PUBLIC SUBMISSION

SUNI Review Complete
Template=ADM-013
E-RIDS=ADM-03

ADD: Stanley Gardocki, Liliana Ramadan, Mary Neely
Comment (1)
Publication Date: 1/19/2021
Citation 86 FR 5267

As of: 2/19/21 4:02 PM
Received: February 17, 2021
Status: Pending_Post
Tracking No. 1k5-9lul-8vpy
Comments Due: February 18, 2021
Submission Type: API

Docket: NRC-2020-0279
DG-1303 Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants

Comment On: NRC-2020-0279-0001
Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants

Document: NRC-2020-0279-DRAFT-0003
Comment on FR Doc # 2021-00940

Submitter Information

Name: Gurcharan Matharu
Address:
110 Harbour Town Court
New Orleans, LA, 70131
Email: Lawnak90@gmail.com

General Comment

COMMENTS ON DRAFT REGULATORY GUIDE DG-1303 Proposed Revision 5 to Regulatory Guide 1.9

The proposed revision of the Regulatory Guide (Revision 5) endorses, with supplements and clarifications, IEEE Std 387-2017, IEEE Standard for Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations, and IEEE Std 2420-2019, IEEE Standard for Combustion Turbine-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations. The IEEE Standards 387 and 2420 frequently use the term accident without considering the regulatory implications and differences between the terms accident and Design Basis Event (DBE). The two Standards are also not in alignment with the intent of upper tier IEEE Standard 308, Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations. IEEE 308 is indirectly incorporated into Regulation via Section 50.55a(h), Codes and Standards, of 10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities as discussed below. The IEEE Working Groups, responsible for these standards, are currently reviewing the intent of the terms used in the Standards and will make changes based on the intent and technical basis for the specific use of the terms and consistency with Regulation.

The comments in the attached document are seeking clarification on the use of terms accident and DBE as used in the Draft RG DG-1303 and conformance to applicable Regulations

Attachments

EDG Trips Bypass Comments for NRC Staff on Draft Guide 1303)

COMMENTS ON DRAFT REGULATORY GUIDE DG-1303
Proposed Revision 5 to Regulatory Guide 1.9

The proposed revision of the Regulatory Guide (Revision 5) endorses, with supplements and clarifications, IEEE Std 387-2017, "IEEE Standard for Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations", and IEEE Std 2420-2019, "IEEE Standard for Combustion Turbine-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations". The IEEE Standards 387 and 2420 frequently use the term 'accident' without considering the regulatory implications and differences between the terms 'accident' and 'Design Basis Event' (DBE). The two Standards are also not in alignment with the intent of upper tier IEEE Standard 308, "Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations". IEEE 308 is indirectly incorporated into Regulation via Section 50.55a(h), "Codes and Standards," of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" as discussed below. The IEEE Working Groups, responsible for these standards, are currently reviewing the intent of the terms used in the Standards and will make changes based on the intent and technical basis for the specific use of the terms and consistency with Regulation.

The comments below are seeking clarification on the use of terms "accident" and "DBE" as used in the Draft RG DG-1303.

BACKGROUND

Definitions in NRC Documents:

Design-basis events: 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," provides the following definition:

> Design-basis events are defined as conditions of normal operation, including anticipated operational occurrences, design-basis accidents, external events, and natural phenomena for which the plant must be designed to ensure functions (b)(1)(i) (A) through (C) of this section [see above items 1, 2 and 3 under definition of safety-related SSCs]
>
> Specifically:
>
> (1) the integrity of the reactor coolant pressure boundary;
> (2) the capability to shut down the reactor and maintain it in a safe shutdown condition; or
> (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the applicable guideline exposures set forth in 10 CFR 50.34(a)(1) or 10 CFR 100.11 ["Determination of Exclusion Area, Low Population Zone, and Population Center Distance"] of this chapter, as applicable.

Anticipated Operational Occurrences: Accident analyses section of plant safety analysis provides guidance on categorization of events according to frequency of occurrence. Each initiating event is categorized as either an anticipated operational occurrence (AOO) or as a postulated accident. AOOs, as defined in Appendix A to 10 CFR Part 50, are those conditions of normal operation that are expected to occur one or more times during the life of the nuclear power unit.

The Standard Review Plan (NUREG 0800) provides some examples of AOOs in pressurized-water reactor (PWR) and boiling-water reactor (BWR) designs.

The Regulation at 10 CFR 50 Appendix A General Design Criteria (GDC) cited in the RG require onsite power systems for mitigating the consequences of accidents and anticipated operational occurrences. Based on the definitions above, the onsite power system is required to mitigate the consequences of DBEs.

REGULATORY BASES:

General Design Criterion (GDC) 17, “Electric power systems,” of Appendix A, ”General Design Criteria for Nuclear Power Plants,” to Title10, Part 50, of the Code of Federal Regulations (CFR) states in part:

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.

