APPENDIX D

Frequently Asked Questions: Safety Issues and Recommendations

Q.1. What risk-significant design improvements can be made for core cooling [e.g., isolation condensers, reactor core isolation cooling (RCIC) system, emergency core cooling system (ECCS), etc.]?

A.1. By definition, station blackout (SBO) means the loss of all off-site and on-site alternating-current (AC) power. ECCSs that can respond when there is no AC power are isolation condensers, the RCIC system, and the high-pressure coolant injection (HPCI) system.

Isolation condensers are used in some BWR/3s (boiling water reactors). Once started by the opening of motor-operated valves, the system runs entirely on natural circulation, condenses the decay heat–generated steam, and returns the condensate to the reactor pressure vessel (RPV). The shell side of the isolation condenser heat exchangers must be replenished within ~8 hours in an extended SBO. Protection of direct-current (DC) power sources from severe external events, natural or man-made, such as fires, flooding, or explosions, will assure availability of isolation condensers without the need for operator intervention to manually open the valves in what might be a hazardous environment.

The RCIC system is used in BWR/4, BWR/5, and BWR/6 reactors, specifically to be able to provide water to the RPV when AC power is lost. As with isolation condensers, the RCIC system needs DC power to be able to operate properly, so protection of DC power will also assure availability of this system. However, unlike the isolation condensers, current RCIC systems cannot run indefinitely due to design constraints on the water temperature that can be pumped. New equipment (e.g., a steam turbine–driven pump design that can operate with water at higher temperature) is available for this duty and, if used together with limiting the containment temperature by early venting when there is no core damage, can provide significantly longer coping times before restoration of normal nuclear power plant (NPP) systems.

The HPCI system is used in BWR/3 and BWR/4 reactors. It was originally provided as a diverse ECCS for use in loss-of-coolant accidents, but it can also back up the RCIC system for SBO in NPPs that have both systems. Since its capacity is seven times that of the RCIC system, it consumes more DC power and has even more restrictive water temperature limits. Improving the protection of DC power sources would also benefit the use of the HPCI system.

Most pressurized water reactors (PWRs) have a steam-driven auxiliary feedwater system (AFS) that is similar to the RCIC system and keeps the steam generators filled with water so that the decay heat from the core can be removed. Some PWRs have motor- or diesel-driven pumps as well. The water source for the pumps is either an emergency feedwater tank or the condensate storage tank, which could provide water for up to 48 hours during a SBO (NPP dependent). In a SBO, atmospheric dump valves on the secondary loops can control secondary-loop pressure and release the decay heat to the environment. In a feed-and-bleed operation, when the AFS is not available, the safety injection tanks are used as a means of injecting cold borated water into the core for core cooling, while the reactor coolant system is bled by using pressurizer power-operated relief valves. Some DC

power is needed to provide the needed information and control for NPP operators, so protection of DC power sources will assure availability of these systems and valves.

Q.2. Should a mix of passive and active safety systems be required in new nuclear power plants to defeat station blackout (SBO)?

A.2. First of all, it needs to be defined what is meant by "passive." At the very least, some action, such as changing the state of one or more valves, is necessary to initiate a safety system operation. As defined by the Electric Power Research Institute, the term "passive" means no use of alternating-current (AC) power or rotating equipment (e.g., pumps). Using this definition, isolation condensers as used in BWR/3s (boiling water reactors) and in the new economic simplified boiling water reactor (ESBWR) would qualify as passive systems, while the reactor core isolation cooling and high-pressure coolant injection steam turbine–driven pumps commonly in use today in BWRs would not be considered passive, even though they do not require AC power for operation.

The current generation of light water reactors (LWRs), which includes the advanced boiling water reactor (ABWR), the European pressurized reactor (EPR), the advanced pressurized water reactor (APWR), and the Korean advanced pressurized reactor (APR-1400) do not use passive safety systems, except for reactor shutdown. Newer LWRs—the AP1000 (under first construction) and the ESBWR (close to being approved by the U.S. Nuclear Regulatory Commission, but not yet constructed)—do have passive emergency core cooling systems and containment heat removal systems. The ESBWR also has isolation condensers.

Mandating use of passive systems sounds attractive, but that is not the only way to assure a better response to SBO than what occurred at the Fukushima Daiichi site. SBO can also be mitigated by improving the robustness of the following:

- on-site AC and direct-current power
- ability to add water to the reactor pressure vessel (RPV) for an extended period of time
- depressurization of the RPV, if necessary.

As long as the approaches selected meet the overarching safety objectives, active versus passive safety systems should remain a design choice.

Q.3. Should the locations of the emergency diesel generators (EDGs) be more diversified at nuclear power plants (NPPs), to protect on-site alternating-current (AC) power from severe external events? For example, should it be required that at least one EDG, its fuel, and related switch gear be housed in a room at sufficiently high elevation and/or in a waterproof room for flood protection, while at least one EDG be housed below grade for airplane crash or terrorist attack protection?

