Development and Demonstration of a Model Based Assessment Approach for Qualification of Embedded Digital Devices in Nuclear Power Applications

PI: Richard Wood
The University of Tennessee

Collaborators: Carl Elks – Virginia Commonwealth University
Carol Smidts – The Ohio State University
H. M. Hashemian – AMS Corporation
Brent Shumaker – AMS Corporation

Program: NEET Advanced Sensors and Instrumentation

ABSTRACT:

Much of the instrumentation and control (I&C) equipment in operating U.S. nuclear power plants (NPPs) is based on very mature, primarily analog technology that is steadily trending toward obsolescence. This legacy analog technology, which is being propagated into new NPP designs, imposes performance penalties and maintenance burdens. Experience in other industries has shown that digital technology can provide substantial benefits in terms of performance, reliability, and maintainability. Nevertheless, the nuclear power industry has been slow to adopt digital technology primarily because of regulatory uncertainty, implementation complexity, and limited availability of nuclear-qualified vendors and products. A specific concern motivating this research is the potential for common-cause failure (CCF) vulnerability associated with embedded digital devices.

The purpose of this research is to develop an effective approach employing science-based methods to resolve concerns about CCF vulnerability that serve to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with embedded digital devices in nuclear power applications. The research objectives address the challenge of establishing high levels of safety and reliability assurance needed for the qualification of embedded digital devices (e.g., microprocessors, programmable logic devices) that are subject to software design faults, complex failure modes, and CCF vulnerability. Specific objectives are: (1) assess the regulatory context for treatment of CCF vulnerability in embedded digital devices, (2) define a classification scheme for embedded digital devices to characterize their functional impact and facilitate a graded approach to their qualification, (3) develop and extend model-based testing methods to enable effective demonstration of whether devices are subject to CCF, which may arise from vulnerabilities introduced at any stage of the design lifecycle, (4) establish a cost-effective testing framework that incorporates automation and test scenario prioritization, and (5) demonstrate the qualification approach through selection and testing of candidate digital device(s).

This research will advance the state of the art in the qualification of advanced instrumentation with embedded digital devices for NPP application by (1) developing novel methods for establishing acceptable proof of operational reliability, (2) applying the developed methods to representative embedded digital devices to ascertain the effectiveness of the methodology, and (3) establishing a cost effective qualification framework that is compliant to existing guidance and standards. The outcomes of this research will contribute substantially to the technical basis for qualifying embedded digital devices in regard to CCF vulnerability. The results will benefit all reactor types by resolving a current impediment to more extensive application of digital devices.