

A New Approach to Ensuring Safety in Software and Human Intensive Systems

Nancy G. Leveson

MIT

and

Safeware Engineering, Inc.

leveson@mit.edu



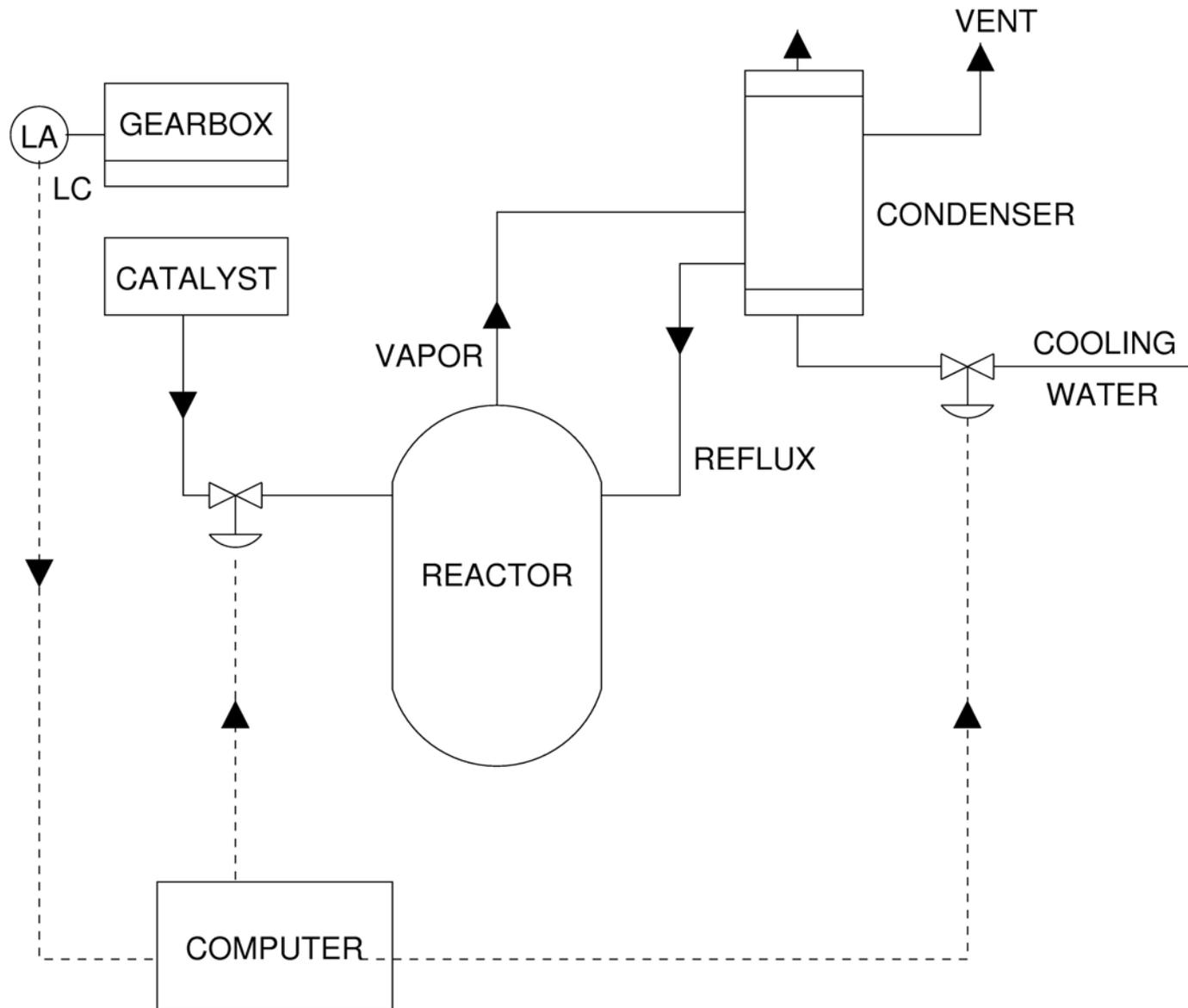
*“It’s never what we don’t know that stops us.
It’s what we do know that just ain’t so.”*

Dean Kamen

Why is a New Approach Needed?

- Accidents in high-tech systems are changing their nature
- We need to change our approaches to safety engineering in response
- Many of the problems arise from the unique aspects of software and the changes it requires in system engineering
- Applying systems thinking to engineering will help

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
 - Related to
 - Interactive complexity and tight coupling
 - Use of computers and software

Interactive Complexity

- Critical factor is intellectual manageability
 - A simple system has a small number of unknowns in its interactions (within system and with environment)
 - Interactively complex (intellectually unmanageable) when level of interactions reaches point where can no longer be thoroughly
 - Planned
 - Understood
 - Anticipated
 - Guarded against

Safety vs. Reliability

- Safety and reliability are NOT the same
 - Sometimes increasing one can even decrease the other.
 - Making all the components highly reliable will have no impact on component interaction accidents.
- For relatively simple, electro-mechanical systems with primarily component failure accidents, reliability engineering can increase safety.
- For complex, software-intensive or human-intensive systems, we need something else.

Software Changes System Engineering

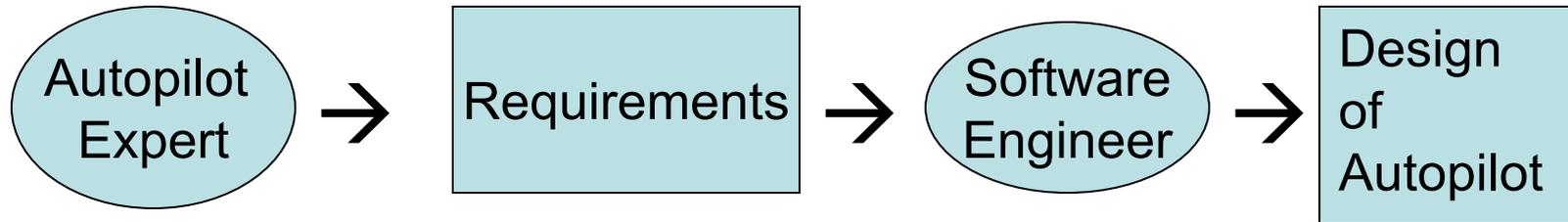
- Software is simply the design of a machine abstracted from its physical realization



- Software “failure modes” are different (do abstractions fail?)
 - Usually does exactly what you tell it to do
 - Problems occur from operation, not lack of operation
 - Usually doing exactly what software engineers wanted

Abstraction from Physical Design

- Software engineers are doing system design



- Most operational software errors related to requirements (particularly incompleteness)

Software-Related Accidents

- Are almost all 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.
- While these things true for hardware, we can thoroughly test hardware and get out requirements and design errors
 - Can only test a small part of potential software behavior

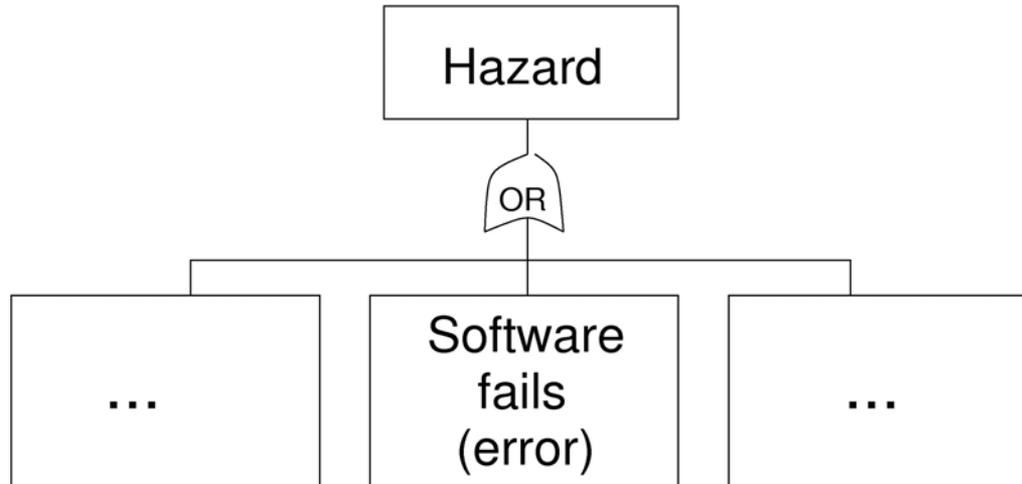
Reliability Approach to Software Safety

Using standard engineering techniques of

- Preventing failures through redundancy
- Increasing component reliability
- Reuse of designs and learning from experience

will not work for software and system accidents

Typical Fault Trees

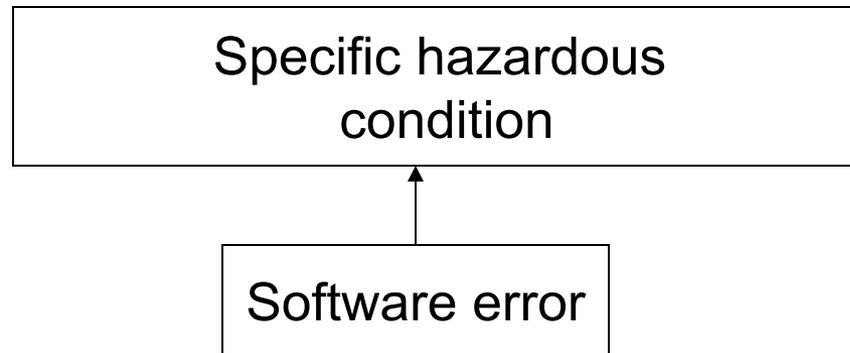


Hazard Cause	Probability	Mitigation
Software Error	0	Test software

PRA and Software

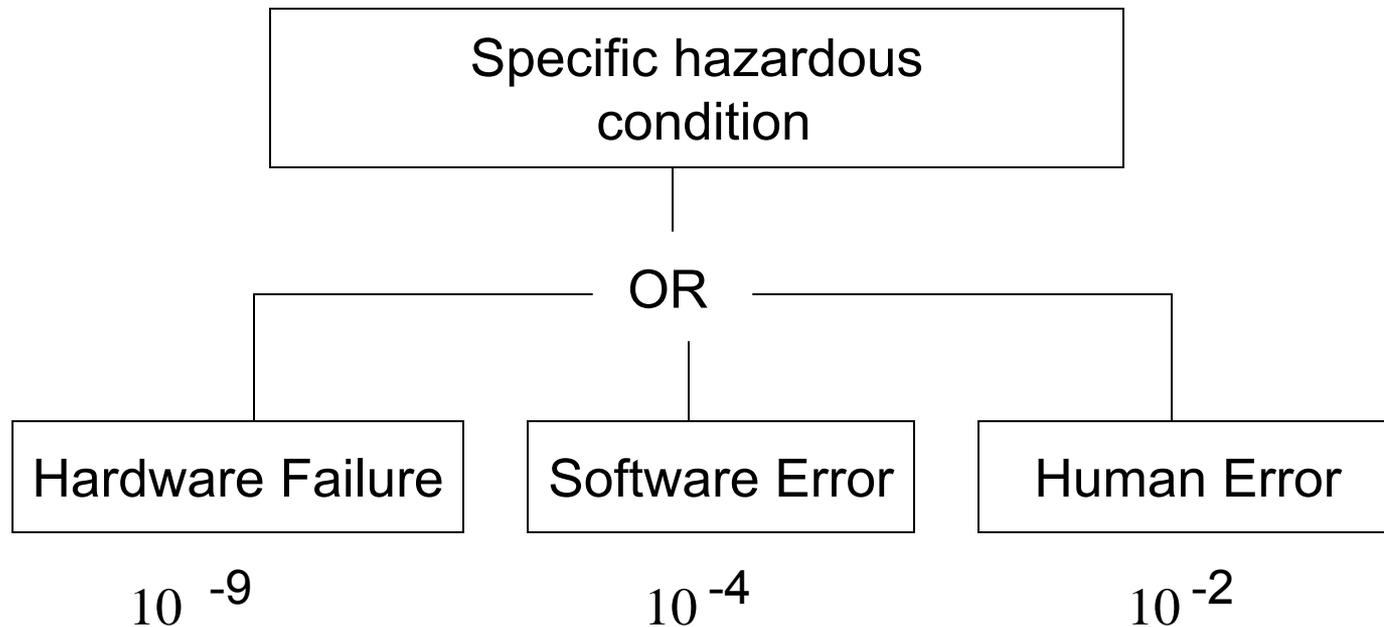
- Software reliability figures cannot be used (even if we knew how to get them)

Wrong!!



