



NASA SAFETY CENTER
SYSTEM FAILURE CASE STUDY



OCTOBER 2015 VOLUME 8 ISSUE 7

The Great Wave of Reform

The Prophetic Fallacy of the Fukushima Daiichi Meltdown

March 11, 2011, off the Pacific coast of Tohoku, Japan: At 14:46 (2:46 p.m.) Japan Standard Time (JST) a magnitude 9.0 earthquake occurred 43 miles east of the Oshika Peninsula. The undersea megathrust earthquake shifted the mainland of Japan an estimated 8 feet east and deviated Earth's axis by estimates between 4 to 10 inches. The Great East Japan Earthquake generated massive tsunami waves that peaked at heights of 133 feet and travelled up to 6 miles into areas of mainland Japan. According to the latest accessible Japanese National Police Agency police reports, the earthquake and tsunami are responsible for 15,891 dead, 6,152 injured and 2,584 missing persons. In addition to the horrific loss of life, 129,290 buildings have been reported collapsed, with another 1,020,777 structures sustaining varying degrees of damage. The disaster also triggered the second Level 7 International Nuclear Event (after Chernobyl) in history — the Fukushima Daiichi nuclear disaster.

PROXIMATE CAUSE

- Loss of electricity and backup power left the Fukushima complex crippled and unable to adequately cool the reactors

UNDERLYING ISSUES

- Disregard of Regulations
- Poor Safety History
- Lack of Response to Natural Disaster Concerns

AFTERMATH

- Recommendation pertaining to the creation of a permanent committee to deal with issues regarding nuclear power in order to supervise regulators and provide security to the public.

BACKGROUND

The Fukushima Daiichi Catastrophe

Analysis of the safety history of the Fukushima Daiichi nuclear power complex reveals a catastrophic failure of prediction on behalf of the plant's Tokyo Electric Power Company (TEPCO) management. How could planners overlook the tsunami?

Hazards of Predicting the Future

In 1958, Arthur C. Clarke, already recognized for major contributions to the fields of rocketry and space flight, began writing a series of magazine essays that were later combined and published

in 1962 as *Profiles of the Future*; a lexicon of universal scientific possibilities.

The book's introductory essay, "Hazards of Prophecy," concerned itself with the two traps of assumptions: "failures of nerve" and "failures of imagination."

Failure of the imagination manifests when presently known facts are respected but vital truths are still unknown, and the possibility of the unknown (the unknown unknowns) is not confessed. Failure of nerve, the more common fallacy (noted by Clarke), "occurs when given



Figure 1. Debris from the upper levels of Unit 4 lies beside the building. Source: IAEA

all the relevant facts the would-be prophet cannot see that they point to an inescapable conclusion.”

WHAT HAPPENED

The seismic activity of the Great East Japan Earthquake forced the emergency shut-down feature on reactors 1, 2 and 3. Off-site electricity to the power plant was also disrupted by the tremors and backup power was tapped from a 66kV transmission line from the Tohoku Electric Power Company Network. However, the back-up line failed to power reactor 1 due to a mismatched circuit connection.

Beginning at 15:37 (3:17 p.m.) JST, the peak tsunami waves broke upon Japan and flooded and destroyed the emergency diesel generators at the Fukushima complex. Seawater cooling pumps and electric wiring system for the DC power supply for reactors 1, 2 and 4 failed shortly after. All power was effectively lost except for emergency diesel generator power to reactor 6. The tsunami also destroyed vehicles, heavy equipment and many installations.

Without power, the operators at the complex worked tirelessly to monitor and cool the overheating reactors, at one point salvaging car batteries from destroyed vehicles to power necessary equipment. Hydrogen explosions from emptying coolant reservoirs led to interruptions in the recovery operations, which failed when the Unit 2 reactor suppression chamber failed and discharged radioactive material.

PROXIMATE CAUSE

The loss of electric power after flooding made it difficult to effectively cool down the reactors in a timely manner. Cooling operations and observing reactor temperatures were heavily dependent on electricity for coolant injection and depressurization of the reactor and reactor containers, and removal of decay heat at the final heat sink. Lack of access due to the disaster obstructed the delivery of necessities like alternative seawater injection via fire trucks.

