Applying Single Failure Criteria to Digital I&C Systems

Abstract: These days it is easy to forget that IEEE 603 single failure criteria (SFC), though written in a time before the advent of digital technology, remains equally applicable to all safety related I&C systems regardless of the technology employed. Applying this criterion to modern digital I&C safety systems and demonstrating that SFC criterion is met has created unique and interesting licensing challenges, particularly when the prospects of common mode software or logic failures are taken into consideration.

Over the years, the nuclear industry and its regulators have found that methods used to demonstrate SFC compliance vary greatly depending on individual system characteristics and logistical limitations such as the inability to perform comprehensive testing of digital systems. A method successfully used for one type of system may be inadequate when applied to a different type of system particularly when different technologies are involved. For this reason, there is currently a renewed interest in producing new guidance for addressing the SFC using a set of methods that is based on best practices that have been developed by technologists in these areas.

The IEEE nuclear power engineering committee (NPEC) is currently developing a revision to IEEE Std. 379, “Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems” to clarify how potential for CCFs in software or logic can be screened or otherwise addressed within the context of a single failure analysis.

This paper explores the challenges presented in applying the SFC criterion to today’s digital upgrade projects. This paper also explores the evolutionary changes that have occurred to the single failure criteria since it was first conceived over 50 years ago.

Author: Richard Stattel USNRC

Relevant Topics: Hazard and Failure Mode Analysis for Digital Systems, I&C Regulations, Standards, and Guidelines

Instrumentation and Control (I&C), Failure Modes and Effects Analysis, Diagnostics, Common Cause Failure (CCF), Common Mode Failure (CMF, Diversity and Defense-in-Depth, Redundancy, Field Programmable Gate Arrays (FPGA), Software, Complex Programmable Logic devices (CPLD).