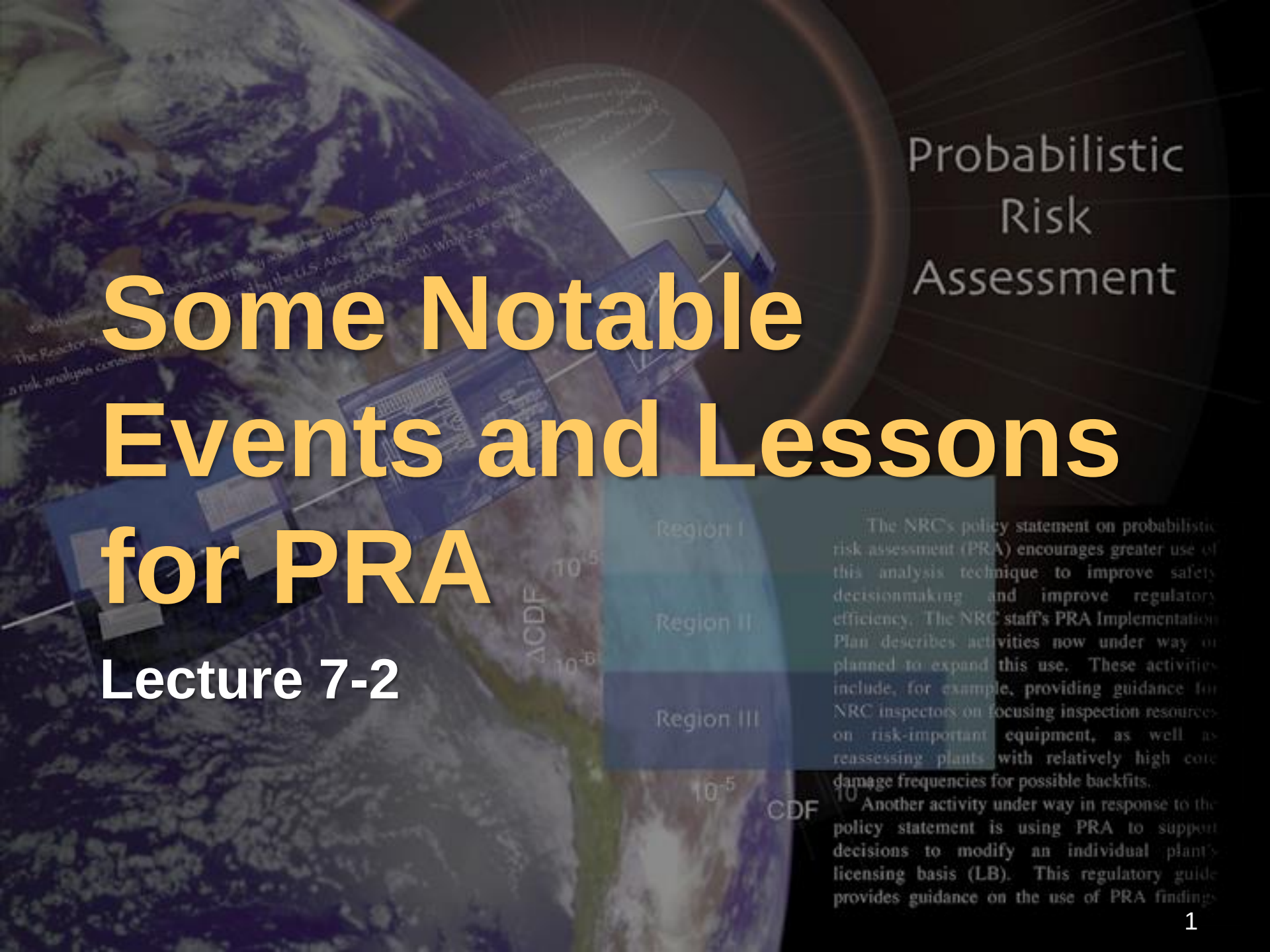


Some Notable Events and Lessons for PRA

Lecture 7-2

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Key Topics

- PRA and RIDM motivation for retrospective analysis
- Lessons from three events
  - Blayais (12/27/1999)
  - Fukushima Dai-ichi (3/11/2011)
  - Narora (3/31/1993)

