A Stroll Down the Risk Acceptance Curve

Dan Meneley, AECL Engineer Emeritus
President, Canadian Nuclear Society

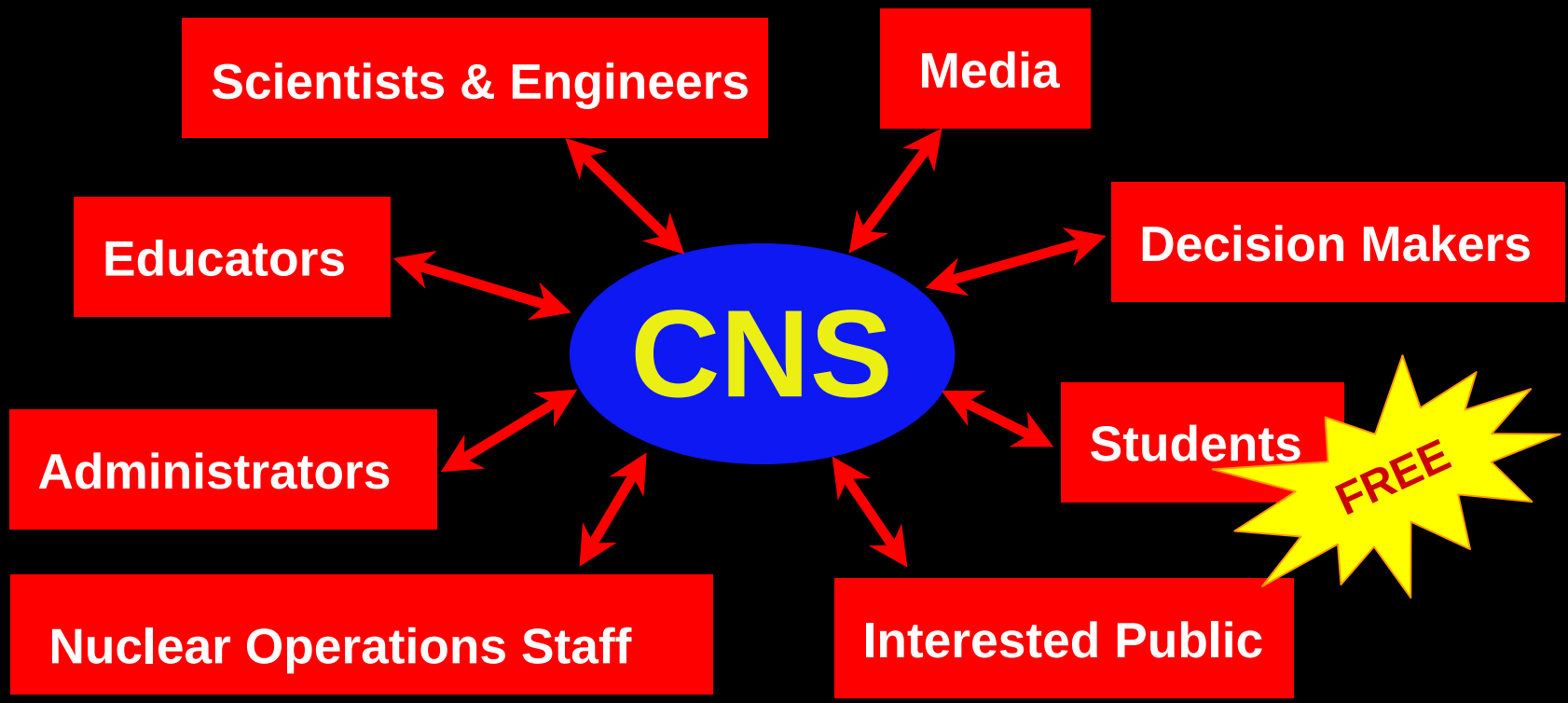
To

Chalk River Branch of CNS

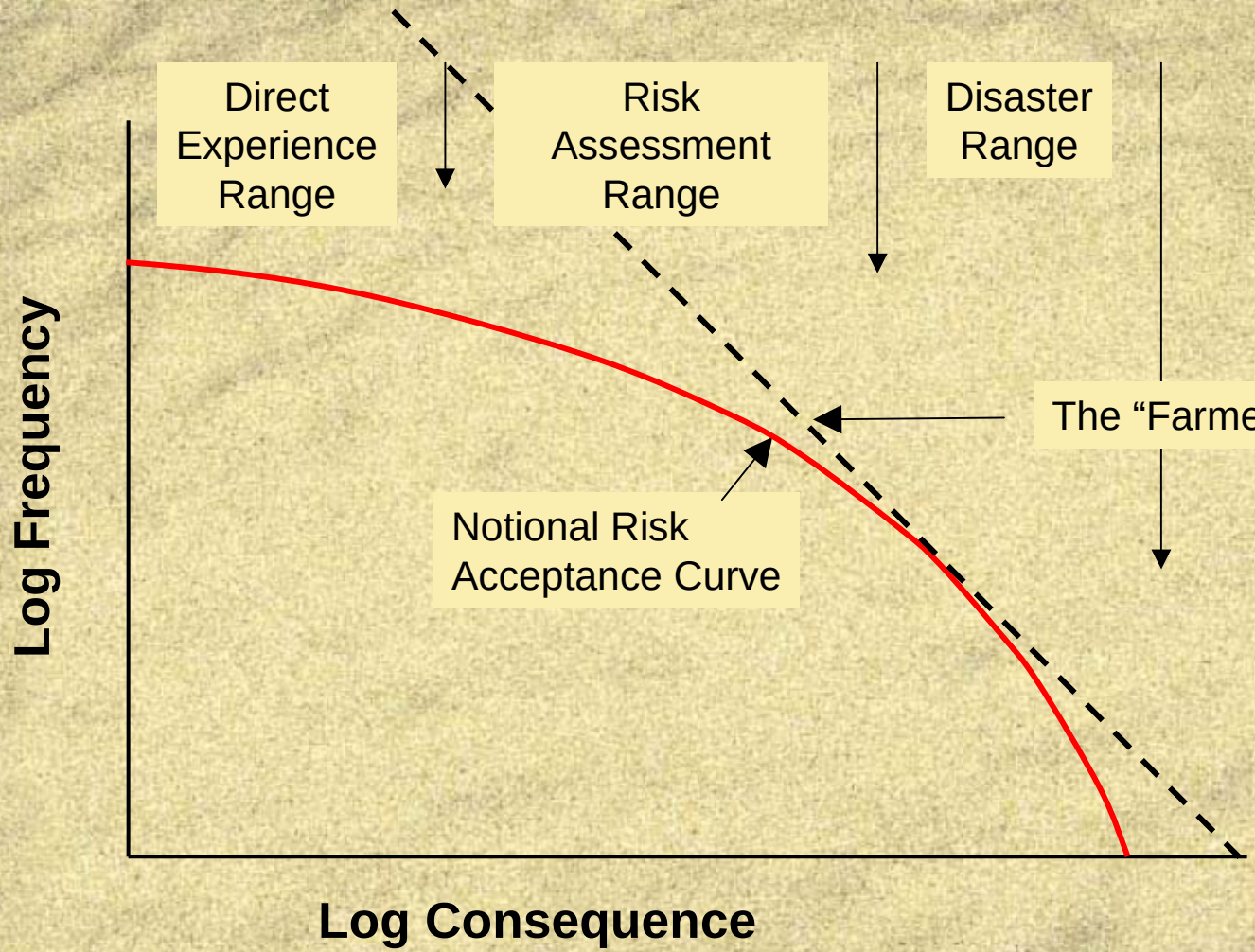
March 07, 2007

The Canadian Nuclear Society

- ***People*** supporting applied nuclear science & technology
- ***Communication*** on technical nuclear issues
- ***Independence*** – no corporate or government mandate
- Established 1979, independently incorporated 1998

