Safer Nuclear Energy for the Future

Lecture 3 -- Future Design Directions

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 lecture outlines some design directions that are now, or could be, pursued to help ensure the safety of power plants in the future.

Recall that design is only a secondary determinant of plant safety, below the primary one of excellent plant operation.

Some Technical, Some Human Design Issues

- A complex system such as a nuclear plant has a long learning cycle. We now are working on the second or third generation - Gen IV is yet to come.
- Major design redirections (e.g. steam generators) require 25-50 years for their introduction into full service
- Conceptually identical reactors, built 20 years apart, are actually very different in detail due to technology changes.
- A new reactor type (e.g. fast breeder reactor) requires about 50 years to become useful within an existing nuclear system.
- The working life span of a nuclear engineer is about 40 years - so the total inventory of engineers, technicians and managers will be replaced in the time taken for a new system to be introduced.

2

The first nuclear power plants were installed in the 1950's. Yet, except for minor details and a narrowing of options, the plants being committed today are in many ways the same as those built 50 years ago.

This is a slowly-changing industry, mainly because it is a very large one with high incremental cost of a single unit. Buyers are very conservative, and good system characteristics take many years to become apparent.

The June 1997 IAEA symposium on future reactors and fuel cycles – the initial effort that has led to the current INPRO study – identified that new systems must be developed in the next decades if nuclear energy is going to make a substantive contribution to the world's energy needs in the long term.

Evolutionary change in both hardware and human subsystems is a very practical way of improving the whole system fairly quickly.

Even using old technology, the usefulness of nuclear energy can be improved greatly through horizontal diversification – e.g. hydrogen production, desalination, process heat, etc.

Examine Human Issues First

We have ~500 power plants operating in the world

If these plants do not operate well, there will be no future for nuclear energy

To replace all existing reactors with safer designs will require at least 50 years

Therefore, good human performance is the paramount safety issue today

3

Human performance can be improved in a relatively short term; much faster than we can change the overall plant hardware.

If human performance in the nuclear industry is not maintained at a very high level, this industry probably will be rejected by human society.

What follows is an outline of current human performance issues at a very general level.

Human Design Issues -- Historical Notes

- Gordon Brooks (1986) – "To a major degree, AECL's technological base resides in the minds of our people. If our people resource becomes depleted, for whatever reasons, then we will lose much of our technological base."
  - Causes
    - People leave the organization
    - People are reassigned to duties that do not utilize their accumulated skills and knowledge
    - People are de-motivated in their established corporate environment
    - People are given conflicting goals, such as over emphasis on meeting cost and schedule targets at the expense of technical quality.
- Dr. Masao Nozawa (1986) – "Quality work arises from within the individual worker and cannot be forced from outside. If you do not have this personal commitment you should not be building nuclear plants".
  - Comments made during debate within the International Nuclear Safety Advisory Group, IAEA.
  - During the same debate, Prof. Dr. Adolf Birkhofer (GRS) noted the increased policy emphasis (in Germany) on engineering and trade professionalism, and less emphasis on "paper" QA.

4

People have been talking about the issues of human performance since the beginning of history.

Some individuals and groups have achieved a very high level of performance, over a relatively short time period.

Unfortunately, words have been much more common than deeds.

Professionalism within the engineering community must be encouraged by senior management.

ßThis is an 'idealized' form of organization chart. It can be applied to any human organization – from smallest to largest. Shown here in 2-dimensional form, but it really is pyramidal – a power pyramid.