- If we knew enough to get the probability of the software doing a specific wrong thing, we would know enough to fix the problem and would not bother to measure it

- If this made sense, we could build a universal fault tree and all systems will have the same risk.



Software Safety vs. Software Reliability/Integrity/Correctness

Example: Pressure Switch that sends out a signal when reaches a threshold

1. Signal safety-increasing →

Require any of three sensors to report below threshold

2. Signal safety-decreasing →

Require all three sensors to report below threshold

What is the Solution?

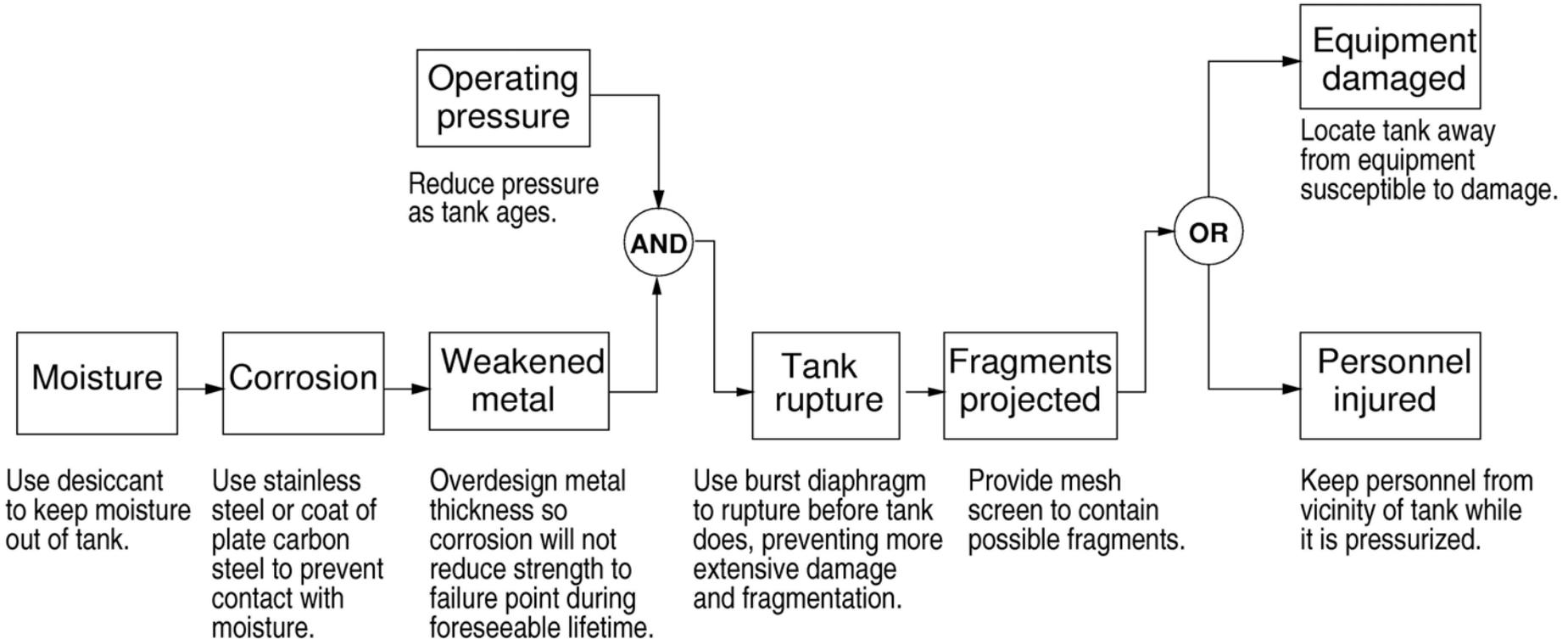
- Enforce discipline and control complexity
 - Limits have changed from structural integrity and physical constraints of materials to intellectual limits
- Improve communication among engineers
- Build safety in by enforcing constraints on behavior
 - Controller contributes to accidents not by “failing” but by:
 1. Not enforcing safety-related constraints on behavior
 2. Commanding behavior that violates safety constraints

Traditional Accident Causation Model

Chain-of-Events Model

- Explains accidents in terms of multiple events, sequenced as a forward chain over time.
 - Simple, direct relationship between events in chain
 - Ignores non-linear relationships, feedback, etc.
 - Events almost always involve component failure, human error, or energy-related event
 - Forms the basis for most safety-engineering and reliability engineering analysis:
 - e.g, FTA, PRA, FMECA, Event Trees, etc.
- and design:
- e.g., redundancy, overdesign, safety margins,

Chain-of-events example



Limitations of Chain-of-Events Model

- Social and organizational factors in accidents
- Component interaction accidents
- Software
- Adaptation
 - Systems are continually changing
 - Systems and organizations migrate toward accidents (states of high risk) under cost and productivity pressures in an aggressive, competitive environment

Limitations (2)

- Human error
 - Define as deviation from normative procedures, but operators always deviate from standard procedures
 - Normative vs. effective procedures
 - Sometimes violation of rules has prevented accidents
 - Less successful actions are natural part of search by operator for optimal performance

Human Error: **Old View**

- Human error is cause of incidents and accidents
- So do something about human involved (suspend, retrain, admonish)
- Or do something about humans in general
 - Marginalize them by putting in more automation
 - Rigidify their work by creating more rules and procedures

Human Error: **New View**

- Human error is a symptom, not a cause
- All behavior affected by context (system) in which occurs
- To do something about error, must look at system in which people work:
 - Design of equipment
 - Usefulness of procedures
 - Existence of goal conflicts and production pressures

STAMP

**A new accident causation
model using Systems Theory
(vs. Reliability Theory)**

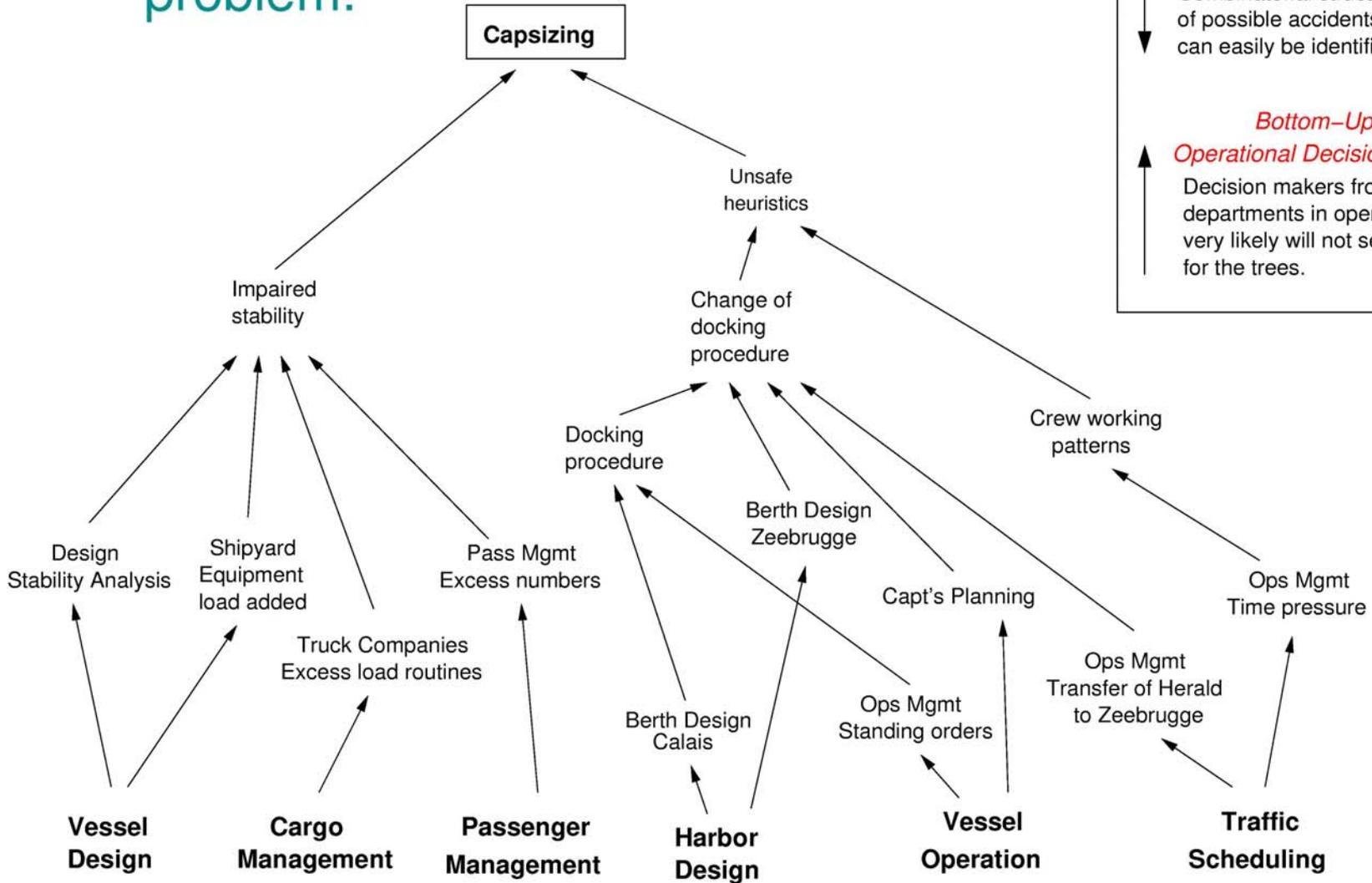
Systems Theory

- Focuses on systems taken as a whole, not on parts taken separate
 - Some properties can only be treated adequately in their entirety, taking into account all social and technical aspects
 - These properties derive from relationships among the parts of the system
 - How they interact and fit together
- Two pairs of ideas
 1. Hierarchy and emergence
 2. Communication and control

Hierarchy and Emergence

- Complex systems can be modeled as a hierarchy of organizational levels
 - Each level more complex than one below
 - Levels characterized by emergent properties
 - Irreducible
 - Represent constraints on the degree of freedom of components at lower level
- Safety is an emergent system property
 - It is NOT a component property
 - It can only be analyzed in the context of the whole

Safety is a system problem.



