Dynamic Safety and Risk Management in Complex Socio-Technical Systems

Nik Dulac
ndulac@mit.edu
MIT-Albany SD Colloquium

April 29th, 2005
Massachusetts Institute of Technology
Cambridge, Ma
Outline

• Motivation
• Problem Statement
• Traditional Approaches and Background
• Core Hypothesis
• Research Approach
• Conclusion and Applications
• Q&A
“The foam debris hit was not the single cause of the Columbia accident, just as the failure of the joint seal that permitted O-ring erosion was not the single cause of Challenger. Both Columbia and Challenger were lost also because of the failure of NASA’s organizational system.”

CAIB, p. 195
Problem Statement

• Many accidents in complex socio-technical systems result from a migration of the system to a state of high risk.
• Once this high-risk state is reached any number of minor triggers could lead to a major loss.

Current approaches to safety and risk analysis do not capture the dynamics of complex socio-technical systems and therefore do not consider this migration toward accidents.
Traditional Approaches

• Traditional approaches to risk analysis focus on failure events in static engineering system designs
  – Failure events are arranged into chains or trees linked together by direct relationships (e.g. FTA, FMEA, PRA, etc.)
  – Explain accidents in terms of multiple events, sequenced as a forward chain over time

• They were created for mechanical systems and later extended to electro-mechanical systems
  – Inadequate for software-intensive SoS that require complex, distributed human decision-making and human-automation interaction
Traditional Approaches (Cont.)

- These approaches are not suited to handle:
  - Social, organizational and cultural factors
  - System accidents resulting from unexpected interactions between system components
  - Software-related accidents where nothing “fails”
  - Human error, because human behavior cannot be decomposed and studied in isolation from its physical and social context
  - Adaptation involving a systematic migration toward higher levels of risk
Key Research Drivers

• Safety is an emergent system property
  – Cannot be understood by studying components in isolation

• Complex socio-technical systems are dynamic
  – Continually adapt to achieve goals while reacting to changes

• Focusing on the “single” proximal cause does not address how the system as a whole may allow an accident
  – Contributions of software and human decision-making
  – Management flaws and safety culture

We need a more powerful model of accident causation that handles those factors and includes the entire socio-technical system.
Core Hypothesis

Safety decision making and dynamics can be modeled, analyzed and engineered like physical systems

- A new dynamic risk management system can be created by combining:
  - STAMP Accident Causation Model
  - System Dynamics Concepts
- These two theoretical foundations have much in common:
  - Consider systems as dynamic and continually adapting
  - Built upon non-linear feedback control theory
  - Recognize the limitations of decision-makers
  - Recognize the importance of physical and social context in decision-making
STAMP Accident Model

• STAMP
  – Systems Theoretic Accident Model and Process
• STAMP defines an accident as the result of control actions inadequately enforcing constraints on the system design or operation
  – System safety goals achieved if safety constraints are continuously enforced throughout the system lifecycle
• Describes each level of the socio-technical structure of a system in terms of levels of control over safety
• Systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control
• The process leading up to an accident can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values
Three types of models are required:

1. **Static safety control structure**
   - Safety requirement and constraint
   - Required control action
   - Context (social, cultural, political, etc.)
   - Mental model requirements
   - Coordination requirements

2. **Structural dynamics**
   - How the static safety control structure changes over time

3. **Behavioral dynamics**
   - Dynamic processes behind the changes (i.e., why the system changes)
System Dynamics Concepts

- System Dynamics
  - Created at MIT in the 1950s by Jay Forrester
  - Grounded in the theory of non-linear dynamics and feedback control
  - Also cognitive and social psychology, organization theory, economics, and other social sciences
  - Provides a framework for dealing with dynamic complexity, where cause and effect are not obviously related
  - Decisions that might appear to have no effect (or positive effect) on safety may in fact degrade safety and increase risk
Dynamic Hypothesis

Resource Pressure → Safety Resources

"Do More with Less"

Safety Priority

System Safety Efficacy

"Problems have been Fixed"

Complacency

Performance Pressure → Expectations

"Limits to Success"

B2

NASA Success

Launch Rate

Perceived Success

B3

Incidents and Accidents

Safety of Shuttle Program
Dynamic Hypothesis (Cont.)

