Evolution of Onsite and Offsite Power Systems in US Nuclear Power Plants

Roy K. Mathew

U.S. Nuclear Regulatory Commission, USA

Abstract

The AC electric power system is the source of power for station auxiliaries during normal operation and for the reactor protection system and emergency safety features during abnormal and accident conditions. Since the construction of early plants in US, the functional adequacy and requirements of the offsite power systems, safety and non safety related onsite electric power systems have changed considerably to ensure that these systems have adequate redundancy, independence, quality, maintenance and testability to support safe shutdown of the nuclear plant. The design of AC systems has evolved from a single train to multiple (up to four) redundant trains in the current evolutionary designs coupled with other auxiliary AC systems.

The early plants were designed to cope with a Loss of Offsite Power (LOOP) event through the use of onsite power supplies only. However operating experience has indicated that onsite and offsite power AC power systems can fail due to natural phenomena (earthquakes, lightning strikes, fires, geomagnetic storms, tsunamis, etc.) or operational abnormalities such as loss of a single phase, switching surges or human error. The onsite DC systems may not be adequately sized to support plant safe shutdown over an extended period if AC power cannot be restored within a reasonable time.

This paper will discuss the requirements to improve availability and reliability of offsite and onsite alternating current (AC) power sources to U.S. Nuclear Power Plants. In addition, the paper will discuss the requirements and guidance beyond design basis events.

1.Commission's Policy Statement and Safety Goals

Commission's Policy Statement on Safety Goals for the Operations of Nuclear Power Plants, which appeared in the Federal Register in August 1986 (51 FR 30028). The approach includes the agency's historical commitment to a defense-in-depth philosophy that ensures that the design basis includes multiple layers of defense.

The Policy Statement on Safety Goals sets forth two qualitative safety goals, which are supported by two quantitative supporting objectives. The following are the qualitative safety goals:

> Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.
>
> Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

The quantitative supporting objectives are as follows:

The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of

prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

> The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

In the Policy Statement on Safety Goals, the Commission emphasized the importance of features such as containment, siting, and emergency planning as "integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy." A cursory review of documents discussing the agency's approach to defense-in-depth provides a range of explanations and applications.

The Commission's policy on probabilistic risk assessment (PRA) ("Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," dated August 16, 1995), states the following:

> Defense-in-depth is a philosophy used by the NRC to provide redundancy for facilities with "active" safety systems, e.g. a commercial nuclear power [plant], as well as the philosophy of a multiple-barrier approach against fission product releases.

An instructive discussion of the defense-in-depth philosophy also appears in director's decisions relating to a petition on Davis-Besse (FirstEnergy Nuclear Operating Company (Davis-Besse Nuclear Power Station, Unit 1), DD-03-3, 58 NRC 151, 163 (2003)).

The decision described defense-in-depth as encompassing the following requirements:

> (1) require the application of conservative codes and standards to establish substantial safety margins in the design of nuclear plants;
>
> (2) require high quality in the design, construction, and operation of nuclear plants to reduce the likelihood of malfunctions, and promote the use of automatic safety system actuation features;
>
> (3) recognize that equipment can fail and operators can make mistakes and, therefore, require redundancy in safety systems and components to reduce the chance that malfunctions or mistakes will lead to accidents that release fission products from the fuel;
>
> (4) recognize that, in spite of these precautions, serious fuel-damage accidents may not be completely prevented and, therefore, require containment structures and safety features to prevent the release of fission products; and
>
> (5) further require that comprehensive emergency plans be prepared and periodically exercised to ensure that actions can and will be taken to notify and protect citizens in the vicinity of a nuclear facility.

2. General Design Requirements for Electric Power Systems

Under the provisions of Title 10 of the Code of Federal Regulations (CFR) 50.34, 52.47, 52.79, 52.137, and 52.157, an application for a construction permit, a design certification, combined license, design approval, or manufacturing license, respectively, must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

These General Design Criteria (GDC) establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission. The GDC are also considered to be generally applicable to other types of nuclear power units and are intended to provide guidance in establishing the principal design criteria for such other units. The principal design criteria for earlier Nuclear Power Plants (pre-GDC) follow the requirements specified by the Atomic Energy Commission (AEC) rules published for 10 Part 50 in the Federal Register on July 11, 1967, and February 10, 1971.

Two key GDCS for the electric power system are provided in GDCs 17 and 18. GDC 17, "Electric Power Systems," in Appendix A to Part 50 establishes design requirements for the electric power systems (both offsite and onsite power systems) of nuclear power plants. Specifically, GDC 17 states: An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components (SSCs) important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences, and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

GDC provides definition for single failure as applied to safety related systems. Specifically, it states that a single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions

GDC 17 explicitly states that the offsite and onsite power system design must meet the failure criterion on a system basis without loss of capability to provide power for all safety functions. By definition of single failure criterion, the complete onsite electric power system (Class 1E) must be capable of sustaining a single failure without loss of capability to provide power for the minimum required safety functions. Hence, the offsite and onsite power systems considered together must be capable of sustaining a double failure, one of which is complete loss of offsite power coupled with a single failure in the onsite power system without loss of capability to provide power for the minimum required safety functions.

