APPROACHES TO PERMITTING THE USE OF DIGITAL INSTRUMENTATION AND CONTROLS IN SAFETY APPLICATIONS

A Report for the House and Senate Committees on Appropriations

By the U.S. Nuclear Regulatory Commission

December 27, 2018

Enclosure

I. INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) developed this report as directed by the Joint Explanatory Statement accompanying the Energy and Water, Legislative Branch, and Military Construction and Veterans Affairs Appropriations Act, 2019 (Public Law 115-244). The Joint Explanatory Statement directed the NRC to submit to the House and Senate Appropriations Committees a report describing approaches to permitting[1] the use of digital instrumentation and controls (I&C) in safety applications outside of the nuclear industry and discussing whether these approaches would be acceptable in nuclear applications. In response to this direction, the NRC has evaluated the approaches used in the civil aviation, automobile, and medical device industries to permit the use of digital I&C and the results are described below focusing on the safety significance involved in each industry as compared to operating nuclear power reactors.

II. BACKGROUND

The NRC evaluates digital I&C systems for use in nuclear reactors as part of its safety reviews of applications for reactor design certifications, combined licenses, operating licenses, and license amendment requests.

The NRC's current regulations provide flexibility for applicants and licensees to use alternatives or request exemptions to the established performance-based requirements. The NRC has incorporated by reference into its regulations several consensus standards developed with industry experts to provide regulatory requirements for particular areas. Specifically for I&C, the NRC has codified the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-1991,[2] "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which establishes minimum functional design criteria for I&C and electrical safety systems. This standard also requires the use of key design criteria, such as independence, isolation, and single-failure tolerance, for plant safety system designs. The NRC's regulations allow applicants and licensees to use alternatives to IEEE Standard 603-1991 as long as a commensurate level of safety and quality can be demonstrated, an option that allows design flexibility. The NRC has published voluntary guidance that describes one method to satisfy regulatory requirements. This guidance endorses consensus standards, including ones that are digital-specific. While this guidance does not represent the only way to satisfy regulatory requirements, it does provide some predictability in the NRC's approach to reviewing I&C features in applications.

The NRC has established a process for dedicating commercial-grade systems and components for use in nuclear safety applications. The NRC also reviews generic digital I&C platforms (some of which were developed for commercial applications) that can subsequently be used for nuclear safety applications. An NRC-approved digital I&C platform can be used by operating nuclear power plants performing digital upgrades of existing safety-related I&C systems and by new reactor licensees in their digital I&C safety applications. The NRC continues to place a high priority on making progress on digital I&C issues so that potential safety benefits can be realized by properly implementing digital I&C upgrades.

---

[1] The Joint Explanatory Statement and this report use the terms "approaches to permitting digital I&C." It should be noted that the regulatory authorities discussed in this report may use other terms such as "regulatory approval" or "certification."

[2] IEEE Std. 603-1991 is an industry consensus standard that is incorporated by reference in 10 CFR 50.55a(h) as part of the requirements for I&C and electrical systems in nuclear power plants. The design criteria within this standard are not specific to the technology employed (e.g. analog vs. digital).

The NRC recently issued Regulatory Issue Summary (RIS) 2002-22, Supplement 1[3] to further detail whether prior NRC approval is required for digital I&C modifications. The NRC is currently developing improved guidance for NRC staff review of LARs to allow for approval of the LAR earlier in the system development process. Under the new process, licensees would not need to wait for completion of the system testing to receive the NRC staff's approval.

The NRC has conducted research studies about how the experience and practices of other industries can be leveraged in the licensing of digital I&C equipment used for nuclear safety applications. For example, the NRC has conducted research[4] on methods to determine the degree to which diversity is considered sufficient to mitigate common cause failure vulnerabilities that may arise from digital I&C safety system designs. As a part of this research, the NRC evaluated approaches used for high-integrity and safety-significant I&C applications in non-nuclear industries that have already transitioned to digital I&C systems. The NRC investigation focused on industries that employ similar I&C technologies and have applications with high consequence hazards. Methods to incorporate diversity that are employed within the aerospace, aviation, chemical process, and rail transportation industries were evaluated. Such methods were described within guidance developed by the National Aeronautics and Space Administration, the FAA, and the Center for Chemical Process Safety. The results of this NRC study revealed that although none of the other high-consequence industries have applications directly analogous to the nuclear power industry, in most cases the methods of addressing common cause failure through diversity used by these non-nuclear industries were comparable to the approaches used in the nuclear power industry. When attempting to transfer regulatory evaluation methods from non-nuclear industries to the nuclear industry, the NRC will need to consider inherent technical and regulatory oversight differences.

