

I&C Issues for New Nuclear Plant Deployment

Ray Torok, Joseph Naser, Layla Sandell
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94304

Tony Harris
Nuclear Energy Institute
1776 I Street, NW
Washington, D.C. 20006

KEYWORDS

Combined Construction & Operating License (COL), Risk-Informed Regulation, Defense-in-Depth and Diversity

ABSTRACT

The U.S. nuclear industry is making significant progress toward overcoming financial, regulatory, and technical barriers to deployment of new nuclear power plants. Progress toward overcoming financial barriers is being made by reducing the uncertainties around capital costs for new nuclear plants. The Energy Bill of 2005 offers key financial incentives for new nuclear power plant construction in three forms, including loan guarantees, production tax credits, and standby support—risk insurance to cover cost associated with delays that are beyond the control of plant sponsors. Regulatory barriers are being overcome with efforts to demonstrate the new plant licensing process. Four plant designs have been certified by the NRC, one design application is currently under review, and four other designs have been submitted for pre-application review. The NRC is also reviewing three utility Early Site Permit applications. Several individual utilities and consortia (groups of utility companies and vendors) are planning to submit Combined Construction & Operating License (COL) applications in 2007-2008, including consortia that have received DOE co-funding to demonstrate the licensing process. Technical barriers are being addressed by industry research including significant work managed by EPRI. Specifically, in the I&C area an industry initiative for new plants was recently started that will identify and prioritize large generic issues, establish resolution paths and schedules, and identify the roles of various stakeholders including utility companies, EPRI, NEI, vendors and the NRC. Through the course of this initiative we will address I&C issues for both existing and new plants. To begin, an industry workshop was held March 28-29, 2006. This paper describes key I&C related technical and regulatory issues and their implications for new plants, and provides a status report on the efforts to resolve them.

INTRODUCTION

There are several unsettled technical and licensing issues in the areas of instrumentation and control (I&C), human factors (HF), and control rooms that need coordinated, proactive industry attention. The issues are unsettled in the sense that there is limited guidance and no consensus among utilities, suppliers, and the NRC in regard to what solutions are technically appropriate and would be acceptable in regulatory space. Some of these issues are already causing protracted regulatory reviews for existing plants, and left untreated, they will likely cause substantial delays and increased costs for new plant combined construction and operating license (COL) approvals.

Both industry and the NRC will have roles in resolving the key issues and addressing them in future design efforts and regulatory reviews. Where needed, the industry will want to minimize costs and risks by defining industry consensus solutions, with corresponding technical bases. NEI is forming an industry working group to coordinate industry efforts and communications with NRC staff. The working group will also help determine priorities and coordinate both new and existing plant resources. EPRI will be represented on the working group. In order to be able to conduct reviews in a timely fashion, the NRC will likely need to enhance and expand staff resources as existing plants are upgraded and new plant reviews become more active.

It is estimated that nine or more combined license applications may be submitted to the NRC in FY2007 and FY 2008. If new plants are to be successfully licensed in a timely, cost-effective manner, the industry and the NRC need to move forward now to develop effective, generic solutions that can be applied before individual plant COL applications are submitted.

The following sections explain the most prevalent issues and proposed resolution strategies, and describe the status of ongoing activities to address them.

I TECHNICAL AND REGULATORY ISSUES

The issues have been grouped in five categories to combine those that involve closely related technical disciplines and resolution approaches. For all the issues, additional industry and/or regulatory guidance is needed to establish a clear, common understanding in regard to what solutions are technically appropriate and would be acceptable in regulatory space. While the primary motivation for this paper was to look at issues that could delay new plant approvals, it is important to note that these same issues are also relevant for existing plant upgrades, and the technical and regulatory solutions for the two groups should be compatible, if not identical. To a great extent, these issues flag the need for an overall shift from the analog I&C technology paradigm of existing plants, to the digital paradigm and design approaches that will characterize new plants.

A. Control Rooms and Digital Control System Architectures

New plants will use all or nearly all digital systems for control, communication and human-system interfaces (HSIs). As a result, they will face a number of issues for which there is limited technical guidance and regulatory precedent. Extensive upgrades to existing plants will test the same issues.