- Insights from Dynamic Hypothesis
  - System structure creates oscillations
  - Risk is allowed to creep up unseen when the program is successful
  - Safety should be looked upon carefully especially when everything seems to be going fine (when success has a strong positive slope)
Research Objective

- Augment STAMP with a dynamic risk management system to achieve three major objectives:
  1. Improve **foresight** ability of decision-makers by increasing the visibility of unintended side-effects
  2. Improve system safety **monitoring** to detect and prevent states of high-risk (Canary-in-the-mine function)
  3. Allow the design and testing of policies to improve the system **robustness** and tolerance to “safety drift”
1. Foresight

- Safety is a non-event
  - Nobody gets credit for delaying a flight because of safety reasons
- Safety often gets a second role when decisions made under high performance and schedule pressure
- It is difficult to predict what will happen in the future, but it is possible to improve the mental models of decision-makers to make them more aware and responsive
- Need to provide decision-makers with tools to improve the visibility of potential unintended effects of decisions
  - Also provides justification to support safety-related decisions under pressure
2. Monitoring

• Canary-in-the-Mine function
  – Alerting decision-makers that the system has reached, or is heading toward an unsafe state

• In many complex systems, large amounts of data is collected to monitor and regulate system health

• Need to identify which metrics are good indicators of the system heading toward a state of high-risk
  – Dynamic risk management system can help focus the search for meaningful metrics

• Once identified, figure out “metrics dynamics”
  – What dynamic patterns indicate an increase in risk
2. Monitoring (Cont.)

- Waiver Dynamics at NASA
  - A waiver is a formalized procedure that, upon approval of the technical rationale behind the request, allows an exception to some internal rule
  - **Waiver used as a pressure valve to keep flying**
  - 3,222 criticality 1/1R items had waivers at the time of Columbia
  - Understanding the “metrics dynamics” provides hints on what patterns to watch for

Capability Trap adapted from Repenning, Sterman, and later, Marais
3. Robustness

- Dynamic STAMP-based risk management models can provide a test bed for creating and testing inherently robust systems and policies.
- Can be used on existing systems, or to evaluate entirely new safety control structures such as that of the Space Exploration Enterprise.
  - Help identify vulnerabilities and design-in robustness from the very beginning of the system lifecycle.
- Overall objective is to design and test systems and policies that will enhance robustness against safety erosion.
  - Through passive “structural” robustness (anticipation).
  - Through active compensation for safety erosion (resilience).
Current Work

- Preliminary model used to study safety decision-making at NASA
- Created based on interactions and work with Columbia Group
Current Work (Cont.)

- Accidents create a temporary priority inversion

- After accidents, there is temporary attention to systemic problems

- This attempt to fix systemic problems is short-lived and has little effect on risk
Current Work (Cont.)

- Scenario 1: Effect of fixing systemic factors vs. fixing problem symptoms
- Scenario 2: Effects of Independent Technical Authority
- Scenario 3: Effects of different levels of contracting
Conclusion

• A new accident model introduces the possibility of more powerful hazard analysis techniques that include software, human decision-making, etc.

• Proposed Dynamic Risk Management System can help achieving three objectives:
  – Improve **foresight** ability of decision-makers
  – Improve risk **monitoring** (Canary-in-the-mine)
  – Improve the system **robustness** to “safety drift”
Projects and Applications

- The research was recently funded by NASA’s Center for Project Management Research (CPMR)
- Currently working with NASA’s Chief Engineer Office to perform a risk analysis for the implementation of the Independent Technical Authority
- Identified candidate projects for field studies and applications: LMA (Atlas and Exploration CER)
Backup Slides
Example Safety Control Structure

- ACES
- Ministry of Health
- BGOS Medical Dept. of Health
- Public Health
- Water System
- Ministry of the Environment
- Walkerton PUC Operations
- Government Testing Labs
- Well 7: Design flaw: No chlorinator
- Well 5: Design flaw: Shallow location
- WPUC Commissioners
- Walkerton Residents
- Private Testing Labs
- Federal, Guid.

Flow of information:
- Reports from ACES to Ministry of Health
- MOE inspection reports to BGOS Medical Dept. of Health
- Guidelines from Ministry of Health to BGOS Medical Dept. of Health
- Hospital reports, input from medical community to Public Health
- Water samples from Government Testing Labs to Walkerton PUC Operations
- Water samples from Water System to Walkerton PUC Operations
- Chlorine residual measurement from Walkerton PUC Operations to Water System
- Approval from Walkerton PUC Operations to Ministry of the Environment
- Operator cert. oversight from Ministry of the Environment to WPUC Commissioners
- Financial Info from Ministry of the Environment to WPUC Commissioners
- Policies, budget from WPUC Commissioners to Walkerton Residents
- Chlorination well selection from Walkerton PUC Operations to Well 7
- No chlorinator from Well 7 to Walkerton Residents
- Minimal overburden Heavy Rains from Farm to Well 5
- Porous Bedrock from Farm to Well 5

