The Missing Link

System Theoretic Approach to Safety

John Helferich

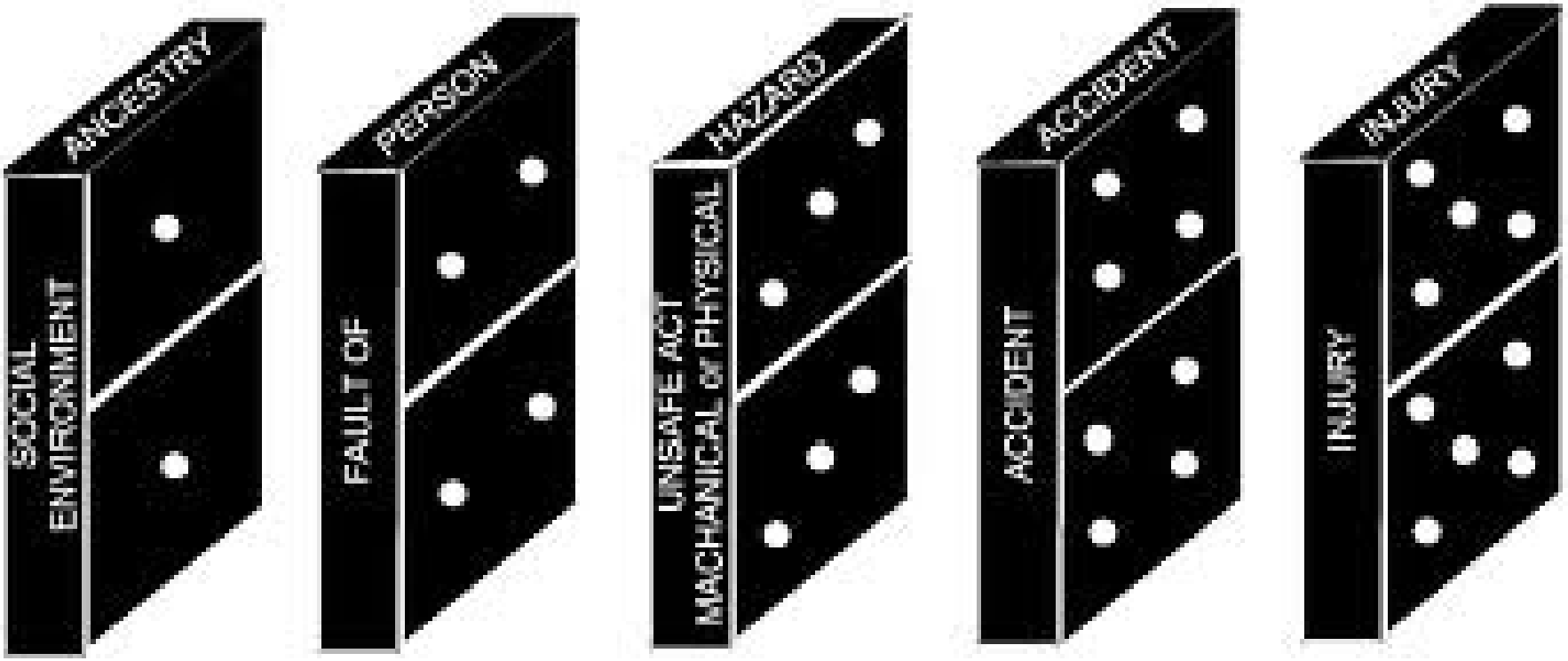
SDM Webinar 7/31/13

What causes accidents?

- Random Chance?
- Operator Error?
- Mechanical Failure?
- Greedy Owners?

