Safer Nuclear Energy for the Future

Lecture 2 -- Past Design Evolution

by

Dan Meneley PhD, PEng
Atomic Energy of Canada Limited (Engineer Emeritus)

Presented at the 28th International Summer College on Physics and Contemporary Needs

30th June to 12 July, 2003
Nathiagali, Pakistan

1

Before looking to the future, we need to take a quick look at the past.

This lectures outlines some of the work that has been done in the past. The systems that we have installed today did not come about by accident; they are the result of a combination of influences – some technical, some otherwise -- .

Similarly, our options for the future are constrained to some degree by the features of the present system. You could say that the installed power system has inertia.

The system that we have in the world today is the result of more than 50 years of work by tens of thousands of people. It is difficult to improve on such a huge enterprise, and building a new and innovative system takes time; usually more than one person's working lifetime.

Some Earlier Prototypes and Successes

	THERMAL											FAST
MODERATOR	GRAPHITE					WATER		HEAVY WATER				NONE
COOLANT / FUEL	Molten Salt	Na	CO_2	H_2O	He	H_2O	H_2O	H_2O	D_2O	Organic	CO_2	Na/NaK
Natural U			MAG-NOX					BLW	CANDU PHWR	OCR		
Enriched U		HALL-AM	AGR	RBMK	HTGR PBMR	PWR	BWR	SGHW	ATUCHA CVTR		KKN, EL4	
Thorium - U	MSBR				THTR	LWBR						
Plutonium-U								ATR				FBR

Every concept was developed by a brilliant and dedicated project team
Only PWR, BWR, and CANDU-PHWR have succeeded up to this date
Concepts failed for unique reasons -- political, technical, economic, safety, public acceptance, etc.
Every concept has its own special performance characteristics -- some good, some bad
Engineering designers maximized the concept's good characteristics and minimized the bad ones

2

In the early days of our industry, literally dozens of small-scale prototype plants were built and operated. Most of these have been shut down and decommissioned for various reasons.

Some concepts ran into technical difficulties at the prototype stage and were discontinued. Others failed for programmatic or political reasons.

Some, such as the MAGNOX gas-graphite system, operated for many years but could not compete with other concepts in more mature markets. The same fate was met by the HTGR concept.

At least one concept, the RBMK, reached commercial maturity only to fail catastrophically and be removed from commercial contention.

Success is defined by those concepts that have been fully developed, have been purchased on a commercial basis, and are still being built or considered for building by today's plant customers.

Three reactors make this list today – PWR, BWR, and PHWR.

Success is Not Permanent

- Three Mile Island Unit 2 (a modern US pressurized water reactor)
  - Errors committed by operators, designers, and regulators
  - Zero environmental or health effects, but large losses (>5 b$)
  - “Unjustified self-confidence” can be seen as the root cause
- Darlington station (designed, built by experienced companies)
  - Delays during construction – OH senior management and government
  - Errors in generator design – Swiss design organization
  - Error in heat transport system design - designers
- Chernobyl (USSR built several plants, and some of them operated well for years)
  - Errors were committed by government, designers, regulators, managers, operators
  - About 40 people were killed (operators, firemen, rescue workers)
  - Huge cost (>10 b$)
- Ontario Hydro Operational Breakdown
  - Errors committed by management, directors, government, unions
  - Staff reduced drastically by management, without proper care
  - Maintenance neglected, units understaffed, so 7 units were forced to shut down
  - Pickering A (and at least some Bruce A) units will be extensively refurbished and restarted

3

Mistakes are evident whenever we read about nuclear energy. Any failure becomes an important news item.

Perfection is not noticed, but is implicitly expected.

One mistake might damage your plant beyond repair and lead to irrecoverable losses.

A successful system (e.g. RBMK) can be destroyed by these mistakes.

We advance through our successes, but we learn through our mistakes.

