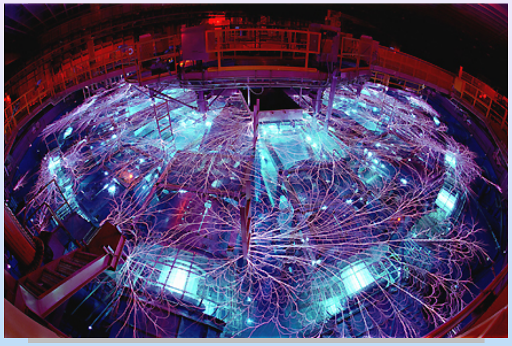
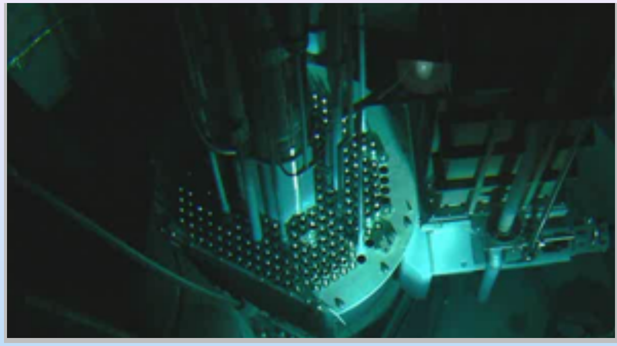
Exceptional service in the national interest

Sandia National Laboratories





Man-Made Catastrophes and Lessons for Risk-Based Decision Making

Ronald Allen Knief, PhD

SAND2016-1526 PE

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Risk-Based Decision Making

- Nuclear-(and RAK-) Centric Progression
  - Industry started out with a deterministic technical focus
  - Augmented by reliability engineering with statistical approach
  - In 1974 – probabilistic risk assessment (PRA) - WASH-1400
  - Subsequent developments made the approach increasingly more believable and useful.
  - Other method, for example:
    - Management Oversight and Risk Tree (MORT)
    - Addresses human factors of equipment handling and operation.

Risk-Based Decision Making

- Nuclear- (and RAK-) Centric Progression
  - Post TMI-2 – Risk management study
    - “Health & safety”
    - Functional capabilities (e.g., people and equipment)
    - Public image and reputation
    - Financial well-being
    - . . . and – more recently – security and safeguards
  - Special interest:
    - Nuclear safety pioneer Edwin Zebroski (1921-2010)
    - . . . sometimes it takes great catastrophes to bring about needed capabilities . . .”

Key "Talking Points"