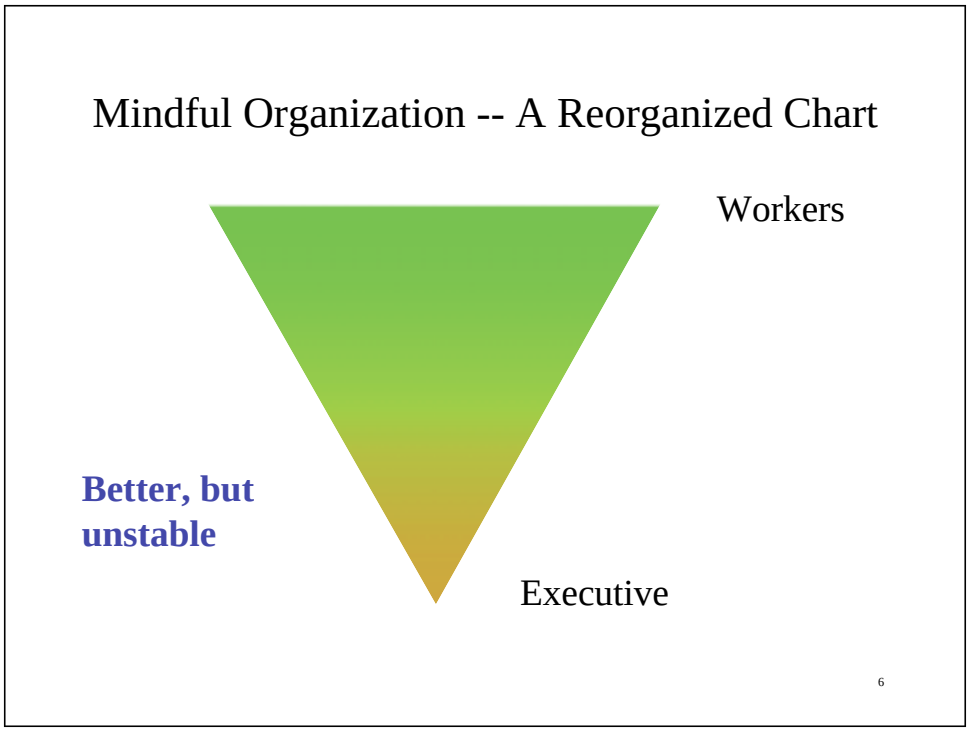
ßThe essence of this chart can be seen in the power and primacy of its apex, personified as THE BOSS.

ßAuthority is found at the top. But, of course, workers (at the bottom) are the ones who make the system work. They are responsible for keeping it running. So, here we have a conundrum.

ßBeing human, most bosses easily accept authority and attempt to place responsibility elsewhere. But responsibility and authority must go together, so the bosses must delegate authority in order to get anything done.

ßReluctant to delegate real authority, most bosses instead construct a set of policies, procedures, practices and platitudes to instruct the workers as to what they must and must not do.

ßBeing human, the workers often devise many ways to thwart the bosses' intent and directions. Good management is required to keep the whole organization moving in the same direction.



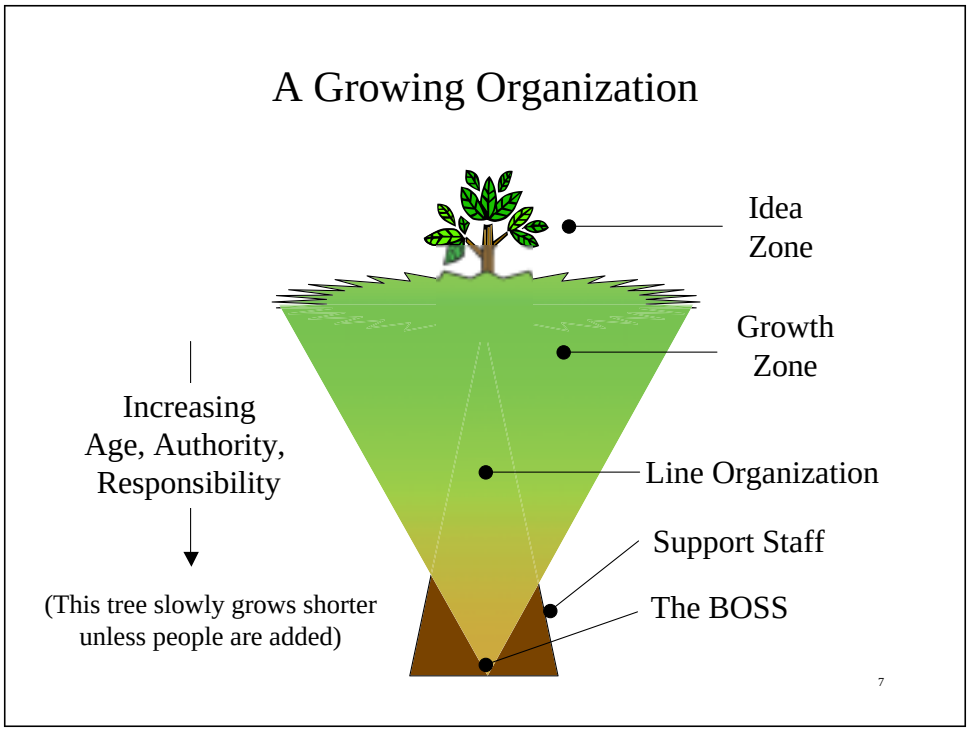
•This also is an 'ideal' organization chart – but reorganized.

