Reducing Accidents in the Oil and Gas Industry

Prof. Nancy Leveson, MIT

leveson@mit.edu

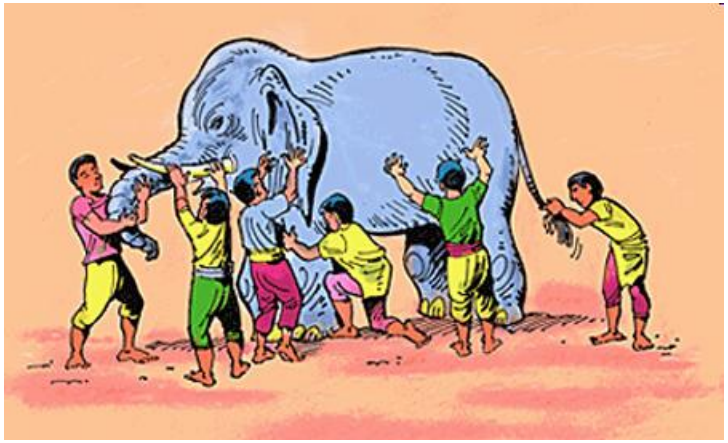
Background

- Practicing and teaching system safety engineering for 30 years.
- Own a 20 year-old company doing safety engineering (Safeware)
- Experience in almost all industries, e.g.,
  - Aerospace (aviation and space exploration)
  - Defense
  - Transportation (automobiles, trains, air traffic control)
  - Oil and Gas, Chemicals
  - Nuclear Power
  - Medicine
- Member of the Baker Panel on the BP Texas City oil refinery explosion (2005-2007)
- Instructor: BP-MIT Management Education Program (2007-2010)

Topics and Major Ideas

- Basic concepts in accident causality
- Common factors in major accidents (including DWH)
- Safety as a control problem
- Establishing appropriate controls to prevent more offshore oil spills

To understand and prevent accidents, must consider system as a whole



And so these men of Hindustan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right
And all were in the wrong.

John Godfrey Saxe (1816-1887)

Jerome Lederer (1968)

"Systems safety covers the total spectrum of risk management. It goes *beyond the hardware* and associated procedures of systems safety engineering. It involves:

- Attitudes and motivation of designers and production people,
- Employee/management rapport,
- The relation of industrial associations among themselves and with government,
- Human factors in supervision and quality control,
- The interest and attitudes of top management,

- The effects of the legal system on accident investigations and exchange of information,
- The certification of critical workers,
- Political considerations
- Resources
- Public sentiment

And many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.”