11/3/2005
MIT Aero/Astro 27
**Scenario A:** Degree of Independence of Safety Oversight Lever

**Scenario B:** Type of Learning Lever

**Scenario C:** Amount of Contracting Lever

**Scenario D:** Accidents cannot happen lever

**Turn off scenarios**

**Scenario Control Panel**

**<System Technical Risk>**

**<Launch Rate>**
Resource Allocation Model

- Schedule Pressure
- External Performance Pressure Index
- Perceived priority of performance
- Allocation Index
- Schedule Pressure Value
- Perceived priority of safety
- Independent External Safety Pressure Index
- Effect of past success on system safety priority
- Perceived success value
- Perceived success in isolation
- Desired fraction of Nasa Funds allocated to safety
- Baseline safety fund allocation
- Allocation gap
- Change in fraction allocated
- Time to adjust allocation fraction
- Minimum safety fund allocation
- Total Nasa Funds Budgeted
- Allocated safety funds
- Gap in safety funds
- Change in safety resources
- Ratio of Available System Safety Resources
- Required Safety Resources
- Required Fraction of Funds Allocated to Safety
- Expectations Index in Isolation
- Expectations Index Value 1
- Perceived Success Index
- Resource Allocation Model
Perceived Success by High-Level Management

Table for Effect of Success on Expectations

Expected Success

Perceived Success Index

Launch Failure Rate

Successful Launch Rate

Launch Success Contribution

Initial Success

Fractional Failure Rate

Accident Occurring

Consecutive launches without an accident

Drainage

Time Step

Months since last accident occurred

Time Drainage

Increase per time period

Time

Isolate Perceived Success Model

Launch Rate

Launch Rate Value (1)

Launch Rate in Isolation (1)

Accidents cannot happen
The Launch Rate Commitments is influenced by various types of pressure including performance pressure from the “Pushing the Limit” loop and external factors such as ISS commitments, Hubble Servicing Requirements, and other Scientific Missions Constraints.
System Safety Status Model

- Perceived Success by Administration in Isolation
  - <Perceived Success Index>
  - <Isolate Safety Status Model>
- Perceived Success by Administration Index Value
- Effect of perceived success on management priority of System Safety Efforts
- Management's Priority of System Safety Efforts
- Normal Respect of System Safety Efforts
- Assignment of High-Level Personnel and Leaders to System Safety
- Rewards and Recognition (promotions, money, glory)
- Priority of Resource Allocation to System Safety
- Power & Authority of Safety Organization
- Effect of Reward and Recognition on Status
- Effect of Power and Authority of Safety Organization on Status
- Effect of degree of independence of safety oversight
- Effect of degree of independence of safety oversight
- Table for effect of degree of independence of safety oversight
- Table for Effect of R&R on Status
- Table for Effect of Perceived Success on Management priority of System Safety Efforts
- Table for Effect of P&A on Status
- Table for Effect of R&R on Status
- Table for Effect of Leaders on Status
- Effect of Power and Authority of Safety Organization on Status
- Table for Effect of Perceived Success on Management priority of System Safety Efforts
- Effect of independence of safety leaders effectiveness
- Table for effect of leader effectiveness
- Effect of independence of safety leaders effectiveness
- Effect of High-Level Personnel and Leaders on Safety Status
- Effect of Safety Resource on Status
- Table for Effect of Safety Resource on Status
- Table for Effect of Power and Authority of Safety Organization on Status
- Status of Safety Organization
- Ability to Attract Quality People
- Level of Morale and Motivation
- Table for Effect of Power and Authority of Safety Organization on Status
- Table for Effect of Safety Resource on Status
- Normal Status of Safety Organization
- Perceived Success by Administration Index Value
- organizational response to safety behavior
- <Degree of Independence of Safety Oversight>
- Table for effect of degree of independence of safety oversight
- System Safety Status Model
Expected Contributions

• STAMP-Based Dynamic risk management methodology and tool
  – Improves **foresight** and decision-making
  – Improves safety and risk **monitoring**
  – Improves system **robustness** to safety erosion

• Research will include the development and evaluation of risk simulation tools to be used by engineers and decision-makers at LMA
Conclusion

• First steps taken to create a comprehensive STAMP-based dynamic risk management system
• Detailed methodology will be developed and applied in industry in the fall
• Research will include risk simulation tools to be used by engineers and decision-makers at LMA