1. Licensing digital control rooms – New plants will all use highly digital control rooms, but none have been built and licensed in the United States, and the licensing issues, acceptance criteria and process are not well defined. For example, what minimum inventory of fixed position and continuously available indicators and controls is appropriate? What technical and regulatory requirements are appropriate for qualified HSIs for accident mitigation, display evaluation, soft controls, computerized procedures, automation, etc? What criteria should be applied to assure appropriate teamwork between operating crew members and between automation and operators? What types of verification and validation (V&V) are appropriate for human factors (HF) features, and how should their scope and rigor be graded based on complexity and/or safety significance and/or other criteria?
2. Licensing Distributed Control System (DCS) architectures – DCS-based plants have not been built and licensed in the United States, so specific, practical solutions for a number of digital technology concerns have not been developed in detail or reviewed and approved by the NRC, for example:
 - Separation of safety and non-safety systems – Digital systems often share information between channels and systems for purposes of data validation, control, calibration, data collection for condition monitoring, etc. Various software and hardware-based schemes are available for controlling such communication to preclude undesired impacts, but there is no guidance, consensus or precedent on requirements or acceptance criteria for such methods.
 - New communications technologies - New plants will likely use communications technologies and solutions that were developed and demonstrated in other industries or are still emerging/evolving, but have not been demonstrated or reviewed for nuclear applications. Examples are wireless, fieldbus and ethernet.
3. Failure management for new human-system interfaces (HSIs) – Practical criteria and methods are needed for addressing partial or large-scale failures of the HSIs normally used by the operators. This is especially applicable to new plant control rooms, which will be more integrated and digital than operating plant control rooms. Specific issues include appropriate operation under degraded I&C and HSI conditions, what backups should be provided, when to switch to backups, and the human factors engineering (HFE) issues associated with switching to backups, as well as integration of backups into the overall control room design.
4. Combined safety/non-safety HSIs - Use of a single HSI to interface with both safety and non-safety equipment is planned in some new plant designs, and technical solutions are being developed. However, these have not been licensed before and will have to address issues regarding protection of safety functions against hardware and software failures in non-safety equipment. This involves developing criteria for use of "priority logic" modules, which ensure that equipment that can respond to either safety or non-safety commands will always respond correctly to conflicting instructions, but will not become a single point of failure that can disable the safety function entirely.

B. Defense-in-Depth and Diversity, Including Risk-Informed Methods

The traditional safety model of a nuclear plant is based on a combination of diversity, separation of safety and non-safety equipment, and hardware redundancy. Digital technology brings both new concerns and new solutions. For example, it may be possible for a single software-related failure to

Copyright 2006 ISA. All rights reserved. www.isa.org

Presented at the 16th Annual Joint POWID/EPRI Controls and Instrumentation Conference
49th Annual ISA POWID Symposium, 4-9 June 2006, San Jose, California

disable multiple channels or systems (called software common-mode failure (CMF) or software common-cause failure (CCF) or digital common-cause failure). Conversely, digital equipment can provide much expanded flexibility in regard to functional diversity, but without using diverse hardware. This raises a need for guidance and acceptance criteria that more realistically reflect the behaviors and effects of the I&C and associated digital equipment relative to reliability and safety.

1. Defense-in-depth and diversity (D3) - With digital systems there is increased concern regarding the potential for digital common-cause failures, including software failures, to disable redundant safety channels or multiple systems that use identical programmable platforms or identical software modules. D3 evaluations are used to assess this issue for I&C modifications, or in the case of new plants, for entire I&C architectures. NRC guidance has been available for several years through the standard review plan (see BTP-19 [1] and NUREG/CR-6303 [2]). In practice however, the existing guidance is flawed; application to real systems has proven problematic, and the regulatory environment has been variable and unpredictable.
2. Application of risk-informed methods to I&C - Use of risk insights and risk-informed methods has been proposed by industry, but no approaches have been reviewed or accepted by NRC. Risk informed approaches would be particularly useful in D3 evaluation to determine where it makes sense to add backups to protect against potential software common-cause failure. EPRI has proposed an approach and submitted a guideline document to NRC for review [3]. However, in the current regulatory environment, use of a risk-informed approach or risk insights in D3 evaluation will require significant additional review time compared to that for a deterministic evaluation. (Note that some new plant D3 evaluations are PRA-based.) In a November 4, 2005 presentation to ACRS, NRC Engineering Research Application Branch noted that “NRC does not yet have the needed technical basis to support” risk-informed reviews, and indicates that the needed basis might yet be some years in development. Having an accepted approach would help plants (and NRC) focus resources on the most safety-significant areas and facilitate timely reviews. Also, this issue will need some degree of resolution to establish a common understanding of the capabilities and limitations of plant PRA models in regard to digital I&C.

