BOEING 737 CRASHES: LESSONS LEARNED FOR NRC DIGITAL INSTRUMENTATION AND CONTROLS EVALUATION PROCESS

September 22, 2022

What We Looked At

In 2017, the Federal Aviation Administration (FAA) certified a redesigned version of Boeing 737, called the 737 MAX 8. This new certified design included a new automated Maneuvering Characteristics Augmentation System (MCAS) to automatically counteract potential stall conditions associated with new aerodynamics of the plane. In October 2018 and March 2019, two MAX 8 aircraft crashed because of repeated MCAS activation. Investigative reports from several authorities examined and identified a series of failures associated with the development, review, implementation, training, and oversight for the MCAS that led to the aircraft crashes.

The U.S. Nuclear Regulatory Commission (NRC) is responsible for ensuring the safe incorporation of digital instrumentation and controls (I&C) technologies into nuclear power plants. The investigative reports about the MCAS design process and FAA certification processes generated lessons potentially applicable to the NRC digital I&C regulatory process. The NRC's I&C staff, in coordination with its human factors engineering (HFE) and risk analysis staffs (henceforth referred to as "the NRC team"), systematically evaluated the findings and recommendations in these investigative reports for their potential implementation in the NRC's digital I&C regulatory process. This evaluation considered the significant differences between the aviation and nuclear industries in several areas, including but not limited to industry scale, design and safety objectives, and regulatory frameworks.

The NRC team focused on (1) identifying potential regulatory gaps in digital I&C licensing and inspection, including associated processes and culture, and (2) identifying elements of the NRC's regulatory oversight and organizational capabilities that should be maintained or improved to support the continued safe use of digital I&C in nuclear power plants. The objective of the NRC team's review was to assess (1) the processes used to introduce new digital I&C technologies into nuclear power plant architectures and (2) the development of highly integrated I&C systems for new reactors.

What We Found

As summarized in this report, the aircraft crashes were the result of several engineering, programmatic, and safety culture failures that resulted in significant flaws in MCAS implementation. The NRC team found it challenging to make an in-depth technical comparison of the safety functions, failure consequences, defense in depth, and risks of an aircraft avionics system to those associated with the digital controls and protection systems at a nuclear power plant.

The NRC team found that no significant gaps exist in the NRC's regulatory infrastructure for digital I&C licensing and inspection as related to the findings and recommendations of the reports. However, based on the investigative report findings, the NRC team identified aspects of the agency's digital I&C regulatory program and organizational capabilities that should be maintained or further improved to ensure the continued safe use of evolving digital I&C technologies in nuclear power plants.

Our Recommendations

Based on the assessment documented in the "Evaluation Summary" and "Regulatory Insights and Recommendations" sections of this report, the NRC team recommends focusing on the following areas to continue to improve digital I&C licensing and regulatory oversight:

- The NRC should continue to improve integration and communication among digital I&C technical reviews, HFE reviews, and subsequent inspection oversight for new or significantly different applications from conception to installation.

- The NRC should continue to improve our oversight programs for digital I&C modifications that are implemented through Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, “Changes, tests and experiments,” that do not require prior NRC approval.

- The NRC should develop guidance for assessing the systems engineering approaches for the digital I&C design and human factors life-cycle evaluation, which are important for ensuring that approved digital I&C designs are appropriately integrated to maintain safety functionality.

- The NRC should explore potential avenues for increasing the collection and communication of digital I&C operating experience to enable application in a quantitative assessment of digital I&C systems in the licensing and oversight processes.

The NRC team recommends maintaining and emphasizing the following NRC program and organizational capabilities in the NRC I&C community:

- A robust and effective safety culture that allows the agency to effectively fulfill its core regulatory and oversight mission to support the continued safe use of digital I&C in nuclear power plants

- A defense-in-depth regulatory approach, with consideration of risk insights and appropriate use of diversity, to mitigate unforeseen digital I&C failures that could adversely impact safety functions

- Knowledge management and the continuous assessment of digital I&C program effectiveness

- Oversight of risk-significant non-safety-related systems and evolving technologies involving highly integrated non-safety-related control systems; specifically, use of a safety-focused review approach should continue

- Application of guidance that allows for a performance-based approach that is technology neutral rather than a prescriptive approach to regulatory guidance

- Continued emphasis on integrated review teams for safety-significant digital I&C modernization license amendment requests

- Continued periodic joint seminars on regulatory approaches for digital technology to be conducted with participants from international and domestic regulators of safety-critical industries

Introduction

BOEING 737 MCAS DEVELOPMENT AND CERTIFICATION CONSIDERATIONS

Boeing installed, larger, more fuel-efficient engines on a new 737 derivative aircraft, referred to as the 737 MAX (Ref. 1), to improve flight economy. The MCAS was one of many upgrades associated with the new Boeing 737 MAX 8 to address significant changes in aerodynamics. The FAA began its review of an amended-type certificate (ATC) application in 2012 and issued its approval in March 2017 (Ref. 2).