Top-Down Accident Analysis:

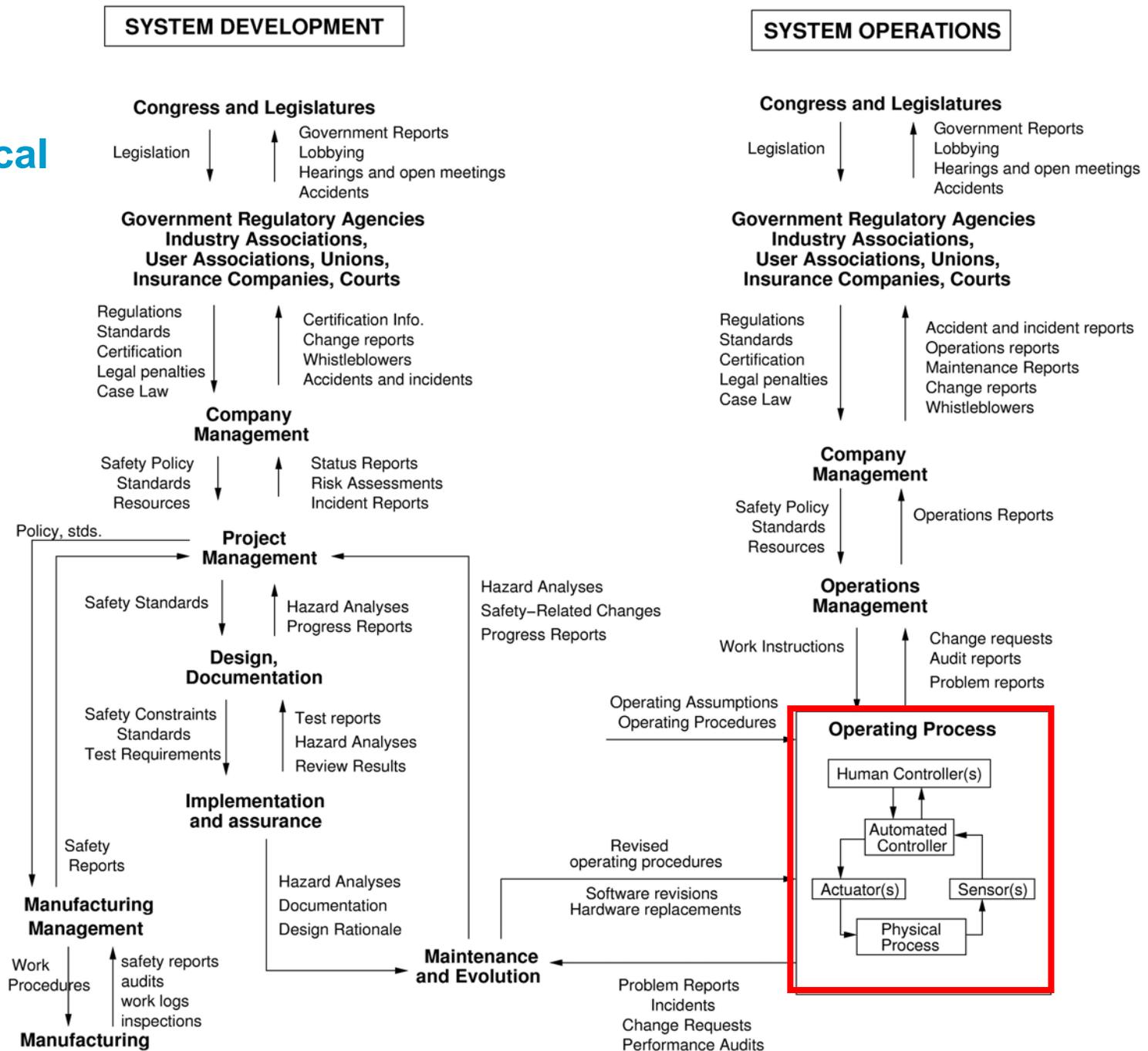
Combinatorial structure of possible accidents can easily be identified.

Bottom-Up

Operational Decision Making:

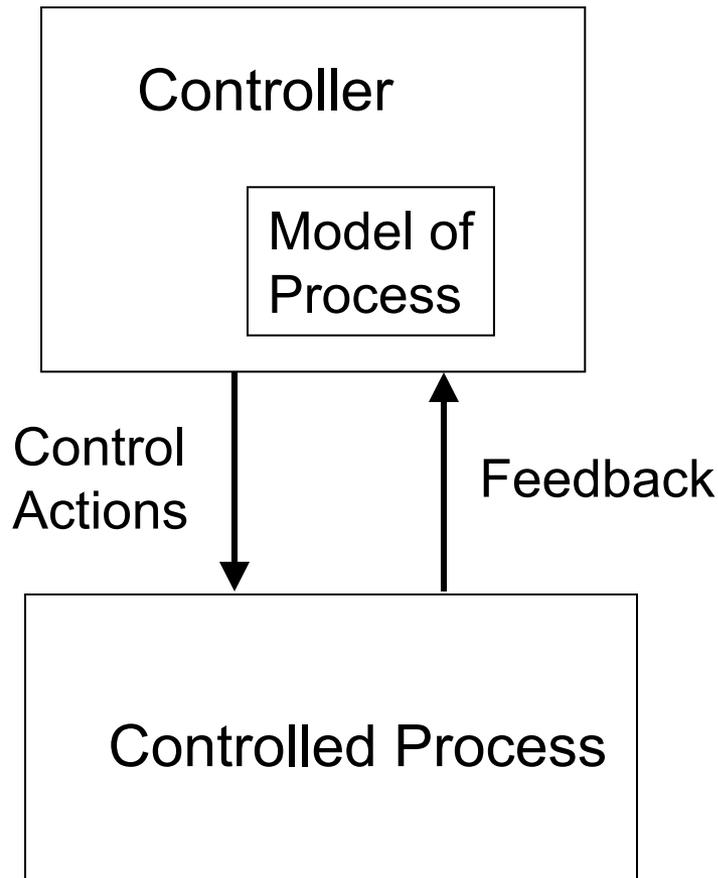
Decision makers from separate departments in operational context very likely will not see the forest for the trees.

Example Hierarchical Control Structure



Communication and Control

- **Control processes operate between levels of control**



Process models must contain:

- Required relationship among process variables
- Current state (values of process variables)
- The ways the process can change state

Relationship Between Safety and Process Models

- Accidents occur when models do not match process and
 - Incorrect control commands given
 - Correct ones not given
 - Correct commands given at wrong time (too early, too late)
 - Control stops too soon

Relationship Between Safety and Process Models (2)

- How do they become inconsistent?
 - Wrong from beginning
 - Missing or incorrect feedback
 - Not updated correctly
 - Time lags not accounted for

Resulting in

Uncontrolled disturbances

Unhandled process states

Inadvertently commanding system into a hazardous state

Unhandled or incorrectly handled system component failures

STAMP Accident Causation Model

- Accidents arise from unsafe interactions among humans, machines, and the environment (not just component failures)

~~“prevent failures”~~
↓

“enforce safety constraints on system behavior”

- Losses are the result of complex dynamic processes, not simply chains of failure events
- Most major accidents arise from a slow migration of the entire system toward a state of high-risk
 - Need to control and detect this migration

A System's Approach to Risk Management

- Safety viewed as a dynamic control problem rather than a component failure problem.
 - O-ring did not control propellant gas release by sealing gap in field joint
 - Software did not adequately control descent speed of Mars Polar Lander
 - Temperature in batch reactor not adequately controlled by system design
- Events are the result of the inadequate control
 - Result from lack of enforcement of safety constraints by system design and operations

Safety Constraints

- Build safety in by enforcing safety constraints on behavior in system design and operations

System Safety Constraint:

Water must be flowing into reflux condenser whenever catalyst is added to reactor

Software Safety Constraint:

Software must always open water valve before catalyst valve

- We have new hazard analysis and safety-driven design techniques to:
 - Identify system and component safety constraints
 - Perform hazard analysis in parallel with design to guide engineering design process

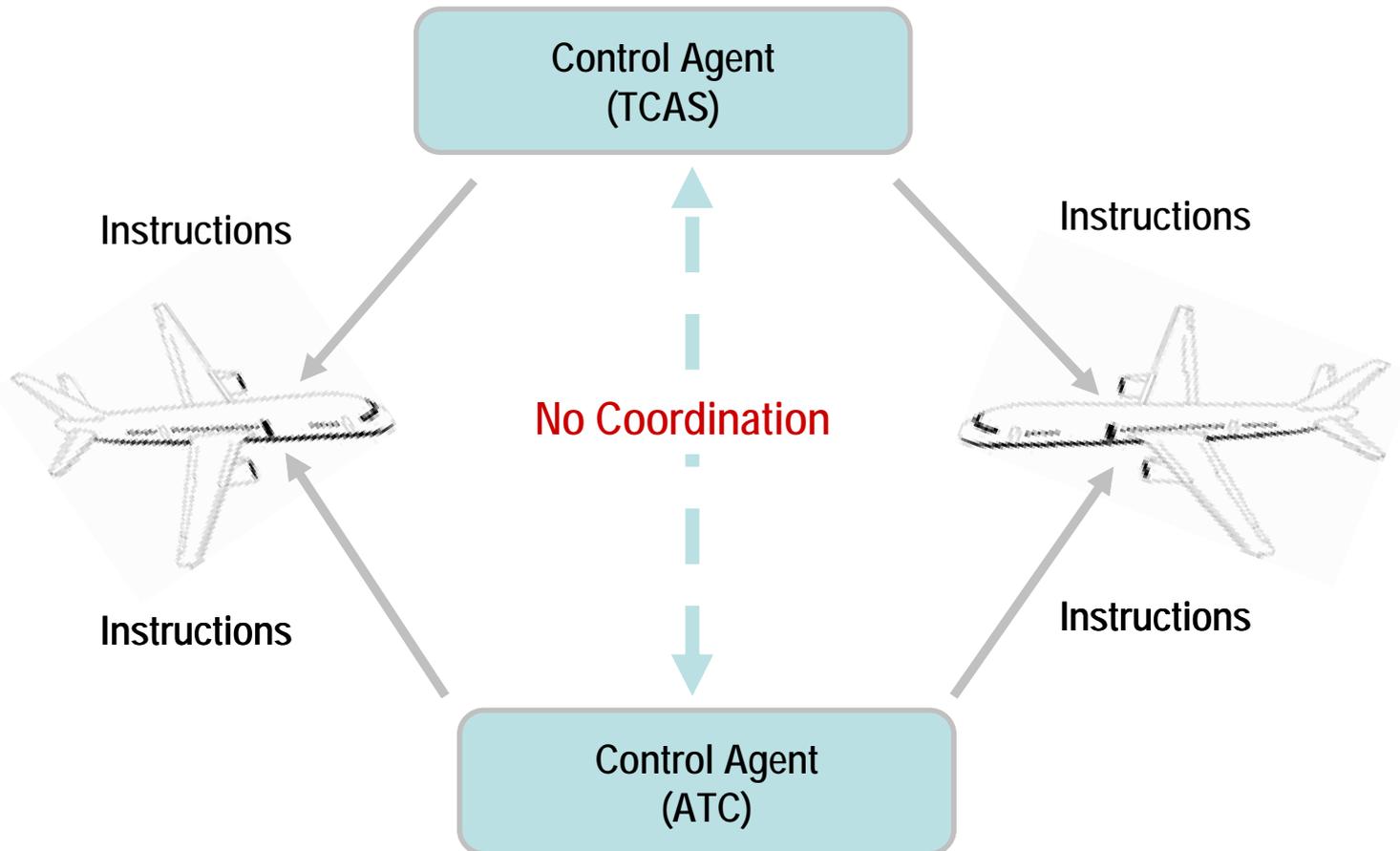
Summary: Accident Causality

- 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

Uncoordinated “Control Agents”

