Photo: Greg Webb/IAEA

Post-Fukushima safety enhancements to nuclear power plants

By James F. Gleason, Joe Hale, Claude Thibault, and Edward L. Quinn

Severe accidents—which assume core damage—need to be addressed in the safety standards for nuclear power plants.

The U.S. Nuclear Regulatory Commission has concluded that the accident at Fukushima Daiichi was caused by a long-lasting, complete loss of power due to common-cause failure of electrical equipment following the March 11, 2011, tsunami and to insufficient provision against severe accidents.[1]

At Fukushima, the defense-in-depth philosophy in existing worldwide safety standards for nuclear plants essentially stopped with the plant's design-basis accident. When the design basis was exceeded by the severe accident, there were no more defense-in-depth levels to deal with the beyond-design-basis conditions, and the plant operators had to improvise their response with the personnel on hand and the tools available to them.

Studies of the Fukushima accident, related near-miss accidents, and existing worldwide nuclear standards are reported herein, along with proposals for standards improvement.

James F. Gleason (<jim.gleason@glseq.com>) is President of GLSEQ LLC; Joe Hale (<joe.hale@us.schott.com>) is Director of Sales and Marketing in the North American Nuclear Safety Division of Schott AG; Claude Thibault (<claude.thibault@glseq.com>) is Senior Engineer and Nuclear Safety Consultant for GLSEQ LLC; and Edward L. Quinn (<tedquinn@cox.net>) is President of Technology Resources and an ANS Past President (1998–1999).

This article was adapted from a paper presented at the ANS Annual Meeting, held June 15–19, 2014, in Reno, Nev.

Common-cause failures

The American Nuclear Society, the American Society of Mechanical Engineers, the Institute of Electrical and Electronics Engineers, and the International Electrotechnical Commission (IEC) all have nuclear safety standards that attempt to prevent common-cause failure of electrical safety-related equipment, but none of them currently address a tsunami.

Several, however, such as IEEE 308,[2] state that the conditions of earthquake, winds, hurricane, tornado, rain, ice, snow, floods, lightning, and extreme temperature conditions are anticipated for Class 1E electrical equipment and that the electrical equipment should be qualified for these conditions. This standard provides no additional information on the events that cause flooding, and so it does not specifically address tsunamis, nor does it note that earthquakes can result in a tsunami.

The safety standards for equipment and seismic qualification, such as IEEE 323,[3] IEC 60780,[4] and ASME QME-1,[5] attempt to prevent common-cause failure if it is occurring because of normal and abnormal conditions and design-basis events. Not addressed in these standards are winds, hurricane, tornado, rain, ice, snow, floods, or lightning.

Severe accidents, near misses

Since 1979, in addition to the severe accident at Fukushima that included core melting at Units 1, 2, and 3, there have been two other severe accidents with core melting: Three Mile Island-2 and Chernobyl. The causes of these severe accidents were diverse.

The TMI-2 accident involved a small leak of water from the reactor system that wasn't correctly diagnosed until after the reactor's nuclear fuel core was severely damaged. Inadequate control room instrumentation and emergency response training proved to be root causes of the operators' inability to respond properly to an unplanned automatic shutdown of the reactor at 4 a.m. on March 28, 1979.

Twenty-eight years ago, in April 1986, an accident occurred at Unit 4 of the Chernobyl nuclear power plant in Ukraine, which at that time was part of the Soviet Union. The accident was caused by six different operator errors in a risky design. Two of the errors involved the use of "cutout switches" in safety shutdown circuits. Unlike nuclear reactors in the United States, Soviet plants had this feature, which was created in naval equipment before the use of nuclear power.

If a nuclear power plant loses all off-site and on-site A-C power, it is dependent on batteries only. The instances when nuclear power plants have been dependent on batteries only have been characterized as severe accident "near misses," of which there have been at least four:[6]

- On July 26, 1984, Susquehanna-2 was

operating at 30 percent power and Unit 1 was operating at 100 percent power when the licensee began preparations for a Unit 2 loss of turbine generator and off-site power startup test. Unit 2 experienced a loss of all A-C power.

- In 1983, Fort St. Vrain experienced a loss of off-site power and the loss of diesel generators during a snowstorm with high winds.
- In 1984, Grand Gulf experienced a loss of off-site power and the loss of diesel generators during tornadoes in the area.
- In 2006, Forsmark (in Sweden) experienced a loss of off-site power and the loss of diesel generators due to a human error in the switchyard.

And so, over a period of 30 years, there have been seven instances of nuclear power plants having lost all A-C power. Without A-C power, which is needed in many nuclear plant designs, severe accidents and beyond-design-basis events occur, and the problem is not limited to plants that have the possibility of experiencing tsunamis.