Resources

- N. Siu, et al., "Qualitative PRA insights from operational events," *Proceedings of 14th International Conference on Probabilistic Safety Assessment and Management (PSAM 14)*, Los Angeles, CA, September 16-21, 2018.
- Institut de Protection et de Sûreté Nucléaire, *Rapport Sur L'Inondation Du Site Du Blayais*, Fontenay-aux-Roses, France, January 2000. (Available from: http://www.irsn.fr/FR/expertise/rapports_expertise/Documents/surete/rapport_sur_l_inondation_du_site_du_blayais.pdf)
- N. Siu, et al., "PSA technology reminders and challenges revealed by the Great East Japan Earthquake: 2016 update," *Proceedings of 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13)*, Seoul, Korea, October 2-7, 2016.
- S.P. Nowlen, M. Kazarians, and F. Wyant, "Risk Methods Insights Gained From Fire Incidents," *NUREG/CR-6738*, 2001.

Other References

- A. Gorbatchev, et al., "Report on flooding of Le Blayais power plant on 27 December 1999," *Proceedings of EUROSAFE 2000*, Cologne, Germany, November 6-7, 2000, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) Gmbh, Cologne, Germany, 2000.
- E. Vial, V. Rebour, and B. Perrin, "Severe storm resulting in partial plant flooding in 'Le Blayais' nuclear power plant," *Proceedings of International Workshop on External Flooding Hazards at Nuclear Power Plant Sites*, Atomic Energy Regulatory Board of India, Nuclear Power Corporation of India, Ltd., and International Atomic Energy Agency, Kalpakkam, Tamil Nadu, India, August 29 – September 2, 2005.
- N. Siu, et al., "PSA technology challenges revealed by the Great East Japan Earthquake," *Proceedings of PSAM Topical Conference in Light of the Fukushima Dai-Ichi Accident*, Tokyo, Japan, April 15-17, 2013.

Other References (cont.)

There is an enormous volume of publicly available information on the Fukushima Dai-ichi reactor accidents and other reactor incidents resulting from the 2011 Great East Japan Earthquake and Tsunami. Useful reports include:

- National Research Council, *Lessons Learned from the Fukushima Accident for Improving Safety of U.S. Nuclear Plants*, National Academies Press, Washington, DC, 2014.
- International Atomic Energy Agency, "The Fukushima Daiichi Accident: Report by the IAEA Director General," *STI/PUB 1710*, Vienna, Austria, 2015.
- Government of Japan, "Investigation Committee on the Accident at the Fukushima Nuclear Power Stations of Tokyo Electric Power Company, Final Report," Tokyo, Japan, 2012.
- Tokyo Electric Power Company, Inc., "Fukushima Nuclear Accident Analysis Report," Tokyo, Japan, 2012.
- The National Diet of Japan, "The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission," Tokyo, Japan, 2012.
- Institute of Nuclear Power Operations, "Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station," *INPO 11-005*, Atlanta, GA, 2011.
- I. Kato, "Safe Shutdown of the Onagawa Nuclear Power Station—the Closest Boiling Water Reactors to the 3/11/11 Epicenter ," Proceedings Symposium on the Future of Nuclear Power, University of Pittsburgh, March 27-28, 2012. Available from https://www.thornburghforum.pitt.edu/sites/default/files/Nuclear%20Symposium%20report%20FINAL%20report%2011_5_12.pdf

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Other References (cont.)

- Useful references on other major events:
  - U.S. Department of Energy, Electric Power Research Institute, Environmental Protection Agency, Federal Emergency Management Agency, Institute of Nuclear Power Operations, and the U.S. Nuclear Regulatory Commission, "Report on the Accident at the Chernobyl Nuclear Power Station," *NUREG-1250*, January 1987.
  - U.S. Nuclear Regulatory Commission, "Three Mile Island Accident of 1979: Knowledge Management Digest," *NUREG/KM-0001*, December 2012.
  - U.S. Nuclear Regulatory Commission, "The Browns Ferry Nuclear Plant Fire of 1975 Knowledge Management Digest," *NUREG/KM-0002, Rev. 1*, February 2014.