I. Catastrophic "accidents" at:

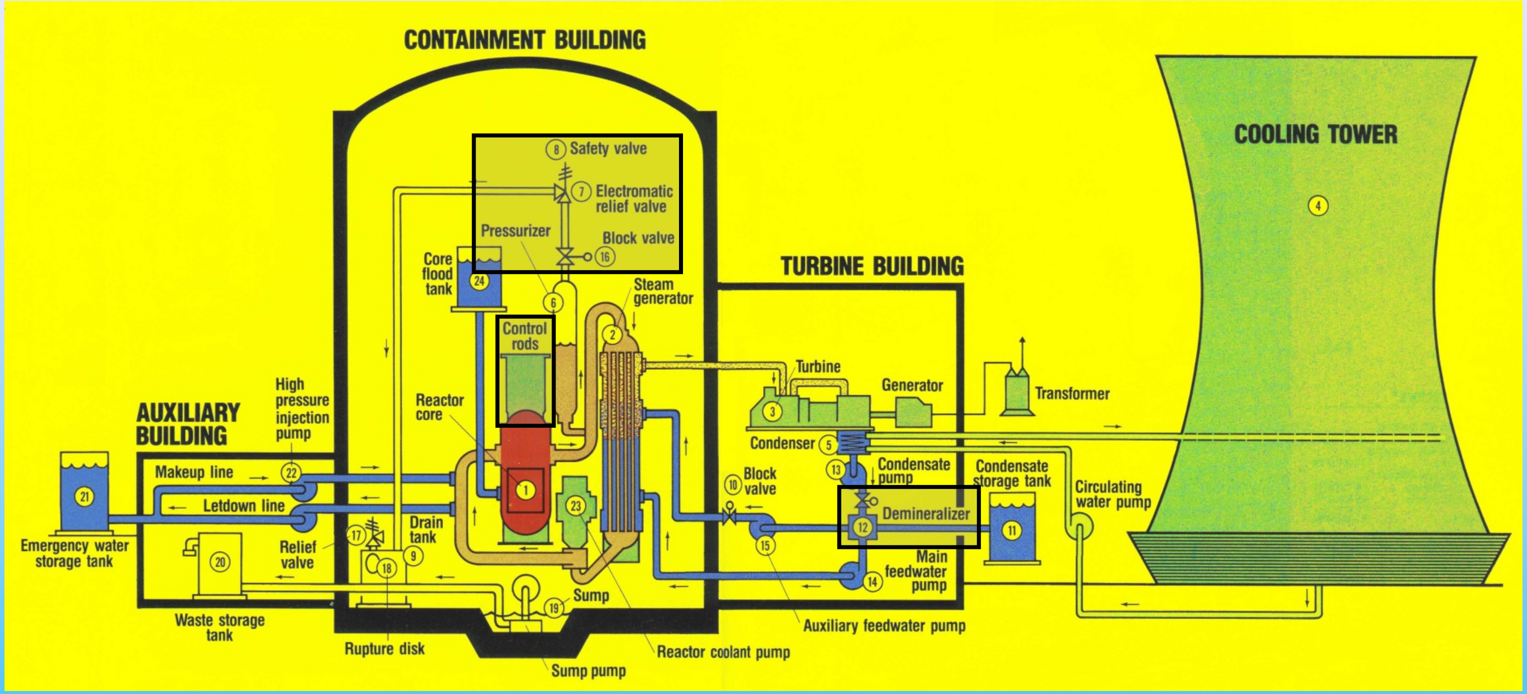
1. Three Mile Island, Unit 2 (TMI-2)
2. Bhopal
3. Challenger
4. Chernobyl, Unit 4

II. Eleven (11) causal factors common to these and other technological and economic "accidents"

Three Mile Island, Unit 2

[March 28, 1979]

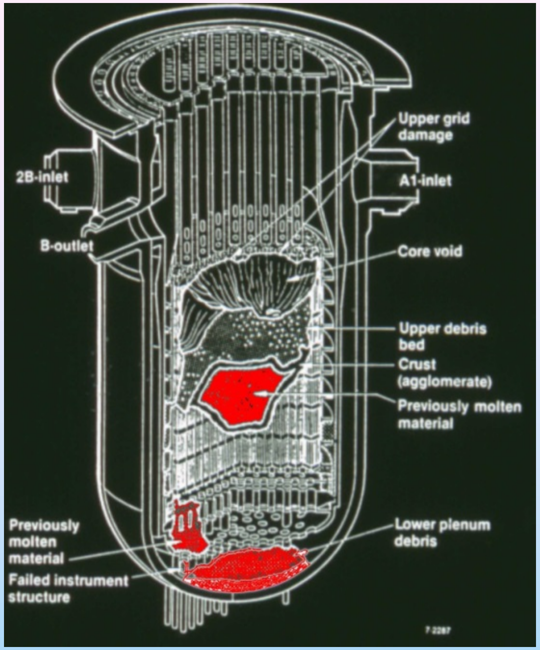
- SCENARIO
  - 4:00-8:00 AM
  - Reactor experienced upset

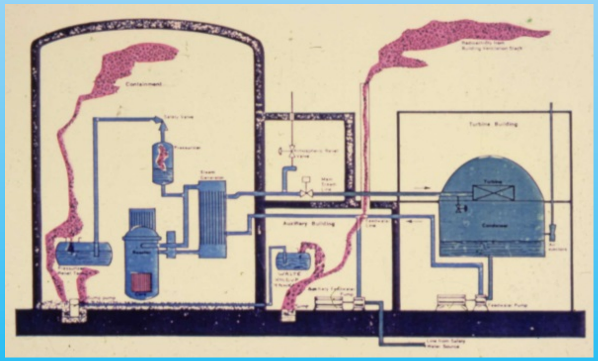


  - Shutdown (control rod “scram” . . .) as designed
  - Relief valve stuck leading to prolonged loss of coolant water inventory

