Hope Creek Safety Related UPS Replacement

Application of RIS 2002-22 Supplement 1 to implement Digital UPS Systems Under 10CFR50.59

NRC Public Meeting

May 9, 2019

PSEG Nuclear LLC

Agenda

- Introduction
- Purpose of meeting
- Scope of Project
- Qualitative Assessment Overview
- System Architecture
- Failure Modes and Effects
- Design Attributes
- Quality of the Design Process
- Operating Experience
- Conclusion

Purpose of Meeting

- **Hope Creek plans to install Ametek NDPP Class 1E digital Uninterruptible Power Supply (UPS) systems under a 10 CFR 50.59 evaluation**

- **A qualitative assessment was prepared using the criteria described in Regulatory Information Summary (RIS) 2002-22 Supplement 1**

- **This meeting seeks to inform NRC staff of the results of the qualitative assessment**
  - Application of RIS guidance
  - Technical approach to addressing design
  - Conclusion that the likelihood of failure is **sufficiently low**

Scope of Project

- **Hope Creek has 8 safety related UPS systems in four safety channels**
  - Two UPS systems per channel
    - One UPS for Bailey Logic system (Main Control Room Interface)
    - One UPS for Emergency Core Cooling System functions
  - Safety Function: Supply 120VAC power to downstream loads

- **All 8 systems will be replaced with Ametek NDPP UPS systems**
  - System replacement will be 1 channel (2 UPS's) per outage
    - First installation scheduled for Spring 2021

Qualitative Assessment Overview

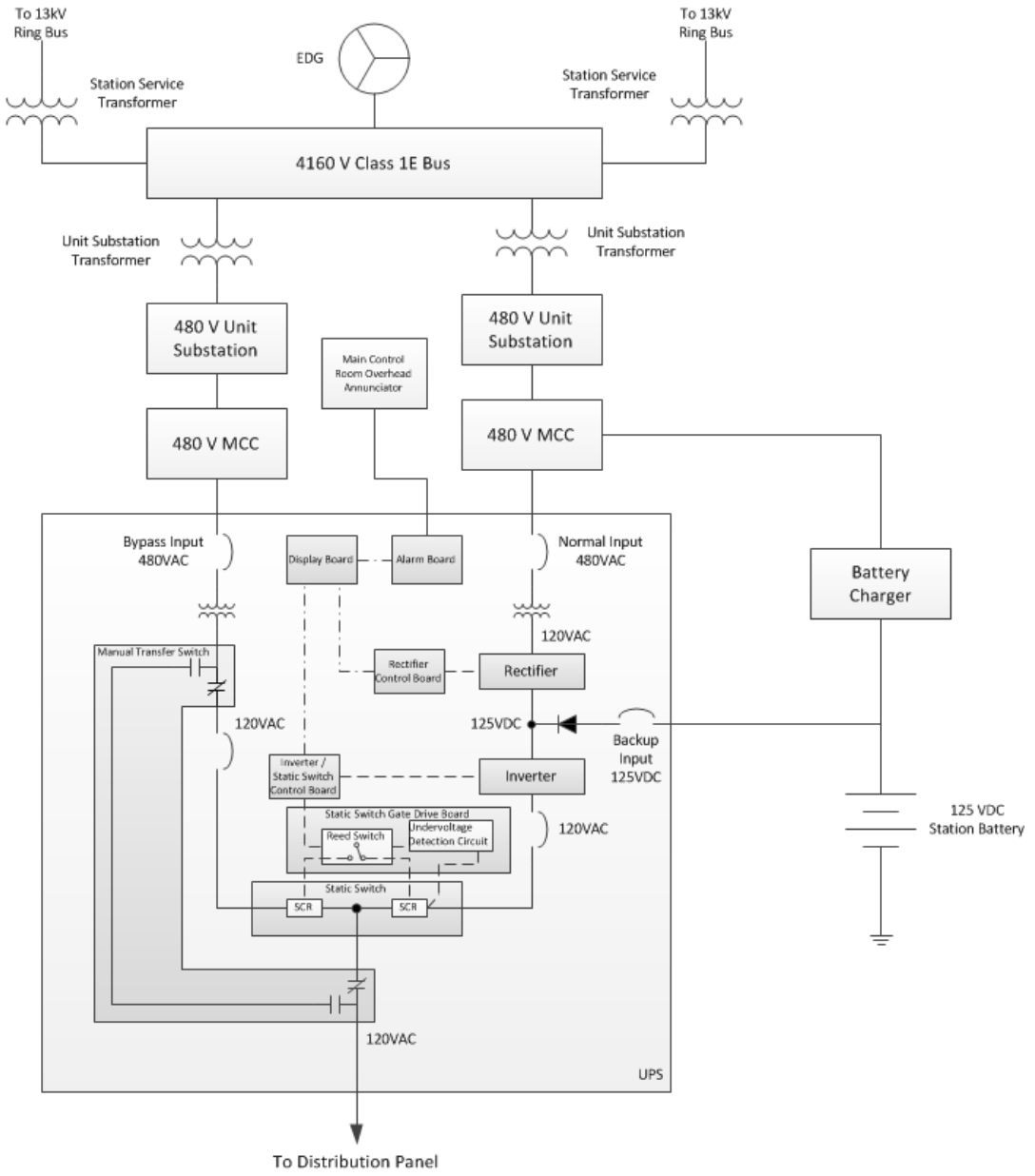
- **Application of guidance under RIS 2002-22, Supplement 1**