Ground clearance constraints required relocation of the physically larger engines to a position forward of the leading edge of the wing. As a result, the aircraft aerodynamics changed, particularly during maneuvers with a high angle of attack (AoA).[1] In particular, if engine thrust were applied while the aircraft was pitched upward at a high AoA, the airplane could pitch up even more and result in an aerodynamic stall (Ref. 3). To address this issue absent other mechanisms, pilots would need to push the nose of the aircraft downward.

To compensate for these flight conditions automatically, Boeing developed the MCAS flight control augmentation system computer software to adjust the aircraft's trim system during manual flight when the 737 MAX reached a limited set of flight configurations involving a high AoA (Ref. 3). The system was specifically designed to automatically (i.e., "uncommanded") counteract additional nose pitch resulting from the larger engine upgrades by adjusting the horizontal stabilizer to pitch the aircraft back down when the AoA sensor exceeded a threshold based on airspeed and altitude. The goal of this modification was to eliminate the need for pilot simulator training requirements by making the aircraft feel and handle exactly like the previous Boeing 737 Next Generation versions to which pilots around the world were already accustomed.

Based on probability and qualitative consequence assumptions, Boeing did not rank MCAS in the highest risk category in the Boeing 737 MAX 8 certification request (Ref. 3). Boeing performed a functional hazard assessment of the software, including a spurious MCAS activation that continued until the pilot took action. While not its intent, the MCAS under failure conditions would have the effect of moving the aircraft's nose down during manual flight if not counteracted by the pilot. Boeing pilots and engineers assumed that commercial pilots would recognize the effect of unintended MCAS activation as a "runaway stabilizer" condition, which is a scenario addressed in commercial pilot training. Boeing tested a single, unintended activation of MCAS and assumed multiple activations of MCAS to be no worse than a single activation (Ref. 4).

The FAA determined that the certification of the MCAS design could be delegated to Boeing using a self-certification process controlled through the FAA's Organization Designation Authorization (ODA) program (Ref. 2). Boeing conducted specific design, implementation, integration, and testing activities in a life-cycle development process for the MCAS. As a result of flight testing, the MCAS was later programmed to also counteract accidental low-speed stalls, with more aggressive authority to increase the rate of down pitch based on AoA sensor information (Ref. 3).

While the Boeing 737 MAX is equipped with two AoA sensors, the MCAS software used input from only one of these sensors (Ref. 3). Boeing had intended for the avionics of all 737 MAX 8 aircraft to be equipped with an alert to pilots when two AoA sensors disagreed by more than 10 degrees for at least 10 seconds. Following certification by the FAA, Boeing discovered that not all 737 MAX aircraft avionics were equipped with this alert but concluded that a cockpit alert was not necessary for safe aircraft operation because no required pilot procedures were associated with the alert. Boeing intended to correct this problem for the entire fleet but was not required to submit a formal notification to the FAA oversight office because it was not deemed to have an

[1] Angle of attack is the angle between the wing mean aerodynamic chord and the direction of relative wind (Ref. 3).

operational impact (Ref. 4). As a result, the FAA did not become aware of this issue until after the Lion Air crash in 2018 (Ref. 4).

Pilots received no flight simulator training on this MCAS feature because Boeing assumed that a pilot would respond to an MCAS-related performance failure in a manner similar to a failure in the automatic trim controls of the horizontal stabilizer, known as runaway stabilizer (Ref. 3). However, with an MCAS performance failure, pilots were challenged to respond in a timely manner due to the difficulty of recognizing it as such (Ref. 1, 3). They were also challenged to manually adjust the horizontal stabilizer to counteract high aerodynamic forces.

MCAS FAILURE

On October 29, 2018, Lion Air Flight 610 crashed into the Java Sea shortly after departing Soekarno-Hatta International Airport, Jakarta, tragically resulting in 189 fatalities. The MCAS response was determined to be a significant contributor to the accident, as it activated approximately 24 times during the flight after receiving faulty data from one of the aircraft's two AoA sensors (Ref. 3). A few months later, on March 10, 2019, Ethiopian Air Flight 302 crashed shortly after departing Addis Ababa Bole International Airport, resulting in 157 fatalities. The reports listed in the "Evaluation Summary" section of this report contain in-depth information on the details of the accident events, technical design and human factors issues, and regulatory issues.

Attributes of NRC Licensing and FAA Certification Approaches

The FAA is responsible for regulating aviation safety, which includes approving the design and manufacture of new aircraft and aviation products before they enter air commerce. Safety-critical equipment applicable to each certified aircraft must receive FAA approval, using a rigorous process demonstrating that the equipment design is appropriate for the equipment's intended functions. At its highest level, FAA's guidance provides a general safety assessment process and includes the ability to apply gradations to development and test activities (Ref. 5). Airworthiness regulations (Ref. 6) require that systems and components, considered separately and in relation to other systems, must be designed so that any failure that would prevent the continued safe flight and landing of the aircraft is extremely improbable. 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 (Ref. 7). These voluntary industry consensus standards and recommended practices are coordinated internationally.

