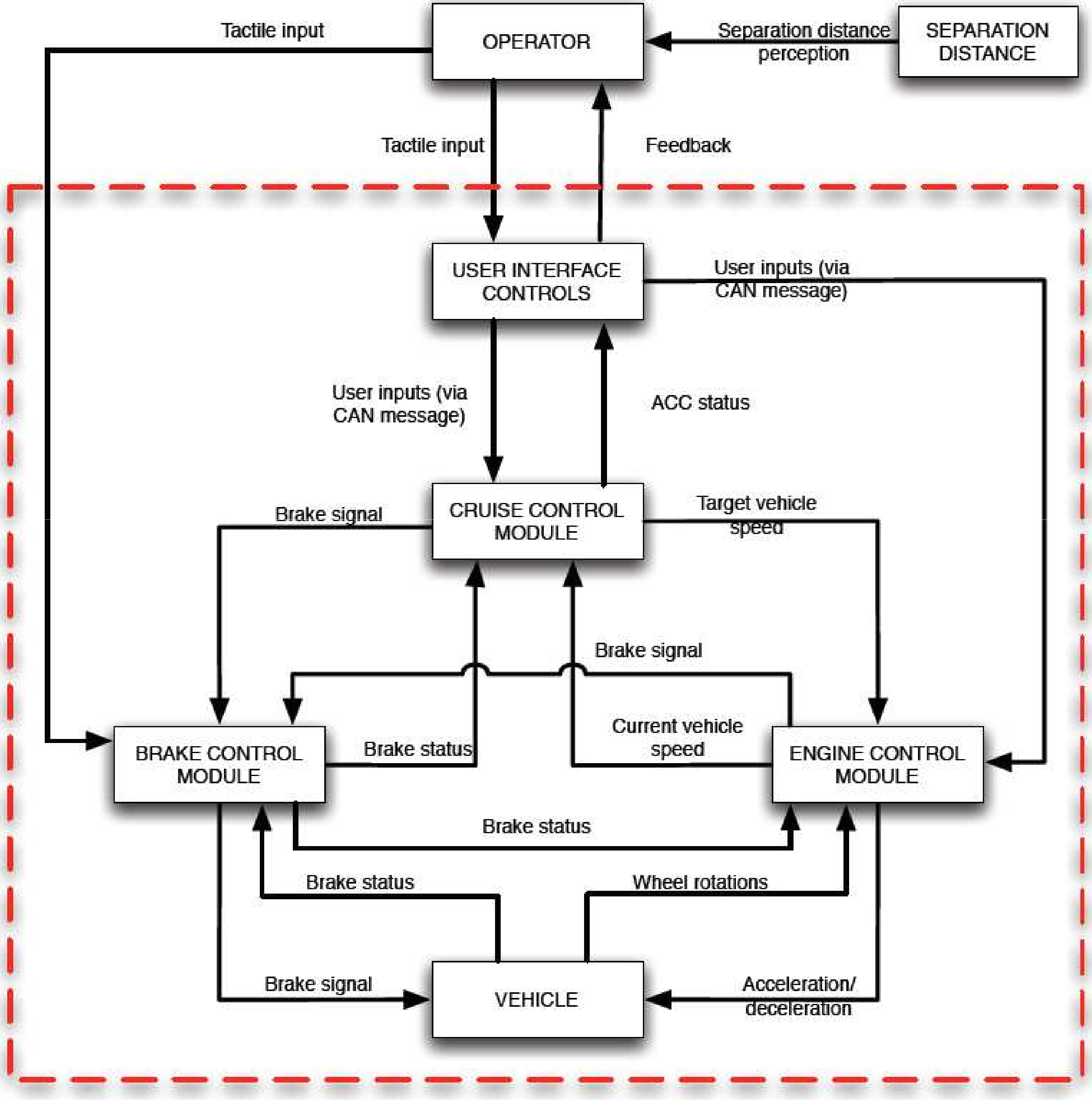
JAMSS JAXA Japan Aerospace Exploration Agency

ACC Control Structure Development



Source of information:

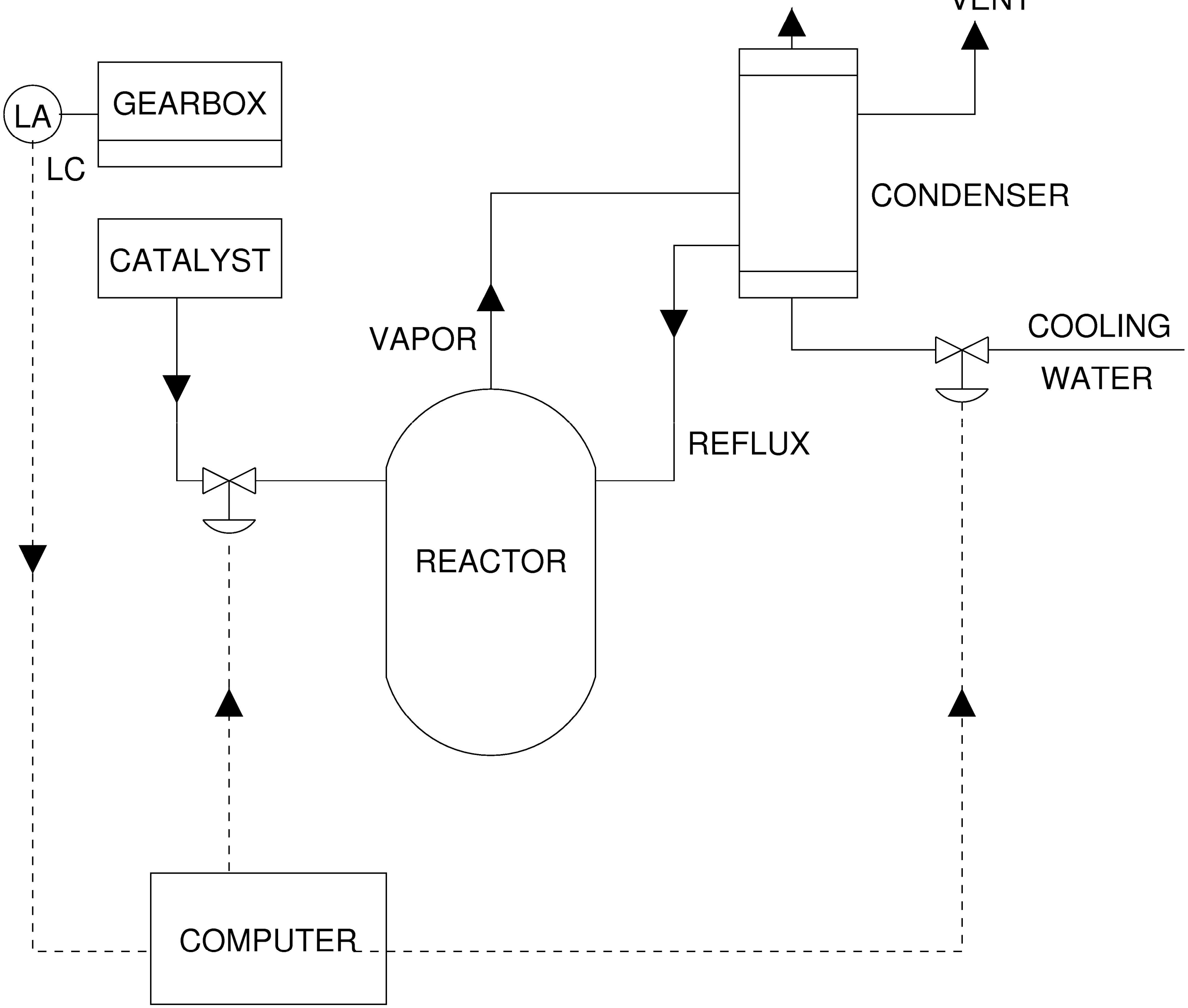
LEVEL 1


OPERATOR
SEPARATION DISTANCE
Separation distance perception
Tactile input
Tactile input
Feedback
USER INTERFACE CONTROLS
User inputs (via CAN message)
User inputs (via CAN message)
ACC status
CRUISE CONTROL MODULE
Brake signal
Target vehicle speed
Brake signal
BRAKE CONTROL MODULE
Brake status
Current vehicle speed
ENGINE CONTROL MODULE
Brake status
Brake status
Wheel rotations
Brake signal
VEHICLE
Acceleration/ deceleration

Exercise

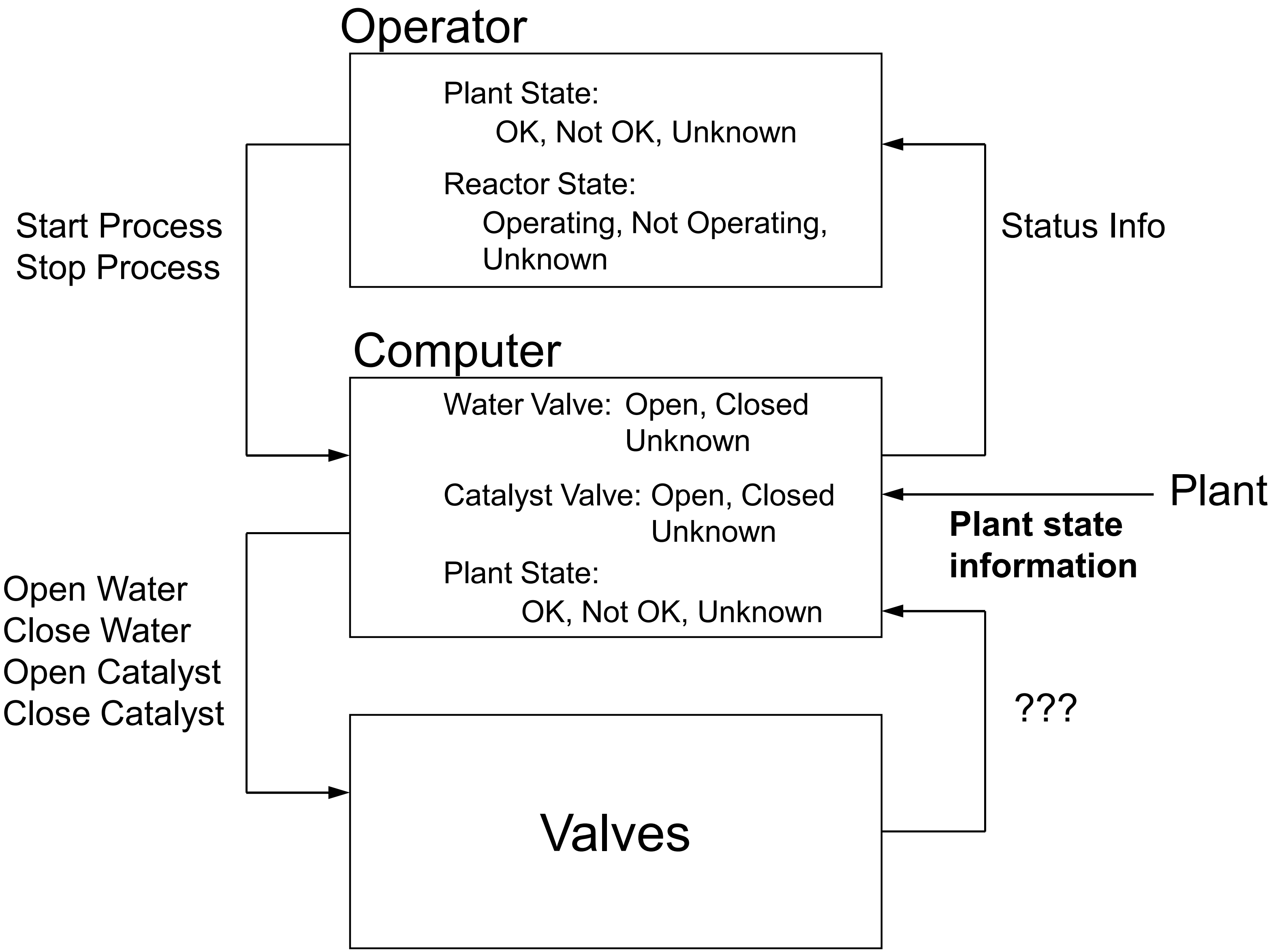
- Draw the functional control structure for your application
  - Start with a VERY simple, very high-level model
  - Identify responsibilities, commands, feedback
  - Refine one box into a more detailed level

Accident with No Component Failures



Exercise

- Draw the high-level control structure for this system.
  - Start with a simple control structure with three boxes
    - Operator
    - Automated controller
    - Controlled process
  - Specify
    - Component responsibilities
    - Control actions
    - Process model for each of the two controllers



Operator

Plant State:
OK, Not OK, Unknown

Reactor State:
Operating, Not Operating,
Unknown

Start Process
Stop Process

Status Info

Computer

Water Valve: Open, Closed
Unknown

Catalyst Valve: Open, Closed
Unknown

Plant State:
OK, Not OK, Unknown

Plant

Plant state information

Open Water
Close Water
Open Catalyst
Close Catalyst

???

Valves

Documentation

- Remember to document all this as go along
  - As part of engineering specifications (not separate) but identified as safety-related
  - In hazard log
- Include
  - Accidents, hazards, high-level safety requirements, control structure
  - Refined safety requirements and allocation to components
  - Analysis results
  - Design decisions
  - Design rationale
  - Tracing between design decisions and safety requirements

STPA Step 1: Identifying Unsafe Control Actions

- We have now established the fundamental information to start the analysis
- Next step (Step 1) is to identify the unsafe control actions that each component can produce.
  - Helps in refining safety requirements and constraints
  - Step 2 will determine the causes of these unsafe control actions. Causes will be used to guide design to eliminate or control them.

Identifying Unsafe Control Actions

Four ways a controller can provide unsafe control:

1. A control action required for safety is not provided
2. An unsafe control action is provided
3. A potentially safe control action is provided too late or too early (at the wrong time) or in the wrong sequence
4. A control action required for safety is stopped too soon or applied too long.

Identifying Unsafe Control Actions

Four ways a controller can provide unsafe control:

1. A control action required for safety is not provided
   - The aircraft are on a near collision course and TCAS does not provide an RA
   - The pilot does not follow the resolution advisory provided by TCAS (does not respond to the RA)
2. An unsafe control action is provided
   - The aircraft are in close proximity and TCAS provides an RA that degrades vertical separation.
   - The pilot incorrectly executes the TCAS resolution advisory.

Identifying Unsafe Control Actions

3. A potentially safe control action is provided too late or too early (at the wrong time) or in the wrong sequence

   ➢ The aircraft are on a near collision course and TCAS provides an RA too late to avoid an NMAC

   ➢ The pilot applies the RA but too late to avoid the NMAC

4. A control action required for safety is stopped too soon or applied too long.

   ➢ TCAS removes an RA too soon

   ➢ The pilot stops the RA maneuver too soon.

Defining System-Level Safety Constraints (Requirements)

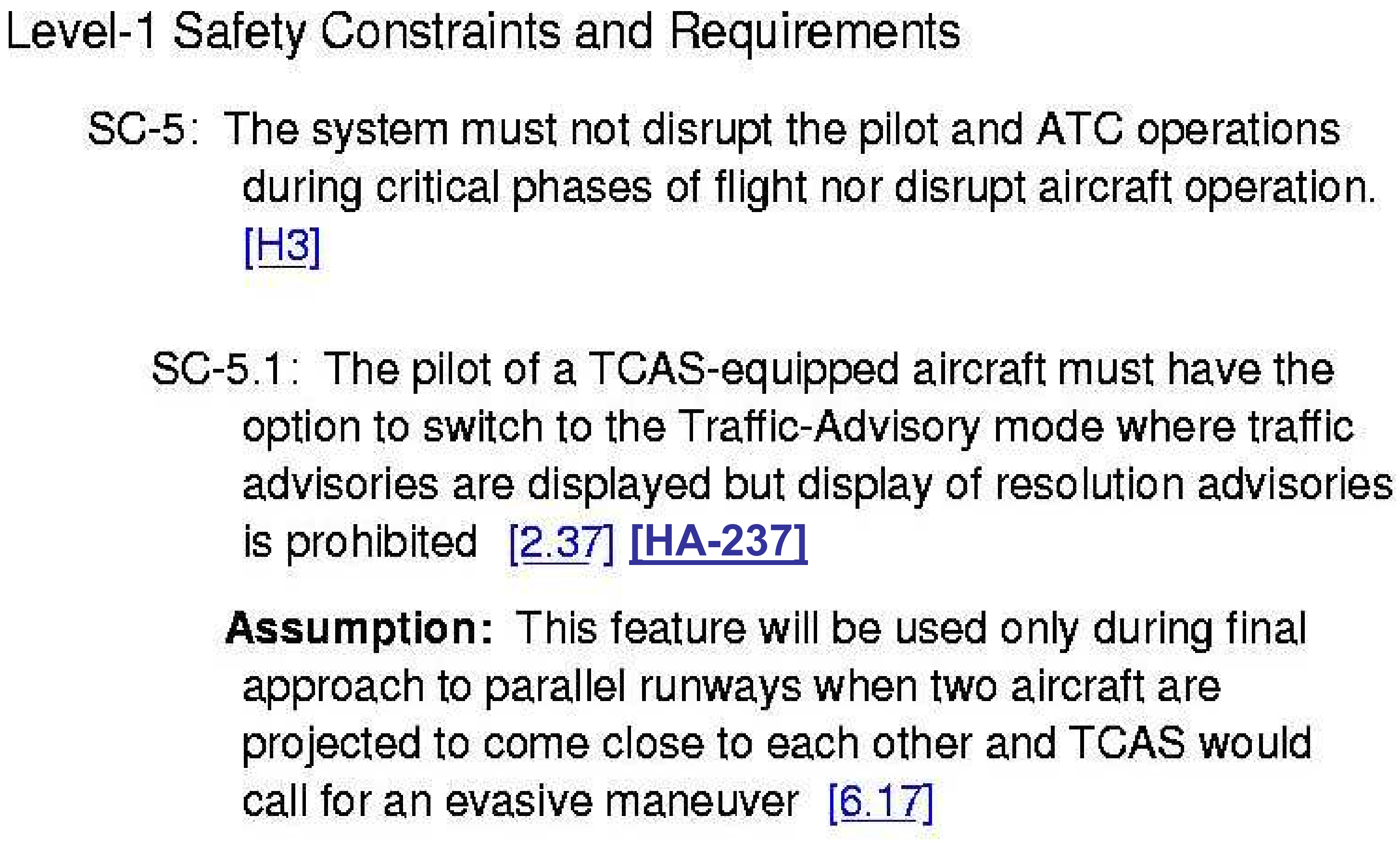
TCAS

- When two aircraft are on a collision course, TCAS must always provide an RA to avoid the collision
- TCAS must not provide RAs that degrade vertical separation
- TCAS must always provide an RA in time to prevent an NMAC
- …

Pilot

- The pilot must always follow the RA provided by TCAS
- …

Refinement of High-Level Safety Constraints and Requirements (Done in Step 2)



Level-1 Safety Constraints and Requirements

SC-5: The system must not disrupt the pilot and ATC operations during critical phases of flight nor disrupt aircraft operation. [H3]

SC-5.1: The pilot of a TCAS-equipped aircraft must have the option to switch to the Traffic-Advisory mode where traffic advisories are displayed but display of resolution advisories is prohibited [2.37] **[HA-237]**

Assumption: This feature will be used only during final approach to parallel runways when two aircraft are projected to come close to each other and TCAS would call for an evasive maneuver [6.17]

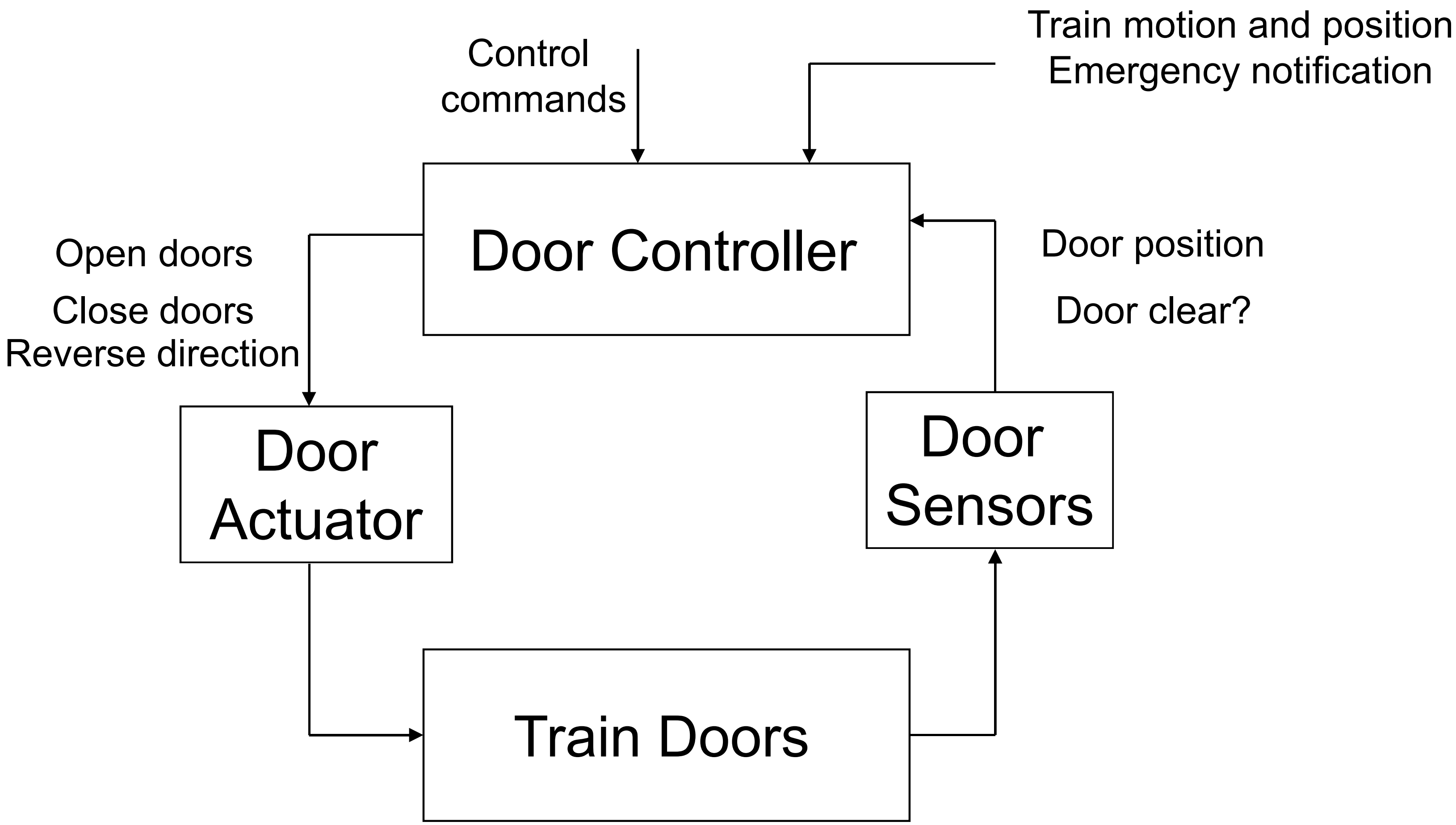
STPA Automated Train Door Example

- Define accident (death or injury of passenger or employee)
- Identify hazards and translate into high-level safety design constraints

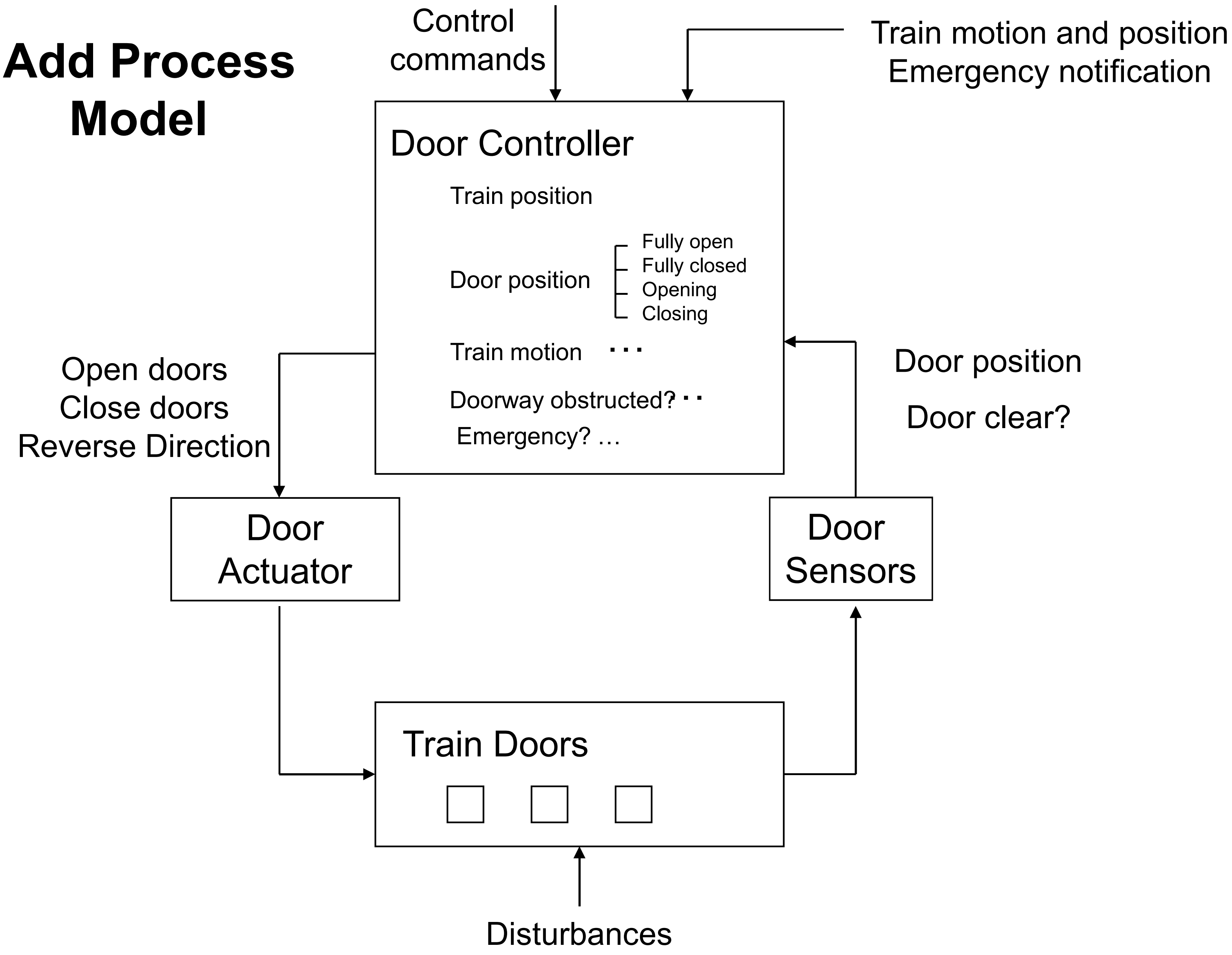
  Door Control System hazards:

  - Doors open while train is in motion or not aligned with station platform
  - Door closes on a person
  - Passengers cannot evacuate in case of an emergency

- Define control structure and basic component safety-related responsibilities



Add Process Model



Control commands

Train motion and position
Emergency notification

Door Controller

Train position

Door position

- Fully open
- Fully closed
- Opening
- Closing

Train motion . . .