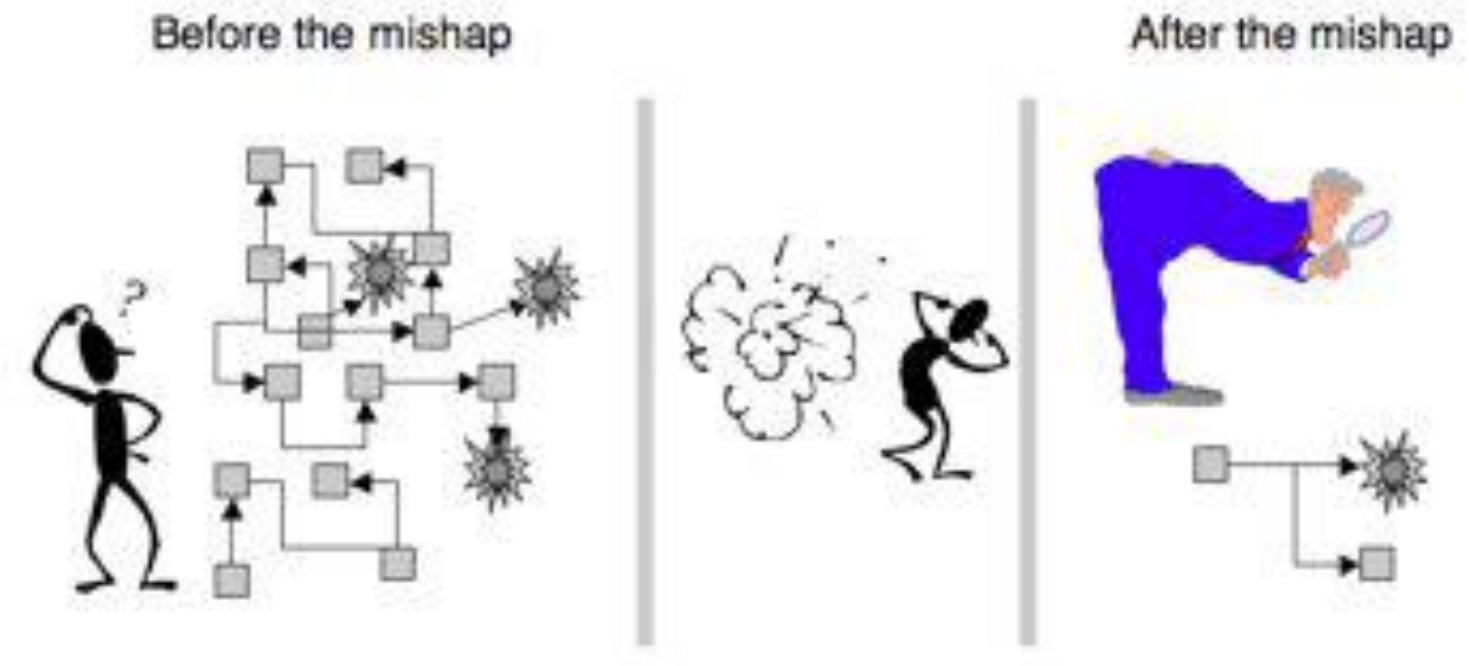
Common Traps in Causal Analysis

- Root cause seduction
- Hindsight bias
- Narrow views of human error
- Blame is the enemy of safety
- Physical design vs. operations

Root Cause Seduction

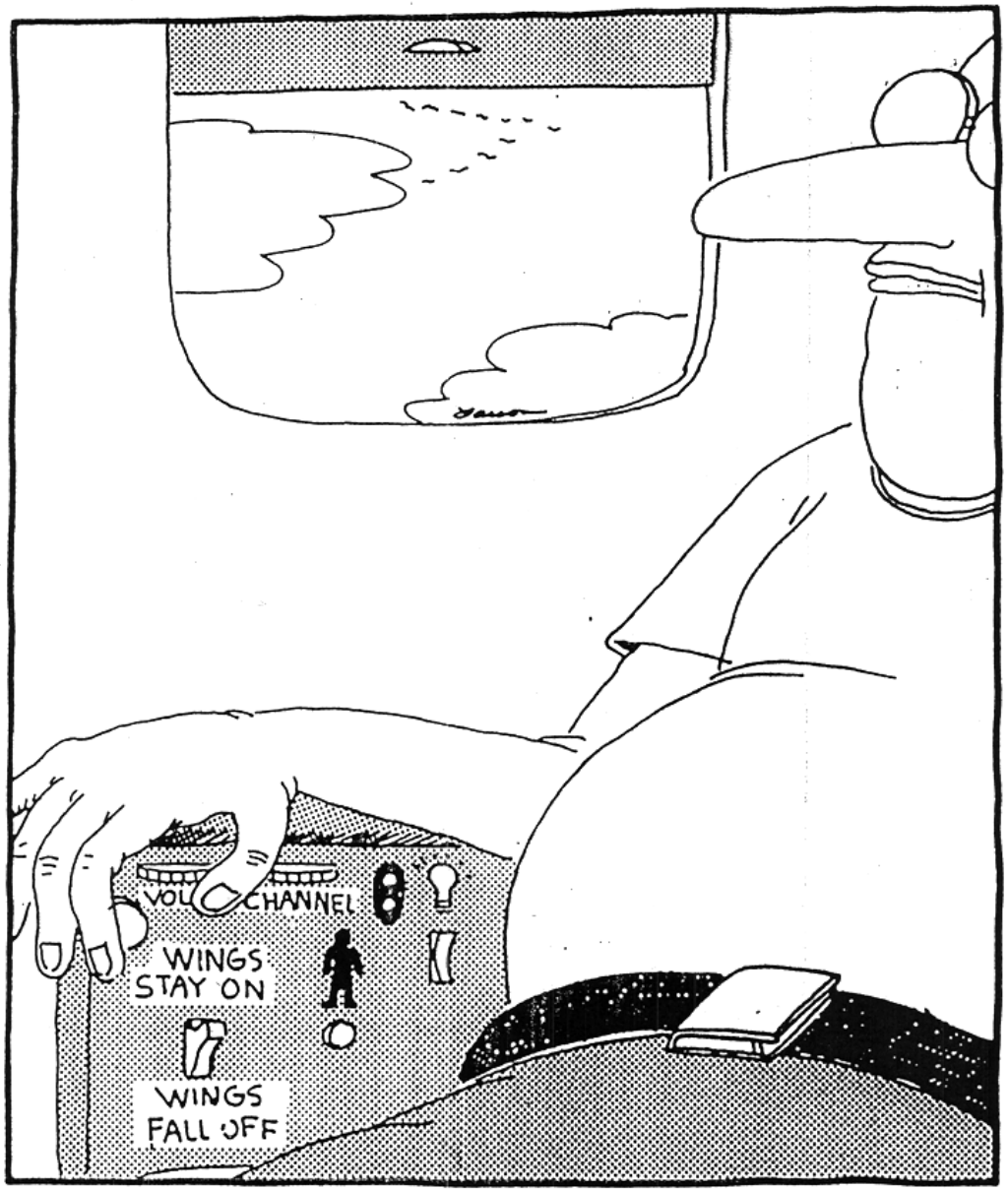
- Assuming there is a root cause gives us an illusion of control.
  - Usually focus on operator error or technical failures
  - Ignore systemic and management factors
  - Leads to a sophisticated “whack a mole” game
    - Fix symptoms but not process that led to those symptoms
    - In continual fire-fighting mode
    - Having the same accident over and over

