Qualitative Assessment

Quality, Reliability, and Common Cause Failure Susceptibility

Developed For

Engineering Change 00001

Replacement of EDG Voltage Regulator Motor Operated Potentiometer (MOP) With Digital Reference Adjuster (DRA)

Revision 3

Table of Contents

1. Activity Identification

The proposed activity will replace the existing Emergency Diesel Generator (EDG) voltage regulator analog motor-operated potentiometer (MOP) with a digital reference adjuster (DRA). The function of the MOP is to provide the operating voltage setpoint for the EDG voltage regulator. The DRA will perform the exact same function as the MOP, that is, provide a variable resistance to establish the EDG voltage regulator operating voltage.

The EDG system is classified as nuclear safety related and is considered an accident mitigation system.

2. Design Function Identification

UFSAR Section 8.3.1.1.7, Standby Power Supplies, states, in part:

> *In addition to the normal power supplies ... redundant 4160 Volt Essential Auxiliary Power Systems of each unit ... are furnished with power from two independent diesel-electric generating units separately housed in Category 1 structures which are a part of the Auxiliary Building.*

Thus, the UFSAR described design function of the EDGs is to provide power to the 4160 Volt Essential Auxiliary Power Systems in the event the normal source of power is compromised.

Although not specifically described in the UFSAR, failure of the MOP could result in subsequent failure of the EDG to regulate voltage. Therefore, the MOP has an impact on an UFSAR described design function.

The DRA will accomplish the exact same function as the MOP. The proposed activity does not create any new design functions to be performed that were not part of the original plant design.

3. Failure Mode Comparison

There are three paths to failure for both the MOP and DRA:

A. Failure due to an internal defect
B. Failure as a result of power loss
C. Failure resulting from environmental factors

Each potential failure mode is evaluated below and a comparison made between the failure modes of the existing MOP and the new DRA.

A. Internal Defect

Failure of the existing MOP due to an internal mechanical/electrical defect may cause the EDG output voltage to:

1) Fail as-is due to a failure of the servo motor to change the position of the wiper
2) Fail to a steady, unintended output state due to an open winding or shorted winding
3) Fail to an erratic output due to dirt or corrosion on the coil or wiper

Similarly, failure of the DRA due to an internal electrical or software design defect may cause the EDG output voltage to:

1) Fail as-is
2) Fail to a steady, unintended voltage (setpoint cannot be changed)
3) Fail to an erratic output state when the setpoint is changed

Inspection of the above failure states reveals the DRA failure modes resulting from an internal defect are bounded by the potential failure modes of the MOP and the end result is the same at the system level (potential inoperability of affected EDG).

Note that failure of the DRA to a steady, unintended voltage (2 above) would not necessarily result in EDG inoperability. Provided the resulting DRA output resistance places the EDG voltage within the Technical Specifications requirements (≥ 3750 V and ≤ 4300 V), the EDG is considered operable even upon failure of the DRA. The DRA adjustable output range equates to an EDG operating voltage range of 3750 V to 4600 V. Therefore, only failure of the DRA that results in an EDG voltage regulator setpoint above 4300 V would result in an inoperable EDG as illustrated in Figure 1 below[1].

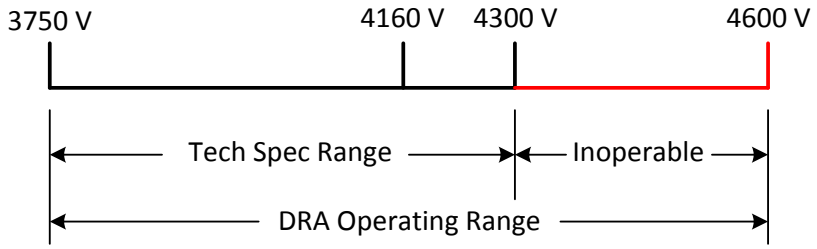

Figure 1

B. Loss of Power

The failure modes on loss of power to the DRA and MOP are different. The MOP maintains its output resistance without regard to control circuit power. The DRA requires power to retain the resistance setpoint. Loss of power to the DRA will cause the output to switch to maximum resistance and thus provide the 4600 V setpoint to the AVR.