Three Mile Island

- SCENARIO
  - Lacking coolant, core fuel and cladding tubes overheated and were damaged
  - A sizable fraction of the fuel melted – some in place, some flowing to the bottom of the reactor vessel.
  - Hydrogen and gaseous radioactivity (xenon and krypton) were liberated to the conltainment building
    - Hydrogen exploded but did not breach the containment building
    - Some radioactive noble gasses (Xe and Kr) escaped (the remainder later were vented via controlled release)





Three Mile Island

- CONSEQUENCES
  - Environmental
    - Statistically 0-1 additional cancer cases
    - “Public apprehension”
  - Functional/Financial
    - Loss of TMI-2 reactor
    - Clean-up costs
    - 6.5-yr to restart TMI-1

Three Mile Island

- Key Decision Points
  1. Project was initiated in response to projected load growth in the PA-NJ area
     - TMI-1 in 1974
     - TMI-2 in 1978 after move from initial NJ site
  2. Babcock & Wilcox (B&W) selected as the reactor designer and supplier
     - Had the fewest nuclear reactors of three U.S. vendors
     - Unique "once through" steam generator
       - More sensitive control of feedwater flows
       - More complex and sensitive control of startup and shutdown

Three Mile Island

- Key Decision Points

3. The Presidential Commission study of the accident noted that:
   - Organization – and, to some extent, Nuclear Regulatory Commission (NRC) – had “mindset" that a severe-damage event could not happen

4. Some of the unstated assumptions – from operator perspective – that contributed to the accident were:
   - Compliance was viewed as assuring safety
   - Lack of systematic reporting, documenting and correcting minor accidents, failures, or deficiencies
   - Operators had limited use of a “generic” simulator; focused on routine ops rather than serious accidents
   - Control room instrument & control devices were also designed for routine operation, not unusual events . . .let alone severe accidents

Bhopal Chemical Plant (India)

[December 1984]

- SYSTEM
  - Chemical Plant Built by U.S.' Union Carbide Company
  - Operated by an local affiliate
- SCENARIO
  - Water inadvertently introduced into large tank containing 45 tons of methyl isocyanate (MIC) contaminated with chloroform
  - Resulting exothermal reaction
  - Mixture was vented to the atmosphere through a relief valve
  - Key safety systems - protective scrubbers and flares to control MIC vapors – did not function

Bhopal

Sandia National Laboratories

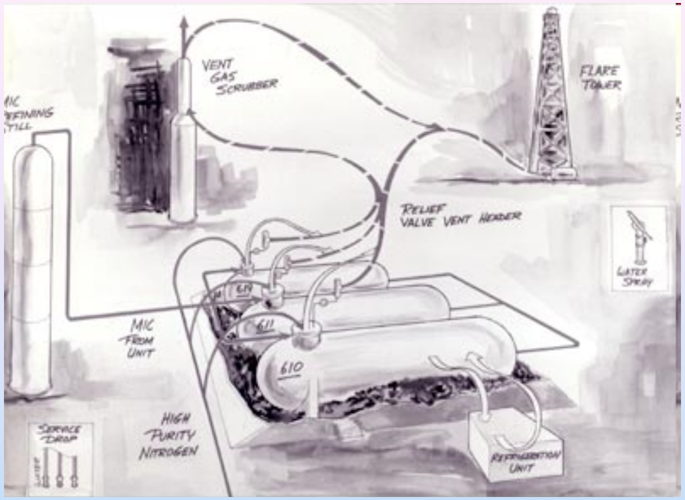
- CONSEQUENCES
  - Ton-quantities of toxic, volatile methyl isocyanate (MIC) escaped to the environment
  - ~20,000 people were sickened by the exposure
    - ~2,000 died within the first two or three weeks.
    - 10 to 15 people died each month for several months after the accident
  - Some health effects persist, involving respiratory insufficiencies

Bhopal

- Key Decision Points
  1. Location in India
     - Large market for the pesticide carbaryl for agriculture
     - Required local majority participation in construction & operation
     - Divided responsibilities developed
       - Managing & monitoring operations policies
       - Personnel selection, supervision, and training
  2. Design and construction
     - Entirely Union Carbide
     - Well-thought-out protective features . . .
     - . . . Incomplete design-basis scenarios, e.g.,
       - Corrosion effects
       - Water & contaminant ingress “sneak circuits”

Bhopal

- Key Decision Points
  3. Operational supervision & audit
     - Confused responsibility
     - Routine safety reviews
       - Did not address deviations from procedures, product specifications, and preventive maintenance
       - Ineffective follow up



  4. Systematic analysis and training for severe events
     - Emergency procedures and drills for leaks & fire
     - . . .not low-probability-high-consequence conditions
     - Procedures & training did not address combinations of minor deficiencies
     - Alarms/sirens same for routine & accident

Bhopal


BHOPAL DISASTER 1984 TO?
THE SUFFERING CONTINUES.
SO DOES THE STRUGGLE.