A.3. In a station blackout situation, if water delivery to the reactor pressure vessel is lost for more than a couple of hours, the fuel will be severely damaged. Therefore, it is more certain to be able to supply AC power from protected on-site sources than to attempt to bring portable power in from outside in such a short time. Preserving on-site AC power (e.g., by placing the EDGs and related equipment in waterproof rooms and their air intake and exhaust above the maximum possible flood level) will certainly allow the NPP staff more options in dealing with a flooding emergency. In

addition, direct-current power (batteries) needs protection so that NPP instrumentation and actuation/control of critical valves remains available. NPPs should review their current capability to defend against floods and ensure that emergency batteries and at least one on-site AC power source are available after such an external event. As further backup, the use of transportable equipment, initially stored far enough away from the flood zone, should also be considered. In addition to the AC power diversity, it is important to have diversity in the makeup water sources, e.g., seawater, fire water, condensate storage tank, a dedicated dam, etc.

Q.4. Should there be regional emergency response centers with prestaged equipment to be deployed during severe accidents? For example, transportable diesel generators or gas-turbine generators (i.e., jet engines) could be rapidly brought to the site (e.g., by air, road, or water) to restore alternating-current power. Who would manage this equipment? Utility companies? The Institute of Nuclear Power Operations (INPO)? The Federal Emergency Management Agency?

A.4. The idea to set up regional response centers to deal with extreme emergencies caused by natural disasters at operating nuclear power stations (NPSs) deserves attention. Since the time for prevention of core damage and meltdown is of the order of 2 to 4 hours after loss of makeup water injection, if the nuclear power plant (NPP) is operating at the time of accident initiation, it is unlikely these regional response centers would be able to affect the early accident progression, which would have to be dealt with entirely at the site. However, the objectives of the regional response centers would be to (a) provide pertinent equipment to the NPP to mitigate and control the emergency situation beyond the station coping time [likely to increase to 12 hours or longer under new regulations proposed by the Nuclear Regulatory Commission (NRC)], (b) provide manpower and advice to operate the equipment provided, and (c) provide manpower and support for the NPP staff communications with their technical support center and the National Emergency (Crisis) Center. All of these support functions were required at the Fukushima Daiichi NPS after the natural disaster. Similar support may be required in the United States following a natural disaster like a severe hurricane, flood, tornado, or earthquake.

A regional response center should not be located too far from a NPP and should have available quick means of transport—e.g., a heavy-duty helicopter—which could take equipment like a fire truck full of water. Alternatively, it could take pumps, small diesel generators, batteries, and compressed air or nitrogen equipment for operating valves, etc. Once again, the time frame for mobilization of equipment and manpower from the regional response center would be beyond the station coping time and the early stages of the accident.

Location and staffing of one regional response center among a cluster of several operating NPPs would be the efficient and preferred option. Such clusters of NPPs occur in the United States, and the costs of a regional response center could be distributed among several NPPs and possibly the federal government and/or the armed forces (e.g., for maintenance and operation of heavy helicopters).

It should be emphasized that a regional response center should not serve the functions of a technical support center or the National Emergency (Crisis) Center for nuclear emergencies. Its function would be focused on the support of the NPP personnel for infrastructure, equipment, and communications. It should coordinate with the regional offices of the NRC and INPO, which would be interested parties in the region where the NPP is located.

The list of equipment and the staff expertise should be decided in consultations with the NPPs that the regional support center would serve. The idea of one response center serving several NPPs has merit since such severe natural emergencies are rare and the costs of equipment and staff expertise could be shared between the NPPs served.

It is essential that the staff of the regional response center maintain their equipment in the best possible condition, since when the equipment would be needed it would have to perform at the best performance level. The same is true about the staff, and they should train regularly, knowing full well that their services may be required very rarely in their service lifetimes.

Q.5. What lessons were learned regarding beyond-design-basis instrumentation?

A.5. Clearly, a nuclear power plant (NPP) suffering a severe (beyond-design-basis) accident would be better served if the operators could discern the state of the reactor plant and the state of the progression of the accident. Such capability could be beneficial for the future of nuclear power.

Perhaps the instrumentation that would be needed for the purposes defined above is absent in some or all NPPs, i.e., in-service NPPs as well as future NPPs currently being marketed. It would be productive to determine what instrumentation could be feasible under specific severe accident environmental conditions and to determine the costs involved for new NPPs and for backfitting old NPPs.

The premise that the operators of a NPP suffering a severe accident could limit the progression of the accident has some merit. There was a time period in the Three Mile Island Unit 2 (TMI-2) accident when the operator (if he had a measurement of the water level in the core and had believed it) could have stopped that accident. In the Fukushima Daiichi accident, a measurement of hydrogen concentration in the reactor building as a function of the accident progression could have been interpreted as a danger signal and could have resulted in earlier and greater attention to venting the primary containment volume so that accumulations of detonation concentrations of hydrogen in the containment buildings may have been avoided.

Instrumentation to measure vessel temperatures at various axial locations would also be beneficial—to indicate, for example, whether the core is still in the original core confines or has moved down into the lower head region. The operator would have a better appreciation of the progression of the accident. It is also clear from the TMI-2 accident that the operator action of restarting the pumps to fill the vessel probably saved the vessel as it was done before the melt transferred to the lower head. Thermocouples in the bottom of the vessel head would provide information to the operator about the possibility of and imminence of the failure of the lower head. This would be of interest if a manual addition of water in the containment became necessary. It should be remembered that not all systems work, or valves open automatically or passively, during an accident.

