New Applications of STAMP: Workplace safety, Engineering Management, Leading Indicators

Nancy Leveson

MIT

Three Topics

- Applying STPA to Other Emergent Properties
- Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development

  Allen Ball, Boeing

- Applying STAMP in Workplace Safety:

  Nancy Leveson (MIT)

  Lori Smith (Boeing)

  Emily Howard (Boeing)

  Larry Hettinger (Liberty Mutual Research Institute for Safety)

A "System Engineering" Process

1. Identify emergent property "X" you are trying to improve
2. Do "research" to understand the problem
   a. Why is "X" not as good as desired?
   b. Can use interviews, team-based inquiry, surveys, etc.
   c. Look at past "incidents," "X" quality escapes in the past, etc.
3. Analyze "organizational culture (values)"
   – What are current cultural values?
   – What are the values you want decision making to be based on in the future?
   – What changes are needed?
4. Create requirements to achieve the desired culture

A “System Engineering” Process (2)

5. Create the “X” organizational control structure
   - Review by stakeholders and people involved
   - Are there obvious weaknesses, e.g., missing feedback?

6. Map the requirements to the control structure:
   - Where are they supposedly being enforced? Are there gaps?
   - What parts of the control structure are contributing to the problems? Why are the current controls not effective?
   - What needs to be changed to improve “X”?
   - Again, get stakeholders and experts involved

7. Identify potential “hazards”, inadequate control actions, and causes of inadequate control

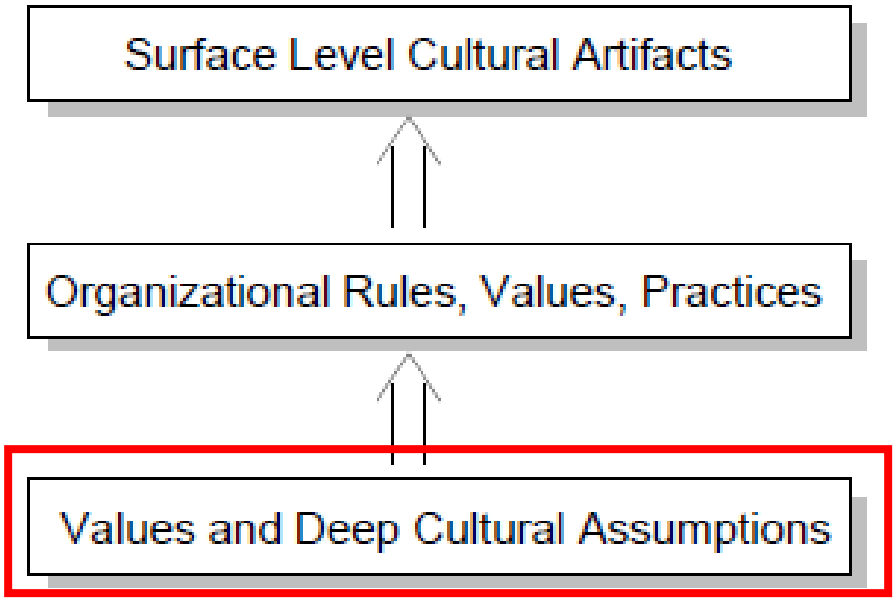
8. Create recommendations

Abbreviated Example

- X is product quality and timeliness
- Understand the problem: examples
  - Start design without understanding requirements
  - Get behind, start skipping steps to make up
  - Cowboy culture that omits basic system engineering processes, e.g., documentation
  - Find errors late (rework involves enormous time and effort)
  - Skip some testing
  - Does not satisfy customer requirements
  - Gets even later and may be abandoned
- Identify cultural flaws leading to inadequate product quality and timeliness

What is Organizational Culture?

