U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Digital I&C Research Relating to Embedded Digital Devices

Bernard F. Dittman, Digital I&C Engineer

Office of Nuclear Regulatory Research,
Division of Engineering,
Instrumentation, Controls, and
Electrical Engineering Branch

Prepared for the
Public Workshop on the
Safe Use of Embedded Digital Devices

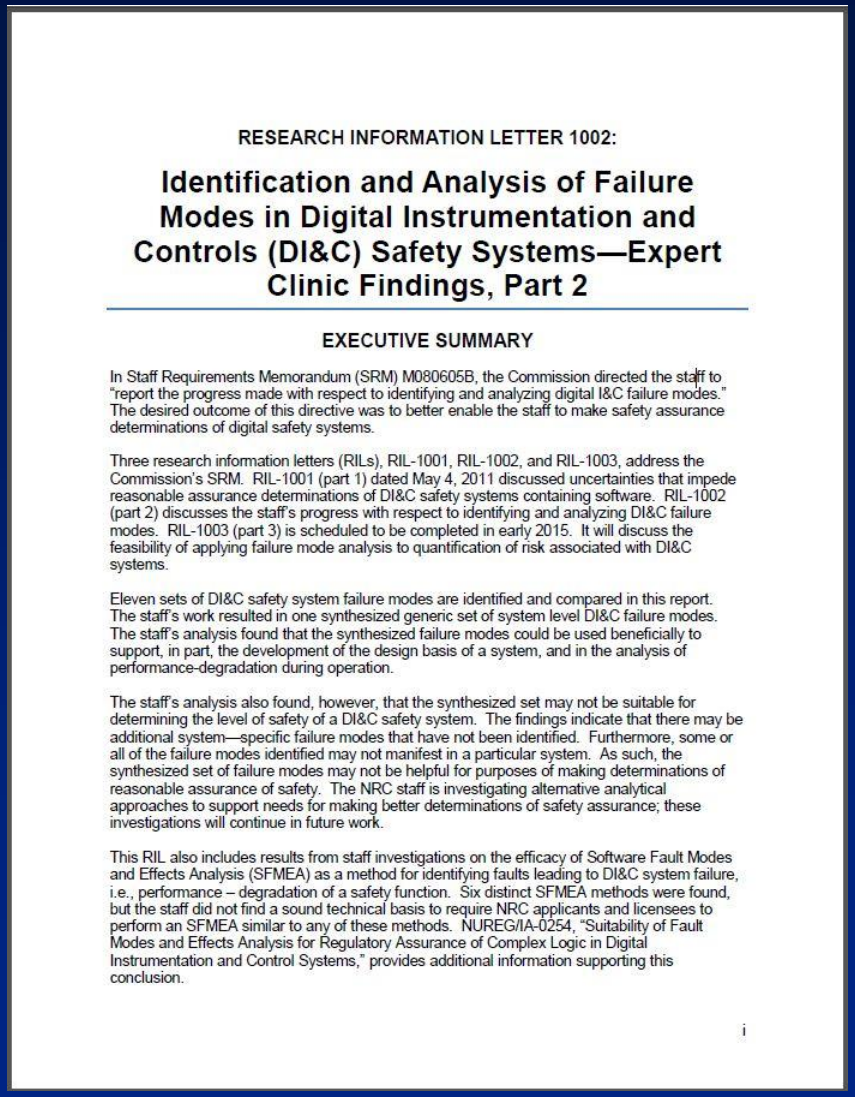
October 9, 2014
Rockville, MD USA

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Recent Research: Failure Modes in Digital I&C

Research Information Letter (RIL) 1002, "Identification and Analysis of Failure Modes in Digital I&C Safety Systems"

- September 3, 2014
- ADAMS Accession No. ML14197A201



RESEARCH INFORMATION LETTER 1002:

Identification and Analysis of Failure Modes in Digital Instrumentation and Controls (DI&C) Safety Systems—Expert Clinic Findings, Part 2

EXECUTIVE SUMMARY

In Staff Requirements Memorandum (SRM) M080605B, the Commission directed the staff to "report the progress made with respect to identifying and analyzing digital I&C failure modes." The desired outcome of this directive was to better enable the staff to make safety assurance determinations of digital safety systems.

