Nuclear Qualification Demonstration of a Cost Effective Common Cause Failure Mitigation in Embedded Digital Devices

PI: Matt Gibson, Sr. Technical Leader, Electric Power Research Institute, Inc. (“EPRI”)

Collaborators: N/A

Program: Advanced Sensors and Instrumentation R&D (NEET 2)

ABSTRACT:

The introduction of digital I&C systems and use of programmable logic and various types of system infrastructure digital technologies as replacement systems has resulted in an increase in system and component complexity when compared to the legacy equipment. This increase in complexity has resulted in a more complicated functional design, failure analyses (particularly Common Cause Failure (CCF) identification and mitigation), and reliability profile which has caused delays in updating the aging I&C systems.

This research discovers the necessary techniques and methods for successful design and implementation of a simple and “inflexible” embedded Field Programmable Gate Array (FPGA) module. EPRI leverages its existing research in CCF and programmable logic technologies to design, construct, and validate an embedded device using the functional requirements of an Emergency Diesel Generator (EDG) Stop/Start module defined in EPRI Technical Update 3002002098, Emergency Diesel Generator Digital Control System Upgrade Requirements. Investigators simplify the implementation and fabrication of the demonstration module to the point that all characteristics of the embedded device are known and validated. Unused or single use circuitry is removed to explore the lower limits of simplicity and for a one-time programmable device, programming circuitry is moved off-board. Tradeoffs for transitioning to an Application Specific Integrated Circuit (ASIC) fabrication are also explored as a part of this research in order to determine whether adequate levels of simplicity are achievable.

The first year of research consists of translating the functional requirements of the EDG module to a set of design specifications which meets the simplicity objectives of the project. In addition, fabrication and infrastructure requirements are developed which define the implementation and fabrication of the demonstration module such that all characteristics of the embedded prototype are known and can be deterministically validated. Testing and validation techniques are developed for use in validating the prototype. The specifications are then used to evaluate and select the implementation technology. An EPRI Technical Report is published to describe insights and methods gathered during this phase of the research.

The second year of research is used to fabricate and validate the embedded device using state-of-the-art testing capabilities in a commercial facility. Key research objectives such as testability, scalability, reliability, and defect identification are demonstrated and a final EPRI Technical Report is published to document the results of this research. The report includes the bounding determinism criteria for design, implementation, and fabrication of the safety-related digital module.

This research describes a new and alternate concept to design, fabricate, and validate embedded digital devices for safety-related applications. The concept offers a lower total cost and reduction in schedule risk by minimizing validation, analysis, and regulatory review overhead. The embedded digital components that can be demonstrated to contain no additional capabilities or characteristics other than that specially required for the functional objectives provides a greater assurance against the introduction of failures through digital I&C upgrades with a potential for reduced quality assurance and regulatory review overhead. These “inflexible” devices have no hidden fabrication or infrastructure to complicate straight forward analysis and validation. While more expensive, they would allow a simple, deterministic validation resulting in dramatically lower total installed cost and a reduction in technical and schedule risk.