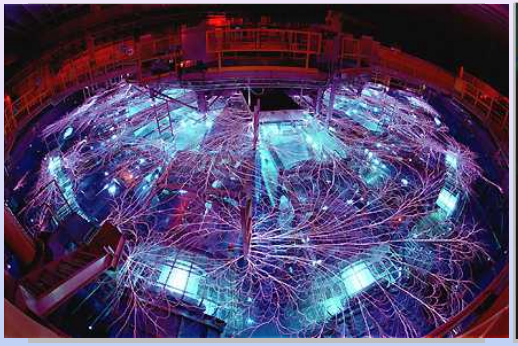
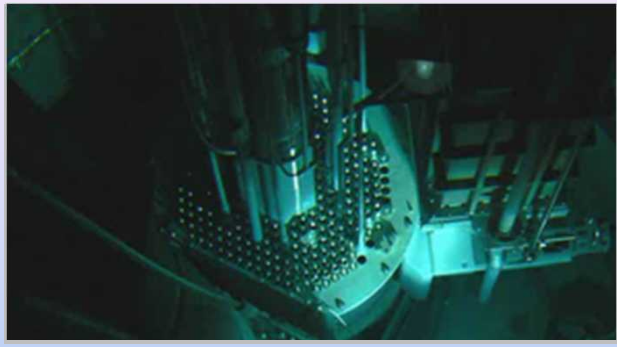
SAND2016-1526PE

Exceptional service in the national interest

Sandia National Laboratories





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

Ronald Allen Knief

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.

Objectives

I. Identify important features of the catastrophic "accidents" at each these locations:
   1. Bhopal
   2. Challenger
   3. Chernobyl
   4. Three Mile Island (TMI)
   5. Others (Piper Alpha, WTC, Shuttle Columbia, Henderson)

II. Explain eleven (11) causal factors common to these accidents and identify key examples for each

Key Organizational Characteristics

Sandia National Laboratories

- Organization characteristics influenced by:
  - Degree of success or failure (private and public organizations)
  - Attributes for success or failure in maintaining safety of operations
- Correlation between catastrophes and organization attributes
  - Use well-defined and readily observable case studies
  - Special focus on major historiacal catastrophes
- Specific engineering events considered here
  - Subject to intensive and extensive study
    - Sequence of events
    - Contributing factors
    - Correlate directly with “mirror image” “good practices” (e.g., as applied by nuclear, chemical, aircraft, and maritime industries
  - This talk from risk management studies by E. L. Zebroski

References

Zebroski, E. L., "Sources of Common Cause Failures in Decision-Making Involved in Man-Made Catastrophes," *Advances in Risk Analysis*, Vol. 7 (1989), Plenum Publishing Corp. pp 443-454

Zebroski, E. L., "Lessons Learned from Man-Made Catastrophes," in R. A. Knief (ed.), *Risk Management: Expanding Horizons in Nuclear Power and Other Industries*, Hemisphere Publishing Corp., New York, 1991

Zebroski, E.L., "Risk Management Lessons from Man-Made Catastrophes Implications for Anti-Terrorism Risk Assessments," in R. A. Knief (ed.), *Risk Management for Tomorrow's Challenges*, American Nuclear Society, 2011.

Bhopal, India

- Scenario
  - Chemical plant
    - Built by Union Carbide Company
    - Operated by an Indian affiliate
  - Accident December 1984
  - Progression
    - Inadvertent introduction of water into large tank containing 45 tons of methyl isocyanate (MIC) contaminated with chloroform
    - Reaction of water with the isocyanate overheated the tank contents
    - Mixture vented to the atmosphere through a relief valve
    - Scrubbers and flares to control MIC vapors did not function

Bhopal, India

- Scenario
  - Chemical plant
  - Accident December 1984
  - Progression
  - 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, India