Edgar Shein



- **Unless change value system and how decisions are made, changing upper levels will not be effective**
- **Organizational culture is set by leaders who establish values under which decisions will be made**

Identify Current Culture Leading to Problems

- Some common examples:
  - Requirements cannot be known in advance so start with design and then specify requirements later
  - Skipping steps will result in getting a late project back on track
  - Documentation is not necessary in development, but only in maintenance
  - Testing can be delayed and done later
  - Reward “cowboys” as they save the day
  - …
- Identify culture (values, decision-making principles) you want
  - Skipping steps makes a late project later
  - Starting without requirements leads to wasted time and effort
  - Quality is determined by upfront development activities
  - …

Next Steps

- Establish requirements to implement desired culture in organizational processes
- Create the system engineering hierarchical control structure
- Where are requirements implemented? Why are the current controls not effective?
  - Many of problems will be found and mitigations identified by reviewing control structure with experts, e.g., incentive structure conflicts with desired culture, missing or delayed feedback so controls ineffective
- Perform STPA, including causal analysis (why are the current controls inadequate?)
- Make recommendations and implement risk management based on leading indicators of increasing risk

Producibility in Aerospace Corp. X (Allen Ball)

- Producibility: An emergent property of product development and manufacturing systems that encapsulates
  - Ability to produce a product within cost and schedule constraints
  - While maintaining a target level of quality
  - And producing a product compliant with applicable requirements
- Producibility risk not traditionally identified in product development until details of product configuration and production system understood
- But cost and complexity determined at earliest stages of product development
- Identified leading indicators of producibility risk early in product development process

Problem

- New product quality and performance problems have driven non-recurring costs and delayed product delivery to customers.
- Wanted improved methods to identify risk early in product development cycle in order to:
  - Allow for effective resource allocation
  - Prevent early introduction of risk in product and process definition
  - Address incompatibility of product definition with manufacturing capability

Accidents (Losses)

Table 4.1: Producibility losses for Aerospace Corporation X assessment

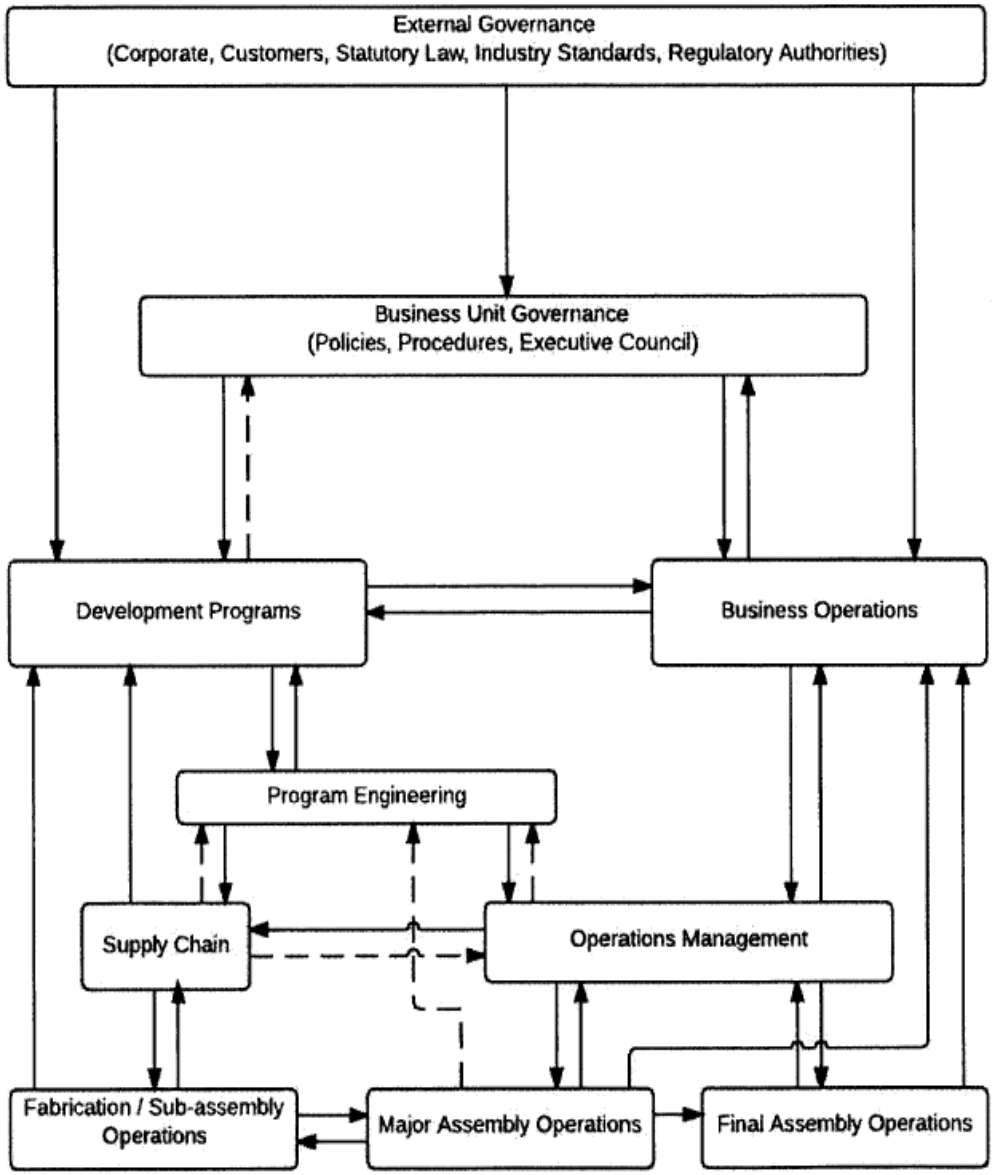
Loss Ref	Producibility Attribute	Potential Loss
L1	Quality	Throughput yield for any fabrication,or assembly process below target %
L2	Product Compliance to Type Design	Product operation or performance is inconsistent with type design requirements or customer expectations as a result of the physical manifestation of product definition
L3	Cost	Exceedence in cost with respect to planned program recurring or nonrecurring budgets
L4	Schedule	Interruption in product flow resulting in a missed commitment to downstream internal or external customer

