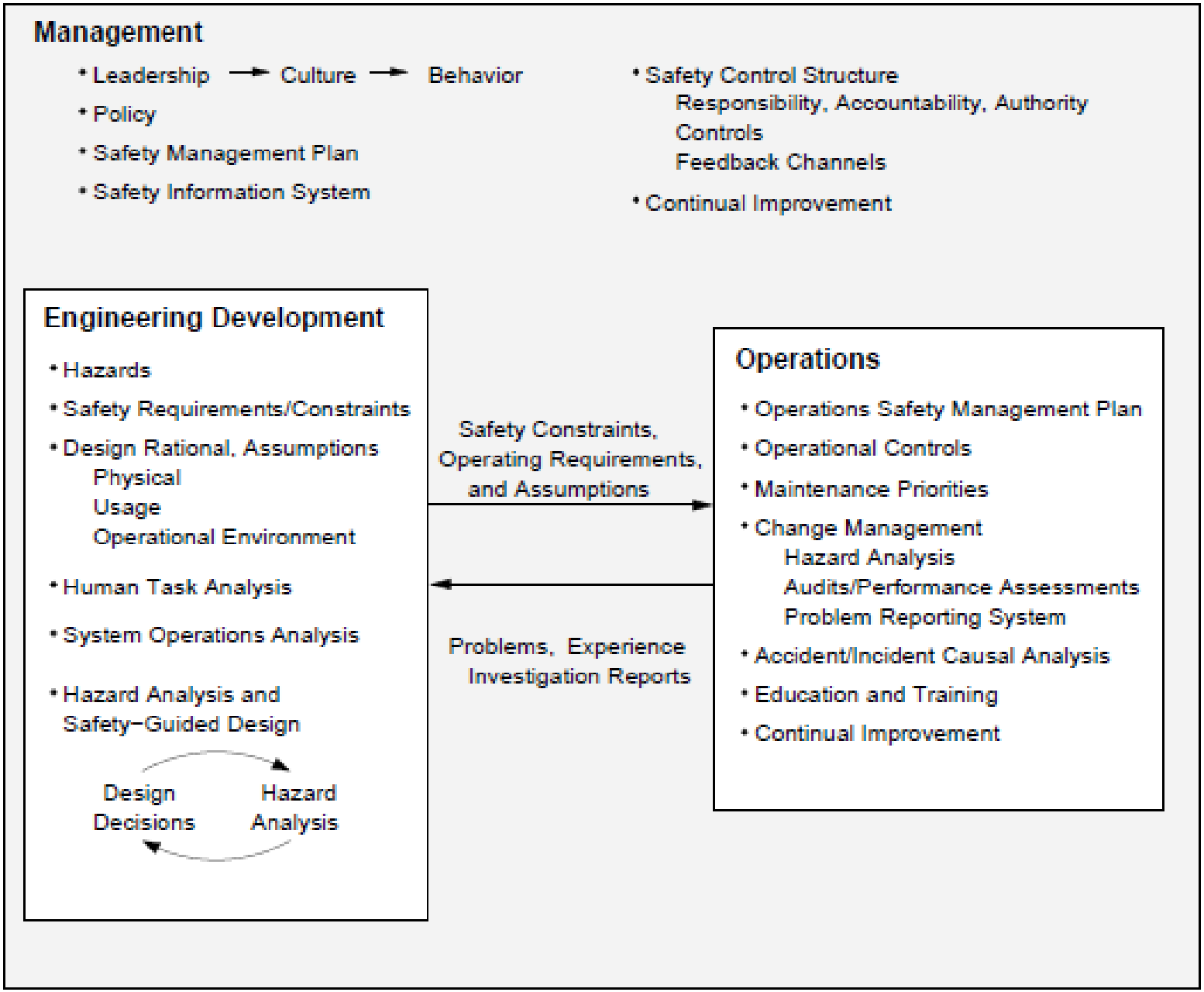