- **Qualitative assessment & failure analysis of new design**
  - Review focused on digital elements of the new UPS
  - Develop application-specific Failure Modes and Effects Analysis (FMEA) for digital elements the UPS
  - Identification of design attributes that serve to prevent or limit failures
  - Assessment of software design development, life cycle and quality assurance
    - Factory visit and thread sample of design documents
  - Review of Operating Experience (OE) from non-safety installations
    - Assessment of nuclear design against non-nuclear industrial models provided by Ametek

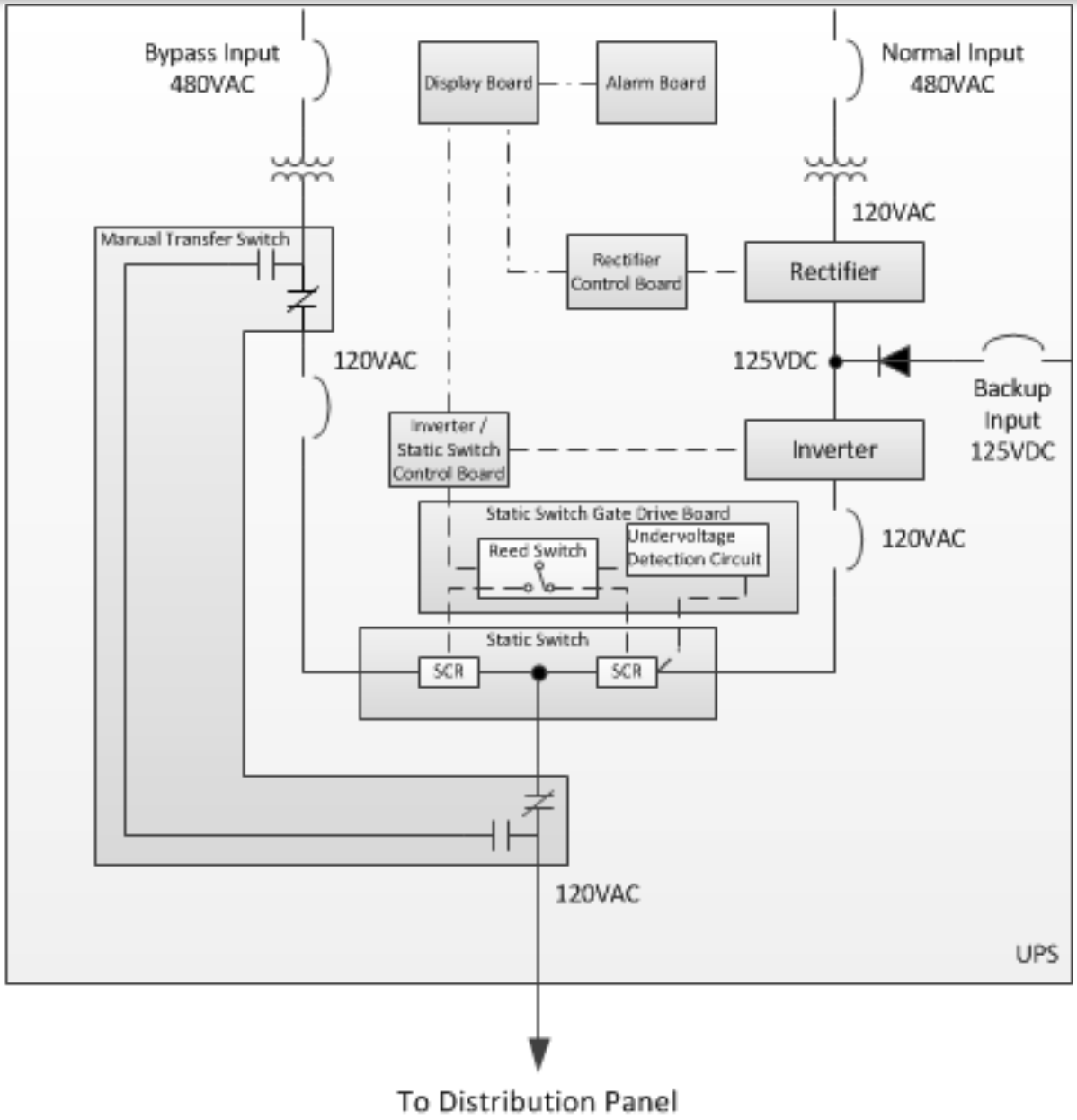
System Architecture

- **Double-Conversion UPS System**
- **Three inputs – Normal 480 VAC, Bypass 480 VAC, Backup 125 VDC (Batteries)**
- **Single 120 VAC Output**
- **Major components**
  - Rectifier
  - Inverter
  - Static Switch
  - Regulating transformer (no digital content)
- **Normal 480 VAC feed transformed to 120 VAC then rectified to 125 VDC**
- **125 VDC is diode auctioneered with emergency 125 VDC from batteries**
- **125 VDC bus feeds inverter which converts to 120 VAC**
- **Upon loss of inverter - static transfer switch swaps to alternate 480 VAC feed via regulating transformer**