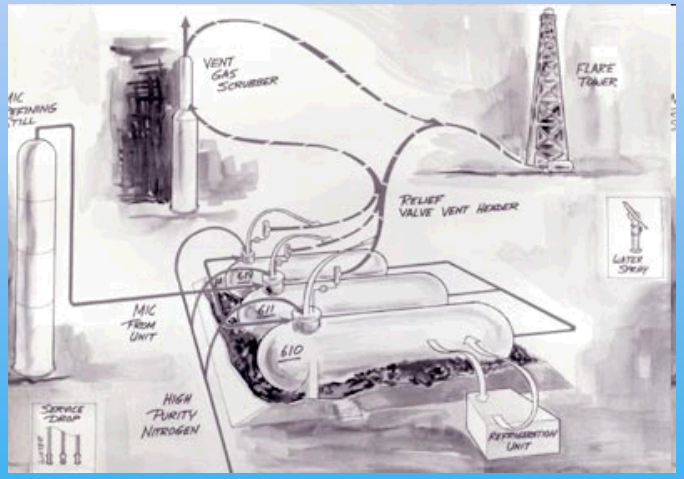
- Key Decision Points
  1. Location in India
     - Large market for the pesticide carbaryl for agriculture
     - Required local majority participation in construction & operation
     - Divided responsibilities developed
       - Managing and monitoring operations policies
       - Personnel selection, supervision, and training
       - Practices eroded with departure of startup crew by 1982

Bhopal, India

- Key Decision Points
  2. Design and construction
     - Entirely under Union Carbide control and supervision
     - Included well-thought-out protective features (e.g., for temperature, venting, bunkering)
     - Incomplete design-basis scenarios assumptions for protective systems were incomplete
       - Chemical reactions
       - Corrosion effects
       - Water & contaminant ingress “sneak circuits”

Bhopal, India

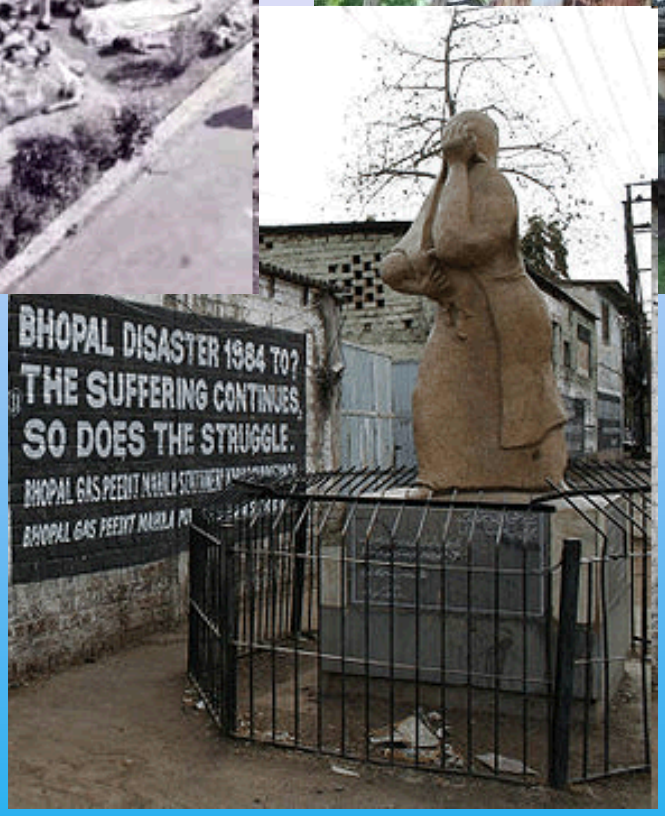
- Key Decision Points
  3. Operational supervision & audit
     - Confused responsibility for plant operation
       - Indian affiliate Union Carbide, Ltd
       - Union Carbide Company (majority owner)
     - Routine safety reviews
       - Did not address deviations from procedures, product specifications, and scheduled preventive maintenance
       - Ineffective follow up



Bhopal, India

- Key Decision Points
  4. Systematic analysis and training for severe events
     - Emergency procedures and drills
       - Leaks of toxic gases (e.g., phosgene used in MIC production)
       - Fire control measures
     - No systematic analysis of low-probability-high-consequence conditions
     - Procedures & training did not sensitize plant personnel that seemingly minor deficiencies could combine to produce major disaster
     - No distinction of alarms/sirens for routine & accident purposes