TMI-2 and Fukushima

The end result of the accidents at TMI-2 and Fukushima was core melt. Action items and lessons learned from TMI were supposed to prevent similar core melt accidents, but did not. Therefore, it is necessary to understand the differences between the accident at TMI and the accident at Fukushima.

The TMI accident environment conditions were mainly within the design basis environment levels. The Fukushima accident was a beyond-design-basis event that significantly exceeded the environmental conditions of the design-basis accident. The Fukushima accident temperature exceeded the design-basis event temperature by 80 percent and the design-basis pressure by 140 percent.[7]

The significance of exceeding the design-basis environmental conditions by such a large amount is not only the loss-of-coolant impact on nuclear fuel, but also the potential impact on containment. Some of the materials and equipment of the containment were not able to perform in these severe-accident environments.

For instance, the excessive environmental conditions exceeded the capability of electrical and mechanical penetrations and door and hatch seals and resulted in leakage paths for radiation and hydrogen. Hydrogen leakage outside of containment at Fukushima resulted in hydrogen explosions and loss of secondary containment.

Hydrogen a significant problem

Some beyond-design-basis events are known as severe accidents. A common definition of a severe accident is an accident that damages the nuclear fuel. The nuclear fuel cladding contains zirconium alloys, which can oxidize from water in the presence of excessive heat. The oxidation of zirconium is an exothermic reaction that generates heat and a large amount of hydrogen, which can be highly explosive, depending on the location, environment, and concentration. As the nuclear fuel continues to heat up, it can have an impact on other surrounding materials, including the reactor vessel. If the hot nuclear fuel breaches the reactor, hydrogen is also generated in the corium and concrete interaction.

Existing combustible gas regulations are inadequate for the following reasons:

1. They assume that explosions are not possible by limiting the amount of oxygen in containment. The triangle diagram of Shapiro-Moffette risk indicates regions of flammability and detonability of the hydrogen/air/steam mixtures.[8] Both detonations and ignition are possible under steam conditions.
2. The existing measurement of hydrogen is done by bulk sampling of gases from containment. The process of bulk sampling dilutes and mixes the hydrogen with other gases so that a true hydrogen concentration is not known. Also, and even more problematic, by definition, the true hydrogen concentration has to be higher than the hy-

Actions taken and planned by the U.S. Nuclear Regulatory Commission

Immediately following the accident at the Fukushima Daiichi nuclear facility, senior Nuclear Regulatory Commission managers and staff reviewed the events and the possible implications for the safety of U.S. nuclear power plants. This Near-Term Task Force (NTTF) issued its report, *Recommendations for Enhancing Reactor Safety in the 21st Century: The Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident,* in July 2011. The NRC subsequently prioritized the NTTF recommendations and other activities related to lessons learned from the Fukushima accident.

To address the most pressing matters, the NRC issued orders in March 2012 that required (1) plant-specific strategies to mitigate the effects of beyond-design-basis natural phenomena that address both multiunit events and reasonable protection of equipment identified to implement such strategies; (2) installation of enhanced spent fuel pool instrumentation; and (3) reliable, hardened containment vents for boiling water reactors with Mark I and Mark II containments. Also in March 2012, the NRC requested information on topics related to seismic and flooding events and on emergency preparedness for dealing with events with the potential to affect multiple reactors.

The NRC's activities generally align with international efforts, which are often described in terms of levels or layers of defense-in-depth. The International Atomic Energy Agency describes defense-in-depth in terms of the historical design basis for nuclear power plants (normal operation, anticipated operational occurrences, and design-basis accidents) and design extension conditions to address measures to (1) prevent core melt, and (2) address severe accidents.

To confirm that U.S. nuclear power plants were maintaining capabilities for dealing with design-basis seismic and flooding events, the NRC requested plant inspections—including the identification of any needed corrective actions—and written reports confirming each plant's compliance with existing requirements.

The orders issued in March 2012 established requirements for beyond-design-basis events and focused on adding mitigating capabilities to prevent core damage. The mitigating strategies address three phases of an accident challenging the core: (1 Phase 1, which relies on installed equipment (e.g., batteries and turbine-driven pumps), (2) Phase 2, which brings portable equipment into service, and (3) Phase 3, which includes assistance from off-site. The NRC has a number of activities under way or planned to evaluate possible enhancements to severe accident capabilities that would address plant conditions should an accident progress to core damage. The containment venting order was revised in June 2013 to require that licensees ensure that venting operations could be performed during severe accident conditions.

The NRC is also evaluating possible rule changes to integrate emergency response procedures, including severe accident management guidelines, and enhanced accident management and filtering strategies for reactor containments. Several longer-term research activities have also been initiated to assess potential concerns such as seismically induced fires and flooding. Regarding the defense-in-depth layer related to emergency preparedness, the NRC has addressed some issues within the order on mitigating strategies and is evaluating other potential enhancements.