Doorway obstructed? . .

Emergency? …

Open doors
Close doors
Reverse Direction

Door position

Door clear?

Door Actuator

Door Sensors

Train Doors

Disturbances

Using a Table Helps to Organize Step 1

- Start from each high level hazard.
- Create a table with a row for each control action and a column for the four types of unsafe control.

Control Action	1) Not providing causes hazard	2) Providing causes hazard	3) Wrong Timing or Order	4) Stopped too soon
Provides door close command	Doors not commanded closed or re-closed before moving	Doors commanded closed while person or object is in the doorway Doors commanded closed during an emergency evacuation	Doors commanded closed too early, before passengers finish entering/exiting Doors commanded closed too late, after train starts moving	Door close command stopped too soon, not completely closed
Provides door open command	Doors not commanded open for emergency evacuation Doors not commanded open after closing while a person or obstacle is in the doorway	Doors commanded open while train is in motion Doors commanded open while train is not aligned at a platform	Doors commanded open before train has stopped or after it started moving (covered by “while train is in motion”) Doors commanded open late after emergency	Door open command stopped too soon during emergency stop

Generating Safety Requirements

- Rewrite entries in table as high-level requirements or constraints on controller.
  - Doors must not be opened until train is stopped and aligned with platform
  - Doors must not be closed if someone is in the doorway.
  - If a person is detected in doorway during door closing, door closing must be stopped and reversed
  - Train must not move with doors open
  - etc.
- Use Step 2 to refine constraints by identifying causes of unsafe control actions.

Class Exercise

- Take the batch chemical reactor example.
- Using the control diagram and process models you drew
  - STEP 1: Create a table of unsafe control actions for the hazard: *Catalyst in reactor without reflux condenser operating (water flowing through it)*

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

Command	Providing causes hazard	Not providing causes hazard	Too early, too late, wrong order	Stopped too soon
Open Water				
Close Water				
Open Catalyst				
Close catalyst				
Send message to op about problem in plant				

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

Command	**Providing causes hazard**	**Not providing causes hazard**	Too early, too late, wrong order	Stopped too soon
Open Water	Not opened when catalyst open	Not hazardous	Open water more than X seconds after catalyst	Stop before fully opened
Close Water	not hazardous	Close while catalyst open	Close before catalyst closes	
Open Catalyst	Not hazardous	Provided when water valve not open	Open catalyst more than X seconds before open water	
Close catalyst	Do not close when water closed	Not hazardous	Close catalyst more than X seconds after close water	Stopped before fully closed
Send message to op about problem in plant	Not hazardous?	Not hazardous?	Not hazardous?	

Resulting High-Level Constraints

- Translate the entries in the table into constraints

STPA Step 2: Identifying Causes and Designing Controls

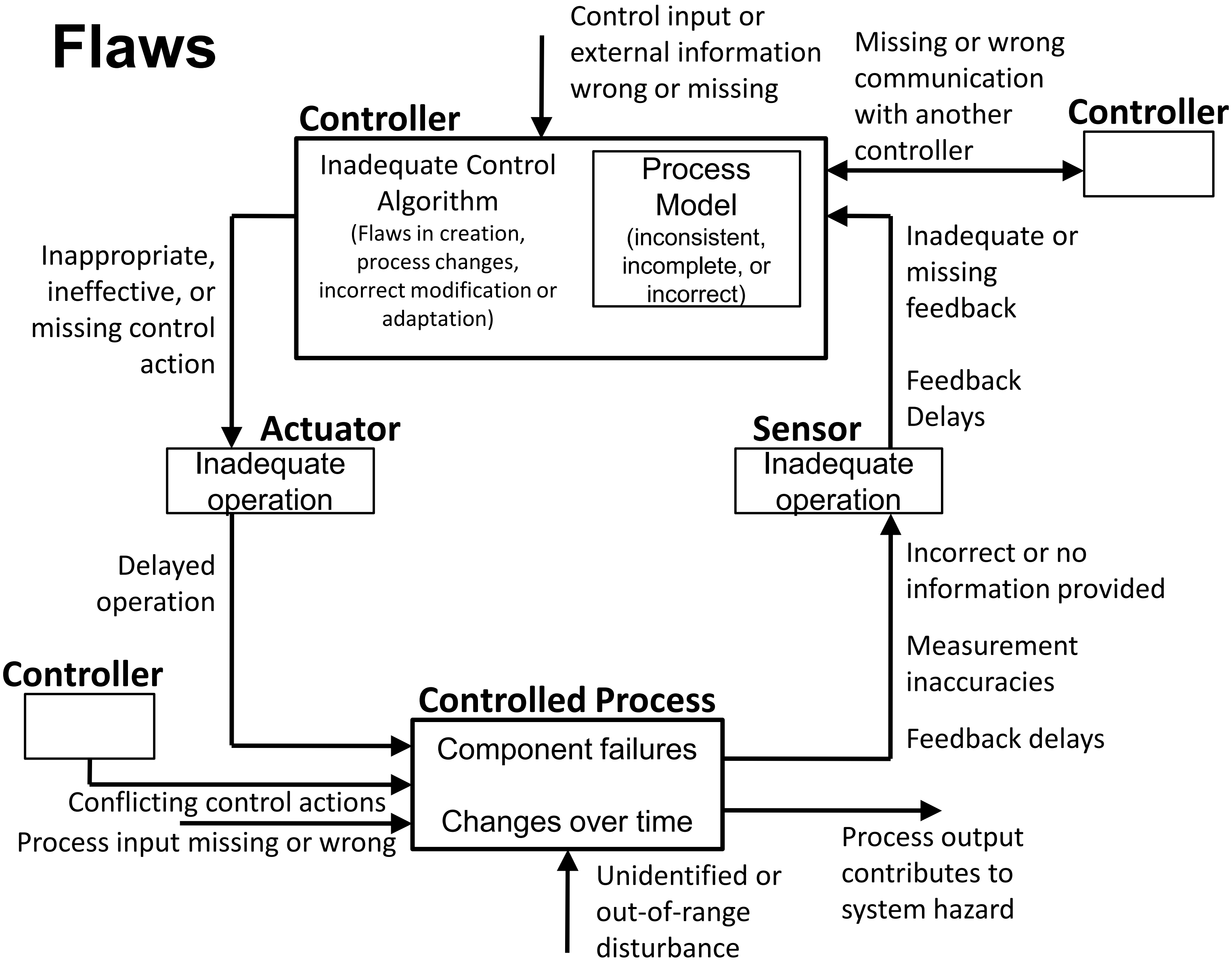
Determine how each potentially hazardous control action identified in Step 1 could occur

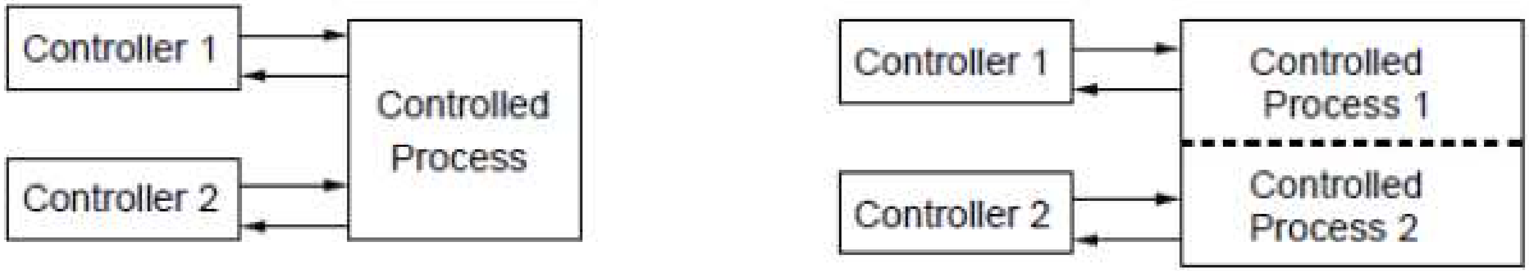
a) For each unsafe control action, examine the parts of control loop to see if they could cause it.

b) Design mitigation measures if they do not already exist or evaluate existing measures if analysis being performed on an existing design.

c) Determine if new hazards created by design changes

Potential Control Flaws


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



(a) Example of an overlap

(b) Example of a boundary area

Problems can occur when there is shared control or at the boundary areas of separately controlled processes.

Exercise Continued

- STEP 2: Identify some causes of the hazardous condition: *Open catalyst valve when water valve not open*

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

Results

- My first guess, without STPA, of the software safety requirement:

  "Always open water valve before catalyst valve"

  turned out to be incomplete

- Need more than this as well as additional design controls (e.g., flow monitor)
- Can potentially provide automated support
- A simple example, but more complex examples have been done and compared with standard safety analysis

Step 3: Operations and Performance Monitoring

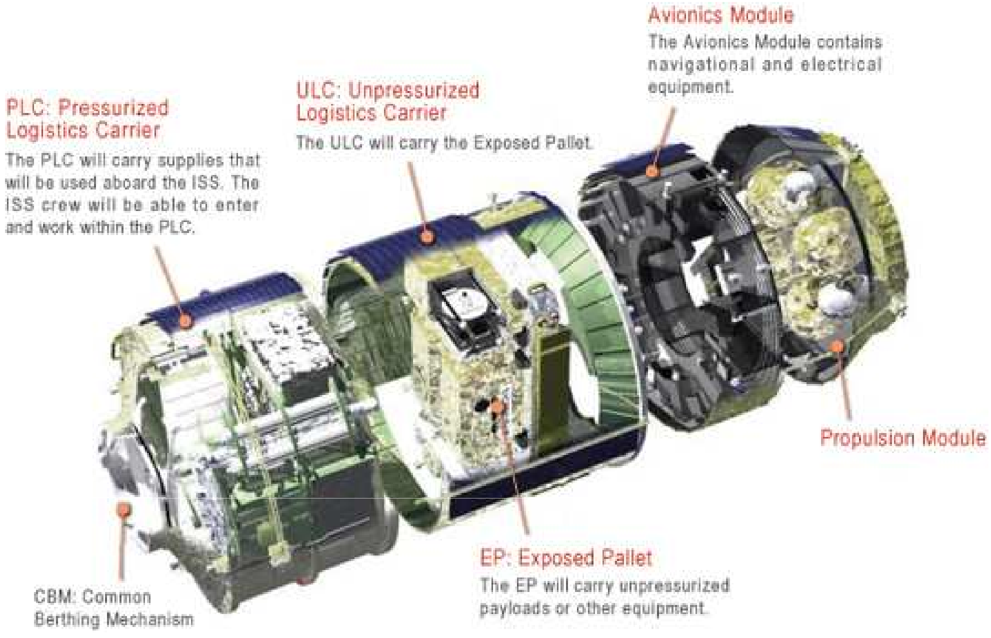
Need to consider how designed controls could degrade over time and build in protection, including

a) Planned performance audits where assumptions underlying the hazard analysis are the preconditions for the operational audits and controls

b) Management of change procedures

c) Incident analysis

HTV: H-II Transfer Vehicle


Avionics Module
The Avionics Module contains navigational and electrical equipment.
ULC: Unpressurized Logistics Carrier
The ULC will carry the Exposed Pallet.
PLC: Pressurized Logistics Carrier
The PLC will carry supplies that will be used aboard the ISS. The ISS crew will be able to enter and work within the PLC.
Propulsion Module
EP: Exposed Pallet
The EP will carry unpressurized payloads or other equipment.
CBM: Common Berthing Mechanism

HTV Specifications

Items	Specifications
Length	9.8 m (including thrusters)
Diameter	4.4 m
Mass	10,500 kg
Propellant	Fuel: MMH Oxidizer: MON3 (Tetroxide)
Cargo capacity (supplies and equipment)	6,000 kg - Pressurized cargo: 4,500 kg - Unpressurized cargo: 1,500 kg
Cargo capacity (waste)	Max. 6,000 kg
Target orbit to ISS	Altitude: 3[illegible] m

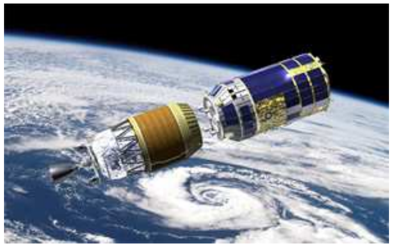
HTV-1 (Sep 10 – Nov 2): successful

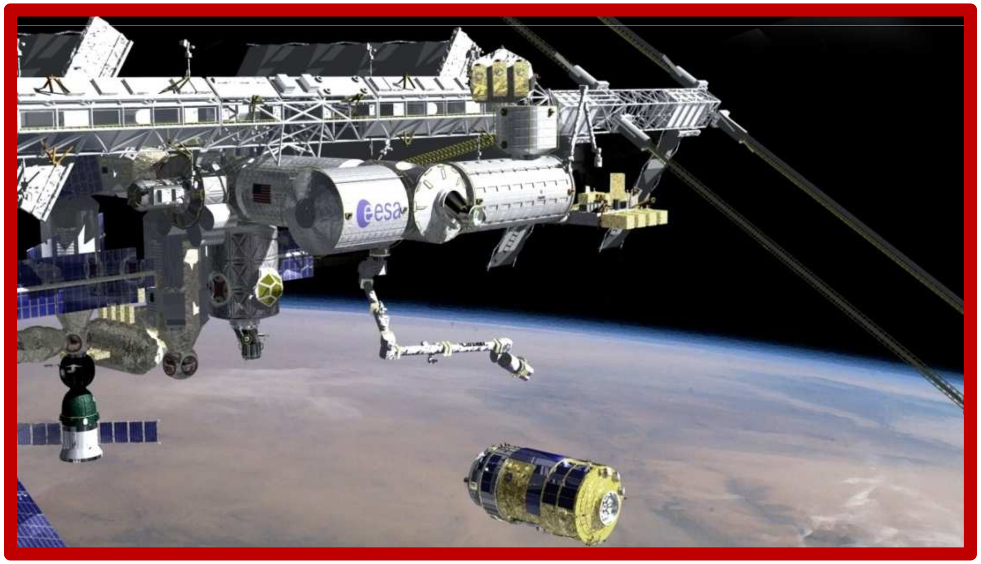
- Launched at the TNSC aboard the H-IIB rocket
- Performed the demonstration tests
- Rendezvoused and berthed with the ISS
- Released and departed from the ISS
- Performed the fiery re-entry and disintegration

HTV Operations

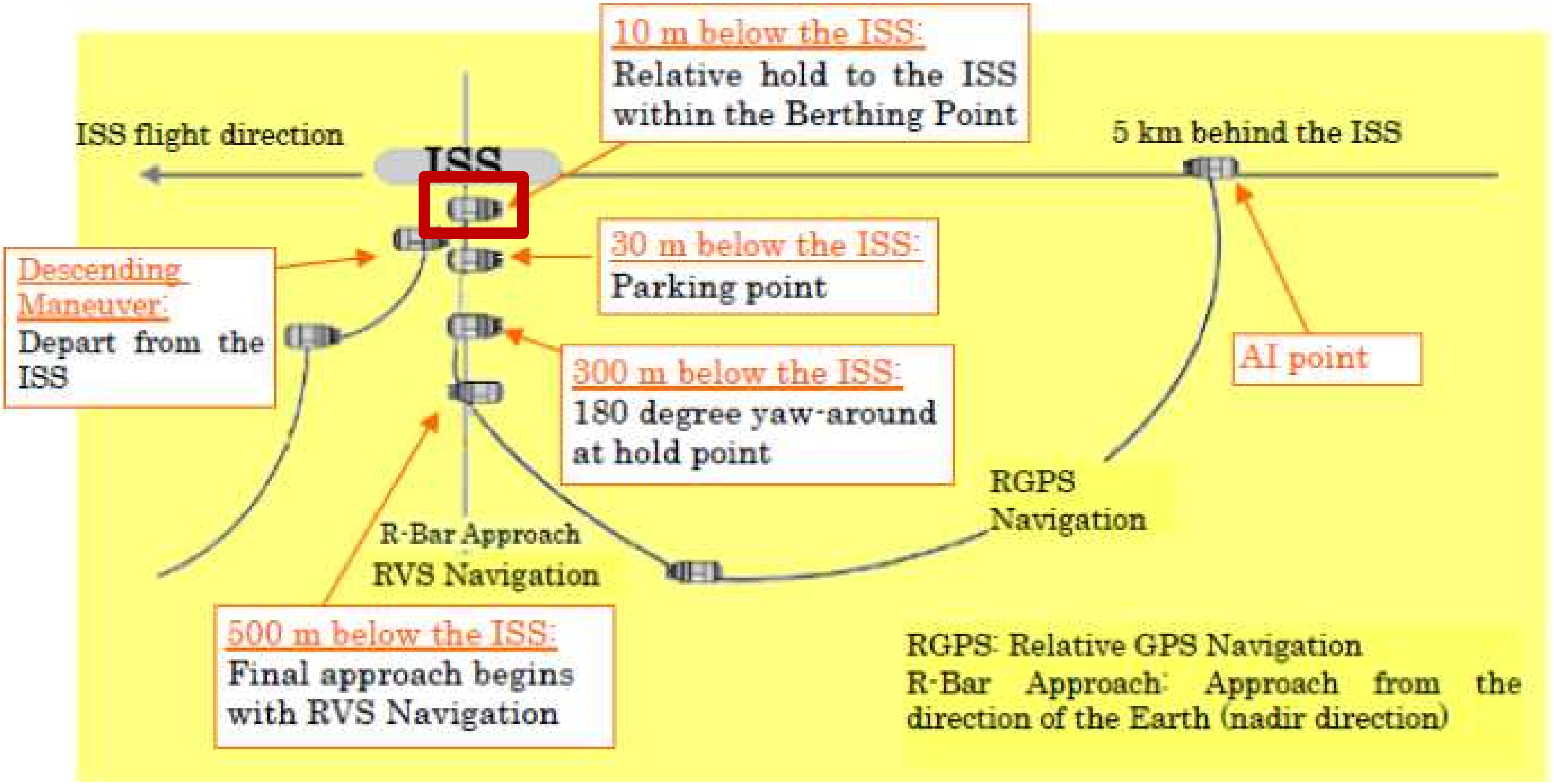
The profile for the HTV operations:

1. Launch
2. Rendezvous with the ISS
3. Berthing with the ISS
4. Operations while berthed with the ISS
5. Undock / Departure from the ISS / Re-entry





PROX Operations

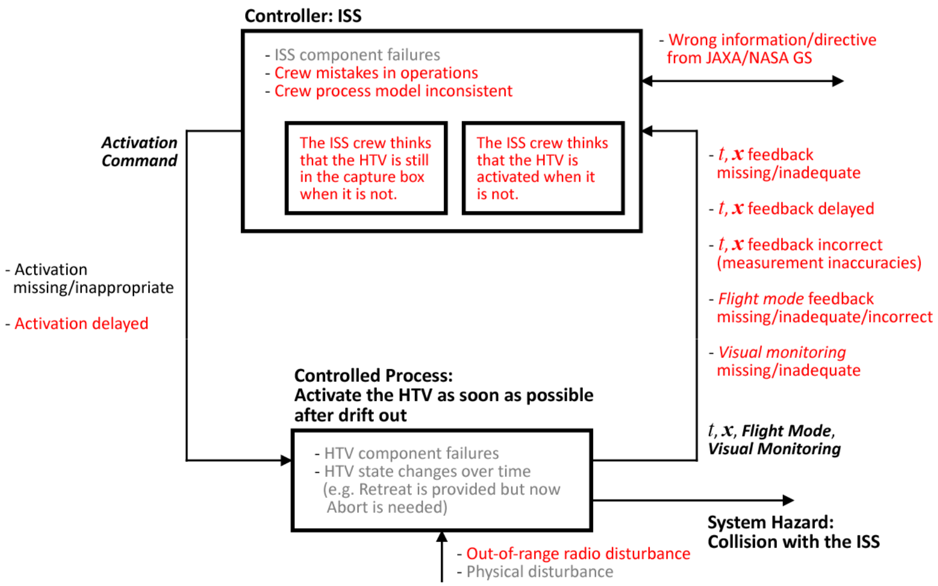

10 m below the ISS:
Relative hold to the ISS within the Berthing Point
ISS flight direction
ISS
5 km behind the ISS
Descending Maneuver:
Depart from the ISS
30 m below the ISS:
Parking point
AI point
300 m below the ISS:
180 degree yaw-around at hold point
RGPS Navigation
R-Bar Approach
RVS Navigation
500 m below the ISS:
Final approach begins with RVS Navigation
RGPS: Relative GPS Navigation
R-Bar Approach: Approach from the direction of the Earth (nadir direction)

HTV's approach sequence during PROX Operations

Comparison between STPA and FTA

Identified by both (STPA and FTA)
Identified by STPA only

- Crew mistakes in operation
- Crew process model inconsistent
- Activation missing/inappropriate
- ISS component failures
- Activation delayed
- HTV component failures
- HTV state changes over time
- Out-of-range radio disturbance
- Physical disturbance
- t, x **feedback missing/inadequate**
- t, x **feedback delayed**
- t, x **feedback incorrect**
- *Flight Mode* **feedback missing/inadequate**
- *Flight Mode* **feedback incorrect**
- *Visual Monitoring* **missing/inadequate**
- Wrong information/directive from JAXA/NASA GS



Controller: ISS

- ISS component failures
- Crew mistakes in operations
- Crew process model inconsistent

The ISS crew thinks that the HTV is still in the capture box when it is not.

The ISS crew thinks that the HTV is activated when it is not.