Section 50.55a, “Codes and Standards,” of 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” requires in 10 CFR 50.55a(h) that protection systems for plants with construction permits issued after January 1, 1971, but before May 13, 1999, must meet the requirements stated in either IEEE Std. 279, “Criteria for Protection Systems for Nuclear Power Generating Stations,” or IEEE Std. 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations.” For nuclear power plants with construction permits issued before January 1, 1971, protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std 603-1991. The safety systems for plants with construction permits issued after May 13, 1999, must meet the requirements of IEEE Std. 603-1991.

IEEE Std. 603-1991 Section 1.2 “Application” states in part that the safety system criteria established herein are to be applied to those systems required to protect the public health and safety by functioning to prevent or mitigate the consequences of design basis events. [Note LOOP is a DBE]

Section 2 “Definitions”:

design basis events - Postulated events used in the design to establish the acceptable performance requirements for the structures, systems, and components.
safety system - A system that is relied upon to remain functional during and following design basis events to ensure: (a) the integrity of the reactor coolant pressure boundary, (b) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (c) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10CFR100 guidelines.

Appendix A of IEEE Std. 603-1991 states the following:

A5. Other Auxiliary Features. Included in the design of most safety systems are components and equipment whose primary function is to increase the availability or reliability of the safety system without directly performing a safety function. These components include, but are not limited to, equipment protection devices, built-in test equipment, isolation devices, etc., as shown in Fig 3. As described in 5.12, these portions of the safety system shall meet only those requirements in this standard required to ensure that they do not degrade the safety system below an acceptable level. Examples of safety system criteria that such portions might not have to meet are operating bypass, maintenance bypass, and bypass indication.

To illustrate the application of these criteria, protective relaying on a Class 1E bus is considered. One function of this protective relaying is to increase the availability and reliability of the Class 1E power system, but from the safety system viewpoint, the essential function is to not cause a spurious tripping when safety system operation is required. Performance of this essential function is the one that falls under the criteria of this standard; requirements for the function of increasing the availability and reliability of the Class 1E power system are contained in IEEE Std 308-1980.

IEEE 308-1980 Section 5.2 states the following:
Relationship Between the Safety System and Class 1E Power System. Those portions of the Class 1E power system that are required to support Safety Systems in the performance of their safety functions shall meet the requirements of IEEE Std 603-1980. In addition, those other normal components, equipment, and systems (that is, overload devices, protective relaying, etc.) within the Class 1E power system that have no direct safety function and are only provided to increase the availability or reliability of the Class 1E power system shall meet those requirements in IEEE Std 603-1980 to assure that those components, equipment, and systems do not degrade the Class 1E power system below an acceptable level.

Components, equipment, or systems required to provide some protective action, such as containment integrity protection, or utilized to provide isolation protection are covered by all of the requirements of IEEE Std 603-1980.

NRC IE Circular 77-16, “Emergency Diesel Generator Electrical Trip Lock-Out Features,” December 13, 1977, states in part:

All holders of operating licenses or construction permits should assure that the appropriate D/G protection trip circuits are provided with automatic by-pass features that prevent them from negating automatic starting or tripping of D/Gs during fast start or emergency operations.

COMMENT 1 Terminology for onsite power systems during DBEs.

Draft RG DG-1303, Section A “INTRODUCTION” subtitle “Purpose” states in part “This guidance helps ensure that the onsite emergency AC power sources: are qualified; have sufficient capacity, capability, independence, and testability; and have the necessary reliability and availability for design basis events (DBEs)”. The “Background” section of the RG states in part “Onsite emergency AC power sources are used to supply power to safety-related equipment or equipment important to safety for all operational events and during accident conditions. These two statements seem to be in conformance with Regulation. Other sections of

the Draft RG limit the onsite power system requirements for Loss of Offsite Power (LOOP) and LOOP concurrent with accident conditions, for example:

a. This "Background" Section provides further criteria for AC power requirements and states "(2) provide power promptly to engineered safety features if a loss of offsite power (LOOP) and an accident occur at the same time, and …
b. Section 2,4 states "Operation of the EDG in parallel with the preferred power source (test mode) and capability to respond to a concurrent accident, LOOP, or combined accident and LOOP signal during this condition.

The LOOP condition had been historically viewed as the incapable/unavailable (degraded voltage or tripped) even though the impact on the NPP varied on its impact, because of the design variations, for causing prompt/delayed turbine runback, plant trip, or unaffected operation. The EDG was designed to have a start on a LOOP as a defense in depth measure to preserve highly reliable power for both trains to have emergency core cooling capability.

Please clarify that the performance requirements for onsite power systems are limited to DBE, AOO, LOOP as well as LOOP with accident conditions. Specifically identify the sections where the usage of word "accident" is in conformance with applicable regulations.

COMMENT 2 Bypass non-critical trips during emergency mode of operation.