The details of these activities and related documents can be found on the NRC website at <www.nrc.gov/reactors/operating/ops-experience/japan-info.html>.—*William Reckley, Special Advisor for Policy, Japan Lessons-Learned Division, Office of Nuclear Reactor Regulation, Nuclear Regulatory Commission* drogen concentration reported. In addition, bulk gas sampling does not provide any information on the location of excessive hydrogen concentrations.

Bulk gas sampling from containment is a complicated system consisting of many moving parts, such as solenoid valves, flow meters, pumps, motors, and gas analyzers. And so, new hydrogen sensors must sim-

The electrical penetrations must be capable of approximately two to three times the normal design pressure of containment to prevent leakage and to provide the necessary electrical integrity for power and instrumentation.

plify how hydrogen is detected; improve the responsiveness and reliability of hydrogen detection; convert hydrogen directly to an electrical signal; locate and measure hydrogen concentration; identify the risk of detonation; and be capable of operating in severe accidents.

Enhancing containment

Because the severe accident at Fukushima exceeded the design basis, and the temperature and pressure levels that were experienced challenged the electrical penetrations and door and hatch seals—and they were not up to the challenge—the severe accident capability of these items needs to be improved. Also, epoxy seals were reported to have been present in the electrical penetrations. Their design basis was exceeded and they leaked hydrogen gas.

The electrical penetrations must be capable of approximately two to three times the normal design pressure of containment to prevent leakage and to provide the necessary electrical integrity for power and instrumentation. The doors and hatches should also be capable of two to three times normal design pressure without leaking, and advanced electrical penetrations using glass-to-metal seals instead of epoxy seals will ensure the severe-accident capability of electrical penetrations. Door and hatch seals also need to be upgraded to ensure mechanical integrity during severe accidents.

The philosophy should be that the penetrations, doors, and hatches are not the weak link for containment integrity.

Enhancing mitigation capability

The worldwide nuclear industry reviews conducted after the severe accidents at the Fukushima units were aimed at minimizing severe accidents and at planning an efficient response in the event that a severe accident occurs. Defense-in-depth for all external hazards was a common outcome of the reviews, as was the prevention of pressurizing containment beyond its limits.

The final report on the peer review of European Union stress tests[9] notes that filtered containment venting is a well-known approach to prevent containment overpressure failure in most light-water reactors and has already been implemented in certain countries. Some other countries are now implementing the filtered venting system, while others are considering improving the existing ones—for example, the filtering efficiency or seismic qualification.

Results/lessons learned

Since severe accidents can happen at any nuclear power plant, they need to be addressed in the standards. Currently, new plants that are (and will be) licensed under 10 CFR Part 52 have some requirements for severe accidents.

Since the severe accident assumes core damage, equipment for mitigation and defense-in-depth should concentrate on maintaining the integrity of the containment. Some of the recommendations based on lessons learned are as follows:

- Hydrogen mitigation systems should be added, with hydrogen sensors that measure, locate, and mitigate hydrogen concentrations.
- Hydrogen mitigation systems should be coordinated with the hydrogen concentration and areas vulnerable to leakage to ensure their effectiveness.
- Sufficient electrical penetration assemblies capable of operating during severe accidents should replace existing or spare penetrations to ensure pressure and electrical integrity during severe accidents.
- Severe-accident mitigation features should be added based on individual plants' severe-accident environments and available mitigation strategies, with the goal of maintaining containment integrity.

In order to avert future catastrophes, the qualification standards and designs need to add the requirements of all the natural phenomenon hazards (winds, hurricane, tornado, rain, ice, snow, floods, and lightning) and evaluate safety equipment to determine whether these hazards apply. If they do, then it is necessary to ensure that the equipment is capable of withstanding each hazard in which it would be expected to operate.

References

1. G. Apostolakis, "A Proposed Risk Management Regulatory Framework," Nuclear Regulatory Commission, Washington, D.C. (2012).

2. IEEE-308–2012, *Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*.

3. IEEE-323–2003, *Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations* (reaffirmed in 2008).

4. IEC 60780, *Nuclear Power Plants—Electrical Equipment of the Safety System–Qualification* (1998).

5. ASME QME-1–2012, *Qualification of Active Mechanical Equipment Used in Nuclear Facilities.*

6. Jim Gleason and Pat Gleason, "Severe Accident Considerations," presented at the International Nuclear Safety Symposium, hosted by the Chinese Nuclear Energy Association, Beijing, China (2013).

Some other countries are now implementing the filtered venting system, while others are considering improving the existing ones—for example, the filtering efficiency or seismic qualification.

7. Presentation by Nuclear Regulation Authority Commissioner Toyoshi Fuketa at the U.S. NRC Regulatory Information Conference, Mar. 13, 2013.

8. NUREG/CR-2726, *Light Water Reactor Hydrogen Manual* (1983).

9. European Nuclear Safety Regulators Group (ENSREG) National Action Plans Workshop Summary Report (2013). NN