The offsite power source is also the 'preferred power supply' as it is preferred to furnish electric energy under accident or post-accident conditions. It is highly reliable and available to mitigate the consequences of all anticipated operational occurrences. It is capable of: Starting and operating all required loads for normal operation and providing power for the shutdown of the station and for the operation of emergency systems and engineered safety features.

Operating experience and a number of probabilistic risk assessments have identified a number of issues significant to reactor safety. To improve the availability and reliability of electric power system evolutionary advanced light water reactors (ALWRs), the staff determined that feeding the safety buses from the offsite power sources through nonsafety buses or from a common transformer winding with nonsafety loads is not the most reliable configuration. Such an arrangement increases the difficulty in properly regulating voltage at the safety buses, subjects the safety loads to transients caused by the nonsafety loads, and adds additional failure points between the offsite power sources and safety loads. Therefore, it is the staff's position that at least one offsite circuit to each redundant safety division should be supplied directly from one of the offsite power sources with no intervening nonsafety buses in such-a manner that the offsite source can power the safety buses upon a failure of any nonsafety bus. In addition, the staff recommended an additional source of power would significantly reduce the number of plant trips

that involve a loss of power to the nonsafety loads and require that the plant be shut down under natural circulation. Such an additional source of power would improve plant safety, because these events continue to be identified as more severe than the turbine-trip-only event in standard plant safety analysis reports. These proposed improvements were approved by the Commission on August 15, 1991.

GDC 18, "Inspection and Testing of Electric Power Systems," of Appendix A to 10 CFR Part 50 requires that electric power systems important to safety be designed to permit appropriate periodic inspection and testing to assess the continuity of the systems and the condition of their components.

Surveillance Requirements and Limiting Conditions for Operation

In accordance with GDC 17, an electric power system is required to supply power to loads important to safety in an NPP. Nuclear plants with more power sources than the number of sources required by GDC 17 may be able to withstand the multiple failures and still satisfy the limiting conditions for operation (LCOs). However, during the normal course of operation, any NPP may lose power sources to the extent that the LCOs are not met. Regulatory Guide 1.93, Revision 1, "Availability of Electric Power Sources," provides specific guidance to address situations in which the number of electric power source is less than the adequate number of power sources. During plant operation, the plants are required to have two qualified offsite power sources and two onsite power systems including redundant DC and vital AC power supplies (inverters).

Plant systems that can adversely impact safe shutdown capability have restrictions on outage times mandated by Federal Regulations. Specifically 10 CFR 50.36(c)(2), requires that the technical specifications (TS) include the limiting conditions for operation (LCOs), which are defined as the lowest functional capability or performance levels of equipment required for safe operation of the facility. Furthermore, the same regulations require that, when an LCO of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the TS until the condition can be met. The operational restrictions in the TS are based on meeting the LCO, period of continued operation, and orderly shutdown. In addition, the same regulation in Section (c)(3) requires test, calibration, or inspection for equipment to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met. The surveillance requirements and their frequencies are specified in each NPP's TS.

Extension of Allowed Outage Times or LCOs for Electric Power Sources

Regulatory Guide (RG) 1.93 provides guidance with respect to operating restrictions, that is Allowed Outage Time (AOT), if the number of available onsite emergency diesel generators (EDGs) and offsite power sources is less than that required by the TS. In particular, this RG prescribes a maximum AOT of 72 hours for an inoperable onsite or offsite power source. The lessons learned from Blackout events in the U.S indicate that restoration of offsite power will take longer than previously considered, indicating that post-deregulation conditions in the U.S challenge grid reliability. The staff now requires that a supplemental power source be available as a backup to the inoperable EDG or offsite power source, to maintain the defense-in-depth design philosophy of the electrical system to meet its intended safety function. The supplemental source must have capacity to bring a unit to safe shutdown (cold shutdown) in case of a loss of offsite power (LOOP) concurrent with a single failure during plant operation .The staff's objective of requiring an extra (i.e., supplemental) power source for an inoperable EDG or offsite power source is to avoid a potential extended Station Blackout (SBO) event during the period of an extended AOT and to enable safe shutdown (cold shutdown) of the unit if normal power sources cannot be restored in a timely manner.

