Systems Safety

PAME Workshop on Safety Culture

16 September 2012

Halifax, Nova Scotia, Canada

Donald Winter – University of Michigan

Department of Naval Architecture and Marine Engineering

Systems and Occupational Safety

- Both systems safety and occupational safety attempt to avoid accidents – events with unplanned and unacceptable consequences
  - Criteria for what is unacceptable varies with time
  - E.g. In late 19th century, US railroad industry experienced 2000 fatal coupling accidents per year – considered acceptable then
  - Acceptable limits for environmental damage changing in 21st century
- Systems safety refers to major accidents impacting multiple workers and/or the public
  - Low probability, high consequence events
  - Not well predicted by occupational safety statistics
  - Typically have complex causality related to unique system technology and/or design

Systems Safety is Hard to Manage

- Complex systems require a holistic approach
  - Subsystem interactions often dominate safety considerations
  - Off nominal conditions can cause accidents w or w/o component failure
- Safety measures and techniques far more complex and expensive than occupational safety approach
- Most systems safety issues not accessible to workers
  - Requires access to all relevant data and
  - Ability to assess complex interactions
- Structure of Offshore Oil and Gas industry complicates systems view
  - Dependency on drilling and service companies
  - Limited dissemination of data

Systems Safety is About Tradeoffs

- Starts with design and goes through well completion
- Must accommodate uncertainties
  - Geology, weather, materials, human factors etc
  - Development of margins of safety against total system risk
  - Risk must be assessed considering all elements of design and construction program
  - Risk must be reassessed as construction proceeds
- Inherent, material tradeoffs between systems safety and efficiency (cost and schedule) e.g.
  - Cost of BoP
  - Schedule impact of cement “squeeze”

Learning From History is Hard

- Typically, systems technology and applications are pushed until an accident occurs
- Investigated to determine cause and avoid repeat
  - Tendency to focus on identifying **the** direct cause
  - Lag in adoption of corrective measures – change is hard
- Learning peaks and then erodes w/ time
  - Memories and personnel change
  - Perception that changing technology obviates experience
  - Hubris builds
- Time frames vary
  - DC-10 cargo door: AA 96 (6/72) to TK 981 (3/74)
  - Titanic (4/1912) to Costa Concordia (1/2012)

Guidelines, Standards and Regulations

- Company, industry and regulator rules are rarely adequate
  - Complex systems rarely repeat a previous accident exactly
  - Levels of detail are invariably inadequate
- Attempts to provide systems safety by exhaustive rules lead to “affirmative defense” mentality
  - Compliance with rules constitutes defensible action whether or not system was safe
  - Limits corporate and personal liability
  - Psychology infects engineers, designers, workers, regulators

Safety Culture

- Culture is what you do when no one tells you what to do
- An effective safety culture establishes the priorities for safety vs cost & schedule trades
  - Those who claim safety is never compromised forget that the only way to achieve that is to do nothing
  - Hard to analytically justify cost to avoid low probability high consequence events
- Tradeoffs need to be conducted by many
  - From drilling engineer to tool pusher
  - From preparation to bid on lease to completion of well

Safety Culture Musts

- Safety priorities and expectations must be clearly stated and communicated to all
  - Management behavior and communication must be consistent at all levels and all times
  - Cannot ignore the inherent conflicts with efficiency
- All actions by management must be consistent
  - Assignments, promotions, compensation etc
  - Rewards for occupational safety do not offset undue pressures for cost and schedule performance
- Starts with CEO priorities and compensation incentives and goes through all levels of management
  - Typical management incentive programs don't work
  - Need zero/0ne multiplier or claw back provisions

Effective Safety Cultures

- An effective safety culture supports thoughtful tradeoffs of safety, cost and schedule throughout the design and implementation of complex systems
  - Sustained margins of safety
  - Timely and proper human decision making
- An effective safety culture supports institutions that can materially contribute to systems safety e.g.
  - Independent Technical Authorities
  - Real Time Operations Centers
- Safety cultures are hard to create but constitute irreplaceable avenues to systems safety