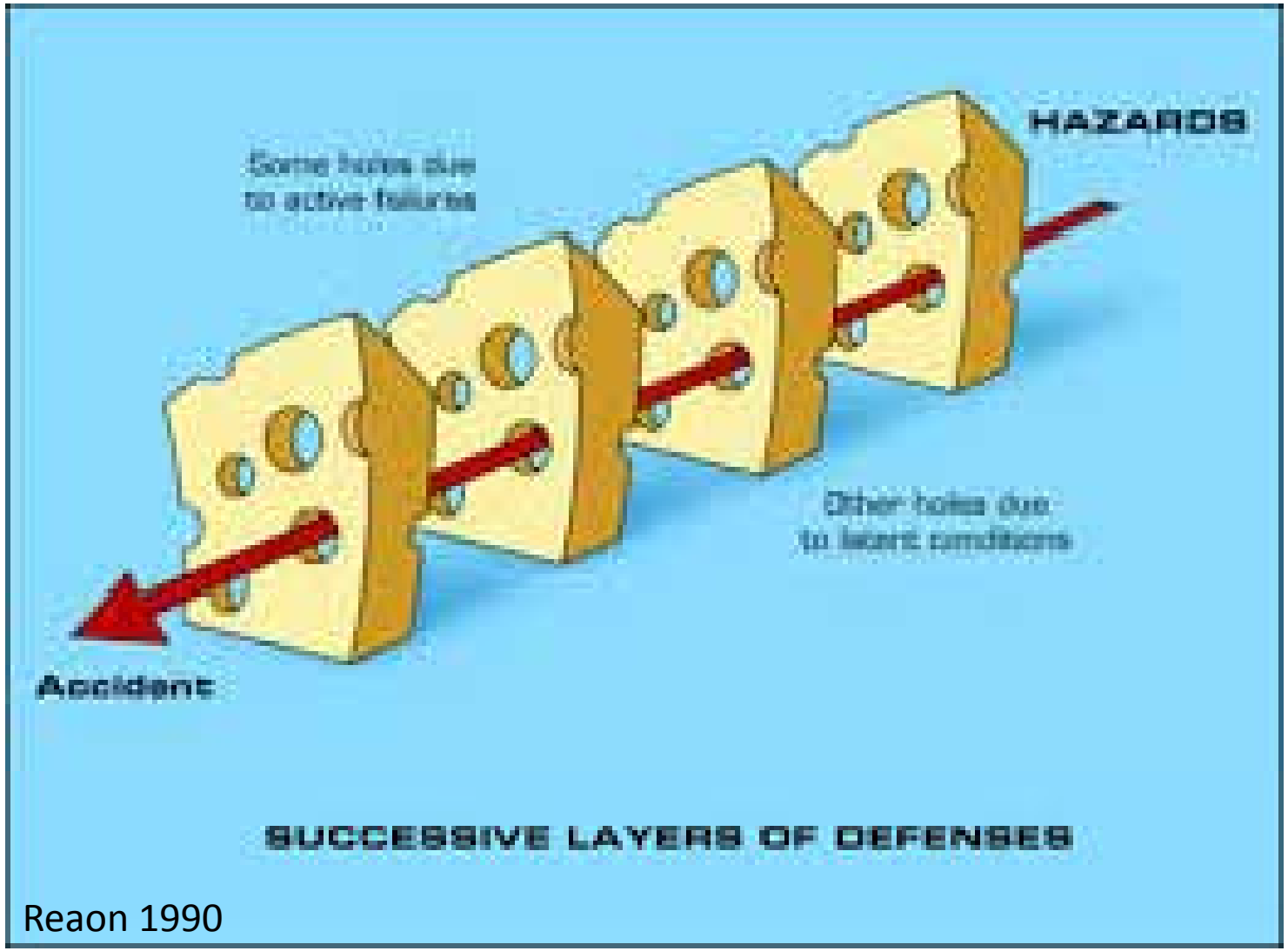
Accident Causation Models

Chain of Events



Heinrich 1931

Accident Causation Models
Swiss Cheese Model



Reaon 1990

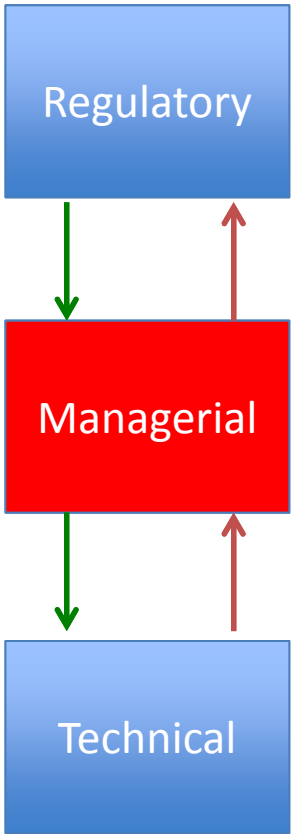
Accident Causation Model
STAMP
(System Theoretic Accident Modeling Process)