Grid Reliability

The transmission system is the source of power to the offsite power system. The transmission system is generally demonstrated to have higher availability and reliability than the on-site emergency power system because of the diverse and multiple generators connected to the transmission system. Hence NPPs generally consider offsite power as the primary source (preferred source) of power for cooling down the reactor during normal and emergency shutdowns. This means that the connections to the grid must have adequate capacity and capability to provide rated power to safety grade electrical equipment in the NPP to perform its function. The degree, to which the grid can maintain an uninterruptible power supply to the NPP with sufficient capacity, and with adequate voltage and frequency, is the measure of grid reliability from the point of view of the NPP.

Although NPPs are designed to cope with a LOOP event through the use of on-site power supplies, LOOP events are considered precursors to station blackout. An increase in the frequency or duration of LOOP events increases the probability of station blackout and hence of core damage. Hence it is important that the transmission system can provide a reliable electrical supply to an NPP, with adequate capacity. Faults on the grid system at a significant distance from a NPP can be the cause of reactor trips or the LOOP. In addition to requiring the grid system and the grid connection to the NPP to be reliable, NPPs also require the grid supply to have sufficient capacity, and to be of an appropriate quality, with both voltage and frequency to be maintained within defined ranges. U.S NPPs disconnect or shut down if the grid frequency goes outside the acceptable range, or if the grid voltage becomes so high or low that voltages within the plant are unacceptable. NPPs also require a stable and reliable grid for other reasons:

— So that the number of unplanned trips of the nuclear unit from power caused by grid faults or unusual grid behavior is small compared with the total number of unplanned trips allowed in the design and safety assessments;
— For commercial reasons so that the nuclear units can achieve a high load factor, unconstrained by grid restrictions or grid faults, and that trips caused by grid behavior do not shorten the life of the plant.

The U.S NRC initiated a regulation, 10 CFR 50.65 (a)(4) which requires NPP owners to assess and manage the increase in risk that may result from proposed maintenance activities before performing the maintenance activities. Grid stability and off-site power availability are examples of emergent conditions that may result in the need for action prior to conducting maintenance activities that could change the conditions of a previously performed assessment. Accordingly, NPP owners are required to perform grid reliability evaluations as part of the maintenance risk assessment before performing any grid-risk-sensitive maintenance activities (such as surveillances, post-maintenance testing, and preventive and corrective maintenance). Such activities could increase risk under existing or imminent degraded grid reliability conditions, including (1) conditions that could increase the likelihood of a plant trip, (2) conditions that could increase the likelihood of a LOOP or SBO, and (3) conditions that could have an impact on the plant's ability to cope with a LOOP or SBO event, such as out-of-service risk-significant equipment (for example, a diesel generator used for onsite power, a battery, a steam-driven pump, or an alternate ac power source).

On August 14, 2003, the largest power outage in U.S. history occurred in the Northeastern United States and parts of Canada. Nine U.S. NPPs tripped. Eight of these lost off-site power, along with one NPP that was already shut down. The length of time until power was available to the switchyard ranged from approximately 1 to 6½ hours. Although the on-site DGs functioned to maintain safe shutdown conditions, this event was significant in terms of the number of plants affected and the duration of the power outage. In response, the US nuclear industry developed protocols between the NPP and the transmission system

operator (TSO), independent system operator (ISO), or reliability coordinator/authority (RC/RA) and the use of transmission load flow analysis tools (analysis tools) by TSOs to assist NPPs in monitoring grid conditions to determine the operability of offsite power systems. (In US, after the deregulation of the electric power industry, the TSO, ISO, or RA/RC is responsible for preserving the reliability of the local transmission system. denote these entities). The use of NPP/TSO protocols and analysis tools by TSOs assist NPPs in monitoring grid conditions for consideration in maintenance risk assessments and any impending challenges to the off-site power systems. A communication interface with the plant's TSO, together with training and other local means to maintain NPP operator awareness of changes in the plant switchyard and off-site power grid, is important to enable the licensee to determine the effects of these changes on the operability of the off-site power system. Hence, these protocols and communications help NPP operators in making conservative decisions for onsite power systems to preclude SBO conditions in the event of a LOOP.

A robust grid that can withstand severe perturbations reduces the probability of a loss of off-site power at a NPP. The robustness of the grid system determines the reliability and availability of off-site power and is evaluated using the following contingencies:

i. The trip of the nuclear power unit is an anticipated operational occurrence (AOO) that can result in reduced switchyard voltage, potentially actuating the plant's degraded voltage protection and separating the plant's safety buses from off-site power. It can also result in grid instability, potential grid collapse, inadequate switchyard voltages, and a subsequent LOOP due to loss of the real and/or reactive power support supplied to the grid from the nuclear unit.

ii. Grid stability and off-site power availability conditions under postulated transients on the grid system need to be evaluated for grid reliability. The results of the grid stability analysis must show that the loss of the largest single supply to the grid does not result in the complete loss of preferred power. The analysis should consider the loss, through a single event, of the largest capacity being supplied to the grid, removal of the largest load from the grid, or loss of the most critical transmission line. This could be the total output of the station, the largest station on the grid, or possibly several large stations if these use a common transmission tower, transformer, or a breaker in a remote switchyard or substation.