•The BOSS obviously is placed in a position of great importance. He has authority over the whole organization, but also commensurate responsibility for keeping the whole thing going. Without his effort, the organization would disintegrate.

•However, now authority and responsibility are located together. As one proceeds UP the organization chart (a.k.a. Tree) the authority to act is progressively narrowed in line with the reduced responsibility at each level.

•Each WORKER has limited but clear responsibility to act within the bounds of his/her delegated authority.

•Any "trouble in the branches" can be quickly traced to its source – the lowest-level junction above which the trouble exists.



It is tempting to expand the comparison to growing things – trees, for example.

The analogy should not be pressed too far. Trees actually stand on the earth.

If time is added as a new variable, it is clear that the next promotion for the BOSS is actually into the earth – he/she will leave this organization and a new BOSS will take his/her place. This tree analogue grows steadily shorter unless people are added to the structure on a regular basis.

The portion of this organization that is not seen obviously is at least as important as the visible part. (The analogy involves the soil and the tree roots as the origin and source of energy for the tree. It is a separate and fascinating, but different, topic.)

A tree analogy is chosen deliberately because everyone can recognize the key features of each part of the tree, as well as the vital relationships between the parts. There is no need to invent new "Harvard Business School" language that can be so deadening for any individual employee, and certainly is hard to believe for the majority of workers.

This analogy clearly identifies the task of the workers – to grow and prosper according to the general rules set within the roots of the tree. It also provides a useful reminder that the individual worker is dependent on the whole tree growing under him/her.

Memory Aids for Safety Managers

- If you work near the trunk of the tree you must be strong -- flexible, but not too flexible.
- If your job is to support the tree you must accept yours as a service role.
- If you work at the bottom of the tree you must be aware of the organization's roots and the sources of its strength.
- If you work half way up the tree you must be aware of your duty to support the branches above you.
- If you work near the top of the tree you must be aware of your duty to think and to grow, and of your interdependence with those below you in the tree.

8

A continuing analogy, and a useful management model.

This image meets the requirement of being understandable and vital for nearly every person. Growth takes place mostly at the top of the tree; the trunk and intermediate branches grow only enough to support the structure above.

If a branch is unproductive for long it is simply cut off from the nutrients passing up the tree, and it dies.

(The inspiration for this imagery was the management system in use in Japan during the 1960's.)

Some Basic Realities

- Large Operations staff – and growing
- Medium demand for engineering staff – and growing (maintenance, refurbishment, technical assistance to operations)
- Intermittent, medium demand for project engineering staff
- Small to medium demand for experienced regulatory staff
- Small demand for new-plant design engineering staff
- Small demand for R&D specialists – shift toward support to operations
- Small to medium demand for educators and trainers

Engineering is a Self-Regulated Profession similar to Medicine and Law

An engineer's primary legal and ethical commitment is to the profession of engineering

9

This slide indicates the main parts of today's nuclear industry.