A primary list of instrumentation that would be of interest for severe (beyond-design-basis) accidents in old and new light water reactors would be for measurement of

- water level in the reactor pressure vessel [already present in pressurized water reactors (PWRs) as the reactor vessel level monitoring system, a TMI-2 backfit system]

- temperatures in the vessel at strategic locations (already present at core exit in PWRs)
- hydrogen concentration in the containment and reactor building at strategic locations
- fission product and radioactivity in the hot leg, steam generators, and containment at several strategic locations
- water and steam flow rates in the piping connecting the vessel to the components in the loops at several locations.

It is recommended that a feasibility study be performed for the number and location of instruments with the risk analyses and the detailed component codes before decision making.

Q.6. What lessons were learned regarding station blackout (SBO) coping mechanisms in light water reactors?

A.6. Any threat, including SBO, will lead to core damage within 1 to 4 hours if there is no makeup water to the reactor pressure vessel (RPV) in a boiling water reactor (BWR). Additionally, in BWRs, in a SBO situation all the reactor decay heat goes to a large pool of water inside the containment, meaning that the containment will heat up and need to be vented to preserve containment integrity. The timing for venting is of the order of 16 hours to 1 day depending on the specific design. Therefore, highest priority needs to be given to makeup water addition or decay heat removal for the RPV. This means assuring the availability of backups to the first line of defense (isolation condenser, reactor core isolation cooling system, and high-pressure coolant injection system) and a relatively rapid ability to depressurize to allow those lower-pressure backup systems to be able to add water. Having backup alternating-current (AC) power (either on-site or transportable) would be helpful, but having direct-current (DC) power for instrumentation, valve motive force, and control of safety and relief valves is essential.

Station blackout is also of potential concern to pressurized water reactors (PWRs), challenging the ability to remove decay heat. Venting is not called upon to preserve the integrity of the containment. PWR containment designs involve either a large free volume and ultimate failure pressures on the order of 7 bar or 100 psig ("large dry" containments) or involve the melting of a large quantity of stored ice ("ice condenser" containments) to limit the increase in containment pressure. Removal of decay heat in SBO scenarios is accomplished using a turbine-driven auxiliary feedwater system (AFS) providing makeup water to the steam generator. Under these conditions, the preferred heat removal mechanism is the operation of a steam generator power-operated relief valve (PORV), sometimes called an atmospheric dump valve, which would also allow cooling down of the primary system. If a steam generator PORV is not available, heat removal, but not cooldown, can be accomplished by a steam generator safety valve. Cooldown of the primary system may be important to prolong the life of the primary coolant pump seals. If these seals were to fail, primary coolant would be lost, an additional challenge to maintaining fuel cooling would be encountered, and the time available to recover power before fuel damage occurred would be reduced. It should be noted that new seal designs are available for some primary-system pumps that limit or eliminate the failure likelihood. In a feed-and-bleed operation, when the AFS is not available, the safety injection tanks are used to inject cold borated water (at lower pressure, 700 psig or ~50 bar) into the core for core cooling, while energy from the reactor coolant system is removed by using pressurizer PORVs.

Longer-term requirements, if AC power is not recovered, include reestablishing primary coolant pump seal cooling (if the specific design requires cooling), maintaining a source of water for the

AFS, and providing DC power for instrumentation and control of the AFS and operation of the steam generator PORV.

Q.7. How can the extension of the evacuation zone be determined when great direct damage is inflicted on the area surrounding the nuclear power plant (NPP) by a natural disaster (i.e., the initiating external event)?

A.7. Fundamental to the U.S. approach to disaster management is a tiered approach to assessment and responsibility for implementation of mitigative actions. Local, state, and federal organizations each have responsibility for assessing conditions and communicating upward along the chain to develop aggregate condition assessments and to deploy resources where they can have the most effect in saving lives and property. Even when the extent of devastation is significant and local disaster management is destroyed, the succeeding tiers of regional, state, and federal managers and responders are able to assume responsibility. Within the United States, disaster management and emergency response start at the local and state levels. However, in the case of managing critical infrastructure facilities such as national security installations, NPPs, communications systems, and transportation centers, the federal government may assume responsibility for the safety and integrity of the installation.

In the case of an accident at a NPP, the U.S. system calls for two federal agencies to assume responsibility for managing public health and safety. The primary role of the Nuclear Regulatory Commission (NRC) is to work in assessing and mitigating radiological releases from the incident, and the Federal Emergency Management Agency (FEMA) has responsibility for assessing the need for, and extent of, any evacuation or shelter-in-place requirements. Both agencies rely on the protective action guide (PAG) manual ("Manual of Protective Action Guides and Protective Actions for Nuclear Incidents," EPA-400-R-92-001, Environmental Protection Agency). This prudent division of responsibility fundamentally ensures that the technical resources of the NRC are entirely focused on responding to the incident and not diverted to managing a civil defense function.

One of the fundamental questions to be addressed is how priorities are established and risks assessed when both a radiological incident and a natural disaster with widespread destruction occur, such as what occurred with the Fukushima Daiichi accident. It is obvious that the Japanese government was neither prepared for nor even considered the consequences of a multireactor station blackout, and while their response to mitigating radioactivity release to the environment failed, it is clear that their efforts to establish evacuation and exclusion zones for the general populace did provide adequate protection. In fact, over a period of 3 or 4 days they successfully evacuated about 185,000 people who lived in ten towns within a 20-km area surrounding the stricken NPPs. All this was carried out during a general effort to relocate people away from the earthquake and tsunami area and to conduct search-and-rescue operations for survivors.