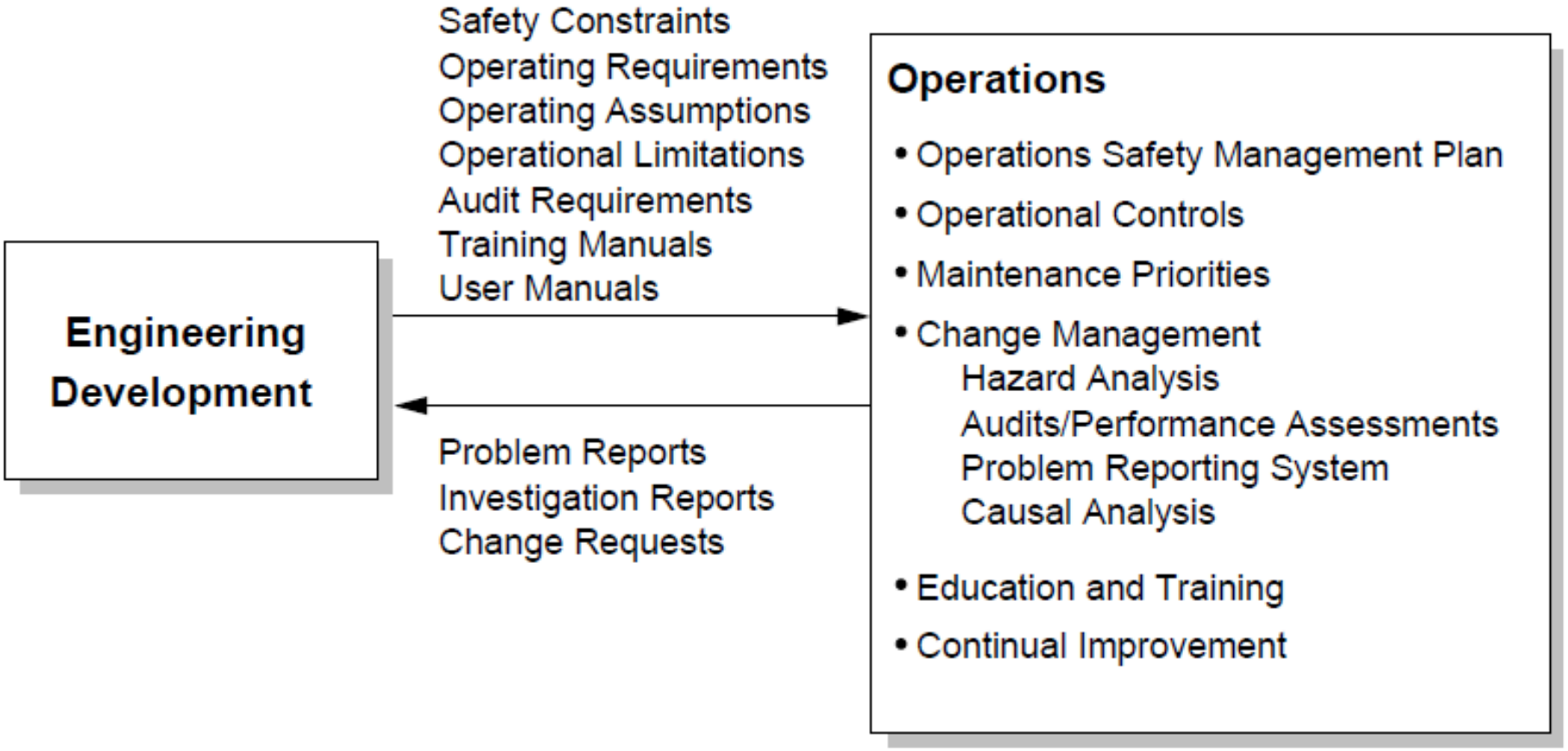