CANDU-PHWR Plant Design Features

- **Good**
  - **Natural uranium**
  - **Good uranium usage**
  - **Fuel dispersed in cool moderator water**
  - **On-power fuelling**
  - **Good dynamic behaviour in transients**
  - **Automated plant operation**
  - **In accidents, fuel is always below melting temperature**
- **Not so Good**
  - **Heavy water is expensive**
  - **Tritium must be controlled**
  - **Complicated piping**
  - **Two coolant systems**
  - **Positive coolant void reactivity**
  - **Pressure boundary opened daily for fuelling**

4

Good

Natural U Cheap fuel can be replaced without large penalty

Good uranium utilization – economic factor

On-power fuelling leads to low in-core defective fuel load

Dynamic behaviour – long neutron lifetime, small negative power coefficient

Automated plant operation reduces operator's workload – more reliable

Low post-accident fuel temperature retains fission products

Not so good

Expensive heavy water is both bad and good – careful attention to leakage

Tritium production is much higher – but this results in good air control in containment

Complicated piping – but mostly small-diameter

Two coolant systems (HTS and moderator) leads to complex water management

Positive coolant void reactivity – power rises after pipe break and SDS must act to reduce power. Leads to great care in reactor shutdown system design.

Frequent opening of HTS increases LOCA probability – but system is automated and controlled

PWR Plant Design Features

- **Good**
  - **Simple fuelling**
  - **High fuel burnup**
  - **Simple primary heat transport system**
  - **Small number of water systems**
  - **Large in-service reactor population**
- **Not So Good**
  - **Fuel is expensive**
  - **Large excess reactivity**
  - **Big pressure vessel**
  - **Big power coefficient**
  - **Fast operator action needed on shutdown**
  - **Short neutron lifetime**
  - **Fuel melting in accidents**

5

Good

Annual fuelling during shutdown – but leads to large operational reactivity control need

High fuel burnup helps economics

Very little external piping reduces chances of pipe breaks

Few water systems – operational simplicity

Large experience base due to large number of plants operating in world

Not so good

Expensive fuel increases operating cost and leads to design with allowance for more in-core defective fuel

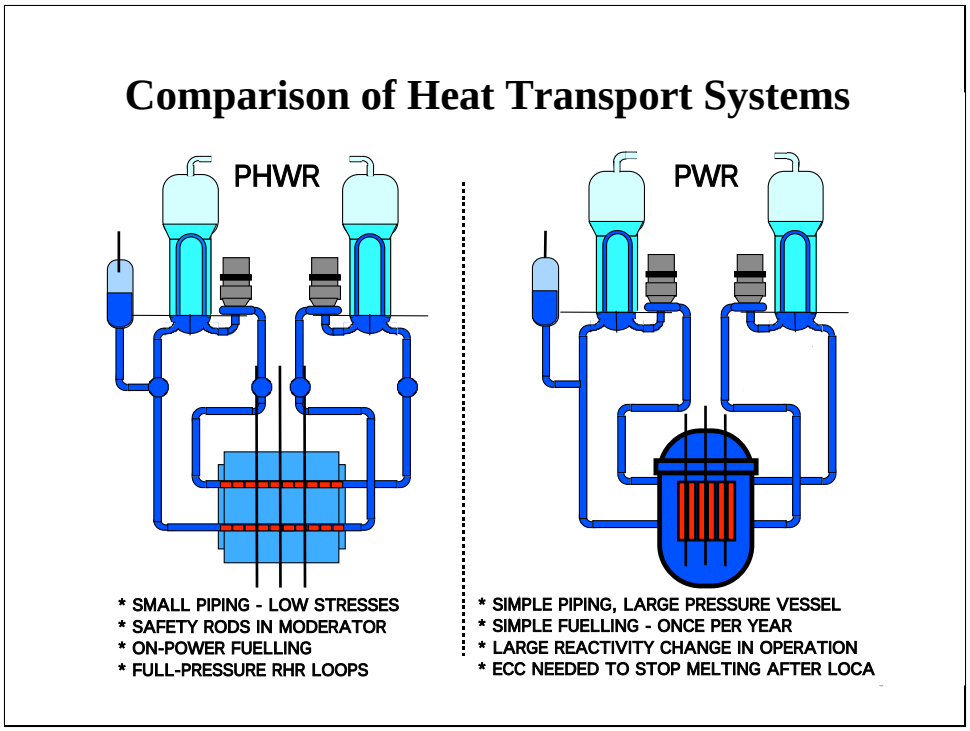
Large pressure vessel must not be allowed to break