From all appearances, the Japanese were conducting a protective action strategy that was fully consistent with International Atomic Energy Agency guidelines. However, on March 16, 2011, NRC Chairman Gregory Jaczko declared that an evacuation of up to 50 miles (80 km) was advisable, and the NRC issued a statement that, "Under the guidelines for public safety that would be used in the United States under similar circumstances, the NRC believes it is appropriate for U.S. residents within 50 miles of the Fukushima reactors to evacuate." ("NRC Provides Protective Recommendations Based on U.S. Guidelines," U.S. NRC News Release 11-050, March 16, 2011;

http://pbadupws.nrc.gov/docs/ML1108/ML110800133.pdf.) Later the same day, President Barack Obama repeated the statements made by Chairman Jaczko.

But, was it really true that an evacuation of that magnitude was appropriate given the circumstances? Was a 50-mile evacuation consistent with U.S. procedures as stated by the chairman and the president? As the crisis unfolded, information was limited and communication strained. Complicating matters were the translators used by the media, who had little technical understanding of the situation. While this led to several alarming and incorrect reports, none were more alarming than the testimony of Chairman Jaczko before the House Energy and Commerce Committee, March 16, 2011, concerning the Unit 4 reactor: "We believe that secondary containment has been destroyed and there is no water in the spent-fuel pool. And we believe that radiation levels are extremely high, which could possibly impact the ability to take corrective measures."

This statement was never substantiated by the NRC and was immediately denied by the Japanese government. Yet, it is the concern over the Unit 4 spent-fuel pool that has been cited as the basis for the NRC's 50-mile evacuation. But a review of the facts shows that even under this extraordinary circumstance, an evacuation of 50 miles from the NPP site was not consistent with either the NRC or the Environmental Protection Agency (EPA) protective strategies. Rather, the PAG manual calls for sheltering-in-place if environmental conditions or other constraints make evacuation impracticable. Sheltering may be the protective action of choice, even at projected doses above the protective action guidelines for evacuation. Section 2.3.1 of the PAG manual states,

> Sheltering may be preferable to evacuation as a protective action in some situations. Because of the higher risk associated with evacuation of some special groups in the population (e.g. those who are not readily mobile), sheltering may be the preferred alternative for such groups as a protective action at projected doses up to 5 rem. In addition, under unusually hazardous environmental conditions use of sheltering at projected doses up to 5 rem to the general population (and up to 10 rem to special groups) may become justified.… In general, sheltering should be preferred to evacuation whenever it provides equal or greater protection.

Moreover, given the scope of the devastation of the Fukushima region and destruction of transportation systems and roadways, the prudent course of action would have been to recommend sheltering and possible relocation, rather than a broad evacuation. The NRC's own guidance on this matter states,

> Evacuation is not the only protective action available to the public. In some situations sheltering may provide protection that is equal to or even greater than evacuation. Sheltering may be the preferred protective action in cases where weather, competing events, or short-term releases are factors.

Evacuations are extreme measures that should only be used to protect the public from imminent danger. Section 1.1 of the EPA PAG states,

> Evacuation is the urgent removal of people from an area to avoid or reduce high-level, short-term exposure, usually from the plume or deposited activity. Relocation, on the other hand, is the removal or continued exclusion of people (households) from contaminated areas to avoid chronic radiation exposure.

In establishing a 20-km evacuation area, the Japanese were, in essence, following the procedures and processes that would have been implemented in the United States by FEMA and the NRC under the early phases of an incident of this magnitude.

Q.8. What lessons were learned regarding hydrogen control in light water reactors?

A.8. In order for hydrogen control to be necessary, the nuclear fuel has to be significantly damaged. Mark I and Mark II boiling water reactor (BWR) containments are inerted with nitrogen, so the production of hydrogen by itself does not pose an immediate explosion risk. However, for an extended station blackout (SBO), venting of the containment is necessary regardless of the state of the fuel in order to relieve the pressure caused by decay heat. If the core is damaged also, the time available before venting is required is significantly shortened because of the pressurization due to hydrogen. In addition, the vent pathway needs to be carefully examined to assure there is a simple exhaust to atmosphere that is not compromised by having common headers that can lead to unintended reverse flow in ductwork back to the nuclear power plant (NPP) or adjacent NPPs. The venting itself needs to be timely; otherwise, if the containment overpressurizes, additional leakage pathways for hydrogen-rich gases can be created through uncontrolled containment leakage at unpredictable locations.

Mark III containments are not inerted; however, they have a large volume compared to Mark I and Mark II containments so that the hydrogen concentrations are much lower. They also have installed igniters or passive autocatalytic recombiners (PARs) to convert the hydrogen, plus oxygen, back into water. Still, in an extended SBO, Mark III containments must also be vented to allow the decay-heat-generated steam to escape. Mark III containments are not currently required to have hardened vents—this situation needs to be examined in some more detail.