- Wrong information/directive from JAXA/NASA GS

Activation Command

- Activation missing/inappropriate
- Activation delayed

- t, x feedback missing/inadequate
- t, x feedback delayed
- t, x feedback incorrect (measurement inaccuracies)
- *Flight mode* feedback missing/inadequate/incorrect
- *Visual monitoring* missing/inadequate

Controlled Process: Activate the HTV as soon as possible after drift out

- HTV component failures
- HTV state changes over time (e.g. Retreat is provided but now Abort is needed)

t, x, ***Flight Mode*, *Visual Monitoring***

System Hazard: Collision with the ISS

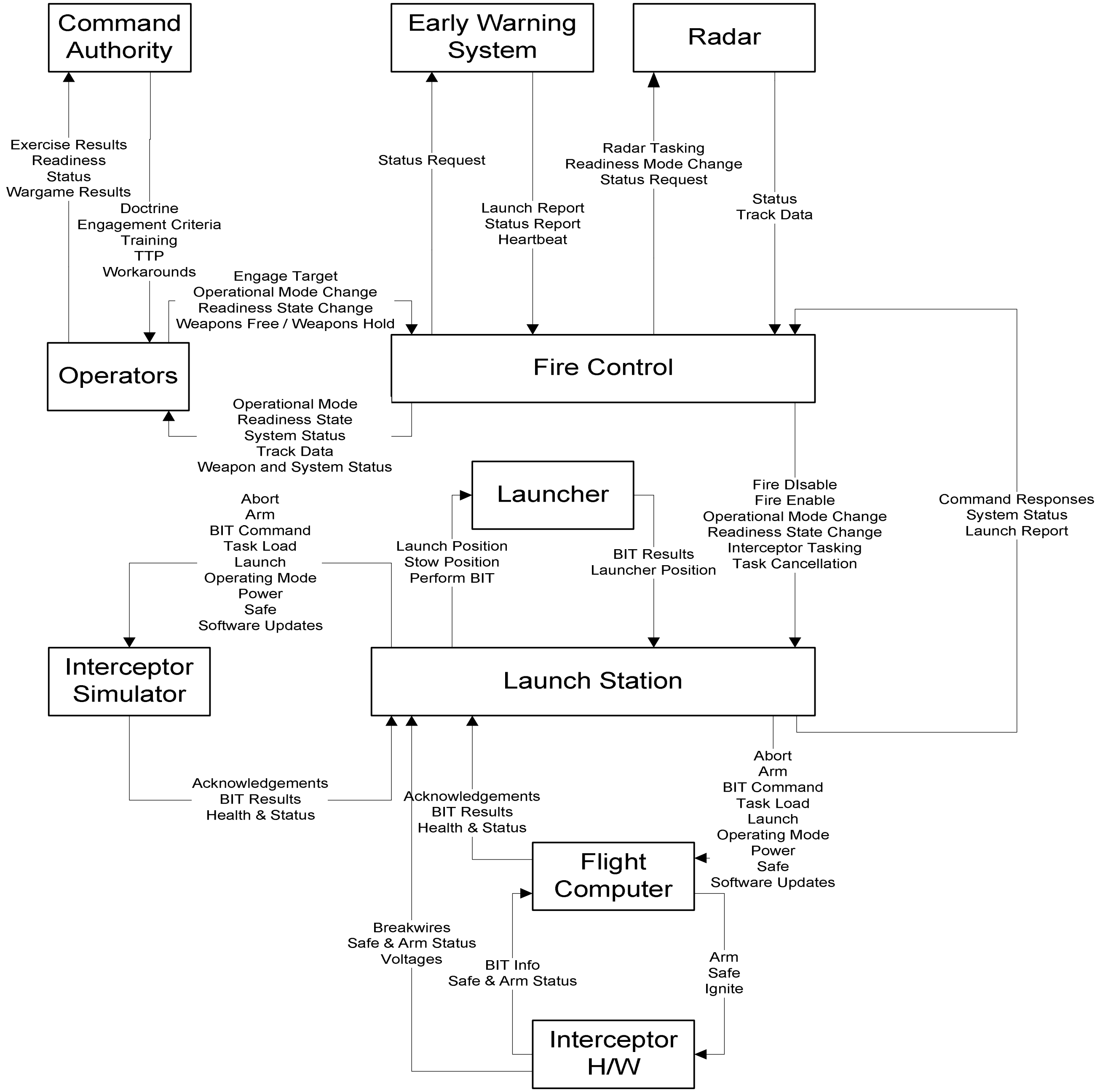
- Out-of-range radio disturbance
- Physical disturbance

Non-advocate Safety Assessment of the Ballistic Missile Defense System using STPA

Ballistic Missile Defense System (BMDS) Non-Advocate Safety Assessment using STPA

- A layered defense to defeat all ranges of threats in all phases of flight (boost, mid-course, and terminal)
- Uses a hit-to-kill interceptor that destroys incoming ballistic missiles through force of impact
- Made up of many existing systems (BMDS Element)
  - Early warning radars
  - Aegis
  - Ground-Based Midcourse Defense (GMD)
  - Command and Control Battle Management and Communications (C2BMC)
  - Others
- MDA used STPA to evaluate the residual safety risk of inadvertent launch prior to deployment and test

Safety Control Structure Diagram for FMIS



Example Causes Identified

1. Providing Fire Enable causes hazard
   - The fire control computer is intended to send the fire enable command to the launch station upon receiving a weapons free command from an FMIS operator and while the fire control system has at least one active track
   - The specification requires an “active” track
   - The software supports declaring tracks inactive after a certain period with no radar input, after the total predicted impact time for the track, and/or after a confirmed intercept
   - One case was not well considered: if an operator de-selects all of these options
   - The inadvertent or intentional entry of a weapons free command would send the fire enable command to the launch station even if there were no threats to engage currently tracked by the system

FMIS Inadequate Controls (cont'd)

2. Providing Fire Enable causes hazard
   - System undergoes periodic system operability testing using an interceptor simulator that mimics the interceptor flight computer
   - Hazard analysis of the system identified the possibility that commands intended for test activities could be sent to the operational system
   - System status information provided by the LS includes whether the LS is connected only to missile simulators or to any live interceptors
   - If the fire control computer detects a change in this state, it will warn the operator and offer to reset into a matching state
   - There is a small window of time before the LS notifies the fire control component of the change during which the fire control software might send a fire enable command intended for test to the live LS

Results of Real BMDS Analysis

- Deployment and testing held up for 6 months because so many scenarios identified for inadvertent launch. In many of these scenarios:
  - All components were operating exactly as intended
  - Complexity of component interactions led to unanticipated system behavior

- STPA also identified component failures that could cause inadequate control (most analysis techniques consider only these failure events)

- As changes are made to the system, the differences are assessed by updating the control structure diagrams and assessment analysis templates.

Evaluation

- STPA worked on this enormously complex system. Why?
  - Top-down analysis
  - Considers hazards and causes due to complex system interactions (more than just failure events)
  - Provides guidance in conducting the analysis
  - Comprehensively addresses the whole of the system, including hardware, software, operators, procedure, maintenance, and continuing development activities
  - Focuses resources on the areas of the system with the greatest impact on safety risk
  - Provides a clear description of problem to decision makers (not just a probability number)

Assurance of Flight Critical Systems (NASA Aviation Safety Program)

- Goal: Development of safe, rapid, and cost effective NextGen systems using a unified safety assurance process for ground based and airborne systems.
  - Demonstrate a new safety assurance approach on a NextGen component
  - Evaluate and compare it with the current approach
  - Create enhanced safety risk management techniques

Problem Statement (2)

- Attempts to re-engineer the NAS in the past have been not been terribly successful and have been very slow, partly due to inability to assure safety of the changes.

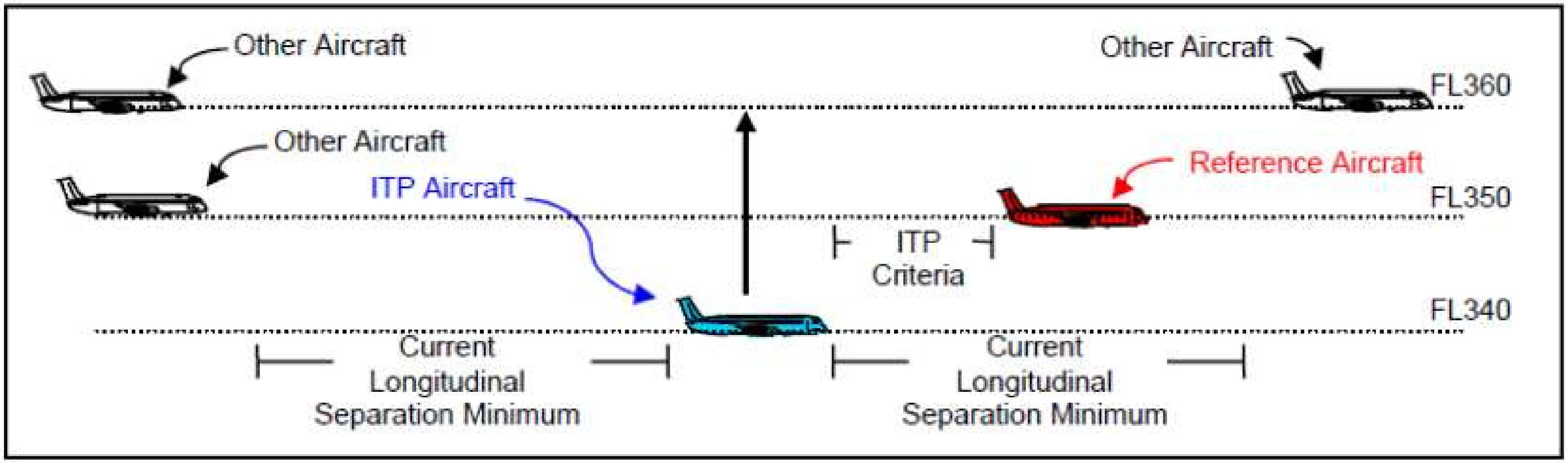
- Question: How can NAS be re-engineered incrementally without negatively impacting safety?

- Hypothesis:
  - Rethinking of how to do safety assurance required to successfully introduce NextGen concepts
  - Applying systems thinking and systems theory can improve our ability to assure safety in these complex systems

Assurance of Flight-Critical Systems (NASA Aviation Safety Program)

- Current ATC systems remarkably safe due to
  - Conservative adoption of new technologies
  - Careful introduction of automation to augment human capabilities
  - Reliance on experience and learning from the past
  - Extensive decoupling of system components
- NextGen violates these assumptions:
  - Increased coupling and inter-connectivity among airborne, ground, and satellite systems
  - Control shifting from ground to aircraft and shared responsibilities
  - Use of new technologies with little prior experience in this environment
- Need to be careful that in trying to fix old problems do not introduce new hazards or new causes of current hazards

In-Trail Procedure (ITP)



- Enables aircraft to achieve FL changes on a more frequent basis.
- Designed for oceanic and remote airspaces not covered by radar.
- Permits climb and descent using new reduced longitudinal separation standards.
- Potential Benefits
  - Reduced fuel burn and CO2 emissions via more opportunities to reach the optimum FL or FL with more favorable winds.
  - Increased safety via more opportunities to leave turbulent FL.
- But standard separation requirements not met during maneuver

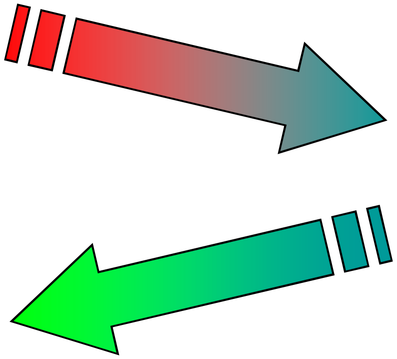
ITP Procedure – Step by Step

Flight Crew

1. Check that ITP criteria are met.
2. If ITP is possible, request ATC clearance via CPDLC using ITP phraseology.

Air Traffic Controller

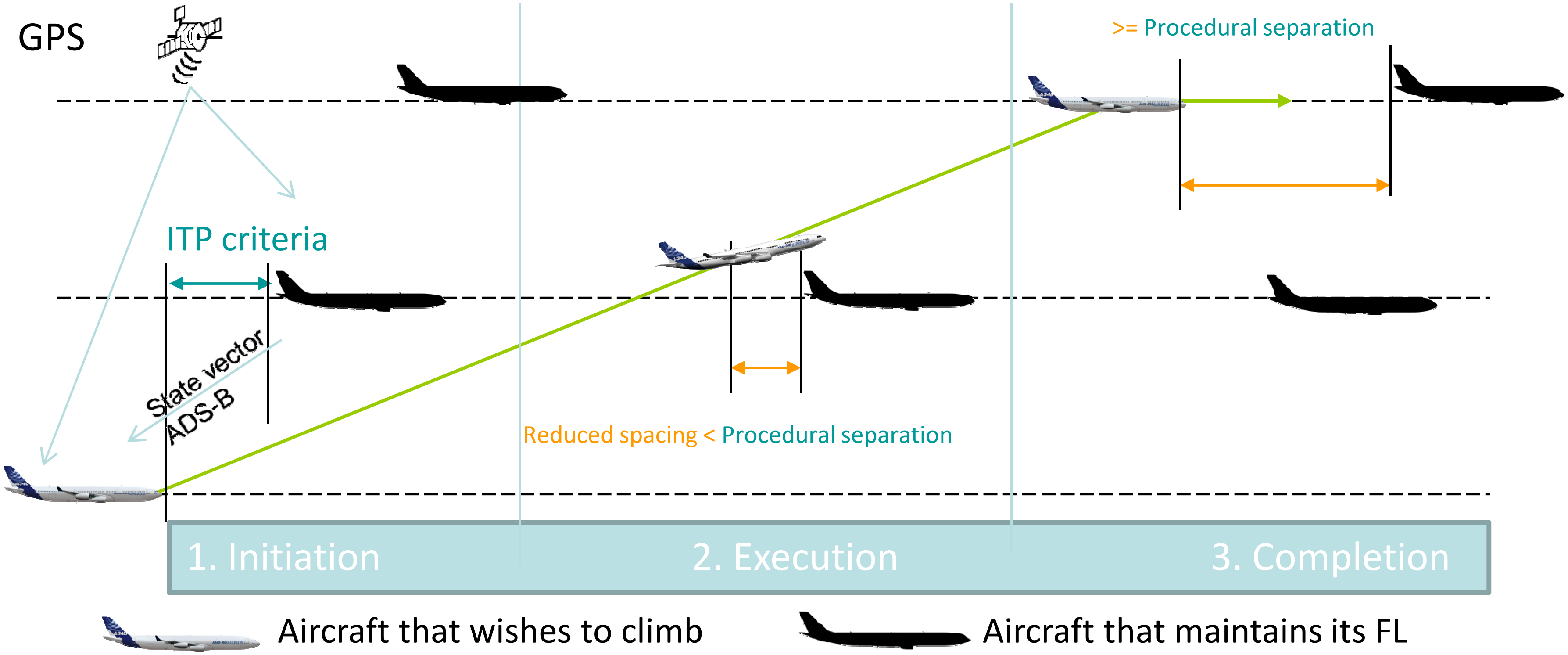
3. Check that there are no blocking aircraft other than Reference Aircraft in the ITP request.
4. Check that ITP request is applicable (i.e. standard request not sufficient) and compliant with ITP phraseology.
5. Check that ITP criteria are met.
6. If all checks are positive, issue ITP clearance via CPDLC.



8. When ITP clearance is received, check that ITP criteria are still met.
9. If ITP criteria are still met, accept ITP clearance via CPDLC.
10. Execute ITP clearance without delay.
11. Report when established at the cleared FL.

Involves multiple aircraft, crew, communications (ADS-B, GPS) , ATC

ATSA ITP Concept – ITP Separation Standards


GPS
>= Procedural separation
ITP criteria
State vector
ADS-B
Reduced spacing < Procedural separation
1. Initiation
2. Execution
3. Completion
Aircraft that wishes to climb
Aircraft that maintains its FL

- Before the ITP maneuver, ITP criteria must be met (i.e. stage 1)
- During an ITP maneuver, the ITP longitudinal separation between aircraft is applied (i.e. stage 2).
- At final FL, procedural separation must exist with aircraft that are already at that final FL (i.e. stage 3).

NextGen Hazards

H-1: A pair of controlled aircraft violates minimum separation standards.

H-2: Aircraft enters an unsafe atmospheric region.

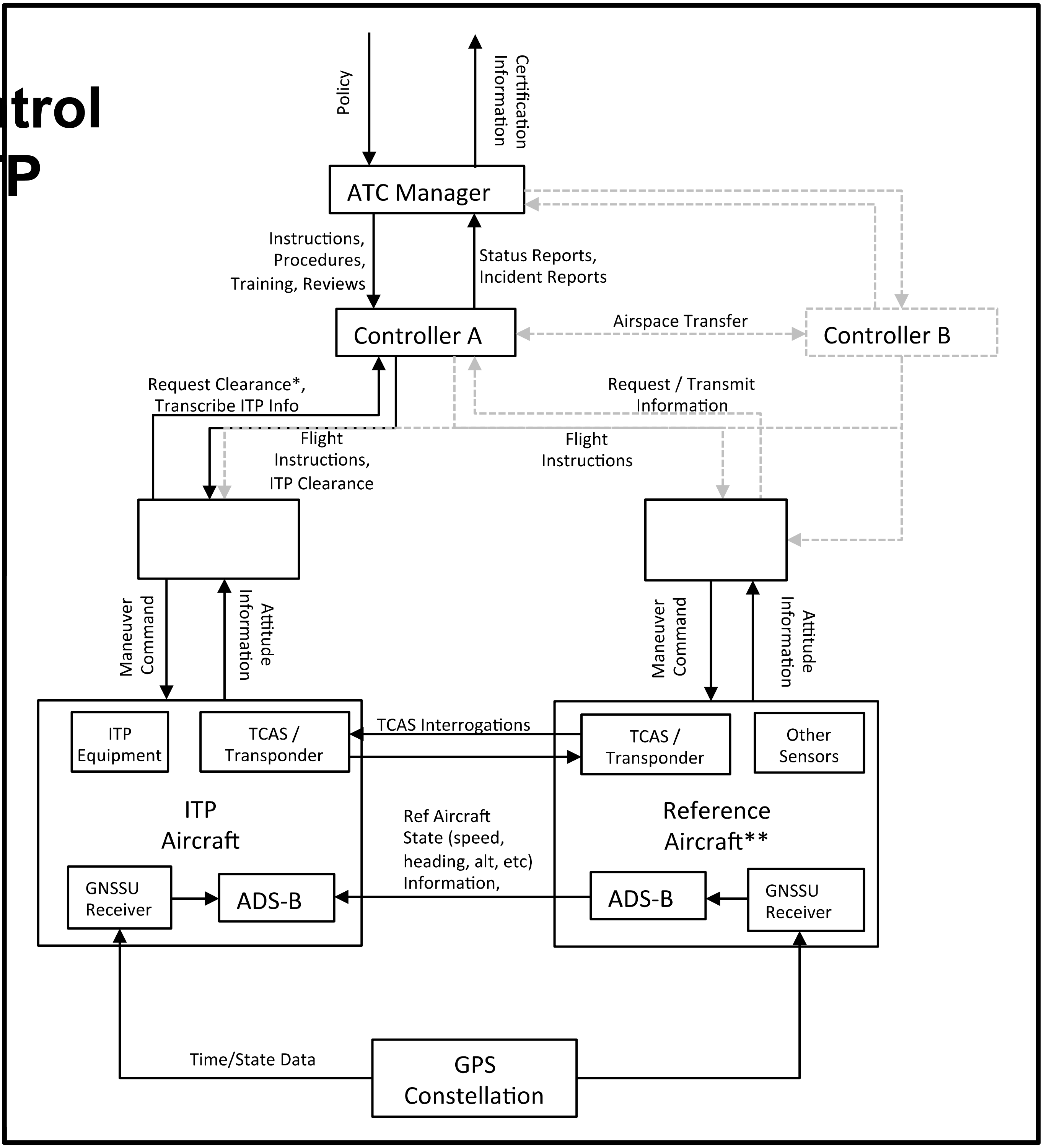
H-3: Aircraft enters uncontrolled state.

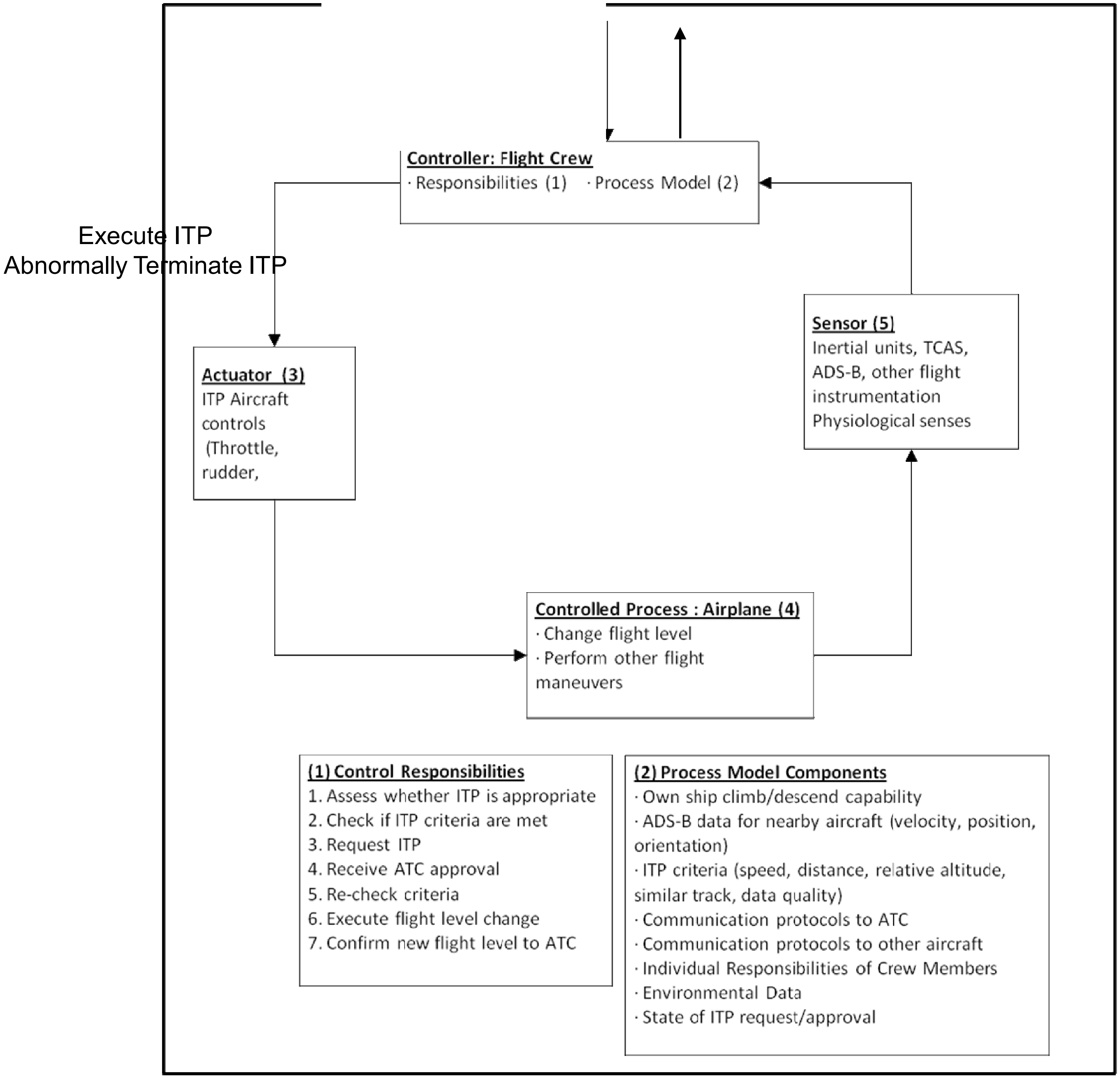
H-4: Aircraft enters unsafe attitude (excessive turbulence or pitch/roll/yaw that causes passenger injury but not necessarily aircraft loss).

H-5: Aircraft enters a prohibited area.

Because ATSA-ITP will be used first in oceanic airspace, only H-1 was considered in the STPA analysis. But later, if it is used elsewhere, the other hazards will need to be considered.