Large negative power coefficient is good for controlling positive reactivity transient – but bad when initial transient leads to rapid fuel cooling

Operators must carry out several operations quickly during shutdown, in order to reach controlled hot shutdown state

Short neutron lifetime demands rapid action in any transient near fuel damage threshold

LOCA accident can result in fuel melting soon after accident – fission product release



This figure does not show the several hundred feeder pipes present in the case of the PHWR – added complexity.

The general conclusion is that when any reactor concept is chosen the designer must accept the whole package of good and bad features that exist for that concept, and then must design to minimize the bad features of the design.

In some concepts it is easier to find a safe, reliable, and economic design

Present Status of Nuclear Supply Energy Systems

- Fission supplies a few percent of total world energy demand
- Number of plants operating is growing, but very slowly
- Public acceptance is marginally positive
- Capital cost, waste management, and weapons proliferation appear to be the main concerns
- Safety is a dominant concern mainly for owners and investors
- Using known fuel reserves, today's electrical power output could be sustained for 50-100 years

7

With about 500 plants operating, the contribution of nuclear energy to the total world energy demand amounts to only a few percent.

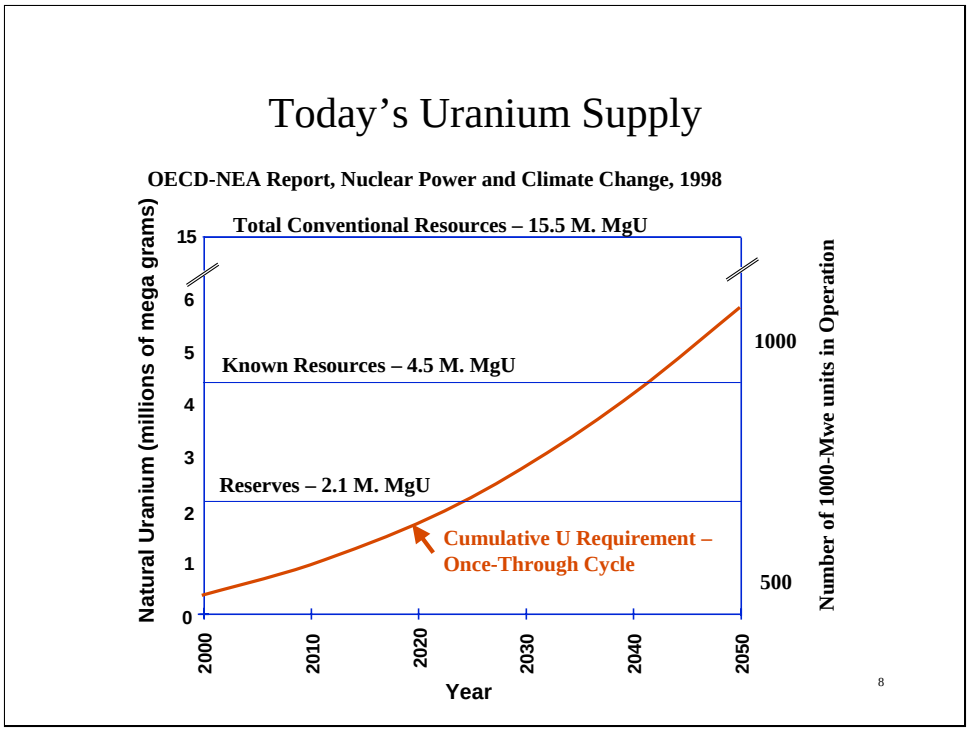
For the past few years, new-plant installation rate has been slow, due mostly to economic and public acceptance factors. Fossil fuel supply shortages are changing that situation.