Safety in Operations



Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Managing/Controlling Change

- Adaptation or change is an inherent part of any system
- A common factor in accidents
- Was a change involved in any of the accidents you studied?
- Controls needed to:
  - Prevent unsafe changes
  - Detect them if they occur

Controls for Planned Changes

- Safety control structure must continue to be effective despite changes (including changes in environment, human behavior, organization)
- Most companies have management of change (MOC) procedures to evaluate impact on safety
  - Cost will depend on quality of documentation and how original hazard analysis done
  - MOC procedures are often skipped. Need to establish responsibility for enforcement

Controls for Unplanned Changes

- How might deal with unplanned and unsafe changes?

Controls for Unplanned Changes

- How might deal with unplanned and unsafe changes?
  1. Need to identify potential unsafe changes
  2. Need to respond (reduce risk)
- What is a leading indicator?

Controls for Unplanned Changes (2)

- Need to interrupt risk re-evaluation process before safety margins seriously eroded
  - Requires an alerting function to person with responsibility
  - Want to allow change as long as does not violate safety constraints
  - Key is to allow flexibility in how safety goals achieved and provide information that allows accurate risk assessment by decision makers.
  - Don’t allow waiving requirements. Re-evaluate them.
  - Establish appropriate feedback loops

Feedback Channels

- Information flow is key to maintaining safety
- Probably not general “leading indicators” but can identify system specific ones using safety constraints.
- Also need to ensure feedback channels are operating effectively. Cultural problems can interfere with feedback
- Three general types:
  - Audits and performance assessments
  - Reporting systems
  - Accident/incident causal analysis

Audits and Performance Assessments

- Starts from safety constraints and assumptions in safety design
- Need to audit entire safety control structure, not just lower levels
- Audit teams must be free of conflicts of interest
- Participatory and non-punitive audits

Accident/Incident Investigation

- CAST must be embedded in organizational structure that allows exploitation of results
- Training: Analysts must be managerially and financially independent.
  - Could use trained teams with independent budgets
  - Need to get away from blame
- Follow-up:
  - Ensure recommendations implemented and are effective
  - Findings should be input to future audits and performance assessments
  - If reoccurrence of same factors, investigate why

Reporting Systems

- If not being used, then find out why.
- Common reasons why not used:
  - Difficult or awkward to use
  - Information appears to go into a black hole. No point in reporting because organization won't do anything anyway
  - Fear information will be used against them
- Examples of successful systems:
  - Nuclear Power
  - Commercial Aviation

Encouraging Reporting

- Maximize accessibility
  - Reporting forms easily and ubiquitously available
  - Not cumbersome to fill in or send up
- Minimize anxiety
  - Written policy that explains
    - What reporting process looks like
    - Consequences of reporting
    - Rights, privileges, protections, and obligations
  - Without written policy, ambiguity exists and people will disclose less
- Act on reports and send information back (provide feedback)

Blame is the Enemy of Safety

- “My UK safety customers are incredibly spooked by [the Nimrod accident report] because of the way it singled out individuals in the safety assessment chain for criticism. It has made a very difficult process of assessing safety risk even more difficult.”

- People stop reporting errors and problems
  - Just Culture movement

Using the Feedback

- Information must be presented in form that people can learn from, apply to daily jobs, and use through system life cycle.
- Precursors almost always exist before major accidents
- Use to update process models, change control algorithms, modify safety control structure, update training and education

(Your operations plan for your project should include how feedback will be obtained and how it will be used)

