NRR-DMPSPEm Resource

From: FREGONESE, Victor <vxf@nei.org>
Sent: Wednesday, July 12, 2017 10:44 AM
To: Drake, Jason
Cc: Morton, Wendell; Rahn, David; 'Archambo, Neil G'; HANSON, Jerud; FREGONESE, Victor
Subject: [External_Sender] Examples for Use in August 2 Meeting
Attachments: Generic NEI Chiller5059 Eval Qualitative Assessment Chiller Controls - Revision 0 - For 8-2 Meeting.pdf; Example Qualitative Assessment- Safety Related - Revision 3 for 8-2 Meeting.pdf

Jason, please find examples to be used in our August 2 meeting tabletops.

Vic Fregonese
Senior Project Manager
Nuclear Generation Division

Nuclear Energy Institute
1201 F Street, NW, Suite 1100
Washington, DC 20004
www.nei.org

M: 704-953-4544
E: vxf@nei.org

Hearing Identifier: NRR_DMPS
Email Number: 188

Mail Envelope Properties (41207040FCA6A84984074E806C73D73EE0FB85)

Subject: [External_Sender] Examples for Use in August 2 Meeting
Sent Date: 7/12/2017 10:44:12 AM
Received Date: 7/12/2017 10:44:22 AM
From: FREGONESE, Victor

Created By: vxf@nei.org

Recipients:
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"'Archambo, Neil G'" <Neil.Archambo@duke-energy.com>
Tracking Status: None
"HANSON, Jerud" <jeh@nei.org>
Tracking Status: None
"FREGONESE, Victor" <vxf@nei.org>
Tracking Status: None
"Drake, Jason" <Jason.Drake@nrc.gov>
Tracking Status: None

Post Office: mbx023-e1-nj-2.exch023.domain.local

Files	**Size**	**Date & Time**
MESSAGE	1459	7/12/2017 10:44:22 AM
Generic NEI Chiller5059 Eval Qualitative Assessment Chiller Controls - Revision 0 - For 8-2 Meeting.pdf	72414	
Example Qualitative Assessment- Safety Related - Revision 3 for 8-2 Meeting.pdf	253249	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

This qualitative assessment supports the replacement of the Acme Nuclear Power Station (ANPS) safety related Chiller Controllers, supporting 50.59 Evaluation Number 2017-yyyy.

This assessment synthesizes data from all references provided in Section 8 to reach these conclusions, including several references (e.g., microprocessor datasheets) embedded in some of the cited references. As this assessment and the 50.59 Evaluation were written concurrently, this assessment references the 50.59 Evaluation for some materials, rather than duplicating the text in multiple places.

1. Activity Identification

The proposed activity replaces the safety related controls only in the existing, original, safety related chillers in the two unit ANPS with new safety related digital chiller controls. The 50.59 Evaluation provides a complete description of the change, in the opening paragraph before Question 1.

Each of the safety related chillers is a divisionally independent island of control. The chillers are in no way tied to, or dependent on, the operation of the Reactor Trip System or the Engineered Safety Features System. IEEE Std. 603 classifies the chillers as auxiliary supporting features.

At the conclusion of this activity, ANPS will replace the obsolete chiller controllers completely. Since the existing compressors, evaporators, motors, valves can support the new more environmentally friendly refrigerant, and since the mechanical equipment is in good condition (with minor maintenance and component replacement to be performed concurrently with the controller installation), only the controllers will be replaced.

With digital controls, additional display capabilities are provided. For this installation, safety related displays are provided local to the chiller and duplicated in the control room. Each display shows only the status for the chiller, avoiding any appearance of cross-connection between chiller controllers. For the control room display, only display capabilities are provided. At the local chiller, the displays provide control and monitoring capabilities for use by a technician or engineer. In order to protect the operation of the chillers, the technician or engineer must log in to the display with a protected, modifiable password, which the software automatically logs out after a short period of inactivity. In the control room, the displays replace existing incandescent lamps used for indication, with less power and heat generation from the upgraded operator displays.

2. Design Function Identification

The Design Function of the safety related chillers and chiller controls is identified in the 50.59 Evaluation, including references to all reviewed UFSAR sections.