“UNSAFE STATE”

BOTH TCAS and ATC provide uncoordinated & independent instructions



Uses for STAMP

- Basis for new, more powerful hazard analysis techniques (STPA)
 - Perform hazard analyses on physical and social systems
 - Inform early architectural trade studies
 - Identify and prioritize hazards and risks
 - Identify system and component safety requirements and constraints (to be used in design)
- Safety-driven design (physical, operational, organizational)
- More comprehensive accident/incident investigation and root cause analysis

Uses for STAMP (2)

- Organizational and cultural risk analysis
 - Identifying physical and project risks
 - Defining safety metrics and performance audits
 - Designing and evaluating potential policy and structural improvements
 - Identifying leading indicators of increasing risk (“canary in the coal mine”)
- New holistic approaches to security

Does it Work? Is it Practical?

- MDA risk assessment of inadvertent launch (technical)
- Architectural trade studies for the space exploration initiative (technical)
 - Evaluated potential architectures with respect to safety
 - Preliminary hazard analysis without needing likelihood estimates (use mitigation potential instead)
- Safety–driven design of a NASA JPL spacecraft (technical)
- NASA Space Shuttle Operations (risk analysis of a new management structure)
- NASA Exploration Systems (risk management tradeoffs among safety, budget, schedule, performance in development of replacement for Shuttle)

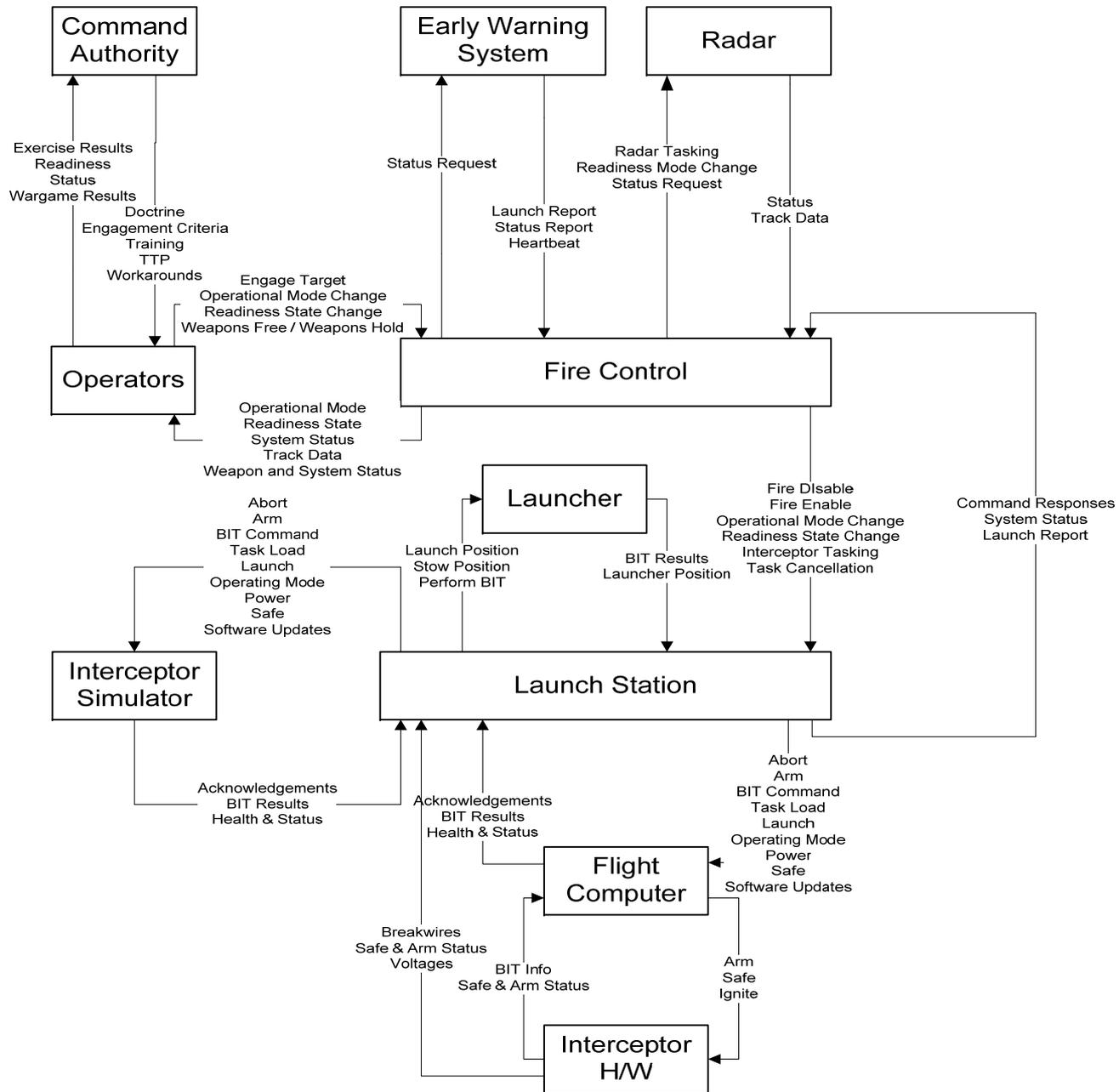
Does it Work? Is it Practical? (2)

- Accident analysis (spacecraft losses, bacterial contamination of water supply, aircraft collision, oil refinery explosion, train accident, chemical plant runaway reaction, etc.)
- Pharmaceutical safety
- Hospital safety (risks of outpatient surgery at Beth Israel MC)
- Corporate fraud (are controls adequate?, Sarbanes-Oxley)
- Food safety
- Train safety (Japan)

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)
- 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



Results

- Deployment and testing held up for 6 months because so many scenarios identified for inadvertent launch (the only hazard considered so far). 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.
- Adopted as primary safety approach for BMDS

Safety-driven Model-based System Engineering Methodology for an Outer Planets Explorer Spacecraft

- Top-down specification and analysis of a deep space exploration mission system with a “Deep Dive” into the area of communications antenna pointing
 - Like Europa Explorer, OPE has a High Gain Antenna (HGA) mounted on a deployable boom
 - Specification encompassed all aspects of the mission system (i.e., spacecraft, launch vehicle, ground network, etc.) to the extent that they informed the deep dive area
- System Goals derived from Europa Explorer Study
 - Generalized to any mission to explore an icy moon of an outer planet

Safety-Driven Design of an Outer Planets Explorer Spacecraft for JPL

- Demonstration:
 - Used intent specifications and SpecTRM tools
 - Defined mission hazards
 - Generated mission safety requirements and design constraints
 - Created spacecraft control structure and system design
 - Performed STPA and generated component safety requirements and design features to control hazards

<http://sunnyday.mit.edu/papers/IEEE-Aerospace.pdf>

(complete specifications also available)

SpecTRM (Specification Tools and Requirements Management)

- Based on intent specifications
- A “CATIA” for logical parts of the system
 - Requirements errors found early when easier to fix
 - Enhance communication and expert review
- Reusable component-based system architectures
 - Reuse of system engineering (not detailed design or code)
 - Capture and communication of design rationale
 - Complete traceability from requirements to design to code
 - Model-based development and executable specifications
 - Easy to read (takes about 10 minutes to learn)
 - Supports simulation-based acquisition

SpecTRM (2)

- Build safety into design from beginning
 - Integrate safety analysis into development environment
 - New more powerful forms of hazard analysis based on STAMP
- Tools
 - Specification generation tools
 - Model execution, animation, and visualization
 - Completeness and consistency analysis
 - Hazard analysis using STPA (in development)
 - Human task analysis
 - Test coverage (requirements)
 - Automatic code generation

Safeware Engineering Corp. <http://safeware-eng.com>

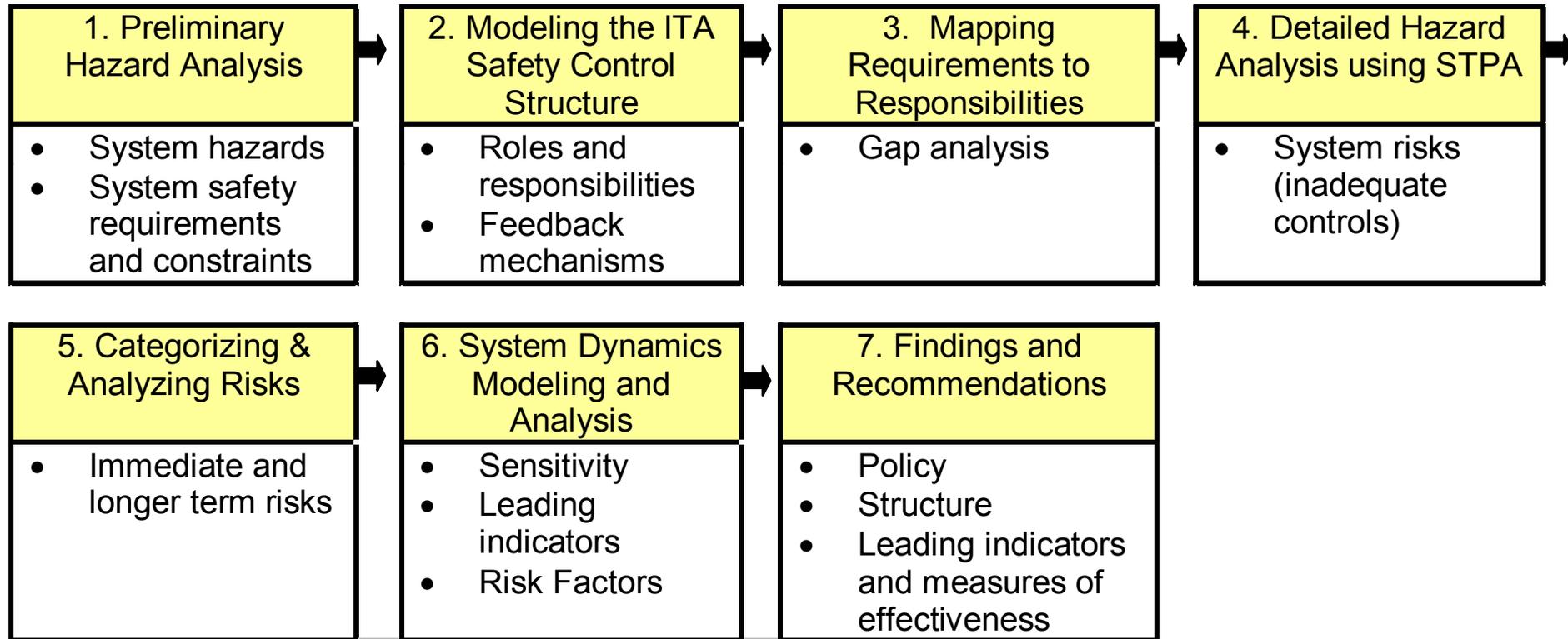
Cultural and Organizational Risk Analysis and Performance Monitoring