Safety Information System

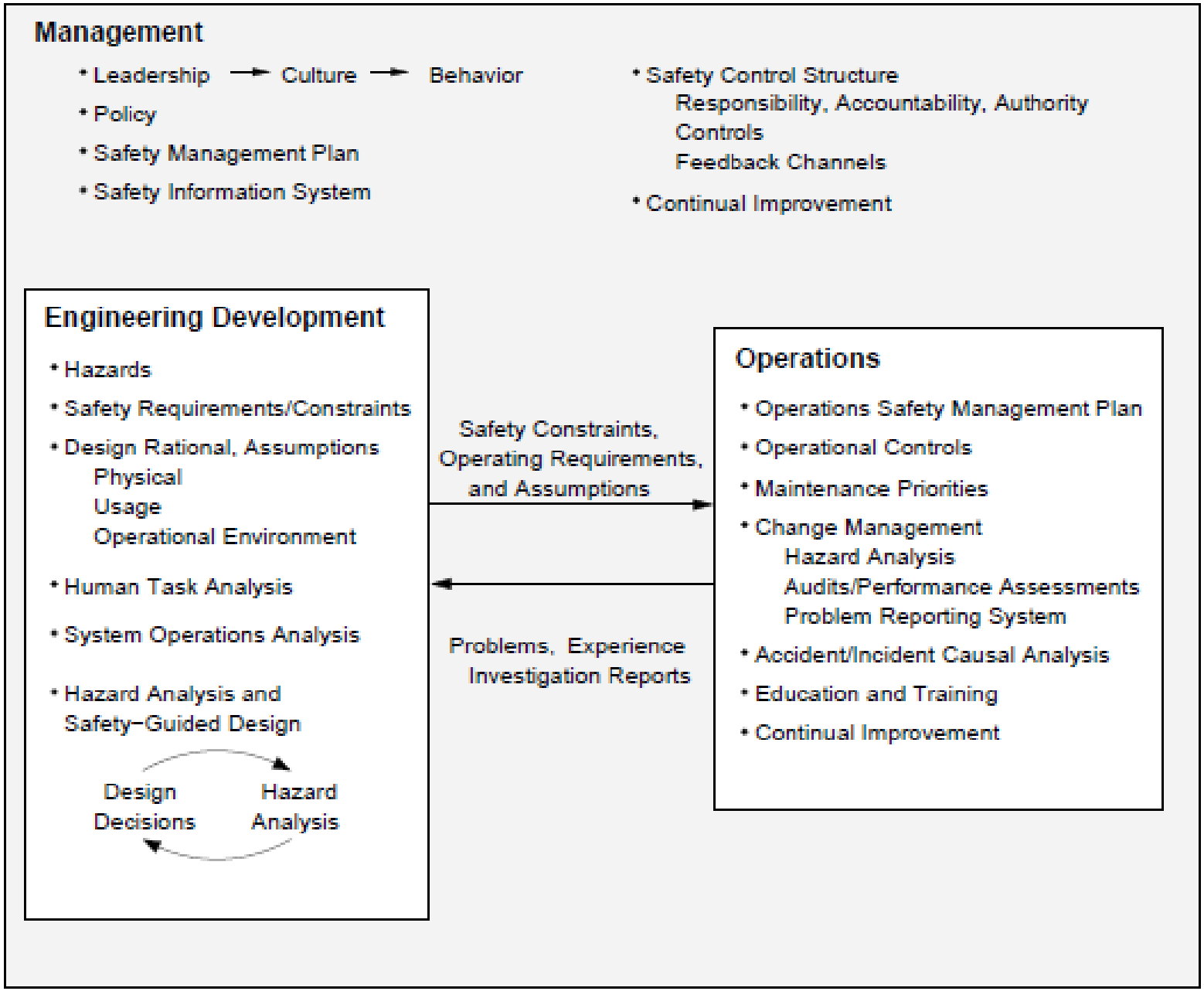
- Second in importance only to management commitment
- Creating and maintaining a successful one requires a culture that values the sharing of knowledge learned from experience (learning culture)
- Important source for identifying leading indicators of potential safety problems and as feedback on hazard analysis process.
- Need communication channels for getting info to those who can understand it and to those making decisions.

Safety Information System: Contents

- Updated safety plan
- Status of activities
- Hazard analysis (HAZOP) results and hazard logs
- Tracking and status information on all known hazards
- Incident and accident tracking
  - Reports
  - Corrective Actions (status)
  - Trend analysis
  - Lessons learned

Other Operations Topics

- Education and training
- Operations Safety Management Plan
- Implications of STAMP for occupational (workplace) safety



Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Major Ingredients of Effective Safety Management

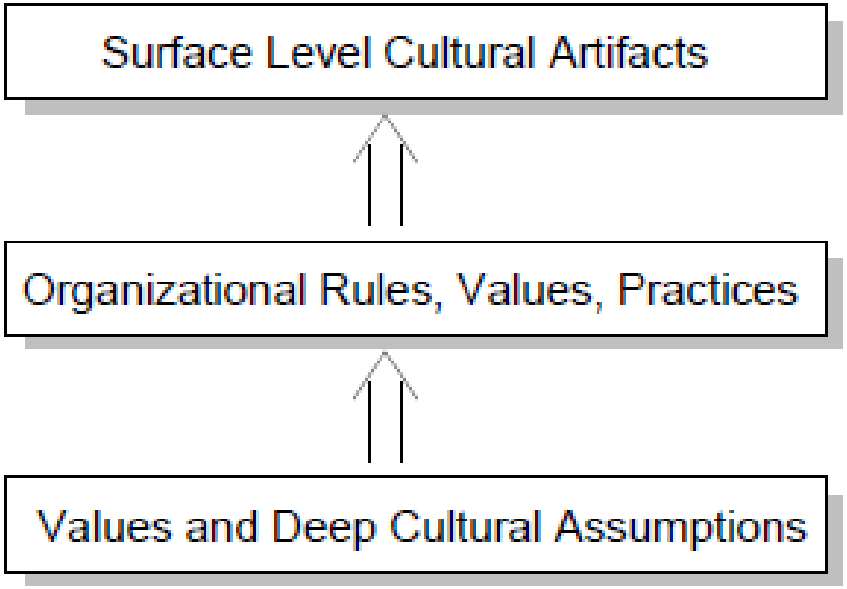
- Commitment and leadership
- Corporate safety policy
- Risk awareness and communication channels
- Controls on system migration toward higher risk
- Strong corporate safety culture
- Safety control structure with appropriate assignment of responsibility, authority, and accountability
- Safety information system
- Continual improvement and training
- Education, training, and capability development