The safety related Design Function is to provide chilled water to the air handlers for controlling temperature in a set of defined, conditioned spaces. The combined Unit 1 and Unit 2 control room is conditioned using chilled water from both the Unit 1 and Unit 2 Chilled Water Systems. The unit-specific conditioned spaces include safety related I&C equipment required for controlling and mitigating accidents and transients.

Although not specifically described in the UFSAR, the failure of the digital controls for one chiller would result in loss of that chiller, which is described in the UFSAR, and thus bounded. The failure of the digital controls in any single chiller cannot affect the operation of the digital controls in any other chiller. Single failure tolerance is provided by use of two 100% chillers. Both chillers in each unit must be in service, else the Limiting Condition of Operations (LCOs) requires transition to cold shutdown.

The replacement digital controllers operate, monitor, and alarm off normal conditions for the replacement chillers. The original, obsolete controls controlled the original chillers but had minimal monitoring and alarming capability.

The proposed modification does not create any new design functions that were not part of the original plant design. The new design does not merge control or monitoring for any other function with the chillers chiller controls. The same spaces that are currently conditioned by the chillers will be the only spaces that will be conditioned using the chilled water system after the modification.

3. Failure Mode Comparison

The improved design of the replacement chiller controllers results from several decades of knowledge gained since design of the original chillers, which eliminates several of the existing internal failure modes in the existing chiller controls. The replacement digital chiller controls have self-test and self-diagnostic features that the designers could not even consider in the original analog controls. Detection of faults and failures in the new digital chillers should result in more timely detection of those faults and failures, with new control room indication provided for each of the chillers.

There are three paths to failure for the digital controllers. Each potential failure mode is evaluated below and an evaluation made between the failure modes of the existing and replacement controllers. Evaluations of the failure modes indicate that the failure mechanisms are likely different, but that the end result is a failure mode for the replacement system that is at least similar or bounded by the failure mode for the existing equipment.

a. Failure due to an Internal Defect

The commercial grade dedicators evaluated the response of the commercial chiller controls to various faults and failures from internal defects, using a single failure assumption, in a Hazards Analysis and a Failure Modes and Effects Analysis. The evaluations are based on single failures occurring in a single chiller controller. Neither the original nor the replacement chillers or chiller controllers are single failure tolerant individually, as each has many single points of vulnerability, but the dual chiller system redundancy provides single failure tolerance. The analyses did not identify any unexpected failure modes. There are no identified failure modes that are not identified automatically by the controller or manually through plant surveillance. The failure modes of the original equipment are equivalent to those of the replacement equipment, although the failure mechanisms are different in some cases.

All of the identified failures are detected and alarmed. Any failure that the software does not detect and alarm is expected to be detected during periodic surveillance tests and calibration checks (i.e., there are no silent failures associated with the new equipment).

b. Failure from Loss of Power

Each chiller compressor motor and chiller controller is supplied from a common safety related vital power source, backed by a separate emergency diesel generator (EDG). Each chiller is supplied from a different electrical division. The chiller shuts down on loss of power. For both original and replacement controls, the chiller restarts automatically when power is restored. For additional equipment protection, the replacement chiller adds detection of a loss of a phase and shuts the compressor motor down before damage occurs.

The replacement chiller controller provides a controlled sequence for startup and shutdown, based on the previous conditions (see the Software Requirements Specification for details). The replacement chiller controller takes longer to restart the chiller than the original chiller controls, such that starts after loss of offsite power (LOOP) do not load the chiller motor to the emergency diesel generator (EDG) at the same time in the sequence. The original controls started the compressor motor at 10 seconds after the EDG restores power to the input bus. The software in the replacement controls does not start the compressor for an additional 40 seconds after power is restored. The loss of chilled water for an additional minute after a LOOP has been determined to not be an issue, based on the thermal inertia in the conditioned spaces. The effects of this minor increase do not cause significant issues in the post-LOOP plant conditions, as demonstrated by the calculation referenced in the 50.59 Evaluation.