- Apply STAMP and STPA at organizational level plus system dynamics modeling and analysis
- Goals:
 - Evaluating and analyzing risk
 - Designing and validating improvements
 - Monitoring risk (“canary in the coal mine”)
Identifying leading indicators of increasing of unacceptable risk

NASA Space Shuttle Operations

- Risk analysis of a new management structure for safety-related decision making
 - Called ITA (Independent Technical Authority)
- Identified organizational (management) risks of new structure
- Identified leading indicators of increasing risk in the Space Shuttle program

The Process

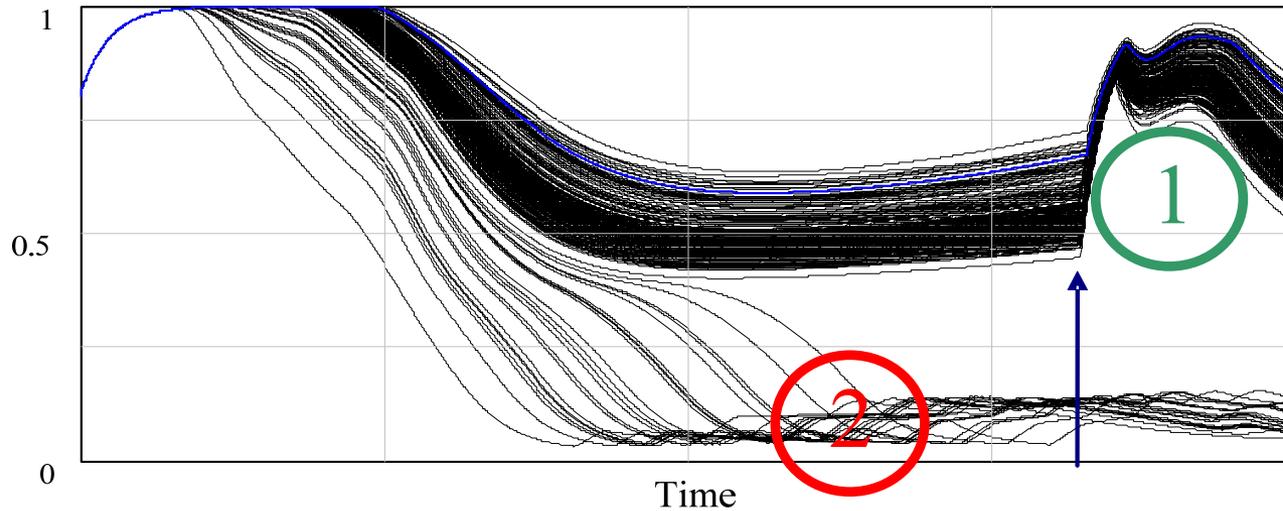


Example Result

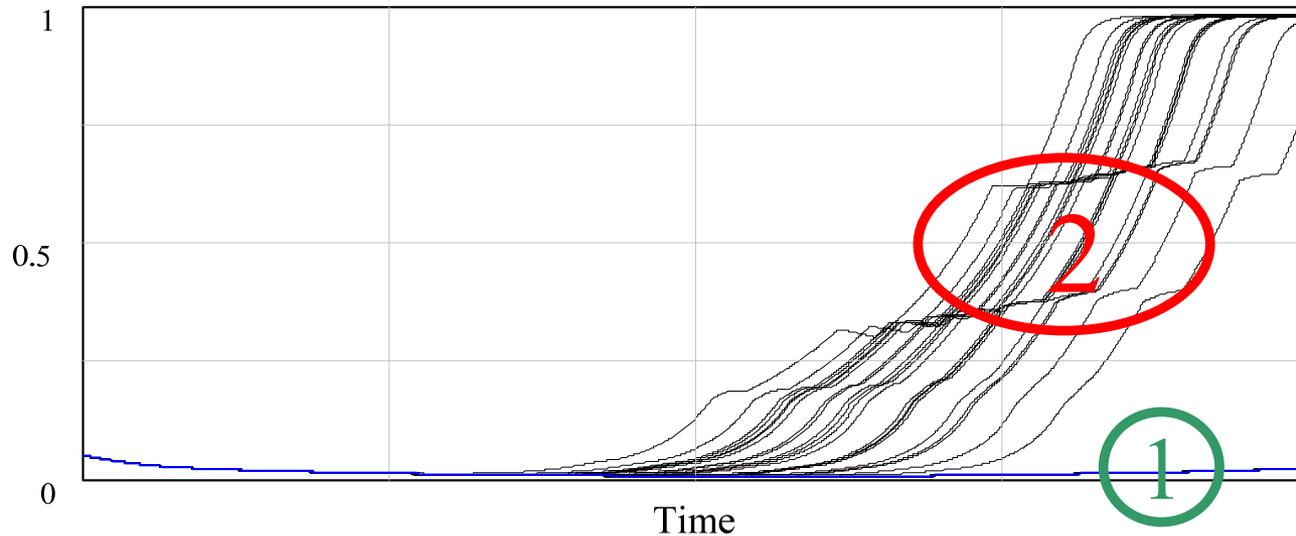
- ITA has potential to significantly reduce risk and to sustain an acceptable risk level
- But also found significant risk of unsuccessful implementation of ITA that needs to be monitored
 - 200-run Monte-Carlo sensitivity analysis
 - Random variations of +/- 30% of baseline exogenous parameter values

