

# 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 human-system interfaces (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 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 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 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
- 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.

# 5. Graded Approaches for HFE

Although human factors engineering (HFE) has been identified as an area that needs more technical and regulatory attention, use of graded approaches to human factors engineering analysis, and verification and validation (V&V) has not been tested in licensing space

Not using graded approaches is potentially a large cost contributor, and using them is an area of licensing risk.

## 6. 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 (BTP-19 and NUREG/CR-6303). In practice however, the existing guidance is flawed, application to real systems has proven problematic, and the regulatory environment has been variable and unpredictable.

# 7. 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. However, recent verbal statements from NRC Staff indicate that 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 (it has never been done, and the current NRR I&C Staff position is that it will not be approved). (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.

## 8. Modeling digital equipment in PRA

There is currently no consensus on how digital equipment could or should be modeled in PRA. Digital I&C technology will become the norm in both new plants and operating plants, so PRA models will have to include digital equipment. PRA models are already falling behind, as digital equipment is being installed in operating plants. Methods are needed for incorporating digital I&C in PRA models. NRC Research activities are in early scoping stages – results are likely several years away.

# 9. Cyber Security

Cyber security has been identified as an important technical and regulatory issue, but requirements and acceptance criteria are not well defined, and practical solutions have not been demonstrated 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.

# 10. Out of Date Review Criteria for Digital Equipment

Review criteria for digital systems are changing; NRC is in the process of updating several sections of Chapter 7 of the Standard Review Plan (SRP) and its associated branch technical positions (BTPs). As an example, the existing SRP guidance really does not adequately address "system integrity," and there are new approaches such as "defensive measures" that might be used to address these; however, they are as yet untested in licensing space.

# 11. Emerging Technologies

Some plants are looking at use of new technologies 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. 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.

# 12. Changing and Undocumented Regulatory Positions

Recent questions and comments from NRC staff suggest that previously established regulatory positions and guidance on key issues related to I&C modernization may be changed or reinterpreted or applied differently in the future. Until these changes and their technical bases are made clear and are well understood by licensees, it will be difficult for utilities to design new I&C systems without substantial technical, regulatory and schedule risks. This same concern applies to new plant design. Specific issues include:

- Defense-in-depth and diversity (D3) - In D3 evaluations for digital upgrades, current regulatory guidance in Branch Technical Position HICB-19 (BTP-19) indicates that a way to justify not adding diverse ESFAS actuation capability to protect against potential software common-cause failure during a large break LOCA is to credit existing leak detection capability. Recent verbal statements from NRC Staff indicate that this approach may no longer be considered acceptable, but no updated guidance has been issued.
- Separation/diversity of RPS and ESFAS - Recent verbal statements from NRC Staff suggest a new position is being adopted that reactor protection and ESFAS must be separate and/or diverse, apparently based on two guidance documents, BTP-19 and a NUREG/CR report (#6303) on performing diversity and defense-in-depth evaluations. Advanced digital system designs may use common, redundant processors for Reactor Protection and ESF actuation functions, which can provide improved reliability. A formal regulatory position and technical basis needs to be developed and vetted, with appropriate industry input.

# 12. Changing and Undocumented Regulatory Positions (cont)

- Inter-channel communications - Advanced digital system designs may use inter-channel communications to improve reliability. The NRC has informally taken issue with this design approach. A formal regulatory position and technical basis needs to be developed and vetted, with appropriate industry input.
- Reevaluation of approved platforms - Recent statements from NRC Staff indicate that they no longer consider existing NRC evaluations of selected digital control platforms adequate, and may revisit the evaluations and corresponding SERs, using different evaluation and acceptance criteria. All plant upgrades will involve substantial additional cost and schedule risk until this issue is resolved.
- New interpretation of common-cause failure criteria - Recent NRC comments on an EPRI guideline on defense-in-depth and diversity (D3) evaluation (EPRI 1002835) indicate that Staff might now consider common-cause failure (including software common-cause failure) a subset of single failure, based in part on IEEE-379, an established standard in the nuclear power industry. This position, if adopted, represents a significant departure from: previous interpretations of IEEE-379; earlier published NRC guidance on software common-cause failure; and precedents set by the designs used in existing U.S. nuclear plants.
- 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.

# 13. NRC Research Delays May Prevent Timely Resolution of Issues

NRC Research is planning work on several of the issues discussed in this paper in order to develop methods, requirements and acceptance criteria for use in future regulatory reviews (see Nov. 4, 2005 presentation to ACRS). However, in most cases, the results won't be available for several years. In the meantime, the NRR positions on key issues could remain unclear and changeable, resulting in unpredictable reviews and significant regulatory risk for utilities planning I&C upgrades or new plants. In some cases NRC is embarking on research that could lead to additional requirements for new plants and operating plants. Specific activities planned by NRC Research include:

- Modeling digital I&C in PRA – Various approaches for modeling digital equipment and assessing failure probabilities will be explored. Results that can be applied to operating plants or new plants are likely many years off .
- ASICs and FPGAs – Projects will develop assessment techniques for application specific integrated circuit (ASIC) and field programmable gate array (FPGA) based equipment. Note that some operating plants are planning to implement this technology in safety applications in the next few years.
- Advanced technologies for new plants - A need for investigation of new I&C technologies is anticipated for advanced reactor designs, e.g., autonomous controls, fully integrated (distributed control system) DCS, new instrumentation, robotics, knowledge-based and other computerized support systems, etc. However, nothing specific has yet been identified, and no research is in progress at this time. NRC expects plans to change based on pre-application reviews and COL applications. Any need for new research to support COL applications could have significant schedule impacts.

# 14. Configuration Management

---

# 15. Simulator Fidelity (for first unit)

---

# 16. NRC Resource Limitations

- Proposed resolution elements
  - Standardized submittals
  - More communication

# 17. Limited Communication Between Industry and Staff for Technical Issues

- Need to facilitate communication
  - Tech issues
  - Research plan