Assessing and Managing Common-Cause Failure Susceptibilities of Digital Instrumentation and Control Systems

Nuclear plant owners/operators need to be able to systematically identify and assess susceptibilities to potential digital system failures and unintended behaviors that can lead to plant system/component failures and incorrect responses, including common-cause failures (CCF). Once identified, these potential vulnerabilities can be managed using both preventive and mitigating measures. While methods for treating safety systems are well developed, consensus guidance for non-safety applications remains elusive. This report provides practical guidance to help utility engineers, equipment suppliers and system integrators in addressing potential CCF concerns for various plant instrumentation and control architectures. The guidance includes a step-by-step approach for identifying and qualitatively assessing susceptibilities in terms of their importance, likelihood, and the measures in place to protect against them. The report also includes guidance on using risk insights and coping analyses to screen and prioritize potential vulnerabilities.

The guidance draws from industry standards and practices, lessons learned, and related EPRI products. It describes recommended practices for assessing CCF susceptibilities and protecting against them for both safety and non-safety applications. Technical considerations include factors that affect the likelihood of both latent software defects and the triggering conditions that can activate them, including early requirements definition of unacceptable behaviors, hazards analysis, software development practices, test coverage, system and functional complexity, and designed-in defensive measures. The guidance addresses the common practice of combining previously segmented analog functions within single digital controllers, as well as the increasing practice of interconnecting digital controllers through communication networks and soft controls. The guidance includes a decision strategy for using coping analysis to investigate the effects of potential failures and misbehaviors in cases where a demonstration of coping capability might be an efficient way to provide assurance of adequate protection. Ultimately, the guideline approach relies on the use of engineering judgment to consider the available evidence and decide if the CCF risks have been managed adequately.