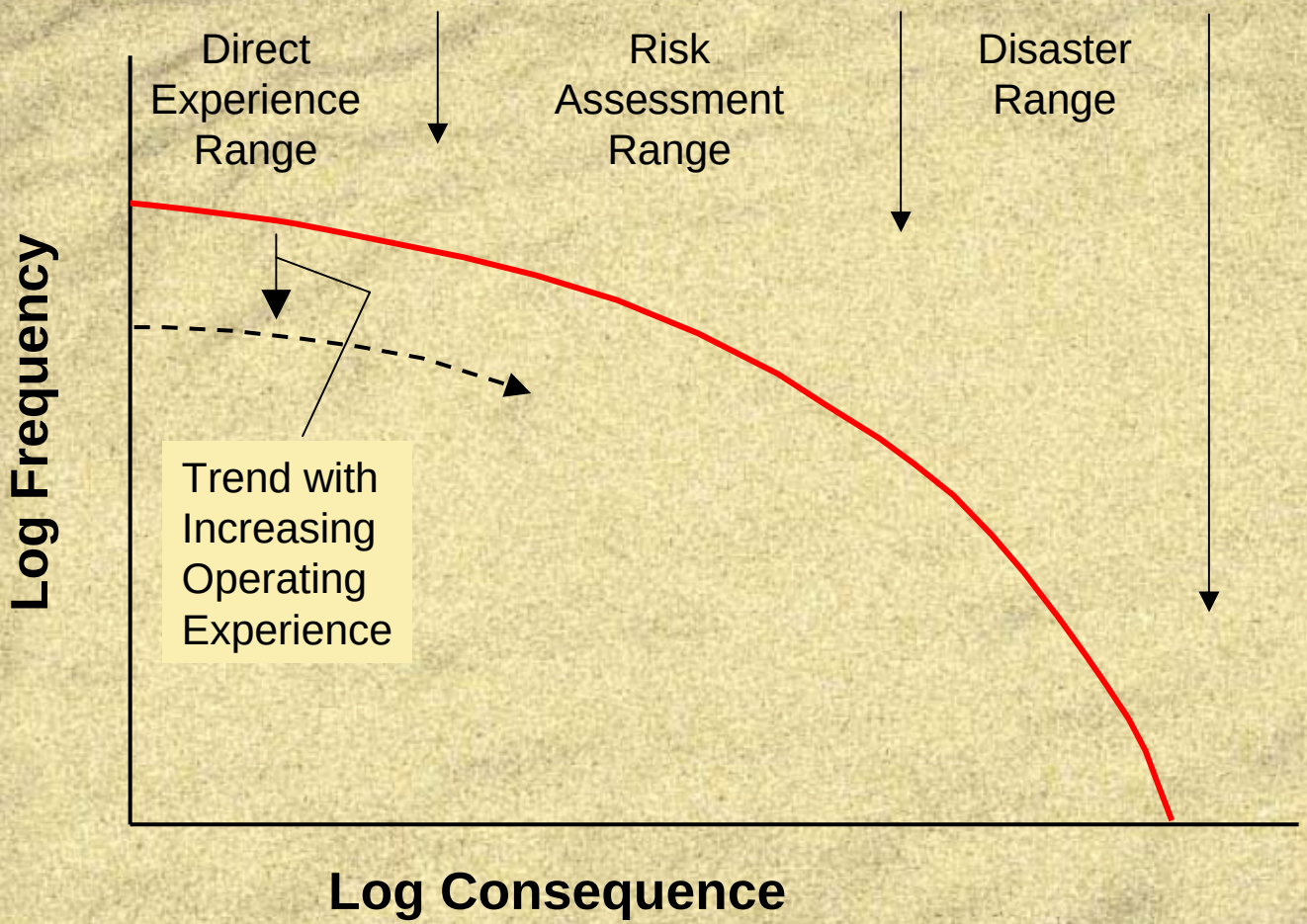


Notional Risk Curves, and Trends



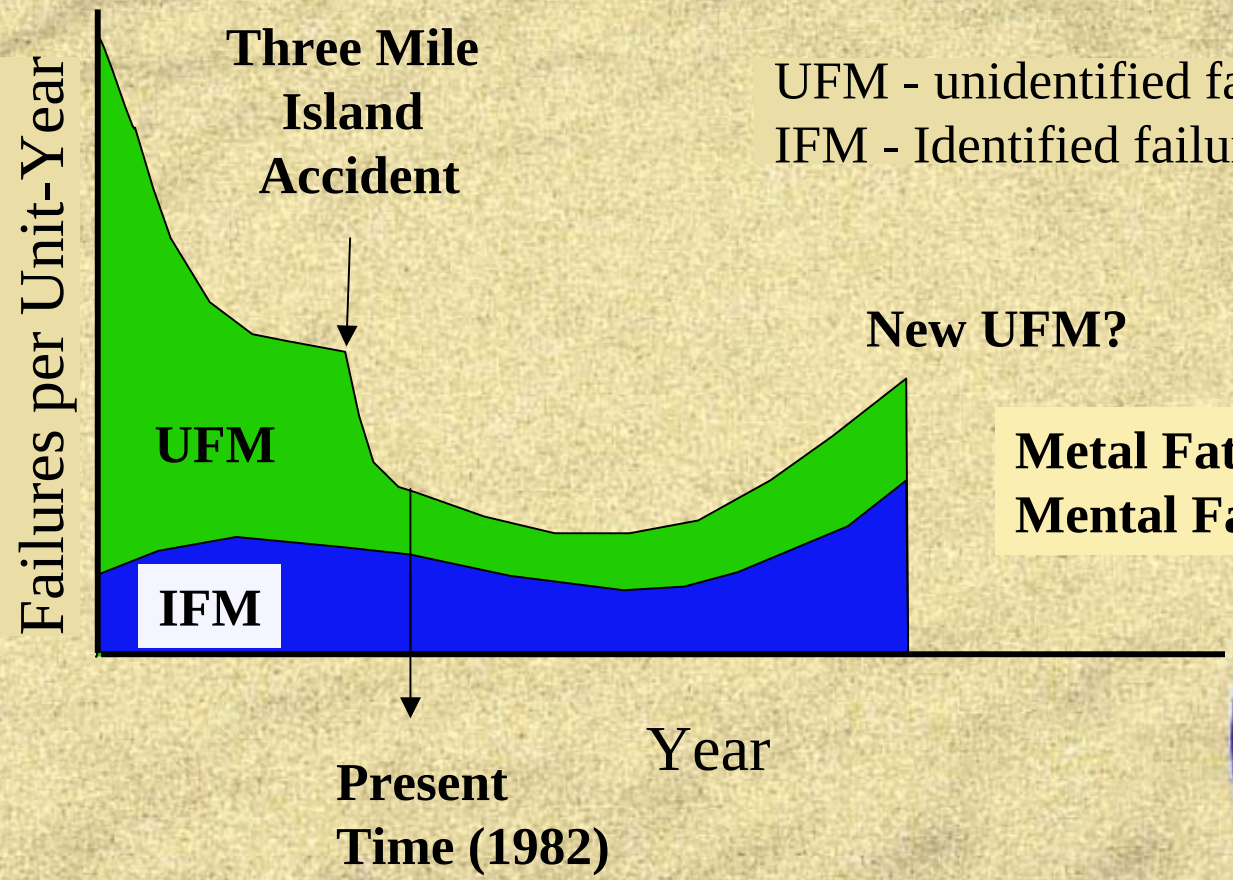
The risk is zero before the first reactor startup.