Successful vs. Unsuccessful ITA Implementation

Indicator of Effectiveness and Credibility of ITA

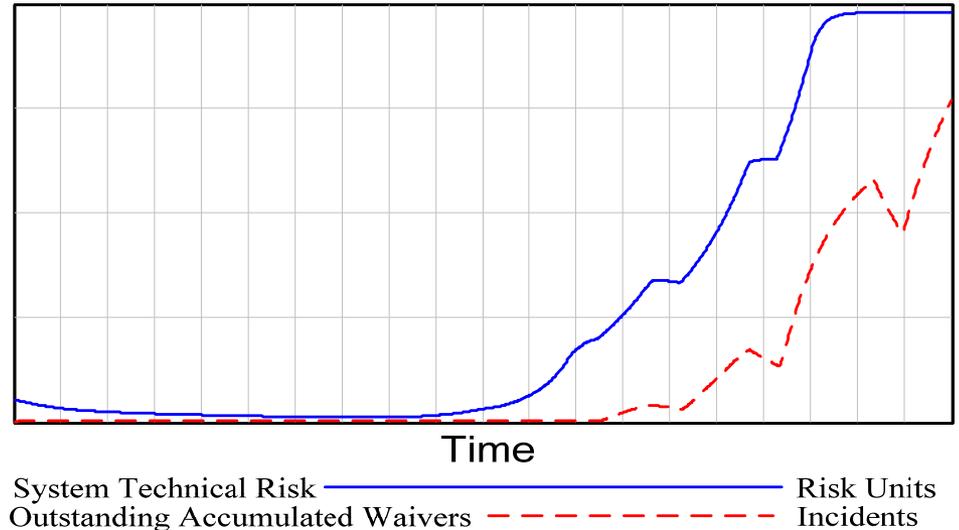


System Technical Risk

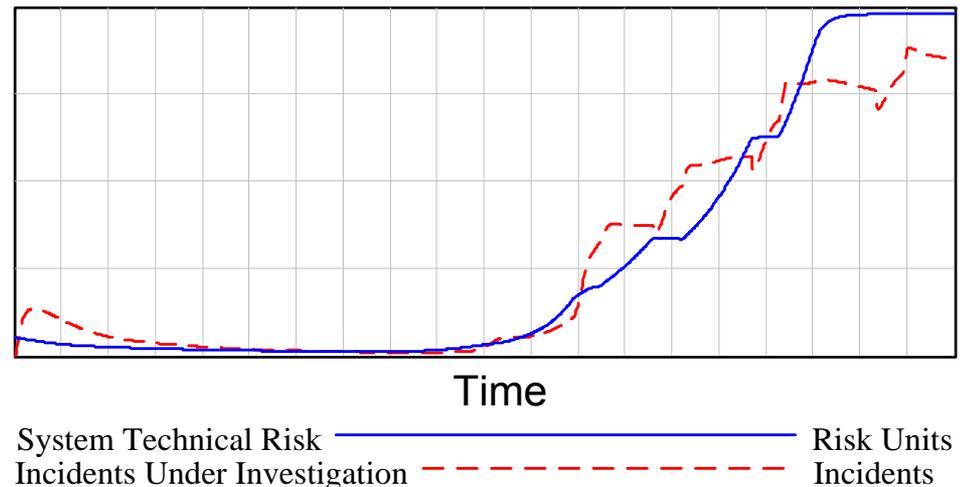


Identification of Lagging vs. Leading Indicators

- Number of waivers issued good indicator but lags rapid increase in risk



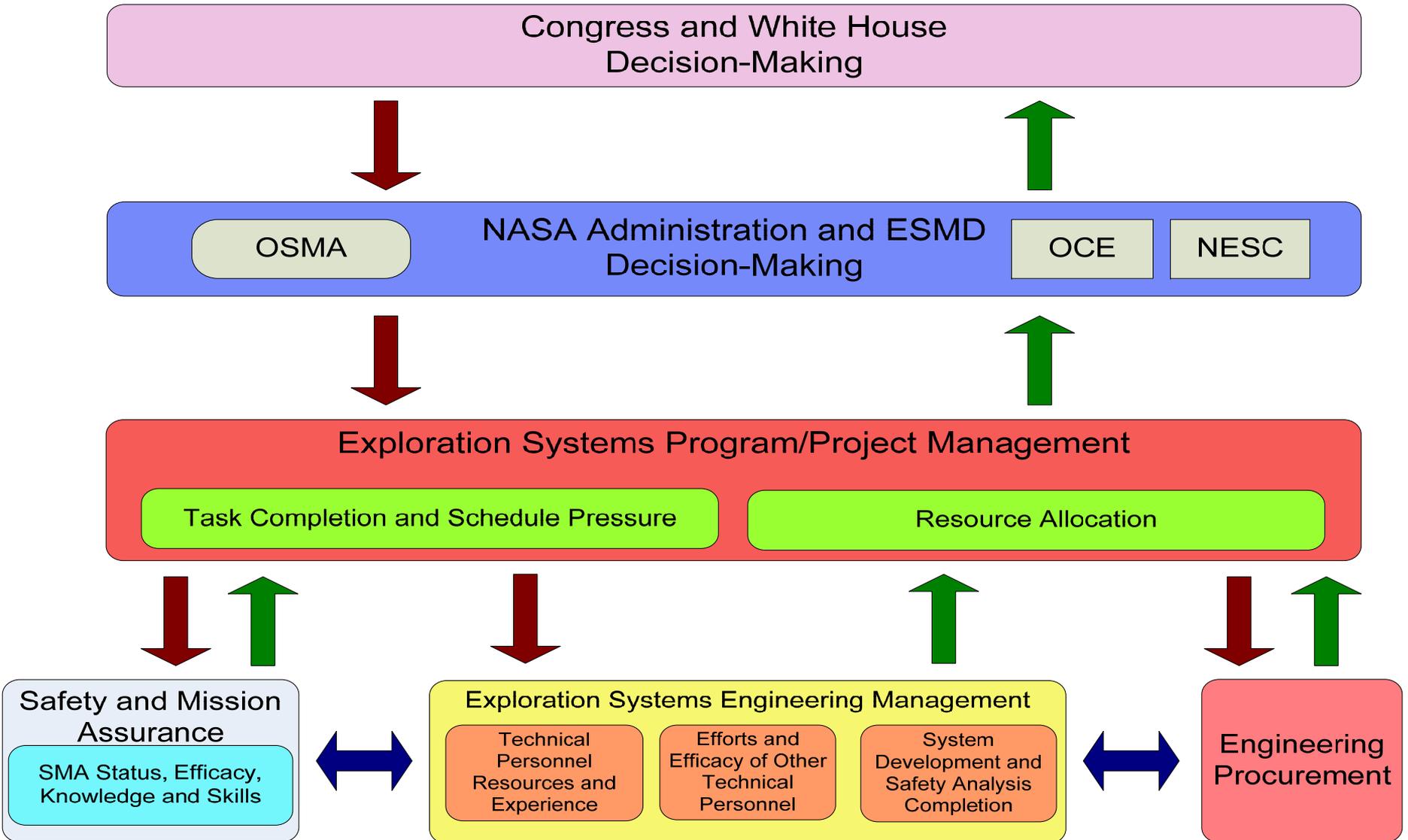
- Incidents under investigation is a better leading indicator



Risk Management in NASA's New Exploration Systems Mission Directorate

- Created an executable model, using input from the NASA workforce, to analyze relative effects of management strategies on schedule, cost, safety and performance risks
- Developed scenarios to analyze risks identified by the Agency's workforce
 - Performed preliminary analysis on the effects of hiring constraints, management reserves, independence of safety decision-making, requirements changes, etc.
- Derived preliminary recommendations to mitigate and monitor program-level risks

Structure of System Dynamics Model



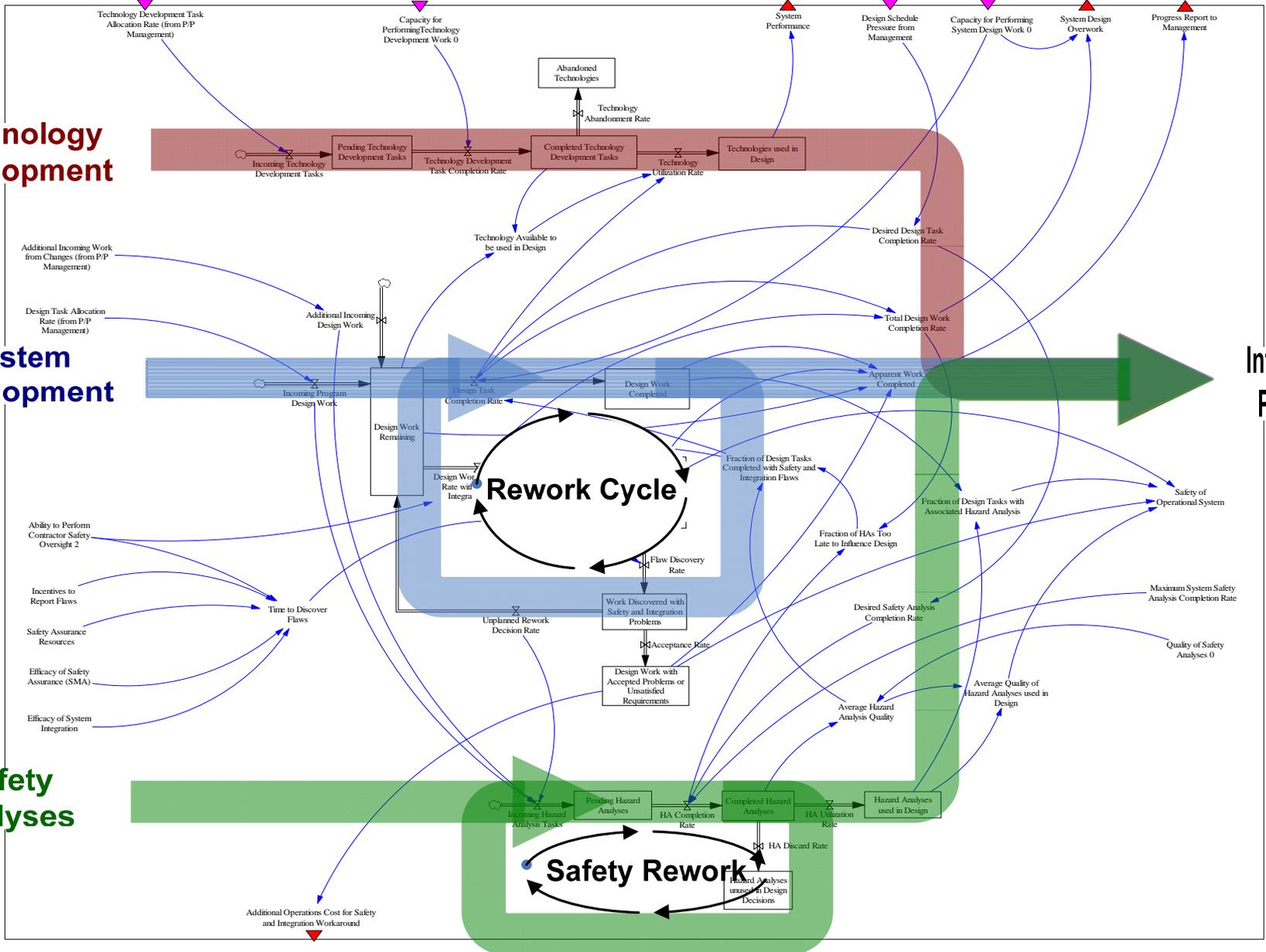
Engineering - System Development Completion and Safety Analyses

Technology Development

System Development

Safety Analyses

Integrated Product



NASA ESMD Workforce Planning

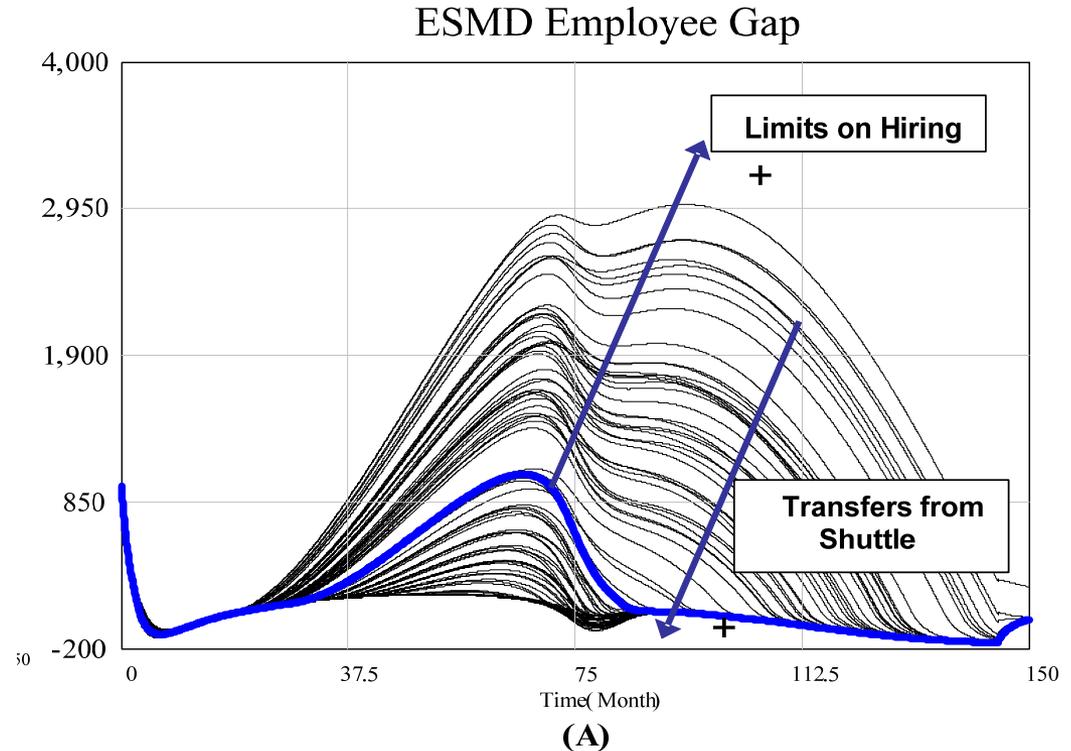
Important Issues:

- Increase in retirements
- Hiring limits
- Transfers

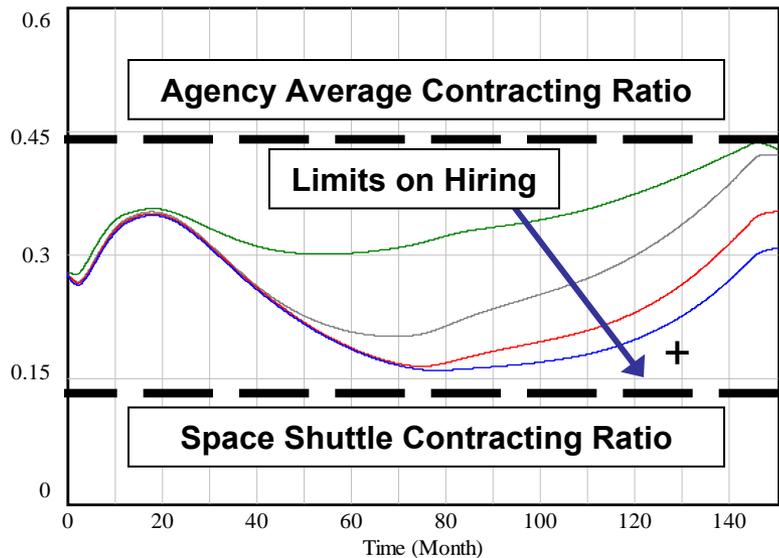
Simulation varied:

- Initial experience distribution of ESMD civil servant workforce
- Maximum civil servant hiring rates
- Transfers from Shuttle ops during Shuttle retirement