Very large capacity additions may be necessary over the next decades. Designers must prepare to overcome some very serious constraints such as siting and long-term fuel supply.

Regulatory agencies are concerned mainly about the potential for weapons proliferation.

Owners are concerned over safety due to financial risks during operation.

Designs must be changed within the next few years due to fuel supply limitations.



This is a simple demonstration of fact that we probably have less than a century to improve the nuclear fuel cycle. Thorium might help.

The situation with oil and gas is much more critical today.

There seems to be plenty of coal, but it creates plenty of problems, too.

Uranium Fuel Supply in the Future

- Known, but low-concentration deposits occur in phosphate ores and in seawater.
- These deposits could be utilized if about ten times more energy could be gained from each gram of uranium extracted, according to Japanese studies. (At least fifty times more potential energy is available than we now produce from each gram.)
- The concentration of uranium in seawater probably is in equilibrium with the sea bottom rock, so that uranium extracted would be replaced through leaching.
- Conclusion: Seawater contains an effectively infinite amount of uranium, if we can learn to recycle our fuel and to take more energy from it.

9

Fuel energy utilization must be increased to the 25% to 50% range. This will require a very different mix of plants than exists today.

Breeder reactors and/or accelerator breeding may be the answer in the long term.

Nuclear Plants Represent New Technology

- In recent years, several authors have begun to look carefully at failure characteristics during the introduction of new technologies of various kinds
- Looking at earlier examples of introduction of such technologies, can we see similarities in accident statistics?
- Are there common characteristics of these technologies that can be used to better understand and predict the behaviour of our plants?
- Are there some measurable parameters that can be used to judge our own safety performance?

10

My own first exposure to this field was in the early 1980's during unrelated collaborative work with Dr. Karl Ott.

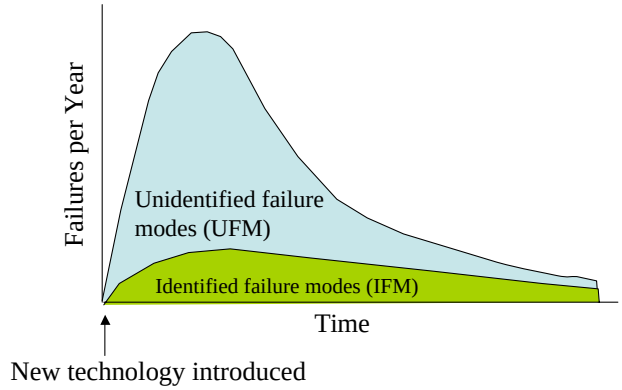
Valeri Legasov presented an introductory paper at the IAEA review meeting for the Chernobyl-4 accident, in Vienna. Legasov wondered whether or not the Soviet Union was capable of managing large and complex technologies.

Most recently, the loss of the space shuttle has raised similar questions

The next few slides outline the findings from these investigations.