Notional Risk Curves, and Trends



A Learning Experience??

Ref. Meneley (1982)



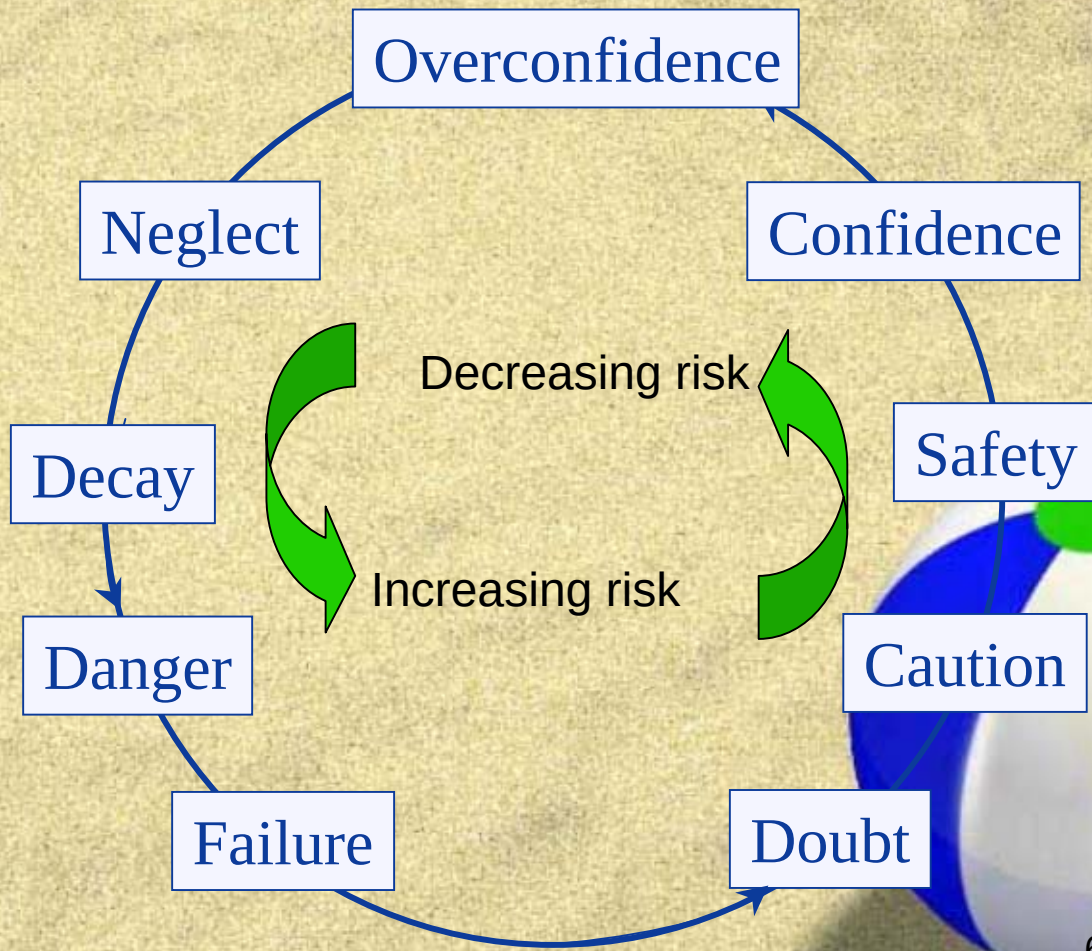
UFM - unidentified failure mode
IFM - Identified failure mode

Metal Fatigue -- or Mental Fatigue?

To Err is ∧ Human

(Machines are too stupid to make mistakes)

The human cycle of performance



Direct Experience Range
Everyday risks, realized costs

- Production loss
- Shutdown
- Personnel injury
- Public injury
- Plant damage

- See Chauncey Starr and Chris Whipple, "Coping with Nuclear Plant Risks", Nuclear Safety 23, 1, (1982)

Down under the trips

- "That parameter looks a bit funny, Charlie. It is different than it was on my last shift."
- A smart monitoring system should be "thinking" in the same way.
- Management should be listening to both of these warning signs

- This issue is MONEY -- it's not how much you make, it's how much you avoid losing.

