The Fukushima Dai-ichi Accident
Some Themes

Peter Bernard Ladkin

University of Bielefeld and Causalis Limited

3 August 2011

Problems

- We have had a major engineering accident with severe consequences
- It is difficult to assess the consequences
- The accident was triggered by a common-cause failure
  - Common cause is natural: major earthquake
  - nevertheless, it is unclear how tsunamis were considered
- Difficult to assess the (engineering) events leading up to the trigger
- The engineering hazard is not unique to earthquake+tsunami
  - Most US power plants are well inland
  - The engineering risk is that of "*station blackout*" due to flooding
- We are here to try to solve a series of ....
  - social
  - engineering
  - political
- ... problems. Or at least to start.

Functional Safety Commonplaces

- Perform a Preliminary Hazard Analysis
  - Identify those phenomena which lead to damage/loss, in some causal sense of "lead"
- Perform a Risk Analysis
  - Classify the severity of each hazard/hazardous event
  - Assess the likelihood of each
- Compare with social "norms"/acceptability
- Derive likelihood constraints from analysis+acceptability
- Iterate
- (Relatively) New: write all this down in a "Safety Case"

A Specific Hazard

- Spent Fuel Pools contain thousands of tons of water
- They are on the 4th floor of the Secondary Containment (Reactor Building)
- Secondary power generation, sometimes electrical/electronic control elements, is in the basement of ....
- There are natural water hazards such as flash floods (from thunderstorms) and tsunamis
- Hazard: flooding make take out secondary power when needed (primary power out: common-cause failure)
  - Common-cause failures not necessarily well analysed in system safety
- ... yielding the hazard known as "*station blackout*"

Station Blackout

- Hazard described by, e.g., Dave Lochbaum of UCS in 1992
- Contained explicity in his book in 1996
- There are instances of it happening!
- In Charles Perrow's "*The Next Catastrophe*" (2007)
- (See *Fukushima Diary* pp 79-80)
- Where is it analysed in US documentation?
- Where is it in a Japanese documentation?
  - Washington Post: TEPCO assessed tsunami risk in a "*single, double-sized page*" in December 2001 (*Fukushima Diary p 100)*
- Thomas Netter: "*since submarines exist they'd be able to design generators to survive [flooding]*" (*Fukushima Diary p 41)*

Documentation and Evaluation

- Tracing back ...
  - what was considered in the way of hazards
  - what was known
  - when
  - by whom
  - what happened as a result
- ... seems to be a matter for scholars, not for engineers, politicians or jurists
- couldn't we ensure it's all in one place for the future?

Proposal

- That, for every safety-critical engineering entity, there be a publically-available **Safety Case**
  - cf. the plethora of documents, court applications, NRC replies, etc., concerning Diablo Canyon (*Fukushima Diary p 4)*
- Proposed in *abnormaldistribution* blog, *Fukushima, the Tsunami Hazard, and Engineering Practice*, 27 March 2011.
  - *http://www.abnormaldistribution.org/2011/03/27/fukushima-the-tsunami-hazard-and-engineering-practice/*
- Thomas, Leveson: Resistance from industry
- Leveson: Full Safety Case not needed; HazAn suffices (SafeCrit Mailing List, 29 March 2011)
  - *http://www.cs.york.ac.uk/hise/safety-critical-archive/2011/0289.html*

HazAn versus RiskAn

- A Safety Case involves
  - not just enumerating hazards (HazAn) but
  - assessing the risks
- RiskAn involves assessing
  - hazard severity (or ?*criticality*?)
  - hazard likelihood
  - likelihood that the hazard will lead to an accident (as foreseen in severity assessment)
- Can we do that here?
- There are unusual difficulties in attempting it

Severity

- Assessing the consequences
  - of the *worst-case outcome* of the hazard
  - this is usual engineering practice (see e.g., Leveson Chapter 9)
- Worst-case outcome mitigated by perceived unlikelihood
  - We can't assess likelihood very well
  - That should - obviously - not prevent us from considering all possible outcomes
  - ....including the worst case
- Observe: **Fukushima was not worst-case!**
  - Worst-case might have been if Plant Manager Masao Yoshida had not ignored government instructions to stop cooling with seawater (*Fukushima Diary* p 112)
- We need to consider **Bad-Case Scenarios** as well!

Level of Damage

- Let's consider pure cash and ignore externalities
- Commercial air
  - 7 accidents per years
  - 200m - (rare) 1bn per accident
  - $\longrightarrow$ 1.5bn per year
- Oil
  - 1 major spill per 10 years
  - 10-20bn per major spill
  - $\longrightarrow$ 1-2bn per year
- Nuclear power
  - 100bn every 25 years (guessing from government decisions + commentary)
  - maybe 1tr or more (Ellims)
  - $\longrightarrow$ **4-40bn per year**!!
- Even this crudely: Nuclear is a lot worse

Other Damage

- Long-term contamination of land
  - unspecific health consequences for residents
  - unspecific effect upon foodstuff
  - unspecific consequences for consumers of that food
  - renders large areas of land unusable for the foreseeable future
- Long-term contamination of ocean
  - unspecific effect upon ocean life
  - unspecific effect upon foodstuff
  - unspecific region of contamination
  - renders ?what? ocean "unusable" for the foreseeable future?
- ? Replacement costs of generated energy?

