
RIC 2024 Hybrid
U.S. Nuclear Regulatory Commission
36th Annual Regulatory Information Conference
ADAPTING TO A
CHANGING LANDSCAPE
MARCH 12-14, 2024
Bethesda North Marriott Hotel
and Conference Center
Rockville, Maryland
#nrcric2024
www.nrc.gov

RIC 2024 Hybrid
U.S. Nuclear Regulatory Commission
36th Annual Regulatory Information Conference
MARCH 12-14, 2024
#nrcric2024
www.nrc.gov

Current Issues in Evaluating Common-Cause Failure of Digital Instrumentation and Control Systems in a Probabilistic Risk Assessment

Gerardo Martinez-Guridi
Reliability and Risk Analyst
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

Disclaimer: This digital exhibit has not been fully reviewed by the NRC staff, including management, and should not be understood as stating an NRC position on any particular technical subject or other matter.

- Digital instrumentation and control (I&C) systems comprise hardware and software, are very flexible, and can include many useful features.
- For a variety of reasons, including potential safety benefits, current licensees have upgraded or replaced some analog I&C systems in current nuclear power plants (NPPs), and designers of new and advanced NPPs of various technologies extensively employ DI&C systems.
- Since a DI&C system can be complex, however, it is difficult to perform rigorous evaluation of system failure probability using probabilistic risk assessment (PRA) methods in a typical application in an NPP.
- For this reason, models of a DI&C system in a PRA of an NPP in many cases have been simplified.

- One frequently used simplification in a PRA is to divide the assessment of the probability of system failure into the probability of failure of hardware and the probability of failure of software.
- This simplification is done for convenience. However, there may be some interactions between the failure of hardware and the failure of software.
- Even with this simplification, it is difficult to develop rigorous and practical techniques for assessing the probability of failure of hardware and the probability of failure of software. This is particularly true for the latter due to the software's complexity.

- Further, identical or similar hardware or software components in redundant trains or channels in a DI&C system may be subject to common-cause failure (CCF).
- In a PRA, CCF is a special form of dependent failure in which the failure of the structure, system, or component has occurred from the same fault.
- The evaluation of the probability of CCF in a PRA also typically uses the simplification of considering the CCF of hardware and of software separately.
- The probability of hardware CCF may be evaluated using the methods for CCF that have been employed in the nuclear industry for decades, provided relevant data are available.
- In the context of PRA, there is no widely accepted rigorous and practical method for evaluating the probability of software failure.
- Assessing the probability of software CCF using probabilistic methods is even more difficult than evaluating the probability of software failure for a single piece of software.

- Each software has its own characteristics. Hence, an evaluation of the probability of an individual software failure or of software CCF for one DI&C system may not be applicable to another DI&C system.
- In general, the failure characteristics of a DI&C system may not be applicable to another DI&C system because the systems may differ from each other.
- Over the years, measures have been implemented to reduce the probability of CCF in DI&C systems, but it is difficult to quantify the reduction in the probability of CCF in a PRA for the reasons stated above.
- Hence, currently, the probability of CCF in a DI&C system for use in a PRA may be considered to be 1. A case-specific assessment of the probability of failure of a DI&C system, including CCF, may be necessary to justify use of a lower probability in a plant-specific PRA.