What, me Worry?

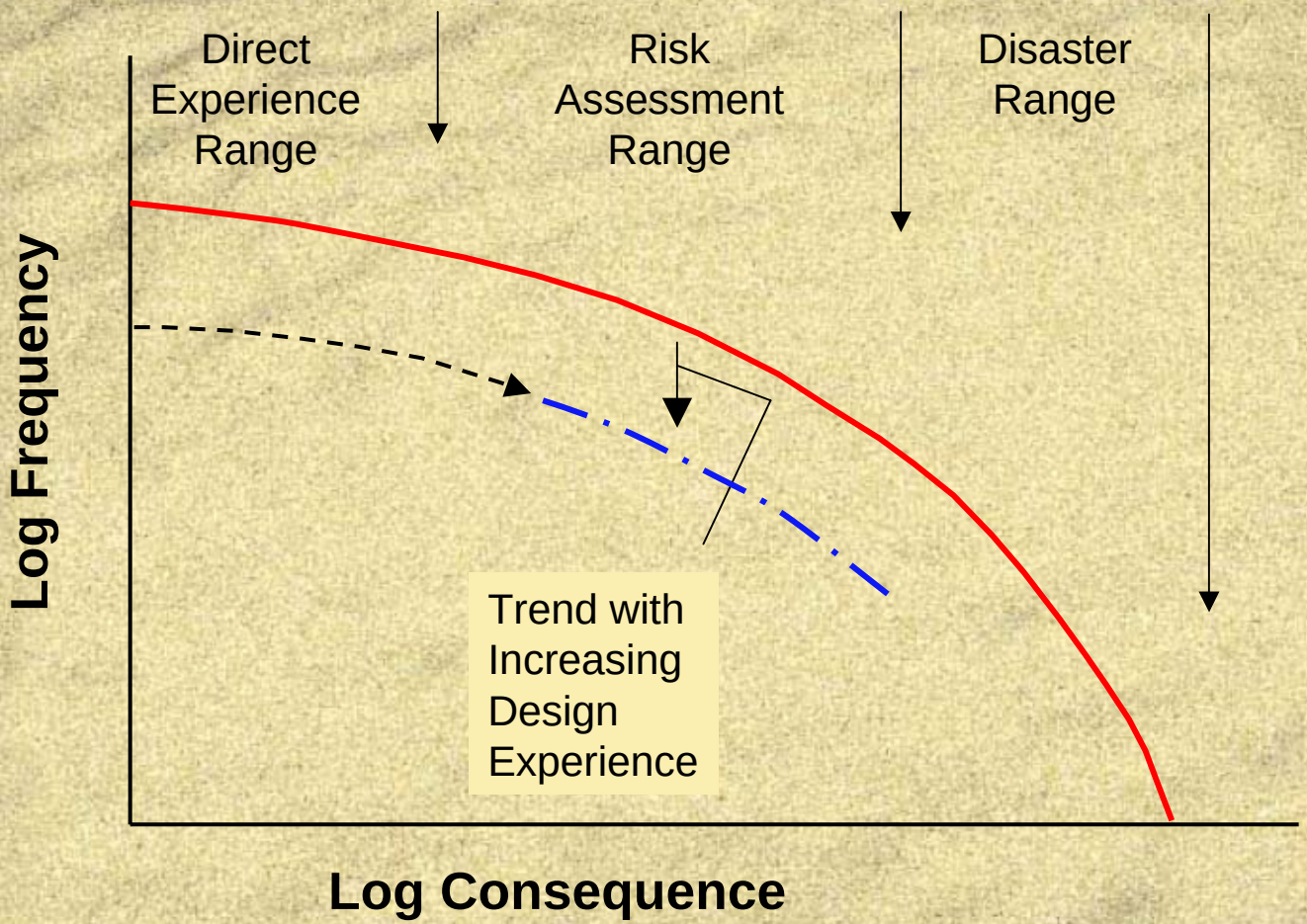
- **The owner should worry**
- **The vendor should worry**
- **The engineer/designer should worry**
- **The regulator should observe actual human performance**

The owner is the most important worrier in this risk range -- the plant is expensive and the demands on its operating reliability are very high.