High-Level Control Structure for ITP





Execute ITP
Abnormally Terminate ITP

Controller: Flight Crew
· Responsibilities (1) · Process Model (2)

Actuator (3)
ITP Aircraft controls (Throttle, rudder,

Sensor (5)
Inertial units, TCAS, ADS-B, other flight instrumentation
Physiological senses

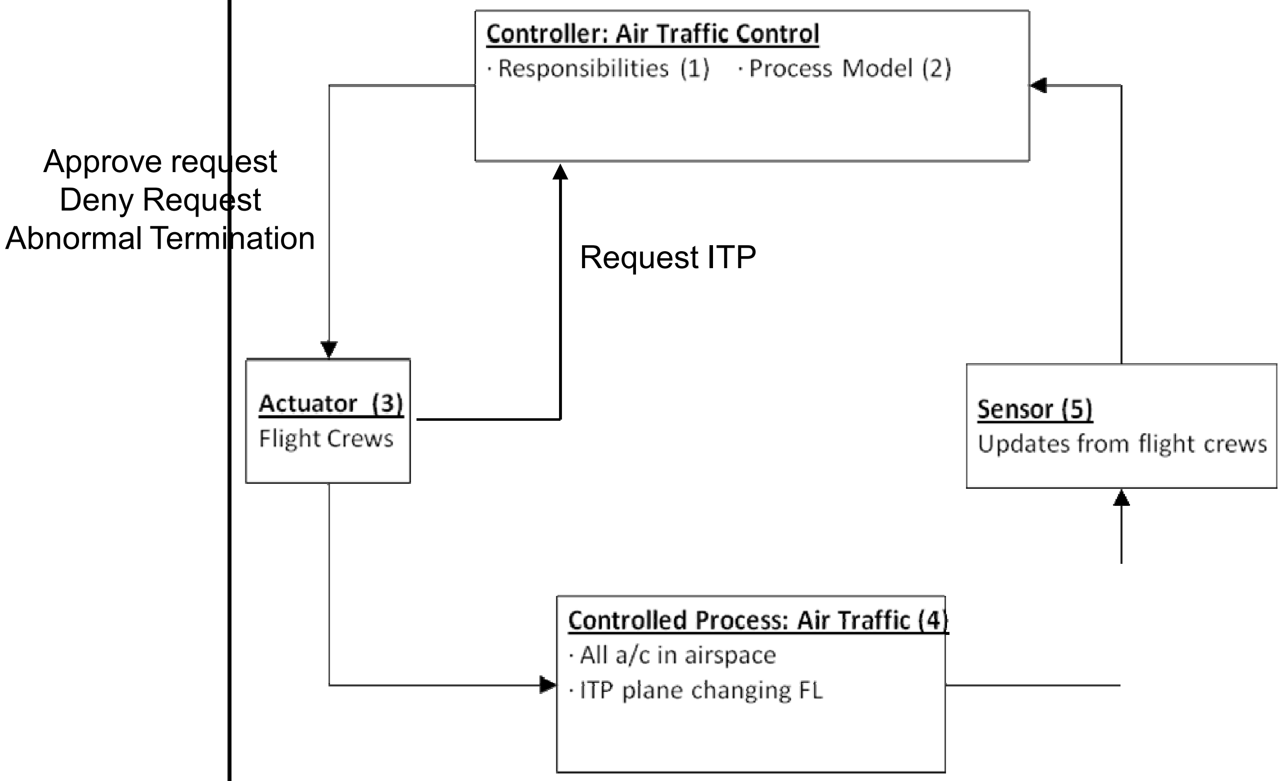
Controlled Process : Airplane (4)
· Change flight level
· Perform other flight maneuvers

(1) Control Responsibilities

1. Assess whether ITP is appropriate
2. Check if ITP criteria are met
3. Request ITP
4. Receive ATC approval
5. Re-check criteria
6. Execute flight level change
7. Confirm new flight level to ATC

(2) Process Model Components

- Own ship climb/descend capability
- ADS-B data for nearby aircraft (velocity, position, orientation)
- ITP criteria (speed, distance, relative altitude, similar track, data quality)
- Communication protocols to ATC
- Communication protocols to other aircraft
- Individual Responsibilities of Crew Members
- Environmental Data
- State of ITP request/approval



Controller: Air Traffic Control

· Responsibilities (1) · Process Model (2)

Approve request
Deny Request
Abnormal Termination

Request ITP

Actuator (3)
Flight Crews

Sensor (5)
Updates from flight crews

Controlled Process: Air Traffic (4)
· All a/c in airspace
· ITP plane changing FL

(1) Control Responsibilities

1. Receive request from FC
2. Analyze ITP data and traffic
3. Communicate approval/ denial

(2) ATC Process Model Components

· Flight Plans of all aircraft in sector
· ITP proximate altitude, position, orientation, track
· Proximate velocity/altitude/position of all aircraft
· Number of craft on each track in sector
· All ITP/RA acting as part of ITP maneuver
· Expected traffic volume
· Communication protocols
· Weather Cells

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		

(Not complete, does not include FC requesting ITP when not safe, considered later)

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

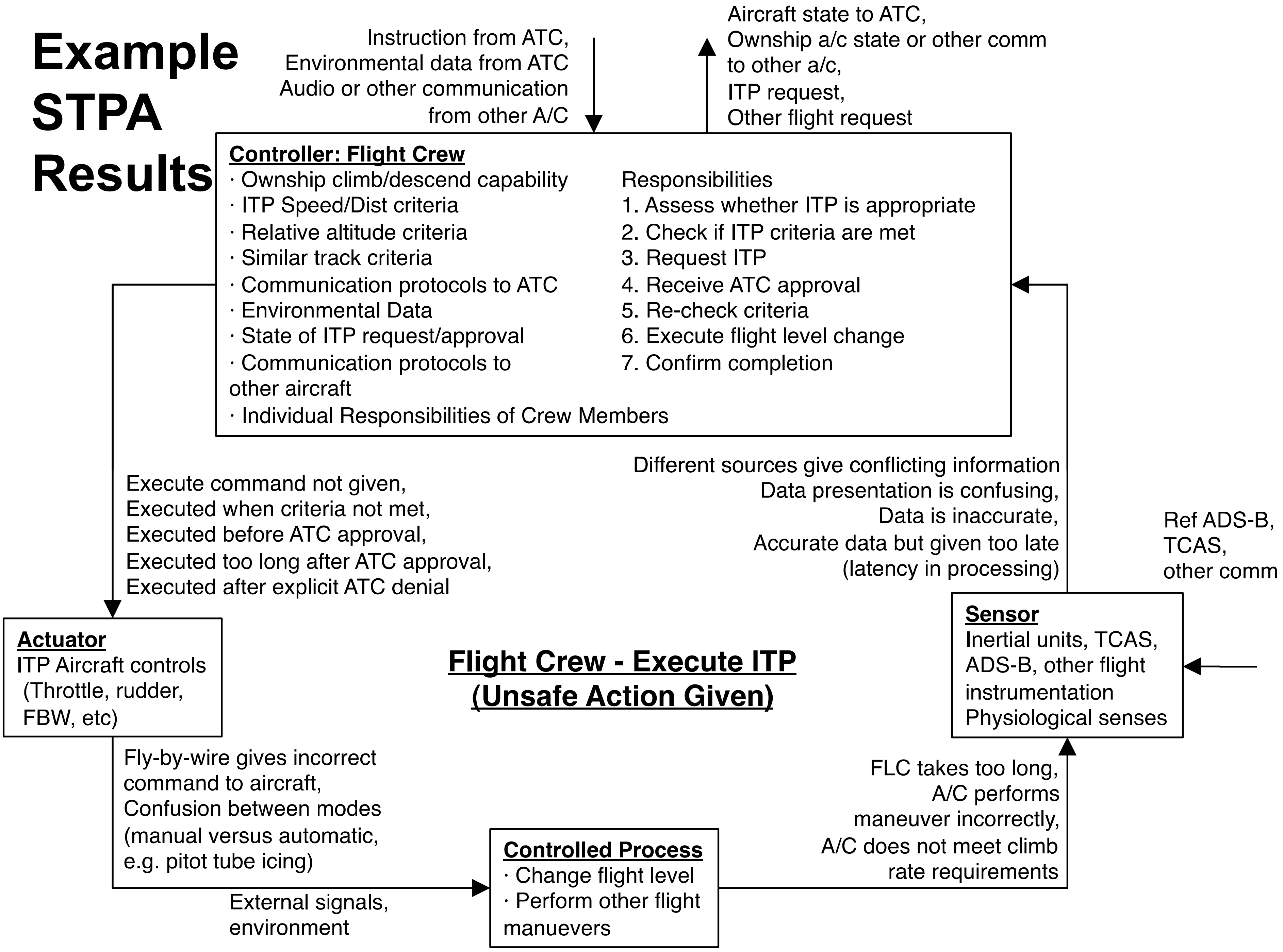
Potentially Hazardous Control Actions for ATC

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon or Applied Too Long
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.

Example STPA Results



Instruction from ATC,
Environmental data from ATC
Audio or other communication
from other A/C

Aircraft state to ATC,
Ownship a/c state or other comm
to other a/c,
ITP request,
Other flight request

Controller: Flight Crew

- Ownship climb/descend capability
- ITP Speed/Dist criteria
- Relative altitude criteria
- Similar track criteria
- Communication protocols to ATC
- Environmental Data
- State of ITP request/approval
- Communication protocols to other aircraft
- Individual Responsibilities of Crew Members

Responsibilities
1. Assess whether ITP is appropriate
2. Check if ITP criteria are met
3. Request ITP
4. Receive ATC approval
5. Re-check criteria
6. Execute flight level change
7. Confirm completion

Execute command not given,
Executed when criteria not met,
Executed before ATC approval,
Executed too long after ATC approval,
Executed after explicit ATC denial

Different sources give conflicting information
Data presentation is confusing,
Data is inaccurate,
Accurate data but given too late
(latency in processing)

Ref ADS-B,
TCAS,
other comm

Actuator
ITP Aircraft controls
(Throttle, rudder,
FBW, etc)

Flight Crew - Execute ITP
(Unsafe Action Given)

Sensor
Inertial units, TCAS,
ADS-B, other flight
instrumentation
Physiological senses

Fly-by-wire gives incorrect
command to aircraft,
Confusion between modes
(manual versus automatic,
e.g. pitot tube icing)

FLC takes too long,
A/C performs
maneuver incorrectly,
A/C does not meet climb
rate requirements

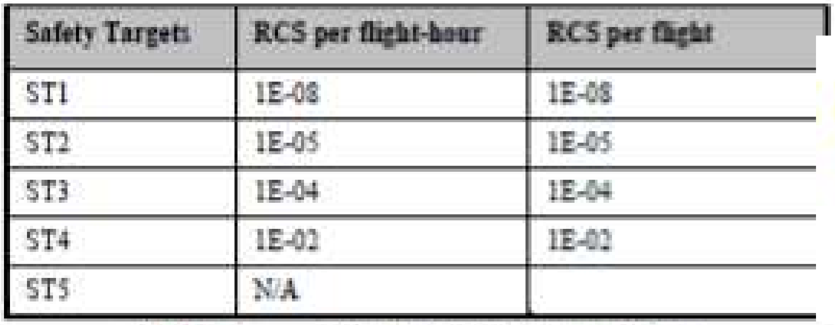
Controlled Process
- Change flight level
- Perform other flight manuevers

External signals,
environment

Limitations of Current Safety Assurance Approach

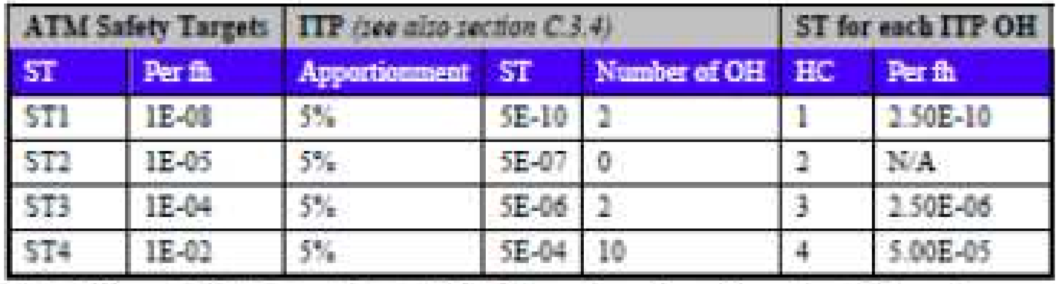
- Barriers and Effects
  - Identify Operational Effects (OEs) that could result from occurrence of an OH
  - Identify barriers that could prevent the OH from leading to a severe OE.
  - Barriers modeled and probability that an OE occurs given that the corresponding OH has occurred is estimated.

e events (based on severity)



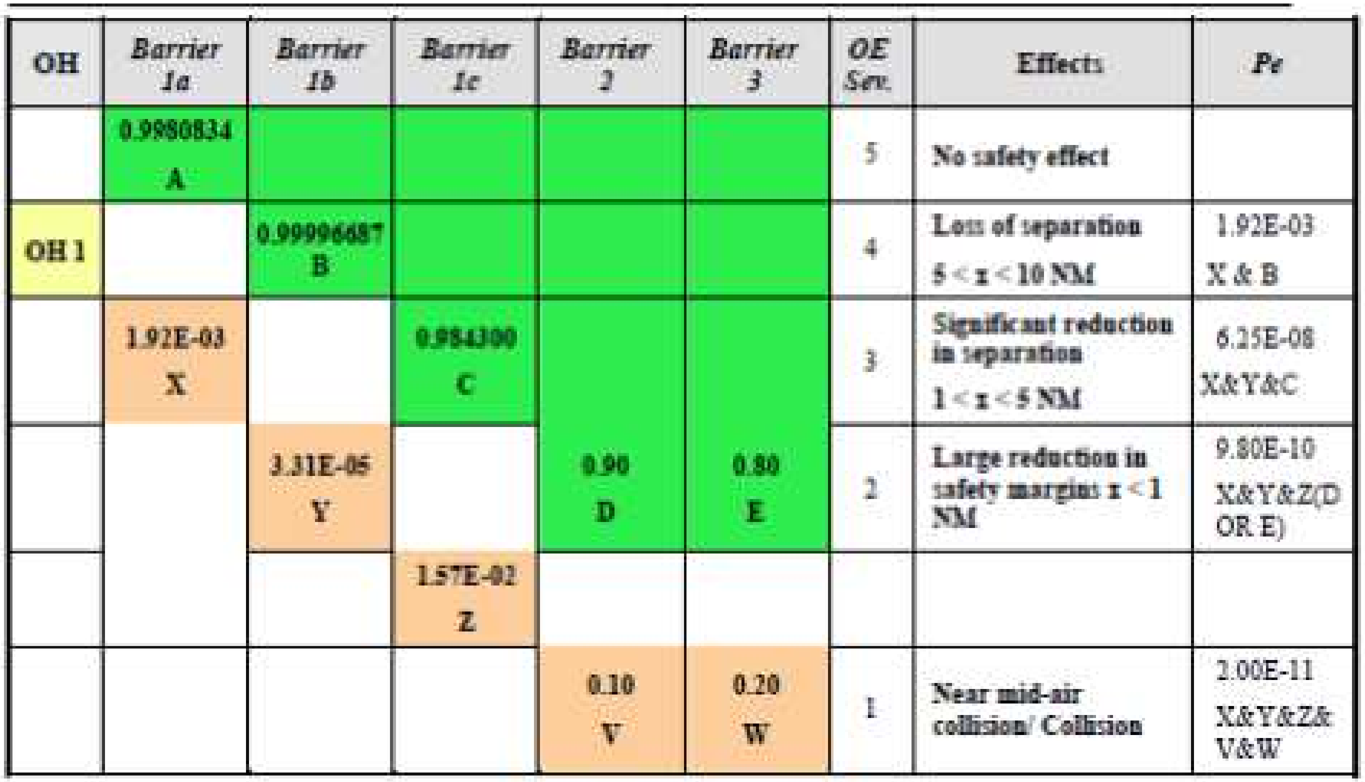
Safety Targets	RCS per flight-hour	RCS per flight
ST1	1E-08	1E-08
ST2	1E-05	1E-05
ST3	1E-04	1E-04
ST4	1E-02	1E-02
ST5	N/A	

Table C.3 OSA - Risk Classification Scheme



ATM Safety Targets		ITP *(see also section C.3.4)*			ST for each ITP OH	
ST	Per fh	Apportionment	ST	Number of OH	HC	Per fh
ST1	1E-08	5%	5E-10	2	1	2.50E-10
ST2	1E-05	5%	5E-07	0	2	N/A
ST3	1E-04	5%	5E-06	2	3	2.50E-06
ST4	1E-02	5%	5E-04	10	4	5.00E-05

Table C.9 Safety Targets for all ATM Hazards and per Operational Hazard



OH	*Barrier 1a*	*Barrier 1b*	*Barrier 1c*	*Barrier 2*	*Barrier 3*	*OE Sev.*	**Effects**	*Pe*
	0.9980834 A	🟩	🟩	🟩	🟩	5	No safety effect	
OH 1		0.99996687 B	🟩	🟩	🟩	4	Loss of separation 5 < x < 10 NM	1.92E-03 X & B
	1.92E-03 X		0.984300 C	🟩	🟩	3	Significant reduction in separation 1 < x < 5 NM	6.25E-08 X&Y&C
		3.31E-06 Y		0.90 D	0.80 E	2	Large reduction in safety margins x < 1 NM	9.80E-10 X&Y&Z(D OR E)
			1.57E-02 Z					
				0.10 V	0.20 W	1	Near mid-air collision/ Collision	2.00E-11 X&Y&Z& V&W

Table C.11 Event Tree for OH1, Interruption of an ITP Maneuver by the flight crew

Legend:

X & Y = XY

A OR B = A + B – AB

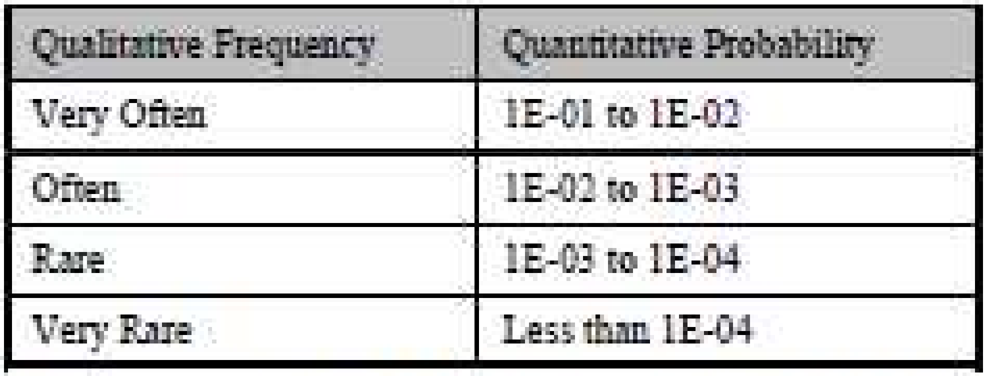
🟩 Green shows the path to the effects when the related barrier succeeds

🟧 Orange shows the path to the effect when the related barrier fails

(It looks like they took a mishmash of techniques from the nuclear power community)

Limitations of Safety Assurance Approach

- Human Error analysis
  - Held workshops with pilots and controllers to assess likelihood of each human error.



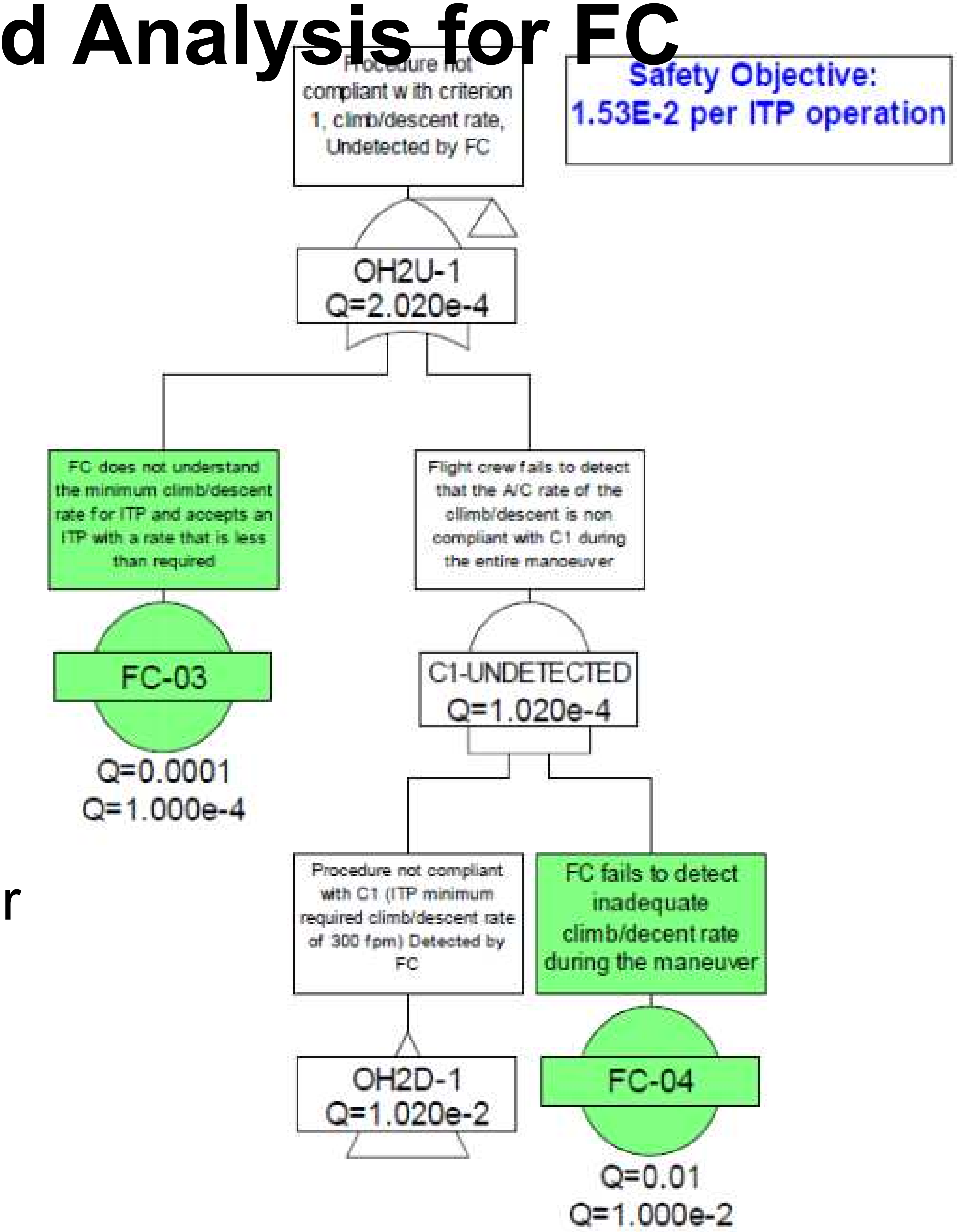
Qualitative Frequency	Quantitative Probability
Very Often	1E-01 to 1E-02
Often	1E-02 to 1E-03
Rare	1E-03 to 1E-04
Very Rare	Less than 1E-04

Table C.4 Qualitative Frequency and Relation to Quantitative Probability for Basic Causes

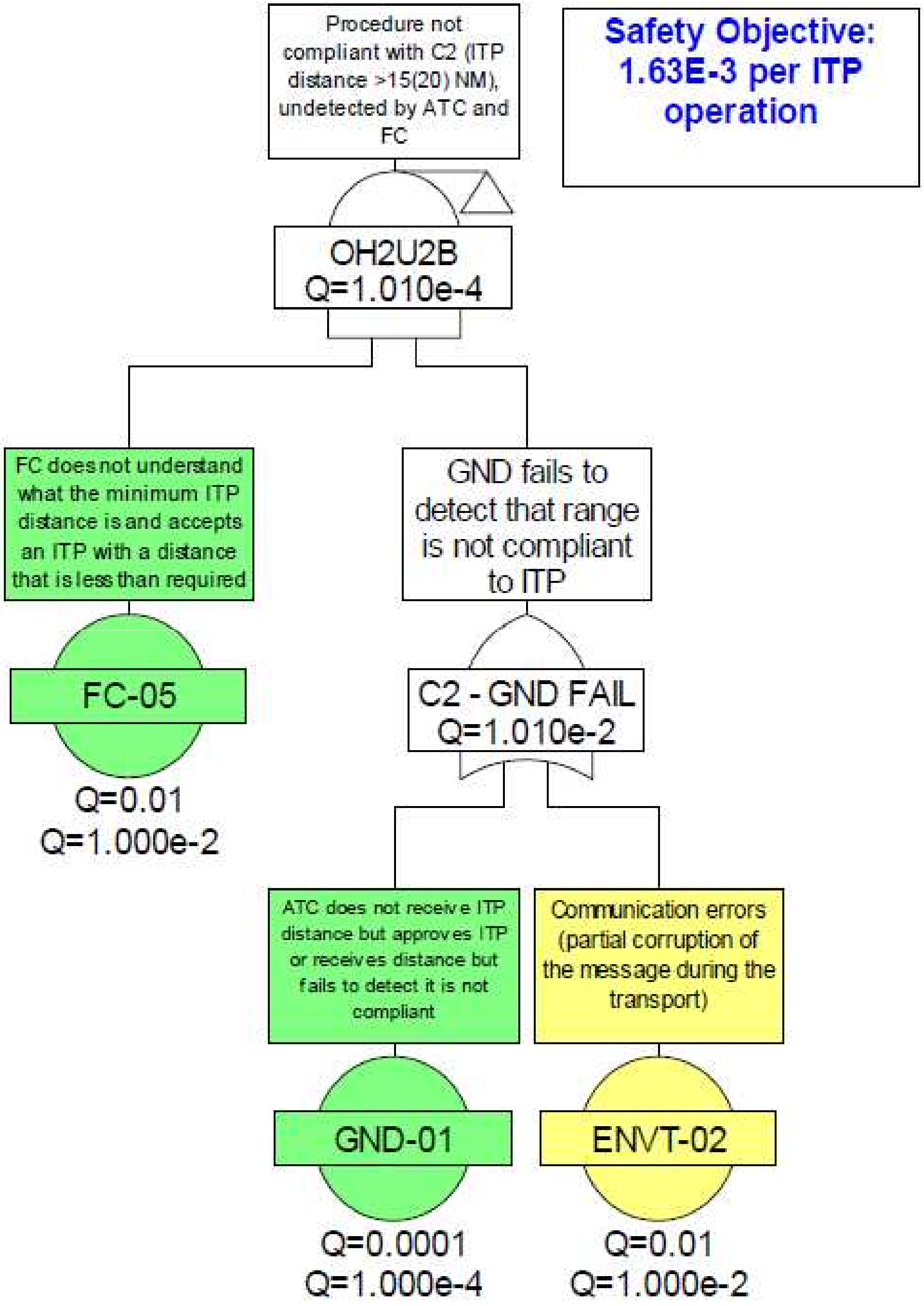
  - Not sure how generated list of human errors but seems incomplete
  - Then created fault trees to determine probabilities

DO-312 Hazard Analysis for FC

- DO-312 begins with Operational Hazards (which are actually basic causes)
  - Then identify chains-of-events (fault trees) that could lead to basic causes
  - Each set of events is assigned a quantitative safety objective
- Human factors
  - Assign probability of error
  - Provides little accounting for why errors may occur


Procedure not compliant w ith criterion 1, climb/descent rate, Undetected by FC
Safety Objective:
1.53E-2 per ITP operation
OH2U-1
Q=2.020e-4
FC does not understand the minimum climb/descent rate for ITP and accepts an ITP with a rate that is less than required
FC-03
Q=0.0001
Q=1.000e-4
Flight crew fails to detect that the A/C rate of the cllimb/descent is non compliant with C1 during the entire manoeuver
C1-UNDETECTED
Q=1.020e-4
Procedure not compliant with C1 (ITP minimum required climb/descent rate of 300 fpm) Detected by FC
OH2D-1
Q=1.020e-2
FC fails to detect inadequate climb/decent rate during the maneuver
FC-04
Q=0.01
Q=1.000e-2

- Assumes that ATC & FC failing to detect distance non-compliance are independent
- Assumes that communication errors are due only to corruption of HF data


Procedure not compliant with C2 (ITP distance >15(20) NM), undetected by ATC and FC
Safety Objective: 1.63E-3 per ITP operation
OH2U2B
Q=1.010e-4
FC does not understand what the minimum ITP distance is and accepts an ITP with a distance that is less than required
FC-05
Q=0.01
Q=1.000e-2
GND fails to detect that range is not compliant to ITP
C2 - GND FAIL
Q=1.010e-2
ATC does not receive ITP distance but approves ITP or receives distance but fails to detect it is not compliant
GND-01
Q=0.0001
Q=1.000e-4
Communication errors (partial corruption of the message during the transport)
ENVT-02
Q=0.01
Q=1.000e-2

DO-312

Execution of an ITP Clearance not Compliant with ITP Criteria
Assumption
AS.40 The probability that ATC does not receive ITP Distance (as part of the ITP climb/descent request) but approves ITP procedure or fails to detect that ITP Distance received in the request is not compliant, is assumed to occur no more frequently than Very Rare.
AS.12 The corruption of information because of HF occurs no more than Often.