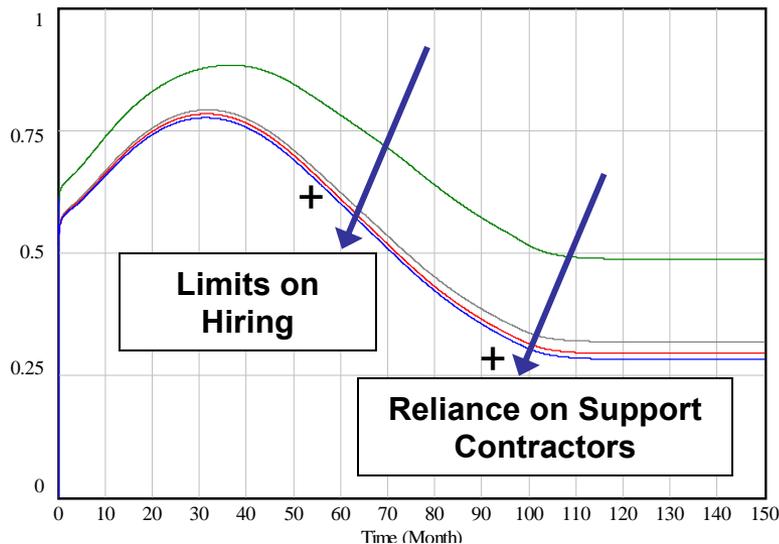
Must increase limits on hiring to finish by 2012



Productive NASA to Support Contractor Headcount Ratio



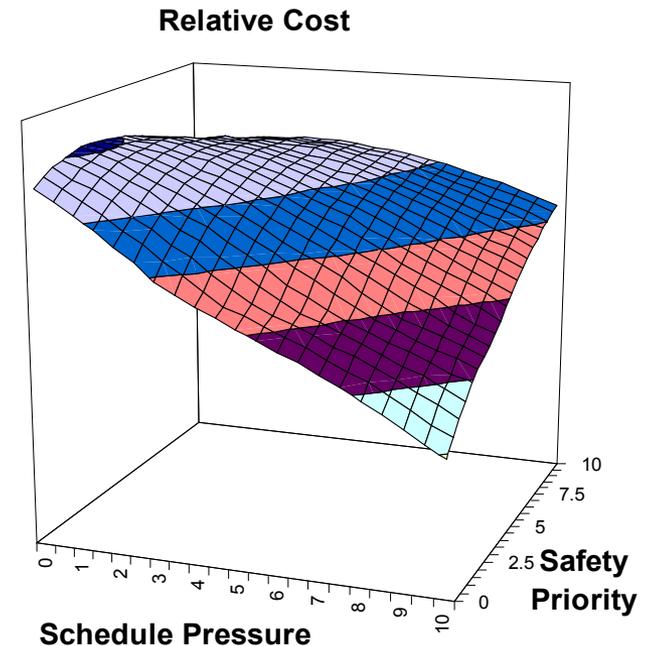
Safety of Operational System



- As reliance on support contractors increases, the ultimate safety of the operational system decreases
 - Difficulty of oversight increases and quality decreases
 - Will a small ratio of civil servants to contractors work in a development environment?

Example: Schedule Pressure and Safety Priority in Developing the Shuttle Replacement

1. Overly aggressive schedule enforcement has little effect on completion time (<2%) and cost, but has a large negative impact on safety
2. Priority of safety activities has a large positive impact, including a positive cost impact (less rework)



STAMP vs. Traditional Approaches

- More comprehensive view of causality
- A top-down system's approach to preventing losses
- Includes organizational, social, and cultural aspects of risk as well as physical
- Handles much more complex systems than traditional safety engineering approaches
- Considers dynamics and changes over time
- Includes software and human decision making and mental models

Some References

- Draft book at <http://sunnyday.mit.edu/book2.html>
- Papers at: <http://sunnyday.mit.edu>

Backup

Safety-Driven Model-Based System Engineering Methodology

Step 1: Identify Mission Goals, Requirements and Constraints.

G1 Characterize the presence of a subsurface ocean on an icy moon of an outer planet. (→HLR3, HLR4)

G2 Characterize the three-dimensional configuration of the icy crust of the icy moon of an outer planet, including possible zones of liquid. (→HLR1, HLR2, HLR3)

G3 Map organic and inorganic surface compositions of the icy moon of an outer planet, especially as related to astrobiology (Clark, 2007). (→HLR2, HLR3)

- G4. Characterize surface features of the icy moon of an outer planet and identify candidate sites for future exploration (Clark, 2007). (→HLR1, HLR2, HLR3)
- G5. Characterize the magnetic field and radiation environment of the icy moon of an outer planet (Clark, 2007). (→HLR4, HLR5)
- G6. Understand the heat source(s) and time history of any ocean that may exist on the icy moon of an outer planet (Clark, 2007). (→HLR2, HLR3)

Mission-Level Requirements

HLR1. The mission shall image TBD% of the surface of the icy moon of the outer planet in the visual spectrum to a resolution of TBD meters. (←G2, G4), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1)

Rationale: Visual data of this resolution will is necessary for characterization of icy crust and identification of candidate sites for exploration.

HLR2. The mission shall image TBD% of the surface of the icy moon of the outer planet moon in the infrared spectrum to a resolution of TBD. (←G2, G3, G4, G6), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1)

Rationale: The infrared radiation emitted by a mass is a function of its temperature and thermal properties. Thus, imaging the IR spectrum of surface provides insights into the physical composition of the icy moon's surface and the location of heat sources.

HLR3. The mission shall image TBD% of the surface of the icy moon of the outer planet in spectra other than visual and infrared, to a resolution of TBD. (←[G1](#), [G2](#), [G3](#), [G4](#), [G6](#)), (→[S/C-G1](#), [S/C-G2](#), [S/C-R1](#), [S/C-R2](#)), (↓[2.1](#))

Rationale: The other bands of the spectrum provide insights into the chemical composition of the icy moon

HLR4. The mission shall measure the magnetic field surrounding TBD% of the icy moon of the outer planet (altitude TBD to altitude TBD). (←[G1](#), [G5](#)), (→[S/C-G1](#), [S/C-G2](#), [S/C-R1](#), [S/C-R2](#)), (↓[2.1](#))

Rationale: These measurements are necessary to characterize the magnetic field of the icy moon of the outer planet. An understanding of this field provides insights in the physical composition of the moon, including the possible existence of an ocean.

HLR5. The mission shall measure the flux of radiation particles of energy levels TBD MeV to TBD MeV in TBD% of the space surrounding the icy moon of the outer planet (altitude TBD to altitude TBD). (←[G5](#)), (→[S/C-G1](#), [S/C-G2](#), [S/C-R1](#), [S/C-R2](#)), (↓[2.1](#))

Rationale: These measurements are necessary to characterize the radiation environment of the icy moon of the outer planet.

Step 2: Define System Accidents or Unacceptable Losses

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)

Step 3: Define mission hazards.

- 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)

Step 4: Define mission-level safety-related constraints:

SC1. The mission must have the necessary functionality for data acquisition at the required times. (\leftarrow H1) (\downarrow 2.1, 2.2, 2.4)

SC2. The mission must be able to return data at the required times. (\leftarrow H2) (\downarrow 2.1, 2.3, 2.4, 2.5)

SC3. Mission scientific investigators must be able to use the data collected throughout the mission at the required times. (\rightarrow H3) (\downarrow 2.1, 2.3, 2.4, 2.5)

SC4. All physical elements of the mission must not unintentionally move along a collision course with an outer planet moon. (\leftarrow H4), (\downarrow 2.1, 2.4)

SC5. All physical elements of the mission that intentionally collide with an outer planet moon must be sterile. (←H4), (↓2.1, 2.4)

SC6. All physical elements of the mission must not unintentionally move along a collision course with Earth. (←H5, H7), (↓2.1, 2.2, 2.4)

SC7 All physical elements of the mission that intentionally collide with the Earth must not cause damage to humans or human assets. (←H5, H7), (↓2.1, 2.2, 2.4)

SC8. All physical elements of the mission must not unintentionally move along a collision course with humans or human assets that are off of Earth (e.g., International Space Station). (←H6, H7), (↓2.1, 2.2, 2.4)

SC9. The Mission must not deny usage of shared space exploration infrastructure to another mission if such a denial would jeopardize that mission's goals (This constraint does not necessarily apply if the Mission's goals are similarly or more severely jeopardized). (←H7), (↓2.1, 2.2, 2.3, 2.4, 2.5)

Step 5: Identify

Environmental constraints and environmental assumption

EA.1 The translation and rotation of the object of study with respect to the Sun and relevant outer planet will be relatively stable over the mission and thus predictable

Customer-derived system design constraints

DC1. The mission must be carried out with existing technologies and space exploration infrastructures as needed (i.e., technologies rated at Technology Readiness Level TBD as defined by NASA). (↓2.1)

Rationale: While technology development is expected to be an ongoing activity of NASA, it is assumed to be beyond the mandate of the mission

Customer programmatic constraints (e.g., budgets, etc.)

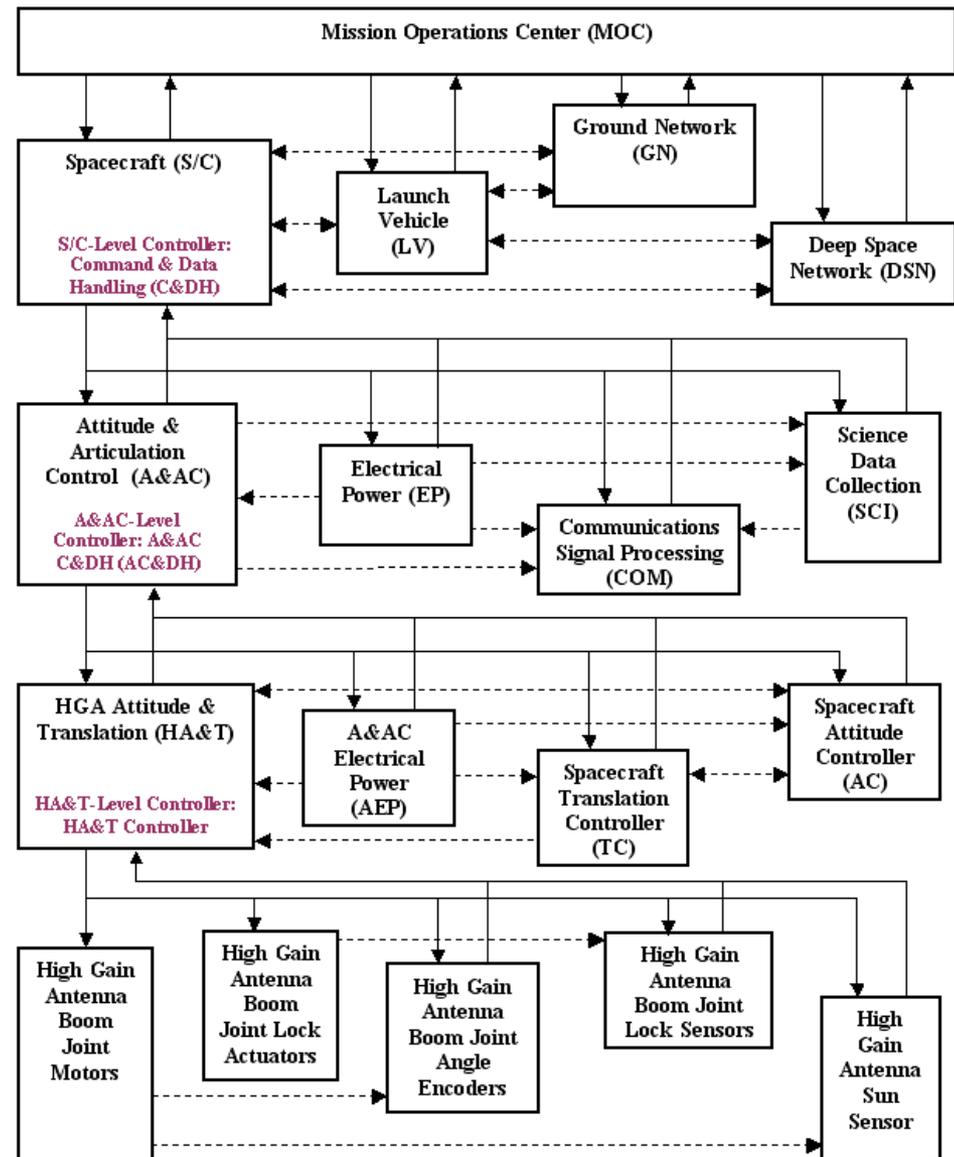
Step 6: Perform a functional decomposition