Commitment and Leadership

- Management open and sincere concern for safety in everyday dealings
- Studies show management support for and participation in safety activities is most effective way to control and reduce accidents.
- Support shown by:
  - Personal involvement
  - Assigning capable people
  - Providing resources
  - Creating appropriate control structure
  - Responding to initiatives by others

What is Safety Culture?

Shein: The Three Levels of Organizational Culture



Safety culture is set by the leaders who establish the values under which decisions will be made.

Safety Culture

- Safety culture is a subset of culture that reflects general attitude and approaches to safety and risk management
- Trying to change culture without changing environment in which it is embedded is doomed to failure
- Simply changing organizational structures may lower risk over short term, but superficial fixes that do not address the set of shared values and social norms are likely to be undone over time.

Examples of Positive Cultural Values and Assumptions

- Incidents and accidents are valued as an important window into systems that are not functioning as they should – triggering causal analysis and improvement actions.
  - Safety information is surfaced without fear
  - Safety analysis is conducted without blame
- Safety commitment is valued

Example Cultural Values and Assumptions (2)

- There is a feeling of openness and honesty, where everyone's voice is valued. Employees feel managers are listening.
  - Trust among all parties (hard to establish, easy to break).
  - Employees feel psychologically safe about reporting concerns
  - Employees believe that managers can be trusted to hear their concerns and will take appropriate action
  - Managers believe employees are worth listening to and are worthy of respect.

Types of Flawed Safety Cultures

- Culture of Denial
  - Risk assessment is unrealistic
  - Credible risks and warnings are dismissed without appropriate investigation (only want to hear good news)
  - Believe accidents are inevitable, the price of productivity
- Compliance Culture
  - Focus on complying with government regulations
  - Produce extensive “safety case” arguments
- Paperwork Culture
  - Produce lots of paper analyses with little impact on design and operations

Culture of Denial Examples

- “Our accident rates are going down”
  - Look at worker injury rates: personal or occupational safety vs. system or process safety
  - Choose statistics that give best result
- “Accidents are the price of productivity. A dangerous domain”
- Mines: “Everyone has lots of safety violations”

Leadership is Key to Changing Culture

- Safety requires passionate and effective leadership
- Tone is set at the top of the organization
- Not just sloganeering but real commitment
- Setting priorities
  - Adequate resources assigned
  - A designated, high-ranking leader
- Minimize blame (“Just Culture”)
- Understand that safety and productivity are not conflicting if take a long-term view

Paul O’Neill and Alcoa

- "I intend to make Alcoa the safest company in America. I intend to go for zero injuries."
- “The board put a crazy hippie in charge and he's going to kill the company”

  “I ordered my clients to sell their stock immediately, before everyone else in the room started calling their clients and telling them the same thing. It was literally the worst piece of advice I gave in my entire career.”

Paul O’Neill and Alcoa (2)

- Within a year of O'Neill's speech, Alcoa's profits hit a record high and continued that way until he retired in 2000.
- All that growth occurred while Alcoa became one of the safest companies in the world.
- Understood that safety and productivity are not conflicting

Leadership is Key to Changing Culture (2)

- Minimize blame (“Just Culture”)
  - Blame is the enemy of safety
- Peer pressure can be effective
  - Moratorium after DWH
- Customers have more power than government
- Engineer the incentive structure to encourage the behavior you want

Food Safety Example

- New alliance of retailers, food growers, and farm workers
  - Workers had little incentive to report safety problems. Paid at a piece rate and taking even 10 minutes to report a safety problem would reduce their pay. One manager said that if workers spotted animal feces in an area where ripe strawberries were ready to be plucked, they might have still simply picked those berries.
  - Teach workers how to spot signs of food contamination and train in good practices in exchange for better pay and working conditions
  - “This program means that instead of one auditor coming around once in a while to check on things, we have 400 auditors on the job all the time.”

Food Safety Example (2)

- Unexpected benefit is worker retention

  "Sure, the money is important, but I also feel good because I am helping to improve quality and safety," Mr. Esteban said. "Those things are important to my family, too."