STPA

Unsafe Control Action: ITP Flight Crew incorrectly executes ITP
Requirement
[1.2.1.1] Once ITP request has been made, all communication between ATC and the FC must occur on the same communication channel
[1.2.1.2] All communication protocols must include definitions of when a communication is complete
[1.10] – [1.17]
[1.18] ATC must have access to current* knowledge of the velocity, heading, and location of all aircraft involved in ITP request *Assumption*: ATC will have this knowledge as part of their overall ability to maintain separation, regardless of ITP clearances.
[1.1.2] ITP shall provide the flight crews of aircraft operating in procedural airspace the ability to determine a clear procedure for communicating data about the desired flight level change and necessary state data to the local air traffic controller

How Can Performance Requirements be Verified?

Example:

> “The likelihood that the ITP equipment provides undetected erroneous information about accuracy and integrity levels of own data shall be less than 1E-3 per flight hour.”

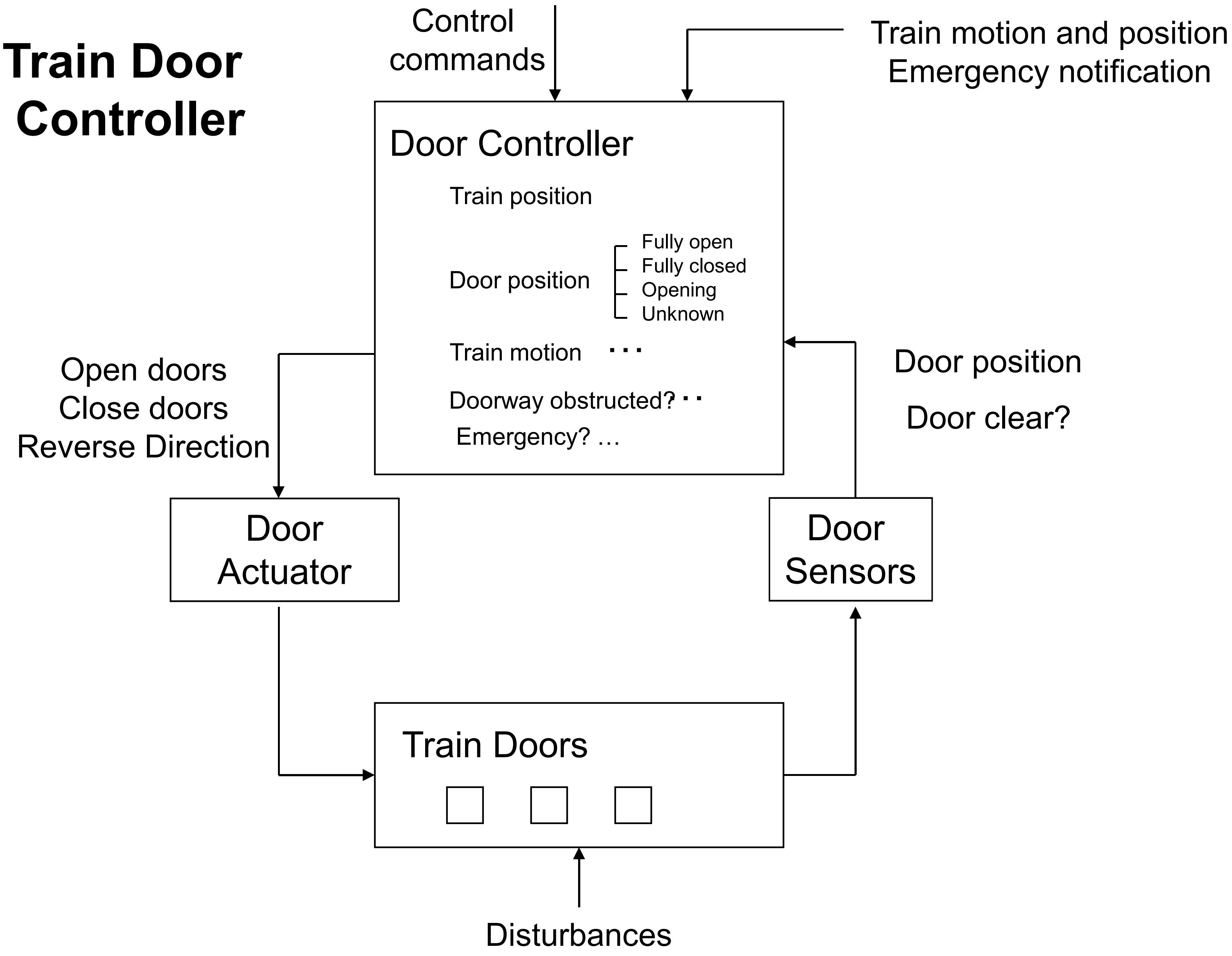
Comparison

- We found many missing requirements
- Example:
  - DO-312 assumes that the reference aircraft will not deviate from its flight plan during ITP execution.
  - There should be a contingency or protocol in the event that the reference aircraft does not maintain its expected speed and trajectory, for example, because of an emergency requiring immediate action (e.g., TCAS alert)

Heuristics to Help with Step 1

- We are creating additional procedures to assist with this step (and others)
- Thomas has defined some guidewords and a procedure to go through this process more rigorously
- Starts with identifying environmental or system state conditions affecting behavior of component
- Then consider for each possible state the result of
  - Providing the control action
  - Not providing it
- Much of this can potentially be automated

Train Door Controller



1) Control actions provided in state that makes them hazardous

Define context conditions (from process model and from hazards)

Train motion: Train is stopped, train is in motion

(Hazard: Doors are opened while train in motion)

Emergency: No emergency, emergency situation requiring evacuation

(Hazard: Doors do not open for emergency evacuation)

Train position: Train is aligned with platform, train is not aligned with platform

(Hazard: doors open when train not aligned with platform)

Control actions provided in state where action is hazardous

Control Action	Condition 1: Train Motion	Condition 2: Emergency	Condition 3: Train Position	Hazardous control action?		
				Provided any time in this context?	**Provided too early in this context?**	**Provided too late in this context?**
Door open command provided	Train is moving	No emergency	(doesn’t matter)	Yes	Yes	Yes
	Train is moving	Emergency exists	(doesn’t matter)	Yes*	Yes*	Yes*
	Train is stopped	Emergency exists	(doesn’t matter)	No	No	Yes
	Train is stopped	No emergency	Not aligned with platform	Yes	Yes	Yes
	Train is stopped	No emergency	Aligned with platform	No	No	No

Control actions provided in state where inaction is hazardous

Control Action	Train Motion	Emergency	Train Position	Door State	Hazardous if not provided in this context?
Door open command not provided	Train is stopped	No emergency	Aligned with platform	Person not in doorway	No[1]
	Train is stopped	No emergency	Aligned with platform	Person in doorway	Yes
	Train is stopped	No emergency	Not aligned with platform	(doesn’t matter)	No
	Train is stopped	Emergency exists	(doesn’t matter)	(doesn’t matter)	Yes
	Train is moving	(doesn’t matter)	(doesn’t matter)	(doesn’t matter)	No

[1] This is not hazardous because it does not lead to any of the identified hazards but clearly not desirable

Safety-Guided Design

- Safety analysis and design should be integrated into system engineering process
  - Most important decisions related to design made in early concept development stage.
  - Once made, very difficult or impossible to change
  - So kludges made to try to fix the problems (usually expensive and not very effective)
  - Cheapest and most effective if design safety in from the beginning
  - Can save money and time doing this (less rework)

Steps in Safety-Guided Design

1. Identify system hazards
2. Translate hazards into system-level safety constraints and requirements.
3. Try to eliminate hazards from system conceptual level.
4. If cannot eliminate, then identify potential for control at system.
5. Create system control structure and assign responsibilities for enforcing safety constraints.

Steps in Safety-Guided Design (2)

6. Refine system safety constraints and design in parallel.
    a. STPA step 1: identify potentially hazardous control actions. Restate as component safety design constraints and requirements.
    b. STPA step 2: determine factors that could lead to violation of safety constraints
    c. Augment basic design to eliminate, mitigate, or control potentially unsafe control actions and behaviors.
    d. Iterate over the process, i.e. perform STPA on the new augmented design and continue to refine the design until all hazardous scenarios are eliminated, mitigated, or controlled.
7. Document design rationale and trace requirements and constraints to the related design decisions

Thermal Tile Robot Example

1. **Identify high-level functional requirements and environmental constraints.**

   e.g. size of physical space, crowded area

2. **Identify high-level hazards**

   a. Violation of minimum separation between mobile base and objects (including orbiter and humans)

   b. Mobile robot becomes unstable (e.g., could fall over)

   c. Manipulator arm hits something

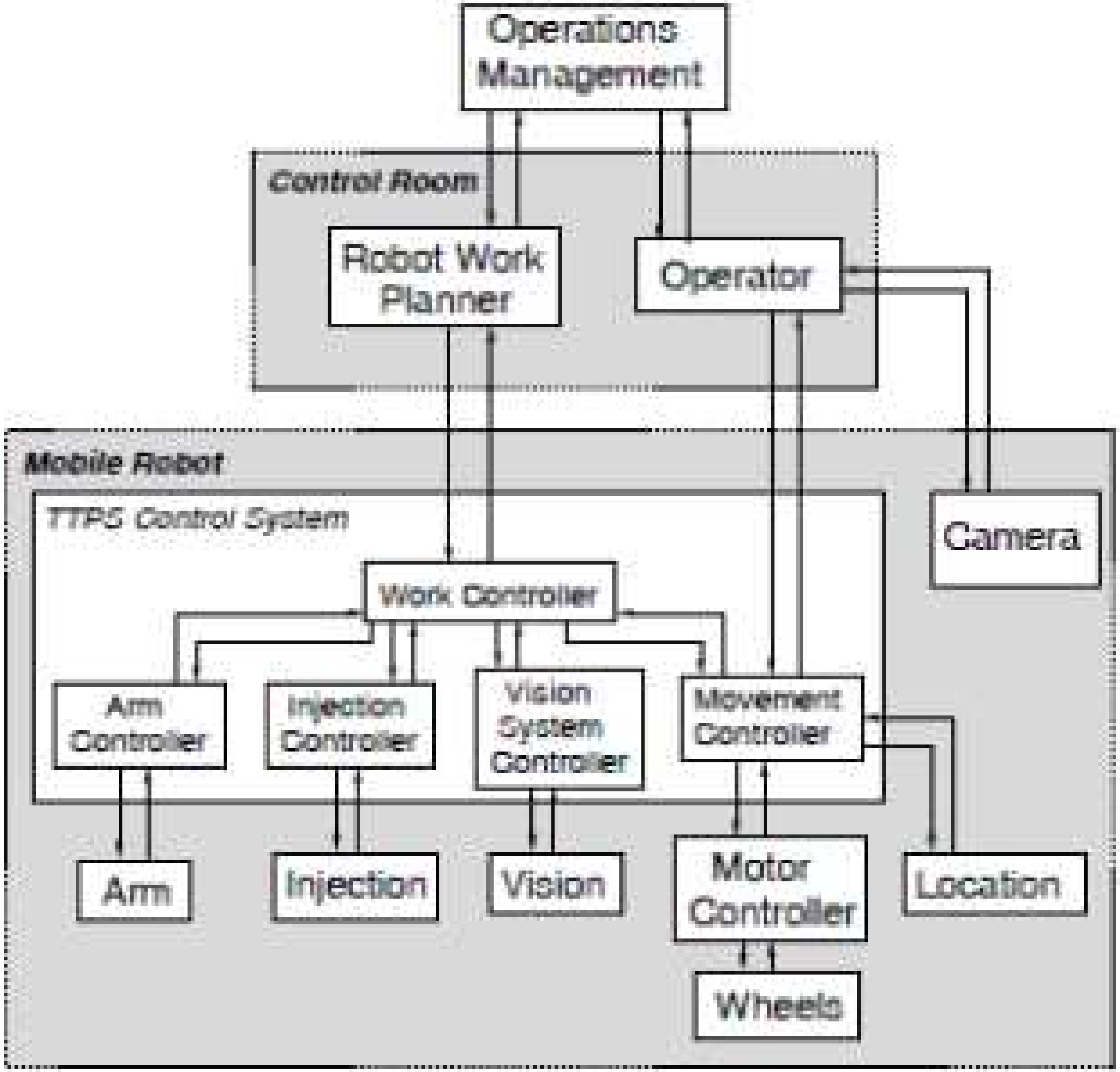
   d. Fire or explosion

   e. Contact of human with DMES

   f. Inadequate thermal control (e.g., damaged tiles not detected, DMES not applied correctly)

   g. Damage to robot

Define preliminary control structure and refine constraints and design in parallel.



3. **Try to eliminate hazards from system conceptual design. If not possible, then identify controls and new design constraints.**

For unstable base hazard

System Safety Constraint:

Mobile base must not be capable of falling over under worst case operational conditions

First try to eliminate:

1. Make base heavy

   Could increase damage if hits someone or something.

   Difficult to move out of way manually in emergency

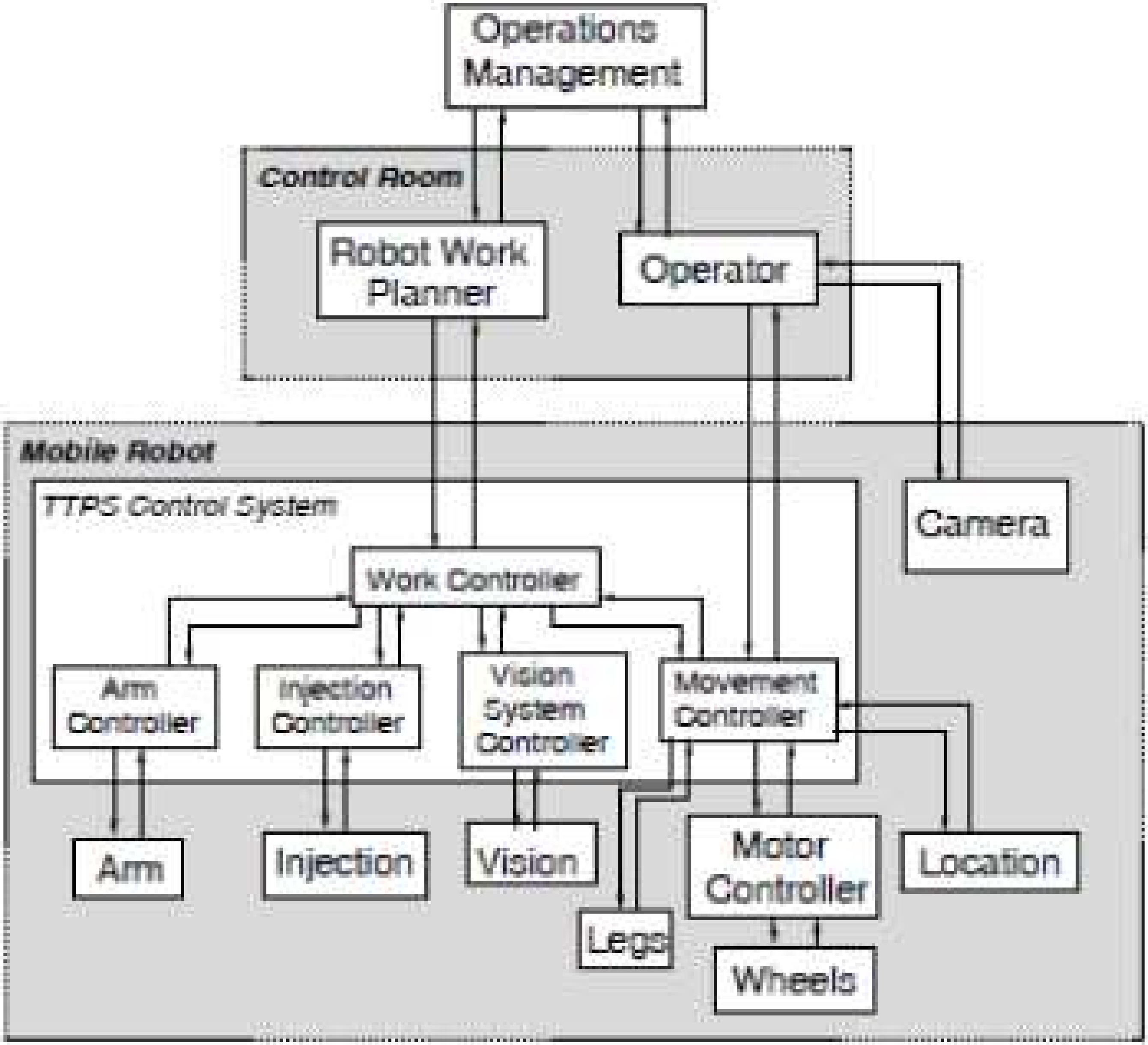
2. Make base long and wide

   Eliminates hazard but violates environmental constraints

3. Use lateral stability legs that are deployed when manipulator arm extended but must be retracted when mobile base moves.

Results in two new design constraints:

- Manipulator arm must move only when stabilizer legs are fully deployed
- Stabilizer legs must not be retracted until manipulator arm is fully stowed.


Operations Management
Control Room
Robot Work Planner
Operator
Mobile Robot
TTPS Control System
Camera
Work Controller
Arm Controller
Injection Controller
Vision System Controller
Movement Controller
Arm
Injection
Vision
Legs
Motor Controller
Location
Wheels

Identify potentially hazardous control actions by each of system components

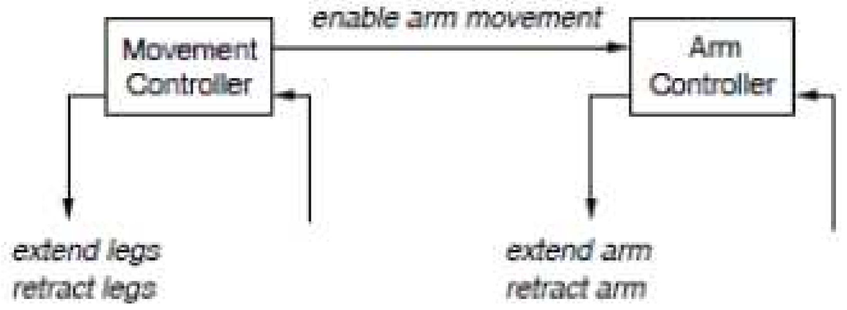
1. A required control action is not provided or not followed
2. An incorrect or unsafe control action is provided
3. A potentially correct or inadequate control action is provided too late or too early (at the wrong time)
4. A correct control action is stopped too soon.

Hazardous control of stabilizer legs:

- Legs not deployed before arm movement enabled
- Legs retracted when manipulator arm extended
- Legs retracted after arm movements are enabled or retracted before manipulator arm fully stowed
- Leg extension stopped before they are fully extended

HAZARD1: Arm extended while legs retracted

HAZARD2: Legs extended during movement



Command	Missing	Incorrect	Timing/Sequencing	Stopped Too Soon
extend legs	Legs not extended before arm extended **H1**	Extend legs during movement **H2**	Extend arm before legs extended **H1**	Stop before fully extended **H1**
retract legs	Not retracted before movement **H2**	Retract while arm extended **H1**	Retract legs before arm fully stowed **H1**	Stop while still partially extended **H1**

Command	Missing	Incorrect	Timing/Sequencing	Stopped Too Soon
extend arm	Do not extend arm when commanded	Extend arm when legs retracted **H1**	Extend arm before legs fully extended **H1**	(tile processing hazard)
retract arm	Not retracted before movement **H2**	(tile processing hazard)	(tile processing hazard)	Stop retraction before fully arm fully stowed and movement starts or legs retracted **H1 H2**

Restate as safety design constraints on components

1. Controller must ensure stabilizer legs are extended whenever arm movement is enabled

2. Controller must not command a retraction of stabilizer legs when manipulator arm extended

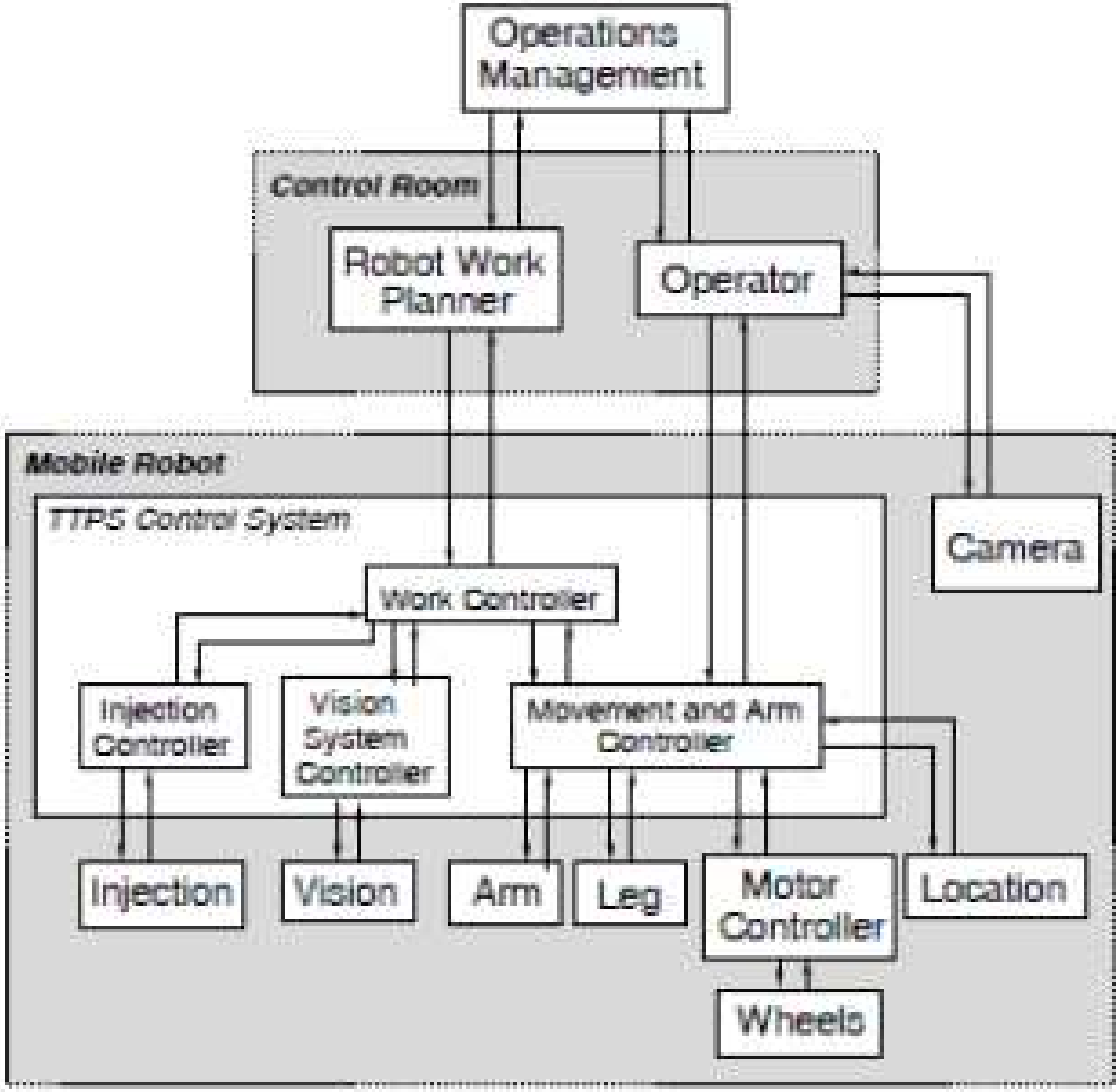
3. Controller must not command deployment of stabilizer legs before arm movements are enabled. Controller must not command retraction of legs before manipulator arm fully stowed

4. Controller must not stop leg deployment before they are fully extended

Do same for all hazardous commands:

e.g., Arm controller must not enable manipulator arm movement before stabilizer legs are completely extended.

