Tolerability of Risk from Critical Infrastructure

Hydro-electric industry risks and catastrophic loss from dam failures

Dr. D.N.D. Hartford

BA, BAI, MA, Ph.D, F.EIC, F.ICE, F.IEI, C.Eng, Eur.Ing, P.Eng, M.ASCE, M.IVA

Principal Engineering Scientist, BC Hydro

BC hydro

FOR GENERATIONS

19-06-2013

Outline

1. A “risk-taker’s” view of regulatory expectations
2. A brief history of Tolerability of Risk from Dams
3. Realization that we had got it wrong
4. Agreements and disagreements within the industry
5. Why we got it wrong
6. How we are rectifying matters
7. Where we stand to day
8. Transferring the matter of risk from dams from the engineers to the public
9. Disclosure, explanation and societal consent
10. Moral issue – are we really talking about protecting life at any cost?
11. What we need to have happen next
12. Is there a way forward? – or will it be a case of “Go directly to jail” in the event of a dam failure?

A “risk-creator’s view”

The regulator should be expecting me to provide the Agency and the public with:

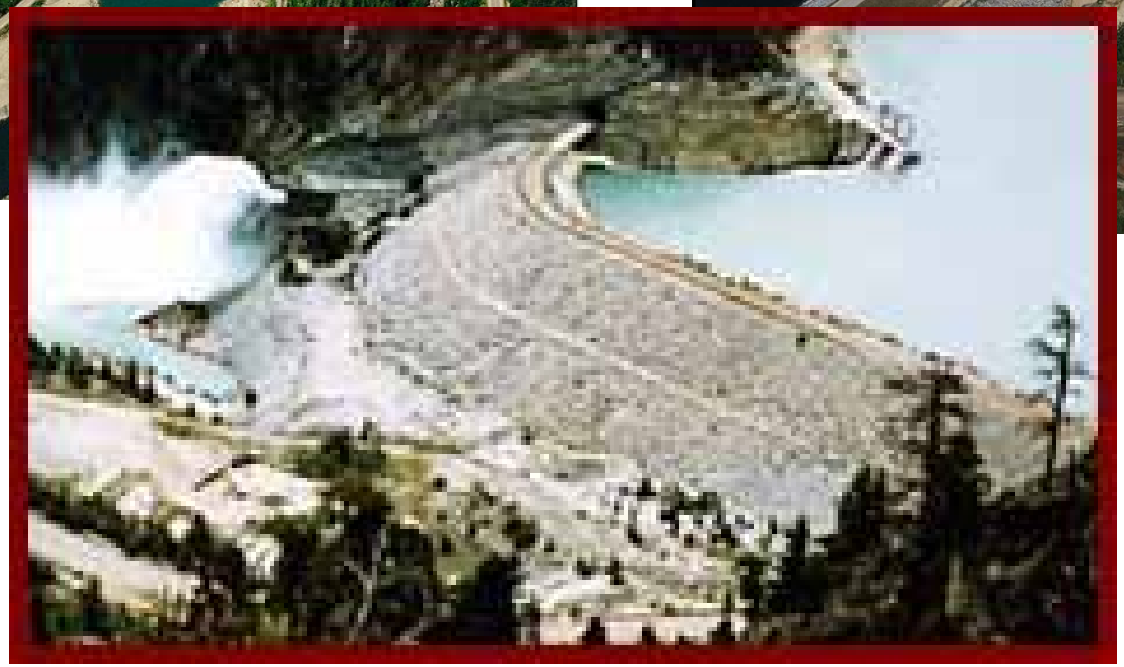
- reliable knowledge in a way that they can make informed decisions about;
- how I propose to control the risk and to what level.

According to Ms. J.H. Bacon, a former “risk regulator” (UK HSE)

- *“Risk-regulation is, I suggest, not first and foremost about protecting people at all costs. It is about making trade-offs. Trade-offs between different risks; between risks to some individuals or groups, and risks to others; between costs and benefits.*

- *It is the nature of risk that, frequently, those who create the risk do not bear its consequences nor its wider costs. So the market does not function properly as a distributive mechanism. The State must intervene to regulate risk.”*

3 Well-known BC Hydro Dams



Our Industry

Is a hazardous process industry

- We create a hazardous product by means of a hazardous process and we deliver it to our customers in a hazardous ways
  - Opportunities for things to go horribly wrong abound
  - Many with the potential for disastrous consequences
- Prior to Bhopal, dam failure accounted for more multiple death catastrophes than any industrial peacetime artefact.