Unlike the situation at the beginning of the nuclear age, today's industry is NOT centered around science. Its center is to be found among the people who work in power plants – only some of them are engineers, and very few are scientists. The majority are trained as skilled workers in many different advanced technologies.

Recognizing the weaknesses in technology management that exist in many industries, many governments have created the self-regulating profession of engineering to manage high-technology issues on behalf of the society.

Engineers in these jurisdictions carry similar responsibility (and authority) over their profession as do doctors and lawyers, via a legally chartered association. .

The profession of engineering has, however, been weakened in many cases through the Imperative Management Approach favoured by modern business.

Engineers must learn to stand up for efficient and safe uses of high technology, as one of the society safety assurance mechanisms.

How Can We Make Safer Plants?

10

Having accepted that there is a need to design, build, and operate safer nuclear plants, how can it be done? We are dealing here with a large and diverse set of variables, and we already know that plants can be operated within a very high standard of public safety. The residual risks lie in the realm of very low probability, albeit with relatively large potential consequences to public health as well as to security of energy supply.

Low probabilities are very difficult to establish with a high level of confidence. A better approach may be to establish absolute limits to consequences, regardless of probability.

We already have sketched some of the principles essential for responsible human management of our industry, and now are ready to look at some of the technical issues.

Any Operating Plant Can Be a Safer Plant

- Even a less-than-perfect plant can be operated very safely by an excellent operating crew
- We can pay close attention to details of each malfunction, repair it, and learn the important lessons
- We can exchange experience freely with other operating crews such as done by the IAEA, WANO. etc.
- Exchange of staff and external audits can reduce the weaknesses inherent in a small closed technical society

11

An excellent operating crew can operate marginally-safe technologies (e.g. aircraft) very safely.

At the same time, a poor operating staff soon can destroy even the safest of power plants (or aircraft). Ignoring warning signs, sloppy maintenance, and many other types of personnel failure can cause expensive damage. The plants are “fragile”.

Nuclear power has a singular and under-appreciated advantage over many technologies, in that the power plant can be immediately made much safer simply by shutting off the chain reaction. This can be done manually, if the operators feel that something is not operating properly. Automatic systems can easily be designed to shut the plant down following sudden failures.

A plant owner must be aware of the need to protect the financial investment in the plant by supporting all efforts of the plant staff to operate the plant safely.

Fundamental Principles of Safe Design

- *Redundancy*: ensure that safety does not depend on any single system functioning correctly
- *Reliability:* design to numerical reliability targets (999/1000)
- *Testability:* ensure systems are testable in-service -- to demonstrate their reliability
- *Independence:* ensure systems which perform the same safety function are independent
- *Separation:* ensure systems which perform the same safety function are spatially separated
- *Diversity:* ensure where possible that systems which perform the same safety functions are of dissimilar design
- *Fail-safe:* ensure system/component fails safe -- if practical

