Above and Beyond

Peter S. Winokur, Ph.D., Chairman
Defense Nuclear Facilities Safety Board

Thanks to D. Minnema, N. Slater-Chandler, J. Abrefah, F. Bamdad, J. Deplitch, M. Helfrich, and J. Kimball

DOE Nuclear Safety Workshop
September 19, 2012

What is "Beyond Design Basis"?

The design basis event simply represents the largest threat that the facility was designed to withstand; it should represent *what may happen,* not *what has happened*

- DOE has no criteria for identifying a design basis event
- Decided by agreement between designer, owner, and regulator

The beyond design basis event simply represents a threat beyond what the facility was designed to withstand

- Typically, it is the same event, only BIGGER
- Owners only need to consider if cost-effective measures could be incorporated into design or operations
- 10 CFR 830 calls out the need for analysis of accidents which may be *beyond the design basis* of the facility

What is the Difference?

The difference between design basis and beyond design basis events is not defined by the boundary between reality and fantasy

- During the last 10 years the world experienced:
  - 5 of the 26 largest recorded earthquakes
  - 8 of the 20 record-setting tornadoes
  - 5 of the 10 most intense Atlantic hurricanes
  - 3 of the 10 “deadliest heat waves”
  - 2 of the 10 “deadliest natural disasters”

  “Recorded history” is ~100-200 years; therefore, predictions of frequency and magnitude may have large inaccuracies
- DOE re-assesses natural phenomenon hazards every ten years; and things do change as the science improves
- The environment is always changing, even within the “short” lifetimes of people and facilities

Example: Wildland Fires

At LANL there have been 11 major wildland fires since 1954, including:

1954: Water Canyon Fire, 6000 acres

1977: La Mesa Fire, 15,000 acres

1996: Dome Fire, 16,516 acres

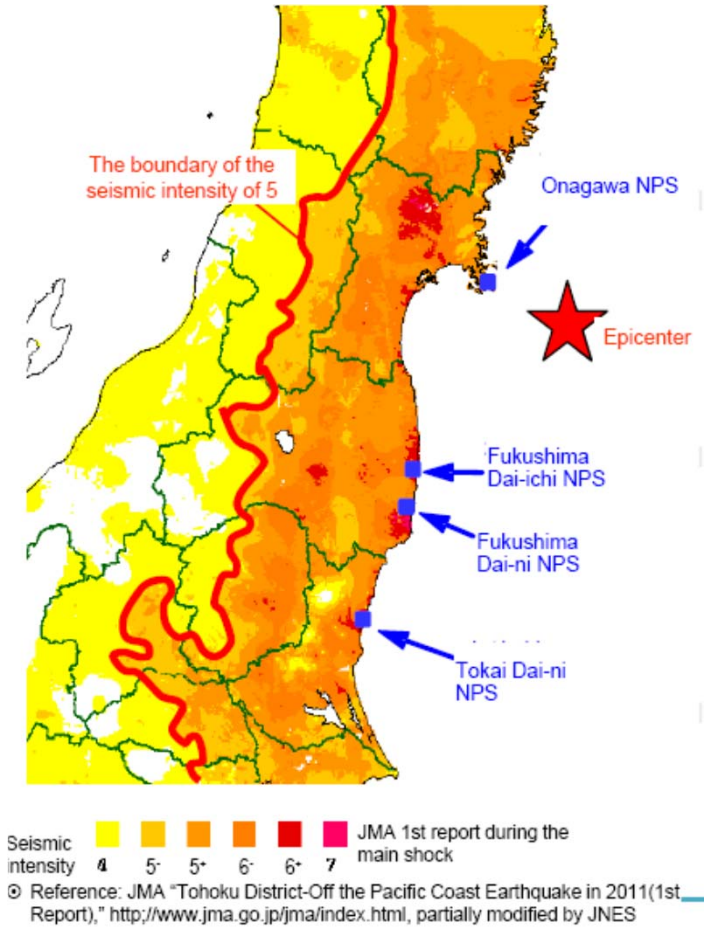
2000: Cerro Grande Fire, 45,000 acres

2011: Las Conchas Fire, 156,000 acres

There is always something bigger waiting to happen

What about Fukushima?

