Prevention of Common Fault-Trigger Combinations for Qualification of Digital Instrumentation and Control Technology

PI: Richard Wood
The University of Tennessee

Collaborators: Carol Smidts – The Ohio State University
Ted Quinn and Jerry Mauck – Technology Resources

Program: RC-8.1

ABSTRACT:

Much of the I&C equipment in operating nuclear power plants (NPPs) in the USA 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 burden. 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. In particular, the potential for common-cause failure (CCF) has been a major impediment to the wide-spread implementation of digital technology at NPPs.

The challenge presented by digital technology is that errors, deficiencies, or defects at any stage of a system's life cycle can result in systematic faults that may remain undetected until operational conditions activate (i.e., trigger) the faulted state to result in failure of a critical function. The potential of CCF compromising multiple systems constitutes the principal credible threat to defeating the defense-in-depth provisions within NPP I&C system architectures. The U.S. Nuclear Regulatory Commission (NRC) guidance identifies two design attributes as being acceptable for eliminating CCF concerns: (1) diversity or (2) testability (i.e., 100% testability). Either solution can result in high costs and remaining licensing uncertainty. Development of enhanced qualification methods to satisfy regulatory requirements (e.g., by preventing conditions that trigger CCF is needed.

The purpose of this research is to develop an effective design evaluation approach based on prevention of concurrent triggering conditions to eliminate prospective CCFs and thereby enable qualification of digital instrumentation and control (I&C) technology for extensive application in NPP modernization. The research objectives address the challenge of qualifying technology potentially subject to systematic undetected faults. Specific objectives are providing the basis for classifying commonality among digital systems and devices, categorizing faults and triggering conditions, determining relationships leading to fault-trigger combinations, and defining a collection of preventive design measures to resolve the potential for concurrent triggering of CCF. It is expected that the methodology developed under this research can be incorporated in design analysis and qualification processes being implemented by the US nuclear power industry.