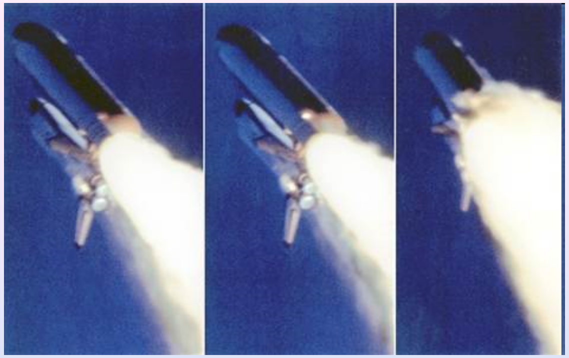
Challenger Space Shuttle

[January 28, 1986]

- SYSTEM
  - "Orbiter"

    With
  - Main engines (3)
  - External tank (150 ft x 30 ft)
    - Liquid O (1.6M lb)
    - Liquid H (0.25M lb)
  - Solid rocket boosters (2)

Challenger



- SCENARIO
  - The shuttle broke apart 73 seconds into its flight and disintegrated over the Atlantic Ocean
  - Initiator: O-ring seal in the right solid rocket booster (SRB) failed at liftoff.
  - Ensuing structural damage of the main propulsion rocket released hydrogen and oxygen and produced a massive explosion.

- CONSEQUENCES
  - Deaths of its seven crew members
  - Loss of the shuttle
  - The spectacular and tragic explosion of the shuttle booster soon after launching viewed by hundreds of millions of people

Challenger

- Key Decision Points

1. Conflicting specifications for capabilities for launching:
   - Commercial & military satellites
   - Variety of low & high orbits
   - Manned space flight, space station assembly & supply

   Excluded continuing development & deployment of expendable launch vehicles
2. Boosters
   - Hydrogen-fueled-main & strap-on, solid-fuel boosters
   - Maintain target payload size and weight
   - Precluded launch-abort personnel-survival features
   - Acceptable risk
     - Working assumption: *Large variety of potential failures on launch would be infrequent*
     - Simple launch-failure statistics: *At least one failure in 20 or 30 launches*

Challenger

- Key Decision Points

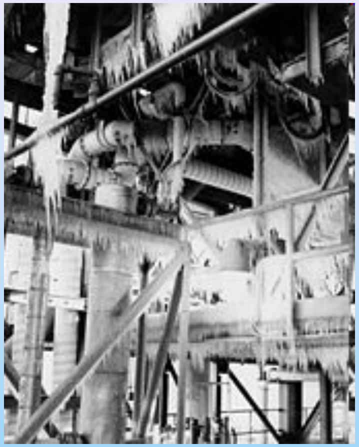
3. Decision-making and organizational situation
   - "Common cause failure of perception" – reluctance to use systematic risk analysis
     - Available and proven techniques
     - Effectively used in the unmanned space program
     - Budget or schedule constraints not the issue
     - Resisted use of systematic, integrated risk assessment

       & associated corrective processes

4. Organizational responsibility for systems safety
   - Not adequately integrated & available at decision-making levels
   - Complex program involved many different contractors
   - Intensive quality control and quality assurance

Challenger

- Key Decision Points
  4. Organizational responsibility for systems safety [cont.]
     - No structure to integrate safety and compliance – e.g., "O“-ring:
       - Safety margins and temperature limits
       - Several organizational levels
       - At least two contractual interfaces removed from schedule & “go-ahead for launch” decisions