Hazards Leading to Potential Loss of Quality

Table 4.2: Hazards contributing to a potential loss of quality

Identifier	Producibility Hazard	Category
PHQ-1	Program manufacturing plan is not defined	Program
PHQ-2	Variation in product definition cannot be controlled with current process capability	Manufacturing & Processing
PHQ-3	Use of new manufacturing process without adequate validation	Novelty
PHQ-4	Aggregation of stochastic variation in assembled product	Complexity
PHQ-5	Process capability does not align with product specifications	Capability
PHQ-6	Skill level of the workforce does not support product definition and process capability	People
PHQ-7	Level of inspection does not adequately assess product attributes	Inspection
PHQ-8	Lack of control in material source	Material
PHQ-9	Lack of understanding of critical system interface control	Criticality
PHQ-10	Tolerances are not satisfied due to inadequate process specification	Requirements
PHQ-11	Production quality does not satisfy lifecycle maintainability demand	Maintainability
PHQ-12	Specified unit cost does not reflect necessary process controls	Design to Cost

Example of Control Structure



Performed STPA (identified key findings)

Table 4.5: Inadequate control assessment for (1) the missing control action between nonconformance reporting and the Production Change Board and (2) PCAS issuance.

Hazard Identifier	Present Control Action	Missing Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing / Order	Stopped Too Soon / Applied Too Long
PHQ-2		(Nonconformances / Process Capability link to PCB)	Product Quality does not provide relevant nonconformances / process capability when product definition requires variation that cannot be controlled by current processes	N/A	Product Quality provides relevant nonconformances / proces capability after product definition is assessed for process compatability	N/A
PHQ-5	PCAS		Production Change Board does not provide the PCAS when changes are required to capture incapable process in product definition	Production Change Board provides the PCAS when process capability is not sufficient for the configuration	Production Change Board provides the PCAS before process capability has been assessed	N/A

Then Identified Causes and Assumptions

Table 4.9: Causality and shaping assumptions for presented inadequate control actions in the interaction of the Product Centers and System Engineering.