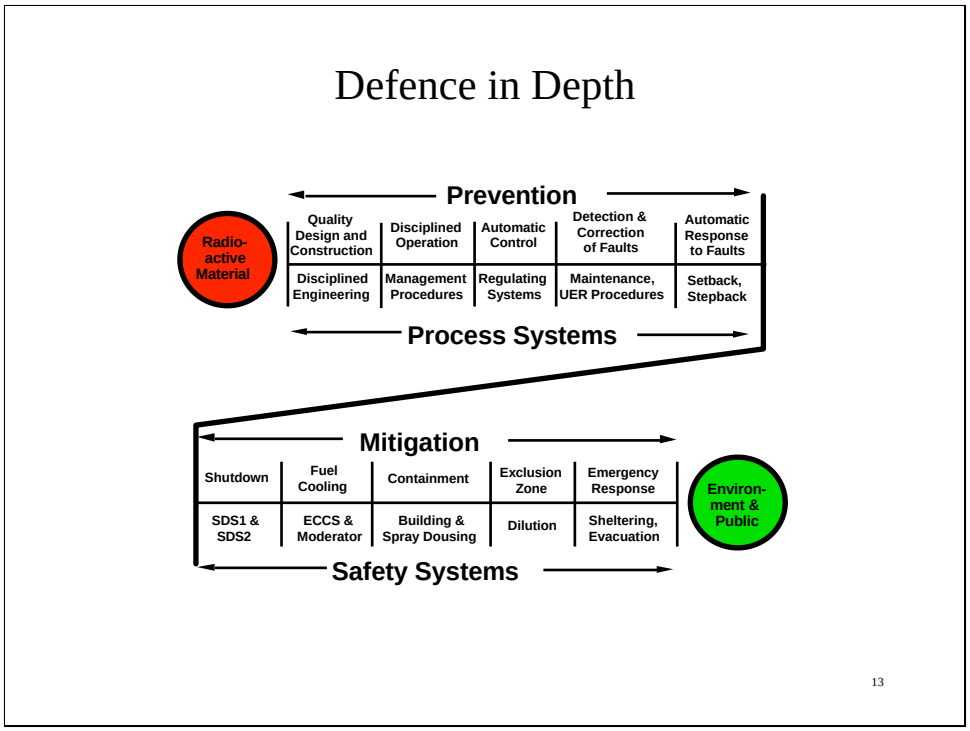
12

These well-established principles of safe design that are used in the nuclear power industry, anticipated the development of the principles of Normal Accident theory described by Charles Perrow.

Taken together, application of these principles as and when practicable can greatly reduce the frequency of Normal Accidents.

Note that these principles are hardware-based. They do not address the question of negative human intervention, or human neglect.

Human error has been at least one of the important elements present in every serious reactor accident to date.



This slide includes at least some of the human-related principles, but only those immediately recognizable as management goals.

Management goals sometimes are subverted in complex organizations.

The best way to ensure that management goals are met, if you are a manager, is to follow them yourself. Also let everyone in you organization know that this is the way you want them to behave.

All of these systems are imperfect. The result can be near-perfect if everything works as designed, and if all the defensive barriers are complete. Even in the event that some barriers are degraded when they are needed, other barriers usually can intercept and mitigate the consequences. But -----

Can New, 'Safer' Plant Designs Improve Public Acceptance?

- **Very Unlikely**
  - Trust has been lost (for whatever reasons) -- regaining trust takes time.
  - Excellent operation, for many years, is both a necessary and a sufficient condition
- **Positive Factors**
  - Need for nuclear energy is increasing as price,and availability of fossil fuels both are getting worse
  - Today, there is much greater attention to achieving excellence in plant operation

14

Even if we build safer plants, it likely will take some decades for many people to feel comfortable about nuclear energy.

The loss of trust, whether justified or not, can be repaired only by a long period of good behaviour.

On the positive side, in the future there may not be many alternatives to use of nuclear energy for energy-intensive human activities. The age of fossil fuels is nearing its end.

Many people have recognized the need for safe operation. Unfortunately, commercial imperatives seem to reinforce a dominating production imperative. A senior manager may be fully aware of the importance of safety, but may still over-emphasize production under pressures from external factors or under his/her own personal ambition.

Caution is advised.

High Reliability Approach*

- Safety is the primary organizational objective
- Redundancy enhances safety: duplication and overlap can make "a reliable system out of unreliable parts"
- Decentralized decision-making permits prompt and flexible field-level responses to surprises
- A "culture of reliability" enhances safety by encouraging uniform action by operators. Strict organizational structure is in place
- Continuous operations, training, and simulations create and maintain a high level of system reliability
- Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations

Accidents can be prevented through good organizational design and management

* Charles Perrow"Normal Accidenst - Living with High-Risk Technologies", Princeton, 1999, ISBN 0-691-00412-9, and Scott Sagan, "The Limits of Safety", Princeton, 1993, ISBN 0-691-03221-1

15

Here is the traditional high-reliability approach, as described by Scott Sagan. Many safety professionals in the nuclear industry will recognize all of them from experience.