Degraded Grid Voltage Protection

The operating events at U.S. operating plants that led to the NRC staff's position regarding degraded voltage protection for nuclear power plant Class 1E electrical safety buses for sustained degraded grid voltage conditions. Specifically, Electrical grid events at the Millstone Station, in July of 1976 demonstrated that when the Class 1E buses are supplied by the offsite power system, sustained degraded voltage conditions on the grid can cause adverse effects on the operation of Class 1E loads. These degraded voltage conditions will not be detected by the Loss-of-Voltage Relays (LVRs) which are designed to detect loss of power to the bus from the offsite circuit(s). The LVR's low voltage dropout setting is generally in the range of 0.7 per unit voltage or less, with a time delay of less than 2 seconds. As a result of further evaluation of the Millstone events, it was determined that improper voltage protection logic can also cause adverse effects on the Class 1E systems and equipment, such as spurious load shedding of Class 1E loads from the standby diesel generators and spurious separation of Class 1E systems from offsite power due to normal motor starting transients. Another degraded voltage event, in September of 1978, at ANO station demonstrated that degraded voltage conditions could exist on the Class 1E buses even with normal transmission network (grid) voltages, due to deficiencies in equipment between the grid and the Class 1E buses (Offsite/Station electric power system design) or by the starting transients experienced during certain accident events not originally considered in the sizing (design) of these circuits. The staff required all NPPs to implement a second level of undervoltage protection scheme with time delay to protect the Class 1E equipment. The staff positions and guidance to meet the NRC requirements are described in NRC Standard Review Plan, Branch Technical Position 8-6.

Open Phase Protection

NRC staff issued Bulletin 2012-01, Design vulnerability in Electric Power Systems," after an operating event at Byron Unit 2 revealed a design vulnerability in the electric power system. Specifically, Byron Station, Unit 2 experienced an automatic reactor trip from full power because of an undervoltage condition on the 6.9-kV buses that power reactor coolant pumps. The undervoltage condition was caused by a broken insulator stack of the phase C conductor for the 345 kV power circuit that supplies both station auxiliary transformers. The open circuit created an unbalanced voltage condition on the two 6.9-kV nonsafety-related RCP buses and the two 4.16-kV engineered safety features (ESF) buses. ESF loads remained energized momentarily, relying on equipment protective devices to prevent damage from an unbalanced overcurrent condition. The overload condition caused several ESF loads to trip. For eight minutes, offsite and onsite power systems were not able to perform their safety functions. Operator manual actions were required to start the emergency diesel generators and energize the ESF buses. Recently, Bruce power plant in Canada and Forsmark, Unit 3, in Sweden reported similar events. The NRC is taking regulatory actions for NPPs to install open phase detection and protection schemes for addressing this design vulnerability.

Station Blackout

Station blackout means the complete loss of ac electric power to the essential and nonessential switchgear buses in a nuclear power plant (i.e., loss of offsite electric power system concurrent with turbine trip and unavailability of the onsite emergency ac power system). Station blackout does not include the loss of available ac power to buses fed by station batteries through inverters or by alternate ac sources as defined in this section, nor does it assume a concurrent single failure or design basis accident.

The station blackout (SBO) rule (10 CFR 50.63) evolved from the results of several plant-specific probabilistic safety studies, operating experience, and reliability, accident sequence, and consequence analyses completed between 1975 and 1988. WASH-1400, "Reactor Safety Study," issued 1975, indicated that SBO could be an important contributor to the total risk from nuclear power plant (NPP) accidents. This study concluded that if an SBO persists for a time beyond the capability of the ac-independent systems to remove decay heat, core melt and containment failure could follow.

In 1980, the Commission designated the issue of SBO as Unresolved Safety Issue (USI) A-44, "Station Blackout," and the staff completed several technical studies to determine if any additional safety requirements were needed. NUREG-1032, "Evaluation of Station Blackout at Nuclear Power Plants," issued June 1988, integrated the findings of the technical studies completed for USI A-44. NUREG-1032 presented the staff's major technical findings for the resolution of USI A-44 and provided the basis for the SBO rule and the accompanying Regulatory Guide (RG) 1.155, "Station Blackout," issued August 1988.