C. Cyber security

Cyber security has been identified as an important technical and regulatory issue [4], but requirements and acceptance criteria are not well defined, and practical solutions have not been widely discussed or approved in nuclear plants. Cyber security details and solutions, especially for advanced programmable I&C and communication systems, have not been proposed or examined by NRC, and there is no consensus on what is needed or what would be accepted – the desired use of wireless technology adds another dimension to this.

D. Credit for Self Testing / Monitoring in Technical Specifications

This issue is about reducing technical specification (TS) surveillance requirements (SR) based on digital technology advances such as self-testing. Current TSs, including those submitted by Westinghouse and GE in their new plant design certifications, are based on analog systems. As a result, traditional SRs were applied. A technical basis needs to be developed for both new and existing plants that will capture technical advancements with digital technology such that significant reductions in SRs (e.g., channel checks, functional testing and calibration) may be justifiable.

E. Emerging technologies

Some designers are looking at use of technologies new to the nuclear industry, such as field programmable gate arrays (FPGAs) or application specific integrated circuits (ASICs). While providing the same functional benefits as solutions based on programmable logic controllers (PLCs), these technologies could also provide cost-effective solutions for complexity, cyber security and rapid obsolescence concerns. However, no industry guidance on requirements or acceptance criteria for use in safety applications currently exists, and NRC research to develop such guidance is years off. Therefore, use of emerging technologies such as ASICs or FPGAs in safety related applications has the potential to greatly extend the review time for both new and existing plant applications. In some cases, work by NRC Research may be needed to develop appropriate acceptance criteria. Licensees may need to plan at least 2 years in advance to have discussions with NRC staff on approaches that involve new or emerging technologies. What constitutes “new” for this purpose should probably be treated quite broadly, and include not just state-of-the-art technology, but anything that has not been previously reviewed, for example, a first of a kind architecture or new way of using a previously reviewed digital platform.

II RESOLUTION APPROACHES

All the issues described above share characteristics that suggest certain commonalities in the resolution approaches. First, they all concern industry-wide, generic regulatory issues that affect both new and operating plants. This is why the Nuclear Energy Institute (NEI) will take a lead role in its capacity as the unified industry voice for regulatory issues. NEI already has the mechanisms in place to provide the necessary guidance and oversight through their working group/task force processes.

Second, all the issues involve problems with limited or deficient technical basis and/or regulatory guidance information, with the corresponding potential for protracted, unpredictable regulatory reviews. Therefore, the resolution approaches should focus on establishing the needed guidance in the appropriate forums as expeditiously as possible. Several document types are routinely used to provide the kinds of generic (independent of plant design type) guidance that are needed:

- NRC publications, such as regulatory guides, branch technical positions (BTPs), and NUREG/CR reports, are for guidance, not regulation, but they provide useful information on NRC staff positions (at least as of the date of publication) as to how technical and regulatory issues might be approached by licensees, such that an NRC review would yield a positive outcome. A draft regulatory guide (DG-1145 [5]), addressing new plant COL application issues, is currently in progress. DG-1145 and the resulting regulatory guide will play an important role in addressing several of the issues described in this paper. However, the COL/FSAR guidance in itself, will not fully resolve the regulatory uncertainty problems. It needs to be supplemented by the other types of guidance documents.
- The Standard Review Plan (SRP, NUREG 0800 [6]) is published by NRC to provide guidance to their inspectors. It helps inspectors know what to look for in their reviews, but is not a good tool for licensee engineers working on system designs to apply directly. The SRP is updated periodically, but because of the rapid evolution of digital technology, the I&C sections are particularly difficult to keep up to date. Also, the SRP gives examples of processes and

approaches without regard to selecting the ones that are best for particular applications. (For example, it might list ten “required” design documents for a software development process, where a real implementation would use one or two documents to address the same set of concerns in a more usable, efficient framework. And for software development, SRP guidance is based on the “waterfall” process, which is now often viewed by experts as flawed and dated.) Many changes to the I&C sections of the SRP are planned in the next few years, and the changes may affect acceptance criteria that will be applied to new plants.