[1] Note that the EDG Automatic Voltage Regulator (AVR) adjustable range is 4160 V ±10% (3744 V to 4576 V).

Technical Specifications Surveillance Requirement (SR) 3.8.1.2 necessitates verification that each EDG starts from standby conditions and achieves steady-state voltage ≥ 3750 V and ≤ 4300 V. Thus, loss of power to the DRA would result in inoperability of the affected EDG. To comply with the single failure criteria, each EDG (and associated DRA) is supplied with separate safety related control power. Therefore, the effects of loss of power to the DRA would be limited to one EDG. Additionally, there are failures currently evaluated in the UFSAR that will result in complete loss of EDG system function [3.d]. Thus, while response to loss of DRA power is different, the result at the EDG system level remains bounded by EDG failures previously evaluated in the UFSAR.

C. Environmental Factors

The DRA has been qualified for temperature, humidity, and seismic stressors using the methods provided in EPRI TR-107330 as endorsed by RG 1.209 and to meet electromagnetic compatibility (EMC) requirements in accordance with RG 1.180 [17][6][7]. EMC testing included both the module's susceptibility to the existing environment and the module's impact on surrounding equipment through emissions. The DRA qualification bounds the environmental conditions expected in the final installed location. Functional testing activities performed after each stage of qualification testing ensure the system will operate properly under conditions specified in the applicable standards for EMC, environmental, and seismic testing.

Each EDG is separated and isolated (physically and electrically) further reducing the vulnerability of a DRA common cause failure (CCF) resulting from environmental factors. Based on this assessment, it can be reasonably concluded that an increase in EDG malfunction likelihood due to environmental variations or seismic stressors is unlikely.

4. Failure Results

The worst-case result of single MOP or DRA failure would be inoperability of the affected EDG. This result is bounded by the results of EDG system malfunctions currently described in the UFSAR.

A postulated simultaneous failure of the DRA on both EDG trains (due to a hardware or software CCF) may result in failure of both EDG trains. A loss-of-offsite-power (LOOP) concurrent with simultaneous failure of both EDG trains would result in a station blackout (SBO), a condition previously described in the plant safety analysis. Therefore, even in the unlikely event of simultaneous failure of the DRA across EDG divisions during a LOOP, the plant remains in an analyzed condition. Note that this particular scenario would require two concurrent but unrelated CCFs - that is, a CCF causing simultaneous failure of the DRA

concurrent with a LOOP which is also considered a CCF as each nuclear plant has two independent sources of offsite power.

Consequently, the result of a DRA malfunction, whether affecting a single EDG or multiple EDGs, is bounded by EDG malfunction results previously described in the UFSAR.

5. Assertions

A. Design Attributes

a. Quality and Reliability

An accepted measure of DRA reliability is by confirming the device complies with current industry and regulatory standards. A commercial grade dedication of the DRA was performed per the requirements of the following industry standards:

1. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," dated October 1996.
2. EPRI TR-107339, "Evaluating Commercial Digital Equipment for High Integrity Applications, A Supplement to EPRI Report TR-106439," dated December 1997.
3. USNRC Standard Review Plan, NUREG-0800, Chapter 7, Instrument and Controls Branch (HICB) Technical Position HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," June 1997.
4. IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," December 17, 2003.
5. IEEE 323-1983, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations."
6. EPRI TR-100516, "Nuclear Power Plant Equipment Qualification Reference Manual," 1992.
7. IEEE 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
8. EPRI TR-102323-R2, "Guidelines for Electromagnetic Interference Testing in Power Plants, Revision 2".
9. U.S. NRC Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, 2003.