System Architecture



System Architecture



Failure Modes of New UPS Design

- **Single Random Hardware Failure**
  - Failure modes of the new digital UPS are bounded by failure analysis in the Hope Creek Updated Final Safety Analysis Report (UFSAR)
- **Loss of Power**
  - Effects of upstream power loss are identical to existing UPS
  - Does not cause a failure of the safety function
- **Systematic Failure of All UPS's Due to a Design Defect**
  - Evaluates postulated failure modes of each of the four controllers (Alarm, Rectifier, Display, Inverter)
  - Provides justification that failure modes have no effect on safety function, or are of sufficiently low likelihood
  - Determination of low likelihood based on design attributes, quality, and operating experience per Section 3 of RIS 2002-22 Supplement 1
  - Design attributes evaluated using supplemental guidance from EPRI 3002005326 – *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems*

Failure Effects

- **Single Random Hardware Failure**
  - Failure effects evaluation assumes loss of 120VAC output
  - No change to failure effects described in the UFSAR

- **Systematic Failure Due to a Design Defect**
  - Common Cause Failure (CCF) likelihood determined to be sufficiently low per results of qualitative assessment
  - Worst case CCF requires unlikely sequence of events
    - Complete loss of UPS function from a CCF can only happen when the 4kV safety buses are de-energized
    - 13-second window during diesel start and load sequence after LOP
  - CCF coping ability assessed despite 'sufficiently low' conclusion
    - Loss of output evaluated concurrent with a LOP (during 13-second diesel start time)
    - Recoverable via manual starting of EDGs

Design Attributes

- **Internal diversity**
  - An analog circuit can force a transfer to bypass on a gross failure of the inverter
- **Limited concurrent triggers**
  - Loss of upstream AC on a Loss of Offsite Power is the only identified common trigger
- **Segmentation**
  - Internal communications provide functional segmentation between sub-systems
  - Safety function processor is isolated from internal communications – complies with DI&C ISG-04 staff position

Design Attributes

- **Self-test and diagnostics**
  - Diagnostics cover initialization data, runtime checks of program memory and RAM, and timeouts for data link activity
  - Redundant communications messages
  - Watchdog timer monitors completion of inverter control function code
- **Diverse indication of failure**
  - Independent transducers monitor battery voltage, output voltage and output current, and provide alarms in the main control room
- **Extensively tested safety function processor**
  - Single loop operating system w/ fixed interval interrupt routine
  - Invariant execution
  - Programmed in Assembly, during testing register values are inspected to ensure correct execution

Quality of the Design Process

- **Sargent & Lundy Review**
  - S&L, on behalf of PSEG, performed reviews of the Ametek software development processes
  - S&L concluded that Ametek has an effective V&V process
  - Review of phase summary and discrepancy reports showed effective identification and correction of issues

- **NRC Inspection Report 99901427/2017-201 [ML17135A403]**
  - Included a review of Ametek's software development lifecycle
    - Later phases were in draft status
  - Concluded lifecycle activities satisfied the regulatory requirements of Appendix B
  - No findings were identified for digital I&C design control

Operating Experience

- **Ametek has extensive industrial and non-1E nuclear operating history on the DPP line of products**
  - Ametek service database was reviewed
  - Hope Creek and Salem operating history of the DPP inverters was reviewed
- **Zero inverter failures identified that were attributed to a software defect**
- **Applicability to the NDPP**
  - NDPP is an evolutionary development from the DPP industrial product line
  - Removal of external digital communications and parallel output functions
  - Addition of runtime memory diagnostics and serial link redundant messaging

Conclusion

- **Conclusion is that the likelihood of systematic failure due to a design defect is sufficiently low**
  - Evaluated per the criteria from Section 3 of RIS 2002-22, Supplement 1

- **Supplemental guidance via preventive measures in EPRI 3002005326**
  - **Reduce the likelihood of a CCF caused by an operating system defect**
    - Table A33-P3 – Demonstrate that a defect will not be activated when the SSC is needed to perform its required function
    - Table A33-P1 – Minimize potential for concurrent activating conditions, demonstrate an activated defect is self-announcing, and reduce defect potential through documented software quality.
  - **Reduce the likelihood of a CCF caused by data communications**
    - Table A39-P4 – Reduce the likelihood of a communication interface design defect

Hope Creek Vital Bus Inverter Replacement

Questions?