Three research information letters (RILs), RIL-1001, RIL-1002, and RIL-1003, address the Commission's SRM. RIL-1001 (part 1) dated May 4, 2011 discussed uncertainties that impede reasonable assurance determinations of DI&C safety systems containing software. RIL-1002 (part 2) discusses the staff's progress with respect to identifying and analyzing DI&C failure modes. RIL-1003 (part 3) is scheduled to be completed in early 2015. It will discuss the feasibility of applying failure mode analysis to quantification of risk associated with DI&C systems.

Eleven sets of DI&C safety system failure modes are identified and compared in this report. The staff's work resulted in one synthesized generic set of system level DI&C failure modes. The staff's analysis found that the synthesized failure modes could be used beneficially to support, in part, the development of the design basis of a system, and in the analysis of performance-degradation during operation.

The staff's analysis also found, however, that the synthesized set may not be suitable for determining the level of safety of a DI&C safety system. The findings indicate that there may be additional system—specific failure modes that have not been identified. Furthermore, some or all of the failure modes identified may not manifest in a particular system. As such, the synthesized set of failure modes may not be helpful for purposes of making determinations of reasonable assurance of safety. The NRC staff is investigating alternative analytical approaches to support needs for making better determinations of safety assurance; these investigations will continue in future work.

This RIL also includes results from staff investigations on the efficacy of Software Fault Modes and Effects Analysis (SFMEA) as a method for identifying faults leading to DI&C system failure, i.e., performance – degradation of a safety function. Six distinct SFMEA methods were found, but the staff did not find a sound technical basis to require NRC applicants and licensees to perform an SFMEA similar to any of these methods. NUREG/IA-0254, "Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in Digital Instrumentation and Control Systems," provides additional information supporting this conclusion.

i

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RIL-1002

Table 13 Failure Mode Set L – Characterization of Failure Modes of a "Generic" Digital Safety System.

ID	Failure Mode	Elaboration	Remarks/Mapping
L.1	No output upon demand	Includes no change in output or no response for any input	⇒A.2
L.2	Output without demand	e.g., Unwanted response	⇒A.3
L.3	Output value incorrect	Incorrect response to input or set of inputs	⇒A.2 Includes: • Value too high or too low; Value stuck at previous value, e.g., ON, OFF
L.4	Output at incorrect time	Too early; Too late.	⇒A.1

▪ ▪ ▪

- Identifies and compares digital I&C failure modes
- Provides a synthesized generic set of system level digital I&C failure modes,

  Failure Mode Set L

- This set may be useful when developing a system's design basis and analyzing degradation of its performance.

Relevance: EDD failure modes could degrade a safety function of a digital I&C safety system.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

On-Going Research: Hazard Analysis of Digital I&C

Research Information Letter 1101

- Provides technical basis to review hazard analysis of digital safety systems

- Will be issued this year
- Draft available ADAMS Accession No. ML13232A001
- ADAMS Accession No. will be ML14237A359 when issued

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RIL-1101

- Highly-integrated digital I&C systems provide increased opportunity for unsafe behavior due to systemic causes.
- Traditional techniques don’t address systemic causes or their contribution to safety function degradation.
- Application of hazard analysis techniques can address systemic causes.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RIL-1101 (continued)

- Identifies ways to address systemic degradation of safety functions, which could otherwise occur, throughout the system's lifecycle.
- Supports reducing the overall hazard space.
- Promotes analyzability of digital I&C safety systems and their safety functions.

Relevance: EDDs could increase the overall hazard space or cause a digital safety system's safety function to become unanalyzable.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Future Research: Designed-in Assurance

- Proof-of-concepts for Digital I&C Safety Systems:
  - Explicit identification of properties essential to safety
  - Model-based design to specify and evaluate these properties
  - Refinement of specifications that preserve properties
  - Mathematical analysis to demonstrate properties are satisfied under the specified conditions
  - Demonstration that a system is correct by construction

Relevance: These techniques could provide a means to ensure EDDs do not degrade a safety function or lead to an unanalyzable safety system.