- Industry guidance documents, such as EPRI topical reports have been used on several occasions to provide guidance to utility engineers, and at the same time establish an industry consensus position for resolution of technical and/or regulatory issues, with appropriate technical bases. Examples relevant to digital I&C issues include the EPRI Digital Upgrade Licensing Guideline, published as NEI 01-01 [7], which addresses application of the 10 CFR 50.59 Rule to digital equipment, and the EPRI “COTS Guideline” on evaluation of commercial off-the-shelf digital equipment (EPRI TR-106439 [8]). Both were reviewed and endorsed by NRC, and the SRP steers readers to the COTS Guideline for guidance on this subject. Advantages of topical reports are that: they enable the industry to be proactive, rather than reactive; they can apply the latest information available; and, they can be developed and published far more quickly than the other types of guidance documents. Industry working groups can be used to guide the effort and ensure a consensus approach, and review cycles can be tailored and streamlined to fit the constraints of the situation. In some cases, EPRI topical reports have been used to provide the technical basis for positions adopted in industry standards.
- Industry standards from IEEE, ISA, ANS and others can also be used to establish industry consensus positions that can be reviewed and endorsed by NRC. In fact, NRC staff members participate on some of the committees that develop such standards. The standards approach has the advantages of a well-defined, systematic approval process, along with periodic reviews and updates. The principal disadvantage is that the development and approval process schedule is unpredictable and can take several years.

The industry should use all of these avenues to the best advantage in a coordinated plan to ensure that the cumulative guidance ultimately made available establishes the needed technical bases and common understandings to support predictable design and licensing efforts. The plan should utilize available resources and approaches to facilitate development of the needed guidance elements, for example:

- Facilitate near-term, detailed discussions between industry and NRC on the key technical issues, to help establish a clear, open dialog early and avoid protracted review cycles later.
- Use existing EPRI reports to derive/develop industry-consensus guidance and technical bases in the form of topical reports (applies in particular to human factors, control rooms, and D3 issues). Use EPRI/NEI/industry working groups to guide development of the topical reports. Where appropriate, involve NRC staff in working group meetings and submit final reports for NRC review and approval.
- Ensure that industry is represented in SRP update planning in regard to scope, priorities, and technical content for the relevant sections. Also provide feedback on SRP updates drafts as they become available.
- Support NRC workshops on DG-1145 in regard to guidance that will be needed for new plant submittals, including providing input on topics that should be addressed in the workshops. Activities should be tailored and supplemented for the specific issues as described below.

A. Control Rooms and Digital Control System Architectures

SRP and DG-1145 focus should be only on those sections that address I&C and human factors (SRP Chapter 7, DG-1145 Chapters 6 and 18). Industry topical reports should draw heavily from the 2005 EPRI publication on control room and HFE issues [9] to capture the latest information, save time and avoid duplication.

B. Defense-in-Depth and Diversity (D3), Including Risk-Informed Methods

In addition to the SRP and DG sections mentioned above, special focus should be given to the planned update of SRP Branch Technical Position HICB-19 (BTP-19), “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems” [1]. Industry topical reports should use or draw heavily from the 2004 EPRI publication on D3 for digital systems (EPRI 1002835 [3]), again to capture the latest information, save time and avoid duplication. Also, industry should pursue discussions with NRC Research in regard to its plans to develop guidance on applying risk-informed approaches to digital equipment.