- Products carry certification to inform consumers

Safety Policy

- Reflects how the company or group values safety
- Should be easy to understand, easily operationalized
- Based on the way the company views safety: guiding principles (safety philosophy)

Corporate Safety Policy

- Provides a clear shared vision of organization's safety goals and values and a way to achieve them.
- Two parts:
  - Short and concise statement of
    - Safety values of organization
    - What is expected of employees with respect to safety
  - Details about how policy will be implemented
- Needs to be followed
  - Establish feedback channels
  - Monitor improvements
  - Identify, prioritize, and implement improvements

Example Operational Safety Philosophy (1) (Colonial Pipeline)

- All injuries and accidents are preventable.
- We will not compromise safety to achieve any business objective.
- Leaders are accountable for the safety of all employees, contractors, and the public.
- Each employee has primary responsibility for his/her safety and the safety of others.
- Effective communication and the sharing of information is essential to achieving an accident-free workplace.
- Employees and contractor personnel will be properly trained to perform their work safely.

Example Operational Safety Philosophy (2) (Colonial Pipeline)

- Exposure to workplace hazards shall be minimized and/or safeguarded.
- We will empower and encourage all employees and contractors to stop, correct and report any unsafe condition.
- Each employee will be evaluated on his/her performance and contribution to our safety efforts.
- We will design, construct, operate and maintain facilities and pipelines with safety in mind.
- We believe preventing accidents is good business.

Communication and Risk Awareness

- In general, risk is unknowable (severity X likelihood)
- In absence of hard evidence, tends to be evaluated downward over time
  - Delays between relaxation of controls and accidents
  - Complacency results from inadequate feedback and process models
- Using STAMP, risk is defined as a function of effectiveness of controls to enforce safe behavior

  Note this is potentially knowable
- Key is communication and feedback (reporting systems)

Controls on System Migration to Higher Risk

- Adaptation is predictable and potentially controllable
- Identify potential causes and institute controls
- Perform audits and performance assessments based on safety constraints identified during system development
- Anchor safety efforts beyond short-term program management pressures

Design Principles for Safety Control Structures

- Need clear definition of expectations, responsibilities, authority, and accountability at all levels of safety control structure
  - See new book for list of responsibilities that need to be assigned.

Safety Control Structure Design (2)

- Where should safety activities be put?
  - Safety permeates every part of development and operations
    - Need not be located in one place, but common methods and approach will strengthen the separate disciplines
    - If distributed, need a clear focus and coordinating body. Don't want fragmented, uncoordinated efforts.
  - Basic Principles:
    1. System safety needs a direct link to decision makers and influence on decision-making (*influence and prestige*)
    2. System safety needs to have *independence* from project management (but not engineering)
    3. Direct communication channels are needed to most of the organization (*oversight and communication*)

Safety Control Structure Design (3)

- Use of working groups for communication
  - Very effective in DoD
  - Different groups at different levels
  - Responsible for coordinating safety efforts at each level, reporting status of outstanding safety issues, providing information to other levels and to external review boards
  - Provides important information sharing: Changes in one subsystem may affect other subsystems and system as a whole

Summary: Safety Management System

- Key components
  - Management commitment
  - Management involvement
  - Employee empowerment
  - Incentive structures
  - Reporting systems
  - Organizational learning and improvement process

Effective Safety Management Systems

- Process safety is integrated into the dominant culture, not a separate sub-culture
- Safety is integrated into line operations: a mixture of top-down re-engineering and bottom-up process improvement
- Individuals have required knowledge, skills, and ability
- Organization has clearly articulated safety vision, values and procedures, shared among stakeholders
- Tensions between safety priorities and other system priorities are addressed through a constructive, negotiated process.
- Key stakeholders (e.g., unions) have full partnership roles and responsibilities regarding system safety
- Passionate, effective leadership at all levels committed to safety as a high priority for the organization

Safety Management System (2)

- Early warning systems for migration toward states of high risk are established and effective
- Effective communication channels exist for disseminating safety information
- Visibility of state of safety at all levels through appropriate feedback
- Results of operating experience, process hazard analyses, audits, near misses, or accident investigations are used to improve process operations and process safety management system.
- Deficiencies found during assessments, audits, inspections and incident investigation are addressed promptly and tracked to completion

16.683J / ESD.863J System Safety
Spring 2016