The NUREG-1032 evaluation of emergency diesel generator (EDG) train reliability used results and data from NUREG/CR-2989, "Reliability of Emergency AC Power Systems at Nuclear Power Plants," issued July 1983. NUREG/CR-2989 used the fault trees from 18 site probabilistic risk assessments (PRAs) and individual plant examinations (IPEs) to find the EDG failure boundary and classify failures. Consistent with the licensee PRAs/IPEs, the NUREG 1032 analyses of EDG unreliability considered planned and unplanned EDG demands and failures to start and load-run, EDG unavailability due to test and maintenance out-of-service (MOOS) while the reactor was in power and nonpower status, EDG failure recovery, and EDG common-cause failures. EDG MOOS while the reactor is at power can be an important consideration because the plant risk is potentially higher because of the possibility of a demand while the EDG is unavailable. EDG unavailability measurement can be based on the hours the EDG is unavailable or on the number of failures per demand. Both measures are unbiased estimates of EDG unavailability and are comparable so long as both measures are based on the same considerations (i.e., both consider MOOS).

In March 1986, the NRC issued draft RG 1.155, which presented an acceptable method to comply with the SBO rule based on plant-specific characteristics and the dominant risk factors from NUREG-1032. The NRC issued the final RG 1.155 in August 1988, which provided for selection of the SBO coping duration based on plant-specific characteristics, including past unit average EDG train performance criteria and emergency ac power system configuration. In general, the plants could select the 0.975 EDG target reliability level to achieve shorter coping durations.

In November 1987, the Nuclear Management and Resources Council (NUMARC) (subsequently renamed the Nuclear Energy Institute) submitted NUMARC 87-00, "Guidelines and Technical Bases for NUMARC Initiatives Addressing Station Blackout at Light Water Reactors," issued November 1987, as an alternative to comply with the SBO rule. By reference in RG 1.155, the staff concluded that NUMARC 87-00 contains guidance acceptable to the staff for meeting the SBO rule. The SBO rule requires that the NRC staff complete a regulatory assessment and notify the licensees of the staff's conclusions regarding the licensees' response to the SBO rule. The NRC completed safety evaluations for each plant.

Extended Loss of All AC Power

The events that occurred at the Fukushima Daiichi Nuclear Power Plant site, however, highlight the possibility that extreme natural phenomena could challenge the prevention, mitigation, and emergency preparedness defense-in-depth layers that are currently in place under the NRC's regulatory framework. The NRC's assessment of insights from the events at Fukushima Daiichi leads the NRC staff to conclude that requirements are necessary for all licensees and applicants (both current and new reactor licensees and applicants including design certifications) to mitigate an extended loss of all ac power condition, including the loss of normal access to the ultimate heat sink resulting from beyond-design-basis external events. In the days following the Fukushima Daiichi nuclear accident in Japan, the NRC Chairman directed the NRC staff to establish a senior-level agency task force to conduct a methodical and systematic review of the NRC's processes and regulations to determine whether the agency should make additional improvements to its regulatory system and to offer recommendations to the Commission for its policy direction. This direction was provided in a tasking memorandum (COMGBJ-11-0002), dated March 23, 2011, from the NRC Chairman to the NRC Executive Director for Operations. In response to this tasking memorandum, the NRC chartered the Near Term Task Force (NTTF).

In SECY 11 0093, the NTTF provided a number of recommendations to the Commission, including a specific proposal for new requirements for long term station blackout mitigation. The NTTF suggested enhanced station blackout mitigation strategies, within NTTF Recommendation 4.1, as follows:

> Initiate rulemaking to revise 10 CFR 50.63 to require each operating and new reactor licensee to: (1) establish a minimum coping time of 8 hours for a loss of all ac power, (2) establish the equipment, procedures, and training necessary to implement an "extended loss of all ac" coping time of 72 hours for core and spent fuel pool cooling and for reactor coolant system and primary containment integrity as needed, and (3) preplan and prestage offsite resources to support uninterrupted core and spent fuel pool cooling, and reactor coolant system and containment integrity as needed, including the ability to deliver the equipment to the site in the time period allowed for extended coping, under conditions involving significant degradation of offsite transportation infrastructure associated with significant natural disasters.

In SRM-SECY-11-0124, the Commission approved the NRC staff's proposed actions to implement without delay the NTTF recommendations as described in SECY-11-0124. The Commission approved the NRC staff's proposed prioritization of the NTTF recommendations, including the staff's proposals for addressing the NTTF recommendations. With regard to the portions of the SRM having relevance to this regulatory action, the Commission directed the staff to:

- Initiate a rulemaking for recommendation 4.1, Station blackout regulatory actions, as an ANPR rather than as a proposed rule.

- Designate the SBO rulemaking associated with NTTF Recommendation 4.1 as a high-priority rulemaking with a goal of completion within 24 to 30 months.

- Craft recommendations that continue to realize the strengths of a performance-based system as a guiding principle. In developing these recommendations, the Commission directed the NRC staff to consider approaches that are flexible and able to accommodate a diverse range of circumstances and conditions. The Commission noted that "in consideration of events beyond the design basis, a regulatory approach founded on performance-based requirements will foster development of the most effective and efficient, site-specific mitigation strategies, similar to how the agency approached the approval of licensee response strategies for the "loss of large area" event under its B.5.b program."
- Monitor nuclear industry efforts underway to strengthen SBO coping times and consider whether any interim regulatory controls (e.g., commitment letters or confirmatory action letters) for coping strategies for SBO events would be appropriate while rulemaking activities are in progress.