Typical Failure Trend for a New Technology

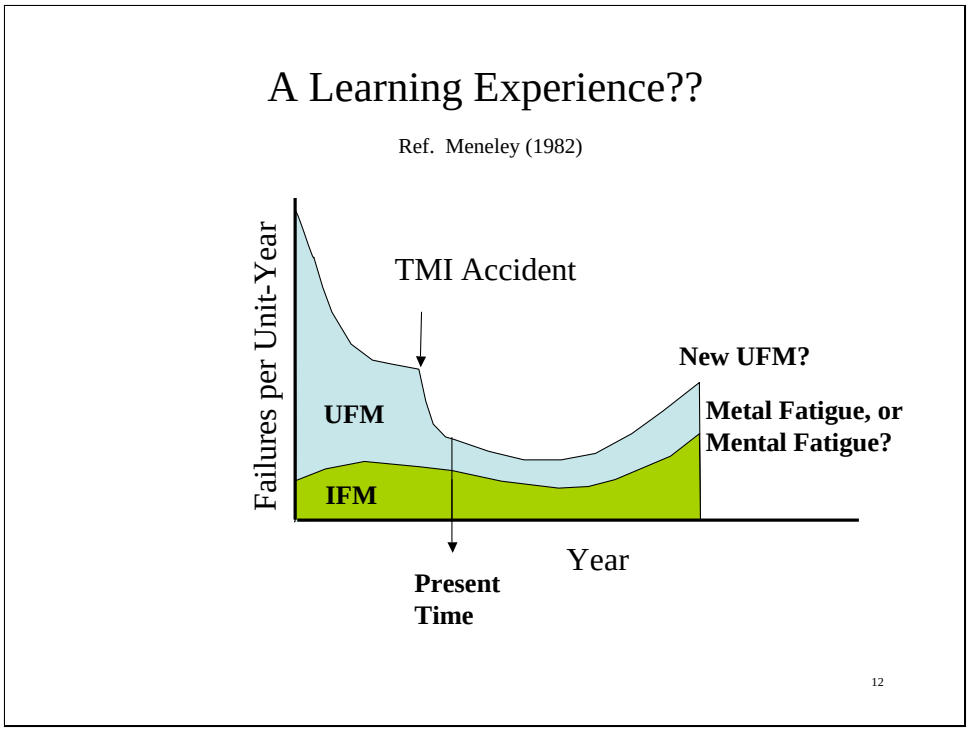
Ref. K.O. Ott and J.F. Marchaterre (1981)



11

Typically, the total failures per year initially increases as the number of in-service units increases. People begin to recognize the failure modes, so the number of UFM then starts to decrease. The number of IFM first increases, then decreases as engineering design modifies the overall system to reduce its failure probability.

For a mature technology, the remaining UFM produce rare “surprise accidents”, and lack f attention, poor maintenance, etc. result in some IFM’s being repeated.



The original of this figure was drawn shortly after the Three Mile Island nuclear accident. That event led to intense reviews of LWR technology and operating practices, and revealed a number of previously unrecognized failure modes.

TMI was a great learning experience – mostly because it happened to someone else's plant, and was not a large cost to CANDU owners.

Many design changes were introduced in the PWR – in principle, some of these changes could introduce new failure modes.

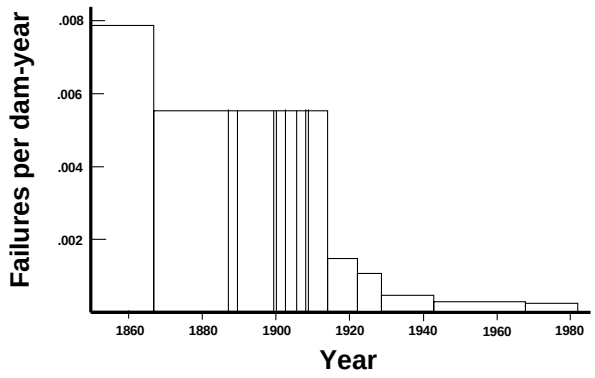
The most likely future pattern would be a period of excellent attention to detail followed by a relaxation and a repeat of earlier IFM accidents.

The world's nuclear industry has (so far) avoided the relaxation – organizations such as INPO, WANO and IAEA recently have paid much attention to operational safety.