Bhopal, India

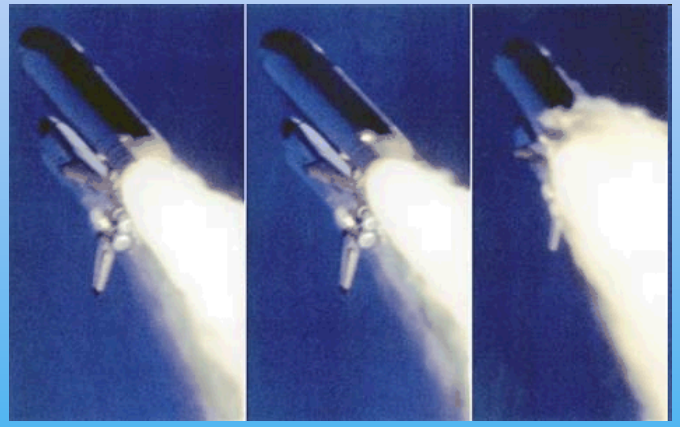


COMMON ATTRIBUTES OF CATASTROPHES

#	ATTRIBUTE	Description	Bhopal
1.	Diffuse Responsibilities	Rigid communication channels Large organizational distances from decision-makers to plant	X
2.	Mindset	. . .that success is routine Neglect severe risks present	X
3.	Rule Compliance	Assume compliance assures safety	(X)
4.	Team Player Emphasis/ Agreement	Dissent on risks discouraged	X
5.	Experience/Lessons from Events	No process for learning from other's experiences	X
6.	Priority to Production/Output Goals vs Safety Improvements		X
7.	Lessons Learned Disregarded/ Narrow Experience	Neglect of precautions widely adopted elsewhere after learning from significant events	X
8.	Design & Operating Features/ Known Hazards	Hazards recognized as avoidable allowed to persist	X
9.	Emergency Procedures for Severe Accidents	Lack of plans, procedures, training or regular drills for severe events	X
10.	Project & Risk Management Techniques	Available methods for hazard and risk assessment not used	X
11.	Organization/Safety Integration	Responsibilities and authorities for recognizing and integrating safety matters undefined	X

Challenger

- Scenario
  - Space Shuttle
  - Accident January 28, 1986
  - Progression
    - The shuttle broke apart 73 seconds into its flight and disintegrated over the Atlantic Ocean
    - The process began after an 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.



Challenger

Sandia National Laboratories

- Scenario
  - Space Shuttle
  - Accident January 28, 1986
  - Progression
  - Consequences
    - Deaths of its seven crew members
    - Loss of the shuttle
    - The spectacular and tragic explosion of the shuttle booster soon after launching was viewed by hundreds of millions of people

Challenger

Sandia National Laboratories

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

     Excluded continuing development and deployment of expendable launch vehicles

Challenger

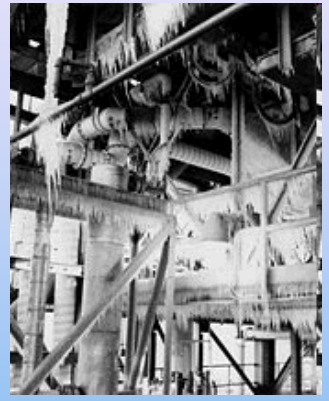
- Key Decision Points
  2. Boosters
     - Proceeded with hydrogen-fueled main booster and strap-on solid fuel boosters
     - Maintaining target payload size and weight
     - Precluded launch abort personnel survival features
     - Working assumption that any of the large variety of potential failures on launch would be so infrequent as to be an acceptable risk
       - Launch failure statistics from considerably simpler systems tended to support estimates of at least one failure in 20 or 30 launches
         (Essentially the level reached at the time of the Challenger accident)

Challenger

- Key Decision Points
  3. Decision-making and organizational situation
     - "Common cause failure of perception" in reluctance to use systematic risk analysis
       - Available and proven technique for recognizing and managing risk exposures
       - Readily available (effectively used in the unmanned space program)
       - Would not have been appreciably limited by budget or schedule constraints
     - Resulted in resistance to use of systematic integrated risk assessment techniques and the associated corrective processes

Challenger

- Key Decision Points
  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
     - No structured process 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