Pressurized water reactor (PWR) containments are similar to BWR Mark III containments except that, provided the steam generators are kept filled with water, the decay heat steam is relieved outside of containment via various steam line relief and/or safety valves that vent to atmosphere, so there is no need to vent the containments. If core damage occurs, hydrogen generation will occur. "Ice condenser" PWR containments have installed hydrogen igniters to ensure that the hydrogen concentration does not reach detonable limits. "Large dry" PWR containments do not reach 10% hydrogen concentration, assuming a 75% fuel cladding metal–water reaction, in compliance with 10 CFR 50.44 (*Code of Federal Regulations*, Title 10, "Energy," Part 50, "Domestic Licensing of Production and Utilization Facilities," Sec. 44, "Combustible Gas Control for Nuclear Power Reactors," Nuclear Regulatory Commission); thus, they do not have specific hydrogen mitigation systems. The newest designs of PWR NPPs already have hydrogen control systems—typically igniters, PARs, or both.

Q.9. Should materials be developed that generate less or no hydrogen upon oxidation by steam [i.e., Zircaloy cladding be replaced with less reactive metals, and ultimately a ceramic, such as silicon carbide (SiC)]?

A.9. It is important to consider possibilities for new cladding materials and products and to perform research and development in this area, but to use these materials in nuclear reactors it is necessary to demonstrate that they provide the same degree of safety and fission-product containment that the current cladding provides, both in normal operation and in accident conditions.

Silicon carbide is a promising material in many nuclear applications, such as the TRISO particle fuel, exhibiting resistance to radiation damage and effects, low corrosion, and good nuclear properties (K. Yueh et al., "Clad in Clay," *Nuclear Engineering International*, p. 14–16, 2010; D. M. Carpenter and M. S. Kazimi, "An Assessment of Silicon Carbide as a Cladding Material for Light Water Reactors," MIT-ANP-TR-132, Massachusetts Institute of Technology, November 2010). However, significant technological and scientific hurdles have to be overcome before SiC cladding can be used in water-cooled nuclear reactors, including difficulties in joining and in designing a ceramic material to create a hermetic seal that would contain the fission products and also provide a degree of ductility. It is also necessary to understand and design for the behavior of the material under accident conditions, such as a reactivity-initiated accident, and better understand its corrosion and stress corrosion limits. If these issues can be resolved, there are further fabrication procedures that would have to be established, and all of this development would have to be tested and validated.

Therefore, it is unlikely that new materials, even in the form of coatings for the current alloys, will be available in the next 10 years to replace zirconium alloys in light water reactors, even with a significant high-priority U.S. government–sponsored development program, so the focus of techniques to improve the safety of nuclear reactors should remain on the current fuel cladding.

Q.10. How can the need for containment venting be eliminated? If containment venting is necessary, how does one ensure it is done in a timely and reliable fashion, so that radioactivity releases are minimized?

A.10. In boiling water reactor (BWR) containments, the heat sink during station blackout (SBO) is inside containment. Therefore, all current BWR containments must be vented, if alternating-current power is not recovered, regardless of the state of the fuel. The only BWR containment design that avoids this need is the economic simplified BWR (ESBWR); however, this feature of the ESBWR required a complete redesign of the emergency core cooling system and the reactor building layout, so it is not retrofittable to current BWRs.

The vent pathway as designed at the Fukushima Daiichi nuclear power station and also at many U.S. BWRs needs to be looked at from the perspective of SBO. First, the installed rupture disks that prevent venting at low containment pressure must be capable of being bypassed. Next, the valve types used and auxiliary supplies needed to operate them should be reviewed to make the pathway simpler to establish. Finally, the vent piping should terminate in a dedicated release point so that if there is hydrogen in the containment atmosphere, it is released and diluted without the possibility of returning to the nuclear power plant through systems that use a common exhaust—or the possible reverse-flow pathways are known and can be completely isolated.

Emergency procedures do not call for pressurized water reactor (PWR) operators to vent the containment. Most PWR containments are of the "large dry" type and involve a very large free volume (when compared to a BWR Mark I containment) and have an ultimate pressure capacity on the order of 7 bar (~100 psig). A second type of containment incorporates large quantities of ice to quench steam and act as an effective heat sink. These design approaches eliminate (or delay, if the auxiliary feedwater system fails) the need for venting and give the operators time to recover electrical systems.

Q.11. Should the filtered/vented containment approach be adopted (as in the French and Swedish examples)? This could provide a balanced approach to controlling containment pressure and radioactivity releases to the atmosphere when containment cooling is not available. Early containment venting can reduce the source term for severe accidents by as much as two orders of magnitude.

A.11. This question assumes that before containment venting is attempted, there is also a significant source term release of radioactivity to the containment. In an extended station blackout (SBO), the heat sink is in the containment in boiling water reactors, and no containment heat removal is available. Therefore, the containment will pressurize, regardless of the state of the reactor fuel. It would be advantageous to be able to permit early containment venting to release the steam from reactor decay heat power when there is no fuel damage. In these circumstances there is little to be gained from additional filtration.

Should events that compromise decay heat removal from the reactor or containment to the ultimate heat sink also involve damage to the reactor fuel, then the issue of radiation release becomes relevant. Tests have shown that European filtered vent designs can reduce releases, particularly of long-half-life cesium-137 (30 years), by two to three orders of magnitude compared to uncontrolled releases under certain circumstances. However, filtered venting (a) is effective only if release does occur through the filters (versus uncontrolled leak points at the containment boundary, as happened at Fukushima Daiichi) and (b) comes with significant capital expense to the nuclear power plant (NPP). Therefore, whether to adopt such a mitigation feature should be dependent on a risk-benefit analysis that is site dependent and includes all aspects, such as the costs of permanent relocation of local inhabitants, land remediation, effect on surrounding industries and agriculture, etc., rather than being a general rule for all NPPs.