c. Failure Resulting from Environmental Factors

The replacement chiller controls have been qualified to operate in the environment in which they will be installed. Failures should not result from exposure to temperature, humidity, seismic, radiation, or electromagnetic compatibility (EMC) stressors that are within the equipment qualification envelope. Exposure to high temperatures will reduce the life of the equipment. The licensee has evaluated each of the listed stressors. Each of the plant stressor levels are well within the generic equipment qualification tests performed by the commercial grade dedicator. Since the equipment is installed in a mild environment, failed equipment can be readily replaced, so there is no requirement for qualified life calculations. Since the EMC tests were performed in accordance with the test requirements, the chiller control cabinet door does not have to be closed to meet EMC requirements. However, the chiller control cabinet door is expected to be closed and secured unless actively working in the cabinet.

4. Failure Results

No new failure modes have been identified that differ between the original and replacement chiller controls. The replacement controls perform self-tests and self-diagnostics that were not performed by the original equipment, supporting more timely detection of faults and failures. Timely detection of failures supports timely maintenance and correction of the failures and thus

maximizes reliability. For these auxiliary supporting features, reliable operation reduces temperature and humidity challenges for the safety systems and provides fewer distractions for control room operators. (Section 5.a.viii below discusses software common cause failure.) The identified failure modes for both the original and replacement chillers include:

- Fail as-is, in the current state, leaving the equipment running in the last valid conditions
- Erroneously stop with no demand to stop
- Erroneously start with no demand to start
- Fail to start when demanded
- Fail to stop when demanded
- Partial advance to the next demanded state
- Failure to respond in a timely manner
- Fail to load or unload to match demanded conditions

Indication of failure detection by the controllers can be:

- On the local display
- On the control room display
- No indication of the failure on either the local display or the control room display
- With an incorrect identification of the failure mode or mechanism

Maintenance will be initiated on indicated failures when detected by the control room operator or by an operator on rounds. Failures can be detected by:

- Visually and audibly annunciated in the control room annunciator from a fail-safe dry contact on the chiller controller,
- Indicated status on the control room display,
- Observation of inappropriate system operation,
- By an operator on rounds through either the local fail-safe Unit Okay (i.e., not Alarm) light or on the local display, or
- By a technician or engineer during surveillance test or calibration activities.

5. Assertions

a. Design Attributes

i. Quality and Reliability

Commercial grade dedication of the hardware and software for both the digital chiller controller and the display was performed in accordance with EPRI TR-106439 and the generic EPRI CGD guidance. The NRC staff has determined that EPRI TR-106439 provides an acceptable method for dedicating commercial grade digital equipment for use as basic components, including requirements for 10 CFR 21 reporting. The commercial vendor built and assembled the mechanical and electronic components, and the dedicator then commercial grade dedicated the assembled controllers and displays. Adherence to the applicable industry and regulatory standards provides a high degree of software, hardware, and

equipment quality and reliability. This assertion is demonstrated by the high reliability of these digital controllers in commercial service (see Section 5.a.viii).

The vendor performed software verification and validation activities under the vendor's ISO-9001 quality program. The dedicator performed additional activities, including a more complete review of the design documentation, code review, and additional unit, integration, and system testing. Issues and concerns uncovered through the V&V efforts were fed back to the vendor, who resolved the issues under their quality program. The completed software was returned and appropriate portions of the dedicator's V&V program were repeated. The final software version was returned to the dedicator and became the vendor's standard commercial software. No safety concerns were uncovered during the review.

ii. Appropriately Simple

The commercial chiller controller has sufficient simplicity. The commercial chiller controller is designed to control chillers of various types. One basic improvement from the previous version is that all compressor types are incorporated into a single firmware version, rather than having multiple firmware versions, with each version only supporting a single chiller variant. The combination of chillers into a single software source simplifies software maintenance, in that corrections are made to a single source code, thus not requiring manual actions to duplicate the software change across multiple chiller control software sets. The commercial chiller controller includes configuration data to set the compressor type, and thus the algorithms to run. The configuration data also selects the inputs and outputs required by the algorithm as well as mapping the inputs and outputs to the hardware. The licensee can modify only a subset of the chiller parameters, with the commercial vendor controlling critical parameters. The software used by the vendor to set these critical parameters is not provided to either the dedicator or the licensee.