At this point, may decide to have arm controller and leg controller in same component


Operations Management
Control Room
Robot Work Planner
Operator
Mobile Robot
TTPS Control System
Camera
Work Controller
Injection Controller
Vision System Controller
Movement and Arm Controller
Injection
Vision
Arm
Leg
Motor Controller
Location
Wheels

To produce detailed scenarios for violation of safety constraints, augment control structure with process models

Arm Movement
Enabled
Disabled
Unknown

Stabilizer Legs
Extended
Retracted
Unknown

Manipulator Arm
Stowed
Extended
Unknown

How could become inconsistent with real state?

- e.g. issue command to extend stabilizer legs but external object could block extension or extension motor could fail

Problems often in startup or shutdown:

e.g., Emergency shutdown while servicing tiles. Stability legs manually retracted to move robot out of way. When restart, assume stabilizer legs still extended and arm movement could be commanded. So use “unknown” state when starting up

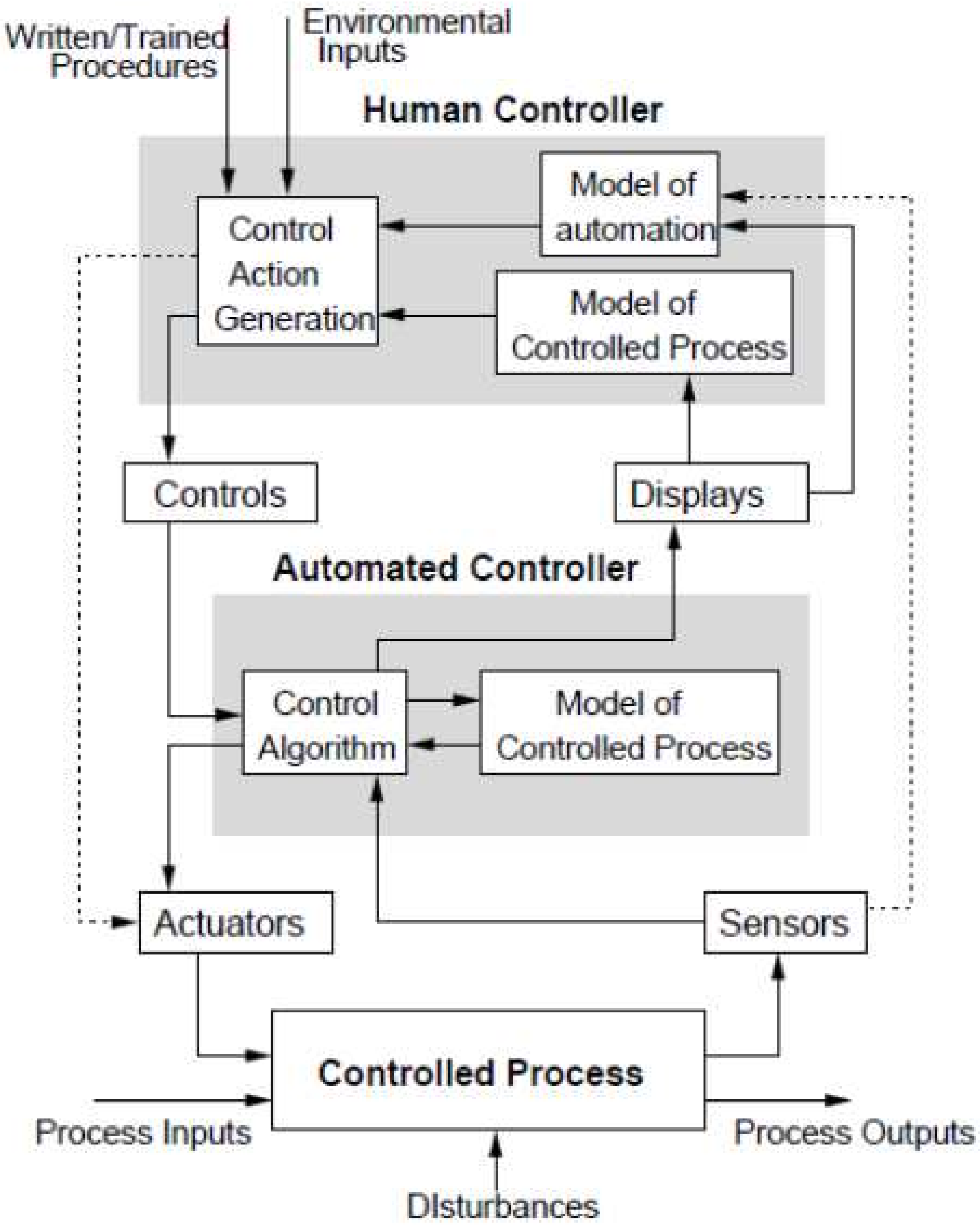
Do not need to know all causes, only safety constraints:

- May decide to turn off arm motors when legs extended or when arm extended. Could use interlock or tell computer to power it off.
- Must not move when legs extended? Power down wheel motors while legs extended.

Check for coordination problems

General Design for Safety Principles

- In addition to identified application-specific design constraints
- Result from:
  - General STAMP principles of accident causation
  - General engineering design principles
  - Causes of past accidents
  - (requirements completeness criteria in *Safeware*)
- Divided into
  - General principles for any controller
  - Special system design principles to reduce human errors
- Details in Chapter 9 of *Engineering a Safer World*


Written/Trained Procedures
Environmental Inputs
Human Controller
Model of automation
Control Action Generation
Model of Controlled Process
Controls
Displays
Automated Controller
Control Algorithm
Model of Controlled Process
Actuators
Sensors
Controlled Process
Process Inputs
Process Outputs
DIsturbances

CAST: Accident/Incident Causal Analysis

Goals for an Accident Analysis Technique

- Minimize hindsight bias
- Provide a framework or process to assist in understanding entire accident process and identifying systemic factors
- Get away from blame (“who”) and shift focus to “why” and how to prevent in the future
- Goal is to determine
  - Why people behaved the way they did
  - Weaknesses in the safety control structure that allowed the loss to occur

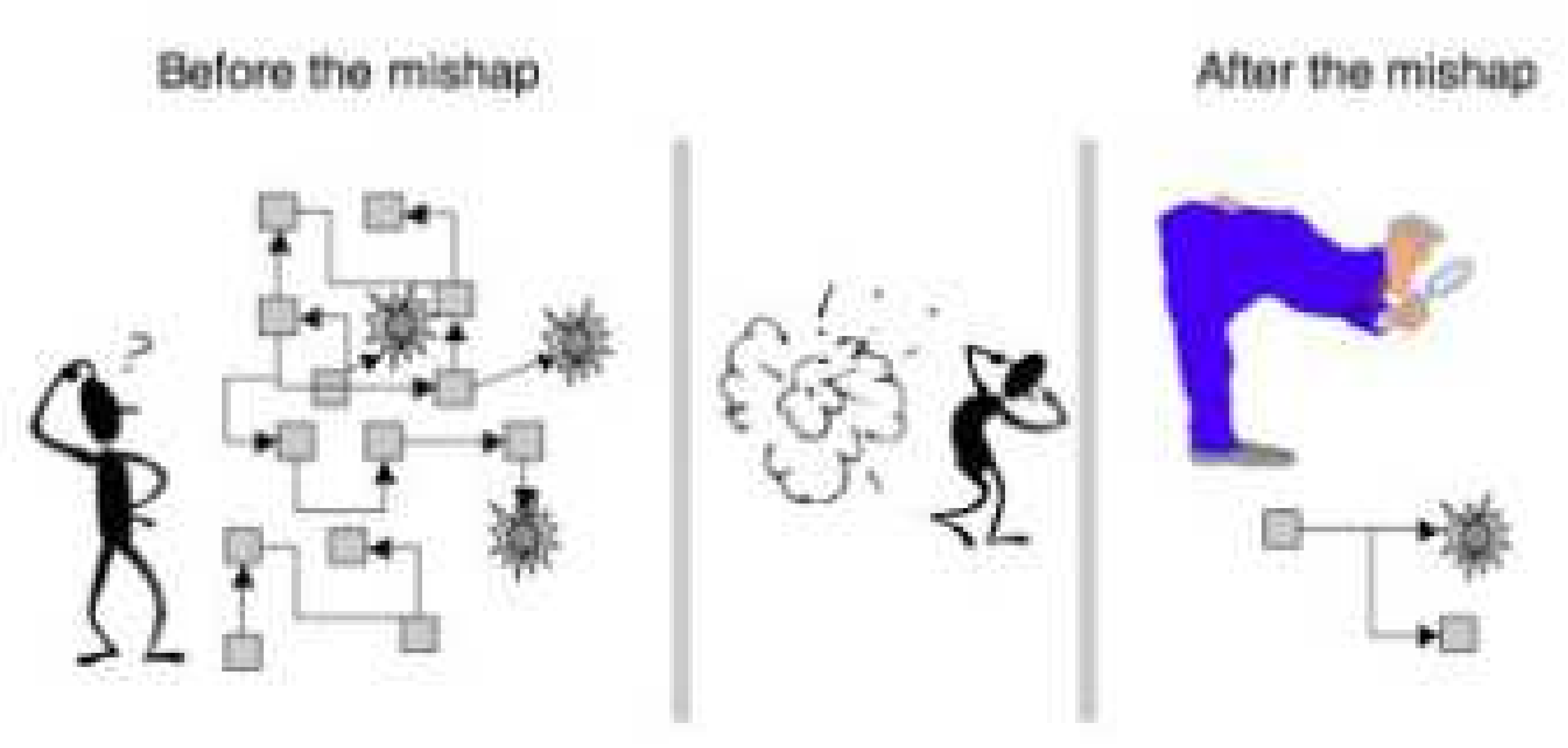
Hindsight Bias

- After an incident
  - Easy to see where people went wrong, what they should have done or avoided
  - Easy to judge about missing a piece of information that turned out to be critical
  - Easy to see what people should have seen or avoided

“shoulda, coulda, woulda”

Hindsight Bias

- Almost impossible to go back and understand how world looked to somebody not having knowledge of outcome
  - Oversimplify causality because can start from outcome and reason backward to presumed or plausible “causes”
  - Overestimate likelihood of the outcome and people’s ability to foresee it because already know outcome
  - Overrate rule or procedure “violations”
  - Misjudge prominence or relevance of data presented to people at the time
  - Match outcomes with actions that went before it: if outcome bad, actions leading to it must have been bad too (missed opportunities, bad assessments, wrong decisions, and misperceptions)



Sidney Dekker, 2009

Hindsight Bias Examples

- Data availability vs. data observability
  - "The available evidence should have been sufficient to give the Board Operator a clear indication that Tank 731 was indeed filling and required immediate attention."

Board Control Valve Position: closed

Bypass Valve: *closed*

Level in tank: 7.2 feet

Flow Meter: *shows no flow*

Flow: *none*

SO_2 alarm: *off*

High level alarm: *off*

  - "Operators could have trended the data" on the control board

Hindsight Bias Examples

- Another example
  - “Interviews with operations personnel did not produce a clear reason why the response to the SO_2 alarm took 31 minutes. The only explanation was that there was not a sense of urgency since, in their experience, previous SO_2 alarms were attributed to minor releases that did not require a unit evacuation.”

Overcoming Hindsight Bias

- Assume nobody comes to work to do a bad job.
  - Assume were doing reasonable things given the complexities, dilemmas, tradeoffs, and uncertainty surrounding them.
  - Simply finding and highlighting people's mistakes explains nothing.
  - Saying what did not do or what should have done does not explain why they did what they did.
- Investigation reports should explain
  - Why it made sense for people to do what they did rather than judging them for what they allegedly did wrong and
  - What changes will reduce likelihood of happening again

Avoiding Hindsight Bias

- Need to consider:
  - Goals person pursuing at time and whether reasonable given circumstances
  - Whether and how goals conflicted with each other (e.g., safety vs. efficiency, production vs. protection)
  - Reasonableness of goal priorities in case of conflicts
  - Unwritten rules and norms that may have played a role in behavior
  - Available vs. observable information
  - Attentional demands
  - Organizational context

Cali American Airlines Crash

Cited probable 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.

CAST (Causal Analysis using System Theory)

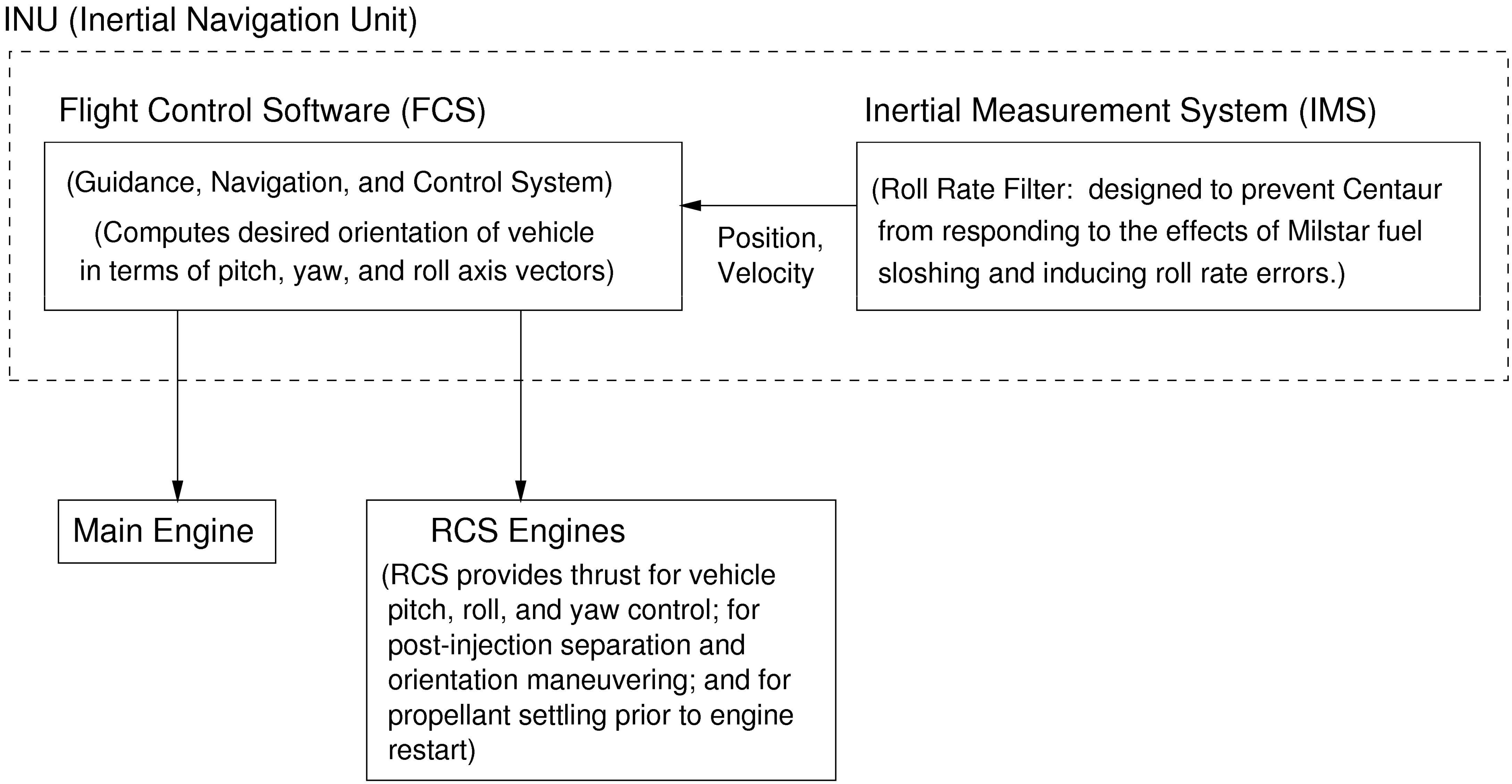
- Identify system hazard violated and the system safety design constraints
- Construct the safety control structure as it was designed to work
  - Component responsibilities (requirements)
  - Control actions and feedback loops
- For each component, determine if it fulfilled its responsibilities or provided inadequate control.
  - If inadequate control, why? (including changes over time)
  - Context
  - Process Model Flaws

CAST (2)

- Examine coordination and communication
- Consider dynamics and migration to higher risk
- Determine the changes that could eliminate the inadequate control (lack of enforcement of system safety constraints) in the future.
- Generate recommendations

Titan IV/Milstar Loss

Physical Control Structure Involved and Component Responsibilities



INU (Inertial Navigation Unit)

Flight Control Software (FCS)

(Guidance, Navigation, and Control System)

(Computes desired orientation of vehicle in terms of pitch, yaw, and roll axis vectors)

Inertial Measurement System (IMS)

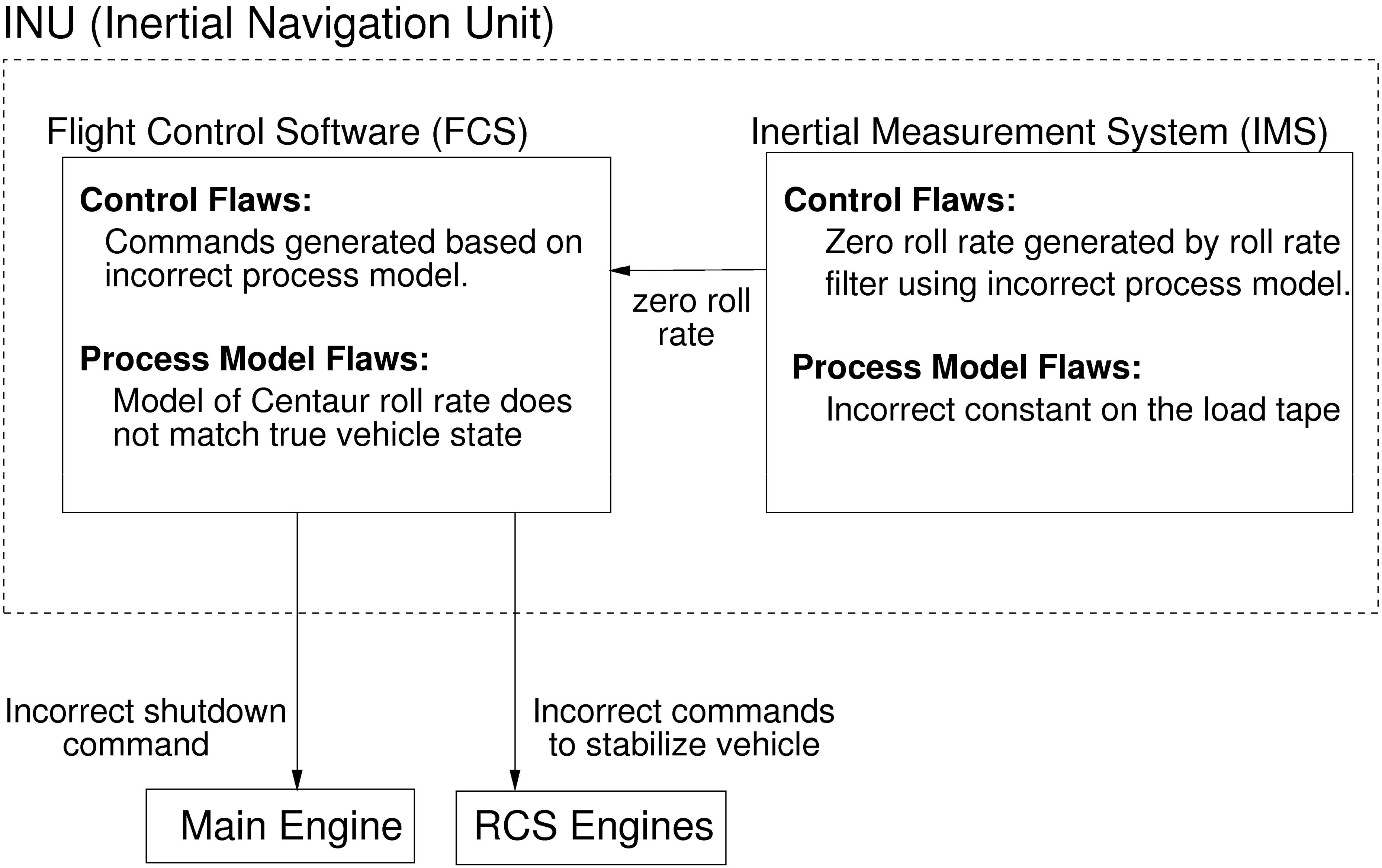
(Roll Rate Filter: designed to prevent Centaur from responding to the effects of Milstar fuel sloshing and inducing roll rate errors.)

Position, Velocity

Main Engine

RCS Engines

(RCS provides thrust for vehicle pitch, roll, and yaw control; for post-injection separation and orientation maneuvering; and for propellant settling prior to engine restart)



INU (Inertial Navigation Unit)

Flight Control Software (FCS)

Control Flaws:

Commands generated based on incorrect process model.

Process Model Flaws:

Model of Centaur roll rate does not match true vehicle state

zero roll rate

Inertial Measurement System (IMS)

Control Flaws:

Zero roll rate generated by roll rate filter using incorrect process model.