The FAA's design approval process includes mandatory requirements and voluntary guidance. The process consists of five phases (Ref. 8) with varying levels of FAA engagement. Through the ODA program, the FAA is authorized to appoint designated engineering representatives[2] as third-party verifiers for the aircraft. These representatives may approve or recommend approval of technical data to the FAA in support of aircraft certification. The ODA program requires that unit members are in a position that provides sufficient authority and time to perform duties without pressure or influence from other parts of the organization and must have no conflicting restraints while performing authorized functions. (FAA Order 8100.15A) The following is an example of the number of staff involved to review a design change to a particular aircraft type:

> Under FAA's ODA program, the Agency's Boeing Aviation Safety Oversight Office (BASOO) provides oversight of authorized functions granted to Boeing. The BASOO is comprised of 45 FAA employees who oversee Boeing's ODA…. The Boeing ODA unit includes approximately 1,500 Boeing-designated ODA representatives. FAA's oversight program is based on managing and supervising an organization, rather than overseeing individual designees. (Ref. 11)

[2] A designated engineering representative is an individual, appointed in accordance with 14 CFR 183.29, "Designated engineering representatives," (Ref. 9) who holds an engineering degree or equivalent, possesses technical knowledge and experience, and meets the qualification requirements of FAA Order 8100.8, "Designee Management Handbook." (Ref. 10)

The ODA program permits the FAA to delegate the certification of well-understood, noncritical, or low-risk designs so the FAA can remain directly involved in the review and approval of higher risk items, such as safety-critical or “new and novel” designs (Ref. 2). Nonetheless, the FAA bears ultimate responsibility for ensuring new aircraft designs are safe and comply with airworthiness standards. Such a delegation practice is not limited to the FAA, as civil aviation authorities worldwide implement similar delegation programs to leverage the product-specific knowledge of manufacturers’ qualified employees to determine a product’s compliance with government regulations and requirements. The 45 FAA and 1500 Boeing personnel at the BASOO performing ODA-related activities were in addition to the main FAA staff who performed the review of the ATC application. The review and approval process for a design change, such as the ATC for the Boeing 737 MAX 8, requires about 5 years to complete.

The NRC licenses and regulates the U.S. civilian use of radioactive materials to provide reasonable assurance of adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. In support of this mission, the NRC is responsible for ensuring the safety of new digital I&C technologies being incorporated into existing and new nuclear facilities. Specifically, the NRC regulates nuclear facility safety systems that use digital I&C technology through licensing and certification approvals of designs for both existing and new reactors, topical report approvals, inspection oversight, and regulation and guidance development.

The NRC has generally licensed operating nuclear power plants under a two-step process described in 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities” (Ref. 12). This process requires a construction permit and an operating license. In 1989, the NRC established alternative licensing processes in 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants” (Ref. 13), including a combined operating license (COL). This process combines a construction permit and an operating license with conditions for plant operation. A COL under 10 CFR Part 52 authorizes construction of the facility and specifies the inspections, tests, and analyses that the applicant must perform, including those for digital I&C safety systems. It also specifies acceptance criteria that are necessary to provide reasonable assurance that the facility has been constructed and will be operated in conformance with the license and applicable regulations. Evidence of meeting the acceptance criteria is documented by the licensee after the licensing decision. The NRC independently inspects vendors and licensees to confirm that selected analyses and tests are addressed appropriately.

The U.S. operating fleet of reactors also continues to implement several types of digital upgrades (including replacement of analog I&C equipment) without NRC approval under the requirements of 10 CFR 50.59 (Ref. 12). For this process, licensees are required to evaluate the effects of digital upgrades on the licensing basis of the plant with respect to potential adverse changes in the likelihood or consequence of existing malfunctions and accidents in the licensing basis. Generally, licensees can make such changes if there is not more than a minimal increase in the likelihood or consequences of malfunctions that can result in previously analyzed events, and their analysis reveals there are no new types of malfunctions or different results of those malfunctions created. The NRC recently issued guidance specific to digital I&C upgrades in Regulatory Issue Summary (RIS) 2002-22, Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” dated May 31, 2018 (Ref. 14), and in Regulatory Guide (RG) 1.187, “Guidance for Implementation of 10 CFR 50.59, ‘Changes, Tests, and Experiments,’” issued in 2021 (Ref. 15). The guidance, in part, focuses on addressing 10 CFR 50.59 criteria in consideration of (1) the existing I&C architectures that form the licensing bases of the plant and (2) potential new failure modes that could be introduced through implementation of the digital I&C. The NRC may elect to inspect selected digital upgrades for conformance to 10 CFR 50.59 and the quality assurance requirements in 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” as well as any other applicable regulatory requirements.