The NRC has also assessed approaches used by nuclear regulatory authorities from other countries for digital I&C permitting. For example, the NRC has participated in the Working Group on Digital I&C (WGDIC)[5] within the Nuclear Energy Agency's (NEA's) Committee on Nuclear Regulatory Activities. This effort was formed to promote harmonization and improvements in nuclear safety through the development of consensus positions to address digital I&C topics and technical issues of concern to NEA member countries, for both operating and new reactors. From this effort, the NRC gained valuable insights into how regulatory authorities from other countries permit the use of digital I&C systems and equipment for nuclear safety applications. One insight gained is that there is a universal recognition that defense-in-depth and diversity provisions are needed to protect against potential common cause failure vulnerabilities that could challenge plant safety. However, nuclear regulatory authorities from different countries accept a variety of methods for demonstrating that common cause failure vulnerabilities are adequately addressed. The NRC is exploring how the permitting approaches used by these regulatory authorities can be incorporated into the NRC's digital I&C regulatory framework to support a more safety-focused review.

---

[3] RIS 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems." A RIS is used to (1) communicate and clarify NRC technical or policy positions on regulatory matters that have not been communicated to or are not broadly understood by the nuclear industry, (2) inform the nuclear industry of opportunities for regulatory relief, (3) communicate previous NRC endorsement of industry guidance on technical or regulatory matters, (4) provide guidance to applicants and licensees on the scope and detail of information that should be provided in licensing applications to facilitate NRC review, and (5) request the voluntary participation of the nuclear industry in NRC-sponsored pilot programs or the voluntary submittal of information which will assist the NRC in the performance of its functions.

[4] NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," February 2009.

[5] The Working Group on Digital I&C was formerly known as the Multinational Design Evaluation Program, Digital Instrumentation and Controls Working Group.

III. COMPARISON OF APPROACHES TO PERMITTING THE USE OF DIGITAL I&C IN SAFETY APPLICATIONS

Safety-critical industries, such as the civil aviation, medical device, automobile, railroad, and chemical process industries, and the military, have adopted the use of digital I&C technologies. However, not all of the industries are subject to an explicit permitting process or regulatory approval for the equipment used in their respective safety applications. This report focuses on the civil aviation, automobile, and medical devices industries because, similar to the civilian nuclear sector, these industries are subject to regulations that require permitting for digital I&C within the broader process of certifying or licensing a whole device or system to assess if application of these components satisfies the relevant safety goals, objectives, and requirements.

A. CIVIL AVIATION

The Federal Aviation Administration's (FAA's) permitting approach, known as its design approval, uses a combination of mandatory requirements and voluntary guidance. The process[6] consists of five phases, each with different levels of engagement between the applicant and FAA, to increase efficiency. One practice used by FAA is the appointment of designated engineering representatives[7] as third party verifiers for the aircraft. This representative may approve or recommend approval of technical data to the FAA in support of aircraft certification. Safety-critical equipment applicable to each certified aircraft must receive approval by the FAA, using a rigorous process demonstrating that the equipment design is appropriate for the equipment's intended functions. At its highest-level, FAA guidance provides a general safety assessment process and includes the ability to apply gradations to development and test activities. Airworthiness regulations[8] for instrument systems of the certified aircraft specify the use of the design principles of single-failure proof designs, independence, and equipment isolation. The FAA has published advisory circulars that recognize voluntary consensus standards for aircraft avionics equipment to address the permitting process for each airframe as a part of the overall aircraft certification process.[9] These voluntary industry consensus standards and recommended practices are coordinated internationally.

For digital I&C specific guidance, Advisory Circular 20-115D[10] recognizes DO-178C, "Software Considerations in Airborne Systems and Equipment Certification," as one consensus standard that supports satisfying airworthiness requirements for airborne systems relating to the production of software. DO-178C applies a graded approach for classifying the software based on the consequences to the aircraft, crew, and passengers due to software failure. Any software that commands, controls, and monitors safety-critical functions is most likely assigned to the highest software level (i.e., its failure may result in catastrophic consequences, including deaths and loss of the airplane). The rigor of software design requirements and development/testing activities is based on the classification of the software. To improve

---

[6] The FAA and Industry Guide to Product Certification, Third Edition, 2017.