The commercial chiller controller software uses a state machine to step through the sequences required to start, operate, load, modulate the chiller loading, unload, and secure the chiller. Some of the advantages offered by state machine based controls include that each controller is always in a defined state, the total number of different states that the controller can be in are defined, and the transitions between all states are well defined and visible in the software (and displayed on the local and control room displays). Well-designed state machine based controls are inherently well defined, visible in the design and in the software, easier to review (during V&V), offer a clearly defined path to testing (during V&V), and more reliable than controls that do not utilize state machine techniques.

The code is made more complex by the addition of self-tests and self-diagnostics. While these features do increase code complexity, these features also provide fault and failure detection, thus protecting the overall health of the chiller mechanical equipment and ensuring that each chiller does not fail silently for all identified failure modes and mechanisms. Experience with the commercial equipment shows that the complexity added by the self-test and diagnostic features supports reliability,

including the potential to shut down the equipment before extensive damage occurs, based on early detection of failing equipment.

iii. Non-Concurrent Triggers

Each of the chillers operates independently of all other chillers. There are no cross-linkages between chillers.

A different, independent safety related bus powers each chiller. A separate, independent emergency diesel generator provides backup power for each chiller.

The same types of sensors are provided for each chiller. The sensors are simple, and are not digital. The potential of common cause failure from the sensors is thus considered unlikely. The software constrains the engineering units into valid ranges, over which the software is designed to remain operable. The software alarms any sensor that provides values outside of valid ranges, and conservatively shuts down the chiller for critical inputs found operating outside valid ranges.

There are two indirect cross-connects between the chillers. One is the chilled water system piping and the chilled water temperature that each chiller independently measures. Both chillers are also cross-connected through the common Service Water System, with each controller individual sampling a permissive for service water flow.

Maintaining chilled water temperature below a maximum value in a plant common chilled water system is an independent safety function in each chiller, helping to maintain the equipment qualification of the safety related I&C cooled by the chilled water system. Each chiller is configured through a separate selector switch wired just to that chiller controller, defining whether the chiller will operate as the lead or lag controller. The selector switch positions are set by manual operator action every few months, rotating through both chillers to provide even wear. Each selector switch sets operating ranges and action limits for each chiller based on the position of the switch, forcing the lead chiller to be the primary by setting the controlled temperature at a low value, and setting the lag chiller to control at pre-set higher chilled water temperature, thus sequentially activating each of the chillers as needed to control chilled water temperature. The lag chiller will only operate as long as required to bring the chilled water temperature down below their action levels, configured in software based on the individual selector switch position. The lag (Position 2) chiller action temperature is set higher than the lead (Position 1) unit. The current state and the software trajectory for each chiller is exceedingly unlikely to be close enough to another chiller to have the potential generate software common cause failures through concurrent triggers.

Like the chilled water temperature, each chiller controller monitors the chilled water flow through the chiller's evaporator, which the software uses as a permissive to allow the chiller to run. Each of the chiller controllers monitors the flow

independently, and shuts down the unit when insufficient chilled water flow occurs through the evaporator (Software Requirements Specification).

Thus, this evaluation concludes that there are no credible concurrent triggers that would initiate a hardware or software common cause failure simultaneously affecting both chillers.

iv. Watchdog Timer

Watchdog timers exist in the commercial chiller controller microprocessor.

For the commercial chiller controller watchdog, the watchdog timer uses the internal microprocessor's count down watchdog timer. The watchdog timer causes a hard reset if the counter counts down through zero. The software resets the watchdog timer using two separate instructions, which the software must execute sequentially to reset the watchdog timer counter. Software watchdog timers are provided within the software to ensure that tasks (threads) are operating correctly. An appropriate clock source has been chosen. Failure of the board or timing out the watchdog timer causes all discrete outputs to de-energize, turning off all motors and solenoids. This de-energization occurs in the hardware, based on the watchdog timer output. Failure of the on-board crystal clock is detected in a simple resistor-capacitor (RC) timer within the microprocessor, which forces a timeout indication if the internal clock should stop, using different, non-clocked microprocessor paths than the internal watchdog timer. Either timeout forces all outputs off, including the fail-safe output relay that drives the Unit Okay (not Alarm) lamp on the chiller control front panel and provides dry contacts to be annunciated in the control room.

