Licensing Process for Upgrading I&C Systems at Nonpower Production or Utilization Facilities (NPUFs)

D. A. Hardesty,* M. D. Muhlheim,† N. Carte,+ R. Alvarado,‡ P. G. Boyle,^ D. Warner,# and A. Adams@

*US Nuclear Regulatory Commission, Washington, DC, 20555, duane.hardesty@nrc.gov; +Norbert.Carte@nrc.gov; ‡Rossnyev.Alvarado@nrc.gov; ^Patrick.Boyle@nrc.gov; #Daniel.Warner@nrc.gov; @Alexander.Adams@nrc.gov

†Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, TN, 37831, muhlheimmd@ornl.gov

INTRODUCTION

Seventeen of the 31 currently licensed and operating Nonpower Production or Utilization Facilities (NPUFs) in the United States are currently upgrading or planning changes to their instrumentation and control (I&C) systems. Three have license amendment requests (LARs) under review by the US Nuclear Regulatory Commission (NRC) under Title 10 of the *Code of Federal Regulations*, Section 50.90 (10 CFR 50.90). Six are performing changes using "50.59" (i.e., 10 CFR 50.59), and eight are planning I&C systems changes or upgrades in the next 6 months. Under 10 CFR 50.59, the licensee is responsible for screening and evaluation of a proposed modification to be implemented without prior NRC approval. Under 10 CFR 50.90, the NRC staff evaluates the proposed modification to be implemented to assess compliance with the regulations and ensure public health and safety will be protected. The NRC staff encourages the use of public meetings *prior* to submittal of the LAR to reduce regulatory uncertainty and discussion of issues that may challenge the staff's ability to assess the systems compliance with NRC regulations.

NPUF Regulation

The NRC is committed to minimum regulation in the oversight of research reactors and testing facilities and welcomes opportunities to work with licensees to achieve this goal. NRC regulatory standards and the degree of scrutiny applied uses a graded approach in the regulatory review process informed by the safety significance of facility design and operation. This ensures that adequate public health and safety are maintained and that licensed activities comply with applicable regulations and are not inimical to the common defense and security.

Differences in Analog vs. Digital

Unlike the point-to-point wiring for analog control systems, a digital control system can communicate with numerous systems and components simultaneously. Digital modifications may also introduce software. Thus, digital I&C modifications may increase the potential likelihood of equipment failures by introducing new shared resources, hardware, or software among multiple functions (e.g., controllers, communication networks or video display units).

An important consideration when applying any digital/computer technology is to ensure that a malfunction (accidental or malicious) cannot prevent/block the safety system or operator from performing the required safety function (e.g., the technology cannot prevent the facility from achieving safe shut down). Another important consideration is to ensure that the operators have diverse means available for viewing the current values of essential operating parameters so that a malfunction cannot "blind" the operator. Attributes of digital I&C systems include independence (physical, electrical, and communications), redundancy, diversity, defense-in-depth, determinism, simplicity, and control of access.

I&C LICENSING PROCESS

The regulations in 10 CFR 50.59(c)(1) state that a licensee may make changes to its facility without requiring a licensing amendment if the change does not require a change to the technical specifications (TSs) or if the change does not meet any of the criteria in 10 CFR 50.59(c)(2). 10 CFR 50.59(c)(2) requires a licensee to obtain a license amendment pursuant to 10 CFR 50.90 prior to implementing a proposed change, test, or experiment if that change, test, or experiment would:

i. result in more than a minimal increase in the frequency of occurrence of an accident,
ii. increase in the likelihood of failure of structures, systems, or components (SSCs) to perform its intended function,
iii. increase in the consequences of an accident
iv. increase in the consequences of a failure of SSCs to perform its intended function,
v. create the possibility for an accident of a different type than any previously evaluated,
vi. create the possibility for a malfunction of an SSC important to safety with a different result,
vii. exceed or alter a design basis limit for a fission product barrier, or

viii. depart from a method of evaluation described in the safety analysis report (SAR) in establishing the safety analyses.

The licensee must answer "no" to all eight criteria for the proposed modification to be made under 10 CFR 50.59. Otherwise, the licensee will have to make changes to its facility under 10 CFR 50.90.

Changes under 10 CFR 50.59

The capability of a licensee may make changes under 10 CFR 50.59 depends upon factors such as the scope of the modification, the affected systems or components, and the conclusions of its 50.59 evaluation.

The analysis of the eight criteria in 10 CFR 50.59(c)(2) should be documented in sufficient detail, either by reference to a source document or by direct statements such that an independent third party could verify the conclusions.

Sufficient detail means that the licensee thoroughly understands the modification. For example, two multi-range linear power channels for a TRIGA reactor are being upgraded to new, digital-based General Atomics (GA) NMP-1000 replacement channels [1]. The new power channels are replacing the existing NMP-1000 power channels. According to GA [2], "[t]he current NMP-1000 architecture (ca. 2013) is very similar to all previous NMP units." Thus, because the old and new channels have the same model number, this appears to be a like-for-like replacement. However, the new NMP-1000s have a microprocessor and a liquid crystal display interface. Thus, the new GA NMP-1000 does not appear to meet the criteria for implementing the change using 10 CFR 50.59 and is undergoing a LAR review because of changes to the human-system interfaces (HSIs) and TSs.