Process Model Flaws:

Incorrect constant on the load tape

Incorrect shutdown command

Incorrect commands to stabilize vehicle

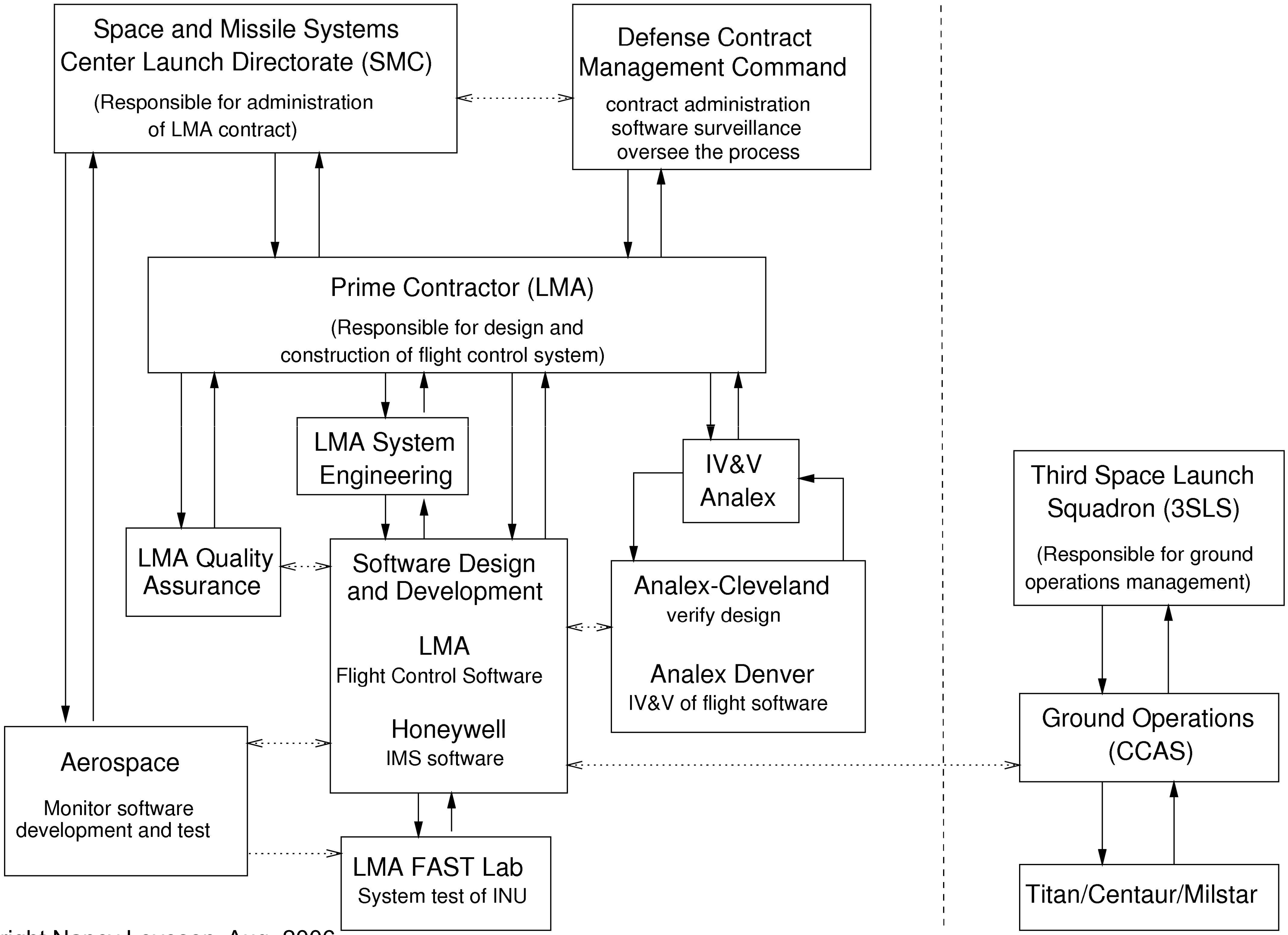
Main Engine

RCS Engines

Titan 4/Centaur/Milstar

DEVELOPMENT

OPERATIONS



Space and Missile Systems Center Launch Directorate (SMC)

(Responsible for administration of LMA contract)

Defense Contract Management Command

contract administration
software surveillance
oversee the process

Prime Contractor (LMA)

(Responsible for design and construction of flight control system)

LMA System Engineering

IV&V Analex

LMA Quality Assurance

Software Design and Development

LMA
Flight Control Software

Honeywell
IMS software

Analex-Cleveland
verify design

Analex Denver
IV&V of flight software

Aerospace

Monitor software development and test

LMA FAST Lab
System test of INU

Third Space Launch Squadron (3SLS)

(Responsible for ground operations management)

Ground Operations (CCAS)

Titan/Centaur/Milstar

Analex IV&V

Safety Constraint:

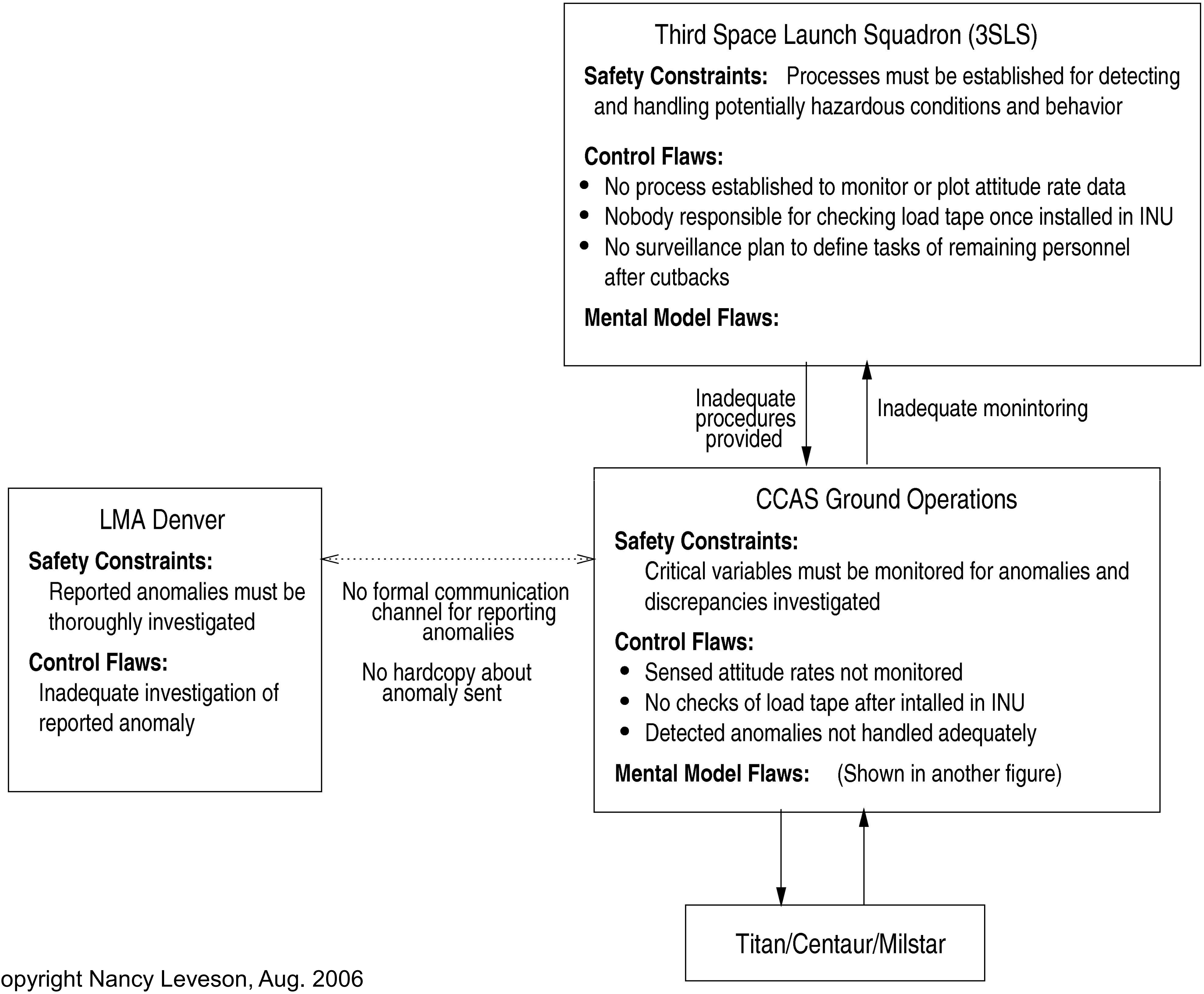
- IV&V must be performed on the as-flown system
- All safety-crtiical data and software must be included

Control Flaws:

- Designed an IV&V process that did not include load tape
- Used default values for testing software implementation
- Validated design constant but not actual constant

Mental Model Flaws:

- Misunderstanding about what could be tested
- Misunderstanding of load tape creation process



Third Space Launch Squadron (3SLS)

Safety Constraints: Processes must be established for detecting and handling potentially hazardous conditions and behavior

Control Flaws:

- No process established to monitor or plot attitude rate data
- Nobody responsible for checking load tape once installed in INU
- No surveillance plan to define tasks of remaining personnel after cutbacks

Mental Model Flaws:

Inadequate procedures provided

Inadequate monintoring

CCAS Ground Operations

Safety Constraints:
Critical variables must be monitored for anomalies and discrepancies investigated

Control Flaws:

- Sensed attitude rates not monitored
- No checks of load tape after intalled in INU
- Detected anomalies not handled adequately

Mental Model Flaws: (Shown in another figure)

LMA Denver

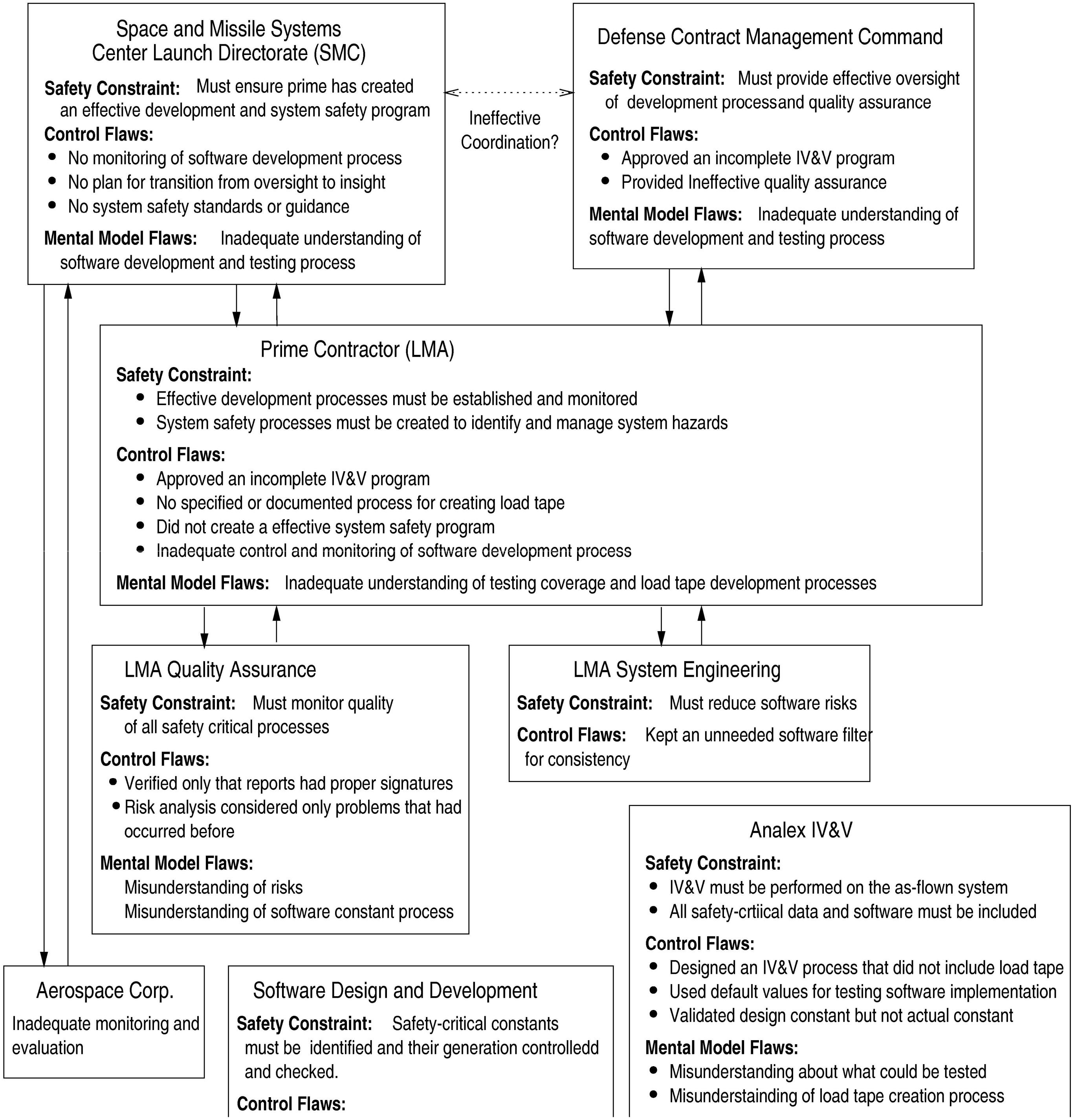
Safety Constraints:
Reported anomalies must be thoroughly investigated

Control Flaws:
Inadequate investigation of reported anomaly

No formal communication channel for reporting anomalies

No hardcopy about anomaly sent

Titan/Centaur/Milstar



Space and Missile Systems Center Launch Directorate (SMC)

Safety Constraint: Must ensure prime has created an effective development and system safety program

Control Flaws:

- No monitoring of software development process
- No plan for transition from oversight to insight
- No system safety standards or guidance

Mental Model Flaws: Inadequate understanding of software development and testing process

Defense Contract Management Command

Safety Constraint: Must provide effective oversight of development processand quality assurance

Control Flaws:

- Approved an incomplete IV&V program
- Provided Ineffective quality assurance

Mental Model Flaws: Inadequate understanding of software development and testing process

Prime Contractor (LMA)

Safety Constraint:

- Effective development processes must be established and monitored
- System safety processes must be created to identify and manage system hazards

Control Flaws:

- Approved an incomplete IV&V program
- No specified or documented process for creating load tape
- Did not create a effective system safety program
- Inadequate control and monitoring of software development process

Mental Model Flaws: Inadequate understanding of testing coverage and load tape development processes

LMA Quality Assurance

Safety Constraint: Must monitor quality of all safety critical processes

Control Flaws:

- Verified only that reports had proper signatures
- Risk analysis considered only problems that had occurred before

Mental Model Flaws:

Misunderstanding of risks
Misunderstanding of software constant process

LMA System Engineering

Safety Constraint: Must reduce software risks

Control Flaws: Kept an unneeded software filter for consistency

Analex IV&V

Safety Constraint:

- IV&V must be performed on the as-flown system
- All safety-crtiical data and software must be included

Control Flaws:

- Designed an IV&V process that did not include load tape
- Used default values for testing software implementation
- Validated design constant but not actual constant

Mental Model Flaws:

- Misunderstanding about what could be tested
- Misunderstainding of load tape creation process

Aerospace Corp.

Inadequate monitoring and evaluation

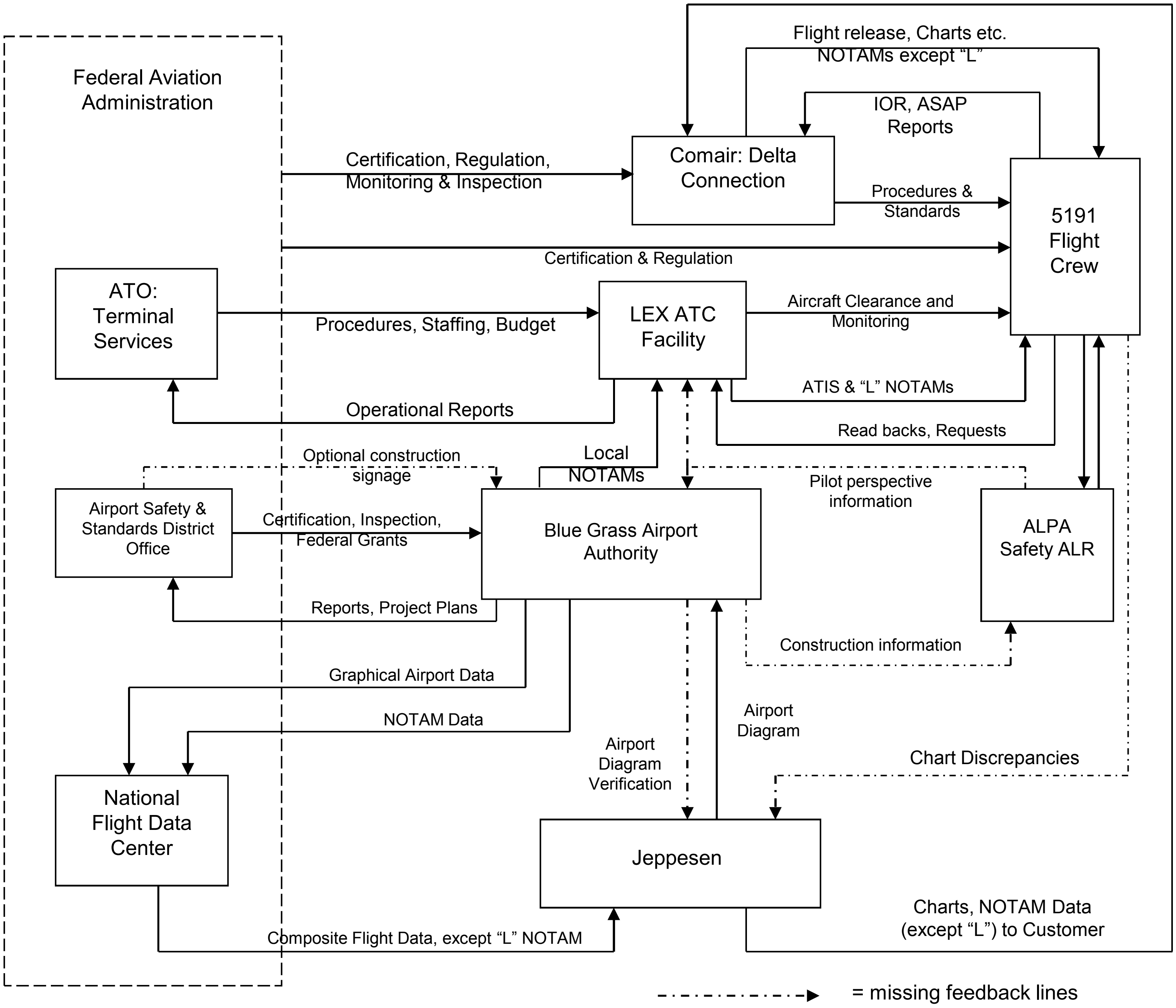
Software Design and Development

Safety Constraint: Safety-critical constants must be identified and their generation controlledd and checked.

Control Flaws:

Identifying Components to Include

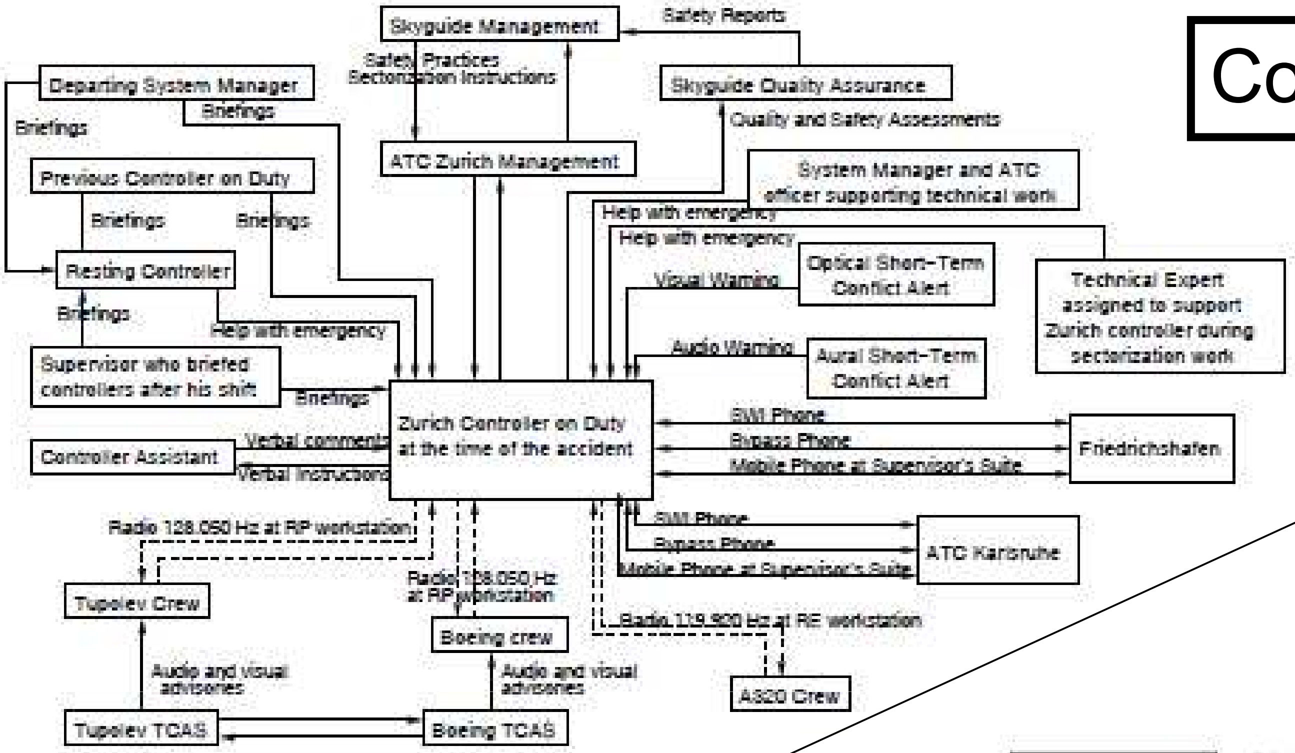
- Start with physical process
- What inadequate controls allowed the physical events?
  - Physical
  - Direct controller
  - Indirect controllers
- Add controls and control components as required to explain the inadequate controls already identified.



Federal Aviation Administration
Comair: Delta Connection
Flight release, Charts etc.
NOTAMs except "L"
IOR, ASAP Reports
Certification, Regulation, Monitoring & Inspection
Procedures & Standards
5191 Flight Crew
Certification & Regulation
ATO: Terminal Services
Procedures, Staffing, Budget
LEX ATC Facility
Aircraft Clearance and Monitoring
ATIS & "L" NOTAMs
Operational Reports
Read backs, Requests
Optional construction signage
Local NOTAMs
Pilot perspective information
Airport Safety & Standards District Office
Certification, Inspection, Federal Grants
Blue Grass Airport Authority
ALPA Safety ALR
Reports, Project Plans
Construction information
Graphical Airport Data
NOTAM Data
Airport Diagram
Airport Diagram Verification
Chart Discrepancies
National Flight Data Center
Jeppesen
Charts, NOTAM Data (except "L") to Customer
Composite Flight Data, except "L" NOTAM

-·-·-·-·-▶ = missing feedback lines

Communications



Skyguide Management

Safety Reports

Safety Practices
Sectorization Instructions

Skyguide Quality Assurance

Quality and Safety Assessments

Departing System Manager

Briefings

Briefings

ATC Zurich Management

Previous Controller on Duty

Briefings

Briefings

System Manager and ATC officer supporting technical work

Help with emergency

Help with emergency

Resting Controller

Optical Short-Term Conflict Alert

Visual Warning

Technical Expert assigned to support Zurich controller during sectorization work

Briefings

Help with emergency

Audio Warning

Aural Short-Term Conflict Alert

Supervisor who briefed controllers after his shift

Briefings

Zurich Controller on Duty at the time of the accident

SWI Phone

Bypass Phone

Mobile Phone at Supervisor's Suite

Friedrichshafen

Controller Assistant

Verbal comments

Verbal Instructions

Radio 128.050 Hz at RP workstation

SWI Phone

Bypass Phone

Mobile Phone at Supervisor's Suite

ATC Karlsruhe

Tupolev Crew

Radio 128.050 Hz at RP workstation

Boeing crew

Radio 119.920 Hz at RE workstation

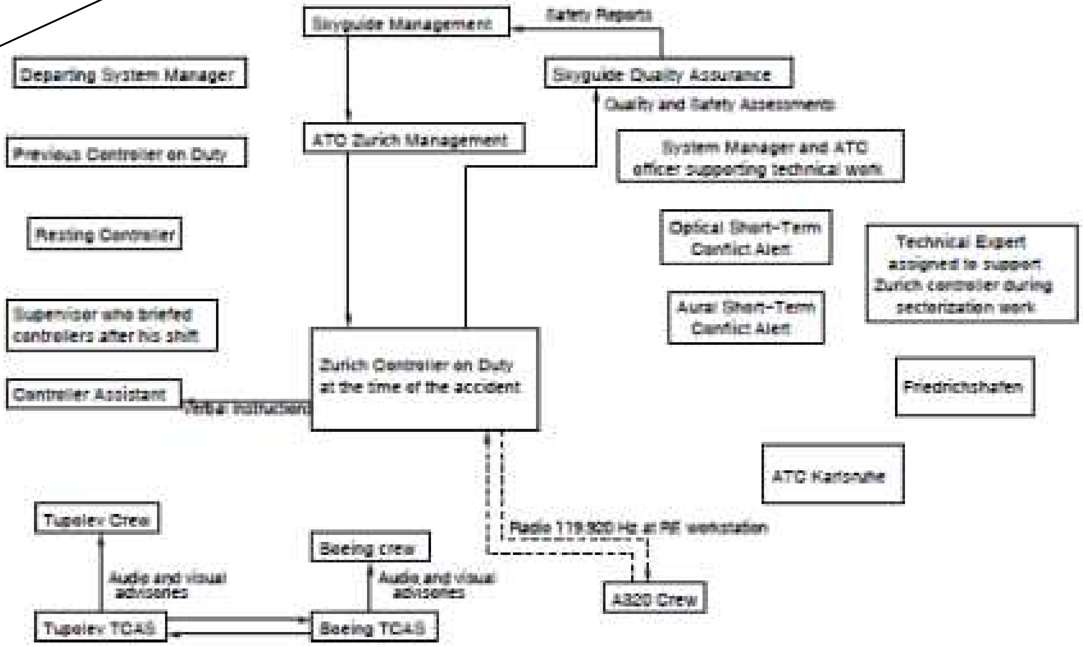
Audio and visual advisories

Audio and visual advisories

A320 Crew

Tupolev TCAS

Boeing TCAS



Skyguide Management

Safety Reports

Skyguide Quality Assurance

Departing System Manager

Quality and Safety Assessments

ATC Zurich Management

Previous Controller on Duty

System Manager and ATC officer supporting technical work

Resting Controller

Optical Short-Term Conflict Alert

Technical Expert assigned to support Zurich controller during sectorization work

Aural Short-Term Conflict Alert

Supervisor who briefed controllers after his shift

Zurich Controller on Duty at the time of the accident

Friedrichshafen

Controller Assistant

Verbal instructions

ATC Karlsruhe

Tupolev Crew

Radio 119.920 Hz at RE workstation

Boeing crew

Audio and visual advisories

Audio and visual advisories

A320 Crew

Tupolev TCAS

Boeing TCAS

Why Our Efforts are Often Not Cost-Effective

- Efforts superficial, isolated, or misdirected
  - Often isolated from engineering design
  - Spend too much time and effort on assurance not designing for safety
    - Focusing on making arguments that systems <u>are</u> safe rather than <u>making</u> them safe
    - “Safety cases”: Subject to confirmation bias
    - Should be trying to prove the system is unsafe, not that it is safe
    - Safety must be built in, it cannot be “assured in”