Evaluation Summary

EVALUATION OF KEY REGULATORY AND TECHNICAL THEMES

The NRC team systematically evaluated the findings and recommendations regarding various MCAS design, development, and regulatory oversight issues from three primary reports:

(1) "Official Report of the Special Committee to Review the Federal Aviation Administration's Aircraft Certification Process," issued 2020 (Ref. 2)

(2) Joint Authorities Technical Review, "Boeing 737 MAX Flight Control System: Observations, Findings, and Recommendations," issued 2019 (Ref. 1)

(3) National Transportation Safety Board, "Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance," issued 2019 (Ref. 16)

The NRC team also considered appropriate aspects from other authoritative reports, including the following:

- House Committee on Transportation & Infrastructure, "Final Committee Report: The Design, Development & Certification of the Boeing 737 Max," issued 2020 (Ref. 17)
- U.S. Department of Transportation, Office of Inspector General, "Timeline of Activities Leading to the Certification of the Boeing 737 MAX 8 Aircraft and Actions Taken After the October 2018 Lion Air Accident," issued 2020 (Ref. 11)
- U.S. Department of Transportation, Office of Inspector General, "Weaknesses in FAA's Certification and Delegation Processes Hindered Its Oversight of the 737 MAX 8," issued 2021 (Ref. 4)
- U.S. Senate Committee on Commerce, Science, & Transportation, "Committee Investigation Report: Aviation Safety Oversight," issued 2020 (Ref. 18)
- "Final KNKT.18.10.35.04 Aircraft Accident Investigation Report," issued 2019 (Ref. 3)

The NRC team assessed whether the findings and recommendations presented in these reports are pertinent to the NRC's digital I&C regulatory process. The NRC team identified two generic categories of findings that were relevant to the NRC's regulatory purview for digital I&C: (A) design and implementation issues and (B) regulatory oversight issues.

Within generic category (A), "Design and Implementation Issues," the NRC team defined the following themes for consideration: (1) design specifications and the application of defense-in-depth principles, (2) operational specifications, (3) safety assessment including hazard analysis and risk assessments, (4) equipment design and implementation, (5) performance monitoring, (6) production and certification, (7) training and operator procedure development, and (8) HFE.

For generic category (B), "Regulatory Oversight Issues," the NRC team identified the following themes for evaluation: (1) certification and licensing standards, (2) amended certification processes, (3) coordination among regulatory standards and certification bodies, (4) delegation of certification and post-certification design change processes, (5) regulating technical innovation, (6) personnel capabilities of the regulator, and (7) safety culture.

The NRC team evaluated the three primary reports in depth and, to the extent practical, aligned specific report findings to one or more of the themes using a matrixed approach. (The team's detailed review notes are documented separately.) The primary focus of the evaluation was to determine how well the NRC's I&C regulatory infrastructure may already address the recommendations discussed in the reports while identifying areas for potential improvement. This effort was challenging because the purpose and focus areas of each of the three reports were significantly different, as were the different responsibilities and charters of the respective organizations that investigated the crash events. The NRC team also adjusted the scope within each of the specific themes to accommodate unique insights that individual reports exposed.

The NRC team's assessment identified for consideration the following regulatory and technical themes and insights from these reports:

- Safety Assessment (including hazard analysis and risk assessments): One of the reports identified the need to understand what needs to go right (performance and design specifications), what could go wrong (human and equipment failure modes), what can prevent things from going wrong (controls and barriers), and the combination of events and scenarios in which the human-equipment system must function (Ref. 2).

  Such a recommendation is applicable to NRC approaches to addressing safety evaluations. NRC regulatory guidance documents (e.g., RG 1.174, dated 2018 (Ref. 19), NUREG-0800, Chapter 18 and its Attachment A (Ref. 20), NUREG-1764 (Ref. 21), NUREG-1852 (Ref. 22)) include an assessment of human performance issues when assessing plant safety margin for responses to identified events, particularly the considerations about human performance and human error. For example, hazard analysis techniques and probabilistic risk assessments consider combinations of equipment failures and operator errors. NRC regulatory guidance addresses criteria for licensing both new designs and changes to existing plant designs. During past digital I&C licensing reviews, technical experts in the disciplines of I&C, human factors, and safety systems coordinated on significant issues during key points of the licensing review. NRC vendor inspectors are involved in the review process on software development and quality assurance-related issues.

- Equipment Design and Implementation: One report identified the need for a safety management system to ensure a holistic, proactive assessment of whether the combination of design, procedures, and training will support effective safety performance (Ref. 2). Such a safety management system requirement for design and manufacturing organizations would help ensure a comprehensive, systematic approach to aviation safety from design to operation.

  The NRC has regulations (e.g., Appendix B to 10 CFR Part 50 (Ref. 12)) and guidance (e.g., RG 1.152, dated 2011 (Ref. 23)) for licensees to ensure a complete, systematic approach to safety from design to operation. For example, Criterion III, "Design Control," of Appendix B to 10 CFR Part 50 establishes quality assurance requirements for the design, manufacture, construction, and operation of structures, systems, and components. Furthermore, RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," provides guidance for complying with NRC regulations for promoting high functional reliability, design quality, and a secure development and operational environment for the use of digital computers in the safety systems of nuclear power plants. NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," issued November 2012 (Ref. 24), discusses integrated system validation, which is defined as "an evaluation, using performance-based tests, to determine whether an integrated system's design (i.e., hardware, software, and personnel elements) meets performance requirements and supports the plant's safe operation."