In addition to determining eligibility to perform a proposed change under 10 CFR 50.59, the SAR for each facility should be updated for all 10 CFR 50.59 changes that impact the "facility as described."

Significant changes are pending for the 10 CFR 50.59 guidance for digital I&C, and licensees should stay current with these changes. Industry and Nuclear Energy Institute (NEI) are working on two documents to replace NEI 01-01 [3]—licensing guidance in Appendix D to NEI 96-07 [4] and technical guidance in NEI 16-16 [5]. New guidance for 10 CFR 50.59 reviews will likely include an interpretation of what qualifies as a *simple device* and will address concerns related to diversity and defense-in-depth, independence, as well as common-cause failures, embedded digital devices [6], software failures, and digital hardware failures.

Amendments per 10 CFR 50.90

Modifications that must be authorized by license amendment are evaluated and approved by NRC staff. Licensees indicate their intention to seek NRC approval of I&C upgrades by submitting a letter of intent. The LAR is docketed by the NRC and, if approved, the NRC staff prepares a written safety evaluation (SE) and issues a license amendment that authorizes the proposed modification. The LAR must contain sufficient detail for the NRC staff to understand the safety of the proposed I&C modification. Specifically, 10 CFR 50.90 states that whenever a Part 50 license holder desires to amend its license, the amendment application must fully describe the changes desired, and it must follow, as far as applicable, the form prescribed for original applications.

In order to approve the LAR, the NRC staff must be able to conclude that there is reasonable assurance that (1) health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with NRC regulations, and (3) issuance of the amendment will not be inimical to the common defense and security of the public.

The guidance provided in NUREG-1537, Format and Content (Part 1) and Acceptance Criteria (Part 2) ensures the quality and uniformity of the staff reviews, makes information about regulatory matters concerning NPUFs widely available, and improves the understanding of the staff review process by the NPUF community and the public. The document covers all aspects of licensing an NPUF. The document can be used for the construction permit and the initial operating license, license renewal, license amendment, decommissioning and license termination, and highly enriched to low-enriched uranium core conversions. Interim Staff Guidance (ISG) for Chapter 7 Parts 1 and 2 (full replacement) [7] is being implemented and updated based on lessons learned during implementation. Licensees use of the ISG is an acceptable method for meeting the requirements for an I&C modification. The draft ISG is being used to review the digital I&C system modifications at Massachusetts Institute of Technology (MIT), Purdue, and UMass-Lowell.

GUIDANCE FOR I&C UPGRADES

Provide a Complete Design with Supporting Documentation

Information is key to properly assessing changes to a facility under 10 CFR 50.59 or 10 CFR 50.90. The SAR provides the design bases, design criteria, and current system design implementation. The licensee must prepare a safety analysis with comprehensive supporting documentation for the modification based on all aspects of what is being modified. One licensee emphasized, based on experience, the need to become literate with the ISG (both Part 1 and Part 2) and to highlight or write down *any* questions early in the process [8].

A thorough understanding of the facility's accident analyses and knowledge of how failures of the affected system are going to impact that accident analysis need to be described and analyzed in sufficient detail. Information needed includes:

- initial conditions,
- initiating events,
- failure modes of the old equipment,
- expected failure modes for the new equipment,
- the impact of these assumed failures on the equipment and systems being controlled by the new equipment,
- limiting conditions, and
- postulated consequences.

This information is vital for comparing the new system to the old system to properly assess potential changes to the facility.

The design information should come from formal documentation on the new design or upgrades, such as the functional requirements specification (FRS), software requirements specification (SRS), hardware development specification, and the failure modes and effects analysis. Requirements traceability is essential because it maps the specification back to the requirements. Test results should demonstrate and document that the performance requirements related to the safety functions have been met. Testing performed should also trace back to specific system requirements.

Some changes may not only require revisions to the SAR or TS(s), but would also benefit from separate documents describing changes specific to the license request. Below are some helpful items to include in an application:

- A complete description of the change
- A safety analysis for what is being changed
- A copy of the revised SAR chapters, with change bars identifying changes related to the LAR
- Revised TS pages (if needed)
- Safety analysis conclusions, to be validated or confirmed by NRC staff

Modifications to I&C May Change TSs

NRC regulations require licensees to obtain a license amendment pursuant to 10 CFR 50.90 if the proposed modification would result in a change to TSs or if the proposed modification meets any of the criteria stated in 10 CFR 50.59(c)(2).

The TSs specify operating limits and conditions and other facility requirements. A TS may need to be changed or modified because of I&C system components being removed, a change to the minimum number of operable channels, analog testing is no longer appropriate or when there are new types of testing, new self-test features, or new or revised surveillance frequency. For example, changing to a digital system may add a watchdog timer, which in turn may be important enough to result in a TS-required scram.