Safety Cases

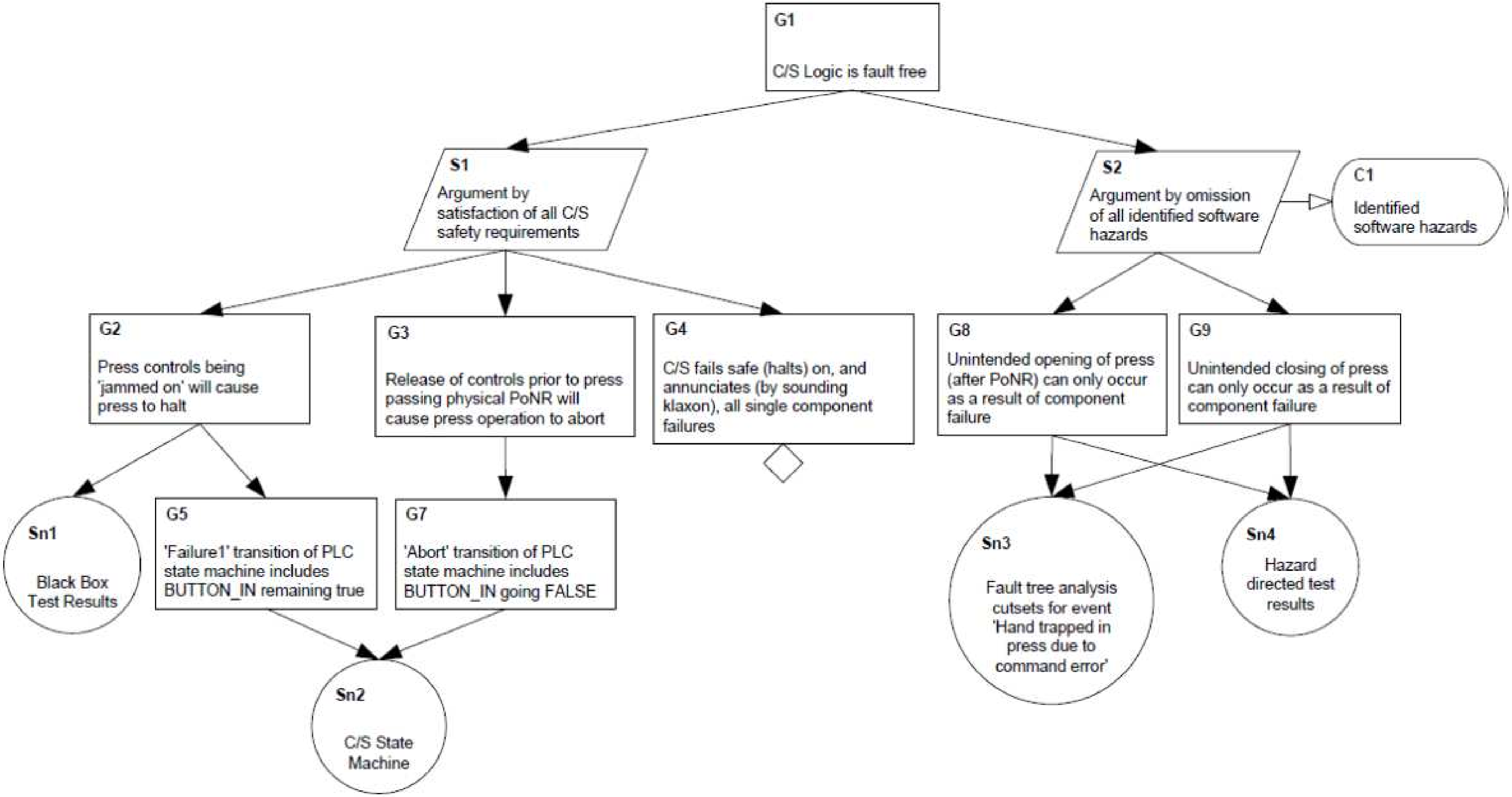
- An argument that system design is safe is <u>not</u> enough
- Have been criticized as a causal factor in accidents
- Subject to confirmation bias
  - A tendency for people to favor information that confirms their preconceptions or hypotheses regardless of whether the information is true.
- Value of system safety is doing what engineers do not do. A different viewpoint.

Confirmation Bias

- People will focus on and interpret evidence in a way that confirms the goal they have set for themselves
  - If the goal is to prove the system is safe, they will focus on the evidence that shows it is safe and create an argument for safety.
  - If the goal is to show the system is unsafe, the evidence used and the interpretation of available evidence will be quite different.
  - People also tend to interpret ambiguous evidence as supporting their existing position.

Confirmation Bias (2)

- Experiments show people tend to test hypotheses in a one-sided way, by searching for evidence consistent with the hypothesis they hold at a given time.
  - Rather than searching through all the relevant evidence, they ask questions that are phrased so that an affirmative answer supports their hypothesis.
  - A related aspect is the tendency for people to focus on one possibility and ignore alternatives.


G1
C/S Logic is fault free
S1
Argument by satisfaction of all C/S safety requirements
S2
Argument by omission of all identified software hazards
C1
Identified software hazards
G2
Press controls being 'jammed on' will cause press to halt
G3
Release of controls prior to press passing physical PoNR will cause press operation to abort
G4
C/S fails safe (halts) on, and annunciates (by sounding klaxon), all single component failures
G8
Unintended opening of press (after PoNR) can only occur as a result of component failure
G9
Unintended closing of press can only occur as a result of component failure
Sn1
Black Box Test Results
G5
'Failure1' transition of PLC state machine includes BUTTON_IN remaining true
G7
'Abort' transition of PLC state machine includes BUTTON_IN going FALSE
Sn3
Fault tree analysis cutsets for event 'Hand trapped in press due to command error'
Sn4
Hazard directed test results
Sn2
C/S State Machine

Why our Efforts are Often Not Cost-Effective (2)

- Safety efforts start too late
  - 80-90% of safety-critical decisions made in early system concept formation
  - Cannot “add” safety to an unsafe design

Why our Efforts are Often Not Cost-Effective (3)

- Using inappropriate techniques for systems built today
  - Mostly used hazard analysis techniques created 40-50 years ago
    - Developed for relatively simple electromechanical systems
    - New technology increasing complexity of system designs and introducing new accident causes
    - Complexity is creating new causes of accidents
  - Should build simplest systems possible, but usually unwilling to make the compromises necessary
    1. Complexity related to the problem itself
    2. Complexity introduced in the design of solution of problem
  - Need new, more powerful safety engineering approaches to dealing with complexity and new causes of accidents

Why our Efforts are Often Not Cost-Effective (4)

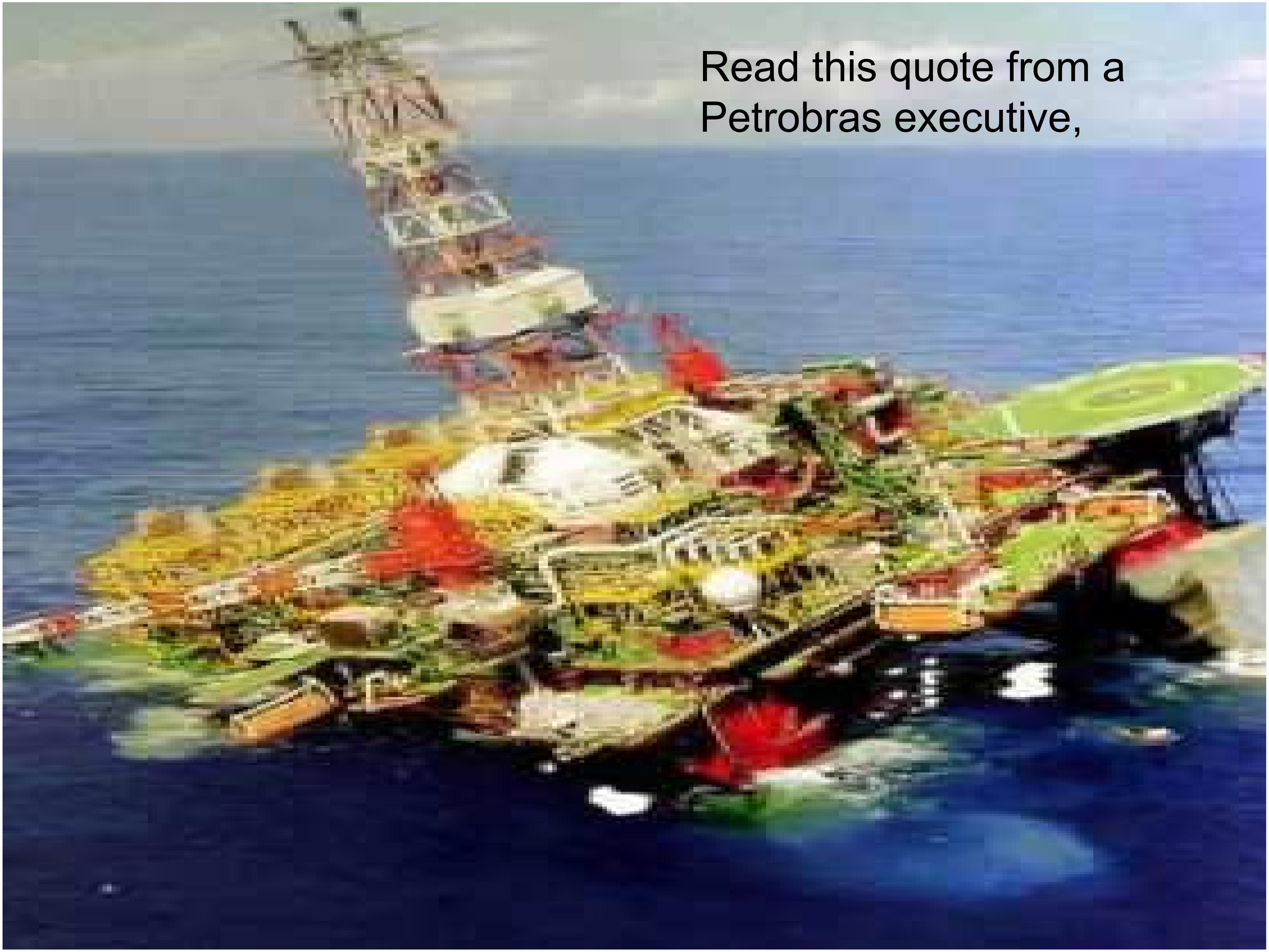
- Focus efforts only on technical components of systems
  - Ignore or only superficially handle
    - Management decision making
    - Operator error (and operations in general)
    - Safety culture
  - Focus on development and often ignore operations
- Inadequate risk communication (inaccurate perceptions of risk)
- Limited learning from events

Safety culture, management, and the sinking of the largest offshore oil platform

March 2001

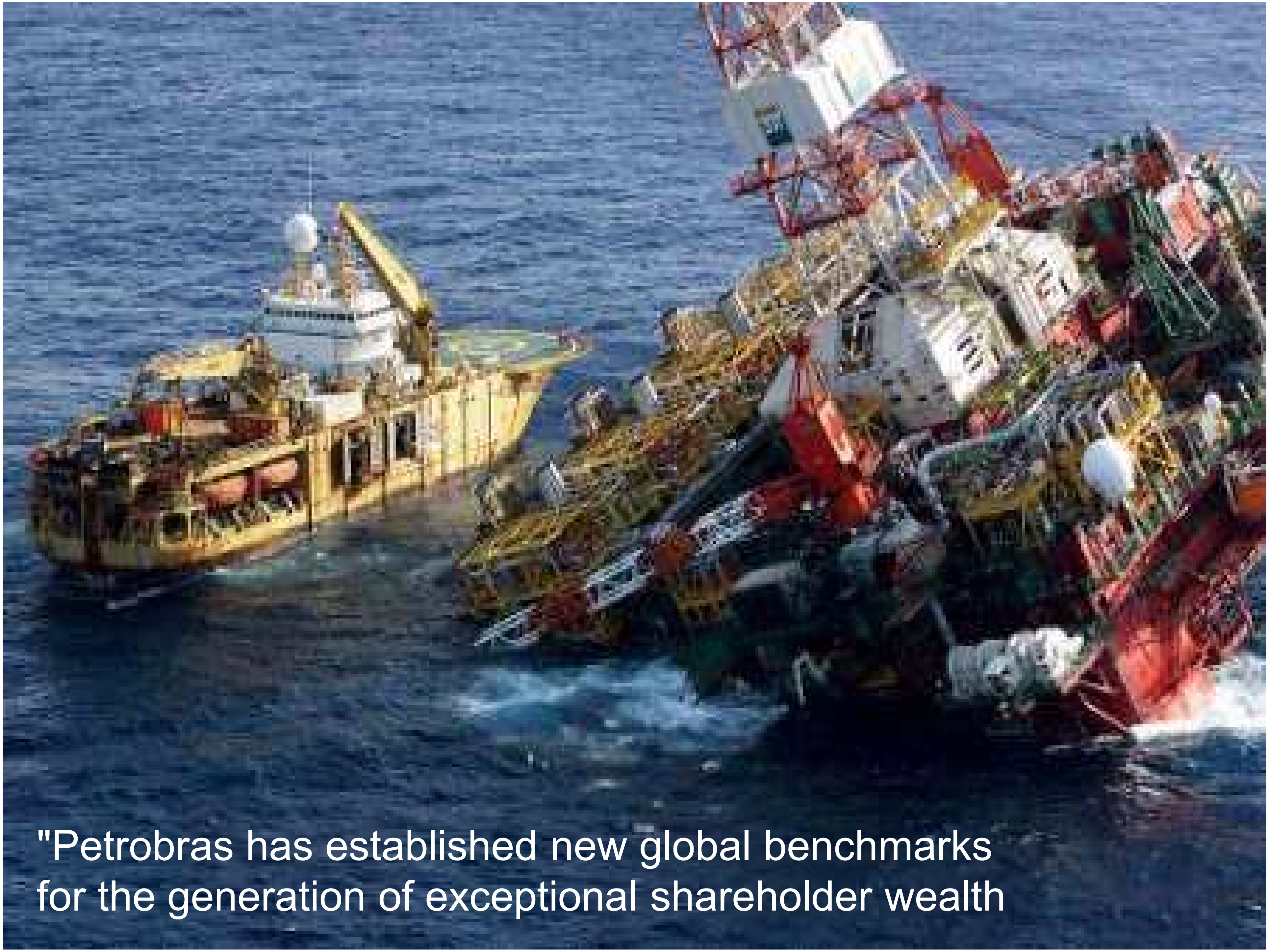
For those of you who may be involved in managing safety-critical projects

Management concern for safety is the single most important factor in achieving it

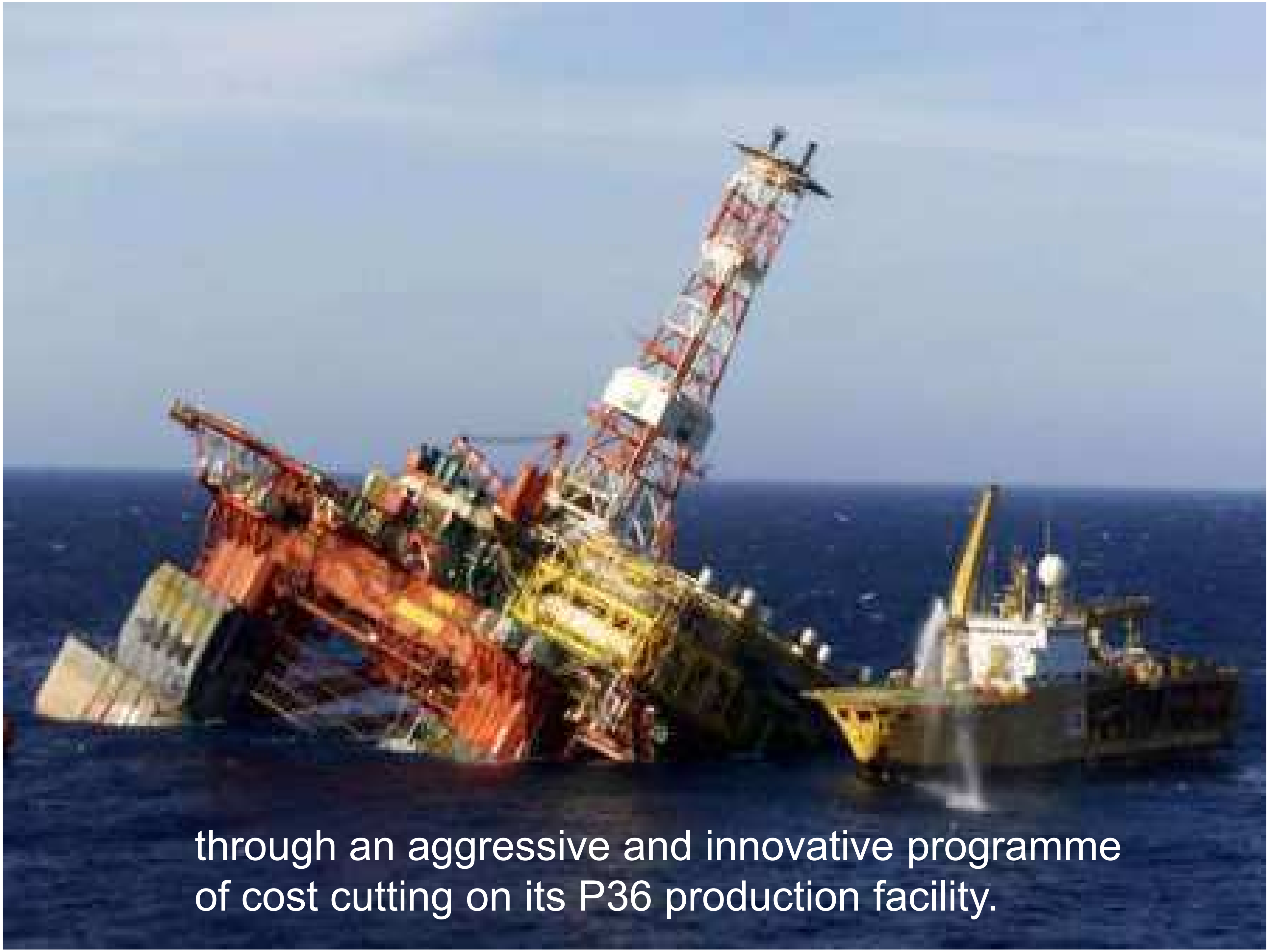


Read this quote from a Petrobras executive,

on the project that sunk into the Atlantic Ocean off the coast of Brazil in March 2001.



"Petrobras has established new global benchmarks for the generation of exceptional shareholder wealth



through an aggressive and innovative programme of cost cutting on its P36 production facility.

Conventional constraints have been successfully challenged

and replaced with new paradigms appropriate to the globalised corporate market place.

Through an integrated network of facilitated workshops, the project successfully rejected the established constricting and negative influences of prescriptive engineering,

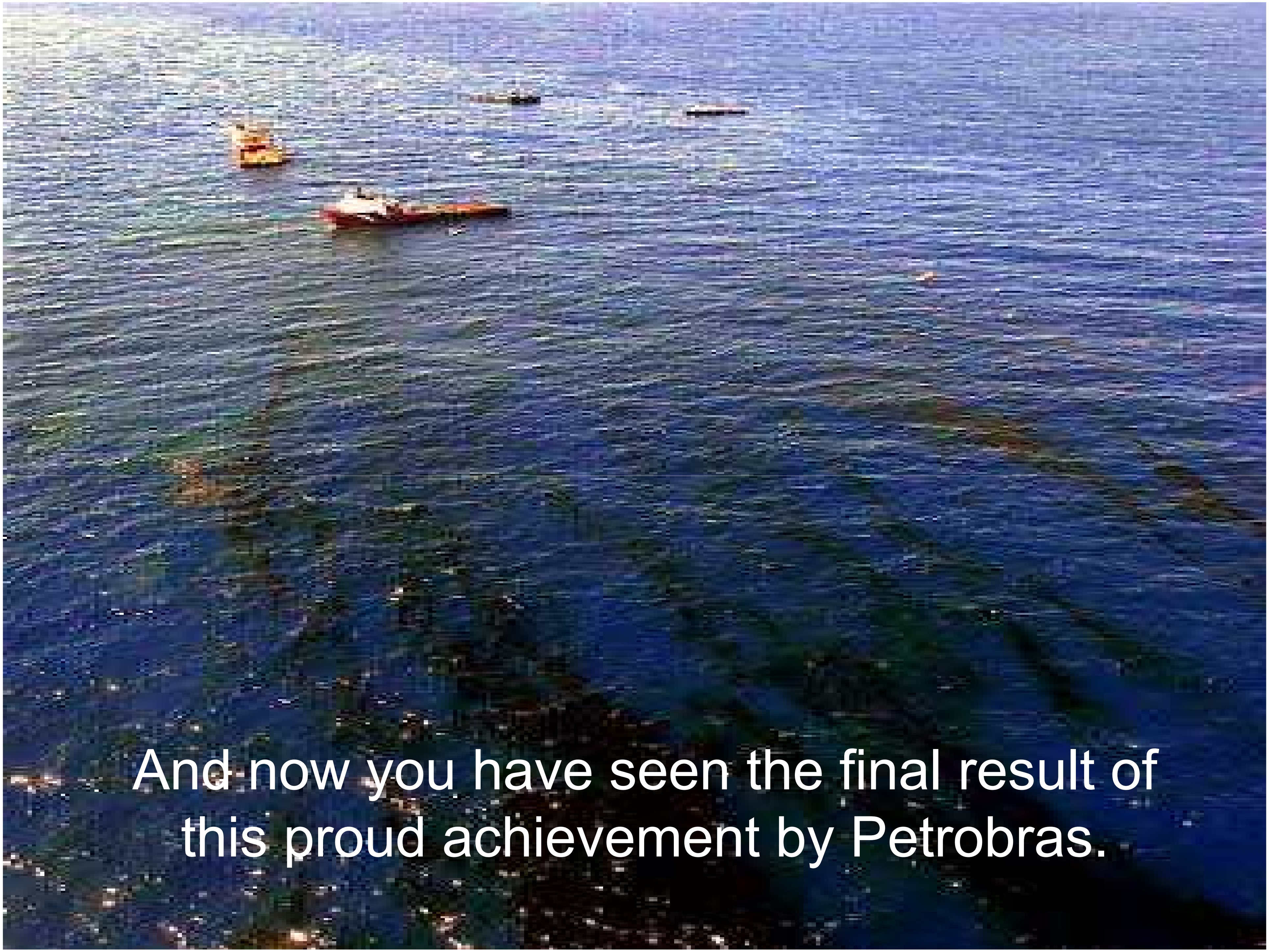
onerous quality requirements, and outdated concepts of inspection and client control.

Elimination of these unnecessary straitjackets has empowered the project's suppliers and contractors to propose highly economical solutions,

with the win-win bonus of enhanced profitability margins for themselves.

The P36 platform shows the shape of things to come

in the unregulated global market economy of the 21st Century.“



And now you have seen the final result of this proud achievement by Petrobras.

A life without adventure is likely to be unsatisfying, but a life in which adventure is allowed to take whatever form it will, is likely to be short.

Bertrand Russell