Safer Nuclear Energy for the Future

Lecture 1 -- Safety Perspectives

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

This series of four lectures investigates the theme of safety – how the world might gain the benefits of nuclear energy with even less risk than exists in the plants operating today.

Given the title of this session, one might expect a prior assumption that today's nuclear plants around the world are **NOT** safe enough. On the contrary, I consider that these plants **are very, very, safe** and are being operated with exceptional care and attention.

So why do future plants need to be safer? I can see two reasons:

1. Many people remain uneasy about the safety of these plants largely because of a very successful world-wide campaign waged against their continued operation, over the past 40 years. A renewed nuclear program must recognize this unease.
2. We expect that a very large number of plants of output typical of today's largest will be needed to satisfy the world's needs for energy, as the price and availability of fossil fuel worsens in the future. People living in a world with thousands of operating nuclear plants will require that the frequency of a major accident at any one of these plants still remains very low. The arithmetic is simple.

Safety perspectives (1)

- These lectures offer the perspective of an engineer retired after more than 40 years in the nuclear industry - in research, design, licensing, education, and management
- Objective -- Study of possible future nuclear plant safety regime
  - Human and technical aspects of safety
  - What can be done within practical constraints?
- Four presentations - this one plus:
  - Future development based on past achievement
  - Today's development directions
  - Some future possibilities for safe design
- Possibilities and limitations of safety improvement
  - Social as well as technological
  - The cheapest design often is not the safest design
  - How safe can it be?

2

The content of these four lectures reflects my own opinions, and in no way represents nor reflects the policies of Atomic Energy of Canada Limited.

It is common to assume that what we need to satisfy the people is a set of safer "technical fixes" that (we assume) will solve the problems of nuclear energy. A slightly different perspective is presented in these lectures.

The topic of safety is very broad. I will present only a few poor images and words as an attempt to convey my own opinion of the important aspects of safety improvement. I will appreciate any comments, questions, and corrections that you wish to present.

The technical examples that I give will relate mstly to the CANDU-PHWR system, simply because it is the system with which I am most familiar. Most of the lessons can be applied, however, to any nuclear plant concept.

Safety Perspectives (2)

- Safety is a state of mind --> do you feel safe, or not?
  - A system that kills rarely, but which still may kill, is not trusted
  - Trust comes from long experience of no harm having been done
  - People will overlook some large risks if benefits are perceived
  - People will accept larger risks if they are in control of those risks
  - Institutions often are mistrusted for reasons unrelated to plant safety
- The task of the safety engineer is to give most people a well-justified, safe feeling about the nuclear energy supply system
  - Reliability, performance, consistency
  - Responsibility, honesty. self-esteem

3

An individual either feels safe or does not feel safe. Hardly an objective concept. However, engineers work in the real world, and this world is governed by people who are governed mostly by this innate feelings, and not by the commonly-used term "cold, hard, facts."

When I tell newly-met acquaintances that I have spent my career working on nuclear power development, the most common first reply is "This is scary, isn't it?" After the next half hour of explanation that it really is not scary, most people are reassured – but not comforted. Most are still scared.

In my own opinion, safety cannot be properly addressed only in rational terms like reliability, defence in depth, and so on. To be successful, proponents must address the underlying fear of nuclear energy, as well.

Safety Perspectives - (3)

- Protection of the plant is clearly in the interest of the owner. The owner's desire for investment protection lines up very well with the regulator's interest as well as the public interest
- Protection of the operating staff aligns very well with the need to control all releases of radioactive material
- Plant economic assessments should account for lifetime outage costs as well as for apportioned accident risk. (Lowest capital cost is NOT the correct bid evaluation measure.)

4

To cover the objective parts first, the plant owner (that mythical hard-headed, objective person) must recognize that the plant he owns is "fragile"* and can suffer severe and expensive damage. This is a fact, but not a fact that features in many sales brochures published by nuclear plant vendors.