Hindsight Bias



(Sidney Dekker, 2009)

“should have, could have, would have”



Fumbling for his recline button Ted unwittingly instigates a disaster

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: System 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

Ref: Sidney Dekker, Jens Rasmussen

“Blame is the Enemy of Safety”

- To prevent accidents in the future, need to focus on why it happened, not who to blame
- Blame is for the courts, prevents understanding what occurred and how to fix it.

Physical Design vs. Operations

- ALL accidents are caused by “human error” (except “acts of God,” like hurricanes)
- Almost always there is:
  - Operator “error”
  - Flawed management decision making
  - Flaws in the physical design of equipment
  - Safety culture problems
  - Regulatory deficiencies
  - Etc.

Baker Panel Findings

- Corporate safety culture
  - Leadership
  - Open, trusting environment
  - Adequate resources provided
  - Proper assignment of responsibility, authority, accountability
- Process Safety Management Systems
- Performance evaluation, corrective action, corporate oversight

Common Factors in Major Accidents

- Flaws in safety culture
  - Culture is the shared values and norms on which decisions are based
  - "Culture of Denial"
    - Our industry is just more risky (President of API)
    - Accidents are inevitable
      - "Stepping off a curb and being hit by a car" (Dudley)
    - Unrealistic risk assessments
    - Only hear good news, arguments that safety is improving
  - "Compliance Culture"
    - Impact of moratorium?

Common Factors in Major Accidents (2)

- Lack of real commitment to safety by leaders
  - Think accidents are the price of production
  - Don’t see long term impacts of accidents on the bottom line, that safety pays
  - Most important factor in distinguishing safe companies from unsafe ones.
  - More than mere sloganeering is required
- Confusion between occupational safety and system safety
  - Using “days off from work” as a measure of system safety
  - Managing to the wrong feedback

Common Factors in Major Accidents (3)

- Confusion between occupational safety and system safety (only this industry)
  - Personal safety focuses on
    - Changing individual behavior
    - Controlling injuries to employees on the job
  - Using “days off from work” as a measure of system safety
  - Managing to the wrong feedback