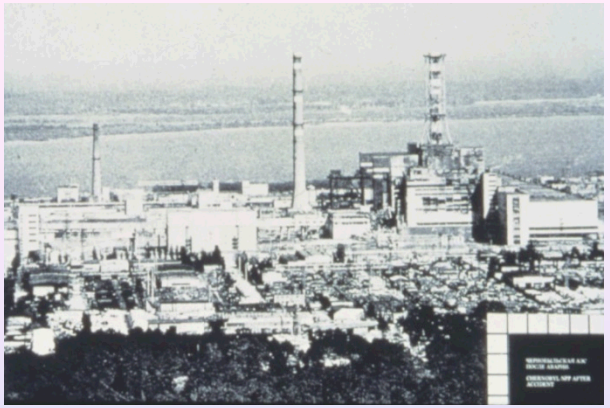


     - Memoranda and analyses raising performance & safety concerns
       - Delays in transmission up the organization chains
       - Numerous stages of editing and potential vetoes
     - Rejected use of PRA/PSA
       - Considered results would be politically unacceptable
       - Prevented focus of attention on dominant risk contributors

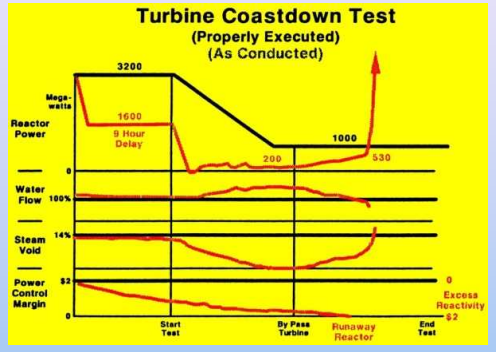
COMMON ATTRIBUTES OF CATASTROPHES

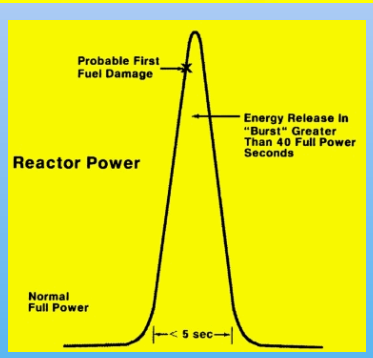
#	ATTRIBUTE	Description	Bhopal	Challenger
1.	Diffuse Responsibilities	Rigid communication channels Large organizational distances from decision-makers to plant	X	X
2.	Mindset	. . .that success is routine Neglect severe risks present	X	X
3.	Rule Compliance	Assume compliance assures safety	(X)	X
4.	Team Player Emphasis/ Agreement	Dissent on risks discouraged	X	X
5.	Experience/Lessons from Events	No process for learning from other's experiences	X	X
6.	Priority to Production/Output Goals vs Safety Improvements		X	X
7.	Lessons Learned Disregarded/ Narrow Experience	Neglect of precautions widely adopted elsewhere after learning from significant events	X	X
8.	Design & Operating Features/ Known Hazards	Hazards recognized as avoidable allowed to persist	X	X
9.	Emergency Procedures for Severe Accidents	Lack of plans, procedures, training or regular drills for severe events	X	X
10.	Project & Risk Management Techniques	Available methods for hazard and risk assessment not used	X	X
11.	Organization/Safety Integration	Responsibilities and authorities for recognizing and integrating safety matters undefined	X	X

Chernobyl



- Scenario
  - Nuclear Power Reactor
  - Accident April 25, 1986
  - Progression
    - Test scheduled that could validate a reliable means of supplying post-shutdown power
    - Test started but delayed for load-management purposes leaving the unit in an increasingly unstable condition
    - Test resumed after extended delay
    - Unstable conditions led operators to mis-perform operations and disable safety systems to allow re-run of test if necessary
    - Eventual attempt to shutdown reactor led to opposite result – “prompt supercritical excursion” (100 times full power)