The regulator (that mythical clear-headed, all-seeing person) is in a position where he/she is charged as the auditor of the owner's performance on behalf of the people – the regulator obviously has a central interest in safety.

These two mythological creatures have, in this case, identical interests. They must be reminded of this fact, occasionally.

The people who own and operate the plant clearly have an interest in its safe operation. If the plant is damaged the first consequence falls on their staff and their financial investment.

Economic assessments (usually discussed before the purchase of a plant) should, but often do not, include the actuarial risk of losses (both production and materiel losses) during plant operation.

•G. Vendryes, Electricite de France

The Human Side of Safety

- A well-designed plant can be operated poorly and as a result might produce a major accident
- A poorly-designed plant can be operated with great care by competent operating staff, and as a result might be safe
- Lapses in care, knowledge, or attention are a consistent pattern in most major accidents
- The real standards of operational safety are determined largely by the philosophy of senior management

5

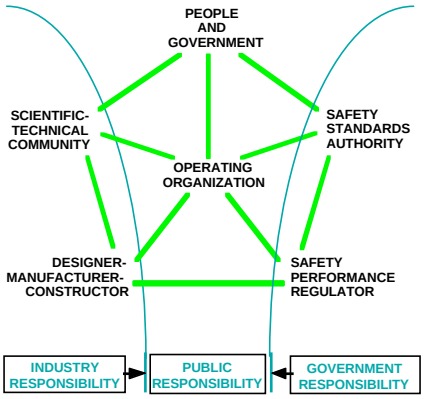
Close ties exist between the specific people running the plant and its achieved safe record of operation. These people are in the front line of safety. (Plants all have excellent radiation safety records until they begin to operate.).

In all industries, post-facto review of accidents always reveals lapses by some humans – politicians, managers, designers, operating personnel, regulators, etc. (After all, machines are too stupid to make mistakes.)

It appears that a distinction can be made between safe and unsafe facilities by examining the attitudes of senior management. These attitudes are infused throughout the organization and eventually cause failures. Poor management is the real root cause of most accidents.

Regulatory oversight at the management level may be the most effective strategy to sustain safe operation.

Idealized Safety Management System



1. Operating organization is at the centre of the action
   --- plants are very safe until they start operating ---
2. Designer must deliver a plant that can be operated safely
3. Regulator must audit the operator to assure public safety
4. Other operator responsibilities:
   ---- protect the workers ----
   ---- protect the plant ----

6

- The diagram is intended only to represent primary working relationships and responsibilities. It is not an organization chart.
- The base triangle shows the designer/builder at one apex and the regulatory staff at the other apex – and both supporting the operating organization that carries the primary responsibility for public safety.
- The authority for action by regulatory staff flows from the government-appointed Safety Standards Authority. Safety Standards are established by the government on behalf of the people. (International standards have no force within a country – but may be adopted by the government in some cases.
- Scientific and technical authority for safety provisions is provided by the scientific community. Members of this community are certified by the government under various education statutes that sometimes include the establishment of self-regulating engineering associations. Together, these two organizations carry technical responsibility for safe plant designs.
- Finally, the operating organization is supported and is delegated the authority to operate the plant within the bounds defined by technical and regulatory requirements.
- Engineering support for operations continues through the whole life of the plant.

Common Failures in Safety Management

- Responsibility is delegated but authority is retained
- "Management Knows Best, and Employees Must Listen"
- Reluctance to respond, especially in case of bad news
- Tendency to find fault - and to punish staff for normal errors
- Lack of knowledge of actual conditions in the plant
- Imposition of an overriding production imperative

7

Management also is made up of human individuals, who are susceptible to failure. Production pressures compete (apparently) with safety goals.

Human nature has a tendency to retain authority and delegate responsibility. This must be recognized by senior managers and must be discouraged.

Looking at many failures in several different industries, experts find very similar root causes of management failures in all of them. This may suggest some means for reducing the chance of error in similar complex organizations.