Common Factors in Major Accidents (4)

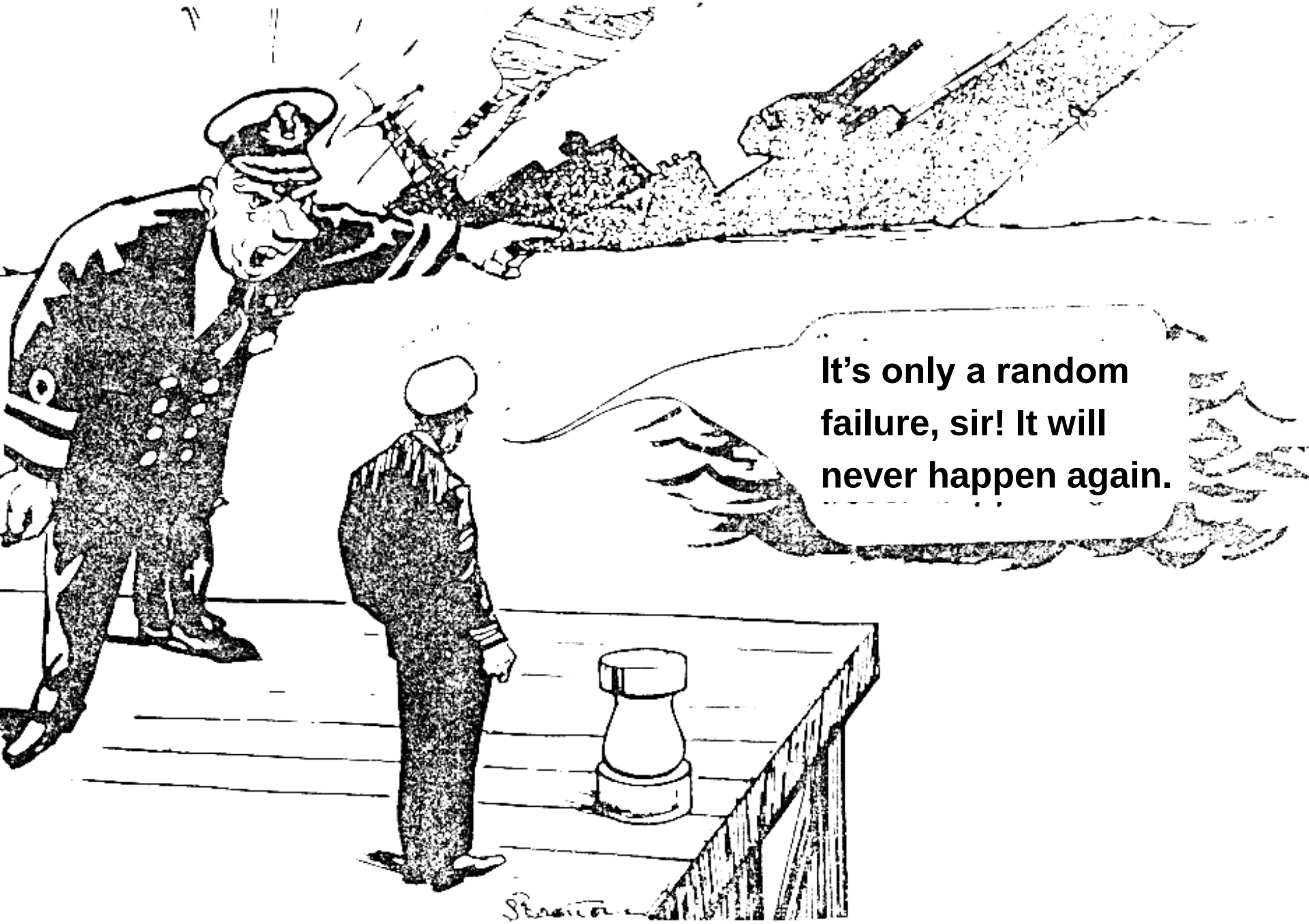
- Inadequate hazard analysis and design for safety
  - Focus on recovery after adverse events
- Flawed communication and problem reporting systems
- Management of change procedures not followed
- Focus on changing humans rather than changing the system in which humans work
- Inadequate causal analysis of incidents/accidents and learning from them