v. Diverse Indication of Failure

Failure of a single chiller can be determined by using one of several different methods that the commercial chiller controller supports to display status. These include: 1) annunciation of failure in the control room under either program control or through watchdog timer time out, 2) examination of the control room display for that chiller, 3) examination of the local display, or 4) observation of the extinguished Unit Okay (i.e. not Alarm) lamp on the local chiller panel.

A perceptible rise in control room temperature is not a diverse indication of failure or trouble in multiple chillers, because the air temperature in the single, merged Unit 1 and Unit 2 control room envelope is unlikely to change significantly based on the other unit's chillers and air movement from heating, ventilation, and air conditioning (HVAC) fans.

However, several rooms exist whose temperature is useful as a diverse means of detecting chiller failure. The unit-specific control room annunciator will annunciate a high temperature in the unit-specific Relay Room. In addition, high temperature in the unit-specific Electrical Equipment Room is annunciated. Loss of both chillers will result in annunciation of over-temperature alarms in both rooms (Reference 8.g) in a timely manner, allowing Operations, Maintenance, and Security to cope with the

failures using an approved procedure prior to any of the affected I&C equipment exceeding its environmental qualification.

vi. Digital Communications

Each safety related digital chiller controller (controlling a single chiller) communicates with the local and control room displays independently. The digital communication uses an industry standard protocol over Ethernet. The digital chiller controller has two separate digital communication links, and sends data to each of the displays. Each of the displays communicates with the digital chiller controller to set the data to be broadcast. Each communication path uses full duplex fiber optic cables, to provide electrical and EMC isolation. The commercial grade dedicator tested specifically for broadcast storms of various messages, and used a commercial test set to stress and validate the cyber security of the digital communications for both the digital chiller controller and the display. These tests did not adversely affect the digital chiller controller or the display.

The digital chiller controller microprocessor has two separate Ethernet media access controllers, each with a separate set of electrical to optical and optical to electrical converters. The Ethernet controllers run separately from the microprocessor, and use direct memory access to send and receive messages of constrained lengths to a separate random access memory integrated circuit used only for communications. The Ethernet controllers have no access to memory used by the microprocessor for program execution. When new messages are received or when a message has been transmitted, the Ethernet media access controller causes an interrupt, which is handled by the digital chiller controller software. No credible faults or failures have been identified that would affect the operation of the safety related chiller control software through message traffic.

Each local and control room display provides data and status indication for the local chiller. Each local and control room display only has data for the chiller with which the display communicates. Both displays attached to a single digital controller are provided with data through separate, safety related full duplex fiber optic communication links. When no one is logged in to the local display, the local display provides display only access. When a user logs in to the local display, the local display provides the ability to control the chiller and to change selected portions of the configuration. The control room display has no ability to control the chiller, both through configuration in the chiller, and from the digital chiller controller's software that allocates the display control features to the local display port only.

Since there is no communication between redundant digital chiller controllers and since each chiller is provided with a separate digital chiller controller, independence is assured between the redundant chillers. The local and control room displays only provides chiller data and status indication for the chiller to which each is attached.

The chilled water controllers each measure the chilled water temperature through independent sensors, and control the operation of the chiller based on pre-configured

temperature setpoints. Each chiller has a separate two position switch to select the unit as the Lead or Lag unit, which configures the pre-configured temperature setpoint values individually, without any wiring or communication between the chillers. If the operator misconfigures one or more switches or if the contact arrangement in a switch does not change appropriately, multiple chillers could be configured as Lead or no chillers could be configured as Lead, for example. In either case, the chilled water system would operate appropriately.

vii. Combining Functions

The functions performed by the chiller controls were originally individual controls for each chiller and remain individual controls for each chiller. The chiller controls still only control the operation of the chiller, with no additional functions added for control or monitoring of any other equipment or plant functions. Each replacement chiller does have improved self-test and self-diagnostic functions, but those functions are only for the single chiller controlled by a single digital chiller controller. Each replacement chiller control only controls the local chiller to which the chiller controller is connected. The chiller controls perform no other functions.