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

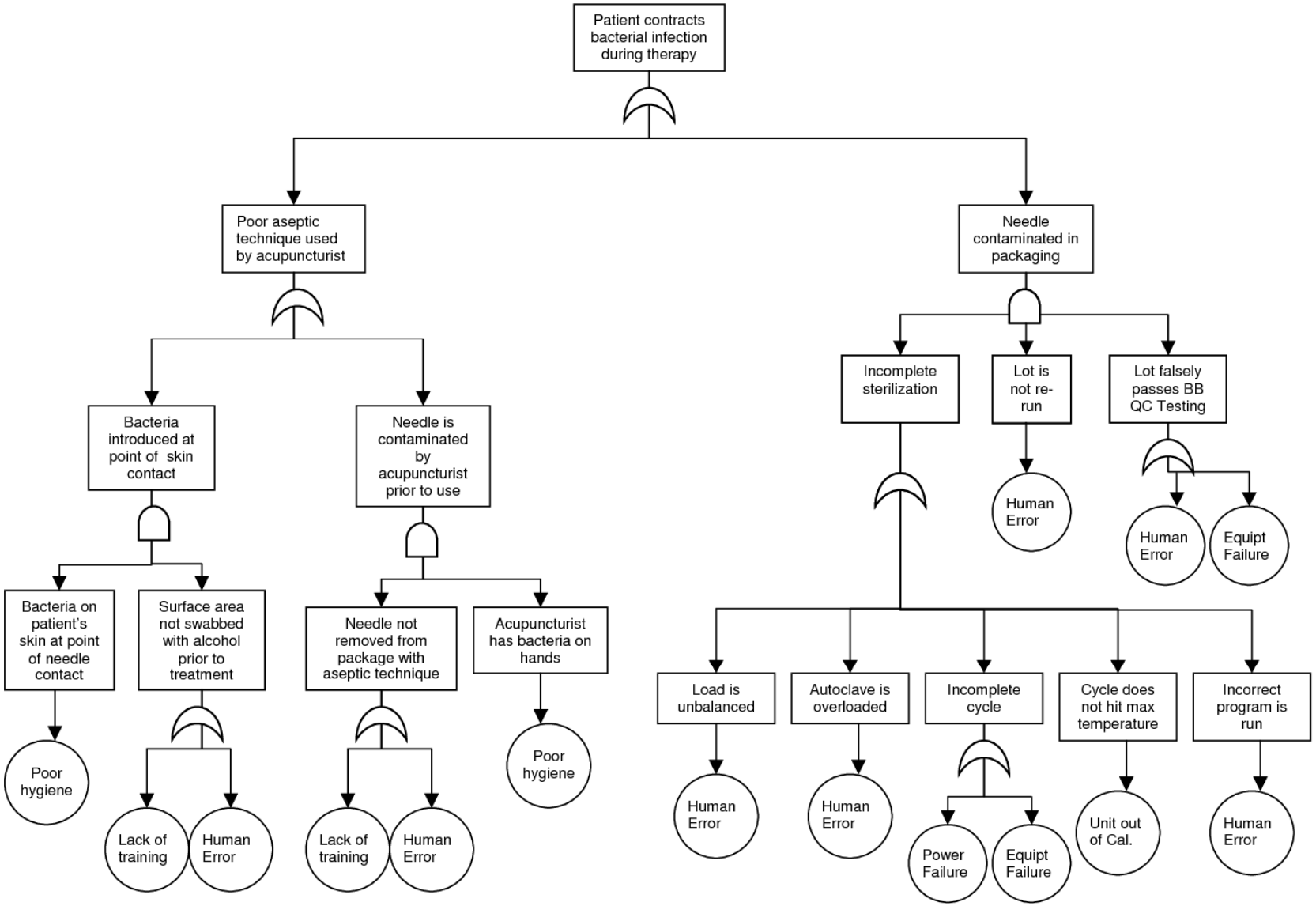
Leveson (2004, 2011), After Fleming (2013)