Qualitative Retrospective Analysis

- Provides empirical lessons for
  - Risk management (e.g., potential improvements in emergency response as well as plant design and operations)
  - Risk assessment (e.g., potentially important failure mechanisms and dependencies)
- No one "best way" to perform analysis, but PRA modeling structure provides a useful perspective

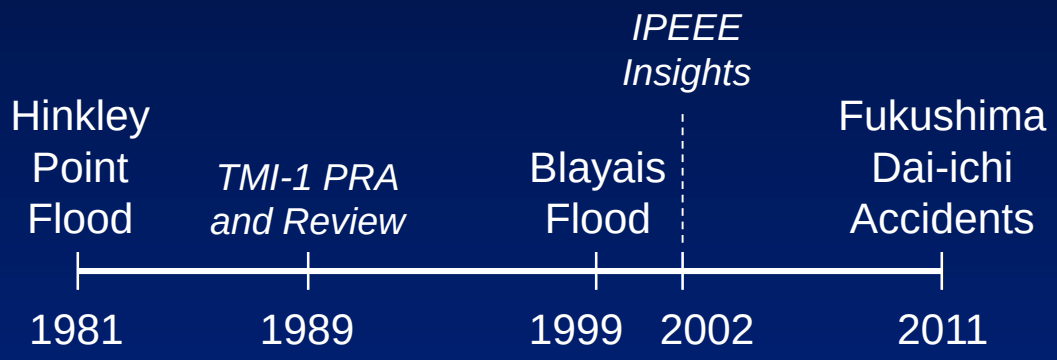
Don't forget: "risk" includes qualitative information

$$\textbf{Risk} \equiv \{s_i, C_i, p_i\}$$

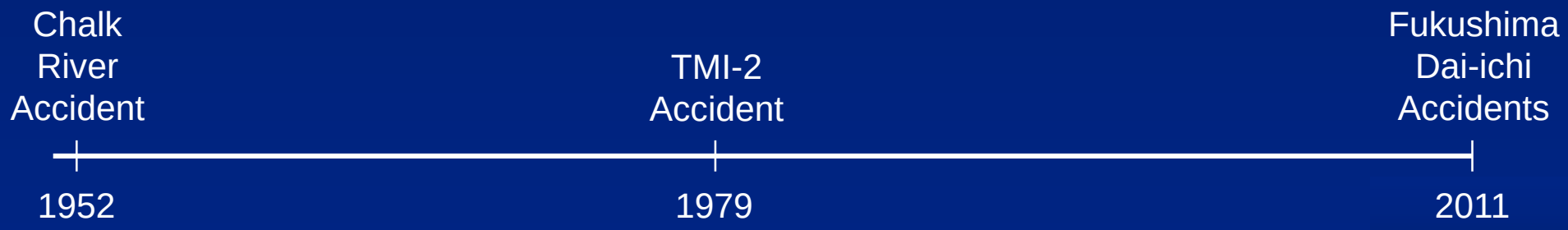
Examples of Past Lessons

Importance of:

- External flooding
- Combined hazards



Large volumes of waste water



Caution – Beware of 20-20 Hindsight

- A.k.a.
  - MMQB (Monday Morning Quarterbacking)
  - "I knew it all along" syndrome
- Available information generally uncertain, limitations can be persistent
  - Simplifications
  - Inconsistencies
  - Factual errors
- Post-event judgments subject to normal human biases
  - Confirmation bias
  - Underestimation/undervaluation of uncertainty
- Often used to assess blame rather than identify lessons for moving forward

NPP PRAs identify millions of possibilities, virtually all of which will not happen. The occurrence or non-occurrence of a scenario does not prove that the PRA is "right" or "wrong."

Example: On "Lack of Imagination"

Early quote captures concern, but is it fair? Helpful?

"…the thought of a tsunami never crossed my mind."

- Tsuneo Futami (<March 26, 2011: D+15)
http://www.nytimes.com/2011/03/27/world/asia/27nuke.html?hp&_r=0

"I could not imagine such a huge tsunami as occurred on 11 March."