One Additional Misconception

"High-consequence, low-probability" accidents

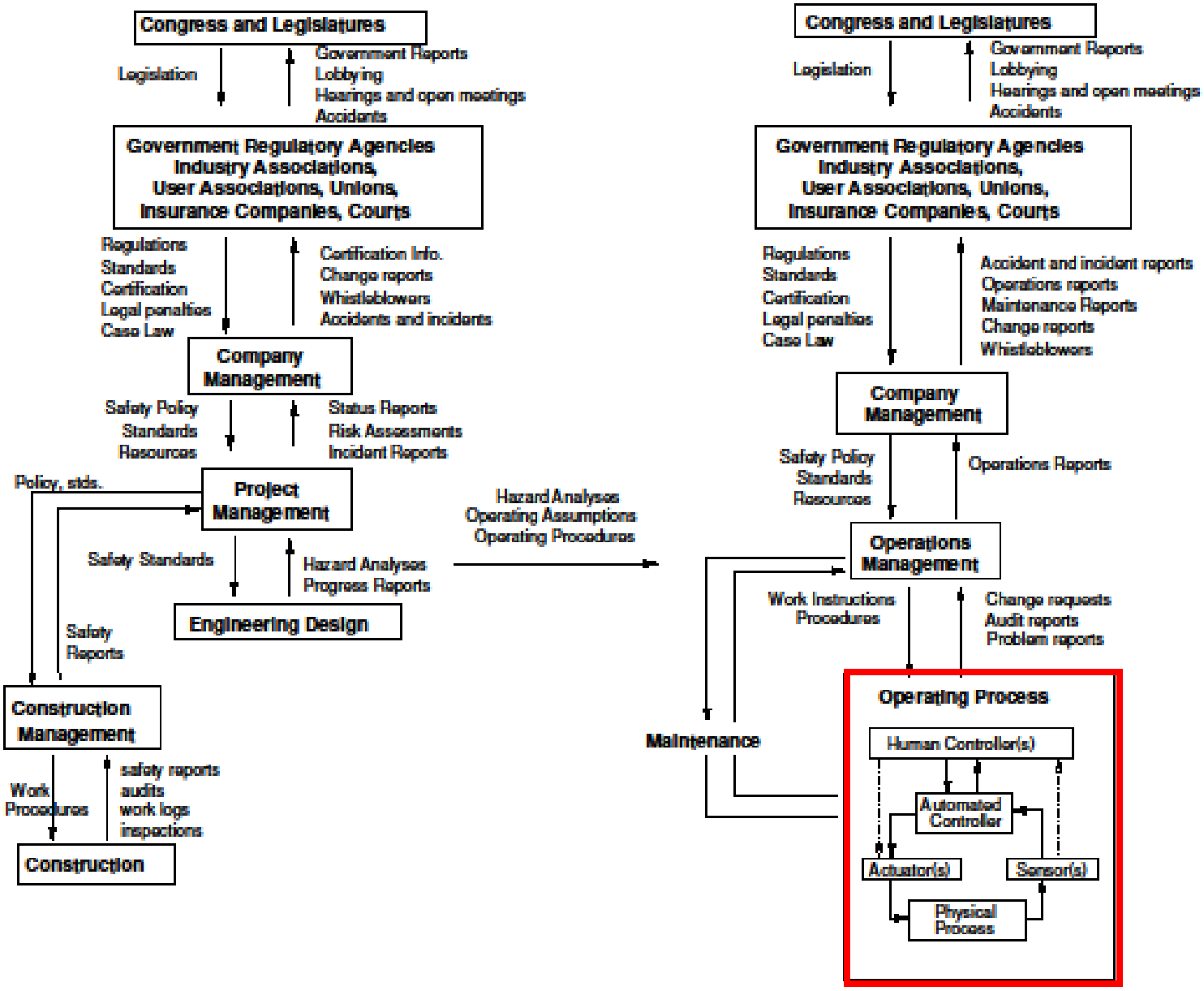
frequency

- Major losses occur because operating under conditions of high risk
  - Not a matter of "if" but only "when"
- Complex systems migrate toward states of high risk
- Accidents take a while to happen, so readjust our estimates of likelihood down over time although risk probably increasing.