- For NTTF Recommendations 4.2 and 5.1, provide the Commission with notation vote papers for its approval of the Orders once the NRC staff has engaged stakeholders and established the requisite technical bases and acceptance criteria.

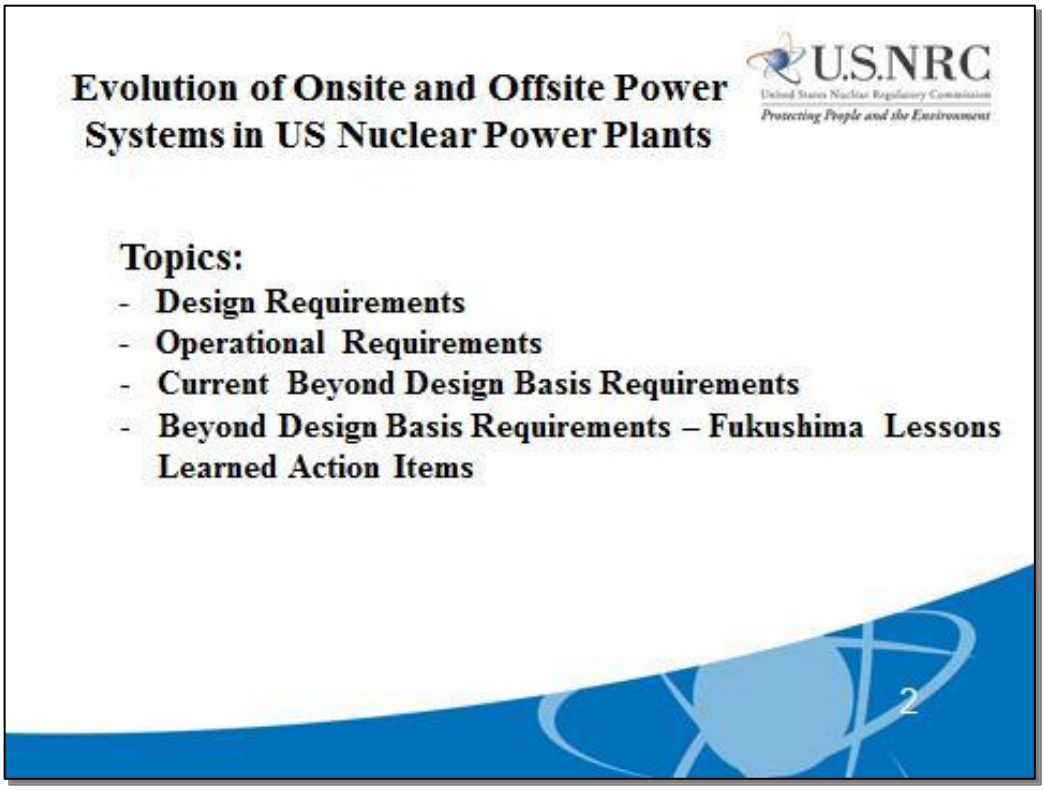
In accordance with SRM-SECY-11-0124, the NRC staff provided SECY-12-0025, Proposed Orders and Requests for Information in Response to Lessons Learned from Japan's March 11, 2011, Great Tohoku Earthquake and Tsunami, to the Commission on February 17, 2012, including the proposed Order to implement enhanced mitigation strategies. As directed by SRM-SECY-12-0025, the NRC staff issued Order EA-12-049, Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events, on March 12, 2012 Order EA-12-049 imposed new requirements to implement mitigation strategies to provide additional capability to respond to beyond-design-basis external events, which can lead to an extended loss of ac power and loss of access to the ultimate heat sink. The Commission concluded that the new requirements were necessary to continue to have reasonable assurance of adequate protection of public health and safety. The Order significantly expanded the scope of the regulatory concerns addressed under NTTF Recommendation 4.2 in SECY-11-0124, as discussed below in the section entitled, Consolidation of Recommendation 4 and 7 Regulatory Activities.

The Order requires a three-phase approach for mitigating beyond-design-basis external events that lead to an extended loss of ac power and loss of normal access to the ultimate heat sink condition. The initial phase requires the use of installed equipment and resources to maintain or restore core cooling, containment, and spent fuel pool cooling. The transition phase requires provision of sufficient, portable, onsite equipment and consumables to maintain or restore these functions until they can be accomplished with resources brought from offsite. The final phase requires the capability to obtain sufficient offsite resources to sustain those functions indefinitely. The Commission concluded that the EA-12-049 requirements were necessary for ensuring continued adequate protection of public health and safety.