NRC staff has determined that EPRI TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications and meets the requirements of 10CFR Part 21. Further, the staff concluded that when digital equipment is dedicated using the methods described in TR-106439, it

may be considered equivalent to digital equipment designed and manufactured under a 10CFR Part 50, Appendix B quality assurance program. [28] Thus, adherence to the above industry and regulatory standards provides a high degree of equipment quality and reliability.

b. Simple Architecture

The DRA is a relatively simple device with a single function, that is, to provide a static resistance value to the EDG voltage regulator for use in establishing the EDG operating voltage setpoint. With the EDG in the normal mode (safety function) of operation, the DRA accepts no input signals (input signals are blocked). With the EDG in the manual (non-safety function) mode of operation, the DRA will accept two separate input signals (voltage raise or lower) which allows an operator to vary the EDG output voltage.

With the EDG in normal mode and the DRA parked at setpoint, the DRA processor continuously loops through seventeen (17) lines of code awaiting user input (voltage raise/lower commands). Aside from the EDG voltage regulator, the DRA does not connect to or interface with any other plant equipment, does not utilize shared resources, nor does the DRA employ network or communication connections.

While in the normal mode of operation, the DRA accepts no inputs, loops through seventeen (17) lines of code, and produces a single static output. As such, the DRA is considered a relatively simple device.

c. Non-Concurrent Triggers

The divisional independence of the EDGs (and corresponding digital reference adjusters) prevents a triggered defect in one division from propagating to the other division, significantly reducing the potential for hardware or software common cause failure simultaneously affecting both EDG trains.

Additionally, each EDG and cabinet containing the DRA is located in its own fully enclosed room thereby significantly reducing the likelihood of a single environmental factor (temperature, humidity, radiation, EMI/RFI, etc.) initiating a CCF of the DRAs across both EDG trains.

Thus, it can be concluded there are no credible concurrent triggers that would initiate a DRA hardware or software CCF simultaneously affecting both EDG trains.

d. Watchdog Timer

The DRA utilizes a hardware version of a watchdog timer that operates internal to the microcontroller. The DRA microcontroller uses a crystal clock to count down a hardware timer. The DRA software generates a pulse to reset the timer before the counter counts

down and the timer expires. As long as the crystal clock continues to oscillate and the software pulses the timer reset, the watchdog timer behaves as if it were built from hardware external to the DRA. This type of watchdog timer design provides the same reliable functionality without the complexity and additional components required to build a purely external watchdog timer (e.g., integrated circuits, resistors, capacitors, and the extra solder joints necessary to assemble these additional components).

Unlike the the DRA watchdog timer, an internal software watchdog timer depends on proper operation of the software to implement the timeout functionality. This type of watchdog timer is generally considered much less reliable, as the software and associated interrupts have to be working correctly for the watchdog timer to function. Failure of the software may not result in failure indication from the watchdog timer.

Timeout of the watchdog timer (typically indicating a processor failure) will force the DRA into an even tighter processing loop that ignores user input. If the watchdog timer senses a failure while the DRA is parked at setpoint, the 4160 V setpoint will be maintained. A failure sensed by the watchdog timer when the DRA is away from setpoint would be indicated by an extinguished lamp in the main control room complex and at the local control panel of the affected EDG.

e. Diverse Indication of Failure

The DRA is maintained at setpoint (4160 V) except when paralleled to the grid (e.g., during normal monthly surveillance). As long as the DRA remains at setpoint, a lamp located in the main control room complex and a lamp located at each local EDG control panel will be lit. If the DRA moves away from setpoint, these lamps will extinguish. Control room operators are required by procedure to perform a control board walk down twice a shift (once during shift turnover and once during mid-shift). Since these lamps would normally be lit, an extinguished lamp would alert an operator of the movement away from setpoint and potential failure of the DRA.