- There are three multiple-reactor sites near the epicenter
- This accident was within the design basis of the nearest site, Onagawa, and the plant survived
- It was not within the design basis for Fukushima Dai-ichi and Dai-ni
- Fukushima Dai-ni survived because of “quick action by an on-duty manager” (quote from Hisashi Ninokata)
- Fukushima Dai-ichi did not survive
- Why the differences?



100 Years Ago

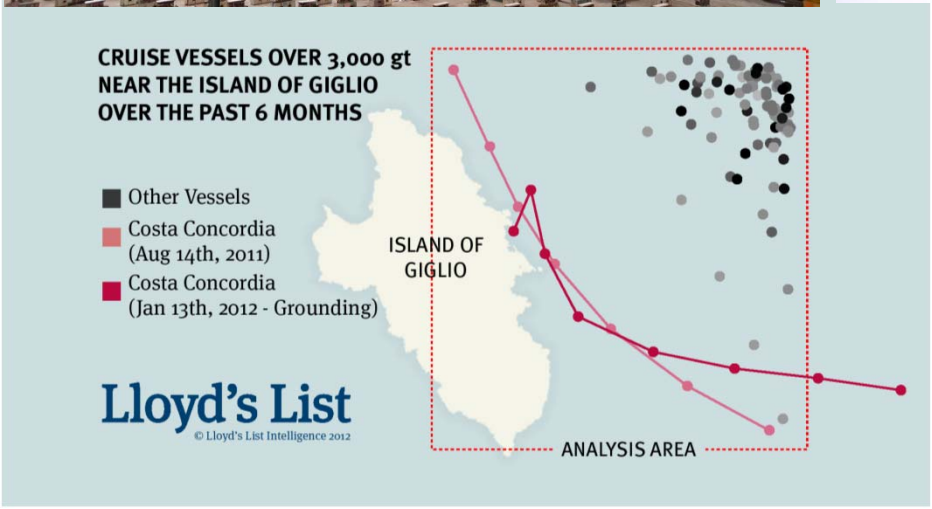
RMS *Titanic* sinks after striking iceberg in North Atlantic April 14, 1912

- Ship was transiting a high-risk area (known icebergs)
- Ship was single-hull design, but with watertight compartments
- Breaching of multiple compartments not expected
- Sinking of ship not anticipated; not enough lifeboats onboard
- Captain and crew ill-prepared to deal with emergency
- Significant and unnecessary loss of life – 1,514 dead

This Year

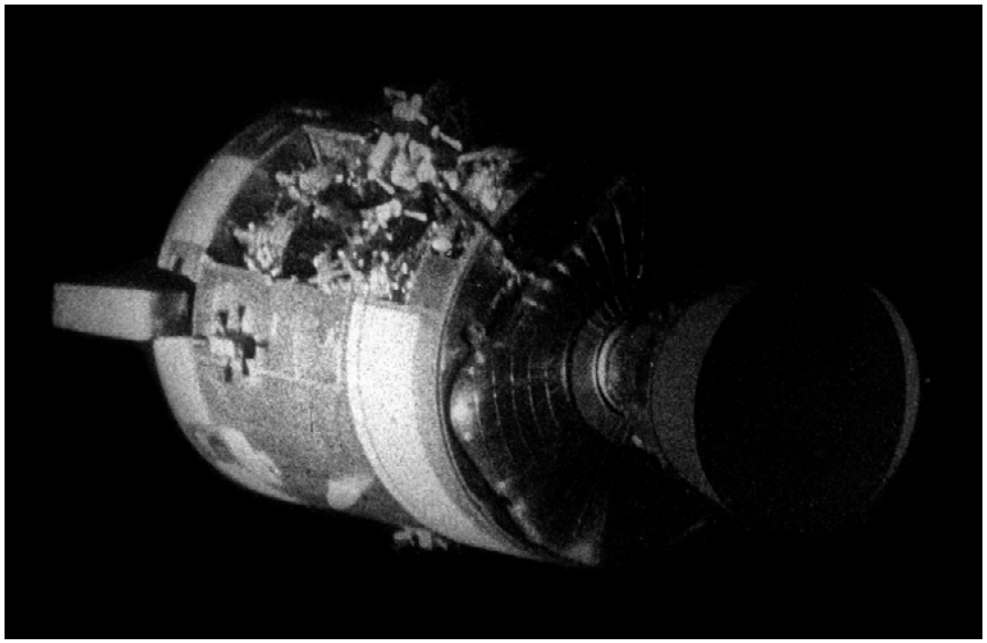
***MS Costa Concordia* sinks near Italy, January 15, 2012**