There has been less obsession with "hypothetical" rare events, and more appropriate attention to the real world of operations, on the part of regulatory agencies

Earth Dam Failure Rate -- USA

Ott, Hoffman, Oedekoven (1984)



13

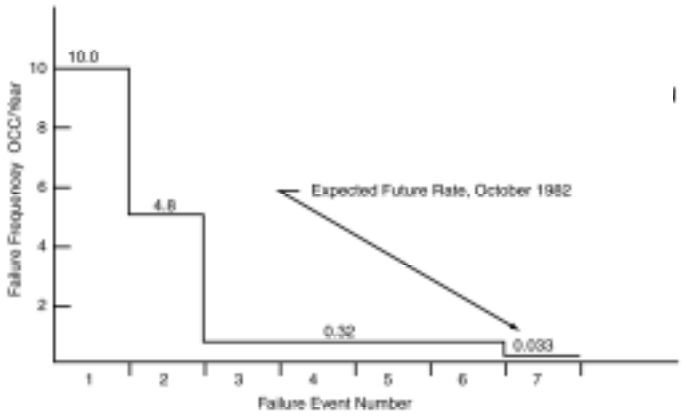
This analysis used isotonic regression to examine the historical failure rates of earth dams in the US.

Following World War I, the failure rate dropped dramatically for two known reasons – (a) earlier failures had generated strong public reaction, and (b) European immigrant engineers brought improved dam technology to the US after that war.

Low failure rates were maintained for many years, until some evidence of forgetting showed up in the failure of the Snake River dam in Idaho in the 1960's. Poor attention to embankment design led to gross failure during the first filling of the dam.

Isotonic Regression Trend Analysis

Pickering A reactor regulating system,
Ref. Sharma (1984)



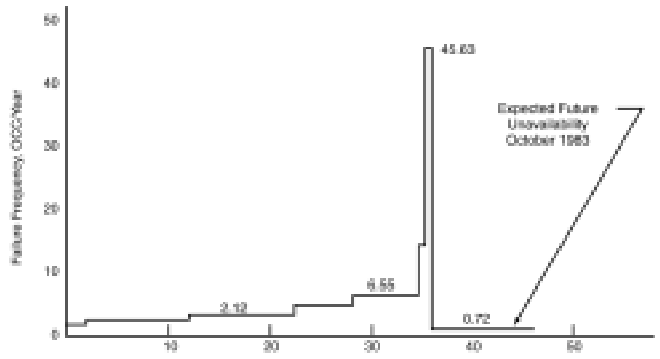
The Pickering A reactor regulating system was analyzed by Aditya Sharma in 1984. The trend shows a rapid drop in failure rate following a review and redesign during the 1970's. The target frequency of .01 failures per year was reached some years later as a result of careful operation and testing.

One failure mode that resulted in a loss of regulation in the early 1980's had been recognized in the earlier design review, but the necessary system modification had not been implemented. That change, when completed, led to targets usually being met after that time.

Later on, installation of a modern RRS system resulted in design targets being met in most reporting intervals.

Isotonic Regression Trend Analysis

Pickering A Emergency Coolant Injection
Ref. Sharma (1984)



15

This graph illustrates the appearance of an unidentified failure mode that had been hidden in the Pickering A ECI system since its installation.

That failure mode (heat exchanger overstress) was found and corrected. The system appeared to operate satisfactorily after that time.

However, tests during re-commissioning of this system following reactor retubing in the 1980's revealed other UFM events, and these also were corrected at that time.

This experience shows that this sort of trend analysis is a useful tool for management to identify trends. Much more detailed investigation might be necessary to find root causes and to correct the problem.

Many different methods might be appropriate in a particular message. But the general lesson is crystal clear: TO ASSURE CONTINUING RELIABLE AND SAFE OPERATION, MANAGEMENT MUST UNDERSTAND PAST FAILURES, AND THEN MUST ACT TO PREVENT THEIR RECURRENCE.