Venting is not expected to be needed in pressurized water reactors (PWRs) for SBO, as the containments have large volumes and the decay heat is removed from the core by the auxiliary feedwater system plus power-operated relief valves in the secondary loops outside of containment, so the energy is not released to the containment. Nonetheless, PWRs in several European countries (e.g., Germany, Sweden, France, and Switzerland) have installed filtered vents of several different technology designs.

Q.12. What risk-significant improvements can be made for spent-fuel cooling?

A.12. Ideally, the identification of risk-significant improvements would be made with the benefit of analyses. Such analyses would begin with a postulation of possible accidents [e.g., an earthquake that damages the spent-fuel pool (SFP) wall and liner, causing containment of the water to be lost, especially in boiling water reactors (BWRs) where the SFP is located high up on the top level of secondary containment] and a clear definition of the end states of interest. For SFP cooling events these end states could include, for example, the frequency of loss of cooling, the frequency of reaching boiling conditions, the frequency of fuel uncovery, the frequency of fuel damage, the frequency of radioactive material release, or the frequency of specific off-site impacts. Such analyses are not available, and it is recommended that consideration of such an exercise be undertaken. However, some suggestions for consideration can be made based on historical events.

Improvements can be divided into two categories: those that have the potential to improve information about the SFP conditions, and those that could potentially be cost-effective means of maintaining SFP level and temperature.

Improved information would include performing a calculation of bulk SPF temperature as a function of time that assumes complete loss of SFP cooling whenever the source changes as used fuel is added or removed from the SFP. Such calculations would be conducted for several times, e.g., at the time of the change, at 3 months, at 1 year, etc.

In the absence of SFP inventory loss by leakage, the SFP inventory should be sufficient to prevent fuel heatup for many days. Means to reliably determine SFP level and temperature for time frames commensurate to SFP heatup scenarios could represent a significant improvement. Video capability could provide valuable information as to whether heavy objects have fallen into the SFP and, at least partially, the physical condition of the fuel.

For the recovery of SFP inventory and temperature, additional means of adding water (e.g., through a pipe that connects to a fire hose and a hand-operated valve outside the reactor building) would be a valuable strategy, given the unavailability of normal makeup water and cooling. As the events at Fukushima Daiichi demonstrated, such means would likely be required from water sources outside the nuclear power plant (NPP), e.g., fire trucks. Note that most NPPs in the United States already have hardened makeup water paths for SFPs, as a result of the post-9/11 safety and security enhancement efforts mandated by the U.S. Nuclear Regulatory Commission.

One accident whose probability should be evaluated is the possibility of an earthquake that damages the SFP wall and liner, causing containment of the water to be lost, especially in BWRs where the SFP is located high up on the top level of secondary containment. Because the SFPs are outside the reactor containment, the likelihood of such an accident and its likely consequences should be evaluated in both a case where off-site power is available and one in which it is not.

Q.13. How can the source term of the spent-fuel pools (SFPs) be reduced (e.g., move to dry cask faster, then to regional storage facilities)?

A.13. The current SFPs at nuclear power plants (NPPs) both in Japan and in the United States contain fuel of various ages and discharge times. A significant fraction of this fuel has a low enough heat generation rate that removal to a dry-storage facility is possible. The removal of this fuel from the SFPs to dry storage would have the benefit of reducing the potential source term in SFPs containing higher-heat-generation rods. Thus, the recommendation is that a concerted effort be made to identify such fuel and remove it from the SFPs to a dry-storage facility. Clearly, there is a heat-generation limit above which it is not possible to cool the fuel passively; thus, there would be little benefit to removing this fuel from the SFP, as active cooling would have to be employed. The time for the heat generation to decrease to a level to where the fuel can be placed in dry storage is estimated at ~5 years, although higher-burnup fuel would take somewhat longer to decay to acceptable levels. Currently the United States does not have centralized storage of nuclear fuel; thus, the recommendation for U.S. NPPs is to move the spent-fuel assemblies to dry casks to be stored on-site. The broader issues of spent fuel management in the United States will not be discussed here; it is noted that the Blue Ribbon Commission on America's Nuclear Future is close to issuing its final recommendations on this topic.

Q.14. Should there be a requirement to avoid identified vulnerabilities, or should nuclear power plants (NPPs) be allowed to design against them? An obvious approach for future NPPs could be to choose sites away from highly seismic areas and coasts, to greatly reduce (and perhaps eliminate) the possibility of damage due to massive earthquakes, tsunamis, and floods.