viii. Defense-in-Depth and Software Common Cause Failure

The safety related chillers provide heat removal for several safety related spaces, including the control room. The commercial vendor implemented and the dedicator evaluated the digital chiller control software to attempt to minimize the potential for software common cause failure. The dedicator uses the same commercial vendor software that the vendor provides for commercial chiller applications, which have equivalent criticality, without the two detected and now corrected chiller software errors that could have affected the safety function of generating chilled water (see Section 5.c).

The digital chiller controller and the display were designed by the vendor to minimize digital obsolescence issues. Both run a small, dedicated purpose commercial operating system. For the digital chiller controller, the software provides tasking, program storage, configuration, and startup sequencing to enable the controller to operate the local chiller, including sampling all inputs, driving all outputs, and communicating with the displays. The display microprocessor runs a modified version of the software which also provides tasking, program storage, configuration and startup sequencing for the display as well as message services for the fiber optic links, storage for a limited set of primitive graphics, and display services for those graphics. The same processing and quality assurance provided for the digital chiller controller (which implements the safety function) was implemented for the display software (which provides a manual control capability when logged in as well as data and status display at all times).

The chiller controls and the display have been commercial grade dedicated in accordance with EPRI TR-106439, to establish the software qualify and ensure that the likelihood of a latent software defect is low. As part of the CGD, the dedicator

performed a Critical Digital Review (CDR) as well as an independent retrospective verification and validation of the software using the commercial vendor's system requirements and software and hardware design documents. The dedicator reviewed the source code. The CGD process, including the CDR, demonstrated that the software is equivalent to software developed under an Appendix B compliant software quality assurance program as defined in IEEE Std. 7-4.3.2. Low software defect likelihood (see Section 5.c) and the divisional independence of the chiller controls prevents a triggered defect in one division from propagating to another division, significantly reducing the probability for a software common cause failure disabling all two chillers.

Based on the quality of the code, the review of the software under an Appendix B nuclear quality assurance program, and the chillers' divisional independence, it is reasonable to conclude that a software common cause failure is unlikely. Further, there is reasonable assurance that failure 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.

In the unlikely event of a software common cause failure across all chillers, ANPS has Operations procedures which remove non-critical heat loads, posts Security guards, opens doors, and sets fans in place to blow conditioned air from other non-safety related HVAC systems into the safety related spaces. The calculations supporting this defense-in-depth process demonstrate that the process, when implemented promptly, controls temperatures in all safety related spaces below the equipment qualification limits.

ix. Environmental Qualification

The dedicator provided the operating environment for the cabinet mounted chiller controls and panel mounted displays in the Equipment Qualification Summary Report. The tested and qualified upper design ambient temperature is 140^{o}F. The environmental testing demonstrates that the controller will operate in 95% relative humidity, with the enclosure door open or closed. ANPS has determined that the qualification limits for the chiller controls and the displays are not exceeded in the installed locations.

x. Seismic Qualification

The dedicator tested the cabinet mounted chiller controls and panel mounted displays and determined that the equipment is qualified for use before, during, and after a seismic event. ANPS has verified that the magnitude and spectra envelope the installation locations. The Equipment Qualification Summary Report provides installation and operational conditions to ensure compliance with the seismic qualification. ANPS will mount the chiller control cabinets and displays in accordance with these requirements.

xi. Radiation Qualification

The cabinet mounted chiller controls and panel mounted displays are installed in mild environments. The radiation exposure and dose rate are small, and well within the capabilities of modern solid state equipment. No further evaluation of radiation qualification is required.

xii. Electromagnetic Compatibility (EMC) Qualification

The cabinet mounted chiller controls and panel mounted displays were tested for EMC based on the requirements of USNRC RG 1.180, Revision 1. The dedicator provides installation and operational conditions in the Equipment Qualification Summary Report to ensure compliance with the EMC qualification. ANPS will install the equipment in accordance with the equipment qualification requirements.

xiii. Hardware Common Cause Failure

By performing adequate equipment qualification tests and by using industrial grade parts, it is reasonable to conclude that hardware CCF is no more likely than other potential common cause failures such as maintenance or calibration errors that are not considered in the UFSAR.

b. Quality Design and Commercial Grade Dedication Process

The standards to which the software documents and V&V were performed are provided in the commercial grade dedicator's nuclear Quality Assurance Manual and in the qualification project documentation.