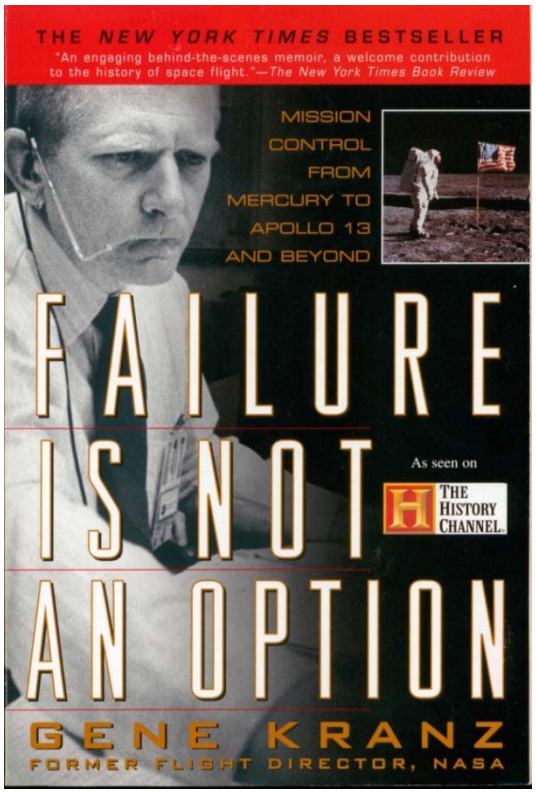
Why Did This Happen?



- Ship in high-risk area (known rocks)
- Ship was designed with double-bottom and watertight compartments
- Ship struck rock ledge above double-bottom, pierced multiple compartments
- Captain ill-prepared for emergency
- Unnecessary loss of life – 32 killed

Other Notable Accidents





- Apollo 13, inflight emergency en route to moon, April 13, 1970
- Explosion in Service Module vents oxygen tanks and damages fuel cells; command ship unable to support crew, lunar module used as “lifeboat”
- Mission control team develops improvised procedures to sustain crew for four days and conduct re-entry maneuver; all three astronauts survive

Other Notable Accidents

- UA Flight 232, DC-10, inflight emergency; July 19, 1989
- Catastrophic rear engine failure destroys all independent hydraulic systems
- All flight controls lost while flying at 37,000 feet; no recovery procedure existed
- Captain Al Haynes, flight instructor Dennis Fitch, and crew kept aircraft aloft for 44 minutes by cross-throttling two remaining engines
- Aircraft crashed during emergency landing at Sioux City, Iowa
- 184 of 295 passengers survived

Other Notable Accidents

- US Airways flight 1549, inflight emergency; January 15, 2009.
- Both engines fail due to multiple Canada Geese strikes (larger than design impact for Airbus A320 engines)
- Captain Chesley Sullenberger and crew ditch aircraft in the Hudson River
- Captain and crew well prepared for emergency; all onboard survive

What was the Difference?