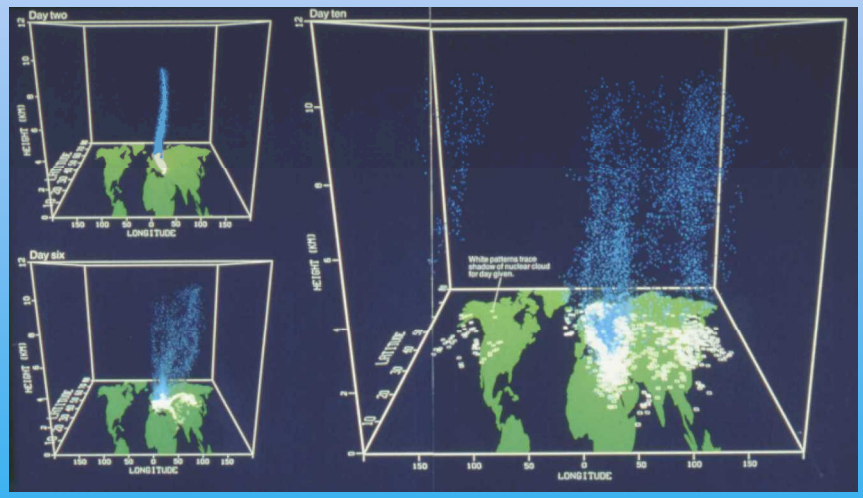




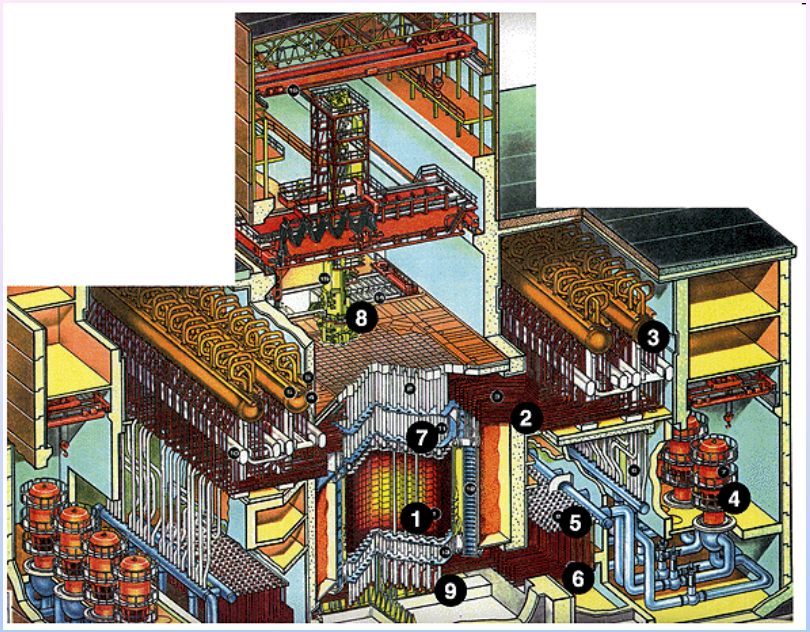
Chernobyl

Sandia National Laboratories

- Scenario
  - Nuclear Reactor
  - Accident April 25, 1986
  - Progression
  - 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



Chernobyl



- Key Decision Points
  1. Goals and objectives of
     – RBMK – design
     - Dual-purpose reactor capable of making:
       - Weapons-grade plutonium or tritium
       - Steam for electric power production and district heating
     - "Penalties"
       - Economic - much lager physical plant than for power-only production
       - Complex (and relatively dangerous) machine for on-power refueling required for Pu production
       - Too large for western steel-reinforced concrete containment building

Chernobyl

- Key Decision Points

2. Retaining plutonium production capability also required pressure-tubes with fuel widely spaced in graphite blocks
   - Plumbing layout more convenient
   - Led to neutron-chain reaction with positive feedback - unstable (requires computer to “fly by wire;” manual operation difficult)
   - Control shutdown system also unstable – led to “positive scram” and prompt super critical”

Chernobyl

- Key Decision Points
  3. Review, audit and enforcement of safety practices and procedures
     - Superficial at best
     - Test procedure that precipitated the accident was not detailed and subject to review and approval by qualified safety engineers
       - Improvised steps (e.g., excessive withdrawal of control rods) were improvised
       - Disabled several safety systems
       - Exceeded specified operating limits

Chernobyl

- Key Decision Points
  4. TMI-2 “lessons learned” were ignored.
     - Assumed that their trained operators (5-1/2-year engineering degree) could not make extended errors – both conceptual and procedural.
     - Severe events not addressed.
  5. Control room instrumentation and controls layout convenient for routine operation
     - Lacked attention to information needed to recognize/manage severe accidents
     - Slow response times
     - Important readings available only from teletype
     - Safety systems could be bypassed or disabled from switches – w/o causing reactor shutdown