See Discussion in Section 5.a.viii above.

c. Operating Experience

The operating experience for the unit shows a reasonable number of commercial units operating. Nuclear experience with this controller, as with the previous model, is limited. As noted in Section 8.7, Performance History Evaluation, in the Critical Digital Review (CDR), over 2,000 of the commercial digital controllers and displays were in operation when the dedicator performed CDR, for a conservative operational history of over 43,000,000 hours across five years, or about 5000 unit-years. Over that operating history, 50 hardware failures occurred on the commercial chiller controller and 40 hardware failures occurred on the display board. Over the period, only two software defects were reported that had the potential to affect the safety function. There were several significant enhancements, adding new display capabilities (e.g., trending, historical data, and graphics capabilities) and new chiller compressor types. Several of the modifications were associated with administrative or testing functionality.

The application software in the chiller controls and displays is a copy of this commercial software, with configuration control and change management provided by the dedicator, and maintained by the commercial vendor. The vendor continues to augment the

commercial software with new compressor types, which are not added to the dedicated version unless required for a safety related application. Any errors, concerns, or issues identified by the commercial vendor, or by the dedicator, and resolved, and will be included in the nuclear version.

As noted elsewhere, the dedicator did find errors in the software, which the commercial vendor has corrected, as noted in the software version history (see CDR). The CDR reports on two defects that had the potential to affect the safety function, which the dedicator found as part of the software qualification activities, prior to completion of commercial grade dedication.

6. Rationale

The chillers are not accident initiators. The chillers are not credited directly with mitigating accidents. The chillers do not protect the barriers directly, including the fuel, fuel cladding, reactor coolant system boundary, or containment boundary. Rather, the chillers are support systems that protect the controls for the systems that mitigate accidents and protect the barriers, along with cooling the control room. As demonstrated in this evaluation, the commercial vendor and the dedicator have worked to minimize the probability of hardware and software common cause failure, which is also demonstrated in the operating history. In the unlikely event of a hardware or software common cause failure that makes all unit chillers inoperable, a procedural means for limiting temperature rise in controlled spaces is available, which maintains temperatures in the controlled spaces within the equipment qualification limits, which would not affect the immediate operability of the controls that mitigate accident conditions.

7. Conclusion

Based on the evidence provided above, ANPS can install the replacement chiller controls under 10 CFR 50.59 without prior approval by the USNRC.

8. Documentation of Evidence and References Consulted

The following sources contain the evidence to support the conclusions in this document:

a. The UFSAR, Technical Specifications, and commitments reviewed as listed in the 50.59 Screening Form
b. *Dedicator's* Critical Digital Review
c. *Dedicator's* Software Verification and Validation Plan
d. *Dedicator's* Software Quality Assurance Plan
e. *Dedicator's* Hazards Analysis
f. *Dedicator's* Failure Modes and Effects Analysis
g. ANPS Operations Procedures, *Loss of Unit 1 Safety Related HVAC* and *Loss of Unit 2 Safety Related HVAC*

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].

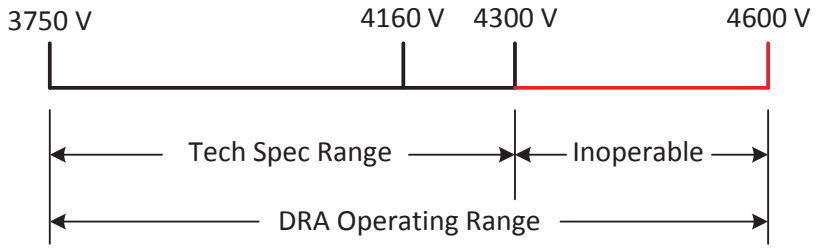

Figure 1

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*