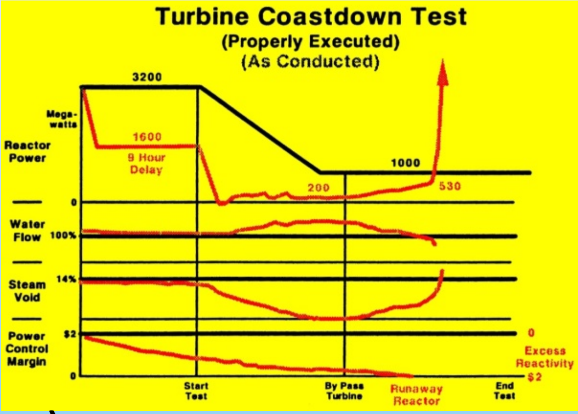


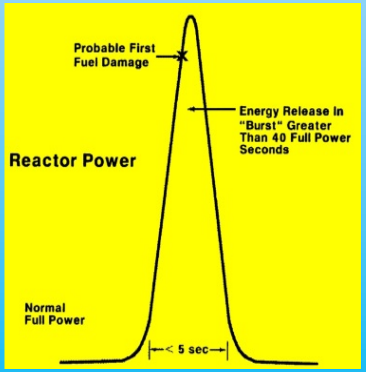
  5. Organizational responsibility for systems safety
     - Memoranda & analyses raised performance & safety concerns
       - Delayed transmission up organization chains
       - Numerous stages of editing; potential vetoes
     - Rejected use of PRA/PSA
       - Results would be politically unacceptable
       - Prevented focus on dominant risk contributors

Chernobyl Nuclear Station

[April 25, 1986]

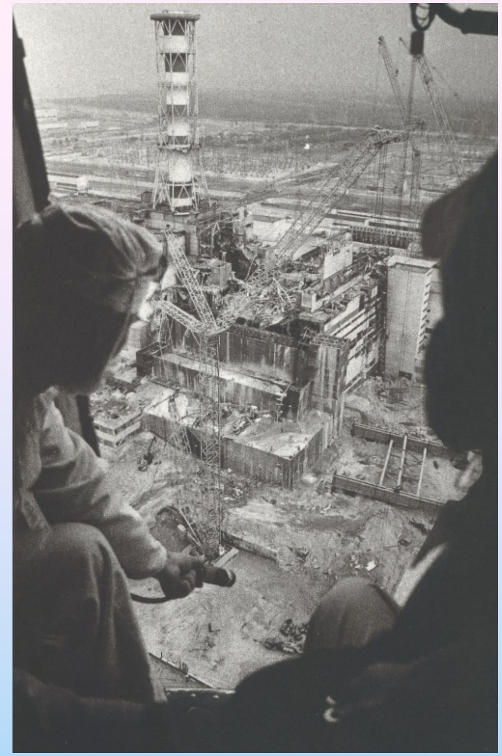
- SCENARIO
  - Test to increase safety & reliability post-shutdown
  - Test started, but quickly delayed due to need for electric power by the local grid
  - Test resumed after multi-hour delay
  - Unstable conditions – Operators:
    - Mis-performed operations
    - Disabled safety systems (possible re-test)
    - Attempt to shut down reactor
      – “Positive scram”
      – “Prompt supercritical excursion” (100 times full power)