The NRC staff plans to issue a proposed rule amending NRC regulations to address these scenarios for both current and new reactors. The final regulatory basis for the SBOMS rulemaking, found at ML13171A061, reflects consideration of feedback from the public meeting, comments received on the

draft regulatory basis, and the ACRS interactions where it was practical to do so within the current schedule. The staff believes that the feedback on the draft rule concepts deserves careful consideration and deliberation and is considering this feedback as it develops the proposed SBOMS rule language. The Final Rule is due to the Commission on December 27, 2016.


CSNI International Workshop on
ROBUSTNESS OF ELECTRICAL SYSTEMS OF NPPs
in Light of the Fukushima Daiichi Accident
Evolution of Onsite and Offsite Power Systems in US
Nuclear Power Plants
ROY K. MATHEW
U.S NUCLEAR REGULATORY COMMISSION
April 1-4, 2014


Evolution of Onsite and Offsite Power Systems in US Nuclear Power Plants
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment
Topics:
- Design Requirements
- Operational Requirements
- Current Beyond Design Basis Requirements
- Beyond Design Basis Requirements – Fukushima Lessons Learned Action Items
2

Design Requirements

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

General design criterion (GDC) 17, "Electric Power Systems," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," in part, requires:

"An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents. ...."

3

Design Requirements – Cont. Defense in Depth

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

- Single failure
- Independence
- Redundancy
- Diversity
- Availability/Reliability
- Operating Experience

4

Design Requirements – Defense in Depth (Cont.)

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

- Second level undervoltage protection or Degraded grid voltage protection
- Open Phase protection
- New Reactor Designs
  - At least one offsite circuit to each redundant safety division should be supplied directly from one of the offsite power sources with no intervening nonsafety buses
  - Additional source of power to improve plant safety

5

Operational Requirements

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

- 10 CFR 50.36(c)(2), requires that the technical specifications (TS) include the limiting conditions for operation (LCOs), which are defined as the lowest functional capability or performance levels of equipment required for safe operation of the facility. Furthermore, the same regulations require that, when an LCO of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the TS until the condition can be met.
- RG 1.93 - Regulatory Positions
  - The intent of each regulatory position is to implement the safest operating mode whenever the available electric power sources are less than the LCO.
  - Various levels of degradation of the electric power system in order of increasing degradation is incorporated in the TS. Whenever the TS allow unrestricted operation to be resumed, such resumption should be contingent on the verification of the integrity and capability of the restored sources.

6

Operational Requirements (Cont.)

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

- To Ensure that NPP is in Safe Operating Mode whenever the Available Electric Power Sources are Less than TS LCO. Continued Power Operation Contingent on the following:
  - Reliability, Availability, and Capability of Remaining Sources
  - Required Maintenance Activities do not Further Degrade the Power System or Jeopardize Plant Safety
  - Continued Compliance With Required Actions in TS

7

Current Beyond Design Basis Requirements - Station Blackout, Security-Related Events

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

- **10 CFR 50.54, Conditions of licenses- Section (hh)(2)**
- Each licensee shall develop and implement guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with loss of large areas of the plant due to explosions or fire
- **10CFR 50.63 Loss of all alternating current power**
- (a) *Requirements*. (1) Each light-water-cooled nuclear power plant licensed to operate must be able to withstand for a specified duration and recover from a station blackout as defined in § 50.2. The specified station blackout duration shall be based on the following factors:
- (i) The redundancy of the onsite emergency ac power sources;
- (ii) The reliability of the onsite emergency ac power sources;
- (iii) The expected frequency of loss of offsite power; and
- (iv) The probable time needed to restore offsite power.

8

Current Beyond Design Basis Requirements Station Blackout (Cont.)

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

- (2) The reactor core and associated coolant, control, and protection systems, including station batteries and any other necessary support systems, must provide sufficient capacity and capability to ensure that the core is cooled and appropriate containment integrity is maintained in the event of a station blackout for the specified duration.
- The capability for coping with a station blackout of specified duration shall be determined by an appropriate coping analysis. Licensees are expected to have the baseline assumptions, analyses, and related information used in their coping evaluations available for NRC review.

9

Current Beyond Design Basis Requirements Station Blackout (Cont.)

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

- **Reg. Guide 1.155, Station Blackout**
  - Specifies a method acceptable to the NRC staff for complying with 10CFR50.63
  - Twenty four pages of detailed guidance
  - EDG Target Reliability Levels
  - Restoration of Offsite Power
  - Ability to Cope with a Station Blackout
  - Quality Assurance Guidance for Non-Safety Systems and Equipment

10

Current Beyond Design Basis Requirements Station Blackout (Cont.)