C. Cyber security

Special focus should be given to the most recent version of Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants” [10], which reflects the most up to date NRC guidance on cyber security. If the regulatory guide position is judged to be inappropriate from the industry perspective, an industry topical report should be considered to present and justify an alternative approach. The industry approach should draw as appropriate from approaches used by other industries and organizations (INL, DOD, DHS, etc.). Coordination with and participation in standards committees and other groups addressing cyber security, e.g., IEEE 7-3.3.2 [11], NITSL, and NRC - Nuclear Security and Incident Response (NSIR) might also be needed.

D. Credit for Self Testing / Monitoring in Technical Specifications

This effort should coordinate with Tech Spec Task Force (TSTF), which is the existing industry mechanism for tech spec change. If appropriate, the industry consensus position should draw from existing EPRI guidelines that address on-line monitoring issues. Also, the new plant designers should be surveyed to see what they are planning in regard to self-testing.

E. Emerging technologies

This activity should utilize existing communication mechanisms to encourage early and frequent information exchange between industry and NRC, e.g.:

- The NEI New Plant Task Force could recommend additional vendor/licensee discussions with NRC staff to provide details about possible new technology concerns related to new plant designs and plans.
- NRC, through a regulatory issue summary (RIS), could explain the emerging technology concern and ask for licensee plans in advance, as appropriate.

- The latest NUREG/CR from NRC Research on Emerging I&C Technologies could be distributed broadly for industry input.
- I&C-related industry conferences and meetings coordinated by ISA, ANS, INPO, EPRI and others should be used to communicate the need for early discussions with NRC regarding new and emerging technology issues.

III CURRENT EFFORTS

On March 28-29, 2006, EPRI and NEI hosted an industry workshop on digital I&C and control room licensing issues in Washington, D.C. The workshop was well attended, with 56 participants representing operating plants, new plant consortia, equipment suppliers, NSSS suppliers, industry consultants, national labs, NEI, EPRI and NRC (I&C Branch in NRR, Research, Human Factors, and New Plants). The workshop objectives were to:

- Identify and prioritize unsettled technical and regulatory issues that need near term coordinated attention
- Identify and discuss candidate resolution strategies for each issue
- Agree on consensus direction for next steps
- Establish dialogue between utilities, vendors and regulators

The workshop was positive and productive and generated a set of high priority issues and resolution approaches, as described above. Formation of the NEI working group that will oversee industry activities is in progress.

Apart from the technical and regulatory issues of concern, a number of recurring themes arose regarding the practicalities of issue resolution:

- Resolution strategies will have to reflect a sense of urgency, especially with respect to new plants – in most cases; solutions are needed quickly to support COLA submittals, and cannot depend on multi-year research projects.
- NRC will likely be resource-limited when COL applications are submitted that could cause significant delays. Industry might help mitigate the problem through use of standardized design and submittal elements where practical, early communications with staff, etc.
- Better and more frequent technical communication between industry and staff will be essential to resolve issues in a timely fashion. This refers both to NRC activities to plan and develop updates to the standard review plan and guidance documents, and to industry activities to develop consensus approaches and technical bases for addressing key issues.
- Addressing issues generically where possible (unless it gives rise to unacceptable schedule impacts).
- Standardization in designs and submittals so that for most reviews, only new or different aspects need be addressed.

IV CONCLUSIONS

High priority issues and likely resolution strategies have been identified – stakeholders have been engaged and recognize the significance of quick resolution to avoid delaying regulatory approvals of

new plant COL applications. A great deal remains to be done in a relatively short time. Successful resolution of these issues will require a coordinated industry effort, with continuing cooperation and an unwavering sense of urgency from all parties.

V REFERENCES

1. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."
2. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.
3. "Guidelines for Performing Defense-In-Depth and Diversity Assessments for Digital Upgrades: Applying Risk Informed and Deterministic Methods", EPRI – 1002835, December 2004.
4. "Cyber Security Program for Power Reactors", NEI 04-04, February 2005.
5. Draft Regulatory Guide 1145, "Combined License Applications for Nuclear Power Plants," (in development).
6. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 7, Instrumentation and Controls."
7. "Guideline on Licensing Digital Upgrades TR-102348 Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule", EPRI 1002833, March 2002.
8. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", EPRI TR-106439, October 1996.
9. "Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance", EPRI – 1010042, December 2005.
10. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2, January 2006.
11. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."