Political Issues

- Is it really so bad?
  - Germany, Switzerland: yes
  - Japan: may very well be: yes
  - France, UK, US: no
- But UK, France, Germany, Switzerland are all next to each other
  - not to speak of Ukraine!
- Are there any political structures in place to organise decisions at the level of physical influence?
  - No
  - Not the EU (look at common "defence policy", even NATO)
  - No near prospect of Russia and allied states joining in

Carrying On

- UK: we don't have tsunamis, we don't have strong earthquakes; we carry on
  - yes, but this is not merely about natural hazards
  - this is about whether engineering practices suffice
  - and whether the polity (politics; business practice; sociology of engineering organisations) suffices to implement good engineering practice
- Germany: we quit in 2022
  - but what about the waste?
  - you can't stop engineering waste disposal for 1,000's of years.....
- US: we carry on, but fix the things we are not good at
  - strong public-interest "watchdog" system (UCS)
  - cooperation between watchdog and regulator
  - but long-term waste disposal remains unsolved for 40 years!

Cooperation - Limited?

- US help declined for a week
  - aerial surveillance, drones
  - satellite surveillance - maybe militarily "classified"?
  - knowledge of handling meltdown event (PWR at TMI)
  - interpretation of data (e.g., over water level in SFP4, *Fukushima Diary*, p 9)
- Information politics
  - Public govt./TEPCO statements: "what we know"
  - No position taken on "possible outcomes"
  - Leads to ignificant difference in thinking and (re)acting! (PBL, *Fukushima Diary*, p18)

Limited Cooperation II

- Operating principle: "*Avoid panicky reaction*" (Seiji Shiroya, *Fukushima Diary* p 59)
  - Wolf Dombrosky, Professor for Catastrophe Management, Steinbeis-University, Berlin: "*I've not come across mass panic in 30 years of work on catastrophe*" (NW, 17 March 2011, translation PBL).
- Information asymmetry due to "*slight delay*" in transmission of information (Govt. spokesman Edano, *Fukushima Diary* p 10)
  - but information is (at least) two-way
  - US surveillance, interpretation, experience (TMI)
  - French nuclear emergency management

Political Attitudes

- NISA (until 12 April 2011): INES Level 4 accident (*Fukushima Diary* pp 8,56)
- French nuclear safety authority, 16 March 2011: INES Level 6 (*Fukushima Diary* p 8)
- IAEA clarification: only country of origin is able to classify
  - This is a mixed political/engineering statement
- EU Environment Minister Oettinger: "*further catastrophic events*" expected; operators "*do not have control*" (*Fukushima Diary* p 9)
- French Environment Minister Koscuisko-Morizet: "*worst-case scenario possible, even probable*" (*Fukushima Diary* p 9)
- UK Chief Scientific Officer Beddington: "*beyond that 20 or 30 kilometers, it's really not an issue for health*" (*Fukushima Diary* p 9)
- Consider: who was right, who was wrong?

Politics of Help

- International political system is technically an anarchy of states (thanks to the Peace of Westfalia, 1648. Münster, Osnabrück)
- There are some somewhat-reliable international structures
  - EU
  - Dominant-neighbor politics
  - Engineering standardisation
  - .... also through limited sources of equipment (Siemens, GE, ...)
- But also exceptions
  - Iran
  - North Korea
  - Pakistani "rogue scientists"

Politics II

- Political structure does not follow environmental influence (e.g., prevailing winds)
- Can engineers ever have a say at this kind of level?
  - And, if so, why would we think they would be any better than professional politicians?
- What about engineers who are critical?
  - Not everyone follows the US NRC / UCS model

Let me move back to pure engineering

Engineering Concepts: Accident

- Definition of term *accident*
  - unwanted, unplanned event resulting in a specified level of loss (Leveson 1995, Ch. 9)
  - Event whose causal consequences include harm (Ladkin, Definitions for Safety Engineering, *http://www.causalis.com*)
- Works well for airplane accidents, rail accidents, auto accidents
- But consider Deepwater Horizon, Fukushima
  - Ongoing series of causally-related events ....
  - .... with different, often independent, intervention possibilities
    - ★ Deepwater Horizon: captain's decision to (not) abandon the rig was independent of the blow-out event itself
    - ★ Fukushima: Yoshida's decision to continue cooling with seawater was independent of meltdown/explosion events
- Conclusion: engineers need a workable definition of accident

Engineering Concepts: Severity and Loss

- *Loss* is
  - what the government pays?
  - what TEPCO pays?
  - what the insurance pays?
  - Externalities (already enumerated) possibly overwhelm these figures
- *Severity* is awaited specified loss
  - As discussed, hard to specify
  - But also, for hazard, a worst-case loss
  - We may need bad-case losses

Engineering Concepts: Hazard

- *Hazard* is
  - "*A phenomenon of a system, or its environment, or both, which substantially raises risk, although the likelihood of an accident still remains less than certain*" (Ladkin, op. cit.)
  - "*a state ... of a system.. that, together with other conditions in the environment... lead inevitably to an accident*" (Leveson, 1995, Ch. 9)
- The siting of the Fukushima plant was clearly a hazard by either definition
  - when the "*system*" is taken to include everything inside the plant
  - which it apparently was not by the builder/operator
- Conclusion: consensus on concepts is important, to ensure that nothing spills out through the semantic cracks!

Finis

- Concepts
- Conception/conceptualisation
- Engineering and politics
- Information politics
- Help, assistance, recovery and political/administrative boundaries
- Engineering standardisation/cross-knowledge
- The Nature of the Waste (*Fukushima Diary* p 20)
- ... just some themes

Thanks for listening!