- Tsuneo Futami (May 17, 2011: M+2)
http://spectrum.ieee.org/tech-talk/energy/nuclear/the-scale-of-the-accident-was-beyond-my-imagination/?utm_source=techalert&utm_medium=email&utm_campaign=051911

Le Blayais (December 27, 1999)

- Two exceptionally strong winter storms ("Lothar" and "Martin") sweep over Western Europe in rapid succession. "Martin" causes a grid disturbance and LOOP at Units 2 and 4.
- Wind-driven waves + major storm surge
  - Overtop and sweep around dike, damage dike
  - Flood site

E. de Fraguier, "*Lessons learned from 1999 Blayais flood: overview of EDF flood risk management plan*," *NRC Regulatory Information Conference*, Rockville, MD, March 9-11, 2010.

- Flood waters pass through penetrations, burst an internal fire door, and flood key areas within the plant.
  - Immerse Unit 1 and 2 low head safety injection and containment spray pumps (but not motors); plant staff declare these inoperable.
  - Immerse the motors of Unit 1 Train A emergency service water pumps.
  - Unit 1 tripped due to problems caused by debris clogging of circulation water filters.
  - Some flooding of auxiliary feedwater and emergency diesel generator rooms but not severe enough to damage.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Confirm following are publicly available

Le Blayais (cont.)

- Offsite flooding and storm damage (downed trees, debris) delay arrival of offsite support personnel (needed to implement emergency action plan).
- Plant adopts shutdown strategy that accounts for grid instability, potential for additional failures.
- Event is serious enough to warrant activation of national crisis teams (utility and regulator).
- Post-event activities include flood hazard re-examinations for all French plants.

Le Blayais – PRA-Oriented Observations*

Category	Sub-Category	Summary	Comments
Hazard	Conditions	Exceptionally strong storm (985 hPa; 180-200 km/h); high tide, storm surge, wind-driven waves at site.	Pre-event conditions from prior storm (regional or organizational) unclear.
	Protection	Dikes (5.7 m) insufficient height and inadequate shape, upgrade suggested by a 1998 EDF study given low priority. (Work scheduled for 2002.) Also problems with detection and warning systems.	
	Onsite Impact	Flooding washed over and around dike (and damaged dike) around 1930 12/27, entered service trenches, underground galleries and then nuclear island through non-leaktight penetrations and door(s). Flooding of rooms with electrical and electronic components, Fuel Building (FB) basement (with low-head safety injection – LHSI – and containment spray system – CSS – pumps), and Emergency Service Water (ESW) pumping station.	

*Based on document review

Le Blayais Observations (cont.)

Category	Sub-Category	Summary	Comments
Fragility	Safe Shutdown SSCs Exposed	See below for failed SSCs. Reports general lack explicit description of SSCs that were exposed but didn't fail.	LHSI and CSS pumps declared inoperable.
	Safe Shutdown SSCs Affected	Loss of 225kV for all units, 400kV for U2/U4, trip of U2/U4. U1/U3 connected to intact portion of grid. (U1 had minor problems due to grid fluctuations.) U2/U4 power restored. U1 tripped. U1 Train A ESW motors, U1/U2 LHSI and CSS failed.	Some uncertainties in the timing of events across the various sources.
	Barrier SSCs affected	Dike embankments moved by flood, lowering dike level; storm damage to administration building. Fire door failed due to differential pressure.	Dike damage only mentioned by early IPSN reports.

Le Blayais Observations (cont.)

Category	Sub-Category	Summary	Comments
Response	Functions Lost	Loss of U1-U4 225kV and U2/U4 400kV offsite power, U1/U2 LHSI and CSS; partial loss U1 ESW.	EDGs started and loaded as designed. ESW degradation probably less significant than at some other plants due to use of air-cooled EDGs.
	Safe Shutdown Path	U2/U4 tripped on LOOP, U1 tripped later. SGs fed by AFW (2 MDP, 1 TDP; 1/3 needed, "no sign of failure during operation"). Maintained in RHR cooling until stabilization of grid and onsite power. U3 in cold shutdown following refueling outage; U4 reconnected to grid 12/30 after restoration of 225kV. Approach considered likelihood of SRV LOCA and Y2K issues.	Some uncertainties in the timing of events across the various sources.
	Recovery	Receding floodwaters allowed access to site at 0250 12/28. Floodwaters pumped out by 12/29 using offsite fire pumps. Pumped water released into Gironde after checking for activity. U1 Train A ESW restored, one LHSI pump and one CSS pump refurbished (but not completely requalified) 1/4/00. Concern with corrosion from chlorine.	