The long term result of good performance is

trust

Notional Risk Curves, and Trends



Risk Assessment Range
Practicing PSA

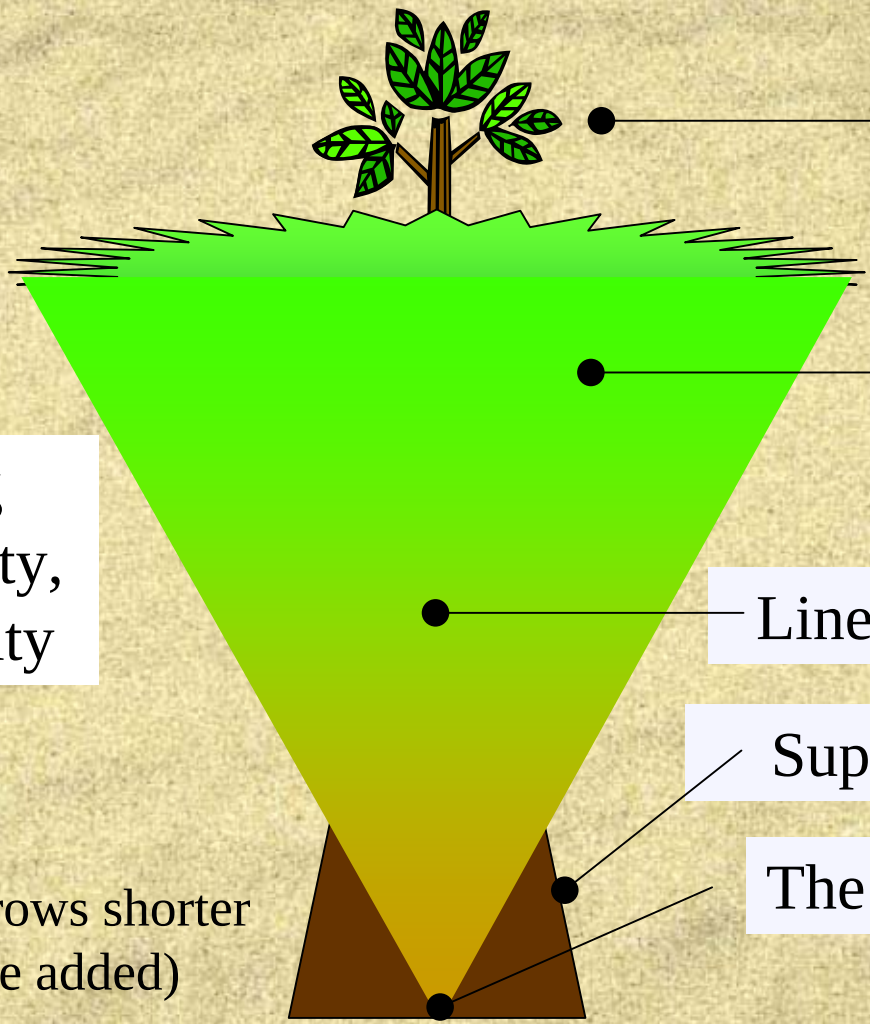
- Upgrade the plant's PSA model using results of operating experience and testing
  - Use results gathered from all similar components and systems
- Track all failure information gathered from world nuclear units - it is better to learn from other peoples' mistakes
- Managers and regulators must pay attention to these results, and how they are handled

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."
  - 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, e.g. over-emphasis on meeting cost & 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". (Comment during debate within the International Nuclear Safety Advisory Group, IAEA)

A Growing Organization



Idea Zone

Growth Zone

Line Organization

Support Staff

The BOSS

Increasing Age, Authority, Responsibility

(This tree slowly grows shorter unless people are added)

Rules vs Expectations

- Life experience tells us that obediently following rigid rules does two undesirable things:
  - It turns a thinking human into a machine (which never makes mistakes)
  - It removes personal responsibility. When something bad happens, "It's not my fault"
- Managers need to do more than expect excellence
  - They need to show it by example
  - They need to recognize it when it occurs
- Regulatory staff also need to accept responsibility
  - The regulatory organization is granted substantial power
  - Commensurate responsibility comes along with that power

Eight Antinomies

(Conclusions of Shunsuke Kondo -- Chairman of the Investigation Committee, Tokai Nuclear Fuel Plant Accident)