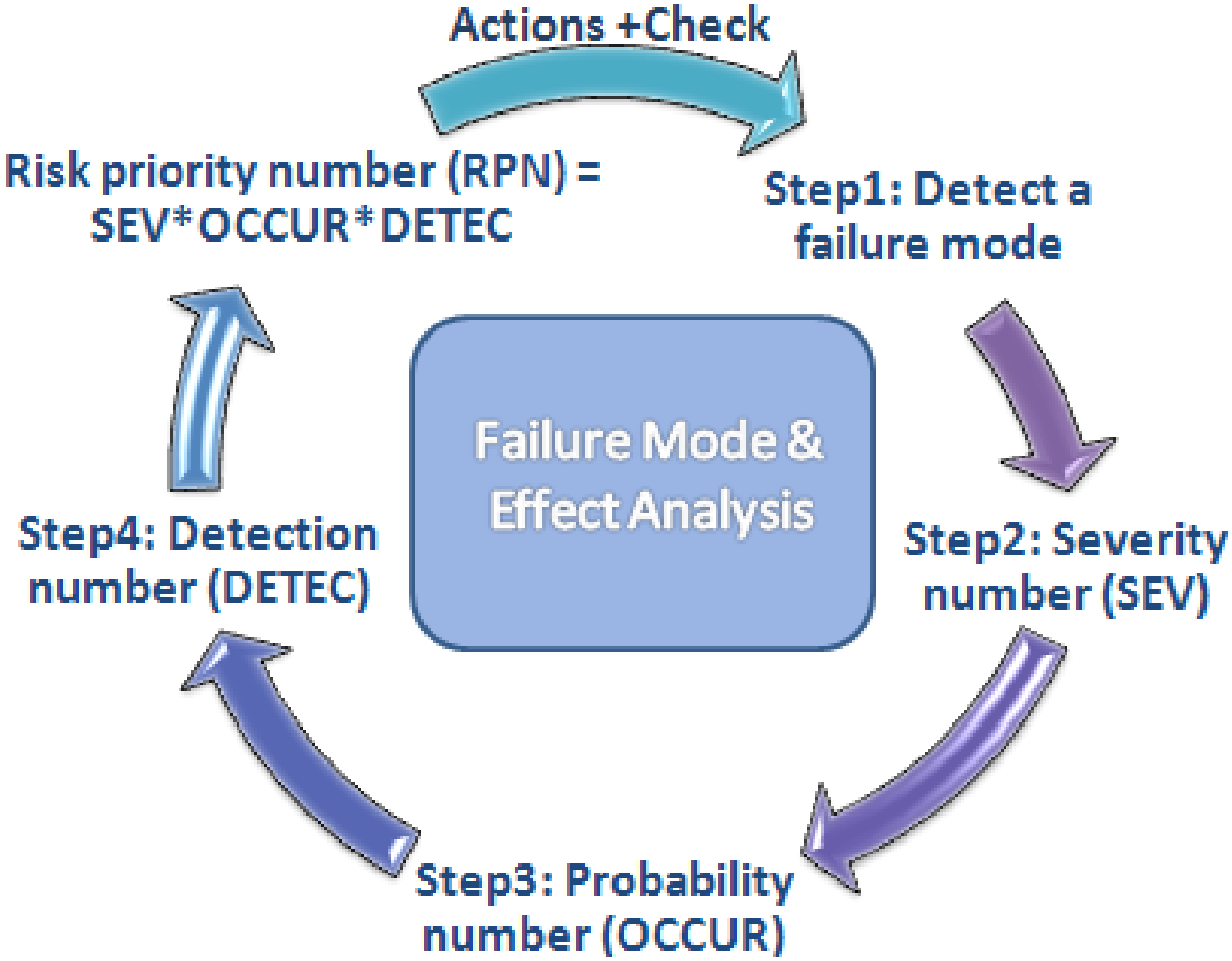
Hazard Analysis
Key to preventing accidents