Learning - and Forgetting - Curves

Ref. Duffey & Saull (2003)

- The type of learning curve postulated in Slides 11 - 15 herein has been found to exist in a wide variety of high-technology industries.
- Using the appropriate measure of operating experience, all of these cases follow a similar learning curve as the industry matures; in addition there is a pattern of forgetting of the lessons learned.
- This type of analysis could be used by plant management as an indicator of the ongoing safety performance their organization

16

John Saull is an aircraft safety expert, and Romney Duffey is Chief Scientist at AECL. Their collaboration has produced an interesting book in which operating experience, learning trends, and forgetting trends were examined in a number of different situations in various industries.

Duffey and Saull found a “Universal Learning Curve” can be applied to all of these experience data.

They also found that a residual accident rate exists, below which one can expect a more or less constant accident rate to continue indefinitely.

This residual rate can be related to the “Normal Accidents” idea developed much earlier by Charles Perrow. Perrow examined several different industries – and concluded that nuclear energy enterprise should be abandoned because of its potential for very high accident consequence at the unavoidable minimum accident rate.

Human Factors Program Elements at NASA

- Collect and analyze data on “close call” incidents
- Develop corrective actions against identified root causes by applying human factors engineering
- Implement a system to provide human performance audits of critical processes -- process FMEA
- Organizational surveys for operator feedback
- Stress designs that limit system complexity and coupling

(Dr. Michael A. Greenfield, NASA, November 17, 1998)

17

This slide is taken from a presentation by Michael Greenfield, Deputy Associate Administrator for Safety and Mission Assurance of the US space agency NASA. He recommended that NASA should undertake very much the same sort of approach to examining operating experience that has been used in the nuclear industry for decades.

A new recommendation presented in Greenfield’s talk was identification of the need to reduce system complexity and coupling in large-scale technological systems, as recommended by Perrow some years earlier.

Power reactors are tightly coupled, complex systems. Simplification and decoupling are recommended design objectives for future plants.

NASA Summary -- November 17, 1998

- NASA nominally works with the theory tat accidents can be prevented through good organizational design and management
- Normal accident theory suggests that in complex, tightly coupled systems, accidents are inevitable
- There are many activities underway to strengthen our safety posture
- NASA's new thrust in the analysis of close-calls provides insight into the unplanned and the unimaginable

To defend against normal accidents, we must understand the complex interactions of our programs, analyze close-calls and mishaps to determine root causes, and USE this knowledge to improve programs and operations.

Institutional Failure?

18

In the light of the recent shuttle failure, this summary seems a little bit sad.

The independent review panel investigating the Columbia disaster has issued its outline report on that accident (NY Times, June 7, 2003). The panel identifies the shuttle failure as only a surface problem; one that is underlain by communications breakdowns, increasing complacency, failure to heed warning signs, budget pressures, administration changes. A familiar story.

The report points to "High-reliability industries such as nuclear power as one place in which NASA might look for solutions to their problems.

A similar set of conclusions can be found in the reports on the earlier shuttle failure some years ago.

Overall, these reports suggest a category that has been identified as "Institutional Failure" by several earlier writings.

Institutional Failure

Ref. Mosey (1983)

- Dominating production imperative
- Failure to allocate adequate or appropriate resources
- Failure to acknowledge or recognize an unsatisfactory or deteriorating safety situation
- Lack of appreciation of the technical safety envelope
- Failure to define and/or assign safety responsibility clearly
- Something more than safety culture
  - Responsibility of senior management **cannot** be delegated
  - Authority to act can be delegated along with commensurate responsibility, but original responsibility of senior management remains **in full force**.

19

David Mosey wrote about Institutional Failure, in 1983. The list above notes the most frequent underlying causes of failures.

It is clear that these failures are typical human failures.

Management, because it (by definition) holds a great deal of authority over system operations, also must accept responsibility for many of the failures in the system. Front-line workers are no less fallible, but the consequences of their poor performance usually is less damaging.

An interesting book by Weick and Sutcliffe of the University of Michigan business school takes up the theme and applies it to a wide analysis of failures in business. That book broadens our understanding of both the effects of the high-reliability approach and the reality of Normal Accidents.