COMMON ATTRIBUTES OF CATASTROPHES

#	ATTRIBUTE	Description	Bhopal	Challenger	Chernobyl
1.	Diffuse Responsibilities	Rigid communication channels Large organizational distances from decision-makers to plant	X	X	X
2.	Mindset	. . .that success is routine Neglect severe risks present	X	X	X
3.	Rule Compliance	Assume compliance assures safety	(X)	X	X
4.	Team Player Emphasis/ Agreement	Dissent on risks discouraged	X	X	X
5.	Experience/Lessons from Events	No process for learning from other's experiences	X	X	X
6.	Priority to Production/Output Goals vs Safety Improvements		X	X	X
7.	Lessons Learned Disregarded/ Narrow Experience	Neglect of precautions widely adopted elsewhere after learning from significant events	X	X	X
8.	Design & Operating Features/ Known Hazards	Hazards recognized as avoidable allowed to persist	X	X	X
9.	Emergency Procedures for Severe Accidents	Lack of plans, procedures, training or regular drills for severe events	X	X	X
10.	Project & Risk Management Techniques	Available methods for hazard and risk assessment not used	X	X	X
11.	Organization/Safety Integration	Responsibilities and authorities for recognizing and integrating safety matters undefined	X	X	X

Chernobyl & Challenger

Sandia National Laboratories

Similarities of Chernobyl and Challenger were noted by Bernstein and Kushment (1987) as follows:

> *Large-scale engineering systems are more than a collection of technological instruments; they are a reflection of their societies and of the management practices and bureaucratic procedures."*

Elements of symmetry they remarked upon include:

- A long-term successful program, dating back to the 1950s for Chernobyl, the 1960s for Challenger.
- Major military involvement in the design, objectives, and control of both programs.
- A transition over time from a mission-oriented effort to ordinary repetitive events.
  - NASA began to run shuttle program like routine commercial airliner.
  - Soviet management went into mass production of 1,000-MW reactors.

Chernobyl & Challenger

Sandia National Laboratories

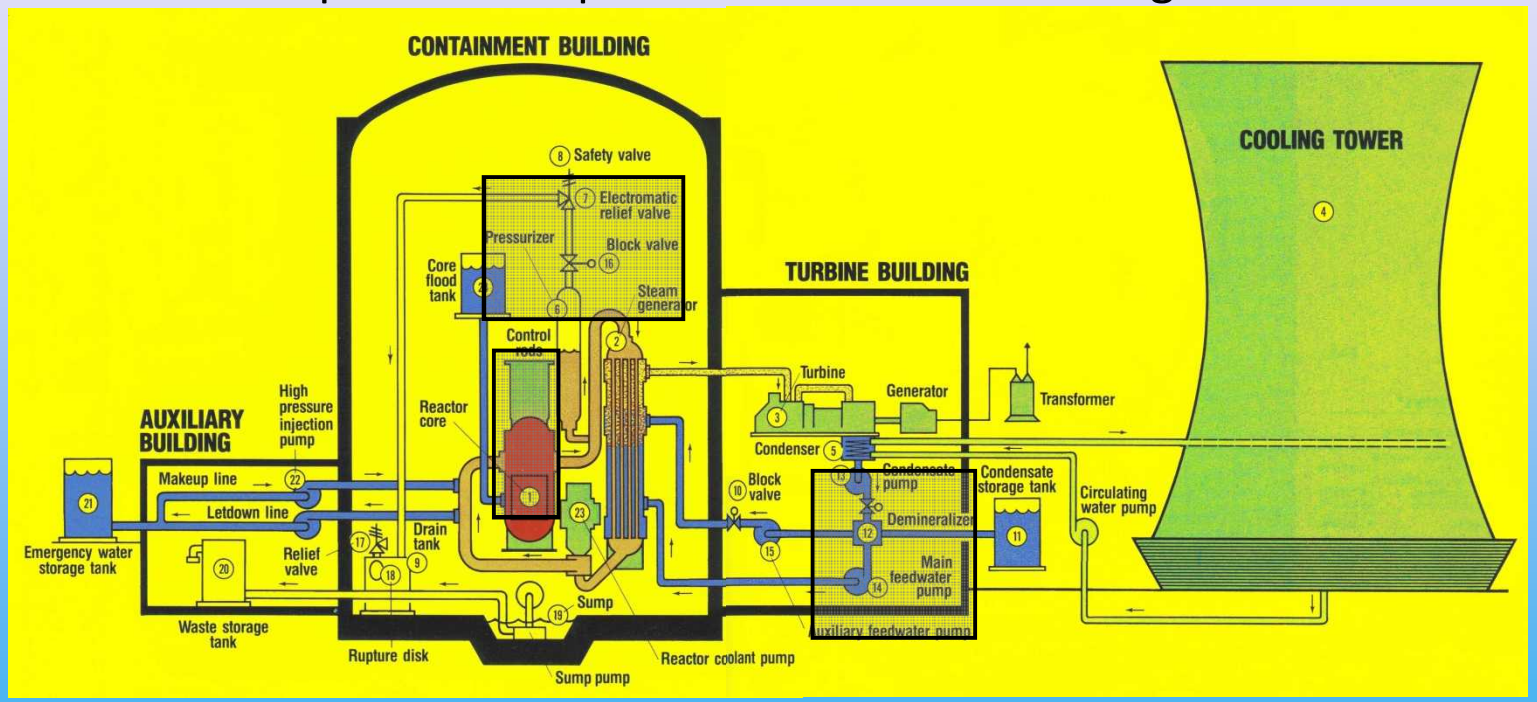
Elements of symmetry (continued):