Hazard Identifier	Inadequate Control Action	Causality	Shaping Assumptions
PHQ-1, PHQ-7,PHP-1,PHP-3, PHP-5,PHP-7	Mitigation Timeline	There is no established process for product and process risk communication to production operations. Risk management inputs and assignment are confined to Engineering and Program Management	Production operations and resources do not have statement of work at early stages of product development.
PHQ-2,PHQ-3,PHQ-6,PHQ-11,PHQ-12,PHP-6	Mitigation Timeline	The risk management process is not capturing process capability risks beyond those associated with new manufacturing techniques.	(1) Manufacturing engineering will provide process risks if required, (2) Existing manufacturing techniques have process control data that can be interpreted so risk mitigaiton is not required
PHQ-4,PHQ-5,PHQ-6,PHP-2,PHP-3,PHP-6,PHP-7	Process Constraints	There is no established development process for process risk assessment or communication from prodution operations to system or design engineering.	Manufacturing engineering will provide process risks if required.
PHQ-9,PHQ-10,PHQ-12,PHP-4	Process Constraints	There is no established development process for configuraiton assesssment by prodution operations to system or design engineering.	Manufacturing engineering will be responsible for identifying build risk during EC release process.

Results from Analysis

Table 4.11: Aggregated counts of identified inadequate and omitted control actions by controlling entities across all phases of governance

Controlling Entity	Hazardous Control Actions	
	Omitted	Inadequate
External Governance	2	28
Business Operations	5	54
Production Operations	3	80
Engineering	1	53
Supply Chain	4	37
Product	3	29

Then Identified Leading Indicators for Early Stage Producibility Risk Assessment

- Methodology from Leveson, built on “Assumption Based Planning”
- Create leading indicators based on assumptions used in managing risks that may not be true:

1. The models and assumptions used during initial decision making and design are correct.

2. The system will be constructed, operated, and maintained in the manner assumed by the designers.

3. The models and assumptions are not violated **by** changes in the system, such as workarounds or unauthorized changes in procedures, or by changes in the environment.

Types of Assumptions to Consider

- Assumptions about the system hazards and the paths to (causes of) hazards.
- Assumptions about the effectiveness of the controls, that is, the shaping and hedging actions, used to reduce or manage hazards.
- Assumptions about how the system will be operated and the environment (context) in which it will operate.
- Assumptions about the development environment and processes
- Assumptions about the organizational and societal safety control structure during operations
- Assumptions about vulnerability or severity in risk assessment that may change over time and thus require a redesign of the risk management and leading indicators system

Ball Conclusions:

- Understanding causation and assumptions showed that
  - Majority of sources of producibility risk were a function of organizational control and temporal phasing of governance due to resource constraints
  - These are more important than current product feature-based sources of producibility risk.

Workplace Safety

- In 2013 Boeing introduced a “Go for Zero – One Day at a Time” effort to improve workplace safety
  - Purpose was to eliminate injuries across all of their workers
  - “Achieve step function improvement in workplace safety”
  - “If we can build the safest airplanes in the world, why can’t we build the safest workplace”
- Early 2015, decided to add “systems-thinking” based approach (STAMP) to improve the results achieved so far
- Concentrated on manufacturing and assembly (not on slips and trips in the office).
- Modeling and analysis have identified many specific improvements that are needed. Implementation of improvements is in progress.

Traditional Approach to Workplace Safety

- Assume workplace injuries due to worker errors
- Based on changing worker behavior through
  - Training
  - Reward and punishment
  - Slogans, signs, “safety moments”
- Investigate accidents by identifying what workers did wrong
  - Do more of the same to change worker behavior
- But workplace safety not significantly improving over time

An alternative is to introduce systems thinking

A Systems View of Workplace Safety

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

A Systems View of Workplace Safety

- Blame is the enemy of safety
  - In most cases, people do not purposely endanger themselves and others
  - Identify why it made sense to act unsafely and use that to information to redesign the system.