The RG states "The primary function of the other protective trips is to increase the availability or reliability of the EDGs. However, these trips could interfere with successful functioning of the EDGs during accident conditions. Past operating experience has shown that spurious operation of a trip circuit can adversely impact EDG operation or reliability. Consequently, it is important to take measures to ensure that spurious actuation of these other protective trips does not prevent the EDGs from performing their safety function during the accident mode of operation." The Draft RG seems to endorse the current recommendation in IEEE Standards 387 and 2420.

Section 4.5.4 "Protection" of IEEE Standard 387 -2017 states the following:

The diesel-generator unit shall be automatically tripped on an engine overspeed and generator differential overcurrent. Protective features, other than engine overspeed and generator differential current, shall be the following:

> Blocked from automatically tripping the diesel-generator unit during an accident condition safety injection actuation signal (SIAS) and combined SIAS with loss of offsite power (LOOP) and shall be annunciated in the plant control room, or…

Any EDG start, other than planned testing, needs to be considered as an emergency start (starting in Synchronous mode -not DROOP, with non-essential protection bypassed) because most EDG control systems do not have the intelligent control systems to detect LOCA condition and revert to emergency mode to provide emergency cooling in the first 2-3hrs. of a LOCA.

The discussion below delineates non-accident related requirements when the onsite power system may be required to perform safety related functions. Please provide clarification that the guidance provided in the draft RG for bypassing non-critical trips, when the DG is operating in response to an emergency operation demand conforms to the regulatory bases discussed above for all DBEs, AOOs, and accidents.

DISCUSSION

The purposes of onsite electric power systems are (1) to provide power promptly to engineered safety features if a loss of offsite power and an accident occur during the same time period and (2) to provide power to equipment needed to maintain the plant in a safe condition if an extended loss of offsite power occurs.

Loss of offsite power (LOOP) can have a major negative impact on a plant's ability to achieve and maintain safe shutdown conditions. Risk analyses have shown that LOOP can represent a majority of the overall risk at some plants. There are significant number of industry studies that indicate the increasing trend in LOOP events during critical operations and during shutdown operations. A LOOP event during shutdown operations may result in loss of shutdown cooling which may be critical during mid-loop operations when RCS inventory is reduced. (Examples - See Table 2.8 “Cold-Shutdown and Refueling Events Analyzed Using ASP Methods, by Vendor” in NUREG-1449 “Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States” An EDG required to operate during a LOOP event during plant shutdown will NOT get an accident signal.

The Regulatory Requirement under GDC 17 requires 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 (AOOs) and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents. LOOP events are included in this requirement.

The Regulatory Requirement under 10 CFR 50.55a(h) via IEEE – 603-1991 clearly requires that spurious trips should be precluded when a safety system is required to perform an essential function. *(Operating history has shown that some features implemented for protection of equipment have resulted in spurious trips).* [EDG operation in emergency mode would be classified as “a safety system is required to perform an essential function”].

SHUTDOWN RISK

Shutdown operations in both PWRs and BWRs introduce a different spectrum of vulnerabilities that may not be applicable during at power operations. A shutdown plant is in a safe condition as long as certain key safety functions are maintained and managed adequately. Those functions are:

- decay heat removal,
- inventory control,
- power availability,
- reactivity control, and
- containment closure capability

Loss of AC power can pose significant challenges during following modes of operation:

Mid-loop Operation: Mid-loop conditions exist whenever the RCS water level is below the top of the flow area of the hot legs at the junction with the reactor vessel. PWR only.

Operation with Potential to Drain Reactor Vessel: A planned maintenance evolution that if it is not conducted properly can lead to a loss of inventory event.
Reduced Inventory Operation: An RCS inventory condition that results in a reactor vessel water level lower than three feet below the reactor vessel flange. Mid-loop is a subset of reduced inventory. (PWR only).

During extended shutdown conditions (Refueling), the plant operators have a single onsite source available in accordance with the Technical Specification requirements. A spurious trip of an operating DG during shutdown can take several hours to trouble shoot and restore in accordance with plant procedures.

AC Power During Shutdown
AC power is required during shutdown conditions to maintain cooling to the reactor core and spent fuel pool, to transfer decay heat to the heat sink, to achieve containment closure when needed, and to support other important functions. Planning and control of outage activities on AC power sources can significantly reduce risk by providing a DEFENSE IN DEPTH that is commensurate with the plant condition. Since one offsite source and one onsite source may be under maintenance, to reduce risk related to an event that off-site and emergency AC power is unavailable, some licensee make arrangements for temporary hookups for AVAILABILITY of alternate AC power. A spurious trip of an operating EDG during shutdown can take several hours to trouble shoot and restore in accordance with plant procedures. In view of the safety significance of onsite AC power systems during plant shutdown, the NRC has approved license amendment requests to allow major maintenance of onsite DGs during online plant operation instead of shutdown conditions.

The following individuals have contributed to these observations:

Gurcharan Singh Matharu (Lawnak90@gmail.com)
Thomas Koshy (Thomask@dnfsb.gov)
Roy Mathew (r.mathew@verizon.net)

February 17, 2021