Le Blayais Observations (cont.)

Category	Sub-Category	Summary	Comments
Response (cont.)	Operator Actions	U4 operators did not treat high water level alarm - considered covered by ongoing LOOP procedure; alarm not relayed to other units, would have led to earlier U1 shutdown.	
	Other Incident Management	Regional directorate notified at 2240; IPSN on-duty engineer (on-duty b/c of "power supply problems") notified at 2400; receding water allowed additional personnel onsite at 0250 12/28, EDF national crisis team mobilized at 0315; DSIN officially notified at 0330; IPSN management notified at 0630; IPSN technical crisis center manned 0745, couldn't rely on PSA model and had to use judgment; Level 2 emergency plan (PUI) activated at request of DSIN at 0900 b/c of reduced safety margin at U1/U2; relief team at 2100.	Mobilization of national crisis teams indicates the perceived seriousness of the event at the time.). External technical experts at IPSN, including experts in PSA, had a major role in determining an appropriate safe shutdown strategy in light of known equipment losses.
	Offsite Impact	Site access lost for several hours (until 0200 12/28); downed trees, power lines, and localized flooding blocked roadways. Also problems with phone communications. Emergency plan Level 1 was postponed (concerns about site access and personnel safety) until 0250, after site access was regained.	Temporary loss of site access was a significant factor in the response.

Le Blayais Observations (cont.)

Category	Sub-Category	Summary	Comments
Long-Term	Post-Event Changes (Blayais)	Plant protective dike now 6.2 m, additional wave protection for wave heights up to 2.7 m, wave breakers in front of dike; inspection program for submerged cables and components that were cleaned; 50 cm portable flood barriers, diesel-driven site drainage pumps, leaktight penetrations and doors. New site flooding operating procedure addresses loss of site access, water quality and fuel supply, accessibility of equipment outside unprotected buildings, multi-unit impact, flood detection, electrical isolation, and management of water release.	
	Post-Event Changes (All French Plants)	All plants re-evaluated, considering additional phenomena, including realistic combinations. Require analysis of risks of offsite inaccessibility, loss of offsite power supplies, heat sink, communications. Changes implemented, costs around 110M euros.	U.S. plants were informed. External flooding within scope of IPEEE, but deterministic screening was allowed. Hazard re-evaluation required following Fukushima.

Blayais Lessons for NPP PRA

- Hazard
  - Multiple hazards
  - Large extent
  - Asymmetrical impact
  - Persistence
- Fragility
  - Declaration of inoperability
  - Willingness to use restored but unstable grid
- Response
  - Multiple shocks
  - Multiple units
  - HRA complexities
    - Onsite damage (ability to perform outside actions)
    - Uncertainty in effectiveness of actions
    - Offsite damage (staffing, external resources, psychological impact)

Fukushima Dai-ichi (March 11, 2011)

- The short version:

> "The March 11, 2011, Great East Japan Earthquake and tsunami sparked a humanitarian disaster in northeastern Japan and initiated a severe nuclear accident at the Fukushima Daiichi nuclear plant. Three of the six reactors at the plant sustained severe core damage and released hydrogen and radioactive materials."
>
> *- National Research Council (2014)*