- Risks, uncertainties, costs, benefits, products and services are facts of life, as is the potential for catastrophic losses.

From engineering standards to risk decisions

In 1993, Gary Salmon, BC Hydro's Director of Dam Safety proposed:

- That the safety of dams should be based on a constant risk-cost criteria
  - That is probability of an accident x the cost of the losses
  - For Loss of Life
    - A risk-cost of 1 life lost per 1,000 years of dam operation
  - For Financial Loss
    - A risk cost of $10,000/year
  - The unique idea was to separate human life from $'s
    - The previous proposal by ASCE and followed up by USBR was in terms of "$'s to save a life" calculations
  - The proposed risk cost of loss of life had no basis – it was just "made up"

I was hired to make Gary Salmon's proposal work

- Including to justify the risk cost criteria
  - I didn't justify Gary's criteria, I
  - Instead, copied the idea of Tolerability of Risk from the UK Health and Safety Executive's Tolerability of Risk from Nuclear Power Stations

To make the proposal work

We needed completely different approaches to

- Analysing the safety of dams,
  - Answering the question *"How Safe is the Dam?"*
- Replacing engineering standards with "risk criteria"
  - Answering the question *"Is the Dam Safe Enough?"*

The way to make the proposal work was to:

- Set the safety of dams in proportion to the consequences of dam failure
- To choose a generally agreed frequency of "death in industrial accidents"

How to get the proposal accepted as the basis for decision-making was not part of the assignment

- The idea was to separately gain industry acceptance in the same way as engineering standards become established

Ball-park view of risk to life "criteria"