As stated in Section 3.A above, failure of the DRA can be classified into one of the following three categories:

1) Fail as-is
2) Fail to a steady, unintended output state
3) Fail to an erratic output state when the setpoint is changed

Failures of the first category (as-is) could occur without any external indication, causing the unit to become unresponsive to user input (e.g., watchdog timer timed out due to processor failure), but would leave the DRA and thus the EDG at operating setpoint. This condition would be detected during maintenance or monthly surveillance. Failures of

the second (steady, unintended output) and third (erratic output) categories would result in spurious EDG system behavior that would be readily apparent to the control room operators.

f. Electromagnetic Compatibility (EMC) Compliance

The DRA was verified to be in compliance with radiated and conducted emissions levels specified in EPRI TR-102323, Revision 2 and NRC Regulatory Guide 1.180, Revision 1. Additionally, the DRA was verified to maintain a stable output resistance during application of radiated, conducted, and surge electromagnetic interference (EMI) at the levels specified in EPRI TR-102323, Revision 2 and NRC Regulatory Guide 1.180, Revision 1. Operator input to the DRA was verified to remain functional (raise resistance, lower resistance, or return to preposition settings, as commanded as well as remain at setpoint when no change is requested) during application of continuous EMI such as radiated or conducted emissions [12].

g. Hardware Common Cause Failure (CCF)

The commercial grade dedication process, based on industry and regulatory accepted practices, ensures the DRA possesses quality commensurate with the existing MOP. The DRA has been analyzed to perform properly within the EDG environment during normal and accident conditions. This analysis included temperature, humidity, seismic, radiation, and EMI/RFI. The DRA will be installed in the voltage regulator excitation systems of both EDG trains. Each EDG and its DRA is separated and isolated (physically and electrically) further reducing the vulnerability of a hardware CCF due to environmental factors. There are no physical or electrical connections between EDG trains preventing a triggered defect in one division from propagating to the other division, providing sufficient assurance that DRA hardware CCF between EDG trains is sufficiently unlikely.

Based on this assessment, it can be reasonably concluded that a DRA hardware CCF resulting in simultaneous failure of both EDG trains is no more likely than other potential common cause failures such as maintenance or calibration errors that are not considered in the UFSAR.

h. Software Common Cause Failure (CCF)

The DRA has been evaluated and qualified to perform its intended function based on industry and regulatory accepted practices. The device has been fully qualified to operate in nuclear safety related applications. The DRA software is relatively simple and has been thoroughly vetted based on the requirements of EPRI TR-106439 and IEEE 7-4.3.2.

Conducting the commercial grade dedication in accordance with EPRI TR-106439 and in compliance with IEEE 7-4.3.2 establishes software quality and signifies the likelihood of a software defect is low. As part of the commercial grade dedication process, a critical digital review based on the requirements of EPRI TR-107339 was performed, including an independent review of the DRA software design which included a line-by-line review of the relevant source code [9]. The commercial grade dedication process, which included the independent software review, demonstrated the software is equivalent to software developed under an Appendix B quality assurance program. Low software defect likelihood together with the divisional independence of the EDGs, which prevents a triggered defect in one division from propagating to the other division, significantly reduces the potential for SCCF between EDG trains.

Based on the relative simplicity of the DRA, the robust review of the device software, and the divisional isolation of the EDGs, it is reasonable to conclude that a SCCF simultaneously affecting more than one EDG train is unlikely. Further, there is reasonable assurance that failures due to software are no more likely than other potential common cause failures such as maintenance or calibration errors that are not considered in the UFSAR.

i. Unlikely Series of Events

In the normal mode of operation, the DRA accepts no user inputs and produces a single static output used to establish the EDG voltage regulator output voltage. The effects of a random failure of a single DRA would be limited to the associated EDG. Depending on the failure state, the affected EDG may or may not remain operable (recall that as long as the EDG output voltage is ≥ 3750 V and ≤ 4300 V, the EDG is considered operable).