We will return to this subject in Lecture 2.

A Mixed Public Response to Coal vs Nuclear

- Some operating organizations operate both fossil-fuelled and uranium-fuelled power plants. Reactions of the public vary widely.
- For example, coal plants are grudgingly accepted as necessary, but nuclear plants are subject of endless debate -- even though coal plants cause far more damage to health, day by day.
- Anti-nuclear groups exacerbate existing fears in the people -- but the fears are fundamental

8

In the area of public response to non-nuclear power plants, many people react positively because of their trust in the operating organization. Others react with fear at various levels. Fear is associated with lack of trust.

Reaction of most people is quite different in the case of a nuclear plant. In that case basic fears are much more common – probably because of association with nuclear bombs, cancer-causing radiation, and genetic damage.

Of course, groups whose purpose is to stop the technology play on these fears and use them to influence the society in general. But the fears are fundamental, and must be dealt with.

The essential requirement for the operating organization is to establish and maintain the public trust. Trust must be earned and deserved.

Why is Nuclear Safety So Important?

- The next few slides compare safety situation in coal plant with that in a nuclear plant.
- It will be seen that safety requirements for a nuclear plant are qualitatively different than those of a fossil-fired plant.

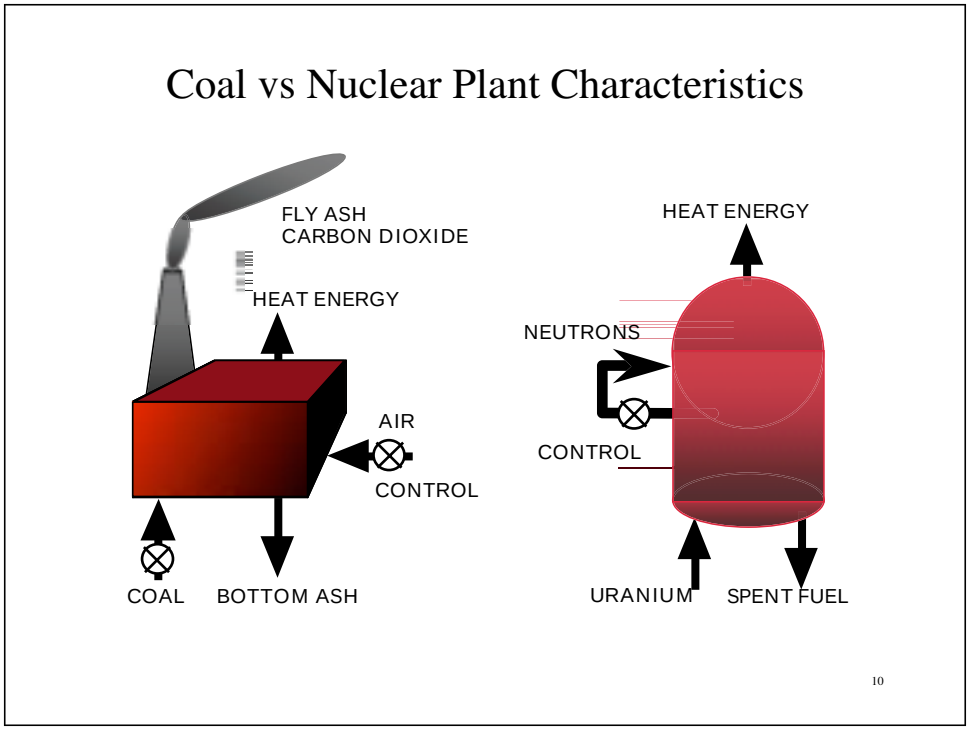
9

Here we look at the difference between a coal-fuelled plant and a uranium-fuelled plant – to illustrate the reason for additional care in the case of nuclear plants.

This is not a condemnation of nuclear power, but an illustration of the importance of understanding the technology that we are using.

Fossil plants and hydraulic plants have different characteristics, some of them good and some detrimental to public safety.