- As technical matters became routine, Soviets politicized their program with questions of party loyalty; adherence to bureaucratic procedure appeared to take precedence over technical ability in the selection of personnel and managers.
- In NASA, the flow of information became very compartmentalized, with memos regarding key safety features such as O-rings, having limited circulation.

> *"Bureaucratic compartmentalization in an open society produced results not unlike those in the Soviet program"*

Three Mile Island

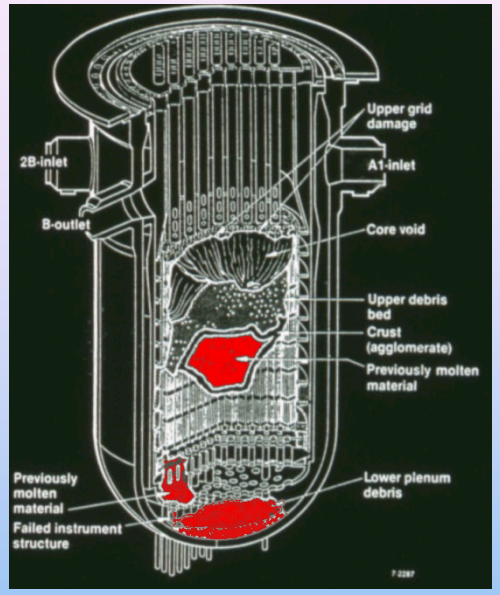
- SCENARIO
  - Nuclear Reactor – Three Mile Island Unit-2 (TMI-2)
  - Accident March 28, 1979 4:00-8:00 AM
  - Progression
    - Reactor experienced upset and shutdown as designed

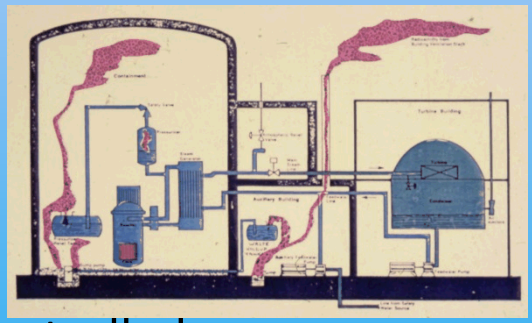


    - Relief valve stuck leading to prolonged loss of coolant water inventory

Three Mile Island

- SCENARIO
  - Nuclear Reactor – Three Mile Island Unit-2
  - Accident March 28, 1979 4:00-8:00 AM
  - Progression
    - Reactor experienced upset . . .
    - Relief valve stuck . . .
    - Lacking coolant, core fuel and cladding tubes and were damaged
    - A sizable fraction of the fuel melted – some in some flowing to the bottom of the reactor vessel.
    - Hydrogen and gaseous radioactivity (xenon and krypton) were liberated to the conltainment
      - Hydrogen exploded but did not breach containment building
      - Some radioactive noble gasses (Xe and Kr) escaped (the remainder later was vented via controlled release)