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

- **System Theoretic Based**
  - Control Based
  - STPA

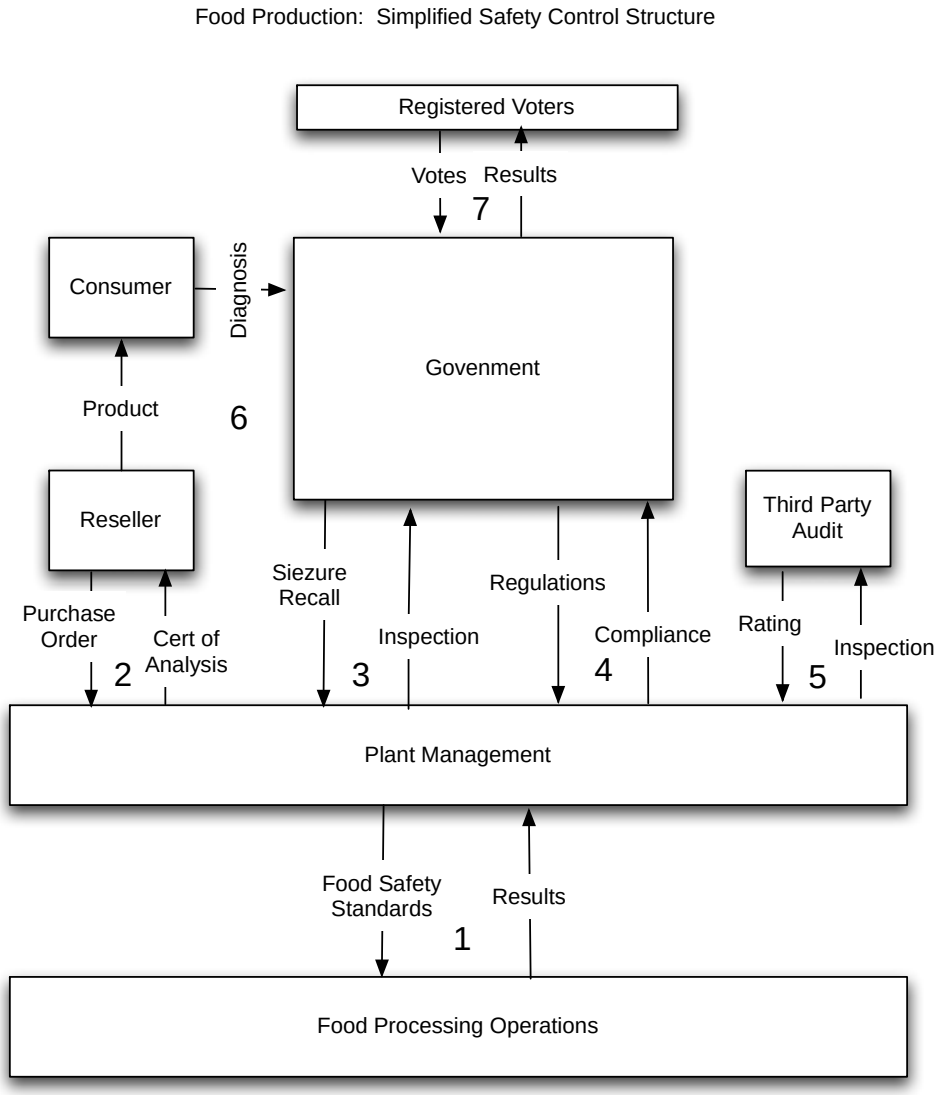
Fault Tree Analysis (FTA) Risk Analysis Example
Acupuncture Needles




Actions +Check
Risk priority number (RPN) = SEV*OCCUR*DETEC
Step1: Detect a failure mode
Failure Mode & Effect Analysis
Step4: Detection number (DETEC)
Step2: Severity number (SEV)
Step3: Probability number (OCCUR)

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]