Human error is a symptom of a system that needs to be redesigned

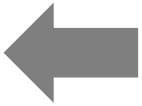
Suggested Workplace Cultural Principles

- All injuries, accidents, and workplace illnesses are preventable.
- Increasing safety and quality leads to decreasing cost and schedule
- Effective, clear, consistent and timely communication and the sharing of information are essential to achieving an accident-free workplace.
- Workplace safety requires continual learning and improvement

"Find a Way" → **"Find a Safe Way"**

Creating Requirements for Cultural Principles

- Establish a Just Culture
- Continuously monitor the safety control structure for migration toward a state of higher risk
- Establish robust and reliable communication channels to ensure accurate risk management
- Establish working groups between design engineers, mechanics, safety focals and managers at all levels



All injuries, accidents, and workplace illnesses are preventable

Facilitating safety promotes business objectives including cost and schedule

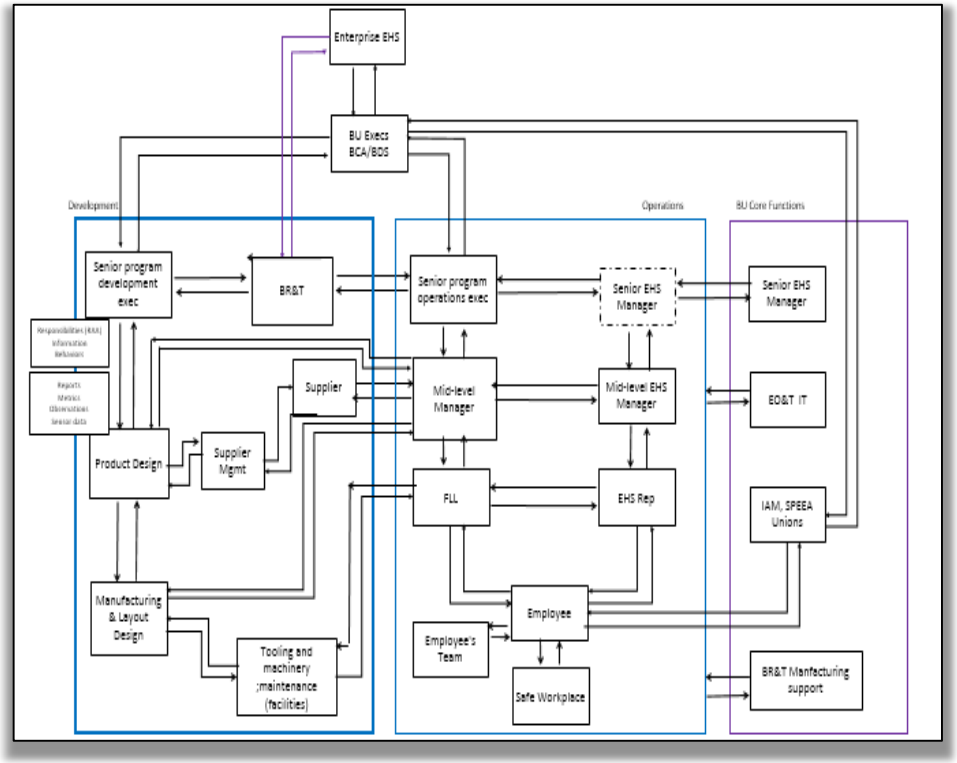
Effective, clear, consistent and timely communication and the sharing of information are essential to achieving an accident-free workplace

Workplace safety requires continual learning and improvement

A Clear Purpose for Each Requirement

Building a Control Structure

- Includes action loop (RAA, information & behaviors) and feedback loop (metrics, observations, etc.)
- Need to address hazards in both development and operations
- Used for engineering analysis to reveal systemic causal conditions of incidents (safety and quality)



Control and Feedback Loops for All Processes

Requirements Gaps Analysis and Risk Analysis

- **Examples of findings** that would not have been discovered with usual techniques
  - Lack of a feedback loop for in-design activities restricts opportunities to improve requirements based on insights from factory worker incidents
  - Lack of interaction among design engineers, IE's, ME's, mechanics causes development to operations disconnects
  - Supply chain issues are contributing to injuries and require more system wide resolution in the attempts to reduce the injuries
  - Current IT infrastructure needs enhancement to provide timely and relevant information to support safety and quality related decisions

To Change Behavior, Change the System

Conclusions

- STAMP is pure system theory and can be applied to any emergent property
  - Demonstrated by Col. Bill Young for cyber security
  - Provides important direction to improve these properties
  - Demonstrations have produced impressive results
- STPA does not require changes to use on the social and organizational parts of control structures
- Demonstration of leading indicators from STAMP have been practical in at least one instance
- Few resources required to get important results