The Missing Link

System Theoretic Approach to Safety
John Helferich
SDM Webinar 7/31/13
What causes accidents?

- Random Chance?
- Operator Error?
- Mechanical Failure?
- Greedy Owners?
Accident Causation Models

Chain of Events

Heinrich 1931
Accident Causation Models
Swiss Cheese Model

Reason 1990
Accident Causation Model
STAMP
(System Theoretic Accident Modeling Process)

System moves to unsafe state due to loss of control

Leveson 2011
Deepwater Horizon
STAMP and STPA

**STAMP: Accident Causation Model**

Accidents arise from complex, dynamic processes, not linear chain of events

Accidents are a control problem, not a failure problem

Accidents prevented by enforcing constraints on component behavior and interactions

Hazard Analysis
Key to preventing accidents

- **Reliability Based**
  - Probabilistic
  - FMEA
  - Fault Tree

- **System Theoretic Based**
  - Control Based
  - STPA
Risk priority number (RPN) = SEV*OCCUR*DETEC

Step 1: Detect a failure mode

Step 2: Severity number (SEV)

Step 3: Probability number (OCCUR)

Step 4: Detection number (DETEC)

Actions + Check

Failure Mode & Effect Analysis
Failure Modes, effects, and Criticality Analysis is an excellent hazard analysis and risk assessment tool, but it suffers from other limitations. This alternative does not consider combined failures or typically include software and human interaction considerations. It also usually provides an optimistic estimate of reliability. Therefore, FMECA should be used in conjunction with other analytical tools when developing reliability estimates. [18]
Decompose the system hierarchy to identify control loops that enforce the safety constraint

Food Production: Simplified Safety Control Structure

Safety Constraint:

Food shall contain no pathogen at point of consumption
Assess each control loop for inadequate control actions.
Inadequate control actions

• Retrospective
  – Accident Analysis
  – How did the system enter an unsafe state?
  – CAST (Causal Analysis using STAMP)

• Prospective
  – System Design and Engineering
  – How can I prevent the hazard from occurring?
  – STPA
Current Food Hazard Control Strategy
Combination of Barriers and Controls

Controls
- Exterior Contaminants
- Transboundary Contamination
- Peanut Roaster
- Finished Product
- Consumption

Barriers
- Building Envelope
- Sanitary Practices
- Pest Control
- Product Separation

HACCP
- Time/Temp

Positive Release

GMPs
STAMP: Example Safety Control Structure

Leveson (2004), Leveson (2011)
“A genuine commitment to safety means not just examining miners’ work practices and behaviors. It means evaluating management decisions up the chain of command - all the way to the boardroom - about how miners’ work is organized and performed.”

Report to the Governor: Governor’s Independent Investigation Panel Final Report: Upper Big Branch Mine Disaster April 5, 2010

Ultimate Culpability for a Mine Disaster\(^1\)

\(^1\) New York Times editorial Nov 30 2012
Thank you

ehelferic@mit.edu