- Amended Certifications Process ("new designs on existing architectures"): One report discussed that while the FAA followed regulations and guidance for determining whether the Boeing design qualified for evaluation as an "amended type certificate," there is opportunity for regulatory improvement in areas

such as (1) understanding and documenting any assumptions related to pilot expectations for the performance of the modified design and whether there is a need for supplemental pilot training, (2) reviewing the cumulative effects of multiple changes to existing certified aircraft designs, and (3) providing a holistic system operational risk assessment and internal communication (Ref. 2).

The NRC has regulations for making changes without NRC approval and guidance for assessing the impact of a proposed I&C change on the existing approved licensing basis for the plant (e.g., 10 CFR 50.59 (Ref. 12)). For license amendment requests, design guidance and human factors guidance exist to ensure designs will achieve safety functions under assumed accident conditions, including an examination of diversity and defense in depth against potential software common-cause failures.

- Delegation of Certification: One report recommended that the FAA and airline industry work together to address potential pressure on an ODA unit to maintain their decision-making structure that operates without pressure or influence from other parts of the organization and ensure it serves as a representative of the FAA Administrator (Ref. 2).

  The NRC I&C regulatory infrastructure does not have a direct correlation to the ODA FAA program for certification. The NRC requires, in part, that each licensee have a quality assurance program for independent validation and verification activities for the digital I&C design, licensing, and operation, which is also subject to an independent NRC inspection. As discussed below, the NRC also cultivates and maintains a robust safety culture for its own employee organization and throughout the oversight of its licensee and applicant organizations.

- Safety Culture: One report (Ref. 1) recommended that "the FAA promote a safety culture that drives a primary focus on the creation of safe products, which in turn comply with certification requirements."

  The NRC defines nuclear safety culture as the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety over competing goals to ensure protection of people and the environment (Ref. 25). The implementation of a safety culture within the NRC involves a series of traits further defining a positive safety culture. These traits describe patterns of thinking, feeling, and behavior that emphasize safety, particularly in goal-conflict situations when safety goals conflict with production, schedule, or cost. Such positive safety culture fosters an environment where issues potentially impacting safety are promptly identified, fully evaluated, and addressed and corrected commensurate with their significance. This safety culture incorporates elements of enforcement to ensure the organizational focus is always on safety, and that no employee or contractor may be subject to discrimination or retaliatory actions if they raise questions about the achievement of safety. The NRC also applies the Principles of Good Regulation, which include "independence," meaning that all available facts and opinions must be sought openly from licensees and other interested members of the public (Ref. 26). As such, final decisions must be based on objective, unbiased assessments of relevant information and must be documented with reasons explicitly stated.

Regulatory Insights and Recommendations

The NRC team's evaluation resulted in a series of generic regulatory lessons and insights for consideration. This section highlights some key insights.

A. Design and Implementation Issues

- The NRC Glossary defines defense in depth as follows:

> An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures. (Ref. 27)

  A defense-in-depth approach continues to be an effective strategy to mitigate the risk resulting from uncertainties in safety margins associated with digital equipment and human performance, particularly when potential unknown and unforeseen failure mechanisms or phenomena exist. The NRC should continue to emphasize the need for applying a defense-in-depth approach to digital I&C and the overall design of a nuclear power plant. Such an approach includes (1) analyzing a proposed digital I&C system design to demonstrate that vulnerabilities to common mode failures have been adequately addressed, (2) examining a digital I&C system to identify hazards that have the potential to cause harm (e.g., radiological consequences, loss of life, damage to the environment), and (3) implementing I&C functional requirements and means to eliminate, prevent, or control those hazards.

- Systematic hazard analysis techniques may be important to address new digital technologies that are highly integrated in nature. The NRC is researching and evaluating options for performing a systematic hazard analysis for digital I&C systems. For example, the NRC intends to endorse Annex D, "Identification and Control of Hazards," of Institute of Electronics and Electrical Engineers (IEEE) Standard 7-4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations" (Ref. 28), to confirm it supports an adequate technical basis for endorsement as a new hazard analysis technique that can be employed by applicants and licensees.

  As discussed in one aircraft accident investigation report (Ref. 3), Boeing relied on a multidisciplinary team approach to choose the single and multiple failure analysis cases for the 737 MAX 8 program. Boeing excluded some cases from the analysis because their consequences were deemed to be bounded by others that were similar in nature. For example, Boeing considered including "Erroneous AOA from a single source" as a case in the analysis but ultimately abstained and, instead, identified other multiple failure conditions that presented, in its view, a more severe hazard to the aircraft (Ref. 3). Therefore, any hazard analysis guidance developed by the NRC should include, for example, guiding principles for adequately determining when analytical cases are worst case or bounding.