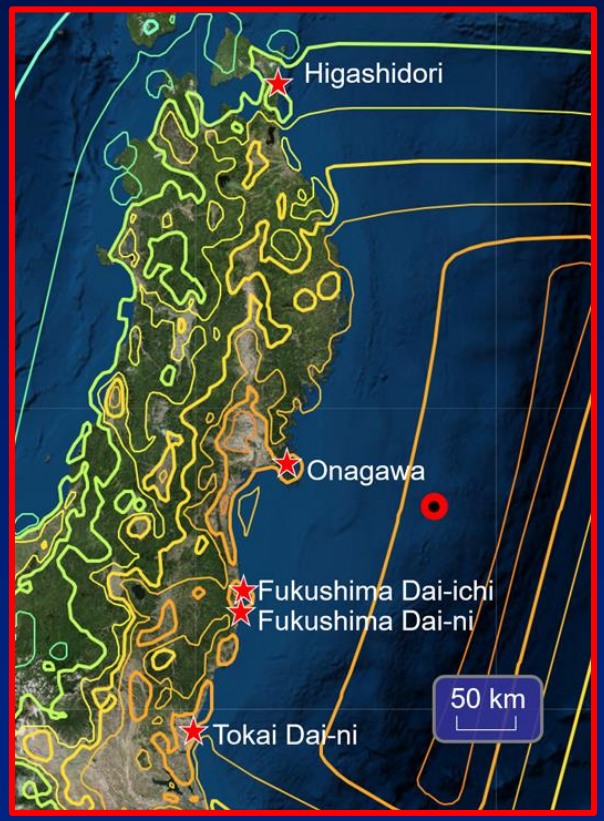
Fukushima Dai-ichi (cont.)

- A longer but only partial version:

Category	Summary
Hazard	• Peak ground acceleration (0.56 g) exceeded design basis. • Tsunami (13.1 m) exceeded latest accepted calculation (6.1 m) • Tsunami warning times: 4 min, 28 min, 45 min • Tsunami arrival times: 40 mi, 50 min • 180 aftershocks > M 5.0, 5 aftershocks > M 7.0
Fragility	• Complete loss of offsite power (collapsed towers, damaged substation) • Key electrical components (e.g., switchgear) on lower floor • Loss of access systems • Seismically isolated Emergency Response Center (ERC) above tsunami run-up • Offsite Center damaged by earthquake, never fully operational
Response	• Loss of power, indications, lighting, communications, physical access • Operators initially confident, “stunned” by progression of events. Worried about conditions offsite. High radiation; older workers selected for volunteer efforts. • Inadequate preparations (procedures, training, staffing); had to develop and implement ad hoc plans “on the fly” (scavenge car batteries for power, use fire engine trucks for pumping) • Extreme conditions (e.g., aftershocks, tsunami warnings, dark, hazardous onsite conditions, evacuations, inadequate supplies and facilities) • External distractions (requests for information, directions for action) • Intentional isolation of cooling systems (non-consequential at Unit 1, important at Unit 3) • Could have been worse (failure of Unit 6 EDG with Unit 5 at full power, lower ERC) or better (no LOOP) • Fundamental belief that event would not occur

The "Other" Plants

Plant	Effects
Fukushima Dai-ni	• PGA > design basis • Tsunami height = 9.1 m (above calculated 5.2 m) • Tsunami arrival time = 35 min • Partial LOOP (one offsite line survived), site flooding
Onagawa	• PGA > design basis • Tsunami height = 13.8 m (above calculated 9.1 m, below site level of 15 m*) • Tsunami arrival time = 45 min • Partial LOOP (one offsite line survived), limited internal flooding, HEAF
Tokai Dai-ni	• Tsunami height = 5.4 m (above calculated 4.88 m, below 7 m sea wall) • Tsunami arrival time = 30 min • LOOP, all EDGs operated
Higashidori	• LOOP, all EDGs operated



Adapted from
https://earthquake.usgs.gov/earthquakes/eventpage/official20110311054624120_30/shakemap/intensity

*Per Kato (2012), initial calculation (1970) was 3 m. Utility chose to set site grade level at 15 m.

Fukushima Lessons for PRA

- Many perspectives, many lists of topics with specific lessons
- More discussion: Lecture 9-1

- PRA scope
- Feedback loops
- "Game over modeling"
- Long duration scenarios
- External hazards analysis
- HRA
- Uncertainties in phenomenological codes
- Searching vs screening

- External Hazards
  - Ensuring defense in depth
  - Full hazard spectrum
  - Correlated hazards
- Human performance and HRA
  - Decision making
  - Ex-control room actions
  - Teamwork
- Level 2 PRA
  - Long duration scenarios
  - Equipment survivability, I&C
  - Environmental conditions and habitability
- Level 3