[7] A designated engineering representative is an individual, appointed in accordance with 14 CFR 183.29, who holds an engineering degree or equivalent, possesses technical knowledge and experience, and meets the qualification requirements of Order 8100.8.

[8] 14 CFR § 25.1309, "Equipment, systems, and installations" is an example of an airworthiness regulation.

[9] 14 CFR Part 21, "Certification Procedures for Products and Articles."

[10] The FAA's Advisory Circular AC 20-115D, "Airborne Software Development Assurance Using EUROCAE ED-12() and RTCA DO-178()," recognizes DO-178C as an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations.

efficiency, the FAA also established a method for approving "Integrated Modular Avionics" as a way to allow an approved generic digital platform to be used for many aircraft applications.

There are many similarities in the high-level regulatory requirements (e.g., single-failure tolerant designs, independence, and equipment isolation) between the nuclear power and civil aviation industries. In addition, both the FAA and the NRC endorse consensus standards as voluntary guidance that applicants and licensees can use to satisfy regulatory requirements. Specific to digital I&C, both the FAA and the NRC have established methods for permitting generic digital I&C platforms that can be used for a variety of safety applications.

Several elements from the FAA's permitting approach could apply to the NRC's digital I&C permitting approach. For example, the NRC could adopt a more graded approach to digital I&C equipment classification that is based on the consequence of the equipment's failure to overall plant safety, with an appropriately applied set of design, development, and testing requirements. The use of third party certifiers is another FAA concept the NRC could adopt as a way to address key critical characteristics required of devices that are dedicated for safety applications under the NRC's commercial grade dedication process. The NRC is considering these elements as part of the overall digital I&C regulatory framework modernization efforts and has held periodic interactions with the FAA to facilitate this effort. The NRC anticipates meeting at the staff level with the FAA on this subject again at the end of January 2019.

B. AUTOMOBILE

The National Highway Traffic Safety Administration (NHTSA) regulates motor vehicle safety under National Traffic and Motor Vehicle Safety Act.[11] The NHTSA has published the Federal Motor Vehicle Safety Standards[12] on design, construction, performance, and durability requirements for motor vehicles and regulates automobile components, systems, and design features. The NHTSA has created a self-certification approach for demonstration of regulatory compliance, in which vehicle and equipment manufacturers certify that their products meet applicable standards. The NHTSA does not pre-approve new motor vehicles or new motor vehicle technologies. For example, in the case of Automated Driving Systems, the NHTSA uses its existing regulatory tools, including interpretations, exemptions, notice-and-comment rulemaking, and defects and enforcement authority. However, the NHTSA has published voluntary guidance[13] to help designers of these systems to analyze, identify, and resolve safety considerations prior to deployment using their own, industry, and other best practices. This voluntary guidance contains elements on the use of a digital I&C system, including performance of a hazard analysis for the Automated Driving Systems, design redundancies, and well-planned software development. The NHTSA regulation requires reporting of safety-related defects and non-compliance and allocating responsibility (between vehicle and equipment manufacturers) for recalling and remedying defects and non-compliance with the law.

The NHTSA's permitting approach has certain aspects that are comparable to the NRC's, including establishment of high-level regulatory requirements and mandatory reporting of safety-related defects of components. The NRC is reviewing how certification of commercially available digital hardware and software by independent third parties with demonstrated expertise and experience can be leveraged in the NRC's overall permitting approach. As

[11] The National Traffic and Motor Vehicle Safety Act has been codified under Title 49 United States Code (USC) Chapter 301: Motor Vehicle Safety.
[12] Federal Motor Vehicle Safety Standards are codified in 49 CFR Part 571.
[13] Automated Driving Systems 2.0: A Vision for Safety.

previously mentioned, the NRC is currently evaluating whether the results of such third-party certifications may be relied on as one way to address key characteristics of devices that are dedicated for safety applications under the NRC's commercial grade dedication process. While the NHTSA's self-certification approach aligns with the product-based nature of the automobile industry (where a single vehicle design can be certified for use and then mass-manufactured for sale), it is fundamentally inconsistent with the NRC's overall permitting approach for nuclear power plants. The NRC will continue to engage with NHTSA to learn about modernizations of the administration's regulatory permitting approach and is coordinating staff-level meetings in the near term.