- Operating experience and related failure rate data are important for justifying reliability claims for digital designs and to ensure such claims remain valid during operation. Digital I&C licensing and inspection efforts that already consider operating experience include, but are not limited to, (1) RIS 2002-22, Supplement 1 (Ref. 14), (2) Branch Technical Position 7-19, Revision 8, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems," issued January 2021 (Ref. 29), and (3) RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water

Reactors", dated 2020 (Ref. 30). However, the NRC staff could benefit from an enhanced understanding of available digital I&C operating experience, allowing incorporation of quantitative assessments if possible, and the preparation of guidance for how to credit it when making reliability determinations for new digital systems, along with any associated limitations. This would also improve the long-term focus of NRC regulatory reviews and inspection activities related to (1) safety-related digital upgrades under 10 CFR 50.59, (2) new and advanced reactor applications, and (3) operating reactor license amendment requests.

Current operating experience available to digital I&C reviewers provides examples of how systems can fail but represents only a small fraction of all digital I&C failures. It does not offer any kind of an estimate of how likely a failure is, making quantitative assessment of proposed licensing actions challenging. Increased interaction between the operating experience staff and the I&C technical review group may allow for identification of additional data sources and facilitate coordination with risk analysts responsible for incorporating quantitative failure rate data into the overall risk assessment associated with these systems.

- Implementing modern systems engineering approaches to safety from conceptual design through operation, maintenance, and human factors evaluation is important for ensuring that an approved, validated, and delivered I&C design has the intended system functionality that is well understood by plant operators. NRC regulations and guidance include those associated with HFE-related considerations such as (1) the organization of human-system interfaces into workstations (including consoles and panels), (2) the arrangement of workstations and supporting equipment in facilities, such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility, and (3) the environmental conditions in which the human-system interfaces function, including temperature, humidity, ventilation, illumination, and noise. The NRC should continue to focus on HFE as a critical component of new digital designs. The NRC staff should continue to emphasize integrated technical teams to track and resolve digital design and HFE technical issues for safety-significant digital I&C reviews.

B. Regulatory Oversight Issues

- Coordination and communication during the digital design review, HFE review, and inspection oversight processes are critical to the digital design regulatory process. The NRC's I&C and HFE staff review digital designs by following a standard review plan and coordinate on common review areas during the license review. Independently, NRC vendor and regional inspectors may inspect design implementation, testing, and installation during and after the regulatory review. The insights emphasize the need to consider holistically the potential evolution of digital designs and associated assumptions from conception to installation within the fields of I&C and HFE.

- The NRC I&C and HFE technical disciplines should pursue even closer communication during the license review phase, challenging each other's assumptions in their respective review areas. The NRC digital I&C staff have also begun to engage NRC risk assessment specialists to provide insights on key licensing review issues within an integrated review strategy under LIC-206, "Integrated Risk-Informed Decision-Making for Licensing Reviews," issued 2019 (Ref. 31).

- The NRC intends to programmatically improve the communications, interactions, and hand-off of safety-important technical issues between licensing and inspection staff for large-scale digital modifications, especially under the new licensing process in Interim Staff Guidance (ISG)-06, Revision 2, "Digital Instrumentation and Controls Licensing Process," issued 2018 (Ref. 32). For example, licensing technical staff will continue to participate in inspection activities after licensing, and vendor inspectors will be invited to participate more directly in the licensing review process. The I&C technical review staff intends to clearly document recommended inspection items at the end of a major

digital licensing review and communicate with region-based inspectors during the testing and site installation of approved digital systems.

- Inspection priorities for digital I&C modifications made under 10 CFR 50.59 without NRC prior approval should be strategic and risk informed. Most digital modifications to nuclear power plants are performed under 10 CFR 50.59. The NRC is beginning a Smart Sample initiative for digital upgrades across the U.S. operating fleet to ensure inspection resources are focused on the most important upgrades based on risk insights and practical experience. For digital I&C, the Smart Sample will rely on insights and experience from vendor and regional inspectors and headquarters digital I&C staff. Inspectors will use the Smart Sample as guidance when inspecting a digital I&C component as part of normal baseline inspections. For the inspection of digital upgrades screened out under 10 CFR 50.59 (e.g., plant modifications that do not require a license amendment and thus may not receive the level of scrutiny that a licensing review would entail), the NRC staff should assess whether additional inspector training would be of use.

- The NRC should continue to focus on risk-significant digital systems, including evolving technologies with highly integrated digital systems. Specifically, staff licensing reviews should continue to follow a safety-focused approach to ensure agency resources are focused on safety-significant items. The NRC should also continue to apply its risk-informing principles based on compliance, defense in depth, safety margins, probabilistic risk assessment, and operational performance.