New HSIs May Create New Malfunctions

New physical interactions with the HSI will require an examination of how the actual physical interface could impact performance of SAR-described design functions. For example, if a new malfunction is created as a result of the physical interaction, then the HSI portion of the digital modification would be deemed adverse and evaluated per 10 CFR 50.59. Examples of new physical interactions include:

- Use of touch screens in place of push-buttons, switches, or knobs;
- A new interface requiring the human user to choose which component is to be controlled;
- Changes to operating procedures;
- Information overload;
- Changes in how a parameter is displayed; and
- Changes in the data acquisition process.

SOME REVIEW EXAMPLES

Analog Recorder Screening

An analog recorder is to be replaced with a new microprocessor-based recorder. The recorder is used for various monitoring purposes, some of which are SAR-described design functions. The new digital recorder is highly dependable and has significant operating experience. Because the performance of its design function is unchanged, it might be assumed that the recorder would screen out of a 10 CFR 50.59 review. However, further analysis reveals that the sampling and recording frequency of the digital recorder are lower than that for the analog recorder, and the related recording function replaces instantaneous readings with time-averaged readings.

Accordingly, the replacement is deemed adverse, so a 10 CFR 50.59 evaluation would be required. Further evaluation of the new recorder would also include reviews of additional features such as networking interfaces, remote control capability, USB ports (intrusion protection), built-in or self-test diagnostics, environmental qualification (e.g., temperature, pressure, humidity), and electromagnetic compatibility to fully determine if the change can be made without prior NRC approval.

Control Rod Drive Replacement

The original control rod drive mechanism used a direct current motor with upper and lower limit switches and a series of potentiometers that provided rod position. Rod position was displayed on the control console. The new system uses a stepper motor with optical encoders for rod position, and it has a programmable logic controller interface with a touch screen display for rod selection.

For digital modifications such as this, the replacement would require a 10 CFR 50.59 evaluation. A qualitative assessment of the design process, relevant operating experience, and the system design features can be used to derive reasonable assurance of adequate quality and low likelihood of failure for the modification. The qualitative assessment considers an aggregate of factors such as system design features, the design process, and operating history.

Software Design Error

A reactor trip channel was designed to trip if a sensor was detected to be failed out of range. The trip channel uses primary and secondary sets of instruments and multiplexors. If the primary sensor signal is out of range, then the trip channel will switch to the secondary sensor. If the secondary sensor value is also out of range, the sensor reading reverts to the last-stored good value.

The design flaw is that a common-cause failure of all sensors of one type could result in continuous use of the last good value. This failure mode was discovered during a design review in which the online SRS did not match the FRS.

This failure is an example of a software design error. The SRS erroneously included the requirement for use of the last valid sensor data when a sensor fails, while the FRS required an automatic trip.

CONCLUSIONS/SUMMARY

For digital I&C changes being reviewed by the NRC or performed under 10 CFR 50.59, reasonable assurance of low likelihood of failure is derived from assessment of factors involving system design features, the quality of the design processes employed, and the operating history of the software and hardware used (i.e., product maturity and in-service experience). The assessment must result in a determination that there is reasonable assurance that the digital I&C modification will exhibit a low likelihood of failure by considering the aggregate of these factors. Additionally, the analysis must contain sufficient detail either by reference or by direct statements, such that an independent third party can verify the conclusions. If the licensee determines that the proposed modification cannot be performed under 10 CFR 50.59, the licensee can redesign the proposed modification so that it can be implemented without requiring a license amendment. In lieu of 10 CFR 50.59, a licensee can still pursue performing proposed modifications as a license amendment under 10 CFR 50.90.

Significant changes are pending for the 10 CFR 50.59 guidance for digital I&C, and licensees should stay current with these changes. Guidance is provided in the ISG for Chapter 7 for NUREG-1537 for LARs and new facilities.

REFERENCES

1. "UMass-Lowell Research Reactor (UMLRR) Safety Analysis Report Chapters 1–7," 2015.
2. L. BOBEK, UMass Lowell, "Digital Upgrade at UMass, Or: How I Learned to Stop Worrying and Love the Phase-0," NPUF Digital I&C Workshop, San Diego, September 2017.
3. Nuclear Energy Institute (NEI) 01-01, EPRI TR-102348, Revision 1, "Guideline on Licensing Digital Upgrades," March 8, 2002.
4. NEI 96-07, Appendix D, Draft Revision 0c. "Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications," May 2017. (ADAMS Accession No. ML17265A000).
5. NEI 16-16 Draft 2, "Guidance for Addressing Digital Common Cause Failure," May 2017. (ML17135A253).
6. RIS 2016-05, "Embedded Digital Devices in Safety-Related Systems," April 29, 2016. (ML15118A015).
7. "Draft Interim Staff Guidance (ISG) Augmenting Chapter 7 of NUREG-1537 Part 1 & Part 2," November 9, 2015. (ML15134A484 and ML15134A486).
8. C. TOWNSEND, "Digital I&C—A Licensing Survival Guide," NPUF Digital I&C Workshop, San Diego, September 2017.