Engineers must be fully aware of the qualitative and quantitative behaviour of the plant for which they are responsible.

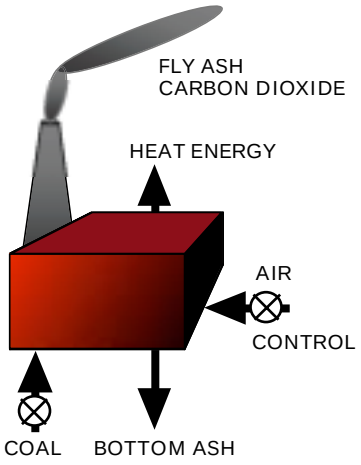


This sketch illustrates the basic inputs and outputs of these plants. Details such as exhaust scrubbers and safety shutdown systems are not shown, for simplicity.

Coal plants are cheap to build but generally more expensive to operate. They produce large quantities of greenhouse gas, miscellaneous toxic materials in airborne form, and huge quantities of solid waste products.

Nuclear plants are relatively expensive to build (mostly because of materials, close tolerances, and demanding safety requirements) and cheaper to operate. They have essentially zero emissions in normal operation. Waste quantities are very small relative to coal-fired plants.

Processes of a Coal-Fuelled Plant



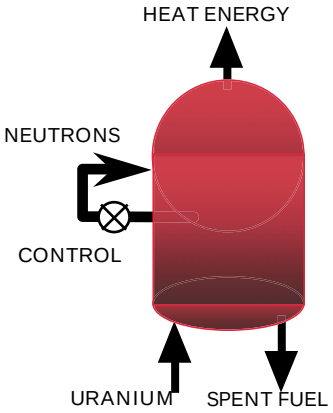
- Process inputs are fuel and air; the flows are controlled to match demand for the primary output, which is heat to boil water. A relatively small amount of heat is needed to raise the fuel-air mixture up to the furnace temperature.
- Fuel flows into the furnace and is burned in a few seconds to produce the secondary outputs - combustion gases and ash. Combustion gases transfer heat to water and steam is produced. Only a small amount of fuel is in the furnace at any time.
- Highest possible temperature is equal to the flame temperature of the fuel. This temperature is below the furnace melting temperature. Combustion gases have a very large volume that makes purification expensive, though still possible. Waste product is carbon dioxide. Tertiary output (bottom ash) has a very large volume and contains toxic materials.

11

Accident risk in this type of plant might come from failure of pressure-retaining components. Such an explosion can destroy the plant and injure the staff, but is unlikely to result in a public-health disaster.

During normal operation this type of plant emits many toxic compounds – it most likely will lead to premature death of many individuals, unless these are removed from exhaust gases.

Nuclear Plant Processes



- A flow diagram is shown in the right-hand side of the Figure. The process uses no air -- no secondary waste output. Fuel is added in batches, daily or yearly. Mass of fuel used is very small compared with the mass needed for a coal plant.
- Tertiary output (fission product material) is sealed inside used fuel bundles.
- Possible to design plant for zero waste output during normal operation. Fuel must be carefully protected from overheating during operation, to ensure that no radioactive materials are released accidentally.
- In most designs the primary output, heat, is carried away from the reactor by water coolant under pressure. This coolant then is used to produce steam.
- An intermediate product (neutrons) is essential to keep the fission process going. The neutrons "flow" through the reactor, slow down, and are absorbed. Control materials are moved into, or out of, the neutron flow as required to regulate the number of neutrons.
- If control is lost it is possible for the neutron flow to increase very quickly and to release large amounts of heat from the fuel. This is possible because a large amount of fuel (in terms of potential energy) is located inside the reactor.

12

Secondary control (neutrons) instead of primary control (air, fuel) coupled with unlimited temperature rise makes a nuclear chain-reacting system qualitatively different than a fossil fire.