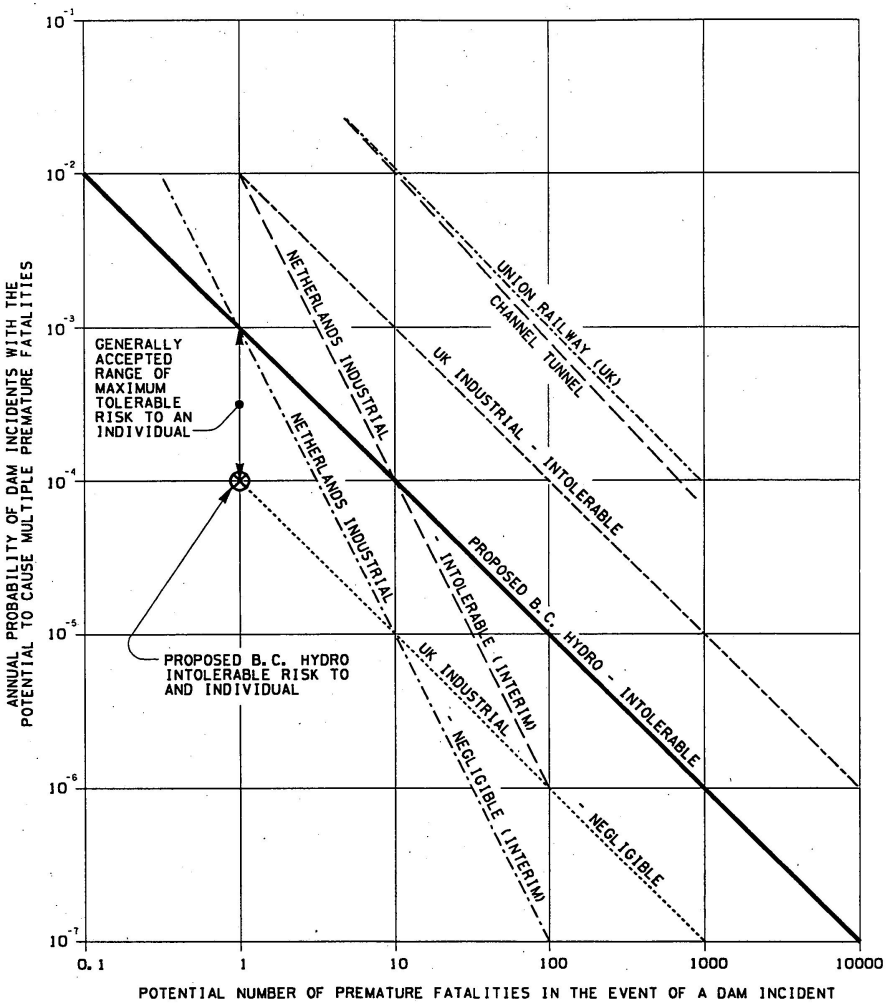


FIG. A-2: COMPARISON OF PROPOSED INDIVIDUAL AND SOCIETAL RISK CRITERIA AND RISK CRITERIA USED IN THE NETHERLANDS AND UNITED KINGDOM

1993 - 1998

BC hydro
FOR GENERATIONS

After 10 intensive tests of the methods over 5 years

- including a risk analysis on a subsequently decommissioned dam
  - Where we got to see how well we had represented the sources of risk in the dam
    - 2 independent groups and one eminent expert reviewer had come to different conclusions
      - None were remotely close!
  - BC Hydro abandoned the proposed “Expected Value” risk evaluation criteria and also abandoned attempts to use these risk analysis methods to “sign-off” on the safety of dams.
    - New Director of Dam Safety!

The “retreat” to established practice proved to be even more problematic.

- Our 5-years experimenting with risk analysis had revealed numerous problems with established practice
  - Such as designing dams to withstand the “Minimum Incredible Earthquake”!
    - And ignoring operational causes of failures!

1998 - 2008

BC hydro
FOR GENERATIONS

Textbook on Risk and Uncertainty in Dam Safety

- Hartford and Baecher (2004) published by Thomas Telford
- Dr. McCann was a contributor to Chapter 4

International Commission on Dams Bulletin 130

- Risk Assessment in Dam Safety Practice – A reconnaissance of the Benefits, Methods and Current Applications
  - Introduced the notion of "risk-informed" dam safety decisions"
    - From NRC 1996 Understanding Risk – Making decisions in a democratic society

Some individuals, companies, NGO's and dam owning organisations:

- became convinced that the "silver bullet" had been not only discovered but,
  - The process of replication of the "silver bullet" had been perfected.

BC Hydro was not convinced – why?

- We realized that *"we didn't have the right science"*, and,
- *We didn't get the science we had right!*

Since 2008

BC hydro
FOR GENERATIONS

Careful examination of what had become “contemporary” risk assessment practice revealed:

- It is a quasi-probabilistic veneer applied to traditional dam safety practice
  - Need to develop a “completely different” approach to dam safety analysis
  - This time based on a different safety management philosophy

Development of “Risk-Informed” Dam Safety Decision-making philosophy:

- based on previously identified concept of “risk-informed” decisions
- UK HSE
  - Working with the architects of the UK HSE framework
- NRC 1996

Abandoned the idea of working towards a solution within the Dam Engineering Community

- Instead work with the architects of the two established risk regulation regimes to develop a new proposal for the basis of risk-informed dam safety decision-making.

To-day our focus is on….

Avoiding being negligent

- Not as straightforward as it looks!
  - Negligence as I understand it: "*criminal negligence, punishable by up to life imprisonment requires proving someone saw a risk and went ahead with the action anyway*".
- My problem is that not only do I see the risks
  - I characterize them in in great detail
- Clear distinction between
  - Failures initiated by natural hazards, and,
  - Failures due to errors or omissions in Design, Construction, Maintenance and Operation
    - Treat them differently in the decision-process