As noted many years ago by Nozawa and others, excellent human performance arises from within an individual and is difficult, if not impossible, to impose from outside.

The blue-highlighted text represents the "prevention" side of good safety management.

Note that the text should be modified to recognize the imperfection of any accident prevention system.

But Then, One Fine Day ----

The Unexpected Happens!

16

Frequently, reviews of major accidents show that a number of unrelated "stopper" situations (our defence in depth components) were passed in sequence before the accident.

(Example: Andrea Doria sinking: – fog – break in fog – pilot sees the liner Stockholm -- turn to port instead of starboard – no ballast in empty fuel tanks – liner with reinforced bow collides on starboard bow – pumps & pipes installed high in center of deck, lines broken – etc., etc.)

Unusual and sometimes completely unexpected events do happen.

The safety objective becomes one of mitigation, rather than prevention.

The lower half of Slide 13 becomes predominant. Dedicated, automatic safety systems respond to restore safe conditions

But these systems also are imperfect!

Many people are still frightened!

Normal Accidents -- The Reality*

- Safety is one of a number of competing objectives
- Redundancy often causes accidents. It increases interactive complexity and opaqueness and encourages risk-taking
- Organizational contradiction: decentralization is needed for complexity and time-dependent decisions, but centralization is needed for tightly coupled systems
- A "Culture of Reliability" is weakened by diluted accountability
- Organizations cannot train for unimagined, highly dangerous, or politically unpalatable operations
- Denial of responsibility, faulty reporting, and reconstruction of history cripples learning efforts

Accidents are inevitable in complex and tightly coupled systems

* Perrow, Sagan, ibid.

17

Scott Sagan's list of the underlying causes of normal accidents, shown here, are primarily human factors.

Accepting the fact of inevitable, though rare, accidents has been usual in the nuclear industry.

However, we wisely nod and relegate such events to the regime of incredulity by quoting probabilities such as 10-7.

Many people feel, intuitively, that Unidentified Failure Modes, Surprises, and strange happenings (dinosaurs) still might defeat all of these systems. They are skeptical.

So, what can a designer do?

Human Imperfection is Universal and Persistent

- A combination of human-oriented procedures as well as careful machine design are both necessary to prevent consequences from rare major accidents.
- It is difficult to sustain a high level of protection over several decades -- but it can be done , at some cost.
- Public knowledge of human imperfection likely is a major cause of doubt of "High Reliability industry".
- It is useful to consider ways to reduce or eliminate the negative consequences of major accidents, as rare as they may be.

18

It is suggested here that the designer should take a look at "Impossible" events; that is, to ignore the occurrence frequency and to look at the maximum consequences.

The designer should look at what can be done t limit the public consequences.

Example: Consider the containment concept, popular in Germany, to install equipment such that one can give assurances that massive public evacuation will never be necessary regardless of any accident inside the plant.

Easy to say, difficult to prove.

Partly as a result of good management, partly because of inherent characteristics, and partly because of good luck, the CANDU-PHWR has an "ultimate" safety case that is quite easy to prove.

To Improve Safety

Change the Human Factors First

<u>This Way is Much Faster</u>

19

To recall the basics – take care of human behaviour first.

During the period of adjustment (about 50 years) leading to safer technologies for nuclear power, manage the existing technology safely.

Evolve the existing technology at the same time, with economics and safety in step together.

<u>Learn from operating experience.</u>

Summary Recommendations

- Reorganize the responsibility and authority structure of operating utilities and other members of the safety management system, to ensure that authority and commensurate responsibility are placed in the same hands.
- Recognize the realities of “normal” accidents.
- Learn to manage the unexpected - it is expected to happen.

20