Post-shutdown decay heat from fission products is large relative to stored heat content of fossil systems

The first principle of nuclear plant safety is to control the rate of fission at all times, so that input energy and output energy are always in balance..

Nuclear Plant Processes - Continued

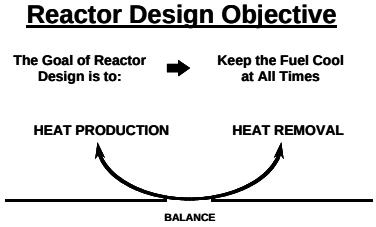
- The fission rate has no intrinsic upper limit. As a result there is no effective limit to fuel temperature. Temperature can rise far above the melting temperature of reactor materials. Coolant that normally contacts the fuel sheath can itself be vaporized at high temperature. Volume increases on vaporization and can lead to overpressure of containment barriers. Continued cooling is required so that fuel temperatures remain low. Control and safety systems are required to prevent the fission rate from exceeding safe limits.
- Reviewing this scenario, structural materials and coolant will degrade at very high temperatures. The radioactive fission products are located inside the fuel, in exactly the same place where most of the fission heat is released. If the fuel is not cooled these radioactive materials eventually will be released.
- So -- KEEP THE FUEL COOL!*

* IAEA Safety Guide NS-R-1 "Design of the Reactor Core for Nuclear Power Plants"

13

A second qualitative difference between fossil-fuelled plants and nuclear plants is that the latter retain almost all of their waste products (fission fragments) inside the fuel. If the fuel s melted these wastes are released – they are the main hazard against which preventive safety action must be taken.

Design Objective for Solid-Fuel Nuclear Plants



- In steady-state operation, heat production is exactly equal to heat removal
- After an accident event, inherent or engineered safety systems must act to restore the balance:
  - Reduce power, or
  - Increase heat removal
- Also, as a precaution:
  - Close containment openings
- Monitor plant status at all times

14

In principle, nuclear plant safety actions are simple.

If an accident event is sudden and significant, automatic systems are designed to reduce power, sustain fuel cooling, and close the containment (if necessary.)

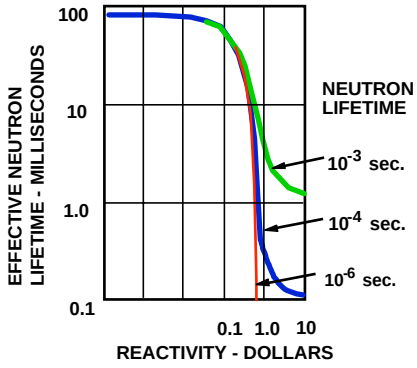
If degradation is slow and unobtrusive, system health monitoring detectors and human operators are relied upon to detect and correct the malfunction.

Special care must be taken during operational shutdown periods, in order to assure protection against inadvertent criticality and sustained fuel cooling.

Following a major accident, the most difficult action is the maintenance of cool fuel in the long term – this requires motive power, cooling, and control as well as an intact cooling circuit. Some reliance is placed on long-term human intervention via designed accident management capability.

Cooling must be maintained for weeks or months.

The Cliff-Edge of Prompt Criticality



- All reactor types respond in a similar way when positive reactivity is small
- Effective neutron lifetime (~cycle time) decreases near prompt critical threshold
- Effective control action is possible only if neutron lifetime is long, for major RIA events
- Inherent negative reactivity feedback is essential if neutron lifetime is long

15

If the reactor contains enough fissile material and a geometry such as to sustain a chain reaction at some reactivity larger than the delayed neutron fraction, there is some possibility of reaching a prompt critical state during or after a major accident.

When the neutron lifetime is short, fission proceeds at a very high rate and control systems are severely challenged. Some sort of inherent shutdown mechanism is required to limit the energy yield.

Long neutron lifetime has a positive influence on protection against consequences of reactivity-initiated-accidents or re-criticality events, in allowing more time for shutdown action before the fuel damage threshold is reached.