UNDERLYING ISSUES

The Nuclear Accident Independent Investigation Commission (NAIIC), formed on Oct. 30, 2011 to investigate the direct and indirect causes of the Fukushima accident, was the first independent commission created in the history of Japan's constitutional government. In its legal investigation, the NAIIC concluded that “the disaster was man-made and the result of collusion between government, the regulators and TEPCO, and a lack of governance by said parties,” citing that the organizational and regulatory systems supported faulty rationales for decisions and actions. Regulators served TEPCO's business interests through tailored regulation and weak enforcement.

Disregard of Regulations

The 1967 construction plans for the Fukushima Daiichi isolation condenser deviated from the original reactor plans submitted to the government in 1966. The changes were not reported in violation of regulation. TEPCO's configuration control was scrutinized in February 2012 by Japan's Nuclear and Industrial Safety Agency (NISA). NISA requested explanation by March 12, 2012; however, TEPCO, unable to supply an official explanation, only speculated on why the change occurred.

In 2002, employees of General Electric (GE), the contractor responsible for designing the reactor, reported to the Japanese government that TEPCO injected air into the containment vessel of Fukushima reactor Number 1 to artificially lower the rate of a leak. The resulting scandal, in addition to a fuel leak at Fukushima Daini, forced TEPCO to temporarily shut down all 17 reactors. Falsified safety records and inspections in conjunction with the number 1 unit dating back to 1989 were revealed by other GE employees. Contractors admitted to falsifying reports at the request of TEPCO. The exposure led to numerous resignations of senior TEPCO executives and more disclosures of previously unreported issues, some of which imply that GE ignored warnings of major design failings from members of its contract staff (who later resigned in protest of negligence) in 1976.



Figure 2. Workers in protective clothing and masks outside the Emergency Response Centre, the main control hub at the Fukushima Daiichi site. Source: IAEA

Poor Safety History

On Dec. 29, 2011, TEPCO officials admitted to events occurring in 1991, where one of two backup generators for Number 1 failed after it was flooded with seawater leaking into the turbine building from a corroded seawater cooling pipe. Superiors were informed about the accident, and of the possibility that a tsunami could inflict similar damage to the generators in the turbine-buildings near the sea. In lieu of moving the generators to higher ground, TEPCO installed leak-proof doors in the generator rooms. After the event, the Japanese Nuclear Safety Commission stated its intent to enforce the installation of additional power supplies and that it would modify safety guidelines for future nuclear plant designs.

According to the NAIIC, regulators and TEPCO were aware of the risk that a total loss of electricity at Fukushima Daiichi would occur if flooding from a tsunami were to reach the level of the site since 2006, and that they were doubly aware of a risk of reactor core damage from loss of seawater pumps in the case of tsunami waves over 10 meters high. The NISA understood the TEPCO had not taken any protective or mitigating measures, but did not provide instructions to TEPCO to do so.

Lack of Response to Natural Disaster Concerns

A 2008 study performed by TEPCO's nuclear supervisory department concluded that there was an immediate need for improved seawater flooding protection. The study additionally mentioned the possible threat of tsunami waves over 10 meters tall. TEPCO headquarters officials dismissed the perceived risk as unrealistic; concluding that, even when presented with historical data, there was a failure to imagine that such conditions would recur.

Concerns from outside of Japan came from the International Atomic Energy Agency (IAEA) regarding the abilities of Japan's nuclear plants to withstand seismic activity; citing that an earthquake of a 7.0 or higher magnitude posed a serious threat at a 2008 G8 Nuclear Safety and Security Group assembly.