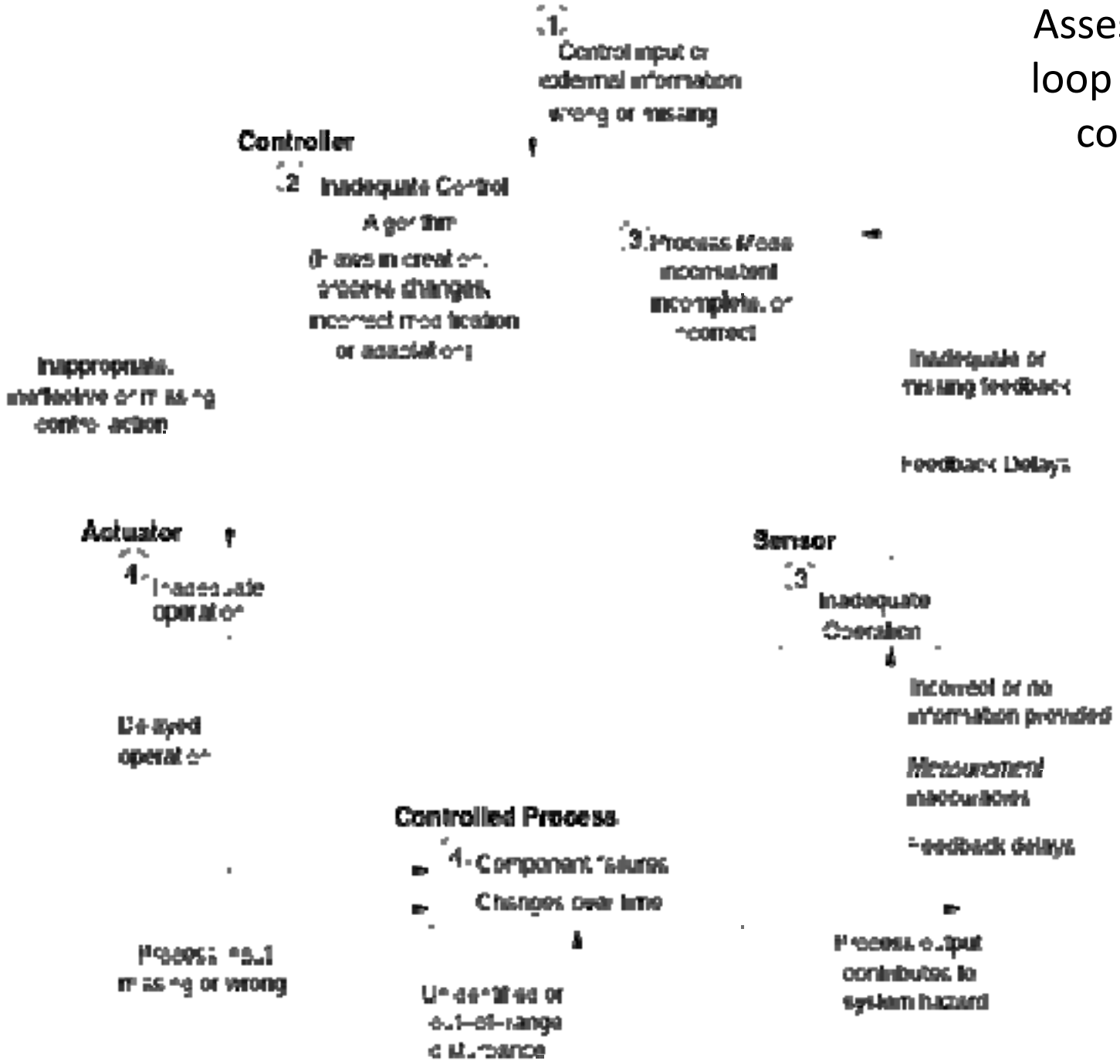
Decompose the system hierarchy to identify control loops that enforce the safety constraint



Safety Constraint:

Food shall contain no pathogen at point of consumption

Assess each control loop for inadequate control actions

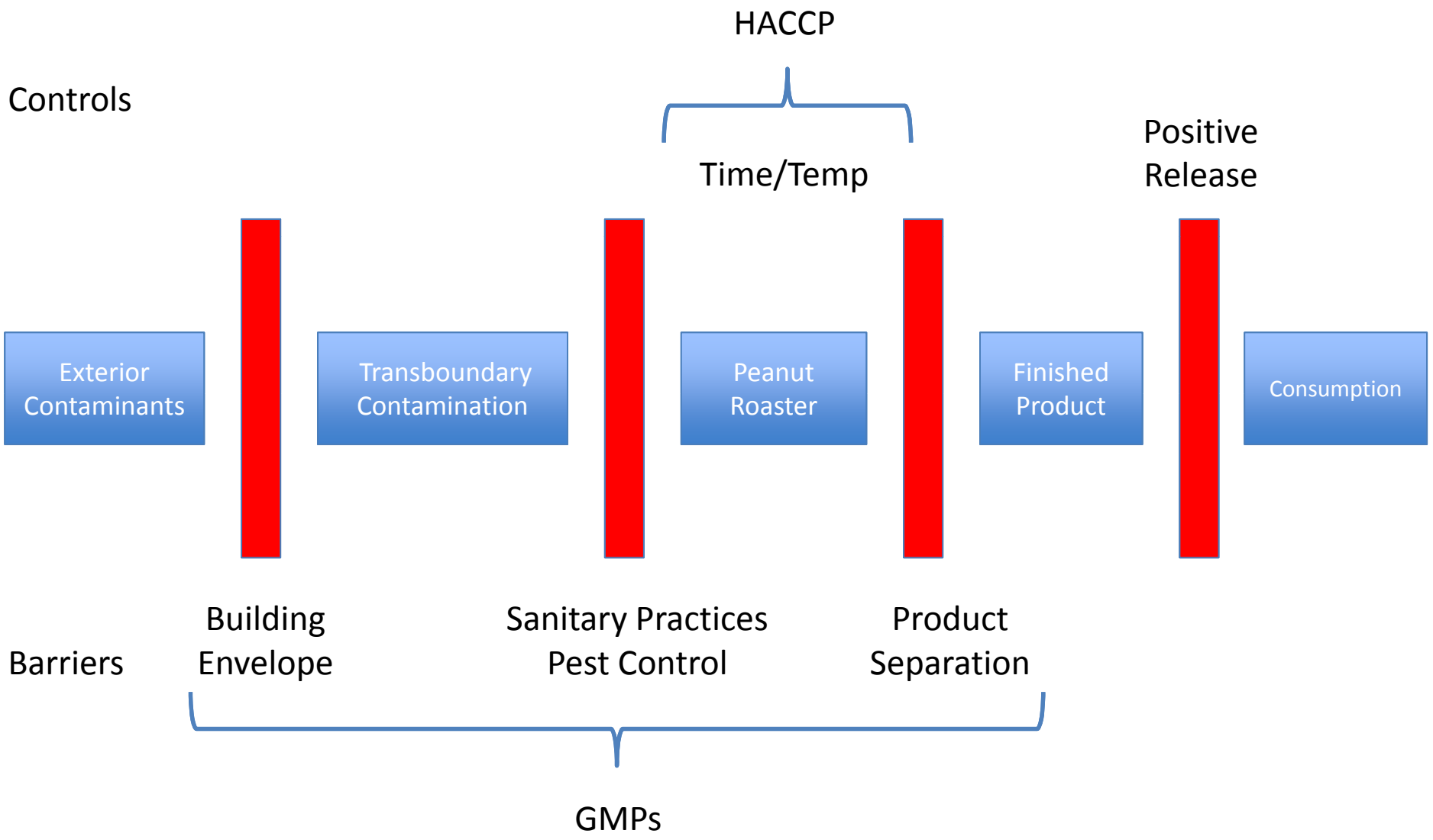


Inadequate control actions

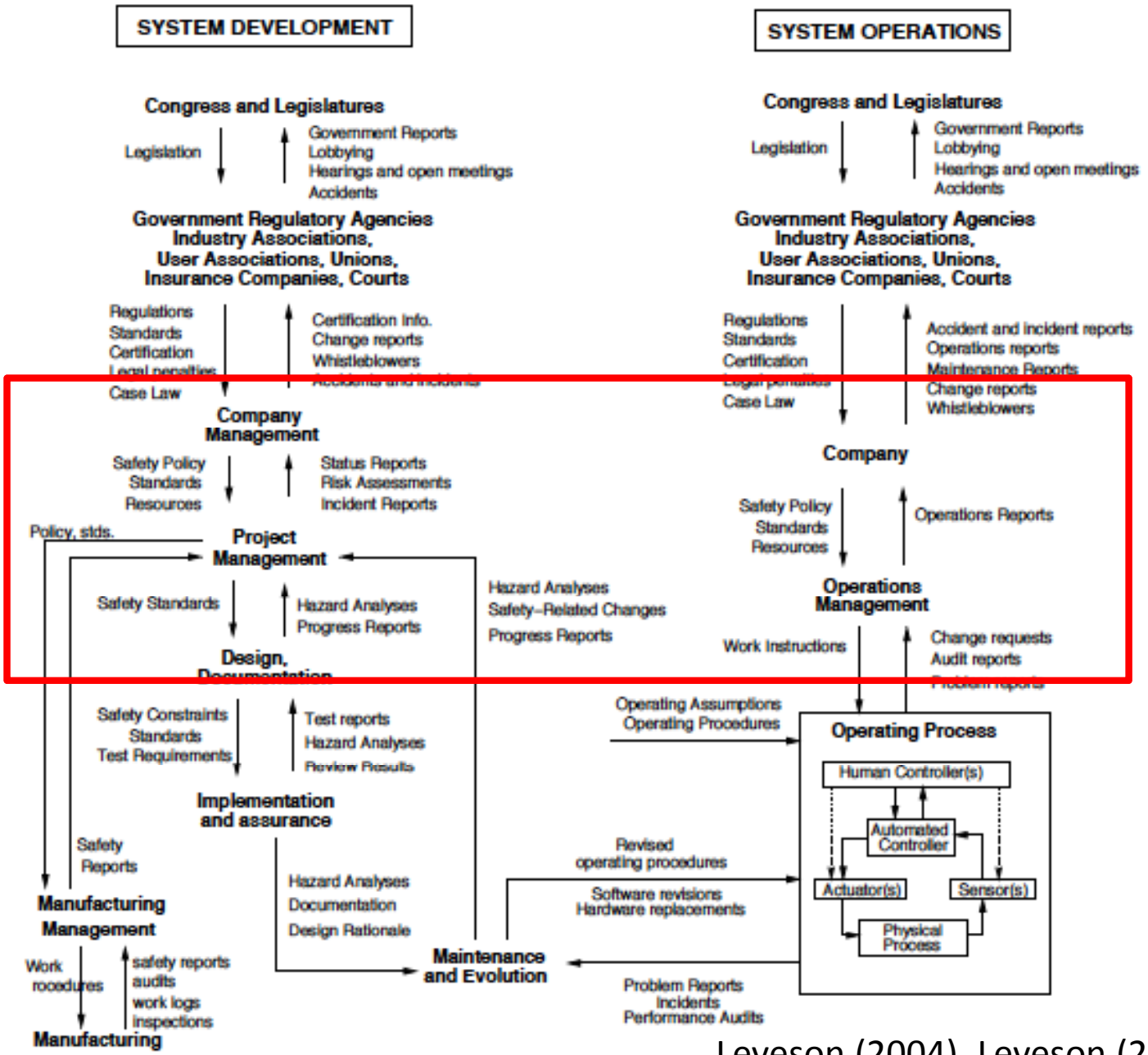
- Retrospective
  - Accident Analysis
  - How did the system enter an unsafe state?
  - CAST (Causal Analysis using STAMP)
- Prospective
  - System Design and Engineering
  - How can I prevent the hazard from occuring?
  - STPA

Current Food Hazard Control Strategy

Combination of Barriers and Controls

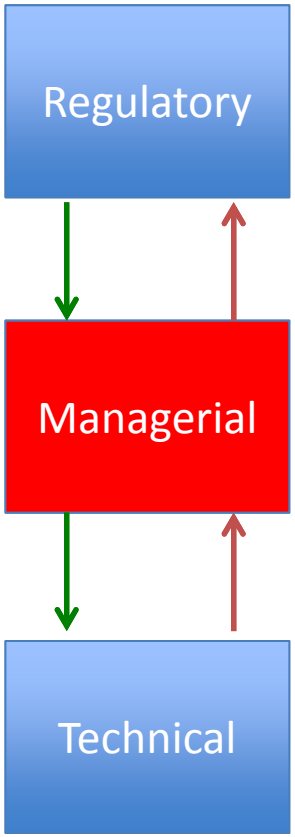


STAMP: Example Safety Control Structure



Leveson (2004), Leveson (2011)

The Missing Loop



"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

helferic@mit.edu