Either inherent characteristics of the reactor or engineered safety devices must be available to achieve rapid shutdown of the chain reaction in all cases.

Freeman Dyson -- The Little Red Schoolhouse*

- At the beginning of the commercial development of this industry, it was thought that civilian nuclear plants should be inherently safe -- power increase should lead to reactivity decrease.
- General Atomics developed the TRIGA reactor - in 1958, a technician stood on top of a TRIGA that was shut down in the middle of a crowded exhibition in Geneva. He pulled out the single control rod as fast as he could. The reactor started up very quickly, without any damage and ran at steady state power. The design is inherently safe
- However, a commercial power reactor must be cheap as well as safe.

* In "Disturbing the Universe", HarperCollins Canada, (1981) ISBN 0-465-016-774

16

The chapter of Freeman Dyson's book with this title describes the activities of a small group of scientists who attempted to define an inherently safe reactor design for civilian application. They succeeded, for a very small reactor size.

Inherent safety was demonstrated by various reactivity-initiated transients involving sudden withdrawal of the control rod from a subcritical TRIGA reactor.

Unfortunately, the cost of electricity production of small reactors is high. It is very much more difficult to design a nuclear plant that is both safe and economical.

"An engineer is a person who can do for one dollar what any fool can do for two dollars."

"Engineered" Safety

- Nuclear power has been a closely regulated industry, from its beginning
- Safety design concepts were developed over many years and in several countries, with the objective of protecting the public
- Ideas of redundancy, diversity, defence in depth, etc.* were developed in great detail and applied to commercial designs
- Enormous sums of money were spent to achieve assure safety – the result was never perfect – and the strain between performance goals and safety goals continued.

The ideal of an "inherently safe" nuclear plant never died.

* e.g. IAEA Safety Series, and various national standards

17

Performance goals were dominant in the beginning, as the industry took its first steps. "Safe Enough" was the predominant philosophy.

A great deal was accomplished – plants became very safe.

Exceptions (accidents) occurred rarely, but often enough to generate public concern.

Opposition groups grew in many countries.

Regulators tried to "fix" the problem with ever-increasing stringency in regulations.

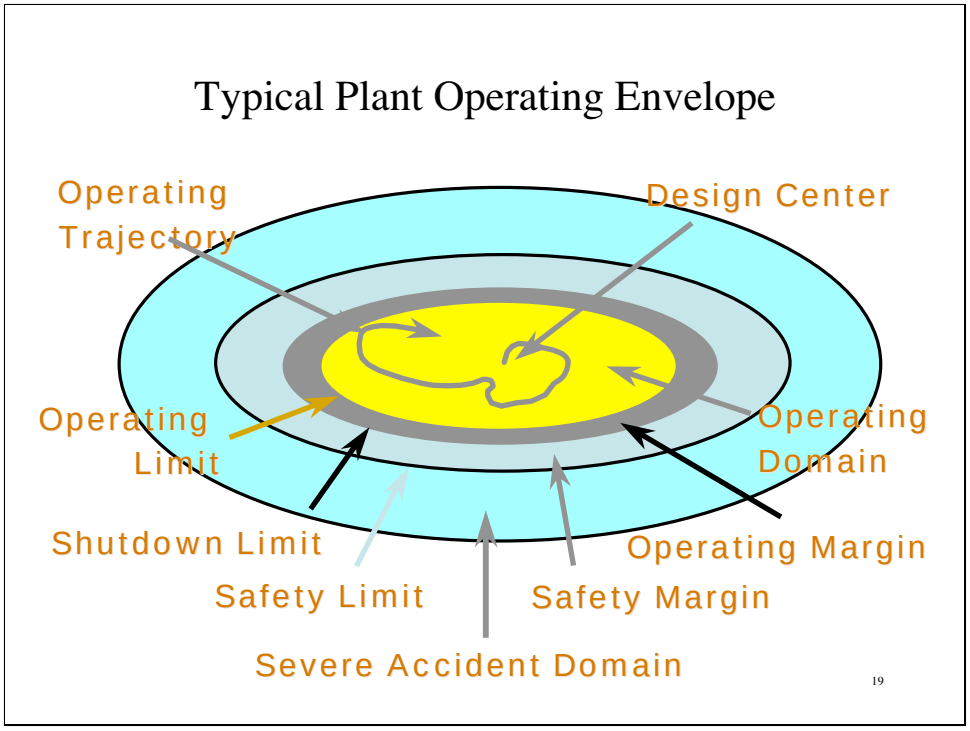
Plant owners resisted regulatory control – claimed that regulators did not foster real safety.