Some Notable Turbine Building Fires

Date	Plant	Notes
6/21/1971	Muhleberg	Oil leak ignites, minor explosion. Dense smoke fills turbine building. Extensive damage (non-safety cables), cleanup of HCl acid required.
12/31/1978	Beloyarsk 2	Burning lube oil spread into a cable shaft and the Control Building (and MCR) via open penetrations. Turbine Building roof collapsed. Secondary fire from oil-filled transformer. Fire fighting hampered by heavy smoke, bitter cold (-47ºC), multiple changes in command.
10/15/1982	Armenia	Power cable ignited at multiple points in two cable galleries (short circuit), propagated to adjacent room. Escaping hydrogen in Turbine Building exploded, started oil fire (~300m^2). Loss of all power and control for Unit 1, 3-hr SBO.
10/2/1987	Fort St. Vrain	Hydraulic oil spray onto hot surface, delay in cutting off oil supply (missing valve handle). Limited damage area. Smoke entered MCR.
10/19/1989	Vandellos 1	Turbine blade failure ruptures oil lines. Hydrogen fire. Cascading, burning oil affects lower floors, fails expansion joint and leads to flooding (as well as fire). Smoke enters control room, other parts of plant. Operators need breathing apparatus to enter dark, smoke-filled areas to perform recovery actions.
10/11/1991	Chernobyl 2	Large oil and hydrogen fire, collapse of Turbine Building roof. Main and emergency feedwater failed by debris or de-energized to allow fire fighting. Minor resuspension of contamination from Unit 4 accident.
3/31/1993	Narora 1	Turbine blade failure causes oil spill and fire. Fire propagates along cable trays into control room. Power lost to auxiliary shutdown panel. 17 hour SBO.

Narora (March 31, 1993)

- Unit 1 operating, Unit 2 cold shutdown
- Turbine blade failure, severe vibrations, ruptured oil lines, release of H_2 => explosion and fire
- Manual reactor trip, “crash” cooldown. All safety-related power sources lost => SBO
- Fire propagated into Control Equipment Room (lack of proper fire barrier penetration seals).
- Major part of fire extinguished in 1.5 hours.
- Diesel-driven fire pumps provide water to steam generators, both trip after 3.5 hours (non-fire CCF?)
- Smoke forces Main Control Room (MCR) abandonment. (Could not re-enter for 13 hours). No power to Unit 1 emergency control room => operators “flying blind” for 4.5 hours. Entered primary containment to read primary loop instrumentation directly.
- EDG started and loaded after 5.5 hours; shutdown cooling pump not energized until 17 hours (declared end of SBO).

Narora Fire Lessons for PRA

- Potential importance of large Turbine Building fires
- Multiple hazards (H_2, oil fire)
- Potential for MCR abandonment due to ex-MCR fires
- Potential for common cause failure of MCR and external emergency shutdown
- Successful actions potentially outside written procedures
  - Use of fire water as backup cooling
  - Entering containment to tap into instrumentation feeds or read form master gauges

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments

- More events => more PRA and RIDM lessons
- Also useful for knowledge base and text mining tool development

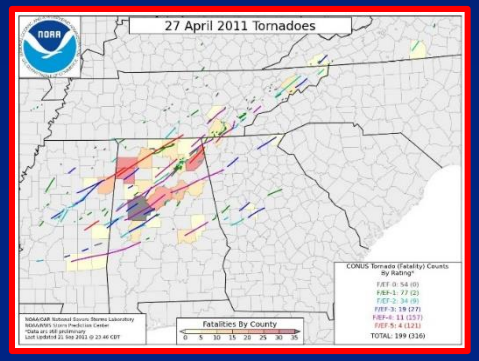
Useful project

Confirmatory:

Multiple hazards
Asymmetrical multi-unit impacts
Less-than-extreme hazards
Hazard persistence
Failure of mitigation SSCs
Failure of implicitly considered SSCs
Warning times and precautionary measures
HRA and emergency response complexities

Less Discussed:

Multiple shocks
Scenario dynamics
Geographical extent and potential for multi-site impacts



.L. Hayes, *Service Assessment: The Historic Tornadoes of April 2011*, U.S. National Weather Service, 2011. (Available from: https://www.weather.gov/media/publications/assessments/historic_tornadoes.pdf)