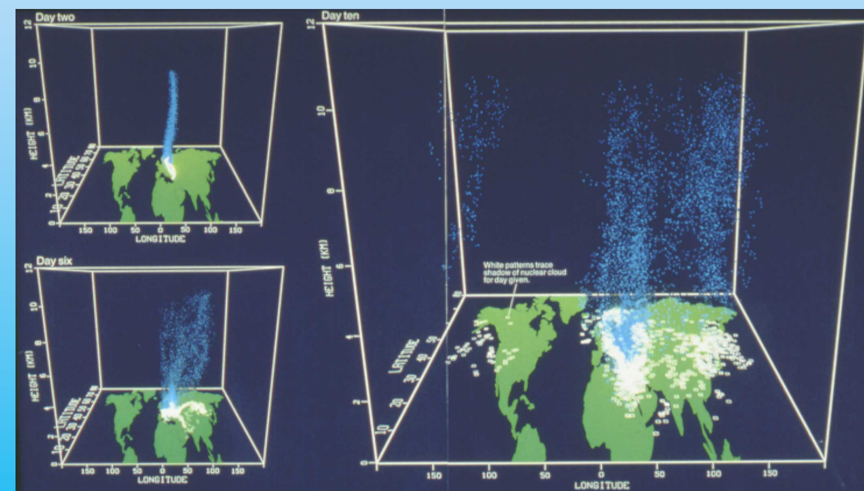




Chernobyl

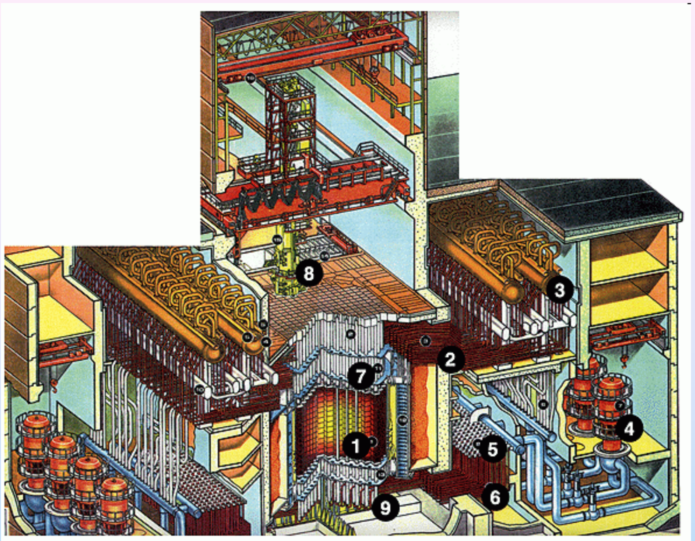
- CONSEQUENCES
  - Reactor destroyed by steam explosion
  - Containment breached and tons of fuel expelled
  - Radioactive contamination
    - Very heavy in three Soviet states
    - Of concern in nearby countries
  - ~50 direct fatalities





Chernobyl

- Key Decision Points
  1. Goals & objectives of Chernobyl RBMK design
     - Dual-purpose reactor
       - Weapons-grade Pu or ^{3}T
       - Steam-electric
     - Expensive – Complex – Large



  2. On-line refueling led to:
     - Low-enrichment fuel in pressure-tubes; widely-spaced in graphite-block moderator
     - Complex plumbing
     - Neutron-chain reaction with positive feedback
       - Routine – computer/“fly by wire”
       - Manual – complex/difficult for operators
     - Shutdown w/ “positive scram” & prompt supercritical

Chernobyl

Sandia National Laboratories

- Key Decision Points
  3. Omit full (PWR-like) containment
     - Consequence of dual Pu-power decision
     - RBMK containment was "industrial" & protected reactor
     - NOTE: Soviet PWRs have "full," robust containment
  4. Review, audit & enforcement of safety and procedures
     - Superficial at best
     - Test procedure (precipitated the accident)
       - Not detailed
       - Not subject to safety-engineer review & approval
     - Improvised steps & disabling safety systems
     - Exceeded specified operating limits ("tech specs")

Chernobyl

- Key Decision Points
  5. TMI-2 "lessons learned" were ignored
     - *". . . this [TMI-2] accident could only have happened in a capitalist country, where profit is more important than safety."*
       – Academician A. Aleksandrov, President of the USSR Academy of Sciences and Director of the Kurchatov Institute as stated in *Pravda*
     - Assumed that their trained operators (5-1/2-yr engr degree) could not make extended errors – conceptual or procedural
     - Severe events not addressed
  6. Control room layout convenient for routine operation
     - Lacked attention to recognize/manage severe accidents
     - Slow response times - important readings only from teletype
     - Safety system bypass/disable w/switches – w/o scram

Common Accident Lessons

Sandia National Laboratories

1. Diffuse responsibility; rigid procedures and communication channels; & large organizational distances between decision makers and "the plant"
2. “Mindset” existed that success is inevitable or routine; severe inherent risks neglected
3. Belief that rule compliance is enough to assure safety
4. Team-player characteristics highly valued
   - Strong emphasis on commonality of experience and viewpoint
   - Dissent not allowed even for evident risk
5. Relevant experience from elsewhere not reviewed systematically

Common Accident Lessons

6. Lessons learned – local and external – were not applied
7. Performance goals & priorities valued over safety analysis
8. Effective emergency procedures, training, and drills for unusual or severe conditions were absent
9. Acceptance of design and operating features involving recognized hazards that were controlled or avoided elsewhere
10. Available project management techniques for systematic risk assessment and control were not used
11. Organizational responsibilities and authorities for recognizing and integrating safety matters were undefined

And more . . .

- Piper Alpha
- Shuttle Columbia
- Henderson Rocket-Fuel Plant
- World Trade Center
- Enron
- BCCI

Sandia National Laboratories

QUESTIONS?