Public Protection is Simple

- Operate plant within its safe operating envelope
  - Operators must fully appreciate the bounds of this envelope
- When the boundary of the safe operating envelope is approached,
  - **Shut down the chain reaction**
  - **Close the containment boundary**
  - **Cool the fuel**
- The third part is more difficult than the first two
  - It is a continuing requirement in time
  - It normally requires support services – power, water, etc.

18

Modern safety design concepts are moving toward greater emphasis on these simple ideas. See IAEA NS-R-1.



This envelope actually exists in a multi-dimensional state space.

The plant normally operates in the yellow domain. The state vector is represented by the "wandering arrow" within this domain.

Regulating systems ensure that the state vector des not go outside the operating limit.

Safety systems act if the vector crosses the shutdown limit boundary.

Plant damage might occur if the vector passes the safety limit boundary.

Safety design concentrates on ensuring the capability of engineered safety systems to respond, and the completeness of the known envelope boundaries.

By far the greatest unknown is the completeness issue. Some say, under the heading of 'Normal Accidents' that unexpected breaches of protection are inevitable. In a broad analysis of various complex, tightly coupled systems including airlines and nuclear plant, Duffey and Saull reach roughly the same conclusion.

Limits of Safety

- Learning reduces the accident rates as a technology matures (Duffey & Saull)
- Unexpected events occur at an approximately constant rate in mature, complex systems such as nuclear power plants (Perrow, Ott & Campbell, Duffey & Saull)
- Complex systems that are tightly coupled in the sense of dynamics) are especially vulnerable to unexpected events (Perrow, Sagan)
- Unexpected events are likely to be initiated at the human-machine interface (Reason).

Duffey & Saull, "Know the Risk", Butterworth Heinemann, (2001), ISBN 0-7506-7596-9
Perrow, "Normal Accidents", Princeton, (1999), ISBN 0- 691-00412-9
Ott & Campbell, "Statistical Evaluation of Design-Error Related Nuclear-Reactor Accidents, NSE 71 (1979)
Sagan, "The Limits of Safety", Princeton (1993), ISBN 0-691-02101-5
Reason, "Human Error", Cambridge, (1990), ISBN 0-521-31419-4

20

In recent years safety experts have recognized that systems such as aircraft and nuclear power plants can be made very safe – but not perfectly safe.

The concept of "normal accidents" has become generally accepted.

The Next Steps

- Utilize concepts that reduce the operators' work load.
- Utilize concepts that minimize the likelihood of plant damage.
- Utilize design concepts that reduce the maximum consequences of any accident
- After shutdown – delay, delay, delay ‡ decay, decay, decay
- Large heat capacity inside containment
- Enhanced accident management systems

21

Given today's capability for automatic control and operation, the panel operator's cognitive ability should be mostly reserved for analytical tasks and trouble-shooting. Extensive engineering support should be made available to the operating staff.

In addition to the well-developed nuclear safety design principles, the idea of "accident management" was introduced to limit maximum consequences.

In the future, plant designs might be chosen to further limit these consequences.

Delay is good – if the Chernobyl containment system had not failed for 24 hours, the public consequences would have been minimal.

Retaining a large heat capacity, along with provision of a slow response capability external to containment (days to weeks) for long-term accident management, can greatly improve ultimate protection.