Absent a coincident LOOP, a CCF that caused simultaneous failure of the DRAs on both EDG trains, to the point where both EDG trains were rendered inoperable, would place the affected nuclear unit in Technical Specifications Limiting Condition for Operation (LCO) 3.8.1.E requiring restoration of one EDG to operable status within 2 hours or initiate unit shutdown. The plant would remain in an analyzed condition.

A postulated DRA CCF simultaneously rendering both EDG trains inoperable coincident with a LOOP would result in a SBO, a previously analyzed plant condition.

The scenario that would place the plant in an unanalyzed condition would require following unlikely series of events:

- A CCF causing simultaneous failure of the DRAs on both EDG trains resulting in loss of both EDGs (note that there are DRA failure modes that would not result in EDG

inoperability; so not only would the DRA have to fail, it would have to fail in such a manner the EDG would be rendered inoperable)

- A concurrent but unrelated CCF causing loss of both offsite power sources to the plant (i.e., a LOOP)
- A concurrent anticipated operational occurrence (AOO) or postulated accident (PA)

The likelihood of an anticipated operational occurrence (AOO) or postulated accident (PA), with a CCF resulting in a concurrent LOOP and with another unrelated but concurrent CCF from a design defect in the DRA is considered remote. Furthermore, grid stability is such that loss of the plant due to an internally generated trip is not likely to have a significant impact on the grid and offsite power is expected to remain available [3.a]. Therefore, while a LOOP concurrent with a CCF of both EDG trains may be worth evaluating, it is not necessary to consider a LOOP concurrent with a PA or AOO that is also concurrent with a CCF of both EDGs as this would be the result of an extremely unlikely series of events.

B. Quality Design Process

An accepted measure of quality of the DRA is by confirming the device complies with appropriate sections of current industry and regulatory standards. A commercial grade dedication of the DRA was performed based on the requirements of the following industry standards:

10. EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” dated October 1996.
11. EPRI TR-107339, “Evaluating Commercial Digital Equipment for High Integrity Applications, A Supplement to EPRI Report TR-106439,” dated December 1997.
12. USNRC Standard Review Plan, NUREG-0800, Chapter 7, Instrument and Controls Branch (HICB) Technical Position HICB-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” June 1997.
13. IEEE Standard 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” December 17, 2003.
14. IEEE 323-1983, “IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations.”
15. EPRI TR-100516, “Nuclear Power Plant Equipment Qualification Reference Manual,” 1992.

16. IEEE 344-1987, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.”
17. EPRI TR-102323-R2, “Guidelines for Electromagnetic Interference Testing in Power Plants, Revision 2.”
18. U.S. NRC Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Revision 1, 2003.

NRC staff has determined that EPRI TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications and meets the requirements of 10 CFR Part 21. Further, the staff concluded that when digital equipment is dedicated using the methods described in EPRI TR-106439, it may be considered equivalent to digital equipment designed and manufactured under a 10 CFR Part 50, Appendix B quality assurance program [5]. Thus, adherence to the above industry and regulatory standards provides a high degree of equipment quality and reliability.

Per NEI 01-01 section 5.3.1, dependability is used in relation to quality and likelihood of failures. Dependability reflects the fact that reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features. For digital systems, the likelihood of software-related failure is minimized using the same basic approach of controlling the design, implementation, operation, and maintenance processes. Compliance with industry standards and regulatory requirements coupled with tests, evaluations, and reviews is used to assure a low likelihood of failure.

Regulatory Guide 1.152 acknowledges that safety system designs may use computers that were not specifically designed for nuclear power plant applications. Clause 5.4.2 of IEEE Standard 7-4.3.2-2003 provides general guidance for commercial grade dedication. However, Regulatory Guide 1.152 states that IEEE Standard. 7-4.3.2-2003 Annex C, “Dedication of Existing Commercial Computers,” has not received NRC endorsement because it provides inadequate guidance. EPRI Report TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” issued October 1996 contains adequate guidance, which the NRC has endorsed in its 1997 Safety Evaluation Report (ML092190664) [5].