A.14. While the approach of building on sites away from danger seems like common sense, its practical implementation is troublesome, as it may restrict the number of sites too severely—particularly in countries like Japan and Taiwan, where seismic-free sites basically do not exist. Figure 1 shows the location of all NPPs worldwide and all earthquakes of magnitude 7.0 and higher from 1973 to 2010. Note that the vast majority of NPPs worldwide are indeed located away from seismic areas. Given their proximity to major earthquake epicenters, the only option for NPP sites in countries like Japan and Taiwan and highly seismic regions of the United States (e.g., California) is to implement a robust NPP design that can cope with the earthquakes, which will occur. In the United States, the Nuclear Regulatory Commission is constantly raising the bar on seismic protection with consideration of ever-rarer and larger-magnitude earthquakes; therefore, what is considered a low-seismic-risk site today may become a high-seismic-risk site tomorrow. As such, a combination of risk avoidance (i.e., not concentrating NPPs in areas of known high seismic risk) and robust antiseismic designs is the most reasonable approach.
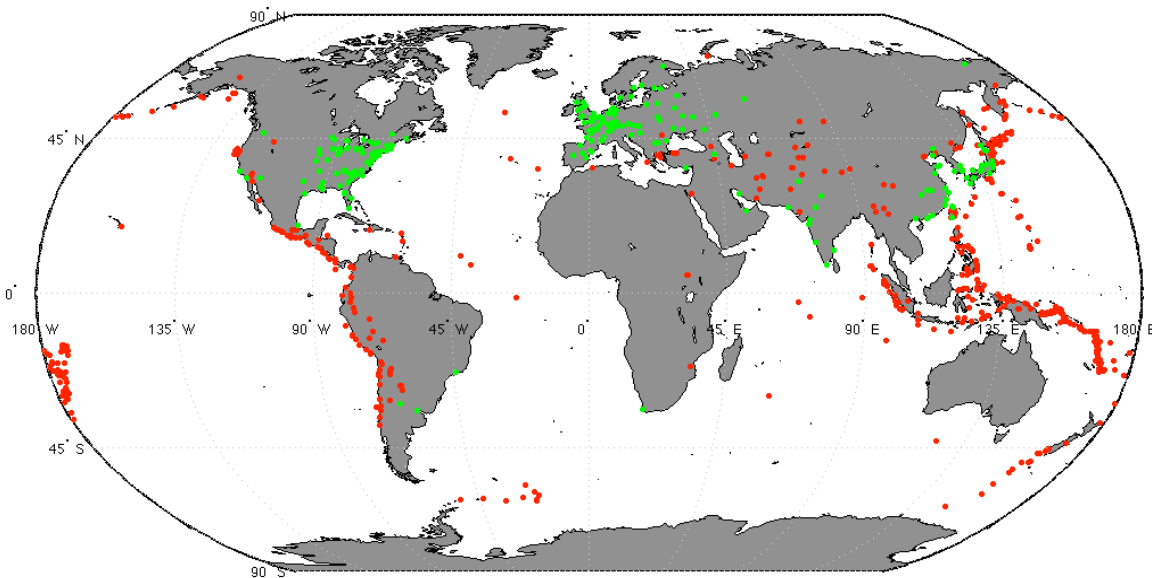

Figure 1. Locations of current and planned commercial NPPs (green dots) and all earthquakes of magnitude ≥7.0 from 1973 to 2010 (red dots). (Courtesy of Massachusetts Institute of Technology graduate student Mark Reed.)

Q.15. Should there be a limit on the number of units allowed at a nuclear power station site?

A.15. While the ability to prevent common-cause failures and cope with simultaneous accidents at existing multiunit sites should be strengthened, the question of limiting the number of units at a site is obviously more relevant to future nuclear power plants (NPPs). The high cost and lengthy schedule to get site approval are powerful incentives for multiunit sites. Thus, realistically, multiunit

sites will continue to exist. However, the number of allowable units at a single NPP site should be determined based on a risk analysis evaluation that accounts for the following, often conflicting, factors: (a) reduction of common-cause vulnerabilities [e.g., enhanced diversity of locations for emergency diesel generators (EDGs) to defeat floods, fires, and plane crashes; increased physical separation of units to prevent unit-to-unit spreading of problems caused by external as well as internal events such as turbine blade missiles], (b) availability of staff and resources to address a severe accident impacting multiple units simultaneously, (c) reduction of potential source terms including consideration of reactor size (e.g., small modular reactors versus large monolithic NPPs), (d) high standardization (i.e., shared learning), (e) shared equipment (e.g., shared EDGs and venting pipes), which has implications on both economics and safety, and (f) the environmental impact of multiunit cooling.

Q.16. When is safe, safe enough? Where do we draw the line? It seems that a rational approach to this question would need to be based on a risk-informed comparison of nuclear energy with other energy sources (particularly its most credible competitors, such as coal and natural gas), including their effects on climate change, global economy, stability and reliability of the energy supply, and geopolitics. But can the decision makers take a risk-informed approach to energy policy? All engineered structures (e.g., power plants, bridges, skyscrapers, dams, and highways) will fail if subjected to loads far enough beyond what they were designed for. Are the design-basis selections of energy industry structures posing high environmental hazard, such as oil drilling platforms offshore, coal mines, and water dams, consistent with those of nuclear power plants (NPPs)? If not, are we as a society irrationally accepting higher risks from certain technologies than from others?

A.16. The consideration of what is an acceptable degree of safety to be demanded of engineered structures has so far not been undertaken in a systematic way. This is partly because of the natural reluctance in assuming that a certain degree of risk (and therefore, a certain number of fatalities) that will result from human activity is acceptable. There is also considerable uncertainty as to what the actual risk is, so that a meaningful comparison of, for example, the environmental effects of various electricity sources can be difficult to perform. This ignorance of the actual risk also makes it difficult to assess the impact of additional safety measures on reducing the risk to the public.