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

- **NUMARC 87-00**
  - Guidelines and Methodologies for Implementing the Nuclear Management an Resources Council (NUMARC) Station Blackout Initiatives
  - Detailed Guidance, Examples, Topical Reports, and Questions & Answers
  - Endorsed by Reg. Guide 1.155 as Acceptable Guidance for Compliance to 10CFR50.63

11

Beyond Design Basis Requirements Fukushima Lessons Learned Action Items

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

- **Industry Response - NRC Mitigating Strategies Order (EA 12-049)**
  - Provides a diverse and flexible means to prevent fuel damage while maintaining containment function in beyond design basis external event conditions resulting in an:
  - Extended Loss of AC Power, and
  - Loss of Normal Access to the Ultimate Heat Sink

  Objective:
  - Establish an essentially indefinite coping capability by relying upon installed equipment, onsite portable equipment, and pre-staged offsite resources

12

Beyond Design Basis Requirements
Fukushima Lessons Learned Action Items (Cont.)

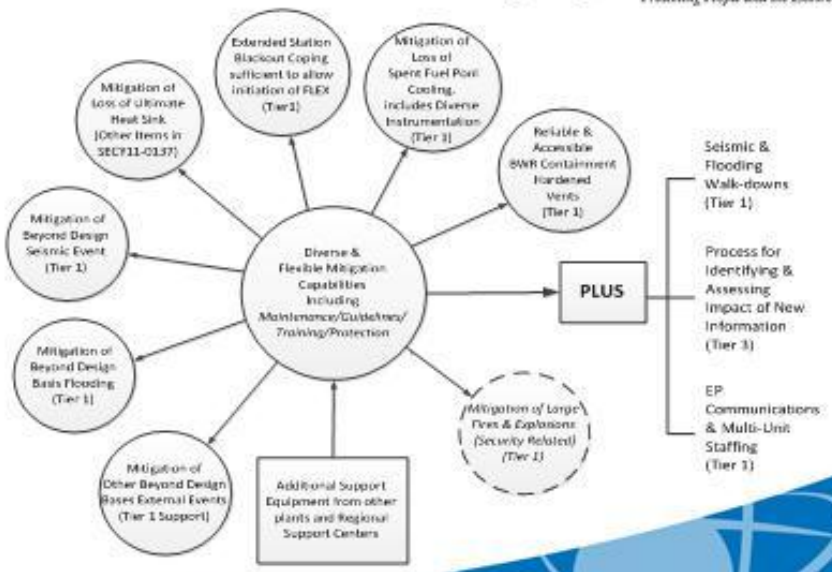
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **FLEX employs a three phase approach:**
  - **Phase 1 - Initially cope by relying on installed plant equipment,**
  - **Phase 2 - Transition from installed plant equipment to onsite FLEX equipment,**
  - **Phase 3 - Obtain additional capability and redundancy from offsite equipment until power, water, and coolant injection systems are restored or commissioned.**
- **Diverse and flexible to enable deployment of the strategies for a range of initiating events and plant conditions**

13

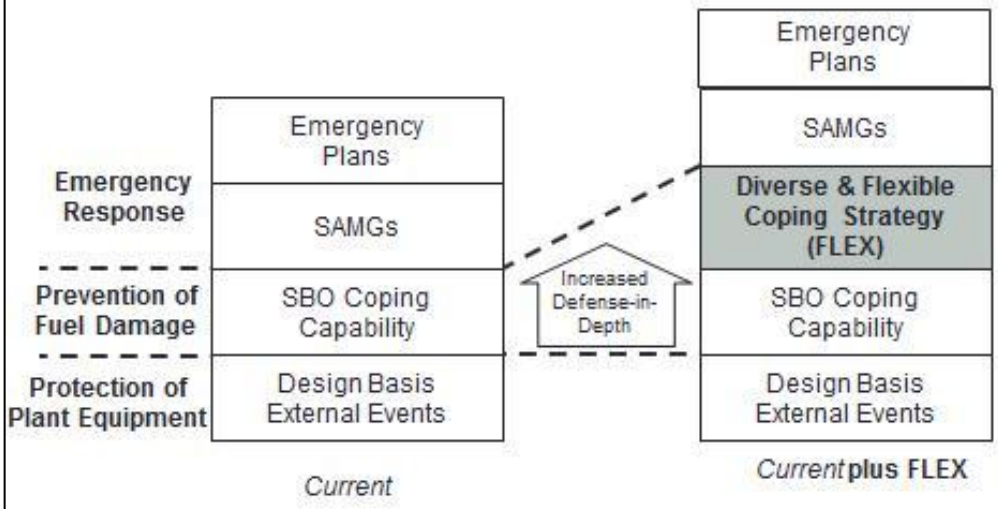
Beyond Design Basis Requirements
Fukushima Lessons Learned Action Items (Cont.)

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



14

Beyond Design Basis Requirements
Fukushima Lessons Learned Action Items (Cont.)



15

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

16