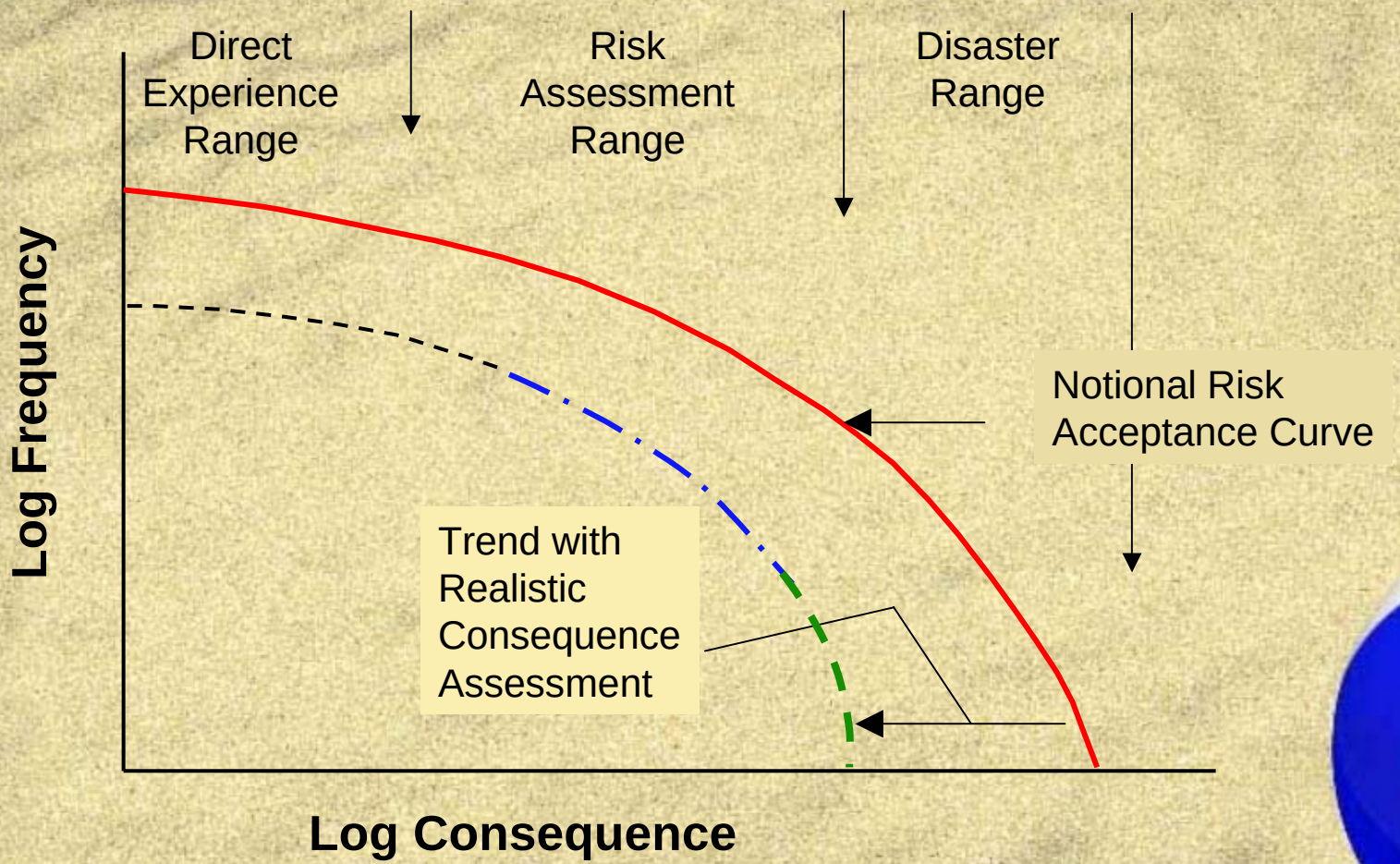
A. **If safety increases, efficiency decreases;**
B. **If regulations are reinforced, creativity is lost;**
C. **If surveillance is reinforced, spirit declines;**
D. **If manuals are introduced, self-management is lost;**
E. **If fool-proof measures are implemented, the level of skills decreases;**
F. **If responsibilities are centered on a key person, the group loses concentricity;**
G. **If responsibilities are too strict, cover-ups result;**
H. **If information disclosure is promoted, situation becomes too conservative.**

Reason and Risk

- James Reason, “Human Error”, Cambridge Univ. Press, (1990), ISBN 0-521-31419-4: “While cognitive psychology can tell us something about an individual’s potential for error, it has very little to say about how these individual tendencies interact within complex groupings of people working in high-risk systems. And it is these collective failures that represent the major residual hazard”

- David Mosey, “Reactor Accidents, Institutional Failure in the Nuclear Industry” 2nd Edition, NEI Special publications, (2006), ISBN 1-903-07745-1: “The {nuclear} industry has the resources, experience, and expertise to develop more effective approaches to safety management which might not only be applicable, but also, one hopes, applied to the management of other technologies.”

Notional Risk Curves, and Trends



The Disaster Range
How Bad Can if Get?

- **People don't believe small probabilities**
  - **Accept the consequences and tell people what they are**
- **Look very carefully at severe accident models.**
- **Maximum consequences depend on the power plant's basic design features and operating conditions**

- J.T. Rogers et. al.: "Severe Accidents in CANDU Reactors", Proc. Int'l Conf. of ICMT, Izmir, Turkey, 1996
- John C. Luxat, "The Consequences of Failure to Shutdown Following a Loss of Coolant Accident in a Pickering NGS A Unit", CNS Bulletin, 9, No. 2 (1988)
- Dan Meneley, "A Reactor Cannot Explode Like a Nuclear Bomb", <http://canteach.candu.org/aecl.html#AECLPAPERS>

Accidents Will Happen

- 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)
- Mindful people hold complex projects together because they understand what is happening (Weick & Sutcliffe)

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

Weick & Sutcliffe, "Managing the Unexpected", Jossy-Bass (Wiley), (2001), ISBN 0-7879-5627-9

CANDU "Disaster" Consequences

- No extensive fuel melting, even following extreme events
  - Molten fuel quenching following LOSDS events
  (Cool moderator water, cool shield tank water)
- Low-dose health effects fall below the LNT line
- Use realistic assumptions in all analysis, plus uncertainties
  - Use Monte Carlo models to account for parameter uncertainties