Figure 3. Storage tanks for contaminated water, a major challenge at the Fukushima Daiichi site. Source: IAEA

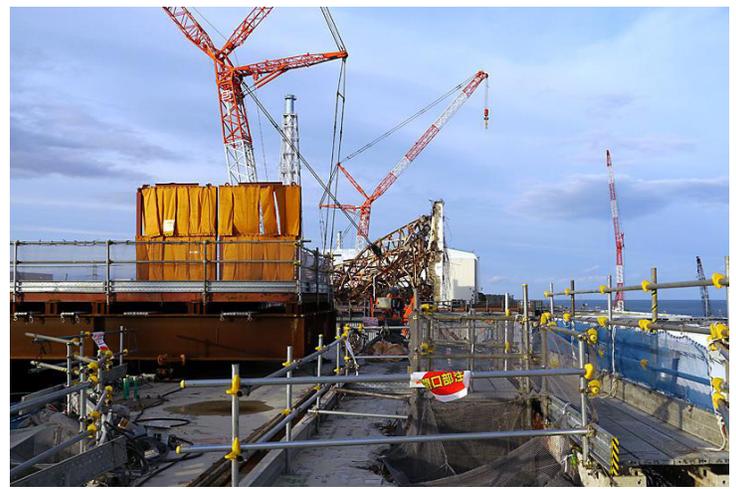


Figure 4. A view from the top of Unit 4, towards Units 3, 2 and 1. The twisted metal and rubble in the middle distance is the top of Unit 3, where cranes have to clear the debris remotely because of high radiation levels. Source: IAEA

On Oct. 2, 2011, the Japanese government released a report from TEPCO to NISA that proved TEPCO was aware of the possibility that the plant could be hit by a tsunami with waves far higher than the 5.7 meters which the plant was designed to withstand. The 2008 simulations based on the destruction caused by the 1896 earthquake in this area, revealed the likelihood of waves between 8.4 and 10.2 meters capable of flooding the site.

Further studies by scientists and an examination of the plant's tsunami resistance measures were not planned by TEPCO before April 2011, and no mitigation was planned before October 2012. TEPCO stated that the company did not feel the need to take prompt action on the estimates, which were still tentative calculations in the research stage. An official of NISA said that these results should have been made public by TEPCO, and that the firm should have taken measures right away; however, NISA believed these actions should have been taken on by the operator and not demanded by regulators. NAIIC viewed this a tacit consent on behalf of NISA to allow for a delay in TEPCO's planned work. After the tsunami, a TEPCO spokesman conceded that TEPCO would have been better prepared if it had taken the study seriously and reinforcement of its reactor houses.

In contrast, the Tokai Nuclear Power Plant protective dike was raised to 6.1 meters after simulations showed the possibility of higher than expected tsunami waves. Even unfinished at the time of the March 11, 2011, tsunami, the dike protected two seawater pumps and emergency diesel generators and allowed for the reactor to be kept in cold shutdown even though external power was lost.

AFTERMATH

The Nuclear Safety Commission Chairman told a parliamentary inquiry in February 2012 that, "Japan's atomic safety rules are inferior to global standards and left the country unprepared for the Fukushima nuclear disaster last March." There were flaws in, and lax enforcement of, the safety rules governing Japanese nuclear power companies, and this included insufficient protection against tsunamis.

The NAIIC made a recommendation pertaining to the creation of a permanent committee to deal with issues regarding nuclear power in order to supervise regulators and provide security to the public. The committee should be responsible for conducting regular investigations and explanatory hearings of regulatory agencies, academics and stakeholders and for establishing an advisory body to stay abreast of industry and government dealings.

The new regulatory body must be independent from the chain of command of the government, operators, and politics; transparent in decision making processes to the national government and exclude involvement of stakeholders in decision making; and technically proficient in nuclear technology.

The NAIIC also made recommendations pertaining to the reforming of nuclear energy laws to adhere to global standards, including the monitoring of operators and backfit of outdated reactors.

Many other organizations and think tanks have suggested possible corrective actions and future improvements after the disaster. Some of the actions relate to failure management such as having at least one diesel generator, fuel, and related switch gear isolated at high elevation or in a waterproof room (or both) to preserve onsite AC power in an emergency. Emergency response organizations could also maintain diesel generators or gas turbine generators that could be rapidly transported to a site to restore power. Regulators could demand more on-site personnel to have independent and timely sources of information and the ability to influence the owner/operator behavior during the accident. Current spent fuel pools could be retrofitted with passive cooling systems that can survive the initiating external event.