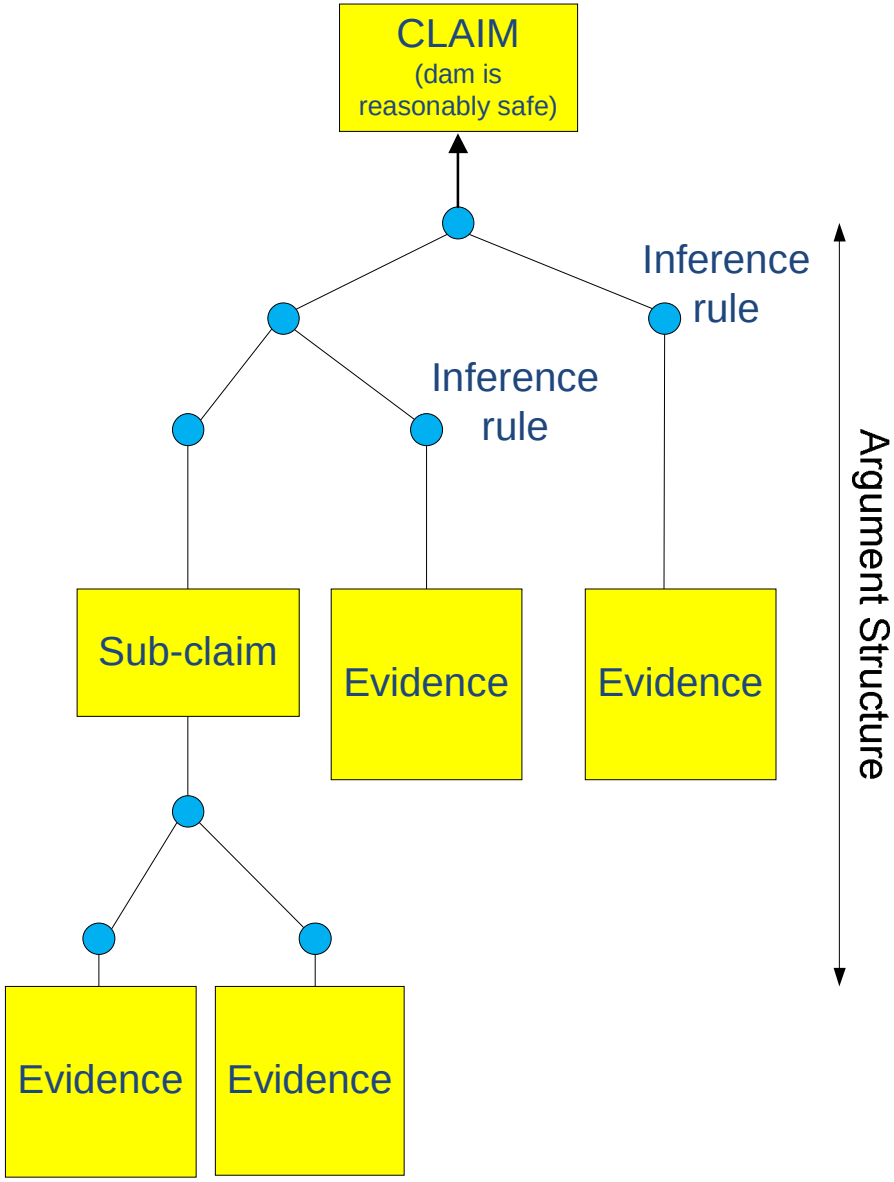
So is it a case of *"Go Directly to Jail"* etc…?