The approach employed by the commercial dedication process satisfies the requirement in Clause 5.4.2 of IEEE 7-4.3.2-2003 as endorsed by Regulatory Guide 1.152 by use of EPRI TR-106439 and EPRI NP-5652.

The DRA is a commercial-off-the-shelf product. The DRA will be used directly in the application for which it was designed. Dedication of hardware and software for use in safety related applications was performed in accordance with EPRI TR-106439.

Based on the qualification activities and the results of the critical digital review as documented in the commercial grade dedication reports, including an operating history survey, the DRA is considered a highly reliable device on a level equal to, or exceeding, the MOP [9][10]. Thus, there is reasonable assurance that the dependability of the EDG system will not be adversely affected by installation of the DRA.

C. Operating Experience

As part of the commercial grade dedication, a review of the DRA operating history was performed to assess the overall quality of the product and its acceptability for use in nuclear safety related applications. The operating history was evaluated by surveying a sample of DRA end users. Reliable performance of the DRA in commercial applications supports its use in nuclear power plant applications.

Operating history was obtained for a total of 15 units from three separate users. All units included in the survey had been in service for a minimum of five years culminating in 113 operating years. Two of the three users consider their application to be critical to operations. These users are more likely to have experienced failures and are expected to have a more thorough record of past failures. The surveyed operating history is considered relevant to nuclear power plant applications. All users surveyed are using the DRA in a generator excitation system.

The results of the operating history review suggest the quality of the DRA is consistent with quality equal to or exceeding other non-digital setpoint adjustment devices (e.g., motor-operated potentiometers) [9].

6. Documentation of Evidence

Elements of the commercial grade dedication documentation provide evidence of the qualitative assessment arguments presented above. The documents listed below detail the environmental qualification of the DRA (including temperature, humidity, seismic, radiation, heat load, and EMI/RFI), quality processes employed, and DRA operating history.

1. CGD-3782, Revision 3; *XYZ Nuclear Plant – EDG Excitation System Replacement Project - Failure Modes and Effects Analysis*
2. CGD-3918, Revision 0; *XYZ Nuclear Plant EDG Excitation System Replacement Project EMC Qualification Report*
3. CGD-3780, Revision 1; *Critical Digital Review of the Digital Reference Adjustor (DRA)*

4. CGD-2813, Revision 1; *Summary of the Generic Qualification of the Microprocessor-Based Digital Reference Adjustor (DRA)*
5. CGD-3885, Revision 0; *XYZ Nuclear Plant EDG Excitation System EQ Report*
6. CGD-3867, Revision 0; *XYZ Nuclear Plant EDG Excitation System Replacement Project Seismic Qualification Report*
7. CGD-3954, Revision 0; *Digital System Hazards Analysis for the XYZ Nuclear Plant EDG Excitation System Replacement Project*

7. Rationale

The assertions made by this assessment are that failure of the DRA is no more likely than failure of the existing MOP it is replacing and a CCF of the DRA due to either hardware or software is no more likely to happen than CCFs caused by maintenance activities which are considered so unlikely they are not considered in the UFSAR. These assertions are based on evidence provided in the DRA commercial grade dedication quality documentation and the supporting arguments made within this qualitative assessment.

In addition, motor-operated potentiometers have been problematic at a number of installations, often because the MOP is considered the weakest link in any voltage regulating system [16]. The problem is typically a case of having a "dirty pot," caused by oxidation of the resistive element or fouling with foreign material (such as dust or dirt), resulting in erratic voltage/volts-ampere reactive (VAR) swings.

Based on the conclusion that the quality and reliability of the DRA is commensurate with that of the MOP and CCF of the DRA is considered unlikely, coupled with the failure history of the existing MOP, the proposed activity will not decrease EDG system reliability and will likely result in a net increase in EDG reliability.