Key	
Command & Data Handling (C&DH)	
Electrical Power (EP)	
Attitude & Articulation Control (A&AC)	
Science Data Collection (SCI)	
Communications Signal Processing (COM)	

Name		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Spacecraft MOC Directive Execution	1	1	1	1						1											
Spacecraft MOC Directive Storage	2		2							1											1
Spacecraft H&S Data Evaluation	3			3	1		1			1											
Spacecraft H&S Data Collection	4	1			4					1											
Spacecraft H&S Data Storage	5	1		1	1	5				1											
Spacecraft H&S Data Retrieval from Storage	6	1				1	6			1											
Spacecraft H&S Data Packetization	7	1					1	7		1											
Spacecraft Power Generation	8	1							8												
Spacecraft Power Distribution	9	1							1	9											
Spacecraft Translation	10	1							1		10	1									
Spacecraft Pointing	11	1							1		1	11	1	1							
Spacecraft Antenna Deployment	12	1							1				12								
Spacecraft Antenna Pointing	13	1							1		1	1	1	13							
Spacecraft Science Data Collection	14	1							1		1	1			14						
Spacecraft Science Data Storage	15	1							1						1	15					
Spacecraft Science Data Retrieval from Storage	16	1							1						1	16					
Spacecraft Science Data Packetization	17	1							1								1	17			
Spacecraft Data Modulation	18	1						1	1									1	18		
Spacecraft MOC Directive Demodulation	19	1							1											1	19
RF Transmission/Reception of Data	20													1	1					1	20

Step 7: Design High-Level System Control Structure

Control Structure Legend	
Diagram Item:	Description:
↓	Control in the form of Directive(s) or Command(s)
↑	Control Feedback in the form of State Information or Sensor Measurements
-----> <----- <----->	Physical and Informational Interaction other than Control and Control Feedback Interactions
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> Functional Element Name Functional Element-Level Controller (if applicable) </div>	Functional Element with the controller of its internal interactions (i.e., the functional element-level interactions)



Step 8: Perform STPA

Identify inadequate control actions

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.

Identify associated safety-related requirements and design constraints along with design decisions to eliminate or control the hazardous control actions

Inadequate Control Actions, Control Flaws, and Inadequate Executions of Control Actions	Relevant High-Level Hazard(s)	Associated Design Decision	Resulting Safety Constraint(s) or Requirements
C&DH-ICA1. The C&DH executes and/or delegates MOC Directives that are wrong.	H1, H2, H4, H5, H6, H7	C&DH-2.1	
C&DH-CF1.1. A change in the state of the spacecraft or spacecraft environment that invalidates assumptions of directives occurs during the time delay between DSN transmittal of the directives and S/C reception of directives.			C&DH-SC1
C&DH-ICA2. The C&DH does not receive an initial set of MOC Directives and/or updates.	H1, H2, H4, H5, H6, H7	C&DH-2.1	
C&DH-CF2.1. The C&DH does not initiate the proper functionality for reception of MOC Directives.			C&DH-SC2

Step 9: Define System Component Specifications:

Define Goals, Requirements, Design Constraints and Safety Constraints for each subsystem or functional component at level 1.

Level 1.1.3: Spacecraft Attitude and Articulation Control (A&AC) Goals, Requirements, and Constraints

Spacecraft Attitude and Articulation Control (A&AC) Goals

A&AC-G1. To provide the spacecraft velocity changes necessary for orbit insertion about the icy moon of the outer planet, maintenance of/changes to that orbit, and spacecraft disposal. (←S/C-R1)

Spacecraft Attitude and Articulation Control (A&AC) Assumptions

A&AC-A1. Telescoping boom segments for the HGA are not practical for this mission. (↓A&AC-2.2.1)

Rationale: *While this assumption is largely a simplifying assumption, the complexity associated with telescoping boom segments for an object as massive as the HGA would warrant a trade study beyond the scope of this study if they were to be considered.*

Spacecraft Attitude and Articulation Control (A&AC) Requirements

A&AC-R1. After release from the launch vehicle, the A&AC shall provide spacecraft velocity changes for spacecraft transit from the release point to the orbit of the outer planet. (←A&AC-G1)

Make design decisions at level 2 to implement the requirements and constraints

A&AC-2.4. A HGA Attitude and Translation (HA&T) Control functional element is used for feedback control of the joint rotations necessary for HGA rotation and translation.

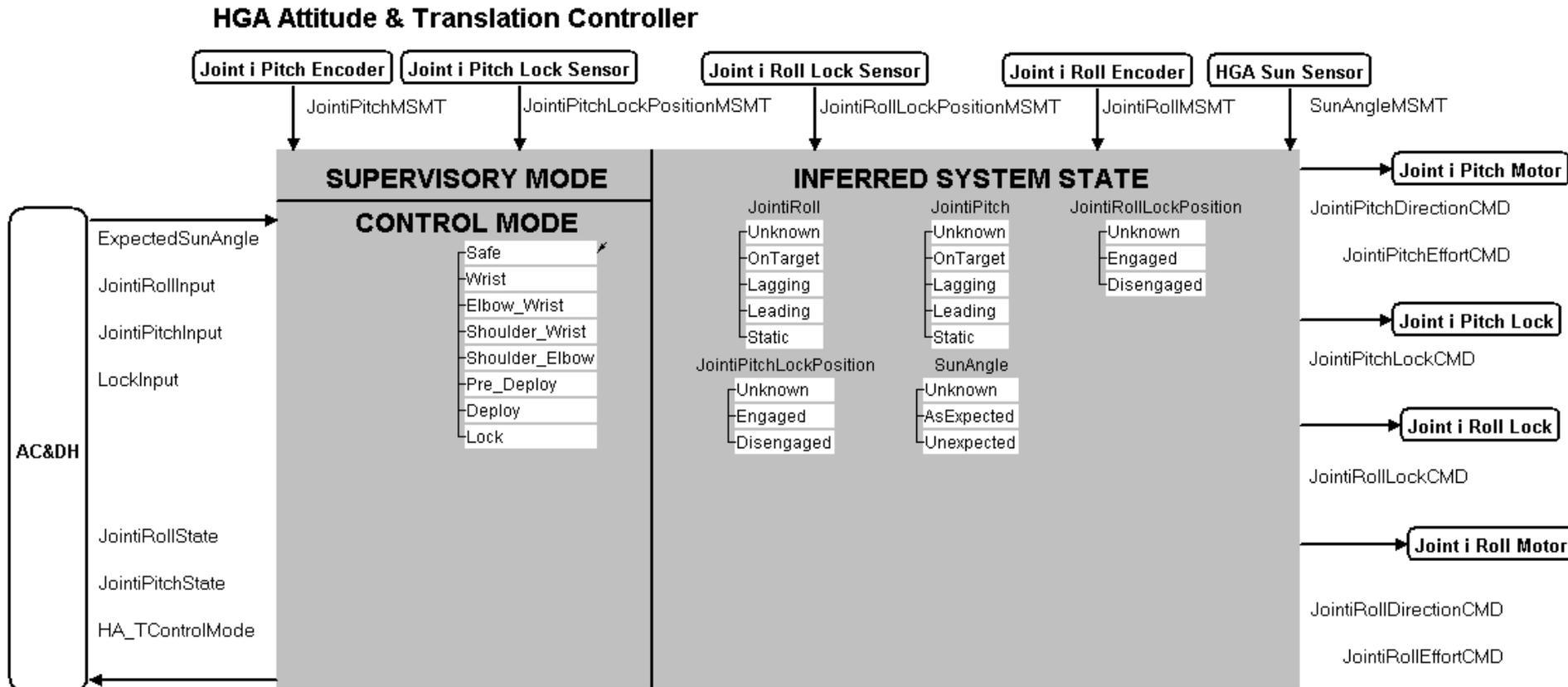
(←A&AC-2.1, A&AC-2.2), (↑A&AC-SC1, A&AC-SC2, A&AC-SC3, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC8, A&AC-SC10, A&AC-SC12, A&AC-SC14, A&AC-SC15, A&AC-SC16), (→HA&T-2.1), (↓AC&DH-G1, HA&T-G1, HA&T-G2, HA&T-G3)

Rationale: HGA restraint, rotation, and translation are coupled heavily due to the multiple boom segment architecture.

A&AC-2.5. A Spacecraft Attitude Controller (AC) functional element is used for feedback control of spacecraft pointing.

(↑A&AC-R6, A&AC-SC15), (↓AC&DH-G1)

Create Control System design at level 3.



Formally specify (model) control system design

DEFINITION

= New Data for WristRollLockPositionMSMT

WristRollLockPositionMSMT was Received		T
--	--	---

= Previous Value of WristRollLockPositionMSMT

WristRollLockPositionMSMT was Received		F
Time Since WristRollLockPositionMSMT was Last Received \leq TBD seconds		T

= Obsolete

System Start	T	*	*
WristRollLockPositionMSMT was Never Received	T	T	*
Time Since WristRollLockPositionMSMT was Last Received $>$ TBD seconds	*	*	T

= Ready to Take Image

<u>Target</u> in state Moon	T	F
<u>Illumination-Valid</u>	*	T
<u>Filter Wheel-Valid</u>	T	T
<u>Power</u> in state Powered	T	T
<u>Data-Storage Capacity</u> in state Above Threshold	*	F

Continue to perform STPA

A&AC-ICA1. The HGA rotates relative to the spacecraft at the wrong time. (←S/C-SC1, S/C-SC2, S/C-SC5, S/C-SC7)

A&AC-CF1.1. The HGA rotates relative to the spacecraft while the spacecraft is within the payload fairing.

Rationale: Because space is constrained within the payload fairing, articulation of the HGA relative to the spacecraft could cause damage to the HGA, launch vehicle, and/or other parts of the spacecraft. The effects of such damage could range from degradation in HGA functionality to partial breakup of the spacecraft and launch vehicle.

Iterate over steps 9.1 – 9.4 until design is set and all hazards are eliminated, mitigated or controlled.

- May result in changes to any part of intent specification.

Step 10: Perform validation tests

Step 11: Generate designs and software code