Three Mile Island

- SCENARIO
  - Nuclear Reactor – Three Mile Island Unit-2 (TMI-2)
  - Accident March 26, 1979 4:00-8:00 AM
  - Progression
  - 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 least nuclear experience 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 studies of the Three Mile Island Accident noted:
   - Organization “mindset" that a severe-damage event could not happen
   - The same mindset was, to some degree, shared by the Nuclear Regulatory Commission (NRC) also shared this mindset

Three Mile Island

- Key Decision Points
  4. Some of the unstated assumptions that contributed to the accident were as follows:
     - Compliance with Federal regulations was viewed as assuring safety
     - Procedures and training for frequent-to-rare system upsets were emphasized
     - Reporting and documenting of minor accidents, component failures, or other observed deficiencies were not systematic
     - Severe damage events, scenarios & possible defense measures were addressed only design & licensing studies
     - Safety analysis report (SAR) addressed single failures (structural, electrical. etc.) & defined “design basis accidents,” but not "beyond design basis" accidents
     - Operators had limited use of a generic control room simulator which modeled routine events but not actual or potential severe accidents
     - Training of operators and supervisors was skill-based
     - Control room instrumentation and control devices were designed for routine operation, not for coping with unusual events let alone severe accidents

COMMON ATTRIBUTES OF CATASTROPHES

#	ATTRIBUTE	Description	Bhopal	Challenger	Chernobyl	Three Mile Island
1.	Diffuse Responsibilities	Rigid communication channels Large organizational distances from decision-makers to plant	X	X	X	(X)
2.	Mindset	. . .that success is routine Neglect severe risks present	X	X	X	X
3.	Rule Compliance	Assume compliance assures safety	(X)	X	X	X
4.	Team Player Emphasis/ Agreement	Dissent on risks discouraged	X	X	X	X
5.	Experience/Lessons from Events	No process for learning from other's experiences	X	X	X	X
6.	Priority to Production/Output Goals vs Safety Improvements		X	X	X	(X)
7.	Lessons Learned Disregarded/ Narrow Experience	Neglect of precautions widely adopted elsewhere after learning from significant events	X	X	X	X
8.	Design & Operating Features/ Known Hazards	Hazards recognized as avoidable allowed to persist	X	X	X	X
9.	Emergency Procedures for Severe Accidents	Lack of plans, procedures, training or regular drills for severe events	X	X	X	X
10.	Project & Risk Management Techniques	Available methods for hazard and risk assessment not used	X	X	X	X
11.	Organization/Safety Integration	Responsibilities and authorities for recognizing and integrating safety matters undefined	X	X	X	X

e . . .

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

Key Organizational Characteristics – Reprise

Sandia National Laboratories

- Root Causes
  - View as merely “communication failures” is oversimplified
  - More aptly: Inherent“integration failures” in management structures
    - Obstacles to the integration of risk assessment with risk management decisions and their implementation
    - From physical and organizational distances between the decision makers and the best-informed technical specialists
    - From multiple industry-industry, industry-government, &/or government-government interfaces
  - Assignments
    - Overlapping jurisdictions
    - Confused changes in responsibilities for risk management decisions and remedy implementation

Key Organizational Characteristics – Reprise

Sandia National Laboratories

- Attributes ["The Table of Eleven"]
  - Readily observable
  - Observable well in advance – months to years
  - Organization may live with one or two w/o consequences
- Attribute-laden organizations
  - High likelihood of a catastrophe
  - Question
    - How soon
    - How great the damage
  - Possible history of sub-catastrophic events – Little or no implementation of "lessons learned"
  - Such catastrophes do not qualify as "accidents"
    - Not "unforeseeable and random"
    - Predisposing attributes are readily observead in advance
  - Range of serious consequences are foreseeable - Properly called **man-made catastrophes**