The difference is Safety Leadership

Safety Culture is the artifact
of ***Safety Leadership***

"The only thing of real importance that leaders do is to create and manage culture…"

– Edgar Schein, MIT

Leaders Make the Difference

- These miraculous recoveries show us what a prepared leader and team can accomplish in an emergency
- All of the accidents highlighted in this talk would be classified as beyond design basis events
- There were no procedures or guides, and very little practical experience to rely on
- Survival came down to a fundamental understanding of the systems and a refusal to accept defeat
- The leaders made the difference
- We need to learn from these events to ensure that we have properly prepared leaders for tomorrow's accidents

Leadership at Fukishima Dai-ichi?

… measures taken at the Fukushima Dai-ichi NPS were inappropriate in comparison with the measures taken at the Fukushima Dai-ni NPS, regardless of different circumstances

… it cannot be denied that the ability to think about and confront the situation independently was poor [at Dai-ichi], and that there was a lack in flexible and proactive thinking, which is necessary in responding to a crisis

Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company

We have concluded that — given the deficiencies in training and preparation — once the total station blackout occurred … it was impossible to change the course of events

The TEPCO Fukushima Nuclear Power Plant accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties

The Fukushima Nuclear Accident Independent Investigation Commission

(all emphasis added)

Are There Broader Lessons?

- Do not assume that past accident experience defines the bounding accident scenario
- Violent events increase the potential for common mode failures
- Large accidents disrupt the surrounding area; consider what is happening around the plant also
- Expect loss of infrastructure during large-scale disasters; lines of communication and chains of command will be completely disrupted
- Expect very distracted workers; high error rates; conflicted priorities
- Anticipate the emergence of cascading events and impacts on multiple facilities that magnify consequences and complicate response efforts
- Anticipate a prolonged emergency time period without off-site support
- Recognize that local community resources will be overwhelmed and incapable of providing support as planned

Secretary's Safety Bulletin

- DOE recognized that lessons from Fukushima can be applicable to its operations
- The complex identified the need to take action to address gaps in existing requirements and guidance
- Some sites initiated severe event exercises
- Yet, 18 months later, no additional guidance and associated actions have been completed
- This workshop is an opportunity for leadership to reinvigorate the effort

HSS Safety Bulletin

Events Beyond Design Safety Basis Analysis

No. 2011-01

PURPOSE

This Safety Alert provides information on a safety concern related to the identification and mitigation of events that may fall outside those analyzed in the documented safety analysis.

BACKGROUND

On March 11, 2011, the Fukushima Daiichi nuclear power station in Japan was damaged by a magnitude 9.0 earthquake and the subsequent tsunami. While there is still a lot to be learned from the accident about the adequacy of design specifications and the equipment failure modes, reports from the Nuclear Regulatory Commission (NRC) have identified some key aspects of the operational emergency at the Fukushima Daiichi nuclear power station. Specifically, following automatic shutdown of the operating reactors due to the earthquake, a complete loss of both the offsite and on-site power systems disabled key cooling systems which eventually led to fuel damage, hydrogen generation, and high radiation levels within the facility.

AREAS FOR ATTENTION

The NRC has reported that the events at the Japanese nuclear power station appear to have been caused by factors directly impacting nuclear safety that were outside the design basis for the facility. Therefore, consistent with the approach being taken to review commercial nuclear power reactors, it is prudent to evaluate facility vulnerabilities to beyond design basis events at Department of Energy (DOE) nuclear facilities and to ensure appropriate provisions are in place to address them.