It’s only a random failure, sir! It will never happen again.

A System View of Safety: Overview

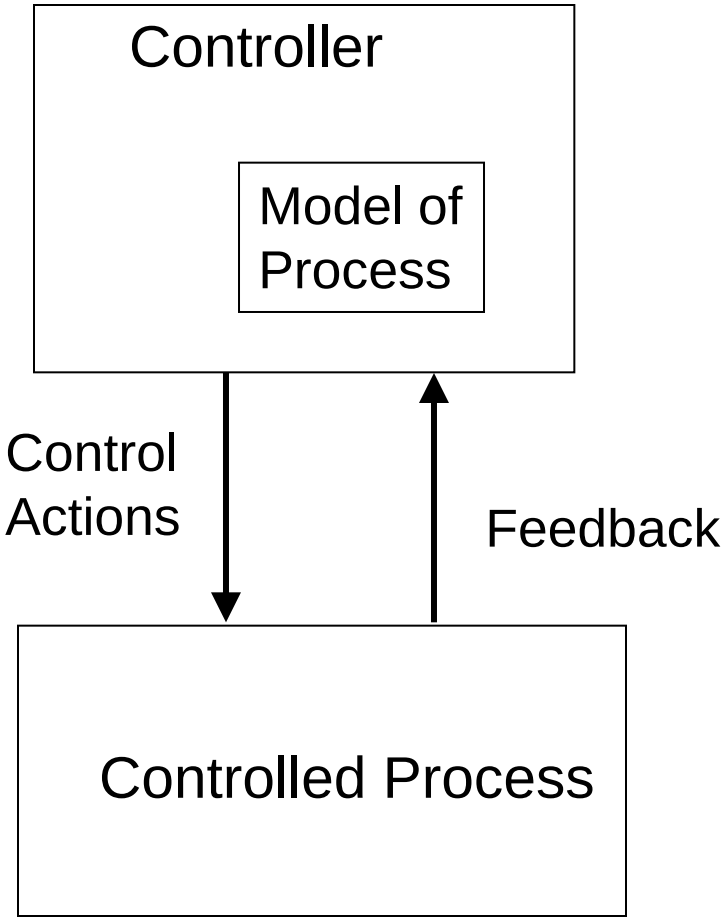
- Safety is a control problem
  - Accidents occur when the system design does not enforce constraints on safe behavior
    - O-ring did not control propellant gas release by sealing gap in field joint of Challenger Space Shuttle
    - Public health system did not adequately control contamination of the egg supply with salmonella
    - Financial system did not adequately control the use of financial instruments
    - DWH design did not adequately control high-pressure gas in the Macondo well
- Events and failures are the result of the inadequate control
  - Result from lack of enforcement of safety constraints in system design and operations


SYSTEM DEVELOPMENT
SYSTEM OPERATIONS
Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Legal penalties
Case Law
Certification Info.
Change reports
Whistleblowers
Accidents and incidents
Company Management
Safety Policy
Standards
Resources
Status Reports
Risk Assessments
Incident Reports
Policy, stds.
Project Management
Safety Standards
Hazard Analyses
Progress Reports
Engineering Design
Safety Reports
Hazard Analyses
Operating Assumptions
Operating Procedures
Construction Management
Work Procedures
safety reports
audits
work logs
inspections
Construction
Operations Reports
Operations Management
Work Instructions
Procedures
Change requests
Audit reports
Problem reports
Maintenance
Operating Process
Human Controller(s)
Automated Controller
Actuator(s)
Sensor(s)
Physical Process

Safety as a Control Problem

- Goal: Design an effective control structure that eliminates or reduces adverse events.
- Controls may be:
  - Physical design
  - Processes
  - Social (cultural, policy, individual self-interest)
- Human error is a symptom of a system that needs to be redesigned