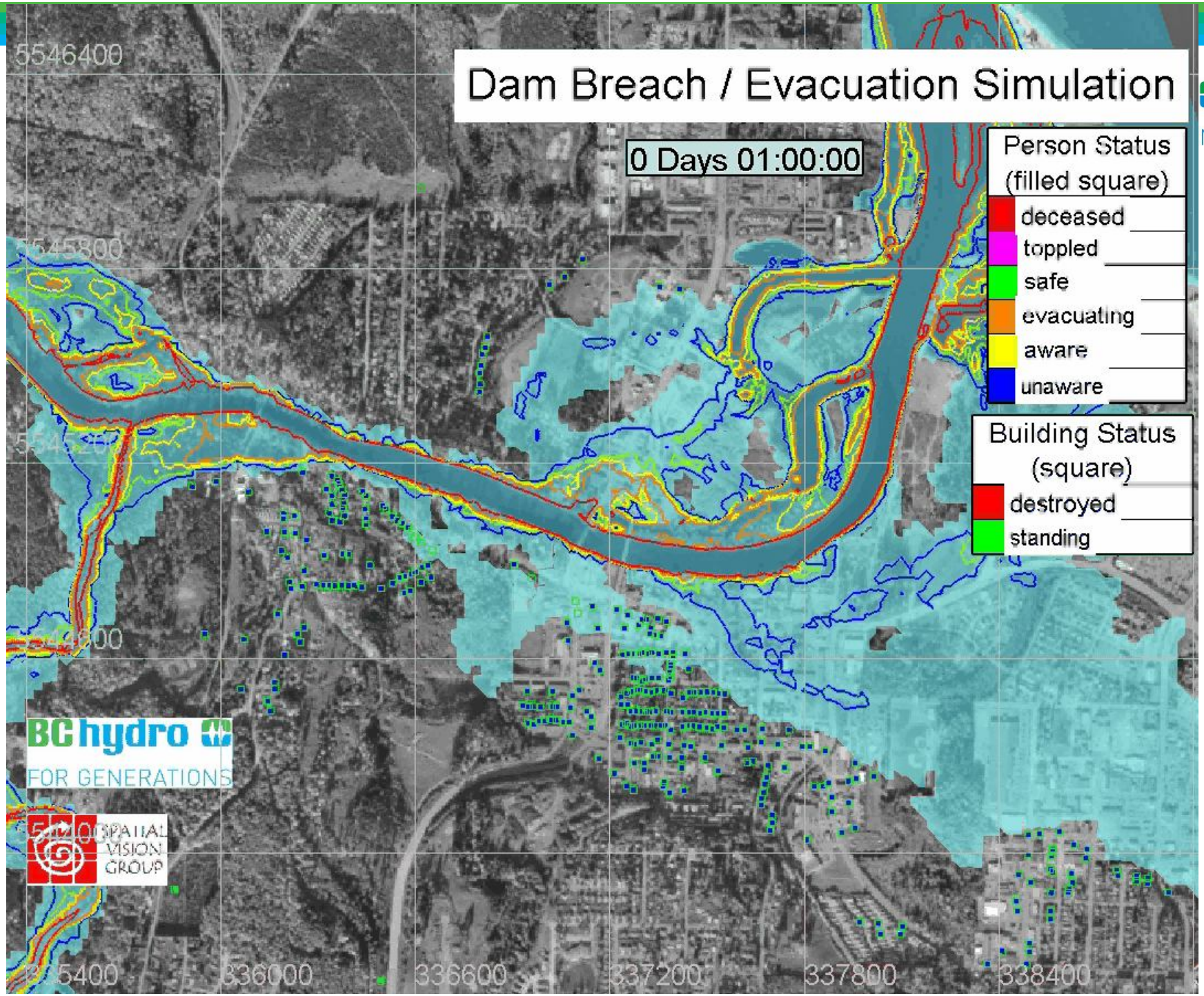
7-tier hierarchy

Meet or exceed all:

1. General Legal Duties
2. General Duties of Dam Ownership
3. Legal Duties associated with Dam Operation and Safety
4. Regulatory requirements with respect to Dam Operation and Safety
5. Conform to established engineering principles for safety of engineered systems
6. Established dam safety standards/criteria and norms
   - And if the safety issue remains unresolved:
7. Perform quantitative risk assessment
   - With specific consideration of Totality of the Consequences of Failure
     - It is not simply a matter of lives lost and damage costs
       - And Cost to Save a Statistical Life
     - What happens when a “statistical life” becomes a real person

Risk decisions must be explained!




Dam Breach / Evacuation Simulation
0 Days 01:00:00
Person Status
(filled square)
deceased
toppled
safe
evacuating
aware
unaware
Building Status
(square)
destroyed
standing
5546400
5545800
5545200
5544600
336000
336600
337200
337800
338400
BC hydro
FOR GENERATIONS
SPATIAL VISION GROUP