- An effective and forthright safety culture remains paramount and allows the agency to effectively fulfill its core regulatory and oversight mission to support the continued safe use of digital I&C in nuclear plants. The NRC should maintain a positive safety culture in our regulation of digital I&C, and NRC staff and management should continue to emphasize and demonstrate safety culture attributes and the NRC Principles of Good Regulation.

- NRC organizational capabilities and knowledge management activities should be enhanced to address long-term attrition of expert agency staff in the digital I&C disciplines.

- Sharing and considering digital technology information and insights with international and domestic regulators provides for a more robust safety program. NRC digital I&C staff should continue periodic seminars and exchanges with other regulators on digital I&C issues. The NRC should continue to participate in I&C domestic and international standard bodies.

Conclusion

Two Boeing 737 MAX aircraft crashes in 2018 and 2019 were the result of a series of engineering, programmatic, and safety culture failures and shortcomings related to MCAS design, implementation, and training. The NRC team found it challenging to make an in-depth technical comparison of the safety functions, failure consequences, defense in depth, and risks associated with the upgrade of an aircraft avionics system to those associated with a digital control safety system of a nuclear facility. In its evaluation of key recommendations from investigative reports about the aircraft accidents, the NRC team did not identify significant gaps in our regulatory infrastructure for digital I&C licensing and inspection. However, the NRC team identified several recommendations that are pertinent for consideration when future enhancements are made to the NRC's digital I&C regulatory evaluation program, regulatory oversight program, and staff organizational capabilities. Such enhancements would serve to ensure the continued safe use of evolving digital I&C technologies in regulated nuclear facilities.

Principal Contributors

- Ismael Garcia
- David Rahn
- Norbert Carte
- Dinesh Taneja
- Sergiu Basturescu
- Jeanne Johnston
- Michael Waters

Reviewers

- David Desaulniers
- David Beaulieu
- Sunil Weerakkody
- Steven Alferink
- Lisa Regner
- Rebecca Sigmon

Disclaimer

The NRC team acknowledges that in our evaluation of the detailed aspects of aircraft system development and the FAA certification processes that are pertinent to these events, we are not aircraft controls or certification experts. The reader should refer directly to the investigative reports and other sources for factual representations and interpretations of the technical and regulatory issues associated with the crash events.

In preparing this report, our goal was not to independently examine or judge Boeing's decision-making processes nor the FAA's regulatory decision-making, and we did not interview either organization. Rather, we based our evaluation on the findings noted in the cited investigative reports. Our assessment was intended to perform an inward evaluation of the NRC's own regulatory structure, tools, interfaces, and methods for licensing and inspection activities associated with the development and implementation of digital I&C technologies and the considerations that are made for human factors evaluation of such technologies.

Finally, it is important to remember that the two crash events caused the tragic loss of 346 lives. We have made a concerted effort to respect that loss of life while learning from the investigative reports to identify lessons that will help us in maintaining our safety mission in the adequate protection of public health and safety for nuclear facilities employing digital I&C technologies.

References

1. Joint Authorities Technical Review, “Boeing 737 MAX Flight Control System: Observations, Findings, and Recommendations,” 2019. https://www.faa.gov/sites/faa.gov/files/2021-08/Final_JATR_Submittal_to_FAA_Oct_2019.pdf

2. “Official Report of the Special Committee to Review the Federal Aviation Administration’s Aircraft Certification Process,” 2020. https://www.transportation.gov/briefing-room/official-report-special-committee-review-federal-aviation-administrations-aircraft-0

3. Komite Nasional Keselamatan Transportasi (KNKT), “Final KNKT.18.10.35.04 Aircraft Accident Investigation Report,” Republic of Indonesia, 2019. http://docs.house.gov/meetings/PW/PW00/20191030/110066/HHRG-116-PW00-20191030-SD002.pdf

4. U.S. Department of Transportation, Office of Inspector General, “Weaknesses in FAA’s Certification and Delegation Processes Hindered Its Oversight of the 737 MAX 8,” 2021. https://www.oig.dot.gov/sites/default/files/FAA%20Certification%20of%20737%20MAX%20Boeing%20II%20Final%20Report%5E2-23-2021.pdf

5. U.S. NRC, “Approaches to Permitting the Use of Digital Instrumentation and Controls in Safety Applications: A Report for the House and Senate Committees on Appropriations.” 2018. https://www.nrc.gov/docs/ML1830/ML18309A327.pdf

6. *Code of Federal Regulations*, Title 14, “Aeronautics and Space,” Section 25.1309, “Equipment, systems, and installations.” https://www.govinfo.gov/app/details/CFR-1999-title14-vol1/CFR-1999-title14-vol1-sec25-1309

7. *Code of Federal Regulations*, Title 14, “Aeronautics and Space,” Part 21, “Certification Procedures for Products and Parts.” https://www.govinfo.gov/app/details/CFR-2011-title14-vol1/CFR-2011-title14-vol1-part21