Accidents as a Control Problem



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

Components of an Effective Safety Management System

- Leadership and commitment
- Strong safety culture (shared values and norms on which decisions are made)
- Hazard analysis and design for safety
  - Physical system
  - Social system and controls
- Reporting systems and communication
- Focus on system in which humans work, not changing humans

Components of an Effective Safety Management System (2)

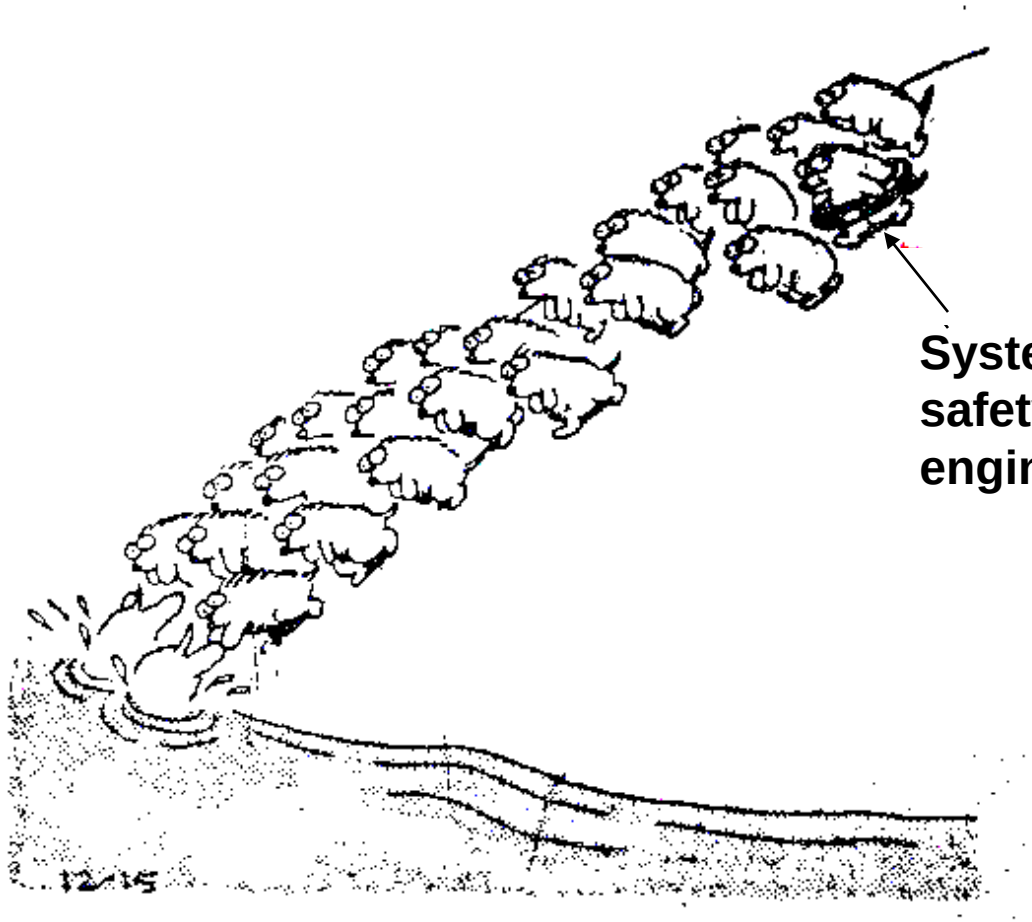
- Management of change
  - Perform regular audits of performance and use to improve system
    - Start from the assumptions in the hazard analysis. Still true?
    - Perform hazard analyses on changes over time (environmental, user, physical systems)
- Feedback and continual improvement/learning
  - Comprehensive accident/incident analysis and re-design of socio-technical system from results
    - Not just the superficial “causes”
  - Look at why safety control structure was ineffective in preventing the loss

Designing Controls over Oil Exploration and Production

- Government
- Industry
- Company

The Far Side

By Gary Larson



Additional information in:

Nancy Leveson, *Engineering a Safer World*

http://sunnyday.mit.edu/safer-world

(to be published by MIT Press, end of 2010)