As a result, safety standards in different industries can vary widely in the actual risk they pose to the public. Different public health measures taken to save human lives can vary from a few dollars to several billion dollars per life saved (T. O. Tengs et al., "Five-Hundred Life-Saving Interventions and Their Cost-Effectiveness," *Risk Anal.*, **15**, *3*, 1995). Such misallocation of resources has real impacts on lives lost, since the most significant risks may not be addressed, and resources may be wasted on risks that are comparatively low. In that sense risks associated with nuclear power tend to be overestimated because of public perception of such a risk. It would be beneficial to the energy policy of the United States if a concerted effort were made by an organization such as the National Academy of Sciences to quantitatively assess the public risk (either from accidents or from normal operation) of various electricity sources so that a rational basis for discussion of the relative merits of such sources could occur. Such an effort should take into account the ensemble of the technology, from cradle to grave (including mining, operation, disposal, etc.). It should also be mentioned that the higher cost of electricity could also translate to greater environmental cost, as the resources used to purchase the higher-cost electricity could have been used for other beneficial purposes. Finally, for a meaningful comparison the energy sources should be compared in the context of delivering a reliable and stable supply of electricity.

Seen from another perspective, nuclear power is a relatively young technology (50 to 60 years old), many of the risks are unfamiliar, and accidents are infrequent enough that not enough knowledge exists of their magnitudes and frequencies. In particular, it is difficult to evaluate the risk (both probability and consequence) of accidents in which there is core damage. Using the historical record amassed so far, it is possible now to start to reassess some of these assumptions so that higher-probability accidents can be considered and their consequences mitigated.

Throughout the history of the nuclear industry, the risk evaluation efforts have centered on accidents such as the large break loss-of-coolant accident (LOCA) and its consequences, because it was thought to be the most likely failure to cause core damage. In actual fact, of the three severe accidents that have so far occurred in commercial NPPs, one was a small break LOCA compounded by operator error (Three Mile Island Unit 2), another was a misguided experiment that resulted in an unstable fuel configuration from a reactivity point of view (Chernobyl), and the third was a loss of off-site and backup power and cooling ability due to an earthquake-tsunami combination (Fukushima Daiichi). It is possible that other accidents should be considered as part of the design basis, such as the prolonged station blackout. This should be done in a manner that would allow current NPPs to continue operating (that would not automatically shut them down) but that identifies the most important concerns from a risk analysis point of view.

Within the current regulatory framework, it is clear that some of the assumptions made in the siting of the Fukushima Daiichi NPP were insufficient and were a major cause of the accident. For example, if a higher tsunami wall had been erected, or if the NPP had been constructed 50 feet above sea level, or if backup diesel generators and oil supplies had been placed high enough out of the reach of the tsunami, most consequences would have been averted. Thus, it makes sense to recommend that utilities review the local estimates for the frequency and severity of natural disasters (e.g., earthquakes, tsunamis, volcanic eruptions, floods, hurricanes, and tornados) that could potentially affect the functioning of the NPP safety systems and prevent a cold shutdown and take appropriate measures to address any concerns.

Q.17. To what extent should severe accident management guidelines/procedures be voluntary versus required? In this context, what are the boundaries between the Nuclear Regulatory Commission (NRC) and the Institute of Nuclear Power Operations (INPO)?

A.17. Historically, nuclear regulations have focused on the consequences of a large break loss-of-coolant accident, an event that has never happened. New regulations and practices after the Three Mile Island Unit 2 (TMI-2) accident have reduced the risk from *internal events* (like TMI-2) to a very small level. However, it is apparent from events like 9/11 and the Fukushima Daiichi accident that nuclear risk to the public is currently dominated by extreme *external events*, whether man-made (e.g., terrorism) or natural (e.g., fire, seismic events, or severe weather).

The Committee recommends the use of probabilistic risk assessment (PRA) to identify those accident sequences (e.g., prolonged station blackout) and end-state conditions (e.g., partial core meltdown) that might be initiated by extreme external events and that carry the largest risk of radiation release to the environment and the public. For the dominant accident sequences and end-state conditions so identified, the Committee recommends the development of (a) a series of prescriptive acceptance criteria that are meant to mitigate the consequences of these accidents and (b) an appropriate set of quality assurance requirements for these criteria. NRC rules for anticipated

transient without scram are a possible model for the treatment of the new accidents. The Committee recognizes that large uncertainties will be present in evaluating the risk of these rare accidents; thus, what sequences and end-state conditions are added to the design basis will ultimately be a judgment call by the regulator and other stakeholders. Nevertheless, the Committee feels this new approach could have a real impact in reducing the overall risk to the public from nuclear power. This approach will also provide a sound technical basis for both the on-site severe accident mitigation strategies and the off-site emergency response strategies (e.g., trigger and size of the evacuation zone), since they could be better optimized for mitigation of the consequences of the high-risk accidents identified by the PRA. The downside of these proposed changes is, of course, an incremental capital and operations and maintenance cost to owners, which would come mostly from equipment retrofits, quality assurance requirements, and additional procedures, with compliance promoted and monitored by INPO and verified by the NRC.