ACTION REQUIRED

For all Hazard Category 1 and 2 nuclear facilities (except for those only classified due to criticality criteria):

- Review how beyond design basis events have been considered or analyzed in accordance with DOE's Nuclear Safety Regulation and any controls that have been put in place that could prevent or mitigate them
- Discuss the ability to safely manage a total loss of power event including a loss of backup capabilities.
- Confirm safety systems are being maintained in an operable condition in accordance with technical safety requirements.
- Confirm emergency plans, procedures, and equipment are current, functional, and have been appropriately tested, including plans and procedures for response to natural phenomena events that could have site-wide impacts or impacts on regional support infrastructure.

Priority should be given to Hazard Category 1 facilities which should be completed by April 14, followed by Hazard Category 2 facilities by May 13, 2011. Provide results from these actions to the Program Secretarial Officer and the Chief Health, Safety and Security Officer.

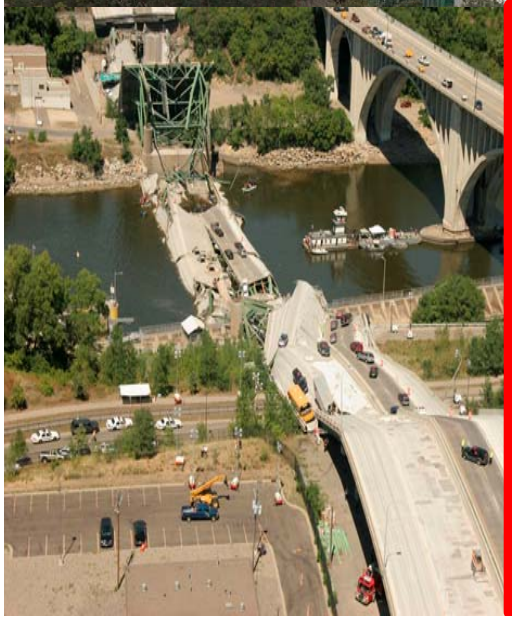
We will continue to monitor the situation, disseminate any lessons-learned derived from these actions, and provide additional guidance and recommendations as appropriate.

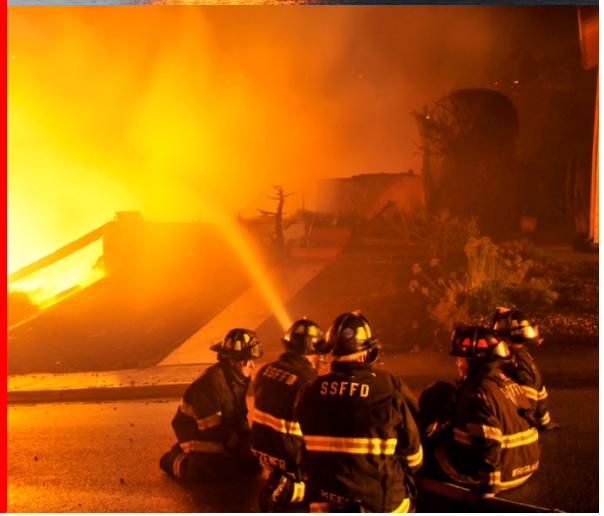
Information contact: Glenn S. Searfoss, Office of Corporate Safety Analysis (HS-30), telephone (301) 903-8085, glenn.searfoss@hq.doe.gov.

Steven Chu
Secretary of Energy

MAR 2 3 2011

Past 5 Years





Above and Beyond

- The Japanese experience illustrates again that “nuclear is different;” we must always act as if the whole world is watching
- Beyond design basis events are real and credible; the failure to believe leads to failure to survive when the event happens
- We cannot design systems to account for all possible accident scenarios; at some point it will come down to the human element
- We must ensure that leaders are ready and able to take action should systems and workers become overwhelmed
- We must hold ourselves to standards ABOVE AND BEYOND the least common denominator; build the defense-in-depth!

Success is a poor reason to decide we don’t need to continue success… So, I for one can stand success… And I suggest that giving up the elements of success is worse than thoughtlessness and worse than unintelligence. *“On Nuclear Weapons, the Triad & the Folly of Global Zero,” by Gen. Larry Welch*