RELEVANCE TO NASA

Fukushima-Daiichi planners used of a narrow slice of historical environmental data when estimating the risk of external initiating event which contributed to a failure of imagination that a tsunami beyond the design basis of the Fukushima-Daiichi break wall could happen again. Beyond the multiple failures on behalf of TEPCO and Japanese nuclear regulatory agencies, the critical question remains of when to draw the line — when safe is safe enough — in the design basis process.

Teams with diverse viewpoints and broad, deep experience can overcome individual cognitive biases that can carve a path toward failure of imagination from the very beginning. Additionally, policy checks and balances on teams, such as NASA technical and safety requirements, are only as effective as the accountability behind them and depend upon how well both operators and regulators understand the technical basis behind such requirements.

Sometimes the rationale behind a requirement stems from the context surrounding a failure. If the rationale (the context) is lost to history, it can rob a team of the technical argument (and nerve) to defend safety margins. In regards to the nuclear power industry, emotionally fueled pressure from the public media outlets may drive governments to enact extensive regulatory changes, which may ultimately prove crippling to existing and future plants. A risk-

informed, unbiased comparison of nuclear energy with credible competitors, such as coal and natural gas energy — including their effects on climate change, global economy, stability and reliability, supply, and geo-politics — would be appropriate, but can the public and policy makers consciously take a risk-informed approach?

However, perhaps harder to overcome is the instance when a regulator itself places public safety below the business interests of a powerful industry. Safety hazards needing thorough mitigation can be perceived instead as business problems that demand efficiencies.

As this case study comes to press, the first Japanese nuclear plant restart took place after a nationwide 48-plant shutdown in 2011. Effects of an historic wave of reform may become visible.

REFERENCES

Acton, James M.; Mark Hibbs. *Why Fukushima Was Preventable*. The Carnegie Papers, Carnegie Endowment for International Peace. March 2012.

Buongiorno, J.; R. Ballinger; M. Driscoll; B. Forget; C. Forsberg; M. Golay; M. Kazimi; N. Todreas; J. Yanch. *Technical Lessons Learned from the Fukushima-Daiichi Accident and Possible Corrective Actions for the Nuclear Industry: An Initial Evaluation*. Center for Advanced Nuclear Energy Systems, Massachusetts Institute of Technology. July 26, 2011.

Caldwell, Cindy. *Reflections on Sensemaking at Fukushima Daiichi*. Highly Reliable Performance: Office of Corporate Safety Analysis, Department of Energy. September 10, 2012. <http://hshpi.wordpress.com/2012/09/10/reflections-on-sensemaking-at-fukushima-daiichi/>, accessed June 5, 2013.

Fukushima Daiichi: Two Years On: Photo Essay. IAEA. March 11, 2013. <https://www.iaea.org/newscenter/multimedia/photoessays/fukushima-daiichi-two-years>, accessed May 5, 2015.

Hultman, Nathan. *Fukushima and the Global "Nuclear Renaissance"*. Brookings Institute March. March 14, 2011. <http://www.brookings.edu/research/opinions/2011/03/14-japan-nuclear-hultman>, accessed July 1, 2013.

Kuroda, Hiroyuki. *Lessons Learned from the TEPCO Nuclear Power Scandal*. Tokyo Electric Power Company. March 27, 2004.

TEPCO, *Reports on the reflection of the changes in the connection method of the drain pipe in Isolation Condenser in Unit 1at Fukushima Daiichi Nuclear Power Station to the re-circulating system*, March 12, 2012.

SYSTEM FAILURE CASE STUDY



Responsible NASA Official: Steve Lilley

steve.k.lilley@nasa.gov

This is an internal NASA safety awareness training document based on information available in the public domain. The findings, proximate causes, and contributing factors identified in this case study do not necessarily represent those of the Agency. Sections of this case study were derived from multiple sources listed under References. Any misrepresentation or improper use of source material is unintentional.

Visit nsc.nasa.gov/SFCS to read this and other case studies online or to subscribe to the Monthly Safety e-Message.