8. Conclusion

The EDG is not an initiator of any accidents described in the UFSAR. Nor will the proposed activity create a scenario where the EDGs could become an accident initiator. Thus, replacement of the EGD voltage regulator MOP with the DRA will not cause an increase in accident frequency or create the possibility for an accident of a different type ***(10 CFR 50.59 Criteria 1 and 5, respectively)***.

Based on the evidence and supporting documentation provided within this qualitative assessment, it is reasonable to conclude the DRA possesses quality and reliability commensurate with the MOP. As a result, replacement of the MOP with the DRA will not result in a more than minimal increase in EDG malfunction likelihood ***(10 CFR 50.59 Criterion 2)***.

Finally, the potential for hardware and software CCF was evaluated with installation of the DRA. The DRA is fully qualified to operate in the installed environment considering temperature, humidity, seismic, radiation, and EMI/RFI. As a result, hardware CCF due to environmental factors is considered no more likely than other potential common cause failures such as maintenance or calibration errors that are not considered in the UFSAR. Software quality was evaluated as part of the commercial grade dedication process, including an independent review of the DRA source code. The results of this review coupled with the relative simplicity of the source code and divisional isolation of the EDGs, preventing a concurrent trigger from propagating from one EDG train to the other, provide strong indication the probability a software defect that would result in a software CCF affecting both EDG trains is remote. Nevertheless, even though considered unlikely, the result of a DRA CCF resulting in simultaneous failure of both EDG trains is already been described in the UFSAR [3.d]. Consequently, replacement of the MOP with the DRA will not create the possibility of a malfunction with a different result. ***(10 CFR 50.59 Criterion 6)***.

9. References Consulted

1. RIS 2017-XX, Update of the Staff Endorsement on the Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule [MLXXXXX]
2. Technical Specifications as Updated Through Amendment 267
3. UFSAR Sections Reviewed (Revision 24):
    a. UFSAR Section 8.2.2; Analysis
    b. UFSAR Section 8.3.1.1.6; Standby Alternating Current Power Supply and Distribution
    c. UFSAR Section 8.3.1.1.6.5; Diesel Generator Starting and Loading Description
    d. UFSAR Table 8-21; Failure Modes and Effects Analysis
    e. UFSAR Chapter 15; Accident Analysis
4. 04KV-002, Rev. 2; *4.16 KV Emergency Bus Degraded Grid Voltage Relay Setpoint Calculation*
5. NRC Letter Endorsing EPRI TR-106439 (TAC No. M94127), Dated July 17, 1997 (ML092190664)
6. NRC Regulatory Guide 1.209, March 2007; *Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants*
7. NRC Regulatory Guide 1.180, Rev. 1; *Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems*

8. CGD Letter LTR-0001, Rev. 0; *Documentation of DRA Reboot Time*

9. CGD-0002, Rev. 1; *Critical Digital Review of the Digital Reference Adjustor (DRA)*

10. CGD-0001, Rev. 1; *Summary of the Generic Qualification of the Microprocessor-Based Digital Reference Adjustor (DRA)*

11. CGD-0006, Revision 3*; XYZ Nuclear Plant – EDG Excitation System Replacement Project - Failure Modes and Effects Analysis*

12. CGD-0003, Revision 0; *XYZ Nuclear Plant EDG Excitation System Replacement Project EMC Qualification Report*

13. CGD-0004, Revision 0; *XYZ Nuclear Plant EDG Excitation System EQ Report*

14. CGD-0005, Revision 0; *XYZ Nuclear Plant EDG Excitation System Replacement Project Seismic Qualification Report*

15. CGD-0007, Revision 0; *Digital System Hazards Analysis for the XYZ Nuclear Plant EDG Excitation System Replacement Project*

16. EPRI Report 1011218, *Final Report, Dated December 2005; Basler SER-CB Voltage Regulators for Emergency Diesel Generators*

17. EPRI TR-107330, December 1996; *Generic Requirements Specification for Qualifying a Commercial Available PLC for Safety Related Application in Nuclear Power Plants*