8. Aerospace Industries Association, Aircraft Electronics Association, General Aviation Manufacturers Association, and Federal Aviation Administration, “The FAA and Industry Guide to Product Certification, Third Edition,” 2017. https://www.faa.gov/aircraft/air_cert/design_approvals/media/cpi_guide.pdf

9. *Code of Federal Regulations*, Title 14, “Aeronautics and Space,” Section 183.29, “Designated engineering representatives.” https://www.govinfo.gov/app/details/CFR-2011-title14-vol3/CFR-2011-title14-vol3-sec183-29

10. Federal Aviation Administration, Order 8100.8, “Designee Management Handbook,” 2011. https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentid/1019601

11. U.S. Department of Transportation, Office of Inspector General, “Timeline of Activities Leading to the Certification of the Boeing 737 MAX 8 Aircraft and Actions Taken After the October 2018 Lion Air Accident,” 2020. https://www.oig.dot.gov/library-item/37940

12. *Code of Federal Regulations*, Title 10, “Energy,” Part 50, “Domestic Licensing of Production and Utilization Facilities.” https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/index.html

13. *Code of Federal Regulations*, Title 10, "Energy," Part 52, "Licenses, Certification, and Approvals for Nuclear Power Plants." https://www.nrc.gov/reading-rm/doc-collections/cfr/part052/index.html

14. U.S. NRC, Regulatory Issue Summary 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems," 2018. https://www.nrc.gov/docs/ML1814/ML18143B633.pdf

15. U.S. NRC, Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, 'Changes, Tests, and Experiments,'" 2021. https://www.nrc.gov/docs/ML2110/ML21109A002.pdf

16. National Transportation Safety Board, "Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance," 2019. https://www.commerce.senate.gov/services/files/D5F47FAD-8DC6-479D-A53E-B727E80603BC

17. House Committee on Transportation & Infrastructure, "Final Committee Report: The Design, Development & Certification of the Boeing 737 Max," 2020. https://transportation.house.gov/committee-activity/boeing-737-max-investigation

18. U.S. Senate Committee on Commerce, Science, & Transportation, "Committee Investigation Report: Aviation Safety Oversight," 2020. https://www.commerce.senate.gov/2020/12/wicker-releases-committee-s-faa-investigation-report

19. U.S. NRC, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," 2018. https://www.nrc.gov/docs/ML1731/ML17317A256.pdf

20. U.S. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 18, "Human Factors Engineering," 2016. https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ch18/index.html

21. U.S. NRC, NUREG-1764, Revision 1, "Guidance for the Review of Changes to Human Actions," 2007. https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1764/

22. U.S. NRC, NUREG-1852, "Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire," 2007. https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1852/

23. U.S. NRC, Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," 2011. https://www.nrc.gov/docs/ML1028/ML102870022.pdf

24. U.S. NRC, NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," 2012. https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0711/index.html

25. U.S. NRC, "Final Safety Culture Policy Statement," *Federal Register,* Vol. 76, pp. 34773–34778, 2011.

26. U.S. NRC, "Principles of Good Regulation," 2014. https://www.nrc.gov/docs/ML1413/ML14135A076.pdf

27. U.S. NRC, Glossary, 2021. https://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html

28. Institute of Electrical and Electronics Engineers (IEEE), "IEEE 7-Std 4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," 2016. https://standards.ieee.org/standard/7-4_3_2-2016.html

29. U.S. NRC, Branch Technical Position 7-19, Revision 8, “Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems,” 2021. https://www.nrc.gov/docs/ML2033/ML20339A647.pdf

30. U.S. NRC, Regulatory Guide 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” 2020. https://www.nrc.gov/docs/ML2009/ML20091L698.pdf

31. U.S. NRC, LIC-206, “Integrated Risk-Informed Decision-Making for Licensing Reviews,” 2019. https://www.nrc.gov/docs/ML1903/ML19031C861.pdf

32. U.S. NRC, DI&C-ISG-06, Revision 2, “Digital Instrumentation and Controls Licensing Process,” 2018. https://www.nrc.gov/docs/ML1826/ML18269A259.pdf

737 MAX Digital Lessons Learned Report DATE September 20, 2022

DISTRIBUTION:

ADAMS Accession No.: ML22241A037; Memo ML22241A039

OFFICE	NRR/DEX/ELTB	NRR/DEX/EEOB	NSIR/DPCP	NRR/DEX/EEOB
NAME	SBasturescu *SB*	DRahn *DR*	IGarcia *IG*	MWaters *MW*
DATE	Aug 30, 2022	Sep 14, 2022	Sep 13, 2022	Sep 14, 2022
OFFICE	NRR/DEX/EEOB	NRR/DEX/ELTB	NRR/DORL/LLPB	RES/DE/ICEEB
NAME	NCarte *NC*	DTaneja *DT*	JPaige MMcConnell for *MM*	CCook *CC*
DATE	Sep 14, 2022	Sep 14, 2022	Sep 15, 2022	Sep 20, 2022

OFFICIAL RECORD COPY