- Most probable result for CANDU: It is not possible to cause early fatalities, in any event.
  - Correct low-dose assumptions in the long term

PWR & CANDU
Different Accidents, Similar Effect

- **CANDU**
  - Large break in heat transport piping
  - Voiding of coolant in the core produces a positive reactivity
  - Small power pulse is terminated by fast shutdown -- small Doppler feedback. Two redundant shutdown systems.
  - Core must be refilled by the emergency core cooling system
  - Moderator will cool debris if ECCS fails

- **PWR**
  - Large break in main steam piping
  - Cool water pumped through the core produces a positive reactivity
  - Large power pulse is terminated by fast shutdown plus Doppler feedback One fast shutdown system (limited depth)
  - Final reactivity is near critical
  - High power fuel elements probably fail and disrupt the core geometry - (flow diversion away from blockage)

Sizewell B nuclear power station

- The findings of NII's assessment of British Energy's periodic safety review
- **Description of plant**
  - Sizewell B nuclear power station is situated on the Suffolk coast, approximately 40 km north east of Ipswich, near the town of Leiston. The Sizewell B PWR is a four-loop plant and is a development of the US Standardised Nuclear Unit Power Plant System (SNUPPS) design, which was augmented mainly to accommodate UK siting and safety requirements.
  - Changes to the SNUPPS design include:
    - two diverse reactor protection systems;
    - an emergency boration (diverse shutdown) system (EBS);
    - four physically segregated trains of protection and safeguards equipment;
    - improved emergency core cooling systems;

How About Coolant Void Reactivity?

- Consequences of piping failure depend on:
  - Voiding rate
  - Reactivity change on coolant void
  - Doppler feedback coefficient of fuel
  - Response time of shutdown systems
  - Prompt neutron lifetime
- We must accept the fact that all reactors have some potential for RIA accidents
  - The void reactivity is not important in severe CANDU accidents
  - Ultimate defences are low peak fuel reactivity, long prompt lifetime, and huge reserve of cool water in and around the core.

Loss of Shutdown - A Thought Experiment

- Energetic FCI in each fuel channel - not simultaneous
- In open air, the result is a series of small explosions
- If the crackers are inside a can, pressure builds up inside until the can bursts
- (If neutron lifetime is short the situation is quasistatic)
- Bursting of the can "synchonizes" the energy release to one instant of time

Conclusion: If a reactor is placed inside a surrounding pressure vessel, then both the power and coolant void coefficients must be negative.

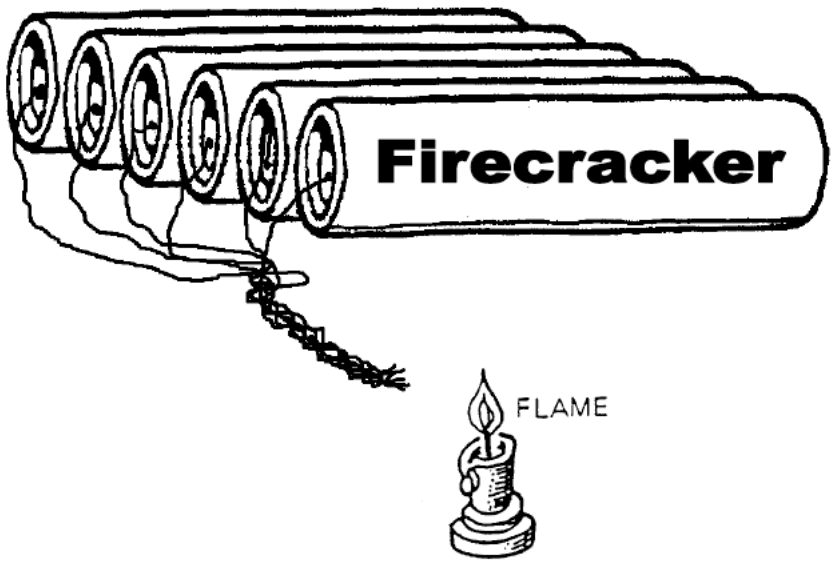


Figure 7 A pressure vessel experiment

How to choose a reactor type

- The same way you should choose a marriage partner:
  - Look around carefully to find a good one
  - Recognize that each and every choice will have some flaws
  - Remember that trading for a new one later on would be painful, and probably expensive

- Then, be prepared to spend the rest of your life trying to correct those flaws

- CANDU designers and operators are lucky -they chose a safe partner

Comparisons - always odious

- Any modern, well-designed and well-managed nuclear power plant is a good neighbour
- Even a poorly designed and poorly managed nuclear power plant can be operated safely by an expert, mindful crew
- ONLY when studying extreme events (such as loss of shutdown or LOCA + LOECC), differences in the inherent characteristics of various designs become important.
- CANDU looks very good in any such comparison.