UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 13, 2015

MEMORANDUM TO: Glenn M. Tracy, Director
Office of New Reactors

FROM: Brian Sheron, Director **/RA/**
Office of Nuclear Regulatory Research

SUBJECT: TRANSMITTAL OF RESEARCH INFORMATION LETTER RIL-1101, "TECHNICAL BASIS TO REVIEW HAZARD ANALYSIS OF DIGITAL SAFETY SYSTEMS"

The Office of Nuclear Regulatory Research (RES) is providing this Regulatory Information Letter (RIL) under User Need Request (UNR) NRO-2011-009, "Hazard Analysis – Development of Technical Basis and Recommendations for Review Guidance for Digital Instrumentation and Control Systems," [Agencywide Documents Access and Management System (ADAMS) Accession No. ML11313A214]. In this UNR, the Office of New Reactors (NRO) asked RES to support improving regulatory guidance for evaluation of an applicant's hazard analysis of digital instrumentation and control (I&C) systems. RIL-1101 is the first of two UNR deliverables. It can be used to integrate hazard analysis into the mPOWER™ iPWR Design-Specific Review Standard (DSRS) Chapter 7. Use of RIL-1101 does not depend on the second UNR deliverable. A separate memo will address the second UNR deliverable.

The enclosed RIL-1101, "Technical Basis to Review Hazard Analysis of Digital Safety Systems," (ADAMS Accession No. ML14237A359) provides the technical basis to support NRC staff reviews of hazard analyses performed by licensees and applicants. RES staff obtained and assimilated information through extensive literature reviews and subject matter expert consultations to produce RIL-1101.

Hazards are the potential for harm. Examples of plant level hazards include radiological consequences leading to disease, loss of life, or damage to the environment. To prevent these hazards, nuclear power plant I&C systems maintain plant processes within acceptable performance limits by making reliable, accurate, and timely measurements that lead to reliable, accurate, and timely control actions. Using redundant, independent, electrically-isolated, and physically-separated components, I&C safety systems sense plant conditions and actuate controls before a limiting safety setting is exceeded to preserve fuel and reactor vessel integrity.

CONTACT: Bernard Dittman, RES/DE/ICEEB
301-251-7494

Digital I&C systems differ from their analog and mechanical counterparts. Rapid changes in digital technology prevent the accumulation of the kind of operating history that applies to analog and mechanical systems. Many unsafe behaviors of digital I&C systems do not relate to physical principles like those used to evaluate the safety and reliability of analog and mechanical systems. Instead, malfunctions of digital I&C systems more often arise from systemic causes associated with characteristics of their design and development. These characteristics can also make verification of digital I&C systems—to the same degree as analog or mechanical systems—unfeasible. Additionally, unlike systems where interconnections and dependencies are readily apparent as wires and pipes to a reviewer or inspector, digital I&C systems can contain less obvious interconnections and dependencies. These more subtle attributes can degrade the safety benefit presumed to exist through redundant, independent, electrically-isolated, and physically-separated safety components.

In RIL-1101, the staff provides examples of system hazards and factors that contribute to degrading the safety function of a digital I&C system. To address hazards rooted in systemic causes, RIL-1101 provides conditions—for each lifecycle stage of a digital I&C system—to reduce the hazard space by addressing factors that contribute to digital I&C safety degradation. These conditions include characteristics and constraints that apply to organizations, processes, and methods used in digital I&C system design and development.

This RIL may be used by NRO licensing staff to develop and support review guidance for a pilot project reviewing new digital technologies in small modular reactors. As RIL-1101 was being developed, RES staff identified opportunities to further support the licensing review staff by improving the effectiveness and efficiency of digital safety system regulatory reviews. These opportunities are being integrated into RES research activities within the I&C Research Plan. Your staff is engaged in planning these activities and you will be informed of these activities.

Staff in the Office of Nuclear Regulatory Research, Division of Engineering (RES/DE) conducted this research. RES provided several draft versions of RIL-1101 to your staff for review, and their comments were addressed throughout the generation of the report. The RES/DE staff is especially thankful for the contributions of Daniel Santos (formerly of NRO) and Norbert Carte of NRR. RES/DE staff is available to provide a presentation to you and your staff that covers the information contained in RIL-1101.

The development of RIL-1101 included peer reviews by qualified, independent, and external specialists. These peer reviews followed Management Directive 3.17, "NRC Information Quality Program," along with the referenced Office of Management and Budget bulletin and guidelines, to ensure the utility, integrity, and objectivity of the RIL-1101.

RES has established an online quality survey with which requesting offices are asked to evaluate the usefulness of RES products and services. This survey can be found on the right-hand side of http://www.internal.nrc.gov/RES/, under the link for “RES Quality Survey.” If your office has not yet completed this brief survey, I would appreciate your support in ensuring its completion within the next 10 working days.

Enclosure:
As stated

RES has established an online quality survey with which requesting offices are asked to evaluate the usefulness of RES products and services. This survey can be found on the right-hand side of http://www.internal.nrc.gov/RES/, under the link for "RES Quality Survey." If your office has not yet completed this brief survey, I would appreciate your support in ensuring its completion within the next 10 working days.

Enclosure:
As stated

DISTRIBUTION:

DE/rf	R. Correia, RES
J. Tappert, NRO	T. Jackson, NRO
I. Jung, NRO	J. Ashcraft, NRO
W. Dean, NRR	J. Lubinski, NRR
J. Thorp, NRR	N. Carte, NRR
S. Arndt, NRR	

ADAMS Accession No.: ML14237A342

OFFICE	RES/DE/ICEEB	RES/DE	RES/DE/ICEEB	TECH EDITOR	D: RES/DE	D: RES
NAME	B. Dittman	S. Birla	R. Sydnor	(via email) QTE	B. Thomas	B. Sheron
DATE	09/17/14	12/11/14	12/16/14	09/17/14	12/31/14	2/13/15

OFFICIAL RECORD COPY