C. MEDICAL DEVICES

The U.S. Food and Drug Administration (FDA) regulates the sale of medical devices marketed in the United States under the Federal Food, Drug and Cosmetic Act and applicable regulations.[14] Medical devices are categorized into one of three classes, based on the degree of risk they present. Class I represents those that present the lowest risk to patients (e.g., hand-held instruments), and Class III represents those that present the highest risk to patients (e.g., implantable pacemakers). Depending on the device classification, the applicant provides the appropriate premarket submission under the portions of the law that are applicable to that device. The FDA also publishes voluntary guidance, including guidance on the use of voluntary consensus standards.[15] A device manufacturer may choose to rely on applicable consensus standards[16] or address issues relevant to permitting in another manner. The use of consensus standards generally only satisfies a portion of a premarket submission. For digital or software-based medical devices, the FDA specifies that in addition to device testing, device manufacturers should conduct appropriate analyses and reviews to avoid errors that may affect operational safety. The premarket submission must include an analysis that identifies the hazards associated with the device, the method of control (hardware or software), the safeguards incorporated, and the identified level of concern.

Some aspects of the medical device permitting approach are similar to the NRC's process, including providing high-level regulatory requirements and endorsement of consensus standards as one way to meet requirements. However, the FDA's process provides a more graded approach for the demonstration of safety and regulatory compliance based on risk. In addition, the performance and evaluation of a hazard analysis has a significant role in the FDA's regulatory process. This risk-informed and hazard analysis-focused approach could be incorporated into the NRC's digital I&C regulatory framework. Currently, the NRC is working to risk-inform practices in the NRC's permitting approach for digital I&C.[17] Although current NRC requirements (e.g., IEEE Std. 603-1991) require the identification of hazards, the NRC staff continues to review hazard analysis methods, such as those required by FDA, for incorporation into the NRC's regulatory guidance for digital I&C.

---

[14] 21 CFR Parts 1-58, 800-1299.

[15] Appropriate Use of Voluntary Consensus Standards in Premarket Submissions for Medical Devices Guidance for Industry and Food and Drug Administration Staff, 2018, available at https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm418448.htm.

[16] FDA publishes a set of recognized consensus standards for medical devices.

[17] The NRC published Design-Specific Review Guidance for NuScale, which adopts a risk-informed approach for safety and compliance demonstration, particularly in the area of I&C.

IV. NRC'S STRATEGIC PLAN FOR PERMITTING THE USE OF DIGITAL I&C IN SAFETY APPLICATIONS[18]

As part of the agency's digital I&C integrated action plan strategic review, the NRC has identified several activities that take into consideration the challenges and potential impediments that may be unique to specific digital I&C applicants. The NRC plans to complete a strategic assessment to identify significant structural changes to the regulations and accompanying guidance that take a performance-based, risk-informed, and graded approach. This effort will also explore potential alternative standards for NRC endorsement, such as international nuclear standards like the International Electrotechnical Commission (IEC) 61513, "Nuclear Power Plants-Instrumentation and Control Important to Safety - General Requirements for Systems." Given the more graded approach IEC nuclear standards have taken for classification of I&C equipment with an appropriate set of design and development criteria, adopting these standards could potentially enhance incorporation of these elements from the FAA's and FDA's permitting approach. As part of this digital I&C regulatory framework strategic improvement project, the NRC is evaluating approaches for improved licensing methods, including those used within non-nuclear safety-critical industries and the military, to develop a performance-based and risk-informed regulatory infrastructure that will anticipate the evolution and future development of digital I&C technology as it is applied to nuclear safety applications.

V. SUMMARY

The NRC recognizes the advantages, including the safety benefits, of using digital technology in nuclear safety applications and continues to adapt the regulatory framework for licensing the use of digital technology in the nuclear industry. As part of the broader initiative on the digital I&C regulatory framework, the NRC continues to evaluate other ways in which processes to permit the use of digital I&C in safety applications outside of the nuclear industry may be incorporated into the NRC's regulatory framework. The NRC has made changes to several aspects of the digital I&C permitting approach. The NRC will continue to develop risk-informed, safety-focused approaches for permitting digital I&C for nuclear power plant safety applications in a manner that provides adequate protection of the public health and safety and the common defense and security.

[18] Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure, Revision 2, 2018.